### [Network Security 1.0](https://lms.netacad.com/course/view.php?id=2137735" \l "section-1)

Tartalom:

### [1-4. modul: Hálózatok védelme](https://lms.netacad.com/course/view.php?id=2137735#section-3)

### [5-7. modul: Eszközök megfigyelése és kezelése](https://lms.netacad.com/course/view.php?id=2137735#section-4)

### [8–10. modul: ACL-ek és tűzfalak](https://lms.netacad.com/course/view.php?id=2137735#section-5)

### [13–14. modul: 2. réteg és végpontbiztonság](https://lms.netacad.com/course/view.php?id=2137735#section-7)

### [15-17. modul: Kriptográfia](https://lms.netacad.com/course/view.php?id=2137735#section-8)

### [18–19. modul: VPN-ek](https://lms.netacad.com/course/view.php?id=2137735#section-9)

### [20–22. modul: ASA](https://lms.netacad.com/course/view.php?id=2137735#section-10)

Első alkalommal ezen a tanfolyamon

Üdvözöljük a Hálózatbiztonság tanfolyamon. Ez a tanfolyam bemutatja a hálózati eszközök telepítéséhez, hibaelhárításához és felügyeletéhez szükséges alapvető biztonsági koncepciókat és készségeket a vállalati adatok integritásának, bizalmasságának és elérhetőségének megőrzése érdekében.

Ezek a tananyagok segítenek a következőkhöz szükséges készségek fejlesztésében:

Ismertesse a modern hálózati infrastruktúrákat fenyegető biztonsági fenyegetéseket.

Biztonságos Cisco eszközök.

Biztosítsa a hálózati infrastruktúrát.

Helyi útválasztó adatbázis és külső AAA-kiszolgálók használatával valósítsa meg az AAA-t Cisco útválasztókon.

A hozzáférés-vezérlési listák (ACL) segítségével mérsékelheti a Cisco útválasztókat és hálózatokat fenyegető veszélyeket.

Biztonságos hálózattervezés, -kezelés és -jelentés megvalósítása.

Valósítsa meg a Cisco IOS tűzfal szolgáltatáskészletét.

Csökkentse a gyakori Layer 2 támadásokat.

Helyezzen el egy helyek közötti VPN-t.

Távoli hozzáférésű VPN megvalósítása.

1.0.2

Hallgatói források

Számos eszköz és erőforrás áll az Ön rendelkezésére, amelyek segítséget nyújtanak a hálózatbiztonsági készségeinek fejlesztéséhez és a munkalehetőségekre való felkészüléshez.

Packet Tracer

A Packet Tracer a hálózat belső működését szimulálja, és ebben a kurzusban használatos. Töltse le és telepítse a Packet Tracer legújabb verzióját itt: Packet Tracer Resources.

Ha még nem ismeri a Packet Tracer alkalmazást, vegyen részt most ezen az INGYENES, rövid online tanfolyamon: Bevezetés a Packet Tracer tanfolyamba.

Használhatja okostelefonját, táblagépét vagy számítógépét a kurzus eléréséhez; mindazonáltal a Packet Tracer tevékenységeket, valamint néhány más tevékenységet, vetélkedőt és vizsgát a legjobban számítógép használatával lehet megtapasztalni.

Csatlakozz közösségeinkhez

Lépjen kapcsolatba más Hálózati Akadémia hallgatóival, és kérjen segítséget a világ minden tájáról a Cisco Networking Academy Facebook-oldalán.

Kapcsolatba léphet társaival a Cisco Networking Academy LinkedIn oldalán.

Munkát szerezni!

Hozzáférés a Career Resources-hoz, amelyet kifejezetten arra szabtak, hogy a NetAcad-hallgatók sikeresek legyenek a munkahelyen.

Keressen nagyszerű munkalehetőségeket a Cisco és a Cisco partnereinél. Regisztráljon most a Talent Bridge-en.

Az iparági minősítés megszerzése garancia a munkáltatók számára, hogy rendelkezik a munka elvégzéséhez szükséges műszaki ismeretekkel. Tekintse meg Tanúsítványok és utalványok oldalunkat.

További tanfolyamok

Válassz egy tanfolyamot, gyakorold a tanultakat, és válj informatikussá. Tekintse meg kurzuskatalógusunkat.

1.0.3

Etikai hackelési nyilatkozat

A Cisco Hálózati Akadémia program célja a globális problémamegoldók létrehozása, amelyek szükségesek a vállalkozásunkban és mindennapi életünkben használt hálózatok kiépítéséhez, méretezéséhez, biztonságossá tételéhez és védelméhez. A jól képzett hálózatbiztonsági szakemberek iránti igény továbbra is exponenciálisan növekszik. A hálózatbiztonsági szakemberré való képzéshez mélyreható ismerete szükséges a hálózati támadások előfordulásának, valamint azok észlelésének és megelőzésének módjáról. Ezek a készségek természetesen magukban foglalják azon technikák megismerését is, amelyeket a fenyegetés szereplői a számítógép- és hálózatbiztonság megkerülésére használnak.

Az adatokhoz, számítógépekhez és hálózati rendszerekhez való jogosulatlan hozzáférés számos joghatóságban bűncselekmény, és gyakran súlyos következményekkel jár, függetlenül az elkövető motivációjától. A tanuló, mint az anyag felhasználója felelőssége, hogy ismerje és betartsa a számítógéphasználati törvényeket.

1.0.4

Befogadó nyelv

A Cisco Networking Academy célja egy befogadó jövő megteremtése mindenki számára. Mivel minden tevékenységünk középpontjában a mi célunk áll, számíthat arra, hogy a Cisco merész, bátor és megfontolt lesz a szerepünk és a társadalmi igazságosság támogatása érdekében tett lépéseink tekintetében.

Büszkék vagyunk arra, hogy csatlakozhatunk a technológiai közösséghez az általunk használt nyelv fejlesztésében. Az általunk használt szavak újragondolása csak az egyik módja annak, hogy csökkentsük a méltányosság és tisztelet előtt álló akadályokat. Az irányelvek értelmében a Cisco Networking Academy tartalmának mentesnek kell lennie a sértő vagy sugalmazó nyelvezettől, grafikáktól és forgatókönyvektől. A feltételeket az alábbiakban leírtak szerint megfelelőbb alternatívákra változtatjuk.

Kifejezés/kifejezés

Csere

mesterszolga

elsődleges/másodlagos VAGY

elsődleges/alárendelt VAGY

vezérlés/adatok (klaszterezéshez)

fehérlista/feketelista

engedély (lista)/blokk (lista) VAGY

engedélyezés (lista)/blokkolás (lista)

A kurzus tantervében továbbra is megjelenhetnek olyan iparági kifejezések, mint a „fekete kalap”. Csapatunk ezen feltételek módosításán is dolgozik.

1.0.5

Videó - Töltse le és telepítse a Packet Tracer programot

Ez a videó bemutatja a Packet Tracer letöltését és telepítését. A Packet Tracer segítségével szimulálja a hálózatok létrehozását és tesztelését a számítógépén. A Packet Tracer egy szórakoztató, otthonra vihető, rugalmas szoftverprogram, amely lehetőséget ad a nemrég megtanult hálózati reprezentációk és elméletek felhasználására hálózati modellek felépítéséhez, valamint viszonylag összetett LAN-ok és WAN-ok felfedezéséhez.

A diákok általában a Packet Tracer-t használják a következőkre:

Készüljön fel a minősítő vizsgára.

Gyakorold a hálózati tanfolyamokon tanultakat.

Feszítse tudásukat egy állásinterjún.

Vizsgálja meg az új te hozzáadásának hatását

1.1.1

A hálózatok célpontok

A hálózatokat rendszeresen támadások érik. Gyakori, hogy a hírekben egy újabb hálózatról olvashatunk, amely kompromittálódott. A hálózati támadások gyors internetes keresése számos cikket ad vissza a hálózati támadásokról, amelyek a feltört szervezetekről szóló híreket, a hálózati biztonságot fenyegető legújabb fenyegetéseket, a szolgáló eszközöket és még sok mást.

A helyzet súlyosságának megértése érdekében a Kapersky fenntartja az aktuális hálózati támadások interaktív Cyberthreat valós idejű térképét. A támadási a Kapersky hálózatbiztonsági termékeiből származnak, minden adatok telepítésére. Az ábra egy minta képernyőképet jelenít meg a webes eszközről, amely valós időben mutatja be ezeket a támadásokat. Számos hasonló eszköz elérhető az interneten, és a kiberfenyegetések térképére keresve is megtalálhatók.

Az ábra a Kaspersky interaktív Cyberthreat valós idejű térképét mutatja az aktuális hálózati támadásokról

1.1.2

A hálózatbiztonság rendben

A hálózati biztonság közvetlenül kapcsolódik a szervezet üzletmenet-folytonosságához. A hálózati biztonság megsértése megzavarhatja az e-kereskedelmet, üzleti adatok elvesztését okozhatja, veszélyeztetheti az emberek magánéletét, és veszélyeztetheti az információk integritását. Ezek a jogsértések a vállalatok bevételkiesését, a szellemi eltulajdonítást, pereket, sőt a közbiztonságot is veszélyeztethetik.

A biztonságos hálózat fenntartása biztosítja a hálózati felhasználók biztonságát és védi a kereskedelmi érdekeket. A hálózat biztonságának megőrzése éberséget igényel a szervezet hálózatbiztonsági szakembereitől. Folyamatos tisztában kell lenniük a hálózatokat erő új és fejlődő fenyegetésekkel és támadásokkal, valamint az eszközök és alkalmazások sebezhetőségeivel.

Számos eszköz áll rendelkezésre a hálózati rendszergazdáknak a fenyegetéscsökkentési technikák alkalmazásában, fejlesztésében és megvalósításában. Például az ábrán látható Cisco Talos Intelligence Group átfogó biztonsági és fenyegetési ajánlata az védelmében és vagyonuk védelmében.

Az ábra a Cisco Talos Intelligence Groupét mutatja

Egy másik csoport, a Cisco Product Security Incident Response Team (PSIRT) a Cisco termékek potenciális sebezhetőségeinek kivizsgálásáért és enyhítéséért felelős. Az ábra egy minta Cisco Security Advisories oldalt jelenít meg, amely valós időben felsorolja a biztonsági réseket, és tájékoztatást nyújt a hálózati rendszergazdáknak azok enyhítésére.

Az ábra egy minta Cisco Security Advisories oldalt jelenít meg

1.1.3

Hálózati támadások vektorai

A támadási vektor egy olyan útvonal, amelyen keresztül a fenyegetés szereplői hozzáférhetnek egy szerverhez, gazdagéphez vagy hálózathoz. A támadási vektorok a vállalati hálózaton belülről vagy kívülről származnak, amint az az ábrán látható. A fenyegetés szereplői például célba vehetnek egy hálózatot az interneten keresztül, hogy megzavarják a hálózati műveleteket, és szolgáltatásmegtagadási (DoS) támadást indítsanak el.

Az ábra a hálózatot mutatja egy szerverrel és több gazdagéppel a tűzfal mögött; a hálózaton lévő gazdagép feltört; a nyilak azt mutatják, hogy külső fenyegetés lehetett az internetről a tűzfalon keresztül, vagy belső fenyegetés a hálózat egy másik gazdagépétől

Külső és belső veszélyek

InternetExternal ThreatCompromised HostInternal Threat

Megjegyzés: DoS támadás akkor fordul elő, amikor egy hálózati eszköz vagy alkalmazás működésképtelenné válik, és már nem képes támogatni a jogos felhasználóktól érkező kéréseket.

Egy belső felhasználó, például egy alkalmazott, véletlenül vagy szándékosan:

Ellophatja és másolhatja a bizalmas adatokat cserélhető adathordozókra, e-mailekre, üzenetküldő szoftverekre és egyéb adathordozókra.

Kompromittálja a belső szervereket vagy hálózati infrastruktúra-eszközöket.

Szüntesse meg a kritikus hálózati kapcsolatot, és okozzon hálózati leállást.

Csatlakoztasson egy fertőzött USB-meghajtót a vállalati számítógépes rendszerhez.

A belső fenyegetések nagyobb károkat okozhatnak, mint a külső fenyegetések, mivel a belső felhasználók közvetlenül hozzáférhetnek az épülethez és annak infrastrukturális eszközeihez. Az alkalmazottak ismerhetik a vállalati hálózatot, annak erőforrásait és bizalmas adatait is.

A hálózatbiztonsági szakembereknek eszközöket és technikákat kell alkalmazniuk a külső és belső fenyegetések mérséklésére.

1.1.4

Adatvesztés

Az adatok valószínűleg a szervezet legértékesebb eszközei. A szervezeti adatok közé tartozhatnak a kutatási és fejlesztési adatok, az értékesítési adatok, a pénzügyi adatok, a humánerőforrás- és jogi adatok, a munkavállalói adatok, a vállalkozói adatok és az ügyfelek adatai.

Adatvesztésről vagy adatszivárgásról beszélünk, amikor az adatok szándékosan vagy akaratlanul elvesznek, ellopják vagy kiszivárogtatják a külvilágba. Az adatvesztés a következőket okozhatja:

A márka károsodása és a hírnév elvesztése

Versenyelőny elvesztése

Ügyfelek elvesztése

Bevételkiesés

Perek/jogi lépések, amelyek pénzbírságot és polgári jogi szankciót vonnak maguk után

Jelentős költségek és intézkedések az érintett felek értesítésére és a jogsértés utáni helyreállításra

A hálózatbiztonsági szakembereknek meg kell védeniük a szervezet adatait. Különféle adatvesztés-megelőzési (DLP) vezérlőket kell megvalósítani, amelyek egyesítik a stratégiát, operatív és taktikai kezelést.

Az általános adatvesztési vektorok a táblázatban jelennek meg.

E-mail/közösségi hálózat

Az adatvesztés gyakoribb vektora az azonnali üzenető szoftver és a közösségi oldalak. Például az elfogott e-mailek vagy azonnali rögzítések, és bizalmas üzenetek fedhetnek fel.

Titkosítatlan eszközök

Az ellopott vállalati laptopok jellemzően bizalmas szervezeti adatokat tartalmaznak. Ha az adatokat nem titkosítási algoritmussal tárolják, akkor a tolvaj értékes bizalmas adatokat nyerhet vissza.

Felhőalapú tárolóeszközök

Az adatok felhőbe mentése számos lehetséges előnnyel jár. Az érzékeny adatok azonban elveszhetnek, ha a felhőhöz való hozzáférés a gyenge biztonsági beállítás miatt veszélybe kerül.

Cserélhető adathordozó

Az egyik kockázat az, hogy egy alkalmazott jogosulatlan adatátvitelt hajthat végre egy USB-meghajtóra. Egy másik kockázat, hogy az értékes vállalati adatokat tartalmazó USB-meghajtó elveszhet.

Papíralapú

A vállalati alaposan meg kell semmisíteni. Például a bizalmas adatokat fel kell aprítani, amikor már nincs rájuk szükség. Ellenkező esetben a tolvaj visszakeresheti az eldobott jelentéseket, és értékes információkhoz juthat.

Nem megfelelő hozzáférés-szabályozás

A jelszavak jelentik az első védelmi vonalat. Az ellopott jelszavak vagy a feltört gyenge jelszavak könnyű hozzáférést biztosíthatnak a támadónak a vállalati adatokhoz.

1.2.1

Campus Area Networks

Minden hálózat célpont. Ennek a kurzusnak a fő hangsúlya azonban a Campus Area Networks (CAN-ok) biztosítására irányul. A Campus Area Networks korlátozott földrajzi területen belül kapcsolódik LAN-okból áll.

A hálózati szakembereknek különféle hálózati biztonsági technikákat kell alkalmazni, hogy megvédjék a szervezet eszközeit a külső és belső fenyegetésektől. A nem megbízható hálózatokhoz fűződő kapcsolatokat több védelmi rétegnek is alaposan meg kell vizsgálnia, hogy elérje a vállalati erőforrásokat. Ezt mélyreható védekezésnek nevezik.

Az ábra egy minta CAN-t mutat be mélyreható védelmi megközelítéssel, amely különféle biztonsági funkciókat és biztonsági eszközöket használ annak biztosítására. A táblázat magyarázatot ad a mélyreható védelmi tervezés azon elemeiről, amelyek az ábrán láthatók.

Az ábra egy példát mutat egy Campus Area Networkre, amely a biztonság mélyreható megközelítését alkalmazza.

Campus Area NetworkInternetAAA szerverASA tűzfalIPSVPN2. rétegű kapcsolókWeb szerverDHCP szerverESA/WSAOtthont adE-mail szerver3. rétegű kapcsolók

VPN

Egy Cisco ISR védett. Virtuális magánhálózatok (VPN) létrehozásával védi a mozgásban lévő adatokat, amelyek a CAN-ból a külvilág felé áramlanak. A VPN-ek biztosítják a hitelesített forrásokból származó adatok bizalmas kezelését és integritását.

ASA tűzfal

A Cisco Adaptive Security Appliance (ASA) tűzfal állapotjelző csomagszűrést hajt végre, hogy kiszűrje a visszatérő forgalmat a külső hálózatról az egyetemi hálózatról.

IPS

A Cisco Intrusion Prevention System (IPS) folyamatosan figyeli a bejövő és kimenő hálózati forgalmat a rosszindulatú tevékenységek szempontjából. Adatokat naplóz a tevékenységről, és megpróbálja blokkolni és jelenteni.

3. rétegű kapcsolók

Ezek az elosztási réteg kapcsolói védettek, és biztonságos redundáns fővonali kapcsolatokat biztosítanak a 2. rétegbeli kapcsolókhoz. Számos különböző biztonsági funkció implementálható, mint például az ACL-ek, a DHCP-snooping, a Dynamic ARP Inspection (DAI) és az IP-forrásvédelem.

2. rétegű kapcsolók

Ezek a hozzáférési réteg kapcsolói védettek, és a felhasználó felé néző port csatlakoztatják a hálózathoz. Számos különböző biztonsági funkció implementálható, mint például a portbiztonság, a DHCP-snooping és a 802.1X felhasználói hitelesítés.

ESA/WSA

A Cisco Email Security Appliance (ESA) és a Web Security Appliance (WSA) fejlett fenyegetések elleni védelme, az alkalmazások láthatóságát és vezérlését, jelentéskészítését és biztonságos mobilitást biztosít az e-mailek és a webes forgalom biztonságának és vezérlésének érdekében.

AAA szerver

A hitelesítési, engedélyezési és könyvelési (AAA) szerver hitelesíti a felhasználókat, engedélyezi, mit tehetnek, és nyomon követi, hogy mit csinálnak.

Otthont ad

A végpontokat különféle szolgáltatások biztosítják, beleértve a vírus- és kártevőirtó szoftvereket, a Host Intrusion Protection System szolgáltatásait és a 802.1X hitelesítési funkciókat.

1.2.2

Kis irodai és otthoni irodai hálózatok

Fontos, hogy minden hálózat védett legyen, mérettől független. A támadók érdeklődnek az otthoni hálózatok és a kis irodai és otthoni irodai (SOHO) hálózatok iránt is. Előfordulhat, ingyenesen használhatják valakit, illegális tevékenységre az internetkapcsolatot, vagy megtekinthetik a pénzügyi tranzakciókat, például online vásárlásokat.

Az otthoni és SOHO hálózatokat általában fogyasztói minőségű router védi. Ezek az útválasztók alapvető biztonsági funkciókat kínálnak, amelyek megfelelően megvédik a belső eszközöket a külső támadóktól.

Az ábrán egy SOHO minta látható, amely fogyasztói minőségű vezeték nélküli útválasztót használ annak biztosítására. A fogyasztói minőségű vezeték nélküli útválasztó integrált tűzfalfunkciókat és biztonságos vezeték nélküli kapcsolatokat kínál. A Layer 2 Switch egy hozzáférési réteg kapcsoló, amely különféle biztonsági intézkedésekkel van megerősítve. A portbiztonságot használó, felhasználó felé néző portokat csatlakoztatja a SOHO hálózathoz. A vezeték nélküli gazdagépek a Wireless Protected Access 2 (WPA2) adattitkosítási technológiával csatlakoznak a vezeték nélküli hálózathoz. A gazdagépeken általában vírus- és kártevőirtó szoftverek vannak telepítve. Ezek a biztonsági intézkedések együttesen átfogó védelmet nyújtanak a hálózat különböző szintjein.

Az ábra egy Small Office Home Office topológiát és annak biztosításának módjait mutatja.

SOHO hálózatInternetVezeték nélküli router2. rétegkapcsolóVezeték nélküli gazdagép

1.2.3

Nagy kiterjedésű hálózatok

A nagy kiterjedésű hálózatok (WAN-ok), amint az az ábrán látható, széles földrajzi területet ölelnek fel, gyakran a nyilvános interneten keresztül. A szervezeteknek biztosítaniuk kell a mozgó adatok biztonságos szállítását, amikor azok a nyilvános hálózaton keresztül telephelyek között haladnak.

A hálózatbiztonsági szakembereknek biztonságos eszközöket kell használniuk a hálózat szélén. Az ábrán a fő helyet egy ASA védi, amely állapotalapú tűzfal funkciókat biztosít, és biztonságos VPN-alagutakat hoz létre a különböző célpontokhoz.

Az ábra egy nagy kiterjedésű hálózatot és annak biztosításának módjait mutatja.

Mobil työntekijäVPNFióktelepRegionális oldalSOHO sajátTársaságiCisco ASA tűzfalFőoldalPOP

Az ábrán egy fióktelep, egy regionális telephely, egy SOHO telephely és egy mobil munkatárs látható. Egy fióktelep csatlakozik a vállalati fő telephelyhez keményített ISR segítségével. Az ISR állandó, mindig bekapcsolt VPN-kapcsolatot tud létrehozni a fő helyszíni ASA tűzfallal. A regionális telephely nagyobb, mint egy fióktelep, és ASA segítségével csatlakozik a vállalati fő telephelyhez. Az ASA állandó, mindig bekapcsolt VPN-kapcsolatot tud létrehozni a fő helyszíni ASA-val. A SOHO jobban egy kis fióktelep, amely Cisco vezeték nélküli útválasztó segítségével csatlakozik a vállalati fő telephelyhez. A vezeték nélküli útválasztó állandó, mindig bekapcsolt VPN-kapcsolatot tud létrehozni a fő helyszíni ASA-val. Alternatív megoldásként a belső SOHO-felhasználók használhatják a Cisco AnyConnect VPN-klienst, hogy biztonságos VPN-kapcsolatot létesítsenek a fő helyszíni ASA-val.

1.2.4

Adatközponti hálózatok

Az adatközponti hálózatok jellemzően egy külső létesítményben vannak elhelyezve érzékeny vagy védett adatok tárolására. Ezek a helyek VPN-technológiával kapcsolódnak a vállalati telephelyekhez ASA-eszközökkel és integrált adatközponti kapcsolókkal, például nagy sebességű Cisco Nexus kapcsolókkal.

A mai adatközpontok hatalmas mennyiségű érzékeny, üzleti szempontból kritikus információt tárolnak. Ezért a fizikai biztonság kulcsfontosságú a működésükhöz. A fizikai biztonság nemcsak a létesítményhez való hozzáférést védi, hanem az embereket és a berendezéseket is. Például tűzriasztók, sprinklerek, szeizmikusan merevítettállványok, redundáns fűtés, szellőztetés és légkondicionálás (HVAC) és UPS-rendszerek védik az embereket, a berendezéseket és az adatokat.

Amint az ábrán is látható, az adatközpontok fizikai biztonsága két területre osztható:

Kerületen kívüli biztonság – idetartozhat a helyszíni biztonsági tisztek, kerítések, kapuk, folyamatos megfigyelés és biztonsági riasztások.

Belső kerületi biztonság – Ez magában foglalja a folyamatos videó megfigyelést, az elektronikus mozgásérzékelőket, a biztonsági csapdákat, valamint a biometrikus hozzáférési és kilépési érzékelőket.

Adatközpont fizikai biztonság

Az ábrán egy adatközpont látható, teteje eltávolítva az épület elrendezését mutatja

A biztonsági csapdák hozzáférést biztosítanak az adatcsarnokokhoz, ahol az adatközpont adatait tárolják. Amint az alábbi ábrán látható, a biztonsági csapda hasonló a légzsiliphez. A személynek először be kell lépnie a biztonsági csapdába a jelvényes azonosító proximity kártyájával. Miután a személy biztonsági csapdán belül van, arcfelismerést, ujjlenyomatot vagy más biometrikus ellenőrzést használnak a második ajtó kinyitásához. A felhasználónak meg kell ismételnie a folyamatot az adatcsarnokból való kilépéshez.

Az ábrán egy adatközpont látható, teteje eltávolítva az épület elrendezését mutatja. A biztonsági csapda kiemelve.

Biztonsági csapdák

Az ábrán egy adatközpont látható, teteje eltávolítva az épület elrendezését mutatja Biztonsági csapdák

Az alábbi ábra azt a biometrikus ujjlenyomat-szkennert mutatja, amely a texasi Allenben található Cisco Allen Data Centerhez való hozzáférés biztosítására szolgál.

Biometrikus hozzáférés

Az ábrán a biometrikus ujjlenyomat-szkenner látható

1.2.5

Felhőhálózatok és virtualizáció

A felhő egyre nagyobb szerepet játszik a vállalati hálózatokban. A felhőalapú számítástechnika lehetővé teszi a szervezetek számára, hogy olyan szolgáltatásokat használjon, mint például az a felhőalapú adattárolás, hogy infrastruktúra hiányában bővíthető kapacitásukat vagy képességeiket. A felhő természeténél fogva kívül esik a hagyományos hálózati peremen, nem téve a szervezet számára, hogy olyan adatközponttal rendelkezzen, amely a hagyományos tűzfal mögött található, de lehet, hogy.

A „felhőalapú számítástechnika” és a „virtualizáció” kifejezéseket gyakran felcserélhetően használhatjuk; azonban mást jelentenek. A virtualizáció a számítási felhő alapja. Enélkül a legszélesebb körben alkalmazott felhőalapú számítástechnika nem lenne lehetséges. A felhőalapú számítástechnika elválasztja az alkalmazást a hardvertől. A virtualizáció elválasztja az operációs rendszert a hardvertől.

A felhőhálózat fizikai és virtuális szerverekből áll, amelyek általában adatközpontokban helyezkednek el. Az adatközpontok azonban egyre gyakrabban használnak virtuális gépeket (VM) arra, hogy szervereket nyújtsanak ügyfeleiknek. A szervervirtuális erőforrások felhasználása a tétlen számítási szempontokat, és konszolidálja a szükséges kiszolgálók számát. Ez a rendszer is lehetővé teszi, hogy egyetlen hardverplatformon operációs rendszer is létezzen. A virtuális gépek azonban hajlamosak bizonyos célzott támadásokra is, az alábbiak szerint.

Hyperjacking – A támadó eltéríthet egy virtuális gép-hipervizort (VM-vezérlő szoftvert), majd indítópontként használhatja az adatközpont hálózatán lévő más eszközök megtámadására.

Azonnali aktiválás – Ha egy bizonyos ideig nem használt virtuális gép online állapotba kerül, előfordulhat, hogy elavult biztonsági házirendjei eltérnek az alapbiztonságtól, és biztonsági réseket vezethetnek be.

Víruskereső viharok – Ez akkor fordul elő, ha az összes virtuális gép egyszerre próbálja meg a vírusvédelmi adatfájlokat letölteni.

A biztonsági csapatok számára elengedhetetlen egy könnyen megvalósítható, de átfogó stratégia, amely megfelel az üzleti igényeknek és megvédi az adatközpontot. A Cisco a Secure Data Center megoldást fejlesztette ki, hogy működjön ezen a kiszámíthatatlan fenyegetési környezetben. A Cisco Secure Data Center megoldása blokkolja a belső és külső fenyegetéseket az adatközpont szélén.

A Cisco Secure Data Center alapvető összetevői a következő szolgáltatásokat nyújtják:

Biztonságos szegmentálás – A biztonságos szegmentálás érdekében az ASA-eszközök és a Cisco Nexus Series kapcsolóiba integrált Virtual Security Gateway adatközponti hálózatban vannak elhelyezve. Ez a virtuális gépek közötti szemcsés biztonságot nyújtja.

Fenyegetésvédelem – Az adatközpont-hálózatokban található ASA-k és IPS-eszközök fenyegetésintelligenciát, passzív operációs rendszer-ujjlenyomatot, valamint hírnév- és kontextuális elemzést használnak a fenyegetések elleni védekezés érdekében.

Láthatóság – A láthatósági megoldásokat olyan szoftverek segítségével biztosítják, mint a Cisco Security Manager, hogy leegyszerűsíteni a műveleteket és a megfelelőségi jelentéseket.

1.2.6

A fejlődő hálózati határ

Korábban az alkalmazottak és az adatforrások egy előre meghatározott területen belül maradtak, amelyet tűzfaltechnológia védett. Az alkalmazottak jellemzően vállalati LAN-hoz csatlakoztatott, cég által kibocsátott számítógépeket használtak, folyamatosan figyeltek és frissítettek, hogy megfeleljenek a biztonsági követelményeknek.

Napjainkban a fogyasztói végpontok, mint például az iPhone-ok, okostelefonok, táblagépek és több ezer egyéb eszköz, a hagyományos PC hatékony helyettesítő vagy kiegészítő válnak. Egyre többen hasznosítanak az eszközöket az információk eléréséhez. Ez a tendencia Bring Your Own Device (BYOD) néven ismert.

A BYOD trendhez igazodva a Cisco kifejlesztette a Borderless Networket. A Borderless Networkben az erőforrásokhoz való hozzáférést a felhasználók számos helyről, sokféle végponti eszközről kialakulhatnak, különféle kapcsolódási módok segítségével.

Ennek az elmosódott hálózati peremnek a támogatására a Cisco eszközök támogatják a mobileszköz-kezelési (MDM) funkciókat. Az MDM a mobileszközök védelmét, megfigyelését és kezelését biztosítja, amely magában foglalja a vállalati tulajdonú eszközöket és az alkalmazottak tulajdonában lévő eszközöket. Az MDM által támogatott és felügyelt eszközök nem csak a kézi eszközöket, például okostelefonokat és táblagépeket foglalják magukban, hanem a laptopokat és az asztali számítógépeket is.

Adat titkosítás

A legtöbb eszköz beépített titkosítási lehetőségekkel, mind eszköz, mind fájl szinten. Az MDM-szolgáltatások biztosíthatják, hogy csak az adattitkosítást támogató és azt engedélyező eszközök férhessenek hozzá a hálózathoz és a vállalati tartalmakhoz.

PIN-kód érvényesítése

A PIN-zár érvényesítése az első és leghatékonyabb lépés az eszközhöz való jogosulatlan hozzáférés megelőzésében. Ezen túlmenően az erős jelszószabályokat MDM is kényszerítheti, csökkentve a brute force támadások valószínűségét.

Adatok törlése

Az elveszett vagy ellopott eszközök távolról teljesen vagy részben törölhetők, akár a felhasználó, akár a rendszergazda az MDM-en keresztül.

Adatvesztés-megelőzés (DLP)

Míg az adatvédelmi funkciók (például PIN zárolás, adattitkosítás és távoli adattörlés) megakadályozzák, hogy illetéktelen felhasználók hozzáférjenek az adatokhoz, a DLP megakadályozza, hogy a jogosult felhasználók gondatlan vagy rosszindulatú dolgokat tegyenek a kritikus adatokkal.

JailBreak/Root detection

A Jailbreak (Apple iOS-eszközökön) és a rootolás (Android-eszközökön) az eszközök kezelésének megkerülésének eszköze. Az MDM-funkciók képesek észlelni az ilyen megkerüléseket, és azonnal korlátozzák az eszköz hozzáférését a hálózathoz vagy más vállalati eszközökhöz.

Mit tanultam ebben a modulban?

Az ügyek jelenlegi állása

A hálózati biztonság közvetlenül kapcsolódik a szervezet üzletmenet-folytonosságához. A hálózati biztonság megsértése megzavarhatja az e-kereskedelmet, üzleti adatok elvesztését okozhatja, veszélyeztetheti az emberek magánéletét, és veszélyeztetheti az információk integritását. Ezek a jogsértések a vállalatok bevételkiesését, a szellemi eltulajdonítást, pereket, sőt a közbiztonságot is veszélyeztethetik. Számos eszköz áll rendelkezésre a hálózati rendszergazdáknak a fenyegetéscsökkentési technikák adaptálásához, fejlesztéséhez és megvalósításához, köztük a Cisco Talos Intelligence Group. A támadási vektor egy olyan útvonalon, amelyen keresztül a fenyegetés szereplői hozzáférhetnek egy szerverhez, gazdagéphez vagy hálózathoz. A támadási vektorok a vállalati hálózaton belülről vagy kívülről származnak. Az adatok fontosak a szervezet legértékesebb eszközei. Különféle DLP-vezérléseket kell megvalósítani, egyesítik a stratégiát, az operatív, és taktikai intézkedéseket. A gyakori adatvesztési vektorok közé tartozik az e-mail és a közösségi hálózatok, a titkosítatlan adateszközök, a felhőalapú tárolóeszközök, a cserélhető adathordozók, a nyomtatott példány és a nem megfelelő hozzáférés-szabályozás.

Hálózati topológia áttekintése

Sokféle hálózat létezik. A CAN-ok korlátozott földrajzi területen belül összekapcsolt LAN-okból. A mélyreható védelmi tervezés elemei közé tartozik a VPN, az ASA tűzfal, az IPS, a 3. rétegbeli kapcsolók, a 2. rétegbeli kapcsolók, az ESA/WSA, az AAA szerver és a gazdagépek. A SOHO hálózatokat jellemző fogyasztói szintű útválasztókkal védik, amelyek integrált tűzfalfunkciókat és biztonságos vezeték nélküli kapcsolatokat biztosítanak. A vezeték nélküli gazdagépek WPA2 adattitkosítási technológia segítségével csatlakoznak a vezeték nélküli hálózathoz. A WAN-ok széles földrajzi területet ölelnek fel. A hálózatbiztonsági szakembereknek biztonságos eszközöket kell használniuk a hálózat szélén. Az adatközponti hálózatok jellemzően egy külső létesítményben vannak elhelyezve érzékeny vagy védett adatok tárolására. Az adatközpont fizikai biztonsága két területre oszlik: kültéri és belső határvédelemre. A biztonsági csapdák megkövetelik, hogy a személy a jelvényazonosítóját használja az első területre való belépéshez. Miután a személy biztonsági csapdán belül van, arcfelismerést, ujjlenyomatot vagy más biometrikus ellenőrzést használnak a második ajtó kinyitásához. A felhőalapú számítástechnika lehetővé teszi a szervezetek számára, hogy olyan szolgáltatásokat használjon, mint például az a felhőalapú adattárolás, hogy infrastruktúra hiányában bővíthető kapacitásukat vagy képességeiket. A tényleges felhőhálózat fizikai és virtuális szerverekből áll, amelyek általában adatközpontokban helyezkednek el. Az adatközpontok azonban egyre gyakrabban használnak virtuális gépeket, hogy szervereket nyújtsanak feleiknek. A virtuális gépek speciális célzott támadásokra is hajlamosak, beleértve a hiperjackelést, az azonnali aktiválást és a víruskereső viharokat. A Cisco Secure Data Center megoldása blokkolja a belső és külső fenyegetéseket az adatközpont szélén. A Cisco Secure Data Center megoldás alapvető összetevői biztonságos szegmentálást, fenyegetés elleni védelmet és láthatóságot biztosítanak. Egyre többen hasznosítanak az eszközöket az információk eléréséhez. Ez a tendencia BYOD néven ismert. A BYOD trendhez igazodva a Cisco kifejlesztette a Borderless Networket. A Borderless Networkben az erőforrásokhoz való hozzáférést a felhasználók számos helyről, sokféle végponti eszközről kialakulhatnak, különféle kapcsolódási módok segítségével. Ennek az elmosódott hálózati élnek a támogatására a Cisco eszközök támogatják az MDM funkciókat. az erőforrásokhoz való hozzáférést a felhasználók számos helyről, sokféle végponti eszközön módosulhatnak, különféle kapcsolódási lehetőségek segítségével. Ennek az elmosódott hálózati élnek a támogatására a Cisco eszközök támogatják az MDM funkciókat. az erőforrásokhoz való hozzáférést a felhasználók számos helyről, sokféle végponti eszközön módosulhatnak, különféle kapcsolódási lehetőségek segítségével. Ennek az elmosódott hálózati élnek a támogatására a Cisco eszközök támogatják az MDM funkciókat.

Bevezetés

2.0.1

Miért vegyem ezt a modult?

Ki támadja hálózatunkat és miért? Ebben a modulban megismerheti a különféle fenyegetés szereplőit. Megismerheti ezen „hackerek” által használt technikákat és eszközöket is. Olvasson tovább, hogy többet megtudjon!

2.0.2

Mit fogok tanulni ebben a modulban?

**Modul címe:** Hálózati fenyegetések

**Modul célja** : Magyarázza el a különböző típusú fenyegetéseket és támadásokat.

| **téma címe** | **Téma Cél** |
| --- | --- |
| **Ki támadja meg hálózatunkat?** | Magyarázza el, hogyan fejlődtek a hálózati fenyegetések. |
| **Fenyegető színész eszközök** | Ismertesse a fenyegető szereplők által használt különféle típusú támadási eszközöket. |
| **Rosszindulatú** | Ismertesse a rosszindulatú programok típusait. |
| **Gyakori hálózati támadások – felderítés, hozzáférés és közösségi tervezés** | Magyarázza el a felderítési, hozzáférési és social engineering hálózati támadásokat. |
| **Hálózati támadások – szolgáltatásmegtagadás, puffertúlcsordulás és kijátszás** | Magyarázza el a szolgáltatásmegtagadást, a puffertúlcsordulást és az elkerülő támadásokat. |

# Ki támadja meg hálózatunkat?

2.1.1

## Fenyegetés, sebezhetőség és kockázat

Támadás alatt állunk, és a támadók hozzá akarnak férni az eszközeinkhez. Az eszközök minden értéket képviselnek a szervezet számára, például adatok és egyéb szellemi tulajdon, szerverek, számítógépek, okostelefonok, táblagépek és még sok más.



A hálózatbiztonsággal kapcsolatos viták jobb megértéséhez fontos ismerni a következő kifejezéseket:

| **Term** | **Magyarázat** |
| --- | --- |
| **Fenyegetés** | Lehetséges veszély egy eszközre, például adatokra vagy magára a hálózatra. |
| **Sebezhetőség** | A rendszer vagy annak kialakításának gyengesége, amelyet egy fenyegetés kihasználhat. |
| **Támadási felület** | A támadási felület egy adott rendszerben a támadó számára elérhető sérülékenységek összessége. A támadási felület különböző pontokat ír le, ahol a támadó bejuthat a rendszerbe, és ahol adatokat nyerhet ki a rendszerből. Például előfordulhat, hogy az operációs rendszernek és a webböngészőnek is biztonsági javításokra van szüksége. Mindegyikük sebezhető a támadásokkal szemben, és ki vannak téve a hálózaton vagy az interneten. Együtt létrehoznak egy támadási felületet, amelyet a fenyegetés szereplője kihasználhat. |
| **Kihasználni** | Az a mechanizmus, amelyet a sebezhetőség kihasználására használnak fel egy eszköz kompromittálására. A kihasználások lehetnek távoliak vagy helyiek. A távoli kihasználás az, amely a hálózaton keresztül működik anélkül, hogy előzetesen hozzáférne a célrendszerhez. A támadónak nincs szüksége fiókra a végrendszerben a biztonsági rés kihasználásához. Helyi kihasználás esetén a fenyegetés szereplőjének valamilyen felhasználói vagy adminisztrátori hozzáférése van a végrendszerhez. A helyi kihasználás nem feltétlenül jelenti azt, hogy a támadó fizikai hozzáféréssel rendelkezik a végrendszerhez. |
| **Kockázat** | Annak a valószínűsége, hogy egy adott fenyegetés kihasználja egy eszköz adott sebezhetőségét, és nemkívánatos következményekkel jár. |

A kockázatkezelés az a folyamat, amely egyensúlyba hozza a védelmi intézkedések működési költségeit az eszköz védelmével elért haszonnal. Négy általános módja van a kockázatkezelésnek, amint az a táblázatban látható:

| **Kockázatkezelési stratégia** | **Magyarázat** |
| --- | --- |
| **Kockázat elfogadása** | Ilyenkor a kockázatkezelési lehetőségek költsége meghaladja magának a kockázatnak a költségét. A kockázatot elfogadják, és nem tesznek semmit. |
| **Kockázatkerülés** | Ez azt jelenti, hogy a kockázatot jelentő tevékenység vagy eszköz megszüntetésével kerülni kell a kockázatnak való kitettséget. A kockázat elkerülése érdekében végzett tevékenység megszüntetésével a tevékenységből származó előnyök is elvesznek. |
| **Kockázatcsökkentési** | Ez csökkenti a kockázatnak való kitettséget vagy csökkenti a kockázat hatását azáltal, hogy intézkedéseket tesz a kockázat csökkentésére. Ez a leggyakrabban alkalmazott kockázatcsökkentési stratégia. Ez a stratégia megköveteli a veszteség költségeinek, a mérséklési stratégiának és a kockázatnak kitett műveletből vagy tevékenységből származó előnyök alapos értékelését. |
| **Kockázatátadás** | A kockázat egy részét vagy egészét átruházzák egy hajlandó harmadik félre, például egy biztosítótársaságra. |

Egyéb gyakran használt hálózati biztonsági kifejezések a következők:

* **Ellenintézkedés** – A fenyegetés mérséklésével vagy a kockázat csökkentésével az eszközök védelme érdekében végrehajtott intézkedések.
* **Hatás** – A fenyegetés által a szervezetnek okozott lehetséges kár.

**Megjegyzés:** A helyi kihasználáshoz belső hálózati hozzáférésre van szükség, például a hálózaton fiókkal rendelkező felhasználónak. A távoli kihasználáshoz nincs szükség fiókra a hálózaton a hálózat sebezhetőségének kihasználásához.

2.1.2

## Hacker kontra fenyegető színész

Mint tudjuk, a „hacker” egy gyakori kifejezés, amelyet fenyegető szereplők leírására használnak. A „hacker” kifejezés azonban többféle jelentéssel bír, az alábbiak szerint:

* Okos programozó, aki képes új programokat kifejleszteni és a meglévő programok módosításait kódolni, hogy hatékonyabbá tegye azokat.
* Hálózati szakember, aki kifinomult programozási készségekkel gondoskodik arról, hogy a hálózatok ne legyenek sebezhetőek a támadásokkal szemben.
* Olyan személy, aki illetéktelenül próbál hozzáférni az interneten lévő eszközökhöz.
* Olyan személy, aki programokat futtat, hogy megakadályozza vagy lelassítsa a nagyszámú felhasználó hálózati hozzáférését, vagy megsértse vagy törölje az adatokat a kiszolgálókon.

Az ábrán látható, hogy vannak White, Gray és Black Hat hackerek. A White hat hacker 1-es, szürke kalap 2-es és fekete kalapos 3-as címkével van ellátva.

123

Szürkekalapos hackerekBlack Hat HackerekWhite Hat Hackerek

Amint az ábrán látható, a hackerek leírására gyakran használják a white hat hacker, black hat hacker és a gray hat hacker kifejezéseket.

1. A fehérkalapos hackerek etikus hackerek, akik jó, etikus és jogi célokra használják programozási készségeiket. Hálózati behatolási teszteket végezhetnek, hogy megkíséreljék a hálózatok és rendszerek kompromittálását azáltal, hogy számítógépes biztonsági rendszerekkel kapcsolatos ismereteiket használják fel a hálózati sebezhetőségek felfedezésére. A biztonsági réseket a fejlesztők és a biztonsági személyzet jelentik, akik megpróbálják kijavítani a biztonsági rést, mielőtt azt kihasználhatnák. Egyes szervezetek díjakat vagy jutalmakat adnak a fehérkalapos hackereknek, ha olyan információkat szolgáltatnak, amelyek segítenek azonosítani a sebezhetőséget.
2. A szürkekalapos hackerek olyan személyek, akik bűncselekményeket követnek el és vitathatatlanul etikátlan dolgokat tesznek, de nem személyes haszonszerzés vagy károkozás céljából. Példa erre az, aki engedély nélkül feltör egy hálózatot, majd nyilvánosságra hozza a biztonsági rést. A szürkekalapos hackerek sebezhetőséget fedhetnek fel az érintett szervezetnek, miután feltörték hálózatukat. Ez lehetővé teszi a szervezet számára a probléma megoldását.
3. A feketekalapos hackerek etikátlan bűnözők, akik személyes haszonszerzés céljából vagy rosszindulatú okokból, például hálózatok megtámadásából megsértik a számítógép és a hálózat biztonságát. A feketekalapos hackerek a sebezhetőségeket kihasználva veszélyeztetik a számítógépes és hálózati rendszereket.

Jó vagy rossz, a hackelés a hálózat biztonságának fontos szempontja. Ebben a kurzusban a fenyegetőző kifejezést akkor használjuk, amikor azokra a személyekre vagy csoportokra utalunk, akik szürke vagy fekete kalapos hackerek közé sorolhatók.

2.1.3

## A fenyegető szereplők evolúciója

A hackelés az 1960-as években kezdődött a telefonfrekvenciával vagy phreaking-el, ami arra utal, hogy különféle hangfrekvenciákat használnak a telefonrendszerek manipulálására. Abban az időben a telefonkapcsolók különféle hangokat, vagyis tone tárcsázást használtak a különböző funkciók jelzésére. A fenyegetettség korai szereplői rájöttek, hogy egy hang fütty segítségével történő utánzásával kihasználhatják a telefonkapcsolókat ingyenes távolsági hívások kezdeményezésére.

Az 1980-as évek közepén a számítógépes betárcsázós modemeket a számítógépek hálózatokhoz való csatlakoztatására használták. A fenyegetés szereplői „háborús tárcsázási” programokat írtak, amelyek egy adott területen minden telefonszámot tárcsáztak számítógépek, faliújság-rendszerek és faxok után kutatva. Amikor egy telefonszámot találtak, jelszófeltörő programokat használtak a hozzáféréshez. Azóta az általános fenyegetés szereplői profilja és indítékai meglehetősen megváltoztak.

A fenyegetés szereplőinek sokféle típusa létezik.

A Script kiddies az 1990-es években jelent meg, és tinédzserekre vagy tapasztalatlan fenyegetési szereplőkre utal, akik meglévő forgatókönyveket, eszközöket és kizsákmányolásokat futtatnak, hogy kárt okozzanak, de általában nem haszonszerzés céljából.

A sebezhetőségi brókerek általában a szürkekalapos hackerekre utalnak, akik megpróbálják felfedezni a visszaéléseket, és bejelentik azokat a szállítóknak, néha nyereményekért vagy jutalomért.

A hacktivisták olyan szürkekalapos hackerekre utalnak, akik különböző politikai és társadalmi eszmék ellen gyülekeznek és tiltakoznak. A hacktivisták nyilvánosan tiltakoznak szervezetek vagy kormányok ellen cikkek, videók közzétételével, bizalmas információk kiszivárogtatásával és elosztott szolgáltatásmegtagadási (DDoS) támadásokkal.

A kiberbûnözõ kifejezés a feketekalapos hackerekre vonatkozik, akik önálló vállalkozók vagy nagy kiberbûnözõ szervezeteknek dolgoznak. A kiberbűnözők minden évben dollármilliárdokat lopnak el a fogyasztóktól és a vállalkozásoktól.

Az államilag támogatott hackerek olyan fenyegetést jelentő szereplők, akik kormányzati titkokat lopnak, hírszerzési információkat gyűjtenek, és szabotálja a külföldi kormányok, terrorista csoportok és vállalatok hálózatait. A világ legtöbb országa bizonyos mértékig részt vesz az államilag támogatott hackelésben. Az egyén nézőpontjától függően ezek fehér vagy fekete kalapos hackerek.

# Hálózati biztonság

v1.0

[Ugrás a tartalomra](https://contenthub.netacad.com/netsec/2.1.4#chunks-container)

Hálózati biztonság

* [1A hálózatok védelme](https://contenthub.netacad.com/netsec/2.1.4#1)
  + [1.0Bevezetés](https://contenthub.netacad.com/netsec/2.1.4#1.0)
    - [1.0.1Első alkalommal ezen a tanfolyamon](https://contenthub.netacad.com/netsec/1.0.1)
    - [1.0.2Hallgatói források](https://contenthub.netacad.com/netsec/1.0.2)
    - [1.0.3Etikai hackelési nyilatkozat](https://contenthub.netacad.com/netsec/1.0.3)
    - [1.0.4Befogadó nyelv](https://contenthub.netacad.com/netsec/1.0.4)
    - [1.0.5Videó - Töltse le és telepítse a Packet Tracer programot](https://contenthub.netacad.com/netsec/1.0.5)
    - [1.0.6Videó – Kezdő lépések a Cisco Packet Tracerben](https://contenthub.netacad.com/netsec/1.0.6)
    - [1.0.7Miért vegyem ezt a modult?](https://contenthub.netacad.com/netsec/1.0.7)
    - [1.0.8Mit fogok tanulni ebben a modulban?](https://contenthub.netacad.com/netsec/1.0.8)
  + [1.1Az ügyek jelenlegi állása](https://contenthub.netacad.com/netsec/2.1.4#1.1)
  + [1.2Hálózati topológia áttekintése](https://contenthub.netacad.com/netsec/2.1.4#1.2)
  + [1.3A hálózatok biztonságának összefoglalása](https://contenthub.netacad.com/netsec/2.1.4#1.3)
* [2Hálózati fenyegetések](https://contenthub.netacad.com/netsec/2.1.4#2)
  + [2.0Bevezetés](https://contenthub.netacad.com/netsec/2.1.4#2.0)
  + [2.1Ki támadja meg hálózatunkat?](https://contenthub.netacad.com/netsec/2.1.4#2.1)
    - [2.1.1Fenyegetés, sebezhetőség és kockázat](https://contenthub.netacad.com/netsec/2.1.1)
    - [2.1.2Hacker kontra fenyegető színész](https://contenthub.netacad.com/netsec/2.1.2)
    - [2.1.3A fenyegető szereplők evolúciója](https://contenthub.netacad.com/netsec/2.1.3)
    - [2.1.4Kiberbűnözők](https://contenthub.netacad.com/netsec/2.1.4)
    - [2.1.5Kiberbiztonsági feladatok](https://contenthub.netacad.com/netsec/2.1.5)
    - [2.1.6Kiberfenyegetés-jelzők](https://contenthub.netacad.com/netsec/2.1.6)
    - [2.1.7A fenyegetés megosztása és a kiberbiztonsági tudatosság növelése](https://contenthub.netacad.com/netsec/2.1.7)
    - [2.1.8Ellenőrizze, hogy megértette – milyen színű a kalapom?](https://contenthub.netacad.com/netsec/2.1.8)
  + [2.2Fenyegető színész eszközök](https://contenthub.netacad.com/netsec/2.1.4#2.2)
  + [2.3Rosszindulatú](https://contenthub.netacad.com/netsec/2.1.4#2.3)
  + [2.4Gyakori hálózati támadások – felderítés, hozzáférés és közösségi tervezés](https://contenthub.netacad.com/netsec/2.1.4#2.4)
  + [2.5Hálózati támadások – szolgáltatásmegtagadás, puffertúlcsordulás és kijátszás](https://contenthub.netacad.com/netsec/2.1.4#2.5)
  + [2.6Hálózati veszélyek összefoglalója](https://contenthub.netacad.com/netsec/2.1.4#2.6)
* [3Mérséklő veszélyek](https://contenthub.netacad.com/netsec/2.1.4#3)
* [4Biztonságos eszközhozzáférés](https://contenthub.netacad.com/netsec/2.1.4#4)
* [5Adminisztrátori szerepkörök hozzárendelése](https://contenthub.netacad.com/netsec/2.1.4#5)
* [6Eszközfigyelés és -kezelés](https://contenthub.netacad.com/netsec/2.1.4#6)
* [7Hitelesítés, engedélyezés és elszámolás (AAA)](https://contenthub.netacad.com/netsec/2.1.4#7)
* [8Hozzáférés-vezérlési listák](https://contenthub.netacad.com/netsec/2.1.4#8)
* [9Tűzfaltechnológiák](https://contenthub.netacad.com/netsec/2.1.4#9)
* [10Zóna alapú házirend tűzfalak](https://contenthub.netacad.com/netsec/2.1.4#10)
* [11IPS technológiák](https://contenthub.netacad.com/netsec/2.1.4#11)
* [12IPS működés és megvalósítás](https://contenthub.netacad.com/netsec/2.1.4#12)
* [13Endpoint Security](https://contenthub.netacad.com/netsec/2.1.4#13)
* [142. rétegbeli biztonsági szempontok](https://contenthub.netacad.com/netsec/2.1.4#14)
* [15Kriptográfiai szolgáltatások](https://contenthub.netacad.com/netsec/2.1.4#15)
* [16Alapvető integritás és hitelesség](https://contenthub.netacad.com/netsec/2.1.4#16)
* [17Nyilvános kulcsú kriptográfia](https://contenthub.netacad.com/netsec/2.1.4#17)
* [18VPN-ek](https://contenthub.netacad.com/netsec/2.1.4#18)
* [19Helyezzen helyek közötti IPsec VPN-eket](https://contenthub.netacad.com/netsec/2.1.4#19)
* [20Bevezetés az ASA-ba](https://contenthub.netacad.com/netsec/2.1.4#20)
* [21ASA tűzfal konfigurációja](https://contenthub.netacad.com/netsec/2.1.4#21)
* [22Hálózatbiztonsági tesztelés](https://contenthub.netacad.com/netsec/2.1.4#22)

1. A hálózatok védelme
2. Bevezetés

# Ki támadja meg hálózatunkat?

2.1.1

## Fenyegetés, sebezhetőség és kockázat

Támadás alatt állunk, és a támadók hozzá akarnak férni az eszközeinkhez. Az eszközök minden értéket képviselnek a szervezet számára, például adatok és egyéb szellemi tulajdon, szerverek, számítógépek, okostelefonok, táblagépek és még sok más.



A hálózatbiztonsággal kapcsolatos viták jobb megértéséhez fontos ismerni a következő kifejezéseket:

| **Term** | **Magyarázat** |
| --- | --- |
| **Fenyegetés** | Lehetséges veszély egy eszközre, például adatokra vagy magára a hálózatra. |
| **Sebezhetőség** | A rendszer vagy annak kialakításának gyengesége, amelyet egy fenyegetés kihasználhat. |
| **Támadási felület** | A támadási felület egy adott rendszerben a támadó számára elérhető sérülékenységek összessége. A támadási felület különböző pontokat ír le, ahol a támadó bejuthat a rendszerbe, és ahol adatokat nyerhet ki a rendszerből. Például előfordulhat, hogy az operációs rendszernek és a webböngészőnek is biztonsági javításokra van szüksége. Mindegyikük sebezhető a támadásokkal szemben, és ki vannak téve a hálózaton vagy az interneten. Együtt létrehoznak egy támadási felületet, amelyet a fenyegetés szereplője kihasználhat. |
| **Kihasználni** | Az a mechanizmus, amelyet a sebezhetőség kihasználására használnak fel egy eszköz kompromittálására. A kihasználások lehetnek távoliak vagy helyiek. A távoli kihasználás az, amely a hálózaton keresztül működik anélkül, hogy előzetesen hozzáférne a célrendszerhez. A támadónak nincs szüksége fiókra a végrendszerben a biztonsági rés kihasználásához. Helyi kihasználás esetén a fenyegetés szereplőjének valamilyen felhasználói vagy adminisztrátori hozzáférése van a végrendszerhez. A helyi kihasználás nem feltétlenül jelenti azt, hogy a támadó fizikai hozzáféréssel rendelkezik a végrendszerhez. |
| **Kockázat** | Annak a valószínűsége, hogy egy adott fenyegetés kihasználja egy eszköz adott sebezhetőségét, és nemkívánatos következményekkel jár. |

A kockázatkezelés az a folyamat, amely egyensúlyba hozza a védelmi intézkedések működési költségeit az eszköz védelmével elért haszonnal. Négy általános módja van a kockázatkezelésnek, amint az a táblázatban látható:

| **Kockázatkezelési stratégia** | **Magyarázat** |
| --- | --- |
| **Kockázat elfogadása** | Ilyenkor a kockázatkezelési lehetőségek költsége meghaladja magának a kockázatnak a költségét. A kockázatot elfogadják, és nem tesznek semmit. |
| **Kockázatkerülés** | Ez azt jelenti, hogy a kockázatot jelentő tevékenység vagy eszköz megszüntetésével kerülni kell a kockázatnak való kitettséget. A kockázat elkerülése érdekében végzett tevékenység megszüntetésével a tevékenységből származó előnyök is elvesznek. |
| **Kockázatcsökkentési** | Ez csökkenti a kockázatnak való kitettséget vagy csökkenti a kockázat hatását azáltal, hogy intézkedéseket tesz a kockázat csökkentésére. Ez a leggyakrabban alkalmazott kockázatcsökkentési stratégia. Ez a stratégia megköveteli a veszteség költségeinek, a mérséklési stratégiának és a kockázatnak kitett műveletből vagy tevékenységből származó előnyök alapos értékelését. |
| **Kockázatátadás** | A kockázat egy részét vagy egészét átruházzák egy hajlandó harmadik félre, például egy biztosítótársaságra. |

Egyéb gyakran használt hálózati biztonsági kifejezések a következők:

* **Ellenintézkedés** – A fenyegetés mérséklésével vagy a kockázat csökkentésével az eszközök védelme érdekében végrehajtott intézkedések.
* **Hatás** – A fenyegetés által a szervezetnek okozott lehetséges kár.

**Megjegyzés:** A helyi kihasználáshoz belső hálózati hozzáférésre van szükség, például a hálózaton fiókkal rendelkező felhasználónak. A távoli kihasználáshoz nincs szükség fiókra a hálózaton a hálózat sebezhetőségének kihasználásához.

2.1.2

## Hacker kontra fenyegető színész

Mint tudjuk, a „hacker” egy gyakori kifejezés, amelyet fenyegető szereplők leírására használnak. A „hacker” kifejezés azonban többféle jelentéssel bír, az alábbiak szerint:

* Okos programozó, aki képes új programokat kifejleszteni és a meglévő programok módosításait kódolni, hogy hatékonyabbá tegye azokat.
* Hálózati szakember, aki kifinomult programozási készségekkel gondoskodik arról, hogy a hálózatok ne legyenek sebezhetőek a támadásokkal szemben.
* Olyan személy, aki illetéktelenül próbál hozzáférni az interneten lévő eszközökhöz.
* Olyan személy, aki programokat futtat, hogy megakadályozza vagy lelassítsa a nagyszámú felhasználó hálózati hozzáférését, vagy megsértse vagy törölje az adatokat a kiszolgálókon.

Az ábrán látható, hogy vannak White, Gray és Black Hat hackerek. A White hat hacker 1-es, szürke kalap 2-es és fekete kalapos 3-as címkével van ellátva.

123

Szürkekalapos hackerekBlack Hat HackerekWhite Hat Hackerek

Amint az ábrán látható, a hackerek leírására gyakran használják a white hat hacker, black hat hacker és a gray hat hacker kifejezéseket.

1. A fehérkalapos hackerek etikus hackerek, akik jó, etikus és jogi célokra használják programozási készségeiket. Hálózati behatolási teszteket végezhetnek, hogy megkíséreljék a hálózatok és rendszerek kompromittálását azáltal, hogy számítógépes biztonsági rendszerekkel kapcsolatos ismereteiket használják fel a hálózati sebezhetőségek felfedezésére. A biztonsági réseket a fejlesztők és a biztonsági személyzet jelentik, akik megpróbálják kijavítani a biztonsági rést, mielőtt azt kihasználhatnák. Egyes szervezetek díjakat vagy jutalmakat adnak a fehérkalapos hackereknek, ha olyan információkat szolgáltatnak, amelyek segítenek azonosítani a sebezhetőséget.
2. A szürkekalapos hackerek olyan személyek, akik bűncselekményeket követnek el és vitathatatlanul etikátlan dolgokat tesznek, de nem személyes haszonszerzés vagy károkozás céljából. Példa erre az, aki engedély nélkül feltör egy hálózatot, majd nyilvánosságra hozza a biztonsági rést. A szürkekalapos hackerek sebezhetőséget fedhetnek fel az érintett szervezetnek, miután feltörték hálózatukat. Ez lehetővé teszi a szervezet számára a probléma megoldását.
3. A feketekalapos hackerek etikátlan bűnözők, akik személyes haszonszerzés céljából vagy rosszindulatú okokból, például hálózatok megtámadásából megsértik a számítógép és a hálózat biztonságát. A feketekalapos hackerek a sebezhetőségeket kihasználva veszélyeztetik a számítógépes és hálózati rendszereket.

Jó vagy rossz, a hackelés a hálózat biztonságának fontos szempontja. Ebben a kurzusban a fenyegetőző kifejezést akkor használjuk, amikor azokra a személyekre vagy csoportokra utalunk, akik szürke vagy fekete kalapos hackerek közé sorolhatók.

2.1.3

## A fenyegető szereplők evolúciója

A hackelés az 1960-as években kezdődött a telefonfrekvenciával vagy phreaking-el, ami arra utal, hogy különféle hangfrekvenciákat használnak a telefonrendszerek manipulálására. Abban az időben a telefonkapcsolók különféle hangokat, vagyis tone tárcsázást használtak a különböző funkciók jelzésére. A fenyegetettség korai szereplői rájöttek, hogy egy hang fütty segítségével történő utánzásával kihasználhatják a telefonkapcsolókat ingyenes távolsági hívások kezdeményezésére.

Az 1980-as évek közepén a számítógépes betárcsázós modemeket a számítógépek hálózatokhoz való csatlakoztatására használták. A fenyegetés szereplői „háborús tárcsázási” programokat írtak, amelyek egy adott területen minden telefonszámot tárcsáztak számítógépek, faliújság-rendszerek és faxok után kutatva. Amikor egy telefonszámot találtak, jelszófeltörő programokat használtak a hozzáféréshez. Azóta az általános fenyegetés szereplői profilja és indítékai meglehetősen megváltoztak.

A fenyegetés szereplőinek sokféle típusa létezik.

Kattintson a gombokra a különböző típusú fenyegető szereplők definícióinak megtekintéséhez.

Script kölykök

Sebezhetőségi brókerek

Hacktivisták

Kiberbűnözők

Államilag támogatott

A Script kiddies az 1990-es években jelent meg, és tinédzserekre vagy tapasztalatlan fenyegetési szereplőkre utal, akik meglévő forgatókönyveket, eszközöket és kizsákmányolásokat futtatnak, hogy kárt okozzanak, de általában nem haszonszerzés céljából.

2.1.4

## Kiberbűnözők

A kiberbűnözők olyan fenyegetés szereplői, akik arra késztetnek, hogy bármilyen szükséges eszközzel pénzt keressenek. Míg a kiberbűnözők néha önállóan dolgoznak, gyakrabban bűnszervezetek finanszírozzák és szponzorálják őket. Becslések szerint világszerte a kiberbűnözők évente több milliárd dollárt lopnak el a fogyasztóktól és a vállalkozásoktól.

A kiberbûnözõk a földalatti gazdaságban tevékenykednek, ahol kizsákmányolást és eszközöket vásárolnak, adnak el és kereskednek. Emellett megvásárolják és eladják az áldozatoktól ellopott személyes adatokat és szellemi tulajdont. A kiberbűnözők kisvállalkozásokat és fogyasztókat, valamint nagyvállalatokat és iparágakat céloznak meg.



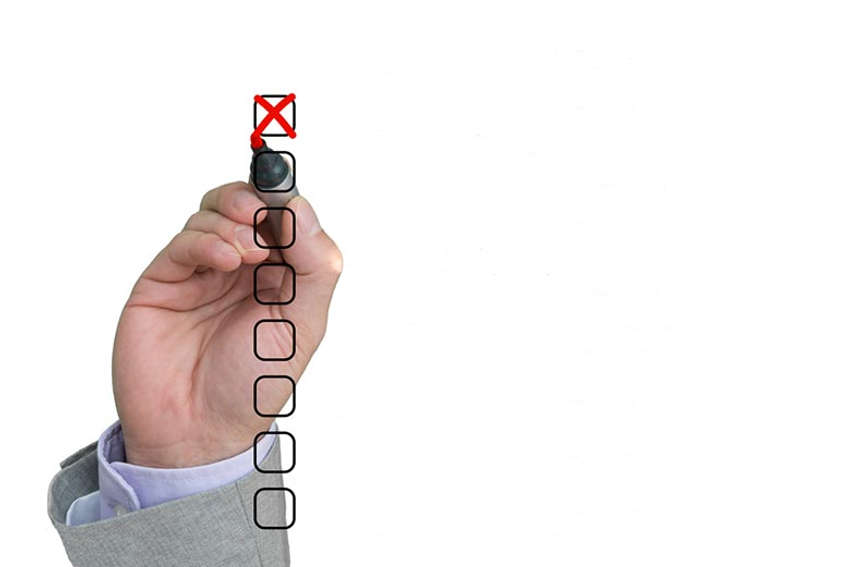
2.1.5

## Kiberbiztonsági feladatok

A fenyegetés szereplői nem tesznek különbséget. Az otthoni felhasználók és a kis- és középvállalkozások, valamint a nagy állami és magánszervezetek sebezhető végberendezéseit célozzák meg.

Az internet és a hálózatok biztonságosabbá tétele érdekében mindannyiunknak jó kiberbiztonsági tudatosságot kell kialakítanunk. A kiberbiztonság megosztott felelősség, amelyet minden felhasználónak gyakorolnia kell. Például jelentenünk kell a kiberbűnözést a megfelelő hatóságoknak, tisztában kell lennünk az e-mailben és az interneten megjelenő lehetséges fenyegetésekkel, és meg kell óvnunk a fontos információkat a lopástól.

A szervezeteknek lépéseket kell tenniük, és meg kell védeniük eszközeiket, felhasználóikat és ügyfeleiket. Kiberbiztonsági feladatokat kell kidolgozniuk és gyakorolniuk, például az ábrán felsoroltakkal.



**Cybersecurity checklist**Trustworthy IT vendorSecurity software up-to-dateRegular penetration testsBackup to cloud and hard diskPeriodically change WIFI passwordSecurity policy up-to-dateEnforce use of strong passwordsTwo factor authentication

2.1.6

## Kiberfenyegetés-jelzők

Számos hálózati támadás megelőzhető a **kompromisszumjelzőkkel** (IOC) kapcsolatos információk megosztásával. Minden támadásnak egyedi azonosítható attribútumai vannak. A kompromisszum jelei a támadás megtörténtének bizonyítékai. Az IOC-k többek között olyan funkciók lehetnek, amelyek azonosítják a rosszindulatú programfájlokat, a támadásoknál használt szerverek IP-címeit, fájlneveket és a rendszerszoftverek jellemző módosításait. Az IOC-ok segítenek a kiberbiztonsági személyzetnek azonosítani, mi történt a támadás során, és védekezési módokat dolgoznak ki a támadás ellen. A NOB összefoglalója egy rosszindulatú program esetében az ábrán látható.

Malware File - "studiox-link-standalone-v20.03.8-stable.exe"

sha256 6a6c28f5666b12beecd56a3d1d517e409b5d6866c03f9be44ddd9efffa90f1e0

sha1 eb019ad1c73ee69195c3fc84ebf44e95c147bef8

md5 3a104b73bb96dfed288097e9dc0a11a8

DNS requests

domain log.studiox.link

domain my.studiox.link

domain \_sips.\_tcp.studiox.link

domain sip.studiox.link

Connections

ip 198.51.100.248

ip 203.0.113.82

Például egy felhasználó kap egy e-mailt, amelyben azt állítja, hogy nagy díjat nyert. Az e-mailben található linkre kattintás támadást eredményez. A NOB tartalmazhatja többek között azt a tényt, hogy a felhasználó nem vett részt a versenyen, a feladó IP-címét, az e-mail tárgysorát, a kattintásra váró URL-t vagy a letöltendő mellékletet.

**A támadás mutatói** (IOA) inkább a támadások mögött meghúzódó motivációra és azokra a lehetséges eszközökre összpontosítanak, amelyek révén a fenyegetett szereplők sebezhető pontokat fenyegetnek vagy fognak kompromittálni az eszközökhöz való hozzáférés érdekében. Az IOA-k a támadók által használt stratégiákkal foglalkoznak. Emiatt az IOA-k ahelyett, hogy egyetlen fenyegetésre reagálnának, segíthetnek proaktív biztonsági megközelítés kialakításában. Ennek az az oka, hogy a stratégiák többféle kontextusban és több támadásban is felhasználhatók. A stratégia elleni védekezés tehát megelőzheti az ugyanazt vagy hasonló stratégiát alkalmazó jövőbeli támadásokat.

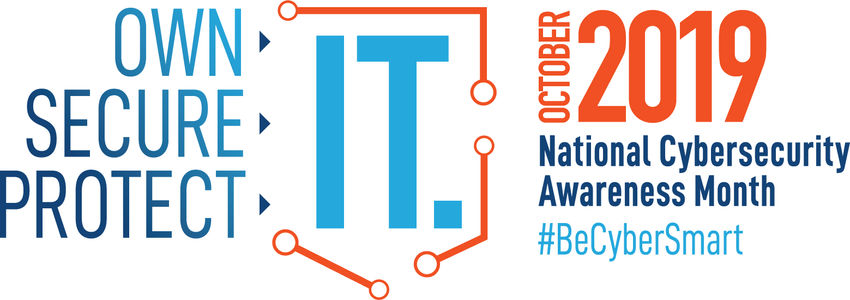
2.1.7

## A fenyegetés megosztása és a kiberbiztonsági tudatosság növelése

A kormányok most aktívan támogatják a kiberbiztonságot. Például az Egyesült Államok Kiberbiztonsági Infrastruktúra és Biztonsági Ügynöksége (CISA) vezető erőfeszítéseket tesz a kiberbiztonsági információk állami és magánszervezetekkel történő megosztásának automatizálására. A CISA az Automated Indicator Sharing (AIS) nevű rendszert használja. Az AIS lehetővé teszi a támadási mutatók megosztását az Egyesült Államok kormánya és a magánszektor között, amint a fenyegetéseket ellenőrizték. A CISA számos forrást kínál, amelyek segítenek korlátozni az Egyesült Államok támadási felületének méretét.

A CISA és a National Cyber ​​Security Alliance (NCSA) minden felhasználó számára előmozdítja a kiberbiztonságot. Például minden októberben évente kampányt tartanak „Nemzeti Kiberbiztonsági Tudatosság Hónap” (NCASM) néven. Ezt a kampányt a kiberbiztonság népszerűsítésére és tudatosítására fejlesztették ki.

A 2019-es NCASM témája a „ **Saját IT. Biztonságos IT. Védje meg az IT-t.**” Ez a kampány arra biztatta az állampolgárokat, hogy legyenek nagyobb biztonságban és személyesebben elszámoltathatók a legjobb biztonsági gyakorlatok online használatával kapcsolatban. A kampány sokféle biztonsági témában tartalmaz anyagokat, többek között:

* A közösségi média biztonsága
* Adatvédelmi beállítások frissítése
* Az eszközalkalmazások biztonságának ismerete
* A szoftver naprakészen tartása
* Biztonságos online vásárlás
* Wi-Fi biztonság
* Ügyféladatok védelme

Az Európai Unió Kiberbiztonsági Ügynöksége (ENISA) tanácsokat és megoldásokat kínál az EU-tagállamok kiberbiztonsági kihívásaira. Az ENISA olyan szerepet tölt be Európában, mint a CISA az Egyesült Államokban.

2.1.8

## Ellenőrizze, hogy megértette – milyen színű a kalapom?

Click the appropriate response for each characteristic to indicate the type of hacker it describes.

I hacked into ATM machines without the manufacturer's authorization and discovered several vulnerabilities. I then contacted the ATM manufacturer to share my findings with them.

**[White Hat](https://contenthub.netacad.com/netsec/2.1.4" \l "White)**

**[Gray Hat](https://contenthub.netacad.com/netsec/2.1.4" \l "Gray)**

**[Black Hat](https://contenthub.netacad.com/netsec/2.1.4" \l "Black)**

I secretly installed a debit card skimmer device on an ATM machine. A few days later, I retrieved it and it had captured the account numbers and pins numbers of over 1000 people. I then proceeded to transfer money from their accounts to an offshore bank account.

**[White Hat](https://contenthub.netacad.com/netsec/2.1.4" \l "White)**

**[Gray Hat](https://contenthub.netacad.com/netsec/2.1.4" \l "Gray)**

**[Black Hat](https://contenthub.netacad.com/netsec/2.1.4" \l "Black)**

My job is to identify weaknesses in the computer system in my company.

**[White Hat](https://contenthub.netacad.com/netsec/2.1.4" \l "White)**

**[Gray Hat](https://contenthub.netacad.com/netsec/2.1.4" \l "Gray)**

**[Black Hat](https://contenthub.netacad.com/netsec/2.1.4" \l "Black)**

I used malware to compromise several corporate systems to steal credit card information and sold that information to the highest bidder.

**[White Hat](https://contenthub.netacad.com/netsec/2.1.4" \l "White)**

**[Gray Hat](https://contenthub.netacad.com/netsec/2.1.4" \l "Gray)**

**[Black Hat](https://contenthub.netacad.com/netsec/2.1.4" \l "Black)**

A biztonsági kizsákmányolásokkal kapcsolatos kutatásaim során egy vállalati hálózaton egy biztonsági résre botlottam, amelyhez hozzáférési jogom van.

**[Fehér kalap](https://contenthub.netacad.com/netsec/2.1.4" \l "White)**

**[Szürke kalap](https://contenthub.netacad.com/netsec/2.1.4" \l "Gray)**

**[Fekete sapka](https://contenthub.netacad.com/netsec/2.1.4" \l "Black)**

Miközben a biztonsági rések után kutattam, jogosulatlanul hozzáfértem egy vállalat hálózatához, és a következő üzenetet hagytam: „Az Ön biztonsága hibás”.

**[Fehér kalap](https://contenthub.netacad.com/netsec/2.1.4" \l "White)**

**[Szürke kalap](https://contenthub.netacad.com/netsec/2.1.4" \l "Gray)**

**[Fekete sapka](https://contenthub.netacad.com/netsec/2.1.4" \l "Black)**

Technológiai cégekkel dolgozom a DNS-hibák kijavításán.

**[Fehér kalap](https://contenthub.netacad.com/netsec/2.1.4" \l "White)**

**[Szürke kalap](https://contenthub.netacad.com/netsec/2.1.4" \l "Gray)**

**[Fekete sapka](https://contenthub.netacad.com/netsec/2.1.4" \l "Black)**

Jelölje beMutasd meg nekemVisszaállítás

[2.0](https://contenthub.netacad.com/netsec/2.1.4" \l "/netsec/undefined.1)

[Bevezetés](https://contenthub.netacad.com/netsec/2.1.4" \l "/netsec/undefined.1)

[2.2](https://contenthub.netacad.com/netsec/2.1.4" \l "/netsec/undefined.1)

[Fenyegető színész eszközök](https://contenthub.netacad.com/netsec/2.1.4" \l "/netsec/undefined.1)

# Fenyegető színész eszközök

2.2.1

## A támadási eszközök bemutatása

A sebezhetőség kihasználásához a fenyegetés szereplőjének rendelkeznie kell egy technikával vagy eszközzel. Az évek során a támadási eszközök kifinomultabbak és nagymértékben automatizáltak lettek. Ezeknek az új eszközöknek a megvalósítása kevesebb technikai tudást igényel.

Az ábrán húzza át a fehér kört az idővonalon, hogy megtekinthesse a kapcsolatot a támadási eszközök kifinomultsága és a használatukhoz szükséges műszaki ismeretek között.

a bal oldalon egy kifinomult támadási sávot, a jobb oldalon pedig egy technikai tudású sávot mutat. 1985-ben a támadások nem voltak túl kifinomultak, és sok technikai tudást igényeltek. Az idő előrehaladtával a támadások kifinomultsága nőtt, és a szükséges technikai tudás csökkent.

### A támadási eszközök kifinomultsága vs. technikai tudás

Magas

Közepes

Alacsony

A támadási eszközök kifinomultsága

Műszaki ismeretek

2.2.2

## A biztonsági eszközök evolúciója

Az etikus hackelés számos különböző típusú eszköz használatát jelenti a hálózat és a végeszközök tesztelésére. A hálózat és rendszerei biztonságának ellenőrzésére számos hálózati penetrációt vizsgáló eszközt fejlesztettek ki. Azonban ezen eszközök közül sokat a fenyegetés szereplői is használhatnak kizsákmányolásra.

A fenyegetőző szereplők különféle hackereszközöket is készítettek. Ezeket az eszközöket kifejezetten aljas okok miatt írták le. A kiberbiztonsági személyzetnek azt is tudnia kell, hogyan kell használni ezeket az eszközöket a hálózati penetrációs tesztek végrehajtásakor.

Fedezze fel a közös hálózati penetrációt vizsgáló eszközök kategóriáit. Figyelje meg, hogyan használnak bizonyos eszközöket a fehér és a fekete kalapok. Ne feledje, hogy a lista nem teljes, mivel az új eszközök folyamatosan fejlesztés alatt állnak.

**Megjegyzés** : Ezen eszközök közül sok UNIX vagy Linux alapú; ezért egy biztonsági szakembernek erős UNIX és Linux háttérrel kell rendelkeznie.

| **Eszköz kategóriák** | **Leírás** |
| --- | --- |
| jelszótörők | A jelszavak jelentik a legsebezhetőbb biztonsági fenyegetést. A jelszótörő eszközöket gyakran jelszó-helyreállító eszközöknek nevezik, és a jelszó feltörésére vagy helyreállítására használhatók. Ez vagy az eredeti jelszó eltávolításával, az adatok titkosításának megkerülésével, vagy a jelszó közvetlen felfedezésével érhető el. A jelszótörők többször is találgatásokat hajtanak végre a jelszó feltörése és a rendszerhez való hozzáférés érdekében. A jelszófeltörő eszközök példái közé tartozik John the Ripper, Ophcrack, L0phtCrack, THC Hydra, RainbowCrack és Medusa. |
| vezeték nélküli hacker eszközök | A vezeték nélküli hálózatok érzékenyebbek a hálózati biztonsági fenyegetésekre. A vezeték nélküli hackereszközöket a vezeték nélküli hálózatok szándékos feltörésére használják a biztonsági rések észlelése érdekében. Vezeték nélküli hackereszközök például az Aircrack-ng, a Kismet, az InSSIDer, a KisMAC, a Firesheep és a NetStumbler. |
| hálózati szkennelés és hacker eszközök | A hálózati szkennelő eszközök a hálózati eszközök, szerverek és gazdagépek nyitott TCP- vagy UDP-portjainak vizsgálatára szolgálnak. A szkennelő eszközök közé tartozik például az Nmap, a SuperScan, az Angry IP Scanner és a NetScanTools. |
| csomagkészítő eszközök | A csomagkészítő eszközöket a tűzfal robusztusságának vizsgálatára és tesztelésére használják speciálisan kialakított hamisított csomagok segítségével. Ilyen eszközök például a Hping, a Scapy, a Socat, a Yersinia, a Netcat, az Nping és a Nemesis. |
| csomagszimatolók | A csomagszimuláló eszközök a hagyományos Ethernet LAN-on vagy WLAN-on belüli csomagok rögzítésére és elemzésére szolgálnak. Az eszközök közé tartozik a Wireshark, a Tcpdump, az Ettercap, a Dsniff, az EtherApe, a Paros, a Fiddler, a Ratproxy és az SSLstrip. |
| rootkit detektorok | A rootkit detektor egy könyvtár- és fájlintegritás-ellenőrző, amelyet a fehér kalap használ a telepített gyökérkészletek észlelésére. Ilyen például az AIDE, a Netfilter és a PF: OpenBSD Packet Filter. |
| fuzzers a sebezhetőségek kereséséhez | A fuzzerek olyan eszközök, amelyeket a fenyegetés szereplői használnak, amikor megpróbálják felfedezni a számítógépes rendszer biztonsági réseit. A fuzzerek közé tartozik például a Skipfish, a Wapiti és a W3af. |
| törvényszéki eszközök | A fehérkalapos hackerek kriminalisztikai eszközöket használnak az adott számítógépes rendszerben létező bizonyítékok minden nyomának kiszúrására. Ilyen eszközök például a Sleuth Kit, a Helix, a Maltego és az Encase. |
| hibakeresők | A fekete kalapok a hibakereső eszközöket használják a bináris fájlok visszafejtésére exploitok írásakor. A fehér kalapok is használják a rosszindulatú programok elemzéséhez. A hibakereső eszközök közé tartozik a GDB, a WinDbg, az IDA Pro és az Immunity Debugger. |
| operációs rendszerek feltörése | A hacker operációs rendszerek olyan speciálisan tervezett operációs rendszerek, amelyek előre telepítve vannak feltörésre optimalizált eszközökkel és technológiákkal. A speciálisan tervezett hacker operációs rendszerek például a Kali Linux, a SELinux, a Knoppix, a Parrot OS és a BackBox Linux. |
| titkosítási eszközök | Ezek az eszközök védik a szervezet adatainak tartalmát azok tárolása vagy továbbítása során. A titkosítási eszközök algoritmussémákat használnak az adatok kódolására, hogy megakadályozzák az adatokhoz való jogosulatlan hozzáférést. Ilyen eszközök például a VeraCrypt, a CipherShed, az Open SSH, az OpenSSL, az OpenVPN és a Stunnel. |
| sebezhetőség kihasználására szolgáló eszközök | Ezek az eszközök azonosítják, hogy egy távoli gazdagép sebezhető-e a biztonsági támadásokkal szemben. A sebezhetőséget kihasználó eszközök például a Metasploit, a Core Impact, az Sqlmap, a Social Engineer Tool Kit és a Netsparker. |
| sebezhetőségi szkennerek | Ezek az eszközök átvizsgálják a hálózatot vagy a rendszert a nyitott portok azonosítására. Használhatók ismert sebezhetőségek, valamint virtuális gépek, BYOD-eszközök és ügyféladatbázisok vizsgálatára is. Ilyen eszközök például a Nipper, a Securia PSI, a Core Impact, a Nessus, a SAINT és az Open VAS. |

2.2.3

## A támadások kategóriái

A fenyegetés szereplői a korábban említett eszközöket vagy eszközök kombinációját használhatják különféle támadások létrehozására. A táblázat a támadások gyakori típusait mutatja be. A támadások listája azonban nem teljes, mivel folyamatosan fedezik fel a hálózatok támadásának új módjait.

Fontos megérteni, hogy a fenyegetés szereplői különféle biztonsági eszközöket használnak e támadások végrehajtására.

| **A támadás kategóriája** | **Leírás** |
| --- | --- |
| lehallgató támadás | Lehallgató támadásról akkor beszélünk, amikor egy fenyegetőző felfogja és meghallgatja a hálózati forgalmat. Ezt a támadást szimatolásnak vagy leskelődésnek is nevezik. |
| adatmódosítási támadás | Az adatmódosítási támadások akkor fordulnak elő, amikor a fenyegetettség szereplője felfogja a vállalati forgalmat, és a küldő vagy a fogadó tudta nélkül módosította a csomagokban lévő adatokat. |
| IP-cím hamisítási támadás | Az IP-címhamisítási támadásról akkor beszélünk, amikor a fenyegető szereplő olyan IP-csomagot hoz létre, amely a vállalati intraneten belüli érvényes címről származik. |
| jelszó alapú támadások | Jelszó alapú támadások akkor fordulnak elő, amikor egy fenyegetést végrehajtó szereplő megszerzi az érvényes felhasználói fiók hitelesítő adatait. A fenyegetés szereplői ezt a fiókot használják más felhasználók listáinak és hálózati információknak a megszerzésére. Módosíthatják a szerver- és hálózati konfigurációkat, valamint módosíthatják, átirányíthatják vagy törölhetik az adatokat. |
| szolgáltatásmegtagadási (DoS) támadás | A DoS támadás megakadályozza a számítógép vagy a hálózat normál használatát az érvényes felhasználók számára. A hálózathoz való hozzáférés után a DoS-támadás összeomolhatja az alkalmazásokat vagy a hálózati szolgáltatásokat. A DoS támadás a számítógépet vagy a teljes hálózatot is eláraszthatja forgalommal, amíg a túlterhelés miatt leállásra nem kerül sor. A DoS támadás blokkolhatja a forgalmat is, aminek következtében a jogosult felhasználók elveszítik a hozzáférést a hálózati erőforrásokhoz. |
| man-in-the-middle támadás (MiTM) | A MiTM támadás akkor következik be, amikor a fenyegetés szereplői a forrás és a cél között helyezkednek el. Mostantól aktívan figyelhetik, rögzíthetik és átláthatóan irányíthatják a kommunikációt. |
| kompromittált kulcstámadás | Kompromittált kulcsú támadás akkor történik, amikor a fenyegetés szereplője titkos kulcsot szerez. Ezt feltört kulcsnak nevezik. A feltört kulcs segítségével biztonságos kommunikációhoz lehet hozzáférni anélkül, hogy a küldő vagy a fogadó tudatában lenne a támadásnak. |
| szippantó támadás | A szippantó egy olyan alkalmazás vagy eszköz, amely képes olvasni, figyelni és rögzíteni a hálózati adatcseréket, valamint beolvasni a hálózati csomagokat. Ha a csomagok nincsenek titkosítva, a szippantó teljes képet ad a csomagon belüli adatokról. Még a beágyazott (alagútba zárt) csomagok is feltörhetők és olvashatók, hacsak nincsenek titkosítva, és a fenyegetés szereplője nem fér hozzá a kulcshoz. |

2.2.4

## Ellenőrizze, hogy megértette – osztályozza a kibertámadásokat

Az űrlap teteje

A következő kérdések megválaszolásával ellenőrizze, hogy megértette-e a kibertámadások típusait.

1. A hackerek hozzáfértek a fiókadatokhoz, és most már a jogosult felhasználókkal azonos jogokkal jelentkezhetnek be a rendszerbe. Milyen típusú támadás ez?



kompromittált kulcs



jelszó alapú



DoS



szociális tervezés

1. Milyen típusú támadások esetén változtathatják meg a fenyegetés szereplői a csomagokban lévő adatokat a küldő vagy a fogadó tudta nélkül?



hallgatózás



szolgáltatás megtagadása



adatmódosítás



IP-cím hamisítás

1. A fenyegetés szereplői a forrás és a cél között helyezkedtek el, hogy a hálózati felhasználók tudta nélkül figyeljék, rögzítsék és irányítsák a kommunikációt. Milyen típusú támadás ez?



MiTM



hallgatózás



DoS



IP-cím hamisítás

1. Egy fenyegetést jelentő szereplő hozzáférést kapott titkosítási kulcsokhoz, amelyek lehetővé teszik számukra, hogy bizalmas információkat olvassanak el. Milyen típusú támadás ez?



hallgatózás



ember-középben



jelszó alapú



kompromittált kulcs

1. Milyen típusú támadások esetén csatlakozik a fenyegetést támadó a hálózathoz, és olvassa el a hálózati felhasználók kommunikációját?



adatmódosítás



hallgatózás



szolgáltatás megtagadása



jelszó alapú

1. A fenyegetés szereplője olyan IP-csomagokat hoz létre, amelyek látszólag a vállalati hálózaton belüli érvényes forrásból származnak. Milyen típusú támadás ez?



hallgatózás



jelszó alapú



MiTM



IP-cím hamisítás

1. Milyen típusú támadások akadályozzák meg, hogy az érvényes felhasználók normálisan használják a számítógépet vagy a hálózatot?



DoS



jelszó alapú



MiTM



IP-cím hamisítás

# Rosszindulatú

2.3.1

## A rosszindulatú programok típusai

A végeszközök különösen ki vannak téve a rosszindulatú programok támadásainak. Ezért ennek a témakörnek a középpontjában a végeszközöket érő fenyegetés áll. Malware a rosszindulatú szoftver vagy rosszindulatú kód rövidítése. Ez egy olyan kód vagy szoftver, amelyet kifejezetten arra terveztek, hogy megsértse, megzavarja, ellopja vagy általában más „rossz” vagy illegitim műveletet végezzen adatokon, gazdagépeken vagy hálózatokon. Fontos tudni a rosszindulatú programokról, mert a fenyegetések szereplői és az online bűnözők gyakran megpróbálják rávenni a felhasználókat, hogy rosszindulatú programokat telepítsenek a biztonsági hiányosságok kihasználása érdekében. Ezenkívül a rosszindulatú programok olyan gyorsan fejlődnek, hogy a rosszindulatú programokkal kapcsolatos biztonsági incidensek rendkívül gyakoriak, mivel a kártevőirtó szoftvereket nem lehet elég gyorsan frissíteni ahhoz, hogy megállítsák az új fenyegetéseket.

Játssza le az animációt, és tekintse meg a három leggyakoribb rosszindulatú programra vonatkozó példákat; vírus, féreg és trójai faló.

The animation shows a network with two PCs and two routers with the routers are connected to each other sit between the two PCs with each PC connected to one of the routers. The PC on the left has an attacker. As the animation plays a text box opens that reads “The primary vulnerabilities for end-user workstations are virus, worm, and Trojan Horse attacks. As the animation continues to play the attacker at the PC on the left sends a virus attack on the network that travels over the network routers to the PC on the right. A text box opens that reads “A virus is malicious software which executes a specific unwanted, and often harmful, function on a computer”. As the animation continues to play the attacker at the PC on the left sends a worm attack on the network that travels over the network routers to the PC on the right. A text box opens that reads “A worm executes arbitrary code and installs copies of itself in the memory of the infected computer. The main purpose of a worm is to automatically replicate itself and spread across the network from system to system”. As the animation continues to play the attacker at the PC on the left sends a Trojan Horse attack on the network that travels over the network routers to the PC on the right. A text box opens that reads “A Trojan horse is a non-self-replicating type of malware. It often contains malicious code that is designed to look like something else, such as a legitimate application or file. When an infected application or file is downloaded and opened, the Trojan horse can attack the end device from within”.

A végfelhasználói munkaállomások elsődleges sebezhetőségét a vírusok, férgek és trójai faló támadások jelentik.

A vírus olyan rosszindulatú szoftver, amely egy adott nem kívánt és gyakran káros funkciót hajt végre a számítógépen.

A féreg tetszőleges kódot hajt végre, és saját másolatait telepíti a fertőzött számítógép memóriájába. A férgek fő célja, hogy automatikusan replikálják magukat, és rendszerről rendszerre terjedjenek a hálózaton.

A trójai faló egy nem önreplikálódó típusú rosszindulatú program. Gyakran tartalmaz olyan rosszindulatú kódot, amelyet úgy terveztek, hogy valami másnak, például legitim alkalmazásnak vagy fájlnak tűnjön. Amikor egy fertőzött alkalmazást vagy fájlt letöltenek és megnyitnak, a trójai faló belülről támadhatja meg a végeszközt.

2.3.2

## Vírusok

A vírus egyfajta rosszindulatú program, amely úgy terjed, hogy egy másolatot beilleszt egy másik programba. A program futtatása után a vírusok egyik számítógépről a másikra terjednek, megfertőzve a számítógépeket. A legtöbb vírus terjedéséhez emberi segítségre van szükség. Például, ha valaki fertőzött USB-meghajtót csatlakoztat a számítógépéhez, a vírus bejut a számítógépbe. A vírus ezután megfertőzhet egy új USB-meghajtót, és átterjedhet új számítógépekre. A vírusok hosszabb ideig szunnyadhatnak, majd egy adott időpontban és napon aktiválódnak.

Egy egyszerű vírus telepítheti magát a futtatható fájl első kódsorába. Aktiválásakor a vírus ellenőrizheti a lemezen más végrehajtható fájlokat, hogy meg tudja fertőzni az összes még nem fertőzött fájlt. A vírusok lehetnek ártalmatlanok, például azok, amelyek képet jelenítenek meg a képernyőn, vagy pusztítóak, például olyanok, amelyek módosítanak vagy törölnek fájlokat a merevlemezen. A vírusok mutációra is programozhatók az észlelés elkerülése érdekében.

A legtöbb vírust ma már USB-memória-meghajtók, CD-k, DVD-k, hálózati megosztások és e-mailek terjesztik. Az e-mail vírusok a vírusok gyakori típusai.

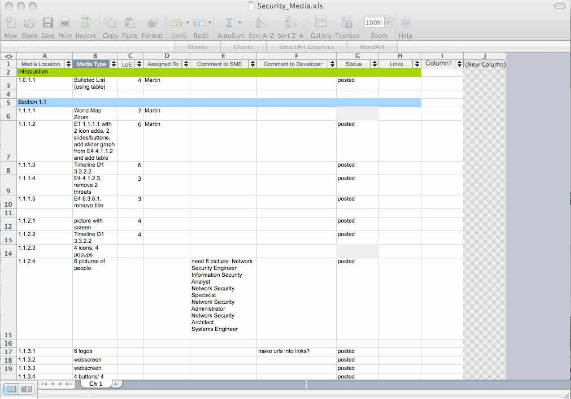
2.3.3

## Trójai lovak

A trójai faló kifejezés a görög mitológiából származik. A görög harcosok Trója népének (a trójaiaknak) egy óriási üreges lovat ajánlottak ajándékba. A trójaiak behozták az óriási lovat fallal körülvett városukba, nem tudva, hogy sok görög harcos van benne. Éjszaka, miután a legtöbb trójai aludt, a harcosok kirohantak a lóból, kinyitották a városkaput, és lehetővé tették, hogy egy jelentős csapat belépjen a városba, és átvegye az uralmat.

A trójai faló kártevő olyan szoftver, amely legitimnek tűnik, de olyan rosszindulatú kódot tartalmaz, amely kihasználja az azt futtató felhasználó jogosultságait, amint az az ábrán látható.

Az ábrán egy trójai faló látható, amely kihasználja a felhasználó jogosultságait számítógép segítségével.



ElpusztítaniTávoli adminisztráció engedélyezéseJelszó továbbítása

Gyakran előfordul, hogy az online játékokhoz trójaiakat kapcsolnak. A felhasználókat általában becsapják, hogy betöltsék és végrehajtsák a trójai falót a rendszerükön. Játék közben a felhasználó nem vesz észre semmilyen problémát. A háttérben a trójai faló telepítve van a felhasználó rendszerére. A trójai faló rosszindulatú kódja a játék bezárása után is tovább működik.

A trójai faló koncepciója rugalmas. Azonnali károkat okozhat, távoli hozzáférést biztosíthat a rendszerhez, vagy egy hátsó ajtón keresztül. Az utasításoknak megfelelően távolról is végrehajthat műveleteket, például "küldje el a jelszófájlt hetente egyszer". A rosszindulatú programok azon tendenciája, hogy adatokat küldenek vissza a kiberbűnözőknek, rávilágít a kimenő forgalom figyelésének szükségességére a támadásjelzők szempontjából.

A személyre szabott trójai falvakat, például azokat, amelyeknek meghatározott célpontjuk van, nehéz észlelni.

2.3.4

## Trójai faló osztályozása

A trójai falókat általában aszerint osztályozzák, hogy milyen károkat okoznak, vagy hogyan sértik meg a rendszert, ahogy az a táblázatban is látható.

| **A trójai faló típusa** | **Leírás** |
| --- | --- |
| Távoli hozzáférés | Engedélyezi a jogosulatlan távoli hozzáférést. |
| Adatküldés | Érzékeny adatokkal, például jelszavakkal látja el a fenyegetés szereplőjét. |
| Pusztító | Elrontja vagy törli a fájlokat. |
| Meghatalmazott | Az áldozat számítógépét forráseszközként használja támadások indításához és egyéb illegális tevékenységek végrehajtásához. |
| FTP | Engedélyezi a jogosulatlan fájlátviteli szolgáltatásokat a végeszközökön. |
| Biztonsági szoftver letiltása | Leállítja a víruskereső programok vagy tűzfalak működését. |
| Szolgáltatásmegtagadás (DoS) | Lelassítja vagy leállítja a hálózati tevékenységet. |
| Billentyűzetfigyelő | Aktívan megkísérel bizalmas információkat, például hitelkártyaszámokat ellopni azáltal, hogy rögzíti a webes űrlapon leadott billentyűleütéseket. |

2.3.5

## Férgek

A számítógépes férgek hasonlóak a vírusokhoz, mert replikálódnak és ugyanolyan típusú károkat okozhatnak. Pontosabban, a férgek úgy replikálják magukat, hogy függetlenül használják ki a hálózatok sebezhetőségeit. A férgek lelassíthatják a hálózatokat, miközben rendszerről rendszerre terjednek.

Míg a vírus futtatásához gazdaprogramra van szükség, a férgek maguk is futhatnak. A kezdeti fertőzésen kívül már nem igényelnek felhasználói részvételt. Miután egy gazdagép megfertőződött, a féreg nagyon gyorsan képes terjedni a hálózaton.

A férgek felelősek az internet legpusztítóbb támadásaiért. 2001-ben a Code Red féreg kezdetben 658 szervert fertőzött meg. 19 órán belül a féreg több mint 300 000 szervert fertőzött meg.

Kezdeti kód Vörös féregfertőzés

Code Red fertőzés 19 órával később



Az SQL Slammer féreg kezdeti fertőzése az internetet megevő féreg néven ismert. Az SQL Slammer egy szolgáltatásmegtagadási (DoS) támadás volt, amely kihasználta a Microsoft SQL Server puffertúlcsordulási hibáját. A csúcson a fertőzött szerverek száma 8,5 másodpercenként megduplázódott. Ez az oka annak, hogy 30 percen belül több mint 250 000 gazdagépet tudott megfertőzni. Amikor 2003. január 25-én megjelent a hétvégén, megzavarta az internetet, a pénzintézeteket, az ATM-es pénzkiadó automatákat és egyebeket. Ironikus módon a biztonsági rés javítását 6 hónappal korábban kiadták. A fertőzött szervereken nem alkalmazták a frissített javítást. Ez ébresztő volt sok szervezet számára egy olyan biztonsági szabályzat bevezetésére, amely megköveteli a frissítések és javítások időben történő alkalmazását.

Kezdeti SQL Slammer fertőzés

SQL Slammer fertőzés 30 perccel később



A férgek hasonló tulajdonságokkal rendelkeznek. Valamennyien kihasználnak egy lehetővé tevő sebezhetőséget, módjuk van elterjedni, és mindegyik tartalmaz egy hasznos terhet.

2.3.6

## Féreg alkatrészek

Az évek során kialakult mérséklő technikák ellenére a férgek tovább fejlődtek, és állandó veszélyt jelentenek. A férgek idővel kifinomultabbakká váltak, de továbbra is általában a szoftveralkalmazások gyenge pontjainak kihasználásán alapulnak.

Az animáció egy féregtámadás 3 összetevőjét mutatja be; lehetővé teszi a sebezhetőséget, a terjedési mechanizmust és a hasznos terhelést.

### Gyakori féregminta

* Sebezhetőség engedélyezése
* Szaporítási mechanizmus
* Hasznos teher

A legtöbb féregtámadás három összetevőből áll, amint azt a fenti animáció felsorolja.

* **Sebezhetőség engedélyezése** – A féreg kihasználó mechanizmussal, például e-mail-melléklet, végrehajtható fájl vagy trójai program segítségével telepíti magát a sérülékeny rendszerre.
* **Terjedési mechanizmus** – Miután hozzáfért egy eszközhöz, a féreg megismétli magát, és új célpontokat keres.
* **Payload** – Minden olyan rosszindulatú kód, amely valamilyen műveletet eredményez, hasznos teher. Ezt leggyakrabban egy hátsó ajtó létrehozására használják, amely lehetővé teszi a fenyegetés szereplőinek hozzáférést a fertőzött gazdagéphez, vagy DoS támadás létrehozására.

A férgek olyan önálló programok, amelyek egy rendszert támadva kihasználnak egy ismert biztonsági rést. Sikeres kihasználás esetén a féreg átmásolja magát a támadó gazdagépről az újonnan kihasznált rendszerre, és a ciklus újra kezdődik. A terjedési mechanizmusaikat általában nehezen észlelhető módon alkalmazzák.

A Code Red féreg által használt szaporítási technika az ábrán látható.

Az ábra a Code Red féreg terjedésének lépéseit mutatja be. Ezek a lépések a következők: 1. lépés – Terjeszkedés 19 napig.2. lépés – Indítsa el a DoS-támadást a következő 7 napra. 3. lépés – Álljon le, és hagyja nyugodni néhány napig. 4. lépés - Ismételje meg a ciklust.

### Code Red Worm Propagation

Szaporítás 19 napig.Indítsa el a DoS támadást a következő 7 napra.Hagyd abba, és aludj néhány napig.Ismételje meg a ciklust.

**Megjegyzés** : A férgek soha nem hagyják abba az interneten való terjedést. Kiszabadulásuk után a férgek tovább szaporodnak, amíg az összes lehetséges fertőzési forrást megfelelően befoltozzák.

2.3.7

## Ransomware

A fenyegetés szereplői vírusokat, férgeket és trójai falókat használtak rakományaik szállítására és egyéb rosszindulatú okokra. A rosszindulatú programok azonban folyamatosan fejlődnek.

Jelenleg a legdominánsabb kártevő a ransomware. A Ransomware olyan rosszindulatú program, amely megtagadja a hozzáférést a fertőzött számítógépes rendszerhez vagy annak adataihoz. A kiberbűnözők ezután fizetést követelnek a számítógépes rendszer felszabadításáért.

A Ransomware a történelem legjövedelmezőbb rosszindulatú programjává fejlődött. 2016 első felében az egyéni és vállalati felhasználókat egyaránt megcélzó ransomware kampányok szélesebb körben elterjedtek és erősebbek lettek.

Több tucat ransomware változat létezik. A Ransomware gyakran használ titkosítási algoritmust a rendszerfájlok és adatok titkosításához. Az ismert zsarolóvírus-titkosítási algoritmusok többségét nem lehet könnyen visszafejteni, így az áldozatoknak nem marad más választásuk, mint kifizetni a kért árat. A fizetések általában Bitcoinban történnek, mivel a bitcoin felhasználói névtelenek maradhatnak. A Bitcoin egy nyílt forráskódú, digitális valuta, amelyet senki sem birtokol és nem irányít.

Az e-mail és a rosszindulatú reklámozás, más néven malvertising, a zsarolóvírus-kampányok vektorai. Társadalmi manipulációt is alkalmaznak, például amikor a magukat biztonsági technikusnak nevező kiberbűnözők otthont hívnak, és rábeszélik a felhasználókat, hogy csatlakozzanak egy olyan webhelyhez, amely letölti a zsarolóprogramot a felhasználó számítógépére.

2.3.8

## Egyéb rosszindulatú programok

Íme néhány példa a modern rosszindulatú programok különféle fajtáira:

| **A rosszindulatú program típusa** | **Leírás** |
| --- | --- |
| Spyware | Arra használják, hogy információkat gyűjtsenek egy felhasználóról, és elküldjék az információkat egy másik entitásnak a felhasználó beleegyezése nélkül. A kémprogramok lehetnek rendszerfigyelők, trójai faló, reklámprogramok, nyomkövető cookie-k és kulcsnaplózók. |
| Adware | Idegesítő felugró ablakokat jelenít meg, hogy bevételt generáljon a szerzőjének. A rosszindulatú program a felkeresett webhelyek nyomon követésével elemezheti a felhasználók érdeklődését. Ezután felugró hirdetéseket küldhet ezekre a webhelyekre. |
| Scareware | Tartalmazza az átverő szoftvereket, amelyek social engineering segítségével sokkolnak vagy szorongást keltenek azáltal, hogy fenyegetés érzékelését keltik. Általában egy gyanútlan felhasználóra irányul, és megpróbálja rávenni a felhasználót, hogy megfertőzze a számítógépet a hamis fenyegetés elhárítása érdekében. |
| Adathalászat | Megkísérli meggyőzni az embereket, hogy érzékeny információkat adjanak ki. Ilyen például a banktól kapott e-mail, amelyben arra kérik a felhasználókat, hogy közöljék számla- és PIN-kódjukat. |
| Rootkitek | Kompromittált rendszerre telepítve. A telepítés után továbbra is elrejti a behatolást, és kiváltságos hozzáférést biztosít a fenyegetés szereplőjének. |

Ez a lista az internet fejlődésével tovább fog bővülni. Mindig új rosszindulatú programokat fejlesztenek ki. A kiberbiztonsági műveletek egyik fő célja az új rosszindulatú programok megismerése és azok azonnali enyhítése.

2.3.9

## Gyakori rosszindulatú programok

A kiberbűnözők folyamatosan módosítják a rosszindulatú programok kódját, hogy megváltoztassák a terjedési és a számítógépek megfertőzésének módját. A legtöbb azonban hasonló tüneteket produkál, amelyek a hálózat és az eszköznapló figyelésével észlelhetők.

A rosszindulatú programokkal fertőzött számítógépek gyakran a következő tünetek közül egyet vagy többet mutatnak:

* Furcsa fájlok, programok vagy asztali ikonok megjelenése
* A víruskereső és tűzfalprogramok kikapcsolnak vagy újrakonfigurálják a beállításokat
* A számítógép képernyője lefagy, vagy a rendszer összeomlik
* Az e-mailek spontán módon, az Ön tudta nélkül kerülnek elküldésre a névjegyzékébe
* A fájlok módosultak vagy törölve lettek
* Megnövekedett CPU és/vagy memóriahasználat
* Problémák a hálózatokhoz való csatlakozáskor
* Lassú számítógép vagy webböngésző sebesség
* Ismeretlen folyamatok vagy szolgáltatások futnak
* Ismeretlen TCP vagy UDP portok nyitva vannak
* A csatlakozások az interneten lévő gazdagépekhez felhasználói beavatkozás nélkül jönnek létre
* Furcsa számítógépes viselkedés

**Megjegyzés:** A rosszindulatú programok viselkedése nem korlátozódik a fenti listára.

2.3.10

## Ellenőrizze, hogy megértette – rosszindulatú program

Az űrlap teteje

Ellenőrizze, hogy megértette-e a rosszindulatú programokat a következő kérdések megválaszolásával.

1. Milyen típusú rosszindulatú programok hajtanak végre tetszőleges kódot, és telepítik maguknak másolatait a fertőzött számítógép memóriájába? Ennek a rosszindulatú programnak az a fő célja, hogy automatikusan replikálja magát rendszerről rendszerre a hálózaton keresztül.



trójai faló



adware



ransomware



féreg

1. Milyen típusú rosszindulatú programok jelenítenek meg általában bosszantó felugró ablakokat, hogy bevételt termeljenek a szerzőjének?



adware



ransomware



ijesztő



adathalászat

1. Milyen típusú rosszindulatú program titkosítja a meghajtón lévő összes adatot, és Bitcoin kriptovalutában kér fizetést a fájlok titkosításának feloldásához?



adathalászat



ijesztő



ransomware



vírus

1. Milyen típusú rosszindulatú programok próbálják rávenni az embereket, hogy közöljék személyazonosításra alkalmas adataikat (PII)?



adathalászat



rootkit



ransomware



trójai faló

# Gyakori hálózati támadások – felderítés, hozzáférés és közösségi tervezés

2.4.1

## A hálózati támadások típusai

A rosszindulatú programok a hasznos teher kézbesítésének eszközei. Kiszállításkor és telepítéskor a hasznos teher felhasználható különféle, hálózattal kapcsolatos támadások kiváltására belülről. A fenyegetés szereplői kívülről is támadhatják a hálózatot.

Miért támadják a fenyegetés szereplői a hálózatokat? Számos motívum létezik, köztük a pénz, a kapzsiság, a bosszú, vagy a politikai, vallási vagy szociológiai meggyőződés. A LAN biztonságának biztosítása érdekében a hálózatbiztonsági szakembereknek meg kell érteniük, hogy milyen típusú támadásokat alkalmaznak ezeknek a fenyegetéseknek a leküzdésére.

A támadások mérséklése érdekében célszerű először kategorizálni a különböző típusú támadásokat. A hálózati támadások kategorizálásával lehetőség nyílik a támadások típusainak kezelésére, nem pedig az egyedi támadásokra.

Bár nincs szabványosított módszer a hálózati támadások kategorizálására, a kurzusban használt módszer a támadásokat három fő kategóriába sorolja.

* Felderítő támadások
* Access Attacks
* DoS támadások

2.4.2

## Felderítő támadások

A felderítés információgyűjtés. Ez hasonló ahhoz, hogy a tolvaj felméri a környéket, háztól-házig járva úgy, mintha eladna valamit. A tolvaj valójában olyan veszélyeztetett otthonokat keres, amelyekbe behatolhat, például lakatlan lakásokat, könnyen nyitható ajtókkal vagy ablakokkal rendelkező lakásokat, valamint azokat, amelyekben nincs biztonsági rendszer vagy biztonsági kamera.

A fenyegető szereplők felderítő (vagy felderítő) támadásokat használnak a rendszerek, szolgáltatások vagy sebezhetőségek jogosulatlan felderítésére és feltérképezésére. A felderítési támadások megelőzik a hozzáférési támadásokat vagy a DoS támadásokat.

A rosszindulatú fenyegetés szereplői által felderítő támadások végrehajtására használt technikák egy részét a táblázat ismerteti.

| **Technika** | **Leírás** |
| --- | --- |
| **Végezze el a cél információs lekérdezését** | A fenyegetés szereplője kezdeti információkat keres egy célpontról. Különféle eszközök használhatók, beleértve a Google keresést, a szervezetek webhelyét, a whois-t stb. |
| **Indítsa el a célhálózat ping-sweepjét** | Az információs lekérdezés általában felfedi a célpont hálózati címét. A fenyegetés szereplője most ping sweep-et kezdeményezhet annak meghatározására, hogy mely IP-címek aktívak. |
| **Indítsa el az aktív IP-címek portellenőrzését** | Ez az elérhető portok vagy szolgáltatások meghatározására szolgál. Portszkennerek például az Nmap, a SuperScan, az Angry IP Scanner és a NetScanTools. |
| **Futtasson sebezhetőség-ellenőrzőket** | Ennek célja az azonosított portok lekérdezése a gazdagépen futó alkalmazás és operációs rendszer típusának és verziójának meghatározásához. Ilyen eszközök például a Nipper, a Secuna PSI, a Core Impact, a Nessus v6, a SAINT és az Open VAS. |
| **Futtasson kizsákmányoló eszközöket** | A fenyegetés szereplője most megkísérli felfedezni a sebezhető szolgáltatásokat, amelyek kihasználhatók. Számos sebezhetőség-kihasználó eszköz létezik, köztük a Metasploit, a Core Impact, az Sqlmap, a Social Engineer Toolkit és a Netsparker. |

Az egyes gombokra kattintva megtekintheti a felderítő támadás előrehaladását az információlekérdezéstől a ping sweepig és a port vizsgálatig.

Internetes információs lekérdezések

Ping Sweepek végrehajtása

Port vizsgálat végrehajtása

Kattintson az ábrán a Lejátszás gombra, ha meg szeretné tekinteni egy fenyegetett szereplő animációját, amely a whois paranccsal keres információt a célpontról.

Az animáció egy fenyegetést ábrázoló szereplőt mutat be, amely hálózathoz csatlakozik p cs-vel és szerverekkel. Az animáció azt mutatja, hogy a fenyegetés szereplője írja be a címet[http://www.whois.net](http://www.whois.net/)egy webböngészőbe. Az animáció most azt mutatja, hogy ki keres mindenkit, aki rekord. a fenyegetés szereplője beír a cisco.com webhelyre, hogy megkeresse a rekordját. a rekord a cisco.com webhelyet és a Cisco San Joséban található fizikai címét mutatja.

Fenyegető színész

2.4.3

## Videó - Felderítő támadások

Play Video

2.4.4

## Access Attacks

A hozzáférési támadások a hitelesítési szolgáltatások, az FTP-szolgáltatások és a webszolgáltatások ismert sebezhetőségeit használják ki. Az ilyen típusú támadások célja webfiókokba, bizalmas adatbázisokba és más érzékeny információkhoz való hozzáférés.

A fenyegetés szereplői hozzáférési támadásokat használnak a hálózati eszközök és számítógépek ellen, hogy adatokat kérjenek le, hozzáférést kapjanak, vagy a hozzáférési jogosultságokat rendszergazdai állapotba emeljék.

**Jelszavas támadások**

Jelszavas támadás során a fenyegetés szereplője különféle módszerekkel próbálja felfedezni a kritikus rendszerjelszavakat. A jelszavas támadások nagyon gyakoriak, és különféle jelszótörő eszközökkel indíthatók.

**Hamisító támadások**

Hamisítási támadások esetén a fenyegetést fellépő eszköz adatok meghamisításával próbál meg egy másik eszköznek kiadni magát. A gyakori hamisítási támadások közé tartozik az IP-hamisítás, a MAC-hamisítás és a DHCP-hamisítás. Ezekről a hamisítási támadásokról a modul későbbi részében részletesebben lesz szó

Egyéb Access támadások a következők:

* Bizalomkizsákmányolások
* Port átirányítások
* Man-in-the-middle támadások
* Puffer túlcsordulási támadások

Az egyes gombokra kattintva megtekintheti a hozzáférési támadások illusztrációját és magyarázatát.

Példa a bizalom kihasználására

Port átirányítási példa

Man-in-the-Middle Attack példa

Puffer túlcsordulási támadás

A bizalom kihasználását célzó támadás során a fenyegetés szereplői jogosulatlan jogosultságokat használnak, hogy hozzáférjenek egy rendszerhez, esetleg veszélyeztetve a célpontot. Kattintson az ábrán a Lejátszás gombra a bizalom kihasználására vonatkozó példa megtekintéséhez.

The animation shows a threat actor at a computer that is not connected. There is a network with a computer labeled system a, another computer labeled system b, and a cloud labeled internet. Each of these connect separately to a firewall. As the animation plays, the words system a trusts system b appear over system a. the words system b trusts everyone appear over system b. Next to the threat actor, the words goal: an attacker wants to gain access to system a. system a blinks. under system a are the words user=psmith; pat smith. a bubble appears over the threat actor that says i can't get access to system a but system be is open. the words user=psmith; pat smith appear next to the threat actor. an arrow goes from the threat actor to the internet, to the firewall, to system b. The words compromised by attacker user=psmith; pat smith appear under system b and system b is shown as compromised. the workds i have control of system b and now have access to system a appear in the threat actors bubble. an arrow goes directly from the threat actor to system a where system a is shown as compromised.

A rendszer

B rendszer

Fenyegető színész

Az A rendszer bízik a B rendszerben

A B rendszer mindenkiben megbízik

user = psmith;  
Pat Smith

user = psmith;  
Pat Smith

Támadó  
felhasználó által feltört = psmith;  
Pat Smith

Internet

Én irányítom a B rendszert, és most hozzáférek az A rendszerhez.

Nem tudok hozzáférni az A rendszerhez, de a B rendszer nyitva van.

2.4.5

## Videó – Hozzáférés és szociális tervezési támadások

Play Video

2.4.6

## Social Engineering támadások

A közösségi manipuláció olyan hozzáférési támadás, amellyel az egyéneket műveletek végrehajtására vagy bizalmas információk felfedésére próbálják manipulálni. Egyes social engineering technikákat személyesen hajtanak végre, míg mások telefont vagy internetet használhatnak.

A szociális mérnökök gyakran az emberek segítőkészségére hagyatkoznak. Az emberek gyengeségeit is zsákmányolják. Például egy fenyegetőző felhívhat egy felhatalmazott alkalmazottat egy sürgős problémával, amely azonnali hálózati hozzáférést igényel. A fenyegetőző fellebbezhet az alkalmazott hiúságára, tekintélyre hivatkozhat néveldobási technikákkal, vagy hivatkozhat az alkalmazott kapzsiságára.

A social engineering technikákkal kapcsolatos információkat a táblázat tartalmazza.

| **Social Engineering Attack** | **Leírás** |
| --- | --- |
| Pretextus | A fenyegetés szereplője úgy tesz, mintha személyes vagy pénzügyi adatokra lenne szüksége a címzett személyazonosságának megerősítéséhez. |
| Adathalászat | A fenyegetőző cselekvő csalárd e-mailt küld, amelyet legitim, megbízható forrásból származónak álcáznak, hogy rávegye a címzettet, hogy rosszindulatú programot telepítsen eszközére, vagy személyes vagy pénzügyi információkat osszon meg. |
| Lándzsa adathalászat | A fenyegetés szereplői célzott adathalász támadást hoznak létre egy adott személyre vagy szervezetre szabva. |
| Levélszemét | Levélszemétként is ismert, ez egy kéretlen e-mail, amely gyakran tartalmaz káros hivatkozásokat, rosszindulatú programokat vagy megtévesztő tartalmat. |
| Valamit valamiért | Ezt néha „Quid pro quo”-nak nevezik, amikor egy fenyegetőző személy személyes adatokat kér egy féltől, például ajándékért cserébe. |
| Beetetés | Egy fenyegetőző egy rosszindulatú programmal fertőzött pendrive-ot nyilvános helyen hagy. Egy áldozat megtalálja a meghajtót, és gyanútlanul behelyezi a laptopjába, és véletlenül rosszindulatú programot telepít. |
| Megszemélyesítés | Az ilyen típusú támadások során a fenyegetőző valaki másnak adja ki magát, hogy elnyerje az áldozat bizalmát. |
| Háttérzárás | Itt a fenyegetettség szereplője gyorsan követi a felhatalmazott személyt egy biztonságos helyre, hogy hozzáférjen egy biztonságos területhez. |
| Vállas szörfözés | Ilyenkor egy fenyegetőző észrevétlenül átnéz valakinek a válla fölött, hogy ellopja a jelszavait vagy más információit. |
| Dumpster búvárkodás | Ez az a hely, ahol a fenyegetettség szereplője a kukák között turkál, hogy bizalmas dokumentumokat fedezzen fel. |

A Social Engineer Toolkit (SET) célja, hogy segítse a white hat hackereket és más hálózatbiztonsági szakembereket abban, hogy social engineering támadásokat hozzanak létre saját hálózataik tesztelése érdekében. Ez egy menüalapú eszközkészlet, amely segíti a social engineering támadások indítását. A SET kizárólag oktatási célokat szolgál. Ingyenesen elérhető az interneten.

A vállalatoknak fel kell tanítaniuk felhasználóikat a social engineering kockázatairól, és stratégiákat kell kidolgozniuk a személyazonosság telefonon, e-mailben vagy személyesen történő érvényesítésére.

Az ábra az ajánlott gyakorlatokat mutatja, amelyeket minden felhasználónak követnie kell.

Az ábra a következő 8 gyakorlatot mutatja be a social engineering támadások elleni védekezéshez: Soha senkinek ne adja meg felhasználónevét / jelszavát; Mindig semmisítse meg a bizalmas információkat a szervezet szabályzatának megfelelően; Mindig jelentse a gyanús személyeket; Mindig zárja le számítógépét, vagy jelentkezzen ki belőle, ha felügyelet nélkül van; Soha ne használja fel újra a munkával kapcsolatos jelszavakat; Soha ne adjon ki munkával kapcsolatos információkat a közösségi oldalakon; Soha ne nyissa meg a nem megbízható forrásból származó e-maileket; Soha ne hagyja felhasználónevét/jelszavát olyan helyen, ahol könnyen megtalálhatóak.

### Ajánlott Social Engineering védelmi gyakorlatok

Védelem a social engineering támadásokkal szembenSoha ne adja meg felhasználónevét/jelszavát senkinek.A bizalmas információkat mindig a szervezet szabályzatának megfelelően semmisítse meg.Mindig jelentse a gyanús személyeket.Mindig zárja le számítógépét, vagy jelentkezzen ki belőle, ha felügyelet nélkül van.Soha ne használja újra a munkával kapcsolatos jelszavakat.Soha ne adjon ki munkával kapcsolatos információkat a közösségi oldalakon.Soha ne nyisson meg nem megbízható forrásból származó e-maileket.Soha ne hagyja felhasználónevét/jelszavát olyan helyen, ahol könnyen megtalálhatóak.

2.4.7

## A leggyengébb láncszem megerősítése

A kiberbiztonság csak annyira erős, amennyire a leggyengébb láncszeme. Mióta a számítógépek és más internetkapcsolattal rendelkező eszközök életünk elengedhetetlen részévé váltak, már nem tűnnek újnak vagy másnak. Az emberek nagyon lazán használják ezeket az eszközöket, és ritkán gondolnak a hálózat biztonságára. A kiberbiztonság leggyengébb láncszeme a szervezeten belüli személyzet lehet, és a társadalmi tervezés komoly biztonsági fenyegetést jelenthet. Emiatt az egyik leghatékonyabb biztonsági intézkedés, amelyet egy szervezet megtehet, a személyzet képzése és a „biztonságtudatos kultúra” kialakítása.

# Hálózati támadások – szolgáltatásmegtagadás, puffertúlcsordulás és kijátszás

2.5.1

## Videó – Szolgáltatásmegtagadási támadások

Play Video

2.5.2

## DoS és DDoS támadások

A szolgáltatásmegtagadási (DoS) támadások valamilyen módon megszakítják a hálózati szolgáltatásokat a felhasználók, eszközök vagy alkalmazások számára. A DoS-támadásoknak két fő típusa van:

* **Elsöprő mennyiségű forgalom** – A fenyegetés szereplője hatalmas mennyiségű adatot küld olyan sebességgel, amelyet a hálózat, a gazdagép vagy az alkalmazás nem tud kezelni. Emiatt lelassul az átvitel és a válaszidő. Ezenkívül összeomolhat egy eszköz vagy szolgáltatás.
* **Rosszindulatúan formázott csomagok** – A fenyegetés szereplője rosszindulatúan formázott csomagot küld egy gazdagépnek vagy alkalmazásnak, és a fogadó nem tudja kezelni. Emiatt a fogadó eszköz nagyon lassan fut vagy összeomlik.

Kattintson az egyes gombra a DoS és DDoS támadások illusztrációjához és magyarázatához.

DoS Attack

DDoS támadás

A Distributed DoS Attack (DDoS) hasonló a DoS támadáshoz, de több, összehangolt forrásból származik. Például egy fenyegetés szereplője fertőzött gazdagépek hálózatát építi ki, amelyeket zombiknak neveznek. A fenyegetés szereplője egy parancs- és vezérlőrendszer (CnC) segítségével irányító üzeneteket küld a zombiknak. A zombik folyamatosan szkennelnek és több gazdát fertőznek meg rosszindulatú botokkal. A bot rosszindulatú programot úgy tervezték, hogy megfertőzze a gazdagépet, és ez egy zombivá tegye, amely képes kommunikálni a CnC rendszerrel. A zombik gyűjteményét botnetnek hívják. Amikor készen áll, a fenyegetés szereplője utasítja a CnC rendszert, hogy a zombik botnetjét hajtsa végre DDoS támadást.

Kattintson az ábrán a Lejátszás gombra a DDoS támadás animációinak megtekintéséhez.

Az animáció azt mutatja be, hogy egy fenyegetés szereplője parancsot küld két botnak, hogy forgalmat küldjön egy webszerverre, hogy túlterhelje azt.

A DDoS kód aktiválva.

WWW.QZXBANK.COM  
webszerver

Fenyegető színész

Internet

Megfertőztem a számítógépeket az interneten keresztül a DDoS kóddal. Most aktiválom mindet.

Túl nagy forgalom miatt vagyok túlterhelve.

A DDoS kód aktiválva.

2.5.3

A DoS támadások komoly kockázatot jelentenek, mivel megszakítják a kommunikációt, és jelentős idő- és pénzveszteséget okoznak. Ezeket a támadásokat viszonylag egyszerű végrehajtani, még egy szakképzetlen fenyegetőző által is.

Kattintson az ábrán a Lejátszás gombra a DoS támadás animációjának megtekintéséhez.

## A DDoS támadások összetevői

Ha a fenyegetés szereplői sok gazdagépet kompromittálhatnak, végrehajthatnak egy elosztott DoS-támadást (DDoS). A DDoS támadások szándékukat tekintve hasonlóak a DoS támadásokhoz, azzal a különbséggel, hogy a DDoS támadások mértéke megnövekszik, mivel több, összehangolt forrásból származik, ahogy az az ábrán is látható. Egy DDoS-támadás több száz vagy több ezer forrást használhat, mint az IoT-alapú DDoS-támadásoknál.

Az ábra egy fenyegetés szereplőt jelenít meg, amely kezelőknek nevezett szerverekhez kapcsolódik. A kezelők számos zombi csatlakoztatására és vezérlésére szolgálnak szolgáltatásmegtagadási támadásokhoz. A botmester utasítására a zombik támadást indítanak egyetlen áldozat házigazdája ellen, hogy elnyomják és elérhetetlenné tegyék.

Ügyfél/támadóÜgynökök/  
ZombikKezelőkA támadó sok köztes gépet, úgynevezett zombit használ a támadás indításához.Áldozat

A következő kifejezések a DDoS támadás összetevőinek leírására szolgálnak:

| **Összetevő** | **Leírás** |
| --- | --- |
| zombik | Ez a kompromittált gazdagépek (azaz ügynökök) csoportjára vonatkozik. Ezek a gazdagépek rosszindulatú kódokat futtatnak, amelyeket robotoknak (vagyis botoknak) neveznek. A zombi rosszindulatú program folyamatosan próbál önterjeszteni, mint egy féreg. |
| botok | A botok olyan rosszindulatú programok, amelyek célja a gazdagép megfertőzése és a kezelőrendszerrel való kommunikáció. A robotok naplózhatják a billentyűleütéseket, begyűjthetik a jelszavakat, rögzíthetik és elemzik a csomagokat stb. |
| botnet | Ez a zombik egy csoportjára vonatkozik, amelyeket önterjesztő rosszindulatú programokkal (azaz botokkal) fertőztek meg, és amelyeket kezelők irányítanak. |
| kezelők | **Ez egy elsődleges parancs- és vezérlő (CnC** vagy **C2)** szerverre vonatkozik, amely zombicsoportokat irányít. A botnet létrehozója használhatja az Internet Relay Chat (IRC) vagy a C2 szerveren lévő webszervert a zombik távoli irányításához. |
| botmaster | Ez a fenyegetés szereplője, aki irányítja a botnetet és a kezelőket. |

**Megjegyzés** : létezik egy feketegazdaság, ahol botneteket lehet vásárolni (és eladni) névleges díj ellenében. Ez a fenyegetés szereplői számára fertőzött gazdagépek botnetjeit biztosíthatja, amelyek készek DDoS-támadást indítani a kiválasztott célpont ellen.

2.5.4

## Videó - Mirai Botnet

A Mirai egy rosszindulatú program, amely az alapértelmezett bejelentkezési adatokkal konfigurált tárgyak internete (IoT) eszközöket célozza meg. Mirai célpontjainak többségét a zárt láncú televíziós (CCTV) kamerák tették ki. Egy brute force szótári támadást használva Mirai végigfutott az interneten széles körben ismert alapértelmezett felhasználónevek és jelszavak listáján.

* root/default
* gyökér/1111
* gyökér/54321
* admin/admin1234
* admin1/jelszó
* vendég/12345
* tech/tech
* támogatás/támogatás

Sikeres hozzáférést követően a Mirai az ezeken az eszközökön futó Linux-alapú BusyBox segédprogramokat vette célba. Ezeket a segédprogramokat arra használták, hogy az eszközöket botokká alakítsák, amelyek egy botnet részeként távolról is vezérelhetők. A botnetet ezután egy elosztott szolgáltatásmegtagadási (DDoS) támadás részeként használták. 2016 szeptemberében egy több mint 152 000 CCTV-ből és digitális videorögzítőből (DVR) álló Mirai botnet felelős az addig ismert legnagyobb DDoS-támadásért. Az 1 Tb/s-ot meghaladó csúcsforgalommal leépítette egy franciaországi székhelyű webtárhely-szolgáltató tárhelyszolgáltatását.

2016 októberében megtámadták a Dyn, egy DNS-szolgáltató szolgáltatásait, ami internetkimaradásokat okozott több millió felhasználó számára az Egyesült Államokban és Európában.

Játssza le a videót, és tekintse meg annak bemutatóját, hogy egy botnet-alapú DDoS támadás hogyan teszi elérhetővé a szolgáltatásokat.

Megjegyzés: 2017 decemberében három amerikai fenyegetés szereplője bűnösnek vallotta magát, mert összeesküvést kötöttek „DDoS-támadások végrehajtására az Egyesült Államokban és külföldön található webhelyek és webtárhely-cégek ellen”. A három elkövetőt akár 10 év börtönbüntetésre és 250 000 dollár pénzbüntetésre is ítélhetik.

Play Video

2.5.5

## Puffer túlcsordulási támadás

Az ábrán egy fenyegetőző látható egy laptoppal. egy nyíl megy a fenyegetés szereplőjétől az interneten, két útválasztón, egy kapcsolón keresztül, és egy áldozatként megjelölt szerverre érkezik. négy egymásra rakott boríték van a kapcsoló mellett.

R2R1S5

ÁldozatInternet

A puffertúlcsordulási DoS támadás során a fenyegetés szereplőjének célja, hogy megtalálja a rendszermemóriával kapcsolatos hibát a szerveren, és azt kihasználja. A puffermemória kihasználása váratlan értékekkel túlterhelve általában működésképtelenné teszi a rendszert, ami DoS támadást idéz elő.

Például egy fenyegetés szereplője a kiszolgálón futó alkalmazás által vártnál nagyobb bemenetet ír be. Az alkalmazás elfogadja a nagy mennyiségű bemenetet, és eltárolja a memóriában. Ennek eredményeként felhasználhatja a kapcsolódó memóriapuffert, és esetleg felülírhatja a szomszédos memóriát, ami végül megrongálhatja a rendszert, és összeomolhat.

A hibásan formázott csomagok használatának korai példája a **Halál Pingje** volt . Ebben az örökölt támadásban a fenyegetés szereplője egy ping of death-t küldött, amely a 65 535 bájtos maximális csomagméretnél nagyobb IP-csomagban lévő visszhang kérés volt. A fogadó gazdagép nem tudna kezelni egy ekkora csomagot, és az összeomlik.

A puffertúlcsordulási támadások folyamatosan fejlődnek. Például a közelmúltban egy távoli szolgáltatásmegtagadási támadással kapcsolatos sebezhetőséget fedeztek fel a Microsoft Windows 10 rendszerben. Konkrétan, egy fenyegetést okozó szereplő rosszindulatú kódot hozott létre a hatókörön kívüli memória eléréséhez. Amikor ehhez a kódhoz hozzáfér a Windows AHCACHE.SYS folyamata, rendszerösszeomlást kísérel meg előidézni, és megtagadja a szolgáltatást a felhasználótól. Keressen az interneten a „TALOS-2016-0191 blogon”, hogy felkeresse a Cisco Talos fenyegetésekkel foglalkozó hírszerzési webhelyét, és elolvassa egy ilyen támadás leírását.

**Megjegyzés** : Becslések szerint a rosszindulatú támadások egyharmada puffertúlcsordulás eredménye.

2.5.6

## Kijátszási módszerek

A fenyegetés szereplői már régen megtanulták, hogy „bújni annyi, mint boldogulni”. Ez azt jelenti, hogy rosszindulatú programjaik és támadási módszereik akkor a leghatékonyabbak, ha nem észlelik őket. Emiatt sok támadás lopakodó kijátszási technikákat használ a támadások hasznos terhének álcázására. Céljuk az észlelés megakadályozása a hálózat és a gazdagép védelmének kikerülésével.

A fenyegetés szereplői által használt kijátszási módszerek közé tartozik:

| **Kijátszási módszer** | **Leírás** |
| --- | --- |
| Titkosítás és alagút | Ez a kijátszási technika alagútkezelést használ a rosszindulatú programok fájlok elrejtésére, vagy titkosítást a kódolásra. Ez megnehezíti számos biztonsági észlelési technika számára a rosszindulatú programok észlelését és azonosítását. Az alagútképzés jelentheti az ellopott adatok elrejtését a törvényes csomagok belsejében. |
| Erőforrások kimerülése | Ez a kijátszási technika túlságosan lefoglalja a célállomást a biztonsági észlelési technikák megfelelő használatához. |
| A forgalom széttagoltsága | Ez a kijátszási technika a rosszindulatú rakományt kisebb csomagokra osztja fel, hogy megkerülje a hálózati biztonsági észlelést. Miután a töredezett csomagok megkerülték a biztonsági észlelőrendszert, a kártevő újra összeáll, és elkezdhet érzékeny adatokat küldeni a hálózatról. |
| Protokoll szintű félreértelmezés | Ez a kijátszási technika akkor fordul elő, ha a hálózati védelmek nem kezelik megfelelően a PDU olyan jellemzőit, mint az ellenőrző összeg vagy a TTL érték. Ez ráveheti a tűzfalat, hogy figyelmen kívül hagyja azokat a csomagokat, amelyeket ellenőriznie kell. |
| Forgalom helyettesítése | Ebben a kijátszási technikában a fenyegetés szereplője megpróbál becsapni egy IPS-t azáltal, hogy elhomályosítja a rakományban lévő adatokat. Ez más formátumba történő kódolással történik. A fenyegetés szereplője például Unicode kódolású forgalmat használhat ASCII helyett. Az IPS nem ismeri fel az adatok valódi jelentését, de a célvégrendszer ki tudja olvasni az adatokat. |
| Forgalmi beillesztés | Hasonló a forgalom helyettesítéséhez, de a fenyegetés szereplője extra bájtokat illeszt be egy rosszindulatú adatsorozatba. Az IPS-szabályok kihagyják a rosszindulatú adatokat, és elfogadják a teljes adatsort. |
| Elforgatás | Ez a technika azt feltételezi, hogy a fenyegető szereplő kompromittál egy belső gazdagépet, és tovább akarja terjeszteni a hozzáférését a veszélyeztetett hálózatba. Példa erre egy fenyegetést okozó szereplő, aki hozzáfért a rendszergazdai jelszóhoz egy feltört gazdagépen, és ugyanazokkal a hitelesítő adatokkal próbál bejelentkezni egy másik gazdagépre. |
| Rootkitek | A rootkit egy összetett támadóeszköz, amelyet tapasztalt fenyegetés szereplői használnak. Integrálódik az operációs rendszer legalacsonyabb szintjeihez. Amikor egy program megpróbálja felsorolni a fájlokat, folyamatokat vagy hálózati kapcsolatokat, a rootkit a kimenet megtisztított változatát mutatja be, kiküszöbölve a terhelő kimenetet. A rootkit célja, hogy teljesen elrejtse a támadó tevékenységét a helyi rendszeren. |
| Proxyk | A hálózati forgalom átirányítható köztes rendszereken keresztül, hogy elrejtse a lopott adatok végső célpontját. Ily módon a vállalat nem blokkolja az ismert parancsokat és vezérlést, mert a proxy célhelye jóindulatúnak tűnik. Ezen túlmenően, ha adatot lopnak el, az ellopott adatok célállomása sok proxy között elosztható, így nem hívják fel a figyelmet arra, hogy egyetlen ismeretlen célállomás szolgál nagy mennyiségű hálózati forgalom célpontjaként. |

Folyamatosan új támadási módszereket fejlesztenek ki. A hálózati biztonsági személyzetnek ismernie kell a legújabb támadási módszereket, hogy észlelni tudja azokat.

2.5.7

## Ellenőrizze, hogy megértette-e a hálózati támadások típusait

Az űrlap teteje

Ellenőrizze a hálózati támadások megértését a következő kérdések megválaszolásával.

1. Mi a leggyengébb láncszem a hálózatbiztonságban?



felderítés



hozzáférés



DoS



szociális tervezés

1. Milyen típusú támadás a farokvágás?



felderítés



hozzáférés



DoS



szociális tervezés

1. Milyen típusú támadás a portellenőrzés?



felderítés



hozzáférés



DoS



szociális tervezés

1. Mi a leggyengébb láncszem a hálózatbiztonságban?



routerek



emberek



TCP/IP



szociális tervezés

# Hálózati veszélyek összefoglalója

2.6.1

## Mit tanultam ebben a modulban?

**Ki támadja meg hálózatunkat?**  
A hálózati biztonság megértéséhez ismernie kell a következő fogalmakat: fenyegetés, sebezhetőség, támadási felület, kihasználás és kockázat. A kockázatkezelés az a folyamat, amely egyensúlyba hozza a védelmi intézkedések működési költségeit az eszköz védelmével elért haszonnal. A kockázatkezelés négy gyakori módja a kockázat elfogadása, a kockázat elkerülése, a kockázat csökkentése és a kockázat átadása. A hacker a fenyegetőzők leírására használt kifejezés. A fehérkalapos hackerek etikus hackerek, akik jó, etikus és jogi célokra használják képességeiket. A szürkekalapos hackerek olyan személyek, akik bűncselekményeket és etikátlan dolgokat követnek el, de nem személyes haszonszerzés vagy károkozás céljából. A feketekalapos hackerek olyan bűnözők, akik személyes haszonszerzés céljából vagy rosszindulatú okokból, például hálózatok megtámadásából megsértik a számítógép és a hálózat biztonságát. A fenyegető szereplők között forgatókönyvíró kölykök, sebezhetőségi brókerek, hacktivisták, kiberbűnözők és államilag támogatott hackerek. Számos hálózati támadás megelőzhető az IOC-k információinak megosztásával. Sok kormány támogatja a kiberbiztonságot. Ilyen szervezetek például a CISA és az NCSA.

**A támadási eszközök bemutatása**  
A fenyegetés szereplői technikát vagy eszközt használnak. A támadási eszközök kifinomultabbak és nagymértékben automatizáltak lettek. Sok eszköz Linux vagy UNIX alapú, és ezek ismerete hasznos a kiberbiztonsági szakemberek számára. Az eszközök közé tartoznak a jelszófeltörők, a vezeték nélküli feltörő eszközök, a hálózatbiztonsági ellenőrző és feltörő eszközök, a csomagkészítő eszközök, a csomagkészítő eszközök, a csomagszimulálók, a rootkit detektorok, a sebezhetőségek keresésére szolgáló fuzzerek, a kriminalisztikai eszközök, a hibakeresők, a hacker operációs rendszerek, a titkosító eszközök, a sebezhetőséget kihasználó eszközök , és sebezhetőségi szkennerek. A támadások kategóriái közé tartoznak a lehallgatási támadások, az adatmódosítási támadások, az IP-cím-hamisítási támadások, a jelszó alapú támadások, a szolgáltatásmegtagadási támadások, a köztes támadások, a feltört kulcsfontosságú támadások és a szippantásos támadások.

**Rosszindulatú**  
Malware a rosszindulatú szoftver vagy rosszindulatú kód rövidítése. A fenyegetés szereplői gyakran megpróbálják rávenni a felhasználókat, hogy rosszindulatú programokat telepítsenek, hogy ezzel kihasználják a végeszközök sebezhetőségét. A kártevőirtó szoftverek gyakran nem frissíthetők elég gyorsan ahhoz, hogy megállítsák az új fenyegetéseket. Három gyakori típus a vírus, a féreg és a trójai faló. A vírus egyfajta rosszindulatú program, amely úgy terjed, hogy egy másolatot beilleszt egy másik programba. A legtöbb vírus USB memóriameghajtókon, CD-ken, DVD-ken, hálózati megosztásokon és e-maileken keresztül terjed. A trójai faló kártevő olyan szoftver, amely legitimnek tűnik, de olyan rosszindulatú kódot tartalmaz, amely kihasználja az azt futtató felhasználó jogosultságait. A trójaiak gyakran megtalálhatók az online játékokon. A trójai falókat általában az általuk okozott kár szerint osztályozzák. A trójai falók típusai közé tartozik a távoli hozzáférés, az adatküldő, a pusztító, a proxy, az FTP, biztonsági szoftver tiltó, DoS és keylogger. A férgek hasonlóak a vírusokhoz, mert szaporodnak, és ugyanolyan típusú károkat okozhatnak. A vírusok futtatásához gazdaprogramra van szükség. A férgek maguk is futhatnak. A legtöbb féregtámadás három összetevőből áll: a sebezhetőség engedélyezéséből, a terjedési mechanizmusból és a hasznos terhelésből. Jelenleg a ransomware a legdominánsabb rosszindulatú program. Megtagadja a hozzáférést a fertőzött rendszerhez vagy annak adataihoz. A kiberbűnözők ezután fizetést követelnek a számítógépes rendszer felszabadításáért. Egyéb rosszindulatú programok közé tartoznak a spyware, adware, a scareware, az adathalászat és a rootkitek. Jelenleg a ransomware a legdominánsabb rosszindulatú program. Megtagadja a hozzáférést a fertőzött rendszerhez vagy annak adataihoz. A kiberbűnözők ezután fizetést követelnek a számítógépes rendszer felszabadításáért. Egyéb rosszindulatú programok közé tartoznak a spyware, adware, a scareware, az adathalászat és a rootkitek. Jelenleg a ransomware a legdominánsabb rosszindulatú program. Megtagadja a hozzáférést a fertőzött rendszerhez vagy annak adataihoz. A kiberbűnözők ezután fizetést követelnek a számítógépes rendszer felszabadításáért. Egyéb rosszindulatú programok közé tartoznak a spyware, adware, a scareware, az adathalászat és a rootkitek.

**Gyakori hálózati támadások – felderítés, hozzáférés és közösségi tervezés**  
A fenyegetés szereplői kívülről is támadhatják a hálózatot. A támadások mérséklése érdekében célszerű kategorizálni a különböző típusú támadásokat. A három fő kategória a felderítés, a hozzáférés és a DoS támadások. A felderítés információgyűjtés. A fenyegetés szereplői jogosulatlanul fedezik fel és térképezik fel a rendszereket, szolgáltatásokat vagy sebezhetőségeket. A felderítési támadások megelőzik a hozzáférési vagy DoS támadásokat. A használt technikák közül néhány a következőket tartalmazza: egy cél információs lekérdezése, a célhálózat ping sweepjének indítása, az aktív IP-címek portvizsgálatának kezdeményezése, a sebezhetőség-ellenőrzők futtatása és a kizsákmányoló eszközök futtatása. A hozzáférési támadások a hitelesítési szolgáltatások, az FTP-szolgáltatások és a webszolgáltatások ismert sebezhetőségeit használják ki. Ezek a támadások közé tartoznak a jelszavas támadások, a hamisítási támadások, a bizalom kihasználását célzó támadások, a portátirányítások, man-in-the-middle támadások és puffertúlcsordulási támadások. A közösségi manipuláció olyan hozzáférési támadás, amely az egyéneket nem biztonságos műveletek végrehajtására vagy bizalmas információk felfedésére próbálja manipulálni. E támadások közé tartozik az ürügy, az adathalászat, a lándzsás adathalászat, a spam, a valamiért valamit, a csalizás, a személyi adatokkal való visszaélés, a farokzárás, a vállon való szörfözés és a szemetesben való merülés.

**Hálózati támadások – szolgáltatásmegtagadás, puffertúlcsordulás és kijátszás**  
A DoS támadások valamilyen módon megszakítják a hálózati szolgáltatásokat a felhasználók, eszközök vagy alkalmazások számára. Két fő típusa létezik: a túlnyomó mennyiségű forgalom és a rosszindulatúan formázott csomagok. A DDoS-támadások szándéka hasonló a DoS-támadásokhoz, azzal a különbséggel, hogy a DDoS-támadások mértéke megnövekszik, mivel több, összehangolt forrásból származik. A DDoS támadások leírására a következő kifejezések használatosak: zombik, botok, botnet, kezelők és botmaster. A Mirai egy rosszindulatú program, amely az alapértelmezett bejelentkezési adatokkal konfigurált IoT-eszközöket célozza meg. Mirai brute force szótári támadást alkalmaz. Sikeres hozzáférés után a Mirai az ezekhez az eszközökhöz tervezett Linux-alapú BusyBox segédprogramokat veszi célba. A puffertúlcsordulási DoS támadás során a fenyegetés szereplőjének célja, hogy megtalálja a rendszermemóriával kapcsolatos hibát a szerveren, és azt kihasználja. A puffermemória kihasználása váratlan értékekkel túlterhelve általában működésképtelenné teszi a rendszert, ami DoS támadást idéz elő. Sok támadás lopakodó kitérési technikákat használ a támadás hasznos terhének álcázására. A kijátszási módszerek közé tartozik a titkosítás és alagútkezelés, az erőforrások kimerítése, a forgalom töredezettsége, a protokollszintű félreértelmezés, a forgalom helyettesítése, a forgalom beillesztése, a pivoting, a rootkitek és a proxyk.

2.6.2

## 2. modul – Hálózati fenyegetések kvíz

Az űrlap teteje

1. Milyen módon használják a zombikat biztonsági támadásokhoz?



Ezek rosszindulatúan létrehozott kódszegmensek, amelyek a legitim alkalmazások helyettesítésére szolgálnak.



Konkrét személyeket céloznak meg vállalati vagy személyes adatok megszerzése érdekében.



Ezek fertőzött gépek, amelyek DDoS támadást hajtanak végre.



Megvizsgálják a gépek egy csoportját a nyitott portokhoz, hogy megtudják, mely szolgáltatások futnak.

1. Mi a példa a helyi kizsákmányolásra?



Puffertúlcsordulási támadás indul egy online vásárlási webhely ellen, és a szerver összeomlását okozza.



A portellenőrzés segítségével megállapítható, hogy a Telnet szolgáltatás fut-e egy távoli kiszolgálón.



Egy fenyegető szereplő megpróbálja megszerezni egy távoli gazdagép felhasználói jelszavát egy trójai által telepített billentyűzetrögzítő szoftver segítségével.



Egy fenyegetés szereplője brute force támadást hajt végre egy vállalati útválasztó ellen, hogy illegális hozzáférést szerezzen.

1. Melyik két állítás írja le a hozzáférési támadásokat? (Válassz kettőt.)



A bizalom kihasználását célzó támadások gyakran magukban foglalják egy laptop használatát, amely csalárd hozzáférési pontként működik a nyilvános helyen, például egy vezeték nélküli hotspoton található összes hálózati forgalom rögzítésére és másolására.



A jelszavas támadások végrehajthatók brute - force támadási módszerek, trójai programok vagy csomagszimulálók használatával .



A puffertúlcsordulási támadások a lefoglalt puffermemórián túlra írnak adatokat, hogy felülírják az érvényes adatokat, vagy kihasználják a rendszereket rosszindulatú kód futtatására.



A portátirányítási támadások egy hálózati adapter kártyát használnak válogatós módban a LAN-on keresztül küldött összes hálózati csomag rögzítésére.



A figyelési szolgáltatások észleléséhez a portellenőrző támadások egy állomás TCP- vagy UDP-portszámait vizsgálják meg.

1. Miért használna egy rootkitet egy hacker?



hogy észlelés nélkül hozzáférjen egy eszközhöz



bináris fájlok visszafejtéséhez



felderítést végezni



hogy megpróbálja kitalálni a jelszót

1. Melyik állítás írja le a támadási felület kifejezést?



Ez a támadó számára elérhető rendszer biztonsági résének teljes összege.



A házigazdák csoportja tapasztalja ugyanazt a támadást.



Ez a szervezet elleni támadások teljes száma egy napon belül.



Ez a hálózati interfész, ahonnan a támadások erednek.

1. Melyik kockázatkezelési terv tartalmazza a kockázatot okozó tevékenység abbahagyását?



kockázat megtartása



kockázatcsökkentési



kockázat megosztás



kockázat elkerülése

1. Milyen nevet adnak egy amatőr hackernek?



piros kalap



fekete sapka



script kölyök



kék csapat

1. Mi az a kifejezés, amikor egy rosszindulatú fél törvényes, megbízható forrásnak álcázott csaló e-mailt küld?



vishing



trójai



adathalászat



hátsó ajtó

1. Melyik két jellemző jellemzi a férget? (Válassz kettőt.)



szoftverkódhoz csatlakozva megfertőzi a számítógépeket



akkor fut le, amikor a szoftver fut a számítógépen



önmásoló \_ \_



új számítógépekre utazik a felhasználó bármilyen beavatkozása vagy ismerete nélkül



alvó állapotban rejtőzik, amíg a támadónak szüksége nem lesz rá

1. A felhasználó telefonhívást kap egy olyan személytől, aki azt állítja, hogy képviseli az IT-szolgáltatásokat, majd a felhasználónév és jelszó megerősítését kéri auditálás céljából. Milyen biztonsági fenyegetést jelent ez a telefonhívás?



levélszemét



DDoS



szociális tervezés



névtelen billentyűnaplózás

1. Melyik kijátszási módszer írja le azt a helyzetet, amikor egy feltört gazdagépen a rendszergazdai jelszóhoz való hozzáférés után a fenyegetés szereplője megpróbál bejelentkezni egy másik gazdagépre ugyanazokkal a hitelesítő adatokkal?



forgatható



erőforrás kimerülése



protokoll - szintű félreértelmezés



forgalom helyettesítése

1. Milyen típusú támadások során próbálja meg megakadályozni a kiberbűnözők a hálózati szolgáltatásokhoz való hozzáférést?



címhamisítás



DoS



MITM



munkamenet-eltérítés

# Hálózati biztonság

v1.0

[Ugrás a tartalomra](https://contenthub.netacad.com/netsec/3.0.1#chunks-container)

Hálózati biztonság

* [1A hálózatok védelme](https://contenthub.netacad.com/netsec/3.0.1#1)
  + [1.0Bevezetés](https://contenthub.netacad.com/netsec/3.0.1#1.0)
    - [1.0.1Első alkalommal ezen a tanfolyamon](https://contenthub.netacad.com/netsec/1.0.1)
    - [1.0.2Hallgatói források](https://contenthub.netacad.com/netsec/1.0.2)
    - [1.0.3Etikai hackelési nyilatkozat](https://contenthub.netacad.com/netsec/1.0.3)
    - [1.0.4Befogadó nyelv](https://contenthub.netacad.com/netsec/1.0.4)
    - [1.0.5Videó - Töltse le és telepítse a Packet Tracer programot](https://contenthub.netacad.com/netsec/1.0.5)
    - [1.0.6Videó – Kezdő lépések a Cisco Packet Tracerben](https://contenthub.netacad.com/netsec/1.0.6)
    - [1.0.7Miért vegyem ezt a modult?](https://contenthub.netacad.com/netsec/1.0.7)
    - [1.0.8Mit fogok tanulni ebben a modulban?](https://contenthub.netacad.com/netsec/1.0.8)
  + [1.1Az ügyek jelenlegi állása](https://contenthub.netacad.com/netsec/3.0.1#1.1)
  + [1.2Hálózati topológia áttekintése](https://contenthub.netacad.com/netsec/3.0.1#1.2)
  + [1.3A hálózatok biztonságának összefoglalása](https://contenthub.netacad.com/netsec/3.0.1#1.3)
* [2Hálózati fenyegetések](https://contenthub.netacad.com/netsec/3.0.1#2)
  + [2.0Bevezetés](https://contenthub.netacad.com/netsec/3.0.1#2.0)
  + [2.1Ki támadja meg hálózatunkat?](https://contenthub.netacad.com/netsec/3.0.1#2.1)
    - [2.1.1Fenyegetés, sebezhetőség és kockázat](https://contenthub.netacad.com/netsec/2.1.1)
    - [2.1.2Hacker kontra fenyegető színész](https://contenthub.netacad.com/netsec/2.1.2)
    - [2.1.3A fenyegető szereplők evolúciója](https://contenthub.netacad.com/netsec/2.1.3)
    - [2.1.4Kiberbűnözők](https://contenthub.netacad.com/netsec/2.1.4)
    - [2.1.5Kiberbiztonsági feladatok](https://contenthub.netacad.com/netsec/2.1.5)
    - [2.1.6Kiberfenyegetés-jelzők](https://contenthub.netacad.com/netsec/2.1.6)
    - [2.1.7A fenyegetés megosztása és a kiberbiztonsági tudatosság növelése](https://contenthub.netacad.com/netsec/2.1.7)
    - [2.1.8Ellenőrizze, hogy megértette – milyen színű a kalapom?](https://contenthub.netacad.com/netsec/2.1.8)
  + [2.2Fenyegető színész eszközök](https://contenthub.netacad.com/netsec/3.0.1#2.2)
    - [2.2.1A támadási eszközök bemutatása](https://contenthub.netacad.com/netsec/2.2.1)
    - [2.2.2A biztonsági eszközök evolúciója](https://contenthub.netacad.com/netsec/2.2.2)
    - [2.2.3A támadások kategóriái](https://contenthub.netacad.com/netsec/2.2.3)
    - [2.2.4Ellenőrizze, hogy megértette – osztályozza a kibertámadásokat](https://contenthub.netacad.com/netsec/2.2.4)
  + [2.3Rosszindulatú](https://contenthub.netacad.com/netsec/3.0.1#2.3)
    - [2.3.1A rosszindulatú programok típusai](https://contenthub.netacad.com/netsec/2.3.1)
    - [2.3.2Vírusok](https://contenthub.netacad.com/netsec/2.3.2)
    - [2.3.3Trójai lovak](https://contenthub.netacad.com/netsec/2.3.3)
    - [2.3.4Trójai faló osztályozása](https://contenthub.netacad.com/netsec/2.3.4)
    - [2.3.5Férgek](https://contenthub.netacad.com/netsec/2.3.5)
    - [2.3.6Féreg alkatrészek](https://contenthub.netacad.com/netsec/2.3.6)
    - [2.3.7Ransomware](https://contenthub.netacad.com/netsec/2.3.7)
    - [2.3.8Egyéb rosszindulatú programok](https://contenthub.netacad.com/netsec/2.3.8)
    - [2.3.9Gyakori rosszindulatú programok](https://contenthub.netacad.com/netsec/2.3.9)
    - [2.3.10Ellenőrizze, hogy megértette – rosszindulatú program](https://contenthub.netacad.com/netsec/2.3.10)
  + [2.4Gyakori hálózati támadások – felderítés, hozzáférés és közösségi tervezés](https://contenthub.netacad.com/netsec/3.0.1#2.4)
    - [2.4.1A hálózati támadások típusai](https://contenthub.netacad.com/netsec/2.4.1)
    - [2.4.2Felderítő támadások](https://contenthub.netacad.com/netsec/2.4.2)
    - [2.4.3Videó - Felderítő támadások](https://contenthub.netacad.com/netsec/2.4.3)
    - [2.4.4Access Attacks](https://contenthub.netacad.com/netsec/2.4.4)
    - [2.4.5Videó – Hozzáférés és szociális tervezési támadások](https://contenthub.netacad.com/netsec/2.4.5)
    - [2.4.6Social Engineering támadások](https://contenthub.netacad.com/netsec/2.4.6)
    - [2.4.7A leggyengébb láncszem megerősítése](https://contenthub.netacad.com/netsec/2.4.7)
    - [2.4.8Lab - Social Engineering](https://contenthub.netacad.com/netsec/2.4.8)
  + [2.5Hálózati támadások – szolgáltatásmegtagadás, puffertúlcsordulás és kijátszás](https://contenthub.netacad.com/netsec/3.0.1#2.5)
    - [2.5.1Videó – Szolgáltatásmegtagadási támadások](https://contenthub.netacad.com/netsec/2.5.1)
    - [2.5.2DoS és DDoS támadások](https://contenthub.netacad.com/netsec/2.5.2)
    - [2.5.3A DDoS támadások összetevői](https://contenthub.netacad.com/netsec/2.5.3)
    - [2.5.4Videó - Mirai Botnet](https://contenthub.netacad.com/netsec/2.5.4)
    - [2.5.5Puffer túlcsordulási támadás](https://contenthub.netacad.com/netsec/2.5.5)
    - [2.5.6Kijátszási módszerek](https://contenthub.netacad.com/netsec/2.5.6)
    - [2.5.7Ellenőrizze, hogy megértette-e a hálózati támadások típusait](https://contenthub.netacad.com/netsec/2.5.7)
  + [2.6Hálózati veszélyek összefoglalója](https://contenthub.netacad.com/netsec/3.0.1#2.6)
    - [2.6.1Mit tanultam ebben a modulban?](https://contenthub.netacad.com/netsec/2.6.1)
    - [2.6.22. modul – Hálózati fenyegetések kvíz](https://contenthub.netacad.com/netsec/2.6.2)
* [3Mérséklő veszélyek](https://contenthub.netacad.com/netsec/3.0.1#3)
  + [3.0Bevezetés](https://contenthub.netacad.com/netsec/3.0.1#3.0)
    - [3.0.1Miért vegyem ezt a modult?](https://contenthub.netacad.com/netsec/3.0.1)
    - [3.0.2Mit fogok tanulni ebben a modulban?](https://contenthub.netacad.com/netsec/3.0.2)
  + [3.1A hálózat védelme](https://contenthub.netacad.com/netsec/3.0.1#3.1)
  + [3.2Hálózati biztonsági szabályzatok](https://contenthub.netacad.com/netsec/3.0.1#3.2)
  + [3.3Biztonsági eszközök, platformok és szolgáltatások](https://contenthub.netacad.com/netsec/3.0.1#3.3)
  + [3.4Gyakori hálózati támadások mérséklése](https://contenthub.netacad.com/netsec/3.0.1#3.4)
  + [3.5Cisco Network Foundation védelmi keretrendszer](https://contenthub.netacad.com/netsec/3.0.1#3.5)
  + [3.6A fenyegetések enyhítése Összefoglaló](https://contenthub.netacad.com/netsec/3.0.1#3.6)
* [4Biztonságos eszközhozzáférés](https://contenthub.netacad.com/netsec/3.0.1#4)
* [5Adminisztrátori szerepkörök hozzárendelése](https://contenthub.netacad.com/netsec/3.0.1#5)
* [6Eszközfigyelés és -kezelés](https://contenthub.netacad.com/netsec/3.0.1#6)
* [7Hitelesítés, engedélyezés és elszámolás (AAA)](https://contenthub.netacad.com/netsec/3.0.1#7)
* [8Hozzáférés-vezérlési listák](https://contenthub.netacad.com/netsec/3.0.1#8)
* [9Tűzfaltechnológiák](https://contenthub.netacad.com/netsec/3.0.1#9)
* [10Zóna alapú házirend tűzfalak](https://contenthub.netacad.com/netsec/3.0.1#10)
* [11IPS technológiák](https://contenthub.netacad.com/netsec/3.0.1#11)
* [12IPS működés és megvalósítás](https://contenthub.netacad.com/netsec/3.0.1#12)
* [13Endpoint Security](https://contenthub.netacad.com/netsec/3.0.1#13)
* [142. rétegbeli biztonsági szempontok](https://contenthub.netacad.com/netsec/3.0.1#14)
* [15Kriptográfiai szolgáltatások](https://contenthub.netacad.com/netsec/3.0.1#15)
* [16Alapvető integritás és hitelesség](https://contenthub.netacad.com/netsec/3.0.1#16)
* [17Nyilvános kulcsú kriptográfia](https://contenthub.netacad.com/netsec/3.0.1#17)
* [18VPN-ek](https://contenthub.netacad.com/netsec/3.0.1#18)
* [19Helyezzen helyek közötti IPsec VPN-eket](https://contenthub.netacad.com/netsec/3.0.1#19)
* [20Bevezetés az ASA-ba](https://contenthub.netacad.com/netsec/3.0.1#20)
* [21ASA tűzfal konfigurációja](https://contenthub.netacad.com/netsec/3.0.1#21)
* [22Hálózatbiztonsági tesztelés](https://contenthub.netacad.com/netsec/3.0.1#22)

1. Mitigating Threats
2. Introduction

# Bevezetés

3.0.1

## Miért vegyem ezt a modult?

A hálózat védelme egy biztonsági szakember feladata. Hogyan maradhat tájékozott a jelenlegi biztonsági környezetről? Milyen szervezetek segíthetnek abban, hogy tájékozottak legyenek a legújabb kockázatokról és eszközökről? Mi köze a hagymának és az articsókának a biztonsághoz? Olvassa el ezt a modult, ha többet szeretne megtudni!

3.0.2

## Mit fogok tanulni ebben a modulban?

**Modul címe:** A fenyegetések enyhítése

**A modul célja** : Ismertesse meg a rosszindulatú programok és a gyakori hálózati támadások hatásainak mérséklésére szolgáló eszközöket és eljárásokat.

| **téma címe** | **Téma Cél** |
| --- | --- |
| **A hálózat védelme** | Ismertesse a hálózat védelmének módszereit és erőforrásait. |
| **Hálózati biztonsági szabályzatok** | Ismertesse meg a hálózati biztonsági szabályzatok többféle típusát. |
| **Biztosítsa a hálózatot** | Magyarázza el a biztonsági platformok célját! |
| **Gyakori hálózati támadások mérséklése** | Ismertesse a gyakori hálózati támadások mérséklésére használt technikákat. |
| **Cisco Network Foundation védelmi keretrendszer** | Ismertesse a Cisco útválasztók és kapcsolók három funkcionális területének biztonságossá tételét. |

[2.6](https://contenthub.netacad.com/netsec/3.0.1" \l "/netsec/undefined.1)

[Hálózati veszélyek összefoglalója](https://contenthub.netacad.com/netsec/3.0.1" \l "/netsec/undefined.1)

[3.1](https://contenthub.netacad.com/netsec/3.0.1" \l "/netsec/undefined.1)

[A hálózat védelme](https://contenthub.netacad.com/netsec/3.0.1" \l "/netsec/undefined.1)

# A hálózat védelme

3.1.1

## Hálózatbiztonsági szakemberek

A szervezetek termelékenységcsökkenést tapasztalnak, ha hálózataik lassúak vagy nem reagálnak. Az adatvesztés és az adatsérülés negatívan befolyásolja az üzleti célokat és a nyereséget. Ezért üzleti szempontból minimálisra kell csökkenteni a rossz szándékú hackerek hatásait.

A hálózatbiztonsági szakemberek felelősek a szervezet adatbiztonságának fenntartásáért, valamint az információk integritásának és bizalmasságának biztosításáért. Ironikus, hogy a hackelés nem szándékosan nagy keresletet generált a hálózatbiztonsági szakemberek iránt. A növekvő hackerek kihasználásának, a hackereszközök kifinomultságának és a kormányzati jogszabályoknak köszönhetően a hálózatbiztonsági megoldások az 1990-es években gyorsan fejlődtek, új munkalehetőségeket teremtve a hálózatbiztonság területén.

A vállalaton belüli biztonsági szakértői munkakörök közé tartozik a Chief Information Officer (CIO), a Chief Information Security Officer (CISO), a Security Operations (SecOps) menedzser, a Chief Security Officer (CSO), a Security Manager és a Network Security Engineer. A beosztástól függetlenül a hálózatbiztonsági szakembereknek mindig egy lépéssel a hackerek előtt kell maradniuk:

* Folyamatosan fejleszteniük kell készségeiket, hogy lépést tarthassanak a legújabb fenyegetésekkel.
* Képzéseken és workshopokon kell részt venniük.
* Fel kell iratkozniuk a fenyegetésekkel kapcsolatos valós idejű hírcsatornákra.
* Naponta át kell nézniük a biztonsági webhelyeket.
* Ismerniük kell a hálózatbiztonsági szervezeteket. Ezek a szervezetek gyakran rendelkeznek a legfrissebb információkkal a fenyegetésekről és sebezhetőségekről.

A Cyber ​​Security Education szervezet számos kiberbiztonsági karriert ismertet, és olyan forrásokat biztosít, amelyek segíthetnek felkészülni ezekre a pályákra.

**Megjegyzés** : Más technológiai szakmákhoz képest a hálózati biztonság nagyon meredek tanulási görbével rendelkezik, és folyamatos szakmai fejlődés iránti elkötelezettséget igényel.

3.1.2

## Hálózati Intelligencia Közösségek

A hálózat hatékony védelme érdekében a biztonsági szakembereknek folyamatosan tájékozottnak kell lenniük a fenyegetésekről és a sebezhetőségekről, ahogy azok fejlődnek. Számos biztonsági szervezet nyújt hálózati intelligenciát. Erőforrásokat, workshopokat és konferenciákat biztosítanak a biztonsági szakemberek számára. Ezek a szervezetek gyakran rendelkeznek a legfrissebb információkkal a fenyegetésekről és sebezhetőségekről.

A táblázat néhány fontos hálózatbiztonsági szervezetet sorol fel.

| **Szervezet** | **Leírás** |
| --- | --- |
| NÉLKÜL | A SysAdmin, Audit, Network, Security (SANS) Institute erőforrásai kérésre nagyrészt ingyenesek, és a következőket tartalmazzák:   * Az Internet Storm Center – a népszerű internetes korai figyelmeztető rendszer * NewsBites, a számítógépes biztonságról szóló cikkek heti kivonata. * @RISK, az újonnan felfedezett támadási vektorok heti összefoglalója, az aktív kizsákmányolásokkal járó sebezhetőségek, valamint a legutóbbi támadások működésének magyarázata * Flash biztonsági figyelmeztetések * Olvasóterem – több mint 1200 díjnyertes, eredeti kutatási dolgozat. * A SANS biztonsági tanfolyamokat is fejleszt. |
| Püspöksüveg | A Mitre Corporation listát vezet a kiemelkedő biztonsági szervezetek által használt gyakori sebezhetőségekről és kitettségekről (CVE), megkönnyítve számukra az adatok megosztását. A CVE az ismert kiberbiztonsági sérülékenységek közönséges neveinek (azaz CVE-azonosítóinak) szótáraként szolgál. |
| ELSŐ | A Forum of Incident Response and Security Teams (FIRST) egy biztonsági szervezet, amely számos kormányzati, kereskedelmi és oktatási szervezettől származó számítógép-biztonsági incidensre adott válaszcsoportot tömörít, hogy elősegítse az együttműködést és a koordinációt az információmegosztás, az incidensmegelőzés és a gyors reagálás terén. |
| SecurityNewsWire | Biztonsági hírportál, amely összesíti a riasztásokkal, kihasználásokkal és sebezhetőségekkel kapcsolatos legfrissebb híreket. |
| (ISC) 2 | Az International Information Systems Security Certification Consortium (ISC 2 ) szállítósemleges oktatási termékeket és karrierszolgáltatásokat nyújt több mint 75 000 iparági szakember számára több mint 135 országban. |
| CIS | A Center for Internet Security (CIS) a kiberfenyegetések megelőzésének, védelmének, reagálásának és helyreállításának fókuszpontja az állami, helyi, törzsi és területi (SLTT) kormányok számára a Multi-State Information Sharing and Analysis Center (MS-ISAC) révén. ). Az MS-ISAC a hét minden napján, 24 órában figyelmeztetéseket és tanácsokat ad kiberfenyegetésekre, sebezhetőség-azonosítást, valamint mérséklést és incidensre adott választ. |

A hatékonyság megőrzése érdekében a hálózatbiztonsági szakembernek:

* **Tartson lépést a legújabb fenyegetésekkel** – Ez magában foglalja a fenyegetésekkel kapcsolatos valós idejű hírfolyamokra való feliratkozást, a biztonsággal kapcsolatos webhelyek rutinszerű böngészését, a biztonsági blogok és podcastok követését és még sok mást.
* **Folytassa a készségek fejlesztését** – Ez magában foglalja a biztonsággal kapcsolatos képzéseken, workshopokon és konferenciákon való részvételt.

**Megjegyzés** : A hálózati biztonság nagyon meredek tanulási görbével rendelkezik, és a folyamatos szakmai fejlődés iránti elkötelezettséget követeli meg.

3.1.3

## Hálózatbiztonsági tanúsítványok

Évente több százezer hálózati biztonsággal kapcsolatos állás marad betöltetlen. A hálózatbiztonsági szakemberek iránti kereslet jóval meghaladja a képzett jelentkezők számát. Az elismert hálózatbiztonsági tanúsítványok megszerzése nagymértékben növeli az Ön képesítését ezekre a pozíciókra. Számos tanúsítvány létezik. A hálózatbiztonsági szakemberek számára a tanúsítványokat a következő szervezetek kínálják:

* Global Information Assurance Certification (GIAC)
* Nemzetközi Információs Rendszerbiztonsági Tanúsító Konzorcium (ISC) 2
* Information Systems Audit and Control Association (ISACA)
* E-kereskedelmi Tanácsadók Nemzetközi Tanácsa (EC-Cuncil)
* Certified Wireless Security Professional (CWSP)

A Cisco felváltotta a Cisco Certified Network Associate Security (210-260 IINS) tanúsítványt egy új CCNP Security tanúsítvánnyal. Ez a minősítés két vizsgából, egy biztonsági alapvizsgából és egy koncentrációs vizsgából áll. Csak egy koncentrációs vizsga szükséges. Az Implementing and Operating Cisco Security Core Technologies (350-701 SCOR) vizsga átjáróként szolgál mind a CCNP, mind a CCIE biztonsági tanúsítványokhoz. Biztonsági alaptanúsítványt is biztosít. Az alapvizsga biztonsági koncepciókra, fenyegetésekre, valamint mérséklési technikákra és technológiákra terjed ki. A specializációk mélyrehatóan összpontosítanak bizonyos Cisco biztonsági technológiákra. A Cisco Certified Specialist biztonsági koncentrációs vizsgák a következők:

* 300-710 SNCF – Hálózatbiztonsági tűzerő
* 300-715 SISE – Cisco Identity Services Engine megvalósítása és konfigurálása
* 300-720 SESA – E-mailek védelme a Cisco Email Security Appliance segítségével
* 300-725 SWSA – A web biztonsága a Cisco Web Security Appliance segítségével
* 300-730 SVPN – Biztonságos megoldások megvalósítása virtuális magánhálózatokkal
* 300-735 SAUTO – Cisco biztonsági megoldások automatizálása és programozása

Sokféleképpen lehet felkészülni ezekre a minősítésekre, beleértve az önálló tanulást, a magánvizsgaoktatást és a felsőoktatást. A Learning at Cisco szervezet, valamint tanulási partnerei tájékoztatást és képzést nyújtanak a legtöbb Cisco minősítő vizsgához.

3.1.4

## Kommunikációs biztonság: CIA

Az információbiztonság az információk és információs rendszerek védelmével foglalkozik a jogosulatlan hozzáférés, használat, nyilvánosságra hozatal, megszakítás, módosítás vagy megsemmisítés ellen. A CIA Triad a terület fogalmi alapjául szolgál.

Az ábra a CIA Triádot mutatja, amely a bizalmasságból, integritásból és elérhetőségből áll.

### CIA Triád

TitoktartásSértetlenségElérhetőség

Amint az ábrán látható, a CIA triász az információbiztonság három összetevőjéből áll:

* **Titoktartás** – Csak az arra jogosult személyek, entitások vagy folyamatok férhetnek hozzá az érzékeny információkhoz.
* **Integritás** – Ez az adatok jogosulatlan módosításokkal szembeni védelmét jelenti.
* **Elérhetőség** – A jogosult felhasználóknak megszakítás nélkül hozzá kell férniük a szükséges hálózati erőforrásokhoz és adatokhoz.

A hálózati adatok titkosíthatók (olvashatatlanná tehetik az illetéktelen felhasználók számára) különféle kriptográfiai alkalmazásokkal. A két IP-telefon felhasználó közötti beszélgetés titkosítható. A számítógépen lévő fájlok titkosíthatók is. Ez csak néhány példa. A kriptográfia szinte bárhol használható, ahol van adatkommunikáció. Valójában az a tendencia, hogy minden kommunikációt titkosítanak.

# Hálózati biztonsági szabályzatok

3.2.1

## Hálózatbiztonsági tartományok

A hálózatbiztonsági szakemberek számára létfontosságú, hogy megértsék a hálózatbiztonság okait. Ismerniük kell a hálózatbiztonság szervezeti követelményeit is, amelyeket a 14 hálózati biztonsági tartomány testesít meg.

A tartományok keretet adnak a hálózati biztonság megvitatásához és az egyes szervezetek által kezelendő működési igények megértéséhez.

A Nemzetközi Szabványügyi Szervezet (ISO)/Nemzetközi Elektrotechnikai Bizottság (IEC) 14 hálózatbiztonsági tartományt határoz meg. Az ISO/IEC 27001 szabvány szerint ez a 14 tartomány az információk és tevékenységek hatalmas birodalmának magas szintű megszervezését szolgálja a hálózatbiztonság égisze alatt. Ezek a tartományok jelentős párhuzamot mutatnak a Certified Information Systems Security Professional (CISSP) tanúsítvány által meghatározott tartományokkal.

A 14 tartomány közös alapként szolgál a szervezeti biztonsági szabványok és a hatékony biztonságkezelési gyakorlat kialakításához. Segítenek a szervezetek közötti kommunikáció megkönnyítésében is.

Ez a 14 tartomány biztosítja a hálózati biztonság elemeinek kényelmes elkülönítését. Bár nem fontos megjegyezni ezt a 14 tartományt, fontos tisztában lenni a létezésükkel és az ISO hivatalos nyilatkozatával. Az ISO 27001 szabványban ezeket az A melléklet 14 vezérlőkészleteként ismerik. Hasznos referenciaként szolgálnak a hálózatbiztonsági szakemberként végzett munkájában.

Az alábbi táblázat rövid leírást ad az egyes tartományokról.

| **Hálózatbiztonsági tartomány** | **Leírás** |
| --- | --- |
| Információbiztonsági szabályzatok | Ez a melléklet a biztonsági szabályzatok létrehozását, felülvizsgálatát és karbantartását hivatott biztosítani. |
| Az információbiztonság szervezése | Ez egy információbiztonsági szervezet által felállított irányítási modell. Felelősséget jelöl ki a szervezeten belüli információbiztonsági feladatokért. |
| Humánerőforrás-biztonság | Ez az alkalmazottak szervezethez való csatlakozásával, beköltözésével és elhagyásával kapcsolatos biztonsági kötelezettségekkel foglalkozik. |
| Vagyonkezelés | Ez arra vonatkozik, ahogyan a szervezetek leltárt és osztályozási sémát készítenek az információs eszközökhöz. |
| Hozzáférés-szabályozás | Ez a hálózatokhoz, rendszerekhez, alkalmazásokhoz, funkciókhoz és adatokhoz való hozzáférési jogok korlátozását írja le. |
| Kriptográfia | Ez az adatok titkosítására és az érzékeny információk kezelésére vonatkozik az adatok titkosságának, integritásának és elérhetőségének védelme érdekében. |
| Fizikai és környezeti biztonság | Ez leírja a fizikai számítógépes létesítmények és berendezések védelmét a szervezeten belül. |
| Hadműveletek biztonsági biztosítása | Ez leírja a rendszerek és hálózatok műszaki biztonsági ellenőrzéseinek kezelését, beleértve a kártevő elleni védelmet, az adatmentést, a naplózást és a megfigyelést, a sebezhetőség kezelését és az ellenőrzési szempontokat. Ez a tartomány az üzleti műveletekben használt szoftverek integritásával is foglalkozik. |
| Kommunikációs biztonság | Ez az adatok hálózaton belüli közlésének biztonságára vonatkozik, akár egy szervezeten belül, akár a szervezet és harmadik felek, például ügyfelek vagy beszállítók között. |
| Rendszerbeszerzés, fejlesztés és karbantartás | Ez biztosítja, hogy az információbiztonság továbbra is központi kérdés maradjon a szervezet folyamataiban a teljes életciklus során, mind a magán, mind a nyilvános hálózatokban. |
| Szállítói kapcsolatok | Ez a szerződéses megállapodások specifikációira vonatkozik, amelyek védik a szervezet információs és technológiai eszközeit, amelyekhez hozzáférhetnek a szervezet számára árukat és szolgáltatásokat nyújtó harmadik felek. |
| Információbiztonsági események kezelése | Ez leírja, hogyan lehet előre látni és reagálni az információbiztonság megsértésére. |
| Üzletmenet-folytonosság menedzsment | Ez az üzleti szempontból kritikus folyamatok és rendszerek védelmét, karbantartását és helyreállítását írja le. |
| Megfelelés | Ez leírja az információbiztonsági irányelveknek, szabványoknak és előírásoknak való megfelelés biztosításának folyamatát. |

3.2.2

## Üzleti szabályzatok

Az üzleti irányelvek olyan iránymutatások, amelyeket egy szervezet dolgoz ki tevékenységei irányítására. A szabályzatok a helyes magatartás normáit határozzák meg a vállalkozás és alkalmazottai számára. A hálózatépítésben a házirendek határozzák meg a hálózaton engedélyezett tevékenységeket. Ez meghatározza az elfogadható használat alapvonalát. Ha az üzletszabályzatot sértő viselkedést észlel a hálózaton, akkor lehetséges, hogy biztonsági megsértés történt.

A táblázatban felsoroltak szerint egy szervezet több irányadó irányelvvel rendelkezhet.

| **Irányelv** | **Leírás** |
| --- | --- |
| **Vállalati irányelvek** | * Ezek a szabályzatok rögzítik mind a munkavállalók, mind a munkáltatók magatartási szabályait és felelősségét. * A politikák védik a munkavállalók jogait, valamint a munkaadók üzleti érdekeit. * A szervezet szükségleteitől függően különféle szabályzatok és eljárások határoznak meg szabályokat az alkalmazottak magatartására, a jelenlétre, az öltözködésre, a magánéletre és a foglalkoztatási feltételekkel kapcsolatos egyéb területekre vonatkozóan. |
| **Munkavállalói szabályzatok** | * Ezeket a házirendeket az emberi erőforrások munkatársai hozzák létre és tartják fenn, hogy azonosítsák az alkalmazottak fizetését, fizetési ütemezését, munkavállalói juttatásait, munkarendjét, szabadságát és még sok mást. * Gyakran áttekintik és aláírják az új alkalmazottakat. |
| **Biztonsági szabályzatok** | * Ezek a házirendek meghatározzák a vállalat biztonsági céljait, meghatározzák a felhasználók és a rendszergazdák viselkedési szabályait, és meghatározzák a rendszerkövetelményeket. * Ezek a célok, szabályok és követelmények együttesen biztosítják a hálózat és a számítógépes rendszerek biztonságát a szervezetben. * A folytonossági tervhez hasonlóan a biztonsági politika is egy folyamatosan fejlődő dokumentum, amely a fenyegetési környezet változásán, a sebezhetőségeken, valamint az üzleti és munkavállalói követelményeken alapul. |

3.2.3

## Biztonsági politika

Az átfogó biztonsági politika számos előnnyel jár, beleértve a következőket:

* Egy szervezet biztonság iránti elkötelezettségét mutatja
* Szabályokat állít be az elvárt viselkedéshez
* Biztosítja a következetességet a rendszer működésében, a szoftver- és hardverbeszerzésben és -használatban, valamint a karbantartásban
* Meghatározza a jogsértések jogi következményeit
* A biztonsági személyzet támogatását biztosítja a vezetőség számára

A biztonsági szabályzatok a felhasználók, a személyzet és a vezetők tájékoztatására szolgálnak a szervezet technológiai és információs eszközök védelmére vonatkozó követelményeiről. A biztonsági szabályzat meghatározza azokat a mechanizmusokat is, amelyekre szükség van a biztonsági követelmények teljesítéséhez, és kiindulási alapként szolgál a számítógépes rendszerek és hálózatok megfelelőség szempontjából történő beszerzéséhez, konfigurálásához és ellenőrzéséhez.

A táblázat azokat a házirendeket sorolja fel, amelyeket a biztonsági szabályzat tartalmazhat.

| **Irányelv** | **Leírás** |
| --- | --- |
| **Azonosítási és hitelesítési szabályzat** | Meghatározza azokat a jogosult személyeket, akik hozzáférhetnek a hálózati erőforrásokhoz és a személyazonosság-ellenőrzési eljárásokhoz. |
| **Jelszó házirendek** | Biztosítja, hogy a jelszavak megfeleljenek a minimális követelményeknek, és rendszeresen cseréljék őket. |
| **Elfogadható felhasználási szabályzat (AUP)** | Azonosítja a szervezet számára elfogadható hálózati alkalmazásokat és felhasználásokat. Az irányelv megsértésének következményeit is azonosíthatja. |
| **Távoli hozzáférési szabályzat** | Meghatározza, hogy a távoli felhasználók hogyan férhetnek hozzá a hálózathoz, és mi érhető el távoli kapcsolaton keresztül. |
| **Hálózat karbantartási szabályzat** | Meghatározza a hálózati eszközök operációs rendszereit és a végfelhasználói alkalmazások frissítési eljárásait. |
| **Incidenskezelési eljárások** | Leírja a biztonsági incidensek kezelését. |

Az egyik leggyakoribb biztonsági házirend-összetevő az AUP. Ezt megfelelő használati szabályzatnak is nevezhetjük. Ez az összetevő határozza meg, hogy a felhasználók mit tehetnek és mit nem tehetnek a különböző rendszerösszetevőkben. Ez magában foglalja a hálózaton engedélyezett forgalom típusát. Az AUP-nak a lehető legkifejezettebbnek kell lennie a félreértések elkerülése érdekében.

Például az AUP felsorolhat olyan webhelyeket, hírcsoportokat vagy nagy sávszélességet igénylő alkalmazásokat, amelyekhez tilos hozzáférni a vállalati számítógépekről vagy a vállalati hálózatról. Minden munkavállalónak meg kell írnia az AUP-t, és az aláírt AUP-kat meg kell őrizni a munkaviszony időtartama alatt.

3.2.4

## BYOD irányelvek

Mostantól sok szervezetnek támogatnia kell a Bring Your Own Device (BYOD) funkciót is. Ez lehetővé teszi az alkalmazottak számára, hogy saját mobileszközeik segítségével hozzáférjenek a vállalati rendszerekhez, szoftverekhez, hálózatokhoz vagy információkhoz. A BYOD számos kulcsfontosságú előnnyel jár a vállalatok számára, beleértve a termelékenység növekedését, az IT- és működési költségek csökkentését, az alkalmazottak jobb mobilitását, valamint az alkalmazottak felvételének és megtartásának nagyobb vonzerejét.

Ezek az előnyök azonban megnövekedett információbiztonsági kockázatot is jelentenek, mivel a BYOD adatszivárgáshoz és a szervezet nagyobb felelősségéhez vezethet.

BYOD biztonsági szabályzatot kell kidolgozni a következők megvalósítására:

* Adja meg a BYOD program céljait.
* Határozza meg, mely alkalmazottak hozhatják magukkal saját eszközeiket.
* Határozza meg, mely eszközök lesznek támogatottak.
* Határozza meg az alkalmazottak hozzáférési szintjét a személyes eszközök használatakor.
* Ismertesse a biztonsági személyzet hozzáférési jogait és az eszközön engedélyezett tevékenységeket.
* Határozza meg, mely előírásokat kell betartani az alkalmazotti eszközök használatakor.
* Határozza meg azokat a biztosítékokat, amelyeket akkor kell bevezetni, ha egy eszköz veszélybe kerül.

A táblázat felsorolja a BYOD biztonsági bevált módszereit a BYOD sebezhetőségeinek enyhítésére.

| **Legjobb gyakorlat** | **Leírás** |
| --- | --- |
| Jelszóval védett hozzáférés | Használjon egyedi jelszavakat minden eszközhöz és fiókhoz. |
| A vezeték nélküli kapcsolat kézi vezérlése | Kapcsolja ki a Wi-Fi- és Bluetooth-kapcsolatot, ha nem használja. Csak megbízható hálózatokhoz csatlakozzon. |
| Tartsa naprakészen | Mindig tartsa frissítve az eszköz operációs rendszerét és egyéb szoftvereit. A frissített szoftverek gyakran tartalmaznak biztonsági javításokat a legújabb fenyegetések vagy kizsákmányolások elleni védekezés érdekében. |
| Adatok biztonsági mentése | Engedélyezze az eszköz biztonsági mentését, ha elveszik vagy ellopják. |
| A „Készülék keresése” engedélyezése | Iratkozzon fel egy eszközkereső szolgáltatásra távoli törlés funkcióval. |
| Biztosítson víruskereső szoftvert | Víruskereső szoftver biztosítása a jóváhagyott BYOD-eszközökhöz. |
| Használjon mobileszköz-kezelő (MDM) szoftvert | Az MDM szoftver lehetővé teszi az informatikai csapatok számára, hogy biztonsági beállításokat és szoftverkonfigurációkat hajtsanak végre minden olyan eszközön, amely a vállalati hálózatokhoz csatlakozik. |

3.2.5

## Szabályozási és szabványoknak való megfelelés

A hálózat biztonságát illetően külső szabályozások is léteznek. A hálózatbiztonsági szakembereknek ismerniük kell azokat a törvényeket és etikai kódexeket, amelyek kötelezőek az információs rendszerbiztonsági (INFOSEC) szakemberekre nézve.

Számos szervezetet bíznak meg biztonsági irányelvek kidolgozásával és végrehajtásával. A megfelelőségi előírások meghatározzák, hogy mely szervezetek felelősek a biztosításért, és a felelősséget, ha nem teljesítik. A megfelelőségi előírások, amelyeket egy szervezetnek be kell tartania, a szervezet típusától és a szervezet által kezelt adatoktól függenek. A konkrét megfelelési szabályokról a tanfolyam későbbi részében lesz szó.

Biztonsági eszközök, platformok és szolgáltatások

3.3.1

A biztonsági hagyma és a biztonsági articsóka

Két általános analógia létezik a mélyreható védekezés leírására.

Biztonsági hagyma

Biztonsági articsóka

A hálózatépítés változó környezete, mint például a határok nélküli hálózatok fejlődése, ezt a hasonlatot a „biztonsági articsóka”-ra változtatta, ami a fenyegetés szereplői számára előnyös.

Ahogy az ábrán is látható, a fenyegetés szereplőinek többé nem kell minden réteget lehámozniuk. Csak bizonyos „articsókaleveleket” kell eltávolítaniuk. A bónusz az, hogy a hálózat minden egyes „levele” olyan érzékeny adatokat fedhet fel, amelyek nem megfelelően védettek.

Például egy fenyegetés szereplője könnyebben feltörhet egy mobileszközt, mint egy belső számítógépet vagy szervert, amelyet védelmi rétegek védenek. Minden mobileszköz egy levél. És levélről levélre, mindez több adathoz vezeti a hackert. Az articsóka szíve az, ahol a legbizalmasabb adatok találhatók. Minden egyes levél egy réteg védelmet nyújt, ugyanakkor utat biztosít a támadáshoz.

Nem kell minden levelet eltávolítani ahhoz, hogy az articsóka szívébe kerüljön. A hacker feldarabolja a biztonsági páncélt a kerület mentén, hogy eljusson a vállalkozás „szívéhez”.

Míg az internetre néző rendszerek általában nagyon jól védettek, a határvédelem pedig jellemzően szilárd, kitartó hackerek, akiket ügyesség és szerencse keveréke segít, végül találnak egy rést a kemény külsőben, amelyen keresztül oda léphetnek be és mehetnek, ahova akarnak. .

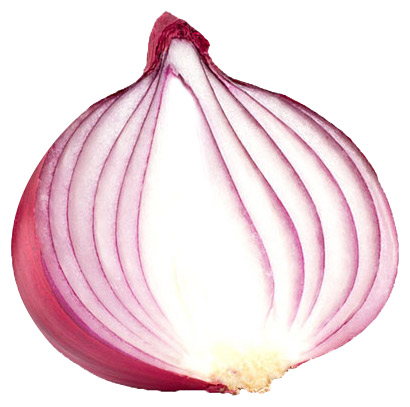
A biztonsági articsóka ábrán egy articsóka látható, benne különböző részekkel. A jobb oldali szavaknál az articsóka egyes szakaszaira mutató nyíl látható: jelszavak; ügyféloldali támadások; adatbázisok; webes alkalmazások; puffer túlcsordul.



JelszavakÜgyféloldali támadásokAdatbázisokWebes alkalmazásokPuffer túlcsordulás  
A mélyreható védelmi megközelítés leírására használt általános analógia a „biztonsági hagyma”. Amint az ábrán látható, a fenyegetés szereplőjének rétegről rétegre kell hámoznia a hálózat védelmét, hasonlóan a hagyma hámozásához. A fenyegetés szereplője csak az egyes rétegek behatolása után éri el a céladatot vagy rendszert.

**Megjegyzés** : Az ezen az oldalon leírt biztonsági hagyma a védekezés mélyreható megjelenítésének egyik módja. Ez nem tévesztendő össze a Security Onion hálózati biztonsági eszközökkel.

A biztonsági hagyma ábra egy hagymát mutat, benne különböző rétegekkel. A hagyma eszközként van megjelölve. Jobb oldalon a különböző rétegekre mutató szavak és nyilak: edzett eszközök; hitelesítés, engedélyezés és elszámolás (AAA); tartalomszűrés; behatolásgátló rendszerek (IPS); tűzfal.



Edzett eszközökHitelesítés, engedélyezés és elszámolás (AAA)TartalomszűrésBehatolás-megelőzési rendszerek (IPS)TűzfalEszközök

3.3.2

Biztonsági tesztelési eszközök

Az etikus hackelés számos különböző típusú eszköz használatát jelenti a hálózat és a végeszközök tesztelésére. A hálózat és rendszerei biztonságának ellenőrzésére számos hálózati biztonsági tesztelőeszközt fejlesztettek ki. A penetrációs tesztelés során hacker technikákat és eszközöket használnak a hálózati biztonsági intézkedések erejének értékelésére. Azonban ezen eszközök közül sokat a fenyegetés szereplői is használhatnak kizsákmányolásra.

A fenyegetőző szereplők különféle hackereszközöket is készítettek. Ezeket az eszközöket kifejezetten aljas okok miatt írták le. A kiberbiztonsági személyzetnek azt is tudnia kell, hogyan kell használni ezeket az eszközöket a hálózati penetrációs tesztek végrehajtásakor.

Fedezze fel a közös hálózati penetrációt vizsgáló eszközök kategóriáit. Figyelje meg, hogyan használnak bizonyos eszközöket a fehér és a fekete kalapok. Ne feledje, hogy a lista nem teljes, mivel az új eszközök folyamatosan fejlesztés alatt állnak.

**Megjegyzés** : Ezen eszközök közül sok UNIX vagy Linux alapú; ezért egy biztonsági szakembernek erős UNIX és Linux háttérrel kell rendelkeznie.

| **Eszköz kategóriák** | **Leírás** |
| --- | --- |
| jelszótörők | A jelszavak jelentik a legsebezhetőbb biztonsági fenyegetést. A jelszótörő eszközöket gyakran jelszó-helyreállító eszközöknek nevezik, és a jelszó feltörésére vagy helyreállítására használhatók. Ez vagy az eredeti jelszó eltávolításával, az adatok titkosításának megkerülésével, vagy a jelszó közvetlen felfedezésével érhető el. A jelszótörők többször is találgatásokat hajtanak végre a jelszó feltörése és a rendszerhez való hozzáférés érdekében. A jelszófeltörő eszközök példái közé tartozik John the Ripper, Ophcrack, L0phtCrack, THC Hydra, RainbowCrack és Medusa. |
| vezeték nélküli hacker eszközök | A vezeték nélküli hálózatok érzékenyebbek a hálózati biztonsági fenyegetésekre. A vezeték nélküli hackereszközöket a vezeték nélküli hálózatok szándékos feltörésére használják a biztonsági rések észlelése érdekében. Vezeték nélküli hackereszközök például az Aircrack-ng, a Kismet, az InSSIDer, a KisMAC, a Firesheep és a NetStumbler. |
| hálózati szkennelés és hacker eszközök | A hálózati szkennelő eszközök a hálózati eszközök, szerverek és gazdagépek nyitott TCP- vagy UDP-portjainak vizsgálatára szolgálnak. A szkennelő eszközök közé tartozik például az Nmap, a SuperScan, az Angry IP Scanner és a NetScanTools. |
| csomagkészítő eszközök | A csomagkészítő eszközöket a tűzfal robusztusságának vizsgálatára és tesztelésére használják speciálisan kialakított hamisított csomagok segítségével. Ilyen eszközök például a Hping, a Scapy, a Socat, a Yersinia, a Netcat, az Nping és a Nemesis. |
| csomagszimatolók | A csomagszimuláló eszközök a hagyományos Ethernet LAN-on vagy WLAN-on belüli csomagok rögzítésére és elemzésére szolgálnak. Az eszközök közé tartozik a Wireshark, a Tcpdump, az Ettercap, a Dsniff, az EtherApe, a Paros, a Fiddler, a Ratproxy és az SSLstrip. |
| rootkit detektorok | A rootkit detektor egy könyvtár- és fájlintegritás-ellenőrző, amelyet a fehér kalap használ a telepített gyökérkészletek észlelésére. Ilyen például az AIDE, a Netfilter és a PF: OpenBSD Packet Filter. |
| fuzzers a sebezhetőségek kereséséhez | A fuzzerek olyan eszközök, amelyeket a fenyegetés szereplői használnak, amikor megpróbálják felfedezni a számítógépes rendszer biztonsági réseit. A fuzzerek közé tartozik például a Skipfish, a Wapiti és a W3af. |
| törvényszéki eszközök | A fehérkalapos hackerek kriminalisztikai eszközöket használnak az adott számítógépes rendszerben létező bizonyítékok minden nyomának kiszúrására. Ilyen eszközök például a Sleuth Kit, a Helix, a Maltego és az Encase. |
| hibakeresők | A fekete kalapok a hibakereső eszközöket használják a bináris fájlok visszafejtésére exploitok írásakor. A fehér kalapok is használják a rosszindulatú programok elemzéséhez. A hibakereső eszközök közé tartozik a GDB, a WinDbg, az IDA Pro és az Immunity Debugger. |
| operációs rendszerek feltörése | A hacker operációs rendszerek olyan speciálisan tervezett operációs rendszerek, amelyek előre telepítve vannak feltörésre optimalizált eszközökkel és technológiákkal. A speciálisan tervezett hacker operációs rendszerek például a Kali Linux, a SELinux, a Knoppix, a Parrot OS és a BackBox Linux. |
| titkosítási eszközök | Ezek az eszközök védik a szervezet adatainak tartalmát azok tárolása vagy továbbítása során. A titkosítási eszközök algoritmussémákat használnak az adatok kódolására, hogy megakadályozzák az adatokhoz való jogosulatlan hozzáférést. Ilyen eszközök például a VeraCrypt, a CipherShed, az Open SSH, az OpenSSL, az OpenVPN és a Stunnel. |
| sebezhetőség kihasználására szolgáló eszközök | Ezek az eszközök azonosítják, hogy egy távoli gazdagép sebezhető-e a biztonsági támadásokkal szemben. A sebezhetőséget kihasználó eszközök például a Metasploit, a Core Impact, az Sqlmap, a Social Engineer Tool Kit és a Netsparker. |
| sebezhetőségi szkennerek | Ezek az eszközök átvizsgálják a hálózatot vagy a rendszert a nyitott portok azonosítására. Használhatók ismert sebezhetőségek, valamint virtuális gépek, BYOD-eszközök és ügyféladatbázisok vizsgálatára is. Ilyen eszközök például a Nipper, a Securia PSI, a Core Impact, a Nessus, a SAINT és az Open VAS. |

3.3.3

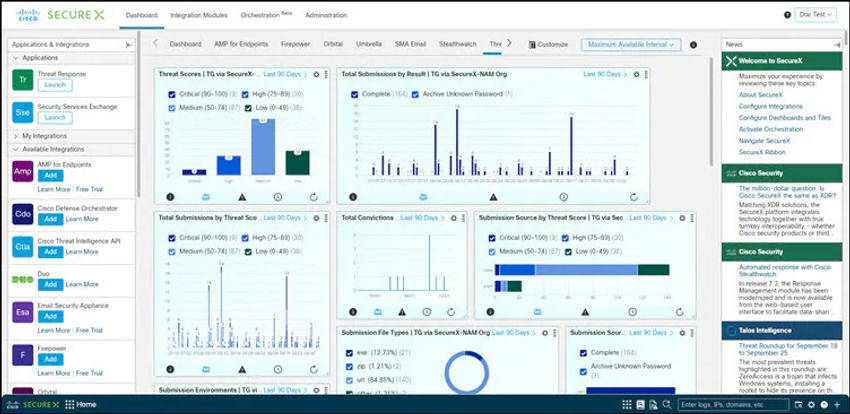
Adatbiztonsági platformok

A Data Security Platforms (DSP) egy olyan integrált biztonsági megoldás, amely a hagyományosan független eszközöket olyan eszközök sorozatává egyesíti, amelyek együtt működnek. A hálózatokat védő és figyelő biztonsági eszközöket gyakran különböző gyártók készítik. Nehéz lehet ezeket az eszközöket oly módon integrálni, hogy a hálózatbiztonságról egységes nézetet lehessen elérni. Jelentős erőforrásokra lehet szükség ahhoz, hogy különböző eszközök és szoftverek legyenek egyetlen vezérlő megoldás alatt. Ezenkívül az ilyen változatos eszközökből származó adatok integrálása a hálózat átfogó felügyeleti nézetébe nagyon nehéz lehet létrehozni és karbantartani.

Az egyik ilyen DSP a FireEye Helix platformja. A FireEye Helix egy felhőalapú biztonsági műveleti platform, amely lehetővé teszi a szervezetek számára, hogy számos biztonsági funkciót egyetlen platformba integráljanak. A Helix eseménykezelést, hálózati viselkedéselemzést, fejlett fenyegetésészlelést, valamint incidensbiztonsági koordinációt, automatizálást és reagálást (SOAR) biztosít a fenyegetések észlelésekor történő reagáláshoz. A Helix emellett a FireEye Mandiant fenyegetések intelligenciájára, incidensre adott válaszaira és biztonsági szakértelmére is támaszkodik.



Egy másik integrált DSP a Cisco SecureX. A SecureX egy lépéssel tovább megy a Cisco Secure portfólióval való erős integrációjával. A Cisco Secure portfóliója olyan technológiák széles készletéből áll, amelyek csapatként működnek – biztosítva az együttműködést a biztonsági infrastruktúrával, beleértve a harmadik féltől származó technológiákat is. Ez egységes láthatóságot, automatizálást és erősebb védelmet eredményez. A Cisco SecureX platform különféle termékekkel működik, amelyek együttesen védik a hálózatot, a felhasználókat és a végpontokat, a felhő szélét és az alkalmazásokat. A SecureX funkcionalitás a Cisco biztonsági termékek széles és változatos portfóliójába van beépítve, beleértve a következő generációs tűzfalakat, VPN-t, hálózati elemzést, identitásszolgáltató motort, fejlett kártevő elleni védelmet (AMP) és sok más olyan rendszert, amelyek a hálózat minden aspektusát biztosítják. .



3.3.4

Videó - Cisco SecureX bemutató

Play Video

3.3.5

Biztonsági szolgáltatások

A fenyegetésekkel kapcsolatos hírszerzési és biztonsági szolgáltatások lehetővé teszik a fenyegetéssel kapcsolatos információk, például a sebezhetőségek, a kompromisszumjelzők (IOC) és a mérséklő technikák cseréjét. Ezeket az információkat nem csak a személyzettel osztják meg, hanem a biztonsági rendszerekkel is. A fenyegetések megjelenésekor a fenyegetésintelligencia szolgáltatások tűzfalszabályokat és IOC-kat hoznak létre és osztanak ki a szolgáltatásra előfizetett eszközökön.

Az egyik ilyen szolgáltatás az ábrán látható Cisco Talos Threat Intelligence Group. A Talos a világ egyik legnagyobb kereskedelmi fenyegetésekkel foglalkozó hírszerző csapata, amely világszínvonalú kutatókból, elemzőkből és mérnökökből áll. A Talos célja, hogy segítsen megvédeni a vállalati felhasználókat, adatokat és infrastruktúrát az aktív ellenfelektől. A Talos csapata információkat gyűjt az aktív, meglévő és újonnan megjelenő fenyegetésekről. A Talos ezután átfogó védelmet nyújt előfizetői számára ezekkel a támadásokkal és rosszindulatú programokkal szemben.

A Cisco Security termékek valós időben használhatják a Talos fenyegetési intelligenciáját, hogy gyors és hatékony biztonsági megoldásokat kínáljanak. A Cisco Talos ingyenes szoftvereket, szolgáltatásokat, erőforrásokat és adatokat is biztosít. A Talos karbantartja a biztonsági incidens-észlelési szabálykészleteket a Snort.org, a ClamAV és a SpamCop hálózati biztonsági eszközökhöz.



Számos felügyelt hálózati biztonsági szolgáltatás érhető el olyan szolgáltatóktól, mint a Cisco, a Sentinel Intrusion Prevention Systems, az IBM, az AT&T és a Core Security. Ezek a szervezetek a szolgáltatások széles skáláját kínálják, beleértve az átfogó menedzselt biztonságot szolgáltatásként (SECcaaS vagy SaaS)

# Gyakori hálózati támadások mérséklése

3.4.1

## A hálózat védelme

Folyamatos éberség és folyamatos oktatás szükséges ahhoz, hogy hálózatát megvédje a támadásoktól. Az alábbiak a legjobb gyakorlatok a hálózat biztosítására:

* Írott biztonsági szabályzat kidolgozása a vállalat számára.
* Tájékoztassa az alkalmazottakat a social engineering kockázatairól, és dolgozzon ki stratégiákat a személyazonosság telefonon, e-mailben vagy személyesen történő érvényesítésére.
* A rendszerekhez való fizikai hozzáférés szabályozása.
* Használjon erős jelszavakat, és gyakran változtassa meg őket.
* Az érzékeny adatok titkosítása és jelszavas védelme.
* Valósítson meg biztonsági hardvereket és szoftvereket, például tűzfalakat, IPS-eket, virtuális magánhálózati (VPN) eszközöket, víruskereső szoftvereket és tartalomszűrést.
* Rendszeresen készítsen biztonsági másolatot, és tesztelje a mentett fájlokat.
* Zárja le a szükségtelen szolgáltatásokat és portokat.
* Tartsa naprakészen a javításokat, ha lehetséges, hetente vagy naponta telepítse őket, hogy megelőzze a puffertúlcsordulást és a jogosultság-eszkalációs támadásokat.
* Végezzen biztonsági auditokat a hálózat teszteléséhez.

3.4.2

## Malware enyhítése

A rosszindulatú programok, beleértve a vírusokat, férgeket és trójai falovakat, komoly problémákat okozhatnak a hálózatokon és a végeszközökön. A hálózati adminisztrátorok számos eszközzel tudják enyhíteni ezeket a támadásokat.

**Megjegyzés** : Az enyhítő technikákat a biztonsági közösség gyakran „ellenintézkedésnek” nevezi.

A vírusok és trójai faló támadások mérséklésének egyik módja az antivírus szoftver. A víruskereső szoftver segít megelőzni a gazdagépek megfertőződését és rosszindulatú kódok terjesztését. A fertőzött számítógépek megtisztítása sokkal több időt vesz igénybe, mint a víruskereső szoftverek és víruskereső definíciók naprakész karbantartása ugyanazokon a gépeken.

A víruskereső szoftver ma a legszélesebb körben alkalmazott biztonsági termék a piacon. Számos vírusirtó szoftvert készítő vállalat, például a Symantec, a McAfee és a Trend Micro több mint egy évtizede foglalkozik vírusok észlelésével és eltávolításával. Sok vállalat és oktatási intézmény mennyiségi licencet vásárol felhasználóinak. A felhasználók bejelentkezhetnek egy webhelyre a fiókjukkal, és letölthetik a víruskereső szoftvert asztali számítógépükre, laptopjukra vagy szerverükre.

A víruskereső termékek frissítési automatizálási lehetőségekkel rendelkeznek, így az új vírusleírások és új szoftverfrissítések automatikusan vagy igény szerint letölthetők. Ez a gyakorlat a hálózat vírusmentességének legkritikusabb követelménye, és ezt a hálózatbiztonsági szabályzatban kell formalizálni.

A víruskereső termékek gazdagép alapúak. Ezeket a termékeket számítógépekre és szerverekre telepítik a vírusok észlelése és eltávolítása érdekében. Ezek azonban nem akadályozzák meg a vírusok bejutását a hálózatba, ezért a hálózatbiztonsági szakembernek tisztában kell lennie a főbb vírusokkal, és nyomon kell követnie a feltörekvő vírusokkal kapcsolatos biztonsági frissítéseket.

A rosszindulatú programok fenyegetésének mérséklésének másik módja a rosszindulatú programok hálózatba való bejutásának megakadályozása. A hálózat peremén lévő biztonsági eszközök az ismert rosszindulatú fájlokat azonosítani tudják a kompromittálás mutatói alapján. A fájlok eltávolíthatók a bejövő adatfolyamból, mielőtt incidenst okoznának. Sajnos a fenyegetések szereplői tisztában vannak ezzel az ellenintézkedéssel, és gyakran annyira módosítják rosszindulatú programjaikat, hogy elkerüljék az észlelést. Ezek a kihasználások bekerülnek a hálózatba, és kikerülik a víruskereső szoftvereket is. Egyetlen enyhítő technika sem lehet 100%-ban hatékony. Biztonsági incidensek lesznek.

3.4.3

## A férgek enyhítése

A férgek inkább hálózatalapúak, mint a vírusok. A féregelhárítás szorgalmat és koordinációt igényel a hálózatbiztonsági szakemberek részéről.

Amint az ábrán látható, a féregtámadásra adott válasz négy szakaszra bontható: elszigetelés, beoltás, karantén és kezelés.

Az ábra egy grafikon, amely leírja a féregtámadások enyhítésének négy fázisát.

1324

ElzárásOltásKaranténKezelés

| **Fázis** | **Válasz** |
| --- | --- |
| 1. Elzárás | Az elszigetelési szakasz magában foglalja a féregfertőzés terjedésének korlátozását a hálózat már érintett területeire. Ez megköveteli a hálózat felosztását és szegmentálását, hogy lelassítsa vagy leállítsa a férget, és megakadályozza, hogy a jelenleg fertőzött gazdagépek más rendszereket célozzanak meg és fertőzzenek meg. Az elszigeteléshez mind a kimenő, mind a bejövő ACL-eket kell használni az útválasztókon és a hálózat vezérlőpontjain lévő tűzfalakon. |
| 2. Beoltás | Az oltási fázis párhuzamosan vagy azt követően zajlik az elszigetelési fázissal. Az oltási fázis során minden nem fertőzött rendszert a megfelelő szállítói javítással javítanak. Az oltási folyamat tovább fosztja a férget minden elérhető célponttól. |
| 3. Karantén | A karantén szakasz magában foglalja a fertőzött gépek felkutatását és azonosítását a zárt területeken, valamint azok leválasztását, blokkolását vagy eltávolítását. Ez megfelelően elszigeteli ezeket a rendszereket a kezelési fázishoz. |
| 4. Kezelés | A kezelési szakasz magában foglalja a fertőzött rendszerek aktív fertőtlenítését. Ez magában foglalhatja a féregfolyamat leállítását, a féreg által bevezetett módosított fájlok vagy rendszerbeállítások eltávolítását, valamint a féreg által a rendszer kihasználásához használt sebezhetőség javítását. Súlyosabb esetekben előfordulhat, hogy a rendszert újra kell telepíteni a féreg és melléktermékeinek eltávolítása érdekében. |

3.4.4

## A felderítő támadások mérséklése

A felderítő támadások jellemzően más támadások előfutárai, amelyek célja a hálózathoz való jogosulatlan hozzáférés, vagy a hálózat működésének megzavarása. A hálózatbiztonsági szakember az előre konfigurált riasztásoktól kapott értesítések segítségével észlelheti, ha felderítő támadás van folyamatban. Ezek a riasztások bizonyos paraméterek, például a másodpercenkénti ICMP-kérelmek számának túllépése esetén aktiválódnak. Az ilyen típusú tevékenységek figyelésére és riasztás generálására különféle technológiák és eszközök használhatók. A Cisco Adaptive Security Appliance (ASA) behatolásmegelőzést biztosít önálló eszközön. Ezenkívül a Cisco ISR támogatja a hálózat alapú behatolásmegelőzést a Cisco IOS biztonsági rendszerképen keresztül.

A felderítő támadások többféle módon mérsékelhetők, beleértve a következőket:

* Hitelesítés végrehajtása a megfelelő hozzáférés biztosítása érdekében.
* Titkosítás használata a csomagszimuláló támadások haszontalanná tételére.
* Szippantásgátló eszközök használata a csomagszimuláló támadások észlelésére.
* Kapcsolt infrastruktúra megvalósítása.
* Tűzfal és IPS használata.

A szippantásgátló szoftverek és hardvereszközök észlelik a gazdagépek válaszidejének változásait, hogy megállapítsák, hogy a gazdagépek nagyobb forgalmat dolgoznak-e fel, mint amennyit a saját forgalmi terhelésük jelez. Bár ez nem szünteti meg teljesen a fenyegetést, egy átfogó mérséklő rendszer részeként csökkentheti a fenyegetés előfordulásának számát.

A titkosítás hatékony a csomagszimuláló támadások mérséklésére is. Ha a forgalom titkosított, a csomagszimuláló használata kevéssé hasznos, mivel a rögzített adatok nem olvashatók.

A portellenőrzést lehetetlen csökkenteni, de a behatolásgátló rendszer (IPS) és a tűzfal használata korlátozhatja a portszkennerrel felderíthető információkat. A ping-sweepek leállíthatók, ha az ICMP-visszhang és a visszhang-válasz ki van kapcsolva a szélső útválasztókon; azonban, ha ezeket a szolgáltatásokat kikapcsolják, a hálózati diagnosztikai adatok elvesznek. Ezenkívül a portvizsgálatok teljes ping-söprés nélkül is futtathatók. A vizsgálat egyszerűen tovább tart, mert az inaktív IP-címeket is megvizsgálja.

Az ábra a felderítő támadások mérséklésének módszereit mutatja be. A támadó két hálózat között kapcsolódik. A támadó fölött nagy piros X van.

### Felderítő támadás mérséklő technikák

Router ARouter BA műsorvezető Aműsorvezető BTámadó

3.4.5

## A hozzáférési támadások mérséklése

Számos technika áll rendelkezésre a hozzáférési támadások mérséklésére. Ide tartozik az erős jelszavas biztonság, a minimális bizalom elve, a kriptográfia, az operációs rendszer és az alkalmazás javítások alkalmazása.

Meglepően sok hozzáférési támadást hajtanak végre egyszerű jelszókitaláláson vagy a jelszavak elleni brute force szótári támadásokon keresztül. Az ez ellen való védekezés érdekében hozzon létre és kényszerítsen ki egy erős hitelesítési szabályzatot, amely a következőket tartalmazza:

* **Használjon erős jelszavakat** – Az erős jelszavak legalább nyolc karakterből állnak, és tartalmaznak nagybetűket, kisbetűket, számokat és speciális karaktereket.
* **Fiókok letiltása meghatározott számú sikertelen bejelentkezés után** – Ez a gyakorlat segít megelőzni a folyamatos jelszókísérleteket.

A hálózatot is a minimális bizalom elve alapján kell kialakítani. Ez azt jelenti, hogy a rendszerek nem használhatják egymást szükségtelenül. Például, ha egy szervezetnek van egy megbízható kiszolgálója, amelyet nem megbízható eszközök, például webszerverek használnak, a megbízható kiszolgálónak nem szabad feltétel nélkül megbíznia a nem megbízható eszközökben.

A kriptográfia minden modern biztonságos hálózat kritikus eleme. A hálózat távoli eléréséhez titkosítás használata javasolt. Az útválasztási protokoll forgalmát is titkosítani kell. Minél jobban titkosított a forgalom, annál kevesebb lehetőségük van a hackereknek az adatok elfogására a köztes támadásokkal.

A titkosított vagy kivonatolt hitelesítési protokollok használata, valamint az erős jelszópolitika nagymértékben csökkenti a sikeres hozzáférési támadások valószínűségét.

Végül tájékoztassa az alkalmazottakat a social engineering kockázatairól, és dolgozzon ki stratégiákat a személyazonosság telefonon, e-mailben vagy személyesen történő érvényesítésére. A többtényezős hitelesítés (MFA) egyre gyakoribb. Ebben a megközelítésben a hitelesítéshez két vagy több független igazolási mód szükséges. Például egy jelszó kombinálható egy szöveges üzenetben elküldött kóddal. Szoftver vagy különálló eszközök használhatók olyan tokenek létrehozására, amelyek csak egy felhasználásra alkalmasak. Ezek a tokenértékek, ha jelszóval együtt vannak ellátva, további biztonsági réteget nyújtanak, amely megakadályozza a fenyegető szereplők által kitalált vagy ellopott jelszavak használatát.

A hozzáférési támadások általában a naplók, a sávszélesség-kihasználás és a folyamatterhelések áttekintésével észlelhetők. A hálózati biztonsági szabályzatnak meg kell határoznia, hogy a naplókat formálisan karbantartsák minden hálózati eszköz és kiszolgáló esetében. A naplók áttekintésével a hálózati biztonsági személyzet megállapíthatja, hogy szokatlanul sok sikertelen bejelentkezési kísérlet történt-e.

3.4.6

## DoS támadások mérséklése

A DoS támadások egyik első jele a nem elérhető erőforrások vagy a szokatlanul lassú hálózati teljesítmény miatti nagyszámú felhasználói panasz. A támadások számának minimalizálása érdekében a hálózatot használó szoftvercsomagnak mindig futnia kell. A hálózati viselkedés elemzése képes észlelni a szokatlan használati mintákat, amelyek azt jelzik, hogy DoS támadás történik. A szervezet hálózati biztonsági szabályzatának elő kell írnia a szokatlan hálózati viselkedés észlelésének eszközét. A szokatlan aktivitást mutató hálózathasználati grafikon DoS támadást is jelezhet.

A DoS támadások egy nagyobb offenzíva részét képezhetik. A DoS támadások problémákat okozhatnak a támadott számítógépek hálózati szegmenseiben. Például egy támadás túllépheti az internet és a LAN közötti útválasztó másodpercenkénti csomagkapacitását, ami nemcsak a célrendszert veszélyezteti, hanem azokat a hálózati eszközöket is, amelyeken a forgalomnak át kell haladnia. Ha a támadást kellően nagy léptékben hajtják végre, az internetkapcsolat teljes földrajzi régiói veszélybe kerülhetnek.

A múltban sok DoS támadás hamisított címekről származott. A Cisco útválasztók és switchek számos hamisítás elleni technológiát támogatnak, mint például a portbiztonság, a DHCP (Dynamic Host Configuration Protocol) lesni, az IP Source Guard, a Dynamic Address Resolution Protocol (DAI) vizsgálat és a hozzáférés-vezérlési listák (ACL).

# Cisco Network Foundation védelmi keretrendszer

3.5.1

## NFP-keretrendszer

A Cisco Network Foundation Protection (NFP) keretrendszer átfogó irányelveket ad a hálózati infrastruktúra védelmére. Ezek az irányelvek képezik a folyamatos szolgáltatásnyújtás alapját.

Az NFP logikusan három funkcionális területre osztja a routereket és switcheket, amint az az ábrán látható:

* **Vezérlősík** – Felelős az adatok helyes irányításáért. A vezérlősík forgalom magának a hálózatnak a működéséhez szükséges eszközök által generált csomagokból áll, mint például az ARP üzenetváltások vagy az OSPF útválasztási hirdetések.
* **Menedzsment sík** - A hálózati elemek kezeléséért felelős. A felügyeleti sík forgalmat hálózati eszközök vagy hálózatfelügyeleti állomások generálják olyan folyamatok és protokollok használatával, mint a Telnet, SSH, TFTP, FTP, NTP, AAA, SNMP, syslog, TACACS+, RADIUS és NetFlow.
* **Adatsík (Forwarding plane)** - Az adatok továbbításáért felelős. Az adatsík forgalom általában a felhasználók által generált csomagokból áll, amelyeket a végeszközök között továbbítanak. A forgalom nagy része az útválasztón vagy kapcsolón keresztül az adatsíkon keresztül halad.

Az ábra a Cisco Network Foundation Protection (NFP) keretrendszer összetevőit mutatja.

### Cisco NFP

Menedzsment munkamenetekAdatsíkIP továbbítási táblázatMenedzsment folyamatokRouting ProtocolIP-útválasztó táblázatIrányítósíkKezelési síkÚtválasztási információk cseréjeKimenő IP-csomagBejövő IP-csomag

3.5.2

## A vezérlősík biztosítása

A vezérlősík forgalom magának a hálózatnak a működéséhez szükséges, eszköz által generált csomagokból áll. A vezérlősík biztonsága az alábbi szolgáltatásokkal valósítható meg, az ábrán látható módon:

* **Útválasztási protokoll hitelesítés** – Az útválasztási protokoll-hitelesítés vagy szomszédos hitelesítés megakadályozza, hogy az útválasztó elfogadja a csalárd útválasztási frissítéseket. A legtöbb útválasztási protokoll támogatja a szomszédos hitelesítést.
* **Control Plane Policing (CoPP)** – A CoPP a Cisco IOS szolgáltatása, amely lehetővé teszi a felhasználók számára a hálózati eszköz útvonal-processzora által kezelt forgalom szabályozását.
* **AutoSecure** – Az AutoSecure zárolhatja a felügyeleti sík funkcióit, valamint az útválasztó továbbítási sík szolgáltatásait és funkcióit.

A CoPP-t úgy tervezték, hogy megakadályozza, hogy a szükségtelen forgalom túlterhelje az útvonalprocesszort. A CoPP szolgáltatás a vezérlősíkot külön entitásként kezeli, saját bemeneti (bemeneti) és kimeneti (kimeneti) portjaival. Szabálykészlet hozható létre és társítható a vezérlősík be- és kimeneti portjaihoz.

Az ábra a Vezérlősík rögzítésének módjait mutatja be.

### Az irányító sík

AdatsíkRouting ProtocolIP-útválasztó táblázatIrányítósíkÚtválasztási információk cseréje

3.5.3

## A menedzsmentsík biztosítása

A felügyeleti sík forgalmat hálózati eszközök vagy hálózatkezelő állomások generálják olyan folyamatok és protokollok használatával, mint a Telnet, SSH és TFTP stb. A felügyeleti sík nagyon vonzó célpont a hackerek számára. Emiatt a menedzsment modult több olyan technológiával építették fel, amelyek az ilyen kockázatok csökkentését szolgálják.

A felügyeleti gazdagépek és a felügyelt eszközök közötti információáramlás lehet sávon kívüli (OOB), ahol az információ olyan hálózaton belül folyik, amelyen nincs éles forgalom. Lehet sávon belüli is, ahol az információ a vállalati termelési hálózaton, az interneten vagy mindkettőn keresztül áramlik.

A felügyeleti sík biztonsága az alábbi szolgáltatásokkal valósítható meg, az ábrán látható módon:

* **Bejelentkezési és jelszó házirend** – Korlátozza az eszközök hozzáférhetőségét. Korlátozza az elérhető portokat, és korlátozza a „ki” és „hogyan” hozzáférési módokat.
* **Jogi értesítés jelenléte** – Jogi közleményeket jelenít meg. Ezeket gyakran egy vállalat jogi tanácsadója dolgozza ki.
* **Biztosítsa az adatok bizalmas kezelését** – Megvédi a helyben tárolt érzékeny adatokat a megtekintéstől vagy másolástól. Erős hitelesítésű felügyeleti protokollokat használ a jelszavak és eszközkonfigurációk felfedését célzó bizalmassági támadások mérséklésére.
* **Szerepkör alapú hozzáférés-vezérlés (RBAC)** – Biztosítja, hogy csak hitelesített felhasználók, csoportok és szolgáltatások kapjanak hozzáférést. Az RBAC és a hitelesítési, engedélyezési és könyvelési (AAA) szolgáltatások olyan mechanizmusokat biztosítanak, amelyek hatékonyan kezelik a hozzáférés-szabályozást.
* **Műveletek engedélyezése** – Korlátozza az adott felhasználó, csoport vagy szolgáltatás által engedélyezett műveleteket és nézeteket.
* **Kezelési hozzáférési jelentés engedélyezése** – Naplók és fiókok minden hozzáféréshez. Rögzíti, hogy ki érte el az eszközt, mi történt és mikor.

Az RBAC korlátozza a felhasználói hozzáférést a felhasználó szerepe alapján. A szerepkörök a munka- vagy feladatfunkciók szerint jönnek létre, és hozzáférési engedélyeket rendelnek hozzá bizonyos eszközökhöz. A felhasználók ezután szerepkörökhöz vannak rendelve, és megkapják az adott szerepkörhöz meghatározott engedélyeket.

A Cisco IOS rendszerben a szerepkör-alapú CLI-hozzáférési szolgáltatás az RBAC-t valósítja meg az útválasztó-felügyeleti hozzáféréshez. A szolgáltatás különböző „nézeteket” hoz létre, amelyek meghatározzák, hogy mely parancsok fogadhatók el, és milyen konfigurációs információk láthatók. A méretezhetőség érdekében a felhasználókat, engedélyeket és szerepköröket általában egy központi adattárszerveren hozzák létre és tartják karban. Ez több eszköz számára is elérhetővé teszi a hozzáférés-vezérlési szabályzatot. A központi adattárszerver lehet egy Cisco Identity Services Engine (ISE), amely hitelesítési, engedélyezési és könyvelési (AAA) hálózati szolgáltatásokat nyújthat.

Az ábra a Kezelősík rögzítésének módjait mutatja be.

### A gazdálkodási terv

Menedzsment munkamenetekMenedzsment folyamatokKezelési sík

3.5.4

## Az adatsík biztosítása

Az adatsík forgalom többnyire az adatsíkon keresztül a routeren keresztül továbbított felhasználói csomagokból áll. Az adatsík biztonsága ACL-ek, hamisításgátló mechanizmusok és 2-es rétegbeli biztonsági szolgáltatások segítségével valósítható meg, amint az az ábrán látható.

Az ábra az Adatsík rögzítésének módjait mutatja be.

### Az adatsík

AdatsíkIP továbbítási táblázatIrányítósíkKimenő IP-csomagBejövő IP-csomag

Az ACL-ek csomagszűrést hajtanak végre annak szabályozására, hogy mely csomagok mozogjanak a hálózaton keresztül, és hová mehetnek ezek a csomagok. Az ACL-eket számos módon használják az adatsík biztosítására:

* **A nem kívánt forgalom vagy felhasználók blokkolása** – Az ACL-ek szűrhetik a bejövő vagy kimenő csomagokat az interfészen. Használhatók a hozzáférés szabályozására forráscímek, célcímek vagy felhasználói hitelesítés alapján.
* **A DoS támadások esélyének csökkentése** – Az ACL-ek segítségével meghatározható, hogy a gazdagépektől, hálózatoktól vagy felhasználóktól érkező forgalom hozzáférhet-e a hálózathoz. Az ASA TCP-elfogó funkciója egy olyan mechanizmus, amely a végállomások, különösen a kiszolgálók védelmére használható a TCP SYN-elárasztó támadásaival szemben.
* **Hamisítási támadások mérséklése** – Az ACL-ek lehetővé teszik a biztonsági szakemberek számára, hogy a hamisítási támadások mérséklésére ajánlott gyakorlatokat hajtsanak végre.
* **Sávszélesség-szabályozás biztosítása** – A lassú linken lévő ACL-ek megakadályozhatják a túlzott forgalmat.
* **Forgalom osztályozása a felügyeleti és vezérlési síkok védelme érdekében** – ACL-ek alkalmazhatók a vty sorokon.

Az ACL-ek hamisítás elleni mechanizmusként is használhatók az érvénytelen forráscímmel rendelkező forgalom elvetésével. Ez azt jelenti, hogy a támadásokat érvényes, elérhető IP-címekről kell indítani, ami lehetővé teszi a csomagok nyomon követését a támadás indítójáig.

Az olyan szolgáltatások, mint például az Unicast Reverse Path Forwarding (uRPF), felhasználhatók a hamisítás elleni stratégia kiegészítésére.

A Cisco Catalyst kapcsolók integrált funkciókat használhatnak a Layer 2 infrastruktúra védelmére. A következő Layer 2 biztonsági eszközök vannak beépítve a Cisco Catalyst kapcsolóiba:

* **Port biztonság** – Megakadályozza a MAC-címek hamisítását és a MAC-címek elárasztását.
* **DHCP leskelődés** – Megakadályozza a kliens támadásokat a DHCP-kiszolgáló és a kapcsoló ellen.
* **Dinamikus ARP-ellenőrzés (DAI)** – A DHCP-snooping-tábla használatával növeli az ARP biztonságát az ARP-mérgezés és -hamisítási támadások hatásának minimalizálása érdekében.
* **IP Source Guard (IPSG)** – Megakadályozza az IP-címek hamisítását a DHCP lekérdezési táblázat segítségével.

Ez a kurzus a kezelési és adatsíkok védelmére használt különféle technológiákra és protokollokra összpontosít.

3.5.5

### Ellenőrizze a megértését – Cisco Network Foundation védelmi keretrendszer

Az űrlap teteje

Ellenőrizze, hogy megértette-e a Cisco Network Foundation védelmi keretrendszerét, és válassza ki a megfelelő választ a következő kérdésekre.

1. Melyik NFP-sík használna jellemzően sávon kívüli (OOB) hozzáférést?



control plane



management plane



data plane

1. Melyik NFP gép használ CoPP-t?



control plane



management plane



data plane

1. Melyik NFP-sík felelős a hozzáférés-vezérlési listák (ACL) alkalmazásáért?



control plane



management plane



data plane

1. A vezérlősík melyikért felelős az alábbi jellemzők közül? (Válassz hármat.)



routing protocol authentication



blocking unwanted traffic or users



logs and accounts for all access



port security



route processor traffic



mitigating spoof attacks



role-based access control



password policy



AutoSecure

1. A felügyeleti sík melyikért felelős az alábbi szolgáltatások közül? (Válassz hármat.)



routing protocol authentication



blocking unwanted traffic or users



logs and accounts for all access



port security



route processor traffic



mitigating spoof attacks



role-based access control



password policy



AutoSecure

1. Az adatsík az alábbi jellemzők közül melyikért felelős? (Válassz hármat.)



routing protocol authentication



blocking unwanted traffic or users



logs and accounts for all access



port security



route processor traffic



mitigating spoof attacks



role-based access control



password policy



AutoSecure

# A fenyegetések enyhítése Összefoglaló

3.6.1

## Mit tanultam ebben a modulban?

**A hálózat**  
védelme A hálózatbiztonsági szakemberek felelősek a szervezet adatbiztonságának fenntartásáért, valamint az információk integritásának és bizalmasságának biztosításáért. A biztonsági szakembereknek folyamatosan tájékozottnak kell lenniük a fenyegetésekről és a sebezhetőségekről, ahogy azok fejlődnek. Számos hálózatbiztonsági szervezet tájékoztatja Önt, köztük a SANS, a Mitre, a FIRST, a SecurityNewsWire, az ISC 2 és a CIS. A hálózatbiztonsági szakemberek számára a tanúsítványokat a következő szervezetek kínálják:

* GIAC
* ISC 2
* ISACA
* EK-Tanács
* CWSP

Az információbiztonság az információk és információs rendszerek védelmével foglalkozik a jogosulatlan hozzáférés, használat, nyilvánosságra hozatal, megszakítás, módosítás vagy megsemmisítés ellen. A CIA Triad a terület fogalmi alapjául szolgál. A CIA triád az információbiztonság három összetevőjéből áll: Titoktartás, Integritás és Elérhetőség.

**Hálózati biztonsági szabályzatok**  
Az ISO/IEC 14 hálózati biztonsági tartományt határoz meg. Az ISO/IEC 27002 szabvány szerint ez a 14 tartomány arra szolgál, hogy magas szinten szervezze meg az információk hatalmas körét a hálózati biztonság égisze alatt. Ezek a tartományok jelentős párhuzamot mutatnak a CISSP-tanúsítvány által meghatározott tartományokkal. A 14 tartomány közös alapként szolgál a szervezeti biztonsági szabványok és a hatékony biztonságkezelési gyakorlat kialakításához. Segítenek a szervezetek közötti kommunikáció megkönnyítésében is. A hálózatépítésben a házirendek határozzák meg a hálózaton engedélyezett tevékenységeket. A biztonsági szabályzatba belefoglalható házirendek közé tartozik az azonosítási és hitelesítési házirend, a jelszóházirend, az elfogadható használat házirendje, a távoli hozzáférési szabályzat, a hálózatkarbantartási szabályzat és az incidenskezelési eljárások. A biztonsági szabályzat egy "élő dokumentum", ami azt jelenti, hogy a dokumentumot rendszeresen frissítik a technológiai, üzleti és alkalmazotti követelmények változásával. Sok vállalatnak a BYOD köré is el kell helyeznie szabályzatot. A hálózat biztonságát illetően külső szabályozások is léteznek. A hálózatbiztonsági szakembereknek ismerniük kell az INFOSEC szakemberekre kötelező érvényű törvényeket és etikai kódexeket.

**Biztonsági eszközök, platformok és szolgáltatások**  
Két általános analógia létezik a mélyreható védelmi megközelítés leírására: a biztonsági hagyma és a biztonsági articsóka. A Security Onion segítségével a fenyegetés szereplőinek rétegről rétegre kell meghámozniuk a hálózat védelmét, hasonlóan a hagyma hámozásához. A hálózatépítés változó környezete, mint például a határok nélküli hálózatok fejlődése, ezt a hasonlatot a „biztonsági articsóka”-ra változtatta, ami a fenyegetés szereplői számára előnyös. A fenyegetés szereplőinek többé nem kell minden réteget lehúzniuk. Csak bizonyos „articsókaleveleket” kell eltávolítaniuk. A hálózat és rendszerei biztonságának ellenőrzésére számos hálózati penetrációt vizsgáló eszközt fejlesztettek ki. Ezen eszközök kategóriái közé tartoznak a jelszófeltörők, a vezeték nélküli feltörő eszközök, a hálózati szkennelő és feltörő eszközök, a csomagkészítő eszközök, a csomagszimulálók, a rootkit detektorok, fuzzerek a sebezhetőségek, kriminalisztikai eszközök, hibakeresők, operációs rendszerek feltörésére, titkosítási eszközök, sebezhetőség-kihasználó eszközök és sebezhetőség-ellenőrzők keresésére. A fenyegetés-felderítő szolgáltatások lehetővé teszik a fenyegetéssel kapcsolatos információk, például a sebezhetőségek, az IOC-k és a mérséklő technikák cseréjét. Az egyik ilyen szolgáltatás a Cisco Talos Threat Intelligence Group.

**Gyakori hálózati támadások mérséklése**  
A hálózat biztonsága érdekében a következő bevált gyakorlatokat alkalmazzák: írásos biztonsági szabályzat kidolgozása, alkalmazottak oktatása, fizikai hozzáférés ellenőrzése a rendszerekhez, erős jelszavak használata és gyakori módosítása, érzékeny adatok titkosítása és jelszavas védelme, biztonsági hardver és szoftver telepítése, biztonsági mentések készítése és tesztelje a biztonsági mentési fájlokat, állítsa le a szükségtelen szolgáltatásokat és portokat, tartsa naprakészen a javításokat, és végezzen biztonsági auditokat és teszteket. A hálózati rendszergazdáknak számos eszközük van a rosszindulatú programok elleni támadások mérséklésére. A vírusok és trójai faló támadások mérséklésének elsődleges eszköze a víruskereső szoftver, amely ma a legszélesebb körben alkalmazott biztonsági termék a piacon. Ezek azonban nem akadályozzák meg a vírusok bejutását a hálózatba, ezért a hálózatbiztonsági szakembernek tisztában kell lennie a főbb vírusokkal, és nyomon kell követnie a feltörekvő vírusokkal kapcsolatos biztonsági frissítéseket. A férgek inkább hálózatalapúak, mint a vírusok. A féregtámadásra adott válasz négy szakaszra bontható: elszigetelés, oltás, karantén és kezelés. A felderítő támadások jellemzően további támadások előfutárai, azzal a céllal, hogy jogosulatlan hozzáférést szerezzenek egy hálózathoz vagy megzavarják a hálózat működését. A hálózatbiztonsági szakember az előre konfigurált riasztásoktól kapott értesítések segítségével észlelheti, ha felderítő támadás van folyamatban. A felderítő támadások többféle módon mérsékelhetők, beleértve a következőket: hitelesítés bevezetése a megfelelő hozzáférés biztosítására, titkosítás használata a csomagszimuláló támadások haszontalanná tételére, szippantásgátló eszközök használata a csomagszimuláló támadások észlelésére, kapcsolt infrastruktúra megvalósítása, tűzfal és IPS. A titkosítás hatékony a csomagszimuláló támadások mérséklésére is. Számos technika áll rendelkezésre a hozzáférési támadások mérséklésére. Ide tartozik az erős jelszavas biztonság, a minimális bizalom elve, a kriptográfia, az operációs rendszer és az alkalmazás javítások alkalmazása. A DoS-támadások számának minimalizálása érdekében egy hálózathasználati szoftvercsomagnak mindig futnia kell. A DoS támadások egy nagyobb offenzíva részét képezhetik. A DoS támadások problémákat okozhatnak a támadott számítógépek hálózati szegmenseiben. A múltban sok DoS támadás hamisított címekről származott. A Cisco útválasztók és kapcsolók számos hamisítás elleni technológiát támogatnak, mint például a portbiztonság, a DHCP-snooping, az IP Source Guard, a Dynamic ARP Inspection és az ACL-ek. operációs rendszer és alkalmazásjavítások alkalmazása. A DoS-támadások számának minimalizálása érdekében egy hálózathasználati szoftvercsomagnak mindig futnia kell. A DoS támadások egy nagyobb offenzíva részét képezhetik. A DoS támadások problémákat okozhatnak a támadott számítógépek hálózati szegmenseiben. A múltban sok DoS támadás hamisított címekről származott. A Cisco útválasztók és kapcsolók számos hamisítás elleni technológiát támogatnak, mint például a portbiztonság, a DHCP-snooping, az IP Source Guard, a Dynamic ARP Inspection és az ACL-ek. operációs rendszer és alkalmazásjavítások alkalmazása. A DoS-támadások számának minimalizálása érdekében egy hálózathasználati szoftvercsomagnak mindig futnia kell. A DoS támadások egy nagyobb offenzíva részét képezhetik. A DoS támadások problémákat okozhatnak a támadott számítógépek hálózati szegmenseiben. A múltban sok DoS támadás hamisított címekről származott. A Cisco útválasztók és kapcsolók számos hamisítás elleni technológiát támogatnak, mint például a portbiztonság, a DHCP-snooping, az IP Source Guard, a Dynamic ARP Inspection és az ACL-ek. sok DoS támadás hamisított címekről származott. A Cisco útválasztók és kapcsolók számos hamisítás elleni technológiát támogatnak, mint például a portbiztonság, a DHCP-snooping, az IP Source Guard, a Dynamic ARP Inspection és az ACL-ek. sok DoS támadás hamisított címekről származott. A Cisco útválasztók és kapcsolók számos hamisítás elleni technológiát támogatnak, mint például a portbiztonság, a DHCP-snooping, az IP Source Guard, a Dynamic ARP Inspection és az ACL-ek.

**Cisco Network Foundation védelmi keretrendszer**  
A Cisco NFP keretrendszer átfogó irányelveket ad a hálózati infrastruktúra védelméhez. Ezek az irányelvek képezik a folyamatos szolgáltatásnyújtás alapját. Az NFP logikailag három funkcionális területre osztja a routereket és switcheket: vezérlősíkra, felügyeleti síkra és adatsíkra (továbbítási síkra). A vezérlősík biztonsága a következő szolgáltatásokkal valósítható meg: útválasztási protokoll hitelesítés, CoPP és AutoSecure. A CoPP-t úgy tervezték, hogy megakadályozza, hogy a szükségtelen forgalom túlterhelje az útvonalprocesszort. A felügyeleti modult számos olyan technológiával építették fel, amelyek célja a fenyegető szereplők kockázatainak mérséklése. A felügyeleti sík biztonsága a következő szolgáltatásokkal valósítható meg: bejelentkezési és jelszó házirend, jogi értesítés bemutatása, az adatok bizalmas kezelésének biztosítása, RBAC, műveletek engedélyezése és a felügyeleti hozzáférési jelentés engedélyezése. Az adatsík biztonsága ACL-ek, hamisításgátló mechanizmusok és 2-es rétegbeli biztonsági szolgáltatások segítségével valósítható meg. Az ACL-eket számos módon használják az adatok védelmére, beleértve a nem kívánt forgalom vagy felhasználók blokkolását, a DoS-támadások esélyének csökkentését, a hamis támadások mérséklését, a sávszélesség szabályozását, a forgalom osztályozását a felügyeleti és vezérlési síkok védelme érdekében. Az ACL-ek hamisítás elleni mechanizmusként is használhatók az érvénytelen forráscímmel rendelkező forgalom elvetésével. funkciók, mint például az urPF, felhasználhatók a hamisítás elleni stratégia kiegészítésére. A következő 2. rétegű biztonsági eszközök vannak beépítve a Cisco Catalyst kapcsolóiba: portbiztonság, DHCP-snooping, DAI és IPSG. A Cisco NFP keretrendszer átfogó irányelveket ad a hálózati infrastruktúra védelméhez. Ezek az irányelvek képezik a folyamatos szolgáltatásnyújtás alapját. Az NFP logikailag három funkcionális területre osztja a routereket és switcheket: vezérlősíkra, felügyeleti síkra és adatsíkra (továbbítási síkra). A vezérlősík biztonsága a következő szolgáltatásokkal valósítható meg: útválasztási protokoll hitelesítés, CoPP és AutoSecure. A CoPP-t úgy tervezték, hogy megakadályozza, hogy a szükségtelen forgalom túlterhelje az útvonalprocesszort. A felügyeleti modult számos olyan technológiával építették fel, amelyek célja a fenyegető szereplők kockázatainak mérséklése. A felügyeleti sík biztonsága a következő szolgáltatásokkal valósítható meg: bejelentkezési és jelszó házirend, jogi értesítés bemutatása, az adatok bizalmas kezelésének biztosítása, RBAC, műveletek engedélyezése és a felügyeleti hozzáférési jelentés engedélyezése. Az adatsík biztonsága ACL-ek, hamisításgátló mechanizmusok és 2-es rétegbeli biztonsági szolgáltatások segítségével valósítható meg. Az ACL-eket számos módon használják az adatok védelmére, többek között: a nem kívánt forgalom vagy felhasználók blokkolása, a DoS támadások esélyének csökkentése, a hamisító támadások mérséklése, a sávszélesség szabályozásának biztosítása, a forgalom osztályozása a felügyeleti és vezérlési síkok védelme érdekében. Az ACL-ek hamisítás elleni mechanizmusként is használhatók az érvénytelen forráscímmel rendelkező forgalom elvetésével. funkciók, mint például az urPF, felhasználhatók a hamisítás elleni stratégia kiegészítésére. A következő 2. rétegű biztonsági eszközök vannak beépítve a Cisco Catalyst kapcsolóiba: portbiztonság, DHCP-snooping, DAI és IPSG. felhasználható a hamisítás elleni stratégia kiegészítésére. A következő 2. rétegű biztonsági eszközök vannak beépítve a Cisco Catalyst kapcsolóiba: portbiztonság, DHCP-snooping, DAI és IPSG. felhasználható a hamisítás elleni stratégia kiegészítésére. A következő 2. rétegű biztonsági eszközök vannak beépítve a Cisco Catalyst kapcsolóiba: portbiztonság, DHCP-snooping, DAI és IPSG.

3.6.2

## 3. modul – Veszélyek enyhítése kvíz

Az űrlap teteje

1. Mi az elsődleges eszköz a vírusok és trójai faló támadások mérséklésére?



blokkolja az ICMP visszhangot és visszhangot - válaszok



Titkosítás



szippantásgátló szoftver



víruskereső szoftver

1. Melyik három elem alkotja a CIA-triádot? (Válassz hármat.)



hozzáférés



elérhetőség



titoktartás



skálázhatóság



sértetlenség



közbelépés

1. Melyik biztonsági megvalósítás biztosítja a vezérlősík védelmét egy hálózati eszköz számára?



AAA a felügyeleti hozzáférés hitelesítéséhez



NTP a konzisztens időbélyegekért az üzenetek naplózásakor



titkosítás a távoli elérésű kapcsolatokhoz



útválasztási protokoll hitelesítés

1. Melyik fenyegetés - felderítő csoport biztosít blogokat és podcastokat , amelyek segítenek a hálózatbiztonsági szakembereknek hatékony és naprakész maradni ?



Püspöksüveg



FireEye



CybOX



Talos

1. A biztonsági szabályzat melyik szakasza határozza meg, hogy csak az arra jogosult személyek férhessenek hozzá a vállalati adatokhoz?



Internet hozzáférési szabályzat



hatóköri nyilatkozat



azonosítási és hitelesítési szabályzat



egyetemi hozzáférési szabályzat



elfogadható felhasználási szabályzat



felhatalmazási nyilatkozat

1. Melyik féregcsillapítási fázis tartalmazza a fertőzött rendszerek aktív fertőtlenítését?



oltás



visszatartás



kezelés



karantén

1. A határok nélküli hálózatok fejlődésével melyik zöldséget használják ma a védelmi - mélyreható megközelítés leírására?



Fejes káposzta



saláta



articsóka



hagyma

1. Hogyan változtatja meg a BYOD a vállalkozások hálózatépítési módját?



A BYOD felhasználók saját maguk felelősek hálózatuk biztonságáért, így csökken a szervezeti biztonsági szabályzatok szükségessége.



A BYOD eszközök drágábbak, mint a szervezet által vásárolt eszközök.



A BYOD megköveteli a szervezetektől, hogy asztali számítógépek helyett laptopokat vásároljanak.



A BYOD rugalmasságot biztosít abban, hogy a felhasználók hol és hogyan férhetnek hozzá a hálózati erőforrásokhoz.

1. A Cisco Network Foundation Protection keretrendszer mely funkcionális területe használ olyan protokollokat, mint a Telnet és az SSH a hálózati eszközök kezelésére?



irányító sík



továbbító repülőgép



kezelési sík



adatsík

1. Milyen biztonsági eszköz teszi lehetővé a fenyegetés szereplői számára, hogy feltörjenek egy vezeték nélküli hálózatot, és észleljék a biztonsági réseket?



NMap



Kattintson a fuzzerekre



SuperScan



KisMac

1. Mi a SANS elsődleges funkciója?



az Internet Storm Center karbantartására



szállítósemleges oktatási termékeket és karrierszolgáltatásokat nyújtani



az együttműködés és a koordináció előmozdítása az információmegosztás, az incidensek megelőzése és a gyors reagálás terén



a gyakori sebezhetőségek és kitettségek listájának karbantartása (CVE)

1. Milyen módszerrel csökkenthető a ping-sweep?



víruskereső szoftver telepítése a gazdagépekre



a szippantásgátló szoftver telepítése az összes hálózati eszközön



blokkolja az ICMP visszhangot és visszhangot - válaszok a hálózat szélén



titkosított vagy kivonatolt hitelesítési protokollok használatával

Bevezetés

4.0.1

Miért vegyem ezt a modult?

Az eszközök hozzáférésének biztosítása kritikus feladat egy hálózatbiztonsági szakember számára. A routerre úgy gondolhat, mint a bekerített udvar zárt kapujára. Ha valaki bejut azon a kapun, egy lépéssel közelebb kerül ahhoz, hogy hozzáférjen az Ön udvarán és házában lévő ingatlanához! Kinek kell engedélyezni a hozzáférést? Hogyan biztosítod a szélső routert? Milyen lépéseket tesz a biztonságos rendszergazdai hozzáférés konfigurálásához? Hogyan konfigurálható fokozott biztonság a virtuális bejelentkezésekhez? Olvasson tovább, hogy többet megtudjon!

4.0.2

Mit fogok tanulni ebben a modulban?

**Modul címe:** Secure Device Access

**Modul célja** : Biztonságos adminisztrátori hozzáférés konfigurálása.

| **téma címe** | **Téma Cél** |
| --- | --- |
| **Rögzítse az Edge Routert** | Magyarázza el, hogyan biztosítható a hálózati kerület. |
| **Konfigurálja a biztonságos adminisztrátori hozzáférést** | Használja a megfelelő parancsokat a jelszavak konfigurálásához Cisco IOS-eszközön. |
| **Konfigurálja a fokozott biztonságot a virtuális bejelentkezésekhez** | Használja a megfelelő parancsokat a virtuális bejelentkezés fokozott biztonságának konfigurálásához. |
| **SSH konfigurálása** | Konfiguráljon egy SSH-démont a biztonságos távoli kezeléshez. |

# Hálózati biztonság

v 1.0

[Ugrás a tartalomra](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                     
*                                   

1. Secure Device Access
2. Secure the Edge Router

# Rögzítse az Edge Routert

4.1.1

## Biztosítsa a hálózati infrastruktúrát

A hálózati infrastruktúra biztonságossá tétele kritikus fontosságú az általános hálózatbiztonság szempontjából. A hálózati infrastruktúra útválasztókat, kapcsolókat, kiszolgálókat, végpontokat és egyéb eszközöket tartalmaz.

Tekintsünk egy elégedetlen alkalmazottat, aki lazán átnéz egy hálózati rendszergazda válla fölött, miközben a rendszergazda bejelentkezik egy szélső útválasztóba. Meglepően egyszerű módja annak, hogy a támadó jogosulatlan hozzáférést szerezzen.

Ha egy támadó hozzáfér egy útválasztóhoz, a teljes hálózat biztonsága és felügyelete veszélybe kerülhet. Például egy támadó törölheti az indítási konfigurációt, és öt percen belül újratöltheti az útválasztót. Amikor az útválasztó újraindul, nem lesz indítási konfigurációja.

Az összes infrastruktúra-eszközhöz való jogosulatlan hozzáférés megakadályozása érdekében megfelelő biztonsági szabályzatokat és ellenőrzéseket kell végrehajtani. Az útválasztók a támadások elsődleges célpontjai, mivel ezek az eszközök közlekedési rendőrökként működnek, amelyek a forgalmat a hálózatokba, hálózatokon kívülre és hálózatok között irányítják.

Az ábrán látható szélső útválasztó az utolsó útválasztó a belső hálózat és egy nem megbízható hálózat, például az internet között. A szervezet teljes internetes forgalma egy szélső útválasztón megy keresztül, amely gyakran a hálózat első és utolsó védelmi vonalaként működik. A szélső útválasztó segít a védett hálózat kerületének védelmében, és olyan biztonsági műveleteket hajt végre, amelyek a szervezet biztonsági szabályzatain alapulnak. Ezen okok miatt elengedhetetlen a hálózati útválasztók biztonságossá tétele.

Az ábra a belső hálózat és a nem megbízható hálózat közötti peremútválasztót mutatja.

### Az Edge Router

Internet Organization untrusted edge router megbízható

4.1.2

## Edge Router biztonsági megközelítések

A peremútválasztó megvalósítása a szervezet méretétől és a szükséges hálózati tervezés összetettségétől függően változik. Az útválasztó implementációi tartalmazhatnak egyetlen útválasztót, amely egy teljes belső hálózatot véd, vagy egy útválasztót, amely az első védelmi vonalként funkcionál a mélyreható védelmi megközelítésben. A három megközelítés egyszerűsített topológiái az ábrán láthatók.

Az ábra egyszerűsített topológiákat mutat be a három szélső útválasztó biztonsági megközelítéséhez.

R1 R1 R2 R1

R2

Internet LAN 1   
192.168.2.0 Internet LAN 1   
192.168.2.0 tűzfal Internetes LAN 1   
192.168.2.0 DMZ tűzfal , egyetlen útválasztós megközelítés , mélyreható védelem, DMZ megközelítés

**Egyetlen router megközelítés**

Az ábrán egyetlen útválasztó csatlakoztatja a védett hálózatot vagy belső helyi hálózatot (LAN) az internethez. Az összes biztonsági házirend be van állítva ezen az eszközön. Ezt gyakrabban alkalmazzák kisebb telephelyeken, például fióktelepeken és kis irodai, otthoni irodai (SOHO) webhelyeken. Kisebb hálózatokban a szükséges biztonsági funkciókat az Integrated Services Routers (ISR) támogathatja anélkül, hogy ez akadályozná az útválasztó teljesítményét.

**Mélyreható védelmi megközelítés**

A mélyreható védelmi megközelítés biztonságosabb, mint az egyetlen útválasztó megközelítés. Több szintű biztonságot használ, mielőtt a forgalom belépne a védett LAN-ba. A védelemnek három elsődleges rétege van: a szélső útválasztó, a tűzfal és egy belső útválasztó, amely a védett LAN-hoz csatlakozik. A szélső útválasztó az első védelmi vonalként működik, és átvizsgáló útválasztóként ismert. A kezdeti forgalomszűrés végrehajtása után a szélső útválasztó minden belső LAN-kapcsolatot átad a második védelmi vonalnak, azaz a tűzfalnak.

A tűzfal általában ott veszi fel, ahol a szélső útválasztó elhagyja, és további szűrést hajt végre. További hozzáférés-vezérlést biztosít a kapcsolatok állapotának nyomon követésével, és ellenőrzőpontként működik. Alapértelmezés szerint a tűzfal megtagadja a külső (nem megbízható) hálózatok és a belső (megbízható) hálózatok közötti kapcsolatok kezdeményezését. Azonban lehetővé teszi a belső felhasználók számára, hogy kapcsolatot létesítsenek a nem megbízható hálózatokkal, és lehetővé teszi a válaszok visszaküldését a tűzfalon keresztül. Felhasználói hitelesítést (hitelesítési proxy) is végrehajthat, amelyben a felhasználókat hitelesíteni kell a hálózati erőforrásokhoz való hozzáféréshez.

A routerek nem az egyetlen eszközök, amelyek mélyreható védelmi megközelítésben használhatók. Más biztonsági eszközök, például behatolásgátló rendszerek (IPS), webes biztonsági berendezések (proxyszerverek) és e-mail biztonsági eszközök (spamszűrés) is megvalósíthatók.

**DMZ megközelítés**

Az ábrán a mélyreható védekezés egy változata látható. Ez a megközelítés magában foglal egy köztes területet, amelyet gyakran demilitarizált zónának (DMZ) neveznek. A DMZ olyan szerverekhez használható, amelyeknek elérhetőnek kell lenniük az internetről vagy más külső hálózatról. A DMZ két router között állítható be, egy belső router csatlakozik a védett hálózathoz és egy külső router csatlakozik a nem védett hálózathoz. Alternatív megoldásként a DMZ egyszerűen egy további port lehet egyetlen útválasztón. A tűzfal a védett és a nem védett hálózatok között helyezkedik el. A tűzfal úgy van beállítva, hogy lehetővé tegye a szükséges kapcsolatokat, például a HTTP-t a külső (nem megbízható) hálózatokról a DMZ nyilvános kiszolgálóihoz. A tűzfal elsődleges védelemként szolgál a DMZ-ben lévő összes eszköz számára.

4.1.3

## Az útválasztó biztonságának három területe

A szélső útválasztó biztonságossá tétele a hálózat biztonságának első fontos lépése. Ha vannak más belső útválasztók is, azokat is biztonságosan be kell állítani. Az útválasztó biztonságának három területét kell fenntartani.

**Fizikai biztonság**

Fizikai biztonság biztosítása az útválasztók számára:

* Helyezze az útválasztót és a hozzá csatlakozó fizikai eszközöket biztonságos, zárt helyiségbe, amely csak arra jogosult személyek számára hozzáférhető, nincs elektrosztatikus vagy mágneses interferencia, tűzoltó, valamint hőmérséklet- és páratartalom-szabályozással rendelkezik.
* Szereljen be szünetmentes tápegységet (UPS) vagy dízel tartalék áramfejlesztőt. Ha lehetséges, használjon redundáns tápegységeket a hálózati eszközökben. Ez csökkenti az áramkimaradás vagy az áramellátás meghibásodása miatti hálózati kimaradás lehetőségét.

**Operációs rendszer biztonsága**

Az útválasztó operációs rendszerek funkcióinak és teljesítményének biztosításához néhány eljárás szükséges:

* Szerelje fel az útválasztókat a lehető legnagyobb memóriával. A memória rendelkezésre állása segíthet csökkenteni a hálózatot bizonyos szolgáltatásmegtagadási (DoS) támadásokból eredő kockázatokat, miközben támogatja a biztonsági szolgáltatások legszélesebb körét.
* Használja az operációs rendszer legújabb, stabil verzióját, amely megfelel az útválasztó vagy hálózati eszköz jellemzőinek. Az operációs rendszerek biztonsági és titkosítási funkciói idővel javulnak és frissülnek, ezért elengedhetetlen a legfrissebb verzió.
* Őrizze meg az útválasztó operációs rendszer képeinek és konfigurációs fájljainak biztonságos másolatát biztonsági másolatként.

**Router keményedés**

A nem használt portokkal és szolgáltatásokkal való esetleges visszaélések kiküszöbölése:

* Biztonságos adminisztratív ellenőrzés. Győződjön meg arról, hogy csak az arra feljogosított személyzet férhet hozzá, és hogy hozzáférési szintje ellenőrzött.
* Tiltsa le a nem használt portokat és csatolókat. Csökkentse az eszközökhöz való hozzáférési módok számát.
* A szükségtelen szolgáltatások letiltása. Sok számítógéphez hasonlóan az útválasztónak is vannak olyan szolgáltatásai, amelyek alapértelmezés szerint engedélyezve vannak. E szolgáltatások némelyike ​​szükségtelen, és a támadók felhasználhatják az útválasztóról és a hálózatról szóló információk gyűjtésére. Ezt az információt ezután egy kizsákmányoló támadás során használhatják fel.

4.1.4

## Biztonságos adminisztrátori hozzáférés

Az adminisztrátori hozzáférés biztosítása rendkívül fontos biztonsági feladat. Ha egy illetéktelen személy adminisztrátori hozzáférést kap egy útválasztóhoz, akkor ez a személy megváltoztathatja az útválasztási paramétereket, letilthatja az útválasztási funkciókat, vagy felfedezhet más rendszereket a hálózaton belül, és hozzáférhet azokhoz.

Az infrastruktúra-eszközhöz való adminisztratív hozzáférés biztosítása számos fontos feladattal jár:

* **Eszköz hozzáférhetőségének korlátozása** – Korlátozza az elérhető portokat, korlátozza az engedélyezett kommunikátorokat és korlátozza a hozzáférési módokat.
* **Minden hozzáférés naplózása és fiókja** – naplózási célból rögzítheti, hogy aki hozzáfér egy eszközhöz, mi történt a hozzáférés során, és mikor történt a hozzáférés.
* **Hozzáférés hitelesítése** – Győződjön meg arról, hogy a hozzáférést csak hitelesített felhasználók, csoportok és szolgáltatások kapják. Korlátozza a sikertelen bejelentkezési kísérletek számát és a bejelentkezések közötti időt.
* **Műveletek engedélyezése** – Korlátozza az adott felhasználó, csoport vagy szolgáltatás által engedélyezett műveleteket és nézeteket.
* **Jelenítse meg a jogi értesítést** – jelenítsen meg egy jogi közleményt, amelyet a vállalat jogtanácsosával együtt kell kidolgozni az eszközhöz való különböző hozzáférési típusokhoz.
* **Biztosítsa az adatok bizalmas kezelését** – Védje meg a helyben tárolt és érzékeny adatokat a megtekintéstől és másolástól. Fontolja meg a kommunikációs csatornán áthaladó adatok szippantással, munkamenet-eltérítéssel és MITM (man-in-the-middle) támadásokkal szembeni sebezhetőségét.

4.1.5

## Biztonságos helyi és távoli hozzáférés

A router adminisztrációs célból elérhető helyileg vagy távolról:

* **Helyi hozzáférés** – Minden hálózati infrastruktúra eszköz elérhető helyben. Az útválasztó helyi eléréséhez általában közvetlen csatlakozásra van szükség a Cisco útválasztó konzolportjához, és olyan számítógépet kell használni, amelyen terminálemulációs szoftver fut, amint az az ábrán látható. A rendszergazdának fizikai hozzáféréssel kell rendelkeznie az útválasztóhoz, és konzolkábelt kell használnia a konzolporthoz való csatlakozáshoz. A helyi hozzáférést általában az eszköz kezdeti konfigurálásához használják.
* **Távoli elérés** – Az adminisztrátorok távolról is elérhetik az infrastruktúra-eszközöket, ahogy az az ábrán is látható. Bár az aux port opció elérhető, a legáltalánosabb távoli hozzáférési mód a Telnet, SSH, HTTP, HTTPS vagy SNMP kapcsolatok engedélyezése az útválasztóhoz a számítógépről. A számítógép lehet helyi hálózaton vagy távoli hálózaton. Ha azonban az eszköz hálózati kapcsolata nem működik, az egyetlen módja annak, hogy telefonvonalon keresztül érje el.

Az ábra a helyi hozzáférési módot mutatja soros kapcsolattal, a távoli hozzáférést SSH módszerrel, valamint a modemes és aux portos távelérést telefonvonalon keresztüli soros kapcsolattal.

### Adminisztratív hozzáférési módszerek

Router con aux vty soros kapcsolat PC terminál emulációs szoftverrel Helyi hozzáférés SSH csatlakozás PC terminál emulációs szoftverrel Router vty aux távelérés SSH soros kapcsolattal Router Modem PSTN aux vty távelérés modemmel és Aux porttal

Egyes távoli elérési protokollok egyszerű szövegként küldenek adatokat, beleértve a felhasználóneveket és jelszavakat is az útválasztónak. Ha a támadó hálózati forgalmat gyűjthet, miközben a rendszergazda távolról bejelentkezik az útválasztóba, akkor a támadó jelszavakat vagy az útválasztó konfigurációs adatait rögzítheti. Emiatt célszerű csak helyi hozzáférést engedélyezni az útválasztóhoz. Bizonyos helyzetekben azonban továbbra is szükség lehet távoli hozzáférésre. A hálózat távoli elérésekor óvintézkedéseket kell tenni:

* A rendszergazda számítógép és az útválasztó közötti összes forgalom titkosítása. Például a Telnet használata helyett használja az SSH 2-es verzióját; vagy a HTTP helyett használjon HTTPS-t.
* Hozzon létre egy dedikált felügyeleti hálózatot. A felügyeleti hálózat csak azonosított adminisztrációs gazdagépeket és kapcsolatokat tartalmazhat az útválasztó dedikált interfészéhez. A hálózathoz való hozzáférés szigorúan ellenőrizhető.
* Konfiguráljon egy csomagszűrőt, hogy csak az azonosított adminisztrációs gazdagépek és az előnyben részesített protokollok férhessenek hozzá az útválasztóhoz. Például csak az adminisztrációs gazdagép IP-címéről érkező SSH-kérések engedélyezése a hálózat útválasztóihoz való csatlakozás kezdeményezéséhez.
* Configure and establish a VPN connection to the local network before connecting to a router management interface.

Ezek az óvintézkedések értékesek, de nem védik teljesen a hálózatot. Más védekezési módokat is alkalmazni kell. Az egyik legalapvetőbb és legfontosabb módszer a biztonságos jelszavak használata.

[4.0](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[4.2](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Configure Secure Administrative Access](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Ugrás a tartalomra](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                         
*                                   

1. Secure Device Access
2. Configure Secure Administrative Access

# Konfigurálja a biztonságos adminisztrátori hozzáférést

4.2.1

## Jelszavak

A hálózati eszközök védelme érdekében fontos az erős jelszavak használata. Íme a követendő szabványos irányelvek:

* Használjon legalább nyolc karakter hosszúságú jelszót, lehetőleg 10 vagy több karaktert. A hosszabb jelszó biztonságosabb jelszó.
* Tegye bonyolulttá a jelszavakat. Ha megengedett, vegyen használjon nagy- és kisbetűket, számokat, szimbólumokat és szóközöket.
* Kerülje az ismétlésen alapuló jelszavakat, a szótárban elterjedt szavakat, betű- vagy számsorokat, felhasználóneveket, rokon- vagy háziállatneveket, életrajzi adatokat, például születési dátumokat, azonosítószámokat, ősök neveit vagy más könnyen azonosítható információkat.
* Szándékosan félreírt egy jelszót. Például Smith = Smyth = 5mYth vagy Security = 5ecur1ty.
* Gyakran változtassa meg a jelszavakat. Ha egy jelszó tudtán kívül kerül veszélybe, a fenyegetés szereplőjének lehetősége korlátozott a jelszó használatára.
* Ne írja le a jelszavakat, és ne hagyja jól látható helyen, például az asztalon vagy a monitoron.

A táblázatok példákat mutatnak be erős és gyenge jelszavakra.

| **Gyenge jelszó** | | **Miért Gyenge** |
| --- | --- | --- |
| titok | | Egyszerű szótári jelszó |
| Kovács | | Anyja leánykori neve |
| toyota | | Autó gyártmánya |
| bob1967 | | A felhasználó neve és születésnapja |
| Blueleaf23 | | Egyszerű szavak és számok |
| **Erős jelszó** | **Miért Erős** | |
| b67n42d39c | Alfanumerikus karaktereket kombinál | |
| 12^h u4@1p7 | Alfanumerikus karaktereket, szimbólumokat kombinál, és szóközt is tartalmaz | |

A Cisco útválasztókon a rendszer figyelmen kívül hagyja a bevezető szóközöket a jelszavaknál, de az első karakter utáni szóközöket nem. Ezért az erős jelszó létrehozásának egyik módja a szóköz használata, és sok szóból álló kifejezés létrehozása. Ezt nevezzük jelmondatnak. Egy jelmondatot gyakran könnyebb megjegyezni, mint egy egyszerű jelszót. Hosszabb és nehezebb kitalálni is.

**Jelszókezelők**   
Használjon jelszókezelőt az online internetes tevékenységeihez szükséges jelszavak védelméhez. A jelszavak biztonságának legjobb gyakorlatának tekinthető, a jelszókezelő automatikusan összetett jelszavakat generál Önnek, és automatikusan beírja azokat, amikor belép ezekre a webhelyekre. A funkció engedélyezéséhez csak egy elsődleges jelszót kell megadnia.

**Többtényezős hitelesítés**   
Ha lehetséges, használjon többtényezős hitelesítést. Ez azt jelenti, hogy a hitelesítéshez két vagy több független igazolási mód szükséges. Például jelszó megadásakor egy kódot is meg kell adnia, amelyet e-mailben vagy szöveges üzenetben küldenek Önnek.

4.2.2

## Jelszavak konfigurálása

Amikor először csatlakozik egy eszközhöz, felhasználói EXEC módban van. Ezt a módot a konzol biztosítja.

To secure user EXEC mode access, enter line console configuration mode using the **line console 0**A nulla az első (és a legtöbb esetben az egyetlen) konzolfelületet jelöli. Next, specify the user EXEC mode password using the **password** password command. Finally, enable user EXEC access using the **login** command.

Sw-Floor-1# **configure terminal**

Sw-Floor-1(config)# **line console 0**

Sw-Floor-1(config-line)# **password cisco**

Sw-Floor-1(config-line)# **login**

Sw-Floor-1(config-line)# **end**

Sw-Floor-1#

A konzolhoz való hozzáféréshez jelszóra lesz szükség a felhasználói EXEC mód eléréséhez.

Ahhoz, hogy rendszergazdai hozzáférést kapjon az összes IOS-parancshoz, beleértve az eszköz konfigurálását is, kiváltságos EXEC módú hozzáférést kell szereznie. Ez a legfontosabb hozzáférési mód, mert teljes hozzáférést biztosít az eszközhöz.

A privilegizált EXEC hozzáférés biztosításához használja a **engedélyezése** titkos jelszó globális konfig parancsot, a példában látható módon.

Sw-Floor-1# **configure terminal**

Sw-Floor-1(config)# **enable secret class**

Sw-Floor-1(config)# **exit**

Sw-Floor-1#

A virtuális terminálvonalak (VTY) lehetővé teszik az eszköz távoli elérését Telnet vagy SSH használatával. Sok Cisco switch legfeljebb 16 VTY-vonalat támogat, amelyek 0-tól 15-ig vannak számozva. A legtöbb útválasztó négy VTY-vonalat támogat, amelyek száma 0-tól 4-ig terjed. Ebben a példában egy hozzáférési réteg kapcsolót konfigurálunk.

A VTY vonalak biztosítása érdekében írja be a Line VTY módot a **VTY 0 15** Global Config paranccsal. Ezután adja meg a VTY jelszót a **jelszó** jelszó paranccsal. Végül engedélyezze a VTY hozzáférést a **Bejelentkezés** paranccsal.

Példa látható a VTY-vonalak kapcsolón való rögzítésére.

Sw-Floor-1# **configure terminal**

Sw-Floor-1(config)# **line vty 0 15**

Sw-Floor-1(config-line)# **password cisco**

Sw-Floor-1(config-line)# **login**

Sw-Floor-1(config-line)# **end**

Sw-Floor-1#

4.2.3

## Jelszavak titkosítása

Az erős jelszavak csak akkor hasznosak, ha titkosak. Számos lépéssel biztosítható, hogy a jelszavak titkosak maradjanak a Cisco útválasztón és kapcsolón, beleértve a következőket:

* Minden egyszerű szöveges jelszó titkosítása
* A jelszó minimális elfogadható hosszának beállítása
* A brutális erejű jelszókitaláló támadások megakadályozása
* Az inaktív, privilegizált EXEC mód elérésének letiltása meghatározott idő elteltével.

A startup-config és a running-config fájlok a legtöbb jelszót egyszerű szöveggel jelenítik meg. Ez biztonsági fenyegetést jelent, mert bárki felfedezheti a jelszavakat, ha hozzáfér ezekhez a fájlokhoz.

Az összes egyszerű jelszó titkosításához használja a **Szolgáltatás jelszó-titkosítási** globális konfigurációs parancsát, a példában látható módon.

Sw-Floor-1# **configure terminal**

Sw-Floor-1(config)# **service password-encryption**

Sw-Floor-1(config)#

A parancs gyenge titkosítást alkalmaz minden titkosítatlan jelszóra. Ez a titkosítás csak a konfigurációs fájlban lévő jelszavakra vonatkozik, a hálózaton keresztül küldött jelszavakra nem. Ennek a parancsnak az a célja, hogy megakadályozza, hogy illetéktelen személyek megtekintsék a konfigurációs fájlban lévő jelszavakat.

A **show running-config** paranccsal ellenőrizze, hogy a jelszavak most titkosítva vannak-e.

Sw-Floor-1(config)# **end**

Sw-Floor-1# **show running-config**

!

(Output omitted)

!

line con 0

password 7 094F471A1A0A

login

!

line vty 0 4

password 7 094F471A1A0A

login

line vty 5 15

password 7 094F471A1A0A

login

!

!

end

4.2.4

## További jelszóbiztonság

Amint a konfigurációs példa mutatja, a **szolgáltatásjelszó-titkosítás** globális konfigurációs parancsa megakadályozza, hogy illetéktelenek megtekintsék a konfigurációs fájlban található egyszerű szöveges jelszavakat. Ez a parancs titkosítja az összes egyszerű szöveges jelszót. Figyelje meg a példában, hogy a „ cisco ” kóddal lett titkosítva jelszó „ 094F471A1A0A ” .

Annak biztosítására, hogy minden konfigurált jelszó legalább meghatározott hosszúságú legyen, használja a **biztonsági jelszavak min-length** length parancsát globális konfigurációs módban.

A fenyegetés szereplői jelszófeltörő szoftvert használhatnak egy hálózati eszköz elleni brute force támadáshoz. Ez a támadás folyamatosan megpróbálja kitalálni az érvényes jelszavakat, amíg az nem működik. használja a **bejelentkezési blokk –** másodpercenkénti **kísérletek** száma **belül globális konfigurációs parancsot.** másodpercen Az ilyen típusú támadások megakadályozása érdekében

A hálózati adminisztrátorok elvonhatják a figyelmüket, és véletlenül nyitva hagyhatnak egy kiemelt EXEC módú munkamenetet a terminálon. Ez lehetővé teheti a belső fenyegetést okozó szereplők számára az eszközkonfiguráció módosítását vagy törlését. Alapértelmezés szerint a Cisco útválasztók 10 perc inaktivitás után kijelentkeznek az EXEC munkamenetből. Ezt a beállítást azonban csökkentheti az **exec-timeout** perc másodpercek sorkonfigurációs paranccsal. Ez a parancs online konzolon, kiegészítő és vty vonalakon alkalmazható.

Például a következő parancsok konfigurálják:

* Minden egyszerű szöveges jelszó titkosított.
* Az új konfigurált jelszavaknak legalább nyolc karakterből kell állniuk.
* Ha háromnál több sikertelen VTY-bejelentkezési kísérlet történik 60 másodpercen belül, akkor zárja le a VTY-vonalakat 120 másodpercre.
* Állítsa be az útválasztót úgy, hogy automatikusan megszakítsa a VTY-vonalon lévő inaktív felhasználót, ha a vonal 5 perc 30 másodpercig tétlen volt.

R1(config)# **service password-encryption**

R1(config)# **security passwords min-length 8**

R1(config)# **login block-for 120 attempts 3 within 60**

R1(config)# **line vty 0 4**

R1(config-line)# **password cisco123**

R1(config-line)# **exec-timeout 5 30**

R1(config-line)# **transport input ssh**

R1(config-line)# **end**

R1#

R1# **show running-config | section line vty**

line vty 0 4

password 7 094F471A1A0A

exec-timeout 5 30

login

transport input ssh

R1#

4.2.5

## Titkos jelszó-algoritmusok

Az MD5-kivonatok már nem tekinthetők biztonságosnak, mert a támadók rekonstruálhatják az érvényes tanúsítványokat. Ez lehetővé teszi a támadók számára, hogy bármilyen webhelyet meghamisítsanak. engedélyezése **titkos** jelszó Az ábrán látható parancs alapértelmezés szerint MD5 hash-t használ. Ezért most azt javasoljuk, hogy minden titkos jelszót 8-as vagy 9-es típusú jelszóval konfiguráljon. A 8-as és a 9-es típust a Cisco IOS 15.3(3)M-ben vezették be. A 8-as és a 9-es típus SHA titkosítást használ. Mivel a 9-es típus valamivel erősebb, mint a 8-as, a kurzus során ezt használjuk, amikor a Cisco IOS engedélyezi.

R1(config)# **enable secret cisco12345**

R1(config)# **do show run | include enable**

enable secret 5 $1$cam7$99EfzkvmJ5h1gEbryLVRy.

R1(config)# **enable secret ?**

0 Specifies an UNENCRYPTED password will follow

5 Specifies a MD5 HASHED secret will follow

8 Specifies a PBKDF2 HASHED secret will follow

9 Specifies a SCRYPT HASHED secret will follow

LINE The UNENCRYPTED (cleartext) 'enable' secret

level Set exec level password

R1(config)# **line con 0**

R1(config-line)# **password ?**

0 Specifies an UNENCRYPTED password will follow

7 Specifies a HIDDEN password will follow

LINE The UNENCRYPTED (cleartext) line password

R1(config-line)#

Az ábra azt mutatja, hogy a 9-es típusú titkosítás konfigurálása nem olyan egyszerű, mint amilyennek látszik. Nem adhatja meg egyszerűen az enable secret 9 értéket és a titkosítatlan jelszót. A parancs ezen formájának használatához be kell illesztenie a titkosított jelszót, amely másolható egy másik útválasztó konfigurációból.

R1(config)# **enable secret 9 cisco12345**

ERROR: The secret you entered is not a valid encrypted secret.

To enter an UNENCRYPTED secret, do not specify type 9 encryption.

When you properly enter an UNENCRYPTED secret, it will be encrypted.

R1(config)# **enable secret 9**

$9$HZWdzLHwhPtZ3U$D9OlUDSGvBy.m8Tf9vCGDJRcYy8zIMbyRJgtxgRkwzY

R1(config)#

Titkosítatlan jelszó megadásához használja az **enable algoritmus típusú** parancs szintaxisát:

Router(config)# **enable algorithm-type** { **md5** | **scrypt** | **sha256**  |  **secret**  } unencrypted password

|  |  |
| --- | --- |
| **Algoritmus kulcsszó** | **Leírás** |
| **md5** | 5. típus; az 5. üzenetkivonat-algoritmust (MD5) választja kivonatolási algoritmusként. |
| **forgatókönyv** | 9. típus; a titkosítást választja kivonatolási algoritmusnak. |
| **sha256** | 8. típus; Kivonatoló algoritmusként a 2. jelszóalapú kulcs-levezetési függvényt (PBKDF2) választja kivonatolási algoritmusként Secure Hash Algorithm, 256 bites (SHA-256). |

Az ábrán egy példa konfiguráció látható. Figyelje meg, hogy a futó konfiguráció most 9-es típusú engedélyezési titkos jelszót mutat.

R1(config)# **enable algorithm-type** ?

md5 Encode the password using the MD5 algorithm

scrypt Encode the password using the SCRYPT hashing algorithm

sha256 Encode the password using the PBKDF2 hashing algorithm

R1(config)# **enable algorithm-type scrypt** ?

secret Assign the privileged level secret (MAX of 25 characters)

R1(config)# **enable algorithm-type scrypt secret cisco12345**

R1(config)# **do show run | include enable**

enable secret 9 $9$Gyk9x3Ve4c0n5k$8.cR3yReBduzHymEyCOcErgPKW8MSKokRN

9KjEg4WQA

R1(config)#

A 8-as és 9-es típusú titkosítást a Cisco IOS 15.3(3)M-ben is bevezették a **titkos felhasználónév** parancshoz. Az enable secret parancshoz hasonlóan, ha egyszerűen megad egy felhasználót a username secret paranccsal, az alapértelmezett titkosítás az MD5 lesz. Használja a **username** name **algorithm-type** parancsot a 9-es típusú titkosítás megadásához. A szintaxist egy példa követi.

Router(config)#  **felhasználónév**  név  **algorithm-type**  {  **md5**  |  **scrypt**  |  **sha256**  |  **titkos**  } titkosítatlan jelszó

R1(config)# **username Bob secret cisco54321**

R1(config)# **do show run | include username**

username Bob privilege 15 secret 5 $1$lmBB$UjOC6JA4f1WgI3/La8wGz/

R1(config)#

R1(config)# **username Bob algorithm-type scrypt secret cisco54321**

R1(config)# **do show run | include username**

username Bob privilege 15 secret 9 $9$9FkS.zTuLs89pk$v5P2y.M6reR18lS

92moKHdFauk8joK0xHICXxGDuurs

R1(config)#

Visszafelé kompatibilitási okokból az **engedélyezési jelszó** , **a felhasználónév jelszava** és **a vonaljelszó** parancsok elérhetők a Cisco IOS rendszerben. Ezek a parancsok alapértelmezés szerint nem használnak titkosítást. A legjobb esetben is csak a 7-es típusú titkosítást tudják használni, ahogy az az ábrán is látható. Ezért ezeket a parancsokat ebben a kurzusban nem használjuk.

R1(config)# **enable password ?**

0 Specifies an UNENCRYPTED password will follow

7 Specifies a HIDDEN password will follow

LINE The UNENCRYPTED (cleartext) 'enable' password

level Set exec level password

R1(config)# **username Bob password ?**

0 Specifies an UNENCRYPTED password will follow

7 Specifies a HIDDEN password will follow

LINE The UNENCRYPTED (cleartext) user password

R1(config**)# line con 0**

R1(config-line)# **password ?**

0 Specifies an UNENCRYPTED password will follow

7 Specifies a HIDDEN password will follow

LINE The UNENCRYPTED (cleartext) line password

4.2.6

## Szintaxis ellenőrző - Biztonságos adminisztratív hozzáférés az R2 -en

Ebben a Syntax Checker tevékenységben biztonságos adminisztrátori hozzáférést konfigurálhat az R2-n.

Titkosítsa az összes jelszót

R2(config)# szolgáltatás jelszó-titkosítás

Állítsa a jelszó minimális hosszát 10 karakterre.

R2(config)# biztonsági jelszavak minimális hossza 10

Hozza létre a JR-ADMIN felhasználói fiókot a cisco12345 titkos jelszavával a SCRYPT kivonatoló algoritmus használatával.

R2(config)# felhasználónév JR-ADMIN algoritmus típusú titkosított titkosítás cisco12345

Hozza létre az ADMIN felhasználói fiókot a cisco54321 titkos jelszavával a SCRYPT kivonatoló algoritmus használatával.

R2(config)# felhasználónév ADMIN algoritmus típusú titkosított titkosítás cisco54321

Állítsa be a konzolsort a következő utasítások szerint:

* Állítsa be a végrehajtó időt 3 percre a konzolsorban.
* Állítsa be a konzolsort a helyi adatbázis használatára a hitelesítéshez.
* A konfiguráció után lépjen ki a vonalkonfigurációs módból.

R2(config)# vonalkonzol 0

R2(config-line)# exec-timeout 3 0

R2(config-line)# helyi bejelentkezés

R2(config-line)# kilépés

Állítsa be a vty sorokat a következő utasítások szerint:

* Állítsa a végrehajtási időt 3 percre a VTY vonalakon.
* Állítsa be a VTY-sorokat a helyi adatbázis használatára a hitelesítéshez.

R2(config)# sor vty 0 4

R2(config-line)# exec-timeout 3 0

R2(config-line)# helyi bejelentkezés

Visszatérés a kiemelt EXEC módba. Jelenítse meg a running-config fájlt, és szűrje le úgy, hogy csak a felhasználónévvel rendelkező sorokat tartalmazza a felhasználói fiók konfigurációjának ellenőrzéséhez.

R2(config-line)# vége

\*Mar 3 08:25:09.868: %SYS-5-CONFIG\_I: Konzolról konzolra konfigurálva

R2# show running-config | tartalmazza a felhasználónevet

felhasználónév JR-ADMIN titkos 9 $9$IznnuC6.5I0YmE$e8kvyaOBRuem54LJIhdAom8pQw3xGkGPeoEbNYU9BnY

felhasználónév ADMIN Secret 9 $9$.9hhYsuBDAaF3.$k5fhqvneSfOa.0ms89TjQX1ant9W3l09zLJjAHAERaU

R2#

Sikeresen biztosította a rendszergazdai hozzáférést az R2-n.

[4.1](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Secure the Edge Router](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[4.3](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Configure Enhanced Security for Virtual Logins](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Ugrás a tartalomra](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                             
*                                   

1. Secure Device Access
2. Configure Enhanced Security for Virtual Logins

# Konfigurálja a fokozott biztonságot a virtuális bejelentkezésekhez

4.3.1

## Javítsa a bejelentkezési folyamatot

A jelszavak és a helyi hitelesítés hozzárendelése nem akadályozza meg, hogy egy eszköz támadás célpontja legyen. A Cisco IOS bejelentkezési fejlesztései nagyobb biztonságot nyújtanak azáltal, hogy lassítják a támadásokat, például a szótár- és a DoS-támadásokat. Az észlelési profil engedélyezése lehetővé teszi a hálózati eszköz konfigurálását, hogy az ismételt sikertelen bejelentkezési kísérletekre a további csatlakozási kérelmek elutasításával (vagy a bejelentkezés blokkolásával) reagáljon. Ez a blokk egy ideig konfigurálható, amelyet csendes időszaknak neveznek. A hozzáférés-vezérlési listák (ACL) használhatók az ismert rendszeradminisztrátorok címeiről származó legitim kapcsolatok engedélyezésére.

A szalaghirdetések alapértelmezés szerint le vannak tiltva, és kifejezetten engedélyezni kell őket. Használja a **szalaghirdetés** globális konfigurációs mód parancsát a megfelelő üzenetek megadásához.

Router(config)#  **banner**  {  **motd**  |  **végrehajtó**  |  **bejelentkezés**  } határoló üzenet határoló

A szalaghirdetések jogi szempontból védik a szervezetet. A szalaghirdetésekben elhelyezendő megfelelő megfogalmazás kiválasztása fontos, és ezt jogi tanácsadónak kell átnéznie, mielőtt elhelyezné a hálózati útválasztókon. Soha ne használja az üdvözlő szót vagy más ismerős üdvözlést, amely félreérthető a hálózat használatára való felhívásként. A következő példa egy megfelelő bannerre.

This equipment is privately owned and access

is logged. Disconnect immediately if you are

not an authorized user. Violators will be

prosecuted to the fullest extent of the law.

User Access Verification:

Username:

4.3.2

## A bejelentkezésbővítési funkciók konfigurálása

Az alábbiakban bemutatott Cisco IOS bejelentkezési bővítési parancsok növelik a virtuális bejelentkezési kapcsolatok biztonságát.

Router(config)#  **bejelentkezési blokk –**  másodpercig  **próbálkozás**  tartó  **belül**  másodperceken   
Router(config)#  **login csendes módú access-class**  { acl-name | acl-szám }   
Router(config)#  **bejelentkezési késleltetés**  másodperc   
Router(config)#  **login on-success log**  [  **minden**  bejelentkezés ]   
Router(config)#  **bejelentkezési hibanapló**  [  **minden**  bejelentkezés ]

Az ábra egy példa konfigurációt mutat. A **login block-for** parancs úgy védekezhet a DoS támadások ellen, hogy letiltja a bejelentkezéseket meghatározott számú sikertelen bejelentkezési kísérlet után. A **csendes módú bejelentkezési** parancs egy ACL-re van leképezve, amely azonosítja az engedélyezett gazdagépeket. Ez biztosítja, hogy csak a feljogosított gazdagépek próbálhassanak bejelentkezni az útválasztóba. A **bejelentkezési késleltetés** parancs megadja, hogy a felhasználónak hány másodpercet kell várnia a sikertelen bejelentkezési kísérletek között. A **sikeres bejelentkezés** és **a sikertelen bejelentkezés** parancs naplózza a sikeres és sikertelen bejelentkezési kísérleteket.

Ezek a bejelentkezési fejlesztések nem vonatkoznak a konzolkapcsolatokra. A konzolcsatlakozások kezelésekor feltételezzük, hogy csak az arra jogosult személyek férhetnek hozzá fizikailag az eszközökhöz.

**Megjegyzés** : Ezek a bejelentkezési fejlesztések csak akkor engedélyezhetők, ha a helyi adatbázist használják a helyi és távoli hozzáférés hitelesítésére. Ha a vonalak csak jelszavas hitelesítésre vannak konfigurálva, akkor a továbbfejlesztett bejelentkezési szolgáltatások nincsenek engedélyezve.

R1(config)# **login block-for 15 attempts 5 within 60**

R1(config)# **ip access-list standard PERMIT-ADMIN**

R1(config-std-nacl)# **remark Permit only Administrative hosts**

R1(config-std-nacl)# **permit 192.168.10.10**

R1(config-std-nacl)# **permit 192.168.11.10**

R1(config-std-nacl)# **exit**

R1(config)# **login quiet-mode access-class PERMIT-ADMIN**

R1(config)# **login delay 10**

R1(config)# **login on-success log**

R1(config)# **login on-failure log**

R1(config)#

4.3.3

## Bejelentkezési fejlesztések engedélyezése

A Cisco IOS-eszközök DoS észlelésének elősegítéséhez használja a **login block-for** parancsot. Az összes többi bejelentkezésbővítő szolgáltatás le van tiltva, amíg a **login block-for** parancsot be nem állítják.

Pontosabban, a **login block-for** parancs figyeli a bejelentkezési eszköz tevékenységét, és két módban működik:

* **Normál mód** – Ezt óra üzemmódnak is nevezik. Az útválasztó folyamatosan számolja a sikertelen bejelentkezési kísérletek számát egy meghatározott időn belül.
* **Csendes üzemmód** – Ezt csendes időszaknak is nevezik. parancsban megadott ideig **Ha a sikertelen bejelentkezések száma meghaladja a beállított küszöbértéket, a rendszer megtagadja a Telnet, SSH és HTTP használatával végzett bejelentkezési kísérleteket a login block-for** .

Ha a csendes mód engedélyezve van, minden bejelentkezési kísérlet, beleértve az érvényes adminisztrátori hozzáférést, nem engedélyezett. Azonban a kritikus gazdagépek, például bizonyos adminisztratív gazdagépek mindenkori hozzáférésének biztosítása érdekében ez a viselkedés felülbírálható ACL-lel. Az ACL létrehozása és azonosítása a **Login Quiet módú hozzáférési osztály** paranccsal. Csendes módban csak az ACL-ben azonosított gazdagépek férhetnek hozzá az eszközhöz.

Az ábrán látható példa egy olyan konfigurációt mutat be, amely egy PERMIT-ADMIN nevű ACL-t használ. A PERMIT-ADMIN feltételeknek megfelelő gazdagépek mentesülnek a csendes mód alól.

R1(config)# **ip access-list standard PERMIT-ADMIN**

R1(config-std-nacl)# **remark Permit only Administrative hosts**

R1(config-std-nacl)# **permit 192.168.10.10**

R1(config-std-nacl)# **permit 192.168.11.10**

R1(config-std-nacl)# **exit**

R1(config)# **login quiet-mode access-class**  **PERMIT-ADMIN**

parancs végrehajtásakor a rendszer **A login block-for** automatikusan egy másodperces késleltetést hív meg a bejelentkezési kísérletek között. A támadó dolgát megnehezítendő, a bejelentkezési kísérletek közötti késleltetési idő növelhető a **bejelentkezési késleltetés** másodpercei paranccsal, az ábrán látható módon. A parancs egységes késleltetést vezet be az egymást követő bejelentkezési kísérletek között. A késleltetés minden bejelentkezési kísérletnél előfordul, beleértve a sikertelen vagy sikeres kísérleteket is. A példa három másodperces késleltetést konfigurál az egymást követő bejelentkezési kísérletek között.

Ez a parancs segít a szótári támadások mérséklésében. Ez egy opcionális parancs. Ha nincs beállítva, a **login block-for** parancs konfigurálása után egy 1 másodperces alapértelmezett késleltetés lép életbe.

A **bejelentkezési blokk** , **a csendes módú hozzáférési osztály** és **a bejelentkezési késleltetés** parancsok segítenek blokkolni a sikertelen bejelentkezési kísérleteket korlátozott ideig. Azonban nem tudják megakadályozni, hogy egy támadó újra próbálkozzon. Honnan tudhatja a rendszergazda, ha valaki jelszó kitalálásával próbál hozzáférni a hálózathoz?

R1(config)# **login delay**  **3**

4.3.4

## Sikertelen kísérletek naplózása

Három olyan parancs konfigurálható, amelyek segítségével a rendszergazda felismerheti a jelszótámadást, ahogy az az ábrán is látható. Mindegyik parancs lehetővé teszi az eszköz számára, hogy rendszernapló-üzeneteket generáljon a sikertelen vagy sikeres bejelentkezési kísérletek esetén.

Az első két parancs, **a sikeres bejelentkezési napló** és **a sikertelen bejelentkezési napló** rendszernapló-üzeneteket generál a sikeres és sikertelen bejelentkezési kísérletekhez. szintaxissal adható meg A naplózási üzenet létrehozása előtti bejelentkezési kísérletek száma az [ **minden** bejelentkezés ] , ahol az alapértelmezett bejelentkezési érték 1 kísérlet. Az érvényes tartomány 1 és 65 535 között van.

Router(config)#  **login on-success log**  [  **minden**  bejelentkezés ]   
Router(config)#  **bejelentkezési hibanapló**  [  **minden**  bejelentkezés ]

alternatívájaként **A bejelentkezési hiba napló** parancsának **a biztonsági hitelesítési hibaarány** parancs konfigurálható úgy, hogy a bejelentkezési hibaarány túllépése esetén naplóüzenetet generáljon.

Router(config)#  **biztonsági hitelesítési hibaarány küszöbérték-naplója**

Használja a **show login** ellenőrzéséhez a **parancsot a bejelentkezési blokk** parancsbeállításokhoz és az aktuális módhoz. Az ábrán az R1 úgy van konfigurálva, hogy 120 másodpercig blokkolja a bejelentkezési gazdagépeket, ha 60 másodpercen belül ötnél több bejelentkezési kérelem sikertelen. Az R1 azt is megerősíti, hogy az aktuális mód normális, és négy bejelentkezési hiba történt az elmúlt 55 másodpercben, mert öt másodperc van hátra a normál módból.

R1# **show login**

A login delay for 10 sec is applied.

Quiet-Mode access list PERMIT-ADMIN is applied.

Router enabled to watch for login Attacks.

If more than 5 login failures occur in 60 sec or less,

login will be disabled for 120 secs.

Router presently in Normal-Mode.

Current Watch Window

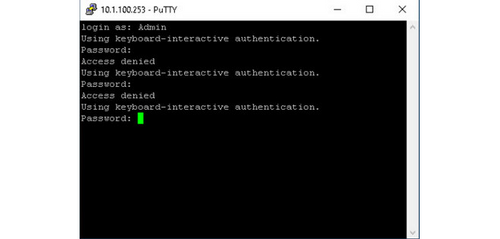
Time remaining: 5 seconds.

Login failures for current window: 4.

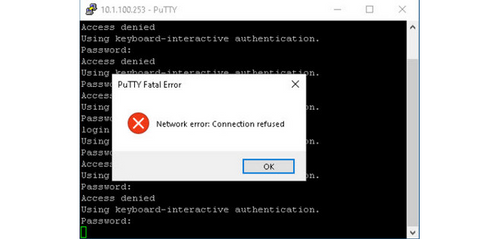
Total login failures:4.

A következő két ábra példákat mutat be arra, hogy mi történik a sikertelen kísérleti küszöb túllépése esetén.

### Sikertelen bejelentkezési kísérletek



### A sikertelen kísérleti küszöb túllépése



A következő parancskimenet megjeleníti a kapott állapotot a **show login** paranccsal. Figyelje meg, hogy most csendes módban van, és további 105 másodpercig csendes üzemmódban marad. Az R1 azt is azonosítja, hogy a PERMIT-ADMIN ACL tartalmazza azon gazdagépek listáját, amelyek csendes módban csatlakozhatnak.

R1#

\*Dec 10 15:38:54.455: %SEC\_LOGIN-1-QUIET\_MODE\_ON: Still timeleft for watching failures

is 12 secs, [user: admin] [Source: 10.10.10.10] [localport: 23] [Reason: Login

Authentication Failed - BadUser] [ACL: PERMIT-ADMIN] at 15:38:54 UTC Wed Dec 10 2008

R1# **show login**

A login delay of 3 seconds is applied.

Quiet-Mode access list PERMIT-ADMIN is applied.

Router enabled to watch for login Attacks.

If more than 5 login failures occur in 60 seconds or

less,logins will be disabled for 120 seconds.

Router presently in Quiet-Mode.

Will remain in Quiet-Mode for 105 seconds.

Restricted logins filtered by applied ACL PERMIT-ADMIN.

R1#

A **bejelentkezési hibák megjelenítése** parancs további információkat jelenít meg a sikertelen kísérletekkel kapcsolatban, például azt az IP-címet, amelyről a sikertelen bejelentkezési kísérletek származtak. megjelenítése parancs minta kimenetét mutatja **Az ábra a bejelentkezési hibák** .

R1# **show login failures**

Total failed logins: 22

Detailed information about last 50 failures

Username SourceIPAddr lPort Count TimeStamp

admin 1.1.2.1 23 5 15:38:54 UTC Wed Dec 10 2008

Admin 10.10.10.10 23 13 15:58:43 UTC Wed Dec 10 2008

admin 10.10.10.10 23 3 15:57:14 UTC Wed Dec 10 2008

cisco 10.10.10.10 23 1 15:57:21 UTC Wed Dec 10 2008

R1#

4.3.5

## Syntax Checker - Configure Enhanced Login Security on R2

Használja a Szintaxis-ellenőrzőt a fokozott bejelentkezési biztonság konfigurálásához az R2-n.

Az R2-n hozzon létre egy elnevezett szabványos hozzáférési listát:

* Permit the host at IP address 192.168.10.10.
* Use the name **PERMIT-ADMIN**.
* After configuration, return to global configuration mode.

R2(config)#ip access-list standard PERMIT-ADMIN

R2(config-std-nacl)#permit 192.168.10.10

R2(config-std-nacl)#exit

Enhance the login process using the following instructions:

* Disable login for 15 seconds if more than 5 failed logins are attempted within 60 seconds.
* The host specified in the PERMIT-ADMIN ACL should never be denied login access.
* Specify a login delay of 10 seconds between failed login attempts.
* Generate Syslog messages for successful login attempts.
* Generate Syslog messages for failed login attempts.
* After configuration, exit global configuration mode.

R2(config)#login block-for 15 attempts 5 within 60

R2(config)#login quiet-mode access-class PERMIT-ADMIN

R2(config)#login delay 10

R2(config)#login on-success log

R2(config)# bejelentkezési hibanapló

R2(config)# kilépés

R2#

\*november 30. 16:14:32.495: %SYS-5-CONFIG\_I: Konzolról konzolra konfigurálva

Jelenítse meg a bejelentkezési beállításokat.

R2# bejelentkezés megjelenítése

A rendszer 10 másodperces bejelentkezési késleltetést alkalmaz.

A csendes mód hozzáférési listája PERMIT-ADMIN van alkalmazva.

Minden sikeres bejelentkezés naplózásra kerül.

Minden sikertelen bejelentkezés naplózásra kerül.

A router engedélyezve van a bejelentkezési támadások figyelésére.

Ha 60 másodpercen belül 5-nél több bejelentkezési hiba történik,

a bejelentkezés 15 másodpercre le lesz tiltva.

A router jelenleg normál módban van.

Jelenlegi óraablak

Hátralévő idő: 15 másodperc.

Bejelentkezési hibák az aktuális ablakhoz: 0.

Összes bejelentkezési hiba: 0.

R2#

Sikeresen biztosította a fokozott bejelentkezési biztonságot az R2-n.

4.3.6

## Videó - Jelszavak és fokozott bejelentkezési biztonság konfigurálása

[4.2](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Configure Secure Administrative Access](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[4.4](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Configure SSH](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Ugrás a tartalomra](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                    
*                                   

1. Secure Device Access
2. Configure SSH

# SSH konfigurálása

4.4.1

## Videó - The Need for SSH

4.4.2

## SSH engedélyezése

A Telnet leegyszerűsíti a távoli eszközök elérését, de nem biztonságos. A Telnet-csomagokban lévő adatok titkosítás nélkül kerülnek továbbításra. Emiatt erősen ajánlott a Secure Shell (SSH) engedélyezése az eszközökön a biztonságos távoli hozzáférés érdekében.

A következő hat lépéssel beállítható egy Cisco-eszköz SSH támogatására:

**1. lépés: Konfiguráljon egyedi eszköz hosztnevet** . Az eszköznek az alapértelmezetttől eltérő egyedi gazdagépnévvel kell rendelkeznie.

**2. lépés: Konfigurálja az IP-tartománynevet** . globális konfigurációs mód parancsával **Állítsa be a hálózat IP tartománynevét az ip domain name** név . A példában az R1 útválasztó a span.com tartományban van konfigurálva. parancsban megadott bitértékkel együtt használják fel **Ezt az információt a titkosítási kulcs generálása rsa general-keys modulus** egy titkosítási kulcs létrehozásához.

**3. lépés: Hozzon létre egy kulcsot az SSH-forgalom titkosításához** . Az SSH titkosítja a forrás és a cél közötti forgalmat. Ehhez azonban létre kell hozni egy egyedi hitelesítési kulcsot a **crypto key generate rsa general-keys modulus** bits globális konfigurációs paranccsal . A modulus bitek határozzák meg a kulcs méretét, és 360 bittől 2048 bitig konfigurálhatók. Minél nagyobb a bitérték, annál biztonságosabb a kulcs. A nagyobb bitértékek esetében azonban hosszabb ideig tart az információ titkosítása és visszafejtése. A minimális ajánlott modulushossz 1024 bit.

**4. lépés: Ellenőrizze vagy hozzon létre egy helyi adatbázis-bejegyzést** . Hozzon létre egy helyi adatbázis felhasználónév bejegyzést a **felhasználónév** globális konfigurációs paranccsal. A példában a **titkos** paramétert úgy használjuk, hogy a jelszót MD5-tel titkosítjuk.

**5. lépés: Hitelesítés a helyi adatbázisban** . A **login local** line configuration paranccsal hitelesítse a vty vonalat a helyi adatbázissal szemben.

**6. lépés: Engedélyezze a vty bejövő SSH-munkameneteket** . Alapértelmezés szerint a beviteli munkamenet nem engedélyezett a vty sorokon. használatával több bemeneti protokollt is megadhat, beleértve a Telnetet és az SSH-t **Az {ssh | szállítási bemenet telnet}** parancsot.

Router# **configure terminal**

Router(config)# **hostname R1**

R1(config)# **ip domain name span.com**

R1(config)# **crypto key generate rsa general-keys modulus 1024**

The name for the keys will be: Rl.span.com % The key modulus size is 1024 bits

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled

R1(config)#

R1(config)# **username Bob secret cisco**

R1(config)# **line vty 0 4**

R1(config-line)# **login local**

R1(config-line)# **transport input ssh**

R1(config-line)# **exit**

R1(config)#

Az SSH ellenőrzéséhez és a generált kulcsok megjelenítéséhez használja a **show crypto key mypubkey rsa** parancsot privilegizált EXEC módban. Ha léteznek kulcspárok, akkor javasolt felülírni azokat a **crypto key zeroize rsa** paranccsal. Ha léteznek kulcspárok, javasoljuk, hogy távolítsa el őket a **crypto key zeroize rsa** paranccsal. A 2. ábra példát mutat az SSH titkosítási kulcsok ellenőrzésére és a régi kulcsok eltávolítására.

R1# **show crypto key mypubkey rsa**

% Key pair was generated at: 21:18:41 UTC Feb 16 2015

Key name: R1.span.com

Key type: RSA KEYS

Storage Device: not specified

Usage: General Purpose Key

Key is not exportable.

Key Data:

30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00CF35DB

A58A1BDB F7C7E600 F189C2F3 2EC6E584 D923EE5B 71841D98 B5472A03 D19CD620

ED125825 5A58412B B7F29234 DE2A1809 6C421AC3 07F298E6 80BE149D 2A262E13

74888DAF CAC8F187 B11111AF A413E76F 6C157CDF DFEF0D82 2961B58C BE1CAD21

176E82B9 6D81F893 06E66C93 94E1C508 887462F6 90AC63CE 5E169845 C1020301 0001

% Key pair was generated at: 21:18:42 UTC Feb 16 2015

Key name: R1.span.com.server

Key type: RSA KEYS

Temporary key

Usage: Encryption Key

Key is not exportable.

Key Data:

307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00AB914D 8172DFBE

DE57ACA9 7B844239 1F3B5942 3943AC0D F54E7746 3895CF54 606C3961 8A44FEB3

1A019F27 D9E71AAE FC73F423 A59CB8F5 50289272 3392CEBC 4C3CBD6D DB9233DE

9DDD9DAD 79D56165 4293AA62 FD1CBAB2 7AB859DC 2890C795 ED020301 0001

R1# **conf t**

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)# **crypto key zeroize rsa**

% All keys will be removed.

% All router certs issued using these keys will also be removed.

Do you really want to remove these keys? [yes/no]: **yes**

R1(config)#

4.4.3

## Növelje az SSH bejelentkezési biztonságot

Az opcionális SSH-parancs beállításainak ellenőrzéséhez használja a **show ip ssh** parancsot az ábrán látható módon. Módosíthatja az alapértelmezett SSH időtúllépési intervallumot és a hitelesítési kísérletek számát is. Az **ip ssh time-out** seconds globális konfigurációs mód paranccsal módosíthatja az alapértelmezett 120 másodperces időtúllépési intervallumot. Ez beállítja, hogy az SSH hány másodpercben tud hitelesíteni egy felhasználót. A hitelesítés után elindul egy EXEC munkamenet, és a vty számára konfigurált szabványos végrehajtási időtúllépés érvényesül.

Alapértelmezés szerint a bejelentkező felhasználó háromszor próbálkozik a helyes jelszó megadásával, mielőtt megszakadna. Eltérő számú egymást követő SSH-újrapróbálkozás konfigurálásához használja az **ip ssh authentication-retries** integer globális konfigurációs mód parancsot.

R1# **show ip ssh**

SSH Enabled - version 2.0

Authentication methods:publickey,keyboard-interactive,password

Authentication timeout: 120 secs; Authentication retries: 3

(output omitted)

R1# **conf t**

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)# **ip ssh time-out 60**

R1(config)# **ip ssh authentication-retries 2**

R1(config)# **^Z**

R1#

\*Feb 16 21:23:51.237: %SYS-5-CONFIG\_I: Configured from console by console

R1# **show ip ssh**

SSH Enabled - version 2.0

Authentication methods:publickey,keyboard-interactive,password

Authentication timeout: 60 secs; Authentication retries: 2

(output omitted)

4.4.4

## Szintaxis-ellenőrző – SSH engedélyezése R2-n

A Syntax Checker segítségével engedélyezze az SSH-t R2-n.

Configure the following:

* Assign the domain name span.com.
* Generate the general RSA keys using the crypto key generate rsa general-keys modulus 1024 command.

R2(config)#ip domain-name span.com

R2(config)#crypto key generate rsa general-keys modulus 1024

The name for the keys will be: R2.span.com

% The key modulus size is 1024 bits

% Generating 1024 bit RSA keys, keys will be non-exportable...

[OK] (elapsed time was 1 seconds)

\*Feb 27 16:41:37.363: %SSH-5-ENABLED: SSH 1.99 has been enabled

Create a local database entry for a user named Bob using algorithm-type SCRYPT hashing with a secret password of cisco54321.

R2(config)#username Bob algorithm-type scrypt secret cisco54321

Configure the vty lines 0-4 to use:

* The local database for login authentication.
* Enable SSH on the vty lines using the transport input ssh command.
* Exit from vty line configuration.

R2(config)#line vty 0 4

R2(config-line)#login local

R2(config-line)#transport input ssh

R2(config-line)#exit

Configure SSH:

* Enable SSH version 2.
* Set the number of authentication retries to 2.
* Set the SSH timeout period of 1 minute.
* Issue the end command to exit configuration mode.

R2(config)#ip ssh version 2

R2(config)#ip ssh authentication-retries 2

R2(config)#ip ssh time-out 60

R2(config)#end

Verify the SSH configuration using the show ip ssh command.

R2#show ip ssh

SH Enabled - version 2.0

Authentication methods:publickey,keyboard-interactive,password

Authentication timeout: 60 secs; Authentication retries: 2

Minimum expected Diffie Hellman key size : 1024 bits

IOS Keys in SECSH format(ssh-rsa, base64 encoded):

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQDNJV02ayJzPD/Ys/HKpy78XVR+QlnBaHaABMEOKGlj

oC4DQf8Z2XRJTzORPrYUfk1FFFVku+ejsy0G+3LoCAUgSdfpg1X4c8DbJhvA1PwPgxPVPklS5yWS+URk

ur4ijJl/cPksQpXQ8i26ye5SlLslV+3I+3TSI3MOEmJP++3vvw==

R2#

You successfully configured SSH on R2.

4.4.5

## Csatlakoztasson egy útválasztót egy SSH-képes útválasztóhoz

Az ügyfélkapcsolatok állapotának ellenőrzéséhez használja a **show ssh** parancsot. Az SSH-képes útválasztóhoz két különböző módon csatlakozhat.

Alapértelmezés szerint, ha az SSH engedélyezve van, a Cisco útválasztó SSH-kiszolgálóként vagy SSH-kliensként is működhet. Szerverként egy útválasztó fogadhat SSH-kliens kapcsolatokat. Kliensként az útválasztó SSH-n keresztül csatlakozhat egy másik SSH-képes útválasztóhoz, amely a következő három lépésben látható.

Az ábrán két soros kapcsolattal összekapcsolt router látható. Mindegyik router egy gigabites ethernet porton keresztül is csatlakozik a hálózathoz.

### Router-router SSH

R1 R2 G0/1 S/0/0/0 G0/1 S/0/0/0

192.168.2.101

A következő példákban az R1 rendszergazdája a **show ssh** parancsot használja az aktuális SSH-kapcsolatok ellenőrzésére. Ezután egy másik rendszergazda bejelentkezik az R1-be az R2-ből. Az R1 rendszergazdája újra ellenőrzi az aktuális SSH-kapcsolatokat.

R1# **show ssh**

%No SSHv2 server connections running.

%No SSHv1 server connections running.

R1#

R2# **ssh -l Bob 192.168.2.101**

Password:

R1>

R1# **show ssh**

Connection Version Mode Encryption Hmac State Username

0 2.0 IN aes128-cbc hmac-sha1 Session started Bob

0 2.0 OUT aes128-cbc hmac-sha1 Session started Bob

%No SSHv1 server connections running.

R1#

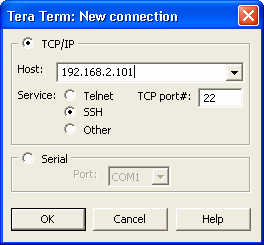
4.4.6

## Csatlakoztasson egy gazdagépet egy SSH-kompatibilis útválasztóhoz

Csatlakozzon egy gazdagépen futó SSH-kliens használatával az alábbi négy ábrán látható módon. Ilyen ügyfelek például a PuTTY, az OpenSSH és a TeraTerm.

A Cisco útválasztóhoz való csatlakozás folyamata a használt SSH-kliens alkalmazástól függően változik. Általában az SSH-kliens SSH-kapcsolatot kezdeményez az útválasztóval. Az útválasztó SSH szolgáltatása kéri a megfelelő felhasználónév és jelszó kombinációt. A bejelentkezés ellenőrzése után az útválasztó úgy kezelhető, mintha a rendszergazda szabványos Telnet munkamenetet használna.

### Host-router SSH



4.4.7

## Lab – Biztonságos adminisztrátori hozzáférés konfigurálása

Ebben a laborban a következő célokat kell teljesítenie:

* 1. rész: Alapvető eszközbeállítások konfigurálása
* 2. rész: Jelszavak konfigurálása és titkosítása az R1 és R3 útválasztókon
* 3. rész: Továbbfejlesztett felhasználói név-jelszó-biztonság konfigurálása az R1 és R3 routeren
* 4. rész: Az SSH-kiszolgáló konfigurálása az R1 és R3 útválasztókon

4.4.8

## Packet Tracer – Biztonságos jelszavak és SSH konfigurálása

A hálózati rendszergazda arra kérte, hogy készítse elő az RTA-t és az SW1-et a telepítéshez. Mielőtt a hálózathoz csatlakozhatnának, engedélyezni kell a biztonsági intézkedéseket.

[Konfigurálja a biztonságos jelszavakat és az SSH-t](https://contenthub.netacad.com/courses/netsec/_common/4.4.8-packet-tracer---configure-secure-passwords-and-ssh.pka)

4.4.9

## Lab - Hálózati eszközök konfigurálása SSH segítségével

Ebben a laborban a következő célokat kell teljesítenie:

* 1. rész: Alapvető eszközbeállítások konfigurálása
* Part 2: Configure the Router for SSH Access
* Part 3: Configure the Switch for SSH Access
* Part 4: SSH from the CLI on the Switch

[4.3](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Configure Enhanced Security for Virtual Logins](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[4.5](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Secure Device Access Summary](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Ugrás a tartalomra](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                                       

1. Secure Device Access
2. Secure Device Access Summary

# Biztonságos eszköz hozzáférés összefoglalója

4.5.1

## Mit tanultam ebben a modulban?

**Rögzítse az Edge Routert**   
Az útválasztók a támadások elsődleges célpontjai, mivel ezek az eszközök közlekedési rendőrökként működnek, amelyek a forgalmat a hálózatokba, hálózatokon kívülre és hálózatok között irányítják. A szélső útválasztó az utolsó útválasztó a belső hálózat és egy nem megbízható hálózat, például az internet között. Az útválasztó biztonságossá tétele elengedhetetlen. Ennek három megközelítése az egyetlen útválasztó megközelítés, a mélyreható védelem és a DMZ megközelítés. Az egyetlen útválasztó megközelítésben az összes biztonság ezen az útválasztón van konfigurálva. Ez gyakori a kisebb webhelyeken, például a SOHO webhelyeken. A mélyreható védelmi megközelítés biztonságosabb, mint az egyetlen útválasztó megközelítés. Több szintű biztonságot használ, mielőtt a forgalom belépne a védett LAN-ba. A védelemnek három elsődleges rétege van: a szélső útválasztó, a tűzfal és egy belső útválasztó, amely a védett LAN-hoz csatlakozik. Más biztonsági eszközök, például behatolásgátló rendszerek (IPS), webes biztonsági berendezések (proxyszerverek) és e-mail biztonsági eszközök (spamszűrés) is megvalósíthatók. A DMZ megközelítés tartalmaz egy köztes területet, amelyet gyakran demilitarizált zónának (DMZ) neveznek. A DMZ két router között állítható be, egy belső router csatlakozik a védett hálózathoz és egy külső router csatlakozik a nem védett hálózathoz. Alternatív megoldásként a DMZ egyszerűen egy további port lehet egyetlen útválasztón. A tűzfal elsődleges védelemként szolgál a DMZ-ben lévő összes eszköz számára. Az útválasztó biztonságának három megőrzendő területe a fizikai biztonság, az operációs rendszer biztonsága és a router keményítése. Az adminisztratív hozzáférés biztosítása annak megakadályozása érdekében, hogy illetéktelen személyek hozzáférjenek egy infrastrukturális eszközhöz, magában foglalja az eszközök hozzáférhetőségének korlátozását, az összes hozzáférés naplózását és elszámolását, a hozzáférés hitelesítését, a műveletek engedélyezését, a jogi értesítés bemutatását és az adatok titkosságának biztosítását. A router adminisztratív célokra elérhető helyileg vagy távolról. További óvintézkedéseket kell tenni a hálózat távoli elérésekor.

**Konfigurálja a biztonságos adminisztrátori hozzáférést**   
A hálózati eszközök védelme érdekében fontos az erős jelszavak használata. A követendő általános irányelvek a hosszabb jelszavak (10 vagy több karakter), az összetett jelszavak használata, a gyakori szótári szavak kerülése, a jelszavak gyakori megváltoztatása és a jelszavak bizalmas kezelése. A jelszavakat és a VTY-vonalakat védeni kell. Az összes egyszerű szöveges jelszó titkosításához használja a **service password-encryption** global config parancsot. A **show running-config** paranccsal ellenőrizze, hogy a jelszavak most titkosítva vannak-e. A **szolgáltatásjelszó-titkosítás** globális konfigurációs parancsa megakadályozza, hogy illetéktelen személyek egyszerű szöveges jelszavakat tekintsenek meg a konfigurációs fájlban. Az MD5-kivonatok már nem tekinthetők biztonságosnak, mert a támadók rekonstruálhatják az érvényes tanúsítványokat. Most azt javasoljuk, hogy az összes titkos jelszót 8-as vagy 9-es típusú jelszó használatával állítsa be.

**Konfigurálja a fokozott biztonságot a virtuális bejelentkezésekhez**   
A Cisco IOS bejelentkezési fejlesztései nagyobb biztonságot nyújtanak azáltal, hogy lassítják a támadásokat, például a szótár- és a DoS-támadásokat. Az észlelési profil engedélyezése lehetővé teszi a hálózati eszköz konfigurálását, hogy az ismételt sikertelen bejelentkezési kísérletekre a további csatlakozási kérelmek elutasításával (vagy a bejelentkezés blokkolásával) reagáljon. Ez a blokk egy ideig konfigurálható, amelyet csendes időszaknak neveznek. A hozzáférés-vezérlési listák (ACL) használhatók az ismert rendszeradminisztrátorok címeiről származó legitim csatlakozás engedélyezésére. A szalaghirdetések jogi szempontból védik a szervezetet. A Cisco IOS bejelentkezési továbbfejlesztési parancsai növelik a virtuális bejelentkezési kapcsolatok biztonságát. A **login block-for** parancs úgy védekezhet a DoS támadások ellen, hogy letiltja a bejelentkezéseket meghatározott számú sikertelen bejelentkezési kísérlet után. A **csendes módú bejelentkezési** parancs egy ACL-re van leképezve, amely azonosítja az engedélyezett gazdagépeket. Ez biztosítja, hogy csak a feljogosított gazdagépek próbálhassanak bejelentkezni az útválasztóba. A **bejelentkezési késleltetés** parancs megadja, hogy a felhasználónak hány másodpercet kell várnia a sikertelen bejelentkezési kísérletek között. A **login on-success** és **login on-failure** parancsok sikeres és sikertelen bejelentkezési kísérletek naplózása. A biztonság fokozása érdekében módosíthatja az alapértelmezett SSH időtúllépési időközt és a hitelesítési kísérletek számát is. Használja az i **p ssh time-out** seconds globális konfigurációs mód parancsot az alapértelmezett 120 másodperces időkorlát módosításához. Az SSH-képes útválasztóhoz két különböző módon csatlakozhat. Alapértelmezés szerint, ha az SSH engedélyezve van, a Cisco útválasztó SSH-kiszolgálóként vagy SSH-kliensként is működhet. Szerverként egy útválasztó fogadhat SSH-kliens kapcsolatokat. Kliensként egy útválasztó SSH-n keresztül csatlakozhat egy másik SSH-képes útválasztóhoz

**SSH konfigurálása**   
A Telnet leegyszerűsíti a távoli eszközök elérését, de nem biztonságos. A Telnet-csomagokban lévő adatok titkosítás nélkül kerülnek továbbításra. Emiatt erősen ajánlott a Secure Shell (SSH) engedélyezése az eszközökön a biztonságos távoli hozzáférés érdekében. A következő hat lépéssel konfigurálható egy Cisco eszköz SSH támogatására: egyedi eszköz hosztnév konfigurálása, IP tartománynév konfigurálása, kulcs generálása az SSH forgalom titkosításához, helyi adatbázis bejegyzés ellenőrzése vagy létrehozása, hitelesítés a helyi adatbázissal , és engedélyezze a vty bejövő SSH-munkameneteket.

4.5.2

## 4. modul – Biztonságos eszköz-hozzáférési kvíz

Az űrlap teteje

1. A vállalati hálózat mely pontján vizsgálják az internetről érkező csomagokat a hálózatba lépés előtt?

Az űrlap alja

Milyen három konfigurációs lépést kell végrehajtani az SSH-hozzáférés megvalósításához egy útválasztóhoz? (Válassz hármat.)

Mi a különbség a Telnet vagy az SSH használata között a hálózati eszközhöz való csatlakozáshoz felügyeleti célból?

Az útválasztó biztonságának mely három területét kell fenntartani, hogy egy szélső útválasztót biztosítsunk a hálózat peremén? (Válassz hármat.)

Mi a jó jelszójavaslat egy Cisco útválasztóhoz?

Mi a célja a szalaghirdetés használatának egy Cisco hálózati eszközön?

A hálózati rendszergazda SSH-n keresztül kapcsolatot létesít egy switch-hez. Milyen jellemző jellemzi egyedileg az SSH kapcsolatot?

Melyik parancs akadályozza meg, hogy az összes titkosítatlan jelszó egyszerű szövegként jelenjen meg a konfigurációs fájlban?

Egy hálózati rendszergazda adja ki a **bejelentkezési blokkot – 180 próbálkozásra 2 30-on belül** parancsot egy útválasztón. Melyik fenyegetést próbálja megakadályozni a hálózati rendszergazda?

Melyik ajánlott biztonsági gyakorlat akadályozza meg a támadókat abban, hogy jelszó-helyreállítást hajtsanak végre egy Cisco IOS útválasztón abból a célból, hogy hozzáférjenek a kiemelt EXEC módhoz?

Egy vállalat azt tervezi, hogy DMZ-t használ szervereihez, és aggódik a hálózati infrastruktúra biztonsága miatt. Melyik eszközt használja a hálózatbiztonsági csapat a szélső útválasztóhoz?

Milyen típusú hozzáférést biztosít a Cisco router vagy switch az **enable secret** paranccsal?

Milyen gyakori biztonsági feladatokat hajtanak végre egy hálózati infrastruktúra-eszköz rendszergazdai hozzáférésének biztosításakor?

[4.4](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Configure SSH](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[5.0](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Ugrás a tartalomra](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                             
*                                 

1. Assigning Administrative Roles
2. Introduction

# Bevezetés

5.0.1

## Miért vegyem ezt a modult?

Ebben a modulban megtudhatja, hogyan konfigurálhatja az adminisztrátori jogosultsági szinteket és a szerepkör alapú CLI-t. Ezek a lépések kritikusak a hálózati eszközökhöz való hozzáférés korlátozásához az adminisztratív felhasználók feladatköre alapján. Kezdjük el!

5.0.2

## Mit fogok tanulni ebben a modulban?

**Modul címe:** Adminisztratív szerepkörök hozzárendelése

**Modul célja** : Parancsengedély konfigurálása jogosultsági szintek és szerepalapú CLI segítségével.

| **téma címe** | **Téma Cél** |
| --- | --- |
| **Konfigurálja a jogosultsági szinteket** | A megfelelő parancsokkal állítsa be az adminisztrátori jogosultsági szinteket a parancsok elérhetőségének szabályozásához. |
| **Szerepkör-alapú CLI konfigurálása** | Használja a megfelelő parancsokat a szerepkör alapú CLI-hozzáférés konfigurálásához a parancsok elérhetőségének vezérléséhez. |

[4.5](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Secure Device Access Summary](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[5.1](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Configure Privilege Levels](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Ugrás a tartalomra](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                               
*                                 

1. Assigning Administrative Roles
2. Configure Privilege Levels

# Konfigurálja a jogosultsági szinteket

5.1.1

## A parancsok elérhetőségének korlátozása

A nagy szervezetek számos különféle munkakört látnak el egy IT-részlegen belül. Nem kell minden munkafunkciónak ugyanolyan szintű hozzáféréssel rendelkeznie az infrastruktúra-eszközökhöz. A Cisco IOS szoftvernek két módja van az infrastruktúra-hozzáférés biztosítására: a jogosultsági szint és a szerepkör alapú CLI. Mindkét módszer segít meghatározni, hogy ki csatlakozhat az eszközhöz, és mit tehet az illető személy vele. A szerepkör alapú CLI hozzáférés nagyobb részletességet és vezérlést biztosít.

Alapértelmezés szerint a Cisco IOS szoftver CLI két szintű hozzáféréssel rendelkezik a parancsokhoz:

* **Felhasználói EXEC mód (1. jogosultsági szint)** – Ez biztosítja a legalacsonyabb EXEC módú felhasználói jogosultságokat, és csak a Router> promptban elérhető felhasználói szintű parancsokat engedélyezi.
* **Privileged EXEC mód (15-ös jogosultsági szint)** – Ez magában foglalja az összes engedélyezési szintű parancsot a Router# promptban.

Összesen 16 kiváltsági szint van, az alábbiak szerint. Minél magasabb a jogosultsági szint, annál több router-hozzáféréssel rendelkezik a felhasználó. Az alacsonyabb kiváltsági szinteken elérhető parancsok is magasabb szinten végrehajthatók.

* **0. szint:** előre meghatározva a felhasználói szintű hozzáférési jogosultságokra. Ritkán használt, de öt parancsot tartalmaz: **letiltja** , **engedélyezze** , **kilépjen** , **segítsen** és **kijelentkezzen** .
* **1. szint** : Az alapértelmezett bejelentkezési szint az útválasztó Router > parancsával . A felhasználó nem hajthat végre módosításokat és nem tekintheti meg a futó konfigurációs fájlt.
* **2-14. szintek** : Testreszabható a felhasználói szintű jogosultságokhoz. Az alacsonyabb szintek parancsai egy másik magasabb szintre, vagy a magasabb szintek parancsai alacsonyabb szintre helyezhetők át.
* **15. szint** : Fenntartva az Enable Mode Privilégiumokhoz ( **Engedélyezés** parancs). A felhasználók módosíthatják a konfigurációkat és megtekinthetik a konfigurációs fájlokat.

Parancsok egyéni jogosultsági szinthez rendeléséhez használja az **alább látható privilégium** globális konfigurációs mód parancsot.

Router(config)#  **privilege**  mode {  **level**  level |  **reset**  } parancsot

| **Parancs** | **Leírás** |
| --- | --- |
| mód | Meghatározza a konfigurációs módot. Használja a **kiváltságot ?** parancsot az útválasztón elérhető útválasztó konfigurációs módok teljes listájának megtekintéséhez. |
| **szint** | (Opcionális) Lehetővé teszi a jogosultsági szint beállítását egy megadott paranccsal. |
| szint | (Nem kötelező) A parancshoz társított jogosultsági szint. Legfeljebb 16 jogosultsági szintet adhat meg a 0 és 15 közötti számok használatával. |
| **Visszaállítás** | (Opcionális) Visszaállítja a parancs jogosultsági szintjét. |
| parancs | (Opcionális) A jogosultsági szint visszaállításához használandó argumentum. |

5.1.2

## Jogosultsági szintek konfigurálása és hozzárendelése

A jogosultsági szint meghatározott parancsokkal történő konfigurálásához használja a **privilege exec level** level **[** parancs **]** . A példa három különböző jogosultsági szintre mutat példákat.

* parancshoz elérhető összes parancshoz **Az 5. jogosultsági szint hozzáfér az előre meghatározott 1. szinthez és a ping** .
* A 10. jogosultsági szint hozzáfér az 5. szinthez elérhető összes parancshoz, valamint az **újratöltés** parancshoz.
* A 15. kiváltsági szint előre meghatározott, és nem kell kifejezetten konfigurálni. Ez a jogosultsági szint hozzáfér az összes parancshoz, beleértve a konfiguráció megtekintését és módosítását.

R1#  **konf t**   
R1(config)# !5. szint és SUPPORT felhasználói konfiguráció   
R1(config)#  **jogosultság végrehajtani 5. szintű ping**   
R1(config)#  **engedélyezi az algoritmus típusú titkosítási titkosítást, 5. szint cisco5**   
R1(config)#  **felhasználónév SUPPORT privilégium 5 algoritmus típusú titkosított titkosítás cisco5**   
R1(config)# !10. szint és JR-ADMIN felhasználói konfiguráció   
R1(config)#  **10. szintű végrehajtási jogosultság újratöltés**   
R1(config)#  **algoritmus-típusú titkosítási titkosítás engedélyezése 10. szint cisco10**   
R1(config)#  **felhasználónév JR-ADMIN privilégium 10 algoritmus típusú titkosított titkosítás cisco10**   
R1(config)# !15. szint és ADMIN felhasználói konfiguráció   
R1(config)#  **engedélyezése algoritmus-típusú titkosítási titkosítási szint 15 cisco123**   
R1(config)#  **felhasználónév ADMIN-jogosultság 15 algoritmus típusú titkosított titkosítás cisco123**

Kétféle módon lehet jelszavakat rendelni a különböző jogosultsági szintekhez:

* Egy adott jogosultsági szinttel rendelkező felhasználóhoz használja a **felhasználónév** globális **jogosultsági** szint **titkos** jelszó konfigurációs mód parancsát
* A jogosultsági szinthez használja a **titkos szintű** jelszó engedélyezése globális konfigurációs mód parancsot

**Megjegyzés** : Mind a **titkos felhasználónév** , mind az **engedélyezési titkos** parancs a 9-es típusú titkosításhoz van konfigurálva.

A **username** paranccsal rendelhet hozzá jogosultsági szintet egy adott felhasználóhoz. Az **enable secret** paranccsal jogosultsági szintet rendelni egy adott EXEC mód jelszavához. Például a SUPPORT felhasználóhoz 5-ös jogosultsági szint van hozzárendelve a cisco5 jelszóval. Azonban, ahogy az alábbi példában látható, bármely felhasználó hozzáférhet az 5-ös jogosultsági szinthez, ha tudja, hogy az engedélyezési titkos jelszó a cisco5. A példa azt is bemutatja, hogy az 5. jogosultsági szint nem tudja újratölteni az útválasztót.

R1> **enable 5**

Password: <cisco5>

R1**# show privilege** Current privilege level is 5

R1# **ping 10.1.1.1**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R1# **reload**

Translating "reload"

% Bad IP address or host name

Translating "reload"

% Unknown command or computer name, or unable to find computer address

R1#

Az alábbi példában a felhasználó engedélyezi a 10-es jogosultsági szintet, amely hozzáfér az **újratöltési** parancshoz. A 10-es jogosultsági szintű felhasználók azonban nem tekinthetik meg a futó konfigurációt.

R1# **enable 10**

Password: <cisco10>

R1# **show privilege**

Current privilege level is 10

R1# **ping 10.1.1.1**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R1# **reload**

System configuration has been modified. Save? [yes/no]: ^C

R1# **show running-config**

^

% Invalid input detected at '^' marker.

R1#

A következő példában a felhasználó engedélyezi a 15. jogosultsági szintet, amely teljes hozzáféréssel rendelkezik a konfiguráció megtekintéséhez és módosításához, beleértve a futó konfiguráció megtekintését is.

R1# **enable 15**

Password:

R1# **show privilege**

Current privilege level is 15

R1# **show running-config** Building configuration...

Current configuration : 1979 bytes

!

! Last configuration change at 15:30:07 UTC Tue Feb 17 2015

!

version 15.4

R1#

5.1.3

## A jogosultsági szintek korlátai

A jogosultsági szintek használatának megvannak a maga korlátai:

* Az útválasztón nincs hozzáférés-vezérlés bizonyos interfészekhez, portokhoz, logikai interfészekhez és bővítőhelyekhez.
* Az alacsonyabb jogosultsági szinteken elérhető parancsok mindig végrehajthatók magasabb szinteken.
* A kifejezetten magasabb jogosultsági szintre beállított parancsok nem érhetők el alacsonyabb jogosultságokkal rendelkező felhasználók számára.
* Ha egy parancshoz több kulcsszót rendel hozzá, akkor hozzáférhet az összes olyan parancshoz, amely ezeket a kulcsszavakat használja. Például **az ip route megjelenítéséhez** parancs elérését **való hozzáférés engedélyezése lehetővé teszi a felhasználó számára az összes show** és **show ip** .

**Megjegyzés** : Ha a rendszergazdának olyan felhasználói fiókot kell létrehoznia, amely a legtöbb, de nem az összes parancshoz hozzáfér, a privilege exec utasításokat be kell állítani minden olyan parancshoz, amelyet 15-nél alacsonyabb jogosultsági szinten kell végrehajtani.

5.1.4

## Szintaxis-ellenőrző – A jogosultsági szintek konfigurálása az R2-n

Ezzel a szintaktikai ellenőrzővel konfigurálhatja az R2 jogosultsági szintjeit.

5. jogosultsági szint konfigurálása:

* A privilege exec level paranccsal biztosíthatja a hozzáférést a **ping** parancshoz.
* 5. szintű titkos jelszavát **Engedélyezze a cisco5** kivonattal van titkosítva **, amely az algoritmus típusú scrypt** .
* Hozzon létre egy helyi adatbázis-bejegyzést egy **Support** nevű felhasználó számára 5-ös jogosultsági szinttel, titkosítsa a jelszót 9-es típusú ( **algoritmus-típusú scrypt** ) kivonattal, és állítsa be a jelszót **cisco5-** re .

R2(config)# jogosultság végrehajtani 5. szintű ping

R2(config)# engedélyezi az algoritmus típusú titkosítási titkosítást, 5. szint cisco5

R2(config)#username Support privilege 5 algorithm-type scrypt secret cisco5

Configure privilege level 10:

* Használja a **privilege exec level** parancsot, hogy hozzáférjen az **újratöltési** parancshoz.
* 10. szintű titkos jelszavát, **Engedélyezze a cisco10** kivonattal van titkosítva **amely az algoritmus típusú scrypt** .
* nevű felhasználó számára **Hozzon létre egy helyi adatbázis-bejegyzést egy Jr-Admin** 10-es jogosultsági szinttel, titkosítsa a jelszót 9-es típusú ( **algoritmus-típusú scrypt** ) kivonattal, és állítsa be a jelszót **cisco10-** re .

R2(config)# jogosultság végrehajtani 10. szintű újratöltés

R2(config)# engedélyezi az algoritmus típusú titkosítási titkosítást 10. szint cisco10

R2(config)# felhasználónév Jr-Admin privilege 10 algoritmus típusú titkosított titkosítás cisco10

Configure privilege level 15:

* Enable a level 15 secret password of **cisco123** that is encrypted with the **algorithm-type scrypt** hashing.
* Create a local database entry for a user named **Admin** with a privilege level of 15, encrypt the password with a type 9 (**algorithm-type scrypt**) hashing, and set the password to **cisco123**.
* Exit configuration mode.

R2(config)#enable algorithm-type scrypt secret level 15 cisco123

R2(config)#username Admin privilege 15 algorithm-type scrypt secret cisco123

R2(config)#exit

R2#

You successfully configured privilege levels on R2.

[5.0](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[5.2](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Configure Role-Based CLI](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Ugrás a tartalomra](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                     
*                                 

1. Assigning Administrative Roles
2. Configure Role-Based CLI

# Szerepkör-alapú CLI konfigurálása

5.2.1

## Szerepkör alapú CLI hozzáférés

Annak érdekében, hogy a jogosultsági szinteknél nagyobb rugalmasságot biztosítson, a Cisco bevezette a szerepalapú CLI hozzáférési szolgáltatást a Cisco IOS 12.3(11)T kiadásában. Ez a funkció finomabb, részletesebb hozzáférést biztosít azáltal, hogy szabályozza, hogy mely parancsok érhetők el az adott szerepkörök számára. A szerepkör alapú CLI hozzáférés lehetővé teszi a hálózati rendszergazdának, hogy különböző nézeteket hozzon létre az útválasztó konfigurációiról a különböző felhasználók számára. Minden nézet meghatározza azokat a CLI-parancsokat, amelyekhez minden felhasználó hozzáférhet.

**Biztonság**

A szerepkör alapú CLI-hozzáférés növeli az eszköz biztonságát azáltal, hogy meghatározza a CLI-parancsok készletét, amelyekhez egy adott felhasználó hozzáférhet. Ezenkívül az adminisztrátorok szabályozhatják a felhasználói hozzáférést az útválasztó adott portjaihoz, logikai interfészeihez és bővítőhelyeihez. Ez megakadályozza, hogy a felhasználó véletlenül vagy szándékosan módosítson egy konfigurációt, vagy olyan információkat gyűjtsön, amelyekhez nem szabad hozzáférnie.

**Elérhetőség**

A szerepkör alapú CLI-hozzáférés megakadályozza, hogy illetéktelen személyek véletlenül végrehajtsák a CLI-parancsokat, és minimalizálja az állásidőt.

**Működési hatékonyság**

A felhasználók csak azokra a portokra és CLI-kre vonatkozó CLI-parancsokat látják, amelyekhez hozzáféréssel rendelkeznek. Ezért az útválasztó kevésbé bonyolultnak tűnik, és a parancsok könnyebben azonosíthatók az eszköz súgó funkciójának használatakor.

5.2.2

## Szerep alapú nézetek

A szerepkör alapú CLI háromféle nézetet biztosít, amelyek meghatározzák, hogy mely parancsok állnak rendelkezésre:

**Gyökérnézet**

A rendszer bármely nézetének beállításához a rendszergazdának gyökérnézetben kell lennie. A gyökérnézet ugyanazokkal a hozzáférési jogosultságokkal rendelkezik, mint a 15. szintű jogosultságokkal rendelkező felhasználó. A gyökérnézet azonban nem azonos a 15. szintű felhasználóval. Csak a gyökérnézet felhasználója konfigurálhat új nézetet, és adhat hozzá vagy távolíthat el parancsokat a meglévő nézetekből.

**CLI nézet**

Egy adott parancskészlet egy CLI nézetbe köthető. A jogosultsági szintekkel ellentétben a CLI-nézetnek nincs parancshierarchiája, és nincsenek magasabb vagy alacsonyabb nézetei. Minden nézethez hozzá kell rendelni az adott nézethez tartozó összes parancsot. Egy nézet nem örököl parancsokat egyetlen másik nézettől sem. Ezenkívül ugyanazok a parancsok több nézetben is használhatók.

**Szupernézet**

A szupernézet egy vagy több CLI nézetből áll. Az adminisztrátorok meghatározhatják, hogy mely parancsok fogadhatók el, és mely konfigurációs információk láthatók. A felülnézetek lehetővé teszik a hálózati rendszergazdák számára, hogy egyszerre több CLI-nézetet rendeljenek hozzá a felhasználókhoz és a felhasználók csoportjaihoz, ahelyett, hogy felhasználónként egyetlen CLI-nézetet kellene hozzárendelnie az adott CLI-nézethez társított összes parancshoz.

A szupervízióknak számos sajátos jellemzője van:

* Egyetlen CLI-nézet több szupernézeten belül is megosztható.
* A parancsok nem konfigurálhatók felügyeleti nézethez. A rendszergazdának parancsokat kell hozzáadnia a CLI nézethez, és hozzá kell adnia azt a CLI nézetet a felügyeleti nézethez.
* A felügyeleti nézetbe bejelentkezett felhasználók hozzáférhetnek minden olyan parancshoz, amely a felügyeleti nézet részét képező bármely CLI-nézethez be van állítva.
* Minden nézethez tartozik egy jelszó, amellyel a szupernézetek között vagy a CLI nézetből a szupernézetre válthat.
* Egy szupernézet törlése nem törli a társított CLI-nézeteket. A CLI nézetek továbbra is elérhetők egy másik felügyeleti nézethez való hozzárendeléshez.

Kattintson a Lejátszás gombra az animációban a nézetek magyarázatához.

Az animáció bemutatja, hogyan jönnek létre a szerepalapú nézetek. Csak a gyökérnézet hozhat létre más nézeteket. A nézetek parancsokat tartalmaznak, és ugyanaz a parancs több nézetben is megjelenhet. A felülnézetek nézeteket tartalmaznak, parancsokat nem. Egy nézet több szupernézethez is használható.

### Szerep alapú nézetek bemutatása

Gyökérnézet

A szupernézetek nézeteket tartalmaznak, parancsokat nem. Két szupernézet használhatja ugyanazt a nézetet.   
Például az 1. és a 2. szupernézetben is elhelyezhető a 4. CLI nézet.

A nézetek parancsokat tartalmaznak. Egy parancs több nézetben is megjelenhet.

A Nézetek és Felülnézetek meghatározásához gyökérnézet szükséges.

**6**

**5**

**Nézet 4**

**Nézet 4**

**3**

**2**

**1**

**Szupernézet 1**

**Szupernézet 2**

**1**

**2**

**3**

**Nézet 4**

**5**

**6**

**CLI nézetek**

5.2.3

## Szerepkör-alapú nézetek konfigurálása

Mielőtt a rendszergazda létrehozhatna egy nézetet, az AAA-t engedélyezni kell az **aaa new-model** paranccsal. A nézetek konfigurálásához és szerkesztéséhez az adminisztrátornak gyökérnézetként kell bejelentkeznie a **nézet engedélyezése** privilegizált EXEC paranccsal. A **nézet engedélyezése a root** parancs is használható. Amikor a rendszer kéri, írja be az **engedélyezési titkos** jelszót.

Egy adott nézet létrehozása és kezelése öt lépésből áll.

**1. lépés:** Engedélyezze az AAA-t az **aaa new-model** globális konfigurációs mód paranccsal. Lépjen ki és lépjen be a gyökérnézetbe az **engedélyezése nézet** paranccsal.

| **Paraméter** | **Leírás** |
| --- | --- |
| **Kilátás** | Ez a paraméter gyökérnézetbe lép, ha nincs megadva nézetnév, ami lehetővé teszi az adminisztrátor számára a CLI-nézetek konfigurálását. A nézet paraméter szükséges a CLI nézet konfigurálásához. |
| view-name | (Opcionális) Ez a paraméter egy megadott CLI nézetbe lép be vagy ki. Ezzel a paraméterrel válthatunk egyik CLI nézetről egy másik CLI nézetre. |

Router#  **engedélyezése**  [  **view**  [ view-name ]]

**2. lépés:** Hozzon létre egy nézetet az **elemző nézet** view-name globális konfigurációs mód paranccsal. Ez lehetővé teszi a nézet konfigurációs módot. A gyökérnézetet nem számítva összesen legfeljebb 15 nézet lehetséges.

Router(config)#  **elemző nézet**  nézetnév

**3. lépés:** Rendeljen titkos jelszót a nézethez a **titkos** jelszó nézet konfigurációs mód parancsával.

Ez beállít egy jelszót a nézethez való hozzáférés védelmére. A jelszót a nézet létrehozása után azonnal létre kell hozni, ellenkező esetben hibaüzenet jelenik meg.

Router(config-view)#  **titkos**  jelszó

**4. lépés:** Rendeljen parancsokat a kiválasztott nézethez a **parancsok** értelmező mód parancsával nézet konfigurációs módban.

Router(config-view)#  **parancsok**  parser-mode {  **include**  |  **tartalmazza-kizárólag**  |  **kizár**  } [  **összes**  ] [  **interfész**  interfésznév | parancs ]

| **Parancsok** | **Leírás** |
| --- | --- |
| **parancsokat** | Parancsokat vagy interfészeket ad a nézethez. |
| elemző mód | Az üzemmód, amelyben a megadott parancs létezik; például EXEC mód. |
| **tartalmazza** | Parancsot vagy felületet ad a nézethez, és lehetővé teszi, hogy ugyanazt a parancsot vagy felületet adják hozzá más nézetekhez. |
| **tartalmazza-kizárólagos** | Parancsot vagy interfészt ad a nézethez, és kizárja, hogy ugyanazt a parancsot vagy felületet adják hozzá az összes többi nézethez. |
| **kizárni** | Kizár egy parancsot vagy interfészt a nézetből. |
| **minden** | "Járó karakter", amely lehetővé teszi, hogy egy megadott konfigurációs módban minden parancs, amely ugyanazzal a kulcsszóval kezdődik, vagy egy adott interfész minden alinterfésze, a nézet része legyen. |
| **interfész**  interfésznév | A nézethez hozzáadott felület. |
| parancs | A nézethez hozzáadott parancs. |

**5. lépés:** parancs beírásával **Lépjen ki a nézet konfigurációs módból az exit** .

Az alábbi példa három nézet konfigurációját mutatja be. Vegye figyelembe a példában, hogy a **titkos** parancs csak az MD5 titkosítást támogatja (5-ös típus). Azt is vegye figyelembe, hogy amikor a jelszó hozzárendelése előtt parancsot adtak hozzá egy nézethez, hiba történt.

R1(config)# **aaa new-model**

R1(config)# **parser view SHOWVIEW**

R1(config-view)#  **secret ?**

0 Specifies an UNENCRYPTED password will follow

5 Specifies an ENCRYPTED secret will follow

LINE The UNENCRYPTED (cleartext) view secret string

R1(config-view)# **secret cisco**

R1(config-view)# **commands exec include show**

R1(config-view)# **exit**

R1(config)#  **parser view VERIFYVIEW**

R1(config-view)#  **commands exec include ping**

% Password not set for the view VERIFYVIEW

R1(config-view)#  **secret cisco5**

R1(config-view)#  **commands exec include ping**

R1(config-view)# **exit**

R1(config)# **parser view REBOOTVIEW**

R1(config-view)# **secret cisco10**

R1(config-view)# **commands exec include reload**

R1(config-view)# **exit**

R1(config)#

Ellenőrizze a nézet konfigurációját a **show running-config** paranccsal.

R1# **show running-config**

<output omitted>

parser view SHOWVIEW

secret 5 $1$GL2J$8njLecwTaLAc0UuWo1/Fv0

commands exec include show

!

parser view VERIFYVIEW

secret 5 $1$d08J$1zOYSI4WainGxkn0Hu7lP1

commands exec include ping

!

parser view REBOOTVIEW

secret 5 $1$L7lZ$1Jtn5IhP43fVE7SVoF1pt.

commands exec include reload

!

5.2.4

## Szintaxis-ellenőrző – Nézetek konfigurálása az R2-n

Ezzel a szintaktikai ellenőrzővel három nézetet állíthat be különböző jogosultságokkal az R2-n.

Enable AAA.

R2(config)#aaa new-model

Configure the first view:

* Create a view called **SHOWVIEW**.
* Assign the view the password **cisco**.
* Allow the view to use all EXEC commands that begin with **show**.
* After configuration, return to global configuration mode.

R2(config)#parser view SHOWVIEW

R2(config-view)#secret cisco

R2(config-view)#commands exec include show

R2(config-view)#exit

Configure the second view.

* Create a view called **VERIFYVIEW**.
* Assign the view the password **cisco5**.
* Allow the view to use the **ping** command.
* After configuration, return to global configuration mode.

R2(config)#

R2(config)#parser view VERIFYVIEW

R2(config-view)#secret cisco5

R2(config-view)#commands exec include ping

R2(config-view)#exit

Configure the third view.

* Create a view called **REBOOTVIEW**.
* Assign the view the password **cisco10**.
* Allow the view to use the **reload** command.
* After configuration, return directly to privileged EXEC mode.

R2(config)#parser view REBOOTVIEW

R2(config-view)#secret cisco10

R2(config-view)#commands exec include reload

R2(config-view)#end

Verify the configured views using the **show running-config | section parser** command.

R2#show running-config | section parser

parser view SHOWVIEW

secret 5 $1$4c8S$8ayWlp1brumavcCek7OUz.

commands exec include show

parser view VERIFYVIEW

secret 5 $1$mV.n$Wl99F.nQQQvuP7QiEzE.40

commands exec include ping

parser view REBOOTVIEW

secret 5 $1$BBYq$L6prAiM.wrcuGbst/9JY51

commands exec include reload

R2#

You successfully configured three views with different privileges on R2.

5.2.5

## Lab – Adminisztrátori szerepkörök konfigurálása

Ebben a laborban a következő célokat kell teljesítenie:

* 1. rész: Az alapvető eszközbeállítások konfigurálása.
* 2. rész: Adminisztrátori szerepkörök konfigurálása.

5.2.6

## Szerepkör alapú CLI felügyeletek konfigurálása

A felülnézet beállításának lépései lényegében megegyeznek a CLI-nézet konfigurálásával, azzal a különbséggel, hogy a **view** view-name paranccsal parancsokat rendelhet hozzá a nézethez. A felügyeleti nézet beállításához a rendszergazdának gyökérnézetben kell lennie. A gyökérnézet használatának megerősítéséhez használja a **nézet engedélyezése** vagy **a gyökérnézet engedélyezése** parancsot. Amikor a rendszer kéri, írja be a **titkos** jelszót.

Négy lépésből áll a szupernézet létrehozása és kezelése.

További információért kattintson az alábbi lépésekre.

Hozzon létre egy nézetet az **elemző nézet** view-name **superview** paranccsal, és lépjen be a felügyeleti nézet konfigurációs módba. Ha hozzáfűzi a **szupernézet** kulcsszót az elemző nézethez, létrejön egy szupernézet, és belép a konfigurációs módba.

Router(config)#  **elemző nézet**  nézetnév  **felügyelet**

Rendeljen titkos jelszót a nézethez a **titkos** jelszó paranccsal. Ez beállít egy jelszót a felügyeleti nézethez való hozzáférés védelmére. A jelszót a nézet létrehozása után azonnal létre kell hozni; ellenkező esetben hibaüzenet jelenik meg.

Router(config-view)#  **titkos**  jelszó

Rendeljen hozzá egy meglévő nézetet a **view** view-name paranccsal nézet konfigurációs módban. Ez hozzáad egy CLI-nézetet a felügyelethez. Több nézet is hozzáadható. A nézetek megoszthatók a szupernézetek között.

Router(config-view)#  **view**  view-name

parancs beírásával kilép a SuperView konfigurációs mód kilépése **A kilépési** .

Egy szupernézethez több nézet is hozzárendelhető, és a nézetek megoszthatók a szupernézetek között. A példa három felügyeleti nézet konfigurálását mutatja be: USER, SUPPORT és JR-ADMIN.

R1(config)# **parser view USER superview**

R1(config-view)# **secret cisco**

R1(config-view)# **view SHOWVIEW**

R1(config-view)# **exit**

R1(config)#

R1(config)# **parser view SUPPORT superview**

R1(config-view)# **secret cisco1**

R1(config-view)# **view** **SHOWVIE**

% Invalid view name SHOWVIE

R1(config-view)# **view** **SHOWVIEW**

R1(config-view)# **view** **VERIFYVIEW**

R1(config-view)# **exit**

R1(config)#

R1(config)# **parser view JR-ADMIN superview**

R1(config-view)# **secret cisco2**

R1(config-view)# **view SHOWVIEW**

R1(config-view)# **view VERIFYVIEW**

R1(config-view)# **view REBOOTVIEW**

R1(config-view)# **exit**

R1(config)#

Az alábbi példa a futó konfigurációban konfigurált szupernézeteket jeleníti meg.

A meglévő nézetek eléréséhez adja meg a **nézet engedélyezése** nézetnév parancsot felhasználói módban, és adja meg az egyéni nézethez rendelt jelszót. Ugyanezzel a paranccsal válthat egyik nézetről a másikra.

R1# **show running-config**

<output omitted>

!

parser view SUPPORT superview

secret 5 $1$Vp1O$BBB1N68Z2ekr/aLHledts.

view SHOWVIEW

view VERIFYVIEW

!

parser view USER superview

secret 5 $1$E4k5$ukHyfYP7dHOC48N8pxm4s/

view SHOWVIEW

!

parser view JR-ADMIN superview

secret 5 $1$8kx2$rbAe/ji220OmQ1yw.568g0

view SHOWVIEW

view VERIFYVIEW

view REBOOTVIEW

!

5.2.7

## Szintaxis-ellenőrző – Szupernézetek konfigurálása az R2-n

Ezzel a szintaxis-ellenőrzővel három szupernézetet állíthat be az R2-n.

Configure the first superview.

* Create a superview called **USER**.
* Assign the superview the password **cisco**.
* Assign it the **SHOWVIEW** view.
* After configuration, return to global configuration view.

R2(config)#parser view USER superview

R2(config-view)#secret cisco

R2(config-view)#view SHOWVIEW

R2(config-view)#exit

Configure the second superview.

* Create a superview called **SUPPORT**.
* Assign the superview the password **cisco1**.
* Assign it the **SHOWVIEW** view.
* Assign it the **VERIFYVIEW** view.
* After configuration, return to global configuration mode.

R2(config)#parser view SUPPORT superview

R2(config-view)#secret cisco1

R2(config-view)#view SHOWVIEW

R2(config-view)#view VERIFYVIEW

R2(config-view)#exit

Configure the third superview.

* Create a superview called **JR-ADMIN**.
* Assign the superview the password **cisco2**.
* Assign it the **SHOWVIEW** view.
* Assign it the **VERIFYVIEW** view.
* Assign it the **REBOOTVIEW** view.
* After configuration, return to privilege EXEC mode.

R2(config)#parser view JR-ADMIN superview

R2(config-view)#secret cisco2

R2(config-view)#view SHOWVIEW

R2(config-view)#view VERIFYVIEW

R2(config-view)#view REBOOTVIEW

R2(config-view)#end

Verify the configured superviews using the **show running-config | section superview** command.

R2#show running-config | section superview

elemző nézet USER nézet

titkos 5 $1$PkVE$fWQNcCofjNnSNO5T5fR9b0

SHOWVIEW megtekintése

elemző nézet SUPPORT szupernézet

titkos 5 $1$AJdD$KXsrFpyr8nsoZaoyJcZGz.

SHOWVIEW megtekintése

VERIFYVIEW megtekintése

elemző nézet JR-ADMIN nézet

titkos 5 $1$jDUK$v1DodSqackdof/Dbg11eJ1

SHOWVIEW megtekintése

VERIFYVIEW megtekintése

REBOOTVIEW megtekintése

R2#

Sikeresen konfiguráltad a szupernézeteket az R2-n.

5.2.8

## Ellenőrizze a szerepkör-alapú CLI-nézeteket

Nézet ellenőrzéséhez használja a **nézet engedélyezése** parancsot. Írja be a nézet nevét az ellenőrzéshez, és adja meg a jelszót a nézetbe való bejelentkezéshez. A kérdőjel ( **?** ) paranccsal ellenőrizze, hogy a nézetben elérhető parancsok helyesek-e.

A példa engedélyezi a FELHASZNÁLÓI nézetet, és felsorolja a nézetben elérhető parancsokat.

R1# **enable view USER**

Password: <cisco1>

R1# **?**

Exec commands:

<0-0>/<0-4> Enter card slot/sublot number

do-exec Mode-independent "do-exec" prefix support

enable Turn on privileged commands

exit Exit from the EXEC

show Show running system information

R1# **show ?** banner Display banner information

flash0: display information about flash0: file system

flash1: display information about flash1: file system

flash: display information about flash: file system

parser Display parser information

usbflash0: display information about usbflash0: file system

Az alábbi példa engedélyezi a SUPPORT nézetet, és felsorolja a nézetben elérhető parancsokat.

R1# **enable view SUPPORT**

Password: <cisco1>

R1# **?**

Exec commands:

<0-0>/<0-4> Enter card slot/sublot number

do-exec Mode-independent "do-exec" prefix support

enable Turn on privileged commands

exit Exit from the EXEC

ping Send echo messages

show Show running system information

R1#

Ez a példa engedélyezi a JR-ADMIN nézetet, és felsorolja a nézetben elérhető parancsokat.

R1# **enable view JR-ADMIN**

Password:

R1# **?**

Exec commands:

<0-0>/<0-4> Enter card slot/sublot number

do-exec Mode-independent "do-exec" prefix support

enable Turn on privileged commands

exit Exit from the EXEC

ping Send echo messages

reload Halt and perform a cold restart

show Show running system information

R1#

Ha nem ad meg nézetet a **nézet engedélyezése** parancshoz, ahogy az itt látható, akkor root felhasználóként jelentkezhet be. A gyökérnézetben használja a **show parser view all** parancsot az összes nézet összegzésének megtekintéséhez. Figyelje meg, hogy a csillag hogyan azonosítja a szupernézeteket.

R1# **show parser view**

Current view is 'JR-ADMIN'

R1# **enable view**

Password:

R1# **show parser view**

Current view is 'root'

R1# **show parser view all**

Views/SuperViews Present in System:

SHOWVIEW

VERIFYVIEW

REBOOTVIEW

USER \*

SUPPORT \*

JR-ADMIN \*

-------(\*) represent superview-------

R1#

[5.1](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Configure Privilege Levels](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[5.3](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Assigning Administrative Roles Summary](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                                                

1. Adminisztrátori szerepkörök hozzárendelése
2. Adminisztratív szerepkörök hozzárendelése – Összefoglaló

# Adminisztratív szerepkörök hozzárendelése – Összefoglaló

5.3.1

## Mit tanultam ebben a modulban?

**Konfigurálja a jogosultsági szinteket**   
A Cisco IOS szoftvernek két módja van az infrastruktúra-hozzáférés biztosítására: a jogosultsági szint és a szerepkör alapú CLI. Alapértelmezés szerint a Cisco IOS szoftver CLI két szintű hozzáféréssel rendelkezik a parancsokhoz: Felhasználói EXEC mód (1. jogosultsági szint) és Privileged EXEC mód (15. jogosultsági szint). Összesen 16 jogosultsági szint van. Minél magasabb a jogosultsági szint, annál több router-hozzáféréssel rendelkezik a felhasználó. A jogosultsági szint meghatározott parancsokkal történő konfigurálásához használja a **privilege exec level** level [ parancs ] . A **username** paranccsal rendelhet hozzá jogosultsági szintet egy adott felhasználóhoz. Az **enable secret** paranccsal jogosultsági szintet rendelni egy adott EXEC mód jelszavához. A jogosultsági szintek használatának megvannak a maga korlátai:

* Az útválasztón nincs hozzáférés-vezérlés bizonyos interfészekhez, portokhoz, logikai interfészekhez és bővítőhelyekhez.
* Az alacsonyabb jogosultsági szinteken elérhető parancsok mindig végrehajthatók magasabb szinteken.
* A kifejezetten magasabb jogosultsági szintre beállított parancsok nem érhetők el alacsonyabb jogosultságokkal rendelkező felhasználók számára.
* Ha egy parancshoz több kulcsszót rendel hozzá, akkor hozzáférhet az összes olyan parancshoz, amely ezeket a kulcsszavakat használja. Például **az ip route megjelenítéséhez** parancs elérését **való hozzáférés engedélyezése lehetővé teszi a felhasználó számára az összes show** és **show ip** .

**Szerepkör-alapú CLI konfigurálása**   
Annak érdekében, hogy a jogosultsági szinteknél nagyobb rugalmasságot biztosítson, a Cisco bevezette a szerepalapú CLI hozzáférési szolgáltatást a Cisco IOS 12.3(11)T kiadásában. A szerepkör alapú CLI hozzáférés lehetővé teszi a hálózati rendszergazdának, hogy különböző nézeteket hozzon létre az útválasztó konfigurációiról a különböző felhasználók számára. A szerepkör alapú parancssori felület háromféle nézetet biztosít, amelyek meghatározzák, hogy mely parancsok állnak rendelkezésre. A gyökérnézet ugyanazokkal a hozzáférési jogosultságokkal rendelkezik, mint a 15. szintű jogosultságokkal rendelkező felhasználó. A gyökérnézet azonban nem azonos a 15. szintű felhasználóval. Csak a gyökérnézet felhasználója konfigurálhat új nézetet, és adhat hozzá vagy távolíthat el parancsokat a meglévő nézetekből. Egy adott parancskészlet egy CLI nézetbe köthető. A jogosultsági szintekkel ellentétben a CLI-nézetnek nincs parancshierarchiája, és nincsenek magasabb vagy alacsonyabb nézetei. Egy nézet nem örököl parancsokat egyetlen másik nézettől sem. A szupernézet egy vagy több CLI nézetből áll. Az adminisztrátorok meghatározhatják, hogy mely parancsok fogadhatók el, és mely konfigurációs információk láthatók. A felügyeleti nézetekkel a hálózati rendszergazda egyszerre több CLI-nézetet rendelhet hozzá a felhasználókhoz és a felhasználók csoportjaihoz, ahelyett, hogy felhasználónként egyetlen CLI-nézetet kellene hozzárendelnie az adott CLI-nézethez társított összes parancshoz. Mielőtt a rendszergazda létrehozhatna egy nézetet, az AAA-t engedélyezni kell a következővel **aaa new-model** parancs. A nézetek konfigurálásához és szerkesztéséhez az adminisztrátornak gyökérnézetként kell bejelentkeznie a **nézet engedélyezése** privilegizált EXEC paranccsal. A **nézet engedélyezése a root** parancs is használható. Amikor a rendszer kéri, írja be az **engedélyezési titkos** jelszót. Egy adott nézet létrehozása és kezelése öt lépésből áll. A felülnézet beállításának lépései lényegében megegyeznek a CLI-nézet konfigurálásával, azzal a különbséggel, hogy a **view** view-name paranccsal parancsokat rendelhet hozzá a nézethez.

5.3.2

## 5. modul – Adminisztratív szerepkörök kiosztása kvíz

Az űrlap teteje

1. Mit kell tenni, mielőtt bármilyen szerepkör - alapú CLI-nézetet létre lehetne hozni?

Az űrlap alja

Melyik három utasítás írja le a parancsjogosultság hozzárendelésére vonatkozó jogosultsági szintek korlátait? (Válassz hármat.)

Melyik két útválasztó parancsot adhatja ki a felhasználó, ha 0-s jogosultsági szintet kap? (Válassz kettőt.)

Mit **globális konfigurációs mód parancs 5. szintje** jelez az alábbi **engedélyezési titkos** ?

Router(config)# **enable secret level 5 csc5io**

megvalósításával Milyen három hálózati fejlesztés érhető el a Cisco IOS szoftver szerepkör alapú CLI hozzáférési funkciójának ? (Válassz hármat.)

A hálózati rendszergazda új nézetet szeretne létrehozni, hogy a felhasználó csak bizonyos konfigurációs parancsokhoz férhessen hozzá. Szerepkör - alapú CLI-ben melyik nézetet kell használnia a rendszergazdának az új nézet létrehozásához?

A hálózati rendszergazda beírja az R1 # **enable view adminview** parancsot . Mi ennek a parancsnak a célja?

Az egyéni jogosultsági szintek melyik tartománya konfigurálható a Cisco útválasztókon?

Melyik parancs helyezi át a **show interface** parancsot a 10-es jogosultsági szintre?

Mi a Cisco útválasztókon létrehozott felhasználói fiókok alapértelmezett jogosultsági szintje?

An administrator assigned a level of router access to the user ADMIN using the commands below.

Router(config)# **privilege exec level 14 show ip route**  
Router(config)# **enable algorithm-type scrypt secret level 14 cisco-level-10**  
Router(config)# **username ADMIN privilege 14 algorithm-type scrypt secret cisco-level-10**

Which two actions are permitted to the user ADMIN? (Choose two.)​

[5.2](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Szerepkör-alapú CLI konfigurálása](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[6.0](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Bevezetés](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                                  
*                               

1. Device Monitoring and Management
2. Introduction

# Bevezetés

6.0.1

## Miért vegyem ezt a modult?

A kiberbűnözők minden lehetséges sebezhetőséget megpróbálnak kihasználni. Például a kiberbűnözők:

* Nyerjen hozzáférést az alapvető peremútválasztóhoz, és törölje az IOS- és az Indítási konfigurációs fájlokat (együttesen rendszerindító fájlokként ismert).
* Hozzáférés egy használaton kívüli szolgáltatáshoz, amely még mindig működik az eszközön.
* Szúrjon be hamis útválasztási információkat egy konvergált OSPF hálózatba.

A modul első része enyhítő technikákat kínál az ilyen támadások ellen.

Honnan tudhatod, ha a hálózatod támadás alatt áll? A modul második része a hálózatfelügyeletet tárgyalja, és a hálózatfigyelő eszközök segítenek a hálózat védelmében és védelmében.

6.0.2

## Mit fogok tanulni ebben a modulban?

**Module Title:** Device Monitoring and Management

**A modul célja** : A hálózati eszközök biztonságos kezelésének és felügyeletének megvalósítása.

| **téma címe** | **Téma Cél** |
| --- | --- |
| **Biztonságos Cisco IOS kép- és konfigurációs fájlok** | Magyarázza el, hogyan használják a Cisco IOS rugalmas konfigurációs funkcióját és a biztonságos másolatot a Cisco IOS kép- és konfigurációs fájlok biztonságához. |
| **Zárolja le az útválasztót az AutoSecure használatával** | Használja az AutoseCure megfelelő parancsát az iOS-alapú útválasztók biztonságának lehetővé tételéhez. |
| **Routing Protocol Authentication** | Használja a megfelelő parancsot az útválasztási protokoll hitelesítésének konfigurálásához. |
| **Biztonságos menedzsment és jelentéskészítés** | Hasonlítsa össze a sávon belüli és a sávon kívüli felügyeleti hozzáférést. |
| **Hálózati biztonság Syslog használatával** | Magyarázza el, hogyan konfigurálható a syslog a rendszeresemények naplózására. |
| **NTP konfiguráció** | Állítsa be az NTP-t, hogy lehetővé tegye a pontos időbélyegzést az összes eszköz között. |
| **SNMP konfiguráció** | Konfigurálja az SNMP-t a rendszerállapot figyeléséhez. |

[5.3](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Assigning Administrative Roles Summary](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[6.1](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Secure Cisco IOS Image and Configuration Files](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                                      
*                               

1. Device Monitoring and Management
2. Secure Cisco IOS Image and Configuration Files

# Biztonságos Cisco IOS kép- és konfigurációs fájlok

6.1.1

## Cisco IOS rugalmas konfigurációs szolgáltatás

A Cisco IOS rugalmas konfigurációs funkciója gyorsabb helyreállítást tesz lehetővé, ha valaki rosszindulatúan vagy véletlenül újraformázza a flash memóriát, vagy törli az indítási konfigurációs fájlt a nem felejtő véletlen hozzáférésű memóriában (NVRAM). A szolgáltatás az útválasztó IOS képfájljának biztonságos munkapéldányát és a futó konfigurációs fájl másolatát tartja karban. Ezeket a biztonságos fájlokat a felhasználó nem tudja eltávolítani, és elsődleges rendszerindítónak nevezik őket.

Íme néhány tény a Cisco IOS rugalmas konfigurációjáról:

* Az elsődleges rendszerindítókészlet konfigurációs fájlja annak a futó konfigurációnak a másolata, amely az útválasztóban volt, amikor a szolgáltatást először engedélyezték.
* A funkció a legkisebb működő fájlkészletet biztosítja a tartós tárhely megőrzése érdekében.
* Nincs szükség extra helyre az elsődleges Cisco IOS képfájl biztonságossá tételéhez. The feature automatically detects image or configuration version mismatch.
* Csak a helyi tárhelyet használják a fájlok védelmére, így kiküszöbölhető a skálázhatósággal kapcsolatos karbantartási kihívások több kép és konfiguráció TFTP-kiszolgálókon történő tárolása miatt.
* A funkció csak konzolmunkameneten keresztül tiltható le.

**Megjegyzés** : A funkció csak a régebbi útválasztókon érhető el, amelyek támogatják a PCMCIA Advanced Technology Attachment (ATA) flash interfészt. Az újabb útválasztók, például az ISR 4000 nem támogatják ezt a funkciót.

6.1.2

## Engedélyezze az IOS Image Resilience funkciót

Az IOS-kép és a futó konfigurációs fájl védelmére szolgáló parancsok a példában láthatók. Az IOS lemezkép biztonságossá tételéhez és a Cisco IOS lemezkép rugalmasságának engedélyezéséhez használja a **biztonságos boot-image** globális konfigurációs mód parancsot. Ha először engedélyezve van, a Cisco IOS -kép rögzítve van, és a naplóbejegyzés generálódik. A Cisco IOS kép ellenálló képessége csak egy konzolos munkameneten keresztül le lehet tiltani a **parancs NO** formájának felhasználásával. This command functions properly only when the system is configured to run an image from a flash drive with an ATA interface. Ezenkívül a futó lemezképet be kell tölteni a perzisztens tárhelyről, hogy elsődlegesként védve legyen. Images that are loaded from a remote location, such as a TFTP server, cannot be secured.

Az útválasztó konfigurációjának pillanatképének elkészítéséhez, és biztonságosan archiválja azt állandó tárolóban, használja a **Secure Boot-Config** Global Configuration Mode parancsot, az ábrán látható módon. A konzolon naplóüzenet jelenik meg, amelyben értesíti a felhasználót, hogy a konfigurációs ellenálló képesség aktiválódik. A konfigurációs archívum rejtett, és nem tekinthető meg vagy távolítható el közvetlenül a parancssori felületből. paranccsal ismételten felhasználhatja **A Secure Boot-Config** a konfigurációs archívum újabb verzióra történő frissítéséhez az új konfigurációs parancsok kiadása után.

parancs kimenetében **dir** A titkosított fájlok nem jelennek meg a CLI-ből kiadott . Ennek az az oka, hogy a Cisco IOS fájlrendszer megakadályozza a biztonságos fájlok listázását. The running image and running configuration archives are not visible in the **dir** command output. Use the **show secure bootset** command to verify the existence of the archive, as shown in the figure.

R1(config)# **secure boot-image**

R1(config)#

Sep 22 12:47:10.183: %IOS\_RESILIENCE-5-IMAGE\_RESIL\_ACTIVE: Successfully secured running image

R1(config)#

R1(config)# **secure boot-config**

R1(config)#

Sep 22 12:47:18.259: %IOS\_RESILIENCE-5-CONFIG\_RESIL\_ACTIVE: Successfully secured config archive [flash0:.runcfg-20200922-124717.ar]

R1(config)#

R1(config)# **exit**

R1#

Sep 22 12:47:22.783: %SYS-5-CONFIG\_I: Configured from console by console

R1# **show secure bootset**

IOS resilience router id FTX1449AJBJ

IOS image resilience version 15.4 activated at 12:47:09 UTC Tue Sep 22 2020

Secure archive flash0:c2900-universalk9-mz.SPA.154-3.M.bin type is image (elf) []

file size is 103727964 bytes, run size is 103907016 bytes

Runnable image, entry point 0x81000000, run from ram

IOS configuration resilience version 15.4 activated at 12:47:18 UTC Tue Sep 22 2020

Secure archive flash0:.runcfg-20200922-124717.ar type is config

configuration archive size 1683 bytes

R1#

6.1.3

## Az elsődleges rendszerindítási kép

Helyezze vissza az elsődleges csizmát egy biztonságos archívumból, miután az útválasztót megsértették, amint azt a következő lépések és a példa mutatja:

**1. lépés** . Reload the router using the **reload** command. Ha szükséges, adja ki a szünetsorozatot a ROM monitor (ROMmon) módba lépéshez.

**2. lépés** . ROMmon módban írja be a **dir** parancsot a biztonságos rendszerindító fájlt tartalmazó eszköz tartalmának listázásához.

**3. lépés** . Indítsa el az útválasztót a biztonságos rendszerindító képfájllal a **boot** paranccsal, majd a flash memória helyével (pl. flash0), egy kettősponttal és a 2. lépésben talált fájlnévvel.

**4. lépés** . Enter global configuration mode and restore the secure configuration to a filename of your choice using the **secure boot-config restore** command followed by the flash memory location (eg flash0), a colon, and a filename of your choice. In the figure, the filename rescue-cfg is used.

**5. lépés** . Lépjen ki a globális konfigurációs módból, és adja ki a **copy** parancsot a mentett konfigurációs fájl futó konfigurációba másolásához.

Router# **reload**

<Issue Break sequence, if necessary>

rommon 1 > **dir flash0:**

program load complete, entry point: 0x80803000, size: 0x1b340

Directory of flash0:

4 103727964 -rw- c2900-universalk9-mz.SPA.154-3.M.bin

rommon 2 > **boot flash0:c2900-universalk9-mz.SPA.154-3.M.bin** <Router reboots with specified image>

Router> **enable**

Router# **conf t**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# **secure boot-config restore flash0:rescue-cfg**

ios resilience:configuration successfully restored as flash0:rescue-cfg

Router(config)# **end**

Router# **copy flash0:rescue-cfg running-config**

Destination filename [running-config]?

%IOS image resilience is already active

%IOS configuration resilience is already active

2182 bytes copied in 0.248 secs (8798 bytes/sec)

R1#

6.1.4

## Biztonságos másolás konfigurálása

A Secure Copy Protocol (SCP) funkciót használják ezeknek a fájloknak a távoli másolására. SCP provides a secure and authenticated method for copying router configuration or router image files to a remote location.

Az SCP támaszkodik:

* SSH a biztonságos kommunikáció érdekében
* AAA hitelesítést és engedélyezést biztosít

**Megjegyzés** : Az AAA konfigurációról részletesebben egy későbbi fejezetben lesz szó.

A következő lépésekkel konfigurálhatja az útválasztót a kiszolgálóoldali SCP-hez helyi AAA-val:

**1. lépés** . Configure SSH, if not already configured.

**2. lépés** . For local authentication, configure at least one local database user with privilege level 15.

**3. lépés** . Engedélyezze az AAA-t az **aaa new-model** globális konfigurációs mód paranccsal.

**4. lépés** . Használja az **AAA hitelesítési bejelentkezési alapértelmezett helyi** parancsot, hogy meghatározza, hogy a helyi adatbázist használják a hitelesítéshez.

**5. lépés** . használja az **AAA engedélyezés EXEC alapértelmezett helyi** A parancs engedélyezése konfigurálásához parancsát. Ebben a példában minden helyi felhasználó hozzáférhet az Exec parancsokhoz.

**6. lépés** . Engedélyezze az SCP szerver-oldalú funkcionalitást az **IP SCP Server engedélyezési** parancs segítségével.

A példában az R1 most egy SCP -kiszolgáló, és SSH kapcsolatokat fog használni a hitelesített és engedélyezett felhasználók biztonságos másolási transzferjeinek elfogadására. Az átvitelek bármely SCP-klienstől származhatnak, függetlenül attól, hogy az ügyfél egy másik útválasztó, kapcsoló vagy munkaállomás.

R1(config)# **ip domain-name span.com**

R1(config)# **crypto key generate rsa general-keys modulus 2048**

R1(config)# **username Bob privilege 15 algorithm-type scrypt secret cisco12345**

R1(config)# **aaa new-model**

R1(config)# **aaa authentication login default local**

R1(config)# **aaa authorization exec default local**

R1(config)# **ip scp server enable**

Tegyük fel most, hogy biztonságosan szeretnénk másolni az R2 nevű útválasztó biztonsági mentési konfigurációját az SCP szerverre, amely R1. parancsát használnánk **másolási** Amint az az alábbi parancs kimenetén látható, az R2 , és meghatározzuk, hogy a forrásfájl helyét először adjuk meg (Flash0: R2backup.cfg), majd a rendeltetési hely (SCP :). Miután megválaszolta a kapcsolatot az SCP szerverhez az R1 -en, a fájlban a fájlt lemásolják.

R2# **copy flash0:R2backup.cfg scp:**

Address or name of remote host []? **10.1.1.1**

Destination username [R2]? **Bob**

Destination filename [R2backup.cfg]?

Writing R2backup.cfg

Password: **<cisco12345>**

!

1381 bytes copied in 8.596 secs (161 bytes/sec)

R2#

Az R1-en megadhatja a **debug ip scp** parancsot, hogy figyelje az átvitel folyamatát, ahogy az a következő példában látható. A leggyakoribb hitelesítési probléma a felhasználónév/jelszó helytelen kombinációja. Hitelesítési hiba is előfordulhat, ha a felhasználónév/jelszó kombináció nem volt konfigurálva a **15-ös privilege** kulcsszóval az SCP-kiszolgálón.

R1# **debug ip scp**

Incoming SCP debugging is on

R1#

\*Feb 18 20:37:15.363: SCP: [22 -> 10.1.1.2:61656] send \*Feb 18 20:37:15.367: SCP: [22 <- 10.1.1.2:61656] recv C0644 1381 R2backup.cfg \*Feb 18 20:37:15.367: SCP: [22 -> 10.1.1.2:61656] send

6.1.5

## Állítsa vissza a router jelszavát

Ha az útválasztót feltörték, vagy helytelenül beállított jelszóból kell helyreállítani, a rendszergazdának jelszó-helyreállítási eljárást kell alkalmaznia, például az alábbi lépésekben bemutatottakat. Biztonsági okokból a jelszó-helyreállítás megköveteli, hogy a rendszergazda fizikai hozzáféréssel rendelkezzen az útválasztóhoz konzolkábellel. Az eszköztől függően a jelszó-helyreállítás részletes eljárása eltérő lehet.

**1. lépés** . Csatlakoztassa a konzolporthoz.

**2. lépés** . A **show version** paranccsal jelenítse meg a konfigurációs regiszter beállítását és dokumentálja az értéket (pl. 0x2102).

**3. lépés** . Kapcsolja be az útválasztót.

**4. lépés** . Adja ki a töréssorozatot (pl. **CTRL-BREAK** ) a ROMMON módba lépéshez.

**5. lépés** . Módosítsa az alapértelmezett konfigurációs regisztert a **confreg 0x2142** paranccsal.

**6. lépés** . Indítsa újra az útválasztót a **reset** paranccsal ROMMON módban.

**7. lépés** . Nyomja meg **a Ctrl-C billentyűkombinációt** a kezdeti beállítási eljárás kihagyásához.

**8. lépés** . Lépjen be a privilegizált EXEC módba.

**9. lépés** . Másolja az indítási konfigurációt a futó konfigurációba a **copy startup-config running-config** paranccsal.

**10. lépés** . Ellenőrizze a konfigurációt.

**11. lépés** . Módosítsa az engedélyezési titkos jelszót.

**12. lépés** . Engedélyezze az összes interfészt a **no shutdown** paranccsal.

**13. lépés** . Állítsa vissza a konfigurációs regiszter beállítását az eredeti beállításra, amelyet a 2. lépésben dokumentált a **config-register** globális konfigurációs paranccsal. A következő újraindításkor az útválasztó ezeket a beállításokat fogja használni, és betölti a módosított jelszót tartalmazó új indítási konfigurációs fájlt.

**14. lépés** . Mentse el a konfigurációs változtatásokat.

6.1.6

## Jelszó visszaállítás

Ha valaki fizikailag hozzáfér egy útválasztóhoz, a jelszó-helyreállítási eljárással potenciálisan átveheti az irányítást az eszköz felett. Ez az eljárás, ha helyesen hajtja végre, érintetlenül hagyja az útválasztó konfigurációját. Ha a támadó nem hajt végre jelentős változtatásokat, az ilyen típusú támadásokat nehéz észlelni. A támadó ezzel a támadási módszerrel felderítheti az útválasztó konfigurációját és a hálózatra vonatkozó egyéb információkat, például a forgalmi áramlásokat és a hozzáférés-szabályozási korlátozásokat.

globális konfigurációs mód paranccsal mérsékelheti ezt a lehetséges biztonsági rést **Az adminisztrátor a no szolgáltatás jelszó-helyreállítás** . Ez a parancs egy rejtett Cisco IOS parancs, és nincsenek argumentumai vagy kulcsszavai. paranccsal van konfigurálva **Ha egy útválasztó a nincs szolgáltatás jelszó-helyreállítási** , a ROMmon módhoz való minden hozzáférés le van tiltva.

Ha a **nincs szolgáltatás jelszó-helyreállítási** parancsot beírja, egy figyelmeztető üzenet jelenik meg, és a szolgáltatás engedélyezése előtt nyugtázni kell, ahogy a példában is látható.

R1(config)# **no service password-recovery**

WARNING:

Executing this command will disable password recovery

mechanism.

Do not execute this command without another plan for

password recovery.

Are you sure you want to continue? [yes/no]: **yes**

R1(config)#

Ha be van állítva, a **show running-config** parancs egy **no service password-recovery** utasítást jelenít meg, ahogy az itt látható.

R1# **show running-config**

Building configuration...

Current configuration : 836 bytes

!

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

no service password-recovery

Az alábbiak szerint az útválasztó indításakor a kezdeti rendszerindítási szekvencia egy üzenetet jelenít meg, amely szerint a JELSZÓ-HELYREÁLLÍTÁSI FUNKCIÓ LETILTVA van.

System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 2006 by cisco Systems, Inc.

PLD version 0x10

GIO ASIC version 0x127

c1841 platform with 131072 Kbytes of main memory

Main memory is configured to 64 bit mode with parity disabled

PASSWORD RECOVERY FUNCTIONALITY IS DISABLED

program load complete, entry point: 0x8000f000, size:0xcb80

Az eszköz helyreállításához a **nincs szolgáltatás jelszó-helyreállítási** parancs beírása után indítsa el a szünetsorozatot öt másodpercen belül azután, hogy a kép kitömörödött a rendszerindítás során. A rendszer kéri, hogy erősítse meg a törésbillentyű műveletet. A művelet megerősítése után az indítási konfiguráció teljesen törlődik, a jelszó-helyreállítási eljárás engedélyezve van, és az útválasztó a gyári alapértelmezett konfigurációval indul. Ha nem erősíti meg a megszakítási műveletet, az útválasztó normál módon indul el, és engedélyezve van a **no service password-recovery** parancs.

**VIGYÁZAT** : Ha az útválasztó flash memóriája sérülés vagy törlés miatt nem tartalmaz érvényes Cisco IOS lemezképet, a ROMmon xmodem parancs nem használható új flash kép betöltésére. Az útválasztó javításához a rendszergazdának új Cisco IOS-képet kell szereznie egy flash SIMM-re vagy egy PCMCIA-kártyára. Ha azonban egy rendszergazda hozzáfér a ROMmonhoz, visszaállíthat egy IOS-fájlt a flash memóriába egy TFTP-kiszolgáló segítségével. A flash képek biztonsági mentésével kapcsolatos további információkért látogasson el a Cisco.com webhelyre.

[6.0](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[6.2](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Lock Down a Router Using AutoSecure](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                                           
*                               

1. Device Monitoring and Management
2. Lock Down a Router Using AutoSecure

# Zárolja le az útválasztót az AutoSecure használatával

6.2.1

## Felfedezési protokollok CDP és LLDP

A Cisco útválasztók kezdetben számos szolgáltatással vannak telepítve, amelyek alapértelmezés szerint engedélyezve vannak. Ez a kényelem és az eszköz üzembe helyezéséhez szükséges konfigurációs folyamat egyszerűsítése érdekében történik. E szolgáltatások némelyike ​​azonban sebezhetővé teheti az eszközt a támadásokkal szemben, ha a biztonság nincs engedélyezve. A rendszergazdák olyan szolgáltatásokat is engedélyezhetnek a Cisco útválasztókon, amelyek jelentős kockázatnak tehetik ki az eszközt. Mindkét forgatókönyvet figyelembe kell venni a hálózat biztosításakor.

A Cisco Discovery Protocol (CDP) egy példa egy olyan szolgáltatásra, amely alapértelmezés szerint engedélyezve van a Cisco útválasztókon. A Link Layer Discovery Protocol (LLDP) egy nyílt szabvány, amely engedélyezhető a Cisco eszközökön, valamint az LLDP-t támogató egyéb gyártói eszközökön.

Az LLDP konfigurációja és ellenőrzése hasonló a CDP-hez. Az ábrán az R1 és az S1 egyaránt LLDP-vel van konfigurálva, az **lldp run** global configuration paranccsal. Mindkét eszköz alapértelmezés szerint CDP-t futtat. A **show cdp szomszédok részletes** és **a show lldp szomszédok részletes** kimenete megmutatja az eszköz címét, platformját és operációs rendszerének részleteit.

R1(config)# **lldp run**

R1(config)# **end**

R1# **show cdp neighbors detail**

-------------------------

Device ID: S1

Entry address(es):

IP address: 192.168.1.254

Platform: cisco WS-C2960-24TT-L, Capabilities: Switch IGMP

Interface: GigabitEthernet0/1, Port ID (outgoing port): FastEthernet0/5

Holdtime : 164 sec

Version :

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE7,

RELEASE SOFTWARE (fc1)

<output omitted>

R1# **show lldp neighbors detail**

------------------------------------------------

Local Intf: Gi0/1

Chassis id: 0022.9121.0380

Port id: Fa0/5

Port Description: FastEthernet0/5

System Name: S1

System Description:

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE7,

RELEASE SOFTWARE (fc1)

<output omitted>

Sajnos a támadóknak nincs szükségük CDP- vagy LLDP-kompatibilis eszközökre ahhoz, hogy összegyűjtsék ezeket az érzékeny információkat. A könnyen elérhető szoftverek, mint például a Universal Network CDP & LLDP Evaluator (UNCLE), lehetővé teszik a hálózat bármely számítógépének, hogy rögzítse és megtekintse a LAN-on küldött CDP és LLDP információkat. Ezenkívül a CDP sebezhető a CDP hamisítási támadásaival szemben, mivel a CDP jól ismert multicast MAC-címet használ. Ez a szolgáltatásmegtagadási támadás egy formája, amely hamis CDP-üzenetekkel boríthatja el az eszközök CDP-tábláit.

6.2.2

## Protokollok és szolgáltatások beállításai

A támadók olyan szolgáltatásokat és protokollokat választanak, amelyek sebezhetőbbé teszik a hálózatot a rosszindulatú kizsákmányolással szemben.

E szolgáltatások közül sokat le kell tiltani vagy korlátozni kell a képességeiket a szervezet biztonsági szükségletei alapján. Ezek a szolgáltatások a hálózatfelderítési protokolloktól (például CDP és LLDP) a globálisan elérhető protokollokig, például az ICMP és más vizsgálóeszközökig terjednek.

A Cisco IOS szoftver egyes alapértelmezett beállításai történelmi okokból állnak fenn. Ezek logikai alapbeállítások voltak a szoftver eredeti írásakor. Az egyéb alapértelmezett beállítások a legtöbb rendszer számára ésszerűek, de biztonsági kockázatot jelenthetnek, ha azokat olyan eszközökben használják, amelyek a hálózat peremvédelmének részét képezik. Megint más alapértelmezett értékeket írnak elő a szabványok, de ezek biztonsági szempontból nem mindig kívánatosak.

A táblázat összefoglalja a protokollok és szolgáltatások jellemzőit és alapértelmezett beállításait.

| **Funkció** | **Alapértelmezett** |
| --- | --- |
| Cisco Discovery Protocol (CDP) | Engedélyezve |
| Link Layer Discovery Protocol (LLDP) | Tiltva |
| Konfiguráció automatikus betöltése | Tiltva |
| FTP szerver | Tiltva |
| TFTP szerver | Tiltva |
| Network Time Protocol (NTP) szolgáltatás | Tiltva |
| Packet assembler/disassembler (PAD) szolgáltatás | Engedélyezve |
| TCP és User Datagram Protocol (UDP) kisebb szolgáltatások | Engedélyezve a 11.3-as és újabb verziókban |
| Maintenance Operation Protocol (MOP) szolgáltatás | A legtöbb Ethernet interfészen engedélyezve van |
| Simple Network Management Protocol (SNMP) | Engedélyezve |
| HTTP vagy HTTPS konfiguráció és felügyelet | A beállítás Cisco eszközfüggő. |
| Domain Name System (DNS) | Engedélyezve |
| Internet Control Message Protocol (ICMP) átirányítások | Engedélyezve |
| IP-forrás útválasztás | Engedélyezve |
| Ujjszerviz | Engedélyezve |
| ICMP elérhetetlen értesítések | Engedélyezve |
| ICMP maszk válasz | Tiltva |
| IP azonosítási szolgáltatás | Engedélyezve |
| TCP életben marad | Tiltva |
| Ingyenes ARP (GARP) | Engedélyezve |
| Proxy ARP | Engedélyezve |

Az alábbi táblázat a protokollokhoz és szolgáltatásokhoz javasolt biztonsági beállításokat mutatja be.

Számos fontos gyakorlat áll rendelkezésre az eszköz biztonságának biztosításában:

* Tiltsa le a szükségtelen szolgáltatásokat és interfészeket.
* Tiltsa le és korlátozza az általánosan konfigurált felügyeleti szolgáltatásokat, például az SNMP-t.
* Tiltsa le a szondákat és vizsgálatokat, például az ICMP-t. Biztosítsa a terminálhoz való hozzáférés biztonságát.
* Az ingyenes és proxy címfeloldási protokollok (ARP) letiltása.
* Az IP-című adások letiltása.

| **Funkció** | **Ajánlást** |
| --- | --- |
| Cisco Discovery Protocol (CDP) | Globálisan vagy interfészenként le kell tiltani, ha nem szükséges. |
| Link Layer Discovery Protocol (LLDP) | Globálisan vagy interfészenként le kell tiltani, ha nem szükséges. |
| Konfiguráció automatikus betöltése | Le van tiltva, ha nem használja a router. |
| FTP szerver | Le kell tiltani, ha nincs rá szükség. |
| TFTP szerver | Le kell tiltani, ha nincs rá szükség. |
| Network Time Protocol (NTP) szolgáltatás | Le van tiltva, ha nincs rá szükség. |
| Packet assembler/disassembler (PAD) szolgáltatás | Ha nincs használatban, kifejezetten le kell tiltani. |
| TCP és User Datagram Protocol (UDP) kisebb szolgáltatások | Kifejezetten tiltsa le ezt a szolgáltatást. |
| Maintenance Operation Protocol (MOP) szolgáltatás | Kifejezetten le kell tiltani, ha nincs használatban. |
| Simple Network Management Protocol (SNMP) | Ha nincs rá szükség, kapcsolja ki ezt a szolgáltatást. |
| HTTP vagy HTTPS konfiguráció és felügyelet | Ha nem szükséges, kapcsolja ki a szolgáltatást. Ha ez a szolgáltatás szükséges, korlátozza a hozzáférést az útválasztó HTTP- vagy HTTPS-szolgáltatásához hozzáférés-vezérlési listák (ACL) segítségével. |
| Domain Name System (DNS) | Tiltsa le, ha nem szükséges. Ha a DNS-keresési szolgáltatásra van szükség, győződjön meg róla, hogy kifejezetten beállította a DNS-kiszolgáló címét. |
| Internet Control Message Protocol (ICMP) átirányítások | Tiltsa le, ha nem szükséges. |
| IP-forrás útválasztás | Ha nincs rá szükség, kapcsolja ki ezt a szolgáltatást. |
| Ujjszerviz | Ha nincs rá szükség, kapcsolja ki ezt a szolgáltatást. |
| ICMP elérhetetlen értesítések | Letiltása a nem megbízható hálózatokhoz vezető interfészeken. |
| ICMP maszk válasz | Letiltása a nem megbízható hálózatokhoz vezető interfészeken. |
| IP azonosítási szolgáltatás | A szolgáltatást kifejezetten le kell tiltani. |
| TCP életben marad | Globálisan engedélyezni kell a TCP-kapcsolatok kezeléséhez és bizonyos szolgáltatásmegtagadási (DoS) támadások megelőzéséhez. A szolgáltatás a Cisco IOS 12.0-s kiadás előtti Cisco IOS szoftverekben engedélyezett, a Cisco IOS 12.0 és újabb verzióiban pedig le van tiltva. Ha nincs rá szükség, kapcsolja ki ezt a szolgáltatást. |
| Ingyenes ARP (GARP) | Minden útválasztó interfészen tiltsa le az ingyenes ARP-ket, hacsak nincs szükség erre a szolgáltatásra. |
| Proxy ARP | Minden interfészen tiltsa le ezt a szolgáltatást, kivéve, ha az útválasztót LAN-hídként használják. |

6.2.3

## Cisco AutoSecure

Az IOS 12.3-as verziójában kiadott Cisco AutoSecure egy olyan szolgáltatás, amely a parancssori felületről indul, és egy parancsfájlt hajt végre. Az AutoSecure először javaslatokat tesz a biztonsági rések kijavítására, majd az ábra szerint módosítja az útválasztó biztonsági konfigurációját.

Az AutoSecure zárolhatja a felügyeleti sík funkcióit, valamint az útválasztó továbbítási sík szolgáltatásait és funkcióit. Számos felügyeleti sík szolgáltatás és funkció létezik:

* Biztonságos BOOTP, CDP, FTP, TFTP, PAD, UDP és TCP kisszerverek, MOP, ICMP (átirányítások, maszkos válaszok), IP-forrás útválasztás, ujjlenyomat, jelszótitkosítás, TCP-megőrzés, ingyenes ARP, proxy ARP és irányított sugárzás
* Jogi értesítés banner használatával
* Biztonságos jelszó és bejelentkezési funkciók
* Biztonságos NTP
* Biztonságos SSH hozzáférés
* TCP elfogó szolgáltatások

Az AutoSecure három továbbítási sík szolgáltatást és funkciót tesz lehetővé:

* Cisco Express Forwarding (CEF)
* Forgalomszűrés ACL-ekkel
* Cisco IOS tűzfal vizsgálat a gyakori protokollokhoz

Az AutoSecure-t gyakran használják a terepen, hogy alapszintű biztonsági házirendet biztosítsanak egy új útválasztón. A funkciók ezután módosíthatók a szervezet biztonsági politikájának támogatása érdekében.

R1# **auto secure**

--- AutoSecure Configuration ---

\*\*\* AutoSecure configuration enhances the security

of the router but it will not make router

absolutely secure from all security attacks \*\*\*

All the configuration done as part of AutoSecure

will be shown here. For more details of why and

how this configuration is useful, and any possible

side effects, please refer to Cisco documentation of

AutoSecure.

At any prompt you may enter '?' for help.

Use ctrl-c to abort this session at any prompt.

Gathering information about the router for

AutoSecure

Is this router connected to internet? [no]:**yes**

6.2.4

## Cisco AutoSecure Command Syntax

Az **automatikus biztonsági** paranccsal engedélyezheti a Cisco AutoSecure szolgáltatás beállítását. Ez a beállítás lehet interaktív vagy nem interaktív. Az ábra az **automatikus biztonságos** parancs parancs szintaxisát mutatja.

Router#  **auto safe**  {  **no-interact**  |  **teljes**  } [  **továbbítás**  |  **menedzsment**  ] [  **ntp**  |  **belépés**  |  **ssh**  |  **tűzfal**  |  **top-intercept**  ]

Itt vannak a parancs paraméterei.

R1# **auto secure ?**

forwarding Secure Forwarding Plane

management Secure Management Plane

no-interact Non-interactive session of AutoSecure

<cr>

R1#

**Megjegyzés** : A lehetőségek platformonként változhatnak.

Interaktív módban az útválasztó felkéri a szolgáltatások és egyéb biztonsági funkciók engedélyezésére és letiltására vonatkozó lehetőségeket. paranccsal is konfigurálható **Ez az alapértelmezett mód, de az automatikus biztonságos teljes** .

paranccsal konfigurálják **A nem interaktív módot az auto safe no-interact** . Ez automatikusan végrehajtja a Cisco AutoSecure szolgáltatást az ajánlott Cisco alapértelmezett beállításokkal. Az **automatikus biztonságos** parancs kulcsszavakkal is megadható bizonyos összetevők, például a felügyeleti sík ( **kezelési** kulcsszó ) és a továbbítási sík ( **továbbítási** kulcsszó ) konfigurálásához.

| **Opcionális paraméterek** | **Leírás** |
| --- | --- |
| **nincs interakció** | A felhasználó nem kér interaktív konfigurációkat. Nem lesznek konfigurálva interaktív párbeszédparaméterek, beleértve a felhasználóneveket vagy jelszavakat. |
| **teljes** | A felhasználót minden interaktív kérdésre fel kell kérni. Ez az alapértelmezett beállítás. |
| **szállítmányozás** | Only the forwarding plane will be secured. |
| **menedzsment** | Csak a felügyeleti sík kerül biztonságba. |
| **ntp** | Meghatározza az NTP szolgáltatás konfigurációját az AutoSecure CLI-ben. |
| **Belépés** | Meghatározza a bejelentkezési szolgáltatás konfigurációját az AutoSecure CLI-ben. |
| **ssh** | Meghatározza az SSH szolgáltatás konfigurációját az AutoSecure CLI-ben. |
| **tűzfal** | Megadja a tűzfal szolgáltatás konfigurációját az AutoSecure parancssori felületen. |
| **tcp-intercept** | Meghatározza a TCP elfogás szolgáltatásának konfigurációját az AutoSecure CLI-ben. |

6.2.5

## Cisco AutoSecure konfigurációs példa

Az **automatikus biztonsági** parancs elindításakor egy CLI varázsló végigvezeti a rendszergazdát az eszköz konfigurációján. Felhasználói bevitel szükséges.

Kattintson az alábbi gombra, ha többet szeretne megtudni a CLI varázsló lépéseiről.

Az **automatikus biztonsági** parancs beírásra kerül. Az útválasztó megjeleníti az AutoSecure konfigurációs varázsló üdvözlő üzenetét, az ábra szerint.

A varázsló információkat gyűjt a külső interfészekről, az ábra szerint

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]: **yes**

Enter the number of interfaces facing the internet [1]:

Interface IP-Address OK? Method Status Protocol

FastEthernet0/0 192.168.10.1 YES manual up up

FastEthernet0/1 192.168.11.1 YES manual up up

FastEthernet0/1/0 unassigned YES unset up down

FastEthernet0/1/1 unassigned YES unset up down

FastEthernet0/1/2 unassigned YES unset up down

FastEthernet0/1/3 nassigned YES unset up down

Serial0/0/0 192.168.2.101 YES manual up up

Serial0/0/1 unassigned YES manual administratively down down

Vlan1 unassigned YES manual up down

Enter the interface name that is facing the internet: **Serial 0/0/0**

Invalid interface name

Enter the interface name that is facing the internet: **Serial0/0/0**

<continued>

Az AutoSecure a szükségtelen szolgáltatások letiltásával védi a felügyeleti síkot, az ábrán látható módon.

Securing Management plane services...

Disabling service finger

Disabling service pad

Disabling udp & tcp small servers

Enabling service password encryption

Enabling service tcp-keepalives-in

Enabling service tcp-keepalives-out

Disabling the cdp protocol

Disabling the bootp server

Disabling the http server

Disabling the finger service

Disabling source routing

Disabling gratuitous arp

<continued>

Az AutoSecure a képen látható módon szalaghirdetést kér.

Here is a sample Security Banner to be shown at every access to device. Modify it

to suit your enterprise requirements.

Authorized Access only

This system is the property of So-&-So-Enterprise.

UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.

You must have explicit permission to access this

device. All activities performed on this device

are logged. Any violations of access policy will result

in disciplinary action.

Enter the security banner {Put the banner between k and k, where k is any character}:

**#**

**\*\*\*\*\*\*\*\*\* AUTHORIZED ACCESS ONLY \*\*\*\*\*\*\*\*\*\*\***

**UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.**

**You must have explicit permission to access this**

**device. Any violations of access policy will result**

**in disciplinary action.**

**#**

<continued>

Az AutoSecure jelszavakat kér, és engedélyezi a jelszavakat és a bejelentkezési funkciókat, az ábrán látható módon.

Enable secret is either not configured or is the same as enable password

Enter the new enable secret: **cisco123**

Confirm the enable secret : **cisco123**

Enter the new enable password: **cisco1**

% Password too short - must be at least 6 characters. Password configuration failed

Enter the new enable password: **cisco321**

Confirm the enable password: **cisco321**

Configuring AAA local authentication

Configuring Console, Aux and VTY lines for local authentication, exec-timeout,

and transport

Securing device against Login Attacks

Configure the following parameters

Blocking Period when Login Attack detected: **120**

Maximum Login failures with the device: **2**

Maximum time period for crossing the failed login attempts: **60**

Configure SSH server? [yes]: **y**

<continued>

Az interfészek biztonságosak, az ábrán látható módon.

Configuring interface specific AutoSecure services

Disabling the following ip services on all interfaces:

no ip redirects

no ip proxy-arp

no ip unreachables

no ip directed-broadcast

no ip mask-reply

Disabling mop on Ethernet interfaces

<continued>

A továbbító sík az ábrán látható módon rögzítve van.

Securing Forwarding plane services...

Enabling CEF (This might impact the memory requirements for your platform)

Enabling unicast rpf on all interfaces connected to internet

Configure CBAC Firewall feature? [yes/no]: **yes**

R1# **auto secure**

--- AutoSecure Configuration ---

\*\*\* AutoSecure configuration enhances the security of the router, but it will not make it

absolutely resistant to all security attacks \*\*\*

AutoSecure will modify the configuration of your device. All configuration changes will be

shown. For a detailed explanation of how the configuration changes enhance security and any

possible side effects, please refer to Cisco.com for Autosecure documentation.

At any prompt you may enter '?' for help.

Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure

<continued>

Amikor a varázsló befejeződött, a futó konfiguráció megjeleníti az összes konfigurációs beállítást és módosítást.

**Megjegyzés** : Az AutoSecure-t az útválasztó kezdeti konfigurálásakor kell használni. Gyári útválasztókon nem ajánlott.

6.2.6

## Szintaxis-ellenőrző – Az automatikus biztonsági parancs használata

Ebben a szintaktikai ellenőrzőben az AutoSecure-t fogja használni az R1 védelmére.

* Állítsa be **a Serial0/0/0-t** az internet felé néző interfészként. **Megjegyzés** : Az interfész neve kis- és nagybetűfüggő.
* Hozzon létre egy motd bannert **a #jogosulatlan hozzáférés tilos!#** használatával .
* hozzon létre egy **Admin01** helyi felhasználónevet és **Admin01pa55 jelszót.** Az útválasztó eléréséhez
* Konfiguráljon **60** másodperces bejelentkezési leállást, ha **másodpercen belül 2** sikertelen bejelentkezési kísérlet történik **30** .
* Használja **az example.com** tartománynevet az SSH-kiszolgálóhoz.
* Ne konfiguráljon CBAC tűzfalat.
* Alkalmazza az AutoSecure konfigurációját a futó konfigurációra.

Az AutoSecure segítségével zárja le az útválasztót.

R1# automatikus biztonság

--- AutoSecure konfiguráció ---

\*\*\* Az AutoSecure konfiguráció növeli a biztonságot

a routert, de attól még nem lesz abszolút ellenálló

minden biztonsági támadásra \*\*\*

Az AutoSecure módosítja az eszköz konfigurációját.

Az összes konfigurációs módosítás megjelenik. A részletes

magyarázat arról, hogy a konfiguráció változásai hogyan növelik a biztonságot

és minden lehetséges mellékhatásról, kérjük, keresse fel a Cisco.com webhelyet

AutoSecure dokumentáció.

Bármelyik parancssorba beírhatja a "?" segítségért.

Használja a ctrl-c billentyűkombinációt a munkamenet megszakításához bármely kérdésre.

Információgyűjtés az AutoSecure útválasztójáról

Ez a router csatlakozik az internethez? [nem]# igen

Adja meg az internet felé néző interfészek számát [1]# 1

Az interfész IP-címe rendben van? Method Status Protocol

Embedded-Service-Engine0/0 hozzárendeletlen IGEN adminisztratívan leállítva

GigabitEthernet0/0 nincs hozzárendelve IGEN törlése adminisztratívan leállt

GigabitEthernet0/1 192.168.1.1 IGEN kézi fel

Serial0/0/0 10.1.1.1 IGEN kézi fel

Serial0/0/1 hozzárendeletlen IGEN törlése adminisztratívan leállt

Adja meg az internet felé néző interfész nevét # Serial0/0/0

Menedzsment repülőgép szolgáltatásainak biztosítása...

Szervizujj letiltása

Szervizpad letiltása

Udp és tcp kis szerverek letiltása

A szolgáltatás jelszavas titkosításának engedélyezése

A tcp-keepalves-in szolgáltatás engedélyezése

A tcp-keepalves-out szolgáltatás engedélyezése

A cdp protokoll letiltása

A bootp szerver letiltása

A http szerver letiltása

Az ujjszolgáltatás letiltása

Forrásútválasztás letiltása

Az ingyenes arp letiltása

Itt van egy minta biztonsági szalaghirdetés, amelyet meg kell jeleníteni

minden eszközhöz való hozzáféréskor. Módosítsa a saját igényei szerint

vállalati követelmények.

Csak engedélyezett hozzáférés

Ez a rendszer a So-&-So-Enterprise tulajdona.

AZ ESZKÖZHEZ AZ ENGEDÉLYTELEN HOZZÁFÉRÉS TILOS.

Ennek eléréséhez kifejezett engedéllyel kell rendelkeznie

eszköz. Az eszközön végzett összes tevékenység

naplózva vannak. A hozzáférési szabályzat megsértése ennek következménye

fegyelmi eljárásban.

Írja be a biztonsági szalaghirdetést {Put the banner between

k és k, ahol k tetszőleges karakter}:

# #Az illetéktelen hozzáférés tilos!#

Helyi felhasználói adatbázis konfigurálása

felhasználónevet Adja meg az Admin01

Írja be a jelszót: Admin01pa55

Erősítse meg a jelszót: Admin01pa55

Az AAA helyi hitelesítés konfigurálása

Konzol, Aux és vty vonalak konfigurálása ehhez

helyi hitelesítés, végrehajtási időtúllépés, szállítás

Az eszköz védelme a bejelentkezési támadásokkal szemben

Állítsa be a következő paramétereket

Blokkolási időszak a bejelentkezési támadás észlelésekor # 60

számú eszközzel Maximális bejelentkezési hibák a 2.

A sikertelen bejelentkezési kísérletek átlépésének maximális időtartama # 30

Konfigurálja az SSH szervert? [yes]# igen

Írja be a domain-name# example.com címet

Interfészspecifikus AutoSecure szolgáltatások konfigurálása

A következő ip-szolgáltatások letiltása az összes felületen:

nincs ip átirányítás

nincs ip proxy-arp

nincs elérhetetlen ip

nincs ip irányított adás

nincs ip-maszk-válasz

Mop letiltása Ethernet interfészeken

Továbbítási repülőgép szolgáltatások biztosítása...

Az unicast rpf engedélyezése az összes csatlakoztatott interfészen

az internetre

Konfigurálja a CBAC tűzfal funkciót? [igen/nem]# nem

Ez a létrehozott konfiguráció:

nincs szervizujj

nincs szervizlap

nincs szolgáltatás udp-small-servers

nincs szolgáltatás tcp-small-servers

szolgáltatás jelszavas titkosítása

szolgáltatás tcp-keepalives-in

szolgáltatás tcp-keepalves-out

nem fut cdp

nincs ip bootp szerver

nincs ip http szerver

nincs ip ujj

nincs ip forrásútvonal

nincs ip gratuitous-arps

nincs ip identd

banner motd ^CUA jogosulatlan hozzáférés TILOS^C

biztonsági jelszavak min-hosszúsága 6

biztonsági hitelesítés hibaaránya 10 napló

felhasználónév Admin01 jelszó 7 15330F010D247B7538326077

aaa új modell

aaa hitelesítés bejelentkezés local\_auth local

vonalkonzol 0

bejelentkezés hitelesítés local\_auth

végrehajtási időtúllépés 5 0

szállítási kimenet telnet

sor aux 0

bejelentkezés hitelesítés local\_auth

végrehajtási időtúllépés 10 0

szállítási kimenet telnet

sor vty 0 4

bejelentkezés hitelesítés local\_auth

szállítási bemenet telnet

tty 1 2. sor

bejelentkezés hitelesítés local\_auth

végrehajtási időtúllépés 15 0

bejelentkezési blokk – 60 próbálkozásra 2 30-on belül

ip domain név ccnasecurity.com

kriptokulcs generálja az RSA általános kulcsok modulusát 1024

ip ssh időtúllépés 60

ip ssh hitelesítés-újrapróbálkozások 2

sor vty 0 4

szállítási bemenet ssh telnet

szolgáltatási időbélyegek hibakeresés dátumidő msec localtime show-timezone

szolgáltatási időbélyegek napló dátumidő msec localtime show-timezone

fakitermelés helyi2

naplózási csapda hibakeresés

szolgáltatási sorszámok

naplózási konzol kritikus

naplózás pufferelt

interfész Embedded-Service-Engine0/0

nincs ip átirányítás

nincs ip proxy-arp

nincs elérhetetlen ip

nincs ip irányított adás

nincs ip-maszk-válasz

nincs felmosva engedélyezve

interfész GigabitEthernet0/0

nincs ip átirányítás

nincs ip proxy-arp

nincs elérhetetlen ip

nincs ip irányított adás

nincs ip-maszk-válasz

nincs felmosva engedélyezve

interfész GigabitEthernet0/1

nincs ip átirányítás

nincs ip proxy-arp

nincs elérhetetlen ip

nincs ip irányított adás

nincs ip-maszk-válasz

nincs felmosva engedélyezve

interfész Serial0/0/0

nincs ip átirányítás

nincs ip proxy-arp

nincs elérhetetlen ip

nincs ip irányított adás

nincs ip-maszk-válasz

interfész Serial0/0/1

nincs ip átirányítás

nincs ip proxy-arp

nincs elérhetetlen ip

nincs ip irányított adás

nincs ip-maszk-válasz

access-list 100 engedélyezi az udp tetszőleges eq bootpc-t

interfész Serial0/0/0

ip ellenőrzése az unicast forrás elérhető-rx-n keresztül engedélyezve-alapértelmezett 100

!

vége

Alkalmazza ezt a konfigurációt a running-config számára? [yes]# igen

A létrehozott konfiguráció alkalmazása a running-config-hoz

A kulcsok neve: R1.ccnasecurity.com

% A kulcsmodulus mérete 1024 bit

% 1024 bites RSA-kulcsok generálása, a kulcsok nem lesznek exportálhatók...

[OK] (az eltelt idő 3 másodperc volt)

R1#

000046: \*Dec 30 22:44:35.503 UTC: %AUTOSEC-1-MODIFIED: Az AutoSecure konfigurációja módosult ezen az eszközön

Sikeresen biztosította az R1-et az AutoSecure segítségével.

6.2.7

### Lab – Automatikus biztonsági szolgáltatások konfigurálása

Ebben a laborban a következő célokat kell teljesítenie:

* 1. rész: Az alapvető eszközbeállítások konfigurálása.
* 2. rész: Automatikus biztonsági funkciók konfigurálása.

[6.1](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Secure Cisco IOS Image and Configuration Files](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[6.3](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Routing Protocol Authentication](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                                                
*                               

1. Device Monitoring and Management
2. Routing Protocol Authentication

# Routing Protocol Authentication

6.3.1

## Dinamikus útválasztási protokollok

A dinamikus útválasztási protokollokat az útválasztók a távoli hálózatok elérhetőségével és állapotával kapcsolatos információk automatikus megosztására használják. A dinamikus útválasztási protokollok számos tevékenységet végeznek, beleértve a hálózatfelderítést és az útválasztási táblák karbantartását.

A dinamikus útválasztási protokollok fontos előnyei a legjobb útvonal kiválasztásának képessége, valamint az új legjobb útvonal automatikus felfedezésének képessége, ha a topológia megváltozik.

A hálózatfelderítés az útválasztási protokoll azon képessége, hogy információkat ossza meg az általa ismert hálózatokról más útválasztókkal, amelyek szintén ugyanazt az útválasztási protokollt használják. Ahelyett, hogy minden útválasztón manuálisan konfigurált statikus útvonalaktól függnének a távoli hálózatokhoz, a dinamikus útválasztási protokoll lehetővé teszi az útválasztók számára, hogy automatikusan tájékozódjanak ezekről a hálózatokról más útválasztóktól. Ezek a hálózatok és a legjobb elérési út mindegyikhez hozzáadódnak az útválasztó útválasztási táblázatához, és egy adott dinamikus útválasztási protokoll által megtanult hálózatként azonosíthatók.

Az ábrán az R1 és R2 útválasztók láthatók, amelyek közös útválasztási protokollt használnak a hálózati információk megosztására.

Az ábra 3 R 1, R 2 és R3 routert ábrázol, amelyek 4 S 1, S 2, S 3 és S4 kapcsolóhoz vannak csatlakoztatva. Az R 1 két gigabites G/0/0 és G0/0/1 kapcsolaton keresztül csatlakozik az S 1 és S 2 kapcsolókhoz. A P C1 a 10.0.1.0/24 és a 2001:db8:acad:1::/64 hálózat 1. kapcsolójához (S 1) csatlakozik, .10 és ::10 kettős verem IP-címmel. A P C2 a 10.0.2.0/24 és 2001:db8:acad:2::/64 hálózaton a 2. kapcsolóhoz (S 2) csatlakozik, .10 és ::10 kettős verem IP-címmel. Az R1-nek pont-pont hálózata van R2-vel és az ISP-hálózatokkal. Az R2 soros csatlakozása S0/1/01 és S0/1/0. Az internetszolgáltató kapcsolata S0/1/1. Az R 1 - R 2 hálózat 10.0.3.0/22 ​​és 2001:db8:acad:3::/64. Az R 2 hálózat 209.165.200.224/30 és 2001:db8:feed:224::/64 az internetszolgáltatónak. Az R 2 két gigabites csatlakozással rendelkezik a 3. (S 3) és a kapcsoló (S4) G0/0/0 és G/0/0/1 kapcsolójához. Az S 3 a 10.0.4.0/24 hálózat és a 2001:db8:acad:4::/64, amely a G0/0/0 R 2 interfészhez csatlakozik. Az S4 hálózat 10.0.5.0/24 és 2001:db8:acad:5::/64, amely a G0/0/1 R 2 interfészhez csatlakozik. A P C3 .10 és ::10 címmel csatlakozik az S 3-hoz. A P C4 0,10 és ::10 címmel csatlakozik az S4-hez. Az R1 és R2 átjárócímek .1-re és ::1-re végződnek. Az R1 és R2 közötti soros interfész R 1 .1 és ::1 és R 2 .2 és ::2 címekkel rendelkezik. Az R 2 és az ISP közötti kapcsolat .225 és .1 az ISP .226 és ::2 között. Az R1 és R2 forgalomirányítók dinamikus útválasztási protokollon keresztül osztanak meg minden változást a hálózaton, az R1-ből kiemelt négyzetekkel, amelyek azt jelzik, hogy megosztom R2-vel az összes hálózatot, amelyről tudok, és értesítem R2-t, ha bármilyen változás történik. Ugyanez vonatkozik az R2-re, amely az R1-et tájékoztatja.

PC1 PC2 PC3 PC4 S1 S2 S4 R1 R2 .10 .10 .10 .10 ::10 ::10 ::10 ::10 10.0.1.0/24 10.0.2.0/24 10.0.4.0/24 10.0.5.0/24 2001:db8:acad:1::/64 2001:db8:acad:2::/64 2001:db8:acad:4::/64 2001:db8:acad:5::/64 G0/0/0 G0/0/1 209.165.200.224/30 2001:db8:feed:224::/64 .1 ::1 .1 ::1 .225 ::1 .1 ::1 S0/1/1 S0/1/1 S3 ::2 10.0.3.0/24 S0/1/0 .2 G0/0/0 G0/0/1 .1 ::1 .1 ::1 ISP 2001:db8:acad:3::/64 .226 ::2

S0/1/1

Megosztom R2-vel az összes hálózatot, amelyről tudok, és szólok R2-nek, ha bármilyen változás történik. Megosztom R1-el az összes hálózatot, amelyről tudok, és szólok R1-nek, ha bármilyen változás történik. Internet

6.3.2

## Routing Protocol Spoofing

Az útválasztó rendszereket megtámadhatják a peer hálózati útválasztók megzavarása, vagy az útválasztási protokollokon belüli információk meghamisítása vagy hamisítása. A meghamisított útválasztási információk általában arra használhatók fel, hogy a rendszereket félretájékoztatják (hazudják) egymást, DoS támadást idézzenek elő, vagy a forgalmat olyan útvonalon kövessék, amelyet általában nem követne. Az útválasztási információk meghamisításának számos következménye van:

* Forgalom átirányítása útválasztási hurkok létrehozásához
* A forgalom átirányítása, hogy az egy nem biztonságos linken is megfigyelhető legyen
* A forgalom átirányítása az elvetéshez

Kattintson a Lejátszás gombra az animáción, ha egy támadásra szeretne példát látni, amely egy útválasztó hurkot hoz létre.

Tegyük fel, hogy egy támadó közvetlenül tudott csatlakozni az R1 és R2 közötti kapcsolathoz. A támadó R1 hamis útválasztási információkat küld, jelezve, hogy az R2 a preferált cél a 192.168.10.0/24 hálózatnak. Bár az R1-nek már van egy útválasztási táblázat bejegyzése a 192.168.10.0/24 hálózathoz, az új útvonalnak alacsonyabb a mérőszáma, ezért ez a preferált bejegyzés az útválasztási táblázatban.

Következésképpen, amikor a PC3 egy csomagot küld a PC1-nek (192.168.10.10/24), R3 továbbítja a csomagot R2-nek, amely viszont továbbítja azt R1-nek. Az R1 nem továbbítja a csomagot a PC1 gazdagépnek. Ehelyett a csomagot az R2-re irányítja, mert a 192.168.10.0 /24-hez a látszólag legjobb út az R2-n keresztül vezet. Amikor az R2 megkapja a csomagot, megnézi az útválasztási táblázatát, és megtalálja az R1-en keresztül a 192.168.10.0/24 hálózathoz vezető útvonalat, majd visszaküldi a csomagot az R1-nek, létrehozva a hurkot. A hurkot az R1-be fecskendezett téves információ okozta.

Az útválasztási protokollokat fenyegető általános fenyegetésekkel kapcsolatos további információkért keressen rá az interneten az RFC 4593 kifejezésre. Csökkentse az útválasztási protokoll támadásait az OSPF hitelesítés konfigurálásával.

Az ábra egy animáció, amely bemutatja, hogyan hozhat létre egy támadó útválasztási hurkot.

### A támadók manipulálhatják a nem hitelesített útválasztási frissítéseket

...de R2 jobban tudja, és visszaküldi a csomagot R1-nek, létrehozva egy hurkot.

Az R1-nek ide kellene továbbítania...

Címzett: 192.168.10.10

Az R1 frissíti az útválasztási táblát.

Tell R1: 192.168.10.10/24 elérhető az R2-n keresztül.

...de a támadó manipulálta R1 útválasztási információit, így R1 továbbítja R2-nek...

6.3.3

## OSPF MD5 Routing Protocol Authentication

Az OSPF támogatja az MD5 használatával történő útválasztási protokoll hitelesítést. Az MD5 hitelesítés globálisan engedélyezhető minden interfészre vagy interfészenként.

Az OSPF MD5 hitelesítés globális engedélyezése:

* **ip ospf message-digest-key** key **md5** jelszó interfész konfigurációs parancs.
* **terület** területazonosító **hitelesítés üzenet-kivonat** útválasztó konfigurációs parancs.
* Ez a módszer minden OSPF-kompatibilis interfészen hitelesítést kényszerít. Ha egy interfész nincs konfigurálva az **e ip ospf message-digest-key** paranccsal, akkor nem tud szomszédságokat kialakítani más OSPF szomszédokkal.

MD5 hitelesítés engedélyezése interfészenként:

* **ip ospf message-digest-key** key **md5** jelszó interfész konfigurációs parancs.
* **ip ospf hitelesítés üzenet-kivonat** interfész konfigurációs parancs.

Az interfész beállítása felülírja a globális beállítást. Az MD5 hitelesítési jelszavaknak nem kell azonosnak lenniük az egész területen. A szomszédok között azonban azonosnak kell lenniük.

Ezen az ábrán az R1 és R2 OSPF-fel van konfigurálva, és az útválasztás megfelelően működik. Az OSPF üzenetek azonban nincsenek hitelesítve vagy titkosítva.

Az ábrán két soros kapcsolaton keresztül csatlakoztatott router látható. Mindegyik router egy gigabites ethernet hálózathoz is csatlakozik.

### Az OSPF hitelesítés nélkül konfigurálva

R1 R2 G0/1 S/0/0/0 S/0/0/0

G0/1

R1# **show run | begin router ospf**

router ospf 1

passive-interface GigabitEthernet0/1

network 10.1.1.0 0.0.0.3 area 0

network 192.168.1.0 0.0.0.255 area 0

!

<output omitted>

!--------------------------------

R2# **show run | begin router ospf**

router ospf 1

passive-interface GigabitEthernet0/1

network 10.1.1.0 0.0.0.3 area 0

network 192.168.2.0 0.0.0.255 area 0

!

<output omitted>

Az alábbi ábrán az R1 és R2 OSPF MD5 hitelesítéssel vannak konfigurálva. A hitelesítés interfészenként van konfigurálva, mivel mindkét útválasztó csak egy interfészt használ az OSPF szomszédságainak kialakításához. Figyelje meg, hogy az R1 konfigurálásakor az OSPF szomszédság elveszik az R2-vel mindaddig, amíg az R2 nincs konfigurálva a megfelelő MD5 hitelesítéssel.

Az ábrán két soros kapcsolaton keresztül csatlakoztatott router látható. Mindegyik router egy gigabites ethernet hálózathoz is csatlakozik.

### OSPF MD5 hitelesítéssel konfigurálva

R1 R2 G0/1 S/0/0/0 S/0/0/0

G0/1

R1# **conf t**

R1(config)# **interface s0/0/0**

R1(config-if)# **ip ospf message-digest-key 1 md5 cisco12345**

R1(config-if)# **ip ospf authentication message-digest**

R1(config-if)#

000209: Feb 20 13:59:35.091 UTC: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.2 on

Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer expired

R1(config-if)#

000210: Feb 20 14:01:09.975 UTC: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.2 on

Serial0/0/0 from LOADING to FULL, Loading Done

----------------------------

R2# **conf t**

000137: Feb 20 13:59:35.091 UTC: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on

Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer expired

R2(config)# **interface s0/0/0**

R2(config-if)# **ip ospf message-digest-key 1 md5 cisco12345**

R2(config-if)# **ip ospf authentication message-digest**

R2(config-if)#

000138: Feb 20 14:01:09.975 UTC: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on

Serial0/0/0 from LOADING to FULL, Loading Done

R2(config-if)#

6.3.4

## OSPF SHA Routing Protocol Authentication

Az MD5 ma már sebezhetőnek számít a támadásokkal szemben, és csak akkor szabad használni, ha nem áll rendelkezésre erősebb hitelesítés. A Cisco IOS 15.4(1)T kiadása hozzáadta az OSPF SHA-hitelesítés támogatását, az RFC 5709 szerint. Ezért a rendszergazdának SHA-hitelesítést kell használnia mindaddig, amíg az összes útválasztó operációs rendszer támogatja az OSPF SHA hitelesítést.

Az OSPF SHA hitelesítés két fő lépésből áll. A parancsok szintaxisa az ábrán látható:

**1. lépés:** Adjon meg egy hitelesítési kulcsláncot globális konfigurációs módban:

* Állítsa be a kulcslánc nevét a **kulcslánc** paranccsal.
* Rendeljen a kulcstartóhoz egy számot és egy jelszót a **kulcs-** és **kulcskarakterlánc-** parancsokkal.
* Adja meg az SHA hitelesítést a **cryptographic-algoritm** paranccsal.
* (Opcionális) Adja meg, hogy ez a kulcs mikor jár le a **send-lifetime** paranccsal.

A parancsok szintaxisa a következő:

Router(config)#  **kulcslánc**  neve   
Router(config-keychain)#  **kulcs**  kulcs-azonosítója   
Router(config-keychain-key)#  **kulcs-**  karakterlánc   
Router(config-keychain-key)#  **cryptographic-algoritm**  {  **hmac-sha-1**  |  **hmac-sha-256**  |  **hmac-sha-384**  |  **hmac-sha-512**  |  **md5**  }   
Router(config-keychain-key)#  **send-lifetime start-time**  {  **végtelen**  |  **végidő**  |  **időtartam**  másodperc }

**2. lépés:** A következő szintaxis segítségével rendelje hozzá a hitelesítési kulcsot a kívánt interfészekhez az **ip ospf hitelesítési kulcslánc** paranccsal.

Router(config)#  **interfész**  típusszáma   
Router(config-if)#  **ip ospf hitelesítési kulcslánc**  neve

Az ábrát követő példában az R1 és R2 OSPF SHA hitelesítéssel van konfigurálva egy **SHA256** kulcskarakterlánc **kulcs és az ospfSHA256** használatával . Figyelje meg, hogy az R1 konfigurálásakor az OSPF szomszédság elveszik az R2-vel mindaddig, amíg az R2 nincs beállítva a megfelelő SHA-hitelesítéssel.

Az ábrán két soros kapcsolaton keresztül csatlakoztatott router látható. Mindegyik router egy gigabites ethernet hálózathoz is csatlakozik.

### OSPF SHA hitelesítéssel konfigurálva

R1 R2 G0/1 S/0/0/0 S/0/0/0

G0/1

R1(config)# **key chain SHA256**

R1(config-keychain)# **key 1**

R1(config-keychain-key)# **key-string ospfSHA256**

R1(config-keychain-key)# **cryptographic-algorithm hmac-sha-256**

R1(config-keychain-key)# **exit**

R1(config-keychain)# **exit**

R1(config)# **interface s0/0/0**

R1(config-if)# **ip ospf authentication key-chain SHA256**

R1(config-if)#

000218: Feb 20 15:06:07.607 UTC: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.2 on Serial0/0/0

from FULL to DOWN, Neighbor Down: Dead timer expired

R1(config-if)#

--------------------------------------

R2(config)# **key chain SHA256**

R2(config-keychain)# **key 1**

R2(config-keychain-key)# **key-string ospfSHA256**

R2(config-keychain-key)# **cryptographic-algorithm hmac-sha-256**

R2(config-keychain-key)# **exit**

R2(config-keychain)# **exit**

R2(config)# **interface s0/0/0**

R2(config-if)# **ip ospf authentication key-chain SHA256**

R2(config-if)#

000142: Feb 20 15:07:22.631: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0

from LOADING to FULL, Loading Done

R2(config-if)#

6.3.5

## Szintaxis-ellenőrző – OSPF SHA Routing Protocol Authentication

Ezzel a szintaktikai ellenőrzővel konfigurálhatja az OSPF hitelesítést az SHA 256 használatával.

To configure OSPF with SHA authentication, you must first configure a key chain:

* Issue the key chain command to create a key chain named **SHA256**.
* Assign the key chain number **1**
* Assign the **key-string** name of **ospfSHA256**.
* Assign **hmac-sha-256** as the **cryptographic-algorithm**.
* Enter **exit** twice to exit key chain configuration.

R1(config)#key chain SHA256

R1(config-keychain)#key 1

R1(config-keychain-key)#key-string ospfSHA256

R1(config-keychain-key)#cryptographic-algorithm hmac-sha-256

R1(config-keychain-key)#exit

R1(config-keychain)# kilépés

Lépjen be az interfész konfigurációs módjába, és rendelje hozzá az **SHA256 kulcsláncot** az OSPF hitelesítéshez az **S0/0/0** rendszeren .

R1(config)# interfész S0/0/0

R1(config-if)# ip ospf hitelesítési kulcslánc SHA256

R1(config-if)#

\*Március 1. 16:52:26.615: %OSPF-5-ADJCHG: 1. folyamat, 10.2.2.2, Serial0/0/0, BETÖLTÉStől TELJES állapotig, Betöltés kész

adja ki az **end parancsot.** A konfigurációs módból való kilépéshez

R1(config-if)# vége

R1#

Sikeresen konfigurálta az NTP-hitelesítést az R1-en.

6.3.6

### Lab – Alapvető eszközkonfiguráció és OSPF hitelesítés

Ebben a laborban a következő célokat kell teljesítenie:

* 1. rész: Az alapvető eszközbeállítások konfigurálása.
* 2. rész: Rögzítse a vezérlősíkot.

6.3.7

### Packet Tracer – OSPF hitelesítés konfigurálása

Ebben a Packet Tracer tevékenységben konfigurálja az OSPF MD5 hitelesítést.

[Konfigurálja az OSPF hitelesítést](https://contenthub.netacad.com/courses/netsec/_common/6.3.7-packet-tracer---configure-ospf-authentication.pka)

[6.2](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Lock Down a Router Using AutoSecure](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[6.4](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Secure Management and Reporting](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                                                
*                               

1. Device Monitoring and Management
2. Secure Management and Reporting

# Biztonságos menedzsment és jelentéskészítés

6.4.1

## A felügyeleti hozzáférés típusai

Kis hálózatban kis számú hálózati eszköz kezelése és felügyelete egyszerű művelet. Egy több száz eszközzel rendelkező nagyvállalatnál azonban a naplóüzenetek figyelése, kezelése és feldolgozása kihívást jelenthet. Jelentési szempontból a legtöbb hálózati eszköz képes naplóadatokat küldeni, amelyek felbecsülhetetlen értékűek lehetnek a hálózati problémák vagy biztonsági fenyegetések hibaelhárítása során. Ezek az adatok valós időben, igény szerint és ütemezett jelentésekben is megtekinthetők.

Az információk naplózásakor és kezelésekor a felügyeleti gazdagépek és a felügyelt eszközök közötti információáramlás két úton haladhat:

* **In-band** – Az információ egy vállalati termelési hálózaton, az interneten vagy mindkettőn keresztül áramlik rendszeres adatcsatornákon keresztül.
* **Sávon kívüli (OOB)** – Információáramlás egy dedikált felügyeleti hálózaton, amelyen nincs termelési forgalom.

Például az ábrán látható hálózatnak két hálózati szegmense van, amelyeket egy Cisco IOS útválasztó választ el, amely tűzfalszolgáltatásokat nyújt a felügyeleti hálózat védelmére. Az éles hálózathoz való csatlakozás lehetővé teszi a felügyeleti gazdagépek számára az internet elérését, és korlátozott sávon belüli felügyeleti forgalmat biztosít. A sávon belüli kezelés csak akkor történik meg, ha az OOB-kezelés nem lehetséges vagy nem elérhető. Ha sávon belüli felügyeletre van szükség, akkor ezt a forgalmat biztonságosan kell továbbítani privát titkosított alagút vagy VPN alagút segítségével.

Az ábra a sávon belüli kezelést szemlélteti.

### In-Band Management

Termelési hálózat Védett felügyeleti hálózat   
(Tűzfal mögött) Az Ethernet-kapcsolaton keresztül az eszközökre/eszközökről küldött konfigurációs és kezelési forgalom sávon belüli konfigurációkezelés. Állapotalapú csomagszűrés és titkosítás szükséges.

Az alábbi ábra a védett felügyeleti hálózat részleteit mutatja be. Itt találhatók a felügyeleti hosztok és terminálkiszolgálók. A felügyeleti hálózatba helyezve a terminálkiszolgálók közvetlen OOB konzolkapcsolatot kínálnak a felügyeleti hálózaton keresztül bármely olyan hálózati eszközhöz, amely felügyeletet igényel az éles hálózaton. A legtöbb eszközt ehhez a felügyeleti szegmenshez kell csatlakoztatni, és az OOB-kezeléssel kell konfigurálni.

Mivel a felügyeleti hálózat adminisztrátori hozzáféréssel rendelkezik a hálózat szinte minden területéhez, nagyon vonzó célpont lehet a hackerek számára. A tűzfal felügyeleti modulja számos olyan technológiát tartalmaz, amelyek célja az ilyen kockázatok csökkentése. Az elsődleges fenyegetés egy hacker, aki megpróbál hozzáférni a felügyeleti hálózathoz. Ez egy olyan feltört felügyelt gazdagépen keresztül valósítható meg, amelyhez a felügyeleti eszköznek hozzá kell férnie. A feltört eszközök veszélyének csökkentése érdekében erős hozzáférés-szabályozást kell megvalósítani a tűzfalon és minden más eszközön. A felügyeleti eszközöket úgy kell beállítani, hogy külön LAN-szegmensek vagy VLAN-ok használatával megakadályozzák a közvetlen kommunikációt ugyanazon a felügyeleti alhálózaton lévő többi gazdagéppel.

Az ábra a sávon kívüli kezelést szemlélteti.

### Sávon kívüli menedzsment

SNMP-kiszolgáló hozzáférés-vezérlése kiszolgáló rendszergazdai védett felügyeleti hálózat   
(Tűzfal mögött) Terminálkiszolgáló Cisco IOS tűzfal VPN-sel az összes eszköz konzolportjához A konzolporton keresztül az eszközökre/eszközökről küldött konfigurációs és kezelési forgalom OOB konfigurációkezelés.

6.4.2

## Sávon kívüli és sávon belüli hozzáférés

Általános szabály, hogy biztonsági okokból az OOB-kezelés megfelelő a nagyvállalati hálózatokhoz. Ez azonban nem mindig kívánatos. Az OOB-kezelés használatára vonatkozó döntés a futó felügyeleti alkalmazások típusától és a megfigyelt protokolloktól függ. Vegyünk például egy olyan helyzetet, amelyben két központi kapcsolót kezelnek és figyelnek OOB-hálózaton keresztül. Ha a két magkapcsoló közötti kritikus kapcsolat meghibásodik az éles hálózaton, előfordulhat, hogy az eszközöket figyelő alkalmazás soha nem állapítja meg, hogy a kapcsolat meghiúsult, és soha nem figyelmezteti a rendszergazdát. Ennek az az oka, hogy az OOB-hálózat úgy tűnik, hogy az összes eszköz egyetlen OOB-felügyeleti hálózathoz csatlakozik. Az OOB-felügyeleti hálózatot nem érinti a lekapcsolt kapcsolat. Az ilyen felügyeleti alkalmazásoknál előnyösebb a sávon belüli, biztonságos módon futtatni a felügyeleti alkalmazást.

Az OOB kezelési irányelvei a következők:

* Biztosítsa a legmagasabb szintű biztonságot.
* Csökkentse a nem biztonságos felügyeleti protokollok termelési hálózaton való átadásának kockázatát.

A sávon belüli felügyelet javasolt kisebb hálózatokban a költséghatékonyabb biztonsági telepítés elérése érdekében. Az ilyen architektúrákban a felügyeleti forgalom minden esetben sávon belül folyik. A lehető legbiztonságosabbá teszik biztonságos felügyeleti protokollok használatával, például Telnet helyett SSH használatával. Egy másik lehetőség biztonságos alagutak létrehozása olyan protokollok használatával, mint az IPsec a forgalomkezeléshez. Ha a felügyeleti hozzáférés nem mindig szükséges, ideiglenes lyukak helyezhetők el a tűzfalban, amíg a felügyeleti funkciókat végrehajtják. Ezt a technikát óvatosan kell használni, és minden lyukat azonnal be kell zárni, amikor a kezelési funkciók befejeződtek.

A sávon belüli kezelési irányelvek a következők:

* Csak azokra az eszközökre vonatkozik, amelyeket felügyelni vagy felügyelni kell.
* Ha lehetséges, használjon IPsec-et, SSH-t vagy SSL-t.
* Döntse el, hogy a felügyeleti csatornának mindig nyitva kell-e lennie.

Végül, ha távoli felügyeleti eszközöket használ sávon belüli kezeléssel, legyen óvatos magának a felügyeleti eszköznek a mögöttes biztonsági réseivel szemben. Az SNMP-kezelőket például gyakran használják a hibaelhárítási és konfigurációs feladatok megkönnyítésére a hálózaton. Az SNMP-vel azonban a legnagyobb körültekintéssel kell bánni, mivel az alapul szolgáló protokollnak saját biztonsági rései vannak.

[6.3](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Routing Protocol Authentication](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[6.5](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Network Security Using Syslog](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                                                      
*                               

1. Device Monitoring and Management
2. Network Security Using Syslog

# Hálózati biztonság Syslog használatával

6.5.1

## Bevezetés a Syslogba

Mint egy Check Engine jelzőfény az autó műszerfalán, a hálózatban lévő alkatrészek jelezhetik, ha valami nincs rendben. A syslog protokollt úgy tervezték, hogy biztosítsa az üzenetek fogadását és megértését. Amikor bizonyos események történnek a hálózaton, a hálózati eszközök megbízható mechanizmusokkal értesítik a rendszergazdát részletes rendszerüzenetekkel. Ezek az üzenetek lehetnek nem kritikusak vagy jelentősek. A hálózati rendszergazdáknak számos lehetőségük van ezen üzenetek tárolására, értelmezésére és megjelenítésére. Azokra az üzenetekre is figyelmeztethetők, amelyek a legnagyobb hatással lehetnek a hálózati infrastruktúrára.

A rendszerüzenetek elérésének legáltalánosabb módja a syslog nevű protokoll használata.

A Syslog egy szabvány leírására használt kifejezés. Ezt a szabványhoz kifejlesztett protokoll leírására is használják. A syslog protokollt UNIX rendszerekre fejlesztették ki az 1980-as években, de először RFC 3164 néven dokumentálta az IETF 2001-ben.

Számos hálózati eszköz támogatja a rendszernaplózást, beleértve az útválasztókat, kapcsolókat, alkalmazásszervereket, tűzfalakat és egyéb hálózati eszközöket. A syslog protokoll lehetővé teszi, hogy a hálózati eszközök rendszerüzeneteiket a hálózaton keresztül elküldjék a rendszernapló-kiszolgálóknak.

Pontosabban, a syslog az 514-es UDP-portot használja az eseményértesítési üzenetek IP-hálózatokon keresztül történő küldésére az eseményüzenet-gyűjtőknek. Az ábrán például egy útválasztó (R1) és egy kapcsoló (S1) látható, amelyek rendszerüzeneteket küldenek egy rendszernapló-szervernek.

Az ábrán egy R 1 jelzésű útválasztó és egy S 1 feliratú kapcsoló látható, amelyek rendszerüzeneteket küldenek egy syslog szervernek.

R1

S1

Syslog Server rendszerüzenetek Rendszerüzenetek

Számos rendszernapló-kiszolgáló szoftvercsomag érhető el Windows és UNIX rendszerhez. Sok közülük ingyenes.

A syslog naplózási szolgáltatás három elsődleges funkciót biztosít, az alábbiak szerint:

* Naplózási információk gyűjtésének képessége megfigyelés és hibaelhárítás céljából
* A rögzített naplózási információk típusának kiválasztásának lehetősége
* Lehetőség a rögzített rendszernapló-üzenetek célhelyeinek megadására

6.5.2

## Syslog művelet

A Cisco hálózati eszközökön a syslog protokoll rendszerüzenetek és **hibakeresési** kimenet elküldésével indul az eszközön belüli helyi naplózási folyamatnak. Az, hogy a naplózási folyamat hogyan kezeli ezeket az üzeneteket és kimeneteket, az eszközkonfigurációkon alapul. Például rendszernapló-üzenetek küldhetők a hálózaton keresztül egy külső rendszernapló-kiszolgálóra. A syslog szerveren lévő üzenetek ezután szűrhetők anélkül, hogy hozzá kellene férniük a tényleges eszközhöz. A külső szerveren tárolt naplóüzenetek és kimenetek különféle jelentésekbe húzhatók a könnyebb olvashatóság érdekében.

Alternatív megoldásként a syslog üzenetek elküldhetők egy belső pufferbe. A belső pufferbe küldött üzenetek csak az eszköz CLI-jén keresztül tekinthetők meg.

Végül a hálózati adminisztrátor megadhatja, hogy csak bizonyos típusú rendszerüzenetek kerüljenek elküldésre különböző célállomásokra. Például az eszköz beállítható úgy, hogy az összes rendszerüzenetet továbbítsa egy külső rendszernapló-kiszolgálónak. A hibakeresési szintű üzeneteket azonban a rendszer a belső pufferbe továbbítja, és csak a rendszergazda érheti el a parancssori felületről.

Amint az ábrán látható, a rendszernapló-üzenetek népszerű célállomásai a következők:

* Naplózási puffer (RAM egy útválasztón vagy kapcsolón belül)
* Konzol vonal
* Végállomás vonal
* Syslog szerver

Az ábra a syslog üzenetek népszerű célhelyeit mutatja be. A kapcsolókon nyilak mutatnak egy naplózási pufferre, egy Console-vonallal ellátott PC-re, egy másik terminálvonal-nevű PC-re és egy rendszernapló-kiszolgálóra.

Naplózási puffer konzolvonal terminálvonal Syslog Server

Lehetőség van a rendszerüzenetek távoli megfigyelésére a naplók megtekintésével egy syslog szerveren, vagy ha Telneten, SSH-n vagy a konzolporton keresztül hozzáfér az eszközhöz.

6.5.3

## Syslog üzenetformátum

A Cisco eszközök rendszernapló-üzeneteket állítanak elő a hálózati események eredményeként. Minden rendszernapló-üzenet tartalmaz egy súlyossági szintet és egy szolgáltatást.

A kisebb numerikus szintek a kritikusabb rendszernapló-riasztások. Az üzenetek súlyossági szintje beállítható annak szabályozására, hogy az egyes üzenettípusok hol jelenjenek meg (pl. a konzolon vagy a többi célállomáson). A syslog szintek teljes listája a táblázatban látható.

| **Súlyosság neve** | **Súlyossági szám** | **Leírás** |
| --- | --- | --- |
| Vészhelyzet | 0. szint | A rendszer használhatatlan |
| Éber | 1. szint | Azonnali intézkedés szükséges |
| Kritikai | 2. szint | Kritikus állapotban |
| Hiba | 3. szint | Hiba állapota |
| Figyelem | 4. szint | Figyelmeztető állapot |
| Értesítés | 5. szint | Normál, de jelentős állapot |
| Tájékoztató | 6. szint | Tájékoztató üzenet |
| Hibakeresés | 7. szint | Hibakeresési üzenet |

Minden syslog szintnek megvan a maga jelentése:

* **0. vészhelyzeti szint – 4. figyelmeztetési szint** : Ezek az üzenetek szoftver- vagy hardverhibákra vonatkozó hibaüzenetek; az ilyen típusú üzenetek azt jelentik, hogy az eszköz működését érinti. A probléma súlyossága határozza meg az alkalmazott rendszernapló tényleges szintjét.
* **5. értesítési szint** : Ez az értesítési szint normál, de jelentős eseményekre vonatkozik. Például az interfész felfelé vagy lefelé történő átmenetei, valamint a rendszer újraindítási üzenetei az értesítések szintjén jelennek meg.
* **6. információs szint** : Ez egy normál információs üzenet, amely nem befolyásolja az eszköz működését. Például, amikor egy Cisco-eszköz elindul, a következő tájékoztató üzenet jelenhet meg: %LICENSE-6-EULA \_ ACCEPT \_ ALL: A végfelhasználói licencszerződést elfogadták.
* **7. hibakeresési szint** parancsok kiadásából jönnek létre **: Ez a szint azt jelzi, hogy az üzenetek különböző hibakeresési** .

6.5.4

## Syslog létesítmények

A rendszernapló-üzenetek a súlyosság megadása mellett a létesítményre vonatkozó információkat is tartalmaznak. A Syslog létesítmények olyan szolgáltatásazonosítók, amelyek azonosítják és kategorizálják a rendszerállapot-adatokat a hiba- és eseményüzenetek jelentéséhez. A rendelkezésre álló naplózási lehetőség a hálózati eszközre jellemző. Például a Cisco IOS Release 15.0(2) verzióját futtató Cisco 2960 Series switchek és a Cisco IOS 15.2(4) kiadását futtató Cisco 1941 routerek 24 létesítménybeállítást támogatnak, amelyek 12 létesítménytípusba sorolhatók.

A Cisco IOS útválasztókon jelentett néhány gyakori rendszernapló-üzenet-szolgáltatási kód:

* **IF** – Azonosítja, hogy a rendszernapló-üzenetet egy interfész hozta létre.
* **IP** – Azonosítja, hogy a rendszernapló-üzenetet az IP hozta létre.
* **OSPF** – Azonosítja, hogy a rendszernapló-üzenetet az OSPF útválasztási protokoll hozta létre.
* **SYS** – Azonosítja, hogy a rendszernapló-üzenetet az eszköz operációs rendszere hozta létre.
* **IPSEC** – Azonosítja, hogy a rendszernapló-üzenetet az IP Security titkosítási protokoll hozta létre.

Alapértelmezés szerint a rendszernapló-üzenetek formátuma a Cisco IOS szoftverben a következő:

%facility-severity-MNEMONIC: description

Például egy Cisco kapcsoló mintakimenete az EtherChannel kapcsolat állapotának felfelé történő módosításához a következő:

%LINK-3-UPDOWN: Interface Port-channel1, changed state to up

Itt a létesítmény LINK és a súlyossági szint 3, a MNEMONIC FELFELÉ.

A leggyakoribb üzenetek a link fel és le üzenetek, valamint azok az üzenetek, amelyeket az eszköz a konfigurációs módból való kilépéskor produkál. Ha az ACL-naplózás be van állítva, az eszköz rendszernapló-üzeneteket generál, ha a csomagok megfelelnek egy paraméterfeltételnek.

6.5.5

## Konfigurálja a Syslog időbélyegeit

Alapértelmezés szerint a naplóüzenetek nincsenek időbélyegzővel ellátva. A példában az R1 GigabitEthernet 0/0/0 interfész le van állítva. A konzolra naplózott üzenet nem azonosítja, hogy mikor módosult az interfész állapota. A naplóüzeneteket időbélyeggel kell ellátni, hogy amikor egy másik célhelyre, például egy Syslog-kiszolgálóra küldik, rögzítésre kerüljön az üzenet létrehozásának időpontja.

A **szolgáltatás időbélyegei log datetime** paranccsal kényszerítheti a naplózott eseményeket a dátum és az idő megjelenítésére. Ahogy a parancskimeneten látható, az R1 GigabitEthernet 0/0/0 interfész újraaktiválásakor a naplóüzenetek a dátumot és az időt is tartalmazzák.

R1# **configure terminal**

R1(config)# **interface g0/0/0**

R1(config-if)# **shutdown**

%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to down

R1(config-if)# **exit**

R1(config)# **service timestamps log datetime**

R1(config)# **interface g0/0/0**

R1(config-if)# **no shutdown**

\*Mar 1 11:52:42: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to down

\*Mar 1 11:52:45: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to up

\*Mar 1 11:52:46: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0,

changed state to up

R1(config-if)#

**Megjegyzés** kulcsszó használatakor **: A datetime** a hálózati eszköz óráját manuálisan vagy NTP-n keresztül be kell állítani, amint azt korábban tárgyaltuk.

6.5.6

## Ellenőrizze, hogy megértette-e a Syslog működését

A kérdések megválaszolásához tekintse meg a következő syslog kimenetet.

\*Jun 12 17:46:01.619: %IFMGR-7-NO\_IFINDEX\_FILE: Unable to open nvram:/ifIndex-table No such file or directory

Az űrlap teteje

1. **Lásd a syslog kimenetet.** Milyen biztonsági szint generálta az üzenetet?

Az űrlap alja

**Lásd a syslog kimenetet.** Mi ennek a syslog-üzenetnek a megjegyzése?

**Lásd a syslog kimenetet.** Mi az a syslog jelentéskészítő szolgáltatás?

6.5.7

## Syslog Systems

A syslog implementációk mindig kétféle rendszert tartalmaznak:

* **Syslog szerverek** – Más néven naplógazdagépek, ezek a rendszerek elfogadják és feldolgozzák a syslog kliensek naplóüzeneteit.
* **Syslog-kliensek** – Útválasztók vagy más típusú berendezések, amelyek naplóüzeneteket generálnak és továbbítanak a rendszernapló-kiszolgálóknak.

Az ábrán látható topológia a 10.2.2.6 IP-címen azonosítja a syslog szervert. A topológia többi kiszolgálója és eszköze syslog kliensként konfigurálható, amelyek syslog üzeneteket küldenek a syslog szervernek.

Az ábra egy syslog topológiát mutat.

### Syslog referencia topológia

R1 G0/1 10.2.2.1 G0/2 10.2.3.1 209.165.200.225/29

G0/0

Nyilvános web   
szerver   
10.2.2.3 Levelezőszerver   
10.2.2.4 FTP/webszerver 10.2.3.2 Felhasználó   
10.2.3.3 Syslog Server   
(naplógazda)   
10.2.2.6 Syslog Client DMZ LAN 10.2.2.0/24 Védett LAN   
10.2.3.0/24

6.5.8

## Syslog konfiguráció

Rendszernaplózás konfigurálása:

**1. lépés** . Állítsa be a cél naplózási gazdagépet a **naplózás** [ **host** ] paranccsal.   
**2. lépés** . (Opcionális) Állítsa be a naplózás súlyosságának (csapda) szintjét a **naplózási csapda** paranccsal.   
**3. lépés** . (Opcionális) Állítsa be a forrásfelületet a **naplózási forrás-interfész** paranccsal.   
**4. lépés** . (Opcionális) Engedélyezze a naplózást az összes engedélyezett célnál a **bejelentkezési** paranccsal.

Kattintson az alábbiakra, ha többet szeretne megtudni a rendszernaplózás beállításának lépéseiről.

Azonosítsa a célrendszernapló-kiszolgálót a **naplózási hoszt** paranccsal

| **Paraméter** | **Leírás** |
| --- | --- |
| gazdagépnév | Megadja a rendszernaplószerverként használni kívánt gazdagép nevét. |
| IP-cím | Megadja a rendszernaplószerverként használni kívánt gazdagép IP-címét. |

Router(config)# **logging host** [hostname | ip-address]

(Opcionális) Állítsa be a naplózás súlyosságának (csapda) szintjét a **naplózási csapda** paranccsal

**Megjegyzés:** Az ISR alapértelmezése a 7. szint (hibakeresés).

Router(config)# **logging trap** level

(Opcionális) Állítsa be a forrásfelületet a **naplózási forrás-interfész** paranccsal. Ez a parancs azt határozza meg, hogy a syslog-csomagok egy adott interfész (pl. visszacsatolási interfész) IPv4- vagy IPv6-címét tartalmazzák, függetlenül attól, hogy a csomag melyik interfészt használja az útválasztóból való kilépéshez.

| **Paraméter** | **Leírás** |
| --- | --- |
| *interfész típusú* | Meghatározza az interfész típusát. |
| *interfész-szám* | Megadja az interfész számát (például 0/1). |

Router(config)# **logging source-interface** *interface-type* *interface-number*

(Opcionális) Engedélyezze a naplózást az összes engedélyezett célnál a **bejelentkezési** paranccsal.

**Megjegyzés:** A Syslog naplózás alapértelmezés szerint engedélyezve van.

Router(config)# **logging on**

Az ábra a syslog hivatkozási topológiát mutatja.

Ez az oldal egy interaktív tevékenységet tartalmaz, melynek címe: Fiber a legjobb választás.

R1 G0/1 10.2.2.1 G0/2 10.2.3.1 209.165.200.225/29

G0/0

Nyilvános web   
szerver   
10.2.2.3 Levelezőszerver   
10.2.2.4 FTP/webszerver 10.2.3.2 Felhasználó   
10.2.3.3 Syslog Server   
(naplógazda)   
10.2.2.6 Syslog   
Kliens DMZ LAN 10.2.2.0/24 Védett LAN   
10.2.3.0/24

Az alábbi ábra az R1 rendszernapló-konfigurációjának mintáját mutatja. használja a **show logging parancsot.** A naplózási konfiguráció és a pufferelt rendszernapló-üzenetek megtekintéséhez

### Minta Syslog konfiguráció

R1(config)# **logging 10.2.2.6**

R1(config)#

\*Sep 25 12:57:14.120: %SYS-6-LOGGINGHOST\_STARTSTOP: Logging to host 10.2.2.6 port 514 started - CLI initiated

R1(config)#

R1(config)# **logging trap informational**

R1(config)# **logging source-interface lo0**

R1(config)# **logging on**

R1(config)# **exit**

R1#

\*Sep 25 12:58:29.591: %SYS-5-CONFIG\_I: Configured from console by console

R1#

R1# **show logging**

Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushes, 0 overruns, xml disabled, filtering disabled)

<Output omitted>

Trap logging: level informational, 83 message lines logged

Logging to 10.2.2.6 (udp port 514, audit disabled,

link up),

7 message lines logged,

0 message lines rate-limited,

0 message lines dropped-by-MD,

xml disabled, sequence number disabled

filtering disabled

Logging Source-Interface: VRF Name:

Loopback0

<Output omitted>

[6.4](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Secure Management and Reporting](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[6.6](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[NTP Configuration](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                                                        
*                               

1. Device Monitoring and Management
2. NTP Configuration

# NTP konfiguráció

6.6.1

## Idő és naptár szolgáltatások

Mielőtt igazán belemerülne a hálózatkezelésbe, az egyetlen dolog, ami segít a pályán maradni, az az, hogy minden összetevője azonos időpontra és dátumra van állítva.

Az útválasztón vagy kapcsolón a szoftveróra elindul, amikor a rendszer elindul. Ez az elsődleges időforrás a rendszer számára. Fontos az idő szinkronizálása a hálózat összes eszközén, mert a hálózatok kezelésének, biztonságának, hibaelhárításának és tervezésének minden vonatkozása pontos időbélyegzést igényel. Ha az idő nincs szinkronizálva az eszközök között, lehetetlen lesz meghatározni az események sorrendjét és az esemény okát.

Az útválasztón vagy kapcsolón a dátum és idő beállításai manuálisan konfigurálhatók, a példában látható módon.

R1# **clock set 16:01:00 sept 25 2020**

\*Sep 25 16:01:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 13:09:49 UTC Fri Sep 25 2020 to 16:01:00 UTC Fri Sep 25 2020, configured from console by console.

Sep 25 16:01:00.001: %PKI-6-AUTHORITATIVE\_CLOCK: The system clock has been set.

R1#

Bár az idő kézi beállítása egyszerű, a legtöbb hálózatban nem praktikus. A hálózat növekedésével nehéz, ha nem lehetetlen biztosítani, hogy minden infrastruktúra-eszköz szinkronizált időben működjön. Még kisebb hálózati környezetben sem ideális a manuális módszer. Ha egy router újraindul, hogyan kap pontos dátumot és időbélyeget?

Egy jobb és skálázhatóbb megoldás az RFC 1305-ben dokumentált Network Time Protocol (NTP) megvalósítása. Az NTP lehetővé teszi a hálózati eszközöknek (azaz az NTP-klienseknek), hogy szinkronizálják időbeállításaikat egy mérvadó NTP időforrással, például egy NTP-kiszolgálóval. Az NTP időforrás lehet egy olyan eszköz (pl. útválasztó) a hálózaton, amely privát elsődleges óraként van kiválasztva, vagy lehet egy nyilvánosan elérhető NTP-szerver az interneten.

Az NTP-forrás és a kliensek megnyitják a 123-as UDP-portot az időbélyegek küldéséhez és fogadásához.

6.6.2

## NTP művelet

Az NTP-hálózatok az időforrások hierarchikus rendszerét használják. Ebben a hierarchikus rendszerben minden szintet rétegnek nevezünk. A rétegszint a mérvadó forrásból származó ugrások száma.

Az ábra egy minta NTP-hálózatot jelenít meg.

Az ábra egy minta Network Time Protocol (NTP) hálózatot jelenít meg. Az NTP-kiszolgálók három szinten vannak elrendezve, amelyek a három réteget mutatják. Az 1. réteg a Stratum 0 óráihoz kapcsolódik. A 0. réteg két NTP órából áll. Az NTP órák 2 Stratum 1 NTP szerverhez csatlakoznak. A Stratum 1 NTP szerverek 3 Stratum 2 NTP szerverhez csatlakoznak. A Stratum 2 NTP szerverek 4 Stratum 3 NTP szerverhez csatlakoznak.

0. réteg 1. réteg 3. réteg 2. réteg

A mintahálózat négy rétegszintből áll, amelyek a következőképpen szerzik meg idejüket:

* A Stratum 1 szerver az idejét a 0. réteg időforrásától kapja.
* A Stratum 2 szerver az idejét a Stratum 1 szervertől kapja.
* A Stratum 3 szerver az idejét a stratum 2 szervertől kapja.

**0. réteg**

Ez azonosítja azt az eszközt, amely a legmegbízhatóbb időforrást biztosítja. A Stratum 0 eszközök, beleértve az atom- és GPS-órákat, a legpontosabb mérvadó időforrások.

Pontosabban, az NTP stratum 0 eszközök nem hálózati nagy pontosságú időmérő eszközök, amelyekről feltételezik, hogy pontosak, és kis késéssel vagy semmilyen késleltetéssel nem járnak hozzájuk. Az ábrán ezeket az óra ikon jelöli.

**1. réteg**

Az NTP stratum 1 eszközök olyan hálózati eszközök, amelyek közvetlenül csatlakoznak a mérvadó időforrásokhoz. A 2. rétegű eszközök elsődleges hálózati időszabványaként működnek.

**2. réteg és alsó**

Az NTP stratum 2 szerverek hálózaton csatlakoznak egy stratum 1 eszközhöz. A Stratum 2 eszközök NTP-kliensek, és idejüket egy stratum 1-szerver, például egy útválasztó NTP-csomagjaival szinkronizálják. Ezek viszont NTP-kiszolgálók lehetnek a 3. rétegű eszközökhöz.

Az NTP rétegszintek egy 0-tól (legmagasabb rétegszint) 15-ig (legalacsonyabb rétegszint) terjedő skálán alapulnak. Például egy alacsony számú rétegszinten lévő NTP-kiszolgáló közelebb van az engedélyezett időforráshoz, mint egy magas rétegszintű kiszolgáló.

A maximális rétegugrások száma 15 (azaz 0-15). Ne feledje, hogy a kiszolgálóval nem szinkronizált NTP-kliensek 16. rétegszinttel rendelkeznek.

Az azonos rétegszinten lévő NTP-kiszolgálók peer-ként konfigurálhatók, hogy redundáns időforrásokat biztosítsanak az ügyfelek számára, vagy szinkronizálják egymást.

6.6.3

## Konfigurálja és ellenőrizze az NTP-t

Az ábra az NTP konfigurációjának és ellenőrzésének bemutatására használt topológiát mutatja.

Az ábra egy topológiát mutat be, amely az NTP konfigurációját és ellenőrzését mutatja be. Egy NTP-szerver a felhőben (Internet) található 209.165.200.225 IP-címmel. Az R1 útválasztó NTP-kiszolgálóként/kliensként van megjelölve, és a felhőre mutató hivatkozással rendelkezik. Az R1 IP-címe 192.168.1.0/24. Az R 1 egy S 1 kapcsolóhoz is csatlakozik, amelyet szintén NTP szervernek/kliensnek neveznek. Az S 1-nek linkelnie kell az NTP-kliensekre, amelyek két emberként jelennek meg a számítógép asztalánál.

R1 S1 209.165.200.225

192.168.1.0/24



NTP kliensek NTP szerver / kliens NTP szerver / kliens Internet NTP szerver

Az NTP hálózaton történő konfigurálása előtt a **show clock** parancs megjeleníti az aktuális időt a szoftver óráján, ahogy az a példában is látható. A **részletes** beállításnál figyelje meg, hogy az időforrás a felhasználói konfiguráció. Ez azt jelenti, hogy az idő manuálisan lett beállítva az **óra** paranccsal.

R1# **show clock detail**

20:55:10.207 UTC Fri Nov 15 2019

Time source is user configuration

Topológiánkban az internetes NTP szerver a mérvadó időforrás. Mindazonáltal a helyi hálózati eszköz kiválasztható mérvadó NTP időforrásként az **ntp master** [ stratum ] globális konfigurációs paranccsal.

A topológiában az R1 az NTP-kiszolgáló NTP-kliense. Az **ntp server** ip-address global config paranccsal állítsa be a 209.165.200.225-öt az R1 NTP-kiszolgálójaként.

Ha ellenőrizni szeretné, hogy az időforrás NTP-re van állítva, használja a **show clock details** parancsot. Figyeljük meg, hogy most az időforrás az NTP.

R1(config)# **ntp server 209.165.200.225**

R1(config)# **end**

R1# **show clock detail**

21:01:34.563 UTC Fri Nov 15 2019

Time source is NTP

A következő példában a **show ntp asszociációk** és **a show ntp status** parancsok használatosak annak ellenőrzésére, hogy az R1 szinkronizálva van-e a 209.165.200.225 számú NTP-kiszolgálóval. Figyelje meg, hogy az R1 szinkronizálva van a 209.165.200.225-ös stratum 1 NTP-kiszolgálóval, amely szinkronizálva van egy GPS-órával. A **show ntp status** parancs megjeleníti, hogy az R1 most egy réteg 2 eszköz, amely szinkronizálva van a 209.165.220.225 számú NTP-kiszolgálóval.

**Megjegyzés** : A kiemelt **st** a réteget jelenti.

R1# **show ntp associations**

address ref clock st when poll reach delay offset disp

\*~209.165.200.225 .GPS. 1 61 64 377 0.481 7.480 4.261

\* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

R1# **show ntp status**

Clock is synchronized, stratum 2, reference is 209.165.200.225

nominal freq is 250.0000 Hz, actual freq is 249.9995 Hz, precision is 2\*\*19

ntp uptime is 589900 (1/100 of seconds), resolution is 4016

reference time is DA088DD3.C4E659D3 (13:21:23.769 PST Fri Nov 15 2019)

clock offset is 7.0883 msec, root delay is 99.77 msec

root dispersion is 13.43 msec, peer dispersion is 2.48 msec

loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000001803 s/s

system poll interval is 64, last update was 169 sec ago.

Ezután az S1 órája úgy van konfigurálva, hogy szinkronizálja az R1-et az **ntp server** paranccsal ellenőrzi **paranccsal, majd a konfigurációt a show ntp Associations** , ahogy a kijelzőn látható.

S1(config)# **ntp server 192.168.1.1**

S1(config)# **end**

S1# **show ntp associations**

address ref clock st when poll reach delay offset disp

\*~192.168.1.1 209.165.200.225 2 12 64 377 1.066 13.616 3.840

\* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

parancs kimenete **A show ntp Associations** ellenőrzi, hogy az S1 órája most szinkronizálva van-e az R1-gyel a 192.168.1.1-nél NTP-n keresztül. Az R1 egy stratum 2 eszköz és NTP-kiszolgáló az S1-hez. Az S1 most egy 3. rétegű eszköz, amely NTP-szolgáltatást tud nyújtani a hálózat többi eszközének, például végberendezéseknek.

S1# **show ntp status**

Clock is synchronized, stratum 3, reference is 192.168.1.1

nominal freq is 119.2092 Hz, actual freq is 119.2088 Hz, precision is 2\*\*17

reference time is DA08904B.3269C655 (13:31:55.196 PST Tue Nov 15 2019)

clock offset is 18.7764 msec, root delay is 102.42 msec

root dispersion is 38.03 msec, peer dispersion is 3.74 msec

loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000003925 s/s

system poll interval is 128, last update was 178 sec ago.

6.6.4

## Packet Tracer – NTP konfigurálása és ellenőrzése

Az NTP szinkronizálja a napszakot az elosztott időkiszolgálók és kliensek között. Noha számos alkalmazás igényel szinkronizált időt, ez a labor a rendszernaplókban felsorolt ​​események és más, több hálózati eszközről származó időspecifikus események korrelációjának szükségességére összpontosít.

[Konfigurálja és ellenőrizze az NTP-t](https://contenthub.netacad.com/courses/netsec/_common/6.6.4-packet-tracer---configure-and-verify-ntp.pka)

[6.5](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Network Security Using Syslog](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[6.7](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[SNMP Configuration](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                                                                  
*                               

1. Device Monitoring and Management
2. SNMP Configuration

# SNMP konfiguráció

6.7.1

## Bevezetés az SNMP-be

Most, hogy a hálózat le van térképezve, és minden összetevője ugyanazt az órát használja, ideje megvizsgálni, hogyan kezelheti hálózatát az egyszerű hálózatkezelési protokoll (SNMP) használatával.

Az SNMP-t arra fejlesztették ki, hogy lehetővé tegye a rendszergazdák számára az olyan csomópontok kezelését, mint a szerverek, munkaállomások, útválasztók, kapcsolók és biztonsági berendezések IP-hálózaton. Lehetővé teszi a hálózati rendszergazdák számára a hálózati teljesítmény figyelését és kezelését, a hálózati problémák megtalálását és megoldását, valamint a hálózat bővítésének tervezését.

Az SNMP meghatározza a felügyeleti információk cseréjét a hálózatfelügyeleti alkalmazások és a felügyeleti ügynökök között. Ez egy alkalmazási réteg protokoll, amely üzenetformátumot biztosít a menedzserek és ügynökök közötti kommunikációhoz. Az SNMP rendszer három elemből áll:

* SNMP menedzser
* SNMP-ügynökök (felügyelt csomópont)
* Menedzsment információs bázis (MIB)

Az SNMP hálózati eszközön történő konfigurálásához először meg kell határozni a kapcsolatot a kezelő és az ügynök között.

Az SNMP-kezelő egy hálózatkezelő rendszer (NMS) része. Az SNMP-kezelő SNMP-kezelő szoftvert futtat.

Amint az ábrán látható, az SNMP-kezelő információkat gyűjthet egy SNMP-ügynöktől a „get” művelet segítségével. A „set” művelet használatával módosíthatja az ügynök konfigurációit. Ezenkívül az SNMP-ügynökök „csapdák” használatával közvetlenül továbbíthatják az információkat a hálózatkezelőnek.

Az ábra egy SNMP-kezelőt mutat, amely információkat gyűjt egy SNMP-ügynöktől. Az ábrán egy PC-ként ábrázolt SNMP Manager egy útválasztóhoz, egy kapcsolóhoz és egy tűzfalútválasztóhoz csatlakozik. Az SNMP Managerhez csatlakoztatott eszközök SNMP-ügynökökként és felügyelt csomópontként vannak megjelölve. A trap feliratú nyíl az SNMP-kezelőre mutat, jelezve, hogy az SNMP-ügynökeszközök csapdákat küldenek az SNMP-kezelőnek. Két nyíl mutat az SNMP-ügynökök felé, Get és Set felirattal. Ezek azt jelzik, hogy az SNMP-kezelő elküldi az SNMP-ügynökök Get és Set műveleteit.

**Felügyelt csomópont** SNMP-ügynök SNMP -ügynök SNMP-ügynök csapda SNMP-kezelő beállítása lekérése **Felügyelt csomópont felügyelt csomópont**

Az SNMP-ügynök és a MIB az SNMP-ügyféleszközökön találhatók. A felügyelendő hálózati eszközök, például kapcsolók, útválasztók, szerverek, tűzfalak és munkaállomások SNMP ügynök szoftvermodullal vannak felszerelve. A MIB adatokat és működési statisztikákat tárol az eszközről.

Az SNMP Manager get kérést küld az SNMP-ügynöknek, hogy hozzáférjen a helyi MIB-ben tárolt adatokhoz. Pontosabban, az SNMP-kezelő lekérdezi az ügynököket, és lekérdezi a MIB-ben az SNMP-ügynököket a 161-es UDP-porton. Az SNMP-ügynökök minden SNMP-trap-et elküldenek a 162-es UDP-porton lévő SNMP-kezelőnek.

6.7.2

## SNMP működés

A felügyelt eszközökön található SNMP-ügynökök információkat gyűjtenek és tárolnak az eszközről és annak működéséről. Ezeket az információkat az ügynök helyileg a MIB-ben tárolja. Az SNMP-kezelő ezután az SNMP-ügynököt használja a MIB-en belüli információk eléréséhez.

Két elsődleges SNMP-kezelő kérés létezik:

* **get request** – Az NMS arra használja, hogy adatokat kérjen le az eszközről.
* **kérés beállítása** – Az NMS az ügynökeszköz konfigurációs változóinak módosítására használja. A beállított kérés az eszközön belül is indíthat műveleteket. Egy beállított kérés például az útválasztó újraindítását, konfigurációs fájl küldését vagy konfigurációs fájl fogadását okozhatja.

műveleteket használja **Az SNMP-kezelő a get** és **set** a táblázatban leírt műveletek végrehajtására.

| **Művelet** | **Leírás** |
| --- | --- |
| **get-kérés** | Lekér egy értéket egy adott változóból. |
| **get-next-request** | Értéket kér le egy táblán belüli változóból; az SNMP-kezelőnek nem kell tudnia a változó pontos nevét. Egy szekvenciális keresést hajtanak végre a szükséges változó megtalálásához egy táblán belül. |
| **get-bulk-request** | Nagy adatblokkokat kér le, például egy táblázat több sorát, amelyek egyébként sok kis adattömb átvitelét igényelnék. (Csak SNMPv2 vagy újabb verzióval működik.) |
| **kap-választ** | Válaszok **get-request, get-next-request** és **set-request-re .** egy NMS által küldött |
| **set-kérés** | Értéket tárol egy adott változóban. |

Az SNMP-ügynök a következőképpen válaszol az SNMP-kezelő kérésére:

* **MIB-változó beszerzése** – Az SNMP-ügynök ezt a funkciót a hálózatkezelőtől érkező GetRequest-PDU-ra válaszolva hajtja végre. Az ügynök lekéri a kért MIB-változó értékét, és ezzel az értékkel válaszol a hálózatkezelőnek.
* **MIB-változó beállítása** – Az SNMP-ügynök ezt a funkciót a hálózatkezelő SetRequest-PDU-jára válaszolva hajtja végre. Az SNMP-ügynök megváltoztatja a MIB-változó értékét a hálózatkezelő által megadott értékre. A beállított kérésre adott SNMP-ügynökválasz tartalmazza az eszköz új beállításait.

Az ábra bemutatja az SNMP GetRequest használatát annak meghatározására, hogy a G0/0/0 interfész felfelé/felfelé áll-e.

Az ábra bemutatja az SNMP GetRequest használatát annak meghatározására, hogy a G0/0/0 interfész felfelé/felfelé áll-e. Egy személy a számítógép asztalánál azt mondja, hogy szeretném ellenőrizni a MIB változót, hogy megtudjam, a G0/0/0 fel/fel van-e. egy SNMP GetRequest küldése az R 1s interfészre. R 1 lekéri a kért MIB változó értékét.

1001 101010 10 11101010 101001010 0 1001000 010 1 011011010 111 0001101 1001 101010 10001101 10 001101 0110 1110 101010

R1

SNMP GET A MIB G0/0/0 Meg akarom nézni a MIB változót, hogy megtudjam, hogy a G0/0/0 up/up.

6.7.3

## Menedzsment információs bázis (MIB)

A MIB hierarchikusan rendezi a változókat. A MIB-változók lehetővé teszik a felügyeleti szoftver számára a hálózati eszköz figyelését és vezérlését. Formálisan a MIB minden változót objektumazonosítóként (OID) határoz meg. Az OID-k egyedileg azonosítják a felügyelt objektumokat a MIB-hierarchiában. A MIB az OID-ket RFC-szabványok alapján OID-hierarchiába rendezi, amely általában faként jelenik meg.

Bármely eszköz MIB-fája tartalmaz néhány ágat számos hálózati eszközre jellemző változókkal, és néhány ágat az adott eszközre vagy gyártóra jellemző változókkal.

Az RFC-k meghatároznak néhány közös nyilvános változót. A legtöbb eszköz megvalósítja ezeket a MIB-változókat. Ezenkívül a hálózati berendezések szállítói, például a Cisco, meghatározhatják a fa saját privát ágait, hogy alkalmazkodjanak az eszközeikre jellemző új változókhoz.

Az ábra a Cisco által meghatározott MIB-struktúra egyes részeit mutatja. Figyelje meg, hogyan írható le az OID szavakkal vagy számokkal, hogy segítsen megtalálni egy adott változót a fában. A Ciscóhoz tartozó OID-k számozása a következő: .iso (1).org (3).dod (6).internet (1).private (4).vállalkozások (1).cisco (9). Ezért az OID 1.3.6.1.4.1.9.

Az ábra a Cisco által meghatározott MIB-struktúra egyes részeit mutatja. A tetején az .iso található, lent a .org, majd a dod, az internet, a privát, a vállalatok és a cisco. A Cisco két oszlopra oszlik, az egyik tetején a helyi változók, alatta pedig az interfészcsoport, a második oszlopban pedig a cisco mgmt, alatta pedig a cisco flash csoport található.

iso (1) org (3) dod (6) internet (1) magán (4) vállalkozások (1) cisco (9) helyi változók (2) interfész csoport (2) cisco mgmt (9) cisco flash csoport (10)

6.7.4

## SNMP verziók

Az SNMP-nek több verziója is létezik:

* **SNMPv1** – Ez a Simple Network Management Protocol, egy teljes internetes szabvány, amelyet az RFC 1157 határoz meg.
* **SNMPv2c** – Ezt az 1901–1908 közötti RFC-k határozzák meg. Közösségi karakterlánc-alapú adminisztrációs keretrendszert használ.
* **SNMPv3** – Ez egy interoperábilis szabványalapú protokoll, amelyet eredetileg a 2273-2275 RFC-k határoztak meg. Biztonságos hozzáférést biztosít az eszközökhöz a csomagok hálózaton keresztüli hitelesítésével és titkosításával. Tartalmazza a következő biztonsági funkciókat: üzenetintegritás annak biztosítására, hogy a csomagot nem manipulálták továbbítás közben, hitelesítés annak megállapítására, hogy az üzenet érvényes forrásból származik-e, és titkosítás, amely megakadályozza, hogy az üzenet tartalmát illetéktelen forrás olvassa el.

Minden verzió SNMP-kezelőket, ügynököket és MIB-ket használ. A Cisco IOS szoftver a fenti három verziót támogatja. Az 1-es verzió egy örökölt megoldás, és manapság nem gyakran találkozunk vele a hálózatokban. Ezért ez a kurzus a 2c és 3 verzióra összpontosít.

Az SNMPv1 és az SNMPv2c is közösségi alapú biztonságot használ. A menedzserek azon közösségét, amely hozzáférhet az ügynök MIB-jához, egy közösségi karakterlánc határozza meg.

Az SNMPv1-től eltérően az SNMPv2c tömeges visszakeresési mechanizmust és részletesebb hibaüzenet-jelentést tartalmaz a felügyeleti állomásoknak. A tömeges visszakeresési mechanizmus táblázatokat és nagy mennyiségű információt kér le, minimalizálva a szükséges oda-vissza utak számát. Az SNMPv2c továbbfejlesztett hibakezelése kibővített hibakódokat tartalmaz, amelyek megkülönböztetik a különféle hibaállapotokat. Ezeket a feltételeket egyetlen hibakód jelenti az SNMPv1-ben. Az SNMPv2c hibakódjai között szerepel a hiba típusa.

**Megjegyzés** : Az SNMPv1 és SNMPv2c minimális biztonsági funkciókat kínál. Pontosabban, az SNMPv1 és az SNMPv2c nem tudja sem a felügyeleti üzenet forrását hitelesíteni, sem titkosítást biztosítani. Az SNMPv3-at leggyakrabban a 3410-3415 RFC-k írják le. Módszerekkel egészíti ki a kritikus adatok biztonságos továbbítását a felügyelt eszközök között.

Az SNMPv3 biztonsági modelleket és biztonsági szinteket egyaránt biztosít. A biztonsági modell egy hitelesítési stratégia, amelyet a felhasználó és a csoport számára állítanak be, amelyben a felhasználó tartózkodik. A biztonsági szint a biztonsági modellben megengedett biztonsági szint. A biztonsági szint és a biztonsági modell kombinációja határozza meg, hogy melyik biztonsági mechanizmust használják az SNMP-csomagok kezelésekor.

Rendelkezésre állnak biztonsági modellek az SNMPv1, SNMPv2c és SNMPv3 számára. A táblázat a biztonsági modellek és szintek különböző kombinációinak jellemzőit azonosítja.

Kattintson az egyes gombra a biztonsági modellek és szintek különböző kombinációinak jellemzőiről szóló további információkért.

| SNMPv1LevelnoAuthNoPrivAuthenticationCommunity stringEncryptionNoResultKözösségi karakterlánc-egyezést használ a hitelesítéshez. | |
| --- | --- |
| **SNMPv1** | |
| **Szint** | noAuthNoPriv |
| **Hitelesítés** | Közösségi karakterlánc |
| **Titkosítás** | Nem |
| **Eredmény** | A hitelesítéshez közösségi karakterlánc-egyezést használ. |

| **SNMPv2c** | |
| --- | --- |
| **Szint** | noAuthNoPriv |
| **Hitelesítés** | Közösségi karakterlánc |
| **Titkosítás** | Nem |
| **Eredmény** | A hitelesítéshez közösségi karakterlánc-egyezést használ. |
| **SNMPv3 noAuthNoPriv** | | |
| **Szint** | noAuthNoPriv | |
| **Hitelesítés** | Felhasználónév | |
| **Titkosítás** | Nem | |
| **Eredmény** | Felhasználónév-egyezést használ a hitelesítéshez (az SNMPv2c továbbfejlesztése). | |

| **SNMPv3 authNoPriv** | |
| --- | --- |
| **Szint** | authNoPriv |
| **Hitelesítés** | Message Digest 5 (MD5) vagy Secure Hash Algorithm (SHA) |
| **Titkosítás** | Nem |
| **Eredmény** | A HMAC-MD5 vagy HMAC-SHA algoritmusokon alapuló hitelesítést biztosít. |

| **SNMPv3 authPriv** | |
| --- | --- |
| **Szint** | authPriv (szükséges a kriptográfiai szoftverkép) |
| **Hitelesítés** | MD5 vagy SHA |
| **Titkosítás** | Data Encryption Standard (DES) vagy Advanced Encryption Standard (AES) |
| **Eredmény** | A HMAC-MD5 vagy HMAC-SHA algoritmusokon alapuló hitelesítést biztosít. Lehetővé teszi a felhasználói alapú biztonsági modell (USM) meghatározását a következő titkosítási algoritmusokkal:   * DES 56 bites titkosítás a CBC-DES (DES-56) szabványon alapuló hitelesítés mellett * 3DES 168 bites titkosítás * AES 128 bites, 192 bites vagy 256 bites titkosítás |

A hálózati rendszergazdának be kell állítania az SNMP-ügynököt a felügyeleti állomás által támogatott SNMP-verzió használatára. Mivel egy ügynök több SNMP-kezelővel is kommunikálhat, lehetséges a szoftver konfigurálása az SNMPv1, SNMPv2c vagy SNMPv3 használatával történő kommunikáció támogatására.

6.7.5

## SNMP sebezhetőségek

Bármely hálózati topológiában legalább egy menedzser csomópontnak SNMP felügyeleti szoftvert kell futtatnia. A felügyelhető hálózati eszközök, például kapcsolók, útválasztók, szerverek és munkaállomások SNMP ügynök szoftvermodullal vannak felszerelve. Ezek az ügynökök felelősek azért, hogy az SNMP-kezelő hozzáférést biztosítsanak egy helyi MIB-hez, amely adatokat tárol az eszköz működéséről.

Az SNMP pontosan azért sebezhető a támadásokkal szemben, mert az SNMP-ügynökök get kéréssel lekérdezhetők, és konfigurációs változtatásokat is elfogadhatnak beállított kérésekkel, ahogy az az ábrán is látható. Egy beállított kérés például az útválasztó újraindítását, konfigurációs fájl küldését vagy konfigurációs fájl fogadását okozhatja. Az SNMP-ügynök csapdák vagy értesítések küldésére is beállítható. Az SNMPv1 és SNMPv2c esetén ezek a kérések és értesítések nincsenek hitelesítve vagy titkosítva.

Az ábra egy SNMP-kezelőt mutat, amely információkat gyűjt egy SNMP-ügynöktől. Az ábrán egy PC-ként ábrázolt SNMP Manager egy útválasztóhoz, egy kapcsolóhoz és egy tűzfalútválasztóhoz csatlakozik. Az SNMP Managerhez csatlakoztatott eszközök SNMP-ügynökökként és felügyelt csomópontként vannak megjelölve. A trap feliratú nyíl az SNMP-kezelőre mutat, jelezve, hogy az SNMP-ügynökeszközök csapdákat küldenek az SNMP-kezelőnek. A fenti szöveg olvasható Az SNMP v1-ben az aszinkron eseményjelentéseket csapdáknak, míg a későbbi verziókban értesítéseknek nevezik. Két nyíl mutat az SNMP-ügynökök felé, Get és Set felirattal. Ezek azt jelzik, hogy az SNMP-kezelő elküldi az SNMP-ügynökök Get és Set műveleteit. Az alábbi szöveg a következő: A kapott és beállított műveletek azok a sebezhetőségek, amelyek megnyitják az SNMP-t támadás előtt.

### SNMP működés

Az SNMPv1-ben az aszinkron eseményjelentéseket "csapdáknak", míg a későbbi verziókban értesítéseknek nevezik. műveletek **A kapott** és **beállított** azok a sebezhetőségek, amelyek megnyitják az SNMP-t támadás előtt. Felügyelt csomópont SNMP-ügynök SNMP -ügynök SNMP -ügynök csapda SNMP- kezelőkészlet beszerzése Felügyelt csomópont felügyelt csomópont

6.7.6

## SNMPv3

Az SNMPv3 hitelesíti és titkosítja a csomagokat a hálózaton keresztül, hogy biztonságos hozzáférést biztosítson az eszközökhöz. Ezzel orvosolták az SNMP korábbi verzióinak sebezhetőségeit.

Az SNMPv3 három biztonsági funkciót kínál:

* **Üzenet integritása és hitelesítése** – Biztosítja, hogy a csomagot nem módosították az átvitel során, és hogy az érvényes forrásból származik.
* **Titkosítás** – Kódolja a csomag tartalmát, hogy megakadályozza, hogy azt illetéktelen forrás lássa.
* **Hozzáférés-szabályozás** – Az egyes megbízottakat bizonyos műveletekre korlátozza az adatok meghatározott részein.

6.7.7

## SNMPv3 biztonsági konfiguráció

Az SNMPv3 csak néhány paranccsal biztosítható, amint az a következő lépésekben látható.

**Megjegyzés** : Az SNMPv3 konfigurációs lehetőségeinek teljes körű megvitatása túlmutat ennek a kurzusnak a keretein.

**1. lépés** . Konfiguráljon egy ACL-t, amely lehetővé teszi a hozzáférést az engedélyezett SNMP-kezelők számára.

Router(config)#  **ip access-list**  acl-name   
Router(config-std-nacl)#  **engedélyezi**  a forrás\_netet

**2. lépés** . Konfiguráljon egy SNMP-nézetet az **snmp-server view** paranccsal, hogy azonosítsa azokat a MIB OID-ket, amelyeket az SNMP-kezelő képes olvasni. Nézet konfigurálása szükséges ahhoz, hogy az SNMP-üzenetek csak olvasási hozzáférésre korlátozódjanak.

Router(config)#  **snmp-server view**  view-name oid-tree

Az SNMPv3 csak néhány paranccsal biztosítható, ahogy az az ábrán is látható.

**3. lépés** . Konfigurálja az SNMP csoport szolgáltatásait az **snmp-server group** paranccsal:

* Állítson be egy nevet a csoportnak.
* Állítsa az SNMP-verziót 3-ra a **v3** kulcsszóval.
* Hitelesítés és titkosítás szükséges a **priv** kulcsszóval.
* Társítson egy nézetet a csoporthoz, és adjon csak olvasási hozzáférést a **read** paranccsal.
* Adja meg az 1. lépésben konfigurált ACL-t.

Router(config)#  **snmp-szerver csoport**  csoportnév  **v3 priv read**  view-name  **access**  [ acl-szám | acl-név ]

**4. lépés** . Konfigurálja az SNMP csoport felhasználói jellemzőit az **snmp-server user** paranccsal:

* Konfiguráljon egy felhasználónevet, és társítsa a felhasználót a 3. lépésben konfigurált csoportnévhez.
* Állítsa az SNMP-verziót 3-ra a **v3** kulcsszóval.
* értékre **Állítsa be a hitelesítés típusát md5** vagy **sha** , és állítson be egy hitelesítési jelszót. Az SHA előnyben részesített, és az SNMP-kezelőszoftvernek támogatnia kell.
* Kérjen titkosítást a **priv** kulcsszóval, és állítson be egy titkosítási jelszót.

Router(config)#  **snmp-szerver felhasználó**  felhasználónév csoportnév  **v3 auth**  {  **md5**  |  **sha**  } auth-password  **priv**  {  **des**  |  **3des**  |  **aes**  {  **128**  |  **192**  |  **256**  }} priv-password

6.7.8

## SNMPv3 biztonsági konfigurációs példa

Az ábra egy példa konfigurációt mutat be az SNMPv3 biztosítására.

**1. lépés** . A szabványos ACL neve PERMIT-ADMIN, és úgy van beállítva, hogy csak a 192.168.1.0/24 hálózatot engedélyezze. A hálózathoz kapcsolódó összes gazdagép hozzáférhet az R1-en futó SNMP-ügynökhöz.

**2. lépés** . Az SNMP-nézet neve SNMP-RO, és úgy van beállítva, hogy tartalmazza a teljes iso-fát a MIB-ből. Éles hálózaton a hálózati rendszergazda valószínűleg úgy konfigurálja ezt a nézetet, hogy csak a hálózat figyeléséhez és kezeléséhez szükséges MIB OID-ket tartalmazza.

**3. lépés** . Egy SNMP-csoport ADMIN néven van konfigurálva. Az SNMP 3-as verzióra van állítva, hitelesítés és titkosítás szükséges. A csoport csak olvasási hozzáféréssel rendelkezik a nézethez (SNMP-RO). A csoport hozzáférését a PERMIT-ADMIN ACL korlátozza.

**4. lépés** . Egy SNMP-felhasználó, BOB, az ADMIN csoport tagjaként van konfigurálva. Az SNMP 3-as verzióra van állítva. A hitelesítés SHA használatára van beállítva, és be van állítva egy hitelesítési jelszó. Bár az R1 támogatja az AES 256-ig terjedő titkosítást, az SNMP-kezelőszoftver csak az AES 128-at támogatja. Tehát a titkosítás AES 128-ra van állítva, és egy titkosítási jelszó is be van állítva.

Az animáció egy fenyegető szereplőt mutat be egy nem csatlakoztatott számítógépen. Létezik egy hálózat a rendszer címkével ellátott számítógéppel, egy másik b rendszer címkével ellátott számítógép és egy felhő feliratú internet. Ezek mindegyike külön csatlakozik egy tűzfalhoz. Az animáció lejátszása közben a rendszer a bízik a rendszerben szavak jelennek meg az a rendszer felett. a „b rendszer mindenkiben bízik” szavak a b rendszer felett jelennek meg. A fenyegetés szereplője mellett a cél szavak: a támadó hozzá akar férni a rendszerhez. rendszer a villog. az a rendszerben a user=psmith szavak vannak; pat Smith. egy buborék jelenik meg a fenyegetés szereplője felett, amely azt mondja, hogy nem férek hozzá az a rendszerhez, de a rendszer nyitva van. a user=psmith szavak; Pat Smith megjelenik a fenyegetőző mellett. egy nyíl a fenyegetés szereplőjétől az internetre, a tűzfalra, a rendszerre megy b. A támadó által feltört szavak user=psmith; pat smith megjelenik a b rendszer alatt, a b rendszer pedig veszélyeztetettként jelenik meg. a fenyegetés szereplői buborékban megjelennek a „b” rendszert irányítom, és most hozzáférek az „a” rendszerhez szavak. egy nyíl közvetlenül a fenyegetés szereplőjétől az a rendszerhez megy, ahol az a rendszer veszélyeztetettként jelenik meg.

192.168.1.0/24

Védett felügyeleti hálózat

R1(config)# **ip access-list standard PERMIT-ADMIN**

R1(config-std-nacl)# **permit 192.168.1.0 0.0.0.255**

R1(config-std-nacl)# **exit**

R1(config)# **snmp-server view SNMP-RO iso included**

R1(config)# **snmp-server group ADMIN v3 priv read SNMP-RO access PERMIT-ADMIN**

R1(config)# **snmp-server user BOB ADMIN v3 auth sha cisco12345 priv aes 128 cisco54321**

R1(config)# **end**

R1#

6.7.9

## Szintaxis-ellenőrző – SNMPv3 biztonsági konfigurációs példa

Ezzel a szintaktikai ellenőrzővel konfigurálhatja az R1-et SNMPv3 hitelesítéssel ACL használatával.

nevű szabványos hozzáférési listát **Állítson be egy PERMIT-ADMIN** az R1-en, hogy csak a 192.168.1.0/24 hálózatot engedélyezze. A folytatáshoz lépjen ki az ACL konfigurációból.

R1(config)#ip access-list standard PERMIT-ADMIN

R1(config-std-nacl)#permit 192.168.1.0 0.0.0.255

R1(config-std-nacl)#exit

Az **snmp-server view** nevű SNMP-nézetet **paranccsal állítson be egy SNMP-RO** úgy, hogy az tartalmazza a teljes ISO-fát a MIB-ből.

R1 (config)# SNMP-szerver nézet SNMP-RO ISO

Az **snmp-server group** nevű SNMP-csoportot **paranccsal állítson be egy ADMIN** . Állítsa be az SNMP-t 3-as verzióra, hitelesítés és titkosítás szükséges. nézethez **Engedélyezze a csak olvasható hozzáférést az SNMP-RO** , és korlátozza a hozzáférést a **PERMIT-ADMIN** ACL használatával.

R1(config)# snmp-server group ADMIN v3 priv read SNMP-RO access PERMIT-ADMIN

Az **snmp-server user** nevű snmp felhasználót **paranccsal adjon hozzá egy BOB** csoport tagjaként **az ADMIN** . jelszóval **Állítsa az SNMP-t 3-as verzióra, és állítsa be a hitelesítést az SHA használatára a cisco12345** . Állítsa be a titkosítást **AES 128-** jelszóval **ra a cisco54321** . A konfiguráció befejezése után használja az **end** parancsot a konfigurációs módból való kilépéshez.

R1(config)# snmp-szerver felhasználó BOB ADMIN v3 auth sha cisco12345 priv aes 128 cisco54321

R1(config)# vége

R1#

Sikeresen konfigurálta az SNMPv3 hitelesítést az R1 ACL használatával.

6.7.10

## SNMPv3 ellenőrzés

Ellenőrizze az SNMPv3 biztonsági konfiguráció nagy részét a futó konfiguráció megtekintésével, az ábrán látható módon. Figyelje meg, hogy az snmp-server felhasználói konfigurációja el van rejtve. használja a **show snmp user parancsot.** A felhasználói adatok megtekintéséhez

Az ábra egy olyan számítógépet mutat, amely egy routerhez csatlakozik a Protected Management Network 192.168.1.0 / 24 felirattal.

192.168.1.0/24

Védett felügyeleti hálózat

R1# **show run | include snmp**

snmp-server group ADMIN v3 priv read SNMP-RO access PERMIT-ADMIN

snmp-server view SNMP-RO iso included

R1# **show snmp user**

User name: BOB

Engine ID: 80000009030030F70DA30DA0

storage-type: nonvolatile active

Authentication Protocol: SHA

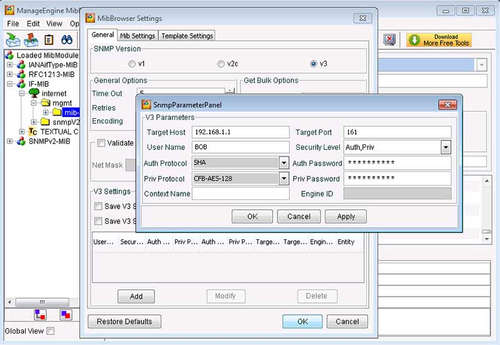
Privacy Protocol: AES128

Group-name: ADMIN

R1#

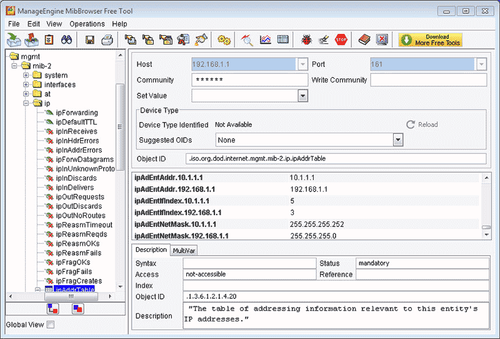
Ellenőrizze, hogy az SNMP-kezelő tud-e get kéréseket küldeni az R1-nek egy SNMP-kezelő eszközzel, például a ManageEngine ingyenes SNMP MIB-böngészőjével. Konfigurálja az eszközt a felhasználói adatokkal az ábrán látható módon. Amikor egy felhasználó be van állítva, az SNMP-kezelő eszköz szolgáltatásaival ellenőrizze, hogy a konfigurált felhasználó hozzáfér-e az SNMP-ügynökhöz.

### Az SNMP-kezelő hozzáférésének konfigurálása az SNMP-ügynökhöz



Az alábbi ábrán a hálózati rendszergazda megadta az IP-címzési táblázat OID-jét. A get kérés visszaadta az összes R1 címzési információt. A hálózati rendszergazda a megfelelő hitelesítő adatokkal hitelesítette.

### Konfigurálja az SNMP Manager Get Request példáját



Ellenőrizze, hogy az adatok titkosítva vannak-e egy protokollelemző, például a Wireshark futtatásával, és rögzítse az SNMP-csomagokat.

Keressen az interneten, és nézze meg Keith Barker bemutatóját az SNMPv3 konfigurálásáról és ellenőrzéséről.

### Titkosított SNMPv3-csomagok Wireshark rögzítése



6.7.11

## Lab – Konfigurálja a Cisco IOS Resilience Management és Reporting szolgáltatást

In this lab, you will complete the following objectives:

* Part 1: Configure basic device settings.
* Part 2: Configure SNMPv3 security using an ACL.
* Part 3: Configure a router as a synchronized time source for other devices using NTP.
* Part 4: Configure syslog support on a router.

6.7.12

## Packet Tracer – Cisco-eszközök konfigurálása Syslog, NTP és SSH műveletekhez

Ebben a csomagjelző tevékenységben a következő célokat fogja kitölteni:

* Konfigurálja a Syslog szolgáltatást
* Naplózott EventsPart generálása
* Manuálisan állítsa be a Switch ClocksPart
* Az NTP ServicePart beállítása
* Ellenőrizze az időbélyegző naplókat

[Configure Cisco Devices for Syslog, NTP, and SSH Operations](https://contenthub.netacad.com/courses/netsec/_common/6.7.12-packet-tracer---configure-cisco-devices-for-syslog-ntp-and-ssh-operations.pka)

[6.6](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[NTP Configuration](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[6.8](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Device Monitoring and Management Summary](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                                                                                                 

1. Device Monitoring and Management
2. Device Monitoring and Management Summary

# Eszközfigyelés és -kezelés összefoglalása

6.8.1

## Mit tanultam ebben a modulban?

**Biztonságos Cisco IOS kép- és konfigurációs fájlok**   
A Cisco IOS rugalmas konfigurációs funkciója gyorsabb helyreállítást tesz lehetővé, ha valaki rosszindulatúan vagy véletlenül újraformázza a flash memóriát, vagy törli az indítási konfigurációs fájlt a nem felejtő véletlen hozzáférésű memóriában (NVRAM). A szolgáltatás az útválasztó IOS képfájljának biztonságos munkapéldányát és a futó konfigurációs fájl másolatát tartja karban. Ezeket a biztonságos fájlokat a felhasználó nem tudja eltávolítani, és elsődleges rendszerindítónak nevezik őket. A funkció csak a régebbi útválasztókon érhető el, amelyek támogatják a PCMCIA Advanced Technology Attachment (ATA) flash interfészt. Az újabb útválasztók, például az ISR 4000 nem támogatják ezt a funkciót. Az IOS lemezkép biztonságossá tételéhez és a Cisco IOS lemezkép rugalmasságának engedélyezéséhez használja a **biztonságos boot-image** globális konfigurációs mód parancsot. Az első engedélyezéskor a futó Cisco IOS lemezkép biztonságossá válik, és naplóbejegyzés jön létre. Ha pillanatképet szeretne készíteni a futó útválasztó konfigurációjáról, és biztonságosan archiválni szeretné az állandó tárolóban, használja a **biztonságos boot-config** globális konfigurációs mód parancsot. Az útválasztó beállítható úgy, hogy a biztonságos képet ROMmon módból indítsa el. A konfigurációs fájl biztonságos helyről a következővel másolható **biztonságos boot-config visszaállítási** parancs. A Secure Copy Protocol (SCP) szolgáltatás biztonságos és hitelesített módszert biztosít az útválasztó konfigurációs vagy képfájljainak távoli helyre másolására. Az SCP az SSH-ra támaszkodik a biztonságos kommunikációhoz, az AAA-ra pedig a hitelesítéshez és engedélyezéshez. Ha az útválasztót feltörték, és a jelszavakat ismeretlen értékre változtatták, jelszó-helyreállítási eljárás létezik az útválasztó konfigurációja nélkül történő indításához, így a jelszavak ismert értékekre cserélhetők. Ez az eljárás a különböző eszközmodelleknél eltérő lehet. Fizikai hozzáférés szükséges az útválasztóhoz és a ROMmon módhoz. A jelszó-helyreállítási eljáráshoz való hozzáférés letiltható a **no service password-recovery** paranccsal.

**Zárolja le az útválasztót az AutoSecure használatával**   
A Cisco útválasztók kezdetben számos szolgáltatással vannak telepítve, amelyek alapértelmezés szerint engedélyezve vannak. E szolgáltatások némelyike, például a Cisco Discovery Protocol (Cisco Discovery Protocol) és a Link Layer Discovery Protocol (LLDP) azonban sebezhetővé teheti a hálózatot a támadásokkal szemben. Mindkét protokoll lehetővé teszi a támadók számára, hogy részletes információkat szerezzenek az útválasztóról. A maximális biztonság érdekében útmutatást adunk az útválasztó egyes szolgáltatásainak konfigurálásához. A Cisco AutoSecure szolgáltatása végrehajt egy parancsfájlt, amely javaslatokat tesz a biztonsági rések javítására, majd módosítja az útválasztó biztonsági konfigurációját. Az AutoSecure három továbbítási sík szolgáltatást tesz lehetővé, a Cisco Express Forwarding (CEF), a forgalomszűrést ACL-ekkel és a Cisco IOS tűzfal vizsgálatát. Az AutoSecure-t gyakran használják a terepen, hogy alapszintű biztonsági házirendet biztosítsanak egy új útválasztón. A funkciók ezután módosíthatók a szervezet biztonsági politikájának támogatása érdekében. Az **automatikus biztonsági** parancs beírásakor a készülék megjeleníti az AutoSecure üdvözlő üzenetét. Az AutoSecure ezután információkat gyűjt az eszköz aktuális konfigurációjáról, és belép egy konfigurációs párbeszédpanelbe. Ezután letiltja és engedélyezi a szolgáltatásokat, és egyéb konfigurációs módosításokat hajt végre az eszközön. Amikor a varázsló befejeződött, a futó konfiguráció megjeleníti az összes konfigurációs beállítást és módosítást. Az AutoSecure-t az útválasztó kezdeti konfigurálásakor kell használni. Gyári útválasztókon nem ajánlott.

**Routing Protocol Authentication**   
A dinamikus útválasztási protokollokat az útválasztók a távoli hálózatok elérhetőségével és állapotával kapcsolatos információk automatikus megosztására használják. A dinamikus útválasztási protokollok számos tevékenységet végeznek, beleértve a hálózatfelderítést és az útválasztási táblák karbantartását. A dinamikus útválasztási protokollok fontos előnyei a legjobb útvonal kiválasztásának képessége, valamint a legjobb új útvonal automatikus felfedezésének képessége, ha a topológia megváltozik. A hálózatfelderítés az útválasztási protokoll azon képessége, hogy dinamikusan megossza az általa ismert hálózatokkal kapcsolatos információkat más, ugyanazt az útválasztási protokollt használó útválasztókkal. Az útválasztó rendszereket megtámadhatják a peer hálózati útválasztók megzavarása, vagy az útválasztási protokollokon belüli információk meghamisítása vagy hamisítása. Ez felhasználható arra, hogy a rendszerek félretájékoztatják (hazudják) egymást, DoS támadást idézzenek elő, vagy a forgalmat olyan útvonalon kövessék, amelyet általában nem követne. Az útválasztási protokoll frissítései MD5 vagy SHA hitelesítés használatára konfigurálhatók. Ez segít abban, hogy az útválasztási protokoll frissítései megbízható forrásokból érkezzenek. Az MD5 hitelesítés elérhető az OSPF útválasztási protokollhoz, azonban a nagyobb biztonság érdekében előnyben részesítik az SHA-t.

**Biztonságos menedzsment és jelentéskészítés**   
A legtöbb hálózati eszköz képes összegyűjteni és továbbítani a naplóinformációkat, amelyek nagyon értékesek lehetnek a hálózati problémák diagnosztizálásában és a biztonsági események észlelésében. Kis hálózatban kis számú hálózati eszköz kezelése és felügyelete egyszerű művelet. Egy több száz eszközzel rendelkező nagyvállalatnál azonban a naplóüzenetek figyelése, kezelése és feldolgozása kihívást jelenthet. A naplófájlt gyűjtő gazdagépek és a felügyelt hálózati eszközök közötti információáramlás két úton haladhat. A sávon belüli információs útvonalak az éles hálózatot, az internetet vagy mindkettőt használják. A felügyeleti forgalom ugyanazon a hálózaton történik, mint a felhasználói forgalom. A sávon kívüli (OOB) felügyeleti útvonalak dedikált felügyeleti hálózatokat használnak, amelyek nem továbbítanak felhasználói forgalmat. Általános szabály, hogy biztonsági okokból az OOB-kezelés megfelelő a nagyvállalati hálózatokhoz. Ez azonban nem mindig kívánatos. Ez a felügyelt felügyeleti alkalmazásoktól és protokolloktól függ. A sávon belüli felügyelet javasolt kisebb hálózatokban a költséghatékonyabb biztonsági telepítés elérése érdekében. Az OOB felügyeleti biztonsági irányelveinek célja a legmagasabb szintű biztonság biztosítása és a nem biztonságos felügyeleti protokollok éles hálózaton való átadásának kockázatának csökkentése. A sávon belüli felügyeletre vonatkozó irányelvek csak azokra az eszközökre vonatkoznak, amelyeket felügyelni vagy felügyelni kell, ha lehetséges, használjon IPSec-et, SSH-t vagy SSL-t, és döntse el, hogy a felügyeleti csatornának mindig elérhetőnek kell lennie. Ha távoli felügyeleti eszközöket használ sávon belüli felügyelettel, ügyeljen magának a felügyeleti eszköznek a mögöttes biztonsági réseire.

**Hálózati biztonság Syslog használatával**   
A rendszerüzenetek elérésének legáltalánosabb módja a syslog nevű protokoll használata. Sok hálózati eszköz támogatja a syslog szabványt. A syslog protokoll lehetővé teszi, hogy a hálózati eszközök rendszerüzeneteiket a hálózaton keresztül elküldjék a rendszernapló-kiszolgálóknak. A rendszernapló-naplózási szolgáltatás lehetőséget biztosít naplózási információk gyűjtésére, a naplózandó információk típusának kiválasztására, valamint a rendszernapló-üzenetek fogadására és tárolására alkalmas céleszközök megadására. parancs kimenetet küldhet **A Cisco hálózati eszközökön a syslog protokoll rendszerüzeneteket és hibakeresési** egy helyi naplózási folyamatnak, amely az eszközön belül van, vagy üzeneteket küldhet egy belső pufferbe. A belső pufferbe küldött üzenetek csak az eszköz CLI-jén keresztül tekinthetők meg. Egy eszköz beállítható úgy, hogy syslog-üzeneteket küldjön egy naplózási puffernek, a konzolvonalnak, egy terminálvonalnak vagy egy külső rendszernapló-kiszolgálónak. A Syslog üzenetek súlyossági szintet tartalmaznak, amely 0-tól 7-ig terjedhet. Minél alacsonyabb a szint száma, annál nagyobb a súlyosság. Például a 0–4. szintű üzenetek szoftver- vagy hardverhibákra vonatkoznak. Az 5. szintű üzenetek normál működést jeleznek, de jelentősek. A 6. szint a normál működési eseményekre vonatkozik, a 7. szint pedig az üzenetek hibakeresésére szolgál. Ezenkívül a rendszernapló-üzenetek tartalmaznak egy syslog-szolgáltatás kódot is. Egyes szolgáltatások jelzik azt a rendszert, összetevőt vagy protokollt, amely az üzenetet jelentette. A **service timestaps log datetime** parancs beállítja az eszközt, hogy rendszeridőbélyegeket használjon az összes üzenethez. Az időbélyegek származhatnak a helyi eszköz órájából, vagy szinkronizálhatók olyan eszközök között, amelyek a Network Time Protocol (NTP) rendszeridőt használják. A rendszernapló-megvalósítások rendszernapló-kiszolgálókból, úgynevezett naplógazdagépekből állnak, amelyek rendszernaplóüzeneteket fogadnak és tárolnak a hálózatról, valamint olyan syslog-kliensekből, amelyek rendszernapló-üzeneteket generálnak és továbbítanak a rendszernapló-kiszolgálóknak. A Cisco eszköz a syslog használatára van konfigurálva úgy, hogy megadja a naplózó gazdagépet a naplózási paranccsal, opcionálisan beállítja a naplózandó üzenetek súlyossági szintjét a naplózási **trap** paranccsal, és opcionálisan beállítja azt a felületet, amely üzenetforrás legyen a **naplózási forrással . interfész** parancsot, és aktiválja a naplózási folyamatot a **bejelentkezési** paranccsal.

**NTP konfiguráció**   
Az útválasztón vagy kapcsolón a szoftveróra elindul, amikor a rendszer elindul. Ez az elsődleges időforrás a rendszer számára. Fontos az idő szinkronizálása a hálózat összes eszközén, mert a hálózatok kezelésének, biztonságának, hibaelhárításának és tervezésének minden vonatkozása pontos időbélyegzést igényel. Ha az idő nincs szinkronizálva az eszközök között, lehetetlen lesz meghatározni az események sorrendjét és az esemény okát. Bár a rendszeridő manuálisan beállítható, sokkal kívánatosabb az eszközöket úgy konfigurálni, hogy a Network Time protokoll (NTP) használatával szinkronizálják az időt az összes hálózati eszköz között. Az NTP lehetővé teszi, hogy a hálózati eszközök (azaz az NTP-kliensek) szinkronizálják időbeállításaikat egy mérvadó NTP időforrással, például egy NTP-kiszolgálóval. Az NTP időforrás lehet egy olyan eszköz (pl. útválasztó) a hálózaton, amely privát elsődleges óraként van kiválasztva, vagy lehet egy nyilvánosan elérhető NTP-szerver az interneten. Az NTP az időforrások hierarchikus rendszerét használja, amelyek rétegekbe vannak rendezve. A Stratum 0 a leghitelesebb időforrás, és használhat atom- vagy GPS-órákat. A Stratum 1 eszközök az időinformációikat Stratum 0 forrásokból szerzik be. A Stratum 1 eszközök a Stratum 0 időforrásokhoz csatlakoznak, és a vállalati hálózatok számára is elérhetők. A Stratum 2 és az alacsonyabb szintű eszközök hálózati szerverként működnek, amelyek időinformációkat szolgáltatnak a hálózati eszközöknek. Stratum 1 eszközökhöz vagy más hálózati eszközökhöz csatlakoznak, amelyek NTP-kiszolgálóként működnek. Legfeljebb 16 NTP-réteg létezik. Minél alacsonyabb a rétegszám, annál közelebb van a forrás a Strata 0 mérvadó forrásához. Az NTP olyan eszközön van konfigurálva, amelyen a **ntp szerver** parancsot.

**SNMP konfiguráció**   
Az SNMP-t (Simple Network Management Protocol) azért fejlesztették ki, hogy lehetővé tegye az adminisztrátorok számára az olyan csomópontok kezelését, mint a szerverek, munkaállomások, útválasztók, kapcsolók és biztonsági berendezések IP-hálózaton. Az SNMP meghatározza a felügyeleti információk cseréjét a hálózatfelügyeleti alkalmazások és a felügyeleti ügynökök között. Ez egy alkalmazási rétegbeli protokoll, amely üzenetformátumot biztosít a menedzserek és ügynökök közötti kommunikációhoz. Az SNMP rendszer három elemet igényel, és egy SNMP-kezelőből, egy SNMP-ügynökből és egy felügyeleti információs bázisból (MIB) áll. Az SNMP-kezelő egy hálózatkezelő rendszer (NMS) része, amely SNMP-felügyeleti szoftvert futtat. Az SNMP-ügynökök hálózati eszközökön találhatók, és lehetővé teszik a hálózati adatgyűjtést és -megosztást. A MIB szabványosított változókat tárol, amelyek hálózati adatokat tartalmaznak. A hálózatmenedzser küldhet egy get kérést az ügynök helyi MIB-jéből való információ lekérésére, vagy küldhet egy set kérést a MIB-ben lévő változó értékének módosítására. A MIB hierarchikusan rendezi a változókat. A MIB-változók lehetővé teszik a felügyeleti szoftver számára a hálózati eszköz figyelését és vezérlését. Az RFC-k meghatároznak néhány általános nyilvános változót, amelyeket a legtöbb eszköz támogat. Ezenkívül a hálózati berendezések szállítói, például a Cisco, meghatározhatják a fa saját privát ágait, hogy alkalmazkodjanak az eszközeikre jellemző új változókhoz. Az SNMP-nek három verziója létezik. Az SNMPv1 elavult, és csak említve van, de az SNMPv2c és az SNMPv3 relevánsak ebben a kurzusban. Az SNMPv2c használatát legalább az SNMPv3 erősen ajánlott. Az SNMPv1 és SNMPv2c minimális biztonsági funkciókat kínál. Pontosabban, az SNMPv1 és az SNMPv2c nem tudja sem a felügyeleti üzenet forrását hitelesíteni, sem titkosítást biztosítani. Az SNMPv3 módszerekkel egészíti ki a kritikus adatok biztonságos átvitelét a felügyelt eszközök között. Az SNMPv3 biztonsági modelleket és biztonsági szinteket egyaránt biztosít. A biztonsági modell egy hitelesítési stratégia, amelyet a felhasználó és a csoport számára állítanak be, amelyben a felhasználó tartózkodik. A biztonsági szint a biztonsági modellben megengedett biztonsági szint. A biztonsági szint és a biztonsági modell kombinációja határozza meg, hogy melyik biztonsági mechanizmust használják az SNMP-csomagok kezelésekor. Az SNMPv3 hitelesíti és titkosítja a csomagokat a hálózaton keresztül, hogy biztonságos hozzáférést biztosítson az eszközökhöz. Ezzel orvosolták az SNMP korábbi verzióinak sebezhetőségeit.

6.8.2

## 6. modul – Eszközfigyelő és -kezelési kvíz

Az űrlap teteje

1. Milyen szolgáltatásra vagy protokollra támaszkodik a Secure Copy Protocol annak biztosítására, hogy a biztonságos másolatok átvitele jogosult felhasználóktól származzon?

Az űrlap alja

Ha az útválasztón jelszó-helyreállítást hajtanak végre, és az NVRAM beállításait kihagyták, melyik lépést kell megtenni a következő lépésben?

Melyik protokollt vagy szolgáltatást használják a Cisco útválasztók szoftveres óráinak automatikus szinkronizálására?

Egy hálózati mérnök szinkronizálni szeretné egy útválasztó idejét egy NTP-kiszolgálóval a 209.165.200.225 IPv4-címen. Az útválasztó kilépési felülete 192.168.212.11 IPv4-címmel van konfigurálva. Melyik globális konfigurációs paranccsal kell beállítani az NTP-kiszolgálót az útválasztó időforrásaként?

Milyen három funkciót biztosít a syslog szolgáltatás? (Válassz hármat.)

Melyik szolgáltatást kell letiltani egy útválasztón, hogy megakadályozzuk, hogy egy rosszindulatú gazdagép hamisan válaszoljon az ARP-kérésekre azzal a szándékkal, hogy átirányítsa az Ethernet-kereteket?

Mi a célja az **ip ospf üzenet - digest - key** key **md5** jelszó parancs és a **területterület** ? - id **hitelesítési üzenet - digest** parancs kiadásának egy útválasztón

Melyik szolgáltatás van alapértelmezés szerint engedélyezve egy Cisco útválasztón, amely jelentős információkat fedhet fel az útválasztóról, és potenciálisan sebezhetőbbé teheti a támadásokkal szemben?

Melyik utasítás írja le az SNMP működését?

SNMPv1 vagy SNMPv2 használata esetén melyik szolgáltatás biztosít biztonságos hozzáférést a MIB objektumokhoz?

Mi a két oka annak, hogy engedélyezze az OSPF útválasztási protokoll hitelesítését a hálózaton? (Válassz kettőt.)

Mik azok az SNMP trap üzenetek?

Melyik technológia teszi lehetővé a rendszernapló-üzenetek szűrését különböző eszközökre az események fontossága alapján?

Mi jellemzi a Cisco IOS Resilient Configuration szolgáltatást?

[6.7](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[SNMP Configuration](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[7.0](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                                                                                 
*                             

1. Authentication, Authorization, and Accounting (AAA)
2. Introduction

# Bevezetés

7.0.1

## Miért vegyem ezt a modult?

Az AAA egy olyan technológia, amely lehetővé teszi a felhasználók hitelesítését és engedélyezését felhasználói azonosító és jelszó alapján. Az AAA helyileg konfigurálható hálózati eszközökön vagy AAA szerverek használhatók. A számvitel naplózhatja a felhasználói munkamenetek részleteit a számlázás vagy a felhasználói viselkedés láthatósága céljából. Fontos, hogy a hálózati biztonsági személyzet jól ismerje az AAA-t és annak konfigurálását.

7.0.2

## Mit fogok tanulni ebben a modulban?

**Modul címe:** Hitelesítés, engedélyezés és elszámolás (AAA)

**Modul célja** : AAA konfigurálása a hálózat biztonságossá tételéhez.

| **téma címe** | **Téma Cél** |
| --- | --- |
| **AAA jellemzők** | Ismertesse az AAA-t. |
| **Helyi AAA hitelesítés konfigurálása** | Állítsa be az AAA-hitelesítést a felhasználók helyi adatbázissal való ellenőrzéséhez. |
| **Szerver-alapú AAA jellemzők és protokollok** | Ismertesse a szerver alapú AAA protokollokat. |
| **Szerver-alapú hitelesítés konfigurálása** | Szerver alapú AAA hitelesítés konfigurálása Cisco útválasztókon. |
| **Szerver alapú engedélyezés konfigurálása** | Használja a megfelelő parancsokat a kiszolgáló alapú AAA engedélyezés és elszámolás konfigurálásához. |

[6.8](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Device Monitoring and Management Summary](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[7.1](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[AAA Characteristics](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                                                                                     
*                             

1. Authentication, Authorization, and Accounting (AAA)
2. AAA Characteristics

# AAA jellemzők

7.1.1

## Hitelesítés AAA nélkül

A hálózati hackerek potenciálisan hozzáférhetnek érzékeny hálózati berendezésekhez és szolgáltatásokhoz. A hozzáférés-szabályozás korlátozza, hogy ki vagy mi használhat bizonyos erőforrásokat. Ezenkívül korlátozza a hozzáférés megadása után elérhető szolgáltatásokat és lehetőségeket. A Cisco-eszközökön sokféle hitelesítés végezhető, és mindegyik módszer különböző szintű biztonságot kínál.

A távoli hozzáférés hitelesítésének legegyszerűbb módja a bejelentkezési és jelszó kombináció konfigurálása a konzolon, a vty vonalakon és az aux portokon, az ábrán látható módon.

Az ábra egy brute force támadást mutat a Telnet ellen. Egy laptop az interneten keresztül csatlakozik egy útválasztóhoz, és a cisc0, cisco1 és cisco12 jelszavakat használja a bejelentkezéshez. A router kimenete %rossz jelszó

User Access VerificationPassword: ciscoPassword: cisco1Password: cisco12% Bad passwords G0/0

S0/0/0

Internet

R1(config)# **line vty 0 4**

R1(config-line)# **password cis5cio**

R1(config-line)# **login**

Ez a módszer a legkönnyebben megvalósítható, de egyben a leggyengébb és legkevésbé biztonságos is. Ez a módszer nem jelent felelősséget. A jelszó birtokában bárki beléphet az eszközbe, és módosíthatja a konfigurációt.

Az SSH a távoli hozzáférés biztonságosabb formája. Felhasználónévre és jelszóra is szükség van, mindkettő titkosítva van az átvitel során. A helyi adatbázis módszer további biztonságot nyújt, mivel a támadónak ismernie kell a felhasználónevet és a jelszót. Nagyobb elszámoltathatóságot is biztosít, mivel a felhasználó bejelentkezésekor rögzítésre kerül a felhasználónév. Bár a Telnet felhasználónévvel és jelszóval konfigurálható, mindkettőt egyszerű szövegként küldik el, ami sebezhetővé teszi a rögzítést és a kihasználást. A helyi adatbázis módszernek vannak bizonyos korlátai. A felhasználói fiókokat minden eszközön helyileg kell konfigurálni, amint az az ábrán látható az SSH konfigurációjához.

A 2. ábra a helyi bejelentkezés és az SSH konfigurálását mutatja. Egy laptop az interneten keresztül csatlakozik az útválasztóhoz, és az adminisztrátor felhasználónevét használja a cisco1 és cisco12 jelszavakkal. A router kimenete %login érvénytelen.

G0/0 S0/0/0

User Access VerificationUsername: AdminPassword: cisco1% Login invalidUsername: AdminPassword: cisco12% Login invalid

Internet

R1(config)# **username Admin algorithm-type scrypt secret Str0ng5rPa55w0rd**

R1(config)# **ip domain-name netsec.com**

R1(config)# **crypto key generate rsa general-keys modulus 2048**

The name for the keys will be: R1.netsec.com

% The key modulus size is 2048 bits

% Generating 2048 bit RSA keys, keys will be non-exportable...

[OK] (elapsed time was 1 seconds)

\*Jan 17 14:32:53.846: %CRYPTO\_ENGINE-5-KEY\_ADDITION: A key named R1.netsec.com has been generated or imported by crypto-engine

\*Jan 17 14:32:53.847: %SSH-5-ENABLED: SSH 1.99 has been enabled

\*Jan 17 14:32:54.116: %CRYPTO\_ENGINE-5-KEY\_ADDITION: A key named R1.netsec.com.server has been generated or imported by crypto-engine

R1(cofig)#

R1(config)# **line vty 0 4**

R1(config-line)# **transport input ssh**

R1(config-line)# **login local**

Egy nagyvállalati környezetben, ahol több útválasztó és kapcsoló kezelhető, időbe telhet a helyi adatbázisok bevezetése és módosítása az egyes eszközökön. Ezenkívül a helyi adatbázis-konfiguráció nem biztosít tartalék hitelesítési módszert. Például mi van akkor, ha a rendszergazda elfelejti az eszköz felhasználónevét és jelszavát? Mivel nem áll rendelkezésre biztonsági mentési módszer a hitelesítéshez, a jelszó-visszaállítás az egyetlen lehetőség.

Jobb megoldás, ha minden eszköz ugyanarra a felhasználónevek és jelszavak adatbázisára hivatkozik egy központi szerverről. Ez a modul megvizsgálja a hálózati hozzáférés biztosításának különféle módszereit AAA használatával a Cisco útválasztók biztonságossá tétele érdekében.

7.1.2

## AAA komponensek

Az AAA hálózati biztonsági szolgáltatások biztosítják az elsődleges keretrendszert a hozzáférés-vezérlés beállításához a hálózati eszközökön. Az AAA egy módja annak, hogy ellenőrizzék, ki férhet hozzá a hálózathoz (hitelesítés), és mit tehet, amíg ott tartózkodik (engedélyezés). Az AAA lehetővé teszi azon műveletek auditálását is, amelyeket a felhasználók a hálózathoz való hozzáférés során (könyvelés) hajtanak végre.

A hálózati és adminisztratív AAA biztonság a Cisco környezetben három funkcionális összetevőből áll:

* **Hitelesítés** – A felhasználóknak és a rendszergazdáknak igazolniuk kell személyazonosságukat, mielőtt hozzáférnének a hálózathoz és a hálózati erőforrásokhoz. A hitelesítés létrehozható felhasználónév és jelszó kombinációk, kihívás- és válaszkérdések, tokenkártyák és egyéb módszerek segítségével. Például: „Diák felhasználó vagyok, és tudom a jelszót, ami ezt bizonyítja.”
* **Engedélyezés** – A felhasználó hitelesítése után az engedélyezési szolgáltatások meghatározzák, hogy a felhasználó mely erőforrásokhoz férhet hozzá, és milyen műveleteket hajthat végre. Példa erre: „A „tanuló” felhasználó csak SSH használatával érheti el az XYZ gazdagépet.
* **Könyvelés és auditálás** – A könyvelés rögzíti a felhasználó tevékenységét, beleértve a hozzáférést, az erőforrás elérésének időtartamát és a végrehajtott változtatásokat. A könyvelés nyomon követi a hálózati erőforrások felhasználását. Példa erre: „A „tanuló” felhasználó 15 percig SSH használatával hozzáfért az XYZ gazdagéphez.

Ez a koncepció hasonló a hitelkártya használatához, amint azt az ábra mutatja. A hitelkártya azonosítja, hogy ki használhatja, mennyit költhet az adott felhasználó, és számot tart arról, hogy a felhasználó milyen termékeket vagy szolgáltatásokat vásárolt.

Az ábrán egy hitelkártya látható a hitelkártya-kivonat mellett. A hitelkártyán lévő számok körül egy téglalap található, amelyen a következő szöveg található: Hitelesítés Ki vagy? A második téglalap a hitelkeret körül van a hitelkártya-kivonaton, és a következő szöveggel: Engedélyezés Mennyit tud költeni? A harmadik téglalap a hitelkártya-összesítő tranzakciós része körül van, és a Számvitel szöveggel. Mit költött rá?



**Hitelesítés**   
  
Ki vagy te? **Engedélyezés**   
  
Mennyit tudsz költeni? **Könyvelés**   
  
mire költötted?

7.1.3

## Hitelesítési módok

Az AAA hitelesítés használható a felhasználók hitelesítésére az adminisztratív hozzáféréshez, vagy a távoli hálózati hozzáféréshez. A Cisco két általános módszert kínál az AAA-szolgáltatások megvalósítására:

* **Helyi AAA hitelesítés** – A helyi AAA helyi adatbázist használ a hitelesítéshez. Ezt a módszert néha önálló hitelesítésnek is nevezik. Ebben a kurzusban erre helyi AAA hitelesítésként hivatkozunk. Ez a módszer helyileg tárolja a felhasználóneveket és jelszavakat a Cisco útválasztóban, és a felhasználók a helyi adatbázis alapján hitelesítik magukat, ahogy az ábrán is látható. Ez az adatbázis ugyanaz, mint a szerep alapú CLI létrehozásához szükséges. A helyi AAA ideális kis hálózatokhoz.

Az ábra Helyi AAA hitelesítés feliratot kapott. Ez egy távoli felhasználóból és egy útválasztóból áll. A router AAA Router felirattal van ellátva. Egy nyíl mutat a felhasználótól a router felé. Ez a nyíl 1-gyel van megjelölve. Egy másik nyíl az útválasztótól a felhasználó felé mutat. 2-es címkével van ellátva. Végül az útválasztót 3-as címkével látták el

1 2

3

Távoli kliens AAA router

1. A kliens kapcsolatot létesít a routerrel.
2. Az AAA router felhasználónevet és jelszót kér a felhasználótól.
3. Az útválasztó hitelesíti a felhasználónevet és a jelszót a helyi adatbázis használatával, és a felhasználó hozzáférést biztosít a hálózathoz a helyi adatbázisban lévő információk alapján.

* **Szerver alapú AAA hitelesítés** - A kiszolgáló alapú módszerrel az útválasztó egy központi AAA kiszolgálóhoz ér el, például a Cisco Secure Access Control System (ACS) for Windows rendszerhez, amely az ábrán látható. A központi AAA szerver tartalmazza az összes felhasználó felhasználónevét és jelszavát. Az útválasztó vagy a távoli hitelesítési betárcsázó felhasználói szolgáltatás (RADIUS) vagy a Terminal Access Controller Access Control System (TACACS+) protokollt használja az AAA-kiszolgálóval való kommunikációhoz. Ha több útválasztó és kapcsoló van, a szerveralapú AAA megfelelőbb, mivel a fiókok központi helyről adminisztrálhatók, nem pedig az egyes eszközökön.

**Megjegyzés:** Ebben a kurzusban a középpontban a hálózati biztonság IPv4-gyel való megvalósítása áll a Cisco útválasztókon, kapcsolókon és adaptív biztonsági eszközökön. Alkalmanként hivatkoznak IPv6-specifikus technológiákra és protokollokra.

Az ábra a Szerver alapú AAA hitelesítés feliratot kapta. Az ábra egy távoli kliensből, egy AAA router címkével ellátott útválasztóból és egy AAA Server nevű kiszolgálóból áll. Ez a szerver csatlakozik az útválasztóhoz. Egy nyíl mutat a távoli kliensről az AAA útválasztóra. Az 1 címkével van ellátva. Egy nyíl mutat az AAA útválasztótól a távoli kliens felé. 2-es címkével van ellátva. Kétfejű nyíl mutat az útválasztó és a szerver között. 3-mal van jelölve. Az AAA router 4-gyel.

### Szerver alapú AAA hitelesítés

1 2 4

3

Távoli kliens AAA router **AAA szerver**

1. A kliens kapcsolatot létesít a routerrel.
2. Az AAA router felhasználónevet és jelszót kér a felhasználótól.
3. Az útválasztó hitelesíti a felhasználónevet és a jelszót egy AAA-szerver segítségével.
4. A felhasználó hozzáférést biztosít a hálózathoz a távoli AAA-szerveren található információk alapján.

7.1.4

## Engedélyezés

Miután a felhasználók sikeresen hitelesítésre kerültek a kiválasztott AAA-adatforráshoz – akár helyi, akár szerveralapú –, az ábrán látható módon jogosultak lesznek bizonyos hálózati erőforrásokra.

Az ábra AAA jogosultság felirattal van ellátva. Az ábra egy távoli kliensből, egy Perimeter router feliratú útválasztóból és egy AAA Server nevű kiszolgálóból áll. Ez a szerver csatlakozik az útválasztóhoz. Kétirányú nyíl mutat az útválasztóról a szerverre. Az 1 feliratú. Egy nyíl mutat az útválasztótól a szerver felé. 2-es címkével van ellátva. Egy nyíl mutat a szerverről az útválasztóra. 3-mal van ellátva.

### AAA engedély

1 2

3

Remote Client Perimeter Router AAA Server

1. A felhasználó hitelesítése után munkamenet jön létre az útválasztó és a szerver között.
2. Az útválasztó engedélyt kér az AAA-kiszolgálótól az ügyfél által kért szolgáltatáshoz.
3. Az AAA szerver PASS/FAIL értéket ad vissza az engedélyezéshez.

Az engedélyezés szabályozza, hogy a felhasználók mit tehetnek és mit nem tehetnek a hálózaton hitelesítésük után. Ez hasonló ahhoz, ahogy a jogosultsági szintek és a szerep alapú parancssori felület a felhasználók számára meghatározott jogokat és jogosultságokat biztosít az útválasztó egyes parancsaihoz.

Az engedélyezést általában AAA-szerver segítségével hajtják végre. Az engedélyezés attribútumokat használ, amelyek leírják a felhasználó hálózathoz való hozzáférését. Ezeket az attribútumokat a rendszer összehasonlítja az AAA adatbázisban található információkkal, és meghatározza az adott felhasználóra vonatkozó korlátozásokat, és elküldi a helyi útválasztónak, amelyhez a felhasználó csatlakozik.

Az engedélyezés automatikus, és nem követeli meg a felhasználóktól, hogy további lépéseket hajtsanak végre a hitelesítés után. Az engedélyezés azonnal megtörténik a felhasználó hitelesítése után.

7.1.5

## Könyvelés

Az AAA Accounting használati adatokat gyűjt és jelentéseket készít. Ezek az adatok felhasználhatók olyan célokra, mint például auditálás vagy számlázás. Az összegyűjtött adatok tartalmazhatják a csatlakozás kezdeti és leállítási idejét, a végrehajtott parancsokat, a csomagok számát és a bájtok számát.

A könyvelés AAA szerverrel valósul meg. Ez a szolgáltatás használati statisztikákat küld vissza az ACS-kiszolgálónak. Ezek a statisztikák kinyerhetők, hogy részletes jelentéseket készítsenek a hálózat konfigurációjáról.

A számvitel egyik széles körben elterjedt alkalmazása az AAA hitelesítéssel való kombinálása. Ez segíti a hálózati adminisztrátorok hozzáférésének kezelését az internetes eszközökhöz. A könyvelés nagyobb biztonságot nyújt, mint a hitelesítés. Az AAA szerverek részletes naplót vezetnek arról, hogy a hitelesített felhasználó pontosan mit csinál az eszközön, ahogy az az ábrán is látható. Ez magában foglalja a felhasználó által kiadott összes EXEC és konfigurációs parancsot. A napló számos adatmezőt tartalmaz, beleértve a felhasználónevet, a dátumot és az időt, valamint a felhasználó által beírt tényleges parancsot. Ez az információ az eszközök hibaelhárítása során hasznos. A rosszindulatú tevékenységeket végrehajtó személyek ellen is befolyást biztosít.

Az ábra AAA számvitel feliratot viseli. Az ábra egy távoli kliensből, egy Perimeter Router nevű útválasztóból és egy nem címkézett szerverből áll. A szerver csatlakozik a routerhez. egy nyíl mutat az útválasztóról a szerverre. 1-es címkével van ellátva. Egy másik nyíl az útválasztóról a szerverre mutat. 2-es címkével van ellátva

### AAA számvitel

1

2

Remote Client Perimeter Router

1. Amikor egy felhasználót hitelesítettek, az AAA könyvelési folyamat egy start üzenetet generál a könyvelési folyamat elindításához.
2. Amikor a felhasználó befejezi, egy stop üzenet kerül rögzítésre, és a könyvelési folyamat véget ér.

Kattintson az alábbiakra, ha többet szeretne megtudni az AAA könyvelés által gyűjtött információk típusairól.

hálózati számvitel:

A hálózati számlázás használati rekordokat gyűjt a különféle távoli elérési kapcsolatokon keresztüli hálózati hozzáféréshez.

kapcsolódási könyvelés:

A kapcsolatok elszámolása információkat rögzít az AAA-kliensből (például Telnet vagy SSH) létrehozott összes kimenő kapcsolatról

EXEC számvitel:

Az EXEC-könyvelés információkat rögzít a hálózati hozzáférési szerveren lévő felhasználói EXEC terminálmunkamenetekről (felhasználói shellekről), beleértve a felhasználónevet, a dátumot, a kezdési és befejezési időpontokat, valamint a hozzáférési szerver IP-címét.

rendszerkönyvelés:

A rendszerkönyvelés az összes rendszerszintű eseményről információkat rögzít (például a rendszer újraindításakor vagy a számlázás be- vagy kikapcsolásakor).

paracs számvitel:

A parancsok elszámolása információkat rögzít a hálózati hozzáférési kiszolgálón végrehajtott, meghatározott jogosultsági szinthez tartozó EXEC shell parancsokról. Minden parancskönyvelési rekord tartalmazza az adott jogosultsági szinthez végrehajtott parancsok listáját, valamint az egyes parancsok végrehajtásának dátumát és időpontját, valamint a végrehajtó felhasználót.

7.1.6

## Ellenőrizze, hogy megértette-e az AAA jellemzőit

Az űrlap teteje

Ellenőrizze, hogy megértette-e az AAA jellemzőit, ha meghatározza, hogy a nyilatkozat hitelesítést, engedélyezést vagy könyvelést ír-e le.

1. Rögzíti a felhasználó tevékenységét, beleértve a hozzáférést, az erőforrás elérésének időtartamát és a végrehajtott változtatásokat.

Az űrlap alja

Létrehozott attribútumkészletet használ, amely leírja a felhasználó hálózathoz való hozzáférését.

Felhasználónév és jelszó kombinációk, kihívás- és válaszkérdések, tokenkártyák és egyéb módszerek felhasználásával jött létre.

Használati adatokat gyűjt és jelentéseket készít, hogy azokat felhasználhassák olyan célokra, mint például auditálás vagy számlázás.

A felhasználóknak és a rendszergazdáknak bizonyítaniuk kell, hogy azok, akiknek mondják magukat.

Mit tehet és mit nem a felhasználó a hálózaton.

Meghatározza, hogy a felhasználó mely erőforrásokhoz férhet hozzá, és mely műveleteket hajthat végre.

Hozzájárulást biztosít a rosszindulatú tevékenységeket végrehajtó egyének ellen.

Egy mód annak szabályozására, hogy ki férhet hozzá a hálózathoz.

[7.0](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[7.2](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Configure Local AAA Authentication](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                                                                                         
*                             

1. Authentication, Authorization, and Accounting (AAA)

# Helyi AAA hitelesítés konfigurálása

7.2.1

## Adminisztrátori hozzáférés hitelesítése

A helyi AAA hitelesítést kisebb hálózatokhoz kell konfigurálni. Kisebb hálózatok azok a hálózatok, amelyek egy vagy két hálózati eszközzel rendelkeznek, amelyek korlátozott számú felhasználó számára biztosítanak hozzáférést. Ez a módszer az eszközön konfigurált és tárolt helyi felhasználóneveket és jelszavakat használja. A rendszeradminisztrátornak fel kell töltenie a helyi biztonsági adatbázist úgy, hogy minden egyes bejelentkező felhasználóhoz felhasználónév- és jelszóprofilt ad meg.

hasonló a **helyi bejelentkezési** A helyi AAA hitelesítési módszer egy kivétellel parancs használatához. Az AAA lehetőséget biztosít a hitelesítés biztonsági mentési módszereinek konfigurálására is.

A helyi AAA szolgáltatások konfigurálása a rendszergazdai hozzáférés hitelesítéséhez néhány alapvető lépést igényel:

**1. lépés** . Adjon hozzá felhasználóneveket és jelszavakat a helyi útválasztó adatbázishoz azon felhasználók számára, akiknek adminisztrátori hozzáférésre van szükségük az útválasztóhoz.

**2. lépés** . Az AAA globális engedélyezése az útválasztón.

**3. lépés** . Konfigurálja az AAA paramétereket az útválasztón.

**4. lépés** . Erősítse meg és hárítsa el az AAA konfigurációt.

Az **ábrán látható aaa hitelesítési bejelentkezési** parancs lehetővé teszi az ADMIN és a JR-ADMIN felhasználók számára, hogy a konzolon vagy a vty terminálvonalakon keresztül bejelentkezzenek az útválasztóba. Az **alapértelmezett** kulcsszó azt jelenti, hogy a hitelesítési módszer minden vonalra vonatkozik, kivéve azokat, amelyeknél egy adott vonalkonfiguráció felülírja az alapértelmezettet. kulcsszó jelzi **A hitelesítés megkülönbözteti a kis- és nagybetűket, ezt a helyi kis- és nagybetűk** . Ez azt jelenti, hogy a jelszó és a felhasználónév is megkülönbözteti a kis- és nagybetűket.

R1(config)# **username JR-ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd**

R1(config)# **username ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd**

R1(config)# **aaa new-model**

R1(config)# **aaa authentication login default local-case**

R1(config)#

7.2.2

## Hitelesítési módszerek

Az AAA engedélyezéséhez először az **aaa new-mode** l globális konfigurációs parancsot kell konfigurálni. Az AAA letiltásához használja a **no formáját.** parancs

Ennek a parancsnak a beírásáig semmilyen más AAA-parancs nem érhető el.

**Megjegyzés:** Fontos tudni, hogy az **aaa new-model** parancs első beírásakor a helyi adatbázist használó, nem látott „alapértelmezett” hitelesítés automatikusan minden sorra érvényes, kivéve a konzolt. Emiatt az AAA engedélyezése előtt mindig konfiguráljon egy helyi adatbázis-bejegyzést.

Az **alább látható aaa hitelesítés bejelentkezési** paranccsal engedélyezheti a konzol, az aux és a vty vonalak hitelesítését. Az **alapértelmezett** kulcsszó minden sorra hitelesítést alkalmaz. Alternatív megoldásként egyéni hitelesítési módszer konfigurálható a listanév használatával .

Router(config)# **aaa authentication login** {**default** | list-name} method1…[ method4 ]

| **Parancs** | **Leírás** |
| --- | --- |
| **alapértelmezett** | A felsorolt ​​hitelesítési módszereket használja, amelyek ezt a kulcsszót követik a módszerek alapértelmezett listájaként, amikor egy felhasználó bejelentkezik. |
| lista név | listanév használata helyett **Az alapértelmezett** az adminisztrátor adhat meg egy nevet a dokumentációs célokra. A név legfeljebb 31 karakterből állhat. |
| 1. módszer... [ 4. módszer ] | Azonosítja azon metódusok listáját, amelyeket az AAA-hitelesítési folyamat az adott sorrendben lekérdez. Legalább egy módszert meg kell adni. Legfeljebb négy módszer adható meg. |

A parancs utolsó része azonosítja a felhasználók hitelesítéséhez lekérdezett metódusok típusát. Legfeljebb négy módszer definiálható, tartalék módszereket biztosítva arra az esetre, ha az egyik módszer nem elérhető. Amikor a felhasználó megpróbál bejelentkezni, az első felsorolt ​​módszer kerül alkalmazásra. A Cisco IOS szoftver csak akkor kísérli meg a hitelesítést a következő felsorolt ​​hitelesítési módszerrel, ha nem érkezik válasz, vagy az előző módszerből eredő hiba lép fel. Ha a hitelesítési módszer megtagadja a felhasználói hozzáférést, a hitelesítési folyamat leáll, és más hitelesítési módszerek nem engedélyezettek.

A helyi hitelesítés előre konfigurált helyi adatbázis használatával engedélyezéséhez használja a **local** vagy **local-case** kulcsszót . The difference between the two options is that **local** accepts a username regardless of case, whereas **local-case** is case-sensitive. For example, if a local database entry with the username ADMIN was configured, the **local** method would accept ADMIN, Admin, or even admin. Ha a **helyi eset-** módszert konfigurálnák, akkor csak az admin elfogadható lenne.

Annak megadásához, hogy a felhasználó hitelesíthesse az engedélyezési jelszót, használja az **enable** kulcsszót. Annak érdekében, hogy a hitelesítés akkor is sikeres legyen, ha minden metódus hibát ad vissza, adjon meg **egyet sem** végső módszerként.

**Megjegyzés** : Biztonsági okokból **használja a none** csak az AAA konfiguráció tesztelésekor kulcsszót. Soha nem szabad élő hálózaton alkalmazni.

A táblázat az általánosan megadható módszereket jeleníti meg.

| **Módszertípus Kulcsszavak** | **Leírás** |
| --- | --- |
| **engedélyezze** | A hitelesítéshez az engedélyezési jelszót használja. |
| **helyi** | A hitelesítéshez a helyi felhasználónév-adatbázist használja. |
| **helyi eset** | A kis- és nagybetűket megkülönböztető helyi felhasználónév-hitelesítést használ. |
| **egyik sem** | Nem használ hitelesítést. |
| **csoport sugara** | Az összes RADIUS-kiszolgáló listáját használja a hitelesítéshez. |
| **csoport tacacs+** | Az összes TACACS+ szerver listáját használja a hitelesítéshez. |
| **csoport**  csoportnév | A RADIUS vagy TACACS+ kiszolgálók egy részhalmazát használja a hitelesítéshez, az aaa group server radius vagy aaa group server tacacs+ parancsban meghatározottak szerint. |

7.2.3

## Alapértelmezett és elnevezett metódusok

paranccsal különböző metóduslistákat lehet alkalmazni a különböző felületekre és vonalakra **A rugalmasság érdekében az aaa hitelesítési bejelentkezési** listanév .

Például egy rendszergazda alkalmazhat egy speciális bejelentkezést az SSH-hoz, majd az alapértelmezett bejelentkezési módot használhatja a vonalkonzolhoz, ahogy a példában is látható.

R1(config)# **username JR-ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd**

R1(config)# **username ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd**

R1(config)# **aaa new-model**

R1(config)# **aaa authentication login default local-case enable**

R1(config)# **aaa authentication login SSH-LOGIN local-case**

R1(config)# **line vty 0 4**

R1(config-line)# **login authentication SSH-LOGIN**

Ebben a példában a vty sor csak a helyi adatbázist használja a hitelesítéshez. Minden más sor (pl. konzol és aux vonal) a helyi adatbázist használja, és az engedélyezési jelszót használja tartalékként, ha nem lennének adatbázis-bejegyzések az eszközön.

Vegye figyelembe, hogy a megnevezett listát kifejezetten engedélyezni kell a sorban a **bejelentkezési hitelesítési** sor konfigurációs parancsával. Ha egy sorra egyéni hitelesítési módszerek listája van alkalmazva, akkor ez a metóduslista felülírja az adott felület alapértelmezett metóduslistáját.

paranccsal vissza lehet térni az alapértelmezett metóduslistához **Ha egyéni hitelesítési metóduslistát alkalmaz egy felületen, a no authentication login** .

7.2.4

## A hitelesítési konfiguráció finomhangolása

További biztonság valósítható meg a vonalon az **aaa helyi hitelesítési kísérletek max-fail** globális konfigurációs mód paranccsal, ahogy a példában is látható. Ez a parancs biztosítja az AAA felhasználói fiókok védelmét azáltal, hogy zárolja azokat a fiókokat, amelyeknél túl sok sikertelen próbálkozás történt.

Router(config)# **aaa local authentication attempts max-fail** [number-of-unsuccessful-attempts]

| **Parancs** | **Leírás** |
| --- | --- |
| sikertelen kísérletek száma | Sikertelen hitelesítési kísérletek száma a kapcsolat megszakítása és a felhasználói fiók zárolása előtt. |

Ellentétben a **bejelentkezési késleltetési** paranccsal, amely késleltetést vezet be a sikertelen bejelentkezési kísérletek között a fiók zárolása nélkül, az **aaa helyi hitelesítési kísérletek max-fail** parancs zárolja a felhasználói fiókot, ha a hitelesítés sikertelen. A zárolt felhasználói fiók mindaddig zárolva marad, amíg azt egy rendszergazda manuálisan nem törli a **clear aaa local user lockout** privileged EXEC mode paranccsal.

Az összes kizárt felhasználó listájának megjelenítéséhez használja a **show aaa local user lockout** parancsot privilegizált EXEC módban, ahogy a példában is látható.

R1# **show aaa local user lockout**

Local-user Lock time

JR-ADMIN 04:28:49 UTC Tue Feb 16 2021

Amikor egy felhasználó bejelentkezik egy AAA-t használó Cisco útválasztóba, egy egyedi azonosító kerül hozzárendelésre a felhasználó munkamenetéhez. A munkamenet teljes élettartama során a munkamenethez kapcsolódó különféle attribútumok összegyűjtésre és tárolásra kerülnek az AAA-adatbázison belül. Ezek az attribútumok magukban foglalhatják a felhasználó IP-címét, az útválasztó eléréséhez használt protokollt (pl. PPP), a kapcsolat sebességét, valamint a fogadott vagy továbbított csomagok vagy bájtok számát.

Az egy AAA munkamenethez gyűjtött attribútumok megjelenítéséhez használja a **show aaa user** parancsot privilegizált EXEC módban. Ez a parancs nem ad információt minden olyan felhasználóról, aki bejelentkezett egy eszközre, hanem csak azok számára, akiket hitelesítettek vagy jogosultak voltak az AAA használatával, vagy akiknek a munkameneteit az AAA modul számolja el.

A **show aaa sessions** paranccsal egy munkamenet egyedi azonosítója jeleníthető meg, ahogy a példában is látható.

R1# **show aaa sessions**

Total sessions since last reload: 4

Session Id: 1

Unique Id: 175

User Name: ADMIN

IP Address: 192.168.1.10

Idle Time: 0

CT Call Handle: 0

7.2.5

## Lab – Helyi AAA-hitelesítés konfigurálása

Ebben a laborban a következő célokat kell teljesítenie:

* 1. rész: Alapvető eszközbeállítások konfigurálása.
* 2. rész: Helyi hitelesítés konfigurálása.
* 3. rész: Helyi hitelesítés konfigurálása AAA használatával.

7.2.6

## Packet Tracer – Helyi AAA konfigurálása a konzolhoz és a VTY hozzáféréshez

Ebben a PT tevékenységben beállíthatja az AAA helyi hitelesítést a konzolon és a VTY vonalakon SSH-val.

[Konfigurálja a helyi AAA-t a konzolhoz és a VTY-hozzáféréshez](https://contenthub.netacad.com/courses/netsec/_common/7.2.6-packet-tracer---configure-local-aaa-for-console-and-vty-access.pka)

[7.1](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[AAA Characteristics](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[7.3](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Server-Based AAA Characteristics and Protocols](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                                                                                             
*                             

1. Authentication, Authorization, and Accounting (AAA)
2. Server-Based AAA Characteristics and Protocols

# Szerver-alapú AAA jellemzők és protokollok

7.3.1

## Hasonlítsa össze a helyi AAA és a szerver alapú AAA megvalósításokat

Az AAA helyi megvalósítása nagyon kis hálózatokban elfogadható. A helyi hitelesítés azonban nem skálázódik jól.

A legtöbb vállalati környezet több útválasztóval, kapcsolóval és egyéb infrastrukturális eszközzel, több útválasztó adminisztrátorral és több száz vagy több ezer felhasználóval rendelkezik, akiknek hozzáférésre van szükségük a vállalati LAN-hoz. A helyi adatbázis fenntartása minden eszközön ekkora hálózat esetén nem kivitelezhető.

Ennek a kihívásnak a megoldására egy vagy több AAA-szerver használható a teljes vállalati hálózat felhasználói és adminisztratív hozzáférési igényeinek kezelésére. Az AAA szerverszoftver képes létrehozni egy központi felhasználói és adminisztratív hozzáférési adatbázist, amelyre a hálózat összes eszköze hivatkozhat. Számos külső adatbázissal is működhet, beleértve az Active Directory-t és a Lightweight Directory Access Protocol-t (LDAP). Ezek az adatbázisok felhasználói fiókadatokat és jelszavakat tárolnak, lehetővé téve a felhasználói fiókok központi adminisztrációját. A redundancia növelése érdekében több szerver is megvalósítható. Az ábra a router rendszergazda felhasználói hitelesítésének folyamatát mutatja be.

Az ábra azt mutatja, hogy a felhasználó egy routerhez csatlakozik, amely három aaa szerverhez csatlakozik. egy nyíl mutat a felhasználótól a router felé. felirattal 1. egy nyíl mutat a routertől a felhasználó felé. felirattal 2. egy kétfejű nyíl mutat az aaa szerverek és a router között. felirattal 3. egy másik kétfejű nyíl mutat a felhasználó és az aaa szerverek között. 4-es címkével van ellátva.

### Szerver alapú hitelesítés

1 2 3

4

AAA   
szerver AAA   
szerver AAA   
szerver

1. A felhasználó kapcsolatot létesít az útválasztóval.
2. A router felhasználónevet és jelszót kér a felhasználótól.
3. Az útválasztó átadja a felhasználónevet és jelszót a Cisco Secure ACS-nek (szervernek vagy motornak).
4. A Cisco Secure ACS hitelesíti a felhasználót. A felhasználó hozzáférést biztosít az útválasztóhoz (adminisztrátori hozzáférés) vagy a hálózathoz a Cisco Secure ACS adatbázisban található információk alapján.

7.3.2

## Cisco Identity Services Engine (ISE)

A Cisco Identity Services Engine (ISE) egy identitás- és hozzáférés-ellenőrzési házirend-platform, amely lehetővé teszi a vállalatok számára, hogy kikényszerítsék a megfelelőséget, fokozzák az infrastruktúra biztonságát, és egyszerűsítsék szolgáltatási műveleteiket. A Cisco ISE architektúrája lehetővé teszi a vállalatok számára, hogy valós idejű környezeti információkat gyűjtsenek a hálózatokról, felhasználókról és eszközökről. Az adminisztrátor ezután felhasználhatja ezeket az információkat proaktív irányítási döntések meghozatalára az identitás különböző hálózati elemekkel való összekapcsolásával. Ezek a hálózati elemek közé tartoznak a hozzáférési kapcsolók, a vezeték nélküli LAN-vezérlők (WLC-k), a VPN-k, az átjárók és az adatközponti kapcsolók.

A BYOD (Bring Your Own Device) egyre gyakoribb, sőt szükséges is sok vállalatnál. A Cisco ISE méltányos hozzáférési házirendeket határoz meg, és kikényszeríti a megfelelőséget minden végeszköznél, beleértve a BYOD-ot is.

A Cisco ISE a Cisco TrustSec fő házirend-összetevője, és egy olyan Cisco-technológia, amely megvédi az olyan eszközöket, mint az adatok, alkalmazások és mobileszközök a jogosulatlan hozzáféréstől. A Cisco ISE egyetlen készülékben egyesíti a szabályzat meghatározását, vezérlését és jelentését. Az ISE együttműködik a meglévő hálózati infrastruktúrával, hogy a hálózati rendszergazdáknak információkat biztosítson a hálózathoz csatlakozó végeszközökről (végpontoknak).

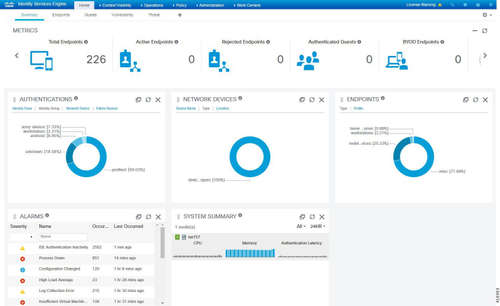
Az ISE számos jellemzője:

* **Eszköz láthatósága** – Láthatóságot és ellenőrzést biztosít afelől, hogy ki és mi tartózkodik folyamatosan a hálózaton vezeték nélküli, vezetékes és VPN-kapcsolatokon keresztül. A Cisco ISE szondák és eszközérzékelők segítségével figyeli, hogyan csatlakoznak az eszközök a hálózathoz. A kiterjedt Cisco ISE profiladatbázis osztályozza az eszközt. Ez biztosítja a megfelelő szintű hálózati hozzáférés biztosításához szükséges láthatóságot és kontextust.
* **Testtartás értékelése** – Meghatározza, hogy az eszköz megfelel-e az eszközbiztonsági szabályzatoknak, mielőtt csatlakozik a hálózathoz. Meg tudja állapítani, hogy az eszköz mentes-e a vírusoktól és a gyanús alkalmazásoktól, és még arról is meggyőződhet, hogy az eszköz víruskereső szoftvere naprakész.
* **Szegmentáció** – A Cisco ISE környezetfüggő adatokat használ a hálózati eszközökről és végpontokról a hálózat szegmentálásának elősegítésére. Biztonsági csoportcímkék, hozzáférés-vezérlési listák, hálózati hozzáférési protokollok és az engedélyezést, hozzáférést és hitelesítést meghatározó házirend-készletek néhány olyan módszer, amellyel a Cisco ISE lehetővé teszi a biztonságos hálózatszegmentálást.
* **Vendégkezelés és biztonságos vezeték nélküli hálózat** – Lehetővé teszi a biztonságos hálózati hozzáférést a látogatók, vállalkozók, tanácsadók és ügyfelek számára.
* **Fenyegetés elleni védelem** – Ha a Cisco ISE fenyegetést vagy sebezhetőségi attribútumot észlel egy végpontról, adaptív hálózati vezérlési házirendek küldése dinamikusan módosítja a végpont hozzáférési szintjeit. A fenyegetés vagy a sebezhetőség értékelése és kezelése után a végpont visszaadható az eredeti hozzáférési szabályzata.

Az ISE környezettudatos identitáskezelést biztosít:

* Annak megállapítása, hogy a felhasználók egy engedélyezett, szabályzatnak megfelelő eszközön férnek-e hozzá a hálózathoz
* Felhasználói identitás, hely és hozzáférési előzmények megállapítása, amelyek felhasználhatók a megfeleléshez és a jelentésekhez
* Szolgáltatások hozzárendelése a hozzárendelt felhasználói szerepkör, csoport és kapcsolódó házirend (munkakör, hely, eszköztípus stb.) alapján
* A hitelesített felhasználók hozzáférésének biztosítása a hálózat meghatározott szegmenseihez, vagy meghatározott alkalmazásokhoz és szolgáltatásokhoz, vagy mindkettőhöz, a hitelesítési eredmények alapján

Az ábra a Cisco ISE felügyeleti konzol nézetét mutatja.



7.3.3

## A TACACS+ és RADIUS protokollok

A TACACS+ és a RADIUS egyaránt hitelesítési protokoll, amelyet az AAA szerverekkel való kommunikációhoz használnak. Ahogy a táblázatban látható, mindegyik más-más képességet támogat.

| **Képességek** | **TACACS+** | **SUGÁR** |
| --- | --- | --- |
| **Funkcionalitás** | Elválasztja az AAA-t az AAA architektúra szerint, lehetővé téve a biztonsági szerver megvalósításának modularitását | Egyesíti a hitelesítést és az engedélyezést, de elkülöníti a könyvelést, így kevesebb rugalmasságot tesz lehetővé a megvalósításban, mint a TACACS+ |
| **Alapértelmezett** | Többnyire Cisco támogatott | Nyílt/RFC szabvány |
| **Szállítási protokoll** | TCP | UDP |
| **PASAS** | Kétirányú kihívás és válasz a Challenge Handshake Authentication Protocol (CHAP) protokollban | Egyirányú kihívás és válasz a RADIUS biztonsági kiszolgálótól a RADIUS ügyfél felé |
| **Titoktartás** | A teljes csomag titkosítva | Jelszó titkosítva |
| **Testreszabás** | Felhasználónként vagy csoportonként engedélyezi az útválasztó parancsait | Nincs lehetősége az útválasztó parancsainak felhasználónkénti vagy csoportonkénti engedélyezésére |
| **Könyvelés** | Korlátozott | Kiterjedt |

Az, hogy a TACACS+ vagy a RADIUS kerül kiválasztásra, a szervezet igényeitől függ. Például egy nagy internetszolgáltató választhatja a RADIUS-t, mert támogatja a számlázó felhasználók számára szükséges részletes elszámolást. A különböző felhasználói csoportokkal rendelkező szervezetek választhatják a TACACS+-t, mert az engedélyezési házirendeket felhasználónként vagy csoportonként alkalmaz.

Fontos megérteni a TACACS+ és RADIUS protokollok közötti sok különbséget.

Ez három kritikus tényező a TACACS+ számára:

* Elválasztja a hitelesítést és az engedélyezést
* Titkosítja az összes kommunikációt
* A 49-es TCP portot használja

Ez négy kritikus tényező a RADIUS számára:

* Egy folyamatként egyesíti a RADIUS hitelesítést és az engedélyezést
* Csak a jelszót titkosítja
* UDP-t használ
* Támogatja a távelérési technológiákat, a 802.1X-et és a Session Initiation Protocol-t (SIP)

Míg mindkét protokoll használható az útválasztó és az AAA-kiszolgálók közötti kommunikációra, a TACACS+ a biztonságosabb protokollnak tekinthető. Ennek az az oka, hogy az összes TACACS+ protokollcsere titkosított, míg a RADIUS csak a felhasználó jelszavát titkosítja. A RADIUS nem titkosítja a felhasználóneveket, a könyvelési információkat vagy a RADIUS-üzenetben található egyéb információkat.

7.3.4

## TACACS+ hitelesítés

A TACACS+ az eredeti TACACS protokoll Cisco továbbfejlesztése. Neve ellenére a TACACS+ egy teljesen új protokoll, amely nem kompatibilis a TACACS korábbi verzióival. A TACACS+-t a Cisco útválasztók és hozzáférési kiszolgálók családja támogatja.

A TACACS+ különálló AAA szolgáltatásokat nyújt. Az AAA szolgáltatások elválasztása rugalmasságot biztosít a megvalósításban, mivel a TACACS+ -ot használhatja engedélyezéshez és számvitelhez egy másik hitelesítési módszer használatakor.

A TACACS+ protokoll bővítményei több típusú hitelesítési kérelmet és válaszkódot biztosítanak, mint az eredeti TACACS specifikációban. A TACACS+ többprotokoll támogatást kínál, mint például az IP és a régi AppleTalk. A normál TACACS+ működés titkosítja a csomag egészét a biztonságosabb kommunikáció érdekében, és a 49-es TCP-portot használja.

Kattintson az ábrán a Lejátszás gombra a TACACS+ hitelesítési folyamat megtekintéséhez.

van egy kliens számítógép, egy útválasztó és egy aaa szerver. egy nyíl mutat a kliensről a routerre. 1 connect felirattal van ellátva. an arrow points from the router to the aaa server. 2 felhasználónév kéréssel van ellátva? an arrow points from the aaa server to the router. a 3 use username felirattal van ellátva. an arrow points from the router to the client. it is labeled 4 username?. an arrow points from the client to the router. it is labeled 5 JR-ADMIN. an arrow points from the router to the aaa server. 6 jr-admin címkével rendelkezik. egy nyíl mutat az útválasztóról az aaa szerverre. it is labeled 7 password prompt? an arrow points from the aaa server to the router. a 8 use password felirattal van ellátva. an arrow points from the router to the client. it is labeled 9 password? egy nyíl mutat a kliensről a routerre. 10 S tr 0 ng P a 5 5 w 0 r d felirattal van ellátva. an arrow points from the router to the aaa server. 11 s TR 0 ng P A 5 5 W 0 R D jelöléssel rendelkezik. an arrow points from the aaa server to the router. it is labeled 12 Accept / Reject

### A TACACS+ hitelesítési folyamat

Password prompt?

Jr-admin

Jr-admin

Felhasználónév?

Használja a „felhasználónevet”

Felhasználónév kérése?

Csatlakozás

Use “Password”

Jelszó?

**Ügyfél**

**AAA**

Str0ngPa55w0rd

Elfogad elutasít

Str0ngPa55w0rd

7.3.5

## RADIUS hitelesítés

A RADIUS, amelyet a Livingston Enterprises fejlesztett ki, egy nyílt IETF szabvány AAA protokoll olyan alkalmazásokhoz, mint a hálózati hozzáférés vagy az IP-mobilitás. RADIUS works in both local and roaming situations and is commonly used for accounting purposes. RADIUS is currently defined by RFCs 2865, 2866, 2867, 2868, 3162 and 6911.

A csomag többi része azonban egyszerű szövegként kerül elküldésre.

A RADIUS egy folyamatként egyesíti a hitelesítést és az engedélyezést. Amikor egy felhasználót hitelesítenek, az a felhasználó is jogosult lesz. A RADIUS az 1645-ös vagy az 1812-es UDP-portot használja a hitelesítéshez, az 1646-os vagy az 1813-as UDP-portot pedig a könyveléshez.

A RADIUS egy általános hitelesítési protokoll is, amelyet a 802.1X biztonsági szabvány használ.

Kattintson a Play elemre az ábrán a RADIUS hitelesítési folyamat megtekintéséhez.

van egy kliens számítógép, egy útválasztó és egy aaa szerver. egy nyíl pont az útválasztótól az ügyfélig. 1 felhasználónév címkével rendelkezik? egy nyíl mutat a kliensről a routerre. it is labeled 2 JR-ADMIN. egy nyíl pont az útválasztótól az ügyfélig. it is labeled 3 password? egy nyíl mutat a kliensről a routerre. 4 s tr 0 ng p a 5 5 w 0 r d jelöléssel rendelkezik. egy nyíl mutat az útválasztóról az aaa szerverre. it is labeled 5 Access - Request (JR-ADMIN, S tr 0 ng P a 5 5 w 0 rd). an arrow points from the aaa server to the router. it is labeled 6 Access - Accept

### A RADIUS-hitelesítés folyamata

Hozzáférés

Access-Request  
(JR-ADMIN, "Str0ngPa55w0rd")

Str0ngPa55w0rd

Jelszó?

Jr-admin

Felhasználónév?

**Ügyfél**

**AAA**

7.3.6

## Ellenőrizze, hogy megértette-e az AAA kommunikációs protokollt

Kattintson az egyes szolgáltatások melletti megfelelő mezőre a kommunikációs protokoll jelzéséhez.

Összeférhetetlen az elődeivel

[TACACS+](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "TACACS+)

[SUGÁR](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "RADIUS)

A méretezhetőség érdekében proxyszervert használ

[TACACS+](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "TACACS+)

[SUGÁR](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "RADIUS)

Elválasztja a hitelesítést és az engedélyezést

[TACACS+](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "TACACS+)

[SUGÁR](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "RADIUS)

Egyesíti a hitelesítést és az engedélyt egy folyamatként

[TACACS+](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "TACACS+)

[SUGÁR](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "RADIUS)

Csak a jelszót titkosítja

[TACACS+](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "TACACS+)

[SUGÁR](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "RADIUS)

Titkosítja az összes kommunikációt

[TACACS+](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "TACACS+)

[SUGÁR](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "RADIUS)

A 49-es TCP portot használja

[TACACS+](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "TACACS+)

[SUGÁR](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "RADIUS)

UDP-t használ

[TACACS+](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "TACACS+)

[SUGÁR](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "RADIUS)

Támogatja a távelérési technológiákat, a 802.1X-et és a SIP-t

[TACACS+](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "TACACS+)

[SUGÁR](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "RADIUS)

[7.2](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Configure Local AAA Authentication](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[7.4](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Configure Server-Based Authentication](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                                                                                                    
*                             

1. Authentication, Authorization, and Accounting (AAA)

# Szerver-alapú hitelesítés konfigurálása

7.4.1

## A kiszolgálóalapú AAA-hitelesítés konfigurálásának lépései

A helyi AAA-hitelesítéstől eltérően a szerveralapú AAA-nak azonosítania kell a különböző TACACS+ és RADIUS-kiszolgálókat, amelyekre az AAA-szolgáltatásnak konzultálnia kell a felhasználók hitelesítése és engedélyezése során.

A szerver alapú hitelesítés konfigurálásához négy alapvető lépés van.

**1. lépés** . Globálisan engedélyezze az AAA-t, hogy engedélyezze az összes AAA-elem használatát. Ez a lépés az összes többi AAA-parancs előfeltétele.

**2. lépés** . Adja meg azt a kiszolgálót, amely AAA szolgáltatásokat nyújt az útválasztó számára. Ez lehet TACACS+ vagy RADIUS szerver.

**3. lépés** . Állítsa be a hálózati eszköz és az AAA-kiszolgáló közötti adatátvitel titkosításához szükséges titkosítási kulcsot.

**4. lépés** . Állítsa be az AAA hitelesítési módszerek listáját úgy, hogy a TACACS+ vagy RADIUS szerverre hivatkozzon. Redundancia érdekében egynél több szerver konfigurálható.

7.4.2

## Konfigurálja a TACACS+ szervereket

A TACACS+ és RADIUS protokollok az ügyfelek és az AAA biztonsági szerverek közötti kommunikációra szolgálnak. Az ábra a témakör AAA hivatkozási topológiáját mutatja.

Az ábrán egy 192.168.1.100 IP-című RADIUS-kiszolgálóhoz csatlakoztatott útválasztó látható. Az útválasztó 192.168.1.101 IP-című TACACS+ szerverhez is csatlakozik.

### Szerver-alapú AAA referencia topológia

R1 192.168.1.100

192.168.1.101

RADIUS Server TACACS+ Szerver

A TACACS+ szerver konfigurálásához globálisan engedélyezze az AAA-t az **aaa new-model** paranccsal. Ezután használja a **tacacs szervernév** parancsot . TACACS+ szerver konfigurációs módban konfigurálja a TACACS+ szerver IPv4-címét az **address ipv4** paranccsal. Az **address ipv4** parancs lehetővé teszi a hitelesítési port és a számlázási port módosítását. IPv6-címet is megadhat az **address ipv6** ipv6-address paranccsal.

Ezután az **egykapcsolatos** paranccsal növelheti a TCP teljesítményét egyetlen TCP-kapcsolat fenntartásával a munkamenet teljes időtartama alatt. Ellenkező esetben alapértelmezés szerint minden munkamenethez megnyílik és bezárja a TCP-kapcsolatot. Ha szükséges, több TACACS+ szerver is azonosítható a megfelelő IPv4-címek megadásával a **tacacs** szervernév paranccsal.

A **kulcskulcs** parancs a megosztott titkos kulcs konfigurálására szolgál a TACACS+ szerver és az AAA-kompatibilis útválasztó közötti adatátvitel titkosítására. Ezt a kulcsot pontosan ugyanúgy kell konfigurálni mind a routeren, mind a TACACS+ szerveren.

A példa egy minta TACACS+ szerverkonfigurációt jelenít meg.

R1(config)# **aaa new-model**

R1(config)#

R1(config)# **tacacs server Server-T**

R1(config-server-tacacs)# **address ipv4 192.168.1.101**

R1(config-server-tacacs)# **single-connection**

R1(config-server-tacacs)# **key TACACS-Pa55w0rd**

R1(config-server-tacacs)# **exit**

R1(config)#

7.4.3

## Konfigurálja a RADIUS szervereket

A RADIUS-kiszolgáló konfigurálásához használja a **radius server** name parancsot. Ezzel sugárkiszolgáló konfigurációs módba kerül.

Mivel a RADIUS UDP-t használ, nincs ezzel egyenértékű **egykapcsolatos** kulcsszó. Ha szükséges, több RADIUS-kiszolgáló azonosítható úgy, hogy **megad egy radius server** name parancsot. mindegyik kiszolgálóhoz

RADIUS-kiszolgáló konfigurációs módban konfigurálja a RADIUS-kiszolgáló IPv4-címét az **address ipv4** ipv4-address paranccsal. IPv6-címet is megadhat az **address ipv6** ipv6-address paranccsal.

A Cisco útválasztók alapértelmezés szerint az 1645-ös portot használják a hitelesítéshez és az 1646-os portot a könyveléshez. Az IANA azonban lefoglalta az 1812-es portot a RADIUS hitelesítési porthoz, és az 1813-as portot a RADIUS elszámolási porthoz. Fontos, hogy ezek a portok illeszkedjenek a Cisco útválasztó és a RADIUS-kiszolgáló között.

A megosztott titkos kulcs konfigurálásához a jelszó titkosításához használja a **kulcs** parancsot. Ezt a kulcsot pontosan ugyanúgy kell konfigurálni az útválasztón és a RADIUS szerveren.

A példa egy minta RADIUS-kiszolgálókonfigurációt jelenít meg.

R1(config)# **aaa new-model**

R1(config)#

R1(config)# **radius server SERVER-R**

R1(config-radius-server)# **address ipv4 192.168.1.100 auth-port 1812 acct-port 1813**

R1(config-radius-server)# **key RADIUS-Pa55w0rd**

R1(config-radius-server)# **exit**

R1(config)#

7.4.4

## Hitelesítés az AAA-kiszolgáló konfigurációs parancsaiban

parancs metóduslistájában **Az AAA biztonsági kiszolgálók azonosítása után a kiszolgálóknak szerepelniük kell az aaa hitelesítési bejelentkezési** . Az AAA szerverek azonosítása a **group tacacs+** vagy **group radius** kulcsszavakkal történik. paranccsal elérhető parancsszintaktikai beállítások megtekintéséhez **Tekintse meg a példát az aaa hitelesítési bejelentkezési** .

R1(config)# **aaa authentication login default ?**

cache Use Cached-group

enable Use enable password for authentication.

group Use Server-group

krb5 Use Kerberos 5 authentication.

krb5-telnet Allow logins only if already authenticated via Kerberos V

Telnet.

line Use line password for authentication.

local Use local username authentication.

local-case Use case-sensitive local username authentication.

none NO authentication.

passwd-expiry enable the login list to provide password aging support

R1(config)# **aaa authentication login default group ?**

WORD Server-group name

ldap Use list of all LDAP hosts.

radius Use list of all Radius hosts.

tacacs+ Use list of all Tacacs+ hosts.

Az alapértelmezett bejelentkezés metóduslistájának konfigurálásához először TACACS+ kiszolgálóval, másodszor RADIUS kiszolgálóval, végül pedig helyi felhasználónév-adatbázissal történő hitelesítéshez adja meg a sorrendet az aaa hitelesítési bejelentkezés alapértelmezett t paranccsal, ahogy a példában **kiemeltük** . Fontos tudni, hogy az R1 csak akkor próbál meg hitelesíteni a RADIUS használatával, ha a TACACS+ szerver nem érhető el. Hasonlóképpen, az R1 csak akkor próbál meg hitelesíteni a helyi adatbázist, ha a TACACS+ és RADIUS szerverek nem elérhetők.

R1(config)# **aaa new-model**

R1(config)#

R1(config)# **tacacs server Server-T**

R1(config-server-tacacs)# **address ipv4 192.168.1.100**

R1(config-server-tacacs)# **single-connection**

R1(config-server-tacacs)# **key TACACS-Pa55w0rd**

R1(config-server-tacacs)# **exit**

R1(config)#

R1(config)# **radius server SERVER-R**

R1(config-radius-server)# **address ipv4 192.168.1.101 auth-port 1812 acct-port 1813**

R1(config-radius-server)# **key RADIUS-Pa55w0rd**

R1(config-radius-server)# **exit**

R1(config)#

R1(config)# **aaa authentication login default group tacacs+ group radius local-case**

7.4.5

## Szintaxis-ellenőrző – Szerver-alapú AAA-hitelesítés konfigurálása

Használja a Szintaxis-ellenőrzőt a szerver alapú AAA hitelesítés konfigurálásához az R1-en. A helyi felhasználónév-adatbázis konfigurálva lett, és a TACACS+ és RADIUS szerverek implementálva lettek a hálózaton.

Configure TACACS+ server settings on router R1 using the following instructions:

* Enable AAA.
* Enter TACACS+ server configuration mode and name the server configuration **SERVER-T**.
* Configure the TACACS+ server address to 192.168.1.100.
* Configure a single persistent TCP connection to the TACACS+ server.
* Configure the shared secret key **TACACS-Pa55w0rd**.
* Exit TACACS+ server configuration mode.

R1(config)#aaa new-model

R1(config)#tacacs server SERVER-T

R1(config-server-tacacs)#address ipv4 192.168.1.100

R1(config-server-tacacs)#single-connection

R1(config-server-tacacs)#key TACACS-Pa55w0rd

R1(config-server-tacasc)#exit

Enter RADIUS server configuration mode and name the configuration **SERVER-R**.

* Configure the RADIUS server address to 192.168.1.101 with the authentication port set to 1812 and the accounting port set to 1813.
* Configure the shared secret key **RADIUS-Pa55w0rd**.
* Exit RADIUS server configuration mode.

R1(config)#radius server SERVER-R

R1(config-radius-server)#address ipv4 192.168.1.101 auth-port 1812 acct-port 1813

R1(config-radius-server)# kulcs RADIUS-Pa55w0rd

R1(config-radius-server)# kilépés

Adjon meg egy alapértelmezett hitelesítési metóduslistát a TACACS+ elsődleges beállítással, a másodlagos RADIUS opcióval és a harmadlagos helyi felhasználónév kis- és nagybetűk közötti hitelesítéssel. A konfiguráció után lépjen ki a konfigurációs módból.

R1(config)# aaa hitelesítés bejelentkezés alapértelmezett csoport tacacs+ csoport sugara helyi kis- és nagybetű

R1(config)# kilépés

R1#

\*Mar 3 17:02:15.123: %SYS-5-CONFIG\_I: Konzolról konzolra konfigurálva

R1#

Sikeresen konfigurálta a szerver alapú AAA hitelesítést.

7.4.6

## Videó bemutató – Konfigurálja a Cisco Routert az AAA RADIUS szerver eléréséhez

Ez a videó bemutatja, hogyan konfigurálhat egy Cisco útválasztót az AAA RADIUS kiszolgáló eléréséhez a következők végrehajtásával:

**1. lépés** . Hozzon létre felhasználókat a RADIUS-kiszolgálón.

**2. lépés** . Állítson be egy titkos kulcsot a RADIUS-kiszolgálón.

**3. lépés** . Ellenőrizze az 1812-es portot a RADIUS hitelesítési porthoz és az 1813-as portot a RADIUS elszámolási porthoz.

**4. lépés** . Állítsa be az SSH-t az útválasztón a távoli hozzáféréshez.

**5. lépés** . Állítson be egy helyi felhasználót az útválasztón a RADIUS-kiszolgáló meghibásodása esetére.

**6. lépés** . Engedélyezze az AAA hitelesítést az útválasztón.

**7. lépés** . Állítsa be az AAA hitelesítési bejelentkezési módszerek listáját.

**8. lépés** . Engedélyezze az útválasztó számára, hogy a RADIUS-kiszolgálót használja hitelesítéshez a következő beállításokkal az útválasztón:

1. RADIUS szerver neve
2. RADIUS-kiszolgáló IP-címe, 1812-es hitelesítési portja és 1813-as elszámolási portja
3. megosztott titkos kulcs

**9. lépés** . Konfigurálja a konzolsort, és adja meg a használni kívánt AAA bejelentkezési hitelesítési módszerek listáját

**10. lépés** . Állítsa be az SSH VTY-vonalait, és adja meg a használandó AAA bejelentkezési hitelesítési módszerek listáját.

**11. lépés** . Tesztelje és ellenőrizze.

7.4.7

### Lab - Telepítse a virtuális gépet

Ebben a laborban a következő célokat kell teljesítenie:

* 1. rész: Személyi számítógép előkészítése virtualizációhoz
* 2. rész: Virtuális gép importálása a VirtualBox Inventoryba

7.4.8

## Lab – Szerver-alapú hitelesítés konfigurálása a RADIUS segítségével

Ebben a laborban a következő célt kell teljesítenie:

A központosított hitelesítés konfigurálása AAA és RADIUS használatával

7.4.9

## Packet Tracer – Szerver alapú hitelesítés konfigurálása TACACS+ és RADIUS segítségével

Ebben a csomagjelző tevékenységben a következő célokat fogja kitölteni:

* Szerver alapú AAA hitelesítés konfigurálása a TACACS+ használatával.
* Ellenőrizze a szerver alapú AAA hitelesítést a PC-B kliensről.
* Szerver alapú AAA hitelesítés konfigurálása RADIUS használatával.
* Ellenőrizze a szerver alapú AAA hitelesítést a PC-C kliensről.

[Szerver-alapú hitelesítés konfigurálása TACACS+ és RADIUS segítségével](https://contenthub.netacad.com/courses/netsec/_common/7.4.9-packet-tracer---configure-server-based-aaa-with-tacacs-and-radius.pka)

[7.3](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Server-Based AAA Characteristics and Protocols](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[7.5](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Configure Server-Based Authorization and Accounting](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                                                                                                       
*                             

1. Authentication, Authorization, and Accounting (AAA)
2. Configure Server-Based Authorization and Accounting

# Szerver-alapú engedélyezés és elszámolás konfigurálása

7.5.1

## Bevezetés a szerveralapú AAA-engedélyezésbe

Míg a hitelesítésnek biztosítania kell az eszköz vagy a végfelhasználó legitimitását, az engedélyezés a hitelesített felhasználók hozzáférésének engedélyezésére és letiltására vonatkozik a hálózati eszköz interfész funkcióihoz.

A TACACS+ protokoll lehetővé teszi a hitelesítés és az engedélyezés elkülönítését. Az útválasztó beállítható úgy, hogy a sikeres hitelesítés után a felhasználót csak bizonyos funkciók végrehajtására korlátozza. Ne feledje, hogy a RADIUS nem választja el a hitelesítést az engedélyezési folyamattól.

Az engedélyezés másik fontos szempontja a felhasználói hozzáférés szabályozásának képessége bizonyos szolgáltatásokhoz. A konfigurációs parancsokhoz való hozzáférés szabályozása nagymértékben leegyszerűsíti az infrastruktúra biztonságát a nagyvállalati hálózatokban.

Az animációban a JR-ADMIN sikeresen létrehozott egy SSH-munkamenetet az útválasztóval, és hitelesítette a TACACS+ AAA-kiszolgálót. Kattintson a Lejátszás gombra, ha meg szeretné tekinteni, hogyan reagál a szerver a különböző parancsokra.

Az animáció egy JR-ADMIN címkével ellátott számítógépet mutat be, amely egy AAA-kiszolgálóhoz csatlakoztatott útválasztóhoz csatlakozik. a számítógép elküldi a show version parancsot az útválasztónak. Az útválasztó elküldi a JR-ADMIN felhasználónak a kérdés parancsot, a jogosultság, parancs megjelenítése verzió? az AAA szerverre. Az aaa szerver az elfogadás szóval válaszol a routernek. Az útválasztó a számítógépnek a verziószámot megjelenítő kimenettel válaszol. a számítógép elküldi a configure terminál parancsot az útválasztónak. A forgalomirányító elküldi a JR-ADMIN felhasználónak, parancs config terminál? az AAA szerverre. Az aaa szerver az elutasítás szóval válaszol az útválasztónak. Az útválasztó a számítógépnek nem engedélyezi a konfigurálást terminállal válaszol.

### AAA szerver engedélyezés

Ne engedélyezze a "terminál konfigurálását"

Elutasít

Parancsengedélyezés a JR-ADMIN felhasználó számára, parancs " config terminal "?

konfigurálja a terminált

Kijelző " verzió megjelenítése " kimenet

Elfogad

Parancsjogosultság a JR-ADMIN felhasználó számára, parancs " show version "?

verzió megjelenítése

Jr-admin

AAA

Az animációban a JR-ADMIN hozzáférhet a **show version** parancshoz, de nem a **configure terminál** parancshoz. Az útválasztó lekérdezi az AAA-kiszolgálót, hogy engedélyezze-e a parancsok végrehajtását a felhasználó nevében. Amikor a felhasználó kiadja a **show version** parancsot, a szerver ACCEPT választ küld. Ha a felhasználó kiadja a **configure terminál** parancsot, a szerver REJECT választ küld.

Alapértelmezés szerint a TACACS+ új TCP-munkamenetet hoz létre minden engedélyezési kérelemhez, ami késésekhez vezethet a felhasználók parancsok beadásakor. kiszolgáló konfigurációs mód parancsával vannak konfigurálva **A teljesítmény javítása érdekében az AAA támogatja az állandó TCP-munkameneteket, amelyek az egykapcsolatos tacacs-** .

7.5.2

## AAA engedélyezési konfiguráció

Az engedélyezés konfigurálásához használja az **aaa authorization** parancsot, az alábbi példák szerint. A jogosultság típusa megadhatja a parancsok vagy szolgáltatások típusait:

* **hálózat** – olyan hálózati szolgáltatásokhoz, mint a PPP és a SLIP
* **exec** - a felhasználói EXEC terminál szekciókhoz
* **parancsok** szintje - parancsengedélyezés megkísérli engedélyezni az összes EXEC mód parancsot, beleértve a globális konfigurációs parancsokat is, amelyek egy adott jogosultsági szinthez vannak társítva

Router(config)# **aaa authorization** (**network** | **exec** | **commands** level){**default** | list-name} method1… [method4]

R1(config)# **aaa authorization exec ?**

WORD Named authorization list.

default The default authorization list.

R1(config)# **aaa authorization exec default ?**

cache Use Cached-group

group Use server-group.

if-authenticated Succeed if user has authenticated.

krb5-instance Use Kerberos instance privilege maps.

local Use local database.

none No authorization (always succeeds).

R1(config)# **aaa authorization exec default group ?**

WORD Server-group name

ldap Use list of all LDAP hosts.

radius Use list of all Radius hosts.

tacacs+ Use list of all Tacacs+ hosts.

Ha az AAA jogosultság nincs engedélyezve, minden felhasználó teljes hozzáférést kap. A hitelesítés elindítása után az alapértelmezés úgy változik, hogy nem engedélyezi a hozzáférést. Ez azt jelenti, hogy az adminisztrátornak létre kell hoznia egy teljes hozzáférési jogosultsággal rendelkező felhasználót, mielőtt engedélyezi az engedélyezést, ahogy a példában is látható. Ennek elmulasztása esetén az aaa engedélyezési parancs beírása után az adminisztrátor azonnal kikerül a rendszerből. Az egyetlen módja annak, hogy ebből helyreálljon, az útválasztó újraindítása. Ha ez egy éles útválasztó, előfordulhat, hogy az újraindítás elfogadhatatlan. Győződjön meg arról, hogy legalább egy felhasználónak mindig teljes joga van.

R1(config)# **username JR-ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd**

R1(config)# **username ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd**

R1(config)# **aaa new-model**

R1(config)# **aaa authorization exec default group tacacs+**

R1(config)# **aaa authorization network default group tacacs+**

7.5.3

## Bevezetés a szerver alapú AAA könyvelésbe

A vállalatoknak gyakran nyomon kell követniük, hogy az egyének vagy csoportok mely erőforrásokat használják fel. Az AAA könyvelés lehetővé teszi a használat nyomon követését. A használat nyomon követésére példa az, amikor egy részleg díjat számít fel egy másik részlegnek a hozzáférésért, vagy amikor az egyik vállalat belső támogatást nyújt egy másik vállalatnak. A könyvelési funkció hasonló a hitelkártya számlakivonatban megadott számviteli adatokhoz, az ábrán látható módon.

Az ábrán egy hitelkártya-kivonat látható, kiemelve a díjakat. és a számvitel szavak mire költötted?

### Hitelkártya könyvelési példa



**Könyvelés**   
  
mire költötted?

Bár a könyvelést általában hálózatkezelési vagy pénzügyi menedzsment kérdésnek tekintik, itt röviden tárgyaljuk, mert olyan szorosan kapcsolódik a biztonsághoz. Az egyik biztonsági probléma, amellyel a könyvelés foglalkozik, egy lista létrehozása a felhasználókról és a napszakról, amikor bejelentkeztek a rendszerbe. Ha például az adminisztrátor tudja, hogy egy dolgozó az éjszaka közepén jelentkezik be a rendszerbe, ez az információ felhasználható a bejelentkezés céljának további vizsgálatára.

A könyvelés megvalósításának másik oka, hogy létre kell hozni egy listát a hálózaton bekövetkezett változásokról, a módosításokat végrehajtó felhasználóról és a változtatások pontos természetéről. Knowing this information helps the troubleshooting process if the changes cause unexpected results.

Ha a könyvelést egy AAA-kiszolgálón konfigurálják, az a számviteli információk központi tárhelyeként működik. Nyomon követi a hálózaton előforduló eseményeket, hasonlóan ahhoz, ahogy a hitelkártyaszámla pénzügyi tevékenységét követi. A Cisco Secure ACS-en keresztül létrehozott minden munkamenet teljes mértékben elszámolható és tárolható a kiszolgálón. Ezek a tárolt információk nagyon hasznosak lehetnek a kezeléshez, a biztonsági auditokhoz, a kapacitástervezéshez és a hálózathasználati számlázáshoz.

Like authentication and authorization method lists, method lists for accounting define the way accounting is performed and the sequence in which these methods are performed. After it is enabled, the default accounting method list is automatically applied to all interfaces, except those that have a user-defined, or custom, accounting method list that has been explicitly defined.

7.5.4

## AAA könyvelési konfiguráció

Az AAA számlázás konfigurálásához használja **aaa accounting parancsot.** a példában látható

The following three parameters are commonly used **aaa accounting** keywords:

* **hálózat** – Futtatja az összes hálózattal kapcsolatos szolgáltatáskérést, beleértve a PPP-t is.
* **exec** – Futtatja az EXEC shell munkamenet elszámolását.
* **CSATLAKOZÁS** - A számvitelt futtatja az összes kimenő kapcsolaton, mint például az SSH és a Telnet.

Router(config)# **aaa accounting** {**network** | **exec** | **connection**} {**default** | list-name} {**start-stop** | **stop-only** | **none** } [**broadcast**] method1...[method4]

R1(config)# **aaa accounting exec ?**

WORD Named Accounting list.

default The default accounting list

Az AAA hitelesítéshez hasonlóan **akár a kulcsszó alapértelmezett** , akár a listanév . használható

Ezután be kell állítani a rekordtípust vagy az eseményindítót. Az eseményindító meghatározza, hogy mely műveletek okozzák a könyvelési rekordok frissítését. A lehetséges kiváltó okok a következők:

* **start-stop** – „Start” könyvelési értesítést küld a folyamat elején és „stop” számviteli értesítést a folyamat végén.
* **csak stop** – „Stop” elszámolási rekordot küld minden esetre, beleértve a hitelesítési hibákat is.
* **nincs** – Letiltja a számviteli szolgáltatásokat egy vonalon vagy interfészen.

A példák bemutatják a parancs szintaxisát és a metóduslista elérhető beállításait.

R1(config)# **aaa accounting exec default start-stop ?**

broadcast Use Broadcast for Accounting

group Use Server-group

R1(config)# **aaa accounting exec default start-stop group ?**

WORD Server-group name

radius Use list of all Radius hosts.

tacacs+ Use list of all Tacacs+ hosts.

A példa egy elszámolási konfigurációt mutat be, amely naplózza az EXEC parancsok és a hálózati kapcsolatok használatát.

R1(config)# **username JR-ADMIN algorithm-type scrypt secret Str0ng5rPa5w0rd**

R1(config)# **username ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd**

R1(config)# **aaa new-model**

R1(config)# **aaa authentication login default group tacacs+**

R1(config)# **aaa authorization exec default group tacacs+**

R1(config)# **aaa authorization network default group tacacs+**

R1(config)# **aaa accounting exec default start-stop group tacacs+**

R1(config)# **aaa accounting network default start-stop group tacacs**+

7.5.5

## Szintaxis-ellenőrző – Az AAA-könyvelés konfigurálása

Használja a Szintaxis-ellenőrzőt a kiszolgáló alapú AAA engedélyezés és elszámolás konfigurálásához az R1-en. A helyi felhasználónév-adatbázis konfigurálva, az AAA engedélyezve van, az AAA-hitelesítés konfigurálva, és a TACACS+ és a RADIUS szerverek implementálva lettek a hálózaton

Az R1 útválasztón egy helyi felhasználónév-adatbázis konfigurálva van, az AAA engedélyezve van, és az AAA-hitelesítés be van állítva. TACACS+ és RADIUS szerverek kerültek a hálózatra. Konfigurálja az R1-et a következő utasítások szerint:

* Állítsa be az alapértelmezett AAA-engedélyezési metóduslistát az EXEC-héjakhoz és a hálózati szolgáltatásokhoz a TACACS+ használatával.
* Konfigurálja az alapértelmezett AAA elszámolási metóduslistát az EXEC-héjakhoz és a TACACS+-t használó hálózati szolgáltatásokhoz, a folyamat elején és végén elküldött indítási és leállítási értesítésekkel.
* A konfiguráció után lépjen ki a konfigurációs módból.

R1(config)# aaa jogosultság végrehajtó alapértelmezett csoport tacacs+

R1(config)# aaa engedélyezési hálózat alapértelmezett csoport tacacs+

R1(config)# aaa accounting exec alapértelmezett start-stop csoport tacacs+

R1(config)# aaa könyvelési hálózat alapértelmezett start-stop csoport tacacs+

R1(config)# kilépés

R1#

\*Mar 3 18:22:23.443: %SYS-5-CONFIG\_I: Konzolról konzolra konfigurálva

R1#

Sikeresen konfigurálta az AAA könyvelést.

[7.4](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Configure Server-Based Authentication](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[7.6](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Authentication, Authorization, and Accounting (AAA) Summary](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                                                                                                                                    

1. Authentication, Authorization, and Accounting (AAA)

# A hitelesítés, engedélyezés és elszámolás (AAA) összefoglalója

7.6.1

## Mit tanultam ebben a modulban?

**AAA jellemzők**   
A helyi hitelesítés konfigurálható hálózati eszközökön olyan felhasználónevekkel és jelszavakkal, amelyek védik a konzolt, a vty vonalakat és a felhasználói EXEC módot. Ez a legkönnyebben megvalósítható hitelesítés, de egyben a leggyengébb és legkevésbé biztonságos is. Az SSH-t kell használni a vty-vonalak távoli eléréséhez, mert a telnet nem biztonságos. Az AAA olyan eszközt biztosít, amellyel a felhasználók hitelesíthetők a felhasználók központi adatbázisában. Az AAA-hitelesítéshez a felhasználóknak és a rendszergazdáknak igazolniuk kell személyazonosságukat felhasználónevekkel és jelszavakkal vagy más módszerekkel. Az AAA-jogosultság segítségével a felhasználók vagy felhasználói csoportok hozzáférését csak azokra a hálózati erőforrásokra korlátozhatja, amelyekhez hozzá kell férniük. Azt is szabályozhatja, hogy a felhasználó mit tehet a különféle erőforrásokkal. Az engedélyezés konfigurálható annak szabályozására, hogy a különböző felhasználók mit tehetnek a hálózati eszközökön. Az AAA-könyvelés rögzíti a felhasználói műveleteket, beleértve a hálózathoz vagy eszközhöz való hozzáférést, a munkamenet időtartamát, valamint a felhasználó által elért erőforrásokat és funkciókat. Az AAA beállítható úgy, hogy hozzáférjen egy helyi felhasználói adatbázishoz, amely egy útválasztón vagy kapcsolón, vagy központi AAA-kiszolgálón van konfigurálva. Miután a hitelesítés sikeresen megtörtént, a rendszer meghatározza a felhasználói hozzáférés jogosultságát. A sikeres hitelesítés után az AAA könyvelés rögzíti a munkamenet kezdetét.

**Helyi AAA hitelesítés konfigurálása**   
A helyi AAA hitelesítést kisebb hálózatokhoz kell beállítani. A felhasználói nevek és jelszavak a hálózati eszközön vannak konfigurálva, hasonlóan ahhoz, amikor a **helyi bejelentkezés** a konzolon és a vty vonalakon van konfigurálva. Az AAA helyi hitelesítés további lehetőségeket biztosít, amelyek nem érhetők el, ha nincs AAA. Például különböző hitelesítési módszerek konfigurálhatók a különböző vonalakon, beleértve a helyi hitelesítés használatát egyes vonalakon, és szerveralapú hitelesítést másokon. Ezenkívül a helyi AAA-hitelesítés beállítható úgy, hogy bizonyos számú bejelentkezési kísérlet után kizárja a felhasználókat. A felhasználó mindaddig ki van zárva, amíg egy rendszergazda manuálisan nem törli a felhasználót a kizárt helyi felhasználók listájáról.

**Szerver-alapú AAA jellemzők és protokollok**   
A helyi hitelesítés nem skálázható jól a sok hálózati eszközzel és felhasználóval rendelkező nagy hálózatokhoz. A régi Cisco Secure ACS AAA kiszolgálót a Cisco ISE váltotta fel. Az ISE számos hozzáféréssel kapcsolatos biztonsági funkciót kínál az AAA-funkciókon túl. A TACACS+ és RADIUS protokollok kommunikációt biztosítanak egy hálózati eszköz és egy AAA szerver között. A protokoll kiválasztása a vállalat igényeit védi. A TACACS+ az összes kommunikációt titkosítja, míg a RADIUS csak a jelszavakat. A TACACS+ különválasztja a hitelesítési és engedélyezési folyamatokat, miközben ezeket a RADIUS-ban egyesíti. Ezenkívül a TACACS+ TCP-t, míg a RADIUS UDP-t használ. Fontos megjegyezni, hogy a RADIUS támogatja a távelérési technológiákat, mint például a 802.1X és a SIP. Vannak más fontos különbségek is a protokollok között.

A TACACS+ az eredeti TACACS protokoll Cisco továbbfejlesztése, és nem kompatibilis az eredeti verzióval. A RADIUS egy nyílt szabványú IETF protokoll. Széles körben használják a VoIP-hez, mert támogatja a SIP-t. A következő generációs protokoll, amely a RADIUS alternatívája, a Diameter AAA.

**Szerver-alapú hitelesítés konfigurálása**   
Az AAA-kiszolgáló alapú hitelesítés konfigurálásának négy alapvető lépése van. Először az AAA-t globálisan engedélyezni kell az eszközön. Másodszor, az AAA szerver IP-címe és protokollja van megadva. Ezután meg kell adni a megfelelő titkosítási kulcsot, amelyet a hálózati eszköz és az AAA-kiszolgáló használni fog. Az eszközt úgy is be kell állítani, hogy az AAA kiszolgálót vagy szervereket használja a hitelesítéshez az **aaa hitelesítési** metódusok listájának megadásával, amely a bejelentkezési csoportot tartalmazza RADIUS, TACACS+ vagy mindkettőként. Ne feledje, hogy a Cisco útválasztók alapértelmezés szerint az 1645-ös portot használják a hitelesítéshez és az 1646-os portot a könyveléshez. Az IANA azonban lefoglalta az 1812-es portot a RADIUS-hitelesítéshez és az 1813-as portot a RADIUS-könyveléshez. Fontos, hogy ezek a portok illeszkedjenek a hálózati eszköz és a RADIUS-kiszolgáló között.

**Szerver alapú hitelesítés és elszámolás konfigurálása**   
Az AAA hitelesítés célja, hogy a hitelesített felhasználók csak azokhoz az erőforrásokhoz férhessenek hozzá, amelyekhez hozzá kell férniük. A hálózati rendszergazdák számára az eszköz parancssorához és a hálózati szolgáltatásokhoz engedélyezett hozzáférés típusa szabályozható. A jogosultság típusa az **aaa jogosultság** paranccsal állítható be. A típusok lehetnek **hálózati** , hálózati szolgáltatásokhoz, **exec** , felhasználói EXEC módhoz és **parancsok** az összes EXEC mód parancshoz, beleértve a konfigurációs parancsokat is. Ha az AAA jogosultság nincs engedélyezve, minden felhasználó teljes hozzáférést kap. A hitelesítés elindítása után az alapértelmezés úgy változik, hogy nem engedélyezi a hozzáférést. Ez azt jelenti, hogy az adminisztrátornak létre kell hoznia egy teljes hozzáférési jogosultsággal rendelkező felhasználót, mielőtt az engedélyezést engedélyezné. után az adminisztrátor azonnal kikerül a rendszerből **Ennek elmulasztása esetén az aaa engedélyezési** parancs beírása . Az egyetlen módja annak, hogy ebből helyreálljon, az útválasztó újraindítása.

Az AAA-könyvelés nyomon követi a felhasználó által elért erőforrásokat vagy azokat az eszközfunkciókat, amelyekhez a rendszergazda hozzáfért. Az elszámolás megvalósításának egyik oka az, hogy létre kell hozni egy listát a hálózati eszközön bekövetkezett változásokról, a módosításokat végrehajtó felhasználóról és a változtatások pontos természetéről. Ezen információk ismerete segíti a hibaelhárítási folyamatot, ha a változtatások váratlan eredményeket okoznak. Az **aaa számviteli** parancs beállításai a következő típusú információkat követik nyomon:

* **hálózat** – minden hálózattal kapcsolatos szolgáltatási kérés, beleértve a PPP-t is
* **exec** - az EXEC shell munkamenet elszámolása
* **kapcsolat** – minden kimenő kapcsolat, például SSH és Telnet elszámolása

A rekordtípus vagy az eseményindító határozza meg, hogy milyen műveletek okozzák a könyvelési rekordok frissítését. A triggerek közé tartozik egy folyamat kezdete és vége, illetve a hitelesítési hibák. A könyvelés eszközvonalon vagy interfészen is letiltható.

7.6.2

## 7. modul – Hitelesítés, engedélyezés és elszámolás (AAA) kvíz

Az űrlap teteje

1. Mi a TACACS+ protokoll jellemzője?

Az űrlap alja

Melyik két protokollt használják a szerver alapú AAA hitelesítés biztosítására? (Válassz kettőt.)

Milyen funkciókat biztosít a TACACS **egykapcsolati az kulcsszó** AAA szolgáltatásokhoz?

Mi az a három beléptető biztonsági szolgáltatás? (Válassz hármat.)

Mi a hálózatbiztonsági elszámolási funkció célja?

Mit biztosít a TACACS+ protokoll az AAA telepítésben?

Melyik kifejezés írja le a webszerver azon képességét, hogy naplót vezessen a szerverhez hozzáférő felhasználókról, valamint a kiszolgáló használatának időtartamáról?

AAA hitelesítés konfigurálásakor Mi az első kötelező feladat a szerver alapú ?

Mi jellemző az AAA számvitelre?

Az AAA-hitelesítési metóduslista konfigurálásakor mi a hatása a **local** kulcsszónak ?

Melyik állítás írja le a különbséget a RADIUS és a TACACS+ között?

Egy felhasználó panaszkodik, hogy nem tud hozzáférni egy AAA-val konfigurált hálózati eszközhöz. Hogyan állapítja meg a hálózati rendszergazda, hogy a felhasználói fiók bejelentkezési hozzáférése le van tiltva?

Az AAA melyik összetevője határozza meg, hogy a felhasználó mely erőforrásokhoz férhet hozzá, és milyen műveleteket hajthat végre?

[7.5](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Configure Server-Based Authorization and Accounting](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[8.0](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                   
*                           

1. Hozzáférés-vezérlési listák
2. Introduction

# Bevezetés

8.0.1

## Miért vegyem ezt a modult?

A zárt közösségben, ahol a nagyszülei élnek, szabályok vonatkoznak arra, hogy ki léphet be és ki léphet ki a helyiségből. Az őr nem emeli fel a kaput, hogy beengedjen a közösségbe, amíg valaki meg nem erősíti, hogy egy jóváhagyott látogatói listán vagy. Hasonlóan az őrhöz a kapuzott közösségben, a hozzáférés-vezérlési listával (ACL) konfigurált interfészen áthaladó hálózati forgalom engedélyezte és megtagadta a forgalmat. Hogyan kell beállítani ezeket az ACL-eket? Hogyan módosíthatja ezeket, ha nem működnek megfelelően, vagy ha más változtatásokat igényelnek? Kezdje el ezt a modult, hogy többet megtudjon!

8.0.2

## Mit fogok tanulni ebben a modulban?

**Modul címe:** Hozzáférés-vezérlési listák

**Modul célja** : A hozzáférés-vezérlési listák (ACL) megvalósítása a forgalom szűrése és a hálózati támadások mérséklése érdekében.

| **téma címe** | **Téma Cél** |
| --- | --- |
| **Bevezetés a hozzáférés-vezérlési listákba** | Ismertesse a szabványos és kiterjesztett IPv4 ACL-eket. |
| **Helyettesítő maszkok** | Magyarázza el, hogyan használnak az ACL-ek helyettesítő karakteres maszkokat. |
| **ACL-ek konfigurálása** | Ismertesse az ACL-ek konfigurálását. |
| **Módosítsa az ACL-eket** | Sorszámok használatával szerkesztheti a meglévő szabványos IPv4 ACL-eket |
| **ACL-ek megvalósítása** | ACL-ek megvalósítása. |
| **Mérsékelje a támadásokat ACL-ekkel** | Használjon ACL-eket a gyakori hálózati támadások mérséklésére. |
| **IPv6 ACL-ek** | Konfigurálja az IPv6 ACL-eket a parancssori felület segítségével. |

[7.6](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Authentication, Authorization, and Accounting (AAA) Summary](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[8.1](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Introduction to Access Control Lists](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                   
*                           

1. Hozzáférés-vezérlési listák
2. Introduction to Access Control Lists

# Bevezetés a hozzáférés-vezérlési listákba

8.1.1

## Mi az ACL?

Az útválasztók a csomag fejlécében található információk alapján hozzák meg az útválasztási döntéseket. Az útválasztó interfészére érkező forgalom kizárólag az útválasztási táblázaton belüli információk alapján kerül továbbításra. Az útválasztó összehasonlítja a cél IP-címét az útválasztási táblázatban szereplő útvonalakkal, hogy megtalálja a legjobb egyezést, majd a legjobb egyezési útvonal alapján továbbítja a csomagot. Ugyanez a folyamat használható a forgalom szűrésére egy hozzáférés-vezérlési lista (ACL) segítségével.

Az ACL olyan IOS-parancsok sorozata, amelyek a csomagok fejlécében található információk alapján a csomagok szűrésére szolgálnak. Alapértelmezés szerint az útválasztónak nincs konfigurálva ACL-je. Ha azonban ACL-t alkalmaznak egy interfészre, az útválasztó elvégzi azt a további feladatot, hogy kiértékeli az összes hálózati csomagot, amint azok áthaladnak az interfészen, és meghatározza, hogy a csomag továbbítható-e.

Az ACL az engedélyezési vagy megtagadási utasítások szekvenciális listáját használja, amelyeket hozzáférés-vezérlési bejegyzéseknek (ACE) neveznek.

**Megjegyzés:** Az ACE-ket általában ACL utasításoknak is nevezik.

Amikor a hálózati forgalom egy ACL-lel konfigurált interfészen halad át, az útválasztó összehasonlítja a csomagon belüli információkat az egyes ACE-ekkel, egymás utáni sorrendben, hogy megállapítsa, a csomag egyezik-e valamelyik ACE-vel. Ezt a folyamatot csomagszűrésnek nevezik.

Az útválasztók által végzett számos feladat ACL-ek használatát igényli a forgalom azonosításához. A táblázat felsorol néhány ilyen feladatot példákkal.

| **Feladat** | **Példa** |
| --- | --- |
| Korlátozza a hálózati forgalmat a hálózati teljesítmény növelése érdekében | * A vállalati házirend tiltja a videoforgalmat a hálózaton a hálózati terhelés csökkentése érdekében. * A házirend kényszeríthető ACL-ek használatával a videoforgalom blokkolására. |
| Biztosítsa a forgalom szabályozását | * A vállalati szabályzat megköveteli, hogy az útválasztási protokoll forgalmát csak bizonyos hivatkozásokra korlátozzák. * Az ACL-ek segítségével olyan házirendet lehet megvalósítani, amely az útválasztási frissítések kézbesítését csak az ismert forrásból származó frissítésekre korlátozza. |
| Biztosítson alapvető biztonsági szintet a hálózati hozzáféréshez | * A vállalati politika megköveteli, hogy a humánerőforrás-hálózathoz való hozzáférést csak az arra jogosult felhasználókra korlátozzák. * Egy házirend kényszeríthető ACL-ek segítségével, hogy korlátozza a hozzáférést a megadott hálózatokhoz. |
| A forgalom szűrése a forgalom típusa alapján | * A vállalati szabályzat előírja, hogy az e-mail forgalmat engedélyezni kell a hálózatba, de meg kell tiltani a Telnet hozzáférést. * A forgalom típus szerinti szűrésére ACL-ek segítségével házirendet lehet megvalósítani. |
| Hosztok képernyője a hálózati szolgáltatásokhoz való hozzáférés engedélyezéséhez vagy megtagadásához | * A vállalati szabályzat megköveteli, hogy bizonyos fájltípusokhoz (pl. FTP vagy HTTP) a hozzáférést felhasználói csoportokra korlátozzák. * Az ACL-ek segítségével házirend implementálható a felhasználók szolgáltatásokhoz való hozzáférésének szűrésére. |
| Adjon elsőbbséget a hálózati forgalom bizonyos osztályainak | * A vállalati forgalom azt határozza meg, hogy a hangforgalmat a lehető leggyorsabban továbbítsák a megszakítások elkerülése érdekében. * Az ACL-ek és a QoS-szolgáltatások használatával házirend implementálható a hangforgalom azonosítására és azonnali feldolgozására. |

8.1.2

## Csomagszűrés

A csomagszűrés a bejövő és/vagy kimenő csomagok elemzésével és adott kritériumok alapján történő továbbításával vagy eldobásával szabályozza a hálózathoz való hozzáférést. A csomagszűrés a 3. vagy a 4. rétegben történhet, amint az az ábrán látható.

Az ábra az OSI modell 7. rétegbeli alkalmazását, a 6. rétegbeli prezentációt, az 5. rétegbeli munkamenetet, a 4. rétegbeli szállítást, a 3. rétegbeli hálózatot, a 2. rétegű adatkapcsolatot és az 1. réteg fizikai rétegét mutatja. Az összes réteg elhalványult, kivéve a 3. réteg hálózati és a 4. réteg szállítási rétegét a kiemelés kedvéért. A narancssárga mezőben oldalt, a csomagszűrés a 3. és a 4. rétegben működik. Két narancssárga nyíl a 3. és 4. rétegre mutat.

7 6 5 4 3 2

1

A csomagszűrés a 3. és 4. rétegben működik Alkalmazás -bemutató munkamenet szállítási hálózat adatkapcsolati fizikai **OSI modellben**

A Cisco útválasztók kétféle ACL-t támogatnak:

* **Szabványos ACL-ek** – az ACL-ek csak a 3. rétegben szűrnek, csak a forrás IPv4-címét használva.
* **Kibővített ACL-ek** – Az ACL-ek a 3. rétegben szűrnek a forrás és/vagy a cél IPv4-címe alapján. A 4. rétegben is szűrhetnek TCP-, UDP-portok és opcionális protokolltípus-információk segítségével a finomabb vezérlés érdekében.

8.1.3

## Számozott és elnevezett ACL-ek

**Számozott ACL-ek**

Az 1-től 99-ig vagy az 1300-tól 1999-ig terjedő ACL-ek szabványos ACL-ek, míg a 100-tól 199-ig, illetve a 2000-tól 2699-ig terjedő ACL-ek kiterjesztett ACL-ek, amint a kimeneten látható.

R1(config)# **access-list ?**

<1-99> IP standard access list

<100-199> IP extended access list

<1100-1199> Extended 48-bit MAC address access list

<1300-1999> IP standard access list (expanded range)

<200-299> Protocol type-code access list

<2000-2699> IP extended access list (expanded range)

<700-799> 48-bit MAC address access list

rate-limit Simple rate-limit specific access list

template Enable IP template acls

R1(config)# **access-list**

**Elnevezett ACL-ek**

A nevesített ACL-ek az előnyben részesített módszer az ACL-ek konfigurálásakor. Pontosabban, szabványos és kiterjesztett ACL-ek nevezhetők el, hogy információt nyújtsanak az ACL céljáról. Például egy kiterjesztett ACL FTP-SZŰRŐ elnevezése sokkal jobb, mint egy számozott ACL 100.

Az **ip access-list** globális konfigurációs parancs egy elnevezett ACL létrehozására szolgál, amint az a következő példában látható.

R1(config)# **ip access-list extended FTP-FILTER**

R1(config-ext-nacl)# **permit tcp 192.168.10.0 0.0.0.255 any eq ftp**

R1(config-ext-nacl)# **permit tcp 192.168.10.0 0.0.0.255 any eq ftp-data**

R1(config-ext-nacl)#

Az alábbiakban összefoglaljuk az elnevezett ACL-ekre vonatkozó szabályokat.

* Adjon nevet az ACL céljának azonosításához.
* A nevek alfanumerikus karaktereket tartalmazhatnak.
* A nevek nem tartalmazhatnak szóközt vagy írásjelet.
* Javasoljuk, hogy a nevet NAGYBETŰVEL írják.
* A bejegyzések hozzáadhatók vagy törölhetők az ACL-en belül.

8.1.4

## ACL művelet

Az ACL-ek meghatározzák azokat a szabályokat, amelyek további vezérlést biztosítanak a bejövő interfészekre belépő, az útválasztón keresztül továbbító csomagok és az útválasztó kimenő interfészeiről kilépő csomagok számára.

Az ACL-ek beállíthatók úgy, hogy a bejövő és a kimenő forgalomra vonatkozzanak, amint az az ábrán látható.

Az ábra egy útválasztó bejövő és kimenő forgalmát mutatja. Középen egy útválasztó található, balra egy narancssárga nyíl, amely a routerre mutat. A nyíl felett a Bejövő AC L felirat látható. A jobb oldalon egy másik narancssárga nyíl látható, de az útválasztótól indul és elfelé mutat. A nyíl felett a Outbound AC L szavak láthatók.

R1

Bejövő ACL Kimenő ACL

**Megjegyzés** : Az ACL-ek nem hatnak azokra a csomagokra, amelyek magától az útválasztótól származnak.

A bejövő ACL kiszűri a csomagokat, mielőtt azok a kimenő interfészre kerülnének. A bejövő ACL hatékony, mert megspórolja az útválasztási keresések többletköltségét, ha a csomagot eldobják. Ha a csomagot az ACL engedélyezi, akkor a rendszer feldolgozza az útválasztáshoz. A bejövő ACL-ek a legjobban akkor használhatók csomagok szűrésére, ha a bejövő interfészhez csatlakoztatott hálózat az egyetlen csomagforrás, amelyet meg kell vizsgálni.

A kimenő ACL szűri a csomagokat az irányítás után, függetlenül a bejövő interfésztől. A bejövő csomagokat a rendszer a kimenő interfészre irányítja, majd a kimenő ACL-en keresztül dolgozza fel őket. A kimenő ACL-ek a legjobbak akkor, ha ugyanazt a szűrőt alkalmazzák a több bejövő interfészről érkező csomagokra, mielőtt kilépnének ugyanabból a kimenő interfészből.

Amikor egy ACL-t alkalmaznak egy interfészre, az egy meghatározott működési eljárást követ. Például itt láthatók azok a műveleti lépések, amelyek akkor használatosak, amikor a forgalom egy konfigurált bejövő szabványos IPv4 ACL-lel rendelkező útválasztó interfészére érkezett.

1. Az útválasztó kivonja a forrás IPv4-címét a csomag fejlécéből.
2. Az útválasztó az ACL tetejétől indul, és sorrendben összehasonlítja a forrás IPv4-címét az egyes ACE-vel.
3. Ha egyezés létrejön, az útválasztó végrehajtja az utasítást, engedélyezve vagy megtagadva a csomagot, és az ACL-ben fennmaradó ACE-ket, ha vannak, nem elemzi a rendszer.
4. Ha a forrás IPv4-címe nem egyezik az ACL-ben szereplő ACE-értékekkel, a csomag elveti, mert az összes ACL-re automatikusan alkalmazva van egy implicit tiltó ACE.

Az ACL utolsó ACE utasítása mindig egy implicit tagadás, amely blokkolja az összes forgalmat. Alapértelmezés szerint ez az utasítás automatikusan szerepel az ACL végén, még akkor is, ha rejtve van, és nem jelenik meg a konfigurációban.

**Megjegyzés** : Az ACL-nek rendelkeznie kell legalább egy engedélyezési utasítással, különben az összes forgalom meg lesz tagadva az implicit deny ACE utasítás miatt.

8.1.5

## Packet Tracer – ACL bemutató

Ebben a tevékenységben megfigyelheti, hogyan lehet egy hozzáférés-vezérlési listát (ACL) használni annak megakadályozására, hogy a ping elérje a távoli hálózatokon lévő gazdagépeket. Miután eltávolította az ACL-t a konfigurációból, a ping sikeres lesz.

[ACL Demonstration](https://contenthub.netacad.com/courses/netsec/_common/8.1.5-packet-tracer---acl-demonstration.pka)

[8.0](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[8.2](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Wildcard Masking](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                      
*                           

1. Hozzáférés-vezérlési listák
2. Helyettesítő karakter maszkolás

# Helyettesítő karakter maszkolás

8.2.1

## Helyettesítő maszk áttekintése

Az előző témakörben megismerkedhetett az ACL-ek céljával. Ez a témakör elmagyarázza, hogy az ACL-ek hogyan használnak helyettesítő karakteres maszkokat. Az IPv4 ACE 32 bites helyettesítő karakter maszkot használ annak meghatározására, hogy a cím mely bitjeit kell megvizsgálni az egyezéshez. A helyettesítő karakteres maszkokat az Open Shortest Path First (OSPF) útválasztási protokoll is használja.

A helyettesítő karakteres maszk hasonló az alhálózati maszkhoz, mivel az ÉS-ezési folyamatot használja annak azonosítására, hogy az IPv4-cím mely bitjei egyeznek. Mindazonáltal különböznek a bináris 1-esek és 0-ák párosítási módjában. Ellentétben az alhálózati maszkokkal, amelyekben a bináris 1 egyenlő egyezéssel, és a bináris 0 nem egyezés, a helyettesítő karakteres maszk esetében ennek az ellenkezője igaz.

A helyettesítő karakteres maszkok a következő szabályokat használják a bináris 1-ek és 0-k párosítására:

* **Helyettesítő karakter maszk bitje 0** – Egyezzen meg a cím megfelelő bitértékével
* **Helyettesítő maszk 1. bitje** – A címben szereplő megfelelő bitérték figyelmen kívül hagyása

A táblázat néhány példát sorol fel a helyettesítő karakteres maszkokra, és azt, hogy mit azonosítanak.

| Helyettesítő karakter maszkUtolsó oktett (binárisan)Jelentés (0 - egyezés, 1 - figyelmen kívül hagyás)0.0.0.000000000Minden oktett egyezése.0.0.0.6300111111Egyezze meg az első három oktettt.Esse meg az utolsó oktett két bal oldali legnagyobb bitjét. 0.0.0.1500001111egyezze meg az első három oktett Illessze az utolsó két bitet.0.0.0.25511111111Az első három oktett egyezése. Az utolsó oktett figyelmen kívül hagyása. | | |
| --- | --- | --- |
| **Helyettesítő maszk** | **Utolsó oktett (binárisan)** | **Jelentés (0 – egyezés, 1 – figyelmen kívül hagyás)** |
| **0.0.0.0** | **00000000** | Egyezik az összes oktett. |
| **0.0.0.63** | **00111111** | * Párosítsd az első három nyolcast! * Párosítsd az utolsó oktett két bal oldali legnagyobb bitjét * Az utolsó 6 bit figyelmen kívül hagyása |
| **0.0.0.15** | **00001111** | * Párosítsd az első három nyolcast! * Párosítsd az utolsó oktett négy bal oldali legnagyobb bitjét * Figyelmen kívül hagyja az utolsó oktett utolsó 4 bitjét |
| **0.0.0.252** | **11111100** | * Párosítsd az első három nyolcast! * Figyelmen kívül hagyja az utolsó oktett hat balra maradt legtöbb bitjét * Párosítsa az utolsó két bitet |
| **0.0.0.255** | **11111111** | * Párosítsa az első három nyolcast * Az utolsó oktett figyelmen kívül hagyása |

8.2.2

## Helyettesítő maszk típusok

A helyettesítő karakteres maszkok használata némi gyakorlatot igényel. Tekintse meg a példákat, hogy megtudja, hogyan használható a helyettesítő karakter maszk egy gazdagép, egy alhálózat és egy IPv4-címtartomány forgalmának szűrésére.

Kattintson az egyes gombra, hogy megtudja, hogyan használják a helyettesítő karakter maszkot az ACL-ekben.

**Helyettesítő maszk az IPv4-címtartományhoz**

Ebben a példában az ACL 10-nek olyan ACE-re van szüksége, amely engedélyezi a 192.168.16.0/24, 192.168.17.0/24, …, 192.168.31.0/24 hálózatok összes gazdagépét. A 0.0.15.255 helyettesítő karakteres maszk megfelelően szűrné ezt a címtartományt.

A táblázat binárisan felsorolja a gazdagép IPv4-címét, a helyettesítő karaktermaszkot és az engedélyezett IPv4-címeket.

A kiemelt helyettesítő karakter maszkbitek azonosítják, hogy az IPv4-cím mely bitjeinek kell egyeznie. Feldolgozáskor a 0.0.15.255 helyettesítő karakter maszk engedélyezi az összes gazdagépet a 192.168.16.0/24 és 192.168.31.0/24 közötti hálózatokban. Az eredményül kapott ACE a 10. ACL-ben **a 10. hozzáférési lista engedélye 192.168.16.0 0.0.15.255.**

| Decimális bináris IPv4-cím192.168.16.011000000.10101000.00010000.00000000Wildcard Mask0.0.15.25500000000.00000000.00000000.00000000.00000000.00000000.00000000.00000000.00000000.00000000.00011111111111111111111111111 .16.0/24to192.168.31.0/2411000000.10101000.00010000.00000000 11000000.10101000.00011111.00000000 | | |
| --- | --- | --- |
|  | **Decimális** | **Bináris** |
| IPv4 cím | 192.168.16.0 | 11000000.10101000.00010000.00000000 |
| Helyettesítő maszk | 0.0.15.255 | 00000000.00000000.00001111.11111111 |
| **Engedélyezett gazdagép IPv4-címek** | **192.168.16.1**  nak nek  **192.168.31.254** | **11000000.10101000.00010000.00000000** |

**Helyettesítő maszk az IPv4-alhálózathoz**

Ebben a példában az ACL 10-nek olyan ACE-re van szüksége, amely engedélyezi az összes gazdagépet a 192.168.1.0/24 hálózaton. A 0.0.0.255 helyettesítő karaktermaszk előírja, hogy a legelső három oktettnek pontosan meg kell egyeznie, de a negyedik oktettnek nem.

A táblázat binárisan felsorolja a gazdagép IPv4-címét, a helyettesítő maszkot és az engedélyezett IPv4-címeket.

Feldolgozáskor a 0.0.0.255 helyettesítő karakter maszk engedélyezi az összes gazdagépet a 192.168.1.0/24 hálózaton. lenne . **Az eredményül kapott ACE a 10-es ACL-ben a 10. hozzáférési lista 192.168.1.0 0.0.0.255 engedélye**

| Decimális bináris IPv4-cím192.168.1.111000000.10101000.00000001.00000001Wildcard maszk0.0.0.25500000000.00000000.00000000.00000000.00000000.00000000.00000000.00000000.00000000.00000000.00000000.00000000.00000000.00000000.00000000.00000000.00000000.00000000.00000000.00000000.00000111911111. .0/2411000000.10101000.00000001.00000000 | | |
| --- | --- | --- |
|  | **Decimális** | **Bináris** |
| IPv4 cím | 192.168.1.1 | 11000000.10101000.00000001.00000001 |
| Helyettesítő maszk | 0.0.0.255 | 00000000.00000000.00000000.11111111 |
| **Engedélyezett gazdagép IPv4-címek** | **192.168.1.1**  nak nek  **192.168.1.254** | **11000000.10101000.00000001.00000000   11000000.10101000.00000001.11111111** |

**Helyettesítő karakter a házigazdához**

Ebben a példában a helyettesítő karakter maszk egy adott gazdagép IPv4-címének megfeleltetésére szolgál. Tegyük fel, hogy az ACL 10-nek olyan ACE-re van szüksége, amely csak a 192.168.1.1 IPv4-című gazdagépet engedélyezi. Emlékezzünk vissza, hogy a „0” egyezést, az „1” pedig a figyelmen kívül hagyást jelenti. Egy adott gazdagép IPv4-címének megfeleltetéséhez minden nullát tartalmazó helyettesítő karakteres maszk (azaz 0.0.0.0) szükséges.

A táblázat binárisan felsorolja a gazdagép IPv4-címét, a helyettesítő karaktermaszkot és az engedélyezett IPv4-címet.

A 0.0.0.0 helyettesítő karakter maszk előírja, hogy minden bitnek pontosan meg kell egyeznie. Ezért az ACE feldolgozása során a helyettesítő karakter maszk csak a 192.168.1.1 címet engedélyezi. lenne . **Az eredményül kapott ACE a 10-es ACL-ben a 10. hozzáférési lista 192.168.1.1 0.0.0.0 engedélye**

| DecimálisBináris IPv4 cím192.168.1.111000000.10101000.00000001.00000001Wildcard Mask0.0.0.000000000.00000000.000000000.000000000.000000000.000000000.000000000.000000000.000000000.000000000.000000000.00000000.061910 11000000.10101000.00000001.00000001 | | |
| --- | --- | --- |
|  | **Decimális** | **Bináris** |
| IPv4 cím | 192.168.1.1 | 11000000.10101000.00000001.00000001 |
| Helyettesítő maszk | 0.0.0.0 | 00000000.00000000.00000000.00000000 |
| **Engedélyezett IPv4-cím** | **192.168.1.1** | **11000000.10101000.00000001.00000001** |

8.2.3

## Helyettesítő maszk számítása

A helyettesítő karakteres maszkok kiszámítása kihívást jelenthet. Az egyik gyorsbillentyű-módszer az alhálózati maszk kivonása a 255.255.255.255-ből. A példákból megtudhatja, hogyan számíthatja ki a helyettesítő karakter maszkot az alhálózati maszk használatával.

Kattintson az egyes gombra az egyes helyettesítő karaktermaszkok kiszámításához.

**1. példa**

Tegyük fel, hogy egy ACE-t akart az ACL 10-ben, hogy hozzáférést biztosítson a 192.168.3.0/24 hálózat összes felhasználója számára. A helyettesítő karakter maszk kiszámításához vonja ki az alhálózati maszkot (azaz 255.255.255.0) a 255.255.255.255-ből, a táblázat szerint.

A megoldás előállítja a 0.0.0.255 helyettesítő maszkot. Ezért az ACE a **10. hozzáférési lista engedélye 192.168.3.0 0.0.0.255.**

| Kezdő érték 255.255.255.255 Az alhálózati maszk kivonása- 255.255.255.000 Az eredményül kapott helyettesítő karakter maszk 0. 0. 0.255 | |
| --- | --- |
|  |  |
| Kiinduló érték | 255.255.255.255 |
| Vonja ki az alhálózati maszkot | - 255.255.255. 0 |
| **Az eredményül kapott helyettesítő karakter maszk** | **0. 0. 0.255** |

**2. példa**

Ebben a példában tegyük fel, hogy egy ACE-t szeretne az ACL 10-ben, hogy engedélyezze a hálózati hozzáférést a 192.168.3.32/28 alhálózat 14 felhasználója számára. Vonja ki az alhálózatot (azaz 255.255.255.240) 255.255.255.255-ből, a táblázat szerint.

Ez a megoldás a 0.0.0.15 helyettesítő karaktermaszkot állítja elő. Ezért az ACE a **10. hozzáférési lista engedélye 192.168.3.32 0.0.0.15.**

| Kezdő érték 255.255.255.255 Az alhálózati maszk kivonása- 255.255.255.240 Az eredményül kapott helyettesítő karakter maszk- 0. 0. 0. 15 | |
| --- | --- |
|  |  |
| Kiinduló érték | 255.255.255.255 |
| Vonja ki az alhálózati maszkot | - 255.255.255.240 |
| **Az eredményül kapott helyettesítő karakter maszk** | **0. 0. 0. 15** |

**3. példa**

Ebben a példában tegyük fel, hogy szüksége van egy ACE-ra az ACL 10-ben, hogy csak a 192.168.10.0 és 192.168.11.0 hálózatokat engedélyezze. Ezt a két hálózatot a 192.168.10.0/23 néven lehetne összefoglalni, ami egy 255.255.254.0 alhálózati maszk. Ismét levonja a 255.255.254.0 alhálózati maszkot a 255.255.255.255-ből, ahogy a táblázatban látható.

Ez a megoldás a 0.0.1.255 helyettesítő maszkot állítja elő. Ezért az ACE a **10. hozzáférési lista engedélye 192.168.10.0 0.0.1.255.**

| Kezdő érték 255.255.255.255 Az alhálózati maszk kivonása- 255.255.254.000 Az eredményül kapott helyettesítő karakter maszk 0. 0. 1.255 | |
| --- | --- |
|  |  |
| Kiinduló érték | 255.255.255.255 |
| Vonja ki az alhálózati maszkot | - 255.255.254. 0 |
| **Az eredményül kapott helyettesítő karakter maszk** | **0. 0. 1.255** |

**4. példa**

Vegyünk egy példát, amelyben egy 10-es ACL-számra van szükség a 192.168.16.0/24 és 192.168.31.0/24 közötti hálózatokhoz. Ez a hálózati tartomány a 192.168.16.0/20-ban foglalható össze, amely egy 255.255.240.0 alhálózati maszk. Ezért vonja ki a 255.255.240.0 alhálózati maszkot a 255.255.255.255-ből a táblázat szerint.

Ez a megoldás a 0.0.15.255 helyettesítő karaktermaszkot állítja elő. Ezért az ACE a **10. hozzáférési lista engedélye 192.168.16.0 0.0.15.255.**

| Kezdő érték 255.255.255.255 Az alhálózati maszk kivonása- 255.255.240.000 Az eredményül kapott helyettesítő karakter maszk 0. 0. 15.255 | |
| --- | --- |
|  |  |
| Kiinduló érték | 255.255.255.255 |
| Vonja ki az alhálózati maszkot | - 255.255.240. 0 |
| **Az eredményül kapott helyettesítő karakter maszk** | **0. 0. 15.255** |

8.2.4

## Helyettesítő maszk kulcsszavak

A bináris helyettesítő karakteres maszkbitek decimális reprezentációival való munka fárasztó lehet. A feladat egyszerűsítése érdekében a Cisco IOS két kulcsszóval azonosítja a helyettesítő karakteres maszkolás leggyakoribb felhasználásait. A kulcsszavak csökkentik az ACL billentyűleütések számát, de ami még fontosabb, a kulcsszavak megkönnyítik az ACE olvasását.

A két kulcsszó a következő:

* **host** – Ez a kulcsszó helyettesíti a 0.0.0.0 maszkot. Ez a maszk kimondja, hogy az összes IPv4-címbitnek egyeznie kell ahhoz, hogy csak egy gazdagépcímet szűrhessen.
* **tetszőleges** – Ez a kulcsszó helyettesíti a 255.255.255.255 maszkot. Ez a maszk azt mondja, hogy hagyja figyelmen kívül a teljes IPv4-címet, vagy fogadjon el bármilyen címet.

Például a parancskimenetben két ACL van konfigurálva. Az ACL 10 ACE csak a 192.168.10.10 gazdagépet, az ACL 11 ACE pedig az összes gazdagépet engedélyezi.

R1(config)# **access-list 10 permit 192.168.10.10**  **0.0.0.0**

R1(config)# **access-list 11 permit**  **0.0.0.0 255.255.255.255**

R1(config)#

kulcsszavak **Alternatív megoldásként a host** és **any** használhatók a kiemelt kimenet helyettesítésére.

A következő parancsok ugyanazt a feladatot hajtják végre, mint az előző parancsok.

R1(config)# **access-list 10 permit**  **host**  **192.168.10.10**

R1(config)# **access-list 11 permit**  **any**

R1(config)#

8.2.5

## Ellenőrizze a megértését – Helyettesítő maszkok az ACL-ekben

Az űrlap teteje

Ellenőrizze, hogy érti-e a helyettesítő karakter maszkokat az ACL-ekben, és válassza ki a LEGJOBB választ a következő kérdésekre.

1. Melyik helyettesítő karaktermaszk engedélyezné csak a 10.10.10.1 gazdagépet?

Megcsináltad!

Az űrlap alja

Melyik helyettesítő karakteres maszk engedélyezné csak a 10.10.0.0/16 hálózatból származó gazdagépeket?

Megcsináltad!

Which wildcard mask would permit all hosts?

You got it!

Which wildcard mask would permit all hosts from the 192.168.10.0/24 network?

You got it!

[8.1](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Introduction to Access Control Lists](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[8.3](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Configure ACLs](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                             
*                           

1. Hozzáférés-vezérlési listák
2. Configure ACLs

# ACL-ek konfigurálása

8.3.1

## Hozzon létre egy ACL-t

Egy korábbi témakörben megtudta, mit csinál az ACL, és miért fontos. Ebben a témakörben megismerheti az ACL-ek létrehozását.

Minden hozzáférés-vezérlési listát (ACL) meg kell tervezni. Ez azonban különösen igaz a többszörös hozzáférés-vezérlési bejegyzést (ACE) igénylő ACL-ekre.

Komplex ACL konfigurálásakor a következőket javasoljuk:

* Használjon szövegszerkesztőt, és írja le a megvalósítandó házirend sajátosságait.
* Adja hozzá az IOS konfigurációs parancsait a feladatok végrehajtásához.
* Az ACL dokumentálásához tegyen megjegyzéseket.
* Másolja és illessze be a parancsokat az eszközre.
* Mindig alaposan tesztelje az ACL-t, hogy megbizonyosodjon arról, hogy megfelelően alkalmazza a kívánt házirendet.

Ezek az ajánlások lehetővé teszik az ACL átgondolt létrehozását anélkül, hogy befolyásolná a hálózat forgalmat.

8.3.2

## Számozott szabványos IPv4 ACL szintaxis

Számozott szabványos ACL létrehozásához használja a következő globális konfigurációs parancsot:

Router(config)# **access-list** access-list-number {**deny** | **permit** | **remark** text} source [source-wildcard] [**log**]

A **no access-list** access-list-number globális konfigurációs paranccsal távolítsa el a számozott szabványos ACL-t.

A táblázat részletes magyarázatot ad a szabványos ACL szintaxisáról.

| **Paraméter** | **Leírás** |
| --- | --- |
| hozzáférési lista-szám | * Ez az ACL decimális száma. * A szabványos ACL számtartomány 1-től 99-ig vagy 1300-tól 1999-ig terjed. |
| **tagadni** | Ez megtagadja a hozzáférést, ha a feltétel teljesül. |
| **engedély** | Ez lehetővé teszi a hozzáférést, ha a feltétel megfelel. |
| **megjegyzés**  szöveget | * (Opcionális) Dokumentációs célból szöveges bejegyzést ad hozzá. * A megjegyzések rendkívül hasznosak, különösen a hosszabb vagy összetettebb ACL-eknél. * Minden megjegyzés legfeljebb 100 karakterből állhat. |
| forrás | * Ez azonosítja a szűrendő forráshálózatot vagy gazdagép címét. * használja az **any kulcsszót.** Az összes hálózat megadásához * Használja a **host** ip-address kulcsszót, vagy egyszerűen írjon be egy IP-címet (a **gazdagép** kulcsszó nélkül) egy adott IP-cím azonosításához. |
| forrás-helyettesítő karakter | (Opcionális) Ez egy 32 bites helyettesítő karaktermaszk, amely a forrásra vonatkozik. Ha kihagyja, az alapértelmezett 0.0.0.0 maszkot feltételezi. |
| **log** | * (Opcionális) Ez a kulcsszó tájékoztató üzenetet generál az ACE egyezése esetén. * Az üzenet tartalmazza az ACL-számot, az illesztett feltételt (azaz engedélyezett vagy tiltott), a forráscímet és a csomagok számát. * Ez az üzenet az első egyező csomaghoz jön létre. * Sajnos az ACL naplózás CPU-igényes lehet, és negatívan befolyásolhatja más funkciókat, ezért csak hibaelhárítási vagy biztonsági okokból érdemes megvalósítani. |

8.3.3

## Szabványos IPv4 ACL-szintaxis névvel

Az ACL elnevezése megkönnyíti a funkciójának megértését. Egy elnevezett szabványos ACL létrehozásához használja a következő globális konfigurációs parancsot:

Router(config)# **ip access-list standard** access-list-name

Ez a parancs belép a megnevezett szabványos konfigurációs módba, ahol beállíthatja az ACL ACE-kat.

Az ACL-nevek alfanumerikusak, megkülönböztetik a kis- és nagybetűket, és egyedinek kell lenniük. Az ACL-nevek nagybetűs írása nem kötelező, de kiemeli őket a running-config kimenet megtekintésekor. Ez csökkenti annak valószínűségét is, hogy véletlenül két különböző ACL-t hozzon létre azonos névvel, de eltérő nagybetűket használva.

**Megjegyzés** : A **no ip access-list standard** access-list-name globális konfigurációs paranccsal távolítson el egy elnevezett szabványos IPv4 ACL-t.

A példában egy elnevezett szabványos IPv4 ACL, NO-ACCESS néven jön létre. Figyelje meg, hogy a prompt elnevezett szabványos ACL konfigurációs módra változik. Az ACE utasítások a megnevezett szabványos ACL alkonfigurációs módban kerülnek bevitelre. A súgó segítségével megtekintheti az összes megnevezett szabványos ACL ACE-beállítást.

A három kiemelt opció a számozott szabványos ACL-hez hasonlóan van konfigurálva. A számozott ACL metódussal ellentétben nincs szükség a kezdeti **ip access-list** parancs megismétlésére minden egyes ACE-hez.

R1(config)# **ip access-list standard NO-ACCESS**

R1(config-std-nacl)# **?**

Standard Access List configuration commands:

<1-2147483647> Sequence Number

default Set a command to its defaults

deny Specify packets to reject

exit Exit from access-list configuration mode

no Negate a command or set its defaults

permit Specify packets to forward

remark Access list entry comment

R1(config-std-nacl)#

8.3.4

## Számozott kiterjesztett IPv4 ACL szintaxis

A kiterjesztett ACL-ek beállításának eljárási lépései ugyanazok, mint a szabványos ACL-ek esetében. A kiterjesztett ACL először konfigurálva van, majd aktiválódik egy interfészen. A parancs szintaxisa és paraméterei azonban bonyolultabbak a kiterjesztett ACL-ek által biztosított további szolgáltatások támogatásához.

Számozott kiterjesztett ACL létrehozásához használja a következő globális konfigurációs parancsot:

Router(config-if)#  **ip access-group**  0 0

Használja a **no access-list** access-list-number globális konfigurációs parancsot a kiterjesztett ACL eltávolításához.

Bár számos kulcsszó és paraméter létezik a kiterjesztett ACL-ekhez, nem szükséges mindegyiket használni egy kiterjesztett ACL konfigurálásakor. A táblázat részletes magyarázatot ad a kiterjesztett ACL szintaxisáról.

| **Paraméter** | **Leírás** |
| --- | --- |
| hozzáférési lista-szám | * Ez az ACL decimális száma. * A kiterjesztett ACL számtartomány 100-tól 199-ig és 2000-től 2699-ig terjed. |
| **tagadni** | Ez megtagadja a hozzáférést, ha a feltétel teljesül. |
| **engedély** | Ez lehetővé teszi a hozzáférést, ha a feltétel megfelel. |
| **megjegyzés**  szöveget | * (Opcionális) Dokumentációs célból szöveges bejegyzést ad hozzá. * Minden megjegyzés legfeljebb 100 karakterből állhat. |
| jegyzőkönyv | * Internetprotokoll neve vagy száma. * A gyakori kulcsszavak közé tartozik **az ip** , **tcp** , **udp** és **icmp** . * Az **ip** kulcsszó minden IP-protokollnak megfelel. |
| forrás | * Ez azonosítja a szűrendő forráshálózatot vagy gazdagép címét. * használja az **any kulcsszót.** Az összes hálózat megadásához * Használja a **host** ip-address kulcsszót, vagy egyszerűen írjon be egy IP-címet (a **gazdagép** kulcsszó nélkül) egy adott IP-cím azonosításához. |
| forrás-helyettesítő karakter | (Opcionális) A forrásra alkalmazott 32 bites helyettesítő karaktermaszk. |
| rendeltetési hely | * Ez azonosítja a szűrendő célhálózatot vagy gazdagép címét. * használja az **any kulcsszót.** Az összes hálózat megadásához * Használja a **gazdagép** ip-címe kulcsszót vagy ip-címet . |
| célhely-helyettesítő karakter | (Opcionális) Ez egy 32 bites helyettesítő karaktermaszk, amely a célhelyre kerül alkalmazásra. |
| operátor | * (Opcionális) Ez összehasonlítja a forrás- és célportokat. * Egyes operátorok közé tartozik **az lt** (kisebb, mint), **a gt** (nagyobb, mint), **az eq** (egyenlő) és **a neq** (nem egyenlő). |
| kikötő | (Opcionális) A TCP- vagy UDP-port decimális száma vagy neve. |
| **alapított** | * (Opcionális) Csak a TCP protokollhoz. * Ez egy 1 utca generációs tűzfal funkció. |
| **log** | * (Opcionális) Ez a kulcsszó tájékoztató üzenetet generál és küld az ACE egyezése esetén. * Ez az üzenet tartalmazza az ACL-számot, az illesztett feltételt (azaz engedélyezett vagy tiltott), a forráscímet és a csomagok számát. * Ez az üzenet az első egyező csomaghoz jön létre. * Ezt a kulcsszót csak hibaelhárítási vagy biztonsági okokból szabad alkalmazni. |

A kiterjesztett IPv4 ACL interfészre történő alkalmazására vonatkozó parancs megegyezik a szabványos IPv4 ACL-ekhez használt paranccsal.

Router(config-if)# **ip access-group** {access-list-number | access-list-name} {**in** | **out**}

Az ACL felületről való eltávolításához először írja be a **no ip access-group** interface configuration parancsot. Az ACL-nek az útválasztóról való eltávolításához használja a **no access-list** globális konfigurációs parancsot.

**Megjegyzés** : A szabványos ACL utasítások rendezésére alkalmazott belső logika nem vonatkozik a kiterjesztett ACL-ekre. Az utasítások konfigurálás közbeni beviteli sorrendje a megjelenítési és feldolgozási sorrendben történik.

8.3.5

## Protokollok és portszámok

A kiterjesztett ACL-ek számos különböző típusú internetes protokollon és porton szűrhetnek. Kattintson az egyes gombra, ha többet szeretne megtudni azokról az internetes protokollokról és portokról, amelyeken a kiterjesztett ACL-ek szűrhetnek.

**Port kulcsszóbeállítások**

kiválasztása *A protokoll* befolyásolja *a portbeállításokat* . Például a következőt választva:

* **A tcp** protokoll a TCP-vel kapcsolatos portokat biztosít
* **Az udp** protokoll UDP-specifikus port lehetőségeket biztosít
* **Az icmp** protokoll az ICMP-vel kapcsolatos portokat (azaz üzeneteket) biztosítana

Ismét figyelje meg, hány TCP-port opció áll rendelkezésre. A kiemelt portok népszerű opciók.

A portok neve vagy száma megadható. A portnevek azonban megkönnyítik az ACE céljának megértését. Figyelje meg, hogy egyes gyakori portnevek (pl. SSH és HTTPS) nincsenek felsorolva. Ezekhez a protokollokhoz meg kell adni a portszámokat.

R1(config)# **access-list 100 permit tcp any any eq ?**

<0-65535> Port number

bgp Border Gateway Protocol (179)

chargen Character generator (19)

cmd Remote commands (rcmd, 514)

daytime Daytime (13)

discard Discard (9)

domain Domain Name System (53)

echo Echo (7)

exec Exec (rsh, 512)

finger Finger (79)

ftp File Transfer Protocol (21)

ftp-data FTP data connections (20)

gopher Gopher (70)

hostname NIC hostname server (101)

ident Ident Protocol (113)

irc Internet Relay Chat (194)

klogin Kerberos login (543)

kshell Kerberos shell (544)

login Login (rlogin, 513)

lpd Printer service (515)

msrpc MS Remote Procedure Call (135)

nntp Network News Transport Protocol (119)

onep-plain Onep Cleartext (15001)

onep-tls Onep TLS (15002)

pim-auto-rp PIM Auto-RP (496)

pop2 Post Office Protocol v2 (109)

pop3 Post Office Protocol v3 (110)

smtp Simple Mail Transport Protocol (25)

sunrpc Sun Remote Procedure Call (111)

syslog Syslog (514)

tacacs TAC Access Control System (49)

talk Talk (517)

telnet Telnet (23)

time Time (37)

uucp Unix-to-Unix Copy Program (540)

whois Nicname (43)

www World Wide Web (HTTP, 80)

**Protokoll opciók**

A négy kiemelt protokoll a legnépszerűbb opció.

**Megjegyzés** : Használja a **?** hogy segítséget kapjon egy összetett ACE beírásakor.

**Megjegyzés:** Ha egy internetprotokoll nem szerepel a listában, akkor megadható az IP protokoll száma. Például az ICMP protokoll száma 1, a TCP 6, az UDP pedig a 17.

R1(config)# **access-list 100 permit ?**

<0-255> An IP protocol number

ahp Authentication Header Protocol

dvmrp dvmrp

eigrp Cisco's EIGRP routing protocol

esp Encapsulation Security Payload

gre Cisco's GRE tunneling

icmp Internet Control Message Protocol

igmp Internet Gateway Message Protocol

ip Any Internet Protocol

ipinip IP in IP tunneling

nos KA9Q NOS compatible IP over IP tunneling

object-group Service object group

ospf OSPF routing protocol

pcp Payload Compression Protocol

pim Protocol Independent Multicast

tcp Transmission Control Protocol

udp User Datagram Protocol

R1(config)# **access-list 100 permit**

8.3.6

## Protokollok és portszámok konfigurációs példák

A kiterjesztett ACL-ek különböző portszám- és portnév-beállításokra szűrhetnek. Ez a példa egy kiterjesztett ACL 100-at konfigurál a HTTP-forgalom szűrésére. Az első ACE a **www** port nevét használja. portot használja **A második ACE a 80-as** . Mindkét ACE pontosan ugyanazt az eredményt éri el.

R1(config)# **access-list 100 permit tcp any any eq www**

R1(config)# **!or...**

R1(config)# **access-list 100 permit tcp any any eq 80**

A portszám konfigurálása akkor szükséges, ha a következő példában látható módon nem szerepel konkrét protokollnév, például SSH (22-es portszám) vagy HTTPS (443-as portszám).

R1(config)# **access-list 100 permit tcp any any eq 22**

R1(config)# **access-list 100 permit tcp any any eq 443**

R1(config)#

8.3.7

## TCP Established Extended ACL

A TCP alapszintű állapotjelző tűzfalszolgáltatásokat is képes végrehajtani a TCP **által létrehozott** kulcsszó használatával. A kulcsszó lehetővé teszi, hogy a belső forgalom kilépjen a belső magánhálózatból, és a visszatérő válaszforgalom belépjen a belső magánhálózatba, amint az az ábrán látható.

A diagram az R 1 útválasztót mutatja 2 hálózati interfésszel: G0/0/0, amely a belső magánhálózathoz csatlakozik, és G0/0/1 csatlakozik a külső nyilvános hálózathoz. A belülről kifelé irányuló TCP-forgalom engedélyezett, és a visszatérés is megengedett, de a kívülről indított TCP-forgalom megtagadva

S1 PC1 R1 G0/0/1 G0/0/0

192.168.10.0/24

LAN 1 Internet magánhálózaton belül nyilvános hálózaton kívül TCP-kérés a PC1-ről a külső nyilvános hálózatra megengedett. A külső nyilvános hálózatról visszatérő TCP válaszforgalom megengedett. A külső nyilvános hálózati gazdagépektől érkező TCP kérések megtagadva.

A külső gazdagép által generált és egy belső gazdagéppel kommunikálni próbáló TCP-forgalom azonban meg van tiltva.

A **létrehozott** kulcsszó arra használható, hogy csak a HTTP-forgalom visszatérését engedélyezze a kért webhelyekről, miközben az összes többi forgalmat letiltja.

A topológiában ennek a példának a kialakítása azt mutatja, hogy a korábban konfigurált ACL 110 kiszűri a forgalmat a belső magánhálózatról. kulcsszó használatával **Az ACL 120 a létrehozott** kiszűri a belső magánhálózatba érkező forgalmat a külső nyilvános hálózatról.

A diagram az R 1 útválasztót mutatja 2 hálózati interfésszel: G0/0/0, amely a belső magánhálózathoz csatlakozik, és G0/0/1 csatlakozik a külső nyilvános hálózathoz. A hozzáférési listák a G0/0/0 interfész bejövő és kimenő adatait egyaránt alkalmazzák a következő parancspéldában

S1 PC1 R1 G0/0/1 G0/0/0

192.168.10.0/24

LAN 1 Internet magánhálózaton belül nyilvános hálózaton kívül 110 120

A példában az ACL 120 úgy van konfigurálva, hogy csak a webes forgalom visszatérését engedélyezze a belső gazdagépekhez. Az új ACL ezután kimenően kerül alkalmazásra az R1 G0/0/0 interfészen. A **show access-lists** parancs mindkét ACL-t megjeleníti. Figyelje meg a mérkőzés statisztikájából, hogy a belső gazdagépek az internetről hozzáfértek a biztonságos webes erőforrásokhoz.

R1(config)# **access-list 120 permit tcp any 192.168.10.0 0.0.0.255 established**

R1(config)# **interface g0/0/0**

R1(config-if)# **ip access-group 120 out**

R1(config-if)# **end**

R1# **show access-lists**

Extended IP access list 110

10 permit tcp 192.168.10.0 0.0.0.255 any eq www

20 permit tcp 192.168.10.0 0.0.0.255 any eq 443 (657 matches)

Extended IP access list 120

10 permit tcp any 192.168.10.0 0.0.0.255 established (1166 matches)

R1#

Figyelje meg, hogy a biztonságos HTTPS-számlálók (azaz a 443-as egyenlet) a 110-es ACL-ben és a visszatérési megállapított számlálók a 120-as ACL-ben növekedtek.

A **beállított** paraméter csak a 192.168.10.0/24 hálózatból származó forgalomra adott válaszok visszatérését engedélyezi a hálózatra. Pontosabban, egyezés akkor következik be, ha a visszatérő TCP szegmens rendelkezik az ACK vagy reset (RST) jelzőbitekkel. Ez azt jelzi, hogy a csomag egy meglévő kapcsolathoz tartozik. paraméter nélkül **Az ACL utasításban beállított** az ügyfelek forgalmat küldhetnek a webszervernek, és fogadhatnak a webszerverről visszatérő forgalmat. Minden forgalom engedélyezett lenne.

8.3.8

## Kiterjesztett IPv4 ACL-szintaxis névvel

Az ACL elnevezése megkönnyíti a funkciójának megértését. Megnevezett kiterjesztett ACL létrehozásához használja a következő globális konfigurációs parancsot:

Router(config)# **ip access-list extended** access-list-name

Ez a parancs belép a megnevezett kiterjesztett konfigurációs módba. Ne feledje, hogy az ACL-nevek alfanumerikusak, megkülönböztetik a kis- és nagybetűket, és egyedinek kell lenniük.

A példában egy NO-FTP-ACCESS nevű kiterjesztett ACL jön létre, és a prompt neve kiterjesztett ACL konfigurációs módra módosul. Az ACE utasítások a megnevezett kiterjesztett ACL alkonfigurációs módban kerülnek bevitelre.

R1(config)# **ip access-list extended NO-FTP-ACCESS**

R1(config-ext-nacl)#

8.3.9

## Kiterjesztett IPv4 ACL-példa néven

A nevesített kiterjesztett ACL-ek lényegében ugyanúgy jönnek létre, mint az elnevezett szabványos ACL-ek.

Az ábrán látható topológia két elnevezett kiterjesztett IPv4 ACL konfigurálásának és interfészre való alkalmazásának bemutatására szolgál:

* **SZÖRFÖZÉS** – Ez lehetővé teszi a belső HTTP és HTTPS forgalom kilépését az internetre.
* **BÖNGÉSZÉS** – Ez csak a webes forgalom visszatérését engedélyezi a belső gazdagépekhez, miközben az R1 G0/0/0 felületről kilépő összes többi forgalom hallgatólagosan meg van tiltva.

A diagram az R 1 útválasztót mutatja 2 hálózati interfésszel: G0/0/0, amely a belső magánhálózathoz csatlakozik, és G0/0/1 csatlakozik a külső nyilvános hálózathoz. A következő parancspéldában a G0/0/0 interfészen a SZÖRFING nevű elnevezésű hozzáférési lista, a G0/0/0 interfészen pedig a BROWSING nevű hozzáférési lista kerül alkalmazásra.

S1 PC1 R1 G0/0/1 G0/0/0

192.168.10.0/24

LAN 1 Internet magánhálózaton belül nyilvános hálózaton kívül SZÖRFÖZÉS BÖNGÉSZÉS

A példa a bejövő SURFING ACL és a kimenő BROWSING ACL konfigurációját mutatja be.

A SURFING ACL lehetővé teszi a HTTP és HTTPS forgalom belső felhasználóktól való kilépését az internethez kapcsolódó G0/0/1 interfészről. Az internetről visszatérő webes forgalmat a BROWSING ACL engedi vissza a belső magánhálózatba.

A SURFING ACL bejövő és a BROWSING ACL kerül alkalmazásra az R1 G0/0/0 interfészen, ahogy a kimeneten látható.

A belső gazdagépek az internetről fértek hozzá a biztonságos webes erőforrásokhoz. **A show access-lists** parancs az ACL statisztikák ellenőrzésére szolgál. Figyelje meg, hogy a biztonságos HTTPS-számlálók (azaz a 443-as egyenlet) száma a SURFING ACL-ben és a BÖNZÉSI ACL-ben a visszatérési számlálók száma nőtt.

R1(config)# **ip access-list extended SURFING**

R1(config-ext-nacl)# **Remark Permits inside HTTP and HTTPS traffic**

R1(config-ext-nacl)# **permit tcp 192.168.10.0 0.0.0.255 any eq 80**

R1(config-ext-nacl)# **permit tcp 192.168.10.0 0.0.0.255 any eq 443**

R1(config-ext-nacl)# **exit**

R1(config)#

R1(config)# **ip access-list extended BROWSING**

R1(config-ext-nacl)# **Remark Only permit returning HTTP and HTTPS traffic**

R1(config-ext-nacl)# **permit tcp any 192.168.10.0 0.0.0.255 established**

R1(config-ext-nacl)# **exit**

R1(config)# **interface g0/0/0**

R1(config-if)# **ip access-group SURFING in**

R1(config-if)# **ip access-group BROWSING out**

R1(config-if)# **end**

R1# **show access-lists**

Extended IP access list SURFING

10 permit tcp 192.168.10.0 0.0.0.255 any eq www

20 permit tcp 192.168.10.0 0.0.0.255 any eq 443 (124 matches)

Extended IP access list BROWSING

10 permit tcp any 192.168.10.0 0.0.0.255 established (369 matches)

R1#

[8.2](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Wildcard Masking](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[8.4](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Modify ACLs](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                               
*                           

1. Hozzáférés-vezérlési listák
2. Modify ACLs

# Módosítsa az ACL-eket

8.4.1

## Két módszer az ACL módosítására

Az ACL konfigurálása után előfordulhat, hogy módosítani kell. A több ACE-vel rendelkező ACL-ek konfigurálása bonyolult lehet. Néha a konfigurált ACE nem adja meg a várt viselkedést. Ezen okok miatt előfordulhat, hogy az ACL-ek kezdetben egy kis próbálkozást és hibázást igényelnek a kívánt szűrési eredmény eléréséhez.

Ez a rész két módszert tárgyal az ACL módosításakor:

* Használjon szövegszerkesztőt
* Sorozatszámok használata

8.4.2

## Szövegszerkesztő módszer

A több ACE-vel rendelkező ACL-eket szövegszerkesztőben kell létrehozni. Ez lehetővé teszi a szükséges ACE-k megtervezését, az ACL létrehozását, majd beillesztését az útválasztó felületére. Ezenkívül leegyszerűsíti az ACL szerkesztését és javítását.

Tegyük fel például, hogy az ACL 1 hibásan lett megadva, és **19-et** helyett **az első oktett 192** használt , amint az a futó konfigurációban látható.

R1# **show run | section access-list**

access-list 1 deny 19.168.10.10

access-list 1 permit 192.168.10.0 0.0.0.255

R1#

A példában az első ACE-nak a 192.168.10.10-es gazdagép megtagadása kellett volna. Az ACE azonban hibásan lett megadva.

A hiba javításához:

* Másolja ki az ACL-t a futó konfigurációból, és illessze be a szövegszerkesztőbe.
* Végezze el a szükséges változtatásokat.
* Távolítsa el a korábban konfigurált ACL-t az útválasztóról. Ellenkező esetben a szerkesztett ACL parancsok beillesztése csak az útválasztó meglévő ACL ACE-jaihoz fűzi hozzá (azaz hozzáadja).
* Másolja és illessze vissza a szerkesztett ACL-t az útválasztóba.

Tegyük fel, hogy az 1. ACL-t most javították. Ezért a hibás ACL-t törölni kell, és a javított ACL 1 utasításokat globális konfigurációs módban kell beilleszteni, ahogy a kimeneten látható.

R1(config)# **no access-list 1**

R1(config)#

R1(config)# **access-list 1 deny 192.168.10.10**

R1(config)# **access-list 1 permit 192.168.10.0 0.0.0.255**

R1(config)#

8.4.3

## Sorozatszám módszer

Az ACL ACE is törölhető vagy hozzáadható az ACL sorozatszámok használatával. A sorszámok automatikusan hozzárendelődnek az ACE beírásakor. parancsban vannak felsorolva **Ezek a számok a show access-lists** . A **show running-config** parancs nem jelenít meg sorszámokat.

Az előző példában az ACL 1 helytelen ACE-ja a 10-es sorszámot használja, ahogy a példában is látható.

R1# **show access-lists**

Standard IP access list 1

10 deny 19.168.10.10

20 permit 192.168.10.0, wildcard bits 0.0.0.255

R1#

használja az **ip access-list standard** Az ACL szerkesztéséhez parancsot. Az utasításokat nem lehet felülírni egy meglévő utasítással azonos sorszámmal. Ezért először az aktuális utasítást kell törölni a **no 10** paranccsal . Ezután a megfelelő ACE hozzáadható a 10-es sorszám segítségével. Ellenőrizze a változtatásokat a **show access-lists** paranccsal a példában látható módon.

R1# **conf t**

R1(config)# **ip access-list standard 1**

R1(config-std-nacl)# **no 10**

R1(config-std-nacl)# **10 deny host 192.168.10.10**

R1(config-std-nacl)# **end**

R1# **show access-lists**

Standard IP access list 1

10 deny 192.168.10.10

20 permit 192.168.10.0, wildcard bits 0.0.0.255

R1#

8.4.4

## Szintaxis-ellenőrző – Módosítsa az IPv4 ACL-eket

Módosítsa az ACL-t sorszámok használatával.

Az ábra egy topológia, amelyben az R1 útválasztó S0/1/0-n keresztül csatlakozik az internethez a 10.1.1.0 / 30-as hálózaton. A LAN 1 az R1 g0/0/0 interfészhez csatlakozik, és egy kapcsolót és egy P C-t tartalmaz. a LAN 1 címe 192.168.10.0 / 24. A LAN 2 az R 1 g0/0/1 interfészhez csatlakozik, és egy kapcsolót és egy P C-t tartalmaz. A LAN 2 címe 192.168.20.0 / 24

10.1.1.0/30 S0/1/0 G0/0/0 G0/0/1 192.168.10.0/24 192.168.20.0/24 .10 .10 PC2 PC1 S1 S2

R1

Internet LAN 1 LAN 2

Használja a **show access-lists** parancsot a konfigurált ACL-ek ellenőrzéséhez.

R1# hozzáférési listák megjelenítése

Szabványos IP hozzáférési lista 1

10 tagadás 19.168.10.10

20 engedély 192.168.10.0, helyettesítő karakter bitek 0.0.0.255

Észreveszi, hogy az ACE 10 hibás, és szerkeszteni kell. Lépjen be a globális konfigurációs módba, és használja az **ip access-list szabványos** parancsot az ACL **1-hez.**

R1# konfigurálja a terminált

R1(config)# ip hozzáférési lista szabvány 1

A hibás ACE-t törölni kell, majd újra be kell írni. Távolítsa el a 10-es sorszámú ACE-t.

R1(config-std-nacl)# no 10

Ezután adja meg újra a megfelelő ACE-t a 10-es sorszámmal, hogy megtagadja a 192.168.10.10 IP-című gazdagép hozzáférését az 1-es LAN-on kívül, és visszatérjen a privilegizált EXEC módba az **end** paranccsal.

R1(config-std-nacl)# 10 deny host 192.168.10.10

R1(config-std-nacl)# vége

Ellenőrizze az új bejegyzést a **show access-lists** paranccsal.

R1# hozzáférési listák megjelenítése

Szabványos IP hozzáférési lista 1

10 tagadás 192.168.10.10

20 engedély 192.168.10.0, helyettesítő karakter bitek 0.0.0.255

Sikeresen módosított egy IPv4 számozott ACL-t az R1-en.

[8.3](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Configure ACLs](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[8.5](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Implement ACLs](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                          
*                           

1. Hozzáférés-vezérlési listák
2. Implement ACLs

# ACL-ek megvalósítása

8.5.1

## ACL konfigurációs irányelvek

Az ACL egy vagy több hozzáférés-vezérlési bejegyzésből (ACE) vagy utasításból áll. Az ACL konfigurálásakor és alkalmazásakor ügyeljen a listában összefoglalt irányelvekre:

* Hozzon létre egy ACL-t globálisan, majd alkalmazza azt.
* Győződjön meg arról, hogy az utolsó utasítás implicit **deny any** vagy **deny ip any any** .
* Ne feledje, hogy az utasítások sorrendje fontos, mert az ACL-ek feldolgozása felülről lefelé történik.
* Amint egy utasítás egyezik, az ACL kilép.
* Mindig szűrje a legspecifikusabbtól a legáltalánosabbig. Például tiltson le egy adott gazdagépet, majd engedélyezze az összes többi gazdagépet.
* Ne feledje, hogy interfészenként, protokollonként és irányonként csak egy ACL engedélyezett.
* Ne feledje, hogy a meglévő ACL új utasításai alapértelmezés szerint az ACL aljára kerülnek.
* Ne feledje, hogy a router által generált csomagokat nem szűrik a kimenő ACL-ek.
* Helyezze el a szabványos ACL-eket a lehető legközelebb a célhoz.
* Helyezze a kiterjesztett ACL-eket a forráshoz a lehető legközelebb.

8.5.2

## Alkalmazzon ACL-t

Az ACL létrehozása után a rendszergazda számos különböző módon alkalmazhatja azt. Az alábbiakban bemutatjuk a parancs szintaxisát az ACL interfészre vagy a vty sorokra történő alkalmazásához.

Router(config-if)# **ip access-group** {acl-# | name} {**in** | **out**}

Router(config-line)# **access-class** {acl-# | name} {**in** | **out**}

Az alábbi ábra egy elnevezett szabványos ACL-t mutat be, amely a kimenő forgalomra vonatkozik.

Az ábra egy topológia, amelyben az R1 útválasztó S0/0/0-n keresztül csatlakozik az internethez. Egy LAN csatlakozik az R 1 g0/0 interfészhez, és tartalmaz egy kapcsolót és egy P C-t. A LAN címe 192.168.10.0 / 24. Cég Az R 1 g0/1 interfészhez csatlakozik egy hálózat, amely egy kapcsolót és egy kapcsolót tartalmaz. P C. A LAN 2 címe 192.168.11.0 / 24

### Szabványos ACL-példa néven

PC1 PC2 S2 S1 S0/0/0 G0/1 G0/0 192.168.10.0/24 192.168.11.0/24 192.168.10.10/24 192.168.11.10/24

R1

A cég

R1(config)# **ip access-list standard NO\_ACCESS**

R1(config-std-nacl)# **deny host 192.168.11.10**

R1(config-std-nacl)# **permit any**

R1(config-std-nacl)# **exit**

R1(config)# **interface g0/0**

R1(config-if)# **ip access-group NO\_ACCESS out**

Ez az ábra két elnevezett kiterjesztett ACL-t mutat. A SURFING ACL a bejövő forgalomra, a BROWSING ACL pedig a kimenő forgalomra vonatkozik.

Az ábra egy topológia egy ISP-útválasztóval a felhőben, amely S0/1/0-n keresztül kapcsolódik az R2-höz. Az R 2 az S0/0/1-en keresztül csatlakozik az R 3 S0/0/1-hez. Az R 2 az S0/0/0-n keresztül csatlakozik az R 1 S0/0/0-hoz. Az R1 a G0/0-n keresztül csatlakozik az S1-hez és a 192.168.10.0 / 24-es hálózathoz. Az R1 a G0/1-en keresztül csatlakozik az S 2-höz, a 192.168.11.0 / 24-es hálózathoz.

### Kiterjesztett ACL-példa néven

R2 R1 R3 S1 S2 ISP S0/0/0 S0/1/0 S0/0/1 S0/0/1 S0/0/0 G0/0 G0/1 192.168.11.0/24 192.168.10.0/24

10.1.1.1/30

R1(config)# **ip access-list extended SURFING**

R1(config-ext-nacl)# **permit tcp 192.168.10.0 0.0.0.255 any eq 80**

R1(config-ext-nacl)# **permit tcp 192.168.10.0 0.0.0.255 any eq 443**

R1(config-ext-nacl)# **exit**

R1(config)# **ip access-list extended BROWSING**

R1(config-ext-nacl)# **permit tcp any 192.168.10.0 0.0.0.255 established**

R1(config-ext-nacl)# **exit**

R1(config)# **interface g0/0**

R1(config-if)# **ip access-group SURFING in**

R1(config-if)# **ip access-group BROWSING out**

Az ábrán egy R1-hez csatlakoztatott számítógép látható. A számítógép IP-címe 192.168.10.10

### ACL néven VTY vonalakon naplózással

192.168.10.10

R1

engedélyezése **A naplóparaméter** egy Cisco útválasztón vagy kapcsolón súlyosan befolyásolja az eszköz teljesítményét. A naplóparamétert csak akkor szabad használni, ha a hálózat támadás alatt áll, és a rendszergazda megpróbálja megállapítani, ki a támadó.

Az ACL-ek interfészekre és vonalakra történő alkalmazása csak egy a sok lehetséges felhasználás közül. Az ACL-ek más biztonsági konfigurációk, például a hálózati címfordítás (NAT), a zónaalapú tűzfalak és a virtuális magánhálózatok szerves részét is képezik.

R1(config)# **ip access-list standard VTY\_ACCESS**

R1(config-std-nacl)# **permit 192.168.10.10 log**

R1(config-std-nacl)# **deny any**

R1(config-std-nacl)# **exit**

R1(config)# **line vty 0 4**

R1(config-line)# **access-class VTY\_ACCESS in**

R1(config-line)# **end**

R1#

R1# **!The administrator accesses the vty lines from 192.168.10.10**

R1#

\*Feb 26 18:58:30.579: %SEC-6-IPACCESSLOGNP: list VTY\_ACCESS permitted 0

192.168.10.10 -> 0.0.0.0, 5 packets

R1# **show access-lists**

Standard IP access list VTY\_ACCESS

10 permit 192.168.10.10 log (6 matches)

20 deny any

Az ACL felületről való eltávolításához először írja be a no ip access-group interface configuration parancsot. Az ACL azonban továbbra is konfigurálva lesz az útválasztón. Az ACL-nek az útválasztóról való eltávolításához használja a no access-list globális konfigurációs parancsot.

8.5.3

## Hol helyezzük el az ACL-eket

Minden ACL-t ott kell elhelyezni, ahol a leghatékonyabb.

Az ábra azt szemlélteti, hogy a szabványos és a kiterjesztett ACL-eket hol kell elhelyezni egy vállalati hálózatban. Tegyük fel, hogy a cél annak megakadályozása, hogy a 192.168.10.0/24 hálózatból induló forgalom elérje a 192.168.30.0/24 hálózatot.

Az ábra szemlélteti, hogyan helyezhet el ACL-t a hálózaton. Ennek a hálózatnak három útválasztója és négy LAN-ja van. A felső közepén egy R 2 nevű router található. Alul és balra egy R 1 nevű router található, amely soros kábellel csatlakozik az R2-höz. Mind az R1, mind az R2 használja az S0/1/0 interfészt. Az R2-től jobbra van egy R3 nevű útválasztó, amely soros kábellel csatlakozik az R2-höz. Mind az R3, mind az R2 használja az S0/1/1 interfészt. R1-nek és R3-nak két-két LAN-ja van. Az R1-nek van egy LAN-ja, amely a G0/0/0-tól a P C1 csomóponttal rendelkező S1 kapcsolóhoz csatlakozik. Ez a 192.168.10.0/24 hálózat, és a P C1 IP-címe 192.168.10.10. Az R1-nek van egy második LAN-ja, amely a G0/0/1-től a P C2 csomóponttal rendelkező S2 kapcsolóhoz csatlakozik. Ez a 192.168.11.0/24 hálózat, és a P C2 IP-címe 192.168.11.10. Az R3-nak van egy LAN-ja, amely a G0/0/0-tól a P C3 csomóponttal rendelkező S3 kapcsolóhoz csatlakozik. Ez a 192.168.30.0/24 hálózat, és a P C3 IP-címe 192.168.30.12. Az R3-nak van egy második LAN-ja, amely a G0/0/1-ből csatlakozik az S4-es kapcsolóhoz, amely egy kiszolgáló csomóponttal rendelkezik. Ez a 192.168.31.0/24 hálózat, és a szerver IP-címe 192.168.31.12. Az R 1 felett van egy doboz, amely azt írja, hogy a kiterjesztett AC L-eket általában a forrás közelében helyezik el. Az R3 felett van egy másik doboz, amely azt írja, hogy a szabványos AC L-eket általában a cél közelében helyezik el.

R2 S0/1/0 S0/1/0 G0/0/0 192.168.11.0/24 192.168.10.10 192.168.11.10 192.168.30.12 192.168.31.12 192.168.30.0/24 192.168.31.0/24 S0/1/1 S0/1/1 G0/0/1 192.168.10.0/24 G0/0/0 G0/0/1 R1 S1 S2 S3 S4 R3 PC1 PC3

PC2

A szabványos ACL-eket általában a cél közelében helyezik el. A kiterjesztett ACL-eket általában a forrás közelében helyezik el.

A kiterjesztett ACL-eket a lehető legközelebb kell elhelyezni a szűrendő forgalom forrásához. Így a nemkívánatos forgalom a forráshálózat közelében megtagadható anélkül, hogy áthaladna a hálózati infrastruktúrán.

A szabványos ACL-eket a lehető legközelebb kell elhelyezni a célhoz. Ha egy szabványos ACL-t helyeztek el a forgalom forrásánál, akkor az "engedélyezés" vagy "megtagadás" az adott forráscím alapján történik, függetlenül attól, hogy a forgalom hová kerül.

Az ACL elhelyezése, és így a használt ACL típusa a táblázatban felsorolt ​​számos tényezőtől is függhet.

| **Az ACL elhelyezését befolyásoló tényezők** | **Magyarázat** |
| --- | --- |
| **A szervezeti kontroll mértéke** | Az ACL elhelyezése attól függhet, hogy a szervezet felügyeli-e mind a forrás-, mind a célhálózatot. |
| **Az érintett hálózatok sávszélessége** | Kívánatos lehet a nem kívánt forgalmat a forrásnál szűrni, hogy megakadályozzuk a sávszélességet igénylő forgalom átvitelét. |
| **Könnyű konfigurálás** | * Lehet, hogy egyszerűbb egy ACL-t megvalósítani a célhelyen, de a forgalom szükségtelenül sávszélességet fog igénybe venni. * Kibővített ACL használható minden útválasztón, ahol a forgalom indult. Ez sávszélességet takarít meg a forgalom forrásnál történő szűrésével, de több útválasztón kiterjesztett ACL-ek létrehozására lenne szükség. |

8.5.4

## Szabványos ACL elhelyezési példa

Az ACL-elhelyezésre vonatkozó irányelveket követve a szabványos ACL-eket a célállomáshoz a lehető legközelebb kell elhelyezni.

Az ábrán az adminisztrátor meg akarja akadályozni, hogy a 192.168.10.0/24 hálózatból induló forgalom elérje a 192.168.30.0/24 hálózatot.

Az ábra bemutatja, hogyan helyezhet el szabványos ACL-t a hálózaton. Ennek a hálózatnak három útválasztója és négy LAN-ja van. A felső közepén egy R 2 nevű router található. Alul és balra egy R 1 nevű router található, amely soros kábellel csatlakozik az R2-höz. Mind az R1, mind az R2 használja az S0/1/0 interfészt. Az R2-től jobbra van egy R3 nevű útválasztó, amely soros kábellel csatlakozik az R2-höz. Mind az R3, mind az R2 használja az S0/1/1 interfészt. R1-nek és R3-nak két-két LAN-ja van. Az R1-nek van egy LAN-ja, amely a G0/0/0-tól a P C1 csomóponttal rendelkező S1 kapcsolóhoz csatlakozik. Ez a 192.168.10.0/24 hálózat. Az R1-nek van egy második LAN-ja, amely a G0/1-től az S2 kapcsolóhoz csatlakozik, amelynek P C2 csomópontja van. Ez a 192.168.11.0/24 hálózat. Az R3-nak van egy LAN-ja, amely a G0/0/0-tól a P C3 csomóponttal rendelkező S3 kapcsolóhoz csatlakozik. Ez a 192.168.30.0/24 hálózat. Az R3-nak van egy második LAN-ja, amely a G0/0/1-től a P C4 csomóponttal rendelkező S4 kapcsolóhoz csatlakozik. Ez a 192.168.31.0/24 hálózat. A tetején egy narancssárga mezőben a 192.168.10.0/24 és 192.168.30.0/24 közötti forgalom blokkolása felirat látható. A soros kábelen van egy tölcsér az R 2 és R 3 között, és a tölcsér széles vége az R 2 oldalon van. A tölcsér mellett található a következő kijelentés: Szűri a forgalmat a 192.168.10.0/24-től az összes R3 által elérhető célállomás felé. Az Ethernet-kábelen van egy második tölcsér az R3 és az S3 között, a széles végével az R3 oldalon. A tölcsér mellett található a „Csak 192.168.10.0/24-ről 192.168.30.0/24-re szűri a forgalmat” utasítás.

R2 S0/1/0 G0/0/0 192.168.11.0/24 192.168.30.0/24 192.168.31.0/24 S0/1/1 G0/0/1 192.168.10.0/24 G0/0/0 R1 S1 S2 S3 S4 R3 PC1 PC3 PC2 S0/1/0 S0/1/1 PC4

G0/0/1

**A webhely B webhely** Minden forgalom blokkolása 192.168.10.0/24 és 192.168.30.0/24 között. Szűri a forgalmat a 192.168.10.0/24-ről az összes R3-mal elérhető úti cél felé. A forgalmat csak a 192.168.10.0/24-ről a 192.168.30.0/24-re szűri.

Az alapvető elhelyezési irányelveket követve a rendszergazda szabványos ACL-t helyez el az R3 útválasztón. Két lehetséges interfész van az R3-on a szabványos ACL alkalmazásához:

* **R3 S0/1/1 interfész (bejövő)** – A szabványos ACL alkalmazható bejövőben az R3 S0/1/1 interfészen a .10-es hálózatról érkező forgalom letiltására. Ugyanakkor a .10-es forgalmat is kiszűrné a 192.168.31.0/24 (ebben a példában 0,31) hálózatba. Ezért a szabványos ACL-t nem szabad erre az interfészre alkalmazni.
* **R3 G0/0/0 interfész (kimenő)** - A szabványos ACL alkalmazható kimenően az R3 G0/0/0 interfészen. Ez nem érinti az R3 által elérhető többi hálózatot. A .10-es hálózatról érkező csomagok továbbra is elérhetik a .31-es hálózatot. Ez a legjobb interfész a szabványos ACL elhelyezéséhez, hogy megfeleljen a forgalmi követelményeknek.

8.5.5

## Packet Tracer – Névvel ellátott szabványos IPv4 ACL-ek konfigurálása

A vezető hálózati rendszergazda arra kérte, hogy hozzon létre egy elnevezett szabványos ACL-t, hogy megakadályozza a fájlkiszolgálóhoz való hozzáférést. Minden kliensnek egy hálózatról és egy adott munkaállomásról egy másik hálózatról meg kell tagadni a hozzáférést.

[Konfigurálja a nevesített szabványos IPv4 ACL-eket](https://contenthub.netacad.com/courses/netsec/_common/8.5.5-packet-tracer---configure-named-standard-ipv4-acls.pka)

8.5.6

## Packet Tracer – Számozott szabványos IPv4 ACL-ek konfigurálása

A szabványos hozzáférés-vezérlési listák olyan útválasztó konfigurációs parancsfájlok, amelyek a forráscím alapján szabályozzák, hogy az útválasztó engedélyezi-e vagy megtagadja-e a csomagokat. Ez a tevékenység a szűrési feltételek meghatározására, a szabványos ACL-ek konfigurálására, az ACL-ek útválasztó interfészekre történő alkalmazására, valamint az ACL megvalósításának ellenőrzésére és tesztelésére összpontosít. Az útválasztók már be vannak állítva.

[Számozott szabványos IPv4 ACL-ek konfigurálása](https://contenthub.netacad.com/courses/netsec/_common/8.5.6-packet-tracer---configure-numbered-standard-ipv4-acls.pka)

8.5.7

## Kibővített ACL elhelyezési példa

A kiterjesztett ACL-eket a forráshoz a lehető legközelebb kell elhelyezni. Ez megakadályozza, hogy nemkívánatos forgalmat küldjenek több hálózaton keresztül, és csak akkor kerüljenek elutasításra, amikor az eléri a célállomást.

A szervezet azonban csak az általa felügyelt eszközökön helyezhet el ACL-eket. Ezért a kiterjesztett ACL elhelyezést a szervezeti ellenőrzés kiterjedésének összefüggésében kell meghatározni.

Az ábrán például az A vállalat meg akarja tagadni a Telnet és az FTP forgalmat B vállalat 192.168.30.0/24-es hálózatához a 192.168.11.0/24-es hálózatáról, miközben engedélyezi az összes többi forgalmat.

Az ábra azt szemlélteti, hogyan helyezhet el kiterjesztett ACL-t a hálózaton. Ennek a hálózatnak három útválasztója és négy LAN-ja van. A felső közepén egy R 2 nevű router található. Alul és balra egy R 1 nevű router található, amely soros kábellel csatlakozik az R2-höz. Mind az R1, mind az R2 használja az S0/1/0 interfészt. Az R2-től jobbra van egy R3 nevű útválasztó, amely soros kábellel csatlakozik az R2-höz. Mind az R3, mind az R2 használja az S0/1/1 interfészt. R1-nek és R3-nak két-két LAN-ja van. Az R1-nek van egy LAN-ja, amely a G0/0/0-tól a P C1 csomóponttal rendelkező S1 kapcsolóhoz csatlakozik. Ez a 192.168.10.0/24 hálózat. Az R1-nek van egy második LAN-ja, amely a G0/0/1-től a P C2 csomóponttal rendelkező S2 kapcsolóhoz csatlakozik. Ez a 192.168.11.0/24 hálózat. Az R3-nak van egy LAN-ja, amely a G0/0/0-tól a P C3 csomóponttal rendelkező S3 kapcsolóhoz csatlakozik. Ez a 192.168.30.0/24 hálózat, és a P C3 IP-címe 192.168.30.12. Az R3-nak van egy második LAN-ja, amely a G0/0/1-től a P C4 csomóponttal rendelkező S4 kapcsolóhoz csatlakozik. Ez a 192.168.31.0/24 hálózat, és a P C4 IP-címe 192.168.31.12. A jobb felső sarokban egy narancssárga mező található, amelyen az FTP és Telnet forgalom blokkolása 192.168.11.0/24 és 192.168.30.0/24 között olvasható. Az R 1 és R 2 közötti soros összeköttetésen egy kék tölcsér található, a tölcsér széles vége az R 1 oldalán S0/1/0. A tölcsér felett egy négyzet található, amely a következőt írja: Megvizsgálja az összes forgalmat, mielőtt kilép az R 1 S0/1/0-ból. Egy második tölcsér, amely a LAN-on van az R1 és az S2 között. A tölcsér kis vége a G0/0/1 felületen van. A tölcsér mellett van egy doboz, amely azt írja ki: Csak a 192.168.11.0/24 forgalomból vizsgálja a forgalmat.

R2 R1 S1 S2 S3 S4 R3 PC1 PC3 PC2 PC4 S0/1/0 G0/0/0 192.168.11.0/24 192.168.30.0/24 192.168.31.0/24 S0/1/1 G0/0/1 192.168.10.0/24 G0/0/0 G0/0/1 S0/1/0

S0/1/1

Megvizsgálja az összes forgalmat az R1 S0/1/0 elhagyása előtt. Csak 192.168.11.0/24-től vizsgálja a forgalmat. **A vállalat B vállalat** FTP és Telnet forgalom blokkolása 192.168.11.0/24-től 192.168.30.0/24-ig.

Számos módja van ezeknek a céloknak a megvalósítására. Az R3 kibővített ACL-je elvégezné a feladatot, de a rendszergazda nem irányítja az R3-at. Ezen túlmenően ez a megoldás lehetővé teszi, hogy a nem kívánt forgalom a teljes hálózaton áthaladjon, csak a célállomáson blokkolják. Ez befolyásolja a hálózat általános hatékonyságát.

A megoldás egy kiterjesztett ACL elhelyezése az R1-en, amely megadja a forrás- és a célcímet is.

Két lehetséges interfész van az R1-en a kiterjesztett ACL alkalmazásához:

* **R1 S0/1/0 interfész (kimenő)** - A kiterjesztett ACL kimenően alkalmazható az S0/1/0 interfészen. Ez a megoldás azonban minden R1-et elhagyó csomagot feldolgoz, beleértve a 192.168.10.0/24-től származó csomagokat is.
* **R1 G0/0/1 interfész (bejövő)** – A kiterjesztett ACL bejövő bejövőben alkalmazható a G0/0/1-en, így csak a 192.168.11.0/24 hálózatból származó csomagok vonatkoznak az ACL-feldolgozásra az R1-en. Mivel a szűrőt csak a 192.168.11.0/24 hálózatot elhagyó csomagokra kell korlátozni, a legjobb megoldás a kiterjesztett ACL alkalmazása a G0/0/1-re.

8.5.8

## Ellenőrizze megértését – ACL-elhelyezési irányelvek

Az űrlap teteje

Ellenőrizze, hogy megértette-e az IPv4 ACL-ek típusait, és válassza ki a LEGJOBB választ a következő kérdésekre.

1. Melyik ACL képes a TCP portszám alapján szűrni?

Az űrlap alja

Melyik állítás igaz az ACL-ekről?

Hol kell elhelyezni egy szabványos ACL-t?

Hol kell elhelyezni egy kiterjesztett ACL-t?

8.5.9

## Ellenőrizze a megértését – Szabványos ACL-ek konfigurálása

Használja ezt a hálózati topológia diagramot a három forgatókönyv megválaszolásához.

Az ábra a referencia topológiát mutatja, amelyet a későbbi interaktív tevékenységek során használni fognak.

192.168.1.66 192.168.1.0/24LAN1 G0/0 G0/1 192.168.2.0/24LAN2 172.16.1.0/30 S0/0/0 S0/0/0 G0/1 192.168.4.0/24LAN4 G0/0 192.168.3.0/24LAN3 192.168.4.12 192.168.3.77 R2

R1

A forgatókönyv végrehajtásához szükség szerint tekintse meg a hálózati topológiai diagramot. Válassza ki a parancsokat a legördülő listákból. A 192.168.1.0 LAN-ba való belépés vezérléséhez állítsa be az útválasztót az ACL-cél eléréséhez. A 192.168.3.77-es gazdagépnek nem kell hozzáférnie ehhez a LAN-hoz, hanem a 192.168.3.0-s hálózat összes többi gazdagépéhez, majd a 192.168.4.0-s hálózat számára engedélyezni kell a hozzáférést. A tevékenység folytatásához kattintson a 2. forgatókönyv gombra.

**R1 konfigurációs parancsok**

8.5.10

## Ellenőrizze megértését – Hozzon létre egy kiterjesztett ACL-nyilatkozatot

Hozzon létre egy számozott ACL-utasítást, amely csak a 10.1.1.0/24-es hálózat felhasználói számára teszi lehetővé a HTTP-hozzáférést a 10.1.3.0/24-es hálózaton lévő webszerverhez. Az ACL az R2 S0/0/0 kimenőre vonatkozik.

Az 1. ábra egy fogd és vidd tevékenység egy kiterjesztett hozzáférési utasítás konfigurálására az 1. forgatókönyvhöz. A 2. ábra egy drag and drop tevékenység egy kiterjesztett hozzáférési nyilatkozat konfigurálásához a 2. forgatókönyvhöz. A 3. ábra egy drag and drop tevékenység kiterjesztett hozzáférési nyilatkozat konfigurálásához a 3. forgatókönyvhöz.

Hozzon létre egy kiterjesztett ACL-t a követelmények és a bemutatott topológia alapján. Válassza ki az ACL utasítás összetevőit a legördülő listákból, hogy balról jobbra olvasva létrehozzon egy érvényes ACL-t a forgatókönyvhöz. Egyes összetevők nem kerülnek felhasználásra.

Az ACL itt kerül alkalmazásra

8.5.11

## Ellenőrizze, hogy megértette-e a kiterjesztett ACL-eket

Kattintson az 1. forgatókönyv, 2. forgatókönyv, 3. forgatókönyv gombra a tevékenység befejezéséhez.   
Az alábbi képen bármikor áttekintheti a topológiát.

Az 1. ábra a következő három tevékenységben használt referencia topológia.

192.168.1.66 192.168.1.0/24LAN1 G0/0 S0/0/0 G0/1 192.168.2.0/24LAN2 172.16.1.0/30 192.168.4.12 192.168.4.0/24LAN4 G0/1 S0/0/0 G0/0 192.168.3.200 192.168.3.0/24LAN3 R1

R2

Kibővített ACL-ek a G0/0 bejövő bejövőre.

Lásd a topológiát a fenti ábrán. Ez a forgatókönyv biztosítja a kiterjesztett ACL 103-at, valamint a táblázatban szereplő forrás és cél kombinációkat. Ezen információk alapján határozza meg, hogy a csomagok engedélyezettek vagy megtagadtak-e. Válassza az Engedélyezés vagy a Megtagadás lehetőséget az egyes forrás- és célkombinációk melletti legördülő listában. A folytatáshoz kattintson a 2. forgatókönyvre.

Forrás

Rendeltetési hely

Engedélyezni vagy megtagadni

8.5.12

## Packet Tracer – Kibővített ACL-ek konfigurálása 1. forgatókönyv

Ebben a Packet Tracer tevékenységben a következő célokat valósítja meg:

* 1. rész: Kiterjesztett számozású IPv4 ACL konfigurálása, alkalmazása és ellenőrzése
* 2. rész: Kibővített IPv4 ACL konfigurálása, alkalmazása és ellenőrzése

[Kibővített ACL-ek konfigurálása 1. forgatókönyv](https://contenthub.netacad.com/courses/netsec/_common/8.5.12-packet-tracer---configure-extended-ipv4-acls---scenario-1.pka)

8.5.13

## Packet Tracer – Kibővített ACL-ek konfigurálása 2. forgatókönyv

Ebben a Packet Tracer tevékenységben a következő célokat valósítja meg:

* 1. rész: Nevesített kiterjesztett IPv4 ACL konfigurálása
* 2. rész: A kiterjesztett IPv4 ACL alkalmazása és ellenőrzése

[Configure Extended ACLs Scenario 2](https://contenthub.netacad.com/courses/netsec/_common/8.5.13-packet-tracer---configure-extended-ipv4-acls---scenario-2.pka)

[8.4](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Modify ACLs](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[8.6](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Mitigate Attacks with ACLs](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                             
*                           

1. Hozzáférés-vezérlési listák
2. Mitigate Attacks with ACLs

# Mérsékelje a támadásokat ACL-ekkel

8.6.1

## Csökkentse a hamisítási támadásokat

Az ACL-ek számos hálózati fenyegetés mérséklésére használhatók, mint például az IP-címhamisítás és a szolgáltatásmegtagadási (DoS) támadások. A legtöbb DoS támadás valamilyen hamisítást használ. Az IP-cím hamisítása felülírja a normál csomaglétrehozási folyamatot azáltal, hogy beszúr egy egyéni IP-fejlécet egy másik forrás IP-címmel. A támadók elrejthetik személyazonosságukat a forrás IP-cím meghamisításával.

Az IP-címeknek számos jól ismert osztálya létezik, amelyeket soha nem szabad forrás IP-címnek tekinteni a szervezet hálózatába érkező forgalom számára. Például az ábrán az S0/0/0 interfész az internethez kapcsolódik, és soha nem fogadhat be bejövő csomagokat a következő címekről:

* Minden nulla cím
* Műsorszórási címek
* Helyi gazdagép címek (127.0.0.0/8)
* Automatikus privát IP-címzés (APIPA) címek (169.254.0.0/16)
* Fenntartott privát címek (RFC 1918)
* IP multicast címtartomány (224.0.0.0/4)

A 192.168.1.0/24 hálózat az R1 G0/0 interfészhez csatlakozik. Ennek az interfésznek csak az adott hálózatból származó forráscímmel rendelkező bejövő csomagokat kell engedélyeznie. Az ábrán látható G0/0 ACL csak a 192.168.1.0/24 hálózatról engedélyezi a bejövő csomagokat. Az összes többit eldobjuk.

Az ábrán egy számítógép látható, amely G0/0-n keresztül csatlakozik az R1-hez 192.168.1.0 / 24 címmel. Az R1 az S0/0/0-n keresztül csatlakozik az internethez.

R1 192.168.1.0/24 G0/0

S0/0/0

Internet

Bejövő S0/0/0:

R1(config)# **access-list 150 deny ip host 0.0.0.0 any**

R1(config)# **access-list 150 deny ip 10.0.0.0 0.255.255.255 any**

R1(config)# **access-list 150 deny ip 127.0.0.0 0.255.255.255 any**

R1(config)# **access-list 150 deny ip 172.16.0.0 0.15.255.255 any**

R1(config)# **access-list 150 deny ip 192.168.0.0 0.0.255.255 any**

R1(config)# **access-list 150 deny ip 224.0.0.0 15.255.255.255 any**

R1(config)# **access-list 150 deny ip host 255.255.255.255 any**

Bejövő G0/0:

R1(config)# **access-list 105 permit ip 192.168.1.0 0.0.0.255 any**

8.6.2

## Engedélyezze a szükséges forgalmat tűzfalon keresztül

A támadások mérséklésének hatékony stratégiája az, ha kifejezetten csak bizonyos típusú forgalmat engedélyezünk a tűzfalon keresztül. Például a tartománynévrendszer (DNS), az egyszerű levelezési átviteli protokoll (SMTP) és a fájlátviteli protokoll (FTP) olyan szolgáltatások, amelyeket gyakran tűzfalon keresztül kell engedélyezni. Az is gyakori, hogy a tűzfalat úgy konfigurálják, hogy lehetővé tegye a rendszergazdák számára a távoli hozzáférést a tűzfalon keresztül. A Secure Shell (SSH), a syslog és az Simple Network Management Protocol (SNMP) példák azokra a szolgáltatásokra, amelyeket egy útválasztónak tartalmaznia kell. Bár ezen szolgáltatások közül sok hasznos, ellenőrizni és felügyelni kell őket. E szolgáltatások kihasználása biztonsági résekhez vezet.

Az ábra egy példa topológiát mutat be ACL-konfigurációkkal, amelyek lehetővé teszik bizonyos szolgáltatások engedélyezését a Serial 0/0/0 interfészen.

Az ábrán egy 200.5.5.5 / 24 címû, internetre csatlakoztatott számítógép látható. Az internet s0/0/0-n keresztül csatlakozik az R 1-hez 10.0.1.1 címmel. Az R1 a G0/1-en keresztül csatlakozik a P C1-hez. Az R1 G0.0-n keresztül csatlakozik egy szerverhez. A szerverhálózat 192.168.20.2 / 24. A szerver alatt a dns, smtp és ft p szöveg található.

R1 PC1 200.5.5.5/24 Serial 0/0/0 10.0.1.1 G0/1

G0/0

Internet 192.168.20.2/24   
DNS, SMTP, FTP

### Bejövő soros 0/0/0

R1(config)# **access-list 180 permit udp any host 192.168.20.2 eq domain**

R1(config)# **access-list 180 permit tcp any host 192.168.20.2 eq smtp**

R1(config)# **access-list 180 permit tcp any host 192.168.20.2 eq ftp**

R1(config)# **access-list 180 permit tcp host 200.5.5.5 host 10.0.1.1 eq 22**

R1(config)# **access-list 180 permit udp host 200.5.5.5 host 10.0.1.1 eq syslog**

R1(config)# **access-list 180 permit udp host 200.5.5.5 host 10.0.1.1 eq snmptrap**

8.6.3

## Csökkentse az ICMP támadásokat

A hackerek az Internet Control Message Protocol (ICMP) visszhangcsomagjait (ping) használhatják a védett hálózaton lévő alhálózatok és gazdagépek felderítésére, valamint DoS árvízi támadások generálására. A hackerek ICMP átirányítási üzenetekkel módosíthatják a gazdagép útválasztási tábláit. Az ICMP visszhang- és átirányítási üzeneteket is blokkolnia kell az útválasztónak.

Számos ICMP-üzenet ajánlott a megfelelő hálózati működéshez, és be kell engedni a belső hálózatba:

* **Echo válasz** – Lehetővé teszi a felhasználók számára, hogy külső gazdagépeket pingeljenek.
* **Source quench** – Azt kéri, hogy a feladó csökkentse az üzenetek forgalmi sebességét.
* **Elérhetetlen** – Az ACL által adminisztratívan letiltott csomagokhoz jön létre.

A hálózat megfelelő működéséhez több ICMP üzenetre van szükség, és engedélyezni kell a hálózatból való kilépést:

* **Echo** – Lehetővé teszi a felhasználók számára, hogy külső gazdagépeket pingeljenek.
* **Paraméterprobléma** – Tájékoztatja a gazdagépet a csomagfejléc-problémákról.
* **Túl nagy a csomag** – Lehetővé teszi a csomagmaximális átviteli egység (MTU) felderítését.
* **Forrás kioltása** – Szükség esetén csökkenti a forgalmat.

Általános szabály, hogy az összes többi kimenő ICMP-üzenettípust blokkolja.

Az ACL-ek az IP-címhamisítás blokkolására, meghatározott szolgáltatások tűzfalon keresztüli szelektív engedélyezésére és csak a szükséges ICMP-üzenetek engedélyezésére szolgálnak. Az ábra egy minta topológiát és lehetséges ACL-konfigurációkat mutat be, amelyek lehetővé teszik bizonyos ICMP-szolgáltatásokat a G0/0 és S0/0/0 interfészeken.

Az ábrán egy internetre csatlakoztatott számítógép látható, amelynek címe 209.165.201.3 / 24. Az internet az R 1-hez csatlakozik az s0/0/0-n keresztül. Az R1 G0.0-n keresztül csatlakozik egy szerverhez. A szerverhálózat 192.168.1.0 / 24.

R1 209.165.201.3/24 S0/0/0 G0/0

192.168.1.0/24

Internet

Bejövő S0/0/0:

R1(config)# **access-list 112 permit icmp any any echo-reply**

R1(config)# **access-list 112 permit icmp any any source-quench**

R1(config)# **access-list 112 permit icmp any any unreachable**

R1(config)# **access-list 112 deny icmp any any**

R1(config)# **access-list 112 permit ip any any**

Bejövő G0/0:

R1(config)# **access-list 114 permit icmp 192.168.1.0 0.0.0.255 any echo**

R1(config)# **access-list 114 permit icmp 192.168.1.0 0.0.0.255 any parameter-problem**

R1(config)# **access-list 114 permit icmp 192.168.1.0 0.0.0.255 any packet-too-big**

R1(config)# **access-list 114 permit icmp 192.168.1.0 0.0.0.255 any source-quench**

R1(config)# **access-list 114 deny icmp any any**

R1(config)# **permit ip any any**

8.6.4

## Csökkentse az SNMP-támadásokat

A felügyeleti protokollok, például az SNMP, hasznosak a hálózati eszközök távoli megfigyeléséhez és kezeléséhez. Ezek azonban továbbra is kihasználhatók. Ha SNMP-re van szükség, az SNMP-sebezhetőségek kihasználása csökkenthető interfész ACL-ek alkalmazásával a nem engedélyezett rendszerek SNMP-csomagjainak kiszűrésére. A kizsákmányolás továbbra is lehetséges, ha az SNMP-csomag olyan címről származik, amelyet hamisítottak, és amelyet az ACL engedélyez.

Ezek a biztonsági intézkedések hasznosak, de a kizsákmányolás megelőzésének leghatékonyabb módja az SNMP-kiszolgáló letiltása azokon az IOS-eszközökön, amelyekhez nincs szükség rá. Az ábrán látható módon használja a **no snmp-server** paranccsal az SNMP-szolgáltatásokat a Cisco IOS-eszközökön.

Az ábrán egy számítógép látható, amelyen egy hacker csatlakozik az internethez. Az internet routerhez csatlakozik. a számítógép képernyőjén az snmp exploit próbálkozása olvasható. A router felett van egy buborék, amelyen az snmp tiltva olvasható. snmp kérés elutasítva.



SNMP kihasználási kísérlet SNMP letiltva,   
SNMP-kérés elutasítva. Internet

Router(config)# **no snmp-server**

8.6.5

## Packet Tracer – IP ACL-ek konfigurálása a támadások mérséklésére

Ebben a Packet Tracerben a következő célokat valósítja meg:

* A tűzfal konfigurálása előtt ellenőrizze az eszközök közötti kapcsolatot.
* Használjon ACL-eket annak biztosítására, hogy az útválasztókhoz csak a PC-C felügyeleti állomásról legyen távoli hozzáférés.
* A támadások mérséklése érdekében konfigurálja az ACL-eket az R1-en és az R3-on.
* Ellenőrizze az ACL működését.

[Konfigurálja az IP ACL-eket a támadások mérséklésére](https://contenthub.netacad.com/courses/netsec/_common/8.6.5-packet-tracer---configure-ip-acls-to-mitigate-attacks.pka)

[8.5](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Implement ACLs](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[8.7](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[IPv6 ACLs](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                               
*                           

1. Hozzáférés-vezérlési listák
2. IPv6 ACLs

# IPv6 ACL-ek

8.7.1

## IPv6 ACL áttekintése

Az elmúlt években sok hálózat megkezdte az átállást az IPv6-os környezetre. Az IPv6-ra való átállás szükségességét részben az IPv4 eredendő gyengeségei okozzák.

Sajnos, ahogy az IPv6-ra való átállás folytatódik, az IPv6-támadások egyre elterjedtebbek. Az IPv4 nem tűnik el egyik napról a másikra. Az IPv4 együtt fog létezni az IPv6-tal, majd fokozatosan felváltja az IPv6. Ez potenciális biztonsági réseket hoz létre. A biztonsági aggályok egyik példája a fenyegetés szereplői, akik az IPv4-et kihasználják az IPv6 kiaknázására kettős veremkörnyezetekben. A kettős verem egy olyan integrációs módszer, amelyben az eszköz IPv4- és IPv6-hálózatokhoz egyaránt csatlakozik. Kettős verem környezetben az eszközök két IP protokoll veremmel működnek.

A fenyegető szereplők titkos támadásokat hajthatnak végre, amelyek a bizalom kihasználását eredményezik kettős halmozott gazdagépek, szélhámos Neighbor Discovery Protocol (NDP) üzenetek és alagútkezelési technikák használatával. A Teredo tunneling például egy IPv6-átmeneti technológia, amely automatikus IPv6-cím hozzárendelést biztosít, amikor az IPv4/IPv6-gazdagépek az IPv4 hálózati címfordító (NAT) eszközök mögött helyezkednek el. Ezt úgy éri el, hogy az IPv6-csomagokat az IPv4 UDP-csomagokba ágyazza. A fenyegetés szereplője megveti a lábát az IPv4 hálózatban. A feltört gazdagép rosszindulatú útválasztó hirdetéseket (RA-kat) küld, amelyek elindítják a kettős halmozott gazdagépeket, hogy IPv6-címet kapjanak. A fenyegetés szereplője ezután ezt a támaszpontot használhatja a hálózaton belüli mozgáshoz vagy elforduláshoz. A fenyegetés szereplője további gazdagépeket is feltörhet, mielőtt a forgalmat visszaküldené a hálózatból, amint az az ábrán látható.

Az ábra egy minta IP v6 kihasználását mutatja az előző szövegből.

### Minta IPv6 Exploit

A fenyegető szereplők forgalma az IPv4-en keresztül nyeri meg a lábát, csaló IPv6 RA-kat küld, és IPv6-gazdagépek használatával forog. Az ismeretlen IPv6-gazdagépek automatikusan konfigurálják a veremeiket az UDP használatával automatikus Teredo-alagutak elindításával. Az IPv4 tűzfal látja és engedélyezi az IPv4 UDP forgalmat.

Ki kell dolgozni és végre kell hajtani egy stratégiát az IPv6-infrastruktúrák és protokollok elleni támadások mérséklésére. Ennek a mérséklő stratégiának magában kell foglalnia a széleken történő szűrést különféle technikák, például IPv6 ACL-ek használatával.

8.7.2

## IPv6 ACL szintaxis

Az IPv6 ACL funkciói hasonlóak az IPv4 ACL-eihez. Az IPv4 szabványos ACL-eknek azonban nincs megfelelője. Ezenkívül minden IPv6 ACL-t névvel kell konfigurálni. Az IPv6 ACL-ek lehetővé teszik a forrás- és célcímek alapján történő szűrést, amelyek egy adott interfészhez be- és kimennek. Támogatják az IPv6-opciófejléceken és az opcionális, felső rétegbeli protokolltípus-információkon alapuló forgalomszűrést is a pontosabb vezérlés érdekében, hasonlóan az IPv4 kiterjesztett ACL-eihez. Az IPv6 ACL konfigurálásához használja az **ipv6 access-list** parancsot, hogy belépjen az IPv6 ACL konfigurációs módba. Ezután használja az ábrán látható szintaxist a hozzáférési lista egyes bejegyzéseinek konfigurálásához úgy, hogy kifejezetten engedélyezze vagy tiltsa a forgalmat. A bemutatott szintaxis az IPv6 ACE szintaxis egyszerűsített változata. Vannak további lehetőségek is. A megadott szintaxisból egyértelműnek kell lennie, hogy az IPv6 ACL-ek lényegesen rugalmasabbak, mint az IPv4 ACL-ek.

Alkalmazzon IPv6 ACL-t egy interfészre az **ipv6 forgalomszűrő** paranccsal.

Router(config)# **ipv6 access-list** access-list-name

Router(config-ipv6-acl)# **deny** | **permit** protocol {source-ipv6-prefix **/** prefix-length | **any** | **host** source-ipv6-address} [ operator [ port-number ]] { destination-ipv6-prefix **/** prefix-length | **any** | **host** destination-ipv6-address } [ operator [ port-number ]] [ **dscp** value ] [ **fragments** ] [ **log** ] [ **log-input** ] [ **sequence** value ] [ **time-range** name ]

| **Paraméter** | **Leírás** |
| --- | --- |
| **tagadni**  |  **engedély** | Meghatározza, hogy a csomagot meg kell-e tiltani vagy engedélyezni. |
| jegyzőkönyv | Adja meg az Internet protokoll nevét vagy számát, vagy egy IPv6-protokoll számát jelző egész számot. |
| forrás-ipv6-előtag  **/**    előtag-hosszúságú cél-ipv6-cím  **/**  előtag-hossz | A forrás- vagy cél IPv6-hálózat vagy hálózatosztály, amelyre vonatkozóan **tiltási** vagy **engedélyezési** feltételeket kell beállítani. |
| **Bármi** | Írja be **az** IPv6 előtag ::/0 rövidítéseként. Ez megfelel az összes címnek. |
| **házigazda** | forrás **A gazdagép** -ipv6-címe vagy cél-ipv6-címe mezőben adja meg azt a forrás- vagy cél IPv6-gazdacímet, amelyre vonatkozóan **tiltási** vagy **engedélyezési** feltételeket kíván beállítani. |
| operátor | (Opcionális) Operandus, amely összehasonlítja a megadott protokoll forrás- vagy célportjait. Az operandusok a következők: **lt** (kisebb, mint), **gt** (nagyobb), **eq** (egyenlő), **neq** (nem egyenlő) és **tartomány** . |
| port-szám | (Opcionális) TCP- vagy UDP-port tizedes szám vagy neve a TCP vagy UDP szűréséhez. |
| **dscp** | (Opcionális) Megfelel egy megkülönböztetett szolgáltatáskódpont-értéket a forgalmi osztály értékével az egyes IPv6-csomagfejlécek Forgalmi osztály mezőjében. Az elfogadható tartomány 0 és 63 között van. |
| **töredékek** | (Opcionális) Megfelel a nem kezdeti töredezett csomagoknak, ahol a töredékkiterjesztés fejléce nullától eltérő töredékeltolást tartalmaz. A **fragments** kulcsszó csak akkor használható, ha a ] operátor [ portszám argumentumai nincsenek megadva. Ha ezt a kulcsszót használja, akkor is egyezik, ha az első töredék nem rendelkezik 4. réteg információval. |
| **log** | (Opcionális) Információs naplózási üzenetet küld a csomagról, amely megfelel a konzolnak küldendő bejegyzésnek. parancs szabályozza **(A konzolra naplózott üzenetek szintjét a naplózási konzol** .) |
| **napló bevitel** | (Opcionális) Ugyanazt a funkciót biztosítja, mint a **napló** kulcsszó, kivéve, hogy a naplózási üzenet tartalmazza a beviteli felületet is. |
| **sorozat**  értéke | (Nem kötelező) Megadja sorszámát a hozzáférési lista utasításának . Az elfogadható tartomány 1 és 4294967295 között van. |
| **időtartomány**  neve | (Választható) Megadja az engedély nyilatkozatra vonatkozó időtartamot. Az időtartomány nevét , és korlátozásait az **időtartomány** , illetve **az abszolút** illetve **periodikus** parancsok adják meg. |

8.7.3

## Konfigurálja az IPv6 ACL-eket

Az IPv6 ACL tartalmaz egy implicit **deny ipv6 any any** . Minden IPv6 ACL tartalmaz implicit engedélyezési szabályokat is, amelyek lehetővé teszik az IPv6 szomszédos felderítését. Az IPv6 Neighbor Discovery Protocol (NDP) megköveteli az IPv6 hálózati réteg használatát szomszédos hirdetések (NA-k) és szomszédos felkérések (NS-ek) küldéséhez. Ha egy adminisztrátor úgy konfigurálja a **deny ipv6** parancsot, hogy nem kifejezetten engedélyezi a szomszédkeresést, akkor az NDP letiltásra kerül.

Az ábrán az R1 engedélyezi a bejövő forgalmat a G0/0-n a 2001:DB8:1:1::/64 hálózatról. Az NA és NS csomagok kifejezetten engedélyezettek. Minden más IPv6-címről származó forgalom kifejezetten meg van tiltva. Ha az adminisztrátor csak az első engedélyezési utasítást konfigurálta, az ACL-nek ugyanaz a hatása. Jó gyakorlat azonban az implicit utasítások explicit konfigurálásával dokumentálni.

Az ábrán egy számítógép látható, amely G0/0-n keresztül csatlakozik az R1-hez 2001:DB8:1:1:: / 64 hálózati címmel.

R1

Internet 2001:DB8:1:1::/64 G0/0

R1(config)# **ipv6 access-list LAN\_ONLY**

R1(config-ipv6-acl)# **permit 2001:db8:1:1::/64 any**

R1(config-ipv6-acl)# **permit icmp any any nd-na**

R1(config-ipv6-acl)# **permit icmp any any nd-ns**

R1(config-ipv6-acl)# **deny ipv6 any any**

R1(config-ipv6-acl)# **end**

R1# **show ipv6 access-list**

IPv6 access list LAN\_ONLY

permit ipv6 2001:DB8:1:1::/64 any sequence 10

permit icmp any any nd-na sequence 20

permit icmp any any nd-ns sequence 30

deny ipv6 any any sequence 40

R1#

8.7.4

## Packet Tracer – IPv6 ACL-ek konfigurálása

Ebben a Packet Tracerben a következő célokat valósítja meg:

* IPv6 ACL konfigurálása, alkalmazása és ellenőrzése
* Konfiguráljon, alkalmazzon és ellenőrizze egy második IPv6 ACL-t

[Konfigurálja az IPv6 ACL-eket.](https://contenthub.netacad.com/courses/netsec/_common/8.7.4-packet-tracer---configure-ipv6-acls.pka)

[8.6](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Mitigate Attacks with ACLs](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[8.8](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Access Control Lists Summary](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                                                          

1. Hozzáférés-vezérlési listák
2. Access Control Lists Summary

# Hozzáférés-vezérlési listák összefoglalása

8.8.1

## Mit tanultam ebben a modulban?

**Bevezetés a hozzáférés-vezérlési listákba**   
Az ACL olyan IOS-parancsok sorozata, amelyek a csomagok fejlécében található információk alapján a csomagok szűrésére szolgálnak. Alapértelmezés szerint az útválasztónak nincs konfigurálva ACL-je. Az ACL az engedélyezési vagy megtagadási utasítások szekvenciális listáját használja, amelyeket ACE-ként ismerünk. A csomagszűrési folyamat akkor következik be, amikor a hálózati forgalom egy ACL-lel konfigurált interfészen halad át, és az útválasztó összehasonlítja a csomagon belüli információkat az egyes ACE-ekkel, egymás utáni sorrendben, hogy megállapítsa, a csomag egyezik-e valamelyik ACE-vel. A csomagszűrés a 3. vagy 4. rétegben történhet. A Cisco útválasztók támogatják a szabványos és kiterjesztett ACL-eket. Az 1-től 99-ig vagy az 1300-tól 1999-ig terjedő ACL-ek szabványos ACL-ek, míg a 100-tól 199-ig vagy a 2000-től 2699-ig terjedő ACL-ek kiterjesztett ACL-ek. Az ACL-ek konfigurálásakor az elnevezett ACL-eket részesítjük előnyben. A név információt nyújt az ACL céljáról. Az ACL-ek meghatározzák azokat a szabályokat, amelyek további vezérlést biztosítanak a bejövő interfészekre belépő, az útválasztón keresztül továbbító csomagok és az útválasztó kimenő interfészeiről kilépő csomagok számára.

**Helyettesítő karakter maszkolás**   
Az IPv4 ACE 32 bites helyettesítő karakter maszkot használ annak meghatározására, hogy a cím mely bitjeit kell megvizsgálni az egyezéshez. A helyettesítő maszkokat az OSPF útválasztási protokoll is használja. A helyettesítő karakteres maszk hasonló az alhálózati maszkhoz, mivel az ÉS-ezési folyamatot használja annak azonosítására, hogy az IPv4-cím mely bitjei egyeznek. Mindazonáltal különböznek a bináris 1-esek és 0-ák párosítási módjában. Ellentétben az alhálózati maszkokkal, amelyekben a bináris 1 egyenlő egyezéssel, és a bináris 0 nem egyezés, a helyettesítő karakteres maszk esetében ennek az ellenkezője igaz. A helyettesítő karakteres maszkok kiszámításának egyik parancsikonja az alhálózati maszk kivonása a 255.255.255.255-ből. A Cisco IOS két kulcsszót kínál, **a host** és **any** , a helyettesítő karakteres maszkolás leggyakoribb használatának egyszerűsítésére. A kulcsszavak csökkentik az ACL billentyűleütések számát, és megkönnyítik az ACE olvasását.

**ACL-ek konfigurálása**   
Komplex ACL konfigurálásakor javasoljuk, hogy használjon szövegszerkesztőt, írja ki a megvalósítandó házirend sajátosságait, adja hozzá az IOS konfigurációs parancsait a feladatok végrehajtásához, tegyen megjegyzéseket az ACL dokumentálásához, és másolja és illessze be a parancsokat. a készülékre. Mindig alaposan tesztelje az ACL-t, hogy megbizonyosodjon arról, hogy megfelelően alkalmazza a kívánt házirendet. Számozott szabványos ACL létrehozásához használja az **access-list** access-list-number { **deny** | **parancsot engedély** | **megjegyzés** szöveg} forrás [ source-wildcard ] [ **log** ] . Elnevezett szabványos ACL létrehozásához használja az **ip access-list standard** access-list-name parancsot . Az ACL-nevek alfanumerikusak, megkülönböztetik a kis- és nagybetűket, és egyedinek kell lenniük. A kiterjesztett ACL-ek beállításának eljárási lépései ugyanazok, mint a szabványos ACL-ek esetében. A kiterjesztett IPv4 ACL interfészre történő alkalmazására vonatkozó parancs megegyezik a szabványos IPv4 ACL-ekhez használt paranccsal: **ip access-group** { access-list-number | access-list-name } { **in** | **ki** }. A kiterjesztett ACL-ek számos különböző típusú internetes protokollon és porton szűrhetnek. A TCP alapvető állapotjelző tűzfalszolgáltatásokat is képes végrehajtani a TCP használatával **megállapított** kulcsszó. A kulcsszó lehetővé teszi a belső forgalom számára, hogy kilépjen a belső magánhálózatból, és a visszatérő válaszforgalom belépjen a belső magánhálózatba.

**ACL-ek módosítása**   
A több ACE-vel rendelkező ACL-eket szövegszerkesztőben kell létrehozni. Ezzel megtervezheti a szükséges ACE-ket, létrehozhatja az ACL-t, majd beillesztheti az útválasztó felületére, és egyszerűbbé teszi az ACL szerkesztését. Az ACL ACE is törölhető vagy hozzáadható az ACL sorozatszámok használatával. A sorszámok automatikusan hozzárendelődnek az ACE beírásakor. parancsban vannak felsorolva **Ezek a számok a show access-lists** .

**ACL-ek megvalósítása**   
Az ACL konfigurálásakor és alkalmazásakor ügyeljen a listában összefoglalt irányelvekre:

* Hozzon létre egy ACL-t globálisan, majd alkalmazza azt.
* Győződjön meg arról, hogy az utolsó utasítás implicit **deny any** vagy **deny ip any any** .
* Ne feledje, hogy az utasítások sorrendje fontos, mert az ACL-ek feldolgozása felülről lefelé történik.
* Amint egy utasítás egyezik, az ACL kilép.
* Mindig szűrje a legspecifikusabbtól a legáltalánosabbig. Például tiltson le egy adott gazdagépet, majd engedélyezze az összes többi gazdagépet.
* Ne feledje, hogy interfészenként, protokollonként és irányonként csak egy ACL engedélyezett.
* Ne feledje, hogy a meglévő ACL új utasításai alapértelmezés szerint az ACL aljára kerülnek.
* Ne feledje, hogy a router által generált csomagokat nem szűrik a kimenő ACL-ek.
* Helyezze el a szabványos ACL-eket a lehető legközelebb a célhoz.
* Helyezze a kiterjesztett ACL-eket a forráshoz a lehető legközelebb.

Minden ACL-t ott kell elhelyezni, ahol a leghatékonyabb. A kiterjesztett ACL-eket a lehető legközelebb kell elhelyezni a szűrendő forgalom forrásához. A szabványos ACL-eket a lehető legközelebb kell elhelyezni a célhoz. Az ACL elhelyezését befolyásoló tényezők közé tartozik a szervezeti irányítás mértéke, az érintett hálózatok sávszélessége és a könnyű konfigurálás.

**Mérsékelje a támadásokat ACL-ekkel**   
Az ACL-ek számos hálózati fenyegetés – például az IP-cím-hamisítás és a DoS-támadások – mérséklésére használhatók. A támadások mérséklésének hatékony stratégiája az, ha kifejezetten csak bizonyos típusú forgalmat engedélyezünk a tűzfalon keresztül. Az ICMP visszhang- és átirányítási üzeneteket is blokkolnia kell az útválasztónak. Ha SNMP-re van szükség, az SNMP-sebezhetőségek kihasználása csökkenthető interfész ACL-ek alkalmazásával a nem engedélyezett rendszerek SNMP-csomagjainak kiszűrésére. Számos ICMP-üzenet ajánlott a megfelelő hálózati működéshez, és be kell engedni a belső hálózatba, beleértve a visszhangválaszt, a forráskioltást és az elérhetetlenséget. Több ICMP-üzenetnek is engedélyeznie kell a hálózatból való kilépést, beleértve a visszhangot, a paraméterproblémát, a túl nagy csomagot és a forráskioltást. Általános szabály, hogy az összes többi kimenő ICMP-üzenettípust blokkolja.

**IPv6 ACL-ek**   
Az IPv6 számos olyan funkcióval rendelkezik, amelyek megfelelnek a modern hálózati követelményeknek: IPsec, mobil IP, RSVP és címskálázhatóság. A kettős verem egy olyan integrációs módszer, amelyben az eszköz IPv4- és IPv6-hálózatokhoz egyaránt csatlakozik. Kettős verem környezetben az eszközök két IP protokoll veremmel működnek. A támadók kettős halmozott gazdagépek, csaló NDP-üzenetek és alagútkezelési technikák használatával hajthatnak végre lopakodó támadásokat, amelyek a bizalom kihasználását eredményezik. Az IPv6-infrastruktúrák és -protokollok elleni támadások mérséklése érdekében a stratégiának tartalmaznia kell a széleken történő szűrést különböző technikák, például IPv6 ACL-ek használatával. Az IPv6 ACL funkciói hasonlóak az IPv4 ACL-eihez. Az IPv4 szabványos ACL-eknek azonban nincs megfelelője. Ezenkívül minden IPv6 ACL-t névvel kell konfigurálni. Az IPv6 ACL-ek lehetővé teszik a forrás- és célcímek alapján történő szűrést, amelyek egy adott interfészhez be- és kimennek. Támogatják az IPv6-opciófejléceken és az opcionális, felső rétegbeli protokolltípus-információkon alapuló forgalomszűrést is a pontosabb vezérlés érdekében, hasonlóan az IPv4 kiterjesztett ACL-eihez.

8.8.2

## Modul – Hozzáférés-vezérlési listák kvíz

Az űrlap teteje

1. Ha ACL-t alkalmaz egy útválasztó interfészére, melyik forgalom számít kimenőnek?

Az űrlap alja

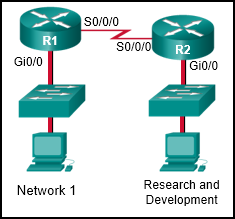
Mi a leggyorsabb módja egyetlen ACE eltávolításának egy elnevezett ACL-ből?

Melyik ICMP üzenettípust kell leállítani a bejövő bejövőben?

Melyik forgatókönyv okozna hibás ACL-konfigurációt és letilt minden forgalmat?

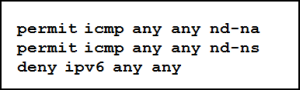
PC1 is connected to switch S1 on port Fa0/2. Port Fa0/1 of switch S1 is connected to port Fa0/1 of router R1. Port S0/1 of router R1 is connected to port S0/1 of router R2. Port Fa0/1 of router R2 is connected to port Fa0/1 of switch S2. Switch S2 is connected to PC2 on port Fa0/2. Below switch S1 is written the network 2001:DB8:CAFE:10::/64. Below switch S2 is written 2001:DB8:CAFE:30::/64. Between router R1 and router R2 is written 2001:DB8:CAFE:12::/64. PC1 has address 2001:DB8:CAFE:10::A/64 and PC2 has address 2001:DB8:CAFE:30::A/64.  
  
To the right of the graphic is the output of commands from router R1.  
R1# **show ipv6 access\-list**  
IPv6 access list Deny\_WEB  
    permit tcp 2001:DB8:CAFE:10::/64 any eq www sequence 10  
    permit tcp 2001:DB8:CAFE:10::/64 any eq 443 sequence 20  
    deny tcp host 2001:DB8:CAFE:10::A any eq www sequence 30  
    deny tcp host 2001:DB8:CAFE:10::A any eq 443 sequence 40  
R1#  
R1# **show running\-config**  
&lt;output omitted&gt;  
interface Serial0/1  
ipv6 address 2001:DB8:CAFE:12::1/64  
ipv6 traffic\-filter Deny\_WEB out

Hivatkozz a kiállításra. Egy hálózati rendszergazda IPv6 ACL-t konfigurál, hogy a 2001:DB8:CAFE:10::/64 hálózaton lévő gazdagépek hozzáférjenek a távoli webkiszolgálókhoz, kivéve a PC1-et. A PC1 felhasználója azonban sikeresen hozzáférhet a PC2 webszerverhez. Miért lehetséges ez?



Hivatkozz a kiállításra. Egy hálózati rendszergazda szabványos ACL-t szeretne létrehozni, hogy megakadályozza a Network 1 forgalom továbbítását a kutatási és fejlesztési hálózatra. Melyik router interfészen és milyen irányban kell a szabványos ACL-t alkalmazni?

Melyik két utasítás írja le a megfelelő általános irányelveket az ACL-ek konfigurálásához és alkalmazásához? (Válassz kettőt.)



Hivatkozz a kiállításra. Melyik állítás írja le az ACE-k funkcióját?

Melyik helyettesítő karakter maszk felel meg a 172.16.0.0 és 172.19.0.0 közötti hálózatoknak?

Milyen módszerrel alkalmazzák az IPv6 ACL-t az útválasztó interfészére?

Milyen típusú ACL kínál nagyobb rugalmasságot és szabályozást a hálózati hozzáférés felett?

Melyik operátort használják egy ACL utasításban egy adott alkalmazás csomagjainak egyeztetésére?

Melyik két kulcsszó használható a hozzáférés-vezérlési listában a helyettesítő karakter maszk vagy a cím és a helyettesítő karakter maszk párjának helyettesítésére? (Válassz kettőt.)

Vegye figyelembe a következő hozzáférési listát.

**hozzáférés - 100-as lista engedélyezése ip host 192.168.10.1 any**   
**hozzáférés - lista 100 deny icmp 192.168.10.0 0.0.0.255 minden visszhang**   
**hozzáférés - 100-as lista engedélyezése ip any any**

Melyik két művelet történik, ha a hozzáférési lista a 192.168.10.254 IP-címmel rendelkező router Gigabit Ethernet portjára kerül? (Válassz kettőt.)

[8.7](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[IPv6 ACLs](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[9.0](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                                        
*                         

1. Firewall Technologies
2. Introduction

# Bevezetés

9.0.1

## Miért vegyem ezt a modult?

A hálózatbiztonságot fenyegető számos fenyegetés mellett hogyan lehet a hálózatokat úgy megtervezni, hogy megvédjék az adatforrásokat, és biztosítsák a hálózati szolgáltatások igény szerinti biztosítását? A hálózati biztonsági infrastruktúra meghatározza az eszközök összekapcsolásának módját a végpontok közötti biztonságos kommunikáció érdekében. Ahogyan sokféle hálózat létezik, sokféleképpen lehet biztonságos hálózati infrastruktúrát kiépíteni. Vannak azonban szabványos tervek, amelyeket a hálózati iparág ajánl a rendelkezésre álló és biztonságos hálózatok eléréséhez. Ez a fejezet azokat az alapvető módokat ismerteti, amelyekkel a tűzfalak használhatók hálózati biztonsági architektúra létrehozására.

9.0.2

## Mit fogok tanulni ebben a modulban?

**Modul címe:** Firewall Technologies

**Modul célja** : Magyarázza el, hogyan valósítják meg a tűzfalakat a hálózat biztonsága érdekében.

| **téma címe** | **Téma Cél** |
| --- | --- |
| **Biztonságos hálózatok tűzfalakkal** | Magyarázza el, hogyan használják a tűzfalakat a hálózatok védelmére. |
| **Tűzfalak a hálózattervezésben** | Ismertesse a tűzfaltechnológiák megvalósításának tervezési szempontjait. |

[8.8](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Access Control Lists Summary](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[9.1](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Secure Networks with Firewalls](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                                           
*           
*                       

1. Firewall Technologies
2. Secure Networks with Firewalls

# Biztonságos hálózatok tűzfalakkal

9.1.1

## Tűzfalak

A tűzfal olyan rendszer vagy rendszerek csoportja, amely hozzáférés-szabályozási szabályzatot kényszerít ki a hálózatok között.

Játssza le az ábrán látható animációt a működő tűzfal megtekintéséhez.

Az animáció egy tűzfalat mutat be az internetet képviselő földgömb és egy belső hálózatot képviselő szerver között. A földgömb megpróbál forgalmat továbbítani a belső hálózatra. Megjelennek a forgalom engedélyezésére és tiltására vonatkozó szabályok. A megengedett forgalom bármely külső címről a webszerverre, az FTP-kiszolgálóra, az SMTP-kiszolgálóra és a belső IMAP-kiszolgálóra irányuló forgalom. A letiltott forgalom az összes bejövő forgalom a belsőleg regisztrált IP-címekkel megegyező hálózati címekkel, minden bejövő forgalom a szerver felé külső címekről, minden bejövő ICMP echo kérés forgalom, minden bejövő MS Active Directory lekérdezés, minden bejövő forgalom az MSSQL szerver lekérdezéseihez, és minden M Domain helyi adás.

### Tűzfal működése

**Tiltsa meg** az összes bejövő forgalmat, ha a hálózati címek megegyeznek a belsőleg regisztrált IP-címekkel.

**Minden bejövő forgalom letiltása** a kiszolgáló felé a külső címekről.

**megtagadása .** Minden bejövő ICMP visszhang kérés forgalom

**Az összes bejövő MS Active Directory lekérdezés elutasítása** .

**Engedélyezze** a forgalmat bármely külső címről a webszerverre.

**Forgalom engedélyezése** az FTP-kiszolgálóhoz.

**Forgalom engedélyezése** az SMTP-kiszolgáló felé.

**Forgalom engedélyezése** a belső IMAP-kiszolgáló felé.

**letiltása .** Az MS SQL szerver lekérdezései felé irányuló összes bejövő forgalom

**megtagadása .** Az összes MS Domain helyi adás

Kattintson az egyes gombra, ha többet szeretne megtudni a tűzfalakról.

Minden tűzfalnak van néhány közös tulajdonsága:

* A tűzfalak ellenállnak a hálózati támadásoknak.
* A tűzfalak jelentik az egyetlen áthaladási pontot a belső vállalati hálózatok és a külső hálózatok között, mivel az összes forgalom a tűzfalon keresztül folyik.
* A tűzfalak kényszerítik a hozzáférés-szabályozási szabályzatot.

A tűzfal hálózaton belüli használatának számos előnye van:

* Megakadályozzák, hogy az érzékeny gazdagépek, erőforrások és alkalmazások nem megbízható felhasználók elé kerüljenek.
* Megtisztítják a protokollfolyamatot, ami megakadályozza a protokollhibák kihasználását.
* Blokkolja a rosszindulatú adatokat a szerverekről és az ügyfelekről.
* Csökkentik a biztonságkezelés bonyolultságát azáltal, hogy a hálózati hozzáférés-szabályozás nagy részét a hálózat néhány tűzfalára terhelik.

A tűzfalaknak is vannak korlátai:

* A rosszul konfigurált tűzfal súlyos következményekkel járhat a hálózatra nézve, például egyetlen hibaponttá válhat.
* Számos alkalmazás adatait nem lehet biztonságosan átadni a tűzfalakon.
* A felhasználók proaktív módon kereshetik a tűzfal körüli módokat, hogy blokkolt anyagokat kapjanak, ami potenciális támadásoknak teszi ki a hálózatot.
* A hálózati teljesítmény lelassulhat.
* Az illetéktelen forgalom a tűzfalon keresztül alagútba helyezhető vagy elrejthető legitim forgalomként.

9.1.2

## A tűzfalak típusai

Fontos, hogy ismerjük a különböző típusú tűzfalakat és azok speciális képességeit, hogy minden helyzethez a megfelelő tűzfalat használjuk.

A csomagszűrő tűzfalak általában az útválasztó tűzfalának részét képezik, amely engedélyezi vagy letiltja a forgalmat a 3. és 4. réteg információi alapján. Állapot nélküli tűzfalak, amelyek egy egyszerű házirend-tábla keresést használnak, amely meghatározott feltételek alapján szűri a forgalmat.

Például az SMTP-kiszolgálók alapértelmezés szerint a 25-ös portot figyelik. A rendszergazda beállíthatja a csomagszűrő tűzfalat úgy, hogy blokkolja a 25-ös portot egy adott munkaállomásról, hogy megakadályozza az e-mail vírus terjedését.

A csomagszűrő (állapotmentes) tűzfal ábra az osi modell 7 rétegét mutatja, kiemelve a 3. és 4. réteget. Ebből a két sorból a következő következik: forrás IP-címe, cél IP-címe, protokoll forrásportszáma, célportszáma, szinkronizálás/indítás (SYN) csomagfogadás.

7. réteg 6. réteg 5. réteg 4. réteg 3. réteg 2. réteg 1. réteg Alkalmazás bemutatás Munkamenet Szállítási Hálózati Adatkapcsolat Fizikai

* Forrás IP-cím
* Cél IP-címe
* Jegyzőkönyv
* Forrás port száma
* Cél port száma
* Csomagfogadás szinkronizálása/indítása (SYN).

Az állapotalapú tűzfalak a legsokoldalúbb és a leggyakoribb tűzfaltechnológiák. Az állapotjelző tűzfalak állapotjelző csomagszűrést biztosítanak az állapottáblázatban tárolt kapcsolati információk felhasználásával. Az állapotalapú szűrés egy tűzfalarchitektúra, amely a hálózati rétegbe van besorolva. Ezenkívül elemzi a forgalmat az OSI 4. és 5. rétegében.

Az állapotjelző tűzfal ábra az osi modell 7 rétegét mutatja, kiemelve a 3., 4. és 5. réteget.

7. réteg 6. réteg 5. réteg 4. réteg 3. réteg 2. réteg 1. réteg Alkalmazás bemutatás Munkamenet Szállítási Hálózati Adatkapcsolat Fizikai

Egy alkalmazásátjáró tűzfal (proxy tűzfal), amint az ábrán látható, az OSI referenciamodell 3., 4., 5. és 7. rétegében szűri az információkat. A tűzfalvezérlés és szűrés nagy része szoftveresen történik. Amikor egy ügyfélnek hozzá kell férnie egy távoli kiszolgálóhoz, csatlakozik egy proxykiszolgálóhoz. A proxyszerver az ügyfél nevében csatlakozik a távoli kiszolgálóhoz. Ezért a szerver csak a proxyszervertől érkező kapcsolatot látja.

Az alkalmazásátjáró tűzfal ábrája az osi modell 7 rétegét mutatja, kiemelve a 7. réteget és a 7. és 6. réteget összekötő sávot oldalra az Application gateway firewall szavakkal, valamint a 3., 4. és 5. réteget az Application gateway szavakkal kiemelve. tűzfal.

7. réteg 6. réteg 5. réteg 4. réteg 3. réteg 2. réteg 1. réteg Alkalmazás bemutatása Munkamenet Szállítási Hálózat Adatkapcsolat Fizikai alkalmazásátjáró tűzfal Alkalmazásátjáró tűzfal

A következő generációs tűzfalak (NGFW) túlmutatnak az állapotalapú tűzfalakon azáltal, hogy:

* Integrált behatolás-megelőzés
* Alkalmazástudatosság és -vezérlés a kockázatos alkalmazások megtekintéséhez és blokkolásához
* Frissítési útvonalak a jövőbeni információs feedek bevonásához
* A fejlődő biztonsági fenyegetések kezelésének technikái

A tűzfalak megvalósításának egyéb módjai a következők:

* **Gazda alapú (szerver és személyes) tűzfal** – PC vagy szerver, amelyen tűzfalszoftver fut.
* **Átlátszó tűzfal** – Szűri az IP-forgalmat egy pár áthidalt interfész között.
* **Hibrid tűzfal** – A különböző típusú tűzfalak kombinációja. Például egy alkalmazás-ellenőrző tűzfal egy állapotjelző tűzfalat kombinál egy alkalmazásátjáró tűzfallal.

9.1.3

## Ellenőrizze, hogy megértette-e a tűzfal típusát

Az űrlap teteje

A következő kérdések megválaszolásával ellenőrizze, hogy tisztában van-e a tűzfalak típusaival.

1. Milyen típusú tűzfal szűri az információkat az OSI referenciamodell 3., 4., 5. és 7. rétegében?

Az űrlap alja

Milyen típusú tűzfal a különféle tűzfaltípusok kombinációja?

Milyen típusú tűzfal része az útválasztó tűzfalának, amely a 3. és 4. réteg információi alapján engedélyezi vagy tiltja a forgalmat?

Milyen típusú tűzfal az a számítógép vagy szerver, amelyen tűzfalszoftver fut?

Milyen típusú tűzfal szűri az IP-forgalmat egy pár áthidalt interfész között?

9.1.4

## A csomagszűrő tűzfal előnyei és korlátai

A csomagszűrő tűzfalak általában az útválasztó tűzfalának részét képezik, amely engedélyezi vagy letiltja a forgalmat a 3. és 4. réteg információi alapján. Ezek állapot nélküli tűzfalak, amelyek egy egyszerű házirend-tábla keresést használnak, amely meghatározott feltételek alapján szűri a forgalmat, amint az az ábrán látható. Például az SMTP-kiszolgálók alapértelmezés szerint a 25-ös portot figyelik. A rendszergazda beállíthatja a csomagszűrő tűzfalat úgy, hogy blokkolja a 25-ös portot egy adott munkaállomásról, hogy megakadályozza az e-mail vírus terjesztését.

Az ábra a csomagszűrő tűzfalak által használt feltételeket mutatja.

7. réteg 6. réteg 5. réteg 4. réteg 3. réteg 2. réteg 1. réteg Alkalmazás bemutatás Munkamenet Szállítási Hálózati Adatkapcsolat Fizikai

* Forrás IP-cím
* Cél IP-címe
* Jegyzőkönyv
* Forrás port száma
* Cél port száma
* Csomagfogadás szinkronizálása/indítása (SYN).

A csomagszűrő tűzfal használatának számos előnye van:

* A csomagszűrők egyszerű engedélyezési vagy megtagadási szabálykészleteket valósítanak meg.
* A csomagszűrők csekély hatással vannak a hálózati teljesítményre.
* A csomagszűrőket könnyű megvalósítani, és a legtöbb útválasztó támogatja őket.
* A csomagszűrők kezdeti biztonságot nyújtanak a hálózati rétegben.
* A csomagszűrők a csúcskategóriás tűzfalak szinte minden feladatát sokkal alacsonyabb költséggel látják el.

A csomagszűrők nem jelentenek teljes tűzfalmegoldást, de a tűzfal biztonsági szabályzatának fontos elemei. A csomagszűrő tűzfal használatának számos hátránya van:

* A csomagszűrők érzékenyek az IP-hamisításra. A fenyegetés szereplői tetszőleges csomagokat küldhetnek, amelyek megfelelnek az ACL-feltételeknek, és átmennek a szűrőn.
* A csomagszűrők nem szűrik megbízhatóan a töredezett csomagokat. Mivel a töredezett IP-csomagok az első töredékben a TCP-fejlécet hordozzák, a csomagszűrők pedig a TCP-fejléc-információkat szűrik, az első töredék utáni összes töredék feltétel nélkül átadásra kerül. A csomagszűrők használatára vonatkozó döntések feltételezik, hogy az első töredék szűrője pontosan érvényesíti a házirendet.
* A csomagszűrők összetett ACL-eket használnak, amelyeket nehéz lehet megvalósítani és karbantartani.
* A csomagszűrők nem tudnak dinamikusan szűrni bizonyos szolgáltatásokat. Például a dinamikus portegyeztetést használó munkamenetek nehezen szűrhetők anélkül, hogy hozzáférést nyitnának a portok egész sorához.

A csomagszűrők állapot nélküliek. Minden egyes csomagot külön-külön vizsgálnak meg, nem pedig a kapcsolat állapotának összefüggésében.

9.1.5

## Az állapotalapú tűzfal előnyei és korlátai

Számos előnye van az állapotalapú tűzfalnak a hálózatban:

* Az állapotjelző tűzfalakat gyakran elsődleges védelmi eszközként használják a nem kívánt, szükségtelen vagy nemkívánatos forgalom kiszűrésével.
* Az állapotalapú tűzfalak erősítik a csomagszűrést azáltal, hogy szigorúbb ellenőrzést biztosítanak a biztonság felett.
* Az állapotjelző tűzfalak javítják a teljesítményt a csomagszűrőkkel vagy proxyszerverekkel szemben.
* Az állapotjelző tűzfalak úgy védekeznek a hamisítás és a DoS támadások ellen, hogy meghatározzák, hogy a csomagok egy meglévő kapcsolathoz tartoznak-e, vagy jogosulatlan forrásból származnak.
* Az állapotalapú tűzfalak több naplóinformációt biztosítanak, mint a csomagszűrő tűzfalak.

Az állapotalapú tűzfalak bizonyos korlátozásokat is tartalmaznak:

* Az állapotjelző tűzfalak nem tudják megakadályozni az alkalmazási réteg támadásait, mert nem vizsgálják a HTTP-kapcsolat tényleges tartalmát.
* Nem minden protokoll állapotalapú. Például az UDP és az ICMP nem generál kapcsolati információkat egy állapottáblázathoz, és ezért nem gyűjtenek annyi támogatást a szűréshez.
* Nehéz nyomon követni a dinamikus portegyeztetést használó kapcsolatokat. Egyes alkalmazások több kapcsolatot nyitnak meg. Ehhez egy teljesen új portra van szükség, amelyeket meg kell nyitni a második csatlakozás engedélyezéséhez.
* Az állapotalapú tűzfalak nem támogatják a felhasználói hitelesítést.

| **Előnyök** | **Korlátozások** |
| --- | --- |
| A védekezés elsődleges eszköze | Nincs alkalmazási réteg ellenőrzése |
| Erős csomagszűrés | Az állapot nélküli protokollok korlátozott nyomon követése |
| Jobb teljesítmény a csomagszűrőkhöz képest | Nehéz védekezni a dinamikus portegyeztetés ellen |
| Véd a hamisítás és a DoS támadások ellen | Nincs hitelesítési támogatás |
| Gazdagabb adatnapló |  |

[9.0](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[9.2](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Firewalls in Network Design](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                                             
*           
*                       

1. Firewall Technologies
2. Firewalls in Network Design

# Tűzfalak a hálózattervezésben

9.2.1

## Közös biztonsági architektúrák

A tűzfal tervezése elsősorban az eszközinterfészekről szól, amelyek a forrás, a cél és a forgalom típusa alapján engedélyezik vagy tiltják a forgalmat. Egyes tervek olyan egyszerűek, mint egy külső hálózat és egy belső hálózat kijelölése, amelyeket a tűzfalon lévő két interfész határoz meg.

Íme három általános tűzfalterv.

Amint az ábrán látható, a nyilvános hálózat (vagy külső hálózat) nem megbízható, a magánhálózat (vagy belső hálózat) pedig megbízható.

A két interfésszel rendelkező tűzfal általában a következőképpen van konfigurálva:

* A magánhálózatból származó forgalom engedélyezett és ellenőrzött, amikor az a nyilvános hálózat felé halad. A nyilvános hálózatról visszatérő és a magánhálózatból származó forgalomhoz kapcsolódó ellenőrzött forgalom megengedett.
* A nyilvános hálózatról kiinduló és a magánhálózatra irányuló forgalom általában le van tiltva.

A privát és nyilvános figura egy felhőt mutat egy nyilvános (nem megbízható) címkével ellátott körben. A felhő az s 0 / 0 / 0-n keresztül csatlakozik a tűzfalhoz. A g 0 / 0 tűzfalport egy bekarikázott v lan 1 privát (megbízható) címkével csatlakozik, amelyen egy szerver és két számítógép található. Van egy nyíl a privát körből a nyilvános körbe, amelyen http, smtp és dns található. Van egy másik nyíl, amely a nyilvános körből a privát körbe megy, a hozzáférés nélkül.

G0/0

S0/0/0

VLAN 1 Nincs hozzáférés HTTP   
SMTP   
DNS privát   
(megbízható) Nyilvános   
(nem megbízható)

A demilitarizált zóna (DMZ) egy olyan tűzfal kialakítás, ahol jellemzően egy belső interfész csatlakozik a magánhálózathoz, egy külső interfész a nyilvános hálózathoz, és egy DMZ interfész, amint az az ábrán látható.

* A magánhálózatból származó forgalmat a nyilvános vagy DMZ hálózat felé haladva ellenőrzik. Ez a forgalom csekély korlátozással vagy korlátozás nélkül engedélyezett. A DMZ-ből vagy a nyilvános hálózatból a magánhálózatba visszatérő ellenőrzött forgalom megengedett.
* A DMZ hálózatból kiinduló és a magánhálózatra irányuló forgalom általában le van tiltva.
* A DMZ hálózatból kiinduló és a nyilvános hálózatra közlekedő forgalom a szolgáltatási igények alapján szelektíven engedélyezett.
* A nyilvános hálózatról induló és a DMZ felé haladó forgalom szelektíven engedélyezett és ellenőrzött. Ez a fajta forgalom jellemzően e-mail, DNS, HTTP vagy HTTPS forgalom. A DMZ-ről a nyilvános hálózatra irányuló visszatérő forgalom dinamikusan engedélyezett.
* A nyilvános hálózatból kiinduló és a magánhálózatra irányuló forgalom blokkolva van.

A zónaalapú házirend-tűzfalak (ZPF-ek) a zónák fogalmát használják további rugalmasság biztosítása érdekében. A zóna egy vagy több interfész csoportja, amelyek hasonló funkciókkal vagy szolgáltatásokkal rendelkeznek. A zónák segítenek meghatározni, hogy hol kell alkalmazni a Cisco IOS tűzfalszabályt vagy házirendet. Az ábrán a LAN 1 és LAN 2 biztonsági házirendjei hasonlóak, és a tűzfalkonfigurációkhoz egy zónába csoportosíthatók. Alapértelmezés szerint az ugyanabban a zónában lévő interfészek közötti forgalomra nem vonatkozik semmilyen szabályzat, és szabadon halad. Azonban minden zóna-zóna forgalom blokkolva van. A zónák közötti forgalom engedélyezéséhez a forgalmat engedélyező vagy ellenőrző szabályzatot kell konfigurálni.

Az egyetlen kivétel ez alól az alapértelmezett **tiltás alól** az útválasztó saját zónája. A self zóna maga az útválasztó, és tartalmazza az összes útválasztó interfész IP-címét. A saját zónát tartalmazó házirend-konfigurációk az útválasztónak szánt és onnan származó forgalomra vonatkoznak. Alapértelmezés szerint az ilyen típusú forgalomra nincs szabályzat. A saját zóna házirendjének megtervezésekor figyelembe veendő forgalom magában foglalja a felügyeleti sík és a vezérlősík forgalmat, például az SSH-t, az SNMP-t és az útválasztási protokollokat.

9.2.2

## Réteges védelem

A réteges védelem különböző típusú tűzfalakat használ, amelyek rétegekben kombinálva mélyítik a szervezet biztonságát. A házirendek érvényesíthetők a rétegek között és a rétegeken belül. Ezek az irányelvek érvényesítési pontjai határozzák meg, hogy a forgalom továbbításra vagy elvetésre kerül-e. Például a nem megbízható hálózatról érkező forgalom először találkozik egy csomagszűrővel a szélső útválasztón. Ha a házirend lehetővé teszi, a forgalom az átvizsgált tűzfalra vagy bástya hosztrendszerre megy, amely több szabályt alkalmaz a forgalomra, és elveti a gyanús csomagokat. A bástya gazdagép egy keményített számítógép, amely jellemzően a DMZ-ben található. Ezután a forgalom egy belső szűrőútválasztóra megy. A forgalom csak azután kerül át a belső célállomásra, hogy sikeresen áthaladt a külső útválasztó és a belső hálózat közötti összes házirend-érvényesítési ponton. Az ilyen típusú DMZ-beállítást átvilágított alhálózati konfigurációnak nevezik.

A többrétegű védelmi megközelítés nem minden, ami a biztonságos belső hálózat biztosításához szükséges. A hálózati rendszergazdának számos tényezőt figyelembe kell vennie a teljes, mélyreható védelem felépítése során:

* A tűzfalak általában nem akadályozzák meg a hálózaton vagy zónán belüli gazdagépektől érkező behatolásokat.
* A tűzfalak nem védenek a csaló hozzáférési pontok telepítése ellen.
* A tűzfalak nem helyettesítik a támadásból vagy hardverhibából eredő biztonsági mentési és katasztrófa-helyreállítási mechanizmusokat.
* A tűzfalak nem helyettesítik a tájékozott rendszergazdákat és felhasználókat.

Az ábrán négy kör látható, egyik a másikban belülről 1-től 4-ig, a középső kör pedig Network Core felirattal.

### A réteges hálózati védelem szempontjai

1 2 4

3

Hálózati mag

1. **Hálózati alapbiztonság** – Védelmet nyújt a rosszindulatú szoftverek és a forgalmi rendellenességek ellen, kikényszeríti a hálózati házirendeket, és biztosítja a túlélést
2. **Kerületi biztonság** – Biztosítja a zónák közötti határokat
3. **Kommunikációs biztonság** – Információbiztonságot nyújt
4. **Végponti biztonság** – Az identitás és az eszköz biztonsági szabályzatának megfelelőséget biztosít

A bevált gyakorlatok ezen részleges listája kiindulópontként szolgálhat a tűzfal biztonsági szabályzatához.

* Helyezze el a tűzfalakat a biztonsági határokon. A tűzfalak a hálózati biztonság kritikus részét képezik, de nem bölcs dolog kizárólag tűzfalra hagyatkozni a biztonság érdekében.
* Alapértelmezés szerint minden forgalom letiltása.
* Csak a szükséges szolgáltatásokat engedélyezze.
* Győződjön meg arról, hogy a tűzfalhoz való fizikai hozzáférést ellenőrizni kell.
* Rendszeresen figyelje a tűzfalnaplókat.
* Gyakorolja a változáskezelést a tűzfal konfigurációs módosításaihoz.
* Ne feledje, hogy a tűzfalak elsősorban a kívülről érkező technikai támadások ellen védenek.

9.2.3

## Ellenőrizze, hogy megértette – Hálózatbiztonsági tervezési koncepciók

Az űrlap teteje

A következő kérdések megválaszolásával ellenőrizze, hogy megértette-e a tűzfalakat a hálózattervezésben.

1. Melyik hálózati biztonsági terv használ általában egy belső, egy külső és egy DMZ interfészt?

Az űrlap alja

Melyik biztonsági terv használ különböző típusú tűzfalakat és biztonsági intézkedéseket, amelyeket a hálózat különböző területein kombinálnak a szervezet biztonságának növelése érdekében?

Melyik három állítás írja le a hálózat megbízható és nem megbízható területeit? (Válassz hármat.)

Melyik hálózattervezés csoportosítja az interfészeket hasonló funkciókkal vagy jellemzőkkel rendelkező zónákra?

Mi a két bevált módszer a tűzfal biztonsági szabályzatának megvalósítása során?

9.2.4

## Packet Tracer – Csomagfolyamat azonosítása

Ebben a Packet Tracer tevékenységben LAN és WAN topológiában figyelheti meg a csomagfolyamot. Megfigyelheti azt is, hogyan változhat a csomagfolyam útja, ha megváltozik a hálózati topológia.

[Azonosítsa a csomagfolyamot](https://contenthub.netacad.com/courses/netsec/_common/9.2.4-packet-tracer---identify-packet-flow.pka)

[9.1](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Secure Networks with Firewalls](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[9.3](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Firewall Technologies Summary](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                                                        
*                       

1. Firewall Technologies
2. Firewall Technologies Summary

# Tűzfaltechnológiák összefoglalója

9.3.1

## Mit tanultam ebben a modulban?

**Biztonságos hálózatok tűzfalakkal**   
Számos különböző típusú tűzfal létezik. A csomagszűrő (állapot nélküli) tűzfalak 3-as és néha 4-es rétegű szűrést biztosítanak. Az állapotjelző tűzfal engedélyezi vagy blokkolja a forgalmat állapot, port és protokoll alapján. Az alkalmazásátjáró tűzfalai (proxy tűzfalak) a 3., 4., 5. és 7. rétegben szűrik az információkat. A következő generációs tűzfalak az alkalmazásátjárókon túl további szolgáltatásokat is nyújtanak, mint például az integrált behatolásmegelőzés, az alkalmazásfigyelés és -vezérlés a kockázatos alkalmazások megtekintéséhez és blokkolásához, valamint hozzáférést biztosít a jövőbeli alkalmazásokhoz. információs feedek és technikák a fejlődő biztonsági fenyegetések kezelésére.

**Tűzfalak a hálózati tervezésben**   
Az általános biztonsági architektúrák határozzák meg a hálózatba belépő és onnan kilépő forgalom határait. Ha olyan topológiát vizsgál, amely hozzáfér külső vagy nyilvános hálózatokhoz, meg kell tudnia határozni a biztonsági architektúrát. Egyes tervek olyan egyszerűek, mint egy külső hálózat és egy belső hálózat kijelölése, amelyeket a tűzfalon lévő két interfész határoz meg. A szolgáltatásokhoz nyilvános hozzáférést igénylő hálózatok gyakran tartalmaznak egy DMZ-t, amelyhez a nyilvánosság hozzáférhet, miközben szigorúan blokkolja a hozzáférést a belső hálózathoz. A ZPF-ek a zónák fogalmát használják a további rugalmasság biztosítására. A zóna egy vagy több interfész csoportja, amelyek hasonló funkciókkal, szolgáltatásokkal és biztonsági követelményekkel rendelkeznek. A réteges biztonsági megközelítés tűzfalakat és egyéb biztonsági intézkedéseket használ a hálózat különböző funkcionális rétegeinek biztonsága érdekében.

9.3.2

## 9. modul – Tűzfaltechnológiák kvíz

Az űrlap teteje

1. generációs tűzfal használatának Mi az előnye a következő az állapotalapú tűzfal helyett?

Az űrlap alja

Az OSI-modell melyik három rétege tartalmaz olyan információkat, amelyeket általában egy állapotalapú tűzfal vizsgál? (Válassz hármat.)

Melyik állítás jellemző a csomagszűrő tűzfalra?

Melyik típusú tűzfalat támogatja a legtöbb útválasztó, és melyik a legkönnyebben megvalósítható?

Milyen típusú forgalmat szoktak blokkolni a demilitarizált zóna megvalósítása során?

Mi az alkalmazásátjáró tűzfal két jellemzője? (Válassz kettőt.)

Milyen típusú tűzfal van általában csekély hatással a hálózati teljesítményre?

Melyik típusú tűzfal része általában az útválasztó tűzfalának, és engedélyezi vagy blokkolja a forgalmat a 3. vagy 4. réteg információi alapján?

Hogyan kezeli a tűzfal a DMZ hálózatból származó és magánhálózatra továbbító forgalmat?

Melyik két protokoll állapotmentes, és nem állítja elő az állapottábla felépítéséhez szükséges kapcsolati információkat? (Válassz kettőt.)

Milyen két előnye van a tűzfalnak a hálózatban való megvalósításának? (Válassz kettőt.)

A ZPF implementálásakor melyik utasítás ír le egy zónát?

[9.2](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Firewalls in Network Design](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[10.0](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                                                        
*                       

1. Firewall Technologies
2. Firewall Technologies Summary

# Tűzfaltechnológiák összefoglalója

9.3.1

## Mit tanultam ebben a modulban?

**Biztonságos hálózatok tűzfalakkal**   
Számos különböző típusú tűzfal létezik. A csomagszűrő (állapot nélküli) tűzfalak 3-as és néha 4-es rétegű szűrést biztosítanak. Az állapotjelző tűzfal engedélyezi vagy blokkolja a forgalmat állapot, port és protokoll alapján. Az alkalmazásátjáró tűzfalai (proxy tűzfalak) a 3., 4., 5. és 7. rétegben szűrik az információkat. A következő generációs tűzfalak az alkalmazásátjárókon túl további szolgáltatásokat is nyújtanak, mint például az integrált behatolásmegelőzés, az alkalmazásfigyelés és -vezérlés a kockázatos alkalmazások megtekintéséhez és blokkolásához, valamint hozzáférést biztosít a jövőbeli alkalmazásokhoz. információs feedek és technikák a fejlődő biztonsági fenyegetések kezelésére.

**Tűzfalak a hálózati tervezésben**   
Az általános biztonsági architektúrák határozzák meg a hálózatba belépő és onnan kilépő forgalom határait. Ha olyan topológiát vizsgál, amely hozzáfér külső vagy nyilvános hálózatokhoz, meg kell tudnia határozni a biztonsági architektúrát. Egyes tervek olyan egyszerűek, mint egy külső hálózat és egy belső hálózat kijelölése, amelyeket a tűzfalon lévő két interfész határoz meg. A szolgáltatásokhoz nyilvános hozzáférést igénylő hálózatok gyakran tartalmaznak egy DMZ-t, amelyhez a nyilvánosság hozzáférhet, miközben szigorúan blokkolja a hozzáférést a belső hálózathoz. A ZPF-ek a zónák fogalmát használják a további rugalmasság biztosítására. A zóna egy vagy több interfész csoportja, amelyek hasonló funkciókkal, szolgáltatásokkal és biztonsági követelményekkel rendelkeznek. A réteges biztonsági megközelítés tűzfalakat és egyéb biztonsági intézkedéseket használ a hálózat különböző funkcionális rétegeinek biztonsága érdekében.

9.3.2

## 9. modul – Tűzfaltechnológiák kvíz

Az űrlap teteje

1. generációs tűzfal használatának Mi az előnye a következő az állapotalapú tűzfal helyett?

Az űrlap alja

Az OSI-modell melyik három rétege tartalmaz olyan információkat, amelyeket általában egy állapotalapú tűzfal vizsgál? (Válassz hármat.)

Melyik állítás jellemző a csomagszűrő tűzfalra?

Melyik típusú tűzfalat támogatja a legtöbb útválasztó, és melyik a legkönnyebben megvalósítható?

Milyen típusú forgalmat szoktak blokkolni a demilitarizált zóna megvalósítása során?

Mi az alkalmazásátjáró tűzfal két jellemzője? (Válassz kettőt.)

Milyen típusú tűzfal van általában csekély hatással a hálózati teljesítményre?

Melyik típusú tűzfal része általában az útválasztó tűzfalának, és engedélyezi vagy blokkolja a forgalmat a 3. vagy 4. réteg információi alapján?

Hogyan kezeli a tűzfal a DMZ hálózatból származó és magánhálózatra továbbító forgalmat?

Melyik két protokoll állapotmentes, és nem állítja elő az állapottábla felépítéséhez szükséges kapcsolati információkat? (Válassz kettőt.)

Milyen két előnye van a tűzfalnak a hálózatban való megvalósításának? (Válassz kettőt.)

A ZPF implementálásakor melyik utasítás ír le egy zónát?

[9.2](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Firewalls in Network Design](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[10.0](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                                                        
*                       

1. Zone-Based Policy Firewalls
2. Introduction

# Bevezetés

10.0.1

## Miért vegyem ezt a modult?

A zónaalapú házirend-tűzfalak (ZPF-ek) egy evolúciós lépést jelentenek a klasszikus tűzfalakon túl. Míg a klasszikus tűzfal alapú biztonsági konfiguráció az útválasztó interfészeken, a ZPF lehetővé teszi az interfészek zónákhoz való hozzárendelését. A biztonsági házirendek meghatározása a zóna és a zónák közötti biztonsági kapcsolatok alapján történik. Több interfész is tehető egy zóna tagjává, és ezekre a csatolókra zónaszabályok vonatkoznak. A biztonsági követelményeket a zónák jellege határozhatja meg, nem pedig az adott interfészen keresztül kommunikáló IP-hálózatok.

Ebben a modulban megismerheti a ZPF-eket, és megtanulhatja, hogyan valósítson meg egy alapvető ZPF-tervet.

10.0.2

## Mit fogok tanulni ebben a modulban?

**Modul címe:** Zóna alapú házirend tűzfalak

**Modul célja** : Zóna alapú házirend tűzfal megvalósítása CLI használatával.

| **téma címe** | **Téma Cél** |
| --- | --- |
| **A ZPF áttekintése** | Magyarázza el, hogyan használhatók a zónaalapú házirend-tűzfalak a hálózat védelmére. |
| **ZPF működés** | Magyarázza el a zóna alapú házirend tűzfal működését. |
| **Konfiguráljon ZPF-et** | Konfiguráljon zónaalapú házirend-tűzfalat CLI-vel. |

[9.3](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Firewall Technologies Summary](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[10.1](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[ZPF Overview](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                                                        
*                       

1. Zone-Based Policy Firewalls
2. ZPF Overview

# A ZPF áttekintése

10.1.1

## A ZPF előnyei

A Cisco IOS Firewallhoz két konfigurációs modell létezik:

* **Klasszikus tűzfal** – A hagyományos konfigurációs modell, amelyben tűzfalszabályzat kerül alkalmazásra az interfészeken.
* **Zóna alapú házirend tűzfal (ZPF)** – Az a konfigurációs modell, amelyben az interfészek a biztonsági zónákhoz vannak rendelve, és a tűzfal házirendje a zónák közötti forgalomra vonatkozik.

Ha a privát zónához egy további interfészt adnak hozzá, a privát zónában az új interfészhez csatlakoztatott gazdagépek továbbíthatják a forgalmat az ugyanabban a zónában lévő meglévő interfész összes gépéhez. Az ábrán egy egyszerű háromzónás hálózat látható.

Az ábra egy alapvető biztonsági zóna topológiát mutat, amely magában foglal egy privát zónát, egy nyilvános zónát és a DMZ zónát.

### Alapvető biztonsági zóna topológia

DMZ Zone Privát zóna Nyilvános zóna Internet

A hálózatbiztonsági szakemberek elsődleges motivációja a ZPF-modellre való átálláshoz a szerkezet és a könnyű használhatóság. A strukturált megközelítés hasznos a dokumentációban és a kommunikációban. A könnyű használhatóság a hálózatbiztonsági megvalósításokat hozzáférhetőbbé teszi a biztonsági szakemberek nagyobb közössége számára.

A ZPF-nek számos előnye van:

* Nem függ az ACL-ektől.
* Az útválasztó biztonsági helyzete blokkolja, hacsak nincs kifejezetten engedélyezve.
* A Cisco Common Classification Policy Language (C3PL) nyelvével a házirendek könnyen olvashatók és hibaelhárítási lehetőségeket kínálnak. A C3PL egy strukturált módszer az eseményeken, feltételeken és műveleteken alapuló forgalmi szabályzatok létrehozására. Ez méretezhetőséget biztosít, mivel egy házirend minden adott forgalmat érint, ahelyett, hogy több ACL-re és ellenőrzési műveletekre lenne szükség a különböző típusú forgalomhoz.
* A virtuális és fizikai interfészek zónákba csoportosíthatók.
* A házirendek a zónák közötti egyirányú forgalomra vonatkoznak.

Amikor eldönti, hogy az IOS klasszikus tűzfalát vagy a ZPF-et kívánja-e megvalósítani, fontos megjegyezni, hogy mindkét konfigurációs modell egyszerre engedélyezhető egy útválasztón. A modellek azonban nem kombinálhatók egyetlen felületen. Például egy interfész nem konfigurálható egyszerre biztonsági zónatagként és IP-ellenőrzés céljából.

10.1.2

## ZPF tervezés

A ZPF-ek tervezése több lépésből áll:

**1. lépés** . **A zónák meghatározása** – Az adminisztrátor a hálózat zónákra való szétválasztására összpontosít. A zónák határozzák meg a hálózat biztonsági határait. A zóna határvonalat határoz meg, ahol a forgalom szabályzati korlátozások alá esik, amikor átlép a hálózat másik régiójába. Például a nyilvános hálózat egy zóna, a belső hálózat pedig egy másik zóna.

**2. lépés** . **Szabályzatok létrehozása zónák között** – Minden egyes "forrás-cél" zónapárhoz (például a belső hálózattól a külső internetig) határozza meg azokat a munkameneteket, amelyeket a forrászónák kliensei kérhetnek a célzónákban lévő szerverektől. Ezek a munkamenetek leggyakrabban TCP és UDP munkamenetek, de lehetnek ICMP szekciók is, például ICMP echo. Az olyan forgalom esetében, amely nem a munkamenetek koncepcióján alapul, az adminisztrátornak meg kell határoznia az egyirányú forgalom áramlását a forrás és a cél között, és fordítva. A házirendek egyirányúak, és a forrás- és célzónákon alapulnak, amelyeket zónapároknak nevezünk.

**3. lépés** . **A fizikai infrastruktúra tervezése** - A zónák azonosítása és a köztük lévő forgalmi igények dokumentálása után az adminisztrátornak meg kell terveznie a fizikai infrastruktúrát. Az adminisztrátornak figyelembe kell vennie a biztonsági és rendelkezésre állási követelményeket a fizikai infrastruktúra kialakításakor. Ez magában foglalja az eszközök számának diktálását a legbiztonságosabb és legkevésbé biztonságos zónák között, valamint a redundáns eszközök meghatározását.

**4. lépés** . **Azonosítsa a zónákon belüli részhalmazokat és egyesítse a forgalmi követelményeket** – A terv minden egyes tűzfaleszközénél a rendszergazdának azonosítania kell azokat a zóna részhalmazokat, amelyek az interfészeihez csatlakoznak, és össze kell vonnia az adott zónák forgalmi követelményeit. Például több zóna is kapcsolódhat közvetve egy tűzfal egyetlen interfészéhez. Ez eszközspecifikus interzone házirendet eredményezne. Bár fontos szempont, a zóna részhalmazok megvalósítása túlmutat ennek a tantervnek a keretein.

Kattintson az egyes gombra a ZPF tervek példáinak megtekintéséhez.

Az ábrán egy LAN-internet ZPF kialakítás látható. A tűzfal elválasztja a belső hálózatot a külső hálózattól.

Internet belül kívül

[10.0](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[10.2](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[ZPF Operation](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                                                          
*                       

1. Zone-Based Policy Firewalls
2. ZPF Operation

# ZPF működés

10.2.1

## ZPF-műveletek

A házirendek azonosítják azokat a műveleteket, amelyeket a ZPF hajt végre a hálózati forgalomnál. Három lehetséges művelet konfigurálható a forgalom feldolgozására protokoll, forrás- és célzónák (zónapárok) és egyéb feltételek szerint.

* **Ellenőrzés** – Cisco IOS állapotjelző csomagellenőrzést hajt végre.
* **Drop** – Ez analóg **az ACL-ben szereplő deny** utasítással. egy **naplózási lehetőség áll rendelkezésre.** Az elutasított csomagok naplózására
* **Megfelel** – Ez analóg **az ACL-ben található engedélyezési** nyilatkozattal. Az átadási művelet nem követi nyomon a kapcsolatok vagy a munkamenetek állapotát a forgalomban.

10.2.2

## Tranzitforgalom szabályai

Az útválasztó interfészein áthaladó forgalom több, az interfész viselkedését szabályozó szabály hatálya alá tartozik. A tranzitforgalmi példához tekintse meg az ábrán látható topológiát.

Az ábra egy alapvető biztonsági zóna topológiát mutat, ahol a tűzfalhoz vezető három kapcsolat mindegyike a nyilvános zónához (internethez), a privát zónához és a DMZ zónához kapcsolódik.

### Alapvető biztonsági zóna topológia

DMZ Zone Private Zone Internet Public Zone

A szabályok attól függnek, hogy a be- és kilépési felületek ugyanannak a zónának a tagjai-e vagy sem:

* Ha egyik interfész sem zónatag, akkor az eredmény a forgalom átengedése.
* Ha mindkét interfész ugyanannak a zónának a tagja, akkor az eredmény a forgalom átengedése.
* Ha az egyik interfész zónatag, de a másik nem, akkor az eredmény a forgalom leállítása, függetlenül attól, hogy létezik-e zónapár.
* Ha mindkét interfész ugyanahhoz a zónapárhoz tartozik, és létezik házirend, akkor az eredményül kapott művelet a házirend által meghatározott ellenőrzés, engedélyezés vagy eldobás.

A táblázat összefoglalja ezeket a szabályokat.

| **Forrás interfész Zóna tagja?** | **A cél interfész zóna tagja?** | **Létezik zóna-pár?** | **Létezik politika?** | **Eredmény** |
| --- | --- | --- | --- | --- |
| NEM | NEM | N/A | N/A | PASS |
| IGEN | NEM | N/A | N/A | CSEPP |
| NEM | IGEN | N/A | N/A | CSEPP |
| IGEN (privát) | IGEN (privát) | N/A | N/A | PASS |
| IGEN (privát) | IGEN (nyilvános) | NEM | N/A | CSEPP |
| IGEN (privát) | IGEN (nyilvános) | IGEN | NEM | PASS |
| IGEN (privát) | IGEN (nyilvános) | IGEN | IGEN | ELLENŐRIZZE |

10.2.3

## Az önzónába történő közlekedés szabályai

Az önzóna maga az útválasztó, és tartalmazza az útválasztó interfészeihez rendelt összes IP-címet. Ez a forgalom, amely az útválasztótól származik, vagy egy útválasztó interfészére irányul. Pontosabban, a forgalom eszközkezelésre, például SSH-ra, vagy forgalomtovábbítási vezérlésre, például útválasztási protokoll forgalomra vonatkozik. A ZPF-re vonatkozó szabályok eltérőek a saját zónára vonatkozóan. A saját zóna forgalmi példájához lásd az előző ábrán látható topológiát.

A szabályok attól függenek, hogy az útválasztó a forgalom forrása vagy célállomása, ahogy az a táblázatban is látható. Ha az útválasztó a forrás vagy a cél, akkor minden forgalom engedélyezett. Az egyetlen kivétel az, ha a forrás és a cél egy adott szolgáltatási szabályzattal rendelkező zónapár. Ebben az esetben a házirend az összes forgalomra vonatkozik.

| **Forrás interfész Zóna tagja?** | **A cél interfész zóna tagja?** | **Létezik zóna-pár?** | **Létezik politika?** | **Eredmény** |
| --- | --- | --- | --- | --- |
| IGEN (saját zóna) | IGEN | NEM | N/A | PASS |
| IGEN (saját zóna) | IGEN | IGEN | NEM | PASS |
| IGEN (saját zóna) | IGEN | IGEN | IGEN | ELLENŐRIZZE |
| IGEN | IGEN (saját zóna) | NEM | N/A | PASS |
| IGEN | IGEN (saját zóna) | IGEN | NEM | PASS |
| IGEN | IGEN (saját zóna) | IGEN | IGEN | ELLENŐRIZZE |

10.2.4

## Ellenőrizze, hogy megértette – Tranzitforgalom szabályai

Az 1. ábra egy interaktív tevékenység, amely a tranzitforgalom szabályait azonosítja. A 2. ábra egy interaktív tevékenység, amely az önzóna forgalom szabályait azonosítja.

### Tevékenység 1. rész – Tranzitforgalom szabályai

Határozza meg a tranzitforgalomra vonatkozó helyes szabályokat a válaszok kiválasztásával a 7 legördülő menüből.

Forrás interfész Zóna tagja?

NEM

IGEN

IGEN (privát)

NEM

A cél interfész zóna tagja?

IGEN (privát)

IGEN (privát)

IGEN (privát)

NEM

NEM

IGEN (privát)

IGEN

IGEN (nyilvános)

IGEN (nyilvános)

IGEN (nyilvános)

Létezik zóna-pár?

N/A

N/A

N/A

N/A

IGEN

Létezik politika?

N/A

N/A

N/A

N/A

N/A

IGEN

Eredmény

CSEPP

CSEPP

ELLENŐRIZZE

Az 1. ábra egy interaktív tevékenység, amely a tranzitforgalom szabályait azonosítja. A 2. ábra egy interaktív tevékenység, amely az önzóna forgalom szabályait azonosítja.

### Tevékenység 2. rész – Saját zóna forgalom szabályai

Határozza meg a saját zóna forgalmára vonatkozó helyes szabályokat a válaszok kiválasztásával a 6 legördülő menüből.

Forrás interfész Zóna tagja?

IGEN (önzóna)

IGEN (önzóna)

IGEN

IGEN (önzóna)

A cél interfész zóna tagja?

IGEN

IGEN

IGEN

IGEN

IGEN (önzóna)

IGEN

IGEN (önzóna)

IGEN (önzóna)

Létezik zóna-pár?

NEM

IGEN

NEM

IGEN

Létezik politika?

PASS

NEM

N/A

NEM

IGEN

Eredmény

PASS

ELLENŐRIZZE

PASS

[10.1](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[ZPF Overview](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[10.3](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Configure a ZPF](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                                                                    
*                       

1. Zóna alapú házirend tűzfalak
2. Konfiguráljon ZPF-et

# Konfiguráljon ZPF-et

10.3.1

## Konfiguráljon ZPF-et

A témakör hátralévő részében az ábrán látható topológiát használjuk a ZPF konfiguráció bemutatására. A lépések sorrendje nem kötelező. Néhány konfigurációt azonban végre kell hajtani. Például be kell állítania egy osztálytérképet, mielőtt osztálytérképet rendelne egy szabályzattérképhez. Hasonlóképpen, addig nem rendelhet házirend-leképezést egy zónapárhoz, amíg nem konfigurálta a házirendet. Ha olyan szakaszt próbál konfigurálni, amely a konfiguráció egy másik, még nem konfigurált részére támaszkodik, az útválasztó hibaüzenettel válaszol.

Az ábra egy zóna alapú házirend tűzfal topológiát mutat be, ahol a tűzfal választ el egy privát zónát a nyilvános zónától (internettől). A HTTP-forgalom megengedett a privát zónából a nyilvános zónába. A HTTP visszatérési forgalom megengedett a nyilvános zónából a privát zónába. Minden más forgalom meg van tiltva.

### Zóna alapú házirend tűzfal konfigurációs lépések

R1 G0/0

S0/0/0

**Privát zóna** HTTP HTTP visszatérő forgalom Bármilyen más forgalom Internet **nyilvános zóna**

1. lépés: Hozza létre a zónákat.   
2. lépés: A forgalom azonosítása osztálytérkép segítségével.   
3. lépés: Határozzon meg egy műveletet egy irányelvtérkép segítségével.   
4. lépés: Határozzon meg egy zónapárt, és illessze azt egy szabályzattérképhez.   
5. lépés: Rendeljen zónákat a megfelelő interfészekhez.

10.3.2

## 1. lépés: Hozza létre a zónákat

Az első lépés a zónák létrehozása. A zónák létrehozása előtt azonban válaszoljon néhány kérdésre:

* Milyen interfészeket kell beépíteni a zónákba?
* Mi lesz az egyes zónák neve?
* Milyen forgalom szükséges a zónák között és melyik irányba?

A példa topológiában két interfész, két zóna és egy irányban áramló forgalom van. A nyilvános zónából származó forgalom nem engedélyezett. Hozza létre a tűzfal privát és nyilvános zónáit a zónabiztonsági paranccsal, az itt látható módon.

Router(config)# **zone security** zone-name

R1(config)# **zone security PRIVATE**

R1(config-sec-zone)# **exit**

R1(config)# **zone security PUBLIC**

R1(config-sec-zone)# **exit**

R1(config)#

10.3.3

## 2. lépés: A forgalom azonosítása

A második lépés az osztálytérkép használata annak a forgalomnak a meghatározására, amelyre a házirendet alkalmazni fogja. Az osztály a csomagok halmazának azonosításának módja annak tartalma alapján, „egyezési” feltételekkel. Általában úgy határoz meg egy osztályt, hogy olyan műveletet alkalmazhasson az azonosított forgalomra, amely egy szabályzatot tükröz. Egy osztályt osztálytérképekkel határozunk meg.

parancs szintaxisát mutatja be **Az alábbi példa a class-map** . Többféle osztálytérkép létezik. ZPF konfiguráció esetén használja az **inspect** kulcsszót az osztálytérkép meghatározásához. Határozza meg, hogyan kell kiértékelni a csomagokat, ha több egyezési feltétel is létezik. A csomagoknak meg kell felelniük az egyezési feltételnek ( **match-any** ) vagy az összes egyezési feltételnek ( **match-all** ), hogy az osztály tagjának tekintsék.

Router(config)# **class-map type inspect** [**match-any** | **match-all**] class-map-name

| **Paraméter** | **Leírás** |
| --- | --- |
| **match-any** | A csomagoknak meg kell felelniük az illesztési feltételek egyikének, hogy az osztály tagjának tekintsék. |
| **egyezés minden** | A csomagoknak meg kell felelniük az összes egyezési feltételnek, hogy az osztály tagjának minősüljenek. |
| osztály-térkép-név | Annak az osztálytérképnek a neve, amelyet az osztály házirendjének konfigurálásához használunk a házirend-térképen. |

Az alábbi példa az egyezési utasítások szintaxisát mutatja be **osztálytérkép** alkonfigurációs módban. Illessze a forgalmat egy ACL-hez, egy adott protokollhoz vagy akár egy másik osztálytérképhez.

Router(config-cmap)# **match access-group** {acl-# | acl-name }

Router(config-cmap)# **match protocol** protocol-name

Router(config-cmap)# **match class-map** class-map-name

| **Paraméter** | **Leírás** |
| --- | --- |
| **megfeleljen a hozzáférési csoportnak** | Beállítja az osztályleképezés egyezési feltételeit a megadott ACL-szám vagy név alapján. |
| **mérkőzés jegyzőkönyve** | Konfigurálja az osztályleképezés egyezési feltételeit a megadott protokoll alapján. |
| **mérkőzés osztály-térkép** | Más osztálytérképet használ a forgalom azonosítására. |

A topológiában a HTTP forgalom áthaladhat az R1-en a PRIVATE zónából a NYILVÁNOS zónába. A HTTP-forgalom engedélyezése során ajánlatos kifejezetten a HTTPS- és DNS-protokollokat beilleszteni, amint az az alábbi példában látható. A forgalom bármelyik utasítással megegyezhet, hogy a HTTP-TRAFFIC osztály tagja legyen.

R1(config)# **class-map type inspect match-any HTTP-TRAFFIC**

R1(config-cmap)# **match protocol http**

R1(config-cmap)# **match protocol https**

R1(config-cmap)# **match protocol dns**

10.3.4

## 3. lépés: Határozzon meg egy műveletet

A harmadik lépés az, hogy egy házirend-térképet használjon annak meghatározására, hogy milyen műveleteket kell tenni az osztályhoz tartozó forgalom esetén. Az alábbi példa a parancs szintaxisát mutatja be a házirend-leképezés konfigurálásához. A művelet egy meghatározott funkció. Általában egy forgalmi osztályhoz kapcsolódik. Például **az inspect** , **drop** , and **pass** műveletek.

R1(config)# **policy-map type** **inspect** policy-map-name

R1(config-pmap)# **class type inspect** class-map-name

R1(config-pmap-c)# {**inspect** | **drop** | **pass**}

| **Paraméter** | **Leírás** |
| --- | --- |
| **vizsgálja meg** | Állapotalapú forgalomirányítást kínáló művelet. Az útválasztó karbantartja a TCP és UDP munkamenet-információit, és engedélyezi a visszatérő forgalmat. |
| **csepp** | Eldobja a nem kívánt forgalmat |
| **pass** | Állapot nélküli művelet, amely lehetővé teszi az útválasztó számára, hogy a forgalmat egyik zónából a másikba továbbítsa |

Az alábbi példa egy házirend-térkép-konfiguráció példáját mutatja be. Az előző lépésben konfigurált HTTP-TRAFFIC osztály egy új, PRIV-TO-PUB-POLICY nevű házirend-leképezéshez van társítva. A harmadik **inspect** parancs úgy konfigurálja az R1-et, hogy fenntartsa az állapotinformációkat minden olyan forgalomra vonatkozóan, amely a HTTP-TRAFFIC osztály tagja.

R1(config)# **policy-map type inspect PRIV-TO-PUB-POLICY**

R1(config-pmap)# **class type inspect HTTP-TRAFFIC**

R1(config-pmap-c)# **inspect**

* **ellenőrzés** – Ez a művelet állapotalapú forgalomirányítást kínál. Például, ha a PRIVÁT zónából a NYILVÁNOS zónába haladó forgalmat ellenőrzik, az útválasztó fenntartja a kapcsolat- vagy munkamenet-információkat a TCP- és UDP-forgalomhoz. Az útválasztó ekkor engedélyezi a NYILVÁNOS zóna gazdagépeitől a PRIVÁT zóna kapcsolódási kéréseire válaszul küldött visszatérő forgalmat.
* **drop** – Ez az alapértelmezett művelet az összes forgalom számára. Hasonlóan az implicit **tagadáshoz** minden ACL végén, az IOS explicit **csökkenést** alkalmaz minden szabályzatleképezés végén. szerepel **osztály-alapértelmezettként** Minden házirend-leképezés konfigurációjának utolsó szakaszában . A házirend-térképen belüli más osztályleképezések is beállíthatók a nem kívánt forgalom visszaszorítására. Az ACL-ekkel ellentétben a forgalom csendben megszűnik, és nem küldenek ICMP elérhetetlen üzeneteket a forgalom forrásának.
* **pass** – Ez a művelet lehetővé teszi az útválasztó számára, hogy a forgalmat egyik zónából a másikba továbbítsa. Az átadási művelet nem követi nyomon a kapcsolatok állapotát. A Pass csak egy irányba engedi a forgalmat. Megfelelő házirendet kell alkalmazni annak érdekében, hogy a visszatérő forgalom az ellenkező irányba haladjon át. Az átadási művelet ideális a kiszámítható viselkedésű biztonságos protokollokhoz, mint például az IPsec. A legtöbb alkalmazásforgalom azonban jobban kezelhető a ZPF-ben az **ellenőrzési** művelettel.

10.3.5

## 4. lépés: Azonosítson egy zóna-párt, és egyeztesse meg a szabályzattal

A negyedik lépés egy zónapár azonosítása, és a zónapár társítása egy szabályzattérképhez. Az alábbi példa a parancs szintaxisát mutatja be. Hozzon létre egy zónapárt a **zónapár biztonsági** paranccsal. Ezután a **service-policy type inspect** paranccsal csatolja a házirend-leképezést és a hozzá tartozó műveletet a zónapárhoz.

Router(config)# **zone-pair security** zone-pair-name **source** {source-zone-name | **self**} **destination** {destination-zone-name | **self}**

Router(config-sec-zone-pair)# **service-policy type inspect** policy-map-name

| **Paraméter** | **Leírás** |
| --- | --- |
| **forrás**  forrás-zónanév | Megadja annak a zónának a nevét, ahonnan a forgalom indul. |
| **rendeltetési hely**  célzóna neve | Megadja annak a zónának a nevét, ahová a forgalom irányul. |
| **maga** | Megadja a rendszer által meghatározott zónát. Azt jelzi, hogy a forgalom magához a routerhez fog-e irányulni, vagy magától onnan indul. |

Az alábbi példa egy zónapár konfiguráció példáját mutatja be. Létrejön egy PRIV-PUB nevű zónapár, amelynek forrászónája a PRIVATE, célzónaként pedig NYILVÁNOS. Ezután az előző lépésben létrehozott házirend-térkép hozzá van rendelve a zónapárhoz.

A tűzfalházirend konfigurálása után a rendszergazda a zónapár biztonsági paranccsal alkalmazza azt a zónapár közötti forgalomra. A házirend alkalmazásához hozzá kell rendelni egy zónapárhoz. A zónapárnak meg kell adnia a forrászónát, a célzónát, valamint a forrás- és célzóna közötti forgalom kezelésére vonatkozó szabályzatot.

R1(config)# **zone-pair security PRIV-PUB source PRIVATE destination PUBLIC**

R1(config-sec-zone-pair)# **service-policy type inspect PRIV-TO-PUB-POLICY**

10.3.6

## 5. lépés: Rendeljen zónákat az interfészekhez

Az ötödik lépés a zónák hozzárendelése a megfelelő interfészekhez. Egy zóna interfészhez való társítása azonnal alkalmazza a zónához társított szolgáltatási szabályzatot. Ha a zónához még nincs konfigurálva szolgáltatási szabályzat, akkor az összes tranzitforgalom megszűnik. A **zónatag biztonsági** paranccsal rendelhet hozzá zónát egy interfészhez, az alábbi példában látható módon.

Router(config-if)# **zone-member security** zone-name

A következő példában a GigabitEthernet 0/0 a PRIVATE zónához, a Serial 0/0/0 pedig a NYILVÁNOS zónához van hozzárendelve.

R1(config)# **interface GigabitEthernet 0/0**

R1(config-if)# **zone-member security PRIVATE**

R1(config-if)# **interface Serial 0/0/0**

R1(config-if)# **zone-member security PUBLIC**

A szolgáltatási szabályzat most aktív. A PRIVATE zónából származó és a NYILVÁNOS zónába irányuló HTTP-, HTTPS- és DNS-forgalom ellenőrzésre kerül. A NYILVÁNOS zónából származó és a PRIVÁT zónába irányuló forgalom csak akkor engedélyezett, ha az eredetileg PRIVÁT zóna gazdagépei által kezdeményezett munkamenet része.

10.3.7

## Ellenőrizze a ZPF konfigurációt

Ellenőrizze a ZPF konfigurációt a futó konfiguráció megtekintésével. Figyeljük meg, hogy az osztálytérkép szerepel az első helyen. Ezután a házirend-térkép az osztálytérképet használja. Figyelje meg a kiemelt **class-default osztályt** is , amely minden más olyan forgalmat eldob, amely nem tagja a HTTP-TRAFFIC osztálynak.

A zónakonfigurációk követik a házirend-leképezés konfigurációit a zóna elnevezésével, zónapárosításával és a zónapárhoz társított szolgáltatási szabályzattal. Végül az interfészekhez zónák vannak hozzárendelve.

R1# **show run | begin class-map**

!

<some output omitted>

!

class-map type inspect match-any HTTP-TRAFFIC

match protocol http

match protocol https

match protocol dns

!

policy-map type inspect PRIV-TO-PUB-POLICY

class type inspect HTTP-TRAFFIC

inspect

class class-default

drop

!

zone security PRIVATE

zone security PUBLIC

zone-pair security PRIV-PUB source PRIVATE destination PUBLIC

service-policy type inspect PRIV-TO-PUB-POLICY

!

interface GigabitEthernet0/0

zone-member security PRIVATE

!

interface Serial0/0/0

zone-member security PUBLIC

!

Az alábbi példa ellenőrzési információkat mutat be a ZPF konfiguráció tesztelése után. Egy 192.168.1.3-as PRIVÁTzóna gazdagép HTTPS-munkamenetet hozott létre a 10.1.1.2-es webszerverrel. Vegyük észre a parancs kimenetében, hogy négy csomag egyezik az **class-default osztályzattal** . Ezt az ellenőrző információt úgy állítottuk elő, hogy a 192.168.1.3 host ping a webszerveren a 10.1.1.2.

R1# **show policy-map type inspect zone-pair sessions**

policy exists on zp PRIV-PUB

Zone-pair: PRIV-PUB

Service-policy inspect : PRIV-TO-PUB-POLICY

Class-map: HTTP-TRAFFIC (match-any)

Match: protocol http

12 packets, 384 bytes

30 second rate 0 bps

Match: protocol https

5 packets, 160 bytes

30 second rate 0 bps

Match: protocol dns

0 packets, 0 bytes

30 second rate 0 bps

Inspect

Number of Established Sessions = 1

Established Sessions

Session 2204E220 (192.168.1.3:1049)=>(10.1.1.2:443) https:tcp

SIS\_OPEN/TCP\_CLOSEWAIT

Created 00:00:14, Last heard 00:00:11

Bytes sent (initiator:responder) [821:1431]

Class-map: class-default (match-any)

Match: any

Drop

4 packets, 160 bytes

R1#

Az alábbi példa négy másik ZPF-ellenőrző parancsot mutat be, amelyek lehetővé teszik a ZPF-konfiguráció bizonyos részei megtekintését.

R1# **show class-map** **type inspect**

Class Map type inspect match-any HTTP-TRAFFIC (id 1)

Match protocol http

Match protocol https

Match protocol dns

R1# **show zone security**

zone self

Description: System Defined Zone

zone PRIVATE

Member Interfaces:

GigabitEthernet0/0

zone PUBLIC

Member Interfaces:

Serial0/0/0

R1# **show zone-pair security**

Zone-pair name PRIV-PUB

Source-Zone PRIVATE Destination-Zone PUBLIC

service-policy PRIV-TO-PUB-POLICY

R1# **show policy-map type inspect**

Policy Map type inspect PRIV-TO-PUB-POLICY

Class HTTP-TRAFFIC

Inspect

Class class-default

Drop

10.3.8

## Szintaxis-ellenőrző – ZPF konfigurálása

1. lépés: Hozza létre a zónákat.

* A zónabiztonság paranccsal hozzon létre egy **PRIVATE** nevű zónát .
* Lépjen ki a config-sec-zone konfigurációs módból.
* A zónabiztonság paranccsal hozzon létre egy **NYILVÁNOS** nevű zónát .
* Lépjen ki a config-sec-zone konfigurációs módból.

R1(config)#zone security PRIVATE

R1(config-sec-zone)#exit

R1(config)#zone security PUBLIC

R1(config-sec-zone)#exit

R1(config)#

Step 2: Identify traffic with a class-map.

* Create an inspect type class-map called **HTTP-TRAFFIC**. The class-map should use the match-any inspection criteria.
* Use the **match protocol** command to allow the HTTP, HTTPS, DNS protocols.
* Exit config-cmap configuration mode.

R1(config-cmap)#class-map type inspect match-any HTTP-TRAFFIC

R1(config-cmap)#match protocol http

R1(config-cmap)#match protocol https

R1(config-cmap)# match protocol dns

R1(config-cmap)# kilépés

3. lépés: Határozzon meg egy műveletet egy irányelvtérkép segítségével.

* Hozzon létre egy vizsgálati típusú házirend-térképet **PRIV-TO-PUB-POLICY** néven .
* Társítsa a **2. lépésben létrehozott HTTP-TRAFFIC** osztályleképezést a házirend-leképezéshez az **osztálytípus inspect** paranccsal.
* Rendelje hozzá a műveletet az **ellenőrzéshez** .
* Lépjen ki a policy-map-c konfigurációs módból.
* Lépjen ki a házirend-térkép konfigurációs módból.

R1(config)# házirend-leképezés típusa vizsgálja meg a PRIV-TO-PUB-POLICY-t

Az R1(config-pmap)# osztálytípus megvizsgálja a HTTP-TRAFFIC-ot

R1(config-pmap-c)# vizsgálat

R1(config-pmap-c)# kilépés

R1(config-pmap)# kilépés

R1(config)#

4. lépés: Határozzon meg egy zónapárt, és illessze azt egy szabályzattérképhez.

* nevű zónapárt **Hozzon létre egy PRIV-PUB** . A forrás a **PRIVÁT** zóna legyen **zóna, a cél pedig a NYILVÁNOS** .
* A **service-policy** paranccsal rendelje hozzá a **PRIV-TO-PUB-POLICY házirend-térképet.** 3. lépésben létrehozott
* Lépjen ki a config-sec-zone-pair módból.

R1(config)# zónapár biztonság PRIV-PUB forrás PRIVÁT célhely NYILVÁNOS

R1(config-sec-zone-pair)# szolgáltatás-házirend típus vizsgálat PRIV-TO-PUB-POLICY

R1(config-sec-zone-pair)# kilépés

Step 5: Assign zones to the appropriate interfaces.

* Assign the zone **PRIVATE** to interface G0/0.
* Assign the zone **PUBLIC** to interface S0/0/0.
* End configuration mode.

R1(config)#interface g0/0

R1(config-if)#zone-member security PRIVATE

R1(config-if)#interface s0/0/0

R1(config-if)#zone-member security PUBLIC

R1(config-if)#end

R1#

Enter the **show run | begin class-map** command to verify your configuration.

R1#show run | begin class-map

!

<némelyik kimenet kimaradt>

!

class-map type inspect match-any HTTP-TRAFFIC

mérkőzés protokoll http

mérkőzés protokoll https

match protocol dns

!

házirend-térkép típusú vizsgálat PRIV-TO-PUB-POLICY

osztály típusa vizsgálja meg a HTTP-TRAFFIC-et

vizsgálja meg

class class-default

csepp

!

zóna biztonság MAGÁN

zóna biztonság NYILVÁNOS

zóna-pár biztonság PRIV-PUB forrás PRIVÁT cél NYILVÁNOS

service-policy típusú vizsgálat PRIV-TO-PUB-POLICY

!

interfész GigabitEthernet0/0

zóna-tag biztonság MAGÁN

!

interfész Serial0/0/0

zóna-tag biztonság NYILVÁNOS

!

R1#

Sikeresen konfigurált egy zónaalapú házirend tűzfalat az R1-en.

10.3.9

## ZPF konfigurációs szempontok

Amikor ZPF-t konfigurál a CLI-vel, több tényezőt is figyelembe kell venni:

* Az útválasztó soha nem szűri az ugyanabban a zónában lévő interfészek közötti forgalmat.
* Egy interfész nem tartozhat több zónához. A biztonsági zónák uniójának létrehozásához adjon meg egy új zónát és a megfelelő házirend-térképet és zónapárokat.
* A ZPF együtt létezhet a klasszikus tűzfallal, bár nem használhatók ugyanazon a felületen. Távolítsa el az **ip inspect** interface configuration parancsot a **zónatag biztonsági** parancs alkalmazása előtt.
* A forgalom soha nem folyhat egy zónához rendelt interfész és egy zóna hozzárendelés nélküli interfész között. konfigurációs parancs alkalmazása **A zónatag** mindig a szolgáltatás ideiglenes megszakítását eredményezi, amíg a másik zónatag be nem állítja.
* Az alapértelmezett zónák közötti házirend az összes forgalom törlése, hacsak a zónapárhoz konfigurált szolgáltatási szabályzat másként nem engedélyezi.
* A **zóna-tag** parancs magát az útválasztót nem védi (az útválasztó felé irányuló és onnan induló forgalmat ez nem érinti), kivéve, ha a zónapárok az előre meghatározott saját zónával vannak konfigurálva.

10.3.10

## Videóbemutató – ZPF-ek

10.3.11

## Packet Tracer – ZPF konfigurálása

Ebben a Packet Tracerben a következő célokat valósítja meg:

* A tűzfal konfigurálása előtt ellenőrizze az eszközök közötti kapcsolatot.
* Konfiguráljon ZPF-et az R3 útválasztón.
* Ellenőrizze a ZPF működését ping, Telnet és webböngésző segítségével.

[Konfiguráljon ZPF-et](https://contenthub.netacad.com/courses/netsec/_common/10.3.11-packet-tracer---configure-a-zpf.pka)

10.3.12

## Lab – ZPF-ek konfigurálása

Ebben a laborban a következő célokat kell teljesítenie:

* Végezze el az útválasztó alapkonfigurációját.
* Használja a CLI-t a ZPF konfigurálásához.
* Használja a CLI-t a konfiguráció ellenőrzéséhez.

[10.2](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[ZPF Operation](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[10.4](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Zone-Based Firewalls Summary](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/1.0.5?lng=en#chunks-container)

*                                                                                                                           

1. Zóna alapú házirend tűzfalak
2. Zone-Based Firewalls Summary

# Zóna alapú tűzfalak összefoglalója

10.4.1

## Mit tanultam ebben a modulban?

**A ZPF áttekintése**   
Az IOS ZPF rugalmas és hatékony helyettesíti a régebbi klasszikus IOS tűzfalat. Ez egy új konfigurációs módot biztosít, amelyben a biztonsági zónákhoz interfészek vannak hozzárendelve, a zónák közötti forgalomra pedig tűzfalszabályok vonatkoznak. A ZPF strukturált és egyszerűsített módszert kínál a hálózati biztonság tervezésére és megvalósítására tűzfal funkciót ellátó útválasztókon.

**ZPF működés**   
A ZPF-ek felhasználó által definiált házirendeket használnak a forrászónából a célzónába tartó meghatározott forgalomra. Három művelet adható meg:

* **Ellenőrzés** – A ZPF állapotalapú csomagellenőrzést végez.
* **Drop** – A forgalom nem haladhat a célállomás felé. Az elutasított csomagok naplózhatók.
* **Pass** – A forgalom a célzónába közlekedhet. Ez nem követi nyomon a kapcsolatok vagy a munkamenetek állapotát.

A tranzit forgalomra az alapértelmezett szabályokat alkalmazzák a be- és kilépő felületek konfigurációja és a házirendek megléte alapján. Például, ha sem a be-, sem a kilépési interfész nincs definiálva egy zóna tagjaként, a forgalom kiléphet a kilépési felületről. Hasonlóképpen, ha mindkét interfész ugyanannak a zónának a tagja, akkor a forgalom áthaladhat. Ha azonban az egyik interfész egy zóna tagja, a másik pedig nem, akkor a forgalom megszűnik. Fontos megérteni ezeket és a modulban tárgyalt többi szabályt.

Létezik egy speciális zóna, amelyet saját zónának neveznek. A self zóna maga a router. Az önzónában az útválasztó interfészek a forgalom forrásaként vagy célpontjaként szolgálnak. Az önzóna forgalom vagy az eszköz felügyeletére, vagy a forgalom továbbításának vezérlésére szolgál. A tranzitforgalomra vonatkozó szabályokhoz hasonlóan léteznek szabályok arra vonatkozóan, hogy a saját zónában hogyan kell kezelni a forgalmat.

**Konfiguráljon ZPF-et**   
A ZPF konfigurálása öt lépésből áll. Először a zónák jönnek létre. Ezután egy vagy több osztályleképezés jön létre annak meghatározására, hogy milyen forgalmat kell társítani egy szabályzathoz. Ezután olyan házirendek jönnek létre, amelyek az osztálytérkép forgalmát az átadási, ledobási vagy ellenőrzési műveletekhez társítják. Ezután létre kell hozni zónapárokat, amelyek társításra kerülnek a házirend-térképekkel. Végül az interfészek zónákhoz vannak társítva. Ezen a ponton a ZPF szabályzat aktív.

10.4.2

## 10. modul – Zóna alapú tűzfalak kvíz

Az űrlap teteje

1. Melyik állítás írja le pontosan a Cisco IOS zónaalapú házirend tűzfal működését?

Az űrlap alja

Hogyan kezeli a ZPF a forgalmat egy zónatag és egy másik zónához nem tartozó interfész között?

konfigurálásakor ? Melyik utasítás írja le azt a tényezőt, amelyet figyelembe kell venni egy zóna alapú házirend tűzfal

megvalósítása során ? Melyik utasítás írja le az interfész viselkedését szabályozó szabályok egyikét a zónaalapú házirend tűzfalkonfiguráció

A ZPF tervezése több lépést igényel. Melyik lépésben határozzuk meg azokat a határokat, ahol a forgalom irányelvi korlátozások alá esik, amikor a hálózat másik régiójába kerül?

Cisco IOS zónaalapú házirend - tűzfal konfigurálásakor melyik két művelet alkalmazható egy forgalmi osztályra? (Válassz kettőt.)

Melyik három állítás írja le a zónaalapú házirend tűzfalszabályokat, amelyek szabályozzák az interfész viselkedését és a zónatagok interfészek közötti forgalmat? (Válassz hármat.)

egy jellemzőjét ? Melyik állítás írja le a zóna alapú házirend tűzfal

tűzfal konfigurációjának melyik lépésében A zónaalapú házirend - azonosítják a forgalmat a szabályzatalkalmazáshoz?

Ha osztályleképezést állít be egy zónaalapú házirend használatakor ? **-tűzfalhoz, hogyan alkalmazzák az egyezési feltételeket a match - all** paraméter

A ZPF tervezésben mit nevezünk én zónának?

Melyik utasítás ír le egy zónát a ZPF Cisco útválasztón való implementálásakor?

[10.3](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Configure a ZPF](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[11.0](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/1.0.5?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                
*                     

1. IPS technológiák

# Bevezetés

11.0.1

## Miért vegyem ezt a modult?

Különféle eszközök és rendszerek együttesen védik a hálózatot több szinten. A biztonsági fenyegetések közé tartozik a rosszindulatú programok és az adatlopás. A hálózat szélén lévő eszközök megakadályozzák, hogy a fenyegetés szereplői behatoljanak és a rosszindulatú programok bejussanak a hálózatba. A gazdagépeken található szoftverrendszerek védelmet nyújtanak a rosszindulatú programok és az adatlopás ellen is. Ebben a modulban megismerheti a hálózati eszközökön és hálózati gazdagépeken működő behatolásészlelő és behatolásgátló rendszereket.

11.0.2

## Mit fogok tanulni ebben a modulban?

**Modul címe:** IPS Technologies

**A modul célja** : Ismertesse meg, hogyan használják a hálózatalapú behatolás-megelőzési rendszereket a hálózat biztonságának elősegítésére.

| **téma címe** | **Téma Cél** |
| --- | --- |
| **IDS és IPS jellemzők** | Ismertesse az IDS és IPS rendszerek funkcióit és működését! |
| **IPS megvalósítások** | Magyarázza el, hogyan valósul meg a hálózatalapú IPS. |
| **IPS a Cisco ISR-eken** | Ismertesse a Cisco ISR útválasztókon elérhető IPS-technológiákat. |
| **Cisco kapcsolt port analizátor** | A Cisco SPAN beállítása. |

[10.4](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Zóna alapú tűzfalak összefoglalója](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[11.1](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[IDS és IPS jellemzők](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                   
*                     

1. IPS technológiák
2. IDS and IPS Characteristics

# IDS és IPS jellemzők

11.1.1

## Nulladik napi támadások

A rosszindulatú programok percek alatt elterjedhetnek az egész világon. A hálózatnak azonnal fel kell ismernie és mérsékelnie kell a rosszindulatú programokat. A tűzfalak csak ennyire képesek, és nem tudnak védelmet nyújtani minden rosszindulatú program és nulladik napi támadás ellen.

A nulladik napi támadás, amelyet néha nulladik napi fenyegetésnek is neveznek, olyan kibertámadás, amely a szoftvergyártó által ismeretlen vagy fel nem tárt szoftversebezhetőségeket próbálja kihasználni, amint az az ábrán is látható. A nulladik nap kifejezés azt a pillanatot írja le, amikor egy korábban ismeretlen fenyegetést azonosítanak.

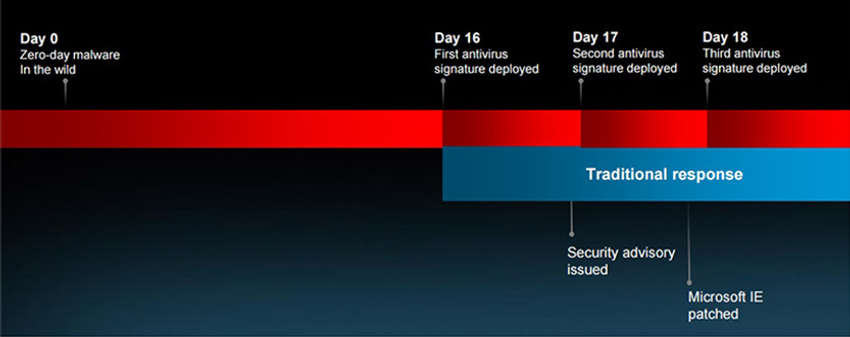
Az ábrán egy nulladik napi támadást illusztráló topológia látható. A nulladik napi támadást egy vörös koponya és keresztezett csontok ábrázolják, akik tűzfalon keresztül próbálnak bejutni a LAN-ba

### Zero-Day Exploit Attack

Remote Worker VPN Remote Branch VPN VPN Firewall LAN Web Server Email Server DNS Server Nulladik napi támadás

Azalatt az idő alatt, amíg a szoftvergyártó egy javítást kifejleszt és kiad, a hálózat sebezhetővé válik ezekkel a visszaélésekkel szemben, amint az az ábrán is látható. Az ilyen gyorsan terjedő támadások elleni védekezés megköveteli a hálózatbiztonsági szakemberektől, hogy kifinomultabb képet kapjanak a hálózati architektúráról. A hálózat néhány pontján már nem lehet visszatartani a behatolásokat.

### A Microsoft Internet Explorer nulladik napi sebezhetősége



11.1.2

## Figyelemmel kíséri a támadásokat

A rosszindulatú programok kizsákmányolásának megakadályozásának egyik módja az, hogy a rendszergazda folyamatosan figyeli a hálózatot és elemzi a hálózati eszközök által generált naplófájlokat. A biztonsági műveleti központ (SOC) eszközei, mint például a biztonsági információ- és eseménykezelés (SIEM), valamint a biztonsági irányítási, automatizálási és válaszadási (SOAR) rendszerek automatizálják a naplófájl-gyűjtési és -elemzési folyamatot. Elfogadott tény, hogy a rosszindulatú programok a legjobb védekezés ellenére is bekerülnek a hálózatba. Emiatt a rosszindulatú programok elleni védelem többrétegű megközelítését kell alkalmazni. Az eszközök által az egyes rétegeken generált naplófájlok segítenek azonosítani, hogy történt-e visszaélés, a kihasználás diagnosztikai jellemzői és a vállalaton belüli kár mértéke. A naplófájlokban összegyűjtött információk segítenek tájékozódni a kizsákmányolásra válaszul hozott intézkedésekről, például a korlátozásról és a mérséklésről.

A behatolásészlelő rendszereket (IDS) a hálózat forgalmának passzív megfigyelésére vezették be. Az ábra azt mutatja, hogy egy IDS-képes eszköz a forgalmi adatfolyamot másolja, és a másolt forgalmat elemzi, nem pedig a ténylegesen továbbított csomagokat.

Az ábra egy topológiát mutat be, amely azt szemlélteti, hogy egy ID S-kompatibilis eszköz átmásolja a forgalmi adatfolyamot az ID S-kompatibilis érzékelőn keresztül, és a másolt forgalmat a felügyeleti konzollal elemzi, nem pedig a ténylegesen továbbított csomagokat.

### Behatolásérzékelő rendszer működése

1 1 3

2

váltása IDS-kompatibilis érzékelőkezelési konzolcél Az

Offline üzemmódban az IDS összehasonlítja a rögzített forgalmi adatfolyamot az ismert rosszindulatú aláírásokkal, hasonlóan a víruskereső szoftverekhez. Az offline munkavégzés több dolgot is jelent:

* Az IDS passzívan működik.
* Az IDS eszköz fizikailag úgy van elhelyezve a hálózatban, hogy a forgalmat tükrözni kell az eléréséhez.
* A hálózati forgalom csak akkor halad át az IDS-en, ha az tükröződik.
* Nagyon kevés késleltetést adnak hozzá a hálózati forgalomhoz.

Bár a forgalmat figyelik, naplózzák és esetleg jelentést is készítenek, az IDS nem tesz semmit a csomagokkal kapcsolatban. Ezt az offline IDS-megvalósítást promiscuous módnak nevezik.

A forgalom másolatával való működés előnye, hogy az IDS nem befolyásolja negatívan a továbbított forgalom csomagfolyamát. A forgalom másolatán való működés hátránya, hogy az IDS nem tudja megakadályozni, hogy a rosszindulatú egycsomagos támadások elérjék a célt. Az IDS-nek gyakran más hálózati eszközök, például útválasztók és tűzfalak segítségére van szüksége ahhoz, hogy válaszoljon egy támadásra.

Jobb megoldás egy olyan eszköz használata, amely azonnal észleli és leállítja a támadást. Ezt a funkciót egy behatolásgátló rendszer (IPS) látja el.

11.1.3

## Behatolás-megelőzési és -észlelő eszközök

A hálózati architektúra paradigmaváltására van szükség a gyorsan mozgó és fejlődő támadások elleni védekezéshez. Ennek tartalmaznia kell a költséghatékony észlelési és megelőzési rendszereket, mint például a behatolásérzékelő rendszereket (IDS) vagy a jobban skálázható behatolásgátló rendszereket (IPS). A hálózati architektúra ezeket a megoldásokat integrálja a hálózat belépési és kilépési pontjaiba.

Az IDS vagy IPS implementációja során fontos ismerni az elérhető rendszerek típusait, a gazdagép alapú és a hálózat alapú megközelítéseket, ezeknek a rendszereknek az elhelyezését, az aláírási kategóriák szerepét, és a Cisco IOS útválasztók lehetséges műveleteit. amikor támadást észlelnek.

Az ábra azt mutatja, hogy egy IPS-eszköz hogyan kezeli a rosszindulatú forgalmat.

Az ábrán egy felhasználó látható a jobb felső sarokban, aki csatlakoztatva van, és forgalmat küld a felhőbe. A felhő csatlakozik egy útválasztóhoz, és azon keresztül továbbítja a forgalmat. A felhő egy ips-kompatibilis érzékelőhöz csatlakozik, amely egy másik útválasztóhoz csatlakozik, amely szintén csatlakozik a felügyeleti konzolhoz és egy laptophoz, amelyet megjelölt célként. Az ips-kompatibilis érzékelő oldalán található egy ikon is a bitgyűjtőhöz. Az azonosítók és IP-k jellemzői közé tartozik, hogy mindkét technológiát szenzorként alkalmazzák, mindkét technológia aláírásokat használ a hálózati forgalom visszaélési mintáinak észlelésére, és mindkettő képes felismerni atomi mintákat (egy csomag) vagy összetett mintákat (több csomag).

### IDS és IPS jellemzők

4 1 2

3

Bit Bucket IPS-kompatibilis   
Szenzorkezelés ​   
A Console Target **IDS és IPS közös jellemzői**

* Mindkét technológiát érzékelőként alkalmazzák.
* Mindkét technológia aláírásokat használ a hálózati forgalom visszaélési mintáinak észlelésére.
* Mindkettő képes felismerni atomi mintákat (egycsomagos) vagy összetett mintákat (többcsomagos).

1. A rosszindulatú forgalmat a hálózaton belüli célállomásra küldik.
2. A forgalmat a hálózatba irányítják, és egy IPS-képes érzékelő fogadja, ahol blokkolva van.
3. Az IPS-kompatibilis érzékelő a forgalommal kapcsolatos naplózási információkat küld a hálózatbiztonsági felügyeleti konzolnak.
4. Az IPS-képes szenzor megöli a forgalmat. (A „Bit Bucket”-nek küldik.)

Mind az IDS, mind az IPS technológiát érzékelőként alkalmazzák. Az IDS vagy IPS érzékelő többféle eszközből állhat:

* IPS szoftverrel konfigurált útválasztó
* Kifejezetten dedikált IDS vagy IPS szolgáltatások nyújtására tervezett eszköz
* Adaptív biztonsági berendezésbe (ASA), kapcsolóba vagy útválasztóba telepített hardvermodul

Az IDS és IPS technológiák aláírásokat használnak a hálózati forgalom mintáinak észlelésére. Az aláírás olyan szabálykészlet, amelyet az IDS vagy IPS használ a rosszindulatú tevékenységek észlelésére. Az aláírások felhasználhatók a biztonság súlyos megsértésének észlelésére, a gyakori hálózati támadások észlelésére és információgyűjtésre. Az IDS- és IPS-technológiák képesek felismerni az atomi aláírási mintákat (egycsomagos) vagy az összetett aláírási mintákat (többcsomagos).

11.1.4

## Az IDS és az IPS előnyei és hátrányai

**Az IDS előnyei és hátrányai**

A táblázat összefoglalja az IDS és az IPS előnyeit és hátrányait.

| **Megoldás** | **Előnyök** | **Hátrányok** |
| --- | --- | --- |
| **IDS** | * Nincs hatással a hálózatra (latencia, jitter) * Érzékelőhiba esetén nincs hálózati hatás * Nincs hálózati hatás, ha az érzékelő túlterhelt | * A válaszművelet nem tudja leállítani a trigger csomagokat * Helyes hangolás szükséges a válaszlépésekhez * Sebezhetőbb a hálózati biztonság kikerülési technikáival szemben |
| **IPS** | * Leállítja a trigger csomagokat * Tud folyamnormalizációs technikákat használni | * Az érzékelővel kapcsolatos problémák befolyásolhatják a hálózati forgalmat * Az érzékelő túlterhelése hatással van a hálózatra * Némi hatás a hálózatra (latencia, jitter) |

Kattintson az egyes gombra, ha többet szeretne megtudni az IDS és IPS érzékelőkről

**IDS előnyei**

Az IDS offline módban kerül telepítésre, ezért:

* Az IDS nincs hatással a hálózati teljesítményre. Pontosabban, nem okoz késleltetést, jittert vagy egyéb forgalommal kapcsolatos problémákat.
* Az IDS nincs hatással a hálózat működésére, ha az érzékelő meghibásodik. Ez csak az IDS adatelemzési képességét érinti.

**Az IDS hátrányai**

Az IDS hátrányai a következők:

* Az IDS-érzékelő nem tudja leállítani a riasztást kiváltó csomagokat, és kevésbé segít az e-mail vírusok és az automatikus támadások, például a férgek észlelésében.
* Az IDS-érzékelők hangolása a behatolásészlelés várható szintjének elérése érdekében nagyon időigényes lehet. Az IDS-érzékelő válaszműveleteit telepítő felhasználóknak jól megtervezett biztonsági szabályzattal kell rendelkezniük, és jól ismerniük kell az IDS-telepítéseiket.
* Az IDS-megvalósítás sebezhetőbb a hálózati biztonság kikerülési technikáival szemben, mivel nincs beépítve.

11.1.5

## Ellenőrizze, hogy megértette-e az IDS és az IPS jellemzőit

Válassza ki minden jellemzőhöz a megfelelő szállítási módot.

Sebezhetőbb a különféle hálózati támadási módszerek által lehetővé tett hálózati biztonsági kijátszási technikákkal szemben

[IDS](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "IDS)

[IPS](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "IPS)

Befolyásolhatja a hálózati teljesítményt a késleltetés és a jitter bevezetésével

[IDS](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "IDS)

[IPS](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "IPS)

Úgy kell megvalósítani, hogy az időérzékeny alkalmazások ne legyenek hátrányosan érintve

[IDS](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "IDS)

[IPS](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "IPS)

Nem lehet leállítani a trigger csomagot, és nem garantált, hogy leállítja a kapcsolatot

[IDS](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "IDS)

[IPS](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "IPS)

Offline módban telepítve

[IDS](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "IDS)

[IPS](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "IPS)

Használhat adatfolyam-normalizációs technikákat, hogy csökkentse vagy megszüntesse a meglévő hálózatbiztonsági kijátszási lehetőségeket

[IDS](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "IDS)

[IPS](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "IPS)

Beállítható úgy, hogy csomagledobást hajtson végre a trigger csomag leállítása érdekében

[IDS](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "IDS)

[IPS](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "IPS)

Elsősorban a lehetséges események azonosítására, az eseményekkel kapcsolatos információk naplózására és   
jelentést az eseményekről

[IDS](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "IDS)

[IPS](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "IPS)

Inline kell telepíteni, és a forgalomnak át kell haladnia rajta

[IDS](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "IDS)

[IPS](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "IPS)

Kevésbé hasznos az e-mail vírusok és az automatizált támadások, például a férgek megállításában

[IDS](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "IDS)

[IPS](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "IPS)

[11.0](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[11.2](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[IPS Implementations](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                     
*                     

1. IPS technológiák
2. IPS Implementations

# IPS megvalósítások

11.2.1

## Az IPS típusai

Az IPS két elsődleges típusa érhető el: gazdagép alapú IPS és hálózat alapú IPS.

**Gazda alapú IPS**

A gazdagép alapú IPS (HIPS) egy olyan szoftver, amely a gazdagépre telepítve figyeli és elemzi a gyanús tevékenységeket. A HIPS jelentős előnye, hogy képes figyelni és védeni az operációs rendszert és az adott gazdagépre jellemző kritikus rendszerfolyamatokat. Az operációs rendszer részletes ismeretében a HIPS képes figyelni a rendellenes tevékenységeket, és megakadályozza, hogy a gazdagép olyan parancsokat hajtson végre, amelyek nem felelnek meg a szokásos viselkedésnek. Ez a gyanús vagy rosszindulatú viselkedés magában foglalhatja a rendszerleíró adatbázis jogosulatlan frissítéseit, a rendszerkönyvtár módosításait, a telepítőprogramok végrehajtását és a puffertúlcsordulást okozó tevékenységeket. A hálózati forgalom is figyelhető annak megakadályozására, hogy a gazdagép szolgáltatásmegtagadási (DoS) támadásban vegyen részt, vagy egy tiltott FTP-munkamenet része legyen.

A HIPS felfogható a víruskereső szoftver, a kártevőirtó szoftver és a tűzfal kombinációjaként. A HIPS-re példa a Windows Defender. Számos védelmi intézkedést biztosít a Windows-gazdagépek számára. A hálózat alapú IPS-sel kombinálva a HIPS hatékony eszköz a gazdagép további védelmére.

A HIPS hátránya, hogy csak helyi szinten működik. Nem rendelkezik teljes áttekintéssel a hálózatról vagy a hálózaton keresztül esetlegesen előforduló koordinált eseményekről. Ahhoz, hogy hatékony legyen a hálózatban, a HIPS-t minden gazdagépen telepíteni kell, és támogatnia kell minden operációs rendszert. A táblázat felsorolja a HIPS előnyeit és hátrányait.

| **Előnyök** | **Hátrányok** |
| --- | --- |
| * A gazdagép operációs rendszerre jellemző védelmet nyújt * Operációs rendszer és alkalmazás szintű védelmet biztosít * Védi a gazdagépet az üzenet visszafejtése után | * Operációs rendszer függő * Telepíteni kell minden gazdagépen |

**Hálózat alapú IPS**

A hálózatalapú IPS megvalósítható dedikált vagy nem dedikált IPS-eszköz, például útválasztó használatával. A hálózati alapú IPS-megvalósítások a behatolásmegelőzés kritikus összetevői. A robusztus biztonsági architektúra biztosítása érdekében a gazdagép alapú IDS/IPS megoldásokat integrálni kell egy hálózat alapú IPS-megvalósítással.

Az érzékelők valós időben észlelik a rosszindulatú és jogosulatlan tevékenységeket, és szükség esetén intézkedhetnek. Amint az ábrán látható, az érzékelők a kijelölt hálózati pontokon vannak elhelyezve. Ez lehetővé teszi a biztonsági menedzserek számára, hogy figyelemmel kísérjék a hálózati tevékenységet, miközben az történik, függetlenül a támadás célpontjának helyétől.

Az ábrán egy tűzfalhoz csatlakoztatott, nem megbízható hálózat látható. A tűzfal egy érzékelőhöz csatlakozik, amelyhez webszerver és dns szerver kapcsolódik. A tűzfal egy másik érzékelőhöz is csatlakozik, amelyhez felügyeleti szerver és útválasztó is van csatlakoztatva. Az útválasztónak van egy másik kapcsolata egy másik érzékelővel, amely laptopokhoz csatlakozik. Az útválasztó, az érzékelő és a laptopok egy vállalati hálózaton belül találhatók.

### Példa az IPS-érzékelő telepítésére

Vállalati hálózati érzékelő érzékelő érzékelő menedzsment   
Szerver Webszerver DNS-kiszolgáló Nem megbízható hálózati tűzfal

11.2.2

## Hálózat alapú IPS

A hálózati alapú IPS érzékelők többféleképpen is megvalósíthatók:

* Cisco Firepower készüléken
* ASA tűzfal eszközön
* ISR routeren
* Virtuális következő generációs IPS-ként (NGIPSv) a VMware számára

A hálózati alapú IPS-re példa a Cisco Firepower NGIPS. Behatolásmegelőzési elemzésre van hangolva. A platform mögöttes operációs rendszerét megfosztják a szükségtelen hálózati szolgáltatásoktól, az alapvető szolgáltatások pedig biztonságosak. Ezt keményedésnek nevezik.

Az összes hálózati alapú érzékelő hardvere három összetevőből áll:

* **NIC** – A hálózatalapú IPS-nek képesnek kell lennie bármely hálózathoz, például Ethernethez, Fast Ethernethez és Gigabit Ethernethez csatlakozni.
* **Processzor** – A behatolásmegelőzéshez CPU-teljesítményre van szükség a behatolásészlelés elemzéséhez és a mintaillesztéshez.
* **Memória** – A behatolásészlelés elemzése memóriaigényes. A memória közvetlenül befolyásolja a hálózati alapú IPS azon képességét, hogy hatékonyan és pontosan észlelje a támadást.

A hálózatalapú IPS valós idejű biztonsági betekintést nyújt a biztonsági vezetőknek hálózataikba, a növekedéstől függetlenül. További gazdagépek adhatók a védett hálózatokhoz anélkül, hogy több érzékelőre lenne szükség. További érzékelőkre csak akkor van szükség, ha a névleges forgalmi kapacitásukat túllépik, ha teljesítményük nem felel meg az aktuális igényeknek, vagy ha a biztonsági politika vagy a hálózat kialakításának felülvizsgálata további érzékelőket tesz szükségessé a biztonsági határok érvényesítése érdekében. Új hálózatok hozzáadásával további érzékelők könnyen telepíthetők.

11.2.3

## Beépítési módok

Az IDS és IPS érzékelők beépített módban (más néven inline interfész páros módban) vagy promiscuous módban (más néven passzív módban) működhetnek.

Amint az ábrán látható, a csomagok nem áramlanak át az érzékelőn promiszkuális módban. Az érzékelő a megfigyelt forgalom másolatát elemzi, nem a tényleges továbbított csomagot. A promiscuous üzemmód előnye, hogy a szenzor nem befolyásolja a továbbított forgalom csomagfolyamát. A promiscuous módban való működés hátránya, hogy bizonyos típusú támadások, például atomtámadások (egycsomagos támadások) esetén az érzékelő nem tudja megakadályozni, hogy a rosszindulatú forgalom elérje a célját. Az illegális érzékelőeszközök által végrehajtott válaszlépések esemény utáni válaszok, és gyakran más hálózati eszközök (például útválasztók és tűzfalak) segítségére van szükségük a támadások megválaszolásához. Az ilyen válaszlépések bizonyos típusú támadásokat megakadályozhatnak. Atomi támadások esetén azonban az egyetlen csomagnak megvan az esélye arra, hogy elérje a célrendszert, mielőtt a hibás alapú érzékelő végrehajthatna egy ACL-módosítást egy felügyelt eszközön (például tűzfalon, kapcsolón vagy útválasztón). Az ábrán a Switched Port Analyzer (SPAN) a gazdagépre belépő, odamenő és onnan érkező forgalom tükrözésére szolgál.

Az ábrán egy IDS érzékelő látható, amely promiscuous módban működik.

### Promiscuous mód

másolatait küldi A SPAN port a forgalom IDS-kompatibilis Sensor Management Server

Ahogy az alábbi ábrán is látható, a soron belüli üzemmódban az IPS közvetlenül a forgalomba kerül, és a késleltetés növelésével lelassítja a csomagtovábbítási sebességet. Az Inline mód lehetővé teszi, hogy az érzékelő leállítsa a támadásokat a rosszindulatú forgalom leállításával, mielőtt az elérné a kívánt célt, így védelmi szolgáltatást nyújt. A beépített eszköz nemcsak a 3. és 4. rétegen dolgozza fel az információkat, hanem a csomagok tartalmát és hasznos terhelését is elemzi a kifinomultabb beágyazott támadások érdekében (3-7. réteg). Ez a mélyebb elemzés lehetővé teszi a rendszer számára, hogy azonosítsa, leállítsa vagy blokkolja azokat a támadásokat, amelyek egy hagyományos tűzfalon keresztülhaladnának. Az IDS érzékelő beépíthető. Az IDS úgy van beállítva, hogy csak riasztásokat küldjön, és ne dobjon el semmilyen csomagot.

Az ábrán egy inline módban működő IPS érzékelő látható.

### Inline mód

IPS érzékelő

11.2.4

## Ellenőrizze megértését – Hasonlítsa össze az IDS- és az IPS-telepítést

Az űrlap teteje

Ellenőrizze, hogy érti-e az IDS-t és az IPS-t, és válassza ki a megfelelő választ a következő kérdésekre.

1. Igaz vagy hamis? A HIPS konfigurálható promiscuous vagy inline módban.

Az űrlap alja

Mi igaz az inline módban futó NIPS-ekre?

Mi igaz a HIPS-re?

Mi a példa a HIPS-re?

[11.1](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[IDS and IPS Characteristics](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[11.3](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[IPS on Cisco ISRs](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                          
*                     

1. IPS technológiák
2. IPS on Cisco ISRs

# IPS a Cisco ISR-eken

11.3.1

## IPS komponensek

Az IPS érzékelő két összetevőből áll:

* **IPS-észlelési és végrehajtási motor** – A forgalom ellenőrzése érdekében az észlelőmotor összehasonlítja a bejövő forgalmat az IPS-támadás-aláíró csomagban található ismert támadási aláírásokkal.
* **IPS-támadás-aláírások csomagja** – Ez az egy fájlban található ismert támadási aláírások listája. Az aláírási csomag gyakran frissül, amint új támadások észlelhetők. A rendszer elemzi a hálózati forgalmat, hogy talál-e egyezést ezeknek az aláírásoknak.

Amint az ábrán látható, a megvalósítható IPS észlelési és végrehajtási motor a router platformjától függ:

* **Cisco IOS Intrusion Prevention System (IPS)** – Ez a régebbi Cisco 800, 1900, 2900 és 3900 sorozatú ISR-eken érhető el. Az IOS IPS már nem támogatott, ezért nem szabad használni.
* **Cisco Snort IPS –** Ez elérhető a Cisco 4000 sorozatú ISR-eken és az 1000v sorozatú Cisco Cloud Services útválasztókon.

A Cisco Snort IPS hagyományos behatolásészlelést és -megelőzést biztosít azáltal, hogy összehasonlítja a hálózati forgalmat az ismert rosszindulatú programok és fenyegetésszignatúrák folyamatosan frissített adatbázisaival. A Cisco IOS IPS aláírásai már nem frissülnek.

Az ábra azt ábrázolja, hogy az iosips a Cisco 800, 1900, 2900 és 3900 sorozatú IS Rs-eken érhető el. Az ábra azt is mutatja, hogy a Snort ips elérhető a Cisco 4000 Series IS Rs és a Cisco Cloud Services útválasztókon az 1000v sorozatban

### Cisco IPS opciók

this is the image's alt text

**Cisco 800, 1900, 2900 és 3900 sorozatú ISR-ek Cisco 4000 sorozatú ISR-ek**

11.3.2

## Cisco IOS IPS

Az útválasztók IPS-ként való működésének engedélyezése költséghatékony módja a fiókirodai hálózatok védelmének. Ahelyett, hogy egy útválasztót és egy dedikált IPS-eszközt vásárolna, a funkciók egy eszközben történő kombinálása nemcsak pénzt takarít meg, hanem leegyszerűsíti a hálózattervezést és az adminisztrációt is.

A múltban a Cisco ISR-t IPS-érzékelőként engedélyezték, amely a csomagokat és a munkameneteket úgy vizsgálta, hogy megfeleljen a Cisco IOS IPS-aláírásainak. Az örökölt Cisco IOS IPS az ábrán látható módon RAM-ban működött. Ez azt jelenti, hogy megosztotta az eszköz memóriáját más Cisco IOS-szolgáltatásokkal.

Amikor a Cisco IOS IPS gyanús tevékenységet észlelt, reagált, mielőtt a hálózat biztonságát veszélyeztették volna. Az eseményt Cisco IOS rendszernapló-üzenetként vagy a Security Device Event Exchange (SDEE) segítségével naplózta.

A hálózati rendszergazda beállíthatja a Cisco IOS IPS-t úgy, hogy válassza ki a megfelelő választ a különféle fenyegetésekre. Például, ha egy munkamenetben lévő csomagok megegyeztek egy aláírással, a Cisco IOS IPS beállítható úgy, hogy a következőképpen válaszoljon:

* Küldjön riasztást egy syslog szerverre vagy egy központi felügyeleti felületre
* Dobd el a csomagot
* Állítsa vissza a kapcsolatot
* A fenyegetés forrás IP-címéről érkező forgalom tiltása meghatározott ideig
* Adott ideig letiltja a forgalmat azon a kapcsolaton, amelyhez az aláírást látták

Az ábra egy útválasztót ábrázol, amely azt jelzi, hogy az ios és az iosips a RAM-ban fut Cisco 800, 1900, 2900 és 3900 sorozatú IS Rs-en.

### Cisco IOS IPS

**RAM**   
• IOS   
• IOS IPS Cisco 800, 1900, 2900,   
és 3900-as sorozatú ISR-ek

11.3.3

## Snort IPS

A Cisco IOS IPS-t támogató eszközök közül sok már nem elérhető, vagy már nem támogatott. Az újabb Cisco 4000 Series Integrated Services Routers (ISR) már nem támogatja az IOS IPS-t. Ehelyett a Snort IPS funkció használatával IPS-szolgáltatásokat nyújtanak. A Snort IPS kiegészíti a 4000-es sorozat meglévő hálózati biztonsági funkcióit anélkül, hogy egy második készüléket kellene telepíteni a fióktelepeken.

A Snort a világ legszélesebb körben alkalmazott IPS-megoldása. Ez egy nyílt forráskódú hálózati IPS, amely valós idejű forgalomelemzést végez, és riasztásokat generál, ha fenyegetéseket észlelnek az IP-hálózatokon. Protokollelemzést, tartalomkeresést vagy egyeztetést is tud végezni, valamint számos támadást és vizsgálatot észlel, például puffertúlcsordulást, lopakodó port-ellenőrzést és így tovább.

A Snort motor egy virtuális szolgáltatástárolóban fut a Cisco 4000 sorozatú ISR-eken. A virtuális szolgáltatástároló egy virtuális gép, amely az ISR útválasztó operációs rendszeren fut. A szolgáltatástárolók olyan alkalmazások, amelyek közvetlenül a Cisco IOS XE útválasztási platformokon tárolhatók. Ezek az alkalmazások az IOS XE operációs rendszer Linux vonatkozásait használják a Linux Virtual Containers (LXC) és a Kernel virtuális gépek (KVM) hosztolására. A Snort tároló Open Virtualization Appliance (OVA) fájlként kerül terjesztésre, amely az útválasztóra van telepítve.

Az IOS IPS-től eltérően a Snort IPS felhasználhatja a szolgáltatástároló számítógépes teljesítményét a biztonság növelésére a platformmal anélkül, hogy ez befolyásolná az útválasztási képességeket vagy más adatsík-funkciókat. A virtuális szolgáltatás három erőforrásprofilt támogat, amelyek jelzik, hogy a Snort-tároló hogyan használja a rendszer CPU-t, RAM-ot és Flash- vagy lemezerőforrásokat.

Az ábra egy útválasztót ábrázol, amely azt jelzi, hogy a Snort konténer RAM-ban fut a Cisco 4000 sorozatú IS Rs ios rendszerével együtt.

### Snort IPS



**RAM**   
•IOS **Container** Cisco 4000 sorozatú ISR-ek

11.3.4

## Horkant művelet

A Snort IPS aláírásokat a Cisco Talos automatikusan eljuttatja az ISR-hez. Jelenleg több mint 30 000 aláírás található a Snort-szabálykészletben. Támogatja továbbá a szabálykészletek testreszabásának lehetőségét, és központi telepítési és kezelési lehetőségeket biztosít a 4000-es sorozatú ISR-ekhez.

A horkantást az alábbi módok egyikében lehet engedélyezni:

* **IDS mód** – A Snort ellenőrzi a forgalmat és riasztásokat jelent, de nem tesz semmit a támadások megelőzése érdekében.
* **IPS mód** – A behatolásészlelésen kívül a támadások megelőzésére is sor kerül.

A hálózati behatolásészlelés és -megelőzés módban a Snort a következő műveleteket hajtja végre:

* Figyeli a hálózati forgalmat, és egy meghatározott szabálykészlet alapján elemzi.
* Támadásosztályozást végez.
* Az egyező szabályokkal szembeni műveleteket hívja elő.

A Snort IPS figyeli a forgalmat, és jelenti az eseményeket egy külső naplószervernek vagy az IOS rendszernaplónak. Az IOS rendszernaplóba való naplózás engedélyezése hatással lehet a teljesítményre a naplóüzenetek lehetséges mennyisége miatt. A Snort-naplókat támogató külső, harmadik féltől származó megfigyelőeszközök használhatók a naplógyűjtéshez és -elemzéshez.

11.3.5

## Snort funkciók

A táblázat felsorolja a Snort IPS szolgáltatásait és előnyeit.

| **Funkció** | **Haszon** |
| --- | --- |
| Aláírás-alapú behatolás-érzékelő rendszer (IDS) és behatolás-megelőzési rendszer (IPS) | A Snort nyílt forráskódú IPS, amely képes valós idejű forgalomelemzésre és csomagnaplózásra az IP-hálózatokon, a 4000-es sorozatú ISR szolgáltatástárolón fut anélkül, hogy további eszközt kellene telepítenie a fióktelepen. |
| Snort szabálykészlet frissítései | A Snort szabálykészlet frissítéseit a 4000-es sorozatú ISR-ekhez a Cisco Talos, a vezető hálózatbiztonsági szakértőkből álló csoport hozza létre, akik éjjel-nappal dolgoznak, hogy proaktívan felfedezzék, értékeljék és reagáljanak a legfrissebb trendekre a hackelési tevékenységek, a behatolási kísérletek, a rosszindulatú programok és a rosszindulatú programok terén. sebezhetőségek. |
| Snort rule set pull | Az útválasztó egyszeri parancsok vagy rendszeres automatizált frissítések segítségével közvetlenül a cisco.com vagy a snort.org webhelyről töltheti le a szabálykészleteket a helyi szerverre. |
| Snort rule set push | A központosított felügyeleti eszköz előre konfigurált házirend alapján tudja lenyomni a szabálykészleteket, ahelyett, hogy az útválasztó közvetlenül letöltené magát. |
| Aláírás engedélyezett listázás | Az engedélyezett listázás lehetővé teszi bizonyos aláírások letiltását a szabálykészletből. A letiltott aláírások bármikor újra engedélyezhetők. |

11.3.6

## Snort rendszerkövetelmények

A szolgáltatástároló infrastruktúra IDS/IPS funkcióval történő futtatásához a Snort IPS ISR 4000-re (azaz 4300-ra vagy magasabbra) minimum 8 GB memóriával (DRAM) és 8 GB vakuval rendelkezik.

Megjegyzés: A Cisco 4200 sorozatú ISR nem támogatja az alapértelmezett Snort IPS megvalósítást.

A Snort IPS funkció aktiválásához biztonsági K9-licenc (SEC) szükséges. Az ügyfeleknek éves előfizetést is kell vásárolniuk a cisco.com oldalon terjesztett aláírási csomagra. A legújabb fenyegetések elleni védelem érdekében a Snort-szabálykészletek időalapú előfizetések, amelyek egy vagy három évig állnak rendelkezésre.

A határidő alapú előfizetések két típusa létezik:

* **Közösségi szabálykészlet** – Ez a készlet korlátozott lefedettséget kínál a fenyegetések ellen, a biztonsági fenyegetésekre adott reakcióra összpontosítva a proaktív kutatási munkával szemben. A közösségi szabálykészletben lévő frissített aláírásokhoz 30 napos késéssel fér hozzá, és ez az előfizetés nem jogosítja fel az ügyfelet a Cisco támogatására.
* **Előfizetői szabálykészlet** – Ez a készlet kínálja a legjobb védelmet a fenyegetésekkel szemben. Tartalmazza a Cisco Talos biztonsági szakértőinek kutatómunkájának felhasználásával a kizsákmányolás előtti lefedettséget. Az előfizetői szabálykészlet biztosítja a leggyorsabb hozzáférést a frissített aláírásokhoz egy biztonsági incidens vagy egy új fenyegetés proaktív felfedezése esetén. Ezt az előfizetést a Cisco teljes mértékben támogatja.

A PulledPork egy szabálykezelő alkalmazás, amely a Snort-szabályfrissítések automatikus letöltésére használható. A PulledPork használatához be kell szereznie egy engedélyezési kódot, az úgynevezett oinkcode-ot a snort.org fiókjából. Az oinkkód regisztrációval ingyenes.

11.3.7

## Ellenőrizze, hogy megértette – IPS a Cisco ISR-eken

Az űrlap teteje

Ellenőrizze, hogy megértette-e a Snort on Cisco ISR-eket a következő kérdések megválaszolásával.

1. Melyik router platformon érhető el a Snort IPS?

Az űrlap alja

Hol működik a Snort motor?

Melyik üzemmódban vizsgálja a Snort IDS a forgalmat és jelenti a riasztásokat, de nem tesz semmit a támadások megelőzésére?

[11.2](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[IPS Implementations](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[11.4](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Cisco Switched Port Analyzer](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                              
*                     

1. IPS technológiák
2. Cisco Switched Port Analyzer

# Cisco kapcsolt port analizátor

11.4.1

## Hálózatfigyelési módszerek

A hálózat mindennapi működése a forgalom, a sávszélesség-használat és az erőforrás-hozzáférés közös mintáiból áll. Ezek a minták együtt a normál hálózati viselkedést azonosítják. A biztonsági elemzőknek alaposan ismerniük kell a normál hálózati viselkedést, mert a rendellenes hálózati viselkedés általában problémát jelez.

A normál hálózati viselkedés meghatározásához hálózati megfigyelést kell megvalósítani. Különféle eszközöket használnak a normál hálózati viselkedés felfedezéséhez, beleértve az IDS-t, a csomagelemzőket, az SNMP-t, a NetFlow-t és másokat.

Ezen eszközök némelyike ​​rögzített hálózati adatokat igényel. Két általános módszer létezik a forgalom rögzítésére és a hálózati megfigyelő eszközökre való elküldésére:

* Hálózati érintések, más néven teszt hozzáférési pontok (TAP)
* Forgalomtükrözés a Switch Port Analyzer (SPAN) vagy más porttükrözési módszerekkel

11.4.2

## Hálózati érintések

A hálózati leágazás tipikusan egy passzív elosztó eszköz, amely egy adott eszköz és a hálózat között van beépítve. Az érintés az összes forgalmat, beleértve a fizikai réteghibákat is, egy elemzőeszközre továbbítja, miközben lehetővé teszi, hogy a forgalom elérje a kívánt célt.

Az ábra egy mintatopológiát mutat be, amely egy hálózati tűzfal és a belső útválasztó közé telepített csapot jelenít meg.

A kép egy hálózati diagram, amely a tűzfal és az útválasztó között elhelyezett hálózati csapot mutat be. A csap egy harmadik porton csatlakoztatott felügyeleti eszközhöz is csatlakozik.

Internet belső hálózatok belső útválasztó tűzfal RX adatfolyam TX adatfolyam hálózat érintés figyelő eszköz

Figyelje meg, hogy a csap egyszerre küldi el a belső útválasztó adási (TX) adatfolyamát és a vételi (RX) adatfolyamot a belső útválasztónak külön dedikált csatornákon. Ez biztosítja, hogy minden adat valós időben érkezzen a felügyeleti eszközhöz. Ezért a kapcsolat figyelése nem befolyásolja vagy rontja a hálózati teljesítményt.

A leágazások általában hibamentesek is, ami azt jelenti, hogy ha egy csap meghibásodik vagy áramszünet, a tűzfal és a belső útválasztó közötti forgalmat ez nem érinti.

Keressen az interneten a réz UTP Ethernet, üvegszálas Ethernet és soros kapcsolatok NetScout Taps-járól.

11.4.3

## Traffic Mirroring és SPAN

A hálózati kapcsolók tervezésük szerint szegmentálják a hálózatot. Ez korlátozza a hálózatfigyelő eszközök számára látható forgalom mennyiségét. Mivel a hálózati megfigyeléshez szükséges adatok rögzítéséhez az összes forgalom rögzítése szükséges, speciális technikákat kell alkalmazni a hálózati kapcsolók által előírt hálózati szegmentáció megkerülésére. A porttükrözés az egyik ilyen technika. A számos vállalati kapcsoló által támogatott porttükrözés lehetővé teszi a kapcsoló számára, hogy az egy vagy több porton fogadott kereteket egy elemzőeszközhöz csatlakoztatott Switch Port Analyzer (SPAN) portra másolja.

A táblázat azonosítja és leírja a SPAN szolgáltatás által használt kifejezéseket.

| **SPAN Term** | **Leírás** |
| --- | --- |
| **Belépő forgalom** | A váltóba belépő forgalom. |
| **Kilépő forgalom** | A váltót elhagyó forgalom. |
| **Forrás (SPAN) port** | A forrásportokat a rendszer figyeli, amint a bejövő forgalom replikálódik (tükröződik) a célportokhoz. |
| **Cél (SPAN) port** | A forrásportokat tükröző port. A cél SPAN portok gyakran csatlakoznak elemző eszközökhöz, például csomagelemzőhöz vagy IDS-hez. |

Az ábrán egy kapcsoló látható, amely összeköt két gazdagépet, és tükrözi a forgalmat egy behatolásérzékelő eszközhöz (IDS) és a hálózatkezelő szerverhez.

A hálózati diagram egy, a hálózatban elhelyezett kapcsolót mutat be, két forrás SPAN porttal és egyetlen cél SPAN porttal.

### SPAN

F0/1 F0/2

G0/1

SPAN port küldi a forgalom másolatait IDS Sensor Management Server Ingress Traffic Egress Traffic Source SPAN Port Source SPAN Port Destination SPAN Port

A kapcsoló továbbítja a bejövő forgalmat az F0/1-en és a kimenő forgalmat az F0/2-n az IDS-hez csatlakozó G0/1 cél SPAN-portra.

A forrásportok és a célportok közötti társítást SPAN szekciónak nevezik. Egy munkamenetben egy vagy több port figyelhető meg. Egyes Cisco kapcsolókon a munkamenet forgalma egynél több célportra is átmásolható. Alternatív megoldásként megadható egy forrás VLAN, amelyben a forrás VLAN összes portja a SPAN forgalom forrásává válik. Minden SPAN-munkamenet tartalmazhat portokat vagy VLAN-okat forrásként, de mindkettőt nem.

**Megjegyzés** : A SPAN Remote SPAN (RSPAN) nevű változata lehetővé teszi a hálózati adminisztrátor számára, hogy a VLAN-ok rugalmasságát kihasználva figyelje a távoli kapcsolókon zajló forgalmat.

11.4.4

## A Cisco SPAN beállítása

A Cisco kapcsolók SPAN szolgáltatása a forrásporton belépő minden egyes keret másolatát elküldi a célporton keresztül a csomagelemző vagy az IDS felé.

A SPAN-munkamenet azonosítására egy munkamenetszám szolgál. A példák a **monitor session** parancsot mutatják be, amely a forrásport és a célport SPAN-munkamenethez való társítására szolgál. Minden munkamenethez külön **monitor session** parancsot használunk. Fizikai port helyett VLAN is megadható.

Switch(config)#  **monitor**  munkamenetszám  **forrás**  [  **interfész**  interfész |  **vlan**  vlan ]

Switch(config)#  **monitor munkamenetszám**  rendeltetési  **hely**  [  **interfész**  interfész |  **vlan**  vlan ]

Az alábbi ábrán a PCA az F0/1-hez, az IDS pedig az F0/2-hez csatlakozik. A cél a PCA által az F0/1-es porton küldött vagy fogadott összes forgalom rögzítése, és ezeknek a kereteknek egy másolatának elküldése az F0/2-es porton lévő IDS-nek (vagy csomagelemzőnek). A kapcsoló SPAN szekciója átmásolja az F0/1 forrásporton küldött és fogadott összes forgalmat az F0/2 célportra.

Az ábra a span portot mutatja, amely a forgalom másolatait küldi a kapcsolóról egy azonosító érzékelőre vagy egy csomaganalizátorra.

### Cisco SPAN konfiguráció

S1 F0/1

F0/2

PCA Packet Analyzer IDS érzékelő vagy SPAN port, amely másolatokat küld a forgalomról

S1(config)# **monitor session 1 source interface fastethernet 0/1**

S1(config)# **monitor session 1 destination interface fastethernet 0/2**

A **show monitor** parancs a SPAN szekció ellenőrzésére szolgál. A parancs megjeleníti a munkamenet típusát, az egyes forgalmi irányok forrásportjait és a célportot. Az alábbi példában a munkamenet száma 1, a forrásport mindkét forgalmi irányhoz F0/1, a célport pedig F0/2. A bemeneti SPAN le van tiltva a célporton, így csak a célportot elhagyó forgalom lesz másolva arra a portra.

S1# **show monitor**

Session 1

---------

Type : Local Session

Source Ports :

Both : Fa0/1

Destination Ports : Fa0/2

Encapsulation : Native

Ingress : Disabled

S1#

**Megjegyzés** : A Remote SPAN (RSPAN) akkor használható, ha a csomagelemző vagy az IDS más kapcsolón van, mint a figyelt forgalom. Az RSPAN kiterjeszti a SPAN-t azáltal, hogy lehetővé teszi több kapcsoló távoli felügyeletét a hálózaton keresztül. Az egyes RSPAN-munkamenetek forgalma egy felhasználó által megadott RSPAN VLAN-on keresztül történik, amely dedikált (az RSPAN-munkamenethez) az összes résztvevő kapcsolóban.

11.4.5

## Szintaxis-ellenőrző – A SPAN konfigurálása és ellenőrzése

Ezzel a szintaktikai ellenőrzővel konfigurálhatja és ellenőrizheti a SPAN-t.

Complete the following steps to configure SPAN on S1:

* Enter global configuration mode.
* Issue the SPAN command to monitor the traffic on source port **fastethernet 0/1**. Use 1 for the session number.
* Capture the session 1 monitored traffic on destination port **fastethernet 0/2**.
* Exit global configuration mode.

S1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)#monitor session 1 source interface fastethernet 0/1

S1(config)#monitor session 1 destination interface fastethernet 0/2

S1(config)#exit

\*Mar 1 00:19:53.908: %SYS-5-CONFIG\_I: Configured from console by console

S1#

Verify that SPAN has been configured to monitor source port F0/1 with captured traffic being sent to F0/2.

S1#show monitor

1. munkamenet

---------

Típus: Helyi munkamenet

Forrás portok:

Mindkettő: Fa0/1

Cél portok: Fa0/2

Tokozás: Natív

Belépés: Letiltva

S1#

Sikeresen konfigurálta és ellenőrizte a SPAN-t.

11.4.6

## Packet Tracer – Helyi SPAN megvalósítása

Ebben a laborban a következő célokat kell teljesítenie:

* 1. rész: Hálózatépítés és kapcsolat ellenőrzése
* 2. rész: A helyi SPAN konfigurálása és a másolt forgalom rögzítése a Wireshark segítségével

[Helyi SPAN megvalósítása](https://contenthub.netacad.com/courses/netsec/_common/11.4.6-packet-tracer---implement-a-local-span.pka)

[11.3](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[IPS on Cisco ISRs](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[11.5](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[IPS Technologies Summary](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                   

1. IPS technológiák
2. IPS Technologies Summary

# IPS Technologies Összefoglaló

11.5.1

## Mit tanultam ebben a modulban?

**IDS és IPS jellemzők**   
A rosszindulatú programok egyre nagyobb veszélyt jelentenek a hálózat biztonságára. Naponta történnek új hálózati támadások. A fenyegetettség területe folyamatosan változik. A hálózati naplók figyelése az egyik módja annak, hogy megtudjuk, hogy visszaélés történt. De addigra már késő. Az IDS és az IPS a hálózatbiztonság többrétegű megközelítésének részét képezik. Az IDS offline módban működik a rosszindulatú forgalom észlelése érdekében a forgalom tükrözésén keresztül. Az IDS figyelmeztetheti a biztonsági személyzetet egy lehetséges támadásról. Bár az IDS semmit sem tesz a hálózati támadások megállítására, nincs hatással a hálózat teljesítményére. Az IPS-eszközök soron belül működnek a hálózati támadások megelőzése érdekében, azonban késleltetést és lelassíthatják a hálózati teljesítményt. Az IDS és IPS eszközök lehetnek IPS szoftverrel felszerelt útválasztók, dedikált eszközök vagy adaptív biztonsági berendezésekbe, kapcsolókba vagy útválasztókba telepített hardvermodulok.

**IPS megvalósítások**   
A behatolásgátló rendszerek lehetnek gazdagép- vagy hálózatalapúak. A HIPS-ek a hálózati gazdagépekre vannak telepítve. Figyelemmel kísérik a gazdagépen végzett tevékenységeket, megakadályozhatják a támadásokat és naplózhatják a gyanús tevékenységeket. A HIPS olyan, mint a kártevőirtó és a tűzfalszoftver kombinációja. A HIPS-eknek többnyire helyi nézetük van a hálózatról, és csak akkor jelentenek hatékony megoldást, ha minden gazdagépen használják. Ezen túlmenően ezek nem lehetnek az egyetlen biztonsági intézkedés a hálózatban, hanem csak egy biztonsági réteg.

A NIPS megvalósítható dedikált eszközzel vagy IPS szoftverrel ellátott routerrel. A hálózati alapú IPS valós időben blokkolja a rosszindulatú szoftvereket és a hálózati támadásokat. A hálózat alapú IPS két módban telepíthető. Promiscuous módban IDS-ként működnek a tükrözött forgalom figyelésével. Bár nem tudják megállítani a hálózati támadásokat, figyelmeztethetik a személyzetet és naplózhatják az információkat, ha támadások történnek. A beépített módú IPS feldolgozza a hálózatba érkező összes forgalmat, és ellenőrzi a 3–7. rétegbeli forgalmat. Az IPS a hálózati forgalom által szállított hasznos terhek, például az e-mail mellékletek tartalmát is ellenőrizheti. Mivel a beépített mód az IPS-t közvetlenül a forgalomba helyezi, a késleltetés növelésével lelassítja a csomagtovábbítási sebességet. Az Inline mód lehetővé teszi, hogy az érzékelő leállítsa a támadásokat a rosszindulatú forgalom leállításával, mielőtt az elérné a kívánt célt.

**IPS a Cisco ISR-eken**   
Az IPS funkció engedélyezése az útválasztókon fiókszinten költséghatékony módja a hálózatok egyetlen eszközzel történő védelmének. Az IPS észlelési és végrehajtási motorja, amely a régi útválasztó platformokon futott, a Cisco IOS IPS volt. A Cisco IOS IPS azonban már nem támogatott. A 4000-es sorozatú ISR esetében a Cisco Snort IPS váltotta fel az IOS IPS-t. A Snort egy virtuális tárolóban fut az útválasztó hardverén. Az IPS funkció nincs hatással az útválasztó forgalomtovábbítási funkcióira. Amikor IPS-ként fut, a Snort figyeli a hálózati forgalmat, és egy meghatározott szabálykészlet alapján elemzi azt. A Snort típus szerint osztályozhatja a támadásokat, és olyan műveleteket hajthat végre a forgalom ellen, mint például riasztások küldése, események naplózása, valamint a forgalom elleni fellépés, ha a támadási szignatúrák megegyeznek. A Snort beállítható úgy, hogy automatikusan frissítse a szabályait olyan internetes forrásokból, mint a Cisco vagy a snort.org. A problémás aláírások letilthatók, és egyéni szabályok hozhatók létre. A Snortot 4300 ISR vagy annál magasabb sebességgel tervezték futtatni. A működéséhez 8 GB DRAM és 8 GB Flash szükséges. Az erőforrásprofilok konfigurálhatók annak szabályozására, hogy a Snort hogyan használja fel az ISR rendszererőforrásait.

**Cisco kapcsolt port analizátor**   
A SPAN egy olyan technológia, amely lehetővé teszi a hálózatfigyelést és az IDS-t szegmentált hálózatokban. A hálózati forgalom tükröződik a forrásportoktól vagy VLAN-októl a megfigyelőeszközhöz vagy IDS-hez csatlakoztatott célportra vagy VLAN-ra. A forrásportokról érkező forgalom átmásolódik és a célportra kerül. A kapcsolóba belépő forgalmat bemenő forgalomnak, a kapcsolóból kilépő forgalmat pedig kilépő forgalomnak nevezzük. A forrásportok továbbítják a figyelni kívánt forgalmat, a célportok pedig a megfigyelő eszközökhöz csatlakoznak. A figyelt forgalom másolása és kiküldése a célporton keresztül történik. A SPAN konfigurációja magában foglalja a forrás és a cél kapcsolóportok meghatározását.

11.5.2

## 11. modul – IPS-technológiák kvíz

Az űrlap teteje

1. Mi az IPS aláírás?

Az űrlap alja

Melyik hálózati technológia használ passzív felosztó eszközt, amely az összes forgalmat, beleértve az 1. rétegbeli hibákat is, egy elemzőeszközre továbbítja?

Mi a jellemzője az inline üzemmódban működő IPS- nek ?

Mi az a nulladik napi támadás?

Mi az IPS jellemzője?

Melyik hálózatfigyelő technológia figyeli passzívan a hálózati forgalmat a támadások észlelése érdekében?

Melyik nyílt forráskódú hálózatfigyelő technológia végez valós idejű forgalomelemzést, és riasztásokat generál, ha fenyegetéseket észlelnek az IP-hálózatokon?

Melyik Cisco platform támogatja a Cisco Snort IPS-t?

Melyik eszköz támogatja a SPAN használatát a rosszindulatú tevékenységek megfigyelésére?

Mi az a gazdagép alapú behatolásérzékelő rendszer (HIDS)?

Milyen hálózatfelügyeleti képességet biztosít a SPAN használata?

Milyen hálózatfigyelő eszközzel lehet átmásolni az egyik porton áthaladó csomagokat, és átküldeni ezeket a másolatokat egy másik portra elemzés céljából?

[11.4](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Cisco Switched Port Analyzer](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[12.0](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                         
*                   

1. IPS Operation and Implementation
2. Introduction

# Bevezetés

12.0.1

## Miért vegyem ezt a modult?

A hálózati architektúra paradigmaváltására van szükség a gyorsan mozgó és fejlődő támadások elleni védekezéshez. Ennek tartalmaznia kell a költséghatékony észlelési és megelőzési rendszereket, mint például a behatolásérzékelő rendszereket (IDS) vagy a jobban skálázható behatolásgátló rendszereket (IPS). A hálózati architektúra ezeket a megoldásokat integrálja a hálózat belépési és kilépési pontjaiba.

Az IDS vagy IPS implementálásakor fontos ismerni a rendelkezésre álló IPS-rendszerek típusait, az aláírási kategóriák szerepét és a lehetséges műveleteket, amelyeket a Cisco IOS útválasztó támadás észlelésekor megtehet.

A modul első része a hagyományos IPS aláírásokat és riasztásokat vizsgálja. A modul további része a Snort IPS-t tárgyalja, amely 4000-es sorozatú ISR-eszközökön fut.

12.0.2

## Mit fogok tanulni ebben a modulban?

**Modul címe:** IPS működés és megvalósítás

**Modul célja** : Magyarázza el, hogyan használják az aláírásokat a rosszindulatú hálózati forgalom észlelésére.

| **téma címe** | **Téma Cél** |
| --- | --- |
| **IPS aláírások** | Ismertesse az IPS aláírásokat. |
| **Cisco Snort IPS** | Magyarázza el, hogy a Cisco Snort IPS hogyan nyújt hálózati biztonsági szolgáltatásokat. |
| **Konfigurálja a Snort IPS-t** | Ismertesse a Snort IPS konfigurálását Cisco ISR G2-n. |

[11.5](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[IPS Technologies Summary](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[12.1](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[IPS Signatures](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                             
*                   

1. IPS Operation and Implementation
2. IPS Signatures

# IPS aláírások

12.1.1

## IPS aláírás attribútumok

A hálózatnak képesnek kell lennie a bejövő rosszindulatú forgalom azonosítására, hogy megállítsa azt. Szerencsére a rosszindulatú forgalom eltérő jellemzőket vagy „aláírásokat” mutat.

fájlhoz hasonló elvileg **A víruskeresők által használt virus.dat** az aláírás olyan szabálykészlet, amelyet az IDS és az IPS használ a tipikus behatolási tevékenységek észlelésére. Az aláírások egyedileg azonosítanak bizonyos vírusokat, férgeket, protokoll-rendellenességeket és rosszindulatú forgalmat (pl. DoS-támadásokat).

A rosszindulatú csomagfolyamatok meghatározott típusú tevékenységgel és aláírással rendelkeznek. Az IPS-érzékelőket úgy kell beállítani, hogy keressenek egyező aláírásokat vagy abnormális forgalmi mintákat. Miközben az érzékelők átvizsgálják a hálózati csomagokat, aláírásokat használnak az ismert támadások észlelésére, és előre meghatározott műveletekkel válaszolnak. Az IDS vagy IPS érzékelő számos különböző aláírás segítségével vizsgálja az adatfolyamot. Az érzékelő akkor lép működésbe, ha egy aláírást egyeztet egy adatfolyammal, például naplózza az eseményt, vagy riasztást küld az IDS vagy IPS kezelőszoftvernek.

Az aláírásoknak három megkülönböztető tulajdonsága is van:

* **Típus** - Atom vagy kompozit
* **Trigger** – Riasztásnak is nevezik
* **Művelet** – Mit fog tenni az IPS

12.1.2

## Az aláírások típusai

Egyes fenyegetések egy csomagban azonosíthatók, míg más fenyegetésekhez sok csomagra és állapotinformációira (pl. IP-címekre, portszámokra stb.) lehet szükség a fenyegetés azonosításához.

Kétféle aláírás létezik:

* **Atomic Signature –** Ez a legegyszerűbb aláírástípus, mivel egyetlen csomag, tevékenység vagy esemény azonosítja a támadást. Az IPS-nek nem kell állapotinformációkat karbantartania, és a forgalomelemzés általában nagyon gyorsan és hatékonyan elvégezhető.
* **Összetett aláírás –** Állapottartó aláírásnak is nevezik, mivel az IPS-nek több adatra van szüksége ahhoz, hogy megfeleljen egy támadási aláírásnak. Az IPS-nek állapotinformációkat is fenn kell tartania, amelyeket eseményhorizontnak nevezünk. Az eseményhorizont hossza aláírásonként változik.

12.1.3

## IPS Signature Riasztások

Bármely IPS-aláírás szíve az aláírás-riasztás, amelyet gyakran aláírásindítónak is neveznek. Az IPS érzékelő aláírási riasztása (vagyis triggerje) bármi lehet, ami megbízhatóan jelezheti a behatolást vagy a biztonsági szabályzat megsértését. A hálózati alapú IPS például aláírási műveletet indíthat el, ha például egy adott karakterláncot tartalmazó hasznos adatot tartalmazó csomagot észlel, amely egy adott TCP-portra megy.

Az IPS aláírási riasztás hasonló az otthoni biztonsági rendszer riasztásához. A betörésjelző kioldó mechanizmusa egy mozgásérzékelő lehet. Ha a betörő riasztó be van kapcsolva, a rendszer érzékeli a helyiségbe belépő egyén mozgását. Ez elindítja a riasztást.

Ezek a kiváltó mechanizmusok alkalmazhatók atomi és kompozit aláírásokra. A kiváltó mechanizmusok lehetnek egyszerűek vagy összetettek. Minden IPS tartalmaz olyan aláírásokat, amelyek ezen alapvető aktiválási mechanizmusok közül egyet vagy többet használnak az aláírási műveletek elindításához.

A táblázatban felsoroltak szerint négy általános IPS-aláírás-indító kategória létezik.

| **Észlelés típusa** | **Előnyök** |
| --- | --- |
| **Minta alapú észlelés** | * Más néven aláírás-alapú észlelés. * A legegyszerűbb kiváltó mechanizmus, mivel egy meghatározott és előre meghatározott atomi vagy összetett mintát keres. * Az IPS-érzékelő összehasonlítja a hálózati forgalmat az ismert támadások adatbázisával, és riasztást vált ki, vagy megakadályozza a kommunikációt, ha egyezést talál. |
| **Anomália alapú észlelés** | * Más néven profil alapú észlelés. * Először meg kell határozni a normál hálózati vagy gazdagép tevékenység profilját. * Ezt a normál profilt általában a forgalom figyelésével és egy alapvonal megállapításával határozzák meg. * A definiálást követően a normál profilban meghatározott küszöbértéket meghaladó tevékenységek aláírási triggert és műveletet generálnak. |
| **Házirend-alapú észlelés** | * Más néven viselkedés alapú észlelés. * Bár hasonló a mintaalapú észleléshez, a rendszergazda manuálisan határozza meg a gyanús viselkedéseket az előzmények elemzése alapján. * A viselkedések használata lehetővé teszi, hogy egyetlen aláírás lefedje a tevékenységek egész osztályát anélkül, hogy minden egyes helyzetet meg kellene határoznia. |
| **Mézes edény alapú észlelés** | * A mézesedény-alapú észlelés egy szervert használ csaliszerverként a támadások vonzására. * A csaliszerverek célja a támadások elcsábítása a termelési eszközökről. * Lehetővé teszi az adminisztrátorok számára a bejövő támadások és rosszindulatú forgalmi minták elemzését az érzékelő aláírásainak hangolásához. |

12.1.4

## IPS aláírási műveletek

Amikor egy aláírás észleli azt a tevékenységet, amelyhez be van állítva, az aláírás egy vagy több műveletet indít el.

Az IPS érzékelőtől függően különféle műveletek engedélyezhetők. A táblázat felsorol néhány műveletet, amelyeket az IPS-érzékelők végezhetnek.

**Megjegyzés:** Az elérhető műveletek az aláírás típusától és a platformtól függenek.

| **Figyelmeztetési kategória** | **Konkrét művelet** | **Leírás** |
| --- | --- | --- |
| Hozzon létre egy figyelmeztetést | Készítsen riasztást | Az IPS riasztásként küldi el az eseményeket. |
| Bőbeszédű figyelmeztetés létrehozása | Az IPS részletes eseményriasztást küld. |
| A tevékenység naplózása | Támadócsomagok naplózása | Naplózza a csomagokat a támadó IP-címéről, és riasztást küld. |
| Napló pár csomagok | Naplózza a csomagokat az áldozat és a támadó IP-címéről, és riasztást küld. |
| Naplózni az áldozatcsomagokat | Naplózza a csomagokat az áldozat IP-címéről, és riasztást küld. |
| A tevékenység tagadása | Inline csomag elutasítása | Leállítja a csomagot. |
| Inline kapcsolat megtagadása | Leállítja az aktuális és a jövőbeli csomagokat ezen a TCP-folyamon. |
| Inline támadó tagadása | Leállítja az aktuális és a jövőbeli csomagokat erről a támadócímről egy adott időtartamra. |
| Állítsa vissza a TCP-kapcsolatot | TCP kapcsolat alaphelyzetbe állítása | TCP-visszaállításokat küld a TCP-folyamat eltérítéséhez és leállításához. |
| Jövőbeli tevékenység blokkolása | Blokkkapcsolat kérése | Kérelmet küld egy blokkoló eszköznek, hogy blokkolja ezt a kapcsolatot. |
| A gazdagép letiltásának kérése | Kérelmet küld egy blokkoló eszköznek, hogy blokkolja ezt a támadó gazdagépet. |
| SNMP trap kérése | Kérelmet küld az érzékelő értesítési alkalmazás összetevőjének az SNMP értesítés végrehajtására. |

12.1.5

## Figyelmeztetések kiértékelése

A kiváltó mechanizmusok téves pozitív vagy hamis negatív riasztásokat generálhatnak. Ezekkel a riasztásokkal foglalkozni kell az IPS-érzékelő alkalmazásakor. Kívánatosak az igazi pozitívumok és a valódi negatívumok, és azt jelzik, hogy az IPS megfelelően működik. A hamis pozitív és hamis negatív eredmények nem kívánatosak, és ki kell vizsgálni őket.

A táblázat a következő négy riasztástípust foglalja össze:

| **Riasztás típusa** | **Hálózati tevékenység** | **IPS tevékenység** | **Eredmény** |
| --- | --- | --- | --- |
| **Igaz pozitív** | Forgalom megtámadása | Riasztás generálva | Ideális beállítás |
| **Igaz negatív** | Normál felhasználói forgalom | Nincs riasztás generálva | Ideális beállítás |
| **Álpozitív** | Normál felhasználói forgalom | Riasztás generálva | Hangolja be az ébresztőt |
| **Hamis negatív** | Forgalom megtámadása | Nincs riasztás generálva | Hangolja be az ébresztőt |

A riasztások az alábbiak szerint osztályozhatók:

* **Igaz pozitív** – (Kívánatos) Ez akkor használatos, ha az IPS riasztást generál, mert ismert támadási forgalmat észlelt. A riasztás tényleges biztonsági incidensnek bizonyult, és azt is jelzi, hogy az IPS szabály megfelelően működött.
* **Igaz negatív** – (Kívánatos) Ez akkor használatos, ha a rendszer a várt módon működik. Nem adnak ki riasztást, mert a rendszeren áthaladó forgalom mentes a fenyegetésektől.
* **Hamis pozitív** – (Nem kívánatos) Ez akkor használatos, ha az IPS riasztást generál a normál felhasználói forgalom feldolgozása után, amelynek nem kellett volna riasztást kiváltania. Az IPS-t be kell hangolni, hogy ezeket a riasztástípusokat valódi negatívra változtassa. A riasztás nem jelez tényleges biztonsági eseményt. A hamis pozitív eredményt eredményező jóindulatú tevékenységet néha jóindulatú triggernek nevezik. A hamis pozitív eredmények költségesek, mert ki kell vizsgálni őket.
* **Hamis negatív** – (Veszélyes) Ez akkor használatos, ha az IPS nem generál riasztást, és a rendszer nem észlel ismert támadásokat. Ez azt jelenti, hogy a kihasználtságokat nem észlelik a működő biztonsági rendszerek. Ezek az események hosszú ideig észrevétlenek maradhatnak, és folyamatos adatvesztést és -károsodást okozhatnak. A cél az, hogy ezek a riasztástípusok valódi pozitív riasztásokat generáljanak.

12.1.6

## Ellenőrizze megértését – IPS aláírási műveletek

Az űrlap teteje

Ellenőrizze, hogy megértette-e az IPS-aláírási műveleteket, és válassza ki a megfelelő választ a következő kérdésekre.

1. Melyik művelet naplózza az IP-címet csak rosszindulatú forrásból, és küld riasztást?

Az űrlap alja

Melyik művelet zár le csak egy rosszindulatú csomagot?

Melyik művelet készteti arra, hogy az IPS-eszköz TCP-visszaállításokat küldjön a TCP-folyamat eltérítéséhez és leállításához?

[12.0](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[12.2](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Cisco Snort IPS](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                     
*                   

1. IPS Operation and Implementation
2. Cisco Snort IPS

# Cisco Snort IPS

12.2.1

## IPS szolgáltatási lehetőségek

A behatolásmegelőzési szolgáltatások a Cisco IOS IPS-t használó első generációs Integrated Services Routereken (ISR G1) voltak elérhetők. A Cisco IOS IPS úgy figyelte és akadályozta meg a behatolásokat, hogy összehasonlította a forgalmat az ismert fenyegetések aláírásaival, és fenyegetés észlelésekor blokkolta a forgalmat.

**Megjegyzés** : A Cisco IOS IPS támogatása 2018-ban megszűnt. Ezért az IOS IPS már nem ajánlott a fiókos útválasztókon.

A szervezeteknek most három lehetőségük van a behatolásmegelőzési szolgáltatások nyújtására.

* **Cisco Firepower Next-Generation IPS (NGIPS)** – Ezek olyan dedikált beépített fenyegetés-megelőzési eszközök, amelyek iparágvezető hatékonyságot biztosítanak az ismert és ismeretlen fenyegetésekkel szemben.
* **Cisco Snort IPS** – Ez egy IPS-szolgáltatás, amely egy második generációs ISR-en (ISR G2) (azaz ISR 4000-en) engedélyezhető. Vegye figyelembe, hogy a Cisco 4000 ISR-ek már nem támogatják a Cisco IOS IPS-t.
* **Külső Snort IPS-kiszolgáló** – Ez hasonló a Cisco Snort IPS-megoldásához, de szükség van egy egyszerű portra (azaz egy SPAN switch-portra) és egy külső Snort IDS/IPS-re.

Mindhárom IPS-szolgáltatás Snortot használ, és szabályfrissítéseket kap a Cisco Talostól.

12.2.2

## IPS

Az NGIPS-ek dedikált IPS-készülékek. A Snort alapvető nyílt technológiájára épülnek, és a sebezhetőségre összpontosító IPS-szabályokat, valamint a Cisco Talos által biztosított beágyazott IP-, URL- és DNS-alapú biztonsági intelligenciákat használnak.

Az NGIPS szolgáltatásai a következők:

* IPS-szabályok, amelyek azonosítják és blokkolják a hálózati sebezhetőségeket célzó támadási forgalmat.
* Szorosan integrált védelem a fejlett rosszindulatú programok ellen a hálózati és végponti tevékenységek fejlett elemzésével.
* Sandbox technológia, amely viselkedési mutatók százait használja a nulladik napi és az elkerülő támadások azonosítására.
* Tartalmazza továbbá az Alkalmazások láthatóságát és vezérlését (AVC), a Cisco Advanced Malware Protection (AMP) hálózatokhoz és az URL-szűrőt.

**Megjegyzés** : Az NGIPS készülékek további tárgyalása nem tartozik a kurzus hatókörébe.

12.2.3

## Snort IPS

A Snort egy nyílt forráskódú hálózati IPS, amely valós idejű forgalomelemzést végez, és riasztásokat generál, ha fenyegetéseket észlelnek az IP-hálózatokon. Protokollelemzést, tartalomkeresést vagy egyeztetést is végezhet, valamint számos támadást és vizsgálatot észlel (pl. puffertúlcsordulás, lopakodó portellenőrzés stb.). A Snort bekerült az InfoWorld Nyílt forráskódú Hírességek Csarnokába, mint a valaha volt legnagyobb nyílt forráskódú szoftverek közé.

A Snort motor mostantól virtuális konténerszolgáltatásként futhat a Cisco 4000 ISR-eken és a Cisco Cloud Services Router 1000v sorozaton. Ideális kisebb szervezetek számára, akik költséghatékony útválasztási és fenyegetésvédelmi megoldást keresnek. Például az ISR G2 fejlett útválasztási képességeket és integrált fenyegetés elleni védelmet nyújthat a Snort IPS használatával.

A Snort IPS más, a 4000-es sorozatú ISR-ekbe integrált biztonsági funkciókkal is megvalósítható, mint például a VPN, a zónaalapú Cisco IOS tűzfalak és a Cisco Cloud Web Security. Ez lehetővé teszi, hogy az ISR átfogó fenyegetésvédelmet nyújtson kis helyigénnyel. Ez döntő fontosságú a kis fióktelepek számára, amelyeknek gondoskodniuk kell a helyi internetkapcsolat biztonságáról. Az ISR-be integrált Snort IPS költséghatékony alternatíva fiókirodák számára, mivel nincs szükség külön tűzfaleszközre.

A Snort IPS a 4000-es sorozatú ISR-en a következő funkciókat kínálja:

* **IDS és IPS mód** – A fenyegetésészlelési vagy -megelőzési mód konfigurálása. Megelőző módban a támadási forgalom megszűnik.
* **Három aláírási szint** – A Snort három szintű aláírásvédelmet biztosít: kapcsolat (legkevésbé biztonságos), kiegyensúlyozott (középső opció) és biztonság (legbiztonságosabb). A biztonsági szint a legbiztonságosabb, mivel ez teszi lehetővé a legtöbb aláírás ellenőrzését.
* **Engedélyezett lista** – Lehetővé teszi bizonyos aláírások kikapcsolását, és segít elkerülni a hamis pozitív jeleket, például az IPS-műveletet kiváltó jogos forgalom. Legfeljebb 1000 bejegyzés támogatható az engedélyezett listában.
* **Snort állapotfigyelés** – A Cisco IOS Software nyomon követi a szolgáltatástárolóban futó Snort motor állapotát.
* **Sikertelen nyitás és bezárás** – IPS-motor meghibásodása esetén az útválasztó konfigurálható úgy, hogy blokkolja a forgalmi áramlást, vagy megkerülje az IPS-ellenőrzést, amíg a Snort motor helyreáll.
* **Aláírás frissítése** – Az automatikus és kézi frissítések támogatottak. A Snort IPS közvetlenül a cisco.com webhelyről vagy egy helyi erőforrás helyről töltheti le az aláírási csomagot HTTP és HTTPS protokollon keresztül.
* **Eseménynaplózás** – Az IPS-naplók elküldhetők egy független naplógyűjtőnek, vagy beépíthetők az útválasztó syslog adatfolyamába. Az IPS-naplók külön küldése segít, ha a biztonsági eseménykezelő eszköz eltér a szokásos syslog-kiszolgálótól.

12.2.4

## A Snort összetevői és szabályai

A Snort IPS a 4000-es sorozatú ISR-ekhez két összetevőből áll:

* **Snort engine** – Ez az IPS-észlelő és végrehajtó motor, amely a 4000-es sorozatú ISR-ekre vonatkozó biztonsági (SEC) licencben található.
* **Snort-szabály-szoftver-előfizetések aláírás-frissítésekhez** – A Snort-szabálykészletek, amelyek a legújabb fenyegetés elleni védelemmel is naprakészek maradnak, időalapú előfizetések, amelyek egy vagy három évig állnak rendelkezésre.

A gyorsan változó fenyegetettség kezelése érdekében fontos annak biztosítása, hogy az aláírások a lehető legfrissebbek legyenek.

A határidő alapú előfizetések két típusa létezik:

* **Közösségi szabálykészlet** – Ingyenesen elérhető, ez az előfizetés korlátozott védelmet kínál a fenyegetésekkel szemben. A közösségi szabálykészlet a biztonsági fenyegetések reaktív reagálására összpontosít, szemben a proaktív kutatási munkával. A frissített aláírásokhoz 30 napos késleltetett hozzáférés is tartozik, ami azt jelenti, hogy a legújabb szabály legalább 30 napos lesz. Ezenkívül nem áll rendelkezésre Cisco ügyfélszolgálat.
* **Előfizetői szabálykészlet** – Ez a szolgáltatás díj ellenében elérhető, és a legjobb védelmet nyújtja a fenyegetésekkel szemben. Tartalmazza a Cisco Talos biztonsági szakértőinek kutatási munkájának felhasználásával végzett előrehaladásokat. Az előfizetői szabálykészlet biztosítja a leggyorsabb hozzáférést a frissített aláírásokhoz egy biztonsági incidens vagy egy új fenyegetés proaktív felfedezése esetén. Ezt az előfizetést a Cisco teljes mértékben támogatja.

**Megjegyzés** : Lépjen kapcsolatba a Cisco ügyfélszolgálatával az előfizetői szabálykészlet licencének beszerzéséhez.

12.2.5

## ISR konténer alkalmazások

Az útválasztók kezdetben csomagfeldolgozó eszközök voltak. Az évek során azonban számos számítási funkció ellátására fejlődtek. Az útválasztók akkora feldolgozási teljesítményre tettek szert, hogy a kiszolgálóalkalmazások már az útválasztón belül is tárolhatók szolgáltatástárolóknak nevezett virtuális gépek segítségével.

Az olyan alkalmazások, mint a Snort IPS, feltölthetők és tárolhatók ezeken az útválasztókon. A szolgáltatástárolók a legtöbb IOS XE platformon támogatottak. Az IOS XE Linux architektúrán alapul, és támogatja a virtuális gépek üzemeltetését.

A Snort motor Linux Service Container alkalmazásként fut az ISR 4000-en, az ábrán látható módon. Ez dedikált számítási erőforrásokat biztosít számára, amelyek az adatsík CPU-terhelésétől függetlenül futnak. Ezenkívül megkönnyíti a Snort motor rendszeres frissítését.

Pontosabban, a Snort motor a 4000-es sorozatú ISR-en konténeralkalmazásként fut. A 4000-es sorozatú ISR többmagos CPU-t használ, a Cisco IOS-XE pedig képes ezeket a magokat vezérlősík vagy adatsík funkciókhoz rendelni. A vezérlősík-függvények által fel nem használt számítási erőforrások más szolgáltatások futtatására is használhatók. Ezeket az alkalmazásokat egy Linux konténer-infrastruktúra tárolja. Az ebben a konténer-infrastruktúrában futó alkalmazások szorosabban integrálhatók a Cisco IOS szoftverrel.

12.2.6

## Snort IPS szabály riasztások

A Snort IPS-ben az aláírásokat „szabályok” segítségével konfigurálják. Ezek a szabályok aláírási riasztásként szolgálnak, összehasonlítva a bejövő forgalmat a Snort szabályokkal. A szabály fejlécének megfelelő forgalom műveletet generál.

A szabályfejléc elvileg hasonló a hozzáférés-vezérlési lista (ACL) utasításához. Ez egy egysoros utasítás, amely azonosítja a rosszindulatú forgalmat.

Az alapszabály fejléc parancs szintaxisa a következő:

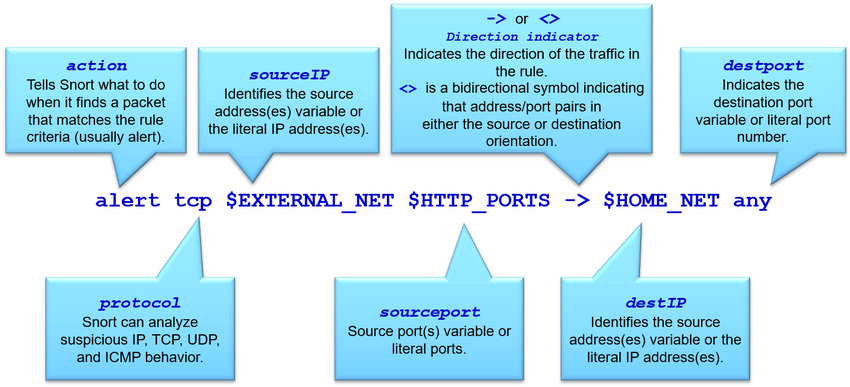
[ művelet ] [ protokoll ] [ forrás-IP ] [ forrásport ] - > [ célIP ] [ destport ] ( [ szabálybeállítások ] )

**Megjegyzés:** A Szabály opciók további szabályinformációkat tartalmaznak.

Például a következő mintafejléc riasztást generál, amikor a szabályfejléc-változókban azonosított gazdagépek/portok TCP-kapcsolata az azonosított célállomások/portok változóihoz megy:

**alert tcp $EXTERNAL \_ NET $HTTP \_ PORTS - > $HOME \_ NET any**

A példa részletes magyarázatához lásd az ábrát.



12.2.7

## Snort IPS Rule Actions

A snort IDS módban vagy IPS módban engedélyezhető.

A Snort IDS mód a következő három műveletet hajthatja végre:

* **Figyelmeztetés** – riasztást generál a kiválasztott riasztási módszerrel.
* **Napló** – naplózza a csomagot.
* **Pass** - Figyelmen kívül hagyja a csomagot.

A Snort IPS mód képes végrehajtani az összes IDS műveletet, valamint a következőket:

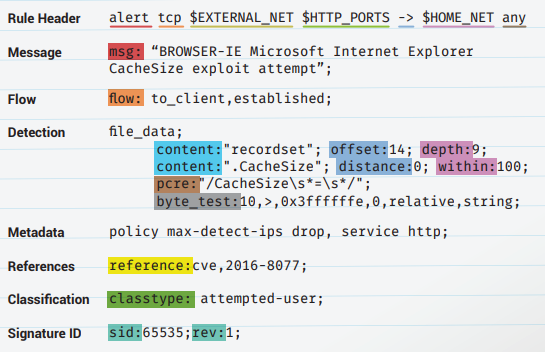
* **Drop** – blokkolja és naplózza a csomagot.
* **Elutasítás** – blokkolja a csomagot, naplózza, majd küldjön egy TCP-reset-et, ha a protokoll TCP, vagy egy ICMP-port elérhetetlen üzenetet, ha a protokoll UDP.
* **Sdrop** – blokkolja a csomagot, de ne naplózza.

12.2.8

## Snort IPS Header Rule Options

A Snort-szabály fejléce szabálybeállításokat (mezőket) is tartalmaz, amelyek további információkat nyújtanak a szabályhoz. Az opciókat pontosvessző (;) választja el, a szabálybeállítás kulcsszavait pedig kettősponttal (:) választja el argumentumaiktól.

Az ábra a figyelmeztető tcp mintaszabály-beállításait jeleníti meg **$EXTERNAL \_ NET $HTTP \_ PORTS - > $HOME \_ NET bármely** szabály fejlécéhez.



A táblázat leírja az általános általános szabályt és a mintaszabály fejlécében található észlelési szabályok beállításait.

**Megjegyzés** : Ez csak néhány a különböző típusú szabályok közül. További példákért keressen az interneten a "snort rule options" kifejezésre.

| **Szabály opció** | **Konkrét művelet** |
| --- | --- |
| **msg:** | Ez egy egyszerű szöveges karakterlánc, amely értelmes üzenetet ad a kimenetre, ha a szabály egyezik. |
| **folyam:** | Meghatározza a hálózati forgalom irányát. |
| **tartalom:** | Egy észlelési szabály beállítás, amely lehetővé teszi a szabály létrehozója számára, hogy olyan szabályokat állítson be, amelyek meghatározott tartalmat keresnek a csomagban lévő hasznos adatban, és az adatok alapján választ indítanak el. Ennek az opciónak az adatai vegyesen szöveges és bináris adatokat tartalmazhatnak |
| **távolság: / eltolás:** | Észlelési szabály kulcsszavai, amelyek lehetővé teszik a szabály létrehozója számára, hogy meghatározza, hol kezdje el a keresést a hasznos teher kezdetéhez vagy a tartalmi egyezés kezdetéhez képest. |
| **belül: / mélység:** | Észlelési szabály kulcsszavai, amelyek lehetővé teszik a szabály létrehozója számára annak meghatározását, hogy mennyivel előre kell keresni egy korábbi tartalomegyezés végéhez képest, és ha megtalálta a tartalomegyezést, milyen messzire keressen rá. |
| **pcre** | Egy észlelési szabály kulcsszó, amely lehetővé teszi a szabályok „perl-kompatibilis reguláris kifejezések” használatával történő megírását, ami bonyolultabb egyezéseket tesz lehetővé. |
| **byte\_test** | Egy észlelési szabály kulcsszó, amely lehetővé teszi egy szabály számára, hogy egy adott számú bájtot teszteljen egy adott bináris értékhez képest. |
| **metaadatok:** | Lehetővé teszi a szabály létrehozója számára, hogy további információkat ágyazzon be a szabállyal kapcsolatban. |
| **referencia:** | Lehetővé teszi, hogy a szabályok külső információforrásokra hivatkozzanak. |
| **osztálytípus:** | Azonosítja a sikeres támadás lehetséges hatását. |
| **sid / rev** | Az aláírás azonosítója ( **sid** ) minden egyes szabály egyedi azonosítója, amely megkönnyíti azok azonosítását. (revision) kulcsszóval együtt kell használni **A rev** a szabály aktuális verziójának jelzésére. |

12.2.9

## Snort IPS működés

A Snort-kompatibilis interfészekre érkező csomagokat az alábbiak szerint ellenőrzik:

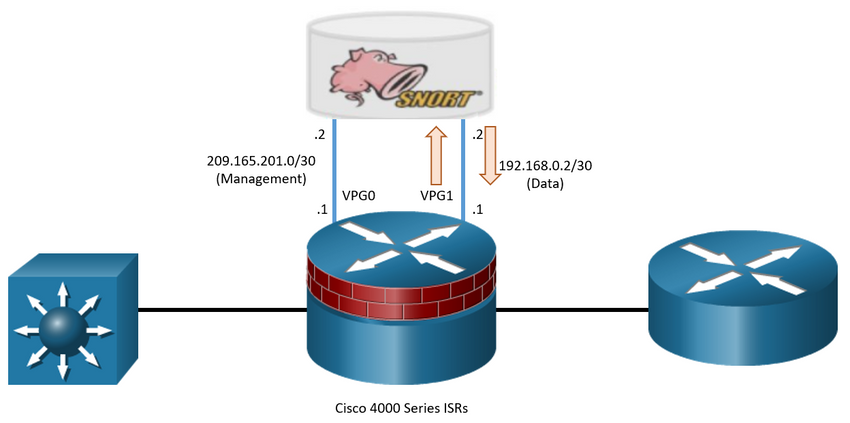
1. A Cisco IOS Software belső virtuális portcsoport (VPG) interfész segítségével továbbítja a vizsgálandó csomagokat a Snort IPS motornak.
2. A Snort IPS ellenőrzi a forgalmat, és megteszi a szükséges intézkedéseket.
3. A Snort eldobja a rossz áramlásokhoz kapcsolódó csomagokat (IPS mód). A jó áramlási csomagok visszakerülnek a routerbe további feldolgozás céljából.

A tárolóalkalmazások és az IOS adatsík közötti csomagcsere VPG interfészek segítségével történik. Ezek az irányított interfészek a router hátsó síkján keresztül csatlakoznak. A megfelelő interfész a konténer oldalán virtuális Ethernet portként jelenik meg.

A Snort IPS két VPG interfészt igényel:

* **Felügyeleti felület** – Ez az az interfész, amely a naplók gyűjtőhöz való forrására és az aláírásfrissítések lekérésére szolgál a Cisco.com webhelyről. Emiatt ez az interfész irányítható IP-címet igényel.
* **Adatfelület** – Ez az az interfész, amely a felhasználói forgalom küldésére szolgál a Snort virtuális tároló szolgáltatás és az útválasztó továbbítási síkja között.

Az ábrán a VPG0 a Snort kezelési forgalomhoz, míg a VPG1 a felhasználói forgalom ellenőrzéséhez használatos. A vizsgálandó felhasználói forgalom a VPG1 segítségével a Snort motorhoz kerül továbbításra, az ábra szerint. A forgalmat ezután ellenőrzik, és vagy elutasítják (eldobják), vagy visszaküldik az útválasztónak az ábrán látható módon.



12.2.10

## Ellenőrizze, hogy megértette – Snort IPS

Az űrlap teteje

Ellenőrizze, hogy megértette-e a Snort IPS-t, és válassza ki a megfelelő választ a következő kérdésekre.

1. Mi a Snort IDS által támogatott három művelet? (Válassz hármat.)

Az űrlap alja

Melyik két lehetőség összetevője az ISR 4000-en futó Snort IPS-nek? (Válassz kettőt.)

[12.1](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[IPS Signatures](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[12.3](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Configure Snort IPS](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                             
*                   

1. IPS Operation and Implementation
2. Configure Snort IPS

# Konfigurálja a Snort IPS-t

12.3.1

## Snort IPS konfigurációs lépések

A Snort IPS támogatott eszközökön történő telepítéséhez hajtsa végre a következő lépéseket:

**1. lépés** . Töltse le a Snort OVA fájlt.   
**2. lépés** . Telepítse az OVA fájlt.   
**3. lépés** . Konfigurálja a Virtual Port Group interfészt.   
**4. lépés** . Aktiválja a virtuális szolgáltatásokat.   
**5. lépés** . Konfigurálja a Snort jellemzőit.   
**6. lépés** . Az IPS engedélyezése globálisan vagy a kívánt interfészeken.   
**7. lépés** . Ellenőrizze a Snort IPS-t.

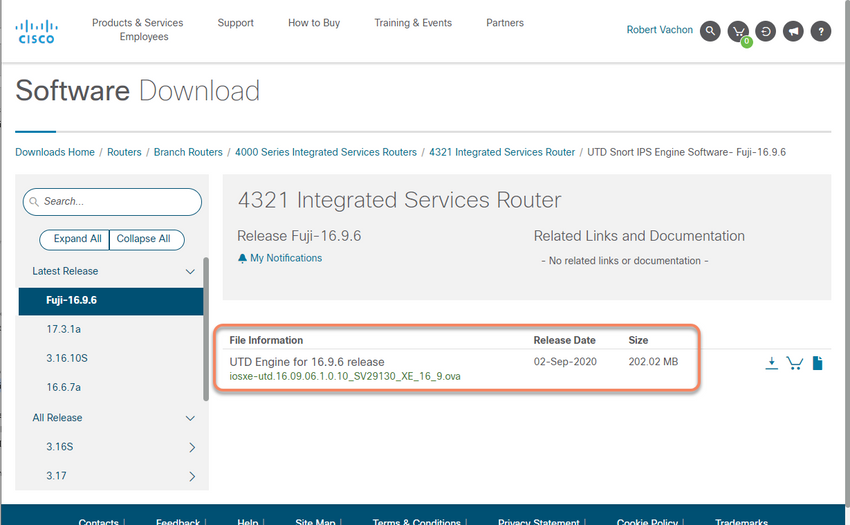
**Megjegyzés:** A Snort IPS funkció csak a biztonsági K9 licenccel rendelkező IOS XE verzióban érhető el. A szolgáltatás engedélyezéséhez biztonsági engedély szükséges. Ez a funkció a Cisco IOS XE 3.16.1S, 3.17S és újabb kiadásaiban érhető el.

12.3.2

## 1. lépés: Töltse le a Snort OVA fájlt

Az Open Virtualization Archive (OVA) egy olyan fájl, amely egy virtuális gép tömörített, telepíthető verzióját tartalmazza. A Snort szolgáltatás OVA-fájlja nincs csomagolva az útválasztóra telepített Cisco IOS XE Release lemezképekkel. Ha azonban az OVA-fájl előre telepítve van az útválasztó flashjében, javasoljuk, hogy töltse le a legújabb OVA-fájlt a Cisco.com webhelyről.

Például az ábrán a felhasználó egy ISR 4321 router OVA-fájlját tölti le az IOS Fuji-16.9.6 használatával.



**Megjegyzés:** A fájlok Cisco.com webhelyről történő letöltéséhez CCO-hozzáférés szükséges.

12.3.3

## 2. lépés Telepítse a Snort OVA fájlt

Az OVA-fájlt le kell tölteni és az ISR-útválasztó számára elérhető fájlhelyre kell menteni (pl. Flash).

Az OVA-fájl telepítéséhez használja a **virtuális szolgáltatás telepítési neve** virtuális szolgáltatásnév **csomag** fájl-url **médiafájl** -rendszer jogosultsága EXEC parancsot. hossza A név 20 karakter, és meg kell adni az OVA fájl teljes elérési útját.

Az alábbiakban egy példa konfiguráció látható.

R1# **virtual-service install name MYIPS package flash:iosxe-utd.16.09.06.1.0.10\_SV29130\_XE\_16\_9.ova**

Installing package 'bootflash:/iosxe-utd.16.09.06.1.0.10\_SV29130\_XE\_16\_9.ova' for virtual-service 'MYIPS'. Once the install has finished, the VM may be activated. Use 'show virtual-service list' for progress.

R1#

\*Oct 5 08:07:45.953: %VMAN-5-PACKAGE\_SIGNING\_LEVEL\_ON\_INSTALL: R0/0: vman: Package 'iosxe-utd.16.09.06.1.0.10\_SV29130\_XE\_16\_9.ova' for service container 'MYIPS' is 'Cisco signed', signing level cached on original install is 'Cisco signed'

R1#

Az OVA fájl telepítése során a rendszer ellenőrzi a biztonsági licencet, és hibaüzenetet küld, ha a licenc nincs meg. Ezért a Cisco IOS XE lemezképet engedélyezni kell a biztonsági licenccel. A kimeneten látható, hogy az OVA Cisco aláírt.

A **show virtual-service list** paranccsal megjelenítheti a virtuális szolgáltatástárolóra telepített összes alkalmazás telepítési állapotát.

12.3.4

## 3. lépés: Konfigurálja a virtuális port csoport interfészt

Ezután két VirtualPortGroup (VPG) interfészt kell konfigurálni a vendég IP-címekkel együtt.

Példánkban a VPG interfészek a következőképpen lesznek konfigurálva:

* **VGP0 –** A felügyeleti forgalom az IPS-kiszolgálókkal való információcserére szolgál. A vendég IP-címének irányíthatónak kell lennie az aláírásfrissítési kiszolgálóhoz és a külső naplószerverhez való csatlakozáshoz. A naplógyűjtők felé irányuló forgalom naplózására is használják.
* **VPG1 –** Ez az ellenőrzésre kijelölt felhasználói forgalomra vonatkozik. Ez nem lehet irányítható, ezért használjon nem irányítható privát IP-címet.

**Megjegyzés** : Ügyeljen arra, hogy megfelelő NAT-ot és útválasztást biztosítson, hogy a felügyeleti VPG elérje a naplószervert, valamint a cisco.com webhelyet az aláírásfrissítési fájlok lekéréséhez.

Az alábbiakban a VPG0 és a VPG1 mintakonfigurációja látható.

R1# **configure terminal**

R1(config)# **interface VirtualPortGroup0**

R1(config-if)# **description Management interface**

R1(config-if)# **ip address 209.165.201.1 255.255.255.252**

R1(config-if)# **exit**

R1(config)#

\*Oct 5 08:13:10.970: %LINEPROTO-5-UPDOWN: Line protocol on Interface VirtualPortGroup0, changed state to up

R1(config)# **interface VirtualPortGroup1**

R1(config-if)# **description Data interface**

R1(config-if)# **ip address 192.168.0.1 255.255.255.252**

R1(config-if)# **exit**

R1(config)#

\*Oct 5 08:13:12.921: %LINEPROTO-5-UPDOWN: Line protocol on Interface VirtualPortGroup1, changed state to up

R1#

12.3.5

## 4. lépés: Aktiválja a Virtuális szolgáltatásokat

A következő lépés a vendég IP-címek konfigurálása ugyanazon az alhálózaton a tárolóoldalon, és aktiválja a virtuális szolgáltatást a kimeneten látható módon.

R1(config)# **virtual-service MYIPS**

R1(config-virt-serv)# **vnic gateway VirtualPortGroup0**

R1(config-virt-serv-vnic)# **guest ip address 209.165.201.2**

R1(config-virt-serv-vnic)# **exit**

R1(config-virt-serv)# **vnic gateway VirtualPortGroup1**

R1(config-virt-serv-vnic)# **guest ip address 192.168.0.2**

R1(config-virt-serv-vnic)# **exit**

R1(config-virt-serv)# **activate**

A **virtual-service** virtual-service-name logikai nevet **parancs konfigurálja a példában szereplő MYIPS** , amely a virtuális tároló szolgáltatás azonosítására szolgál.

A **vnic gateway VirtualPortGroup** interface-number parancs virtuális hálózati csatolókártya (vNIC) átjárófelületet hoz létre a virtuális tároló szolgáltatáshoz. Ezenkívül leképezi a vNIC-átjáró interfészt a virtuális portcsoportra, és belép a virtuális szolgáltatás vNIC-konfigurációs módjába.

A **vendég IP-cím** ip-address parancs egy vendég vNIC-címet konfigurál a vNIC-átjáró felületéhez.

Végül az **activate** parancs aktiválja a virtuális tárolószolgáltatásba telepített alkalmazást.

12.3.6

## 5. lépés: Konfigurálja a Snort specifikációit

A következő lépés a Snort üzembe helyezési módjának (azaz IPS vagy IDS mód) konfigurálása, a Snort naplók elküldésének helye, a Snorthoz konfigurálandó házirend és profil és egyebek.

Tekintse meg a minta parancs kimenetét.

R1(config)# **utd engine standard**

R1(config-utd-eng-std)# **logging host 10.10.10.254**

R1(config-utd-eng-std)# **logging syslog**

R1(config-utd-eng-std)#

R1(config-utd-eng-std)# **threat-inspection**

R1(config-utd-engstd-insp)# **threat protection**

R1(config-utd-engstd-insp)# **policy balanced**

R1(config-utd-engstd-insp)#

R1(config-utd-engstd-insp)# **signature update occur-at daily 0 0**

R1(config-utd-engstd-insp)# **signature update server cisco username Bob password class**

R1(config-utd-engstd-insp)# **logging level warning**

R1(config-utd-engstd-insp)#

R1(config-utd-engstd-insp)# **exit**

R1(config-utd-eng-std)# **exit**

R1(config)#

Az **utd engine standard** parancs konfigurálja az UTD szabványos motort, és belép az UTD szabványos motorkonfigurációs módba.

A **naplózási gazdagép** és **naplózási syslog** parancsok lehetővé teszik a vészhelyzeti üzenetek naplózását a kiszolgálón.

A **fenyegetés-ellenőrzési** parancs konfigurálja a Snort-motor fenyegetésvizsgálatát. Itt adhatja meg, hogy a Snort melyik üzemmódban legyen:

* **fenyegetésvédelem –** A Snort IPS módban lesz.
* **fenyegetésészlelés –** A Snort IDS módban lesz.

A **házirend** parancs három, a Snort által használt és a Cisco Talos által biztosított biztonsági házirendet határoz meg, amint az a következő súgópéldán látható.

R1(config-utd-engstd-insp)# **policy ?**

balanced Set the policy to balanced (this is the default option)

connectivity Set the policy to connectivity (stresses on connectivity over

security)

security Set the policy to security (provide mode exhaustive coverage)

R1(config-utd-engstd-insp)# **policy**

A három házirend-beállítás a legkisebb védelemtől a legnagyobb védelemig a következő:

* **kapcsolat** – Ez biztosítja a legkevesebb védelmet, mivel a csatlakozást helyezi előtérbe a biztonsággal szemben. Körülbelül 1000 szabály van előre betöltve ezzel a házirenddel.
* **kiegyensúlyozott** – Ez az alapértelmezett házirend. Kezdeti telepítésekhez ajánlott. Ez a házirend megpróbálja egyensúlyba hozni a hálózat biztonsági igényeit és teljesítményjellemzőit. Körülbelül 8000 szabály van előre betöltve ezzel a házirenddel.
* **biztonság** – Ez biztosítja a legnagyobb védelmet. Olyan szervezetek számára készült, amelyek kivételesen aggódnak a biztonság miatt. Az ügyfelek ezt a házirendet olyan védett hálózatokon alkalmazzák, amelyek alacsonyabb sávszélesség-igényekkel, de sokkal magasabb biztonsági követelményekkel rendelkeznek. Körülbelül 12 000 szabály van előre betöltve ezzel a házirenddel.

**Megjegyzés:** Az IPS rendszer teljesítményét negatívan befolyásolja, ha több szabályt engedélyez.

Az **aláírásfrissítési** parancs konfigurálja az aláírás-frissítési intervallum paramétereit. Mintakimenetünkben a Snort minden este éjfélkor frissíti az aláírásait.

Az **aláírásfrissítési kiszolgáló** parancs konfigurálja az aláírásfrissítési kiszolgáló paramétereit. Meg kell adnia az aláírás frissítési paramétereit a kiszolgáló adataival. Ha a Cisco.com webhelyet használja aláírás-frissítésekhez, meg kell adnia a felhasználónevet és a jelszót. Ha helyi szervert használ az aláírások frissítéséhez, a szerver beállításai alapján megadhatja a felhasználónevet és a jelszót. Mintakimenetünkben a Snort frissíti a cisco.com oldalról származó aláírási fájlját a Bob felhasználónév és a jelszóosztály használatával.

Végül a **naplózási szint** parancs határozza meg a generálandó syslog üzenetek típusát.

12.3.7

## 6. lépés: Engedélyezze az IPS-t globálisan vagy a kívánt interfészeken

A szervezeti követelmények alapján a Snort globálisan (azaz minden interfészen) vagy kiválasztott interfészeken engedélyezhető.

A kimenetben található példa globálisan engedélyezi az UTD-t az összes interfészen, és meghatározza, hogy mi a teendő, ha a Snort motor meghibásodik.

R1(config)# **utd**

R1(config-utd)# **all-interfaces**

R1(config-utd)#

R1(config-utd)# **engine standard**

R1(config-engine-std)# **fail close**

R1(config-engine-std)# **exit**

R1(config-utd)# **exit**

R1(config)#

Az **összes interfész** opció az egyesített fenyegetés elleni védelmet (UTD) konfigurálja az eszköz összes 3. rétegbeli interfészén.

A **motor standard** parancsa konfigurálja a Snort-alapú UTD-motort, és belép a normál motorkonfigurációs módba. Ebből a módból megadhatjuk, hogy a Snort hogyan viselkedjen UTD-motorhiba esetén.

Konkrétan a Snort a következőkre konfigurálható:

* **hibanyitás** (alapértelmezett) – UTD motorhiba esetén ez az opció átengedi a teljes IPS/IDS forgalmat ellenőrzés nélkül.
* **fail-close** – Ha engedélyezve van, ez az opció leállítja az összes IPS/IDS forgalmat UTD motorhiba esetén. Ezért a forgalom nem indulhat el.

Alternatív megoldásként a Snort csak bizonyos interfészeken engedélyezhető, az ábrán látható módon.

**Megjegyzés** : Hibaüzenet jelenik meg, ha a globális konfigurációt először konfigurálták.

R1(config)# **interface G0/0/0**

R1(config-if)# **utd enable**

R1(config-if)# **exit**

R1(config)# **interface G0/0/1**

R1(config-if)# **utd enable**

R1(config-if)# **exit**

R1(config)#

Engedélyezheti az UTD engedélyezett lista funkciót is. Ez lehetővé teszi a letiltandó (nem használandó) IPS aláírásazonosítók azonosítását.

Például, ha egy IPS helytelenül fenyegetésként azonosítja a normál felhasználói forgalmat (azaz hamis pozitív eredmény), akkor ezeket az aláírásokat hozzáadhatjuk az engedélyezett listához. Az IPS nem használ aláírásokat az engedélyezési listában.

Ehhez lépjen be az UTD engedélyezett lista konfigurációs módjába, és azonosítsa az ellenőrzésből kizárandó aláírásazonosítókat. Az engedélyezett lista aláírási azonosítójának konfigurálása után a Snort lehetővé teszi az áramlás áthaladását az eszközön riasztások és visszaesések nélkül.

Tegyük fel például, hogy az IPS helytelenül rosszindulatúként azonosította a **Branch1** felhasználói forgalmát , és **a 21555-ös azonosítót** rendelte hozzá . Ez az aláírás hozzáadható az engedélyezett listához, az ábrán látható módon.

R1(config)# **utd threat-inspection whitelist**

R1(config-utd-whitelist)# **signature id 21555 comment traffic from Branch 1**

R1(config-utd-whitelist)#

12.3.8

## 7. lépés: Ellenőrizze a Snort IPS-t

A Snort IPS megvalósítása után ellenőrizni kell a konfigurációt a megfelelő működés érdekében.

Számos **show** parancs használható a Snort IPS konfigurációjának és működésének ellenőrzésére.

* **show virtual-service list** – A parancs megjeleníti az alkalmazások által használt erőforrások áttekintését.
* **show virtual-service details** – A parancs megjeleníti azon erőforrások listáját, amelyek egy adott alkalmazáshoz vannak kötve, beleértve a csatolt eszközöket is.
* **show utd engine standard config** – A parancs megjeleníti az UTD konfigurációt.
* **show utd engine standard status** – A parancs megjeleníti az UTD motor állapotát.
* **show platform hardver qfp aktív szolgáltatás utd stats** - A parancs ellenőrzi az adatsíkot. Ellenőrzi az encap, decap, átirányítás és újrainjektálás növekményeit, és megjeleníti a "zöld" állapotot.

12.3.9

## Szintaxis-ellenőrző – A Snort IPS konfigurálása

Ebben a Syntax Checker tevékenységben a 2–6. lépést kell végrehajtania a snort IPS konfigurálásához:

**2. lépés** . Telepítse a Snort OVA fájlt.   
**3. lépés** . Konfigurálja a Virtual Port Group interfészt.   
**4. lépés** . Aktiválja a virtuális szolgáltatásokat.   
**5. lépés** . Konfigurálja a Snort jellemzőit.   
**6. lépés** . Az IPS engedélyezése globálisan vagy a kívánt interfészeken.

**Step 1** is to download to Snort OVA file from cisco.com.

**Step 2**: Install the OVA file **iosxe-utd.16.09.06.1.0.10\_SV29130\_XE\_16\_9.ova** in flash. Use the virtual service name **MYIPS**.

R1#virtual-service install name MYIPS package flash:iosxe-utd.16.09.06.1.0.10\_SV29130\_XE\_16\_9.ova

Installing package 'bootflash:/iosxe-utd.16.09.06.1.0.10\_SV29130\_XE\_16\_9.ova' for virtual-service 'MYIPS'. Once the install has finished, the VM may be activated. Use 'show virtual-service list' for progress.

R1#

\*Oct 5 08:07:45.953: %VMAN-5-PACKAGE\_SIGNING\_LEVEL\_ON\_INSTALL: R0/0: vman: Package 'iosxe-utd.16.09.06.1.0.10\_SV29130\_XE\_16\_9.ova' for service container 'MYIPS' is 'Cisco signed', signing level cached on original install is 'Cisco signed'

**Step 3**: Configure Virtual Port Group interfaces using the following specifications:

* Enter global configuration mode and then interface configuration mode for **VirtualPortGroup0**.
* Describe the interface as **Management interface**.
* Assign the IP address 209.165.201.1 255.255.255.252.
* Exit interface configuration mode.

R1#configure terminal

R1(config)#interface VirtualPortGroup0

R1(config-if)#description Management interface

R1(config-if)#ip address 209.165.201.1 255.255.255.252

R1(config-if)#exit

R1(config)#

\*Oct 5 08:13:10.970: %LINEPROTO-5-UPDOWN: Line protocol on Interface VirtualPortGroup0, changed state to up

* Enter interface configuration mode for **VirtualPortGroup1**.
* Describe the interface as **Data interface**.
* Assign the IP address 192.168.0.1 255.255.255.252.
* Exit interface configuration mode.

R1(config)#interface VirtualPortGroup1

R1(config-if)#description Data interface

R1(config-if)#ip address 192.168.0.1 255.255.255.252

R1(config-if)#exit

R1(config)#

\*Oct 5 08:13:12.921: %LINEPROTO-5-UPDOWN: Line protocol on Interface VirtualPortGroup1, changed state to up

**Step 4**: Activate the virtual services using the following specifications:

* Name the virtual service **MYIPS**
* Create a vNIC for VirtualPortGroup0.
* Assign the vNIC the guest IP address 209.165.201.2.
* Exit vNIC configuration mode.
* Create a vNIC for VirtualPortGroup1.
* Assign the vNIC the guest IP address 192.168.0.2.
* Exit vNIC configuration mode.
* Activate the virtual service.
* Exit virtual service configuration mode.

R1(config)#virtual-service MYIPS

R1(config-virt-serv)#vnic gateway VirtualPortGroup0

R1(config-virt-serv-vnic)#guest ip address 209.165.201.2

R1(config-virt-serv-vnic)#exit

R1(config-virt-serv)#vnic gateway VirtualPortGroup1

R1(config-virt-serv-vnic)#guest ip address 192.168.0.2

R1(config-virt-serv-vnic)#exit

R1(config-virt-serv)#activate

R1(config-virt-serv)#exit

**Step 5**. Configure snort specifics using the following specifications:

* Enter configuration mode for the UTD engine.
* Log traffic from host 10.10.10.254 using syslog.
* Enter threat inspection mode.
* Set the inspection to protection with a balanced policy.
* Configure the signature update for daily at 0 0.
* Configure the username **Bob** and password **class** for the signature update server.
* Enter **exit** twice to return to global configuration mode.

R1(config)#utd engine standard

R1(config-utd-eng-std)#logging host 10.10.10.254

R1(config-utd-eng-std)#logging syslog

R1(config-utd-eng-std)#threat-inspection

R1(config-utd-engstd-insp)#threat protection

R1(config-utd-engstd-insp)#policy balanced

R1(config-utd-engstd-insp)#signature update occur-at daily 0 0

R1(config-utd-engstd-insp)#signature update server cisco username Bob password class

R1(config-utd-engstd-insp)#logging level warning

R1(config-utd-engstd-insp)#exit

R1(config-utd-eng-std)#exit

**Step 6**. Enable IPS globally or on desired interfaces using the following specifications:

* Enter configuration mode for UTD interfaces.
* Configure all interfaces as UTD interfaces.
* Set the engine to standard.
* If the UTD engine fails, all traffic should be dropped.
* Enter **exit** twice to return to global configuration mode.
* Enable UTD on **G0/0/0** and **G0/0/1** exiting interface configuration mode each time.

R1(config)#utd

R1(config-utd)#all-interfaces

R1(config-utd)#engine standard

R1(config-engine-std)#fail close

Az űrlap teteje

R1(config-engine-std)#

Az űrlap alja

12.3.10

## Ellenőrizze, hogy megértette – A Snort IPS megvalósítása

Az űrlap teteje

Ellenőrizze, hogy megértette-e a Snort IPS megvalósítását, és válassza ki a megfelelő választ a következő kérdésekre.

1. Which type of file contains a compressed, installable version of the Snort IPS virtual machine?

Az űrlap alja

Which Snort IPS interface statement is true?

[12.2](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Cisco Snort IPS](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[12.4](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[IPS Operation and Implementation Summary](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                

1. IPS Operation and Implementation
2. IPS Operation and Implementation Summary

# IPS működési és megvalósítási összefoglaló

12.4.1

## Mit tanultam ebben a modulban?

**IPS aláírások**   
Az IPS aláírásoknak három attribútuma van: típus, trigger és művelet. Az aláírás típusa lehet atomos vagy összetett. Az aláírás-riasztások használhatnak mintaalapú észlelést, anomália-alapú észlelést, házirend-alapú észlelést vagy mézesedény-alapú észlelést. Az IPS aláírási műveletek közé tartozik a riasztás generálása, a tevékenység naplózása, a tevékenység megtagadása, a TCP-kapcsolat alaphelyzetbe állítása és a jövőbeni tevékenységek blokkolása. A kiváltó mechanizmusok olyan eredményeket generálhatnak, mint a valódi pozitív, a valódi pozitív, a hamis negatív és a hamis negatív eredmények.

**Cisco Snort IPS**   
A behatolás elleni védelem a modern Cisco hálózatokban dedikált NGIPS Firepower-kompatibilis eszközök, Snort IPS ISR 4000 útválasztón vagy külső Snort IPS szerver használatával biztosított. A Snort IPS az ISR-eszközön IDS- vagy IPS-szolgáltatásokat is nyújthat. Előre meghatározott biztonsági szintekkel rendelkezik (pl. kapcsolat, kiegyensúlyozott és biztonság). Hivatkozhat egy engedélyezett listára, visszajelzést adhat a Snort motor állapotáról, felkínálja a feladatmegnyitási és -bezárási feladatátvételt, valamint automatikus aláírás-frissítéseket és naplózást. A Snort IPS egy Snort motorból és Snort szabálykészletből áll. Vannak ingyenesen elérhető közösségi szabályok, térítés ellenében pedig előfizetői szabályok. A Snort IPS az ISR 4000 útválasztók által támogatott Linux szolgáltatástároló virtuális gépben fut. A Snort IPS szabályfejlécekből és szabályopciókból álló szabályokat használ a rosszindulatú forgalom azonosítására.

**Konfigurálja a Snort IPS-t**   
A Snort IPS konfigurálásához egy ISR 4000 eszközön le kell töltenie a legújabb OVA-fájlt, telepítenie kell az útválasztóra, konfigurálnia kell a VPG interfészt, aktiválnia kell a virtuális szolgáltatásokat, konfigurálnia kell a Snort IPS jellemzőit, és engedélyeznie kell az UTD-t. A Snort konfigurálása és aktiválása után a show parancsok lehetővé teszik a működésének ellenőrzését.

12.4.2

## 12. modul – IPS működési és megvalósítási kvíz

Az űrlap teteje

1. Melyik IPS-aláírás-triggerkategória használja a legegyszerűbb aktiválási mechanizmust, és keres egy meghatározott és előre meghatározott atomi vagy összetett mintát?

Az űrlap alja

Milyen kifejezés írja le az IDS vagy IPS által a tipikus behatolási tevékenység észlelésére használt szabálykészletet?

Milyen típusú riasztás jön létre, ha az IPS a normál hálózati felhasználói forgalmat helytelenül támadási forgalomként azonosítja?

Mi jellemzi a Snort előfizetői szabálykészlet kifejezésalapú előfizetést?

Melyik besorolás jelzi, hogy a riasztást tényleges biztonsági eseményként ellenőrizték?

Melyik behatolás-megelőzési szolgáltatás volt elérhető az első generációs ISR-útválasztókon, és amelyet a Cisco már nem támogat?

Melyik állítás írja le helyesen a Snort VPG interfész konfigurációját?

Milyen három műveletet hajthat végre a Snort IDS módban? (Válassz hármat.)

Melyik eszköz egy dedikált beépített fenyegetés-megelőzési eszköz, amely hatékony az ismert és az ismeretlen fenyegetésekkel szemben?

Melyik szabályművelet okozza, hogy a Snort IPS blokkolja a csomagot naplózás nélkül?

Mi az IPS-szabályfrissítések forrása Cisco behatolásgátló szolgáltatás használata esetén?

[12.3](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Configure Snort IPS](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[13.0](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                      
*                 

1. Endpoint Security
2. Introduction

# Bevezetés

13.0.1

## Miért vegyem ezt a modult?

A végpontok érzékenyek az adatlopásra. A hálózat úgy fejlődött, hogy hagyományos végpontokat és új, könnyű, hordozható, fogyasztói végpontokat, például okostelefonokat, táblagépeket, hordható eszközöket és másokat is magában foglal. Ezek az új végpontok elmosták a hálózati határt, mivel a hálózati erőforrásokhoz való hozzáférést a felhasználók bármikor kezdeményezhetik különböző csatlakozási módok használatával számos helyről. Milyen módszereket használnak a végpontok védelmére? Olvasson tovább, hogy megtudja a végpontok védelméről!

13.0.2

## Mit fogok tanulni ebben a modulban?

**Modul címe:** Endpoint Security

**Modul célja** : Ismertesse a végpontok sebezhetőségeit és a védelmi módszereket.

| **téma címe** | **Téma Cél** |
| --- | --- |
| **A végpont biztonsági áttekintése** | Ismertesse a végpontok biztonságát és az engedélyező technológiákat. |
| **802.1X hitelesítés** | Ismertesse a 802.1x komponensek funkcióit! |

[12.4](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[IPS Operation and Implementation Summary](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[13.1](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Endpoint Security Overview](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                             
*                 

1. Endpoint Security
2. Endpoint Security Overview

# A végpont biztonsági áttekintése

13.1.1

## LAN Elements Security

A sajtó általában a vállalati hálózatokat ért külső hálózati támadásokkal foglalkozik. Íme néhány példa az ilyen támadásokra:

* DoS támadások egy szervezet hálózata ellen, hogy csökkentsék vagy akár leállítsák a nyilvános hozzáférést
* Egy szervezet webszerverének megsértése a webes jelenlét megrongálására
* Egy szervezet adatszervereinek és gazdagépeinek megsértése bizalmas információk ellopása céljából

Különféle hálózati biztonsági eszközökre van szükség a hálózat peremének külső hozzáféréstől való védelméhez. Amint az ábrán látható, ezek az eszközök tartalmazhatnak VPN-szolgáltatásokat nyújtó hardver ISR-t, ASA tűzfalat, IPS-t és AAA-kiszolgálót.

Az ábra egy topológiát mutat be a hálózat peremét biztosító biztonsági eszközökkel.

Internet Perimeter AAA   
Szerver VPN tűzfal IPS ESA/WSA Web   
Szerver e-mail   
Server DNS   
Server Hosts LAN

Sok támadás a hálózaton belülről eredhet, és származik is. Ezért a belső LAN biztosítása ugyanolyan fontos, mint a külső hálózat kerületének biztosítása. Biztonságos LAN nélkül a szervezeten belüli felhasználók továbbra is ki vannak téve a hálózati fenyegetéseknek és leállásoknak, amelyek közvetlenül befolyásolhatják a szervezet termelékenységét és haszonkulcsát. A belső gazdagép behatolása után a támadó kiindulópontja lehet ahhoz, hogy hozzáférjen a kritikus rendszereszközökhöz, például a kiszolgálókhoz és a bennük lévő érzékeny információkhoz.

Pontosabban, két belső LAN-elemet kell biztosítani:

* **Végpontok** – A gazdagépek általában laptopokból, asztali számítógépekből, szerverekből és IP-telefonokból állnak, amelyek érzékenyek a rosszindulatú programokkal kapcsolatos támadásokra. A végpontok közé tartoznak a videokamerák, az értékesítési pontok és a tárgyak internete eszközei is.
* **Hálózati infrastruktúra** – A LAN-infrastruktúra-eszközök végpontokat kötnek össze, és általában kapcsolókat, vezeték nélküli eszközöket és IP-telefonos eszközöket foglalnak magukban. A legtöbb ilyen eszköz érzékeny a LAN-hoz kapcsolódó támadásokra, beleértve a MAC-címtáblázat túlcsordulási támadásait, a hamisítási támadásokat, a DHCP-vel kapcsolatos támadásokat, a LAN-vihartámadásokat, az STP-manipulációs támadásokat és a VLAN-támadásokat.

Ez a modul a végpontok biztosítására összpontosít.

13.1.2

## Hagyományos végpontbiztonság

A múltban az alkalmazottak végpontjai a vállalat által kibocsátott számítógépek voltak, amelyek egy világosan meghatározott LAN-körvonalon belül helyezkedtek el. Ezeket a gazdagépeket tűzfalak és IPS-eszközök védték, amelyek jól működtek a LAN-hoz csatlakoztatott és a tűzfal mögött lévő gazdagépekkel.

A végpontok hagyományos gazdagép alapú biztonsági intézkedéseket is alkalmaztak:

* **Vírus- és kártevőirtó szoftver** – A gazdagépre telepített szoftver a vírusok és rosszindulatú programok észlelésére és mérséklésére. A vírusirtó szoftvereket kínáló cégek közé tartozik a Norton, a TotalAV, a McAfee, a MalwareBytes és még sokan mások.
* **Gazda alapú IPS** – Ez a helyi gazdagépre telepített szoftver a rendszerkonfiguráció és az alkalmazástevékenység megfigyelésére és jelentésére, naplóelemzésre, eseménykorrelációra, integritás-ellenőrzésre, házirend-érvényesítésre, rootkit észlelésre és riasztásra. Ilyen például többek között a Snort IPS, az OSSEC és a Malware Defender.
* **Gazda alapú tűzfal** – Ez egy gazdagépre telepített szoftver, amely a bejövő és kimenő kapcsolatokat csak az adott gazdagép által kezdeményezett kapcsolatokra korlátozza. Egyes tűzfalszoftverek megakadályozhatják a gazdagép megfertőződését, és megakadályozhatják, hogy a fertőzött gazdagépek rosszindulatú programokat terjeszthessenek más gazdagépekre. Egyes operációs rendszerekben, például Windowsban, vagy olyan cégek által gyártott, mint a NetDefender, a Zonealarm, a Comodo Firewall és még sokan mások.

13.1.3

## A határok nélküli hálózat

A hálózat úgy fejlődött, hogy hagyományos végpontokat és új, könnyű, hordozható, fogyasztói végpontokat, például okostelefonokat, táblagépeket, hordható eszközöket és másokat is magában foglal. A dolgozók új „hozza saját eszközét” (BYOD) igényei a végpontok biztonságának más megközelítését kívánják meg. Ezek az új végpontok elmosták a hálózati határt, mivel a hálózati erőforrásokhoz való hozzáférést a felhasználók bármikor kezdeményezhetik különböző csatlakozási módok használatával számos helyről.

Van néhány probléma a végpontok biztosításának hagyományos módszerével. Sok hálózatban a hálózati alapú eszközök eltérnek egymástól, és jellemzően nem osztanak meg egymással információkat. Ezenkívül az új végponteszközök nem megfelelőek a hagyományos gazdagép-alapú végpont-biztonsági megoldásokhoz az eszközök és az ezeken az eszközökön elérhető operációs rendszerek sokfélesége miatt.

A kihívás az, hogy lehetővé tegyük ezeknek a heterogén eszközöknek, hogy biztonságosan csatlakozzanak a vállalati erőforrásokhoz.

13.1.4

## A határok nélküli hálózat végpontjainak biztonsága

A nagyobb szervezetek védelmet igényelnek a támadás előtt, alatt és után. Az informatikai rendszergazdáknak meg kell tudniuk válaszolni a következő kérdéseket:

* Honnan jött a támadás?
* Mi volt az exploit módszer és a belépési pont?
* Milyen rendszereket érintett?
* Mit csinált az exploit?
* Hogyan térjünk ki a kizsákmányolásból?
* Hogyan enyhíthetjük a sebezhetőséget és a kiváltó okot?

A szervezeteknek meg kell védeniük végpontjaikat az új fenyegetésekkel szemben, és biztosítaniuk kell az alábbi táblázatban felvázolt védelmi intézkedéseket.

| **Intézkedés** | **Célja** |
| --- | --- |
| **kártevőirtó szoftver** | A végpontok védelme a rosszindulatú programok ellen. |
| **spam szűrés** | Akadályozza meg, hogy a spam e-mailek elérjék a végpontokat. |
| **blokklistázás** | Megakadályozza, hogy a végpontok rossz hírű webhelyekhez kapcsolódjanak azáltal, hogy azonnal blokkolják a kapcsolatokat a legújabb hírnévintelligencia alapján. |
| **adatvesztés megelőzés (DLP)** | Megakadályozza az érzékeny információk elvesztését vagy ellopását. |

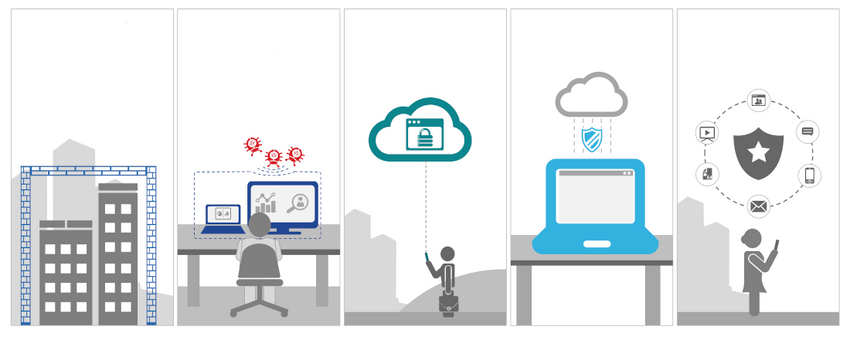
13.1.5

## Hálózati alapú rosszindulatú programok elleni védelem

A határok nélküli hálózat új biztonsági architektúrái a biztonsági kihívásokat úgy kezelik, hogy a végpontok hálózati szkennelési elemeket használnak. Ezek az eszközök sokkal több szkennelési réteget biztosítanak, mint amennyit egyetlen végpont tudna. A hálózati alapú rosszindulatú programokat megelőző eszközök is képesek megosztani egymással az információkat, hogy megalapozottabb döntéseket hozzanak.

A határok nélküli hálózat végpontjainak védelme hálózat-alapú, valamint gazdagép alapú technikákkal is megvalósítható, amint az az ábrán látható.

Az ábra a következő szakaszok általános ikonjait mutatja be: következő generációs tűzfalak, behatolásgátló rendszerek, hálózati hozzáférés-vezérlés, átjáró-biztonság és végpontok biztonsága.



Átjáró biztonság Új generációs tűzfalak Behatolásgátló rendszerek Hálózati hozzáférés-felügyelet Végpontbiztonság

Az alábbiakban példákat mutatunk be olyan eszközökre és technikákra, amelyek hálózati szinten valósítják meg a gazdagépvédelmet.

* **Advanced Malware Protection (AMP)** – Végpontvédelmet biztosít a vírusok és rosszindulatú programok ellen.
* **Email Security Appliance (ESA)** – Ez biztosítja a SPAM és a potenciálisan rosszindulatú e-mailek kiszűrését, mielőtt azok elérnék a végpontot. Ilyen például a Cisco ESA.
* **Web Security Appliance (WSA)** – Ez biztosítja a webhelyek szűrését és blokkolását, hogy megakadályozza a gazdagépek veszélyes helyekre jutását az interneten. A Cisco WSA szabályozza, hogy a felhasználók hogyan férnek hozzá az internethez, és érvényesítheti az elfogadható használati szabályzatokat, szabályozhatja a hozzáférést bizonyos webhelyekhez és szolgáltatásokhoz, és kereshet rosszindulatú programokat.
* **Network Admission Control (NAC)** – Ez csak engedélyezett és megfelelő rendszerek számára teszi lehetővé a hálózathoz való csatlakozást.

Ezek a technológiák egymással összhangban működnek, hogy nagyobb védelmet nyújtsanak, mint amennyit a gazdagép-alapú csomagok képesek nyújtani, amint az az ábrán látható.

Az ábra egy kört mutat a közepén, amelyen kiberbiztonsági műveletek vannak jelölve. Középen van egy négyzet a következő szavakkal: következő generációs tűzfal, következő generációs IPS, végpont HIDS érzékelők, WSA, ESA és egyéb infrastrukturális eszközök, alul a telepítés szóval. A bal felső sarokban egy szövegmező található, amelyen az AMP public/private cloud szavak szerepelnek, valamint egy körre mutató nyíl. A jobb felső sarokban található a szövegdoboz a sandboxing szóval és a körre mutató nyíllal. A jobb alsó sarokban található a szövegdoboz a harmadik fél integrációja szavakkal és a körre mutató nyíllal. A bal alsó sarokban található egy szövegdoboz Talos / fenyegetés grid intelligencia szavakkal és egy körre mutató nyíllal.

AMP   
Nyilvános/Privát   
Cloud Sandboxing Talos/Threat Grid   
Intelligencia Harmadik fél   
Integráció Következő   
Generáció   
Tűzfal Következő   
Generáció   
IPS végpont   
HIDS   
Érzékelők Egyéb   
Infrastruktúra   
Eszközök ESA WSA telepítési kiberbiztonsági műveletek

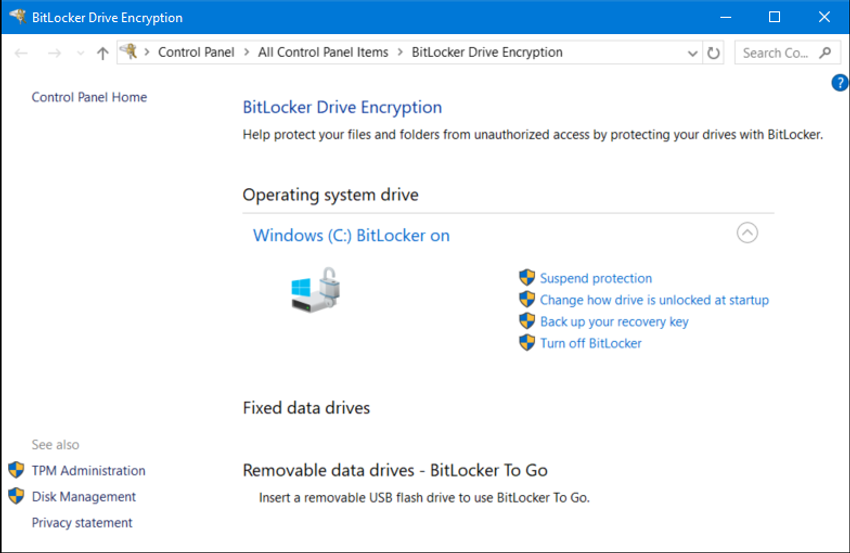
13.1.6

## Helyi adatok hardveres és szoftveres titkosítása

A végpontok is érzékenyek az adatlopásra. Például, ha egy vállalati laptop elveszik vagy ellopják, a tolvaj átkutathatja a merevlemezt érzékeny információk, kapcsolatfelvételi adatok, személyes adatok és egyebek után.

A megoldás a lemezmeghajtó helyi titkosítása erős titkosítási algoritmussal, például 256 bites AES titkosítással. A titkosítás megvédi a bizalmas adatokat az illetéktelen hozzáféréstől. A titkosított lemezkötetek csak normál olvasási/írási hozzáféréshez csatlakoztathatók az engedélyezett jelszóval.

Az olyan operációs rendszerek, mint a MAC OSX, natív módon biztosítanak titkosítási lehetőségeket. A Microsoft Windows 10 operációs rendszer natív titkosítást is biztosít. Az egyes fájlok, mappák és meghajtók konfigurálhatók adatok titkosítására. A Windows rendszerben a BitLocker meghajtótitkosítást biztosít, amint az az ábrán látható. A fájlok titkosíthatók is, de mivel az alkalmazások titkosítatlan biztonsági másolatokat készíthetnek, a teljes mappát, amelyben a fájl tárolja, titkosítani kell.



13.1.7

## Hálózati hozzáférés-szabályozás

A hálózati hozzáférés-vezérlés (NAC) célja, hogy csak engedélyezett és megfelelő rendszerek – akár felügyelt, akár nem menedzselt – férhessenek hozzá a hálózathoz. Egyesíti a végpont-biztonsági technológiákat a felhasználó- vagy eszközhitelesítéssel és a hálózati biztonsági szabályzat érvényesítésével. A NAC-rendszerek megtagadhatják a hálózati hozzáférést a nem megfelelő eszközöktől, karanténba helyezhetik azokat, vagy csak korlátozott hozzáférést biztosíthatnak a számítási erőforrásokhoz, így megóvják a nem biztonságos csomópontokat a hálózat megfertőzésétől.

A NAC rendszerek a következő képességekkel rendelkezhetnek:

* **Profilalkotás és láthatóság** – Ez felismeri és profilba hozza a felhasználókat és eszközeiket, mielőtt a rosszindulatú kód kárt okozna.
* **Vendéghálózati hozzáférés** – Ez egy testreszabható, önkiszolgáló portálon keresztül kezeli a vendégeket, amely magában foglalja a vendégregisztrációt, a vendéghitelesítést, a vendégszponzorálást és a vendégkezelési portált.
* **Biztonsági helyzet ellenőrzése** – Ez a felhasználó típusa, eszköztípusa és operációs rendszer szerint értékeli a biztonsági irányelveknek való megfelelést.
* **Reagálás az incidensekre** – Ez csökkenti a hálózati fenyegetéseket azáltal, hogy olyan biztonsági házirendeket kényszerít ki, amelyek blokkolják, elkülönítik és megjavítják a nem megfelelő gépeket rendszergazdai beavatkozás nélkül.

A NAC-rendszereknek ki kell terjeszteniük a NAC-t minden hálózati hozzáférési módra, beleértve a LAN-okon, távoli hozzáférési átjárókon és vezeték nélküli hozzáférési pontokon keresztüli hozzáférést.

A Cisco Identity Services Engine (ISE) egyetlen rendszerben egyesíti az AAA-t és a hálózati eszközök profilozását.

13.1.8

## NAC funkciók

A NAC-rendszerek célja annak biztosítása, hogy csak olyan gazdagépek lépjenek be a hálózatba, amelyek hitelesítettek, és amelyeknek biztonsági helyzetét megvizsgálták és jóváhagyták. Előfordulhat például, hogy egy bizonyos ideig nem telephelyen használt vállalati laptopok nem kapták meg az aktuális biztonsági frissítéseket, vagy megfertőződhettek más rendszerektől. Ezek a rendszerek nem csatlakozhatnak a hálózathoz, amíg meg nem vizsgálják, frissítik és jóváhagyják őket.

A hálózati hozzáférést biztosító eszközök végrehajtó rétegként működhetnek, amint az az ábrán látható. Arra kényszerítik az ügyfeleket, hogy hitelesítést és engedélyezést kérjenek egy RADIUS-kiszolgálótól. A RADIUS-kiszolgáló lekérdezhet más eszközöket, például egy víruskereső kiszolgálót, és válaszolhat a hálózati végrehajtóknak.

Az ábra olyan hálózati hozzáférési eszközöket mutat be, amelyek a biztonságot azáltal kényszerítik ki, hogy a felhasználóknak lekérdezniük kell egy RADIUS-kiszolgálót hitelesítéshez és engedélyezéshez.

### A hálózati hozzáférési eszközök erősítik a biztonságot

Végrehajtási hitelesítő adatok Hálózati hozzáférést próbáló állomások Hálózati hozzáférési eszközök Házirend-kiszolgáló döntése   
Pontok és kárelhárítás EAP/UDP,   
EAP/802.1x értesítési hitelesítő adatok Hozzáférési jogok hitelesítő adatok HTTPS AAA RADIUS kiszolgáló szállítói kiszolgálók

13.1.9

## Ellenőrizze, hogy megértette-e – a végpont biztonsági áttekintése

Az űrlap teteje

Ellenőrizze, hogy megértette-e a végpontok biztonságát, és válassza ki a megfelelő választ a következő kérdésekre.

1. Mi akadályozza meg, hogy a végpontok olyan webhelyekhez kapcsolódjanak, amelyek a legújabb hírnévintelligencia alapján rossz hírnévvel rendelkeznek?

Az űrlap alja

Mi védi meg a végpontokat a rosszindulatú szoftverektől?

Mi akadályozza meg az érzékeny információk elvesztését vagy ellopását?

Mi szűri ki a nem kívánt e-maileket, mielőtt azok elérnék a végpontot?

[13.0](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[13.2](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[802.1X Authentication](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                               
*                 

1. Endpoint Security
2. 802.1X Authentication

# 802.1X hitelesítés

13.2.1

## Biztonság 802.1X port alapú hitelesítéssel

Az IEEE 802.1X szabvány egy portalapú hozzáférés-vezérlési és hitelesítési protokollt határoz meg, amely megakadályozza, hogy a jogosulatlan munkaállomások nyilvánosan elérhető kapcsolóportokon keresztül csatlakozzanak a LAN-hoz. A hitelesítési kiszolgáló hitelesít minden munkaállomást, amely egy kapcsolóporthoz csatlakozik, mielőtt elérhetővé tenné a switch vagy a LAN által kínált szolgáltatásokat.

Az ábra azt mutatja, hogy a 802.1X port alapú hitelesítéssel a hálózatban lévő eszközök meghatározott szerepkörrel rendelkeznek.

Az ábra egy topológia diagram, amely 8 0 2,1 X szerepet mutat. Van egy hitelesítő feliratú kapcsoló egy hitelesítési szerverhez (sugár) csatlakozva. a kapcsoló két különálló számítógéphez is csatlakozik, amelyek supplicant felirattal vannak ellátva. A kapcsoló alatti szöveg azt mondja, hogy az ügyfél hitelesítési állapota alapján szabályozza a hálózathoz való fizikai hozzáférést. A szerver alatti szöveg kliens hitelesítést végez. A kérelmező számítógép állapotai alatti szöveg hozzáférést igényel, és válaszol a kapcsolótól érkező kérésekre.

### 802.1X topológia

Supplicant Authenticator Authentication Server (RADIUS) Kérelmező Hozzáférést igényel, és válaszol a kapcsoló kéréseire. Szabályozza a fizikai hozzáférést a hálózathoz az ügyfél hitelesítési állapota alapján Kliens hitelesítést hajt végre

A 802.1x szerepkörök a következők:

* **Kérelmező (kliens)** – Az az eszköz (munkaállomás), amely hozzáférést kér a LAN-hoz és a kapcsolószolgáltatásokhoz, majd válaszol a kapcsolótól érkező kérésekre. A munkaállomáson 802.1X-kompatibilis ügyfélszoftvernek kell futnia. (A port, amelyhez az ügyfél csatlakozik, a kérelmező [ kliens ] az IEEE 802.1X specifikációban.)
* **Hitelesítő (Switch)** – Ez az eszköz a kliens hitelesítési állapota alapján szabályozza a hálózathoz való fizikai hozzáférést. A kapcsoló közvetítőként (proxy) működik a kliens (kérő) és a hitelesítési szerver között, azonosító információkat kér a klienstől, ellenőrzi ezeket az információkat a hitelesítési szerverrel, és választ továbbít az ügyfélnek. A kapcsoló egy RADIUS szoftverügynököt használ, amely az EAP (Extensible Authentication Protocol) keretek tokozásáért és kicsomagolásáért, valamint a hitelesítési szerverrel való interakcióért felelős.
* **Hitelesítési szerver** – Ez a szerver végzi el az ügyfél tényleges hitelesítését. A hitelesítési kiszolgáló ellenőrzi a kliens azonosságát, és értesíti a kapcsolót, hogy az ügyfél jogosult-e a LAN-hoz és a kapcsolószolgáltatásokhoz. Mivel a kapcsoló proxyként működik, a hitelesítési szolgáltatás átlátható az ügyfél számára. Az EAP-kiterjesztésekkel rendelkező RADIUS biztonsági rendszer az egyetlen támogatott hitelesítési szerver.

A munkaállomás hitelesítéséig a 802.1X hozzáférés-vezérlés csak a LAN-on keresztüli kiterjeszthető hitelesítési protokoll (EAPOL), a Cisco Discovery Protocol (Cisco Discovery Protocol) és a Spanning Tree Protocol (STP) forgalmat engedélyezi azon a porton keresztül, amelyhez a munkaállomás csatlakozik. Miután a hitelesítés sikeres, a normál forgalom áthaladhat a porton.

A kapcsoló port állapota határozza meg, hogy az ügyfél megkapja-e a hozzáférést a hálózathoz. Ha 802.1X portalapú hitelesítésre van beállítva, a port nem engedélyezett állapotban indul. Ebben az állapotban a port nem engedélyez minden be- és kimenő forgalmat, kivéve a 802.1X protokollt, az STP- és CDP-csomagokat. Amikor egy kliens hitelesítése sikeresen megtörtént, a port átvált az engedélyezett állapotba, lehetővé téve a kliens számára a forgalom normális áramlását. Ha a kapcsoló kéri a kliens azonosítóját (hitelesítő kezdeményezése), és az ügyfél nem támogatja a 802.1X szabványt, a port jogosulatlan állapotban marad, és az ügyfél nem kap hozzáférést a hálózathoz.

Ezzel szemben, ha egy 802.1X-kompatibilis kliens csatlakozik egy porthoz, és a kliens elindítja a hitelesítési folyamatot (a kérelmező kezdeményezése) az EAPOL-start keret elküldésével egy olyan switch-re, amely nem futja a 802.1X protokollt, nem érkezik válasz, és az ügyfél elkezdi a keretek küldését, mintha a port engedélyezett állapotban lenne.

Az ábra a teljes üzenetváltást mutatja a kérelmező, a hitelesítő és a hitelesítő szerver között. A kapszulázás a következőképpen történik:

* **A kérelmező és a hitelesítő között** – az EAP adatok EAPOL keretekbe vannak zárva.
* **A hitelesítő és a hitelesítési szerver között** – az EAP-adatok RADIUS segítségével vannak beágyazva.

Az ábra a 8 0 2.1 X üzenetváltási folyamatot mutatja.

### 802.1X üzenetváltás

Supplicant Authenticator Authentication Server (RADIUS) EAPOL-Start EAP-Request/Identity EAP-Request/Identity EAP-Request/OTP (One-Time-Password) EAP-Response/OTP EAP-Success EAPOL-Logoff Access RADIUSRADIUS- Request Kihívás RADIUS-hozzáférés – Kérelem RADIUS-hozzáférés – Port elfogadása Jogosulatlan port EAPOL EAP RADIUS EAP

Ha a kliens hitelesítése sikeresen megtörtént (a kapcsoló „elfogadó” keretet kap a hitelesítési kiszolgálótól), a port állapota engedélyezettre változik, és a hitelesített klienstől származó összes keret engedélyezve van a porton keresztül.

Ha a hitelesítés sikertelen, a port jogosulatlan állapotban marad, de a hitelesítés újra megkísérelhető. Ha a hitelesítési kiszolgáló nem érhető el, a kapcsoló újraküldheti a kérést. Ha a megadott számú próbálkozás után nem érkezik válasz a kiszolgálótól, a hitelesítés meghiúsul, és a hálózati hozzáférés nem biztosított.

Amikor egy ügyfél kijelentkezik, EAPOL-kijelentkezési üzenetet küld, aminek következtében a kapcsolóport jogosulatlan állapotba kerül.

13.2.2

## A 802.1X engedélyezési állapot szabályozása

Szükséges lehet egy kapcsolóport konfigurálása a 802.1X hitelesítési folyamat felülbírálásához. Ehhez használja a **hitelesítési portvezérlő** interfész konfigurációs parancsot a port engedélyezési állapotának vezérléséhez. A parancs paraméterei alább láthatók. A hitelesítő kapcsoló egyedi portja ezzel a paranccsal van konfigurálva, ebben az esetben az S1 F0/1 portja. Alapértelmezés szerint egy port **kényszerengedélyezett** állapotban van, ami azt jelenti, hogy 802.1x hitelesítés nélkül is képes forgalmat küldeni és fogadni.

Az ábra egy topológiai diagram, amely a hitelesítési kiszolgáló és a kérelmező közötti Hitelesítő kapcsolót mutatja.

S1

F0/1

Supplicant Authenticator Authentication Server (RADIUS)

S1(config-if)# **authentication port-control ?**

auto PortState set to automatic

force-authorized PortState set to AUTHORIZED **<--default**

force-unauthorized PortState set to UnAuthorized

S1(config-if)# **authentication port-control**

| **Paraméter** | **Leírás** |
| --- | --- |
| **auto** | Engedélyezi a 802.1X port alapú hitelesítést, és a portot jogosulatlan állapotban indítja el. Ez idő alatt csak az EAPOL, az STP és a CDP keretek az egyetlen típusú keret, amely a porton keresztül küldhető vagy fogadható, amíg az ügyféleszközt nem hitelesítik. |
| **erőszakos felhatalmazással** | A port normál forgalmat küld és fogad az ügyfél 802.1x-alapú hitelesítése nélkül. Ez az alapértelmezett beállítás. |
| **erőszakos jogosulatlan** | A port jogosulatlan állapotban marad, figyelmen kívül hagyva az ügyfél minden hitelesítési kísérletét. A kapcsoló nem tud hitelesítési szolgáltatásokat nyújtani az ügyfélnek a porton keresztül. |

Az **automatikus** kulcsszót meg kell adni a 802.1X hitelesítés engedélyezéséhez. Ezért a 802.1X porton való engedélyezéséhez használja a **hitelesítési port-vezérlő automatikus** interfész konfigurációs parancsot.

Ha a kliens hitelesítése sikeresen megtörtént (Accept keretet kap a hitelesítési kiszolgálótól), a port állapota engedélyezettre változik, és a hitelesített klienstől származó összes keret átkerül a porton. Ha a hitelesítés sikertelen, a port jogosulatlan állapotban marad, de a hitelesítés újra megkísérelhető. Ha a hitelesítési kiszolgáló nem érhető el, a kapcsoló újra elküldheti a kérést. Ha a megadott számú próbálkozás után nem érkezik válasz a kiszolgálótól, a hitelesítés meghiúsul, és a hálózati hozzáférés nem biztosított.

Amikor egy ügyfél kijelentkezik, EAPOL-kijelentkezési üzenetet küld, aminek következtében a kapcsoló portja jogosulatlan állapotba vált.

Ha egy port kapcsolati állapota felülről lefelé változik, vagy ha EAPOL-kijelentkezési keret érkezik, a port visszatér a jogosulatlan állapotba.

13.2.3

## 802.1X konfiguráció

Ez a forgatókönyv ugyanazt a topológiát valósítja meg, mint fent. A kapcsoló F0/1 pontjához egy PC csatlakozik, és az eszközt 802.1X-en keresztül hitelesítik egy RADIUS szerverrel. Ellentétben a korábbi AAA-forgatókönyvekkel, amelyekben a rendszergazdákat hitelesítették az útválasztó konfigurációs soraihoz, ebben a forgatókönyvben a végpont hitelesítése a hálózathoz való hozzáférés megadása előtt megtörténik.

A 802.1X konfigurálása néhány alapvető lépést igényel:

**1. lépés** . Engedélyezze az AAA-t az **aaa new-model** paranccsal.   
**2. lépés** . Jelölje ki a RADIUS-kiszolgálót, és konfigurálja a címét és a portjait.   
**3. lépés** . Hozzon létre egy 802.1X portalapú hitelesítési metóduslistát az **aaa hitelesítési pont1x** paranccsal.   
**4. lépés** . Globálisan engedélyezze a 802.1X portalapú hitelesítést a **dot1x system-auth-control** paranccsal.   
**5. lépés** . Engedélyezze a portalapú hitelesítést az interfészen a **hitelesítés port-control auto** paranccsal.   
**6. lépés** . Engedélyezze a 802.1X hitelesítést az interfészen a **dot1x pae** paranccsal. A **hitelesítési** beállítások beállítják a Port Access Entity (PAE) típusát, így az interfész csak hitelesítőként működik, és nem válaszol a kérelmezőnek szánt üzenetekre.

Az alábbiakban egy példa konfiguráció látható.

S1(config)# **aaa new-model**

S1(config)# **radius server NETSEC**

S1(config-radius-server)# **address ipv4 10.1.1.50 auth-port 1812 acct-port 1813**

S1(config-radius-server)# **key RADIUS-Pa55w0rd**

S1(config-radius-server)# **exit**

S1(config)#

S1(config)# **aaa authentication dot1x default group radius**

S1(config)# **dot1x system-auth-control**

S1(config)#

S1(config)# **interface F0/1**

S1(config-if)# **description Access Port**

S1(config-if)# **switchport mode access**

S1(config-if)# **authentication port-control auto**

S1(config-if)# **dot1x pae authenticator**

13.2.4

## Szintaxis-ellenőrző – 802.1x port-hitelesítés konfigurálása

Ezzel a szintaktikai ellenőrzővel gyakorolhatja a 802.1X port-hitelesítés konfigurálását egy 2960-as kapcsolón.

Configure a RADIUS server on S1 using the following instructions:

* Enable AAA.
* Enter RADIUS server configuration mode and name the configuration **NETSEC**.
* Configure the RADIUS server address to **10.1.1.50** with the authentication port of **1812** and the accounting port of **1813**.
* Configure the shared secret key **RADIUS-Pa55w0rd**.
* Exit RADIUS configuration mode.

S1(config)#aaa new-model

S1(config)#radius server NETSEC

S1(config-radius-server)#address ipv4 10.1.1.50 auth-port 1812 acct-port 1813

S1(config-radius-server)#key RADIUS-Pa55w0rd

S1(config-radius-server)#exit

Hajtsa végre a következő lépéseket a 802.1x port alapú hitelesítés konfigurálásához:

* Adjon meg egy 802.1x portalapú alapértelmezett hitelesítési metóduslistát az elsődleges RADIUS beállítással.
* Globálisan engedélyezze a 802.1x port alapú hitelesítést.

S1(config)# aaa hitelesítés pont1x alapértelmezett csoportsugár

S1(config)# dot1x system-auth-control

Hajtsa végre a következő lépéseket a 802.1X hitelesítés engedélyezéséhez az interfészen:

* interfész konfigurációs módjába **Lépjen be az F0/1** .
* Konfigurálja az interfészt hozzáférési kapcsolóportként.
* Port-alapú hitelesítés engedélyezése az interfészen az **auto** paraméterrel.
* Engedélyezze a 802.1x hitelesítést a Port Access Entity (PAE) típussal, hogy az interfész csak hitelesítőként működjön.
* használja az **end parancsot.** A konfigurációs módból való kilépéshez

S1(config)# interfész F0/1

S1(config-if)# switchport mód hozzáférés

S1(config-if)# hitelesítési port-vezérlés auto

S1(config-if)# dot1x pae hitelesítő

S1(config-if)# vége

\*Mar 3 18:22:23.443: %SYS-5-CONFIG\_I: Konzolról konzolra konfigurálva

Sikeresen konfigurálta a 802.1x port-hitelesítést egy 2960-as kapcsolón.

[13.1](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Endpoint Security Overview](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[13.3](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Endpoint Security Summary](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                

1. Endpoint Security
2. Endpoint Security Summary

# Végpont biztonsági összefoglaló

13.3.1

## Mit tanultam ebben a modulban?

**Az Endpoint Security bemutatása**   
A végpontok hagyományosan PC-k, szerverek és nyomtatók voltak. A mai hálózatban azonban a végpontok közé tartoznak a telefonok, táblagépek, laptopok, Internet of Things eszközök, hálózati videokamerák és sok más dolog is. A végpontok biztonsága korábban gazdagép alapú biztonsági intézkedésektől függött, például kártevőirtó szoftvertől, gazdagép alapú IPS-től és gazdagép alapú tűzfalszoftvertől. Számos eszköz és technológia javítja a gazdagép alapú végpontvédelmet. Ezek közül néhány e-mail biztonsági berendezés, webes biztonsági berendezés, NAC és a Cisco Identity Services Engine. A végpontok adatvesztés elleni védelmének másik módja a helyi adatok fájl-, mappa- vagy meghajtószintű titkosítása. Erre a célra a Microsoft Windows 10-hez olyan szoftverek tartoznak, mint a BitLocker.

A hálózati hozzáférés-vezérlés egy olyan rendszer, amely képes ellenőrizni, hogy a hálózatot megkísérlő végpontok megfelelnek-e a hálózati biztonsági szabályzatoknak. Kezeli a felhasználói hitelesítést, és felléphet olyan eszközök ellen, amelyek sértik a biztonsági irányelveket, mivel elavult biztonsági szoftverrel rendelkeznek. Még a hozzáférés engedélyezése előtt is intézkedhet annak érdekében, hogy az eszközök megfeleljenek a megfelelőségi szabványnak. A NAC könnyen kezelhető módszereket is kínálhat a hálózathoz való csatlakozást igénylő vendégszámítógépek hálózati hozzáférésének biztosítására. A Cisco ISE egyetlen rendszerben egyesíti az AAA-t és a NAC-t.

**802.1X hitelesítés**   
A 802.1X olyan eszközt biztosít, amellyel a hitelesítő hálózati hozzáférési kapcsoló közvetítőként működhet az ügyfél és a hitelesítési szerver között. A kapcsoló a hitelesítési információkat továbbítja a klienstől a szerver felé. Ha a hitelesítés sikeres, a kliens hozzáférhet a hálózathoz a csatlakoztatott kapcsolóporton keresztül. Ha az engedélyezés sikertelen, a kapcsoló nem engedi, hogy az ügyfélvégpont csatlakozzon a hálózathoz. A rendszer az EAP-t és az EAPOL-t használja a hitelesítési forgalom továbbítására a kapcsoló és a hitelesítő kapcsoló között. A kapcsoló EAP-t és RADIUS-t használ a hitelesítési szerverrel való kommunikációhoz. A 802.1X hitelesítési folyamat vezérelhető a hitelesítő portnak a **hitelesítési port-vezérlő** paranccsal történő konfigurálásával. A port beállítható a hitelesítési folyamat során, engedélyezett hozzáférést biztosíthat, vagy jogosulatlan állapotba kerülhet. Ebben az állapotban egyetlen eszköz sem tud csatlakozni a hálózathoz.

A 802.1X portalapú hitelesítés az AAA globális aktiválásával és a RADIUS-kiszolgáló nevének, címének és portjainak megadásával konfigurálható. Ezt követően a hitelesítő interfész 802.1X paraméterekkel konfigurálva van.

13.3.2

## 13. modul – Végpontbiztonsági kvíz

Az űrlap teteje

1. Egy kapcsoló a következő parancsot tartalmazza a 802.1X telepítés részeként.

**cím ipv4 10.1.1.50 hitelesítés - 1812-es port acct - 1813-as port**

Mi ennek a parancsnak a célja?

Az űrlap alja

Melyik eszközt használják hitelesítési kiszolgálóként a 802.1X megvalósításban?

Mi a NAC rendszer két fő képessége? (Válassz kettőt.)

Melyik Cisco készülék használható a hálózati forgalom tartalmának szűrésére a forgalom jelentésére és letiltására a webszerver hírneve alapján?

Melyik paranccsal engedélyezhető az AAA a 802.1X konfigurációs folyamat részeként egy Cisco-eszközön?

A kapcsolóport, amelyhez az ügyfél csatlakozik, a 802.1X protokollhoz van konfigurálva. Az ügyfélnek hitelesítenie kell magát, mielőtt adatokat továbbíthat a hálózatra. Melyik két 802.1X szerepkör közé vannak beágyazva az EAP-adatok RADIUS használatával? (Válassz kettőt.)

Melyik gazdagép alapú biztonsági intézkedést használják a bejövő és kimenő kapcsolatok korlátozására?

Melyik biztonsági szolgáltatást nyújtja a 802.1x?

Miért fontos a végpontok védelme?

A webhelyek minősítése a webhelyek legfrissebb hírnevére vonatkozó intelligencia alapján történik. Melyik végpont biztonsági intézkedés akadályozza meg, hogy a végpontok rossz besorolású webhelyekhez kapcsolódjanak?

Mikor **a hitelesítési port - vezérlő parancsot a 802.1X megvalósítás során?** használjuk

802.1X hitelesítés használatakor melyik eszköz szabályozza a hálózathoz való fizikai hozzáférést a kliens hitelesítési állapota alapján?

Egy portot konfiguráltak a 802.1X protokollhoz, és az ügyfél sikeresen hitelesítette. Melyik 802.1X állapot kapcsolódik ehhez a számítógéphez?

[13.2](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[802.1X Authentication](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[14.0](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                      
*               

1. Layer 2 Security Considerations
2. Introduction

# Bevezetés

14.0.1

## Miért vegyem ezt a modult?

A biztonság csak annyira erős, mint a leggyengébb láncszem. A 2. réteg hozzáférést biztosít a hálózat felhasználói számára, és a hálózati infrastruktúra lényeges részét képezi. A 2. rétegű eszközök redundanciát biztosítanak azáltal, hogy több nagy sebességű útvonalat kínálnak a hálózat nagy szegmenseinek összekapcsolásához. Azáltal, hogy hozzáférést biztosít az összes belső hálózati felhasználó számára, hozzáférést biztosít a fenyegetés szereplőinek is, akik megpróbálhatják lerombolni a hálózati infrastruktúrát. Ezért hálózati biztonsági adminisztrátorként gondosan ügyelnie kell a 2. rétegbeli infrastruktúrát érő fenyegetések mérséklésére. Folytassa az olvasást, hogy többet megtudjon a 2. réteget fenyegető számos lehetséges fenyegetésről, valamint az e fenyegetések enyhítésére rendelkezésre álló különféle eszközökről. A 2. réteg a leggyengébb láncszem!

14.0.2

## Mit fogok tanulni ebben a modulban?

**Modul címe:** 2. rétegbeli biztonsági szempontok

**Modul célja** : Biztonsági intézkedések végrehajtása a 2. rétegbeli támadások mérséklésére.

| **téma címe** | **Téma Cél** |
| --- | --- |
| **2. réteg biztonsági fenyegetések** | Ismertesse a 2. rétegbeli sebezhetőségeket. |
| **MAC asztali támadások** | Ismertesse a MAC-címhamisítási támadásokat. |
| **Csökkentse a MAC asztali támadásokat** | Konfigurálja a port biztonságát. |
| **Csökkentse a VLAN-támadásokat** | Magyarázza el, hogyan mérsékelheti a VLAN-támadásokat. |
| **Mérsékelje a DHCP-támadásokat** | Használja a megfelelő parancsokat a DHCP Snooping megvalósításához a támadások mérséklése érdekében. |
| **Az ARP támadások mérséklése** | Használja a megfelelő parancsokat az ARP-támadások mérséklésére. |
| **Csökkentse a címhamisítási támadásokat** | Használja a megfelelő parancsokat a címhamisítási támadások mérséklésére. |
| **Spanning Tree Protocol** | Ismertesse a Spanning Tree Protocol működését! |
| **Csökkentse az STP-támadásokat** | Konfiguráljon biztonsági intézkedéseket az STP-támadások mérséklésére. |

[13.3](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Endpoint Security Summary](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[14.1](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Layer 2 Security Threats](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                       
*               

1. Layer 2 Security Considerations
2. Layer 2 Security Threats

# 2. réteg biztonsági fenyegetések

14.1.1

## Ismertesse a 2. rétegbeli sebezhetőségeket

Az OSI referenciamodell hét rétegre oszlik, amelyek egymástól függetlenül működnek. Amint az ábrán látható, minden réteg egy meghatározott funkciót lát el, és vannak olyan alapvető elemei, amelyeket ki lehet használni.

Az ábra az OSI modell rétegeit és azok funkcióit mutatja be.

HTTP, HTTPS, POP3, IMAP, SSL, SSH, … Protokollok / Portok IP-címek Ethernet keretek Fizikai kapcsolatok 7 6 5 4 3 2 1 Alkalmazás bemutatás Munkamenet Szállítás Hálózati Adatkapcsolat Fizikai

A hálózati rendszergazdák rutinszerűen biztonsági megoldásokat vezetnek be a 3. rétegtől a 7. rétegig terjedő elemek védelmére VPN-ek, tűzfalak és IPS-eszközök segítségével. Azonban, amint az alábbi ábrán látható, ha a 2. réteg sérül, akkor a felette lévő összes réteg is érintett. Például, ha egy alkalmazott vagy látogató, aki hozzáfér a belső hálózathoz, képes rögzíteni a 2. rétegbeli képkockákat, akkor a fenti rétegeken megvalósított összes biztonság haszontalan lenne. Az alkalmazott a 2. rétegbeli LAN hálózati infrastruktúrában is pusztítást okozhat.

Az ábra azt mutatja, hogy ha a 2. réteg veszélybe kerül, akkor az összes fenti réteg is az.

### Az alacsonyabb szintek a magasabb szinteket érintik

HTTP, HTTPS, POP3, IMAP, SSL, SSH, … Protokollok / Portok IP-címek Ethernet keretek Fizikai linkek Kezdeti kompromisszum sérülve 7 6 5 4 3 2 1 Alkalmazás bemutatása Munkamenet Adatkapcsolat Hálózat Szállítási Fizikai

14.1.2

## Válts támadási kategóriákat

A biztonság csak annyira erős, mint a rendszer leggyengébb láncszeme, és a 2. réteget tekintik ennek a leggyengébb láncszemnek. Ennek az az oka, hogy hagyományosan a LAN-ok egyetlen szervezet adminisztratív irányítása alatt álltak. Alapvetően megbíztunk minden olyan személyben és eszközben, aki a LAN-unkhoz kapcsolódik. Manapság a BYOD és a kifinomultabb támadások révén LAN-jaink sebezhetőbbé váltak a behatolásokkal szemben. Ezért a Layer 3-Layer 7 védelme mellett a hálózatbiztonsági szakembereknek mérsékelniük kell a 2. rétegbeli LAN-infrastruktúra elleni támadásokat is.

A 2. rétegbeli infrastruktúra elleni támadások mérséklésének első lépése a 2. réteg alapvető működésének és a 2. rétegbeli infrastruktúra által jelentett fenyegetéseknek a megértése.

A 2. rétegbeli LAN-infrastruktúra elleni támadásokat a táblázat kiemeli.

**Megjegyzés** : Ennek a modulnak a középpontjában a gyakori Layer 2 támadások állnak.

| **típus** | **Leírás** |
| --- | --- |
| MAC asztali támadások | Tartalmazza a MAC-tábla túlcsordulási (más néven MAC-cím-elárasztási) támadásokat. |
| VLAN támadások | Tartalmazza a VLAN ugrás és a VLAN kettős címkézéses támadásokat. Ez magában foglalja a közös VLAN-on lévő eszközök közötti támadásokat is. |
| DHCP támadások | Tartalmazza a DHCP-éheztetést és a DHCP-hamisítási támadásokat. |
| ARP támadások | Tartalmazza az ARP-hamisítást és az ARP-mérgezési támadásokat. |
| Címhamisítási támadások | Tartalmazza a MAC- és IP-cím-hamisítási támadásokat. |
| STP támadások | Tartalmazza a Spanning Tree Protocol manipulációs támadásait. |

Az alábbi ábra áttekintést nyújt a Cisco megoldásokról, amelyek segítenek a Layer 2 támadások mérséklésében.

Az ábra egy piramis, amelynek négy szintje fentről lefelé, IPSG, DAI, DHCP leskelődés és portbiztonság.

Portbiztonság DHCP Snooping DAI IPSG

| **téma címe** | **Téma Cél** |
| --- | --- |
| Kikötői biztonság | A portbiztonság számos típusú támadást megakadályoz, beleértve a MAC tábla túlcsordulási támadásait és a DHCP éhezési támadásokat. |
| DHCP leskelődés | A DHCP Snooping megakadályozza a DHCP éhezést és a DHCP hamisítást a gazember DHCP szerverek által. |
| Dinamikus ARP ellenőrzés (DAI) | A DAI megakadályozza az ARP-hamisítást és az ARP-mérgezést okozó támadásokat. |
| IP Source Guard (IPSG) | Az IP Source Guard megakadályozza a MAC- és IP-címhamisítási támadásokat. |

Ezek a 2. rétegbeli megoldások nem lesznek hatékonyak, ha a felügyeleti protokollok nincsenek biztonságosak. Példa erre, ha a támadók könnyen telnet-elhetnek egy switchbe. A Syslog, az SNMP, a TFTP, a telnet, az FTP és a legtöbb egyéb általános hálózatkezelési protokoll nem biztonságos. Ezért a következő stratégiák alkalmazása javasolt:

* Mindig használja e protokollok biztonságos változatait, például az SSH-t, az SCP-t és az SSL-t.
* Fontolja meg a sávon kívüli (OOB) felügyelet használatát.
* Használjon dedikált felügyeleti VLAN-t, ahol csak a felügyeleti forgalom található.
* Használjon ACL-eket a nem kívánt hozzáférés kiszűrésére.

14.1.3

## Ellenőrizze megértését – azonosítsa a 2. rétegbeli veszélyeket és mérséklő intézkedéseket

### 2. réteg támadások és mérséklés

Az űrlap teteje

Ellenőrizze, hogy megértette-e a 2. rétegbeli támadásokat és azok mérséklését, és válassza ki a megfelelő választ a következő kérdésekre.

1. Milyen típusú támadás történik, amikor egy fenyegetőző hamis MAC- vagy IP-című csomagokat küld?

Az űrlap alja

Mi akadályozza meg a sokféle támadást, beleértve a MAC-tábla túlcsordulási támadásait és a DHCP-éheztetési támadásokat?

Milyen típusú támadások küldenek hamis címkéréseket a szervernek, amíg az összes címet fel nem használják, és egyik sem válik elérhetővé a jogos felhasználók számára?

Mi akadályozza meg a DHCP éhezést és hamisítást?

Mi akadályozza meg a MAC- és IP-címhamisító támadásokat?

[14.0](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[14.2](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[MAC Table Attacks](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                          
*               

1. Layer 2 Security Considerations
2. MAC Table Attacks

# MAC asztali támadások

14.2.1

## Kapcsolja át az alapokat

A kapcsolók MAC-címeket használnak a keretek továbbítására (vagy elvetésére) a hálózat más eszközeire. Ha egy kapcsoló csak továbbítana minden keretet, amelyet az összes porton keresztül kapott, akkor a hálózat annyira túlterhelt lenne, hogy valószínűleg teljesen leállna.

A 2. rétegű Ethernet switch 2. rétegű MAC-címeket használ a továbbítási döntések meghozatalához. Teljesen nem ismeri a keret adatrészében hordozott adatokat (protokollt), például IPv4-csomagot, ARP-üzenetet vagy IPv6 ND-csomagot. A switch kizárólag a 2. rétegű Ethernet MAC-címek alapján hozza meg a továbbítási döntéseit.

Az Ethernet switch megvizsgálja a MAC-címtáblázatát, hogy minden egyes keretre vonatkozóan továbbítási döntést hozzon, ellentétben az örökölt Ethernet-elosztókkal, amelyek a bejövő port kivételével az összes portot megismétlik. Az ábrán a négyportos kapcsoló éppen be volt kapcsolva. A táblázat a MAC-címtáblázatot mutatja, amely még nem tanulta meg a négy csatlakoztatott számítógép MAC-címét.

**Megjegyzés** : A MAC-címek rövidítése ebben a témakörben bemutatás céljából.

A diagram négy gazdagépet mutat be a hozzájuk tartozó MAC-címekkel együtt, amelyek egy switch 1-4 portjaihoz csatlakoznak. A portokat MAC-címekre leképező MAC-címtábla jelenleg üres.

A B C D 1 2 3

4

| Táblázat felirata | |
| --- | --- |
| **MAC-cím táblázat** | |
| **Kikötő** | **Mac cím** |
|  |  |
|  |  |

MAC   
00-0A MAC   
00-0B MAC   
00-0C MAC   
00-0D

A kapcsoló MAC-címtáblázata üres.

**Megjegyzés** : A MAC-címtáblázatot néha tartalomcímezhető memória (CAM) táblának is nevezik. Míg a CAM-tábla kifejezés meglehetősen gyakori, ebben a kurzusban MAC-címtáblázatként fogjuk hivatkozni rá.

14.2.2

## Váltás a tanulás és továbbítás között

A kapcsoló dinamikusan építi fel a MAC-címtáblázatot azáltal, hogy megvizsgálja a porton fogadott keretek forrás MAC-címét. A kapcsoló úgy továbbítja a kereteket, hogy egyezést keres a keretben lévő cél MAC-cím és a MAC-címtáblázat bejegyzése között.

Kattintson a Tanulás és Továbbítás gombra a folyamat illusztrációjához és magyarázatához.

**Vizsgálja meg a forrás MAC-címét**

Minden kapcsolóba belépő keretet ellenőriznek, hogy új információkat találjanak. Ezt úgy teszi, hogy megvizsgálja a keret forrás MAC-címét és a port számát, ahol a keret belépett a kapcsolóba. Ha a forrás MAC-cím nem létezik, akkor a bejövő portszámmal együtt hozzáadódik a táblázathoz. Ha a forrás MAC-cím létezik, a kapcsoló frissíti a frissítési időzítőt az adott bejegyzéshez a táblázatban. Alapértelmezés szerint a legtöbb Ethernet switch 5 percig megőrzi a bejegyzést a táblázatban.

Az ábrán például a PC-A Ethernet keretet küld a PC-D-nek. A táblázat azt mutatja, hogy a kapcsoló hozzáadja a PC-A MAC-címét a MAC-címtáblázathoz.

**Megjegyzés** : Ha a forrás MAC-címe létezik a táblázatban, de egy másik porton, a kapcsoló ezt új bejegyzésként kezeli. A bejegyzés helyére ugyanaz a MAC-cím kerül, de az aktuálisabb portszám.

Az ábrán négy gazdagép, A-D, egy kapcsolóhoz csatlakozik az 1-4 portokon. A 00-0A MAC-című A gazdagép (ebben a példában leegyszerűsítve) az 1-es porton lévő kapcsolóhoz csatlakozik. Az A gazdagép egy keretet küld a cél MAC-címe 00-0D. A keretben lévő MAC forrás 00-0A. A kapcsoló leképezi az 1-es portot a 00-0A MAC-címre a MAC-címtáblázatában.

A B C D 1 2 3

4

| Táblázat felirata | |
| --- | --- |
| **MAC-cím táblázat** | |
| **Kikötő** | **Mac cím** |
| 1 | 00-0A |
|  |  |

MAC   
00-0A MAC   
00-0B MAC   
00-0C MAC   
00-0D Cél MAC   
00-0D Forrás MAC   
00-0A típusú adat FCS

1. A PC-A Ethernet keretet küld.
2. A kapcsoló hozzáadja a PC-A portszámát és MAC-címét a MAC-címtáblázathoz.

14.2.3

## Keretek szűrése

Mivel egy kapcsoló különböző eszközökről fogad kereteket, képes feltölteni a MAC-címtáblázatát minden egyes keret forrás MAC-címének vizsgálatával. Ha a kapcsoló MAC-címtáblázata tartalmazza a cél MAC-címét, akkor képes a keret szűrésére és egyetlen portra továbbítani.

Kattintson az egyes gombra, ha egy illusztrációt és magyarázatot szeretne látni arról, hogyan szűri a kapcsoló a kereteket.

Az ábrán a PC-D a PC-A-nak válaszol. A kapcsoló a PC-D MAC-címét látja a bejövő keretben a 4-es porton. A kapcsoló ezután elhelyezi a PC-D MAC-címét a 4-es porthoz tartozó MAC-címtáblázatba.

Az ábrán négy A-D gazdagép látható, amelyek egy kapcsolóhoz csatlakoznak az 1-4 portokon. A 00-0D MAC-című D gazdagép a 4-es porton csatlakozik a switch-hez. A D gazdagép egy keretet küld, amelynek MAC-címe 00 -0A és 00-0D forrás MAC. A kapcsoló leképezi a 4-es portot a 00-0D MAC-címre a MAC-címtáblázatában.

A B C D 1 2 3

4

| Táblázat felirata | |
| --- | --- |
| **MAC-cím táblázat** | |
| **Kikötő** | **Mac cím** |
| 1 | 00-0A |
| 4 | 00-0D |

MAC   
00-0A MAC   
00-0B MAC   
00-0C MAC   
00-0D Cél MAC   
00-0A Forrás MAC   
00-0D Típusadatok ​ FCS

A kapcsoló hozzáadja a PC-D portszámát és MAC-címét a MAC-címtáblázatához.

14.2.4

## MAC-címtábla elárasztása

Minden MAC-tábla fix méretű, és ennek következtében a kapcsolók kifogyhatnak a MAC-címek tárolására szolgáló erőforrásokból. A MAC-címeket elárasztó támadások kihasználják ezt a korlátozást azáltal, hogy hamis forrású MAC-címekkel bombázzák a kapcsolót, amíg a kapcsoló MAC-címtáblája meg nem telik.

Amikor ez megtörténik, a kapcsoló a keretet ismeretlen unicastként kezeli, és elkezdi elárasztani az összes bejövő forgalmat ugyanazon a VLAN-on az összes porton anélkül, hogy a MAC-táblára hivatkozna. Ez a feltétel most lehetővé teszi, hogy a fenyegetés szereplője rögzítse az egyik gazdagéptől a másikra küldött összes keretet a helyi LAN-on vagy helyi VLAN-on.

**Megjegyzés** : A forgalom csak a helyi LAN-on vagy VLAN-on belül van elárasztva. A fenyegetés szereplője csak azon a helyi LAN-on vagy VLAN-on belül tudja rögzíteni a forgalmat, amelyhez a fenyegetőző csatlakozik.

Az ábra azt mutatja, hogy a fenyegetés szereplői hogyan használhatják egyszerűen a hálózati támadási eszköz **macof-ot** a MAC-címtáblázat túlcsordulására.

Az ábrán egy kapcsolóhoz csatlakoztatott számítógép látható, mellette a V LAN feliratú felhő 10. A fenyegetés szereplőjétől a kapcsoló felé mutató nyíl 1. A kapcsoló felirata 2. egy nyíl a kapcsolótól a kapcsolóig. kezelni színész 3. A fenyegető színész 4

1 2 3

4

Fenyegetés Actor VLAN 10

1. A fenyegetés szereplője a VLAN 10-hez csatlakozik, és **a macof** segítségével gyorsan generál sok véletlenszerű forrás- és cél MAC- és IP-címet.
2. Rövid időn belül megtelik a kapcsoló MAC-táblázata.
3. Amikor a MAC-tábla megtelik, a kapcsoló elkezdi elárasztani az összes fogadott keretet. Amíg **a macof** fut, a MAC-tábla tele marad, és a kapcsoló továbbra is elárasztja az összes bejövő keretet a VLAN 10-hez társított minden porton.
4. A fenyegetés szereplője ezután csomagszimuláló szoftvert használ a képkockák rögzítésére a VLAN 10-hez csatlakoztatott bármely eszközről.

Ha a fenyegetés szereplője leállítja **a macof** futását, vagy felfedezik és leállítják, a kapcsoló végül kiöregíti a régebbi MAC-cím bejegyzéseket a táblázatból, és újra kapcsolóként kezd működni.

14.2.5

## MAC-címtábla támadások mérséklése

Az olyan eszközöket, mint **a macof,** az teszi annyira veszélyessé, hogy a támadó nagyon gyorsan képes MAC-tábla túlcsordulási támadást létrehozni. Például egy Catalyst 6500 kapcsoló 132 000 MAC-címet tud tárolni a MAC-címtáblázatában. Egy olyan eszköz, mint **a macof,** másodpercenként akár 8000 hamis képkockával is eláraszthat egy kapcsolót; néhány másodperc alatt létrehoz egy MAC-címtábla túlcsordulási támadást. parancs minta kimenetét mutatja **A példa a macof** egy Linux gazdagépen.

# **macof -i eth1**

36:a1:48:63:81:70 15:26:8d:4d:28:f8 0.0.0.0.26413 > 0.0.0.0.49492: S 1094191437:1094191437(0) win 512

16:e8:8:0:4d:9c da:4d:bc:7c:ef:be 0.0.0.0.61376 > 0.0.0.0.47523: S 446486755:446486755(0) win 512

18:2a:de:56:38:71 33:af:9b:5:a6:97 0.0.0.0.20086 > 0.0.0.0.6728: S 105051945:105051945(0) win 512

e7:5c:97:42:ec:1 83:73:1a:32:20:93 0.0.0.0.45282 > 0.0.0.0.24898: S 1838062028:1838062028(0) win 512

62:69:d3:1c:79:ef 80:13:35:4:cb:d0 0.0.0.0.11587 > 0.0.0.0.7723: S 1792413296:1792413296(0) win 512

c5:a:b7:3e:3c:7a 3a:ee:c0:23:4a:fe 0.0.0.0.19784 > 0.0.0.0.57433: S 1018924173:1018924173(0) win 512

88:43:ee:51:c7:68 b4:8d:ec:3e:14:bb 0.0.0.0.283 > 0.0.0.0.11466: S 727776406:727776406(0) win 512

b8:7a:7a:2d:2c:ae c2:fa:2d:7d:e7:bf 0.0.0.0.32650 > 0.0.0.0.11324: S 605528173:605528173(0) win 512

e0:d8:1e:74:1:e 57:98:b6:5a:fa:de 0.0.0.0.36346 > 0.0.0.0.55700: S 2128143986:2128143986(0) win 512

Egy másik ok, amiért ezek a támadóeszközök veszélyesek, az az, hogy nemcsak a helyi kapcsolót érintik, hanem más csatlakoztatott 2. rétegbeli kapcsolókat is. Amikor egy kapcsoló MAC-címtáblázata megtelik, elkezdi elárasztani az összes portot, beleértve azokat is, amelyek más Layer 2 switchekhez csatlakoznak.

A MAC-címtáblázat túlcsordulási támadásainak mérséklése érdekében a hálózati rendszergazdáknak be kell vezetniük a portbiztonságot. A portbiztonság csak meghatározott számú forrás MAC-cím megtanulását teszi lehetővé a porton. A port biztonságáról a modul későbbi részében lesz szó.

[14.1](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Layer 2 Security Threats](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[14.3](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Mitigate MAC Table Attacks](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                   
*               

1. Layer 2 Security Considerations
2. Mitigate MAC Table Attacks

# Csökkentse a MAC asztali támadásokat

14.3.1

## Biztonságos nem használt portok

A 2. rétegű eszközöket a vállalat biztonsági infrastruktúrájának leggyengébb láncszemének tekintik. A 2. rétegű támadások a legegyszerűbben telepíthetők a hackerek számára, de ezek a fenyegetések néhány gyakori 2. rétegű megoldással is mérsékelhetők.

Az összes kapcsolóportot (interfészt) rögzíteni kell, mielőtt a kapcsolót üzemi használatra telepítenék. A portok biztonsága a funkciójától függ.

Egy egyszerű módszer, amellyel sok rendszergazda segít megvédeni a hálózatot az illetéktelen hozzáféréstől, az, hogy letiltja a kapcsoló összes nem használt portját. Például, ha egy Catalyst 2960 switch 24 porttal rendelkezik, és három Fast Ethernet kapcsolat van használatban, célszerű letiltani a 21 használaton kívüli portot. Keresse meg az egyes nem használt portokat, és adja ki a Cisco IOS **leállítási** parancsát. Ha egy portot később újra aktiválni kell, akkor a **no shutdown** paranccsal engedélyezhető.

Porttartomány konfigurálásához használja az **interface range** parancsot.

Switch(config)# **interface range** type module/first-number - last-number

Például az S1-en az Fa0/8–Fa0/24 portok leállításához a következő parancsot kell beírnia.

S1(config)# **interface range fa0/8 - 24**

S1(config-if-range)# **shutdown**

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

(output omitted)

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down

S1(config-if-range)#

14.3.2

## Csökkentse a MAC-címtáblázat támadásait

A MAC-címtábla túlcsordulási támadásainak megelőzésének legegyszerűbb és leghatékonyabb módja a portbiztonság engedélyezése.

A portbiztonság korlátozza a porton engedélyezett érvényes MAC-címek számát. Lehetővé teszi az adminisztrátor számára, hogy manuálisan konfigurálja a MAC-címeket egy porthoz, vagy engedélyezze a switch számára, hogy dinamikusan tanuljon meg korlátozott számú MAC-címet. Amikor egy portbiztonsággal konfigurált port keretet kap, a keret forrás MAC-címét a rendszer összehasonlítja a porton kézzel konfigurált vagy dinamikusan megtanult biztonságos forrás MAC-címek listájával.

Egy porton az engedélyezett MAC-címek számának egyre korlátozásával a portbiztonság segítségével ellenőrizhető a hálózathoz való jogosulatlan hozzáférés, amint az az ábrán látható.

A grafikon három eszközhöz csatlakoztatott kapcsoló látható. A kapcsoló felett található egy MAC-címtábla 0/1-es porttal, megengedett MAC AA:AA:AA, 0/2-es MAC BB:BB:BB és 0/2-es MAC CC:CC:CC porttal. A kapcsoló azt a 0/1 portot mutatja, amely AA:AA:AA MAC-című számítógéphez csatlakozik. Ezen a linken zöld pipa látható. Ezután a kapcsoló 0/2-es portja egy rosszindulatú laptophoz csatlakozik, amelynek MAC-címe BA:AD:01. A linken van egy piros kör, amelyen keresztül egy vonal van. A kapcsoló 0/3-as portja szintén egy BA:AD:02 MAC-című, rosszindulatú laptophoz csatlakozik. Ezen a linken is van egy piros kör, amelyen egy vonal van.

MAC: AA:AA:AA MAC: BA:AD:01 MAC: BA:AD:02 0/1 0/2 0/3 Port engedélyezett MAC 0/1 0/2 0/3 AA:AA:AA BB:BB :BB CC:CC:CC

**Megjegyzés** : A MAC-címek 24 bitesek az egyszerűség kedvéért.

14.3.3

## Port Security engedélyezése

Figyeljük meg a példában, hogy a **switchport port-security** parancsot elutasították. Ennek az az oka, hogy a portbiztonság csak manuálisan konfigurált hozzáférési portokon vagy manuálisan konfigurált fővonali portokon konfigurálható. Alapértelmezés szerint a 2. rétegbeli kapcsolóportok dinamikus automatikusra vannak állítva (trunking bekapcsolva). Ezért a példában a port a **switchport mód hozzáférési** interfész konfigurációs paranccsal van konfigurálva.

**Megjegyzés** : A trönk portok biztonsága túlmutat a tanfolyam keretein.

S1(config)# **interface f0/1**

S1(config-if)# **switchport port-security**

Command rejected: FastEthernet0/1 is a dynamic port.

S1(config-if)# **switchport mode access**

S1(config-if)# **switchport port-security**

S1(config-if)# **end**

S1#

Használja a **show port-security interface** parancsot a FastEthernet 0/1 aktuális portbiztonsági beállításainak megjelenítéséhez, az alábbi példában látható módon. Figyelje meg, hogy a portbiztonság engedélyezve van, és a port állapota Biztonságos leállítás, ami azt jelenti, hogy nincsenek csatlakoztatva eszközök, és nem történt megsértés. Ezenkívül a szabálysértési mód a Leállítás, és a megengedett maximális MAC-címek száma 1. Ha egy eszköz csatlakozik a porthoz, a kapcsoló port állapota a Secure-up feliratot jeleníti meg, és a kapcsoló automatikusan hozzáadja az eszköz MAC-címét biztonságosként. MAC. Ebben a példában egyetlen eszköz sem csatlakozik a porthoz.

S1# **show port-security interface f0/1**

Port Security : Enabled

Port Status : Secure-down

Violation Mode : Shutdown

Aging Time : 0 mins

Aging Type : Absolute

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 1

Total MAC Addresses : 0

Configured MAC Addresses : 0

Sticky MAC Addresses : 0

Last Source Address:Vlan : 0000.0000.0000:0

Security Violation Count : 0

S1#

**Megjegyzés** paranccsal van konfigurálva **: Ha egy aktív port a switchport port-security** , és egynél több eszköz csatlakozik ahhoz a porthoz, a port átvált hibaletiltás állapotba. Ezt a feltételt ebben a témakörben később tárgyaljuk.

A portbiztonság engedélyezése után más portbiztonsági jellemzők is konfigurálhatók a példában látható módon.

S1(config-if)# **switchport port-security ?**

aging Port-security aging commands

mac-address Secure mac address

maximum Max secure addresses

violation Security violation mode

S1(config-if)# **switchport port-security**

14.3.4

## Korlátozza és tanulja meg a MAC-címeket

A porton engedélyezett MAC-címek maximális számának beállításához használja a következő parancsot:

Switch(config-if)#  **switchport port-security maximális**  értéke

A port alapértelmezett biztonsági értéke 1. A konfigurálható biztonságos MAC-címek maximális száma a kapcsolótól és az IOS-től függ. Ebben a példában a maximum 8192.

S1(config)# **interface f0/1**

S1(config-if)# **switchport port-security maximum ?**

<1-8192> Maximum addresses

S1(config-if)# **switchport port-security maximum**

A kapcsolót háromféleképpen lehet beállítani úgy, hogy megismerje a biztonságos porton lévő MAC-címeket:

**1 . Manuálisan konfigurált**

A rendszergazda manuálisan konfigurál egy statikus MAC-cím(eke)t a következő paranccsal a porton lévő minden biztonságos MAC-címhez:

Switch(config-if)#  **switchport port-security mac-address**  mac-address

**2 . Dinamikusan tanult**

A **switchport port-security** parancs beírásakor a porthoz csatlakoztatott eszköz aktuális forrás-MAC-ja automatikusan védetté válik, de nem kerül hozzáadásra az indítási konfigurációhoz. Ha a kapcsolót újraindítják, a portnak újra meg kell tanulnia az eszköz MAC-címét.

**3 . Dinamikusan tanult – ragadós**

Az adminisztrátor a következő paranccsal engedélyezheti a kapcsoló számára, hogy dinamikusan tanulja meg a MAC-címet, és „ragassza” őket a futó konfigurációhoz:

Switch(config-if)# **switchport port-security mac-address sticky**

A futó konfiguráció mentése a dinamikusan tanult MAC-címet véglegesíti az NVRAM-ban.

A következő példa a FastEthernet 0/1 teljes portbiztonsági konfigurációját mutatja be, a Fa0/1 porthoz csatlakoztatott gazdagéppel. Az adminisztrátor legfeljebb 2 MAC-címet ad meg, manuálisan konfigurál egy biztonságos MAC-címet, majd a portot úgy konfigurálja, hogy dinamikusan tanulja meg a további biztonságos MAC-címeket a 2 biztonságos MAC-cím erejéig. használja a **show port-security interface** és a **show port-security address parancsot.** A konfiguráció ellenőrzéséhez

\*Mar 1 00:12:38.179: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up

\*Mar 1 00:12:39.194: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

S1#**conf t**

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)#

S1(config)# **interface fa0/1**

S1(config-if)# **switchport mode access**

S1(config-if)# **switchport port-security**

S1(config-if)# **switchport port-security maximum 2**

S1(config-if)# **switchport port-security mac-address aaaa.bbbb.1234**

S1(config-if)# **switchport port-security mac-address sticky**

S1(config-if)# **end**

S1# **show port-security interface fa0/1**

Port Security : Enabled

Port Status : Secure-up

Violation Mode : Shutdown

Aging Time : 0 mins

Aging Type : Absolute

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 2

Total MAC Addresses : 2

Configured MAC Addresses : 1

Sticky MAC Addresses : 1

Last Source Address:Vlan : a41f.7272.676a:1

Security Violation Count : 0

S1# **show port-security address**

Secure Mac Address Table

-----------------------------------------------------------------------------

Vlan Mac Address Type Ports Remaining Age

(mins)

---- ----------- ---- ----- -------------

1 a41f.7272.676a SecureSticky Fa0/1 -

1 aaaa.bbbb.1234 SecureConfigured Fa0/1 -

-----------------------------------------------------------------------------

Total Addresses in System (excluding one mac per port) : 1

Max Addresses limit in System (excluding one mac per port) : 8192

S1#

parancs kimenete **A show port-security interface** ellenőrzi, hogy a portbiztonság engedélyezve van-e, van-e egy gazdagép csatlakoztatva a porthoz (azaz Secure-up), összesen 2 MAC-cím engedélyezett, és az S1 megtanult egy MAC-címet. statikusan és egy MAC-címet dinamikusan (azaz ragadósan).

A **show port-security address** parancs kimenete felsorolja a két tanult MAC-címet.

14.3.5

## Port biztonság öregedés

A portbiztonsági öregítés használható a porton lévő statikus és dinamikus biztonságos címek öregedési idejének beállítására. Portonként kétféle öregítés támogatott:

* **Abszolút** – A porton lévő biztonságos címek a megadott öregedési idő után törlődnek.
* **Inaktivitás** – A porton lévő biztonságos címek csak akkor törlődnek, ha inaktívak a megadott öregedési ideig.

Az öregítés segítségével távolítsa el a biztonságos MAC-címeket egy biztonságos porton a meglévő biztonságos MAC-címek manuális törlése nélkül. Az öregedési időkorlátok is növelhetők, hogy a korábbi biztonságos MAC-címek megmaradjanak, még új MAC-címek hozzáadásakor is. A statikusan konfigurált biztonságos címek öregítése portonként engedélyezhető vagy letiltható.

A **switchport port-security aging** paranccsal engedélyezheti vagy letilthatja a statikus öregítést a biztonságos porton, vagy beállíthatja az öregítési időt vagy típust.

Switch(config-if)# **switchport port-security aging** { **static** | **time** time | **type** {**absolute** | **inactivity**}}

| **Paraméter** | **Leírás** |
| --- | --- |
| **statikus** | Az öregedés engedélyezése a statikusan konfigurált biztonságos címeknél ezen a porton. |
| **idő**  idő | Adja meg ennek a portnak az öregítési idejét. A tartomány 0 és 1440 perc között van. Ha az idő 0, az öregedés le van tiltva ezen a porton. |
| **típusú abszolút** | Állítsa be az abszolút öregedési időt. Az összes biztonságos cím ezen a porton pontosan a megadott idő (percekben) lejárta után öregszik, és törlődik a biztonságos címek listájáról. |
| **típusú inaktivitás** | Állítsa be az inaktivitási öregedés típusát. Ezen a porton a biztonságos címek csak akkor avulnak el, ha a megadott időtartamon belül nincs adatforgalom a biztonságos forráscímről. |

**Megjegyzés** : A MAC-címek 24 bitesek az egyszerűség kedvéért.

A példa azt mutatja, hogy egy rendszergazda 10 perces inaktivitásra konfigurálja az öregedés típusát, majd a **show port-security interface** parancsot használja a konfiguráció ellenőrzésére.

S1(config)# **interface fa0/1**

S1(config-if)# **switchport port-security aging time 10**

S1(config-if)# **switchport port-security aging type inactivity**

S1(config-if)# **end**

S1# **show port-security interface fa0/1**

Port Security : Enabled

Port Status : Secure-up

Violation Mode : Shutdown

Aging Time : 10 mins

Aging Type : Inactivity

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 2

Total MAC Addresses : 2

Configured MAC Addresses : 1

Sticky MAC Addresses : 1

Last Source Address:Vlan : a41f.7272.676a:1

Security Violation Count : 0

S1#

14.3.6

## Portbiztonsági megsértési módok

Ha a porthoz csatlakoztatott eszköz MAC-címe eltér a biztonságos címek listájától, akkor portsértés történik. Alapértelmezés szerint a port hibamentes állapotba kerül.

A portbiztonság megsértése módjának beállításához használja a következő parancsot:

Switch(config-if)# **switchport port-security violation** { **protect** | **restrict** | **shutdown**}

Az alábbi táblázat a különböző kapcsolási módokat írja le.

| **Mód** | **Leírás** |
| --- | --- |
| **Leállitás**  (alapértelmezett) | A port azonnal átvált a hiba miatt letiltott állapotba, kikapcsolja a port LED-jét, és rendszernapló-üzenetet küld. Növeli a szabálysértés-számlálót. Ha egy biztonságos port hiba miatt letiltott állapotban van, a rendszergazdának újra engedélyeznie kell azt a **leállítási** és **leállítási** parancsok megadásával. |
| **korlátoz** | A port addig dobja el az ismeretlen forráscímű csomagokat, amíg el nem távolít elegendő számú biztonságos MAC-címet ahhoz, hogy a maximális érték alá csökkenjen, vagy megnövelje a maximális értéket. Ebben az üzemmódban a biztonsági megsértések számlálója növekszik, és rendszernapló-üzenetet generál. |
| **védeni** | Ez a legkevésbé biztonságos a biztonsági megsértési módok közül. A port addig dobja el az ismeretlen MAC-forráscímű csomagokat, amíg el nem távolít elegendő számú biztonságos MAC-címet ahhoz, hogy a maximális érték alá csökkenjen, vagy megnövelje a maximális értéket. A rendszer nem küld rendszernapló üzenetet. |

A következő táblázat bemutatja, hogyan reagál a kapcsoló a konfigurált szabálysértési mód alapján.

| **Szabálysértési mód** | **Elveti a szabálysértő forgalmat** | **Syslog üzenetet küld** | **Növelje a szabálysértés-számlálót** | **Leállítja a portot** |
| --- | --- | --- | --- | --- |
| Védje | Igen | Nem | Nem | Nem |
| Korlátoz | Igen | Igen | Igen | Nem |
| Leállitás | Igen | Igen | Igen | Igen |

A következő példa azt mutatja be, hogy egy rendszergazda a biztonsági megsértést „korlátozásra” változtatja. parancs kimenete **A show port-security interface** megerősíti, hogy a változtatás megtörtént.

S1(config)# **interface f0/1**

S1(config-if)# **switchport port-security violation restrict**

S1(config-if)# **end**

S1#

S1# **show port-security interface f0/1**

Port Security : Enabled

Port Status : Secure-up

Violation Mode : Restrict

Aging Time : 10 mins

Aging Type : Inactivity

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 2

Total MAC Addresses : 2

Configured MAC Addresses : 1

Sticky MAC Addresses : 1

Last Source Address:Vlan : a41f.7272.676a:1

Security Violation Count : 0

S1#

14.3.7

## Hiba tiltott állapotban lévő portok

Mi történik, ha a portbiztonság megsértése leáll, és port megsértése történik? A port fizikailag le van állítva, és hiba miatt letiltott állapotba kerül, és ezen a porton nem küldenek vagy fogadnak forgalmat.

A példában a portbiztonság megsértése visszaáll az alapértelmezett leállítási beállításra. Ezután az a41f.7272.676a MAC-című gazdagépet leválasztják, és egy új gazdagépet csatlakoztatnak a Fa0/1-hez.

Figyelje meg, hogy a konzolon portbiztonsággal kapcsolatos üzenetek sorozata jön létre.

S1(config)# **int fa0/1**

S1(config-if)# **switchport port-security violation shutdown**

S1(config-if)# **end**

S1#

\*Mar 1 00:24:15.599: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

\*Mar 1 00:24:16.606: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down

\*Mar 1 00:24:19.114: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up

\*Mar 1 00:24:20.121: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

S1#

\*Mar 1 00:24:32.829: %PM-4-ERR\_DISABLE: psecure-violation error detected on Fa0/1, putting Fa0/1 in err-disable state

\*Mar 1 00:24:32.838: %PORT\_SECURITY-2-PSECURE\_VIOLATION: Security violation occurred, caused by MAC address a41f.7273.018c on port FastEthernet0/1.

\*Mar 1 00:24:33.836: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

\*Mar 1 00:24:34.843: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down

S1#

**Megjegyzés** : A port protokoll és a kapcsolat állapota lefelé módosul, és a port LED kialszik.

A példában a **show interface** parancs a port állapotát **err-disabledként** azonosítja . interface parancs kimenete **A show port-security** mostantól a port állapotát Secure-shutdownként mutatja a Secure-up helyett. A biztonsági megsértés számlálója 1-gyel növekszik.

S1# **show interface fa0/1 | include down**

FastEthernet0/18 is down, line protocol is down (err-disabled)

(output omitted)

S1# **show port-security interface fa0/1**

Port Security : Enabled

Port Status : Secure-shutdown

Violation Mode : Shutdown

Aging Time : 10 mins

Aging Type : Inactivity

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 2

Total MAC Addresses : 2

Configured MAC Addresses : 1

Sticky MAC Addresses : 1

Last Source Address:Vlan : a41f.7273.018c:1

Security Violation Count : 1

S1#

Az adminisztrátornak meg kell határoznia, mi okozta a biztonság megsértését. Ha egy biztonságos porthoz illetéktelen eszköz csatlakozik, a biztonsági fenyegetés a port újbóli engedélyezése előtt megszűnik.

A következő példában az első gazdagép újracsatlakozik a Fa0/1-hez. A port újbóli engedélyezéséhez először használja a **shutdown** parancsot, majd a **no shutdown** paranccsal állítsa működőképessé a portot, ahogy a példában is látható.

S1(config)# **interface fa0/1**

S1(config-if)# **shutdown**

S1(config-if)#

\*Mar 1 00:39:54.981: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

S1(config-if)# **no shutdown**

S1(config-if)#

\*Mar 1 00:40:04.275: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up

\*Mar 1 00:40:05.282: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

S1(config-if)#

14.3.8

## Ellenőrizze a port biztonságát

Miután konfigurálta a portbiztonságot egy kapcsolón, ellenőrizze az egyes interfészeket, és ellenőrizze, hogy a portbiztonság megfelelően van-e beállítva, és ellenőrizze, hogy a statikus MAC-címek megfelelően vannak-e konfigurálva.

**Portbiztonság minden interfészhez**

A kapcsoló portbiztonsági beállításainak megjelenítéséhez használja a **show port-security** parancsot. A példa azt jelzi, hogy csak egy port van konfigurálva a switchport port-security paranccsal.

S1# **show port-security**

Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action

(Count) (Count) (Count)

---------------------------------------------------------------------------

Fa0/1 2 2 0 Shutdown

---------------------------------------------------------------------------

Total Addresses in System (excluding one mac per port) : 1

Max Addresses limit in System (excluding one mac per port) : 8192

S1#

**Portbiztonság egy adott interfészhez**

Használja a **show port-security interface** parancsot egy adott interfész részleteinek megtekintéséhez, amint az korábban és ebben a példában is látható.

S1# **show port-security interface fastethernet 0/1**

Port Security : Enabled

Port Status : Secure-up

Violation Mode : Shutdown

Aging Time : 10 mins

Aging Type : Inactivity

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 2

Total MAC Addresses : 2

Configured MAC Addresses : 1

Sticky MAC Addresses : 1

Last Source Address:Vlan : a41f.7273.018c:1

Security Violation Count : 0

S1#

**Ellenőrizze a tanult MAC-címeket**

Annak ellenőrzésére, hogy a MAC-címek „tapadnak-e” a konfigurációhoz, használja a **show run** parancsot a FastEthernet 0/19 példájában látható módon.

S1# **show run interface fa0/1**

Building configuration...

Current configuration : 365 bytes

!

interface FastEthernet0/1

switchport mode access

switchport port-security maximum 2

switchport port-security mac-address sticky

switchport port-security mac-address sticky a41f.7272.676a

switchport port-security mac-address aaaa.bbbb.1234

switchport port-security aging time 10

switchport port-security aging type inactivity

switchport port-security

end

S1#

**Ellenőrizze a biztonságos MAC-címeket**

Az összes kapcsolófelületen kézzel konfigurált vagy dinamikusan betanított biztonságos MAC-cím megjelenítéséhez használja a **show port-security address** parancsot a példában látható módon.

S1# **show port-security address**

Secure Mac Address Table

-----------------------------------------------------------------------------

Vlan Mac Address Type Ports Remaining Age

(mins)

---- ----------- ---- ----- -------------

1 a41f.7272.676a SecureSticky Fa0/1 -

1 aaaa.bbbb.1234 SecureConfigured Fa0/1 -

-----------------------------------------------------------------------------

Total Addresses in System (excluding one mac per port) : 1

Max Addresses limit in System (excluding one mac per port) : 8192

S1#

14.3.9

## Szintaxis-ellenőrző – A portbiztonság megvalósítása

A megadott követelmények alapján valósítsa meg a kapcsoló interfész portbiztonságát

You are currently logged into S1. Configure FastEthernet 0/5 for port security by using the following requirements:

* Use the interface name **fa0/5** to enter interface configuration mode.
* Enable the port for access mode.
* Enable port security.
* Set the maximum number of MAC address to 3.
* Statically configure the MAC address aaaa.bbbb.1234.
* Configure the port to dynamically learn additional MAC addresses and dynamically add them to the running configuration.
* Return to privileged EXEC mode.

S1(config)#interface fa0/5

S1(config-if)#switchport mode access

S1(config-if)#switchport port-security

S1(config-if)#switchport port-security maximum 3

S1(config-if)#switchport port-security mac-address aaaa.bbbb.1234

S1(config-if)#switchport port-security mac-address sticky

S1(config-if)#end

Enter the command to verify port security for all interfaces.

S1#show port-security

Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action

(Count) (Count) (Count)

---------------------------------------------------------------------------

Fa0/5 3 2 0 Shutdown

---------------------------------------------------------------------------

Total Addresses in System (excluding one mac per port) : 0

Max Addresses limit in System (excluding one mac per port) : 8192

Enter the command to verify port security on FastEthernet 0/5. Use **fa0/5** for the interface name.

S1#show port-security interface fa0/5

Port Security : Enabled

Port Status : Secure-up

Violation Mode : Shutdown

Aging Time : 0 mins

Aging Type : Absolute

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 3

Total MAC Addresses : 2

Configured MAC Addresses : 1

Sticky MAC Addresses : 1

Last Source Address:Vlan : 0090.2135.6B8C:1

Security Violation Count : 0

Enter the command that will display all of the addresses to verify that the manually configured and dynamically learned MAC addresses are in the running configuration.

S1#show port-security address

Secure Mac Address Table

-----------------------------------------------------------------------------

Vlan Mac Address Type Ports Remaining Age

(mins)

---- ----------- ---- ----- -------------

1 0090.2135.6b8c SecureSticky Fa0/5 -

1 aaaa.bbbb.1234 SecureConfigured Fa0/5 -

-----------------------------------------------------------------------------

Total Addresses in System (excluding one mac per port) : 0

Max Addresses limit in System (excluding one mac per port) : 8192

You have successfully configured and verified port security for the interface.

14.3.10

## SNMP MAC-címértesítés

A hálózatmenedzsereknek egy módra van szükségük annak nyomon követésére, hogy ki használja a hálózatot és hol található. Például, ha az Fa0/1 port biztonságos egy kapcsolón, akkor SNMP-csapda jön létre, amikor az adott porthoz tartozó MAC-cím bejegyzés eltűnik a MAC-táblázatból.

A MAC-címértesítési szolgáltatás SNMP-csapdákat küld a hálózatkezelő állomásnak (NMS), amikor új MAC-címet adnak hozzá, vagy egy régi címet törölnek a továbbítási táblázatokból. A MAC-címekről szóló értesítések csak dinamikus és biztonságos MAC-címekhez jönnek létre.

A MAC-címértesítés lehetővé teszi a hálózati adminisztrátor számára, hogy figyelje a megtanult MAC-címeket, valamint azokat a MAC-címeket, amelyek elévülnek és eltávolítják a kapcsolóból. Például az ábrán a MAC C-vel rendelkező laptop lekapcsolódott a hálózatról. A kapcsoló végül időtúllép az Fa0/3 porton, és SNMP trap értesítést küld az NMS szervernek.

A **mac-címtábla értesítési** globális konfigurációs parancsával engedélyezheti a MAC-címértesítés funkciót egy kapcsolón.

Az ábra egy laptopot mutat, amely le van választva az F0/3-ról, és ennek eredményeként a kapcsoló idővel túllépi az F0/3-as portot, és SNMP trap értesítést küld az NMS-kiszolgálónak.

F0/2 F0/1 F0/3

F0/4

MAC A MAC B MAC C MAC D NMS SNMP csapdák

14.3.11

## Packet Tracer – A portbiztonság megvalósítása

Ebben a Packet Tracer tevékenységben konfigurálhatja és ellenőrizheti a kapcsoló portbiztonságát. A port biztonsága lehetővé teszi a port bejövő forgalmának korlátozását azáltal, hogy korlátozza azokat a MAC-címeket, amelyek forgalmat küldhetnek a portba.

[A portbiztonság megvalósítása](https://contenthub.netacad.com/courses/netsec/_common/14.3.11-packet-tracer---implement-port-security.pka)

[14.2](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[MAC Table Attacks](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[14.4](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Mitigate VLAN Attacks](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                         
*               

1. Layer 2 Security Considerations
2. Mitigate VLAN Attacks

# Csökkentse a VLAN-támadásokat

14.4.1

## VLAN ugráló támadások

A VLAN-ok külön szórási tartományok létrehozására szolgálnak a kapcsolókon. Az egyik VLAN-ban található végpontok nem tudnak kommunikálni egy másik VLAN-on lévő végpontokkal, kivéve, ha ezt egy útválasztó vagy a 3. rétegbeli kapcsoló engedélyezi. A VLAN-ok segítségével elkülöníthetők az érzékeny tartalmak a többi hálózati forgalomtól. Például vendég VLAN hozható létre egy szervezet vendégei számára. Ezek a vendégek nem férhetnek hozzá más VLAN-okon átvitt érzékeny vállalati tartalomhoz. A VLAN-támadások megkerülhetik a VLAN-tervezés szándékát azáltal, hogy jogosulatlan felhasználók számára hozzáférhetnek olyan VLAN-okhoz, amelyekhez nem kellene hozzáférniük. A VLAN-támadások két típusa a VLAN-ugrásos támadás és a kettős VLAN-címkézéses támadás.

A VLAN ugrásos támadás lehetővé teszi, hogy az egyik VLAN-ból érkező forgalmat egy másik VLAN lássa útválasztó segítsége nélkül. Egy alap VLAN-ugrásos támadásban a fenyegetés szereplője úgy konfigurálja a gazdagépet, hogy kapcsolóként működjön, hogy kihasználja a legtöbb kapcsolóporton alapértelmezés szerint engedélyezett automatikus trönkölési port szolgáltatást.

A fenyegetés szereplője úgy konfigurálja a gazdagépet, hogy a csatlakozó kapcsolóval meghamisítsa a 802.1Q jelzést és a Cisco által védett Dynamic Trunking Protocol (DTP) jelzést a fővonalon. Sikeres esetben a kapcsoló fővonali kapcsolatot létesít a gazdagéppel, az ábra szerint. Mostantól a fenyegetés szereplője hozzáférhet a switch összes VLAN-jához. A fenyegetés szereplője bármely VLAN-on küldhet és fogadhat forgalmat, hatékonyan ugrálva a VLAN-ok között.

A támadó egy kapcsolóhoz csatlakozik, amely egy másik kapcsolóhoz csatlakozik egy 802.1Q fővonalon keresztül. A második kapcsoló a V LAN 10 1. kiszolgálójával és a 20. V LAN 2. kiszolgálóval csatlakozik. A támadó jogosulatlan 802.1Q fővonali kapcsolatot hozott létre a kapcsolóval, hogy hozzáférjen a szerver V LAN-jához. egy nyíl a támadóról a kapcsolóra mutat, és jogosulatlan trunk felirattal van ellátva.

802.1Q Trunk 802.1Q VLAN 20 Server1 VLAN 10 Server 2 Attacker hozzáférést kap a kiszolgáló VLAN-hoz Jogosulatlan trönk

14.4.2

## VLAN kettős címkézésű támadás

A fenyegetés szereplői bizonyos helyzetekben beágyazhatnak egy rejtett 802.1Q címkét a keretbe, amely már rendelkezik 802.1Q címkével. Ez a címke lehetővé teszi, hogy a keret olyan VLAN-hoz jusson, amelyet az eredeti 802.1Q címke nem adott meg.

Kattintson az egyes lépésekre egy dupla címkézéses támadás példájának és magyarázatának megtekintéséhez.

A fenyegetés szereplője egy dupla címkével ellátott 802.1Q keretet küld a kapcsolónak. A külső fejlécben található a fenyegetés szereplőjének VLAN-címkéje, amely megegyezik a fővonali port natív VLAN-jával. Ebben a példában tegyük fel, hogy ez a VLAN 10. A belső címke az áldozat VLAN, ebben a példában a VLAN 20.

A támadó egy kapcsolóhoz csatlakozik, amely egy másik, natív V LAN 10-re beállított kapcsolóval rendelkezik. A második kapcsolóhoz egy célállomás tartozik a V LAN 20-ban. A támadó egy keretet küld az első kapcsolónak, amely a következőkből áll: a következő mezők: Ethernet, V LAN 10, V LAN 20 és adatok.

1

Ethernet VLAN 10 VLAN 20 Data Trunk Natív VLAN = 10 Cél (VLAN 20)

A VLAN kettős címkézéses támadása egyirányú, és csak akkor működik, ha a támadó egy olyan porthoz csatlakozik, amely ugyanabban a VLAN-ban található, mint a fővonali port natív VLAN-ja. Az ötlet az, hogy a kettős címkézés lehetővé teszi a támadó számára, hogy adatokat küldjön a VLAN-on lévő gazdagépeknek vagy szervereknek, amelyeket egyébként blokkolna valamilyen hozzáférés-vezérlési konfiguráció. Feltehetően a visszatérő forgalom is engedélyezett lesz, így a támadó képes kommunikálni a normál esetben blokkolt VLAN-on lévő eszközökkel.

**VLAN támadás mérséklése**

A VLAN ugrás és a VLAN kettős címkézéses támadások megelőzhetők a következő fővonal-biztonsági irányelvek végrehajtásával, amint azt az előző modulban tárgyaltuk:

* Tiltsa le a trönkölést az összes hozzáférési porton.
* Tiltsa le az automatikus fővonalakat a fővonali hivatkozásokon, hogy a fővonalakat kézzel kell engedélyezni.
* Győződjön meg arról, hogy a natív VLAN-t csak fővonali kapcsolatokhoz használja.

14.4.3

## VLAN ugrásos támadások mérséklése

A VLAN ugrásos támadások mérsékléséhez kövesse az alábbi lépéseket:

**1. lépés** : Tiltsa le a DTP (automatikus trönkelés) egyeztetéseket a nem trönkös portokon a **switchport mód hozzáférési** interfész konfigurációs parancsával.   
**2. lépés** : Tiltsa le a nem használt portokat, és helyezze őket egy nem használt VLAN-ba. A példában ez a VLAN 1000.   
**3. lépés** : Manuálisan engedélyezze a fővonali kapcsolatot egy trönkporton a **switchport mode trunk** paranccsal.   
**4. lépés** paranccsal tiltsa le a DTP (automatikus trunking) tárgyalásokat a trunking portokon **: A switchport nonegotiate** .   
**5. lépés** : Állítsa be a natív VLAN-t a VLAN 1-től eltérő VLAN-ra a **switchport trunk native vlan** vlan \_ number paranccsal.

Tegyük fel például a következőket:

* A 0/1–fa0/16 FastEthernet portok aktív hozzáférési portok
* A 0/17 és 0/20 közötti FastEthernet portok jelenleg nincsenek használatban
* A 0/21 és 0/24 közötti FastEthernet portok fővonali portok.

A VLAN ugrás a következő konfiguráció megvalósításával mérsékelhető.

S1(config)# **interface range fa0/1 - 16**

S1(config-if-range)# **switchport mode access**

S1(config-if-range)# **exit**

S1(config)#

S1(config)# **interface range fa0/17 - 20**

S1(config-if-range)# **switchport mode access**

S1(config-if-range)# **switchport access vlan 1000**

S1(config-if-range)# **shutdown**

S1(config-if-range)# **exit**

S1(config)#

S1(config)# **interface range fa0/21 - 24**

S1(config-if-range)# **switchport mode trunk**

S1(config-if-range)# **switchport nonegotiate**

S1(config-if-range)# **switchport trunk native vlan 999**

S1(config-if-range)# **end**

S1#

* A 0/1-től 0/16-ig terjedő FastEthernet portok hozzáférési portok, ezért a trönkölés tiltva van azáltal, hogy kifejezetten hozzáférési portokká teszik őket.
* A 0/17-től 0/20-ig terjedő FastEthernet portok nem használt portok, le vannak tiltva, és nem használt VLAN-hoz vannak rendelve.
* A 0/21-től 0/24-ig terjedő FastEthernet portok fővonali kapcsolatok, és manuálisan engedélyezhetők trönkként a DTP letiltásával. A natív VLAN is megváltozott az alapértelmezett VLAN 1-ről VLAN 999-re.

14.4.4

## Szintaxis-ellenőrző – VLAN-ugrásos támadások mérséklése

Csökkentse a VLAN ugrásos támadásokat a switch ellen a megadott követelmények alapján.

You are currently logged into S1. The ports status of the ports are as follows:

* FastEthernet ports 0/1 through 0/4 are used for trunking with other switches.
* FastEthernet ports 0/5 through 0/10 are unused.
* FastEthernet ports 0/11 through 0/24 are active ports currently in use.

Use **range fa0/1 - 4** to enter interface configuration mode for the trunks.

S1(config)#interface range fa0/1 - 4

Configure the interfaces as nonnegotiating trunks assigned to default VLAN 99.

S1(config-if-range)#switchport mode trunk

S1(config-if-range)#switchport nonegotiate

S1(config-if-range)#switchport trunk native vlan 99

S1(config-if-range)# exit

Use **range fa0/5 - 10** to enter interface configuration mode for the unused ports.

S1(config)#interface range fa0/5 - 10

Configure the unused ports as access ports, assign them to VLAN 86, and shutdown the ports.

S1(config-if-range)#switchport mode access

S1(config-if-range)#switchport access vlan 86

% Access VLAN does not exist. Creating vlan 86

S1(config-if-range)#shutdown

\*Mar 1 00:28:48.883: %LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down

\*Mar 1 00:28:48.900: %LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down

\*Mar 1 00:28:48.908: %LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

\*Mar 1 00:28:48.917: %LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

\*Mar 1 00:28:48.942: %LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down

\*Mar 1 00:28:48.950: %LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down

\*Mar 1 00:28:49.890: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down

\*Mar 1 00:28:49.907: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to down

S1(config-if-range)# exit

Use range **fa0/11 - 24** to enter interface configuration mode for the active ports and then configure them to prevent trunking.

S1(config)#interface range fa0/11 - 24

S1(config-if-range)#switchport mode access

S1(config-if-range)# end

S1#

You have successfully mitigated VLAN hopping attacks on this switch.

14.4.5

## Privát VLAN-ok

A VLAN-ok broadcast tartományok. Bizonyos helyzetekben azonban hasznos lehet megszegni ezt a szabályt, és csak a minimálisan szükséges L2 kapcsolatot engedélyezni a VLAN-on belül.

A privát VLAN-ok (PVLAN) 2. rétegbeli leválasztást biztosítanak az ugyanazon a szórási tartományon belüli portok között. Háromféle PVLAN port létezik:

* **Promiscuous** - A kóbor port mindenkivel beszélhet. Minden interfésszel képes kommunikálni, beleértve a PVLAN-on belüli izolált és közösségi portokat is.
* **Elszigetelt** – Egy izolált port csak nem megfelelő portokkal tud kommunikálni. Egy izolált port teljes 2. rétegbeli elválasztással rendelkezik ugyanazon a PVLAN-on belüli többi porttól, de nem a szokatlan portoktól. A PVLAN-ok blokkolják az összes forgalmat az elszigetelt portokra, kivéve a nem megfelelő portokról érkező forgalmat. Az elszigetelt portról érkező forgalom csak a nem megfelelő portokra kerül továbbításra.
* **Közösség** – A közösségi kikötők kommunikálhatnak más közösségi és tisztességtelen kikötőkkel. Ezek az interfészek a 2. rétegben el vannak választva az összes többi interfésztől a többi közösségben vagy a PVLAN-on belüli elszigetelt portokon.

Az ábrán látható példa azt szemlélteti, hogy mely portok kapcsolhatók össze. A PVLAN által nyújtott biztonság megkerülhető a router proxyként való használatával.

"P"   
Promiszózus "C" port   
közösségi portok **"I"   
Elszigetelt portok VLAN 102 VLAN 105 Elsődleges   
VLAN 100**

Például az alábbi ábrán a PC-A és a PC-B el van választva egymástól. A PC-A azonban támadást indíthat a PC-B ellen, ha olyan csomagokat küld, amelyek a PC-A forrás IP-címével és MAC-címével, a PC-B cél IP-címével, de az R1-es MAC-címmel rendelkeznek. Az S1 továbbítja a keretet az R1-nek, mert az F0/5 titkos portként van konfigurálva. Az R1 újraépíti a keretet a PC-B MAC-címével, és továbbítja az S1-nek. Az S1 ezután továbbítja a keretet a PC-B-nek.

**Megjegyzés** : A PVLAN-okat főleg a szolgáltatók helymeghatározási helyein használják. Egy másik tipikus alkalmazást találhatunk a szállodákban, ahol minden szoba külön külön porton lenne összekötve.

Az ábra egy topológia egy kapcsolóhoz csatlakoztatott routerrel. Két P C is csatlakozik a kapcsolóhoz. Minden számítógép egy elkülönített porton van. A router egy szokatlan porton van. Az elsődleges V LAN a 172.16.0.0/24.

### PVLAN proxy támadás

PC-A S1 PC-B R1 G0/0 F0/5 F0/6

F0/18

Elsődleges VLAN   
172.16.0.0/24 Isolated Ports Promiscuous Port

Az ilyen típusú támadások mérséklése érdekében állítson be egy ACL-t, amely megtagadja a forgalmat egyazon alhálózathoz tartozó forrás- és cél IP-címmel, amint az az alábbi konfigurációban látható.

R1(config)# **ip access-list extended PVLAN**

R1(config-ext-nacl)# **deny ip 172.16.0.0 0.0.0.255 172.16.0.0 0.0.0.255**

R1(config-ext-nacl)# **permit ip any any**

R1(config-ext-nacl)# **interface g0/0**

R1(config-if)# **ip access-group PVLAN in**

R1(config-if)#

14.4.6

## PVLAN Edge funkció

Egyes alkalmazások megkövetelik, hogy a 2. rétegben ne továbbítsanak forgalmat ugyanazon a kapcsolón lévő portok között, hogy az egyik szomszéd ne lássa a másik szomszéd által generált forgalmat.

Ilyen környezetben a PVLAN Edge funkció használata biztosítja, hogy ne legyen unicast, broadcast vagy multicast forgalom a switch PVLAN peremportjai között, ahogy az az ábrán is látható. A PLVAN Edge szolgáltatást védett portoknak is nevezik.

A PVLAN Edge szolgáltatás a következő jellemzőkkel rendelkezik:

* A védett portok nem továbbítanak semmilyen forgalmat (például unicast, multicast vagy broadcast) semmilyen más portra, amely szintén védett port. Az adatforgalom nem továbbítható a 2. réteg védett portjai között; csak a vezérlőforgalom kerül továbbításra, mert ezeket a csomagokat a CPU feldolgozza és szoftveresen továbbítja. A védett portok között áthaladó összes adatforgalmat egy Layer 3 eszközön keresztül kell továbbítani.
* A védett port és a nem védett port közötti továbbítás a szokásos módon történik.
* Az alapértelmezés szerint nincs megadva védett port.

Az ábrán egy felhőhöz és két számítógéphez kapcsolódó kapcsoló látható. a felhő másik oldalához csatlakozik egy szerver. Egy kétirányú nyíl található egy számítógép és a szerver között. A két számítógép között van egy kétirányú nyíl, piros körrel, rajta piros perjel. A másik számítógép és a szerver között egy kétirányú nyíl található. A számítógép melletti címkén a védett portok olvashatók. a nyíl közepe közelében lévő címke nem védett portokat ír (alapértelmezett).

### A 2. rétegbeli forgalom korlátozása a kapcsolóportok között

Nem védett portok (alapértelmezett) Védett portok

14.4.7

## PVLAN Edge konfigurálása

A PVLAN Edge szolgáltatás konfigurálásához írja be a **switchport védett** interfész konfigurációs mód parancsát.

A PVLAN Edge szolgáltatás fizikai interfészen vagy EtherChannel csoporton konfigurálható. Ha a PVLAN Edge szolgáltatás engedélyezve van egy portcsatornához, akkor a port-csatorna csoport összes portjára engedélyezve van. A védett port letiltásához használja a **no switchport protected** interface konfigurációs mód parancsot.

A PVLAN Edge szolgáltatás konfigurációjának ellenőrzéséhez használja a **show interfaces interface-id** switchport globális konfigurációs mód parancsot, az alábbi példában látható módon.

Switch# **show interfaces gigabitethernet1/0/1 switchport**

Name: G1/0/1

Switchport: Enabled

Administrative Mode: dynamic auto

Operational Mode: static access

Administrative Trunking Encapsulation: negotiate

Operational Trunking Encapsulation: native

Negotiation of Trunking: On

Access Mode VLAN: 1 (default)

Trunking Native Mode VLAN: 1 (default)

Voice VLAN: none

(output omitted)

Operational private-vlan: none

Trunking VLANs Enabled: ALL

Pruning VLANs Enabled: 2-1001

Capture Mode Disabled

Capture VLANs Allowed: ALL

Protected: false

Unknown unicast blocked: disabled

Unknown multicast blocked: disabled

Voice VLAN: none (Inactive)

Appliance trust: none

A PVLAN él egy olyan szolgáltatás, amelynek csak helyi jelentősége van a kapcsoló számára, és nincs elválasztás a különböző switcheken található két védett port között. A védett portok nem továbbítanak semmilyen forgalmat (egyedi, csoportos vagy broadcast) más olyan portra, amely egyben ugyanazon a kapcsolón védett port is. A forgalom nem továbbítható a 2. réteg (L2) védett portjai között; A védett portok között áthaladó összes forgalmat egy Layer 3 (L3) eszközön keresztül kell továbbítani.

14.4.8

## Videó - Privát VLAN bemutató és bemutató

Ez a videó és az oktatóanyag a privát VLAN-konfigurációt mutatja be, és a következőket tartalmazza:

* A privát VLAN-ok előnyei
* Példák a privát VLAN megvalósítására
* A privát VLAN-portok típusai
* Privát VLAN konfigurálása 3560 többrétegű kapcsolón
* A switchport védett parancs használata 2960-as kapcsolón

[14.3](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Mitigate MAC Table Attacks](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[14.5](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Mitigate DHCP Attacks](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                            
*               

1. Layer 2 Security Considerations
2. Mitigate DHCP Attacks

# Mérsékelje a DHCP-támadásokat

14.5.1

## DHCP támadások

A DHCP-támadások két típusa a DHCP-éhezés és a DHCP-hamisítás. Mindkét támadást mérsékli a DHCP-snooping megvalósítása.

**DHCP éhezési támadás**

A DHCP éhező támadás célja a kliensek összekapcsolására szolgáló DoS. A DHCP éhezési támadásokhoz olyan támadási eszközre van szükség, mint a Gobbler.

A Gobbler képes megvizsgálni a bérelhető IP-címek teljes körét, és megpróbálja lízingelni mindet. Pontosabban, hamis MAC-címekkel hoz létre DHCP-felderítési üzeneteket.

**DHCP hamisítási támadás**

DHCP-hamisítási támadás akkor következik be, amikor egy rosszindulatú DHCP-kiszolgáló csatlakozik a hálózathoz, és hamis IP-konfigurációs paramétereket ad meg a törvényes ügyfeleknek. Egy szélhámos szerver sokféle félrevezető információt közölhet:

* **Hibás alapértelmezett átjáró** – A szélhámos szerver érvénytelen átjárót vagy saját IP-címet ad meg a köztes támadás létrehozásához. Ez teljesen észrevétlen maradhat, mivel a behatoló elfogja a hálózaton keresztüli adatáramlást, majd továbbítja azt a valódi alapértelmezett átjáróhoz.
* **Hibás DNS-szerver** – A rosszindulatú kiszolgáló helytelen DNS-szervercímet ad meg, amely egy rosszindulatú webhelyre irányítja a felhasználót.
* **Hibás IP-cím** – A rosszindulatú szerver érvénytelen IP-címet ad meg, ami ténylegesen DoS-támadást hoz létre a DHCP-kliens ellen.

Kattintson az egyes lépésekre egy DHCP-hamisítási támadás példájának és magyarázatának megtekintéséhez.

**A fenyegető szereplő Rogue DHCP-kiszolgálót csatlakoztat**

Egy fenyegetést végrehajtó szereplő sikeresen csatlakoztatja a csaló DHCP-kiszolgálót egy kapcsolóporthoz ugyanazon az alhálózaton és VLAN-on, mint a célügyfelek. A rogue szerver célja, hogy hamis IP-konfigurációs információkat közöljön az ügyfelekkel.

egy rosszindulatú DHCP-szerver egy hálózat kapcsolójához csatlakozik

DHCP-kiszolgáló Rogue DHCP-kiszolgáló

14.5.2

## DHCP támadások mérséklése

A DHCP éhezés elleni támadások könnyen mérsékelhetők a portbiztonság használatával. A DHCP-hamisítási támadások mérséklése azonban nagyobb védelmet igényel.

Például a Gobbler egyedi MAC-címet használ minden DHCP-kéréshez és portbiztonsághoz. A portbiztonságot be lehet állítani ennek enyhítésére. A Gobbler azonban úgy is konfigurálható, hogy minden kérésnél ugyanazt az interfész MAC-címet használja más hardvercímmel. Ez hatástalanná tenné a kikötőbiztonságot.

A DHCP-hamisítási támadások mérsékelhetők a megbízható portokon végzett DHCP-snooping segítségével. A DHCP leskelődés a DHCP-kiéheztetés elleni támadások mérséklésében is segít azáltal, hogy korlátozza a nem megbízható portok által fogadható DHCP-felderítési üzenetek számát. A DHCP snooping létrehoz és karbantart egy DHCP snooping kötési adatbázist, amelyet a kapcsoló használhat a nem megbízható forrásokból származó DHCP-üzenetek kiszűrésére. A DHCP snooping-összerendelési táblázat tartalmazza az ügyfél MAC-címét, IP-címét, DHCP-bérleti idejét, kötési típusát, VLAN-számát és interfészinformációit minden egyes nem megbízható kapcsolóporton vagy interfészen.

Az adminisztratív irányítása alatt álló eszközök, például a kapcsolók, útválasztók és szerverek megbízható források. A tűzfalon kívüli vagy a hálózaton kívüli eszközök nem megbízható források. Ezenkívül az összes hozzáférési portot általában nem megbízható forrásként kezelik. Az ábra egy példát mutat megbízható és nem megbízható portokra.

Az ábra egy DHCP-kiszolgálót mutat a topológia jobb felső részén, amely az alatta lévő elosztási kapcsolóhoz csatlakozik. Az elosztó kapcsoló egy másik elosztó kapcsolóhoz csatlakozik a diagramtól balra, és az alatta lévő hozzáférési kapcsolóhoz. A másik elosztó kapcsoló alá egy hozzáférési kapcsoló van csatlakoztatva. Mindkét hozzáférési kapcsolónak van kapcsolata mindkét elosztó kapcsolóval, de egymással. A jobb oldali hozzáférési kapcsoló alatt van egy PC, a másik hozzáférési kapcsoló alatt pedig egy rogue karakterrel ellátott PC. Az ábra egy lila négyzetet mutat a megbízható portokhoz és egy piros kört a nem megbízható portokhoz. Lila négyzetek vannak a DHCP-kiszolgáló és a terjesztési kapcsoló között, valamint az egyes kapcsolók közötti kapcsolatok között. A két P C és a hozzáférési kapcsolók között azonban van egy piros kör.

DHCP-kliens DHCP-kiszolgáló Rogue DHCP-kiszolgáló Megbízható port Nem megbízható port

**Megjegyzés** : Nagy hálózatban a DHCP-kötési tábla létrehozása az engedélyezést követően időbe telhet. Például, ha a DHCP bérleti ideje 4 nap, 2 napba is beletelhet, amíg a DHCP leskelődéssel kitölti a táblázatot.

Ha a DHCP-snooping engedélyezve van egy interfészen vagy VLAN-on, és egy kapcsoló nem megbízható porton fogad egy csomagot, a kapcsoló összehasonlítja a forráscsomag-információkat a DHCP-snooping-kötési táblázatban tárolt adatokkal. A kapcsoló megtagadja a konkrét információkat tartalmazó csomagokat:

* Jogosulatlan DHCP-kiszolgáló üzenetek nem megbízható portról
* Jogosulatlan DHCP kliens üzenetek, amelyek nem tartják be a leskelődő kötési táblázatot vagy a sebességkorlátokat
* DHCP-közvetítő-ügynök csomagok, amelyek nem megbízható porton tartalmazzák a 82-es opció adatait

**Megjegyzés** : Az ugyanazt a MAC-címet használó Gobbler elleni küzdelemhez a DHCP-snooping arra is készteti a kapcsolót, hogy ellenőrizze a Client Hardware Address (CHADDR) mezőt a DHCP-kérésben. Ez biztosítja, hogy megegyezzen a hardver MAC-címével a DHCP-snooping-kötési táblázatban és a MAC-címmel a MAC-táblázatban. Ha nincs egyezés, a kérést elveti.

**Megjegyzés** : Hasonló mérséklő technikák állnak rendelkezésre DHCPv6 és IPv6 kliensekhez. Mivel az IPv6-eszközök az útválasztó Router Advertisement (RA) üzenetéből is megkaphatják a címzési információkat, léteznek enyhítő megoldások is a csaló RA-üzenetek megelőzésére.

14.5.3

## A DHCP Snooping megvalósításának lépései

Kövesse az alábbi lépéseket a DHCP leskelődés engedélyezéséhez:

**1. lépés** . Engedélyezze a DHCP lekérdezést az **ip dhcp snooping** globális konfigurációs paranccsal.   
**2. lépés** . Megbízható portokon használja az **ip dhcp snooping trust** interface konfigurációs parancsot.   
**3. lépés** . Korlátozza a nem megbízható portokon másodpercenként fogadható DHCP-felderítési üzenetek számát az **ip dhcp snooping limit rate** interfész konfigurációs paranccsal.   
**4. lépés** . engedélyezheti a VLAN-on vagy egy sor VLAN-on keresztüli DHCP-snooping-ot . **Az ip dhcp snooping** vlan globális konfigurációs paranccsal

14.5.4

## DHCP Snooping konfigurációs példa

Ennek a DHCP-snooping példának a referencia topológiája az ábrán látható. Figyelje meg, hogy az F0/5 egy nem megbízható port, mert PC-hez csatlakozik. Az F0/1 egy megbízható port, mert csatlakozik a DHCP szerverhez.

A grafikon egy jelmagyarázat található, amelyen egy lila négyzet alakú megbízható port és egy piros kör látható a topológiai diagram alatt. Ezután az ábra egy LAN-hálózatot mutat be megbízható és nem megbízható portokkal rendelkező kapcsolóval. A kapcsoló bal oldalára egy PC van csatlakoztatva a jobb oldalon pedig egy DHCP csatlakozik hozzá. A PC-hez csatlakozó interfészen egy piros kör jelzi a nem megbízható interfészt és a DHCP szerverhez csatlakoztatott interfészen a megbízható port lila négyzete látható.

192.168.10.10 F0/5 S1

F0/1

DHCP szerver megbízható port Nem megbízható port

Az alábbiakban egy példa látható arra, hogyan konfigurálható a DHCP-snooping S1-en. Figyelje meg, hogyan van először engedélyezve a DHCP leskelődés. Ekkor a DHCP szerver upstream interfésze kifejezetten megbízható. Ezután a FastEthernet portok F0/5-től F0/24-ig terjedő tartománya alapértelmezés szerint nem megbízható, így a sebességkorlátozás másodpercenként hat csomagra van beállítva. Végül a DHCP-snooping engedélyezve van a VLANS 5, 10, 50, 51 és 52-n.

S1(config)# **ip dhcp snooping**

S1(config)# **interface f0/1**

S1(config-if)# **ip dhcp snooping trust**

S1(config-if)# **exit**

S1(config)# **interface range f0/5 - 24**

S1(config-if-range)# **ip dhcp snooping limit rate 6**

S1(config-if-range)# **exit**

S1(config)# **ip dhcp snooping vlan 5,10,50-52**

S1(config)# **end**

S1#

Használja a **show ip dhcp snooping** privileged EXEC parancsot a DHCP snooping ellenőrzéséhez, és **mutassa meg az ip dhcp snooping kötést,** hogy megtekinthesse azokat a klienseket, amelyek megkapták a DHCP információkat, ahogy a példában is látható.

**Megjegyzés** : A DHCP-figyelést a Dynamic ARP Inspection (DAI) is megköveteli, amely a következő téma.

S1# **show ip dhcp snooping**

Switch DHCP snooping is enabled

DHCP snooping is configured on following VLANs:

5,10,50-52

DHCP snooping is operational on following VLANs:

none

DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled

circuit-id default format: vlan-mod-port

remote-id: 0cd9.96d2.3f80 (MAC)

Option 82 on untrusted port is not allowed

Verification of hwaddr field is enabled

Verification of giaddr field is enabled

DHCP snooping trust/rate is configured on the following Interfaces:

Interface Trusted Allow option Rate limit (pps)

----------------------- ------- ------------ ----------------

FastEthernet0/1 yes yes unlimited

Custom circuit-ids:

FastEthernet0/5 no no 6

Custom circuit-ids:

FastEthernet0/6 no no 6

Custom circuit-ids:

S1# **show ip dhcp snooping binding**

MacAddress IpAddress Lease(sec) Type VLAN Interface

------------------ --------------- ---------- ------------- ---- --------------------

00:03:47:B5:9F:AD 192.168.10.11 193185 dhcp-snooping 5 FastEthernet0/5

14.5.5

## Szintaxis-ellenőrző – DHCP-támadások mérséklése

A következő topológia és meghatározott követelmények alapján hajtsa végre a DHCP-snoopot egy kapcsolóhoz.

A szintaxis-ellenőrző topológiája egy elosztási kapcsolóval rendelkezik, amely egy hozzáférési kapcsoló G0/1 interfészéhez van csatlakoztatva. A hozzáférési kapcsoló F0/1 interfésze balra csatlakozik a PC-hez, a jobb oldalon pedig a G0/2 switch interfész egy szerverhez csatlakozik.

S1 F0/1 G0/1

G0/2

DHCP szerver

You are currently logged into S1. Enable DHCP snooping globally for the switch.

S1(config)#ip dhcp snooping

Enter interface configuration mode for **g0/1 - 2**, trust the interfaces, and return to global configuration mode.

S1(config)#interface range g0/1 - 2

S1(config-if-range)#ip dhcp snooping trust

S1(config-if-range)#exit

Enter interface configuration mode for **f0/1 - 24**, limit the DHCP messages to no more than 10 per second, and return to global configuration mode.

S1(config)#interface range f0/1 - 24

S1(config-if-range)#ip dhcp snooping limit rate 10

S1(config-if-range)#exit

Enable DHCP snooping for VLANs **10,20,30-49**.

S1(config)#ip dhcp snooping vlan 10,20,30-49

S1(config)# exit

Enter the command to verify DHCP snooping.

S1#show ip dhcp snooping

Switch DHCP snooping is enabled

DHCP snooping is configured on following VLANs:

10,20,30-49

DHCP snooping is operational on following VLANs:

none

DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled

circuit-id default format: vlan-mod-port

remote-id: 0cd9.96d2.3f80 (MAC)

Option 82 on untrusted port is not allowed

Verification of hwaddr field is enabled

Verification of giaddr field is enabled

DHCP snooping trust/rate is configured on the following Interfaces:

Interface Trusted Allow option Rate limit (pps)

----------------------- ------- ------------ ----------------

GigabitEthernet0/1 yes yes unlimited

Custom circuit-ids:

GigabitEthernet0/2 yes yes unlimited

Custom circuit-ids:

FastEthernet0/1 no no 10

Custom circuit-ids:

Enter the command to verify the current DHCP bindings logged by DHCP snooping

S1#show ip dhcp snooping binding

MacAddress IpAddress Lease(sec) Type VLAN Interface

------------------ --------------- ---------- ------------- ---- --------------------

00:03:47:B5:9F:AD 10.0.0.10 193185 dhcp-snooping 5 FastEthernet0/1

S1#

You have successfully configured and verified DHCP snooping for the switch.

[14.4](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Mitigate VLAN Attacks](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[14.6](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Mitigate ARP Attacks](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                
*               

1. Layer 2 Security Considerations
2. Mitigate ARP Attacks

# Az ARP támadások mérséklése

14.6.1

## ARP támadások

Emlékezzünk vissza, hogy a gazdagépek ARP-kéréseket küldenek egy adott IPv4-címmel rendelkező gazdagép MAC-címének meghatározására. Ez általában az alapértelmezett átjáró MAC-címének felderítése érdekében történik. Az alhálózaton lévő összes gazdagép fogadja és feldolgozza az ARP-kérést. Az ARP-kérésben egyező IPv4-címmel rendelkező gazdagép ARP-választ küld.

Az ARP RFC szerint az ügyfelek kéretlen ARP-kérést küldhetnek, amelyet „ingyenes ARP-nek” neveznek. Amikor egy gazdagép ingyenes ARP-t küld, az alhálózat más gazdagépei az ARP-táblázatukban tárolják az ingyenes ARP-ben található MAC-címet és IPv4-címet.

A probléma az, hogy a támadó egy hamisított MAC-címet tartalmazó ingyenes ARP-üzenetet küldhet egy kapcsolónak, és a kapcsoló ennek megfelelően frissíti a MAC-táblázatát. Ezért bármely gazdagép állíthatja, hogy az általa választott IP- és MAC-cím kombináció tulajdonosa. Egy tipikus támadásban a fenyegetés szereplői kéretlen ARP-válaszokat küldhetnek az alhálózat más gazdagépeinek a fenyegetést okozó szereplő MAC-címével és az alapértelmezett átjáró IPv4-címével.

Az interneten számos eszköz áll rendelkezésre az ARP emberközép-támadások létrehozására, például a dsniff, a Cain & Abel, az ettercap, a Yersinia és mások. Az IPv6 ICMPv6 Neighbor Discovery Protocolt használ a 2. rétegbeli címfeloldáshoz. Az IPv6 stratégiákat tartalmaz a szomszédos hirdetések hamisításának csökkentésére, hasonlóan ahhoz, ahogy az IPv6 megakadályozza a meghamisított ARP-válaszokat.

Az ARP-hamisítás és az ARP-mérgezés mérséklése a Dynamic ARP Inspection (DAI) megvalósításával csökkenthető.

Kattintson az egyes lépésekre az ARP-hamisítás és az ARP-mérgezés példájának és magyarázatának megtekintéséhez.

**Normál állapot konvergált MAC-táblázatokkal**

Minden eszköz rendelkezik egy pontos MAC-táblázattal, amely tartalmazza a LAN-on lévő többi eszköz megfelelő IPv4- és MAC-címét.

A hálózat két gazdagépből áll – P C1-ből és P C2-ből, egy fenyegetési szereplőből –, amelyek az R1 útválasztóhoz csatlakoztatott switch-hez csatlakoznak. A P C1 IP-címe 10.0.0.11, MAC-értéke pedig BB:BB:BB. A fenyegetés szereplőjének, a P C2-nek az IP-címe 10.0.0.12, a MAC-je pedig CC:CC:CC. Az R 1 IP-je 10.0.0.1, MAC-ja pedig AA:AA:AA. Jelenleg a P C1-en lévő ARP-tábla a 10.0.0.1-es IP-címet AA:AA:AA MAC-címre, a 10.0.0.12-es IP-címet pedig a CC:CC:CC MAC-címre képezi le. A P C2 ARP-táblázata leképezi az IP 10.0.0.1-et az AA:AA:AA MAC-címre, a 10.0.0.11-es IP-címet pedig a BB:BB:BB MAC-címre. Az R1 ARP-táblázata a 10.0.0.11 IP-címet a BB:BB:BB MAC-címre, a 10.0.0.12-es IP-címet pedig a CC:CC:CC MAC-címre képezi le.

PC1 PC2

R1

Megjegyzés: A MAC-címek 24 bitesek az egyszerűség kedvéért. R1 ARP gyorsítótár PC1 ARP gyorsítótár PC2 ARP gyorsítótár MAC: CC:CC:CC IP: 10.0.0.12 MAC: BB:BB:BB IP: 10.0.0.11 MAC: AA:AA:AA IP: 10.0.0.1

|  |  |
| --- | --- |
| **IP-cím** | **Mac cím** |
| 10.0.0.1 | AA:AA:AA |
| 10.0.0.11 | BB:BB:BB |

|  |  |
| --- | --- |
| **IP-cím** | **Mac cím** |
| 10.0.0.11 | BB:BB:BB |
| 10.0.0.12 | CC:CC:CC |

|  |  |
| --- | --- |
| **IP-cím** | **Mac cím** |
| 10.0.0.1 | AA:AA:AA |
| 10.0.0.12 | CC:CC:CC |

14.6.2

## Videó - ARP hamisítás

14.6.3

## Dinamikus ARP ellenőrzés

Egy tipikus ARP-támadás során a fenyegetés szereplője kéretlen ARP-kéréseket küldhet az alhálózat más gazdagépeinek a fenyegetettség szereplőjének MAC-címével és az alapértelmezett átjáró IP-címével. Az ARP-hamisítás és az ebből eredő ARP-mérgezés megelőzése érdekében a kapcsolónak biztosítania kell, hogy csak érvényes ARP-kérések és válaszok kerüljenek továbbításra.

A dinamikus ARP-ellenőrzés (DAI) DHCP-figyelést igényel, és segít megelőzni az ARP-támadásokat:

* Érvénytelen vagy indokolatlan ARP-kérések továbbítása ugyanazon VLAN más portjaira
* Az összes ARP-kérés és válasz elfogása nem megbízható portokon
* Minden egyes elfogott csomag ellenőrzése érvényes IP-MAC-kötéshez
* Az ARP eldobása és naplózása Érvénytelen forrásból érkező kérések az ARP-mérgezés megelőzése érdekében
* Hiba az interfész letiltásakor, ha az ARP-csomagok konfigurált DAI-számát túllépik

14.6.4

## DAI végrehajtási irányelvek

Az ARP-hamisítás és az ARP-mérgezés esélyének csökkentése érdekében kövesse az alábbi DAI-megvalósítási irányelveket:

* Engedélyezze a DHCP-snoopot globálisan.
* Engedélyezze a DHCP-figyelést a kiválasztott VLAN-okon.
* DAI engedélyezése a kiválasztott VLAN-okon.
* Megbízható interfészek konfigurálása a DHCP leskelődéshez és az ARP ellenőrzéshez.

Általában tanácsos az összes hozzáférési kapcsoló portját nem megbízhatóként konfigurálni, és minden olyan uplink portot, amely más kapcsolókhoz csatlakozik, megbízhatóként konfigurálni.

Az ábrán látható mintatopológia a megbízható és a nem megbízható portokat azonosítja.

A grafikon egy jelmagyarázat látható egy lila négyzet alakú megbízható porttal és egy piros körrel, amely felett egy LAN diagram látható, amely a Dynamic ARP Inspection Trust-ot mutatja. Az ábra egy LAN-hálózatot mutat be megbízható és nem megbízható portokkal. Az egyik interfészen a bal alsó sarokban egy támadó található az egyik számítógépen, a bal felső sarokban pedig egy hagyományos PC. Mindkét eszköz csatlakozik a switch-hez, és mindkettő kapcsolóportján piros kör látható, amely nem megbízható portot jelöl. A kapcsolótól jobbra egy útválasztó található, amely szintén a kapcsolóhoz csatlakozik. Az útválasztó kapcsolatának kapcsolóján egy lila négyzet található, amely az ARP megbízható kapcsolatát szimbolizálja.

PC-A S1 R1 F0/1 F0/2

F0/24

Nem megbízható port Megbízható port VLAN 10

14.6.5

## DAI konfigurációs példa

Az előző topológiában az S1 két felhasználót köt össze a VLAN 10-en. A DAI úgy lesz konfigurálva, hogy csökkentse az ARP-hamisítás és az ARP-mérgezés támadásait.

Amint a példában látható, a DHCP lekérdezés engedélyezve van, mert a DAI működéséhez a DHCP lekérdezési kötési tábla szükséges. Ezután a DHCP leskelődés és az ARP ellenőrzés engedélyezve van a VLAN10 számítógépeken. Az útválasztó uplink portja megbízható, ezért megbízhatóként van konfigurálva a DHCP leskelődéshez és az ARP ellenőrzéshez.

S1(config)# **ip dhcp snooping**

S1(config)# **ip dhcp snooping vlan 10**

S1(config)# **ip arp inspection vlan 10**

S1(config)# **interface fa0/24**

S1(config-if)# **ip dhcp snooping trust**

S1(config-if)# **ip arp inspection trust**

A DAI úgy is konfigurálható, hogy ellenőrizze a cél- vagy forrás MAC- és IP-címeket:

* **Cél MAC** – Ellenőrzi a cél MAC-címét az Ethernet fejlécben az ARP csomagtörzsben lévő cél MAC-címével.
* **Forrás MAC** – Ellenőrzi a forrás MAC-címét az Ethernet-fejlécben a küldő MAC-címével az ARP-csomag törzsében
* **IP-cím** – Ellenőrzi, hogy az ARP-csomag törzsében vannak-e érvénytelen és váratlan IP-címek, beleértve a 0.0.0.0, 255.255.255.255 címeket és az összes IP csoportos küldési címet.

Az **ip arp ellenőrzés validate** { **src-mac** [ **dst-mac** ] [ **ip** ] } globális konfigurációs parancs a DAI beállítására szolgál, hogy az érvénytelen IP-címek esetén eldobja az ARP-csomagokat. Akkor használható, ha az ARP-csomagok törzsében lévő MAC-címek nem egyeznek meg az Ethernet-fejlécben megadott címekkel. Figyelje meg a következő példában, hogy csak egy parancs konfigurálható. Ezért több **ip arp ellenőrzés validálási** parancs beírása felülírja az előző parancsot. Ha egynél több érvényesítési módszert szeretne megadni, írja be őket ugyanabba a parancssorba, ahogyan a következő kimenetben látható és ellenőrzött.

S1(config)# **ip arp inspection validate ?**

dst-mac Validate destination MAC address

ip Validate IP addresses

src-mac Validate source MAC address

S1(config)# **ip arp inspection validate src-mac**

S1(config)# **ip arp inspection validate dst-mac**

S1(config)# **ip arp inspection validate ip**

S1(config)# **do show run | include validate**

ip arp inspection validate ip

S1(config)# **ip arp inspection validate src-mac dst-mac ip**

S1(config)# **do show run | include validate**

ip arp inspection validate src-mac dst-mac ip

S1(config)#

14.6.6

## Szintaxis-ellenőrző – Az ARP-támadások mérséklése

Valósítsa meg a DAI-t egy kapcsolóhoz a következő topológia és meghatározott követelmények alapján.

A szintaktikai ellenőrző topológiája egy elosztási kapcsolóval rendelkezik, amely a hozzáférési kapcsolók G0/1 interfészéhez csatlakozik. A hozzáférési kapcsolók F0/1 interfésze balra csatlakozik a PC-hez, a jobb oldalon pedig a G0/2 switch interfész egy szerverhez csatlakozik.

S1 F0/1 G0/1

G0/2

DHCP szerver

Jelenleg be van jelentkezve az S1-be. Engedélyezze a DHCP globális lekérdezését a kapcsoló számára.

S1(config)# ip dhcp leskelődés

interfész konfigurációs módjába **Lépjen be a g0/1 - 2** , bízzon a DHCP-snooping és a DAI interfészeiben, majd térjen vissza a globális konfigurációs módba.

S1(config)# interfész tartomány g0/1 - 2

S1(config-if-range)# ip dhcp leskelődő bizalom

S1(config-if-range)# ip arp ellenőrzési megbízhatóság

S1(config-if-range)# kilépés

Engedélyezze a DHCP leskelődést és a DAI-t a **10,20,30-49** VLAN-ok esetében .

S1(config)# ip dhcp snooping vlan 10,20,30-49

S1(config)# ip arp ellenőrzés vlan 10,20,30-49

S1(config)#

Sikeresen konfigurálta a DAI-t a kapcsolóhoz.

[14.5](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Mitigate DHCP Attacks](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[14.7](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Mitigate Address Spoofing Attacks](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                  
*               

1. Layer 2 Security Considerations
2. Mitigate Address Spoofing Attacks

# Csökkentse a címhamisítási támadásokat

14.7.1

## Címhamisítási támadások

A MAC-címek és az IP-címek többféle okból is hamisíthatók. Hamisítási támadások akkor fordulnak elő, amikor az egyik gazdagép a másiknak adja ki magát, hogy egyébként hozzáférhetetlen adatokat fogadjon, vagy hogy megkerülje a biztonsági konfigurációkat.

A kapcsolók által a MAC-címtáblázat feltöltésére használt módszer a MAC-címhamisítás néven ismert sebezhetőséghez vezet. MAC-címhamisítási támadások akkor fordulnak elő, amikor a támadók megváltoztatják gazdagépük MAC-címét, hogy az megfeleljen a célállomás másik ismert MAC-címének, amint az az ábrán látható. A támadó gazdagép ezután egy keretet küld a hálózaton keresztül az újonnan konfigurált MAC-címmel.

Az ábrán egy támadó és egy kapcsolóhoz csatlakoztatott szerver látható. A szerver mac-címe aabbc c. van egy nyíl, amely a támadótól a kapcsoló 2-es portjára mutat, a spoofed mac address aabbc c szavakkal. van egy mac-címtábla a switch-hez, ahol az aabbcc van az 1-es port cellájában, a tábla 2-es port cellájában pedig semmi.

### A támadó meghamisítja a szerver MAC-címét

AABBCC 2

1

Mac cím:   
**AABBCC** támadó meghamisított MAC-címe:   
**AABBCC** 2-es port 1- es kapcsolóport

Amikor a kapcsoló megkapja a keretet, megvizsgálja a forrás MAC-címét. A kapcsoló felülírja az aktuális MAC-tábla bejegyzést, és hozzárendeli a MAC-címet az új porthoz, az alábbi ábrán látható módon. Ezután akaratlanul továbbítja a célállomásnak szánt kereteket a támadó gazdagépnek.

Az ábrán egy támadó és egy kapcsolóhoz csatlakoztatott szerver látható. A szerver mac-címe aabbc c. van egy nyíl, amely a támadótól a kapcsoló 2-es portjára mutat, a spoofed mac address aabbc c szavakkal. van egy mac címtábla a switch-hez, ahol a 2-es port cellájában aabbcc van, a táblázat 1-es port cellájában pedig semmi.

### Kapcsoló Frissíti a MAC-táblázatot hamisított címmel

2 1

AABBCC

Mac cím:   
**AABBCC** támadó meghamisított MAC-címe:   
**AABBCC** 2-es port 1- es kapcsolóport

Amikor a kapcsoló megváltoztatja a MAC táblát, a célállomás nem kap forgalmat addig, amíg forgalmat nem küld. Amikor a célállomás forgalmat küld, a kapcsoló fogadja és megvizsgálja a keretet, aminek eredményeként a MAC-tábla még egyszer átíródik, és a MAC-címet az eredeti porthoz igazítja. Annak megakadályozására, hogy a kapcsoló visszaállítsa a meghamisított MAC-címport-hozzárendeléseket a megfelelő állapotba, a támadó gazdagép létrehozhat egy programot vagy szkriptet, amely folyamatosan kereteket küld a kapcsolónak, így a kapcsoló megőrzi a helytelen vagy hamisított információkat. A 2. rétegben nincs olyan biztonsági mechanizmus, amely lehetővé tenné a kapcsoló számára a MAC-címek forrásának ellenőrzését, ami miatt a hamisítás nagyon sebezhetővé válik.

Az IP-cím meghamisítása az, amikor egy szélhámos PC eltéríti a szomszéd érvényes IP-címét, vagy véletlenszerű IP-címet használ. Az IP-címhamisítást nehéz mérsékelni, különösen, ha olyan alhálózaton belül használják, amelyhez az IP tartozik.

14.7.2

## Címhamisítási támadások mérséklése

A MAC- és IP-címhamisítás elleni védelem érdekében konfigurálja az IP Source Guard (IPSG) biztonsági funkciót. Az IPSG ugyanúgy működik, mint a DAI, de minden csomagot megvizsgál, nem csak az ARP-csomagokat. A DAI-hoz hasonlóan az IPSG is megköveteli, hogy engedélyezve legyen a DHCP leskelődés.

Pontosabban, az IPSG nem megbízható 2. rétegbeli hozzáférési és fővonali portokon van telepítve. Az IPSG dinamikusan karbantartja a portonkénti VLAN ACL-eket (PVACL) az IP-MAC és a kapcsolóport közötti kötések alapján. Kezdetben a porton lévő összes IP-forgalom blokkolva van, kivéve azokat a DHCP-csomagokat, amelyeket a DHCP-snooping folyamat rögzít. A PVACL akkor kerül telepítésre a portra, ha az ügyfél érvényes IP-címet kap a DHCP-kiszolgálótól, vagy amikor a felhasználó statikus IP-forrás-összerendelést konfigurált.

Ez a folyamat az ügyfél IP-forgalmát az összerendelésben konfigurált forrás IP-címekre korlátozza. Minden olyan IP-forgalom, amelynek forrás IP-címe nem az IP-forrás-összerendelésben szereplő IP-cím, kiszűrésre kerül. Ez a szűrés korlátozza a gazdagép azon képességét, hogy a szomszédos gazdagép IP-címének igénylésével megtámadja a hálózatot.

Minden nem megbízható porthoz az IP-forgalom biztonsági szűrésének két lehetséges szintje van:

* **Forrás IP-cím szűrő** – Az IP-forgalom szűrése a forrás IP-címe alapján történik, és csak olyan IP-forgalom engedélyezett, amelynek forrás IP-címe megegyezik az IP-forrás-összerendelés bejegyzésével. Amikor új IP-forrás bejegyzés-összerendelés jön létre vagy törlődik a porton, a PVACL automatikusan beállítja magát, hogy tükrözze az IP-forrás-összerendelés változását.
* **Forrás IP- és MAC-címszűrő** – Az IP-forgalom a MAC-címen kívül a forrás IP-címe alapján is szűrésre kerül. Csak olyan IP-forgalom engedélyezett, amelynek forrás-IP- és MAC-címei megegyeznek az IP-forrás kötési bejegyzésével.

14.7.3

## Az IP Source Guard beállítása

Vizsgálja meg az ábrán látható IP Source Guard hivatkozási topológiát.

Az ábra az s 1 f0/24-éhez csatlakoztatott R 1-et mutatja. Az s1 a pca-hoz 192.168.10.10 / 2 hálózattal f 0 / 1-en keresztül, a pcb pedig 192.168.10.11 / 2 hálózattal f 0 / 2-n keresztül csatlakozik. mind a p cs a v lan 10-ben van.

PC-A PC-A F0/24 192.168.10.10/24 F0/2 S1 R1 192.168.10.11/24

F0/1

VLAN 10

Az IP Source Guard engedélyezve van a nem megbízható portokon az **ip verify source** paranccsal, az alábbi konfigurációban látható módon. Ne feledje, hogy a funkció csak 2. rétegbeli hozzáférési vagy fővonali porton konfigurálható, és DHCP-snooping szükséges az érvényes IP-cím és MAC-cím párok megtanulásához.

S1(config)# **interface range fastethernet 0/1 - 2**

S1(config-if-range)# **ip verify source**

S1(config-if-range)# **end**

S1#

A **show ip verify source** paranccsal ellenőrizze az IP Source Guard konfigurációját az alábbiak szerint. A példában az F0/1 és F0/2 portok IP Source Guard védelemmel vannak konfigurálva. Minden interfészhez egy érvényes DHCP-kötés tartozik

S1# **show ip verify source**

Interface Filter-type Filter-mode IP-address Mac-address Vlan

--------- ----------- ----------- --------------- ----------------- ----

F0/1 ip active 192.168.10.10 10

F0/2 ip active 192.168.10.11 10

S1#

14.7.4

## Szintaxis-ellenőrző - Az IP-forrás őrének konfigurálása

Ezzel a szintaktikai ellenőrzővel konfigurálhatja az IP Source Guard.

interfészeken **Az IP forrás őr engedélyezése nem megbízható F0/1-2** .

S1(config)# interfész tartomány F0/1 - 2

S1(config-if-range)# ip ellenőrizze a forrást

Használja a **do** parancsot a globális konfigurációs módban az IP-forrás őr beállításainak megjelenítéséhez.

S1(config-if-range)# nem mutatja az ip ellenőrzési forrást

Interfész Szűrő típusú Szűrőmódú IP-cím Mac-cím Vlan

--------- ----------- ----------- --------------- ---- ------------- ----

F0/1 ip aktív 192.168.10.10 10

F0/2 ip aktív 192.168.10.11 10

S1(config-if-range)#

Sikeresen konfigurálta az IP-forrás őrt.

[14.6](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Mitigate ARP Attacks](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[14.8](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Spanning Tree Protocol](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                           
*               

1. Layer 2 Security Considerations
2. Spanning Tree Protocol

# Spanning Tree Protocol

14.8.1

## Spanning Tree Protocol

A Spanning Tree Protocol (STP) egy hurokmegelőző hálózati protokoll, amely lehetővé teszi a redundanciát, miközben hurokmentes 2. rétegbeli topológiát hoz létre. Az IEEE 802.1D az STP eredeti IEEE MAC áthidaló szabványa.

Kattintson az ábrán a Lejátszás gombra az STP működés közbeni animációjának megtekintéséhez.

Az ábra egy animáció, amelyen 4 db és 3 kapcsoló látható. A három kapcsoló háromszögben kapcsolódik egymáshoz. három db csatlakozik az s 2-hez. pc 1 küld egy broadcast keretet. az s 2 fogadja. Az s 2 továbbítja az összes portot, kivéve a kiinduló portot és a blokkolt portot az s 3-ra. A másik két p cs és s1 fogadja a keretet. s 1 továbbítja az adást az összes porton, kivéve a kiinduló portot. a keretet a pc 4 és az s 3 fogadja. s 3 visszaküldi a keretet s 2-re. s 2 eldobja a keretet, mert blokkolt porton kapta.

### STP normál működés

A PC1 broadcast keretet küld.

Az S2 továbbítja az üzenetszórást az összes porton, kivéve a kiinduló portot és a blokkolt portot.

Az S1 továbbítja az üzenetszórást az összes porton, kivéve a kiindulási portot.

Az S3 fogadja a keretet, és visszaküldi az S2-nek.

Az S2 eldobja a keretet, mert blokkolt porton fogadta.

Trunk 2

Trunk1

Trunk 3

14.8.2

## STP újraszámítás

Kattintson a Lejátszás gombra a következő ábrán, ha meg szeretné tekinteni az STP újraszámítását hiba esetén.

Az ábra az előző animációval megegyező topológiájú animáció. Az animációban az S 2 és S 1 közötti fővonali kapcsolat meghibásodott. S 2 feloldja a 2. fővonal portjának blokkolását. P C1 üzenetszórási keretet küld az S 2-nek. S 2 továbbítja az üzenetszórást az összes kapcsolóporton, kivéve a kiinduló portot és a Trunk 1 meghibásodott kapcsolatát. S 3 továbbítja a broadcast out minden elérhető kapcsolót kikötők kivételével. S 1 csak az F0/3-ból továbbítja az adást.

### Az STP kompenzálja a hálózati hibát

Az S2 és S1 közötti fővonali kapcsolat meghibásodott.

Az S2 feloldja a Trunk2 portjának blokkolását.

A PC1 egy broadcast keretet küld az S2-nek.

Az S2 továbbítja a szórást az összes kapcsolóporton, kivéve a kiinduló portot és a Trunk1 meghibásodott hivatkozását.

Az S3 továbbítja az üzenetszórást az összes elérhető kapcsolóporton, kivéve a kiinduló portot.

Az S1 csak az F0/3-ból továbbítja az adást.

2. csomagtartó

Csomagtartó 1

3. csomagtartó

14.8.3

## 2. réteg hurkok

Az STP engedélyezése nélkül a 2. rétegbeli hurkok képződhetnek, aminek következtében a broadcast, multicast és ismeretlen unicast keretek a végtelenségig hurkolhatnak. Ez nagyon rövid időn belül, néha néhány másodpercen belül tönkreteheti a hálózatot. Például az üzenetszórási kereteket, például az ARP-kéréseket, a rendszer az eredeti bemeneti port kivételével az összes kapcsolóporton továbbítja. Ez biztosítja, hogy a szórási tartományban lévő összes eszköz képes legyen a keret fogadására. Ha egynél több útvonalon kell a keretet továbbítani, akkor végtelen hurok keletkezhet. Amikor hurok lép fel, a kapcsolón lévő MAC-címtáblázat folyamatosan változik a szórási keretekből származó frissítésekkel, ami a MAC-adatbázis instabilitását eredményezi. Ez magas CPU kihasználtságot okozhat, ami miatt a kapcsoló nem tudja továbbítani a kereteket.

A hurkok által érintett keretek nem csak a broadcast keretek közé tartoznak. A hurkolt hálózatra küldött ismeretlen unicast keretek duplikált keretek megérkezését eredményezhetik a céleszközre. Ismeretlen unicast keretről beszélünk, ha a switch nem tartalmazza a cél MAC-címet a MAC-címtáblázatában, és a keretet minden porton ki kell küldenie, kivéve a bemeneti portot.

Az animáció megtekintéséhez kattintson az ábrán a Lejátszás gombra. Amikor az animáció szünetel, olvassa el a műveletet leíró szöveget. Az animáció rövid szünet után folytatódik.

Az ábra egy animáció, amelynek topológiája megegyezik az előző animációval. Nincsenek blokkolt portok. A pc 1 egy broadcast keretet küld. Az s 2 frissíti a Mac-címtáblázatot. A pc 1s mac-címe f0-/11-re van leképezve. s 2 továbbítja az adást az összes porton, kivéve a fogadó portot. Az s 3 és az s 1 frissíti a Mac-címtáblázatait a pc 1 információival. s 3 és s 1 továbbítja az adást az összes porton, kivéve a fogadó portot. s 1 és s 3 csomagot kap az 1-es számítógépről egy új porton. ennek megfelelően frissítik a mac-címtáblázatukat. s 1 és s 3 továbbítja az adást az összes porton, kivéve a fogadó portot. Az s 2 frissíti a pc 1 mac-címtáblázatát azzal a porttal, amelyen utoljára fogadta a broadcast keretet. s 2 továbbítja a broadcast keretet az összes porton, kivéve az utoljára vett portot. a ciklus újra kezdődik.

S3 MAC táblázat

S1 MAC táblázat

S2 MAC táblázat

S3 MAC táblázat

S1 MAC táblázat

S2 MAC táblázat   
PC1 = F0/11

S3 MAC táblázat   
PC1 = F0/2

S2 MAC táblázat   
PC1 = F0/11

S1 MAC táblázat   
PC1 = F0/1

S3 MAC táblázat   
PC1 = F0/1

S2 MAC táblázat   
PC1 = F0/11

S1 MAC táblázat   
PC1 = F0/2

S3 MAC táblázat   
PC1 = F0/1

S2 MAC táblázat   
PC1 = F0/1

S1 MAC táblázat   
PC1 = F0/2

Az S2 frissíti a MAC-címtáblázatot. A PC1 MAC-címe F0/11-re van leképezve.

Az S2 a vételi port kivételével minden porton továbbítja az adást.

Az S3 és az S1 frissíti a MAC-címtáblázatát a PC1 információkkal.

Az S3 és S1 a vételi port kivételével az összes porton továbbítja a sugárzást.

Az S1 és S3 csomagot kap a PC1-től egy új porton. Ennek megfelelően frissítik a MAC-címtáblázatukat.

Az S1 és S3 a vételi port kivételével az összes porton továbbítja a sugárzást.

Az S2 frissíti a PC1 MAC-címtáblázatát azzal a porttal, amelyen utoljára vette a broadcast keretet.

Az S2 továbbítja a broadcast keretet az összes porton, kivéve az utolsó vett portot. A ciklus újra kezdődik.

2. csomagtartó

1. csomagtartó

3. csomagtartó

14.8.4

## STP port szerepek

A feszítőfa algoritmus egyetlen kapcsolót jelöl ki gyökérhídként, és azt használja referenciapontként az összes útvonalszámításhoz. Az ábrán a gyökérhidat (S1 kapcsoló) választási eljárással választjuk ki. Az STP-ben részt vevő összes kapcsoló BPDU-kereteket cserél annak meghatározására, hogy melyik kapcsoló rendelkezik a legalacsonyabb hídazonosítóval (BID) a hálózaton. A legalacsonyabb BID-vel rendelkező kapcsoló automatikusan a feszítőfa-algoritmus-számítások gyökérhídjává válik.

**Megjegyzés** : Az egyszerűség kedvéért tételezzük fel, amíg másképp nem jelezzük, hogy az összes kapcsoló összes portja a VLAN 1-hez van hozzárendelve. A kapcsolók az alapértelmezett PVST+-val vannak konfigurálva. Minden kapcsolónak egyedi MAC-címe van a VLAN 1-hez társítva.

az ábra ugyanaz a topológia, mint az előző animációk. Az s 1 gyökérhídként van jelölve, a többi kapcsolóhoz csatlakoztatott portok pedig kijelölt porttal vannak ellátva. A kapcsoló azon portja, amelyre minden kapcsolat megy, gyökérporttal van ellátva. a két másik kapcsoló közötti portokat kijelölt port és alternatív port jelölik. az alternatív porton van egy piros kör, rajta egy piros perjel.

### STP portok

F0/1 172.17.10.21 172.17.10.23 172.17.10.22 F0/2 172.17.10.27 F0/3 F0/11 F0/18 F0/6 F0/2 F0/1 F0/2 F0/1 PC2 PC1 PC3 S3 S1 S2

PC4

Trunk3 Trunk1 Trunk2 Gyökérhíd gyökérportja Kijelölt Port Kijelölt Port Gyökérport Kijelölt Port Alternatív Port

A BPDU egy üzenetküldő keret, amelyet kapcsolók cserélnek STP-re. Minden BPDU tartalmaz egy BID-t, amely azonosítja a BPDU-t küldő kapcsolót. A BID egy prioritási értéket, a küldő kapcsoló MAC-címét és egy opcionális kiterjesztett rendszerazonosítót tartalmaz. A legalacsonyabb BID értéket e három mező kombinációja határozza meg.

A gyökérhíd meghatározása után a feszítőfa algoritmus kiszámítja a hozzá vezető legrövidebb utat. Mindegyik kapcsoló a feszítőfa algoritmusát használja annak meghatározására, hogy mely portokat blokkolja. Míg a feszítőfa algoritmus meghatározza a legjobb útvonalat a gyökérhídhoz a szórási tartományban lévő összes kapcsolóporthoz, a forgalom nem kerül továbbításra a hálózaton. A feszítőfa algoritmus az útvonal- és a portköltségeket is figyelembe veszi a blokkolandó portok meghatározásakor. Az útvonalköltség kiszámítása a portsebességekhez társított portköltség-értékek felhasználásával történik minden egyes kapcsolóporthoz egy adott útvonalon. A portköltség értékek összege határozza meg a gyökérhíd teljes útköltségét. Ha egynél több útvonal közül lehet választani, a feszítőfa algoritmus a legalacsonyabb útköltséggel rendelkező utat választja.

Amikor a feszítőfa algoritmus meghatározta, hogy mely útvonalak a legkívánatosabbak az egyes kapcsolókhoz képest, portszerepeket rendel a résztvevő kapcsolóportokhoz. Az STP port szerepei a következők:

* **Alternatív** – Az alternatív vagy tartalék portok blokkolt állapotban vannak a hurkok megelőzése érdekében. Az alternatív portok csak azokon a fővonali kapcsolatokon vannak kiválasztva, amelyek egyik vége sem gyökérport.
* **Root** – A gyökérportok olyan kapcsolóportok, amelyek a legközelebb vannak a gyökérhídhoz.
* **Kijelölt** – A kijelölt portok mind olyan nem root portok, amelyekre az STP engedélyezi a forgalom továbbítását a hálózaton. A kijelölt portok kiválasztása fővonalonként történik. Ha a törzs egyik vége gyökérport, akkor a másik vége egy kijelölt port. A gyökérhíd összes portja kijelölt port

A fenti ábra a hálózat portszerepeinek kapcsolatát mutatja a gyökérhíddal, és azt, hogy engedélyezik-e a forgalom továbbítását. Az ábrán a Trunk2-nek csak az egyik vége van blokkolva. Ez lehetővé teszi a gyorsabb átállást továbbítási állapotba, ha a hálózat változása szükségessé teszi.

**Megjegyzés** : Az adminisztratív módon leállított portot letiltott portnak nevezzük.

14.8.5

## STP Root Bridge

Amint az ábrán látható, minden átívelő fapéldány (kapcsolt LAN vagy broadcast tartomány) rendelkezik egy kapcsolóval, amelyet gyökérhídként jelöltek meg. A gyökérhíd referenciapontként szolgál az összes feszítőfa számításhoz, hogy meghatározzák, mely redundáns útvonalakat kell blokkolni.

Egy választási folyamat határozza meg, hogy melyik kapcsoló lesz a gyökérhíd.

az ábrán három kapcsoló látható, az S 1, S 2 és S 3. Mindegyik egy fővonallal csatlakozik a másik kettőhöz. Az S2-hez P C1, P C2 és P C3 kapcsolódik. Az S1-hez P C4 van csatlakoztatva. Mindegyik kapcsoló megmutatja a hídazonosítót, a prioritást és a Mac-címet. A legalacsonyabb prioritási érték miatt az S 1 gyökérhídként szerepel.

PC2 PC1 PC3 S3 S2 F0/1 172.17.10.21 172.17.10.23 172.17.10.22 F0/2 PC4 172.17.10.27 F0/3 F0/18 F0/2 F0/1 F0/2 F0/1 F0/11 F0/6

S1

Trunk3 Bridge azonosító:   
Prioritás = 32769   
MAC-cím = 000A00222222 Trunk1 Trunk2 gyökérhídhíd azonosítója:   
Prioritás = 24577   
MAC-cím = 000A00333333 Hídazonosító:   
Prioritás = 32769   
MAC-cím = 000A00111111

Az alábbi ábra a BID mezőket mutatja. A BID egy prioritási értékből, egy kiterjesztett rendszerazonosítóból és a kapcsoló MAC-címéből áll.

Az ábrán a hídazonosító mezők láthatók. Ezek közé tartozik a prioritás, a kiterjesztett rendszerazonosító és a MAC-cím.

### Hídazonosító (BID) mezők

A híd prioritása kiterjesztve   
Rendszerazonosító MAC-cím Gyökérhíd- hídazonosító a kiterjesztett rendszerazonosítóval 4 bit 12 bit 48 bit

A sugárzási tartomány összes kapcsolója részt vesz a választási folyamatban. Miután egy kapcsoló elindul, két másodpercenként BPDU-kereteket kezd kiküldeni. Ezek a BPDU-keretek tartalmazzák a switch BID-t és a gyökérazonosítót.

Ahogy a kapcsolók továbbítják BPDU-kereteiket, a broadcast tartomány kapcsolói kiolvassák a gyökérazonosító információt a BPDU-keretekből. Ha a fogadott BPDU gyökérazonosítója alacsonyabb, mint a fogadó kapcsoló gyökérazonosítója, akkor a fogadó kapcsoló frissíti a gyökérazonosítóját, amely a szomszédos kapcsolót gyökérhídként azonosítja. A kapcsoló ezután az alacsonyabb gyökérazonosítójú új BPDU-kereteket továbbítja a többi kapcsolónak. Végül a legalacsonyabb BID-vel rendelkező kapcsolót a rendszer a feszítőfa példány gyökérhídjaként azonosítja.

Minden átívelő fa példányhoz van egy gyökérhíd. Lehetséges több különálló gyökérhíd. Ha az összes kapcsoló összes portja a VLAN 1 tagja, akkor csak egy átívelő fapéldány létezik. A kiterjesztett rendszerazonosító szerepet játszik az átívelő fa példányok meghatározásában.

14.8.6

## STP útvonal költsége

Amikor a gyökérhidat kiválasztották a feszítőfa-példányhoz, a feszítőfa-algoritmus elindítja a gyökérhídhoz vezető legjobb útvonalak meghatározását a szórási tartományban lévő összes célból. Az útvonalinformációkat a célállomástól a gyökérhídig tartó útvonalon az egyes portköltségek összegzése határozza meg. Mindegyik „célállomás” valójában egy kapcsolóport.

Az alapértelmezett portköltségeket a port működési sebessége határozza meg. A táblázatból látható, hogy a 10 Gb/s Ethernet portok portköltsége 2, az 1 Gb/s Ethernet portok portköltsége 4, a 100 Mb/s Fast Ethernet portok portköltsége 19 és 10 Mb/ s Az Ethernet portok portköltsége 100.

| **Link sebessége és neve** | **Költség (Átdolgozott IEEE-specifikáció)** | **Költség (korábbi IEEE specifikáció)** |
| --- | --- | --- |
| 10 Gb/s | 2 | 1 |
| 1 Gb/s | 4 | 1 |
| 100 Mb/s | 19 | 10 |
| 10 Mb/s | 100 | 100 |

**Megjegyzés** : Amint újabb, gyorsabb Ethernet-technológiák válnak elérhetővé, az útköltség értékei változhatnak, hogy alkalmazkodjanak az új sebességekhez. A táblázatban szereplő nemlineáris számok a régebbi Ethernet-szabvány néhány fejlesztését tartalmazzák. Az értékek megváltoztak, hogy megfeleljenek a 10 Gb/s Ethernet szabványnak. A nagy sebességű hálózatokhoz kapcsolódó folyamatos változás szemléltetésére a Catalyst 4500 és 6500 switchek támogatják a hosszabb útköltség módszerét; például 10 Gb/s 2000, 100 Gb/s 200, 1 Tb/s pedig 20 útköltség.

Bár a kapcsolóportokhoz alapértelmezett portköltség tartozik, a portköltség konfigurálható. Az egyéni portköltségek konfigurálhatósága rugalmasságot biztosít a rendszergazdának a gyökérhídhoz vezető átívelő fa útvonalak manuális vezérléséhez.

Egy interfész portköltségének konfigurálásához adja meg a **spanning-tree cost value** parancsot interfész konfigurációs módban. Az érték 1 és 200 000 000 között lehet.

Az alábbi példában az F0/1 kapcsolóport 25 portköltséggel lett konfigurálva **feszítőfa költség 25 interfész konfigurációs mód parancsával.** az F0/1 interfészen található

S2# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

S2(config)# **interface f0/1**

S2(config-if)# **spanning-tree cost 25**

S2(config-if# **end**

S2#

Ha vissza szeretné állítani a portköltséget az alapértelmezett 19-es értékre, írja be a **nincs feszítőfa költség** interfész konfigurációs mód parancsot.

S2# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

S2(config)# **interface f0/1**

S2(config-if)# **no spanning-tree cost**

S2(config-if)# **end**

S2#

Az útvonal költsége megegyezik a gyökérhídhoz vezető útvonal összes portköltségének összegével. A legalacsonyabb költségű útvonalak előnyben részesülnek, és az összes többi redundáns útvonal le van tiltva. Az alábbi példában az S2-től az S1 gyökérhídig az 1-es útvonalon keresztül elért út költsége 19 (az IEEE által meghatározott egyéni portköltség alapján), míg a 2-es útvonalon elért út költsége kétszer 19 vagy 38. Mivel az elérési út Az 1-es általános útvonal költsége alacsonyabb a gyökérhídhoz, ez az előnyben részesített útvonal. Az STP ezután blokkolva konfigurálja a redundáns elérési utat, megakadályozva ezzel a hurok előfordulását.

Az ábra az S 2-től az egyik átkapcsolásig (gyökérhíd) vezető két utat és azok költségét mutatja. Ez szükséges annak meghatározásához, hogy a 2. kapcsoló melyik portja lesz a gyökérport.

PC2 PC1 PC3 S3 S1 S2 PC4 F0/1 172.17.10.21 172.17.10.23 172.17.10.22 F0/2 172.17.10.27 F0/3 F0/11 F0/18 F0/6 F0/2 F0/1 F0/2

F0/1

Hídazonosító:   
Prioritás = **32769**   
MAC-cím = 000A00222222 Hídazonosító:   
Prioritás = **27577**   
MAC-cím = 000A00333333 Hídazonosító:   
Prioritás = **32769**   
MAC-cím = 000A00111111 3. főtörzs1 híd 2. fő fővonal 2. útvonala 1. út 2. út

A gyökérhíd port- és útvonalköltségének ellenőrzéséhez írja be a **show spanning-tree** parancsot. A Költség mező a gyökérhíd teljes útköltsége. Ez az érték attól függően változik, hogy hány kapcsolóporton kell áthaladni a gyökérhídhoz való eljutáshoz. Az alábbi kimenetben minden interfész 19-es egyedi portköltséggel is azonosítható.

S2# **show spanning-tree**

VLAN001

Spanning tree enabled protocol ieee

Root ID Priority 27577

Address 000A.0033.3333

Cost 19

Port 1

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 000A.0011.1111

Hello time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300

Interface Role Sts Cost Prio.Nbr Type

----------- ----- ---- ----- --------- -----------------

F0/1 Root FWD 19 128.1 Edge P2p

F0/2 Desg FWD 19 128.2 Edge P2p

14.8.7

## Válassza ki a Root Bridge-et

Ha egy rendszergazda azt szeretné, hogy egy adott kapcsoló gyökérhíddá váljon, a hídprioritás értékét úgy kell beállítani, hogy az alacsonyabb legyen, mint a hálózat összes többi kapcsolójának hídprioritásértéke. Két különböző módszer létezik a hídprioritás értékének konfigurálására egy Cisco Catalyst kapcsolón.

Az 1. ábra három kapcsolót mutat, amelyek a fővonali összeköttetésekkel vannak összekötve.

S2 S3 S1 F0/2 F0/2 F0/1 F0/2 F0/1

F0/1

Törzs1 törzs2 törzs3

Lásd a fenti topológiát. Kattintson a gombokra a hídprioritás konfigurálásának két módszerére vonatkozó példák megtekintéséhez, valamint annak ellenőrzéséhez, hogy egy híd rootként működik-e.

Annak biztosítására, hogy a kapcsoló a legalacsonyabb hídprioritásértékkel rendelkezzen, használja a **spanning-tree vlan** vlan-id **root elsődleges** parancsot globális konfigurációs módban. A kapcsoló prioritása az előre meghatározott 24 576 értékre vagy a 4 096 legmagasabb többszörösére van állítva, ami kisebb, mint a hálózaton észlelt legalacsonyabb hídprioritás.

Ha alternatív gyökérhídra van szükség, használja a **spanning-tree vlan** vlan-id **root másodlagos** globális konfigurációs mód parancsot. Ez a parancs a kapcsoló prioritását az előre meghatározott 28 672 értékre állítja be. Ez biztosítja, hogy az alternatív kapcsoló legyen a gyökérhíd, ha az elsődleges gyökérhíd meghibásodik. Ez azt feltételezi, hogy a hálózat többi kapcsolója az alapértelmezett 32 768-as prioritási értékkel rendelkezik.

Ebben a példában az S1 elsődleges gyökérhídként van hozzárendelve a **spanning-tree vlan 1 root elsődleges** paranccsal, az S2 pedig másodlagos gyökérhídként van konfigurálva a **spanning-tree vlan 1 root másodlagos** paranccsal.

S1(config)# **spanning-tree VLAN 1 root primary**

S1(config)# **end**

-----------------------

S2(config)# **spanning-tree root secondary**

S2(config)# **end**

14.8.8

## Szintaxis-ellenőrző – A Root Bridge konfigurálása és ellenőrzése

Bevezető szöveg. Ez lehet egy pontokkal felsorolt ​​lista arról, hogy mit fognak tenni, vagy bármilyen más megfelelő szöveg

You are logged into S3:

* Configure the priority for VLAN 1 on S3 to 24567.
* Enter the **end** command to return to privileged EXEC mode.

S3(config)#spanning-tree vlan 1 priority 24576

S3(config)#end

------------------------

You are now logged into S2:

* Configure S2 to be the secondary root for VLAN 1.
* Enter the **end** command to return to privileged EXEC mode.

S2(config)#spanning-tree vlan 1 root secondary

S2(config)#end

------------------------

You are now logged into S1:

* Configure S1 to be the primary root for VLAN 1.
* Enter the **end** command to return to privileged EXEC mode.

S1(config)#spanning-tree vlan 1 root primary

S1(config)#end

Display the current spanning tree status on S1.

S1#show spanning-tree

VLAN0001

Átfogó fa engedélyezett protokoll ieee

Gyökérazonosító prioritás 24577

Cím: 000A.0033.0033

Ez a híd a gyökér

Üdvözlési idő 2 mp Max. életkor 20 mp Továbbítási késleltetés 15 mp

Hídazonosító prioritás 24577 (prioritás: 24576 sys-id-ext 1)

Cím: 000A.0033.0033

Üdvözlési idő 2 mp Max. életkor 20 mp Továbbítási késleltetés 15 mp

Érlelési idő 15 mp

Interfész Szerep Sts Költség Prio.Nbr Típus

------------------- ---- --- --------- -------- ------- ------------------

Fa0/1 Desg FWD 4 128.1 P2p

Fa0/2 Desg FWD 4 128.2 P2p

S1#

Sikeresen konfigurálta és ellenőrizte a Root Bridge-et.

14.8.9

## Videó - Figyelje meg az STP működését

14.8.10

## Packet Tracer – Vizsgálja meg az STP Loop Prevenciót

Ebben a Packet Tracer tevékenységben a következő célokat valósítja meg:

* Hozzon létre és konfiguráljon egy egyszerű három kapcsolós hálózatot STP-vel.
* Tekintse meg az STP működését
* Kapcsolja ki az STP-t, és tekintse meg újra a műveletet.

[Vizsgálja meg az STP hurok megelőzést](https://contenthub.netacad.com/courses/netsec/_common/14.8.10-packet-tracer---investigate-stp-loop-prevention.pka)

14.8.11

## Ellenőrizze, hogy megértette – az STP célja

Az űrlap teteje

Ellenőrizze, hogy megértette-e az STP célját, és válassza ki a megfelelő választ a következő kérdésekre.

1. Melyik állítás írja le az STP-t?

Az űrlap alja

STP nélkül az Ethernet LAN-on melyik háromféle keret okozhat katasztrofális hurkot a hálózatban? (Válassz hármat.)

Milyen eszközt választ a Spanning Tree Algorithm? Az összes többi kapcsoló egyetlen legalacsonyabb költségű utat határoz meg ehhez az eszközhöz.

[14.7](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Mitigate Address Spoofing Attacks](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[14.9](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Mitigate STP Attacks](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                    
*               

1. Layer 2 Security Considerations
2. Mitigate STP Attacks

# Csökkentse az STP-támadásokat

14.9.1

## STP támadás

A fenyegetés szereplői a gyökérhíd meghamisításával és a hálózat topológiájának megváltoztatásával manipulálhatják a Spanning Tree Protocolt (STP), hogy támadást hajtsanak végre. A támadók gyökérhídként jeleníthetik meg gazdáikat; és ezért rögzíti az azonnali váltott tartomány teljes forgalmát.

Az STP-manipulációs támadás végrehajtásához a támadó gazdagép STP-hídprotokoll adategységeket (BPDU-kat) sugároz, amelyek konfigurációs és topológia-módosításokat tartalmaznak, amelyek átívelő fa újraszámítását kényszerítik ki, amint az az ábrán látható. A támadó gazdagép által küldött BPDU-k alacsonyabb hídprioritást jelentenek be, hogy megkíséreljék őket gyökérhídnak választani.

**Megjegyzés** : Ezek a problémák akkor fordulhatnak elő, ha valaki rosszindulatú szándék nélkül Ethernet-kapcsolót ad hozzá a hálózathoz.

Az ábrán egy fenyegetésügynök és két kapcsoló látható, amelyek háromszögben vannak összekapcsolva, a támadóval alul. Mindkét port a támadó és a bal felső kapcsoló között továbbítódik. A kapcsolók közötti kapcsolat mindkét portja továbbító. A támadó és a jobb felső kapcsoló közötti kapcsolaton a támadó portja blokkol, a kapcsoló portja pedig továbbítást végez. A bal felső kapcsoló jelenleg a gyökérhíd 8192-es prioritással. A támadó mindkét kapcsolóra STPBPD Us-t küldött 0-s prioritással.

STP BDPU prioritás = 0 gyökérhíd STP BDPU prioritása = 0 továbbítási blokk prioritás = 8192

Siker esetén a támadó gazdagép lesz a gyökérhíd, amint az az alábbi ábrán látható, és most már számos olyan képkockát rögzíthet, amelyek egyébként nem lennének elérhetőek.

Az ábrán egy fenyegetésügynök és két kapcsoló látható, amelyek háromszögben vannak összekapcsolva, a támadóval alul. A támadó a gyökérhíd lett. Mindkét port a támadó és a bal felső kapcsoló között továbbítódik. A támadó és a jobb felső kapcsoló közötti kapcsolat mindkét portja szintén továbbító. A felső kapcsolók közötti kapcsolaton a bal oldali kapcsolóport továbbító, a jobb oldali kapcsolóport blokkol.

Előre Block Root Bridge

Ezt az STP-támadást a BPDU Guard alkalmazása az összes hozzáférési porton enyhíti.

14.9.2

## STP támadások mérséklése

Az STP-manipulációs támadások mérséklése érdekében használja a Cisco STP-stabilitási mechanizmusait a kapcsolók általános teljesítményének javítására, és csökkenti a topológiaváltások során elveszett időt.

Ezek az STP stabilitási mechanizmusai:

* **PortFast** – A PortFast azonnal továbbítási állapotba hozza a hozzáférési vagy fővonali portként konfigurált interfészt a blokkoló állapotból. Ez megkerüli a hallgatási és tanulási állapotokat. Minden végfelhasználói porton alkalmazni kell. A PortFast csak akkor konfigurálható, ha a porthoz egy gazdagép csatlakozik, egy másik kapcsoló nem.
* **BPDU Guard** – A BPDU őr azonnali hiba miatt letiltja a BPDU-t fogadó portot. Általában a PortFast-kompatibilis portokon használják. Alkalmazni minden végfelhasználói portra.
* **Root Guard** – Gyökérvédő megakadályozza, hogy a nem megfelelő kapcsoló gyökérhíddá váljon. A gyökérvédelem korlátozza azokat a kapcsolóportokat, amelyeken keresztül a gyökérhíd áthaladhat. Alkalmazza az összes olyan portot, amely nem válhat root porttá.
* **Hurokvédő** – A hurokvédő megakadályozza, hogy az alternatív vagy gyökérportok kijelölt portokká váljanak olyan hiba miatt, amely egyirányú kapcsolathoz vezet. Alkalmazzon minden olyan portra, amely nincs vagy kijelölhető.

Ezek a szolgáltatások kényszerítik a gyökérhíd elhelyezését a hálózatban, és kényszerítik az STP tartomány határait.

Az ábra kiemeli azokat a portokat, amelyeken ezeket a funkciókat meg kell valósítani.

Az ábra azokat a portokat szemlélteti, ahol a Cisco STP stabilitási jellemzőit meg kell valósítani. egy elsődleges gyökérhíd és egy másodlagos gyökérhíd kapcsolódik egymáshoz. mindkét port hurokvédő felirattal van ellátva. ezek a gyökérhidak egy kapcsolóhoz vannak kötve. ezek a portok a hidakon gyökérvédővel, a kapcsoló portjai pedig hurokvédő felirattal vannak ellátva. a kapcsoló számítógépekhez csatlakozik. ezek a portok portfast és bpdu guard felirattal vannak ellátva.

### STP stabilitási mechanizmusok

S1

Elsődleges   
Gyökérhíd másodlagos   
Root Bridge PortFast BPDU Guard Root Guard Loop Guard

14.9.3

## A PortFast konfigurálása

A PortFast megkerüli az STP figyelési és tanulási állapotokat, hogy minimálisra csökkentse azt az időt, ameddig a hozzáférési portoknak várniuk kell az STP konvergálására. Ha a PortFast engedélyezve van egy másik kapcsolóhoz csatlakozó porton, fennáll annak a veszélye, hogy feszítőfa hurok jön létre.

interface konfigurációs paranccsal engedélyezhető **A PortFast az interfészen a spanning-tree portfast** . Alternatív megoldásként a Portfast globálisan konfigurálható az összes hozzáférési porton a **spanning-tree portfast alapértelmezett** globális konfigurációs paranccsal.

Annak ellenőrzésére, hogy a PortFast globálisan engedélyezve van-e, használhatja a **show running-config | begin span** parancs vagy a **show spanning-tree summary** parancs. Annak ellenőrzéséhez, hogy a PortFast engedélyezve van-e egy interfészen, használja a **show running-config interface** type/number parancsot, ahogy az a következő példában látható. a **show spanning-tree interface** type/number **detail parancs is.** Ellenőrzésre használható

Figyelje meg a figyelmeztető üzeneteket, amelyek akkor jelennek meg, ha a PortFast engedélyezve van.

S1(config)# **interface fa0/1**

S1(config-if)# **switchport mode access**

S1(config-if)# **spanning-tree portfast**

%Warning: portfast should only be enabled on ports connected to a single

host. Connecting hubs, concentrators, switches, bridges, etc... to this

interface when portfast is enabled, can cause temporary bridging loops.

Use with CAUTION

%Portfast has been configured on FastEthernet0/1 but will only

have effect when the interface is in a non-trunking mode.

S1(config-if)# **exit**

S1(config)# **spanning-tree portfast default**

%Warning: this command enables portfast by default on all interfaces. You

should now disable portfast explicitly on switched ports leading to hubs,

switches and bridges as they may create temporary bridging loops.

S1(config)# **exit**

S1# **show running-config | begin span**

spanning-tree mode pvst

spanning-tree portfast default

spanning-tree extend system-id

!

interface FastEthernet0/1

switchport mode access

spanning-tree portfast

!

interface FastEthernet0/2

!

interface FastEthernet0/3

!

interface FastEthernet0/4

!

interface FastEthernet0/5

!

(output omitted)

S1#

14.9.4

## BPDU Guard konfigurálása

Annak ellenére, hogy a PortFast engedélyezve van, az interfész továbbra is figyel a BPDU-kra. A váratlan BPDU-k véletlenek lehetnek, vagy egy kapcsoló hálózathoz való jogosulatlan kísérletének részei.

Ha egy BPDU Guard-kompatibilis porton BPDU-k érkeznek, az a port hibaletiltás állapotba kerül. Ez azt jelenti, hogy a port le van tiltva, és manuálisan újra kell engedélyezni, vagy automatikusan vissza kell állítani a **hibás helyreállítási ok bpduguard** globális paranccsal.

engedélyezhető egy porton **A BPDU Guard a spanning-tree bpduguard enable** interfész konfigurációs paranccsal . Alternatív megoldásként használja a **spanning-tree portfast bpduguard alapértelmezett** globális konfigurációs parancsot a BPDU-védelem globális engedélyezéséhez az összes PortFast-kompatibilis porton.

A feszítőfa állapotával kapcsolatos információk megjelenítéséhez használja a **show spanning-tree summary** parancsot. A példában a PortFast default és a BPDU Guard egyaránt engedélyezett alapértelmezett állapotként a hozzáférési módban konfigurált portoknál.

**Megjegyzés** : Mindig engedélyezze a BPDU Guard funkciót az összes PortFast-kompatibilis porton.

S1(config)# **interface fa0/1**

S1(config-if)# **spanning-tree bpduguard enable**

S1(config-if)# **exit**

S1(config)# **spanning-tree portfast bpduguard default**

S1(config)# **end**

S1# **show spanning-tree summary**

Switch is in pvst mode

Root bridge for: none

Extended system ID is enabled

Portfast Default is enabled

PortFast BPDU Guard Default is enabled

Portfast BPDU Filter Default is disabled

Loopguard Default is disabled

EtherChannel misconfig guard is enabled

UplinkFast is disabled

BackboneFast is disabled

Configured Pathcost method used is short

(output omitted)

S1#

14.9.5

## Szintaxis-ellenőrző - Az STP-támadások mérséklése

A PortFast és a BPDU Guard megvalósítása a következő topológián és meghatározott követelményeken alapuló kapcsolóhoz

A szintaktikai ellenőrzőnek van egy topológiája, ahol két 3. elosztási rétegű kapcsoló található a diagram tetején, amelyeket egy fővonal köt össze. Mindkét 3. rétegbeli kapcsolónak van egy fővonali kapcsolata, amelyek ugyanahhoz a 2. szintű hozzáférési kapcsolóhoz csatlakoznak alább. Ennek neve S1, és a G0/1-en és a G0/2-n van csatlakoztatva. Az S 1 alatt több P C található, a kapcsoló oldalán pedig az F0/1 - F0/24.12.1.5 hozzáférési portok szerepelnek.

G0/1 G0/2 F0/1 - F0/24

S1

Trunk Trunk trönk hozzáférési portjai

You are currently logged into S1. Complete the following steps to implement PortFast and BPDU Guard on all access ports:

* interfész konfigurációs módjába **Lépjen be a fa0/1 - 24** .
* Konfigurálja a portokat a hozzáférési módhoz.
* Visszatérés a globális konfigurációs módba.
* Alapértelmezés szerint engedélyezze a PortFast minden hozzáférési porthoz.
* Alapértelmezés szerint engedélyezze a BPDU Guard szolgáltatást az összes hozzáférési porthoz.

S1(config)# interfész tartomány fa0/1 - 24

S1(config-if-range)# switchport módú hozzáférés

S1(config-if-range)# kilépés

S1(config)# spanning-tree portfast default

S1(config)# spanning-tree portfast bpduguard alapértelmezett

S1(config)# kilépés

Ellenőrizze, hogy a PortFast és a BPDU Guard alapértelmezés szerint engedélyezve van-e az STP összefoglaló információinak megtekintéséhez.

S1# a feszítőfa összefoglalását mutatja

A kapcsoló pvst módban van

Gyökérhíd ehhez: nincs

A kiterjesztett rendszerazonosító engedélyezve van

A Portfast Default engedélyezve van

A PortFast BPDU Guard Default engedélyezve van

A Portfast BPDU szűrő alapértelmezése le van tiltva

A Loopguard Default le van tiltva

Az EtherChannel hibás konfigurációs védelem engedélyezve van

Az UplinkFast le van tiltva

A BackboneFast le van tiltva

A használt konfigurált Pathcost metódus rövid

(kimenet kimaradt)

S1#

Sikeresen konfigurálta és ellenőrizte a PortFast és a BPDU Guard kapcsolót.

14.9.6

## A Root Guard konfigurálása

Vannak olyan kapcsolók a hálózatban, amelyek soha, semmilyen körülmények között nem válhatnak STP gyökérhídjává. A Root Guard módot biztosít a gyökérhidak elhelyezésének kényszerítésére a hálózatban azáltal, hogy korlátozza, hogy melyik kapcsoló válhat gyökérhídvá.

A Root Guard a legjobban olyan portokra telepíthető, amelyek olyan kapcsolókhoz csatlakoznak, amelyek nem lehetnek a gyökérhíd. Ha egy root-guard-kompatibilis port olyan BPDU-kat fogad, amelyek jobbak, mint az aktuális gyökérhíd által küldött port, akkor a port gyökér inkonzisztens állapotba kerül. Ez gyakorlatilag megegyezik az STP figyelési állapottal, és ezen a porton nem továbbítják az adatforgalmat. A helyreállítás azonnal megtörténik, amint a sértő eszköz már nem küld kiválóbb BPDU-kat.

A **spanning-tree guard root** interfész konfigurációs paranccsal konfigurálhatja a gyökérőrséget egy felületen.

Az ábrán D1 a gyökérhíd. Ha a D1 meghibásodik, csak a D2 kapcsoló legyen a gyökérhíd. Annak biztosítására, hogy az S1 soha ne legyen gyökérhíd, a D1 és D2 F0/1 interfészét engedélyezni kell a Root Guard számára.

Az ábra egy topológia, amely azt mutatja, hogy ha egy támadó gazdagép hamisított BPD Us-t küld ki, hogy a gyökérhíd legyen, a kapcsoló a BPDU fogadásakor figyelmen kívül hagyja a BPDU-t, és a portot gyökérbe helyezi. - inkonzisztens állapot

F0/1 F0/1 S1 D1

D2

Root Bridge Root Guard

Ha meg szeretné tekinteni azokat a Root Guard portokat, amelyek kiváló BPDU-kat kaptak, és gyökérinkonzisztens állapotban vannak, használja a **show spanning-tree inconsistent ports** parancsot.

**Megjegyzés** : A gyökérvédelem szükségtelennek tűnhet, mert a rendszergazda manuálisan nullára állíthatja egy kapcsoló híd prioritását. Ez azonban nem garantálja, hogy ezt a kapcsolót választják gyökérhídnak. Egy másik kapcsoló továbbra is gyökérré válhat, ha annak prioritása nulla és MAC-címe alacsonyabb.

14.9.7

## A Loop Guard konfigurálása

A kétirányú kapcsolatokon a forgalom mindkét irányban folyik. Ha valamilyen okból az egyirányú forgalom meghiúsul, ez egyirányú kapcsolatot hoz létre, amely 2. rétegbeli hurkot eredményezhet. Az STP a BPDU-k folyamatos vételére vagy továbbítására támaszkodik a port szerepkör alapján. A kijelölt port BPDU-kat küld, a nem kijelölt port pedig BPDU-kat fogad. A 2. rétegű hurok általában akkor jön létre, amikor egy redundáns topológiában lévő STP-port leállítja a BPDU-k fogadását, és hibásan átvált a továbbítási állapotba.

Az STP Loop Guard funkció további védelmet nyújt a Layer 2 hurkok ellen. Ha a BPDU-k nem érkeznek egy nem kijelölt Loop Guard-kompatibilis porton, a port átvált egy hurokkonzisztens blokkoló állapotba a figyelés/tanulás/továbbítás állapot helyett. A Loop Guard szolgáltatás nélkül a port egy kijelölt port szerepkört vesz fel, és hurkot hozna létre.

Amint az itt látható, a Loop Guard minden nem Root Guard porton engedélyezve van a **feszítőfa őr hurok** interfész konfigurációs parancsával.

**Megjegyzés** : A Loop Guard globálisan is engedélyezhető a **spanning-tree loopguard alapértelmezett** globális konfigurációs paranccsal. Ez engedélyezi a Loop Guard funkciót az összes pont-pont kapcsolaton.

Az ábra azt mutatja, hogy a Loop Guard minden nem gyökérőr porton engedélyezve van egy három kapcsolós topológiában.

D1 S1 D2 F0/1

F0/1

Root Bridge Root Guard Loop Guard

14.9.8

## Szintaxis-ellenőrző - Loop Guard konfigurálása

Valósítsa meg a PortFast, a BPDU Guard és a Loop Guard kapcsolót.

Configure S1 using the following instructions:

* Configure PortFast globally for all non-trunking ports on the switch.
* Enable BPDU guard globally on all ports with PortFast enabled.
* Enable Loop guard globally on all point-to-point links.
* Exit global configuration mode.

S1(config)#spanning-tree portfast default

%Warning: this command enables portfast by default on all interfaces. You

should now disable portfast explicitly on switched ports leading to hubs,

switches and bridges as they may create temporary bridging loops.

S1(config)#spanning-tree portfast bpduguard default

S1(config)#spanning-tree loopguard default

S1(config)#end

Verify that PortFast, BPDU guard, and Loop guard are enabled on switch S1.

S1#show spanning-tree summary

Switch is in pvst mode

Root bridge for: none

Extended system ID is enabled

Portfast Default is enabled

PortFast BPDU Guard Default is enabled

Portfast BPDU Filter Default is disabled

Loopguard Default is enabled

EtherChannel misconfig guard is enabled

UplinkFast is disabled

BackboneFast is disabled

Configured Pathcost method used is short

Name Blocking Listening Learning Forwarding STP Active

---------------------- -------- --------- -------- ---------- ----------

VLAN0001 1 0 0 5 6

---------------------- -------- --------- -------- ---------- ----------

1 vlan 1 0 0 5 6

S1#

Sikeresen konfigurálta és ellenőrizte a PortFast, a BPDU őrt ​​és a Loop Guard szolgáltatást.

14.9.9

## Lab - STP Security konfigurálása

Ebben a laborban a következő célokat kell teljesítenie:

* 1. rész: Az alapvető kapcsolóbeállítások konfigurálása.
* 2. rész: Biztonságos fővonali portok konfigurálása.
* 3. rész: Védelem az STP-támadások ellen.
* 4. rész: A portbiztonság konfigurálása és a nem használt portok letiltása.

14.9.10

## Packet Tracer – STP biztonság megvalósítása

Ebben a Packet Tracerben a következő célokat valósítja meg:

* Rendelje hozzá a központi kapcsolót gyökérhídként.
* Biztonságos feszítőfa-paraméterek az STP-manipulációs támadások megelőzése érdekében.
* A MAC-tábla túlcsordulási támadásainak megelőzése érdekében engedélyezze a portbiztonságot.

[Az STP biztonság megvalósítása](https://contenthub.netacad.com/courses/netsec/_common/14.9.10-packet-tracer---implement-stp-security.pka)

14.9.11

## Packet Tracer – 2. rétegű VLAN biztonság

Ebben a Packet Tracerben a következő célokat hajtja végre a 2. rétegbeli kapcsolók biztonságának konfigurálásához:

* Konfigurálja az alapvető beállításokat.
* SSH konfigurálása.
* Konfigurálja a biztonságos fővonalakat és hozzáférési portokat olyan funkciók engedélyezésével, mint a portbiztonság, a gyökérvédelem, a BPDU-védelem, a hurokvédelem és a PVLAN Edge.
* A DHCP Snooping beállítása.

[2. rétegű VLAN biztonság](https://contenthub.netacad.com/courses/netsec/_common/14.9.11-packet-tracer---layer-2-vlan-security.pka)

[14.8](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Spanning Tree Protocol](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[14.10](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Layer 2 Security Considerations Summary](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                   

1. Layer 2 Security Considerations
2. Layer 2 Security Considerations Summary

# 2. réteg biztonsági szempontok összefoglalása

14.10.1

## Mit tanultam ebben a modulban?

**2. réteg biztonsági fenyegetések**   
A biztonság az OSI-modell minden szintjén megvalósul. Ha azonban a 2. réteget megzavarja egy kibertámadás, az összes felette lévő réteget érinti. A 2. rétegben számos támadás fordulhat elő, beleértve a MAC-tábla támadásokat, a VLAN-támadásokat, a DHCP-támadásokat, az ARP-támadásokat, a címhamisítási támadásokat és az STP-támadásokat. Fontos a 2. réteg védelme a protokollok biztonságos változatainak, például SSH, SCP és SSL használatával. A sávon kívüli felügyelet használata, amikor csak lehetséges, és egy dedikált VLAN létrehozása a felügyeleti forgalom számára, szintén csökkenti a sikeres 2. rétegbeli támadások valószínűségét. Ezenkívül ACL-eket kell használni a nem kívánt hozzáférés kiszűrésére. A portbiztonság, a DHCP Snooping, a DAI és az IP Source Guard elérhető a Cisco switcheken a 2. rétegbeli támadások közvetlen mérséklése érdekében.

**MAC asztali támadások**   
A 2. rétegbeli kapcsolók MAC-címeket használnak a továbbítási döntések meghozatalához. A kapcsoló egy MAC-táblázatot használ, amely a MAC-címeket a kapcsolóportokhoz rendeli hozzá. A kapcsoló a fogadott keretek MAC-táblázatában megkeresi a cél MAC-címét. Ezután továbbítja a forgalmat a megfelelő portra. Ha a kapcsoló nem ismeri fel a cél MAC-címét, elárasztja az ismeretlen célhoz tartozó kereteket az összes portról, kivéve azt a portot, amelyről a keretek származtak. Ezeket ismeretlen unicast üzeneteknek nevezzük. A kapcsoló dinamikusan tanulja meg a MAC-címeket a portjairól származó keretek forráscímeiből. A Layer 2 támadások egyik típusa véletlenszerű MAC-forráscímű keretekkel árasztja el a kapcsolót. A kapcsoló megpróbálja hozzáadni ezeket a kereteket a MAC-táblához, amíg a tábla meg nem telik. A következő kereteket a rendszer ezután ismeretlen unicast üzenetként kezeli, és a fogadó port kivételével az összeset kiküldi. Mivel ezek a keretek elárasztottak, a fenyegetés szereplői a hálózaton küldött összes forgalmat fogadhatják. A fenyegető színész eszközök, mint pl **A macof** gyorsan túlterhelheti egy kapcsoló MAC tábláját, ami a MAC tábla túlcsordulási kihasználását okozza. Mivel az ismeretlen unicast címek elárasztása magába foglalhatja a fővonali portokat más kapcsolókhoz, a kihasználás széles körű zavarokat okozhat.

**Csökkentse a MAC asztali támadásokat**   
A 2. rétegű eszközöket a vállalat biztonsági infrastruktúrájának leggyengébb láncszemének tekintik, mivel a 2. rétegű támadások a legkönnyebben telepíthetők a hackerek számára. Emiatt a Cisco számos 2. rétegbeli biztonsági intézkedést fejlesztett ki a switch IOS-ben. A 2. rétegbeli támadások megelőzésének egyszerű, de hatékony módja az összes használaton kívüli port leállítása. A portbiztonság egyszerű módja a MAC-cím túlcsordulási támadásainak közvetlen kezelésére. A portbiztonsággal szabályozható az egy porton megtanulható MAC-címek száma és a címek megtanulásának módja. A portbiztonsági öregedés a biztonságos MAC-címek biztonságos portról történő eltávolítására használható a meglévő biztonságos MAC-címek manuális törlése nélkül. Az öregedési időkorlátok is növelhetők, hogy a korábbi biztonságos MAC-címek megmaradjanak, még új MAC-címek hozzáadásakor is. Portbiztonsági megsértések esetén a kapcsolóport beállítható úgy, hogy **leálljon** , **korlátozza** az ismeretlen MAC-címekről származó keretek továbbítását, és rendszernapló-üzenetet adjon ki, vagy **védelmet** , hogy eldobja a kereteket az ismeretlen gazdagéptől, de ne adjon ki rendszernapló-üzenetet. A védelem a legkevésbé biztonságos lehetőség. A port biztonsága miatt leállított port **err-disabled** állapotba kerül. A portot manuálisan újra engedélyezni kell a **leállítási** és **leállítási** parancsok nélkül, hogy visszatérjen a biztonságos állapotba.

**Csökkentse a VLAN-támadásokat**   
A VLAN-ok felhasználhatók az érzékeny forgalom és a többi forgalom elkülönítésére. A VLAN ugrás és a VLAN kettős címkézési támadások lehetővé teszik a fenyegetés szereplői számára, hogy hozzáférjenek azokhoz a VLAN-okhoz, amelyekhez nincs jogosultságuk. A VLAN ugrásos támadások során a fenyegetés szereplője egy gazdaszámítógépet kapcsol egy switch-hez, majd megpróbálja elérni, hogy a kapcsolóport DTP segítségével trönkké váljon. A fenyegetőző számítógép megpróbál egy másik kapcsolóként működni, amelyet egy törzs köt össze. A fővonalak alapértelmezés szerint az összes VLAN-hoz forgalmazzák, így ha egy fenyegető szereplő egy trönkezett kapcsolaton keresztül tud számítógépet csatlakoztatni, akkor az összes VLAN-forgalom elfogható. A VLAN kettős címkézéses támadásaiban a fenyegetés szereplői a jogos címke mellett hamis VLAN-címkét is hozzáadnak a rosszindulatú forgalomhoz. Ez lehetővé teheti a fenyegetés szereplői számára, hogy jogosulatlan forgalmat küldjenek más VLAN-okba. A VLAN-ugrásos és a kettős címkézéses támadások mérsékelhetők a trunking és a trunk egyeztetés letiltásával minden olyan kapcsolóporton, amelyhez a felhasználók hozzáférnek, és biztosítják, hogy a natív VLAN-t csak a fővonali kapcsolatokon használják. A privát VLAN-portok sebezhetőek lehetnek a PVLAN-proxy támadásokkal szemben, amelyek során a fenyegetés szereplői meghamisíthatják az alapértelmezett átjáró-útválasztó cél MAC-címét. Az útválasztó ezután engedélyezi az illetéktelen forgalom bejutását a cél VLAN-okba. A PVLAN proxy támadások a hozzáférés-felügyeleti listák használatával mérsékelhetők.

**Mérsékelje a DHCP-támadásokat**   
A DHCP-támadások két típusa a DHCP-éhezés és a DHCP-hamisítás. Mindkét támadást mérsékli a DHCP-snooping megvalósítása. A DHCP éhező támadás célja a kliensek összekapcsolására szolgáló DoS. A DHCP éhezési támadásokhoz olyan támadási eszközre van szükség, mint a Gobbler. DHCP-hamisítási támadás akkor következik be, amikor egy rosszindulatú DHCP-kiszolgáló csatlakozik a hálózathoz, és hamis IP-konfigurációs paramétereket ad meg a törvényes ügyfeleknek. A DHCP éhezés elleni támadások könnyen mérsékelhetők a portbiztonság használatával. A DHCP-hamisítási támadások mérsékelhetők a megbízható portokon végzett DHCP-snooping segítségével. A DHCP leskelődés a DHCP-kiéheztetési támadások mérséklésében is segít azáltal, hogy korlátozza a nem megbízható portok által fogadható DHCP-felderítési üzenetek számát. A DHCP snooping létrehoz és karbantart egy DHCP snooping kötési adatbázist, amelyet a kapcsoló használhat a nem megbízható forrásokból származó DHCP-üzenetek kiszűrésére. A DHCP leskelődés globálisan aktiválva van. A törvényes DHCP-kiszolgálókhoz csatlakozó portok ezután megbízhatóként vannak konfigurálva. Ezenkívül a nem megbízható portok konfigurálhatók a DHCP kérések sebességkorlátozására.

**Az ARP támadások mérséklése**   
Az ARP RFC szerint a kliensek ingyenes ARP kéréseket küldhetnek. Amikor az alhálózat más gazdagépei ingyenes ARP-kérést kapnak, a gazdagépek az ingyenes ARP-ben található MAC-címet és IPv4-címet tárolják az ARP-táblájukban. A támadó egy hamisított MAC-címet tartalmazó ingyenes ARP-üzenetet küldhet egy kapcsolónak, és a kapcsoló ennek megfelelően frissíti a MAC-táblázatát. Ezért bármely gazdagép bármely IP- és MAC-cím tulajdonosának vallhatja magát. Egy tipikus támadásban a fenyegetés szereplői kéretlen ARP-válaszokat küldhetnek az alhálózat más gazdagépeinek a fenyegetést okozó szereplő MAC-címével és az alapértelmezett átjáró IPv4-címével. Címhamisítási támadások akkor fordulnak elő, amikor a fenyegetés szereplői hamis IP- vagy MAC-címeket tartalmazó csomagokat hoznak létre. MAC-címhamisítási támadások akkor fordulnak elő, amikor a fenyegetés szereplői megváltoztatják gazdagépük MAC-címét, hogy megfeleljen a célállomás másik ismert MAC-címének. A meghamisított MAC-cím miatt a kapcsoló egy másik gazdagépnek szánt csomagokat küldhet a fenyegetést jelentő számítógépnek. Ez különösen akkor jelenthet problémát, ha a hamisított MAC-cím az alapértelmezett átjáróé. A DAI csökkentheti az ARP-hamisítást azáltal, hogy biztosítja, hogy csak érvényes ARP-kérések és válaszok kerüljenek a hálózatba. A DAI megköveteli, hogy a DHCP-snooping globálisan legyen konfigurálva. A DAI megbízható interfészeken és VLAN-okon konfigurálható.

**Csökkentse a címhamisítási támadásokat**   
Hamisítási támadások akkor fordulnak elő, amikor az egyik gazdagép a másiknak adja ki magát, hogy egyébként hozzáférhetetlen adatokat fogadjon, vagy hogy megkerülje a biztonsági konfigurációkat. MAC-címhamisítási támadások akkor fordulnak elő, amikor a támadók megváltoztatják gazdagépük MAC-címét, hogy megfeleljen a célállomás másik ismert MAC-címének. Amikor egy kapcsoló megkapja a hamisított kereteket, a kapcsoló felülírja az aktuális MAC-tábla bejegyzést, és hozzárendeli a MAC-címet az új porthoz. A fenyegetettséget fellépő számítógép immár képes fogadni a hamis címmel rendelkező gazdagépnek szánt forgalmat. Az IP-cím meghamisítása az, amikor egy szélhámos PC eltéríti a szomszéd érvényes IP-címét, vagy véletlenszerű IP-címet használ. Az IP-címhamisítást nehéz mérsékelni, különösen, ha olyan alhálózaton belül használják, amelyhez az IP tartozik. A MAC- és IP-címhamisítás elleni védelem érdekében konfigurálja az IPSG-t. Az IPSG úgy működik, mint a DAI, de minden csomagot megvizsgál, nem csak az ARP-csomagokat. A DAI-hoz hasonlóan az IPSG is megköveteli, hogy engedélyezve legyen a DHCP leskelődés. Minden nem megbízható porthoz konfigurálható egy forrás IP-cím vagy egy forrás IP- és MAC-címszűrő.

**Spanning Tree Protocol**   
Az STP egy hurokmegelőző hálózati protokoll, amely lehetővé teszi a redundanciát, miközben hurokmentes 2. rétegbeli topológiát hoz létre. Az STP engedélyezése nélkül a 2. rétegbeli hurkok képződhetnek, aminek következtében a broadcast, multicast és ismeretlen unicast keretek a végtelenségig hurkolhatnak. Ez nagyon rövid időn belül, néha néhány másodpercen belül tönkreteheti a hálózatot. A feszítőfa algoritmus egyetlen kapcsolót jelöl ki gyökérhídként, és azt használja referenciapontként az útvonalszámításokhoz. A feszítőfa algoritmus kiszámítja a legrövidebb utat a gyökérhídhoz, és lehetővé teszi a továbbítást a legjobb utat képező törzseken. Az alternatív portok blokkolva vannak. A kijelölt portok mind nem root portok, amelyek a fán átívelően lehetővé teszik a forgalom továbbítását. Ha egy útvonal elérhetetlenné válik, az átívelő fa lehetővé teszi az alternatív portok számára a forgalom továbbítását. A feszítőfa hídprotokoll adategységeket használ a kapcsolók közötti kommunikációhoz egy átfogó fa topológiában.

**STP támadások mérséklése**   
A fenyegetés szereplői a gyökérhíd meghamisításával és a hálózat topológiájának megváltoztatásával manipulálhatják az STP-t, hogy támadást hajtsanak végre. A támadók gyökérhídként jeleníthetik meg gazdáikat; és ezért rögzíti az azonnali váltott tartomány teljes forgalmát. A Cisco switchek számos STP stabilitási mechanizmussal rendelkeznek, mint például a PortFast, a BPDU Guard, a Root Guard és a Loop Guard. A PortFast lehetővé teszi, hogy a hozzáférési portok feszítőfa továbbítási állapotba lépjenek anélkül, hogy átmennének az átmeneti feszítőfa állapotokon. A BPDU őr azonnali hibája letiltja a BPDU-t fogadó portot. Ez a nem fővonali portokon van konfigurálva, amelyeken általában engedélyezve van a PortFast. A Root Guard megakadályozza, hogy egy nem megfelelő kapcsoló gyökérhíddá váljon. A hurokvédő megakadályozza, hogy az alternatív vagy gyökérportok kijelölt portokká váljanak olyan hiba miatt, amely egyirányú kapcsolathoz vezet.

14.10.2

## 14. modul – 2. rétegbeli biztonsági szempontok kvíz

Az űrlap teteje

1. Mi az egyetlen típusú forgalom, amelyet egy PVLAN védett port továbbít más védett portokra?

Az űrlap alja

Egy hálózati rendszergazda konfigurálja a DAI-t egy kapcsolón az **ip arp check validte src - mac** paranccsal . Mi ennek a konfigurációs parancsnak a célja?

Melyik enyhítési terv a legjobb egy olyan DoS-támadás meghiúsításához, amely MAC-címtábla túlcsordulást okoz?

Milyen hálózati támadások célja DoS létrehozása az ügyfelek számára, megakadályozva, hogy DHCP-bérletet szerezzenek?

Ha a biztonság aggodalomra ad okot, melyik OSI réteg tekinthető a hálózati rendszer leggyengébb láncszemének?

Ha két kapcsoló azonos prioritással és ugyanazzal a kiterjesztett rendszerazonosítóval van konfigurálva, mi határozza meg, hogy melyik kapcsoló lesz a gyökérhíd?

Melyik utasítás írja le egy kapcsoló viselkedését, amikor a MAC-címtábla megtelt?

Egy kiberbiztonsági elemző a macof eszközzel értékeli a szervezet gerinchálózatában telepített kapcsolók konfigurációit. Milyen típusú LAN-támadást céloz meg az elemző az értékelés során?

Mi határozza meg, hogy egy adott VLAN-hoz melyik kapcsoló lesz az STP gyökérhídja?

Milyen lépéseket tehet a hálózati rendszergazda a VLAN ugrásos támadások veszélyének mérséklése érdekében?

Melyik két Cisco-megoldás segít megelőzni a DHCP éhezési támadásokat? (Válassz kettőt.)

Mi az egyetlen típusú port, amelyre egy elszigetelt port továbbíthatja a forgalmat egy privát VLAN-on?

Milyen további biztonsági intézkedéseket kell engedélyezni az IP Source Guard mellett a címhamisítás elleni védelem érdekében?

[14.9](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Mitigate STP Attacks](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[15.0](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                  
*             

1. Cryptographic Services
2. Introduction

# Bevezetés

15.0.1

## Miért vegyem ezt a modult?

A kriptográfiai szolgáltatások a hálózatbiztonság alapvető elemei. A számítógépes hálózatokon folytatott kommunikáció nagy része valamilyen szinten titkosított. A hálózati üzeneteket gyakran kétszer vagy háromszor titkosítják, attól függően, hogy a forgalom hogyan történik. A hálózati kommunikáció egyik alapelve, hogy mindig feltételezzük, hogy üzeneteit elfogják. Emiatt mindig használjon titkosított szolgáltatásokat, amikor azok elérhetők. Sok esetben nincs más választása, mint megtenni.

15.0.2

## Mit fogok tanulni ebben a modulban?

**Modul címe:** Kriptográfiai szolgáltatások

**A modul célja** : Ismertesse meg, hogyan működnek együtt a titkosítás, a hash-ek és a digitális aláírások a titkosság, integritás és hitelesítés érdekében.

| **téma címe** | **Téma Cél** |
| --- | --- |
| **Kommunikáció biztosítása** | Magyarázza el a biztonságos kommunikáció követelményeit, beleértve az integritást, a hitelesítést és a titkosságot. |
| **Kriptográfia** | Ismertesse a kriptográfiát. |
| **Rejtjel elemzés** | Ismertesse a kriptoanalízist. |
| **Kriptológia** | Ismertesse a kriptológiát. |

15.0.3

## Lab - Kódok létrehozása

A titkos kódokat évezredek óta használják. Az ókori görögök és spártaiak szitalemet használtak (rímel Olaszországra) az üzenetek kódolására. A rómaiak Caesar-rejtjelet használtak az üzenetek titkosításához. Néhány száz évvel ezelőtt a franciák a Vigenère-rejtjelet használták az üzenetek kódolására. Manapság számos módja van az üzenetek kódolásának.

Ebben a laborban üzeneteket hozhat létre és titkosíthat online eszközök segítségével.

[14.10](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Layer 2 Security Considerations Summary](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[15.1](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Secure Communications](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                     
*             

1. Kriptográfiai szolgáltatások
2. Biztonságos kommunikáció

# Biztonságos kommunikáció

15.1.1

## Hitelesítés, integritás és bizalmasság

A biztonságos kommunikáció biztosítása érdekében mind a nyilvános, mind a magán infrastruktúrán keresztül a hálózati adminisztrátor első célja a hálózati infrastruktúra biztonsága, beleértve az útválasztókat, kapcsolókat, szervereket és gazdagépeket. Ez eszközerősítéssel, AAA hozzáférés-vezérléssel, ACL-ekkel, tűzfalakkal, a fenyegetések IPS-sel történő figyelésével, a végpontok Advanced Malware Protection (AMP) használatával, valamint az e-mail és webes biztonság érvényesítésével a Cisco Email Security Appliance (ESA) és a Cisco Web Security segítségével valósítható meg. Appliance (WSA). Az ábra egy példát mutat egy biztonságos hálózati topológiára.

Az ábra egy példát mutat egy biztonságos hálózati infrastruktúrára. az avpn összeköti a fő webhelyet a távoli ággal. tűzfal csatlakozik a belső és a külső hálózat között. Az esa / wsa és az ips technológiákat használják a hálózaton lévő gazdagépek védelmére.

Remote Branch Firewall IPS Web Server Email Server DNS Server VPN ESA/WSA VPN

A következő cél az adatok biztonságossá tétele a különböző hivatkozásokon keresztül. Ez magában foglalhatja a belső forgalmat is, de nagyobb aggodalomra ad okot a szervezeten kívülre a fióktelepekre, a távmunkahelyekre és a partneroldalakra továbbított adatok védelme.

A kommunikáció biztonságának három fő célja van:

* **Hitelesítés** – Ez garantálja, hogy az üzenet nem hamis, és valóban a hiteles forrásból származik. A modern hálózatok a hash üzenet hitelesítési kóddal (HMAC) biztosítják a hitelesítést.
* **Integritás** – Ez garantálja, hogy senki nem fogta el az üzenetet és nem változtatta meg; hasonló a keretben lévő ellenőrző összeg függvényhez. Ezt az SHA-2 vagy SHA-3 hash-generáló algoritmuscsalád megvalósítása biztosítja.
* **Titoktartás** – Ez garantálja, hogy ha az üzenetet rögzítik, azt nem lehet megfejteni. Ezt szimmetrikus vagy aszimmetrikus titkosítási algoritmusokkal biztosítják.

**Megjegyzés:** Ezek az elsődleges célok hasonlóak, de nem azonosak a számítógépes hálózat biztosításának és karbantartásának három fő kérdésével, amelyek a titkosság, az integritás és a rendelkezésre állás.

A legnépszerűbb szimmetrikus titkosítási algoritmus az Advanced Encryption Standard (AES). A szimmetrikus titkosítási algoritmusok azon a feltevésen alapulnak, hogy minden kommunikáló fél ismeri az előre megosztott kulcsot.

Az adatok bizalmas kezelése aszimmetrikus algoritmusokkal is biztosítható, beleértve a Rivest, Shamir és Adleman (RSA) és a nyilvános kulcsú infrastruktúrát (PKI). Az aszimmetrikus titkosítási algoritmusok azon a feltételezésen alapulnak, hogy a két kommunikáló fél korábban nem osztott meg titkot, és ehhez biztonságos módszert kell létrehoznia.

15.1.2

## Hitelesítés

Két elsődleges módszer létezik a forrás érvényesítésére a hálózati kommunikációban: hitelesítési szolgáltatások és adatleutasítási szolgáltatások.

A hitelesítés garantálja, hogy az üzenet attól a forrástól származik, amelyről azt állítja, hogy származik. A hitelesítés hasonló a biztonságos személyi azonosító szám (PIN) megadásához az ATM-nél történő bankoláshoz, amint az az ábrán látható. A PIN kódot csak a felhasználó és a pénzintézet ismerheti. A PIN egy közös titok, amely segít megvédeni a hamisításokat.

### Az ATM hitelesítési PIN-kód megadása



A hálózati kommunikációban a hitelesítés kriptográfiai módszerekkel valósítható meg. Ez különösen fontos olyan alkalmazások vagy protokollok esetében, mint például az e-mail vagy az IP, amelyek nem rendelkeznek beépített mechanizmussal a forrás meghamisításának megakadályozására.

Az adatok visszautasítása egy hasonló szolgáltatás, amely lehetővé teszi az üzenet küldőjének egyedi azonosítását. A visszautasítás nélküli szolgáltatások mellett a feladó nem tagadhatja, hogy ő volt az üzenet forrása. Úgy tűnhet, hogy a hitelesítési szolgáltatás és a visszautasítási szolgáltatás ugyanazt a funkciót tölti be. Bár mindkettő a feladó bizonyított személyazonosságának kérdésével foglalkozik, van különbség a kettő között.

A letagadhatatlanság legfontosabb része az, hogy az eszköz nem tudja megtagadni vagy cáfolni az elküldött üzenet érvényességét. A letagadhatatlanság azon a tényen alapul, hogy csak a feladó rendelkezik az üzenet kezelésének egyedi jellemzőivel vagy aláírásával. Még a fogadó eszköz sem tudhatja, hogy a küldő hogyan kezelte ezt az üzenetet a hitelesség bizonyítása érdekében, mert a fogadó ekkor úgy teheti, mintha ő lenne a forrás.

Ha a fő gond az, hogy a fogadó eszköz ellenőrizze a forrást, és nincs aggodalom a forrást utánzó fogadó eszköz miatt, akkor nem számít, hogy a küldő és a fogadó is tudja-e, hogyan kell kezelni az üzenetet a hitelesség biztosítása érdekében. A hitelesség és a tagadhatatlanság egy példája az azonos vállalat két számítógépe közötti adatcsere, szemben az ügyfél és egy e-kereskedelmi webhely közötti adatcsere. A szervezeten belül adatot cserélő két számítógépnek nem kell bizonyítania a másiknak, hogy melyikük küldött üzenetet.

Ez a gyakorlat nem fogadható el üzleti alkalmazásokban, például termékek online vásárlásakor. Ha az online áruház tudja, hogyan jött létre a hitelesség bizonyítására vevő üzenet, akkor könnyen meghamisíthatja a „hiteles” rendeléseket. Ebben az esetben a feladónak kell az egyetlen félnek lennie, aki ismeri az üzenet létrehozásának módját. A webáruház bizonyíthatja másoknak, hogy a megrendelést valóban a vásárló küldte, és a vásárló nem hivatkozhat a megrendelés érvénytelenségére.

15.1.3

## Adatintegritás

Az adatok integritása biztosítja, hogy az üzenetek továbbítása során ne változzanak. Az adatok integritásával a fogadó ellenőrizheti, hogy a fogadott üzenet megegyezik-e az elküldött üzenettel, és nem történt-e manipuláció.

Az európai nemesség az ábrán látható módon a boríték lezárására szolgáló viaszpecsét létrehozásával biztosította az iratok adatsértetlenségét. A pecsétet gyakran pecsétgyűrűvel hozták létre. Ezeken a pecsétgyűrű tulajdonosának családi címere, kezdőbetűi, portréja vagy személyes jelképe vagy mottója volt látható. A borítékon lévő sértetlen pecsét garantálta a boríték tartalmának sértetlenségét. Az egyedi pecsétgyűrű lenyomata alapján a hitelességet is garantálta.

### Viaszpecsét, amely biztosítja az integritást



15.1.4

## Adatok bizalmas kezelése

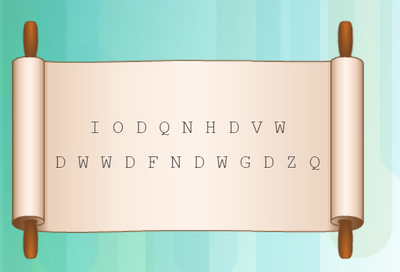
Az adatok bizalmas kezelése biztosítja a magánélet védelmét, így csak a címzett olvashatja el az üzenetet. Ez titkosítással érhető el. A titkosítás az adatok titkosításának folyamata, hogy azokat illetéktelen felek ne tudják könnyen elolvasni.

A titkosítás engedélyezésekor az olvasható adatokat egyszerű szövegnek vagy egyértelmű szövegnek, míg a titkosított változatot titkosított szövegnek vagy titkosított szövegnek nevezzük. Ebben a kurzusban a titkosított szöveg kifejezést fogjuk használni. Az egyszerű szövegben olvasható üzenetet titkosított szöveggé alakítják, amely az olvashatatlan, álcázott üzenet. A visszafejtés megfordítja a folyamatot. Az üzenet titkosításához és visszafejtéséhez kulcsra van szükség. A kulcs az egyszerű szöveg és a titkosított szöveg közötti kapcsolat.

A történelem során különféle titkosítási algoritmusokat és módszereket használtak. Azt mondják, Julius Caesar úgy biztosította az üzeneteket, hogy két ábécét rakott egymás mellé, majd az egyiket meghatározott számú hellyel eltolja. A műszakban a helyek száma a kulcs. A nyílt szöveget ezzel a kulccsal alakította át titkosított szöveggé, és csak a tábornokai tudták megfejteni az üzeneteket, akiknél a kulcs is volt. Ezt a módszert ma Caesar-rejtjelnek nevezik. Az ábrán egy Caesar-rejtjelet használó kódolt üzenet látható.

Az ábrán egy tekercs ábrázolása látható, rajta egy kódolt caesar-rejtjellel

### Kódolt Caesar titkosított üzenet



A hash függvény használata egy másik módja az adatok bizalmas kezelésének. A hash függvény egy karakterláncot általában rövidebb, rögzített hosszúságú értékké vagy kulccsá alakít át, amely az eredeti karakterláncot képviseli. A kivonatolás és a titkosítás közötti különbség az adatok tárolási módjában van. Titkosított szöveg esetén az adatok egy kulccsal visszafejthetők. A hash funkcióval az adatok bevitele és a hash funkcióval való konvertálása után a sima szöveg eltűnik. A kivonatolt adatok egyszerűen összehasonlításra szolgálnak. Például amikor a felhasználó beír egy jelszót, a jelszó kivonatolásra kerül, majd összehasonlításra kerül a tárolt kivonatolt értékkel. Ha a felhasználó elfelejti a jelszót, a tárolt érték visszafejtése lehetetlen, és a jelszót vissza kell állítani.

A titkosítás és a kivonatolás célja a titkosság garantálása, hogy csak az arra jogosult személyek tudják elolvasni az üzenetet

15.1.5

## Ellenőrizze, hogy megértette-e a biztonságos kommunikáció célját

Az űrlap teteje

Ellenőrizze, hogy megértette-e a bizalmasságot, az integritást és a hitelesítést azáltal, hogy azonosítja mindegyik jellemzőit.

1. Biztosítja a magánélet védelmét, hogy csak a címzett tudja elolvasni az üzenetet.

Az űrlap alja

Biztosítja, hogy az üzenetek továbbítása során ne változzanak.

Garantálja, hogy az üzenet abból a forrásból származik, amelyről azt állítja, hogy származik.

A banki szolgáltatásokban ez úgy érhető el, hogy az ATM-nél biztonságos személyazonosító számot (PIN) igényel.

A titkosítás és a kivonatolás biztosítja, hogy csak az arra jogosult entitások olvassák el az üzenetet.

Az üzenet titkosításához és visszafejtéséhez kulcsra van szükség.

A fogadó ellenőrizheti, hogy a fogadott üzenet azonos-e az elküldött üzenettel, és nem történt-e manipuláció.

[15.0](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[15.2](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Cryptography](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                        
*             

1. Kriptográfiai szolgáltatások
2. Cryptography

# Kriptográfia

15.2.1

## Rejtjelezett szöveg létrehozása

A kriptográfia története több ezer évvel ezelőtt diplomáciai körökben kezdődik. Egy király udvarának hírnökei titkosított üzeneteket vittek el más udvarokba. Alkalmanként más bíróságok, amelyek nem vettek részt a kommunikációban, megpróbálták ellopni az általuk ellenfélnek tekintett királyságnak küldött üzeneteket. Nem sokkal később a katonai parancsnokok titkosítást kezdtek használni az üzenetek védelmére.

Kattintson az alábbiakra, ha többet szeretne megtudni a rejtjelekről és a rejtjelező eszközökről.



A scytale egy olyan eszköz, amelyet transzponáló rejtjel generálására használnak. Egy ismert átmérőjű rúd köré egy papírcsíkot vagy más anyagot tekernek az ábrán látható módon. Az üzenetet a papírra írják sorok között. A csík eltávolítása után az üzenet addig olvashatatlan, amíg egy másik, azonos átmérőjű rúd köré nem tekerjük.

15.2.2

## Transzpozíciós titkosítások

Az átültetési titkosításokban nem cserélnek betűket; egyszerűen átrendeződnek. Az ilyen típusú titkosításra példa a FLANK EAST ATTACK AT DAWN üzenet, és átültetve az NWAD TA KCATTA TSAE KNALF olvasására. Ebben a példában a kulcs a betűk megfordítása.

Az átültetési titkosítás egy másik példája a vasúti kerítés titkosítása. Ebben az átültetésben a szavak úgy vannak kiírva, mintha vasúti kerítés lenne. Elhelyezkednek, hol elöl, hol középen, hol hátul, több párhuzamos vonalon át.

A modern titkosítási blokk titkosítási algoritmusok, mint például az AES és az örökölt 3DES, még mindig az átültetést használják az algoritmus részeként.

Kattintson az alábbiakra, ha többet szeretne megtudni az egyszerű transzponálási titkosítás használatáról.

Az ábra egy egyszerű szöveges üzenet példája.

FLANK KELET

TÁMADÁS HAJNALBAN

Az egyszerű szöveges üzenet 3-as kulccsal lesz kódolva. Ez a kulcsérték azt határozza meg, hogy három sorra van szükség a titkosított kód létrehozásához.

15.2.3

## Helyettesítő rejtjelek

A helyettesítő titkosítások az egyik betűt egy másikkal helyettesítik. A legegyszerűbb formájukban a helyettesítő titkosítások megtartják az eredeti üzenet betűgyakoriságát.

A Caesar-rejtjel egyszerű helyettesítő rejtjel volt.

Mivel az egész üzenet ugyanazon az egyetlen kulcsváltáson alapult, a Caesar-rejtjelet monoalfabetikus helyettesítő rejtjelnek nevezik. Meglehetősen könnyű feltörni is. Emiatt találták fel a többalfabetikus rejtjeleket, például a Vigenère-rejtjelet. A módszert eredetileg Giovan Battista Bellaso írta le 1553-ban, de a sémát később tévesen a francia diplomatának és kriptográfusnak, Blaise de Vigenère-nek tulajdonították.

Kattintson az alábbiakra, ha többet szeretne megtudni a helyettesítő titkosításokról.

Az ábra egy egyszerű szöveges üzenet példáját mutatja.

OLDAL-KELETI TÁMADÁS HAJNALBAN

Az egyszerű szöveges üzenet 3-as kulccsal lesz kódolva.

15.2.4

## Egy összetettebb helyettesítő titkosítás

A Vigenère-rejtjel a Caesar-rejtjelen alapul, azzal a különbséggel, hogy a szöveget úgy titkosítja, hogy minden egyszerű szöveges betűhöz eltérő többalfabetikus kulcseltolódást használ. A különböző kulcseltolódást a küldő és a fogadó közötti megosztott kulcs segítségével azonosítják. Az egyszerű szöveges üzenet az ábrán látható Vigenère titkosítási táblázat segítségével titkosítható és visszafejthető.

Az ábrán egy Vigenère-tábla nevű táblázat látható.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **a** | **b** | **c** | **d** | **Ez** | **f** | **g** | **h** | **én** | **j** | **k** | **l** | **m** | **n** | **O** | **p** | **q** | **r** | **s** | **t** | **ban ben** | **ban ben** | **Ban ben** | **x** | **és** | **Val vel** |
| **A** | a | b | c | d | Ez | f | g | h | én | j | k | l | m | n | O | p | q | r | s | t | ban ben | ban ben | Ban ben | x | és | Val vel |
| **B** | b | c | d | Ez | f | g | h | én | j | k | l | m | n | O | p | q | r | s | t | ban ben | ban ben | Ban ben | x | és | Val vel | a |
| **C** | c | d | Ez | f | g | h | én | j | k | l | m | n | O | p | q | r | s | t | ban ben | ban ben | Ban ben | x | és | Val vel | a | b |
| **D** | d | Ez | f | g | h | én | j | k | l | m | n | O | p | q | r | s | t | ban ben | ban ben | Ban ben | x | és | Val vel | a | b | c |
| **ÉS** | Ez | f | g | h | én | j | k | l | m | n | O | p | q | r | s | t | ban ben | ban ben | Ban ben | x | és | Val vel | a | b | c | d |
| **F** | f | g | h | én | j | k | l | m | n | O | p | q | r | s | t | ban ben | ban ben | Ban ben | x | és | Val vel | a | b | c | d | Ez |
| **G** | g | h | én | j | k | l | m | n | O | p | q | r | s | t | ban ben | ban ben | Ban ben | x | és | Val vel | a | b | c | d | Ez | f |
| **H** | h | én | j | k | l | m | n | O | p | q | r | s | t | ban ben | ban ben | Ban ben | x | és | Val vel | a | b | c | d | Ez | f | g |
| **én** | én | j | k | l | m | n | O | p | q | r | s | t | ban ben | ban ben | Ban ben | x | és | Val vel | a | b | c | d | Ez | f | g | h |
| **J** | j | k | l | m | n | O | p | q | r | s | t | ban ben | ban ben | Ban ben | x | és | Val vel | a | b | c | d | Ez | f | g | h | én |
| **K** | k | l | m | n | O | p | q | r | s | t | ban ben | ban ben | Ban ben | x | és | Val vel | a | b | c | d | Ez | f | g | h | én | j |
| **L** | l | m | n | O | p | q | r | s | t | ban ben | ban ben | Ban ben | x | és | Val vel | a | b | c | d | Ez | f | g | h | én | j | k |
| **M** | m | n | O | p | q | r | s | t | ban ben | ban ben | Ban ben | x | és | Val vel | a | b | c | d | Ez | f | g | h | én | j | k | l |
| **N** | n | O | p | q | r | s | t | ban ben | ban ben | Ban ben | x | és | Val vel | a | b | c | d | Ez | f | g | h | én | j | k | l | m |
| **O** | O | p | q | r | s | t | ban ben | ban ben | Ban ben | x | és | Val vel | a | b | c | d | Ez | f | g | h | én | j | k | l | m | n |
| **P** | p | q | r | s | t | ban ben | ban ben | Ban ben | x | és | Val vel | a | b | c | d | Ez | f | g | h | én | j | k | l | m | n | O |
| **K** | q | r | s | t | ban ben | ban ben | Ban ben | x | és | Val vel | a | b | c | d | Ez | f | g | h | én | j | k | l | m | n | O | p |
| **R** | r | s | t | ban ben | ban ben | Ban ben | x | és | Val vel | a | b | c | d | Ez | f | g | h | én | j | k | l | m | n | O | p | q |
| **S** | s | t | ban ben | ban ben | Ban ben | x | és | Val vel | a | b | c | d | Ez | f | g | h | én | j | k | l | m | n | O | p | q | r |
| **T** | t | ban ben | ban ben | Ban ben | x | és | Val vel | a | b | c | d | Ez | f | g | h | én | j | k | l | m | n | O | p | q | r | s |
| **BAN BEN** | ban ben | ban ben | Ban ben | x | és | Val vel | a | b | c | d | Ez | f | g | h | én | j | k | l | m | n | O | p | q | r | s | t |
| **BAN BEN** | ban ben | Ban ben | x | és | Val vel | a | b | c | d | Ez | f | g | h | én | j | k | l | m | n | O | p | q | r | s | t | ban ben |
| **BAN BEN** | Ban ben | x | és | Val vel | a | b | c | d | Ez | f | g | h | én | j | k | l | m | n | O | p | q | r | s | t | ban ben | ban ben |
| **x** | x | és | Val vel | a | b | c | d | Ez | f | g | h | én | j | k | l | m | n | O | p | q | r | s | t | ban ben | ban ben | Ban ben |
| **ÉS** | és | Val vel | a | b | c | d | Ez | f | g | h | én | j | k | l | m | n | O | p | q | r | s | t | ban ben | ban ben | Ban ben | x |
| **VAL VEL** | Val vel | a | b | c | d | Ez | f | g | h | én | j | k | l | m | n | O | p | q | r | s | t | ban ben | ban ben | Ban ben | x | és |

A Vigenère titkosítási táblázat működésének szemléltetésére tegyük fel, hogy a feladónak és a fogadónak van egy közös titkos kulcsa, amely ezekből a betűkből áll: SECRETKEY. A feladó ezt a titkos kulcsot használja az egyszerű szövegű FLANK EAST ATTACK AT DAWN kódolásához:

* Az F ( **F** LANK) kódolása az F oszlop és az S betűvel kezdődő sor metszéspontjának ( **S** ECRETKEY) alapján történik, ami az X rejtjelbetűt eredményezi.
* Az L (F **L** ANK) kódolása úgy történik, hogy az L oszlop és az E-vel kezdődő sor metszéspontját nézzük (S **E** CRETKEY), ami a P titkosítási betűt eredményezi.
* Az A (FL **A** NK) kódolása úgy történik, hogy az A oszlop és a C-vel kezdődő sor metszéspontját nézzük (SE **C** RETKEY), ami a C titkosító betűt eredményezi.
* Az N (FLA **N** K) kódolása az N oszlop és az R betűvel kezdődő sor metszéspontja alapján történik (SEC **R** ETKEY), ami az E rejtjelező betűt eredményezi.
* A K (FLAN **K** ) kódolása úgy történik, hogy a K oszlop és az E-vel kezdődő sor metszéspontját nézzük (SECR **E** TKEY), ami az O titkosító betűt eredményezi.

A folyamat addig folytatódik, amíg a teljes FLANK EAST ATTACK AT DAWN szöveges üzenetet nem titkosítják. A folyamat megfordítható is. metszéspontját **Például az F továbbra is az X rejtjelbetű, ha az F sor ( F** LANK) és az S-vel kezdődő oszlop **( S** ECRETKEY) nézve kódoljuk.

A Vigenère titkosítás használatakor, ha az üzenet hosszabb, mint a kulcs, a kulcs megismétlődik. Például a SECRETKEYSECRETKEYSEC szükséges a FLANK EAST ATTACK AT DAWN kódolásához:

* **Titkos kulcs** : SECRETKEYSECRETKEYSEC
* **Egyszerű szöveg:** FLANKEASTATTACKATDAWN
* **Titkosított szöveg:** XPCEOXKURSXVRGDKXBSAP

Bár a Vigenère titkosítás hosszabb kulcsot használ, még mindig feltörhető. Emiatt jobb titkosítási módszerre volt szükség.

15.2.5

## Egyszeri Pad Rejtjelek

Gilbert Vernam az AT&T Bell Labs mérnöke volt, aki 1917-ben feltalálta, majd szabadalmaztatta az adatfolyam titkosítót. Az egyszer használatos pad rejtjelét is ő találta fel. Vernam egy teletípus-rejtjelet javasolt, amelyben egy tetszőlegesen hosszú, nem ismétlődő számsorozatból álló, előkészített kulcsot papírszalagon tartanak, az ábrán látható módon. Ezután karakterenként kombinálták az egyszerű szöveges üzenettel, hogy létrehozzák a titkosított szöveget.

### Példa egyszeri pad-eszközre



A rejtjelezett szöveg megfejtéséhez ugyanazt a papírszalag-billentyűt ismét karakterenként kombinálták, létrehozva az egyszerű szöveget. Mindegyik szalagot csak egyszer használták fel; innen az egyszeri betét név. Mindaddig, amíg a kulcsszalag nem ismétlődik, vagy nem használják fel újra, az ilyen típusú titkosítás immunis a kriptoanalitikus támadásokkal szemben. Ennek az az oka, hogy a rendelkezésre álló rejtjelezett szöveg nem jeleníti meg a kulcs mintáját.

Az egyszer használatos betétek valós világban való használata számos nehézséggel jár. Az egyik nehézség a véletlenszerű adatok létrehozásának kihívása. A számítógépek, mivel rendelkeznek matematikai alappal, nem képesek valódi véletlenszerű adatokat létrehozni. Ezenkívül, ha a kulcsot többször használják, könnyen eltörheti. Az RC4 egy példa erre a típusú titkosításra, amelyet széles körben használnak az interneten. Ismétlem, mivel a kulcsot egy számítógép generálja, ez nem igazán véletlen. Ezeken a problémákon kívül a kulcsok elosztása is kihívást jelent az ilyen típusú titkosítással.

[15.1](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Secure Communications](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[15.3](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Cryptanalysis](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                          
*             

1. Kriptográfiai szolgáltatások
2. Cryptanalysis

# Rejtjel elemzés

15.3.1

## Feltörő kód

Amióta létezik kriptográfia, addig létezik kriptoanalízis is. A kriptoanalízis a titkosított információ jelentésének meghatározásának gyakorlata és tanulmányozása (a kód feltörése), a megosztott titkos kulcshoz való hozzáférés nélkül. Ezt kódtörésnek is nevezik.

A történelem során számos példa volt a kriptoanalízisre:

* A Vigenère-rejtjel teljesen biztonságos volt egészen addig, amíg a 19. században Charles Babbage angol kriptográfus fel nem törte.
* Mária, a skót királynő I. Erzsébet királynő leverését tervezte a trónról, és titkosított üzeneteket küldött összeesküvőtársainak. Az ebben a cselekményben használt kód feltörése Mária lefejezéséhez vezetett 1587-ben.
* Az Enigma-titkosított kommunikációt a németek használták tengeralattjáró hajóik navigálására és irányítására az Atlanti-óceánon. Lengyel és brit kriptoanalitikusok feltörték a német Enigma kódot. Winston Churchill azon a véleményen volt, hogy ez fordulópont volt a második világháborúban.

15.3.2

## A kód feltörésének módszerei

A kriptoanalízisben számos módszert alkalmaznak:

* **Brute-force módszer** – A támadó minden lehetséges kulcsot kipróbál, tudván, hogy végül az egyik működni fog.
* **Titkosított szöveges módszer** – A támadó több titkosított üzenet titkosított szövegével rendelkezik, de nem ismeri a mögöttes egyszerű szöveget.
* **Ismert egyszerű szöveges módszer** – A támadó több üzenet titkosított szövegéhez fér hozzá, és tud valamit a titkosított szöveg mögött meghúzódó egyszerű szövegről.
* **Választott egyszerű szöveges módszer** – A támadó kiválasztja, hogy a titkosítóeszköz mely adatokat titkosítsa, és megfigyeli a titkosított szöveg kimenetét.
* **Választott titkosított szöveg módszer** – A támadó választhat különböző titkosított szöveget a visszafejtéshez, és hozzáfér a visszafejtett egyszerű szöveghez.
* **Meet-in-the-Middle módszer** – A támadó ismeri a nyílt szöveg egy részét és a megfelelő titkosított szöveget.

**Megjegyzés:** A módszerek megvalósításának részletei túlmutatnak ennek a kurzusnak a keretein.

A legegyszerűbb megértési módszer a brute-force módszer. Például, ha egy tolvaj megpróbálna ellopni egy, az ábrán látható kombinációs zárral rögzített kerékpárt, akkor maximum 10 000 különböző lehetőséggel (0000-től 9999-ig) kell próbálkoznia. Minden titkosítási algoritmus ki van téve ennek a támadásnak. A brute-force támadás átlagosan a kulcstérben, amely az összes lehetséges kulcs halmaza, körülbelül 50 százalékban sikerül.

A modern kriptográfusok célja, hogy elég nagy kulcstérrel rendelkezzenek ahhoz, hogy túl sok időt és pénzt igényeljen egy brute force támadás végrehajtása.

15.3.3

## Példa a feltörő kódra

A kriptográfiai módszer kiválasztásakor vegye figyelembe a Caesar titkosított kódot. A kód feltörésének legjobb módja a nyers erő alkalmazása. Mivel csak 25 lehetséges elforgatás van, viszonylag kicsi az erőfeszítés, hogy az összes lehetséges forgatást kipróbáljuk, és megnézzük, melyik ad vissza valamit, aminek van értelme.

Tudományosabb megközelítés az a tény, hogy az angol ábécé egyes karaktereit gyakrabban használják, mint másokat. Ezt a módszert frekvenciaelemzésnek nevezik. Például az alábbi ábrán látható grafikon az angol nyelvű betűk gyakoriságát mutatja. Az E, T és A betűk a legnépszerűbbek az angol nyelvben. A J, Q, X és Z betűk a legkevésbé népszerűek. Ennek a mintának a megértése segíthet felderíteni, hogy valószínűleg mely betűk szerepelnek a titkosított üzenetben.

Az ábra egy grafikon, amely felvázolja a betűk gyakoriságát az angol nyelvben.

### Az angol ábécé gyakorisági elemzése

14.00% 12.00% 10.00% 8.00% 6.00% 4.00% 2.00% 0.00% A B C D E F G H I J K L M N O P Q R S T U V W X Y

Z

A grafikon felvázolja az angol nyelvű betűk gyakoriságát.

Például az E, T és A betűk a legnépszerűbbek.

Az ábrán látható IODQN HDVW DWWDFN DW GDZQ Caesar-rejtjelezett üzenetben a D titkosítási betű hatszor, míg a W titkosítási betű négyszer jelenik meg. Nagy a valószínűsége annak, hogy a rejtjel D és W betűi vagy az E, T vagy A egyszerű szöveget jelölik. Ebben az esetben a D az A betűt, a W pedig a T betűt jelöli.

A támadónak először csak a titkosított D betűt kell lecserélnie népszerű egyszerű szöveges betűkre, beleértve az E, T és végül A betűket. Az A kipróbálása felfedné a 3-as eltolási mintát, és a támadó megfejtheti a teljes üzenetet.

Az ábra egy példát mutat egy üzenet megfejtésére a betűgyakoriság-elemzés segítségével.

IO D QN H D V W   
D WW D FN D W G D ZQ

**Rejtjelezett szöveg**

Ebben a titkosított üzenetben 6 alkalommal fordul elő a rejtjel D betűje és 4 alkalommal a W titkosítási betű.

15.3.4

## Ellenőrizze, hogy megértette-e a kódot

Ebben a tevékenységben az alábbi táblázatok segítségével keresheti meg a különböző szavak titkosított értékeit. Az utolsó kérdésben a titkosított szöveget dekódolja, hogy felfedje az egyértelmű szöveget. Az egyértelmű szöveg a felső sorban, a kódolt szövegértékek pedig az alsó sorban találhatók.

Az 1. diagram 26 oszlopból és két sorból álló táblázat. A felső sorban az a betűvel kezdődő angol ábécé látható. Az alsó sor szintén az angol ábécé, de w betűvel kezdődik, és a z betű után ismét a betűvel kezdődik.

### 1. diagram

W X Y Z A B C D E F G H I J K L M N O P Q R S T U V A B C D E F G H I J K L M N O P Q R S T U V W X Y

Z

A 2. diagram 26 oszlopból és két sorból álló táblázat. A felső sorban az a betűvel kezdődő angol ábécé látható. Az alsó sor szintén az angol ábécé, de az u betűvel kezdődik, és a z betű után ismét a betűvel kezdődik.

### 2. diagram

W X Y Z A B C D E F G H I J K L M N O P Q R S T U V A B C D E F G H I J K L M N O P Q R S T U V W X Y

Z

Az 1. diagram 26 oszlopból és két sorból álló táblázat. A felső sorban az a betűvel kezdődő angol ábécé látható. Az alsó sor szintén az angol ábécé, de a z betűvel kezdődik, és az a betűvel megfordítva folytatódik.

### 3. diagram

W X Y Z A B C D E F G H I J K L M N O P Q R S T U V V U T S R Q P O N M L K J I H G F E D C B A Z Y X

W

Az űrlap teteje

Gyakorolja a szöveg kódolását és dekódolását az alábbi feladatok végrehajtásával.

1. Lásd az 1. táblázatot. Mi a titkosított szöveg a TITKOSÍTÁS kifejezéshez?

Az űrlap alja

Lásd a 2. táblázatot. Mi az AUTHENCITY szó titkosított szövege?

Lásd a 3. táblázatot. Mi az INTEGRITY szó titkosított értéke?

Lásd a 3. táblázatot. Mi az FMVMXIBKGVW titkosított szöveg egyszerű szöveges értéke?

[15.2](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Cryptography](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[15.4](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Cryptology](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                             
*             

1. Kriptográfiai szolgáltatások
2. Cryptology

# Kriptológia

15.4.1

## Titkos kódok készítése és feltörése

Az ábra azt mutatja, hogy a kriptográfia plusz kriptoanalízis = kriptológia.

### Kriptológia = kriptográfia + kriptoanalízis

+

Kriptográfia Kriptanalízis Kriptológia

A kriptológia a titkos kódok készítésének és feltörésének tudománya. Amint az ábrán látható, a kriptológia két külön tudományágat egyesít:

* **Kriptográfia** – kódok fejlesztése és használata
* **Kriptanalízis** – ezeknek a kódoknak a feltörése

A két tudományág között szimbiotikus kapcsolat van, mert mindegyik erősíti a másikat. A nemzetbiztonsági szervezetek mindkét tudományág gyakorlóit alkalmazzák, és egymás ellen dolgoznak.

Előfordult már, hogy az egyik tudományág megelőzte a másikat. Például a Franciaország és Anglia közötti százéves háború alatt a kriptográfiai elemzők vezették a kriptográfusokat. Franciaország tévesen azt hitte, hogy a Vigenère-rejtjel törhetetlen, majd a britek feltörték. Egyes történészek úgy vélik, hogy a titkosított kódok és üzenetek sikeres feltörése nagy hatással volt a második világháború kimenetelére. Jelenleg úgy vélik, hogy a kriptográfusok állnak az élen.

15.4.2

## Kriptanalitikusok

A kriptoanalízist gyakran használják a kormányok katonai és diplomáciai megfigyelés során, a vállalatok a biztonsági eljárások erősségének tesztelésére, a rosszindulatú hackerek pedig a webhelyek gyenge pontjainak kihasználására.

A kriptanalitikusok olyan személyek, akik titkos kódok feltörésére kriptoanalízist végeznek. A munkakör leírásának mintája az ábrán látható.

Míg a kriptoanalízis gyakran huncut célokhoz kapcsolódik, valójában szükségszerű. A kriptográfia ironikus ténye, hogy lehetetlen bizonyítani, hogy bármely algoritmus biztonságos. Csak azt lehet bizonyítani, hogy nem sebezhető az ismert kriptoanalitikus támadásokkal szemben. Ezért szükség van matematikusokra, tudósokra és biztonsági igazságügyi szakértőkre, hogy továbbra is megpróbálják feltörni a titkosítási módszereket.



15.4.3

## A titok a kulcsokban van

A kommunikáció és a hálózatépítés világában a hitelesítés, az integritás és az adatok bizalmas kezelése sokféle módon valósul meg különféle protokollok és algoritmusok segítségével. A protokoll és az algoritmus kiválasztása a hálózati biztonsági szabályzat céljainak eléréséhez szükséges biztonsági szinttől függően változik.

Például az üzenet integritása érdekében az üzenet-kivonat 5 (MD5) gyorsabb, mint a Secure Hash Algorithm 2 (SHA2). Azonban az MD5, de ma már nem biztonságos. A bizalmas kezelés az örökölt 3DES vagy a biztonságosabb AES használatával valósítható meg. A választás itt is a hálózati biztonsági szabályzat dokumentumában meghatározott biztonsági követelményektől függ. További szempontok az adatok titkosításához és visszafejtéséhez szükséges számítási teljesítmény, valamint a protokoll elfogadása a biztonsági közösségben. A táblázat felsorol néhány gyakori kriptográfiai hash-t, protokollt és algoritmust.

| **Sértetlenség** | **Hitelesség** | **Titoktartás** |
| --- | --- | --- |
| MD5 (örökölt) | HMAC-MD5 (örökölt) | 3DES (örökölt) |
| ITAL | HMAC-SHA-256 | AES |
|  | RSA és DSA |  |

A régi titkosítási algoritmusok, mint például a Caesar-rejtjel vagy az Enigma-gép, az algoritmus titkosságán alapultak a titkosság elérése érdekében. A modern technológiában, ahol a visszafejtés gyakran egyszerű, gyakran használnak nyilvános domain algoritmusokat. A legtöbb modern algoritmussal a sikeres visszafejtéshez a megfelelő kriptográfiai kulcsok ismerete szükséges. Ez azt jelenti, hogy a titkosítás biztonsága a kulcsok titkosságában rejlik, nem az algoritmusban.

15.4.4

## Ellenőrizze, hogy megértette – Kriptológiai terminológia

Az űrlap teteje

Ellenőrizze, hogy megértette-e a kriptográfiai terminológiát, és válassza ki a megfelelő választ a következő kérdésekre.

1. Mi az a rejtjel, amely az egyik betűt a másikra cseréli, esetleg megtartja az eredeti üzenet betűgyakoriságát?

Az űrlap alja

Mi az a kriptográfiai elemzési módszer, amelyben a támadó minden lehetséges kulcsot kipróbál, tudván, hogy végül az egyik működni fog?

Milyen titkosítási módszert használ a 3DES az algoritmus részeként?

Mi az a kifejezés, amikor egy eszköz nem tudja cáfolni a kapott üzenet érvényességét?

Mi a gyakorlat és a tanulmányozás a titkosított információ jelentésének meghatározásában a megosztott titkos kulcshoz való hozzáférés nélkül?

15.4.5

## Lab – Fedezze fel a titkosítási módszereket

Ebben a laborban a következő célokat kell teljesítenie:

* 1. rész: Előre titkosított üzenet megfejtése a Vigenère titkosítással.
* 2. rész: Hozzon létre egy Vigenère titkosítással titkosított üzenetet, és fejtse vissza.

[15.3](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Cryptanalysis](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[15.5](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Cryptographic Services Summary](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                          

1. Kriptográfiai szolgáltatások
2. Cryptographic Services Summary

# A kriptográfiai szolgáltatások összefoglalója

15.5.1

## Mit tanultam ebben a modulban?

**Kommunikáció biztosítása**   
Amellett, hogy a hálózat és a hálózati eszközök biztonságosak és védve vannak a támadásoktól, a hálózatbiztonsági személyzet gondoskodik az adatok védelméről is az átvitel során. A kommunikáció biztonságának három fő célja:

* **Hitelesítés** – Ez garantálja, hogy az üzenet nem hamis, és valóban a hiteles forrásból származik.
* **Integritás** – Ez garantálja, hogy senki nem fogta el az üzenetet és nem változtatta meg; hasonló a keretben lévő ellenőrző összeg függvényhez.
* **Titoktartás** – Ez garantálja, hogy ha az üzenetet rögzítik, azt nem lehet megfejteni.

A hitelesítést a HMAC biztosíthatja. Az integritást az örökölt MD5 vagy az SHA hash-generáló algoritmuscsalád biztonságos tagjainak használata biztosítja. Az adatok titkosságát szimmetrikus titkosítási algoritmusok biztosítják, beleértve az örökölt 3DES-t és AES-t. A szimmetrikus titkosítási algoritmusok azon az előfeltevésen alapulnak, hogy a kommunikáló fél mindkét fél ismer egy előre megosztott kulcsot. Az aszimmetrikus algoritmusok, mint például az RSA és a PKI, azon a feltételezésen alapulnak, hogy a kommunikáló felek nem ismernek egy előre megosztott kulcsot, és biztonságos kulcscserét kell létrehozniuk.

A hálózati kommunikációban a hitelesítés bizonyítja, hogy az üzenet valóban érvényes forrásból származik. Az adatok visszautasítása a hitelesítéshez hasonló szolgáltatás, mivel lehetővé teszi az üzenet küldőjének egyedi azonosítását. Az adatok integritása biztosítja, hogy az üzenetek továbbítása során ne változzanak. Az adatok bizalmas kezelése biztosítja a magánélet védelmét, így csak a címzett olvashatja el az üzenetet.

**Kriptográfia**   
A kriptográfiát évezredek óta használják a kommunikáció biztonságára. A történelmi rejtjelek közé tartozik az ókori Görögországból származó scytale, a Caesar-rejtjel és a Vigenère-rejtjel. A Vigenère-rejtjel a többalfabetikus helyettesítő titkosítás egy fajtája, amelyet 1863-ig feltörhetetlennek tartottak. Az Enigma Machine egy elektromechanikus eszköz volt, amely olyan kódolt üzeneteket állított elő, amelyeket nagyon nehéz volt feltörni a második világháború alatt. A titkosítás három típusa:

* **Transzponálás** – A kódolt szöveghez az átrendezett betűket használják. Annak érdekében, hogy a kulcs megosztható legyen, a betűket meghatározott számú karakterrel eltolták.
* **Helyettesítés** – Ez az, amikor az átlátszó szövegben különböző betűkkel helyettesítik a betűket.
* **Egyszeri billentyû** – Ez egy elõkészített kulcs, amely tetszõlegesen hosszú, nem ismétlõdõ számsorozatból áll, amelyet papírszalagon tartottak. Ezután karakterenként kombinálták az egyszerű szöveges üzenettel, hogy létrehozzák a titkosított szöveget. A kulcsokat csak egyszer használták, és előre megosztották őket.

**Rejtjel elemzés**   
A kriptoanalízis vagy kódtörés a titkosított információ jelentésének meghatározásának gyakorlata és tanulmányozása (a kód feltörése), a megosztott titkos kulcshoz való hozzáférés nélkül. A kriptoanalízis számos módszere:

* **Brute-force módszer** – A támadó minden lehetséges kulcsot kipróbál, tudván, hogy végül az egyik működni fog.
* **Titkosított szöveges módszer** – A támadó több titkosított üzenet titkosított szövegével rendelkezik, de nem ismeri a mögöttes egyszerű szöveget.
* **Ismert egyszerű szöveges módszer** – A támadó több üzenet titkosított szövegéhez fér hozzá, és tud valamit a titkosított szöveg mögött meghúzódó egyszerű szövegről.
* **Választott egyszerű szöveges módszer** – A támadó kiválasztja, hogy a titkosítóeszköz mely adatokat titkosítsa, és megfigyeli a titkosított szöveg kimenetét.
* **Választott titkosított szöveg módszer** – A támadó választhat különböző titkosított szöveget a visszafejtéshez, és hozzáfér a visszafejtett egyszerű szöveghez.
* **Meet-in-the-Middle módszer** – A támadó ismeri a nyílt szöveg egy részét és a megfelelő titkosított szöveget.

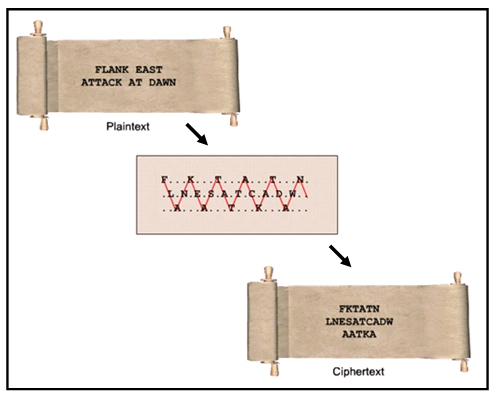
A modern kriptográfusok célja, hogy elég nagy kulcstérrel rendelkezzenek ahhoz, hogy túl sok időt és pénzt igényeljen egy brute force támadás végrehajtása. A betűk gyakoriságának elemzése egy nyelvben segíthet az egyszerű helyettesítési és transzponálási rejtjelek feltörésében.

**Kriptológia**   
A kriptológia a titkos kódok készítésének és feltörésének tudománya. Egyesíti a kriptográfiát és a kriptoanalízist. A kommunikáció és a hálózatépítés világában a hitelesítés, az integritás és az adatok bizalmas kezelése sokféle módon valósul meg különféle protokollok és algoritmusok segítségével. Az algoritmus kiválasztása a biztonsági követelményektől, a titkosításhoz és visszafejtéshez rendelkezésre álló hardvererőforrásoktól, valamint az algoritmus biztonsági közösségben való elfogadásától függ. Gyakran használnak nyilvános domain algoritmusokat. A legtöbb modern algoritmussal a sikeres visszafejtéshez a megfelelő kriptográfiai kulcsok ismerete szükséges. Ez azt jelenti, hogy a titkosítás biztonsága a kulcsok titkosságában rejlik, nem az algoritmusban.

15.5.2

## 15. modul – Kriptográfiai szolgáltatások kvíz

Az űrlap teteje

1. 

Az űrlap alja

Hivatkozz a kiállításra. Milyen típusú titkosítási módszer látható?

Mi az adatintegritás biztosításának két célja? (Válassz kettőt.)

A hálózatbiztonsági szakértő feladata egy olyan biztonsági intézkedés végrehajtása, amely figyeli az adatközpontban lévő kritikus fájlok állapotát, és azonnali riasztást küld, ha bármely fájl módosul. A biztonságos kommunikáció mely aspektusával foglalkozik ez a biztonsági intézkedés?



Milyen típusú támadás teszi lehetővé a támadó számára, hogy nyers erőt alkalmazzon?

Miért használnák a HMAC-ot a különféle hivatkozásokon áthaladó adatok védelmére?

Mi áll a kriptoanalízis középpontjában?

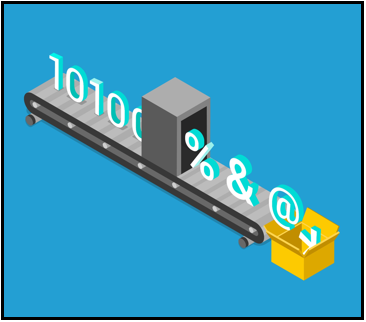
Mi a kriptológia?

A biztonságos kommunikáció melyik célja érhető el az adatok titkosításával?

Mi a célja a visszautasítás nélküli szolgáltatásnak a biztonságos kommunikációban?

Mi a példa az átültetési titkosításra?

A webszerver rendszergazdája úgy konfigurálja a hozzáférési beállításokat, hogy a felhasználóknak először hitelesítést kell végezniük bizonyos weboldalak elérése előtt. Melyik információbiztonsági követelményt elégíti ki a konfiguráció?



Mivel az adatokat helyi merevlemezen tárolják, melyik módszer védi meg az adatokat az illetéktelen hozzáféréstől?

[15.4](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Cryptology](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[16.0](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                        
*           

1. Basic Integrity and Authenticity
2. Introduction

# Bevezetés

16.0.1

## Miért vegyem ezt a modult?

Mit tudsz a kriptográfiáról? Mi ez és hogyan lehet megvalósítani? A hivatkozásokon áthaladó adatok biztonsága érdekében ismernie kell az adatok védelmét és integritásának megőrzését. Ebben a modulban megismerheti a kriptográfiát és a digitális adatkommunikációban betöltött szerepét. Kezdjük el.

16.0.2

## Mit fogok tanulni ebben a modulban?

**Modul címe:** Alapvető integritás és hitelesség

**A modul célja** : Magyarázza el, hogyan használják a kriptográfiát az adatok integritásának és hitelességének biztosítására.

| **téma címe** | **Téma Cél** |
| --- | --- |
| **Integritás és hitelesség** | Ismertesse a kriptográfia szerepét az adatok integritásának és hitelességének biztosításában! |
| **Kulcskezelés** | Ismertesse a kulcskezelés összetevőit! |
| **Titoktartás** | Magyarázza el, hogy a kriptográfiai megközelítések hogyan javítják az adatok bizalmas kezelését. |

[15.5](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Cryptographic Services Summary](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[16.1](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Integrity and Authenticity](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                            
*           

1. Basic Integrity and Authenticity
2. Integrity and Authenticity

# Integritás és hitelesség

16.1.1

## Biztonságos kommunikáció

A szervezeteknek támogatást kell nyújtaniuk az adatok biztonságos közlekedéséhez, miközben azok a linkeken keresztül haladnak. Ez magában foglalhatja a belső forgalmat is, de még fontosabb a szervezeten kívülre, fióktelepekre, távmunkás telephelyekre és partneroldalakra továbbított adatok védelme.

Ez a biztonságos kommunikáció négy eleme:

* **Adatok integritása** – Garantálja, hogy az üzenetet nem módosították. A továbbítás alatt lévő adatok bármilyen változását észleli. Az integritást a Secure Hash Algorithmusok (SHA-2 vagy SHA-3) végrehajtása biztosítja. Az MD5 üzenetfeldolgozó algoritmust még mindig széles körben használják. Azonban eredendően nem biztonságos, és sebezhetőséget okoz a hálózatban. Vegye figyelembe, hogy az MD5-öt kerülni kell.
* **Eredeti hitelesítés** – Garantálja, hogy az üzenet nem hamis, és valóban attól származik, akitől azt állítja. Számos modern hálózat biztosítja a hitelesítést olyan algoritmusokkal, mint például a hash-alapú üzenet-hitelesítési kód (HMAC).
* **Adatok bizalmas kezelése** – Garantálja, hogy csak az arra jogosult felhasználók olvashatják az üzenetet. Ha az üzenetet elfogják, azt nem lehet megfejteni ésszerű időn belül. Az adatok bizalmas kezelése szimmetrikus és aszimmetrikus titkosítási algoritmusokkal valósul meg.
* **Adatok visszautasítása** – Garantálja, hogy a feladó nem tudja megtagadni vagy cáfolni az elküldött üzenet érvényességét. A letagadhatatlanság azon a tényen alapul, hogy csak a feladó rendelkezik az üzenet kezelésének egyedi jellemzőivel vagy aláírásával.

A kriptográfia szinte bárhol használható, ahol van adatkommunikáció. Valójában az a tendencia, hogy minden kommunikációt titkosítanak.

16.1.2

## Kriptográfiai hash-függvények

Kivonatokat használnak az adatok integritásának ellenőrzésére és biztosítására. A hitelesítés ellenőrzésére is használják. A kivonatolás egy egyirányú matematikai függvényen alapul, amely viszonylag könnyen kiszámítható, de lényegesen nehezebb visszafordítani.

A kávé őrlése jó analógiája az egyirányú funkciónak. A szemes kávét könnyű őrölni, de szinte lehetetlen az összes apró darabot összerakni az eredeti kávészemek újjáépítéséhez.

Amint az ábrán látható, a hash függvény egy változó bináris adatblokkot vesz fel, amelyet üzenetnek nevezünk, és egy rögzített hosszúságú, tömörített reprezentációt állít elő, amelyet hash-nek nevezünk. Az eredményül kapott hash-t néha üzenetkivonatnak, kivonatnak vagy digitális ujjlenyomatnak is nevezik.

Az ábrán egy nyomtatott papírlap látható, melynek oldalán a következő szavak szerepelnek: egyszerű szöveges üzenet (tetszőleges hosszúságú adatok). Egy nyíl a papírról egy tölcsérbe kerül, amely mellett a hash funkció szavak vannak. Egy nyíl megy ki a tölcsérből egy szövegmezőbe: e883aacb24c09f és a rögzített hosszúságú hash érték szavak.

e883aa0b24c09f

Egyszerű szöveges üzenet (tetszőleges hosszúságú adatok) Hash-függvény Fix hosszúságú hash-érték

A hash függvényekkel számításilag nem kivitelezhető, hogy két különböző adathalmaz ugyanazt a hash kimenetet adja. Ezenkívül a hash értéke minden alkalommal változik, amikor az adatokat módosítják vagy módosítják. Emiatt a kriptográfiai hash értékeket gyakran „digitális ujjlenyomatoknak” nevezik. Ezek az ujjlenyomatok használhatók duplikált adatfájlok, fájlverzióváltozások és hasonló alkalmazások észlelésére. Ezeket az értékeket az adatok véletlen vagy szándékos megváltoztatása vagy véletlen adatsérülése elleni védekezésre használják.

A kriptográfiai hash funkciót számos különböző helyzetben alkalmazzák entitáshitelesítési, adatintegritási és adathitelességi célokra.

16.1.3

## Kriptográfiai hash művelet

Matematikailag a **h= H(x)** egyenlet arra szolgál, hogy megmagyarázza, hogyan működik egy hash algoritmus. Amint az ábrán látható, egy **H** bemenetet vesz **hash függvény x** , és egy fix méretű karakterlánc **h** hash értéket ad vissza .

Az ábrán egy olyan kör látható, amelyben H(x) található. A tetején van egy szövegdoboz, amely tetszőleges hosszúságú szöveget ír, és egy nyíl, amely a körbe megy, és az x-re mutat. A szövegmezőtől jobbra található az x és egy egyszerű szöveges üzenet ikonja. Középen egy szövegdoboz található a hash függvény szavakkal és a körön belüli h-ra mutató nyíllal. A szövegdoboz jobb oldalán egy H betű, egy tölcsér ikon és a szavak hash funkciója található. Alul van egy szövegdoboz, amely a körből vezet, és a hash szavakkal, a szövegdoboz mellett a h betűvel és egy téglalappal, amelyben e883aa0b24c09f van.

x H h H(x)

e883aa0b24c09f

Kivonat függvény Tetszőleges hosszúságú szöveg Kivonatoló függvény Hash érték Egyszerű szöveges üzenet

Az ábrán látható példa a matematikai folyamatot foglalja össze. A kriptográfiai hash függvénynek a következő tulajdonságokkal kell rendelkeznie:

* A bemenet bármilyen hosszúságú lehet.
* A kimenet mindig rögzített hosszúságú.
* **H(x)** viszonylag könnyen kiszámítható bármely adott x-re.
* **H(x)** egyirányú és nem visszafordítható.
* **A H(x)** ütközésmentes, ami azt jelenti, hogy két különböző bemeneti érték eltérő hash-értéket eredményez.

Ha egy hash függvényt nehéz megfordítani, akkor egyirányú hash-nek tekintendő. A nehezen invertálható azt jelenti, hogy **h** hash érték mellett számításilag nem lehetséges olyan bemenetet találni **x-** hez , amelyre **h=H(x)** .

16.1.4

## MD5 és SHA

A hash függvények az üzenet integritását biztosítják. Segítenek abban, hogy az adatok véletlenül se változzanak meg, és hogy amit elküldtek, az valóban az, amit megkaptak.

**Megjegyzés:** A fenyegetés szereplői szándékos változtatásokat hajthatnak végre.

Az ábrán a feladó 100 dolláros pénzátutalást küld Alexnek. A feladó biztosítani akarja, hogy az üzenet véletlenül se változzon meg a címzetthez vezető úton.

Az ábra egy olyan üzenet hash-számítását mutatja, amelyben a kezdő és a befejező hash eltérő. Az elküldött üzenet szerint: Fizessen Alexnek 100,00 dollárt. A kapott üzenetben ez áll: Fizessen Jeremynek 1000,00 dollárt. A kezdő hash 4ehlDx67NMop9, a befejező hash pedig 12ehqPx67NMoX.

**Fizessen** Alexnek 100,00 USD száz és 00/100 dollár 4ehlDx67NMop9 kezdő hash **Fizetés** Jeremynek 1000,00 ezer dollár 100/100 dollár 12ehqPx67NMoX végkivonat eltérő

A hash algoritmus a következőképpen működik:

1. A küldő eszköz beviszi az üzenetet egy kivonatoló algoritmusba, és kiszámítja a **4ehiDx67NMop9** rögzített hosszúságú hash-ét .
2. Ezt a hash-t ezután csatolják az üzenethez, és elküldik a címzettnek. Az üzenet és a hash is egyszerű szövegben van.
3. A fogadó eszköz eltávolítja a hash-t az üzenetből, és beviszi az üzenetet ugyanabba a kivonatolási algoritmusba. Ha a számított hash megegyezik az üzenethez csatolt kivonattal, akkor az üzenet nem módosult az átvitel során. Ha a hash-ek nem egyenlőek, ahogy az az ábrán látható, akkor az üzenet integritásában már nem lehet megbízni.

Négy jól ismert hash függvény létezik:

* **MD5 128 bites kivonattal** – A Ron Rivest által kifejlesztett és számos internetes alkalmazásban használatos MD5 egy egyirányú funkció, amely 128 bites hash üzenetet állít elő. Az MD5-öt örökölt algoritmusnak tekintik, ezért kerülni kell, és csak akkor szabad használni, ha nem áll rendelkezésre jobb alternatíva. Ehelyett az SHA-2 vagy az SHA-3 használata javasolt.
* **SHA-1** – Az Egyesült Államok Nemzetbiztonsági Ügynöksége (NSA) fejlesztette ki 1995-ben. Nagyon hasonlít az MD5 hash funkcióira. Több verzió létezik. Az SHA-1 160 bites hash üzenetet hoz létre, és valamivel lassabb, mint az MD5. Az SHA-1 ismert hibáival rendelkezik, és egy örökölt algoritmus.
* **SHA-2** – Az NSA fejlesztette ki. Tartalmazza az SHA-224-et (224 bites), az SHA-256-ot (256 bites), az SHA-384-et (384 bites) és az SHA-512-t (512 bites). Ha SHA-2-t használ, akkor lehetőség szerint az SHA-256, SHA-384 és SHA-512 algoritmusokat kell használni.
* **SHA-3** – Az SHA-3 a legújabb kivonatoló algoritmus, amelyet a Nemzeti Szabványügyi és Technológiai Intézet (NIST) vezetett be az SHA-2 kivonatoló algoritmusok családjának alternatívájaként. Az SHA-3 tartalmazza az SHA3-224-et (224 bites), az SHA3-256-ot (256 bites), az SHA3-384-et (384 bites) és az SHA3-512-t (512 bites). Az SHA-3 család új generációs algoritmusok, és lehetőség szerint érdemes használni.

Míg a hash-t fel lehet használni a véletlen változások észlelésére, nem használható a fenyegetés szereplői által végrehajtott szándékos változtatások elleni védekezésre. A kivonatolási eljárás során nem érkezik egyedi azonosító információ a küldőtől. Ez azt jelenti, hogy bárki számíthat kivonatot bármilyen adatra, feltéve, hogy rendelkezik a megfelelő hash funkcióval.

Például, amikor az üzenet áthalad a hálózaton, a potenciális fenyegetettség elfoghatja az üzenetet, megváltoztathatja azt, újraszámíthatja a hash-t, és hozzáfűzheti az üzenethez. A fogadó eszköz csak a hozzáfűzött hash alapján érvényesíti.

Ezért a kivonat ki van téve a köztes támadásoknak, és nem nyújt biztonságot a továbbított adatok számára. A „man-in-the-middle” támadásokkal szembeni integritás biztosítása érdekében az eredet hitelesítése is szükséges.

16.1.5

## Eredet hitelesítés

Eredeti hitelesítés és integritásbiztosítás hozzáadásához használjon kulcsos hash üzenet-hitelesítési kódot (HMAC). A HMAC egy további titkos kulcsot használ a hash függvény bemeneteként.

**Megjegyzés:** Más üzenet hitelesítési kód (MAC) módszerek is használatosak. A HMAC-ot azonban számos rendszer használja, beleértve az SSL-t, az IPsec-et és az SSH-t.

Kattintson az egyes gombra, ha illusztrációt és magyarázatot szeretne látni a HMAC használatával történő eredethitelesítésről.

Amint az ábrán látható, a HMAC kiszámítása bármely olyan kriptográfiai algoritmussal történik, amely a kriptográfiai hash függvényt titkos kulccsal kombinálja. A hash függvények a HMAC-k védelmi mechanizmusának alapját képezik.

Csak a küldő és a fogadó ismeri a titkos kulcsot, és a hash függvény kimenete mostantól a bemeneti adatoktól és a titkos kulcstól függ. Csak a titkos kulcshoz hozzáféréssel rendelkező felek számíthatják ki a HMAC függvény kivonatát. Ez legyőzi a köztes támadásokat, és hitelesíti az adatok eredetét.

Ha két fél megoszt egy titkos kulcsot, és HMAC-funkciókat használ a hitelesítéshez, az egyik fél által kapott üzenet megfelelően felépített HMAC-kivonat azt jelzi, hogy a másik fél volt az üzenet kezdeményezője. Ez azért van, mert a másik fél birtokában van a titkos kulcs.

Az ábra a hmac kivonatoló algoritmust mutatja

e883aa0b24c09f

Rögzített hosszúságú hitelesített hash érték adatok tetszőleges hosszúságú titkos kulcs hash függvény egyszerű szöveges üzenete

16.1.6

## Lab – A dolgok kivonatolása

Ebben a laborban a következő célokat kell teljesítenie:

* Kivonatok létrehozása OpenSSL-lel
* Hashes ellenőrzése

[16.0](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[16.2](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Key Management](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                
*           

1. Basic Integrity and Authenticity
2. Key Management

# Kulcskezelés

16.2.1

## A kulcskezelés jellemzői

A kulcskezelést gyakran a kriptorendszer tervezésének legnehezebb részének tekintik. Sok kriptorendszer meghibásodott a kulcskezelés hibái miatt, és minden modern kriptográfiai algoritmushoz kulcskezelési eljárások szükségesek. A gyakorlatban a kriptográfiai rendszerek elleni támadások többsége a kulcskezelési szintre irányul, nem pedig magára a kriptográfiai algoritmusra.

Amint a táblázatból látható, a kulcskezelésnek számos alapvető jellemzőjét figyelembe kell venni.

| **Jellegzetes** | **Leírás** |
| --- | --- |
| Kulcsgenerálás | Caesarra volt bízva, hogy válassza ki a rejtjel kulcsát. A Vigenère titkosítási kulcsot is a küldő és a fogadó választja ki. Egy modern kriptográfiai rendszerben a kulcsgenerálás általában automatizált, és nem marad a végfelhasználóra. Jó véletlenszám-generátorok használata szükséges annak biztosításához, hogy minden kulcs egyformán generálódik, így a támadó nem tudja megjósolni, hogy melyik kulcsot használják nagyobb valószínűséggel. |
| Kulcsellenőrzés | Egyes kulcsok jobbak, mint mások. Szinte minden kriptográfiai algoritmusnak van néhány gyenge kulcsa, amelyeket nem szabad használni. A kulcsellenőrzési eljárások segítségével a gyenge kulcsok azonosíthatók és újra előállíthatók a biztonságosabb titkosítás érdekében. A Caesar-rejtjellel a 0 vagy 25-ös kulcs használata nem titkosítja az üzenetet, ezért nem szabad használni. |
| Kulcscsere | A kulcskezelési eljárásoknak biztonságos kulcscsere-mechanizmust kell biztosítaniuk, amely lehetővé teszi a kulcsanyagról való biztonságos megállapodást a másik féllel, valószínűleg nem megbízható médiumon keresztül. |
| Kulcstárolás | Egy modern többfelhasználós operációs rendszeren, amely titkosítást használ, egy kulcs tárolható a memóriában. Ez lehetséges problémát jelent, ha a memóriát a lemezre cserélik, mivel a felhasználó számítógépére telepített trójai program hozzáférhet a felhasználó privát kulcsaihoz. |
| Kulcs élettartama | A rövid kulcs-élettartamok használata javítja a nagy sebességű kapcsolatokon használt örökölt rejtjelek biztonságát. Az IPsec-ben a 24 órás élettartam jellemző. Az élettartam 30 percre való módosítása azonban javítja az algoritmusok biztonságát. |
| Kulcs visszavonása és megsemmisítése | A visszavonás minden érdekelt felet értesít arról, hogy egy bizonyos kulcsot feltörtek, és azt már nem szabad használni. A megsemmisítés törli a régi kulcsokat oly módon, hogy megakadályozza a rosszindulatú támadók visszaszerzését. |

16.2.2

## Kulcshossz és kulcstér

A kulcsok leírására használt két kifejezés a következő:

* **Kulcshossz** – Kulcsméretnek is nevezik, ez a bitben megadott mérték. Ebben a kurzusban a kulcshossz kifejezést fogjuk használni.
* **Kulcstér** – Az adott kulcshossz által generálható lehetőségek száma.

A kulcshossz növekedésével a kulcstér exponenciálisan növekszik:

* Egy 2 bites (2 2 ) kulcshossz = 4-es billentyűtér, mivel négy lehetséges billentyű (00, 01, 10 és 11).
* Egy 3 bites (2 3 ) kulcshossz = 8-as billentyűtér, mert nyolc lehetséges billentyű (000, 001, 010, 011, 100, 101, 110, 111).
* Egy 4 bites (2 4 ) kulcshossz = 16 lehetséges billentyűből álló billentyűtér.
* Egy 40 bites (2 40 ) kulcshossz = 1 099 511 627 776 lehetséges billentyűből álló billentyűtér.

A táblázat az AES titkosítási algoritmus jellemzőit mutatja be. Figyelje meg, hogyan használ az AES hosszú kulcsokat. Ez drámaian megnöveli a kulcsteret, ami befolyásolja a kód feltöréséhez szükséges időt.

| **Jellegzetes** | **Leírás** |
| --- | --- |
| **Algoritmus teljes név** | Fejlett titkosítási szabvány |
| **Idővonal** | Hivatalos szabvány 2001 óta |
| **Algoritmus típusa** | Szimmetrikus |
| **Kulcsméret (bitekben)** | 128, 192 és 256 |
| **Sebesség** | Magas |
| **Ideje feltörni  (feltételezve, hogy egy számítógép másodpercenként 255 billentyűt próbálhat ki)** | 149 billió év |
| **Erőforrás fogyasztás** | Alacsony |

16.2.3

## A Keyspace

Egy algoritmus kulcstere az összes lehetséges kulcsérték halmaza. bites kulcs **Egy n** 2 bites kulcsteret hoz létre **n** lehetséges kulcsértékek. Egy bit hozzáadásával a kulcshoz a kulcstér gyakorlatilag megduplázódik.

Ahogy a táblázat mutatja, a DES 56 bites kulcsaival több mint 72 000 000 000 000 000 kulcstere (2 56 ) lehetséges kulcsokat. Ha egy bitet adunk a kulcs hosszához, a kulcstér megduplázódik, és a támadónak kétszer annyi időre van szüksége a kulcstér kereséséhez. Egy további bit hozzáadása az 57 bites kulcsmérethez azt jelenti, hogy a támadónak négyszer annyi időt vesz igénybe a kulcstér keresése. Ha további 4 bitet adunk az 56 biteshez, akkor 60 bites kulcs jön létre. Egy 60 bites kulcs feltörése 16-szor hosszabb ideig tart, mint egy 56 bites kulcs.

| **DES kulcs** | **Keyspace** | **Hozzávetőleges szám  lehetséges kulcsok közül** |
| --- | --- | --- |
| 56 bites | 2 56  11111111 11111111 11111111  11111111 11111111 11111111 11111111 | ~72,000,000,000,000,000 |
| 57 bites | 2 57  11111111 11111111 11111111  11111111 11111111 11111111 11111111 **1** | ~144,000,000,000,000,000 |
| 58 bites | 2 58  11111111 11111111 11111111  11111111 11111111 11111111 11111111 **11** | ~288,000,000,000,000,000 |
| 59 bites | 2 59  11111111 11111111 11111111  11111111 11111111 11111111 11111111 **111** | ~576,000,000,000,000,000 |
| 60 bites | 2 60  11111111 11111111 11111111  11111111 11111111 11111111 11111111 **1111** | ~1,152,000,000,000,000,000 |

**Megjegyzés** : A hosszabb kulcsok biztonságosabbak; ugyanakkor erőforrásigényesebbek is. Óvatosan kell eljárni a hosszabb kulcsok kiválasztásakor, mert ezek kezelése jelentősen megterhelheti a processzort az alacsonyabb kategóriás termékekben.

Szinte minden algoritmusnak van néhány gyenge kulcsa a kulcsterében, amelyek lehetővé teszik a támadó számára, hogy egy parancsikon segítségével megtörje a titkosítást. A gyenge kulcsok a titkosítás szabályszerűségeit mutatják. Például a DES-nek négy kulcsa van, amelyek titkosítása megegyezik a visszafejtéssel. Ez azt jelenti, hogy ha ezen gyenge kulcsok egyikét a nyílt szöveg titkosításához használják, a támadó a gyenge kulcsot használhatja a titkosított szöveg visszafejtésére és a nyílt szöveg felfedésére.

A DES gyenge kulcsai azok, amelyek 16 azonos alkulcsot hoznak létre. Ez akkor fordul elő, ha a kulcsbitek:

* Váltakozó egyesek és nullák (0101010101010101)
* Váltakozó F és E (FRESH FRESH FRESH)
* E0E0E0E0F1F1F1F1
* 1F1F1F1F0E0E0E0E

Nagyon valószínűtlen, hogy ilyen kulcsokat választanak, de a hálózati rendszergazdáknak továbbra is ellenőrizniük kell az összes implementált kulcsot, és meg kell akadályozniuk a gyenge kulcsok használatát. A kézi kulcsgenerálásnál különösen ügyeljen arra, hogy elkerülje a gyenge kulcsok meghatározását.

**Megjegyzés** : A DES egy örökölt titkosítási algoritmus, ezért nem szabad használni. Itt csak a kulcstér fogalmának illusztrálására használjuk.

16.2.4

## A kriptográfiai kulcsok típusai

Többféle kriptográfiai kulcs generálható:

* **Szimmetrikus kulcsok** – Két, VPN-t támogató router között cserélhetők
* **Aszimmetrikus kulcsok** – biztonságos HTTPS-alkalmazásokban használatosak
* **Digitális aláírás** – biztonságos webhelyhez való csatlakozáskor használatos
* **Kivonatkulcsok** – Szimmetrikus és aszimmetrikus kulcsgeneráláshoz, digitális aláírásokhoz és más típusú alkalmazásokhoz használják

A kulcs típusától függetlenül minden kulcs hasonló problémákkal küzd. A megfelelő kulcshossz kiválasztása egy kérdés. Ha a kriptográfiai rendszer megbízható, az egyetlen módja annak, hogy megtörjük, brute force támadással. Ha a kulcstér elég nagy, a keresés rendkívül sok időt vesz igénybe, így az ilyen kimerítő erőfeszítés nem praktikus. A táblázat összefoglalja azt a kulcshosszt, amely az adatok jelzett ideig történő védelméhez szükséges.

| **A védelem időtartama** | **Szimmetrikus kulcs** | **Aszimmetrikus kulcs** | **Digitális aláírás** | **Hash** |
| --- | --- | --- | --- | --- |
| 3 év | 80 | 1248 | 160 | 160 |
| 10 év | 96 | 1776 | 192 | 192 |
| 20 év | 112 | 2432 | 224 | 224 |
| 30 év | 128 | 3248 | 256 | 256 |
| Védelem a kvantumszámítógépek ellen | 256 | 15424 | 512 | 512 |

Átlagosan a támadónak át kell keresnie a kulcstér felét, mielőtt megtalálja a megfelelő kulcsot. A keresés végrehajtásához szükséges idő a támadó rendelkezésére álló számítógép teljesítményétől függ.

A jelenlegi kulcshosszúság könnyen jelentéktelenné tehet minden próbálkozást, mert kellően hosszú kulcs használata esetén több millió vagy milliárd évbe telik a keresés befejezése.

A modern, megbízható algoritmusokkal a védelem erőssége kizárólag a kulcs méretétől függ. A kulcs hosszát úgy válassza meg, hogy az megfelelő ideig védje az adatok bizalmasságát vagy integritását. Az érzékenyebb és tovább titokban tartandó adatoknak hosszabb kulcsokat kell használniuk.

16.2.5

## Választható kriptográfiai kulcsok

A teljesítmény egy másik kérdés, amely befolyásolhatja a kulcshossz kiválasztását. Az adminisztrátornak jó egyensúlyt kell találnia az algoritmusok sebessége és védelmi erőssége között, mert egyes algoritmusok, például a Rivest, Shamir és Adleman (RSA) algoritmusok lassan futnak a nagy kulcshosszok miatt. Törekedjen a megfelelő védelemre, miközben lehetővé teszi a nem megbízható hálózatokon keresztüli kommunikációt.

A támadó becsült finanszírozása szintén befolyásolja a kulcs hosszának megválasztását. Amikor felméri annak kockázatát, hogy valaki megszegi a titkosítási algoritmust, becsülje meg a támadó erőforrásait és azt, hogy mennyi ideig kell védeni az adatokat. Például a klasszikus DES-t egy 1 millió dolláros gép néhány perc alatt meg tudja törni. Ha a védett adatok lényegesen többet érnek, mint a feltörő eszköz beszerzéséhez szükséges 1 millió dollár, akkor más algoritmust kell használni. Valójában a DES ma már túl gyengének számít ahhoz, hogy bármilyen alkalmazáshoz használjuk.

A technológia és a kriptoanalitikai módszerek gyors fejlődése miatt az adott alkalmazáshoz szükséges kulcshossz folyamatosan növekszik. Az RSA algoritmus erősségének része a nagy számok faktorálásának nehézsége. Például a 12 tényezője 1 x 12, 2 x 6 és 3 x 4. Ezért egy 1024 bites szám nagyon nagy szám, sok tényezővel. Ennek a számnak a 2048 bitesre növelése még több tényezőt eredményez. Természetesen ez az előny elveszik, ha egyszerű módot találunk nagy számok faktorálására, de a kriptográfusok ezt a lehetőséget valószínűtlennek tartják.

A „minél hosszabb a kulcs, annál jobb” szabály érvényes, kivéve az esetleges teljesítményi okokat. A rövidebb kulcsok gyorsabb feldolgozást jelentenek, de kevésbé biztonságosak. A hosszabb kulcsok lassabb feldolgozást jelentenek, de biztonságosabbak.

16.2.6

## Ellenőrizze megértését – a kulcskezelés jellemzői

Az űrlap teteje

Ellenőrizze, hogy megértette-e a kulcskezelés jellemzőit, és válassza ki a LEGJOBB választ a következő kérdésekre.

1. Melyik jellemző segít azonosítani a gyenge kulcsot és újra létrehozni egy új cserekulcsot?

Az űrlap alja

Melyik jellemző hoz létre új kulcsokat a titkosításhoz?

Melyik jellemző az a mechanizmus, amely biztonságos megállapodást tesz lehetővé a kulcsanyagról a másik féllel egy nem megbízható adathordozón?

[16.1](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Integrity and Authenticity](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[16.3](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Confidentiality](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                          
*           

1. Basic Integrity and Authenticity
2. Confidentiality

# Titoktartás

16.3.1

## Adatok bizalmas kezelése

Az aszimmetrikus és a szimmetrikus titkosítás az a két titkosítási osztály, amelyet az adatok bizalmas kezelésére használnak. Ez a két osztály a kulcsok használatában különbözik.

A szimmetrikus titkosítási algoritmusok, mint például a Data Encryption Standard (DES), a 3DES és az Advanced Encryption Standard (AES) azon a feltevésen alapulnak, hogy minden kommunikáló fél ismeri az előre megosztott kulcsot. Az adatok bizalmas kezelése aszimmetrikus algoritmusokkal is biztosítható, beleértve a Rivest, Shamir és Adleman (RSA) és a nyilvános kulcsú infrastruktúrát (PKI).

**Megjegyzés:** A DES egy örökölt algoritmus, ezért nem szabad használni. A 3DES-t lehetőleg kerülni kell.

Az ábra rávilágít néhány különbségre a szimmetrikus és az aszimmetrikus titkosítás között.

Az ábra a szimmetrikus és az aszimmetrikus titkosítás közötti különbségeket mutatja. A szimmetrikus titkosítás jellemzői a következők: ugyanazt a kulcsot használja az adatok titkosításához és visszafejtéséhez; a kulcs hossza rövid (40 bit - 256 bit); gyorsabb, mint az aszimmetrikus titkosítás; és gyakran használják tömeges adatok, például VPN-forgalom titkosítására. Az aszimmetrikus titkosítás jellemzői a következők: különböző kulcsokat használ az adatok titkosításához és visszafejtéséhez; a kulcsok hosszúak (512 bit – 4096 bit); a számítási feladatok elvégzése ezért lassabb, mint a szimmetrikus titkosítás; és gyakran használják gyors adattranzakciókhoz, például HTTPS-hez a banki adatok elérésekor.

Szimmetrikus titkosítás Aszimmetrikus titkosítás

* Ugyanazt a kulcsot használja az adatok titkosításához és visszafejtéséhez.
* A kulcsok rövidek (40 bit – 256 bit).
* Gyorsabb, mint az aszimmetrikus titkosítás.
* Általában tömeges adatok titkosításához használják, például VPN-forgalomban.
* Különböző kulcsokat használ az adatok titkosításához és visszafejtéséhez.
* A kulcsok hosszúak (512 bit – 4096 bit).
* Számítási szempontból ezért lassabb, mint a szimmetrikus titkosítás.
* Gyakran használják gyors adattranzakciókhoz, például HTTPS-hez a banki adatok elérésekor.

16.3.2

## Szimmetrikus titkosítás

A szimmetrikus algoritmusok ugyanazt az előre megosztott kulcsot használják az adatok titkosításához és visszafejtéséhez. Az előre megosztott kulcsot, más néven titkos kulcsot, a küldő és a fogadó ismeri, mielőtt bármilyen titkosított kommunikációra sor kerülhetne.

A szimmetrikus titkosítás működésének szemléltetésére vegyünk egy példát, ahol Alice és Bob különböző helyeken élnek, és titkos üzeneteket akarnak váltani egymással a levelezőrendszeren keresztül. Ebben a példában Alice titkos üzenetet akar küldeni Bobnak.

Az ábrán Alice-nek és Bobnak ugyanaz a kulcsa van egyetlen lakathoz. Ezeket a kulcsokat a titkos üzenetek küldése előtt kicserélték. Alice ír egy titkos üzenetet, és egy kis dobozba teszi, amit a kulcsával a lakattal lezár. Elküldi a dobozt Bobnak. Az üzenet biztonságosan zárva van a dobozban, miközben a doboz áthalad a postarendszeren. Amikor Bob megkapja a dobozt, a kulcsával kinyitja a lakatot, és előveszi az üzenetet. Bob ugyanazt a dobozt és lakatot használhatja, hogy titkos választ küldjön vissza Alice-nek.

Az ábra a szövegben leírt szimmetrikus titkosítási analógiát mutatja.

### Példa szimmetrikus titkosításra

Kulcskulcs Üzenettitkosítás Előre megosztott kulcs !@#IQ Az üzenet visszafejtése $

Manapság a szimmetrikus titkosítási algoritmusokat gyakran használják a VPN-forgalomhoz. Ennek az az oka, hogy a szimmetrikus algoritmusok kevesebb CPU-erőforrást használnak, mint az aszimmetrikus titkosítási algoritmusok. Ez lehetővé teszi, hogy VPN használatakor gyors legyen az adatok titkosítása és visszafejtése. Szimmetrikus titkosítási algoritmusok használatakor, mint minden más típusú titkosításnál, minél hosszabb a kulcs, annál tovább tart, amíg valaki megtalálja a kulcsot. A legtöbb titkosítási kulcs 112 és 256 bit közötti. A titkosítás biztonságosságának biztosítása érdekében legalább 128 bites kulcshosszt kell használni. Használjon hosszabb kulcsot a biztonságosabb kommunikáció érdekében.

A szimmetrikus titkosítási algoritmusokat néha blokk-rejtjelként vagy adatfolyam-rejtjelként osztályozzák. Kattintson a gombokra a két titkosítási mód megismeréséhez.

**A blokkrejtjelek** egy fix hosszúságú nyílt szövegblokkot alakítanak át egy közös, 64 vagy 128 bites titkosított szöveg blokkká. A gyakori blokkrejtjelek közé tartozik a 64 bites blokkméretű DES és a 128 bites AES.

Az ábrán egy egyszerű szöveges üzenet látható, amely 64 bites blokkokban van titkosítva.

01010010110010101

010100101100010101

Egyszerű szöveges üzenet titkosított üzenet 64 bit 64 bit 64 bit Blokktitkosítás – A titkosítás 64 bites blokkokban fejeződik be. üres üres 1100101

A jól ismert szimmetrikus titkosítási algoritmusokat a táblázat ismerteti.

| **Szimmetrikus titkosítási algoritmusok** | **Leírás** |
| --- | --- |
| **Adattitkosítási szabvány (DES)** | Ez egy örökölt szimmetrikus titkosítási algoritmus. Rövid kulcshosszt használ, ami a legtöbb jelenlegi felhasználáshoz nem biztonságos. |
| **3DES (hármas DES)** | A DES helyettesíti, és háromszor megismétli a DES algoritmus folyamatát. Lehetőség szerint kerülni kell, mivel a tervek szerint 2023-ban megszűnik. Ha megvalósul, használjon nagyon rövid kulcsélettartamot. |
| **Fejlett titkosítási szabvány (AES)** | Az AES egy népszerű és ajánlott szimmetrikus titkosítási algoritmus. 128, 192 vagy 256 bites kulcsok kombinációit kínálja a 128, 192 vagy 256 bites adatblokkok titkosításához. |
| **Szoftver-optimalizált titkosítási algoritmus (SEAL)** | A SEAL egy gyorsabb alternatív szimmetrikus titkosítási algoritmus az AES-hez. A SEAL egy adatfolyam-rejtjel, amely 160 bites titkosítási kulcsot használ, és kisebb hatással van a CPU-ra, mint más szoftveralapú algoritmusok. |
| **Rivest ciphers (RC) sorozat algoritmusai** | Ezt az algoritmust Ron Rivest fejlesztette ki. Számos változatot fejlesztettek ki, de az RC4 volt a legelterjedtebb a használatban. Az RC4 egy adatfolyam titkosítás, amelyet a webes forgalom biztosítására használtak. Megállapították, hogy számos sebezhetősége van, amelyek bizonytalanná tették. Az RC4-et nem szabad használni. |

16.3.3

## Aszimmetrikus titkosítás

Az aszimmetrikus algoritmusokat, amelyeket nyilvános kulcsú algoritmusoknak is neveznek, úgy tervezték, hogy a titkosításhoz használt kulcs eltérjen a visszafejtéshez használt kulcstól, amint az az ábrán látható. A visszafejtési kulcs ésszerű időn belül nem számítható ki a titkosítási kulcsból és fordítva.

Az ábra egy példát mutat az aszimmetrikus titkosításra, ahol a titkosítási kulcs különbözik a visszafejtési kulcstól.

### Példa aszimmetrikus titkosításra

Encryption Key Plaintext Encrypted Encryption Plaintext Decryption Decryption Key

Az aszimmetrikus algoritmusok nyilvános kulcsot és privát kulcsot használnak. Mindkét kulcs képes a titkosítási folyamatra, de a visszafejtéshez a kiegészítő páros kulcsra van szükség. A folyamat visszafordítható is. A nyilvános kulccsal titkosított adatok titkosításának feloldásához privát kulcsra van szükség. Az aszimmetrikus algoritmusok ezzel az eljárással biztosítják a bizalmasságot és a hitelességet.

Mivel egyik félnek sincs közös titka, nagyon hosszú kulcsokat kell használni. Az aszimmetrikus titkosítás 512 és 4096 bit közötti kulcshosszúságot használhat. A 2048 bitnél nagyobb vagy azzal egyenlő kulcshosszúságok megbízhatóak, míg az 1024 vagy annál rövidebb kulcsok nem tekinthetők elegendőnek.

Példák az aszimmetrikus kulcsalgoritmusokat használó protokollokra:

* **Internet Key Exchange (IKE) –** Ez az IPsec VPN-ek alapvető összetevője.
* **Secure Socket Layer (SSL) –** Ez most az IETF szabványos Transport Layer Security (TLS) néven van megvalósítva.
* **Secure Shell (SSH) –** Ez a protokoll biztonságos távoli hozzáférést biztosít a hálózati eszközökhöz.
* **Pretty Good Privacy (PGP) –** Ez a számítógépes program titkosítási adatvédelmet és hitelesítést biztosít. Gyakran használják az e-mailes kommunikáció biztonságának növelésére.

Az aszimmetrikus algoritmusok lényegesen lassabbak, mint a szimmetrikus algoritmusok. Tervezésük számítási problémákon alapul, mint például rendkívül nagy számok faktorálása vagy rendkívül nagy számok diszkrét logaritmusainak kiszámítása.

Mivel lassúak, az aszimmetrikus algoritmusokat jellemzően kis volumenű kriptográfiai mechanizmusokban használják, mint például a digitális aláírások és a kulcscsere. Az aszimmetrikus algoritmusok kulcskezelése azonban általában egyszerűbb, mint a szimmetrikus algoritmusoké, mivel általában a két titkosító vagy visszafejtő kulcs közül az egyik nyilvánossá tehető.

Az aszimmetrikus titkosítási algoritmusok gyakori példái a táblázatban találhatók.

| **Aszimmetrikus titkosítási algoritmus** | **Kulcs hossza** | **Leírás** |
| --- | --- | --- |
| **Diffie-Hellman (DH)** | 512, 1024, 2048, 3072, 4096 | A Diffie-Hellman algoritmus lehetővé teszi, hogy két fél megállapodjon egy kulcsban, amellyel titkosíthatják az egymásnak elküldeni kívánt üzeneteket. Ennek az algoritmusnak a biztonsága attól a feltételezéstől függ, hogy könnyű egy számot egy bizonyos hatványra emelni, de nehéz kiszámítani, hogy a szám és az eredmény alapján melyik hatványt használtuk. |
| **Digital Signature Standard (DSS) és Digital Signature Algorithm (DSA)** | 512 - 1024 | A DSS a DSA-t határozza meg a digitális aláírások algoritmusaként. A DSA egy nyilvános kulcsú algoritmus, amely az ElGamal aláírási sémán alapul. Az aláírás-létrehozási sebesség hasonló az RSA-hoz, de az ellenőrzéshez 10-40-szer lassabb. |
| **Rivest, Shamir és Adleman titkosítási algoritmusok (RSA)** | 512-től 2048-ig | Az RSA a nyilvános kulcsú kriptográfiára szolgál, amely a nagyon nagy számok faktorálásának jelenlegi nehézségén alapul. Ez az első olyan algoritmus, amelyről ismert, hogy alkalmas aláírásra, valamint titkosításra. Széles körben használják az elektronikus kereskedelmi protokollokban, és biztonságosnak tartják, ha kellően hosszú kulcsokat és naprakész implementációkat használnak. |
| **EIGamal** | 512 - 1024 | Egy aszimmetrikus kulcsú titkosítási algoritmus nyilvános kulcsú titkosításhoz, amely a Diffie-Hellman kulcsmegállapodáson alapul. Az ElGamal rendszer hátránya, hogy a titkosított üzenet nagyon nagy, körülbelül kétszer akkora lesz, mint az eredeti üzenet, ezért csak kis üzenetekhez, például titkos kulcsokhoz használják. |
| **Elliptikus görbe technikák** | 224 vagy magasabb | Az elliptikus görbe kriptográfiája számos kriptográfiai algoritmus, például Diffie-Hellman vagy ElGamal adaptálására használható. Az elliptikus görbe titkosításának fő előnye, hogy a kulcsok sokkal kisebbek lehetnek. |

16.3.4

## Aszimmetrikus titkosítás – Titoktartás

Aszimmetrikus algoritmusokat használnak a titkosság biztosítására a jelszó előzetes megosztása nélkül. Az aszimmetrikus algoritmusok titoktartási célja akkor indul el, amikor a titkosítási folyamatot a nyilvános kulccsal elindítják.

A folyamat a következő képlettel foglalható össze:

**Nyilvános kulcs (titkosítás) + Privát kulcs (Decrypt) = Titoktartás**

Amikor a nyilvános kulcsot használják az adatok titkosításához, a privát kulcsot kell használni az adatok visszafejtéséhez. Csak egy gazdagép rendelkezik privát kulccsal; ezért a titoktartás megvalósul.

Ha a magánkulcs sérül, egy másik kulcspárt kell létrehozni a feltört kulcs helyett.

Kattintson a gombokra, ha meg szeretné tekinteni, hogyan használhatók a privát és nyilvános kulcsok a Bob és Alice közötti adatcsere titkosságára.

Alice kéri és megszerzi Bob nyilvános kulcsát.

Az ábrán a bal oldalon az alice számítógép, a jobb oldalon pedig a bob számítógép látható. A bob számítógép bal oldalán van egy kulcs a Bob nyilvános kulcsa szavakkal. Egy nyíl megy az alice pc-ről a bob pc-re a következő szavakkal: kérhetem a nyilvános kulcsát? Egy másik sor egy nyíllal, amely a bobtól az alice-ig megy, és az itt található szavakkal az én nyilvános kulcsom. Alul: nyilvános kulcs (titkosítás) + privát kulcs (dekódolás) = titkosság.

Nyilvános kulcs (titkosítás) + Privát kulcs (Dekódolás) = Titoktartás Kérhetem a nyilvános kulcsát? Itt van a nyilvános kulcsom. Alice Bob Bob nyilvános kulcsa

16.3.5

## Aszimmetrikus titkosítás – hitelesítés

Az aszimmetrikus algoritmusok hitelesítési célja akkor indul el, amikor a titkosítási folyamatot a titkos kulccsal elindítják.

A folyamat a következő képlettel foglalható össze:

**Privát kulcs (titkosítás) + Nyilvános kulcs (Decrypt) = hitelesítés**

Amikor a privát kulcsot használják az adatok titkosításához, a megfelelő nyilvános kulcsot kell használni az adatok visszafejtéséhez. Mivel csak egy gazdagép rendelkezik a privát kulccsal, csak ez a gazdagép tudta titkosítani az üzenetet, biztosítva a feladó hitelesítését. Általában nem tesznek kísérletet a nyilvános kulcs titkosságának megőrzésére, így tetszőleges számú gazdagép tudja visszafejteni az üzenetet. Amikor egy gazdagép sikeresen visszafejt egy üzenetet nyilvános kulccsal, akkor megbízható, hogy a privát kulcs titkosította az üzenetet, ami ellenőrzi, hogy ki a feladó. Ez a hitelesítés egy formája.

Kattintson a gombokra, ha meg szeretné tekinteni, hogyan használhatók a privát és nyilvános kulcsok a Bob és Alice közötti adatcsere hitelesítésére.

Alice titkosítja az üzenetet a privát kulcsával. Alice elküldi a titkosított üzenetet Bobnak. Bobnak igazolnia kell, hogy az üzenet valóban Alice-től érkezett.

Az ábrán az alice számítógép látható, mellette egy tanúsítvány, egy pluszjel és egy Alice privát kulcsa feliratú kulccsal, egy nyíllal, amely egy titkosítási algoritmus feliratú tölcsérbe megy. Egy nyíl jön ki a tölcsérből egy szövegdobozba, amely titkosított szöveget olvas. Alul a privát kulcs (titkosítás) + nyilvános kulcs (dekódolás) = hitelesítés szavak találhatók.

+

Titkosított szöveg Alice privát kulcsának titkosítási algoritmusa Privát kulcs (titkosítás) + Nyilvános kulcs (Dekódolás) = Alice hitelesítés

16.3.6

## Aszimmetrikus titkosítás – Integritás

A két aszimmetrikus titkosítási folyamat kombinálása biztosítja az üzenetek bizalmas kezelését, hitelesítését és integritását.

A következő példa a folyamat illusztrálására szolgál. Ebben a példában az üzenet Bob nyilvános kulcsával lesz titkosítva, a titkosított hash pedig Alice privát kulcsával lesz titkosítva a titkosság, hitelesség és integritás biztosítása érdekében.

Alice üzenetet akar küldeni Bobnak, hogy csak Bob tudja elolvasni a dokumentumot. Más szóval, Alice biztosítani akarja az üzenetek bizalmas kezelését. Alice Bob nyilvános kulcsát használja az üzenet titkosításához. Csak Bob tudja megfejteni a privát kulcsával.

Az ábrán az alice számítógép látható, mellette egy egyszerű szöveges papírlappal, egy pluszjellel és egy Bob nyilvános kulcsa feliratú kulccsal, amely egy nyíllal megy a titkosítási algoritmus tölcsérbe. Egy nyíl megy ki a tölcsérből egy szövegdobozba, amely titkosított szöveget olvas.

+

Titkosított szöveg Bob nyilvános kulcsú titkosítási algoritmusa, Alice Plaintext

16.3.7

## Diffie-Hellman

A Diffie-Hellman (DH) egy aszimmetrikus matematikai algoritmus, amely lehetővé teszi két számítógép számára, hogy azonos megosztott titkot generáljanak anélkül, hogy korábban kommunikáltak volna. Az új megosztott kulcsot valójában soha nem cserélik ki a küldő és a fogadó között. Mivel azonban mindkét fél ismeri, a kulcsot egy titkosító algoritmus használhatja a két rendszer közötti forgalom titkosításához.

Íme két példa a DH általános használatára:

* Az adatok cseréje IPsec VPN segítségével történik
* SSH adatok cseréje történik

A DH működésének szemléltetéséhez lásd az ábrát.

Az ábra szemlélteti, hogyan működik a Diffie-Hellman algoritmus színek használatával. Tegyük fel, hogy Alice és Bob megállapodott abban, hogy 50 milliliter (50 ml) sárga festékkel kezdenek. Alice 50 ml vörös festéket ad a sárga festékhez, így 100 ml narancssárga festéket készít. Bob összekeveri 50 ml sárga festékét 50 ml kék festékkel, így 100 ml zöld festéket hoz létre. Alice küld Bobnak 100 ml narancssárga festéket, Bob pedig a 100 ml zöld színű festéket. Alice ezután további 50 ml vörös festéket ad Bob 100 ml zöld festékéhez, így 150 ml barna festéket készít. Bob további 50 ml kék festéket kever 100 ml Alice narancssárga festékhez, így 150 ml pontosan ugyanolyan színű barna színű festéket készít, mint amit Alice készített.

+ + = = + + =

=

Megállapodtunk Color Alice titkos színéről Alice nyilvános színéről Bob nyilvános színéről Alice titkos színéről Alice végső színéről Alice Megállapodott a Color Bob titkos színéről Bob nyilvános színéről Alice nyilvános színéről Bob titkos színéről Bob végső színéről Bob

A DH-kulcs-egyeztetési folyamat leegyszerűsítése érdekében az ábrán látható színeket használjuk az összetett hosszú számok helyett. A DH kulcscsere azzal kezdődik, hogy Alice és Bob megegyeznek egy tetszőleges közös színben, amelyet nem kell titokban tartani. A példánkban elfogadott szín a sárga.

Ezután Alice és Bob kiválaszt egy titkos színt. Alice a pirosat választotta, míg Bob a kéket. Ezeket a titkos színeket soha senkivel nem osztjuk meg. A titkos szín az egyes felek titkos titkos kulcsát jelenti.

Alice és Bob most összekeverik a közös színt (sárgát) a megfelelő titkos színükkel, hogy nyilvános színt hozzanak létre. Ezért Alice összekeveri a sárgát a piros színével, hogy nyilvános narancssárgát hozzon létre. Bob összekeveri a sárgát és a kéket, hogy nyilvános zöld színt hozzon létre.

Alice elküldi a nyilvános színét (narancs) Bobnak, Bob pedig a nyilvános színét (zöld) Alice-nek.

Alice és Bob mindegyike keveri a kapott színt a saját, eredeti titkos színével (Alice piros és Bob kék). Az eredmény egy végső barna színkeverék, amely megegyezik a partner végső színkeverékével. A barna szín a Bob és Alice közötti közös titkos kulcsot jelöli.

A DH biztonsága azon alapul, hogy nagyon nagy számokat használ a számításaiban. Például egy DH 1024 bites szám nagyjából megegyezik egy 309 számjegyből álló decimális számmal. Figyelembe véve, hogy egy milliárd 10 tizedesjegyű (1 000 000 000), könnyen elképzelhető, milyen bonyolult nem egy, hanem több 309 jegyű decimális számmal dolgozni.

A Diffie-Hellman különböző DH csoportokat használ a kulcsmegállapodási folyamatban használt kulcs erősségének meghatározására. A magasabb csoportszámok biztonságosabbak, de a kulcs kiszámításához több időre van szükség. A következők azonosítják a Cisco IOS Software által támogatott DH-csoportokat és a hozzájuk tartozó prímszámértéket:

* DH 1. csoport: 768 bit
* DH 2. csoport: 1024 bit
* DH 5. csoport: 1536 bit
* DH csoport 14: 2048 bit
* DH csoport 15: 3072 bit
* DH 16. csoport: 4096 bit

**Megjegyzés** : A DH-kulcs-megállapodás alapulhat elliptikus görbe kriptográfián is. A 19., 20. és 24. DH csoportokat, amelyek elliptikus görbe kriptográfián alapulnak, a Cisco IOS Software is támogatja.

Sajnos az aszimmetrikus kulcsrendszerek rendkívül lassúak bármilyen tömeges titkosításhoz. Ezért gyakori, hogy a forgalom nagy részét szimmetrikus algoritmussal, például 3DES vagy AES segítségével titkosítják, és a DH algoritmust használják a titkosítási algoritmus által használt kulcsok létrehozására.

16.3.8

## Videó - Kriptográfia

16.3.9

## Ellenőrizze, hogy megértette-e a titkosítási algoritmusok osztályozását

Az űrlap teteje

1. Igaz vagy hamis? Az aszimmetrikus titkosításban a titkosítás és a visszafejtés ugyanazt a kulcsot használja.

Az űrlap alja

Mi a példa szimmetrikus titkosítási algoritmusra?

Melyik algoritmus biztosít aszimmetrikus titkosítást?

Melyik hash funkció a legbiztonságosabb?

16.3.10

## Lab – Adatok titkosítása és visszafejtése OpenSSL használatával

Ebben a laborban a következő célokat kell teljesítenie:

* Üzenetek titkosítása OpenSSL-lel
* Üzenetek visszafejtése OpenSSL-lel

16.3.11

## Lab – Adatok titkosítása és visszafejtése hacker eszközzel

Ebben a laborban a következő célokat kell teljesítenie:

* Beállítási forgatókönyv
* Fájlok létrehozása és titkosítása
* Helyezze vissza a titkosított ZIP-fájlok jelszavait

16.3.12

## Lab - Telnet és SSH vizsgálata Wiresharkban

Ebben a laborban a következő célokat kell teljesítenie:

* Vizsgáljon meg egy Telnet munkamenetet a Wireshark segítségével
* Vizsgáljon meg egy SSH-munkamenetet a Wireshark segítségével

[16.2](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Key Management](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[16.4](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Basic Integrity and Authenticity Summary](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                     

1. Basic Integrity and Authenticity
2. Basic Integrity and Authenticity Summary

# Az alapvető integritás és hitelesség összefoglalása

16.4.1

## Mit tanultam ebben a modulban?

**Integritás és hitelesség**   
Ez a biztonságos kommunikáció négy eleme: adatintegritás, eredet-hitelesítés, adatok bizalmas kezelése és az adatok letagadhatatlansága. A kriptográfia szinte bárhol használható, ahol van adatkommunikáció. Kivonatokat használnak az adatok integritásának ellenőrzésére és biztosítására. A kivonatolás egy egyirányú matematikai függvényen alapul, amely viszonylag könnyen kiszámítható, de lényegesen nehezebb visszafordítani. A kriptográfiai hash funkció a hitelesítés ellenőrzésére is használható. A hash függvény egy változó bináris adatblokkot vesz fel, amelyet üzenetnek neveznek, és egy rögzített hosszúságú, tömörített reprezentációt állít elő, amelyet hash-nek neveznek. Az eredményül kapott hash-t néha üzenetkivonatnak, kivonatnak vagy digitális ujjlenyomatnak is nevezik. Matematikailag a **h= H(x)** egyenlet arra szolgál, hogy megmagyarázza, hogyan működik egy hash algoritmus. hash függvény **A H** bemenetet vesz **egy x** , és egy fix méretű karakterlánc **h** hash értéket ad vissza . A kriptográfiai hash függvénynek a következő tulajdonságokkal kell rendelkeznie:

• A bemenet bármilyen hosszúságú lehet.   
• A kimenet fix hosszúságú.   
• **H(x)** viszonylag könnyen kiszámítható bármely adott **x** esetén .   
• **H(x)** egyirányú és nem visszafordítható.   
• **A H(x)** ütközésmentes, ami azt jelenti, hogy két különböző bemeneti érték eltérő hash-értéket eredményez.

A négy jól ismert hash-függvény az MD5 128 bites kivonattal, az SHA-1, az SHA-2 és az SHA-3. Míg a kivonat felhasználható a véletlen változtatások észlelésére, nem lehet arra használni, hogy megvédje magát azon szándékos változtatásoktól, amelyeket a fenyegetés szereplői hajtanak végre egy ember a közepén támadás során. Származási hitelesítés is szükséges a védelem biztosításához.

Eredeti hitelesítés és integritásbiztosítás hozzáadásához használjon kulcsos hash üzenet-hitelesítési kódot (HMAC). A HMAC egy további titkos kulcsot használ a hash függvény bemeneteként. Más üzenet hitelesítési kód (MAC) módszerek is használatosak. A HMAC-ot azonban számos rendszer használja, beleértve az SSL-t, az IPsec-et és az SSH-t.

**Kulcskezelés**   
A kulcskezelést gyakran a kriptorendszer tervezésének legnehezebb részének tekintik. A kriptográfiai rendszerek elleni támadások többsége a kulcskezelési szintre irányul, nem pedig magára a kriptográfiai algoritmusra. A kulcskezelés alapvető jellemzői a kulcsgenerálás, a kulcsellenőrzés, a kulcscsere, a kulcstárolás, a kulcsok élettartama, valamint a kulcsok visszavonása és megsemmisítése. A billentyűk leírására használt két kifejezés a kulcshossz és a billentyűtér. A kulcshossz növekedésével a kulcstér exponenciálisan növekszik. Egy algoritmus kulcstere az összes lehetséges kulcsérték halmaza. Az n bites kulcs 2^n lehetséges kulcsértékkel rendelkező kulcsteret hoz létre. Egy bit hozzáadásával a kulcshoz a kulcstér gyakorlatilag megduplázódik. Szinte minden algoritmusnak van néhány gyenge kulcsa a kulcsterében, amelyek lehetővé teszik a támadó számára, hogy egy parancsikon segítségével megtörje a titkosítást. A gyenge kulcsok a titkosítás szabályszerűségeit mutatják. A létrehozható kriptográfiai kulcsok többféle típusa közé tartoznak a szimmetrikus kulcsok, az aszimmetrikus kulcsok, a digitális aláírások és a hash kulcsok. A modern, megbízható algoritmusokkal a védelem erőssége kizárólag a kulcs méretétől függ. A kulcs hosszát úgy válassza meg, hogy az megfelelő ideig védje az adatok bizalmasságát vagy integritását. Az érzékenyebb és tovább titokban tartandó adatoknak hosszabb kulcsokat kell használniuk. A teljesítmény egy másik kérdés, amely befolyásolhatja a kulcshossz kiválasztását. Az adminisztrátornak jó egyensúlyt kell találnia az algoritmusok sebessége és védelmi erőssége között, mert egyes algoritmusok, például a Rivest, Shamir és Adleman (RSA) algoritmusok lassan futnak a nagy kulcshosszok miatt.

**Titoktartás**   
Az adatok titkosságának biztosítására két titkosítási osztályt használnak: aszimmetrikus és szimmetrikus titkosítást. Ez a két osztály a kulcsok használatában különbözik. A szimmetrikus titkosítási algoritmusok, mint például a Data Encryption Standard (DES), a 3DES és az Advanced Encryption Standard (AES) azon a feltevésen alapulnak, hogy minden kommunikáló fél ismeri az előre megosztott kulcsot. Az adatok bizalmas kezelése aszimmetrikus algoritmusokkal is biztosítható, beleértve a Rivest, Shamir és Adleman (RSA) és a nyilvános kulcsú infrastruktúrát (PKI). A szimmetrikus algoritmusok ugyanazt az előre megosztott kulcsot használják az adatok titkosításához és visszafejtéséhez. Az előre megosztott kulcsot, más néven titkos kulcsot, a küldő és a fogadó ismeri, mielőtt bármilyen titkosított kommunikációra sor kerülhetne. A szimmetrikus titkosítási algoritmusokat gyakran használják a VPN-forgalomhoz, mivel a szimmetrikus algoritmusok kevesebb CPU-erőforrást használnak, mint az aszimmetrikus titkosítási algoritmusok. A titkosítás biztonságosságának biztosítása érdekében legalább 128 bites kulcshosszt kell használni. Használjon hosszabb kulcsot a biztonságosabb kommunikáció érdekében. A szimmetrikus titkosítási algoritmusokat néha blokk-rejtjelként vagy adatfolyam-rejtjelként osztályozzák. A blokkrejtjelek egy fix hosszúságú nyílt szövegblokkot alakítanak át egy közös, 64 vagy 128 bites titkosított szöveg blokkká. Az adatfolyam-titkosítók egy bájton vagy egy bitenként titkosítják a nyílt szöveget. Az adatfolyam-rejtjelek alapvetően egy blokk-rejtjelek, amelyek blokkmérete egy bájt vagy bit. Az adatfolyam-rejtjelek általában gyorsabbak, mint a blokkos titkosítások, mivel az adatok folyamatosan titkosítva vannak. Az aszimmetrikus algoritmusokat, amelyeket nyilvános kulcsú algoritmusoknak is neveznek, úgy tervezték, hogy a titkosításhoz használt kulcs eltérjen a visszafejtéshez használt kulcstól. Az aszimmetrikus titkosítás 512 és 4096 bit közötti kulcshosszúságot használhat. A 2048 bitnél nagyobb vagy azzal egyenlő kulcshosszúságok megbízhatóak, míg az 1024 vagy annál rövidebb kulcsok nem tekinthetők elegendőnek. Az aszimmetrikus kulcsalgoritmusokat használó protokollok például az Internet Key Exchange (IKE), a Secure Socket Layer (SSL), a Secure Shell (SSH) és a Pretty Good Privacy (PGP) protokollok. A folyamat a következő képlettel foglalható össze: Privát kulcs (titkosítás) + Nyilvános kulcs (Dekódolás) = Hitelesítés. A Diffie-Hellman (DH) egy aszimmetrikus matematikai algoritmus, amely lehetővé teszi két számítógép számára, hogy azonos megosztott titkot generáljanak anélkül, hogy korábban kommunikáltak volna. Az új megosztott kulcsot valójában soha nem cserélik ki a küldő és a fogadó között. A DH-t általában IPsec VPN és SSH adatcsere esetén használják.

16.4.2

## 16. modul – Alapvető integritás és hitelesség kvíz

Az űrlap teteje

1. Melyik biztonsági funkciót biztosítják a titkosítási algoritmusok?

Az űrlap alja

Milyen típusú kriptográfiai kulcsot használnak a biztonságos webhelyhez való csatlakozáskor?

Mire céloz a legtöbb kriptográfiai rendszertámadás?

Milyen típusú támadások ellen véd a HMAC-k használata?

Mi az aszimmetrikus titkosítás jellemzője?

Mi az oka annak, hogy a HMAC további titkos kulcsot használ a hash függvény bemeneteként?

Mi a DH algoritmus célja?

Melyik állítás írja le a Szoftver – optimalizált titkosítási algoritmust (SEAL)?

Melyik adatbiztonsági összetevőt biztosítják a kivonatoló algoritmusok?

Melyik két algoritmus használ hash-függvényt az üzenet integritásának biztosítására? (Válassz kettőt.)

A biztonsági kulcskezelés mely jellemzői felelősek azért, hogy biztosítsák, hogy ne használjanak gyenge kriptográfiai kulcsokat?

Mi a funkciója a Diffie - Hellman algoritmusnak az IPsec keretrendszeren belül?

[16.3](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Confidentiality](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[17.0](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                     
*         

1. Public Key Cryptography
2. Introduction

# Bevezetés

17.0.1

## Miért vegyem ezt a modult?

Hogyan biztosíthatjuk a kommunikációt olyan webhelyek között, amelyekkel soha nem kommunikáltunk? Honnan tudhatjuk, hogy a most letöltött szoftver legitim, és nem manipulálta harmadik fél bűnszervezet?

A válasz a digitális aláírások használatával a digitális tanúsítványok biztosítására és a kódaláírásra. A digitális aláírások kezelése és terjesztése a nyilvános kulcsú infrastruktúra (PKI) segítségével történik.

Ebben a modulban megismerheti a digitális aláírásokat, valamint azt, hogyan használják a PKI-t az adatok titkosságának biztosítására és a hitelesítés biztosítására.

17.0.2

## Mit fogok tanulni ebben a modulban?

**Modul címe:** Nyilvános kulcsú kriptográfia

**A modul célja** : Ismertesse meg, hogyan használják a nyilvános kulcsú infrastruktúrát az adatok titkosságának és hitelesítésének biztosítására.

| **téma címe** | **Téma Cél** |
| --- | --- |
| **Nyilvános kulcsú kriptográfia digitális aláírással** | Magyarázza el a nyilvános kulcsú kriptográfiát. |
| **A hatóságok és a PKI Trust System** | Magyarázza el, hogyan működik a nyilvános kulcsú infrastruktúra. |
| **A kriptográfia alkalmazásai és hatásai** | Magyarázza el, hogy a kriptográfia használata hogyan befolyásolja a kiberbiztonsági műveleteket. |

[16.4](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Basic Integrity and Authenticity Summary](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[17.1](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Public Key Cryptography with Digital Signatures](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                      
*         

1. Public Key Cryptography
2. Public Key Cryptography with Digital Signatures

# Nyilvános kulcsú kriptográfia digitális aláírással

17.1.1

## A digitális aláírás áttekintése

A digitális aláírás egy matematikai technika, amelyet a hitelesség, az integritás és a letagadhatatlanság biztosítására használnak. A digitális aláírások speciális tulajdonságokkal rendelkeznek, amelyek lehetővé teszik az entitás hitelesítését és az adatok integritását. Ezenkívül a digitális aláírások biztosítják a tranzakció letagadását. Vagyis a digitális aláírás jogi bizonyítékként szolgál arra, hogy az adatcsere megtörtént. A digitális aláírások aszimmetrikus kriptográfiát használnak.

Kattintson a gombokra a digitális aláírás tulajdonságainak felfedezéséhez.

Az aláírás nem hamisítható, és bizonyítja, hogy az aláíró, és senki más nem írta alá a dokumentumot.

A digitális aláírásokat általában a következő két helyzetben használják:

1. **Kód-aláírás** – Adatintegritási és hitelesítési célokra használják. A kódaláírást a szállító webhelyéről letöltött végrehajtható fájlok integritásának ellenőrzésére használják. Aláírt digitális tanúsítványokat is használ a fájlok forrásaként szolgáló webhely hitelesítésére és identitásának ellenőrzésére.
2. **Digitális tanúsítványok** – Ezek hasonlóak a virtuális személyazonosító kártyához, és a rendszer azonosságának hitelesítésére szolgálnak a szállító webhelyével, valamint titkosított kapcsolat létrehozására a bizalmas adatok cseréjéhez.

Három digitális aláírás szabványos (DSS) algoritmus használható a digitális aláírások generálására és ellenőrzésére:

* **Digitális aláírási algoritmus (DSA)** – A DSA az eredeti szabvány a nyilvános és privát kulcspárok generálására, valamint a digitális aláírások generálására és ellenőrzésére.
* **Rivest-Shamir Adelman algoritmus (RSA)** – Az RSA egy aszimmetrikus algoritmus, amelyet általában digitális aláírások generálására és ellenőrzésére használnak.
* **Elliptikus görbe digitális aláírási algoritmus (ECDSA)** – Az ECDSA a DSA egy újabb változata, amely digitális aláírás hitelesítést és letagadhatatlanságot biztosít a számítási hatékonyság, a kis aláírásméret és a minimális sávszélesség további előnyeivel.

Az 1990-es években az RSA Security Inc. megkezdte a nyilvános kulcsú titkosítási szabványok (PKCS) közzétételét. 15 PKCS volt, bár 1 már visszavonásra került a jelen írás időpontjában. Az RSA azért tette közzé ezeket a szabványokat, mert rendelkeztek a szabványokkal kapcsolatos szabadalmakkal, és népszerűsíteni akarták azokat. A PKCS nem ipari szabvány, de jól elismert a biztonsági iparban, és a közelmúltban kezdtek fontossá válni az olyan szabványügyi szervezetek számára, mint az IETF és a PKIX munkacsoport.

17.1.2

## Digitális aláírások kódaláíráshoz

A digitális aláírásokat általában a szoftverkód hitelességének és integritásának biztosítására használják. A végrehajtható fájlok digitálisan aláírt borítékba vannak csomagolva, amely lehetővé teszi a végfelhasználó számára az aláírás ellenőrzését a szoftver telepítése előtt.

A digitális aláíró kód számos biztosítékot nyújt a kóddal kapcsolatban:

* A kód hiteles, és valójában a kiadótól származik.
* A kódot nem módosították, mióta elhagyta a szoftver kiadóját.
* A kiadó tagadhatatlanul közzétette a kódot. Ez biztosítja a közzététel cselekményének visszautasítását.

Az Egyesült Államok kormányának szövetségi információfeldolgozási szabványának (FIPS) 140-3. számú kiadványa előírja, hogy az internetről letölthető szoftvereket digitálisan alá kell írni és ellenőrizni kell. A digitálisan aláírt szoftver célja annak biztosítása, hogy a szoftvert nem manipulálták, és az a megbízható forrásból származik, ahogy azt állítják. A digitális aláírások annak ellenőrzésére szolgálnak, hogy a kódot nem manipulálták-e fenyegetés szereplői, és nem illesztettek-e be rosszindulatú kódot a fájlba harmadik fél.

Click the buttons to access the properties of a file that has a digitally signed certificate.

This executable file was downloaded from the internet. The file contains a software tool from Cisco Systems.



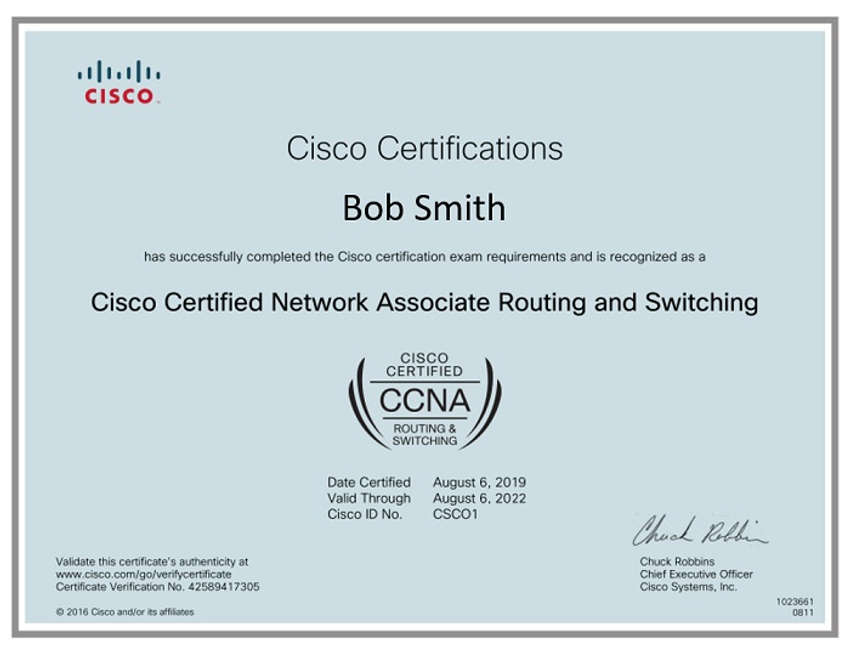
17.1.3

## Digitális aláírások digitális tanúsítványokhoz

A digitális tanúsítvány egyenértékű az elektronikus útlevéllel. Lehetővé teszi a felhasználók, a gazdagépek és a szervezetek számára, hogy biztonságosan cseréljenek információkat az interneten keresztül. Pontosabban, digitális tanúsítványt használnak annak hitelesítésére és ellenőrzésére, hogy az üzenetet küldő felhasználó az, akiről azt állítják, hogy ő maga. A digitális tanúsítványok arra is használhatók, hogy bizalmas kezelést biztosítsanak a fogadó számára a válasz titkosításának eszközeivel.

A digitális tanúsítványok hasonlóak a fizikai tanúsítványokhoz. Például az ábrán látható papíralapú Cisco Certified Network Associate Security (CCNA-S) tanúsítvány azonosítja, hogy kinek adták ki a tanúsítványt, ki engedélyezte a tanúsítványt, és mennyi ideig érvényes a tanúsítvány. A digitális tanúsítványok is hasonló információkat szolgáltatnak.

Az ábra egy példát mutat a CCNA-tanúsítványra, amely rámutat, hogy kinek adták ki, Bob Smithnek, a lejárati dátumra, 2022. augusztus 6-ára, valamint a tanúsító hatóságra, Chuck Robbinsra.



Lejárati dátum A tanúsító hatóság kiállítva:

A digitális tanúsítvány függetlenül ellenőrzi a személyazonosságot. A digitális aláírásokat annak ellenőrzésére használják, hogy egy műterméket, például fájlt vagy üzenetet küldtek-e az ellenőrzött személy. Más szóval, a tanúsítvány igazolja a személyazonosságot, az aláírás pedig azt, hogy valami származik ebből az azonosságból.

Ez a forgatókönyv segít megérteni a digitális aláírás használatának módját. Bob rendelést erősít meg Alice-szel. Alice Bob weboldaláról rendel. Alice csatlakozott Bob webhelyéhez, és miután a tanúsítványt ellenőrizték, Bob tanúsítványa Alice webhelyén tárolódik. A tanúsítvány tartalmazza Bob nyilvános kulcsát. A nyilvános kulcsot Bob digitális aláírásának ellenőrzésére használják.

Tekintse meg az ábrát a digitális aláírás használatának megtekintéséhez.

Az ábrán a bob-számítógép látható egy szövegdobozsal, amelyen a rendelés megerősítése és a felette lévő adatszó olvasható. Egy nyíl egy másik szövegdobozhoz nyúlik, amelyen 1c34d56 olvasható... Egy nyíl egy másik szövegdobozhoz vezet, amelyen 0a77b3440 olvasható... és a nyíl mellett a „titkosít” szavak egy bob privát kulcs feliratú kulcs képével. A harmadik nyíl a 0a szövegmezőből egy felhőbe megy, amelyben az aláírt adatok szavak szerepelnek, és egy doboz, amely a rendelés aláírásának megerősítése 0a77b3440 feliratot tartalmazza... Szavak az alján: Bob megerősíti a rendelést, és a számítógépe elkészíti a megerősítés kivonatát. A számítógép Bob privát kulcsával titkosítja a hash-t. A titkosított hash, amely a digitális aláírás, hozzá van fűzve a dokumentumhoz. A megrendelés visszaigazolását ezután elküldik Alice-nek az interneten keresztül.

1 2

3

Bob Data Private Key Encrypt Hash Bob Rendelés megerősítése 1c34d56… 0a77b3440… megerősítése Megrendelés aláírásának   
---------   
0a77b3440… Aláírt adatok

Bob megerősíti a rendelést, és számítógépe elkészíti a visszaigazolás kivonatát. A számítógép Bob privát kulcsával titkosítja a hash-t. A titkosított hash, amely a digitális aláírás, hozzá van fűzve a dokumentumhoz. A megrendelés visszaigazolását ezután elküldik Alice-nek az interneten keresztül.

Amikor Alice megkapja a digitális aláírást, a következő folyamat történik.

Az ábra ugyanazt a felhőt mutatja aláírt adatokkal és rendelés megerősítésével, mint az utolsó ábra egy bekarikázott számmal, amelyen Bob nyilvános kulcs és dekódolás van, egy hash és egy aláírás ellenőrzött dobozok, amelyek az alice számítógéphez vezetnek.

= 2 3

1

Megrendelés megerősítése 1c34d56… 1c34d56… Aláírás   
---------   
0a77b3440… Nyilvános kulcs Aláírás visszafejtése Ellenőrizve Alice Hash Bob megerősítése Megrendelés aláírásának   
---------   
0a77b3440… Aláírt adatok

1. Alice vevőkészüléke elfogadja a rendelés visszaigazolását a digitális aláírással, és megkapja Bob nyilvános kulcsát.
2. Alice számítógépe ezután Bob nyilvános kulcsával visszafejti az aláírást. Ez a lépés felfedi a küldő eszköz feltételezett hash értékét.
3. Alice számítógépe létrehoz egy kivonatot a fogadott dokumentumról, annak aláírása nélkül, és ezt összehasonlítja a dekódolt aláírás-kivonattal. Ha a hash-ek egyeznek, a dokumentum hiteles. Ez azt jelenti, hogy a visszaigazolást Bob küldte, és az aláírása óta nem változott.

[17.0](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[17.2](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Authorities and the PKI Trust System](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                           
*         

1. Public Key Cryptography
2. Authorities and the PKI Trust System

# A hatóságok és a PKI Trust System

17.2.1

## Nyilvános kulcs kezelése

Az internetes forgalom két fél közötti forgalomból áll. Amikor aszimmetrikus kapcsolatot hozunk létre két gazdagép között, a gazdagépek kicserélik nyilvános kulcsú információikat.

Például az SSL-tanúsítvány egy olyan digitális tanúsítvány, amely megerősíti egy webhely tartományának azonosságát. Az SSL webhelyén való megvalósításához SSL-tanúsítványt kell vásárolnia a domainhez egy SSL-tanúsítvány-szolgáltatótól. A megbízható harmadik fél alapos vizsgálatot végez a hitelesítő adatok kiadása előtt. E mélyreható vizsgálat után a harmadik fél nehezen hamisítható hitelesítő adatokat (azaz digitális tanúsítványt) bocsát ki. Ettől kezdve minden olyan személy, aki megbízik a harmadik félben, egyszerűen elfogadja a harmadik fél által kiadott hitelesítő adatokat.

Amikor a számítógépek HTTPS-en keresztül próbálnak csatlakozni egy webhelyhez, a webböngésző ellenőrzi a webhely biztonsági tanúsítványát, és ellenőrzi, hogy az érvényes-e, és egy megbízható tanúsító hatóságtól (CA) származik-e. Ez igazolja, hogy a webhely azonosítása igaz. A digitális tanúsítványt a webböngésző helyileg menti, majd felhasználja a további tranzakciókban. A webhely nyilvános kulcsát a tanúsítvány tartalmazza, és a webhely és az ügyfél közötti jövőbeni kommunikáció ellenőrzésére szolgál.

Az SSL-tanúsítvány-szolgáltató és a hitelesítésszolgáltatók megbízható harmadik felek, amelyek a kormányzati engedélyezési irodákhoz hasonló szolgáltatásokat nyújtanak.

Az ábrán Alice látható a bal oldalon. A jobb oldalon felül egy nagy középület, alatta pedig egy kisebb épület. Alice felől egy nyíl megy a legfelső épület felé, amelyen az a felirat szerepel, hogy allic kér jogosítványt. A jogosítványikonon egy nyíl látható, amely Alice-re mutat, és a személyazonosságának igazolása után kapja meg a jogosítványát. Egy másik sor az alice-től a kisebb épületig tart, az alice megpróbálja beváltani egy csekket. A pipa ikonnal ellátott jogosítványon van egy nyíl, amely az alice-hez vezet, és a következő szavakkal: személyazonossága elfogadásra került a jogosítvány ellenőrzése után.

Alice jogosítványt kér. Személyazonosságának bizonyítása után kapja meg a vezetői engedélyét. Alice megpróbál beváltani egy csekket. Személyazonosságát a jogosítvány ellenőrzése után fogadják el.

A nyilvános kulcsú infrastruktúra (PKI) specifikációkból, rendszerekből és eszközökből áll, amelyek digitális tanúsítványok létrehozására, kezelésére, terjesztésére, használatára, tárolására és visszavonására szolgálnak. A tanúsító hatóság (CA) egy olyan szervezet, amely digitális tanúsítványokat hoz létre úgy, hogy nyilvános kulcsot köt egy megerősített azonosításhoz, például egy webhelyhez vagy egy személyhez. A PKI egy bonyolult rendszer, amelyet arra terveztek, hogy megvédje a digitális identitást még a legkifinomultabb fenyegetés szereplői vagy nemzetállamok általi feltörésétől is.

Néhány példa a tanúsító hatóságokra: IdenTrust, DigiCert, Sectigo, GlobalSign és GoDaddy. Ezek a CA-k díjat számítanak fel szolgáltatásaikért. A Let's Encrypt egy non-profit CA, amely ingyenes tanúsítványokat kínál.

17.2.2

## A nyilvános kulcsú infrastruktúra

A PKI szükséges a nyilvános titkosítási kulcsok nagyszabású terjesztésének és azonosításának támogatásához. A PKI keretrendszer nagymértékben méretezhető bizalmi kapcsolatot tesz lehetővé.

A digitális tanúsítványok létrehozásához, kezeléséhez, tárolásához, terjesztéséhez és visszavonásához szükséges hardvereket, szoftvereket, személyeket, irányelveket és eljárásokat tartalmazza.

Az ábra a PKI főbb elemeit mutatja.

Az ábrán egy számítógépen lévő felhasználó látható, felette a PKI-tanúsítvány felirat és egy bekarikázott egyes szám. A számítógép mellett van egy bekarikázott 2-es szám a tanúsítványtároló szavakkal. A felhasználótól jobbra egy bekarikázott három középület ikon látható PKI tanúsító hatóság felirattal, ettől jobbra pedig egy négy és egy henger feliratú tanúsítvány adatbázis.

1 2 3

4

Tanúsítványtároló PKI-tanúsítvány PKI-tanúsítványszolgáltató tanúsítvány adatbázis

1. A PKI-tanúsítványok tartalmazzák egy entitás vagy egyén nyilvános kulcsát, annak célját, a tanúsítványt érvényesítő és kibocsátó tanúsító hatóságot (CA), azt a dátumtartományt, amelyen belül a tanúsítvány érvényes, és az aláírás létrehozásához használt algoritmust.
2. Az igazolástároló egy helyi számítógépen található, és a kiadott tanúsítványokat és privát kulcsokat tárolja.
3. A PKI-tanúsítvány (CA) egy megbízható harmadik fél, amely személyazonosságuk ellenőrzése után PKI-tanúsítványokat bocsát ki entitások és személyek számára. Ezeket a tanúsítványokat privát kulcsával írja alá.
4. A tanúsítvány adatbázis tárolja a CA által jóváhagyott összes tanúsítványt.

A következő ábra azt mutatja be, hogyan működnek együtt a PKI elemei:

* Ebben a példában Bob megkapta a digitális tanúsítványát a CA-tól. Ez a tanúsítvány minden alkalommal használatos, amikor Bob más felekkel kommunikál.
* Bob kommunikál Alice-szel.
* Amikor Alice megkapja Bob digitális tanúsítványát, kommunikál a megbízható CA-val, hogy ellenőrizze Bob személyazonosságát.

Az ábrán a jobb felső sarokban egy tanúsítvány adatbázis ikon látható, amely egy középületi ikonhoz köti a hitelesítési hatóság feliratú vonalat, és mellette a bekarikázott egyes szám a PKI tanúsítványt kiadja szavakkal. Egy nyíl egy Bob nevű számítógép-felhasználóhoz megy, aki mellett a bekarikázott kettes szám van, egy nyíl pedig az alice számítógép-felhasználóhoz vezet a PKI-tanúsítvány cseréje szavakkal. Az alice számítógép felett a PKI-tanúsítványt ellenőrzi szavak, egy bekarikázott 3-as szám és egy nyíl mutat vissza a tanúsító hatóságra.

1 2

3



Tanúsítványkibocsátó tanúsítvány adatbázis Bob Alice kicseréli a PKI-tanúsítványt , igazolja a PKI-tanúsítvány kiadásait, a PKI-tanúsítványt

1. **PKI-tanúsítványt állít ki** . Bob először tanúsítványt kér a CA-tól. A CA hitelesíti Bobot, és eltárolja Bob PKI-tanúsítványát a tanúsítvány-adatbázisban.
2. **Kicseréli a PKI-tanúsítványt** . Bob PKI-tanúsítványa segítségével kommunikál Alice-szel.
3. **Ellenőrzi a PKI-tanúsítványt** . Alice a megbízható CA nyilvános kulcsával kommunikál. A CA a tanúsítvány-adatbázisra hivatkozik Bob PKI-tanúsítványának érvényesítéséhez.

**Megjegyzés** : Nem minden PKI-tanúsítvány érkezik közvetlenül a CA-tól. A regisztrációs hatóság (RA) egy alárendelt CA, és egy gyökér CA tanúsítja, hogy meghatározott felhasználási célokra állítson ki tanúsítványokat.

17.2.3

## A PKI Hatósági Rendszer

Sok szállító felügyelt szolgáltatásként vagy végfelhasználói termékként kínál CA-kiszolgálókat. Néhány ilyen szállító többek között a Symantec Group (VeriSign), a Comodo, a Go Daddy Group, a GlobalSign és a DigiCert.

A szervezetek a magán PKI-ket Microsoft Server vagy Open SSL használatával is megvalósíthatják.

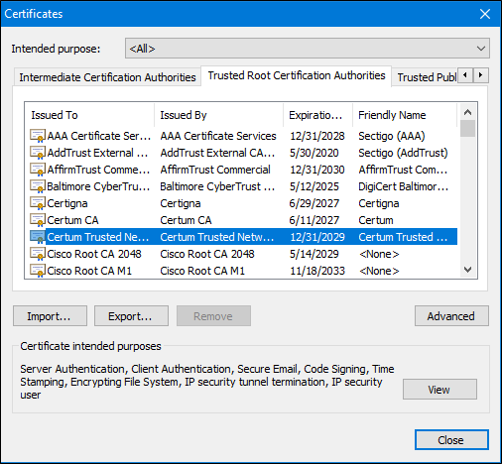
A hitelesítésszolgáltatók, különösen a kihelyezett tanúsítványok olyan osztályok alapján bocsátanak ki tanúsítványokat, amelyek meghatározzák a tanúsítvány megbízhatóságát.

A táblázat az osztályok leírását tartalmazza. A táblázat a VeriSign által meghatározott osztályok leírását tartalmazza. A digitális tanúsítványosztályokra nincs szabvány, ezért a CA-tól függően különböző osztályok léteznek. Más CA-k használhatnak három osztályú rendszert. Az osztályszámot az határozza meg, hogy a tanúsítvány kiállításakor mennyire volt szigorú az az eljárás, amely a birtokos személyazonosságát igazolta. Minél magasabb az osztályszám, annál megbízhatóbb a tanúsítvány. Ezért az 5. osztályú tanúsítványban sokkal jobban megbíznak, mint egy alacsonyabb osztályú tanúsítványban.

| **Osztály** | **Leírás** |
| --- | --- |
| 0 | Olyan helyzetekben történő tesztelésre használják, amikor nem végeztek ellenőrzést. |
| 1 | Olyan személyek használják, akiknek e-mail-címük ellenőrzésére van szükség. |
| 2 | Olyan szervezetek használják, amelyekhez személyazonosság igazolása szükséges. |
| 3 | Szerverekhez és szoftveraláírásokhoz használják. A személyazonosság és jogosultság független ellenőrzését és ellenőrzését a tanúsító hatóság végzi. |
| 4 | Vállalatok közötti online üzleti tranzakciókhoz használják. |
| 5 | Magánszervezetekhez vagy állami biztonsághoz használják. |

Például egy 1. osztályú tanúsítványhoz szükség lehet egy e-mail-válaszra a tulajdonostól, hogy megerősítse, hogy szeretne jelentkezni. Ez a fajta megerősítés a tulajdonos gyenge hitelesítését jelenti. 3. vagy 4. osztályú tanúsítvány esetén a leendő tulajdonosnak igazolnia kell személyazonosságát és hitelesítenie kell a nyilvános kulcsot legalább két hivatalos személyazonosító okmánnyal való személyes megjelenéssel.

Néhány CA nyilvános kulcs előre be van töltve, például a webböngészőkben felsoroltak. Az ábra a gazdagép tanúsítványtárolójában található különböző VeriSign-tanúsítványokat jeleníti meg. A listán szereplő CA-k bármelyike ​​által aláírt tanúsítványokat a böngésző legitimnek tekinti, és automatikusan megbízhatónak tekinti őket.



**Megjegyzés** : A vállalat belső használatra is megvalósíthatja a PKI-t. A PKI használható a hálózathoz csatlakozó alkalmazottak hitelesítésére. Ebben az esetben a vállalkozás a saját hitelesítésszolgáltatója.

17.2.4

## A PKI Trust System

A PKI-k különböző bizalmi topológiákat alkothatnak. A legegyszerűbb az egygyökér PKI topológia.

Amint az alábbi ábrán látható, egyetlen hitelesítésszolgáltató, az úgynevezett root CA, adja ki az összes tanúsítványt a végfelhasználóknak, amelyek általában ugyanazon a szervezeten belül vannak. Ennek a megközelítésnek az előnye az egyszerűsége. Nagy környezetre azonban nehéz méretezni, mert szigorúan központosított adminisztrációt igényel, ami egyetlen hibapontot teremt.

Az ábrán egy root ca feliratú szerver látható, mellette egy tanúsítvány. Két nyíl mutat egy számítógépre. minden számítógép mellett van egy tanúsítvány is.

### Egygyökér PKI topológia

Root CA

Nagyobb hálózatokon a PKI CA-k két alapvető architektúrával kapcsolhatók össze:

**Kereszthitelesítésű CA topológiák** – Amint az alábbi ábrán látható, ez egy peer-to-peer modell, amelyben az egyes CA-k bizalmi kapcsolatokat létesítenek más CA-kkal a CA-tanúsítványok kereszthitelesítésével. Bármelyik CA tartomány felhasználói is biztosak lehetnek abban, hogy megbízhatnak egymásban. Ez redundanciát biztosít, és kiküszöböli az egyszeri meghibásodást.

Az ábra ugyanazt a beállítást mutatja, mint az előző egygyökér pki topológia, de ez kb 1-es címkével van ellátva. Van egy kétirányú nyíl e topológia és egy másik, kb 2-es topológia között. Egy nyíl mutat a kb 2 topológiából. egy másik, azonos topológiájú, kb 3-as címkével.

### Cross Certified CA

CA1 CA2

CA3

**Hierarchikus CA topológiák** – Amint az alábbi ábrán látható, a legmagasabb szintű CA-t gyökér CA-nak nevezzük. Tanúsítványokat állíthat ki a végfelhasználóknak és egy alárendelt CA-nak. Az al-CA-k különféle üzleti egységek, tartományok vagy bizalmi közösségek támogatására hozhatók létre. A gyökér CA fenntartja a kialakult „bizalmi közösséget” azáltal, hogy biztosítja, hogy a hierarchia minden entitása megfeleljen a gyakorlatok minimális készletének. Ennek a topológiának az előnyei közé tartozik a megnövekedett méretezhetőség és kezelhetőség. Ez a topológia jól működik a legtöbb nagy szervezetben. Azonban nehéz lehet meghatározni az aláírási folyamat láncolatát.

A hierarchikus és a kereszttanúsítási topológia kombinálható hibrid infrastruktúra létrehozásához. Példa erre az, amikor két hierarchikus közösség kereszttanúsíthatja egymást annak érdekében, hogy az egyes közösségek tagjai megbízhassanak egymásban.

Az ábrán egy root ca feliratú szerver látható, mellette egy tanúsítvány. Két nyíl egy-egy alárendelt ca-ra mutat, mindegyik egygyökös pki topológiával.

### Hierarchikus CA

Root CA alárendelt CA

17.2.5

## Különböző PKI-szállítók együttműködési képessége

A PKI és a támogató szolgáltatások, például a Lightweight Directory Access Protocol (LDAP) és az X.500 címtárak közötti együttműködés aggodalomra ad okot, mert sok CA-szállító javasolt és vezetett be saját fejlesztésű megoldásokat, ahelyett, hogy a szabványok kidolgozására várna.

**Megjegyzés** : Az LDAP és az X.500 protokollok, amelyek a címtárszolgáltatások (például a Microsoft Active Directory) lekérdezésére szolgálnak a felhasználónév és jelszó ellenőrzésére.

Ennek az interoperabilitási aggálynak a megoldására az IETF közzétette az Internet X.509 nyilvános kulcsú infrastruktúra tanúsítási szabályzatát és hitelesítési gyakorlati keretrendszerét (RFC 2527). Az X.509 3. verzió (X.509 v3) szabvány határozza meg a digitális tanúsítvány formátumát.

Tekintse meg az ábrát az X.509 v3 formátum használatára az internet infrastruktúrájában.

Az ábrán egy külső webszerver látható, amely a bekarikázott 1-es számmal és SSL-lel van ellátva, és amely tűzfalhoz csatlakozik. A tűzfalnak van egy másik kapcsolata az alatta lévő VPN-koncentrátorral, amelyet bekarikázva 2-es számmal és az IP se c szavakkal jelöltek. A tűzfalnak van egy harmadik kapcsolata is egy felhő címkével ellátott internethez. A tűzfal egy másik kapcsolattal rendelkezik egy vállalati hálózati felhőhöz, amely tartalmaz egy CA-szervert, egy internetes levelezőszervert, amely mellett a bekarikázott 3-as szám és az S / MIME, valamint olyan szervereket, amelyek mellett a Cisco Secure ACS és a négyes számú EAP - TLS található. szavak mellette.

### X.509v3 alkalmazások

1 2 3

4

Internet Enterprise Network VPN Concentrator Külső webszerver Internet levelezőszerver Cisco Secure ACS CA kiszolgáló SSL S/MIME EAP-TLS IPsec

1. **SSL** – A biztonságos webszerverek X.509.v3-at használnak a webhely-hitelesítéshez az SSL- és TLS-protokollokban, míg a webböngészők X.509v3-at használnak a HTTPS-kliens-tanúsítványok megvalósítására. Az SSL a legszélesebb körben használt tanúsítvány alapú hitelesítés.
2. **IPsec** – Az IPsec VPN-ek X.509-tanúsítványokat használnak, ha RSA-alapú hitelesítést használnak az internetes kulcscseréhez (IKE).
3. **S/MIME** – Azok a felhasználói levelezőügynökök, amelyek a biztonságos/többcélú internetes levelezőkiterjesztések (S/MIME) protokolljával támogatják a levelezés védelmét, X.509 tanúsítványokat használnak.
4. **EAP-TLS** – A Cisco switchek tanúsítványok segítségével hitelesíthetik azokat a végberendezéseket, amelyek 802.1x-es LAN-portokhoz csatlakoznak a szomszédos eszközök között. A hitelesítés a TLS-sel bővíthető hitelesítési protokollon (EAP-TLS) keresztül proxyszerelhető egy központi ACS-hez.

17.2.6

## Tanúsítvány regisztráció, hitelesítés és visszavonás

A CA hitelesítési eljárás első lépése a hitelesítésszolgáltató nyilvános kulcsának egy másolatának biztonságos beszerzése. Minden rendszernek, amely kihasználja a PKI-t, rendelkeznie kell a CA nyilvános kulcsával, amelyet önaláírt tanúsítványnak neveznek. A CA nyilvános kulcsa ellenőrzi a CA által kiadott összes tanúsítványt, és létfontosságú a PKI megfelelő működéséhez.

**Megjegyzés** : Csak a gyökér CA bocsáthat ki önaláírt tanúsítványt, amelyet a PKI-n belül más CA-k felismernek vagy ellenőrzöttek.

Számos rendszer, például webböngésző esetében a CA-tanúsítványok kiosztása automatikusan történik. A webböngésző előre telepítve van nyilvános CA gyökértanúsítványokkal. A szervezetek és webhelydomainjeik nyilvános tanúsítványaikat továbbítják a webhely látogatóinak. A hitelesítésszolgáltatók és a tanúsítványtartomány-regisztrátorok privát és nyilvános tanúsítványokat hoznak létre és osztanak ki a tanúsítványokat vásárló ügyfelek számára.

A tanúsítvány regisztrációs folyamatát a gazdagép rendszer használja a PKI-re való regisztrációhoz. Ehhez a CA-tanúsítványok sávon belül, hálózaton keresztül kerülnek lekérésre, és a hitelesítés sávon kívül (OOB) történik telefonon.

A regisztrációt követően a két fél közötti hitelesítés többé nem függ a CA-kiszolgáló jelenlététől, mivel minden felhasználó kicseréli a nyilvános kulcsokat tartalmazó tanúsítványait.

A hitelesítéshez már nincs szükség a CA-szerver jelenlétére, és minden felhasználó kicseréli a nyilvános kulcsokat tartalmazó tanúsítványait.

A tanúsítványokat időnként vissza kell vonni. Például egy digitális tanúsítvány visszavonható, ha a kulcs sérül, vagy ha már nincs rá szükség.

Íme a két leggyakoribb visszavonási mód:

* **Tanúsítvány-visszavonási lista (CRL)** – A visszavont tanúsítványok sorozatszámainak listája, amelyek érvénytelenítésre kerültek, mert lejártak. A PKI entitások rendszeresen lekérdezik a CRL-tárat, hogy megkapják az aktuális CRL-t.
* **Online Certificate Status Protocol (OCSP)** – Internet protokoll, amellyel az OCSP-kiszolgálótól lekérdezik az X.509 digitális tanúsítvány visszavonási állapotát. A visszavonási információk azonnal egy online adatbázisba kerülnek.

17.2.7

## Lab – Tanúsítványkibocsátó üzletek

Ebben a laborban a következő célokat kell teljesítenie:

* Az Ön böngészője által megbízható tanúsítványok
* A középső ember ellenőrzése

[17.1](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Public Key Cryptography with Digital Signatures](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[17.3](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Applications and Impacts of Cryptography](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                            
*         

1. Public Key Cryptography
2. Applications and Impacts of Cryptography

# A kriptográfia alkalmazásai és hatásai

17.3.1

## PKI alkalmazások

Hol használhatja a PKI egy vállalkozás? Az alábbiakban egy rövid lista található a PKI-k általános használatáról:

* SSL/TLS tanúsítvány alapú társhitelesítés
* Biztonságos hálózati forgalom IPsec VPN-ek segítségével
* HTTPS webes forgalom
* A hálózathoz való hozzáférés szabályozása 802.1x hitelesítéssel
* Biztonságos e-mail az S/MIME protokoll használatával
* Biztonságos azonnali üzenetküldés
* Alkalmazások jóváhagyása és engedélyezése kódaláírással
* A felhasználói adatok védelme a titkosító fájlrendszerrel (EFS)
* Kétfaktoros hitelesítés megvalósítása intelligens kártyákkal
* USB tárolóeszközök biztonsága

17.3.2

## Titkosított hálózati tranzakciók

A biztonsági elemzőnek képesnek kell lennie arra, hogy felismerje és megoldja a PKI-vel kapcsolatos megoldások vállalati hálózaton történő engedélyezésével kapcsolatos lehetséges problémákat.

Fontolja meg, hogy az SSL/TLS forgalom növekedése miként jelent komoly biztonsági kockázatot a vállalatok számára, mivel a forgalom titkosított, és normál eszközökkel nem lehallgatható és felügyelhető. A felhasználók SSL/TLS kapcsolaton keresztül rosszindulatú programokat vezethetnek be, vagy bizalmas információkat szivárogtathatnak ki.

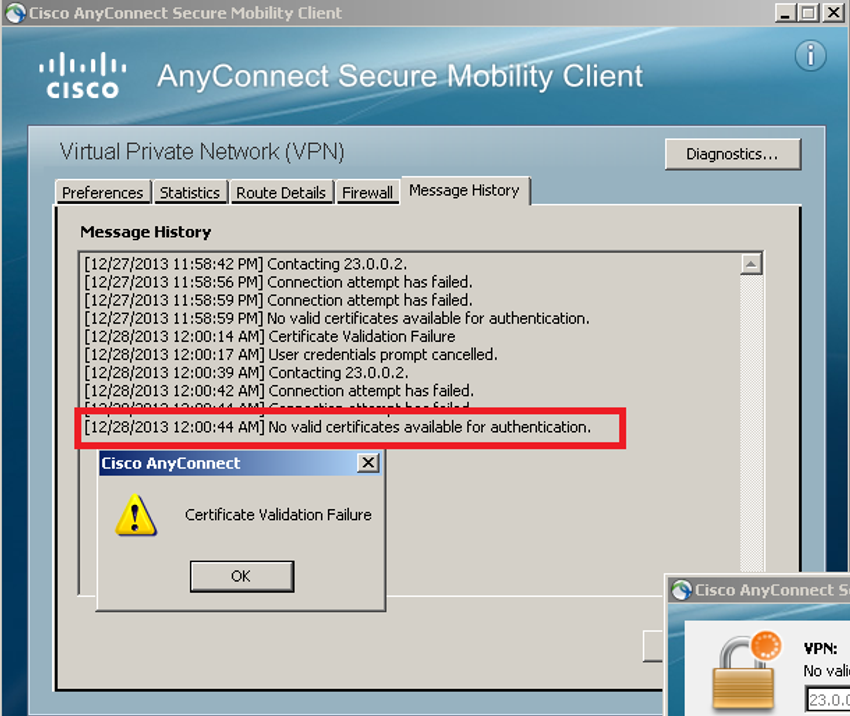
A fenyegetést okozó szereplők az SSL/TLS használatával a szabályozási megfelelőség megsértését, vírusokat, rosszindulatú programokat, adatvesztést és behatolási kísérleteket vezethetnek be a hálózatba.

A webszerver tanúsítványának érvényesítéséhez egyéb SSL/TLS-problémák is társulhatnak. Amikor ez megtörténik, a böngészők biztonsági figyelmeztetést jelenítenek meg. A biztonsági figyelmeztetésekhez kapcsolódó PKI-vel kapcsolatos problémák a következők:

* **Érvényességi dátumtartomány** – Az X.509v3 tanúsítványok „nem előtte” és „nem utána” dátumot adnak meg. Ha az aktuális dátum a tartományon kívül esik, a webböngésző üzenetet jelenít meg. Lehet, hogy a lejárt tanúsítványok egyszerűen adminisztrátori felügyelet eredménye, de komolyabb állapotokat is tükrözhetnek.
* **Aláírás-ellenőrzési hiba** – Ha egy böngésző nem tudja érvényesíteni a tanúsítványon lévő aláírást, nincs garancia arra, hogy a tanúsítványban lévő nyilvános kulcs hiteles. Az aláírás ellenőrzése sikertelen lesz, ha a CA-hierarchia gyökértanúsítványa nem érhető el a böngésző tanúsítványtárolójában.

Az ábra egy példát mutat be egy aláírás-ellenőrzési hibára a Cisco AnyConnect Mobility VPN Client alkalmazásban.

### Aláírás-érvényesítési hiba



Ezen problémák némelyike ​​elkerülhető annak köszönhetően, hogy az SSL/TLS protokollok bővíthetők és modulárisak. Ezt titkosítási csomagnak nevezik. A titkosítási csomag kulcsfontosságú összetevői a MAC (Message Authentication Code Algorithm), a titkosítási algoritmus, a kulcscsere algoritmus és a hitelesítési algoritmus. Ezek a teljes protokoll cseréje nélkül módosíthatók. Ez nagyon hasznos, mert a különböző algoritmusok folyamatosan fejlődnek. Mivel a kriptográfiai elemzés továbbra is feltárja ezen algoritmusok hibáit, a rejtjelkészlet frissíthető, hogy javítsa ezeket a hibákat. Amikor a titkosítási csomagon belüli protokollverziók megváltoznak, az SSL/TLS verziószáma is megváltozik.

17.3.3

## Titkosítás és biztonsági figyelés

A hálózat figyelése nagyobb kihívást jelent, ha a csomagokat titkosítják. A biztonsági elemzőknek azonban tisztában kell lenniük ezekkel a kihívásokkal, és a lehető legjobban kezelniük kell őket. Például, amikor helyek közötti VPN-eket használnak, az IPS-t úgy kell elhelyezni, hogy figyelni tudja a titkosítatlan forgalmat.

A HTTPS megnövekedett használata azonban a vállalati hálózatban új kihívásokat vet fel. Mivel a HTTPS végpontok közötti titkosított HTTP-forgalmat vezet be (TLS/SSL-en keresztül), nem olyan egyszerű betekinteni a felhasználói forgalomba.

A biztonsági elemzőknek tudniuk kell, hogyan lehet megkerülni és megoldani ezeket a problémákat. Íme egy lista azokról a dolgokról, amelyeket egy biztonsági elemző megtehet:

* Konfiguráljon szabályokat az SSL és a nem SSL forgalom, a HTTPS és a nem HTTPS SSL forgalom megkülönböztetésére.
* Növelje a biztonságot a szervertanúsítvány-ellenőrzéssel CRL-ek és OCSP használatával.
* Végezzen kártevő elleni védelmet és URL-szűrést a HTTPS-tartalomra.

A kriptográfia dinamikus és folyamatosan változik. A biztonsági elemzőnek jól ismernie kell a kriptográfiai algoritmusokat és műveleteket, hogy ki tudja vizsgálni a kriptográfiával kapcsolatos biztonsági incidenseket.

A kriptográfia két fő módon befolyásolja a biztonsági vizsgálatokat. Először is, a támadások kifejezetten magukat a titkosítási algoritmusokat célozzák. Miután az algoritmust feltörték, és a támadó megszerezte a kulcsokat, az elfogott titkosított adatokat a támadó visszafejtheti és elolvashatja, így felfedheti a személyes adatokat. Másodszor, a biztonsági vizsgálatot is érinti, mert az adatok titkosítással jól láthatóan elrejthetők. Például a TLS/SSL-lel titkosított parancs- és vezérlési forgalmat valószínűleg nem látja a tűzfal. A parancs- és vezérlőszerver és egy biztonságos hálózatban lévő fertőzött számítógép közötti parancs- és vezérlőforgalom nem állítható le, ha az nem látható és nem érthető. A támadó továbbra is használhatja a titkosított parancsokat több számítógép megfertőzésére, és esetleg botnet létrehozására. Az ilyen típusú forgalom a forgalom visszafejtésével és az ismert támadási szignatúrákkal való összehasonlításával, vagy a rendellenes TLS/SSL forgalom észlelésével észlelhető. Ez vagy nagyon nehéz és időigényes, vagy „hit-or-miss” folyamat.

[17.2](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Authorities and the PKI Trust System](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[17.4](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Public Key Cryptography Summary](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                                     

1. Public Key Cryptography
2. Public Key Cryptography Summary

# Nyilvános kulcsú kriptográfiai összefoglaló

17.4.1

## Mit tanultam ebben a modulban?

**Nyilvános kulcsú kriptográfia**   
A digitális aláírás egy matematikai technika, amelyet három alapvető biztonsági szolgáltatás nyújtására használnak: hitelesség, integritás és letagadhatatlanság. A digitális aláírás tulajdonságai az, hogy hitelesek, megváltoztathatatlanok, nem használhatók fel újra, és nem cáfolhatók. A digitális aláírásokat általában a következő két helyzetben használják: kódaláírás és digitális tanúsítványok. Három DSS-algoritmus használható a digitális aláírások generálására és ellenőrzésére: DSA, RSA és ECDSA. A digitálisan aláírt kód biztosítékot nyújt a szoftverkóddal kapcsolatban: a kód hiteles, és ténylegesen a kiadótól származik, a kódot nem módosították, mióta elhagyta a szoftver kiadóját, és tagadhatatlanul a kiadó tette közzé a kódot. A digitális tanúsítvány egyenértékű az elektronikus útlevéllel. Lehetővé teszi a felhasználók, gazdagépek és szervezetek számára, hogy biztonságosan cseréljenek információkat az interneten keresztül. Pontosabban, digitális tanúsítványt használnak annak hitelesítésére és ellenőrzésére, hogy az üzenetet küldő felhasználó az, akiről azt állítják, hogy ő maga.

**A hatóságok és a PKI Trust System**   
Amikor két gazdagép között biztonságos kapcsolatot létesítenek, a gazdagépek kicserélik nyilvános kulcsú információikat. Vannak megbízható harmadik felek az interneten, amelyek digitális tanúsítványok segítségével ellenőrzik e nyilvános kulcsok hitelességét. A PKI specifikációkat, rendszereket és eszközöket tartalmaz, amelyek digitális tanúsítványok létrehozására, kezelésére, terjesztésére, használatára, tárolására és visszavonására szolgálnak. A PKI-re van szükség a nyilvános titkosítási kulcsok nagyszabású terjesztésének támogatásához. A PKI keretrendszer nagymértékben méretezhető bizalmi kapcsolatot tesz lehetővé. Sok szállító felügyelt szolgáltatásként vagy végfelhasználói termékként kínál CA-kiszolgálókat. Néhány ilyen szállító többek között a Symantec Group (VeriSign), a Comodo, a Go Daddy Group, a GlobalSign és a DigiCert. Az osztályszámot az határozza meg, hogy mennyire volt szigorú az az eljárás, amely a tanúsítvány kiállításakor ellenőrizte a tulajdonos személyazonosságát, és az ötös a legmagasabb. A PKI-k különböző bizalmi topológiákat alkothatnak. A legegyszerűbb az egygyökér PKI topológia. A PKI és a támogató szolgáltatásai közötti interoperabilitás aggodalomra ad okot, mert sok CA-szállító javasolt és vezetett be saját megoldást ahelyett, hogy a szabványok kidolgozására várna. Az interoperabilitási probléma megoldása érdekében az IETF közzétette az RFC 2527 szabványt.

**A kriptográfia alkalmazásai és hatásai**   
A PKI-k számos általános felhasználása létezik, köztük néhány itt felsorolt: SSL/TLS-tanúsítvány alapú társhitelesítés, HTTPS webforgalom, biztonságos azonnali üzenetküldés és USB-tárolóeszközök védelme. A biztonsági elemzőnek képesnek kell lennie arra, hogy felismerje és megoldja a PHI-vel kapcsolatos megoldások engedélyezésével kapcsolatos lehetséges problémákat a vállalati hálózaton. Például a fenyegetések szereplői használhatják az SSL/TSL-t a szabályozási megfelelőség megsértésére, vírusokra, rosszindulatú programokra, adatvesztésre és behatolási kísérletekre a hálózaton. A webszerver tanúsítványának érvényesítéséhez más, SSL/TSL-lel kapcsolatos problémák is társulhatnak. A biztonsági figyelmeztetésekkel kapcsolatos PKI-problémák közé tartozik az érvényességi dátumtartomány és az aláírás ellenőrzése. Ezen problémák némelyike ​​elkerülhető annak köszönhetően, hogy az SSL/TSL protokollok bővíthetők és modulárisak. Ezt titkosítási csomagnak nevezik. A rejtjelkészlet kulcsfontosságú összetevői a MAC, a titkosítási algoritmus, a kulcscsere algoritmus és a hitelesítési algoritmus. A kriptográfia dinamikus és folyamatosan változik. A kriptográfiával kapcsolatos biztonsági incidensek kivizsgálásához alaposan ismernie kell az algoritmusokat és a műveleteket. A titkosított kommunikáció olvashatatlanná teheti a hálózatbiztonsági adatok hasznos adatait a kiberbiztonsági elemzők számára. A titkosítás használható a rosszindulatú programok elrejtésére, valamint a fertőzött gazdagépek és a parancs- és vezérlőkiszolgálók közötti forgalom szabályozására. Ezenkívül a rosszindulatú programok titkosítással elrejthetők, az adatok pedig titkosíthatók a kiszűrés során, ami megnehezíti az észlelést.

17.4.2

## 17. modul – Hálózati és eszközbiztonsági kvíz konfigurálása

Az űrlap teteje

1. Mi a hálózati biztonságban használt nyilvános kulcsú infrastruktúra (PKI) két fontos összetevője? (Válassz kettőt.)

Az űrlap alja

Mi a kódaláírás célja?

Melyik utasítás írja le a tanúsítványosztályok használatát a PKI-ben?

Milyen szerepet játszik az RA a PKI-ben?

Melyik protokoll használ X.509 tanúsítványokat a levelezőügynökök által végzett levélvédelem támogatására?

Milyen protokollt használnak az X.509 tanúsítvány visszavonási állapotának lekérdezésére?

Milyen módon növeli a HTTPS használata a biztonsági megfigyelési kihívásokat a vállalati hálózatokon belül?

Milyen technológiát alkalmaznak a szoftverkód hitelességének és integritásának biztosítására?

A digitális tanúsítványok melyik CA osztályát használnák az egyének az e-mailek ellenőrzéséhez?

Mi a digitális tanúsítvány célja?

Mi a megfelelő felhasználás az 5. osztályú digitális tanúsítványokhoz?

[17.3](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Applications and Impacts of Cryptography](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[18.0](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                                           
*       

1. VPNs
2. Introduction

# Bevezetés

18.0.1

## Miért vegyem ezt a modult?

Üdvözöljük a VPN-ekben!

Önt vagy valakit, akit ismer, feltörtek valaha nyilvános WiFi használata közben? Meglepően könnyen kivitelezhető.

A probléma megoldása a virtuális magánhálózatok (VPN) és az IP-biztonság (IPsec) kiegészítő védelme. A VPN-eket a távoli dolgozók gyakran használják szerte a világon. Vannak személyes VPN-ek is, amelyeket akkor használhat, ha nyilvános WiFi-t használ. Valójában sokféle VPN létezik, amelyek IPsec-et használnak a forrás és a cél közötti IP-csomagok védelmére és hitelesítésére.

18.0.2

## Mit fogok tanulni ebben a modulban?

**Modul címe:** VPN-ek

**A modul célja** : Magyarázza el a VPN-ek célját.

| **téma címe** | **Téma Cél** |
| --- | --- |
| **VPN áttekintése** | Ismertesse a VPN-eket és előnyeiket. |
| **VPN topológiák** | Hasonlítsa össze a távoli hozzáférést és a helyek közötti VPN-eket. |
| **Az IPsec bemutatása** | Ismertesse az IPsec protokollt és alapvető funkcióit. |
| **IPsec protokollok** | Hasonlítsa össze az AH és ESP protokollokat. |
| **Internetes kulcscsere** | Ismertesse az IKE protokollt! |

[17.4](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Public Key Cryptography Summary](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[18.1](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[VPN Overview](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                                           
*       

1. VPNs
2. VPN Overview

# VPN áttekintése

18.1.1

## Virtuális magánhálózatok

A helyek és felhasználók közötti hálózati forgalom biztonsága érdekében a szervezetek virtuális magánhálózatokat (VPN) használnak végpontok közötti magánhálózati kapcsolatok létrehozásához. A VPN virtuális, mivel magánhálózaton belül továbbítja az információkat, de ezek az információk valójában egy nyilvános hálózaton keresztül kerülnek továbbításra. A VPN magánjellegű, mivel a forgalom titkosított, hogy az adatok bizalmasak maradjanak, miközben a nyilvános hálózaton keresztül továbbítják azokat.

Az ábra különböző típusú VPN-ek gyűjteményét mutatja, amelyeket a vállalat fő webhelye kezel. Az alagút lehetővé teszi a távoli helyek és a felhasználók számára, hogy biztonságosan hozzáférjenek a fő webhely hálózati erőforrásaihoz.

Az ábra különböző típusú VP N-ket mutat be, amelyeket egy vállalati főoldal kezel. A fő oldalon egy Cisco ASA tűzfal látható, amely a vállalati hálózathoz csatlakozik, valamint az interneten keresztül egy üzleti partner Cisco útválasztójához, egy regionális iroda Cisco ASA tűzfalához, egy kis irodai/otthoni irodai Cisco útválasztóhoz és a Cisco AnyConnecten keresztül távolról csatlakozik mobil munkatárshoz. .

Üzleti partner Cisco Router regionális irodával Cisco ASA tűzfallal SOHO Cisco Routerrel mobil munkatárs Cisco AnyConnect vállalati főoldallal Cisco ASA Firewall Internet

* A Cisco Adaptive Security Appliance (ASA) tűzfal segítségével a szervezetek biztonságos, nagy teljesítményű kapcsolatot biztosítanak, beleértve a VPN-eket és a mindig elérhető hozzáférést a távoli fiókok és mobilfelhasználók számára.
* A SOHO a kis irodai otthoni iroda rövidítése, ahol egy VPN-kompatibilis útválasztó VPN-kapcsolatot biztosít a vállalat fő helyére.
* A Cisco AnyConnect egy olyan szoftver, amellyel a távoli dolgozók kliens alapú VPN-kapcsolatot hozhatnak létre a fő hellyel.

A VPN-ek első típusai szigorúan IP-alagutak voltak, amelyek nem tartalmazták az adatok hitelesítését vagy titkosítását. Például a Generic Routing Encapsulation (GRE) a Cisco által kifejlesztett alagútkezelési protokoll, amely nem tartalmaz titkosítási szolgáltatásokat. Az IPv4- és IPv6-forgalom IP-alagúton belüli beágyazására szolgál virtuális pont-pont kapcsolat létrehozására.

18.1.2

## VPN előnyei

A modern VPN-ek már támogatják a titkosítási funkciókat, például az Internet Protocol Security (IPsec) és a Secure Sockets Layer (SSL) szolgáltatást a helyek közötti hálózati forgalom biztonsága érdekében.

A VPN-ek fő előnyei a táblázatban láthatók.

| Táblázat felirata | |
| --- | --- |
| **Haszon** | **Leírás** |
| **Költségmegtakarítás** | A költséghatékony, nagy sávszélességű technológiák megjelenésével a szervezetek VPN-ek segítségével csökkenthetik kapcsolódási költségeiket, ugyanakkor növelhetik a távoli kapcsolat sávszélességét. |
| **Biztonság** | A VPN-ek az elérhető legmagasabb szintű biztonságot nyújtják fejlett titkosítási és hitelesítési protokollok használatával, amelyek megvédik az adatokat az illetéktelen hozzáféréstől. |
| **Méretezhetőség** | A VPN-ek lehetővé teszik a szervezetek számára az internet használatát, így egyszerűvé téve új felhasználók hozzáadását jelentős infrastruktúra hozzáadása nélkül. |
| **Kompatibilitás** | A VPN-ek a WAN-kapcsolatok széles skáláján megvalósíthatók, beleértve az összes népszerű szélessávú technológiát. A távoli dolgozók kihasználhatják ezeket a nagy sebességű kapcsolatokat, hogy biztonságosan hozzáférhessenek vállalati hálózatukhoz. |

[18.0](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[18.2](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[VPN Topologies](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                                              
*       

1. VPNs
2. VPN Topologies

# VPN topológiák

18.2.1

## Site-to-Site és távoli hozzáférésű VPN-ek

A VPN-eket általában a következő konfigurációk egyikében telepítik: helyek közötti vagy távoli hozzáférés.

További információért kattintson az egyes VPN-típusokra.

A helyek közötti VPN akkor jön létre, amikor a VPN-lezáró eszközöket, más néven VPN-átjárókat előre konfigurálják a biztonságos alagút létrehozásához szükséges információkkal. A VPN-forgalom csak ezen eszközök között titkosított. A belső gazdagépek nem tudnak arról, hogy VPN-t használnak.

Az ábra egy helyek közötti VPN-kapcsolatot ábrázol. A kliens laptopja csatlakozik a hálózati VPN-átjáróhoz, amely routerként jelenik meg. A VPN-átjáró az interneten keresztül (felhőként) csatlakozik egy másik VPN-átjáróhoz, amely ASA tűzfalként jelenik meg.

Az Internet Client nem ismeri a VPN VPN Gateway VPN Gateway-t

18.2.2

## Távoli hozzáférésű VPN-ek

Az előző témakörben megismerkedhetett a VPN alapjaival. Itt megtudhatja a VPN-ek típusait.

A VPN-ek több okból is logikus megoldássá váltak a távoli hozzáféréshez. Amint az ábrán látható, a távoli hozzáférésű VPN-ek lehetővé teszik a távoli és mobil felhasználók számára, hogy biztonságosan csatlakozzanak a vállalathoz egy titkosított alagút létrehozásával. A távoli felhasználók biztonságosan reprodukálhatják vállalati biztonsági hozzáférésüket, beleértve az e-maileket és a hálózati alkalmazásokat. A távoli hozzáférésű VPN-ek azt is lehetővé teszik a vállalkozók és partnerek számára, hogy szükség szerint korlátozott hozzáférést kapjanak az adott szerverekhez, weboldalakhoz vagy fájlokhoz. Ez azt jelenti, hogy ezek a felhasználók hozzájárulhatnak az üzleti termelékenységhez a hálózat biztonságának veszélyeztetése nélkül.

A távoli hozzáférésű VPN-eket általában a felhasználó dinamikusan engedélyezi, ha szükséges. Távoli hozzáférésű VPN-ek IPsec vagy SSL használatával hozhatók létre. Az ábrán látható módon a távoli felhasználónak távoli hozzáférésű VPN-kapcsolatot kell kezdeményeznie.

Az ábra két módot mutat be, amellyel egy távoli felhasználó távelérési VPN-kapcsolatot kezdeményezhet: kliens nélküli VPN és kliens alapú VPN.

Az ábra két módszert mutat be, amellyel egy távoli felhasználó kezdeményezhet távoli hozzáférésű VPN-kapcsolatot: kliens nélküli VPN és kliensalapú VP N. Az egyik felhasználó laptopja SSLVPN-alagúton keresztül csatlakozik a központhoz az interneten keresztül a felhasználói webböngészőn keresztül. Egy második laptop csatlakozik a központhoz az interneten keresztül a Cisco AnyConnect Secure Mobility Client segítségével.



Felhasználói számítógép   
böngészővel Cisco AnyConnect Secure Mobility Client Internet **SSL VPN Tunnel Headquarters** SSL VPN Workplace Resources

* **Kliens nélküli VPN-kapcsolat** – A kapcsolat egy webböngésző SSL-kapcsolattal védett. Az SSL-t leginkább a HTTP-forgalom (HTTPS) és az e-mail protokollok, például az IMAP és a POP3 védelmére használják. Például a HTTPS valójában egy SSL alagutat használó HTTP. Először az SSL-kapcsolat jön létre, majd a HTTP-adatok cseréje történik a kapcsolaton keresztül.
* **Kliens alapú VPN-kapcsolat** – A VPN-kliens szoftvert, például a Cisco AnyConnect Secure Mobility Client telepíteni kell a távoli felhasználó végeszközére. A felhasználóknak kezdeményezniük kell a VPN-kapcsolatot a VPN-kliens használatával, majd hitelesíteniük kell a cél VPN-átjárót. A távoli felhasználók hitelesítésekor hozzáférhetnek a vállalati fájlokhoz és alkalmazásokhoz. A VPN-kliens szoftver IPsec vagy SSL használatával titkosítja a forgalmat, és az interneten keresztül továbbítja azt a cél VPN-átjáróhoz.

18.2.3

## SSL VPN-ek

Amikor egy ügyfél SSL VPN-kapcsolatot egyeztet a VPN-átjáróval, valójában a Transport Layer Security (TLS) használatával csatlakozik. A TLS az SSL újabb verziója, és néha SSL/TLS-ként fejezik ki. Mindazonáltal mindkét kifejezést gyakran felcserélve használják.

Az SSL a nyilvános kulcsú infrastruktúrát és a digitális tanúsítványokat használja a társak hitelesítésére. Mind az IPsec, mind az SSL VPN technológia gyakorlatilag bármilyen hálózati alkalmazáshoz vagy erőforráshoz kínál hozzáférést. Ha azonban a biztonság kérdése, az IPsec a legjobb választás. Ha a támogatás és a könnyű üzembe helyezés az elsődleges probléma, fontolja meg az SSL-t. A megvalósított VPN módszer típusa a felhasználók hozzáférési követelményein és a szervezet informatikai folyamatain alapul. A táblázat összehasonlítja az IPsec- és az SSL-távelérési telepítéseket.

| Táblázat felirata | | |
| --- | --- | --- |
| **Funkció** | **IPsec** | **SSL** |
|  | Az IPsec a 3. rétegben működik, az OSI modell hálózati rétegében, közvetlenül az IP felett. | Az SSL az OSI modell 7. rétegében, az Alkalmazási rétegben működik, a HTTP-forgalmat titkosítja, nem az IP-csomagokat. |
| **A kapcsolat bonyolultsága** | **Közepes** – Mert ehhez egy gazdagépen előre telepített VPN-kliens szükséges. | **Alacsony** – Csak webböngésző szükséges a gazdagépen. |
| **Csatlakozási lehetőség** | **Korlátozott** – Csak meghatározott konfigurációjú eszközök csatlakozhatnak. | **Kiterjedt** – Bármely webböngészővel rendelkező eszköz csatlakozhat. |

Fontos megérteni, hogy az IPsec és az SSL VPN-ek nem zárják ki egymást. Ehelyett kiegészítik egymást; mindkét technológia különböző problémákat old meg, és egy szervezet megvalósíthatja az IPsec-et, az SSL-t vagy mindkettőt, a távmunkások igényeitől függően.

18.2.4

## Site-to-Site IPsec VPN-ek

A helyek közötti VPN-ek hálózatok összekapcsolására szolgálnak egy másik nem megbízható hálózaton, például az interneten. A helyek közötti VPN-ben a végállomások normál titkosítatlan TCP/IP-forgalmat küldenek és fogadnak egy VPN-lezáró eszközön keresztül. A VPN-lezáró eszközt általában VPN-átjárónak nevezik. A VPN-átjáró eszköz lehet útválasztó vagy tűzfal, amint az az ábrán látható. Például az ábra jobb oldalán látható Cisco Adaptive Security Appliance (ASA) egy önálló tűzfaleszköz, amely a tűzfalat, a VPN-koncentrátort és a behatolásmegelőzési funkciókat egyetlen szoftverképben egyesíti.

Az ábra egy IPsec-alagutat használó helyek közötti VPN-kapcsolatot mutat be. A kliens laptop csatlakozik a hálózati VPN-átjáróhoz, amely routerként jelenik meg. A VPN-átjáró az interneten keresztül (felhőként) csatlakozik egy másik VPN-átjáróhoz, amely ASA tűzfalként jelenik meg. A két VPN-átjáró közötti kapcsolat IPsec-et használ a VPN-alagút védelmére.

Az Internet IPsec Tunnel Client nem ismeri a VPN VPN Gateway VPN Gateway-t

A VPN-átjáró beágyazza és titkosítja a kimenő forgalmat. Ezután a forgalmat egy VPN-alagúton keresztül az interneten keresztül továbbítja a célhely VPN-átjárójához. A fogadás után a fogadó VPN-átjáró eltávolítja a fejléceket, visszafejti a tartalmat, és továbbítja a csomagot a célállomás felé a magánhálózatán belül.

A helyek közötti VPN-ek általában IP-biztonsággal (IPsec) jönnek létre és védik őket.

18.2.5

## Ellenőrizze megértését – Hasonlítsa össze a távoli hozzáférést és a helyek közötti VPN-eket

Az űrlap teteje

Ellenőrizze, hogy megértette-e a VPN jellemzőit, és válassza ki a megfelelő választ a következő kérdésekre.

1. Melyik VPN támogatja a dinamikusan változó kapcsolati információkat, és szükség esetén engedélyezhető?

Az űrlap alja

Milyen típusú VPN használatos, amikor a gazdagép normál TCP/IP forgalmat küld és fogad VPN-átjárón keresztül?

Milyen típusú VPN használatos, ha a VPN-kapcsolat mindkét oldala előre ismeri a VPN konfigurációt?

Milyen típusú VPN-t használnak, ha a belső gazdagépek nem tudják, hogy VPN létezik?

Milyen típusú VPN-t használnak, ha a távmunkás eszköz felelős a VPN létrehozásáért?

[18.1](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[VPN Overview](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[18.3](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[IPsec Overview](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                                                     
*       

1. VPNs
2. IPsec Overview

# IPsec Overview

18.3.1

## Video - IPsec Concepts

In the previous topic you learned about types of VPNs. It is important to understand how IPsec works with a VPN.

Click Play in the figure for a video about IPsec.

18.3.2

## IPsec Technologies

Az IPsec egy IETF-szabvány (RFC 2401-2412), amely meghatározza, hogyan lehet biztonságos VPN-t biztosítani az IP-hálózatokon keresztül. Az IPsec védi és hitelesíti az IP-csomagokat a forrás és a cél között. Az IPsec képes megvédeni a forgalmat a 4-es rétegtől a 7-es rétegig.

Az IPsec keretrendszer használatával az IPsec a következő alapvető biztonsági funkciókat biztosítja:

* **Titoktartás** – Az IPsec titkosítási algoritmusokat használ annak megakadályozására, hogy a kiberbűnözők elolvassák a csomag tartalmát.
* **Integritás** – Az IPsec kivonatoló algoritmusokat használ annak biztosítására, hogy a csomagok ne változzanak a forrás és a cél között.
* **Eredeti hitelesítés** – Az IPsec az Internet Key Exchange (IKE) protokollt használja a forrás és a cél hitelesítésére. A hitelesítési módszerek közé tartozik az előre megosztott kulcsok (jelszavak), digitális tanúsítványok vagy RSA-tanúsítványok használata.
* **Diffie-Hellman** – Biztonságos kulcscsere jellemzően a DH-algoritmus különböző csoportjaival.

Az IPsec nem kötődik a biztonságos kommunikációra vonatkozó speciális szabályokhoz. A keretrendszer ezen rugalmassága lehetővé teszi az IPsec számára, hogy a meglévő IPsec-szabványok frissítése nélkül könnyedén integráljon új biztonsági technológiákat. A jelenleg elérhető technológiák sajátos biztonsági funkciójukhoz igazodnak. Az ábrán az IPsec-keretrendszerben látható nyitott helyek az adott IPsec-funkcióhoz rendelkezésre álló lehetőségek bármelyikével feltölthetők egyedi biztonsági társítás (SA) létrehozásához.

Az ábra az IPsec keretrendszer beállításait mutatja be. Öt IPsec-funkció van, az IPsec-protokoll, a bizalmas kezelés, az integritás, a hitelesítés és a Diffie-Hellman. Minden funkciónak vannak elérhető opciói. Az IPsec Protocol beállításai a következők: AH, ESP vagy ESP + A H. A Titoktartás beállításai: DES, 3 DES, AES vagy SEAL. Az Integrity opciói: MD 5 vagy SH A. A hitelesítés lehetőségei: PSK vagy RS A. A Diffie-Hellman opciói a következők: DH 1, DH 2, DH 5 stb.

**IPsec Framework** IPsec Protokoll Titoktartás Integritás Hitelesítés Diffie-Hellman **Choices** AH ESP ESP + AH DES 3DES AES SEAL MD5 SHA PSK RSA DH1 DH2 DH5 DH...

A biztonsági funkciókat a táblázat tartalmazza.

| **IPsec funkció** | **Leírás** |
| --- | --- |
| **IPsec protokoll** | Az IPsec-protokoll közül választhat: Authentication Header (AH) vagy Encapsulation Security Protocol (ESP). Az AH hitelesíti a 3. rétegbeli csomagot. Az ESP titkosítja a Layer 3 csomagot. **Megjegyzés** : Az ESP+AH ritkán használatos, mivel ez a kombináció nem képes sikeresen áthaladni a NAT-eszközön. |
| **Titoktartás** | A titkosítás biztosítja a 3. rétegű csomag titkosságát. A biztonságos választások közé tartozik az Advanced Encryption Standard (AES) vagy a Software-Optimized Encryption Algorithm (SEAL). Kerülendő örökölt algoritmusok közé tartozik a Data Encryption Standard (DES) és a Triple DES (3DES). |
| **Sértetlenség** | Az integritás egy hash algoritmus segítségével biztosítja, hogy az adatok változatlan formában érkezzenek a célállomásra. Ilyen például a Secure Hash Algorithm (SHA) és az üzenet-kivonat 5 (MD5). Az MD5 nem biztonságos, ezért kerülni kell. Az SHA-nak több verziója is létezik. Az SHA-1 az eredeti verzió, ezért kerülendő. Ehelyett az SHA-256 ajánlott az érzékeny információk védelme érdekében. Az SHA-384 és az SHA-512 szükséges a nagyobb jelentőségű minősített információk védelméhez. |
| **Hitelesítés** | Az IPsec az Internet Key Exchange (IKE) szolgáltatást használja a felhasználók és eszközök hitelesítésére, amelyek önállóan tudnak kommunikációt folytatni. Az IKE többféle hitelesítést használ, beleértve a felhasználónevet és jelszót, az egyszeri jelszót, a biometrikus adatokat, az előre megosztott kulcsokat (PSK) és a digitális tanúsítványokat a Rivest, Shamir és Adleman (RSA) algoritmus segítségével. |
| **Diffie-Hellman** | Az IPsec a DH-algoritmust használja, hogy nyilvános kulcscsere-módszert biztosítson két partner számára egy megosztott titkos kulcs létrehozásához. Számos DH-algoritmuscsoport közül lehet választani. Azonban ne használja az 1., 2. és 5. DH csoportot, mivel ezek már nem ajánlottak. Ehelyett a 14-es, 15-ös vagy 16-os DH-csoportok tekinthetők biztonságosnak, az elliptikus görbe 19-es, 20-as, 21-es és 24-es DH-csoportja pedig a legbiztonságosabbnak. |

Az ábra példákat mutat be SA-kra két különböző megvalósításhoz. Az SA az IPsec alapvető építőköve. VPN-kapcsolat létrehozásakor a partnereknek ugyanazt az SA-t kell megosztaniuk a kulcscsere-paraméterek egyeztetéséhez, megosztott kulcs létrehozásához, egymás hitelesítéséhez és a titkosítási paraméterek egyeztetéséhez. Figyelje meg, hogy az 1. példa SA nem használ titkosítást.

Az ábra az S As példáit mutatja két különböző megvalósításhoz. Az első példában az AH az IPsec-protokollhoz, a Titoktartáshoz nincs kiválasztva, az MD 5 az Integrity, a PSK a hitelesítéshez és a DH 16 a Diffie-Hellman számára. A második példa az ESP-t az IPsec protokollhoz, az AES-t a bizalmassághoz, az SHA-t az integritáshoz, az RSA-t a hitelesítéshez és a DH 24-et a Diffie-Hellmanhoz.

### IPsec biztonsági asszociációs példák

IPsec Protokoll Bizalmasság Integritás Diffie-Hellman hitelesítés AH MD5 PSK DH16 ESP AES SHA RSA DH24 **SA 1. példa SA 2. példa**

18.3.3

## IPsec Protocol Encapsulation

Az IPsec-protokoll-beágyazás kiválasztása a keretrendszer első építőköve. Az IPsec a csomagokat hitelesítési fejléc (AH) vagy Encapsulation Security Protocol (ESP) használatával zárja be. Az AH vagy az ESP választása meghatározza, hogy mely további építőelemek állnak rendelkezésre.

Az ábra az IPsec keretrendszer beállításait mutatja be. Az IPsec Protokoll opciót az AH, ESP és ESP + A H opciók jelzik.

**IPsec-keretrendszer** IPsec-protokoll Titoktartás Integritás Hitelesítés Diffie-Hellman **Choices** AH ESP ESP + AH DES 3DES AES SEAL MD5 SHA RSA PSK DH1 DH2 DH5 DH...

* Az AH csak akkor megfelelő, ha a titoktartás nem kötelező vagy megengedett. Biztosítja az adatok hitelesítését és integritását, de nem biztosítja az adatok titkosságát (titkosítást). Az összes szöveget titkosítatlanul továbbítják.
* Az ESP titkosságot és hitelesítést egyaránt biztosít. Az IP-csomag titkosításával titkosítást biztosít. Az ESP hitelesítést biztosít a belső IP-csomaghoz és az ESP-fejléchez. A hitelesítés biztosítja az adatok eredetének hitelesítését és az adatok integritását. Bár az ESP-ben mind a titkosítás, mind a hitelesítés nem kötelező, legalább az egyiket ki kell választani.

18.3.4

## Titoktartás

A titoktartást az adatok titkosításával érik el, az ábrán látható módon. A titkosság mértéke a titkosítási algoritmustól és a titkosítási algoritmusban használt kulcs hosszától függ. Ha valaki brute force támadással próbálja feltörni a kulcsot, a próbálkozási lehetőségek száma a kulcs hosszának függvénye. Az összes lehetőség feldolgozásának ideje a támadó eszköz számítógépes teljesítményének függvénye. Minél rövidebb a kulcs, annál könnyebb eltörni. Egy 64 bites kulcs körülbelül egy évig is eltörhet egy viszonylag kifinomult számítógépen. Egy 128 bites kulcs ugyanazzal a géppel nagyjából 10-et vehet igénybe 19 vagy 10 kvintimillió év a visszafejtés.

Az ábra egy felhasználót ábrázol, aki egy másik felhasználónak száz dollárt küld az interneten keresztül, és titkosítja/visszafejti az átutalást. Gail száz dollárt küld Jeremynek. Kulcshossz és titkosítási algoritmus használatával az átutalás titkosítva van, így a száz dollárból 4ehiDx67NMop9eRU781OPotVBn45TR lesz. A titkosított adatokat az interneten keresztül továbbítják. Az adatokat elfogó fenyegetett szereplő nem tudja elolvasni az adatokat, mert azok titkosítottak. amint az adatokat megkapta Jeremys számítógépe, az adatokat dekódolja, így Gail száz dollárt kap.

+

+

**Gail Jeremy** fizessen Jeremynek 100 dollárt   
  
Száz dolláros titkosítási algoritmus visszafejtési algoritmusa Fizessen Jeremynek 100 dollárt   
  
Száz dollár 4ehiDx67NMop9eR   
U781OPotVBn45TR Internet 4ehiDx67NMop9eR   
U781OPotVBn45TR Hmmm... Nem tudok olvasni semmit. Fenyegető színész

Az ábrán kiemelt titkosítási algoritmusok mind szimmetrikus kulcsú kriptorendszerek.

Az ábra bemutatja a különböző titkosítási algoritmusok eltérő kulcshosszúságát és erősségét. A titkosítás különböző titkosítási algoritmusai a következők: DES, 3 ES, AES vagy SEAL. A DES kulcshossza 56 bit, ez a legkevésbé biztonságos titkosítási algoritmus. A 3 DES a második legkevésbé biztonságos titkosítási algoritmus, kulcs hossza háromszor 56 bit. Az AES biztonságosabb a 128, 192 és 256 bites kulcsokkal. Egy másik biztonságosabb lehetőség a SEAL, amelynek kulcshossza 160 bit.

**IPsec-keretrendszer** IPsec-protokoll Titoktartás Integritás Hitelesítés Diffie-Hellman **Choices** AH DES 3DES AES SEAL MD5 SHA PSK RSA DH1 DH2 DH5 DH... **Legkevésbé biztonságos Legbiztonságosabb** kulcs hossza:   
56 bites Kulcs hossza:   
56 bites (3-szor) Kulcshosszak:   
128 bites   
192 bites   
256 bites Kulcs hossza:   
160 bites

* A DES 56 bites kulcsot használ, ezért kerülendő.
* A 3DES az 56 bites DES egy változata. Három független 56 bites titkosítási kulcsot használ 64 bites blokkonként, ami lényegesen erősebb titkosítási erősséget biztosít a DES-hez képest. A DES számítási szempontból megterhelő, és már nem tekinthető biztonságosnak.
* Az AES a leginkább ajánlott szimmetrikus titkosítási algoritmus. Erősebb biztonságot nyújt, mint a DES, és számításilag hatékonyabb, mint a 3DES. Az AES három különböző kulcshosszúságot kínál: 128 bites, 192 bites és 256 bites.
* A SEAL egy adatfolyam titkosítás, ami azt jelenti, hogy folyamatosan titkosítja az adatokat, nem pedig adatblokkokat. A SEAL 160 bites kulcsot használ, és nagyon biztonságosnak tekinthető.

18.3.5

## Sértetlenség

Az adatintegritás azt jelenti, hogy a fogadott adatok pontosan ugyanazok, mint az elküldött adatok. Lehetséges, hogy az adatok elfoghatók és módosíthatók. Például az ábrán tegyük fel, hogy egy 100 dolláros csekket írnak Alexnek. A csekket ezután elküldik Alexnek, de egy fenyegetőző feltartóztatja. A fenyegetőző színész megváltoztatja a csekken szereplő nevet Jeremyre, a csekken szereplő összeget pedig 1000 dollárra, és megpróbálja beváltani. A módosított ellenőrzésben a hamisítás minőségétől függően a támadó sikeres lehet.

Az ábra egy csekket ábrázol, amelyet egy fenyegető szereplő lefogott, és az adatokat megváltoztatják, ami eltérő hash-eredményeket eredményez. Alex fizetésének kezdőlapja 4ehiDx67NMop9 volt. Elfogták, és a nevet Jeremyre változtatták, így a hash 12ehqPx67NMoX lett. A kezdő és a befejező hash eltérő, 4ehiDx67NMop9 és 12ehqPx67NMoX.

**Fizessen Alexnek 100,00 USD** száz és 00/100 dollár **4ehiDx67NMop9 kezdő hash Fizetés Jeremynek 1000,00** ezer dollár 100/100 dollár **12ehqPx67NMoX végkivonat** eltérő

Mivel a VPN-adatok továbbítása a nyilvános interneten keresztül történik, az adatok integritásának bizonyítására van szükség annak biztosítására, hogy a tartalom nem változott meg. A hash algoritmus garantálja az üzenet integritását egy hash érték használatával. Az ábra a két leggyakoribb kivonatolási algoritmust emeli ki.

**Megjegyzés:** A Cisco mostantól az SHA-1-et örököltnek minősíti, és az integritás érdekében legalább az SHA-256-ot ajánlja.

Az ábra bemutatja a különböző hash algoritmusokat és kulcshosszukat. A különböző kivonatolási algoritmusok az MD 5 és az SH A. A kettő közül az MD 5 a legkevésbé biztonságos 128 bites kulcshosszal. Az SHA biztonságosabb a 160 bites kulcshosszal.

**IPsec-keretrendszer** IPsec-protokoll Titoktartás Integritás Hitelesítés Diffie-Hellman **Choices** AH AH AH AES SEAL MD5 SHA DH1 DH2 DH5 DH... **Legkevésbé biztonságos Legbiztonságosabb** kulcs hossza:   
128 bites kulcs hossza:   
160 bites

* A Message-Digest 5 (MD5) 128 bites megosztott titkos kulcsot használ. A változó hosszúságú üzenetet és a 128 bites megosztott titkos kulcsot egyesítik, és a HMAC-MD5 hash algoritmuson futják végig. A kimenet egy 128 bites hash. Az MD5 már nem biztonságos, kerülni kell.
* A Secure Hash Algorithm (SHA) 160 bites titkos kulcsot használ. A változó hosszúságú üzenetet és a 160 bites megosztott titkos kulcsot egyesítik, és a HMAC-SHA-1 algoritmuson keresztül futják. A kimenet egy 160 bites hash. Az SHA-256 vagy magasabb szint biztonságosnak tekinthető.

18.3.6

## Hitelesítés

Ha távolsági üzleti tevékenységet folytat, tudnia kell, hogy ki áll a telefon, e-mail vagy fax másik végén. Ugyanez igaz a VPN-hálózatokra is. A VPN-alagút másik végén lévő eszközt hitelesíteni kell, mielőtt a kommunikációs útvonal biztonságosnak tekinthető. Az ábra a két társhitelesítési módszert emeli ki.

Az ábra a különböző hitelesítési lehetőségeket mutatja. A lehetőségek közül a PSK a legkevésbé biztonságos, az RSA pedig a biztonságosabb.

**IPsec-keretrendszer** IPsec-protokoll Titoktartás Integritás Hitelesítés Diffie-Hellman **Choices** AH ESP ESP + AH DES 3DES AES SEAL PSK RSA DH1 DH2 DH5 DH... **Legkevésbé biztonságos Legbiztonságosabb**

* Az előre megosztott titkos kulcs (PSK) értéke minden partnerbe manuálisan kerül beírásra. A PSK más információkkal kombinálva alkotja a hitelesítési kulcsot. A PSK-k manuálisan könnyen konfigurálhatók, de nem jól skálázhatók, mivel minden IPsec-társat minden olyan társ PSK-jával kell konfigurálni, amellyel kommunikál.
* A Rivest, Shamir és Adleman (RSA) hitelesítés digitális tanúsítványokat használ a társak hitelesítésére. A helyi eszköz levezet egy hash-t, és titkosítja azt a privát kulccsal. A titkosított hash-t az üzenethez csatolják, és továbbítják a távoli véghez, és aláírásként működik. A távoli végén a titkosított hash dekódolása a helyi vég nyilvános kulcsával történik. Ha a visszafejtett hash megegyezik az újraszámított hash-sel, akkor az aláírás eredeti. Az alagút biztonságossá tétele előtt minden partnernek hitelesítenie kell a másik partnerét.

Az ábra egy példát mutat a PSK hitelesítésre. A helyi eszközön a hitelesítési kulcsot és az identitásinformációkat egy hash-algoritmuson keresztül küldik el, hogy létrehozzák a kivonatot a helyi társhoz (Hash \_ L). Az egyirányú hitelesítés a Hash \_ L elküldésével jön létre a távoli eszközre. Ha a távoli eszköz önállóan képes létrehozni ugyanazt a hash-t, a helyi eszköz hitelesítése megtörténik. Miután a távoli eszköz hitelesítette a helyi eszközt, a hitelesítési folyamat az ellenkező irányban kezdődik, és minden lépés megismétlődik a távoli eszköztől a helyi eszközig.

Az ábra egy példát mutat a PSK hitelesítésre. A helyi eszközön a hitelesítési kulcsot és az identitásinformációkat a hash algoritmuson keresztül küldik el a hash létrehozásához. A hash elküldésre kerül a távoli eszközre. A távoli eszköz önállóan hozza létre és számítja ki ugyanazt a hash-t, hogy összehasonlítsa a kapott és a számított hash-t. A hash-ek megegyeznek, és a helyi eszköz hitelesítve van.

### PSK hitelesítés

+

+

**Helyi** hitelesítés Kulcsazonosító információ Hash Algorithm Hitelesítő hash   
(Hash\_L) Internet **Remote** Auth. Kulcsazonosító információ Hash Algoritmus Számított hash   
=   
Fogadott hash (Hash\_L)

Az alábbi ábra egy példát mutat az RSA hitelesítésre. A helyi eszközön a hitelesítési kulcsot és az identitásinformációkat a kivonatoló algoritmuson keresztül küldik el, hogy létrehozzák a helyi társhoz tartozó hash-t (Hash \_ L). Ezután a Hash \_ L titkosításra kerül a helyi eszköz privát titkosítási kulcsával. Ez létrehoz egy digitális aláírást. A digitális aláírás és a digitális tanúsítvány továbbításra kerül a távoli eszközre. Az aláírás visszafejtésére szolgáló nyilvános titkosítási kulcsot a digitális tanúsítvány tartalmazza. A távoli eszköz ellenőrzi a digitális aláírást a nyilvános titkosítási kulccsal történő visszafejtéssel. Az eredmény a Hash \_ L. Ezután a távoli eszköz önállóan létrehozza a Hash \_ L értéket a tárolt információkból. Ha a kiszámított Hash \_ L egyenlő a dekódolt Hash \_ L értékkel, a helyi eszköz hitelesítésre kerül. Miután a távoli eszköz hitelesítette a helyi eszközt, a hitelesítési folyamat az ellenkező irányban kezdődik, és minden lépés megismétlődik a távoli eszköztől a helyi eszközig.

Az ábra egy példát mutat az RSA hitelesítésre. A helyi eszközön a hitelesítési kulcsot és az identitásinformációkat a hash algoritmuson keresztül küldik el a hash létrehozásához. A hash-t ezután a helyi eszközök titkos kulcsával titkosítják, ami digitális aláírást eredményez. Az eszközök digitális tanúsítványa és digitális aláírása elküldésre kerül a távoli eszközre. A távoli eszköz visszafejti a digitális aláírást a helyi eszközök nyilvános kulcsával, ami a hash-t eredményezi. A távoli eszköz önállóan hozza létre és számítja ki ugyanazt a hash-t, hogy összehasonlítsa a kapott és a számított hash-t. A hash-ek megegyeznek, és a helyi eszköz hitelesítve van.

### RSA hitelesítés

+ + +

=

**Helyi** hitelesítés Kulcsazonosító információ . Hash Hash\_L privát kulcs titkosítási algoritmus Digitális tanúsítvány Digitális aláírás Internet **távoli** hitelesítés Kulcsazonosító információ Számított Hash digitális aláírás hash visszafejtő algoritmus Dekódolt hash\_L nyilvános kulcsú digitális tanúsítvány

18.3.7

## Biztonságos kulcscsere Diffie-Hellmannel

A titkosítási algoritmusok szimmetrikus, megosztott titkos kulcsot igényelnek a titkosítás és a visszafejtés végrehajtásához. Hogyan jutnak hozzá a titkosító és visszafejtő eszközök a megosztott titkos kulcshoz? A legegyszerűbb kulcscsere módszer egy nyilvános kulcs cseremódszer, például Diffie-Hellman (DH) használata, ahogy az az ábrán látható.

Az ábra a különböző Diffie-Hellman opciókat mutatja. A Diffie-Hellman opciói a legkevésbé biztonságostól a legbiztonságosabbig terjednek: a DH 1 a legkevésbé biztonságos, a DH 2, DH 5, DH 14, DH15, DH 16, DH 19, DH 20, DH 21 és DH 24 a legbiztonságosabb. .

**IPsec Framework** IPsec Protokoll Titoktartás Integritás Hitelesítés Diffie-Hellman **Choices** AH ESP ESP + AH DES 3DES AES SEAL MD5 SHA PSK RSA DH1 DH2 DH5 DH... DH 14, 15, 16   
DH 19, 20, 21, 24 **biztonságos Legbiztonságosabb Legkevésbé**

A DH lehetőséget biztosít két társ számára egy megosztott titkos kulcs létrehozására, amelyet csak ők ismernek, még akkor is, ha nem biztonságos csatornán kommunikálnak. A DH kulcscsere változatai DH csoportokként vannak megadva:

* Az 1-es, 2-es és 5-ös DH-csoport a továbbiakban nem használható. Ezek a csoportok 768 bites, 1024 bites és 1536 bites kulcsméretet támogatnak.
* A 14-es, 15-ös és 16-os DH-csoport nagyobb kulcsméreteket használ, 2048 bites, 3072 bites és 4096 bites, és 2030-ig ajánlott használni.
* A 19-es, 20-as, 21-es és 24-es DH-csoport 256 bites, 384 bites, 521 bites és 2048 bites kulcsmérettel támogatja az elliptikus görbe kriptográfiát (ECC), amely csökkenti a kulcsok generálásához szükséges időt. A 24-es DH csoport az előnyben részesített következő generációs titkosítás.

A választott DH-csoportnak elég erősnek kell lennie, vagy elegendő bittel kell rendelkeznie ahhoz, hogy megvédje az IPsec-kulcsokat a tárgyalás során. Például, ha az AES 128 bites kulcsot választja, használja a 14-es, 19-es, 20-as vagy 24-es csoportot. Ha azonban az AES-256-ot vagy magasabbat választja, használja a 21-es vagy 24-es DH-csoportot.

18.3.8

## Videó – IPsec szállítási és alagútmódok

18.3.9

## Ellenőrizze, hogy megértette – IPsec

Az űrlap teteje

Ellenőrizze, hogy megértette-e az IPsec-et, és válassza ki a megfelelő választ a következő kérdésekre.

1. Az IPsec mely OSI-rétegekben tudja megvédeni a forgalmat? (Válassz négyet.)

Az űrlap alja

Melyik IPsec-funkció használ előre megosztott jelszavakat, digitális tanúsítványokat vagy RSA-tanúsítványokat?

Igaz vagy hamis: Az IPsec-keretrendszert minden új szabvány kifejlesztésekor frissíteni kell.

Mely választási lehetőségeket támogatja az IPsec? (Válassz kettőt.)

Mely választási lehetőségek biztosítják a Titoktartás funkciót az IPsec-keretrendszerben? (Válassz hármat.)

Mely választási lehetőségek biztosítják az Integrity funkciót az IPsec keretrendszerben? (Válassz kettőt.)

Milyen lehetőségek állnak rendelkezésre az IPsec-keretrendszer hitelesítési funkciójához? (Válassz kettőt.)

Mely Diffie-Hellman csoportválasztások nem ajánlottak már?

[18.2](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[VPN Topologies](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[18.4](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[IPsec Protocols](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                                                         
*       

1. VPNs
2. IPsec Protocols

# IPsec protokollok

18.4.1

## Az IPsec-protokoll áttekintése

A két fő IPsec-protokoll a hitelesítési fejléc (AH) és az Encapsulation Security Protocol (ESP). Az IPsec protokoll a keretrendszer első építőköve. Az AH vagy az ESP választása meghatározza, hogy mely további építőelemek állnak rendelkezésre.

Az AH az 51-es IP-protokollt használja, és csak akkor megfelelő, ha a titoktartás nem kötelező vagy megengedett. Biztosítja az adatok hitelesítését és integritását, de nem biztosítja az adatok titkosságát (titkosítást). Az összes szöveget titkosítatlanul továbbítják.

Az ESP az 50-es IP-protokollt használja, és mind a bizalmas kezelést, mind a hitelesítést biztosítja. Az IP-csomag titkosításával titkosítást biztosít. Az ESP hitelesítést biztosít a belső IP-csomaghoz és az ESP-fejléchez. A hitelesítés biztosítja az adatok eredetének hitelesítését és az adatok integritását. Bár az ESP-ben mind a titkosítás, mind a hitelesítés nem kötelező, legalább az egyiket ki kell választani.

Az ábra a különböző IPsec-protokoll-beállításokat mutatja. A lehetőségek a következők: AH, ESP és ESP + A H.

**IPsec-keretrendszer** IPsec-protokoll Titoktartás Integritás Hitelesítés Diffie-Hellman **Choices** AH ESP ESP + AH DES 3DES AES SEAL MD5 SHA RSA PSK DH1 DH2 DH5 DH...

18.4.2

## Hitelesítési fejléc

Az AH úgy éri el a hitelességet, hogy kulcsolt egyirányú hash függvényt alkalmaz a csomagra, hogy létrehozzon egy hash vagy üzenet kivonatot. A hash-t a szöveggel kombinálják, és egyszerű szövegként továbbítják, amint az az ábrán látható. A fogadó a csomag bármely részében az átvitel során bekövetkező változásokat észleli azáltal, hogy ugyanazt az egyirányú hash funkciót hajtja végre a fogadott csomagon, és összehasonlítja az eredményt a küldő által biztosított üzenet kivonat értékével. A hitelesség garantált, mert az egyirányú hash egy megosztott titkos kulcsot is alkalmaz a két rendszer között.

Az AH függvény a teljes csomagra vonatkozik, kivéve azokat az IP-fejlécmezőket, amelyek általában változnak az átvitel során. Azokat a mezőket, amelyek általában változnak a szállítás során, változó mezőknek nevezzük. Például a Time to Live (TTL) mező változtathatónak tekinthető, mivel az útválasztók módosítják ezt a mezőt.

Az AH folyamat a következő sorrendben megy végbe:

1 . Az IP-fejléc és az adathordozó kivonatolása a megosztott titkos kulcs használatával történik.

Az ábrán látható, hogy az AH IPsec protokollt használva a hash a szöveggel kombinálva, egyszerű szövegben kerül továbbításra.

R1

R2

Minden adat egyszerű szövegben Choices SHA MD5 RSA PSK DH2 DH1 DH.. DH5 Integritás Diffie-Hellman hitelesítés

2 . A hash egy új AH fejlécet épít fel, amelyet beilleszt az eredeti csomagba, ahogy az alábbi ábrán látható.

Az ábra egy új AH fejléccel mutatja be a kivonatot, amely az eredeti csomagba kerül.

R1

IP HDR AH adatok IP fejléc + adat + kulcs hash hitelesítési adatok   
(00ABCDEF) Internet

3 . Az új csomag továbbításra kerül az IPsec peer routerhez.

4 . A peer router kivonatolja az IP-fejlécet és az adathordozót a megosztott titkos kulcs segítségével, kivonja a továbbított hash-t az AH-fejlécből, és összehasonlítja a két hash-t, az alábbi ábrán látható módon.

Az ábra azt mutatja be, hogy a peer router kivonatolja az IP-fejlécet és az adathordozót a megosztott titkos kulcs segítségével, kivonja a továbbított hash-t az AH-fejlécből, és összehasonlítja a két hash-t.

R2

=

IP-fejléc AH adatok IP-fejléc + adat + kulcs újraszámított hash   
(00ABCDEF) Hash fogadott   
(00ABCDEF) Hash Internet

A hash-eknek pontosan meg kell egyeznie. Ha egy bit megváltozik az átvitt csomagban, a fogadott csomag hash kimenete megváltozik, és az AH fejléc nem egyezik.

Az AH támogatja az MD5 és SHA algoritmusokat. Előfordulhat, hogy az AH nem működik, ha a környezet NAT-ot használ.

18.4.3

## Encapsulation Security Protocol

Ha az ESP van kiválasztva IPsec-protokollként, akkor egy titkosítási algoritmust is ki kell választani. A Cisco termékek támogatják a 3DES, AES és SEAL szabványokat. A 3DES-t azonban kerülni kell. Ha a 3DES-t végre kell hajtani, akkor állítsa be a kulcsok rövid élettartamát.

Az ESP integritást és hitelesítést is biztosíthat. Először a hasznos adatot titkosítják. Ezután a titkosított hasznos adatot egy hash algoritmuson keresztül küldi el, például SHA-256 vagy újabb. A hash hitelesítést és adatintegritást biztosít az adathordozó számára. Vegye figyelembe, hogy az MD5 és az SHA-1 kerülendő.

Opcionálisan az ESP érvényesítheti a visszajátszás elleni védelmet is. Az újrajátszás elleni védelem ellenőrzi, hogy minden egyes csomag egyedi-e, és nincs-e duplikált. Ez a védelem biztosítja, hogy a hacker ne tudja elkapni a csomagokat, és nem illesztheti be a megváltozott csomagokat az adatfolyamba. Az anti-replay úgy működik, hogy nyomon követi a csomagok sorszámait, és egy csúszó ablakot használ a cél végén.

Amikor kapcsolat jön létre a forrás és a cél között, a számlálók nullára indulnak. Minden alkalommal, amikor egy csomagot elküldenek, a forrás sorszámot fűz a csomaghoz. A cél a csúszó ablak segítségével határozza meg, hogy mely sorszámok várhatók. A rendeltetési hely ellenőrzi, hogy a csomag sorszáma nem duplikált-e, és a megfelelő sorrendben érkezik-e.

Például, ha a célhelyen a csúszóablak egyre van állítva, akkor a rendeltetési hely az első sorszámú csomagot várja. Miután megkapta, a tolóablak kettőre mozdul el. Amikor egy újrajátszott csomag észlelése történik, például a célállomás egy második csomagot kap egy sorszámmal, hibaüzenetet küld a rendszer, a visszajátszott csomagot eldobja, és az eseményt naplózza.

Az anti-replay jellemzően ESP-ben használatos, de az AH-ban is támogatott.

Az ábrán látható, hogy az ESP titkosítást biztosít az adathordozók titkosításával. Az ESP keretrendszer a bizalmas, integritás, hitelesítés és Diffie-Hellman összetevők kiválasztásával épül fel.

R1

R2

Choices Az adatok titkosítva vannak Integritás hitelesítés Diffie-Hellman MD5 SHA PSK RSA DES 3DES AES SEAL DH1 DH2 DH5 DH... Titoktartás

18.4.4

## Az ESP titkosít és hitelesít

Ha a hitelesítés és a titkosítás is ki van választva, először a titkosítás történik. Ennek a feldolgozási sorrendnek az egyik oka, hogy megkönnyíti a visszajátszott vagy hamis csomagok gyors észlelését és elutasítását a fogadó eszköz által. A csomag visszafejtése előtt a vevő hitelesíteni tudja a bejövő csomagokat. Ezzel gyorsan észlelheti a problémákat, és potenciálisan csökkentheti a DoS támadások hatását. Ismétlem, az ESP titkosítással bizalmasságot, hitelesítéssel pedig integritást biztosít.

Eddig a pontig az IPsec vitája az IPv4-re összpontosított. Az IPsec-et azonban eredetileg az IPv6-csomagok biztonságának biztosítására hozták létre. Ezért az IPv4 és IPv6 IPsec-megvalósításai hasonlóak a szabványokat illetően. Az IPv4-ben az AH és az ESP IP protokoll fejlécek. Az IPv6 a kiterjesztés fejléceit használja 50-es következő fejléc értékkel az ESP-nél és 51-es az AH-nál.

Az ábra az ESP-hitelesítést, a titkosított IP-datagramot és a trailert, valamint az ESP-trailert mutatja, amelyek részt vesznek a kivonatolási folyamatban.

R1

R2

IP HDR adatok IP HDR adatok Új IP HDR ESP HDR adatok ESP Előzetes IP HDR ESP   
Hitelesítés Titkosított Hitelesített internet

18.4.5

## Közlekedési és alagút módok

Az ESP és az AH két különböző módban, szállítási módban és alagút módban alkalmazható az IP-csomagokra, amint az az alábbi ábrán látható.

Az ábra az IP-csomagokra két különböző módban, szállítási módban és alagút módban alkalmazott ESP-t és AH-t mutatja.

IP HDR ESP HDR Data ESP Előzetes ESP   
Hitelesítés Szállítási mód Hitelesített Titkosított Új IP HDR ESP HDR Data ESP Előzetes IP HDR ESP   
Hitelesítés Titkosított Hitelesített alagút mód

**Szállítási mód**   
Szállítási módban a biztonság csak az OSI modell és a feletti szállítási rétege számára biztosított. A szállítási mód védi a csomag hasznos terhét, de az eredeti IP-címet egyszerű szövegben hagyja. Az eredeti IP-címet használják a csomag interneten keresztüli továbbítására. Az ESP szállítási módot a gépek között használják.

**Alagút mód**   
Az alagút mód biztonságot nyújt a teljes eredeti IP-csomag számára. Az eredeti IP-csomagot titkosítják, majd egy másik IP-csomagba kapszulázzák. Ez az úgynevezett IP-in-IP titkosítás. A külső IP-csomagon lévő IP-cím a csomag interneten keresztüli továbbítására szolgál.

Az ábra azt mutatja, hogy az ESP alagút módot egy gazdagép és egy biztonsági átjáró, vagy két biztonsági átjáró között használják.

Vállalati irodai HR szerverek Távoli irodai internet Otthoni iroda Vállalati irodai HR szerverek Internet

Az ESP alagút módot egy gazdagép és egy biztonsági átjáró, vagy két biztonsági átjáró között használják, amint az az ábrán látható.

A gazdagéptől az átjáróig tartó alkalmazások esetén előfordulhat, hogy az otthoni irodában nincs útválasztó az IPsec-beágyazás és titkosítás végrehajtásához. Ebben az esetben a PC-n futó IPsec kliens végzi el az IPsec IP-in-IP tokozását és titkosítását. Átjárók közötti alkalmazások esetén ahelyett, hogy az IPsec-et a távoli és vállalati irodák összes számítógépére töltené be, könnyebb a biztonsági átjárók végrehajtani az IP-ben titkosítást és beágyazást. A vállalati irodában az útválasztó kibontja és visszafejti a csomagot.

Az ábra azt mutatja, hogy az AH szállítási mód hitelesítést és integritást biztosít a teljes csomag számára. Nem titkosítja az adatokat, de védve van a módosítástól.

IP HDR AH HDR adatátviteli mód hitelesített Új IP HDR AH HDR adat IP HDR hitelesített alagút mód

Amint az ábrán látható, az AH szállítási mód hitelesítést és integritást biztosít a teljes csomag számára. Nem titkosítja az adatokat, de védve van a módosítástól. Az AH alagút mód az IP-csomagot egy AH-val és egy új IP-fejléccel zárja be, és aláírja a teljes csomagot az integritás és a hitelesítés érdekében.

18.4.6

## Ellenőrizze, hogy megértette – Hasonlítsa össze az AH-t és az ESP-t

Az űrlap teteje

Ellenőrizze, hogy megértette-e az AH és az ESP közötti különbségeket, és válassza ki, hogy az alábbi állítások **igazak** vagy **hamisak** .

1. Az ESP biztosítja az adatok hitelesítését és integritását.

Az űrlap alja

Az ESP titkosságot és hitelesítést biztosít.

Az AH nem biztosítja az adatok titkosságát (titkosítást).

Az AH titkosítást biztosít az IP-csomag titkosításával.

Az ESP hitelesítést biztosít a belső IP-csomaghoz és az ESP-fejléchez.

[18.3](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[IPsec Overview](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[18.5](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Internet Key Exchange](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                                                           
*       

1. VPNs
2. Internet Key Exchange

# Internetes kulcscsere

18.5.1

## Az IKE protokoll

Az Internet Key Exchange (IKE) protokoll egy kulcskezelési protokoll szabvány. Az IKE-t az IPsec-szabvánnyal együtt használják. Amint az ábrán látható, az IKE automatikusan egyeztet az IPsec biztonsági társításokról, és lehetővé teszi az IPsec biztonságos kommunikációt. Az IKE továbbfejleszti az IPsec-et azáltal, hogy funkciókat ad hozzá, és leegyszerűsíti az IPsec-szabvány konfigurációját. Az IKE nélkül az IPsec-konfiguráció bonyolult, manuális konfigurációs folyamat lenne, amely nem skálázható jól.

Az ábra azt mutatja, hogy az IKE automatikusan egyeztet az IPsec biztonsági társításokról, és lehetővé teszi az IPsec biztonságos kommunikációt.

IPsec Protokoll Bizalmasság Integritás Diffie-Hellman hitelesítés ESP SHA PSK DH14 ESP SHA PSK DH14 AES AES Helyi Peer Remote Peer Az IKE egyezteti az SA-kat a társak között.

Az IKE egy hibrid protokoll, amely kulcscsere protokollokat valósít meg az Internet Security Association Key Management Protocol (ISAKMP) keretrendszerén belül. Az ISAKMP (ejtsd: „Ice-a-camp”) határozza meg az üzenetformátumot, a kulcscsere-protokoll mechanikáját és a tárgyalási folyamatot az IPsec SA felépítéséhez.

Ahelyett, hogy a kulcsokat közvetlenül a hálózaton továbbítaná, az IKE adatcsomag-sorozat cseréje alapján számítja ki a megosztott kulcsokat. Ezzel letiltja a harmadik fél számára a kulcsok visszafejtését, még akkor is, ha a harmadik fél rögzítette a kulcsok kiszámításához használt összes kicserélt adatot. Az IKE az 500-as UDP-portot használja az IKE-információk cseréjére a biztonsági átjárók között. Az 500-as UDP-port csomagokat engedélyezni kell minden olyan IP-interfészen, amely egy biztonsági átjárót csatlakozik.

18.5.2

## 1. és 2. fázis kulcsfontosságú tárgyalás

Az IKE az ISAKMP-t használja a kulcstárgyalások 1. és 2. fázisához. Az 1. fázis egy biztonsági társítást (kulcsot) tárgyal két IKE-társ között. Az 1. fázisban egyeztetett kulcs lehetővé teszi az IKE társak számára a biztonságos kommunikációt a 2. fázisban. A 2. fázis egyeztetés során az IKE kulcsokat (biztonsági társításokat) hoz létre más alkalmazásokhoz, például az IPsechez.

Az 1. fázisban két IPsec-társ végzi az SA-k kezdeti egyeztetését. Az 1. fázis alapvető célja az ISAKMP házirend egyeztetése, a társak hitelesítése és egy biztonságos alagút létrehozása a társak között. Ezt az alagutat használják majd fel a 2. fázisban az IPsec-házirend egyeztetésére, amint az az ábrán látható.

Az ábra az IKE 1. és 2. fázisának kulcsfontosságú tárgyalásait mutatja. Az 1. fázis egyezteti az ISAKMP házirendet egy alagút létrehozásához. A 2. fázis megtárgyalja az IPsec-házirendet a biztonságos forgalom alagúton való továbbítására.

3 2 1 1 2

3

Az ISAKMP szabályzat megtárgyalása Az ISAKMP szabályzat megtárgyalása DH kulcscsere Ellenőrizze a partner azonosságát Ellenőrizze a partner azonosságát DH kulcscsere 10. irányelv   
AES   
ITAL   
PSK   
DH14   
élettartamra szóló szabályzat 15   
AES   
ITAL   
PSK   
DH14   
élettartam 1. fázis – ISAKMP szabályzat megtárgyalása alagút létrehozásához. 2. fázis – Az IPsec-házirend megtárgyalása a biztonságos forgalom alagúton való továbbításához. IPsec-házirend megtárgyalása Az IPsec-házirend megtárgyalása

**Megjegyzés** : Az IKE-irányelv és az ISAKMP-irányelv kifejezések egyenértékűek. Ebben a kurzusban az ISAKMP-házirend kifejezést használjuk, hogy jobban illeszkedjenek a parancsokhoz ( **crypto isakmp policy** , **show isakmp policy** stb.), valamint annak tisztázása érdekében, hogy az ISAKMP házirend az IKE 1. fázisú alagútjára vonatkozik.

Az 1. fázis megvalósítható fő módban vagy agresszív módban. A fő mód használatakor a két IKE-társ identitása el van rejtve. Az agresszív módban kevesebb időbe telik, mint a fő módban a kulcsok egyeztetése a társak között. Mivel azonban a hitelesítési kivonatot az alagút létrehozása előtt titkosítatlanul küldik el, az agresszív mód ki van téve a brute force támadásoknak.

**Megjegyzés** : A Cisco IOS szoftverben az IKE hitelesítés alapértelmezett művelete a fő mód elindítása. A Cisco IOS szoftver azonban agresszív módban reagál az agresszív módot kezdeményező IKE-társra.

18.5.3

## 2. fázis: SA-k tárgyalása

Az IKE 2. fázisának célja az IPsec-alagút biztonságossá tételéhez használt IPsec biztonsági paraméterek egyeztetése, az ábrán látható módon. Az IKE 2. fázisát gyors módnak nevezik, és csak azután fordulhat elő, hogy az IKE az 1. fázisban biztonságos alagutat hozott létre. Az SA-kat az ISAKMP IKE-folyamat egyezteti az IPsec nevében, amelynek működéséhez titkosítási kulcsokra van szüksége. A Gyors mód egyezteti az IKE Phase 2 SA-kat. Ebben a fázisban az IPsec által használt SA-k egyirányúak; ezért minden adatfolyamhoz külön kulcscsere szükséges.

A Gyors mód egy új IPsec SA-t is újratárgyal, amikor az IPsec SA élettartama lejár. Alapvetően a gyors mód frissíti a megosztott titkos kulcsot létrehozó kulcsanyagot. Ez az 1. fázis DH-cseréjéből származó kulcsanyagon alapul.

Az ábra azt mutatja, hogy az IKE 2. fázisa a két útválasztó közötti IPsec-alagút biztonságossá tételére szolgáló IPsec biztonsági paraméterek egyeztetésére szolgál.

### Gyors mód

R1 R2 10.0.1.3

192.168.1.3

Host A Host B Negotiate IPsec   
Biztonsági paraméterek

Az IKE 2. verziója, az RFC 5996-on alapuló következő generációs kulcskezelési protokoll az IKE protokoll továbbfejlesztése. Az IKE 2-es verziója támogatja a NAT-észlelést és a NAT-bejárást (NAT-T) az 1. fázisban. Ha mindkét VPN-eszköz NAT-T-képes, és észlelik, hogy NAT-eszközön keresztül csatlakoznak egymáshoz, a NAT-T automatikusan észleli. és automatikusan egyeztetett. A NAT-T beágyazza az ESP-csomagokat az UDP-n belül, és mind a Forrás-, mind a Célportot 4500-nak rendeli hozzá. Mostantól az ESP-csomagok áthaladhatnak a NAT-on.

18.5.4

## Videó - IKE 1. és 2. fázis

[18.4](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[IPsec Protocols](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[18.6](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[VPNs Summary](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                                                                  

1. VPNs
2. VPNs Summary

# VPN-összefoglaló

18.6.1

## Mit tanultam ebben a modulban?

**VPN áttekintése**   
A szervezetek virtuális magánhálózatokat (VPN) használnak végpontok közötti magánhálózati kapcsolatok létrehozására, amelyeket nyilvános hálózaton keresztül továbbítanak. A VPN magánjellegű, mivel a forgalom titkosított, hogy az adatok bizalmasak maradjanak, miközben a nyilvános hálózaton keresztül továbbítják azokat.

A modern VPN-ek már támogatják a titkosítási funkciókat, például az Internet Protocol Security (IPsec) és a Secure Sockets Layer (SSL) szolgáltatást a helyek közötti hálózati forgalom biztonsága érdekében. Az előnyök közé tartozik:

* Költségmegtakarítás
* Biztonság
* Méretezhetőség
* Kompatibilitás

**VPN topológiák**   
Kétféle VPN-topológia létezik:

* **Helyek közötti VPN-ek** – Akkor jön létre, amikor a VPN-átjárók előre be vannak állítva a biztonságos alagút létrehozásához szükséges információkkal. A VPN-forgalom csak ezen eszközök között titkosított. A belső gazdagépek nem tudnak arról, hogy VPN-t használnak.
* **Távoli hozzáférésű VPN-ek** – Ezek a VPN-ek lehetővé teszik a távoli és mobil felhasználók számára, hogy biztonságosan csatlakozzanak a vállalathoz egy titkosított alagút létrehozásával.

A távelérési kapcsolatok a következők lehetnek:

* **Clientless** – A kapcsolat egy webböngésző SSL-kapcsolattal védett. Az SSL a nyilvános kulcsú infrastruktúrát és a digitális tanúsítványokat használja a társak hitelesítésére.
* **Kliens alapú** – A kapcsolat egy ügyfélalkalmazás, például a gazdagépen található Cisco AnyConnect Secure Mobility Client segítségével biztosított.

**IPsec áttekintése**   
Az IPsec egy keretrendszer, amellyel meghatározható, hogy a VPN-kapcsolat miként biztosítja a bizalmasságot, az integritást és a származási hitelesítést. Nem kötődik semmilyen speciális protokollhoz, amely lehetővé teszi számára az új biztonsági technológiák használatával történő integrációt. VPN-kapcsolat létrehozásakor a partnereknek ugyanazt az SA-t kell megosztaniuk a kulcscsere-paraméterek egyeztetéséhez, megosztott kulcs létrehozásához, egymás hitelesítéséhez és a titkosítási paraméterek egyeztetéséhez.

Az IPsec a következőket kínálja:

* **Titoktartás** – Szimmetrikus titkosítási protokollok (azaz AES, SEAL, 3DES és DES) használata.
* **Integritás** – Hashed Message Authentication Code (HMAC) kivonatoló algoritmusok (pl. SHA vagy MD5) használata.
* **Hitelesítés** – előre megosztott titok vagy RSA használata.

A DH lehetőséget biztosít két társ számára egy megosztott titkos kulcs létrehozására, amelyet csak ők ismernek, még akkor is, ha nem biztonságos csatornán kommunikálnak.

**IPsec protokollok**   
A két fő IPsec protokoll a következő:

* **Hitelesítési fejléc (AH)** – 51-es IP-protokoll, amely csak hitelesítést biztosít.
* **Encapsulation Security Protocol (ESP)** – 50-es IP-protokoll, amely hitelesítést és titkosítást biztosít.

Az ESP és az AH alkalmazható IP-csomagokra szállítási mód vagy alagút mód használatával.

**Internetes kulcscsere**   
Az Internet Key Exchange (IKE) protokoll egy kulcskezelési protokoll szabvány, amely az IPsec biztonsági társítások automatikus egyeztetésére és az IPsec biztonságos kommunikációjának lehetővé tételére szolgál. Az IKE az 500-as UDP-portot használja az IKE-információk cseréjére a biztonsági átjárók között.

Az IKE az ISAKMP-t használja a kulcstárgyalások 1. és 2. fázisához. Az 1. fázis egy biztonsági társítást (kulcsot) tárgyal két IKE-társ között. Az 1. fázisban egyeztetett kulcs lehetővé teszi az IKE társak számára a biztonságos kommunikációt a 2. fázisban. A 2. fázis egyeztetés során az IKE kulcsokat (biztonsági társításokat) hoz létre más alkalmazásokhoz, például az IPsechez.

18.6.2

## 18. modul – VPN-kvíz

Az űrlap teteje

1. Egy hálózati rendszergazda VPN alagutat tervez. Miért válassza a mérnök a fő módot az IKE 1. fázisához?

Az űrlap alja

Mi a két VPN-kapcsolat típusa? (Válassz kettőt.)

Melyik IPsec keretprotokoll biztosítja az adatok integritását és hitelesítését, de nem biztosítja az adatok bizalmas kezelését?

Mi használható VPN-átjáróként a VPN közötti helyek beállításakor ?

Melyik két típusú VPN példa a vállalati felügyelt távoli hozzáférésű VPN-ekre? (Válassz kettőt.)

Milyen típusú VPN-hez lehet szükség a Cisco VPN Client szoftverre?

Melyik protokoll nyújt hitelesítési, integritási és bizalmassági szolgáltatásokat, és melyik a VPN egy típusa?

Melyik IPsec biztonsági funkció garantálja, hogy a VPN-en keresztül kapott adatok nem módosultak az átvitel során?

egyik jellemzőjét VPN Melyik állítás írja le a helyek közötti - ek ?

Mi az a VPN-típus, amely általában átlátható a végfelhasználó számára?

Melyik állítás írja le a VPN-t?

Mi az IKE célja?

[18.5](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Internet Key Exchange](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[19.0](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                                                                          
*     

1. Implement Site-to-Site IPsec VPNs
2. Introduction

# Bevezetés

19.0.1

## Miért vegyem ezt a modult?

Mostanra már rendelkezik alapvető ismeretekkel a VPN-ekről. Hogyan konfigurálhat helyek közötti VPN-t? Ha be van állítva, hogyan lehet tesztelni? Ez a modul ezeket a témákat fedi le.

19.0.2

## Mit fogok tanulni ebben a modulban?

**Modul címe:** Helyek közötti IPsec VPN-ek megvalósítása

**Modul célja** : Helyek közötti IPsec VPN konfigurálása előre megosztott kulcsú hitelesítéssel, CLI használatával.

| **téma címe** | **Téma Cél** |
| --- | --- |
| **Helyek közötti IPsec VPN konfigurálása** | Ismertesse az IPsec-egyeztetést és az IPsec-konfiguráció öt lépését. |
| **ISAKMP szabályzat** | Használja a megfelelő parancsokat az ISAKMP-házirend konfigurálásához. |
| **IPsec házirend** | Használja a megfelelő parancsokat az IPsec-házirend konfigurálásához. |
| **Kriptotérkép** | Használja a megfelelő parancsot a Cryptomap konfigurálásához és alkalmazásához. |
| **IPsec VPN** | Konfigurálja az IPsec VPN-t. |

[18.6](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[VPNs Summary](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[19.1](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Configure a Site-to-Site IPsec VPN](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                                                                              
*     

1. Implement Site-to-Site IPsec VPNs
2. Configure a Site-to-Site IPsec VPN

# Helyek közötti IPsec VPN konfigurálása

19.1.1

## IPsec tárgyalás

Ahhoz, hogy egy IPsec VPN alagút működőképes legyen, először meg kell történnie az IPsec egyeztetésnek. A VPN létrehozására irányuló IPsec-tárgyalási folyamat öt lépésből áll, amelyek magukban foglalják az IKE 1. és 2. fázisát.

Kattintson az alábbiakra, ha többet szeretne megtudni az 5 lépésről.

Az Internet Security Association Key Management Protocol (ISAKMP) alagút akkor indul el, amikor A gazdagép „érdekes” forgalmat küld a B gazdagépnek. A forgalom akkor tekinthető érdekesnek, ha a társak között halad, és megfelel az ACL-ben meghatározott feltételeknek.

Az ábra az IPsec VPN-egyeztetés 1. lépését mutatja: Az A gazdagép érdekes forgalmat küld a B gazdagépnek.

10.0.1.3 192.168.1.3 R1 R2 R1

R2

A házigazda B. műsorvezető

Az A gazdagép érdekes forgalmat küld a B gazdagépnek

19.1.2

## Site-to-Site IPsec VPN topológia

A helyek közötti VPN megvalósításához meg kell adni az IKE 1. és 2. fázisának beállításait. Az 1. fázis konfigurációjában a két hely a szükséges ISAKMP biztonsági társításokkal van konfigurálva, hogy biztosítva legyen az ISAKMP alagút létrehozása. A 2. fázis konfigurációjában a két hely az IPsec biztonsági társításokkal van konfigurálva, hogy biztosítsák az IPsec alagút létrehozását az ISAKMP alagúton belül. Mindkét alagút csak akkor jön létre, ha érdekes forgalmat észlel.

Ebben a részben az XYZCORP ábrán látható topológiát használjuk a helyek közötti IPsec VPN megvalósítás bemutatására. Mindkét útválasztó IP-címzéssel és statikus útválasztással van konfigurálva. Egy kiterjesztett ping az R1-en ellenőrzi, hogy a LAN-ok közötti útválasztás működik-e.

Az ábra a helyek közötti IPsec VPN topológiát mutatja, amelyet ebben a szakaszban használunk az interfészek és statikus útvonalak konfigurálásához.

R1 R2 10.0.1.0/24 192.168.1.0/24 10.0.1.3 192.168.1.3 S0/0/0172.30.2.1

S0/0/0172.30.2.2

XYZCORP Site 1 Site 2 Internet

Az interfész és az R1 és R2 alapértelmezett útválasztási konfigurációi a példában láthatók.

**R1# show run**

<output omitted>

!

interface GigabitEthernet0/0

ip address 10.0.1.1 255.255.255.0

!

interface Serial0/0/0

ip address 172.30.2.1 255.255.255.0

!

ip route 192.168.1.0 255.255.255.0 Serial0/0/0

!=========================================

R2# **show run**

<output omitted>

!

interface GigabitEthernet0/0

ip address 192.168.1.1 255.255.255.0

!

interface Serial0/0/0

ip address 172.30.2.2 255.255.255.0

!

ip route 10.0.1.0 255.255.255.0 Serial0/0/0

!

Egy kiterjesztett ping az R1-en ellenőrzi, hogy a LAN-ok közötti útválasztás működik-e, amint az a példa kimenetén látható.

R1# **ping 192.168.1.1 source 10.0.1.1**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:

Packet sent with a source address of 10.0.1.1

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R1#

19.1.3

## IPsec VPN konfigurációs feladatok

**Biztonságpolitikai követelmények**

Az összes XYZCORP VPN-t a következő biztonsági szabályzattal kell megvalósítani:

* A forgalom titkosítása AES 256 és SHA segítségével.
* Hitelesítés a PSK segítségével.
* Kulcscsere a 14-es DH csoporttal.
* Az ISAKMP alagút élettartama 1 óra.
* Az IPsec tunnel ESP-t használ 15 perces élettartammal.

**Konfigurációs feladatok:**

A szabályzat teljesítéséhez szükséges konfigurációs feladatok a következők:

**1. feladat:** Konfigurálja az ISAKMP-házirendet az IKE 1. fázisához   
**2. feladat:** Állítsa be az IPsec-házirendet a 2. fázishoz   
**3. feladat:** Konfiguráljon egy kriptográfiai térképet az IPsec-házirendhez   
**4. feladat:** Alkalmazza az IPsec-házirendet   
**5. feladat:** Ellenőrizze, hogy az IPsec-alagút működőképes-e

19.1.4

## Meglévő ACL-konfigurációk

Bár az XYZCORP nem rendelkezik meglévő ACL-konfigurációval, éles hálózatban ez nem így lenne. A peremi útválasztók általában korlátozó biztonsági politikát alkalmaznak, blokkolva az összes forgalmat, kivéve a kifejezetten engedélyezett forgalmat. A helyek közötti IPsec VPN megvalósítása előtt győződjön meg arról, hogy a meglévő ACL-ek nem blokkolják az IPsec-tárgyalásokhoz szükséges forgalmat. Itt látható az ACL parancs szintaxisa, amely lehetővé teszi az ISAKMP, ESP és AH forgalmat.

Router(config)# **ip access-list extended** name  
 Router(config-ext-nacl)# **permit udp** source wildcard destination wildcard **eq isakmp**  
 Router(config-ext-nacl)# **permit esp** source wildcard destination wildcard  
 Router(config-ext-nacl)# **permit ahp** source wildcard destination wildcard

Az alábbi példa egy ACL-konfigurációt mutat be, amely lehetővé teszi az IPsec-tárgyalásokhoz szükséges forgalmat. Az R2-nek hasonló konfigurációja lenne.

R1(config)# **ip access-list extended INBOUND**

R1(config-ext-nacl)# **permit ip 192.168.1.0 0.0.0.255**  **10.0.1.0 0.0.0.255**

R1(config-ext-nacl)# **permit icmp host 172.30.2.2** **host 172.30.2.1**

R1(config-ext-nacl)# **permit udp host 172.30.2.2 host 172.30.2.1 eq isakmp**

R1(config-ext-nacl)# **permit esp host 172.30.2.2 host 172.30.2.1**

R1(config-ext-nacl)# **permit ahp host 172.30.2.2 host 172.30.2.1**

R1(config-ext-nacl)# **deny ip any any**

R1(config-ext-nacl)# **exit**

R1(config)# **interface serial0/0/0**

R1(config-if)# **ip access-group INBOUND in**

19.1.5

## Broadcast és Multicast forgalom kezelése

Az XYZCORP topológia statikus útválasztást használ, így nincs csoportos küldés vagy broadcast forgalom, amelyet az alagúton kell átirányítani. De mi van, ha az XYZCORP az EIGRP vagy az OSPF bevezetése mellett dönt? Ezek az útválasztási protokollok multicast címeket használnak az útválasztási információk cseréjéhez a szomszédokkal. Az IPsec csak az unicast forgalmat támogatja. A forgalomirányítási protokoll forgalom engedélyezéséhez a helyek közötti IPsec VPN-megvalósításban résztvevő partnereket egy Generic Routing Encapsulation (GRE) alagúttal kell konfigurálni a csoportos küldés forgalomhoz.

A GRE támogatja a többprotokollú alagútkezelést, amint az az ábrán látható. Egy IP-alagúton belül több OSI Layer 3 protokoll csomagtípust is képes beágyazni. Egy további GRE-fejléc hozzáadása a hasznos terhelés és az alagút IP-fejléc közé biztosítja a többprotokollos funkcionalitást. A GRE támogatja az IP multicast tunnelinget is. Az alagúton keresztül használt útválasztási protokollok lehetővé teszik az útválasztási információk dinamikus cseréjét a virtuális hálózatban. A GRE nem biztosít titkosítást. A GRE konfiguráció túlmutat ennek a kurzusnak a keretein.

Az ábra az általános útválasztási beágyazást jeleníti meg, a GRE alagúttal Carrier Protocolként és az IP hálózatot szállítási protokollként. A GRE támogatja a több protokollos alagútkezelést.

### Általános Routing Encapsulation

**GRE alagút**   
(Carrier Protocol) IP-hálózat   
(Transport Protocol) Eredeti IP-csomag   
(Passenger Protocol) IP GRE IP TCP adatok

19.1.6

## Ellenőrizze, hogy megértette-e az IPsec-tárgyalás lépéseit

Az eszközkomponens azonosító nélkül hívott meg

Ellenőrizze, hogy megértette-e az IPsec-egyeztetés lépéseit, ha a legördülő menük segítségével rendeli meg a lépéseket.

**Leírás**

**Lépés száma**

Megkezdődik az IKE 1. fázisa. A társak tárgyalják az ISAKMP SA szabályzatát. Biztonságos alagút jön létre, amikor a társak megállapodnak a házirendben, és hitelesítik őket.

Az IPsec-alagút akkor ér véget, amikor az IPsec SA-kat manuálisan törlik, vagy amikor lejár az élettartamuk.

Az ISAKMP alagút akkor indul el, amikor A gazdagép „érdekes” forgalmat küld a B gazdagépnek.

Az IPsec alagút létrehozása és az adatok átvitele történik az IPsec társak között az IPsec SA-k alapján.

Megkezdődik az IKE 2. fázisa. Az IPsec-társak a hitelesített biztonságos alagutat használják az IPsec SA-házirend egyeztetésére. A megosztott házirend egyeztetése határozza meg az IPsec-alagút létrehozásának módját.

[19.0](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[19.2](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[ISAKMP Policy](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                                                                                 
*     

1. Implement Site-to-Site IPsec VPNs
2. ISAKMP Policy

# ISAKMP szabályzat

19.2.1

## Az alapértelmezett ISAKMP házirendek

Az első feladat az ISAKMP-házirend konfigurálása az IKE 1. fázishoz. Az ISAKMP-házirend felsorolja azokat az SA-kat, amelyeket az útválasztó az IKE 1. fázisalagút létrehozásához használni kíván. A Cisco IOS már az alapértelmezett ISAKMP házirendekkel érkezik. Az alapértelmezett házirendek megtekintéséhez írja be a **show crypto isakmp default policy** parancsot az ábra utáni példában látható módon.

Az ábra a helyek közötti IPsec VPN topológiát mutatja, amelyet ebben a szakaszban használunk az interfészek és statikus útvonalak konfigurálásához.

R1 R2 10.0.1.0/24 192.168.1.0/24 10.0.1.3 192.168.1.3 S0/0/0172.30.2.1

S0/0/0172.30.2.2

XYZCORP Site 1 Site 2 Internet

R1# **show crypto isakmp default policy**

Default IKE policy

Default protection suite of priority 65507

encryption algorithm: AES - Advanced Encryption Standard (128 bit keys).

hash algorithm: Secure Hash Standard

authentication method: Rivest-Shamir-Adleman Signature

Diffie-Hellman group: #5 (1536 bit)

lifetime: 86400 seconds, no volume limit

Default protection suite of priority 65508

encryption algorithm: AES - Advanced Encryption Standard (128 bit keys).

hash algorithm: Secure Hash Standard

authentication method: Pre-Shared Key

Diffie-Hellman group: #5 (1536 bit)

lifetime: 86400 seconds, no volume limit

Default protection suite of priority 65509

encryption algorithm: AES - Advanced Encryption Standard (128 bit keys).

hash algorithm: Message Digest 5

authentication method: Rivest-Shamir-Adleman Signature

Diffie-Hellman group: #5 (1536 bit)

lifetime: 86400 seconds, no volume limit

Default protection suite of priority 65510

encryption algorithm: AES - Advanced Encryption Standard (128 bit keys).

hash algorithm: Message Digest 5

authentication method: Pre-Shared Key

Diffie-Hellman group: #5 (1536 bit)

lifetime: 86400 seconds, no volume limit

Default protection suite of priority 65511

encryption algorithm: Three key triple DES

hash algorithm: Secure Hash Standard

authentication method: Rivest-Shamir-Adleman Signature

Diffie-Hellman group: #2 (1024 bit)

lifetime: 86400 seconds, no volume limit

Default protection suite of priority 65512

encryption algorithm: Three key triple DES

hash algorithm: Secure Hash Standard

authentication method: Pre-Shared Key

Diffie-Hellman group: #2 (1024 bit)

lifetime: 86400 seconds, no volume limit

Default protection suite of priority 65513

encryption algorithm: Three key triple DES

hash algorithm: Message Digest 5

authentication method: Rivest-Shamir-Adleman Signature

Diffie-Hellman group: #2 (1024 bit)

lifetime: 86400 seconds, no volume limit

Default protection suite of priority 65514

encryption algorithm: Three key triple DES

hash algorithm: Message Digest 5

authentication method: Pre-Shared Key

Diffie-Hellman group: #2 (1024 bit)

lifetime: 86400 seconds, no volume limit

Az R1-nek nyolc alapértelmezett ISAKMP-házirendje van, a legbiztonságosabbtól (65507-es házirend) a legkevésbé biztonságosig (65514-es szabályzat). Ha a rendszergazda nem definiált más házirendet, az R1 a legbiztonságosabb alapértelmezett házirendet próbálja meg használni. Ha az R2-nek van egyezési szabályzata, akkor az R1 és R2 sikeresen egyeztetheti az IKE 1. fázisú ISAKMP alagútját anélkül, hogy a rendszergazda bármilyen konfigurációval rendelkezne. Nyolc alapértelmezett irányelv rugalmasságot tesz lehetővé a tárgyalások során. Ha nincs megállapodás a legbiztonságosabb alapértelmezett házirend használatára, az R1 megpróbálja a következő legbiztonságosabb házirendet használni.

Ebben a példában az alapértelmezett házirendek egyike sem egyezik az XYZCORP biztonsági szabályzatával. Tehát új ISAKMP-házirendet kell konfigurálni.

19.2.2

## Szintaxis egy új ISAKMP-házirend konfigurálásához

Új ISAKMP-házirend konfigurálásához használja a **crypto isakmp házirend** parancsot az ábrán látható módon. A parancs egyetlen érve a házirend prioritásának beállítása (1 és 10000 között). A társak a legalacsonyabb számú (legmagasabb prioritású) házirend használatával próbálnak tárgyalni. A társaknak nincs szükségük egyező prioritási számokra.

ISAKMP-házirend konfigurációs módban az IKE 1. fázisú alagút SA-k konfigurálhatók. A **HAGLE** emlékeztető segítségével emlékezzen az öt konfigurálandó SA-ra:

* **H** hamu
* **Hitelesítés** ​
* **G** csoport
* **Élettartam** ​
* **Titkosítás** ​

R1(config)# **crypto isakmp policy ?**

<1-1000> Priority of protection suite

R1(config)# **crypto isakmp policy 1**

R1(config-isakmp)# **?**

ISAKMP commands:

authentication Set authentication method for protection suite

default Set a command to its defaults

encryption Set encryption algorithm for protection suite

exit Exit from ISAKMP protection suite configuration mode

group Set the Diffie-Hellman group

hash Set hash algorithm for protection suite

lifetime Set lifetime for ISAKMP security association

no Negate a command or set its defaults]]>

19.2.3

## ISAKMP házirend-konfiguráció

Az XYZCORP biztonsági szabályzat követelményeinek teljesítése érdekében konfigurálja az ISAKMP házirendet a következő SA-kkal:

* A hash az SHA
* A hitelesítés előre megosztott kulcs
* A csoport 14
* Élettartam 3600 másodperc
* A titkosítás AES

A példa az ISAKMP házirend konfigurációját mutatja be. használja a **show crypto isakmp policy** A konfiguráció ellenőrzéséhez parancsot. Az R2 egyenértékű konfigurációval rendelkezik.

R1(config)# **crypto isakmp policy 1**

R1(config-isakmp)# **encryption aes 256**

R1(config-isakmp)# **hash sha**

R1(config-isakmp)# **authentication pre-share**

R1(config-isakmp)# **group 24**

R1(config-isakmp)# **lifetime 3600**

R1(config-isakmp)# **end**

R1# **show crypto isakmp policy**

Global IKE policy

Protection suite of priority 1

encryption algorithm: AES - Advanced Encryption Standard (256 bit keys).

hash algorithm: Secure Hash Standard

authentication method: Pre-Shared Key

Diffie-Hellman group: #24 (2048 bit, 256 bit subgroup)

lifetime: 3600 seconds, no volume limit

R1#

19.2.4

## Előre megosztott kulcs konfigurálása

Az XYZCORP biztonsági házirend előírja, hogy egy előre megosztott kulcsot kell használni a partnerek közötti hitelesítéshez. Az adminisztrátor megadhat egy gazdagépnevet vagy egy IP-címet a peer számára. A parancs szintaxisa alább látható.

Router(config)# **crypto isakmp key** keystring **address** peer-address  
 Router(config)# **crypto isakmp key** keystring **hostname** peer-hostname

kulcskifejezést **Az XYZCORP a cisco12345** és a peer IP-címét használja, amint az az ábra utáni példákban látható.

Az ábra a helyek közötti IPsec VPN topológiát mutatja, amelyet ebben a szakaszban használunk az interfészek és statikus útvonalak konfigurálásához.

R1 R2 10.0.1.0/24 192.168.1.0/24 10.0.1.3 192.168.1.3 S0/0/0172.30.2.1

S0/0/0172.30.2.2

XYZCORP Site 1 Site 2 Internet

R1# **conf t**

R1(config)# **crypto isakmp key cisco12345 address 172.30.2.2**

R1(config)#

R2# **conf t**

R2(config)# **crypto isakmp key cisco12345 address 172.30.2.1**

R2(config)#

19.2.5

## Szintaxis-ellenőrző – Előre megosztott kulcs konfigurálása

Ezzel a szintaktikai ellenőrzővel konfigurálhatja az R2 ISAKMP-házirendjét.

Configure the ISAKMP policy with priority 1 using the following SA parameters:

* Hash is SHA
* Authentication is pre-shared
* Diffie-Hellman Group is 24
* Lifetime is 3600 seconds
* Encryption is AES with a 256 bit key

R2(config)# crypto isakmp házirend 1

R2(config-isakmp)# hash sha

R2(config-isakmp)# hitelesítési előmegosztás

R2(config-isakmp)# csoport 24

R2(config-isakmp)# élettartama 3600

R2(config-isakmp)# titkosítás aes 256

Állítsa be az előre megosztott ISAKMP-kulcsot a cisco12345 kulcs és a 172.30.2.1, mint a társ IP-címének használatával.

R2(config-isakmp)# crypto isakmp kulcs cisco12345 cím 172.30.2.1

Használja a do parancsot a konfigurációs módban az ISAKMP-házirend megjelenítéséhez.

Az R2(config-isakmp)# a kriptográfiai isakmp szabályzatot mutatja

Globális IKE politika

1. prioritású védelmi csomag

titkosítási algoritmus: AES - Advanced Encryption Standard (256 bites kulcsok).

hash algoritmus: Secure Hash Standard

hitelesítési módszer: Előre megosztott kulcs

Diffie-Hellman csoport: #24 (2048 bites, 256 bites alcsoport)

élettartam: 3600 másodperc, nincs hangerőkorlát

R2(config-isakmp)#

Sikeresen konfigurálta az ISAKMP-házirendet.

[19.1](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Configure a Site-to-Site IPsec VPN](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[19.3](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[IPsec Policy](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                                                                                  
*     

1. Implement Site-to-Site IPsec VPNs
2. IPsec Policy

# IPsec házirend

19.3.1

## Határozza meg az érdekes forgalmat

Bár az IKE 1. fázisú alagút ISAKMP-házirendje konfigurálva van, az alagút még nem létezik. paranccsal ellenőrizheti **show crypto isakmp sa** Ezt az alábbi ábrán látható . Az IKE 1. fázisáról szóló tárgyalások megkezdése előtt érdekes forgalmat kell észlelni. Az XYXCORP helyek közötti VPN esetében érdekes forgalom az 1. és 2. hely LAN közötti engedélyezett kommunikáció.

Az ábra a helyek közötti IPsec VPN topológiát mutatja, amelyet ebben a szakaszban használunk az interfészek és statikus útvonalak konfigurálásához.

R1 R2 10.0.1.0/24 192.168.1.0/24 10.0.1.3 192.168.1.3 S0/0/0172.30.2.1

S0/0/0172.30.2.2

XYZCORP Site 1 Site 2 Internet

R1# **show crypto isakmp sa**

IPv4 Crypto ISAKMP SA

dst src state conn-id status

IPv6 Crypto ISAKMP SA

R1#

Érdekes forgalom meghatározásához állítson be minden útválasztót egy ACL-lel, hogy engedélyezze a forgalmat a helyi LAN-ról a távoli LAN-ra, amint az az alábbi példákban látható R1 és R2 esetében. konfigurációjában fogják használni **Az ACL-t a kriptográfiai leképezés** annak meghatározására, hogy milyen forgalom indítja el az IKE 1. fázisának kezdetét.

R1# **conf t**

R1(config)# **access-list 101 permit ip 10.0.1.0 0.0.0.255 192.168.1.0 0.0.0.255**

R1(config)#

R2# **conf t**

R2(config)# **access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.1.0 0.0.0.255**

R2(config)#

19.3.2

## Az IPsec átalakítási készlet konfigurálása

A következő lépés az IPsec-alagúton keresztül küldött adatok átalakításához használt titkosítási és kivonatolási algoritmusok készletének konfigurálása. Ezt transzformációs halmaznak nevezik. Az IKE 2. fázisának tárgyalásai során a partnerek megállapodnak az IPsec transzformációs készletről, amelyet az érdekes forgalom védelmére használnak.

Konfiguráljon egy transzformációs készletet a **crypto ipsec transform-set** paranccsal, az itt látható módon. Először adjon meg egy nevet a transzformációs halmaznak ( **R1-R2 ).** a példában

R1(config)# **crypto ipsec transform-set ?**

WORD Transform set tag

R1(config)# **crypto ipsec transform-set R1-R2 ?**

ah-md5-hmac AH-HMAC-MD5 transform

ah-sha-hmac AH-HMAC-SHA transform

ah-sha256-hmac AH-HMAC-SHA256 transform

ah-sha384-hmac AH-HMAC-SHA384 transform

ah-sha512-hmac AH-HMAC-SHA512 transform

comp-lzs IP Compression using the LZS compression algorithm

esp-3des ESP transform using 3DES(EDE) cipher (168 bits)

esp-aes ESP transform using AES cipher

esp-des ESP transform using DES cipher (56 bits)

esp-gcm ESP transform using GCM cipher

esp-gmac ESP transform using GMAC cipher

esp-md5-hmac ESP transform using HMAC-MD5 auth

esp-null ESP transform w/o cipher

esp-seal ESP transform using SEAL cipher (160 bits)

esp-sha-hmac ESP transform using HMAC-SHA auth

esp-sha256-hmac ESP transform using HMAC-SHA256 auth

esp-sha384-hmac ESP transform using HMAC-SHA384 auth

esp-sha512-hmac ESP transform using HMAC-SHA512 auth

A transzformációs halmaz elnevezése után a titkosítási és kivonatolási algoritmus bármelyik sorrendben konfigurálható. A példák az R1 és R2 transzformációs készlet konfigurációját mutatják be.

R1(config)# **crypto ipsec transform-set R1-R2 esp-aes esp-sha-hmac**

R1(config)#

R2(config)# **crypto ipsec transform-set R1-R2 esp-aes esp-sha-hmac**

R2(config)#

19.3.3

## Szintaxis-ellenőrző – IPsec átalakítási készlet konfigurálása

Ezzel a szintaktikai ellenőrzővel konfigurálhatja az R2 IPsec-házirendjét.

Állítsa be az IPsec-házirendet az R2-n. Hozzon létre egy kiterjesztett hozzáférési listát 102, amely leírja az érdekes forgalmat 192.168.1.0/24 és 10.0.1.0/24 között.

R2(config)# hozzáférési lista 102 engedélyezése ip 192.168.1.0 0.0.0.255 10.0.1.0 0.0.0.255

nevű IPsec transzformációs készletet **Konfigurálja az R1-R2** a következő utasítások szerint:

* Használja **az esp-aes-t** a titkosításhoz.
* Használja **az esp-sha-hmac-et** a hash-hez.

R2(config)# crypto ipsec transzformációs készlet R1-R2 esp-aes esp-sha-hmac

R2(config)#

Sikeresen konfigurálta az IPsec-házirendet.

[19.2](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[ISAKMP Policy](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[19.4](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Crypto Map](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                                                                                    
*     

1. Implement Site-to-Site IPsec VPNs
2. Crypto Map

# Kriptotérkép

19.4.1

## Szintaxis a kriptográfiai térkép konfigurálásához

Most, hogy az érdekes forgalom meghatározásra került, és egy IPsec-transzformációs készlet konfigurálva van, itt az ideje, hogy ezeket a konfigurációkat összekapcsolja az IPsec-házirend többi részével egy titkosítási térképen. Az alábbiakban látható a kriptográfiai térképkészlet indításának szintaxisa. A sorszám fontos több titkosítási leképezési bejegyzés konfigurálásakor. Az XYZCORP-nak csak egy titkosítási térkép-bejegyzésre lesz szüksége, hogy megfeleljen a forgalomnak, és figyelembe vegye a fennmaradó SA-kat. Bár az **ipsec-manual** opció látható, annak használata meghaladja a kurzus kereteit.

Router(config)# **crypto map** map-name seq-num { **ipsec-isakmp** | **ipsec-manual** }

| **Paraméter** | **Leírás** |
| --- | --- |
| térképnév | Azonosítja a kriptográfiai térképkészletet. |
| sorszám | A kriptográfiai térkép bejegyzéshez hozzárendelt sorszám. Használja a **crypto map** map-name seq-num parancsot kulcsszó nélkül a meglévő titkosítási térkép bejegyzés vagy profil módosításához. |
| **ipsec-isakmp** | Azt jelzi, hogy az IKE-t az IPsec létrehozására fogják használni az ezen kriptotérkép-bejegyzésben meghatározott forgalom védelmére. |
| **ipsec-kézikönyv** | Azt jelzi, hogy az IKE-t nem fogják használni az IPsec SA-k létrehozására a kriptográfiai leképezési bejegyzésben meghatározott forgalom védelmére. |

Az alábbiakban láthatók a kriptográfiai térkép-bejegyzés elérhető konfigurációi, amikor kriptográfiai térkép konfigurációs módban van. A térkép neve **R1-R2 \_ MAP** , a sorszám pedig **10** .

R1(config)# **crypto map R1-R2\_MAP 10 ipsec-isakmp**

% NOTE: This new crypto map will remain disabled until a peer

and a valid access list have been configured.

R1(config-crypto-map)# **?**

Crypto Map configuration commands:

default Set a command to its defaults

description Description of the crypto map statement policy

dialer Dialer related commands

disable Disable this crypto-map-statement.

exit Exit from crypto map configuration mode

match Match values.

no Negate a command or set its defaults

qos Quality of Service related commands

reverse-route Reverse Route Injection.

set Set values for encryption/decryption

19.4.2

## Kriptotérkép konfigurációja

A konfiguráció befejezéséhez, hogy megfeleljen az XYZCORP IPsec biztonsági szabályzatának, tegye a következőket:

**1. lépés** Kösd össze az ACL-t és a transzformációs készletet a térképhez.   
**2. lépés:** Adja meg a társ IP-címét.   
**3. lépés** Konfigurálja a DH csoportot.   
**4. lépés:** Konfigurálja az IPsec alagút élettartamát.

Az R1 és R2 titkosítási térkép konfigurációi az alábbiakban láthatók.

R1(config)# **crypto map R1-R2\_MAP 10 ipsec-isakmp**

% NOTE: This new crypto map will remain disabled until a peer

and a valid access list have been configured.

R1(config-crypto-map)# **match address 101**

R1(config-crypto-map)# **set transform-set R1-R2**

R1(config-crypto-map)# **set peer 172.30.2.2**

R1(config-crypto-map)# **set pfs group24**

R1(config-crypto-map)# **set security-association lifetime seconds 900**

R1(config-crypto-map)# **exit**

R1(config)#

R2(config)# **crypto map R1-R2\_MAP 10 ipsec-isakmp**

% NOTE: This new crypto map will remain disabled until a peer

and a valid access list have been configured.

R2(config-crypto-map)# **match address 102**

R2(config-crypto-map)# **set transform-set R1-R2**

R2(config-crypto-map)# **set peer 172.30.2.1**

R2(config-crypto-map)# **set pfs group24**

R2(config-crypto-map)# **set security-association lifetime seconds 900**

R2(config-crypto-map)# **exit**

R2(config)#

Használja a **show crypto map** parancsot a kriptográfiai térkép konfigurációjának ellenőrzéséhez, ahogy az R1 esetében látható. Minden szükséges SA-nak a helyén kell lennie. Figyelje meg, hogy a kimenet azt mutatja, hogy jelenleg egyetlen interfész sem használja a titkosítási térképet.

R1# **show crypto map**

Crypto Map IPv4 "R1-R2\_MAP" 10 ipsec-isakmp

Peer = 172.30.2.2

Extended IP access list 101

access-list 101 permit ip 10.0.1.0 0.0.0.255 192.168.1.0 0.0.0.255

Security association lifetime: 4608000 kilobytes/900 seconds

Responder-Only (Y/N): N

PFS (Y/N): Y

DH group: group24

Mixed-mode : Disabled

Transform sets={

R1-R2: { esp-aes esp-sha-hmac } ,

}

Interfaces using crypto map R1-R2\_MAP:

R1#

19.4.3

## Alkalmazza és ellenőrizze a kriptográfiai térképet

A titkosítási leképezés alkalmazásához lépjen be az interfész konfigurációs módjába a kimenő felülethez, és konfigurálja a **kriptográfiai leképezés** leképezése parancsot. Az alábbiakban az XYZCORP konfigurációja látható. Figyelje meg, hogy a **kriptográfiai térkép** megjelenítése most azt mutatja, hogy a soros 0/0/0 interfész a titkosítási térképet használja. Az R2 ugyanazzal a paranccsal van konfigurálva a Serial 0/0/0 interfészén.

R1(config)# **interface serial0/0/0**

R1(config-if)# **crypto map R1-R2\_MAP**

R1(config-if)#

\*Mar 19 19:36:36.273: %CRYPTO-6-ISAKMP\_ON\_OFF: ISAKMP is ON

R1(config-if)# **end**

R1# **show crypto map**

Crypto Map IPv4 "R1-R2\_MAP" 10 ipsec-isakmp

Peer = 172.30.2.2

Extended IP access list 101

access-list 101 permit ip 10.0.1.0 0.0.0.255 192.168.1.0 0.0.0.255

Security association lifetime: 4608000 kilobytes/900 seconds

Responder-Only (Y/N): N

PFS (Y/N): Y

DH group: group24

Mixed-mode : Disabled

Transform sets={

R1-R2: { esp-aes esp-sha-hmac } ,

}

Interfaces using crypto map R1-R2\_MAP:

Serial0/0/0

19.4.4

## Szintaxis-ellenőrző – A kriptográfiai térkép konfigurálása, alkalmazása és ellenőrzése

Ezzel a szintaktikai ellenőrzővel konfigurálhat, alkalmazhat és ellenőrizhet titkosítási leképezést az R2-n.

Configure the crypto map on R2 to bind the transform set and IPsec policy using the following parameters:

* Crypto map name is **R1-R2\_MAP**.
* Sequence number is **10**.
* Bind access list 102 and transform set **R1-R2**.
* Peer IP address is 172.30.2.1.
* Diffie-Hellman Group is **group24**.
* SA lifetime is 900 seconds.

R2(config)#crypto map R1-R2\_MAP 10 ipsec-isakmp

% NOTE: This new crypto map will remain disabled until a peer

and a valid access list have been configured.

R2(config-crypto-map)#match address 102

R2(config-crypto-map)#set transform-set R1-R2

R2(config-crypto-map)#set peer 172.30.2.1

R2(config-crypto-map)#set pfs group24

R2(config-crypto-map)#set security-association lifetime seconds 900

Alkalmazza az **R1-R2 \_ MAP-ot** az s0/0/0 interfészre.

R2(config-crypto-map)# interfész s0/0/0

R2(config-if)# kriptográfiai leképezés R1-R2\_MAP

\*Március 19. 19:36:36.273: %CRYPTO-6-ISAKMP\_ON\_OFF: Az ISAKMP BE van kapcsolva

A kriptográfiai térkép megjelenítéséhez használja a **do** parancsot konfigurációs módban.

Az R2(config-if)# megmutatja a kriptográfiai térképet

Crypto Map IPv4 "R1-R2\_MAP" 10 ipsec-isakmp

Peer = 172.30.2.1

Kibővített IP-hozzáférési lista 102

hozzáférési lista 102 engedély ip 192.168.1.0 0.0.0.255 10.0.1.0 0.0.0.255

Biztonsági társítás élettartama: 4608000 kilobájt/900 másodperc

Csak válaszadó (I/N): N

PFS (I/N): I

DH csoport: csoport24

Vegyes mód: Letiltva

Transform sets={

R1-R2: {esp-aes esp-sha-hmac},

}

Az R1-R2\_MAP titkosítási térképet használó interfészek:

Sorozat0/0/0

R2(config-if)#

Sikeresen konfigurálta és alkalmazta a kriptográfiai térképet.

[19.3](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[IPsec Policy](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[19.5](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[IPsec VPN](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                                                                                        
*     

1. Implement Site-to-Site IPsec VPNs
2. IPsec VPN

# IPsec VPN

19.5.1

## Érdekes forgalom küldése

Most, hogy az ISAKMP- és az IPsec-házirendek is be vannak állítva, és a titkosítási leképezést alkalmazták a megfelelő kimenő interfészekre, tesztelje a két alagutat úgy, hogy érdekes forgalmat küld a linken keresztül.

Az R1 LAN interfészéről érkező forgalom, amely az R2 LAN interfészére irányul, érdekes forgalomnak számít, mert megegyezik a mindkét útválasztón konfigurált ACL-ekkel. Az R1-től érkező kiterjesztett **ping** hatékonyan teszteli a VPN konfigurációt. A kiterjesztett **ping** parancs szintaxisa és eredményei az alábbiakban láthatók. Az első ping meghiúsult, mert néhány ezredmásodpercbe telik az ISAKMP és az IPsec alagút létrehozása.

R1# **ping 192.168.1.1 source 10.0.1.1**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:

Packet sent with a source address of 10.0.1.1

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/4 ms

R1#

19.5.2

## Ellenőrizze az ISAKMP és az IPsec alagutakat

Érdekes forgalom küldése valójában nem jelenti azt, hogy az alagutak létrejöttek. Az R1 és R2 akkor is átirányítja a forgalmat a két LAN között, ha az ISAKMP és az IPsec házirend-konfiguráció hibás. Az alagutak létrehozásának ellenőrzéséhez használja a **show crypto isakmp sa** és **a show crypto ipsec sa** parancsokat. Az alábbi kimeneten figyelje meg, hogy az alagút aktív a két társ, a 172.30.2.1 és a 172.30.2.2 között, és ezek az **R1-R2\_MAP** kriptográfiai térképet használják.

R1# **show crypto isakmp sa**

IPv4 Crypto ISAKMP SA

dst src state conn-id status

172.30.2.2 172.30.2.1 QM\_IDLE 1005 ACTIVE

IPv6 Crypto ISAKMP SA

R1#

R1# **show crypto ipsec sa**

interface: Serial0/0/0

Crypto map tag: R1-R2\_MAP, local addr 172.30.2.1

protected vrf: (none)

local ident (addr/mask/prot/port): (10.0.1.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)

current\_peer 172.30.2.2 port 500

PERMIT, flags={origin\_is\_acl,}

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4

#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 172.30.2.1, remote crypto endpt.: 172.30.2.2

plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0

current outbound spi: 0xD3E56A5F(3555027551)

PFS (Y/N): Y, DH group: group24

inbound esp sas:

spi: 0x5D620493(1566704787)

transform: esp-aes esp-sha-hmac ,

in use settings ={Tunnel, }

conn id: 2019, flow\_id: Onboard VPN:19, sibling\_flags 80004040, crypto map: R1-R2\_MAP

sa timing: remaining key lifetime (k/sec): (4155730/802)

IV size: 16 bytes

replay detection support: Y

Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0xD3E56A5F(3555027551)

transform: esp-aes esp-sha-hmac ,

in use settings ={Tunnel, }

conn id: 2020, flow\_id: Onboard VPN:20, sibling\_flags 80004040, crypto map: R1-R2\_MAP

sa timing: remaining key lifetime (k/sec): (4155730/802)

IV size: 16 bytes

replay detection support: Y

Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

R1#

19.5.3

## Szintaxis-ellenőrző – Ellenőrizze az ISAKMP és IPsec alagutakat

Ezzel a szintaktikai ellenőrzéssel ellenőrizze az R2 IPsec VPN-jét.

Establish the tunnel on R2 by by pinging 10.0.1.1 with a source address of 192.168.1.1.

R2#ping ip 10.0.1.1 source 192.168.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.0.1.1, timeout is 2 seconds:

Packet sent with a source address of 192.168.1.1

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/4 ms

Display the ISAKMP tunnel status.

R2#show crypto isakmp sa

IPv4 Crypto ISAKMP SA

dst src state conn-id status

172.30.2.1 172.30.2.2 QM\_IDLE 1005 ACTIVE

IPv6 Crypto ISAKMP SA

Display the IPsec tunnel status.

R2#show crypto ipsec sa

interface: Serial0/0/0

Crypto map tag: R1-R2\_MAP, local addr 172.30.2.2

protected vrf: (none)

local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (10.0.1.0/255.255.255.0/0/0)

current\_peer 172.30.2.1 port 500

PERMIT, flags={origin\_is\_acl,}

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4

#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 172.30.2.2, remote crypto endpt.: 172.30.2.1

plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0

current outbound spi: 0xD3E56A5F(3555027551)

PFS (Y/N): Y, DH group: group24

inbound esp sas:

spi: 0x5D620493(1566704787)

transform: esp-aes esp-sha-hmac ,

in use settings ={Tunnel, }

conn id: 2019, flow\_id: Onboard VPN:19, sibling\_flags 80004040, crypto map: R1-R2\_MAP

sa timing: remaining key lifetime (k/sec): (4155730/802)

IV size: 16 bytes

replay detection support: Y

Status: ACTIVE(ACTIVE)

<output omitted>

R2#

You have successfully verified the IPsec VPN.

19.5.4

## Videó – Site-to-Site IPsec VPN konfiguráció

19.5.5

## Packet Tracer – Helyek közötti IPsec VPN konfigurálása és ellenőrzése

Ebben a Packet Tracerben a következő célokat valósítja meg:

* Ellenőrizze a kapcsolatot az egész hálózaton
* Konfigurálja az R1 útválasztót, hogy támogassa a helyek közötti IPsec VPN-t R3-mal

[Helyek közötti IPsec VPN konfigurálása és ellenőrzése](https://contenthub.netacad.com/courses/netsec/_common/19.5.5-packet-tracer---configure-and-verify-a-site-to-site-ipsec-vpn.pka)

19.5.6

## Lab – Helyek közötti VPN konfigurálása

Ebben a laborban a következő célokat kell teljesítenie:

* Konfigurálja az alapvető eszközbeállításokat.
* Konfiguráljon helyek közötti VPN-t a Cisco IOS használatával.

[19.4](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Crypto Map](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[19.6](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Implement Site-to-Site IPsec VPNs Summary](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                                                                                             

1. Implement Site-to-Site IPsec VPNs
2. Implement Site-to-Site IPsec VPNs Summary

# Helyezze el a helyek közötti IPsec VPN-összefoglalót

19.6.1

## Mit tanultam ebben a modulban?

**Konfiguráljon egy helyek közötti VPN-t**   
A VPN létrehozására irányuló IPsec-egyeztetés öt lépésből áll, amelyek magukban foglalják az IKE 1. és 2. fázisát. Az ISAKMP alagút akkor indul, amikor az A gazdagép „érdekes” forgalmat küld a B gazdagépnek. A forgalom akkor tekinthető érdekesnek, ha a társak között halad, és megfelel a kritériumoknak. amelyek az ACL-ben vannak meghatározva. Megkezdődik az IKE 1. fázisa. A társak tárgyalják az ISAKMP SA szabályzatát. Amikor a társak megállapodnak a házirendben és hitelesítik őket, és létrejön egy biztonságos alagút. Megkezdődik az IKE 2. fázisa. Az IPsec-társak a hitelesített biztonságos alagutat használják az IPsec SA-házirend egyeztetésére. A megosztott házirend egyeztetése határozza meg az IPsec-alagút létrehozásának módját. Létrejön az IPsec alagút, és az adatok átvitele történik meg az IPsec társak között az IPsec SA-k alapján. Az IPsec-alagút akkor ér véget, amikor az IPsec SA-kat manuálisan törlik, vagy amikor lejár az élettartamuk. A helyek közötti VPN megvalósításához meg kell adni az IKE 1. és 2. fázisának beállításait. Az 1. fázis konfigurációjában a két hely a szükséges ISAKMP biztonsági társításokkal van konfigurálva, hogy biztosítva legyen az ISAKMP alagút létrehozása. A 2. fázis konfigurációjában a két hely az IPsec biztonsági társításokkal van konfigurálva annak biztosítására, hogy az ISAKMP alagúton belül IPsec alagút jöjjön létre. Mindkét alagút csak akkor jön létre, ha érdekes forgalmat észlel. Az IPsec csak az unicast forgalmat támogatja. A csoportos küldés útválasztási protokoll forgalmának engedélyezéséhez a helyek közötti IPsec VPN-megvalósításban részt vevő partnereket egy Generic Routing Encapsulation (GRE) alagúttal kell konfigurálni a csoportos küldés forgalomhoz. A GRE támogatja a többprotokollú alagútkezelést. Egy IP-alagúton belül több OSI Layer 3 protokoll csomagtípust is képes beágyazni. A hasznos adat és az alagút IP-fejléc közé egy további GRE-fejléc hozzáadása biztosítja a többprotokollos funkcionalitást. A GRE támogatja az IP multicast tunnelinget is. Az alagúton keresztül használt útválasztási protokollok lehetővé teszik az útválasztási információk dinamikus cseréjét a virtuális hálózatban. A GRE nem biztosít titkosítást.

**ISAKMP szabályzat**   
Az ISAKMP házirend felsorolja azokat az SA-kat, amelyeket az útválasztó hajlandó használni az IKE 1. fázisú alagút létrehozásához. A Cisco IOS már az alapértelmezett ISAKMP házirendekkel érkezik. Az alapértelmezett házirendek megtekintéséhez írja be a **show crypto isakmp default policy** parancsot. Az útválasztó megkísérli a legbiztonságosabb alapértelmezett házirendet használni, ha a rendszergazda nem definiált más házirendet. Új ISAKMP-házirend konfigurálásához használja a **crypto isakmp házirend** parancsot. Az öt konfigurálandó SA a hash, a hitelesítés, a csoportos, az élettartam és a titkosítás (HAGLE).

**IPsec házirend**   
Bár az IKE 1. fázisú alagút ISAKMP-házirendje konfigurálva van, az alagút még nem létezik. paranccsal ellenőrizzük **Ezt a show crypto isakmp sa** . Érdekes forgalom meghatározásához konfiguráljon minden útválasztót egy ACL-lel, hogy engedélyezze a forgalmat a helyi LAN-ról a távoli LAN-ra. Az ACL-t a kriptográfiai leképezés konfigurációjában fogja használni annak meghatározására, hogy milyen forgalom indítja el az IKE 1. fázisának kezdetét. Konfigurálja az IPsec-alagúton keresztül küldött adatok átalakításához használt titkosítási és kivonatolási algoritmusokat. Konfiguráljon egy transzformációs készletet a **crypto ipsec transform-set** paranccsal.

**Kriptotérkép**   
Most, hogy az érdekes forgalom meghatározása megtörtént, és egy IPsec-transzformációs készlet konfigurálva van, itt az ideje, hogy ezeket a konfigurációkat összekapcsolja az IPsec-házirend többi részével egy kriptográfiai térképen. Az IPsec biztonsági szabályzatnak való megfelelés érdekében a konfigurálás befejezéséhez össze kell kötnie az ACL-t és az átalakítási készletet a leképezéssel, meg kell adnia a társ IP-címét, konfigurálnia kell a DH csoportot, és konfigurálnia kell az IPsec alagút élettartamát. A **kriptográfiai térkép megjelenítése** paranccsal ellenőrizze a kriptográfiai térkép konfigurációját. A titkosítási leképezés alkalmazásához lépjen be az interfész konfigurációs módjába a kimenő felülethez, és konfigurálja a **kriptográfiai leképezés** leképezése parancsot.

**IPsec VPN**   
Az ISAKMP és az IPsec házirendek konfigurálása és a titkosítási leképezés alkalmazása után a megfelelő kimenő interfészeken tesztelje a két alagutat úgy, hogy érdekes forgalmat küld a hivatkozáson keresztül. A kiterjesztett ping hatékonyan teszteli a VPN konfigurációt. Az alagutak létrehozásának ellenőrzéséhez használja a **show crypto isakmp sa** és **a show crypto ipsec sa** parancsokat.

19.6.2

## 19. modul – Helyek közötti IPsec VPN-kvíz megvalósítása

Az űrlap teteje

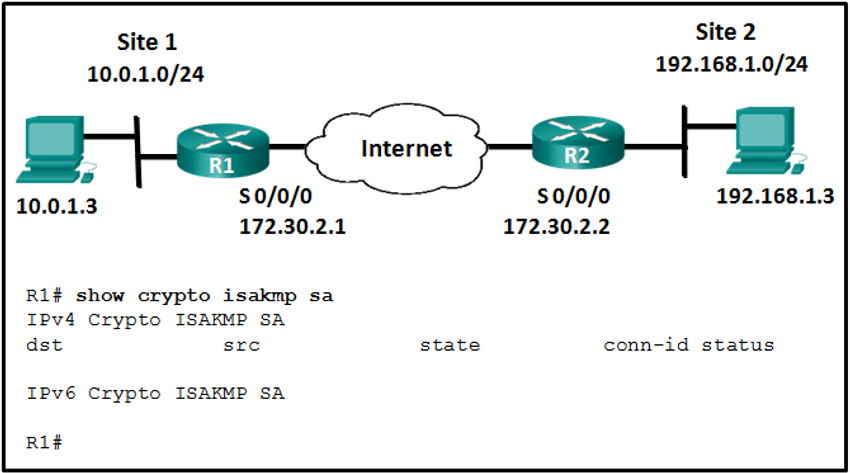
1. Mit definiál az ISAKMP szabályzat?

Az űrlap alja

Melyik az az öt biztonsági társítás, amelyet ISAKMP-házirend-konfigurációs módban kell konfigurálni?

Milyen parancs vagy művelet ellenőrzi, hogy létrejött-e VPN-alagút?

ek létrehozásához VPN Milyen három protokollt kell engedélyezni a vállalati tűzfalon keresztül az IPsec helyek közötti - ? (Válassz hármat.)

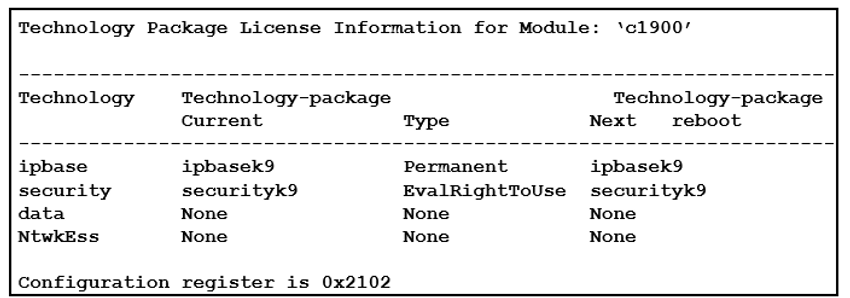


Hivatkozz a kiállításra. Az IKE 1. fázisú alagút ISAKMP-házirendje be van állítva, de az alagút még nem létezik. Milyen lépéseket kell megtenni az IKE 1. fázisáról szóló tárgyalások megkezdése előtt?

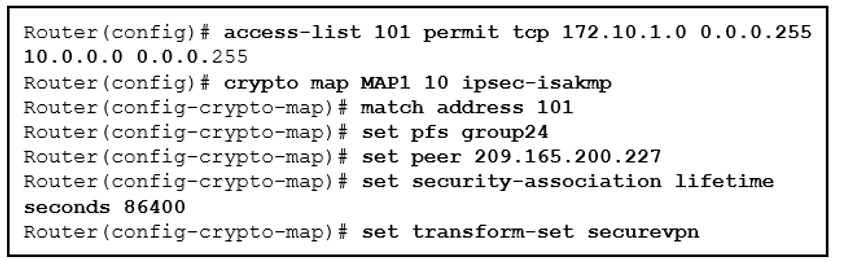
Miről tárgyalnak egy IPsec-alagút létrehozása két IPsec-gazda között az IKE 1. fázisában?

Egy hálózati elemző egy kriptográfiai térképet konfigurál, és éppen hozzákötötte az ACL-t és az átalakítási készletet a térképhez, és beállította az IPsec alagút élettartamát. Milyen további lépéssel fejeződik be a kriptográfiai térkép konfigurálása?

Mi az első lépés az IPsec VPN létrehozásához?



Hivatkozz a kiállításra. parancs részleges kimenetére **Tekintettel a show version** egy útválasztón, ha egy hálózati mérnök el akarja kezdeni az IPsec VPN konfigurálását, mi lenne a következő lépés?



Hivatkozz a kiállításra. Hogyan kezeli az útválasztó a 101-es hozzáférési listának nem megfelelő forgalmat?

[19.5](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[IPsec VPN](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[20.0](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                                                                                                 
*   

1. Introduction to the ASA
2. Introduction

# Bevezetés

20.0.1

## Miért vegyem ezt a modult?

Ebben a modulban megismerheti a Cisco ASA Firewall modelleket. Melyik modell a legjobb választás? Ez a szervezet követelményeitől függ. Olvasson tovább, hogy többet megtudjon!

20.0.2

## Mit fogok tanulni ebben a modulban?

**Modul címe:** Bevezetés az ASA-ba

**A modul célja** : Ismertesse, hogyan működik az ASA fejlett állapotjelző tűzfalként.

| **téma címe** | **Téma Cél** |
| --- | --- |
| **ASA megoldások** | Hasonlítsa össze az ASA megoldásokat más útválasztó tűzfaltechnológiákkal. |
| **Az ASA 5506-X FirePOWER szolgáltatásokkal** | Ismertessen három ASA-telepítési forgatókönyvet. |

[19.6](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Implement Site-to-Site IPsec VPNs Summary](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[20.1](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[ASA Solutions](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                                                                                                       
*   

1. Introduction to the ASA
2. ASA Solutions

# ASA megoldások

20.1.1

## ASA tűzfalmodellek

Az IOS útválasztó tűzfal megoldása megfelelő kis fióktelepekhez és a Cisco IOS rendszerben jártas rendszergazdák számára. Az IOS tűzfalmegoldások azonban nem skálázhatók jól, és általában nem tudják kielégíteni a nagyvállalatok igényeit.

A Cisco ASA FirePOWER Services termékcsaláddal dedikált tűzfalszolgáltatásokat kínál egyetlen eszközben. Ezek a következő generációs tűzfal (NGFW) eszközök, amelyek integrált fenyegetésvédelmet biztosítanak a teljes támadási kontinuumon.

Számos ASA-modell létezik, amelyek megfelelnek a különféle szervezetek igényeinek. A Cisco ASA eszközök számos követelménynek és hálózatméretnek megfelelően méretezhetők. Az ASA-modell kiválasztása a szervezet követelményeitől függ, például a maximális átviteli sebességtől, a másodpercenkénti maximális kapcsolatoktól és a költségvetéstől.

A következő ábrák ezeket a modelleket és állapotalapú ellenőrzési teljesítményüket mutatják be.

Minden modell fejlett állapotalapú tűzfal funkciókat és VPN-funkciókat kínál. A legnagyobb különbség a modellek között az egyes modellek által kezelt maximális forgalom, valamint az interfészek száma és típusa.

Kattintson az alábbiakra, ha többet szeretne megtudni a különböző ASA modellekről.

Ez a modell kis irodai és otthoni irodai (SOHO) és kisvállalkozások számára alkalmas.



A Cisco a modern x86-os szerverek megnövekedett energiaellátásának kihasználásával támogatja a számítási infrastruktúra virtualizációját is. A Cisco Adaptive Security Virtual Appliance (ASAv) az ASA készülékek erejét a virtuális tartományba hozza. A kiszolgáló-hipervizor létrehozhat egy virtuális kapcsolót, amely számos típusú virtuális gép (VM) támogatására képes. A Cisco ASAv virtuális gépként működik, amely a kiszolgáló interfészeit használja a forgalom feldolgozására.

A fizikai Cisco ASA eszközökhöz hasonlóan az ASAv is támogatja a helyek közötti VPN, a távoli hozzáférésű VPN és az ügyfél nélküli VPN funkciókat.

**Megjegyzés:** Az ASAv nem támogatja a fürtözést és a több kontextust.

Az ügyfelek igényeinek megfelelő illeszkedés érdekében a Cisco ASAv öt modellben kapható:

* **Cisco ASAv5** – Ez a készülék 2 GB memóriát igényel, és akár 100 Mb/s állapotalapú ellenőrzési átviteli sebességet biztosít.
* **Cisco ASAv10** – Ez a készülék 4 GB memóriát igényel, és akár 1 Gb/s állapotalapú ellenőrzési adatátvitelt biztosít.
* **Cisco ASAv30** – Ez a készülék 8 GB memóriát igényel, és akár 2 Gb/s állapotalapú ellenőrzési adatátvitelt biztosít.
* **Cisco ASAv50** – Ez a készülék 16 GB memóriát igényel, és akár 10 Gb/s állapotalapú ellenőrzési átviteli sebességet biztosít.
* **Cisco ASAv100** – Ez a készülék 32 GB memóriát igényel, és akár 20 Gb/s állapotalapú ellenőrzési átviteli sebességet biztosít.

**Megjegyzés** : Ennek a modulnak a középpontjában az ASA 5506-X áll, amelyet kisvállalkozások, fiókirodák és vállalati távmunkások megvalósítására terveztek.

20.1.2

## Videó - Cisco ASA következő generációs tűzfaleszközök

20.1.3

## Fejlett ASA tűzfal funkciók

Kattintson az alábbi gombra, ha többet szeretne megtudni a speciális funkciókról.

Az ábra szerint egyetlen ASA több virtuális eszközre particionálható. Minden virtuális eszközt biztonsági kontextusnak nevezünk. Mindegyik kontextus egy független eszköz, saját biztonsági szabályzattal, interfészekkel és rendszergazdákkal. A több kontextus hasonló a több önálló eszköz használatához. Számos szolgáltatás több környezeti módban támogatott, beleértve az útválasztási táblákat, a tűzfalfunkciókat, az IPS-t és a felügyeletet. Egyes funkciók nem támogatottak, beleértve a VPN-t és a dinamikus útválasztási protokollokat.

Az ábra az ASA virtualizáció topológiáját mutatja. egy útválasztó csatlakozik az internethez és egyetlen eszközhöz. az asa eszköz 3 biztonsági kontextusra van felosztva, amelyek biztonsági kontextus a, biztonsági kontextus b és biztonsági kontextus c. három ügyfél csatlakozik egyetlen asa eszközhöz, de saját, egyéni biztonsági környezetéhez.

Internet Single ASA-eszköz biztonsági kontextus A Biztonsági kontextus C Ügyfél A Ügyfél B Ügyfél C Biztonsági kontextus B

20.1.4

## Cisco Firepower sorozat

Hagyományosan a szervezetek dedikált eszközöket használtak hálózatuk védelmére. A Cisco következő generációs tűzfala (NGFW) a bevált tűzfaltechnológiát fejlett fenyegetés- és kártevő-észlelési képességekkel kombinálja.

Ezek az NGFW-k több biztonsági réteget egyetlen platformba tömörítenek, kiküszöbölve a több megoldás vásárlásának és kezelésének költségeit. Ez az integrált megközelítés a kategória legjobb biztonsági technológiáját ötvözi a többrétegű védelemmel, amely egyetlen eszközbe van integrálva.

A Cisco ASA 5500-X FirePOWER Services eszközökkel az új Cisco NGFW részei. A kis és közepes fiókirodák számára készült ASA 5500-X FirePOWER Services szolgáltatással egyesíti az ASA 5500 állapotjelző tűzfal funkcióit a következő fejlett fenyegetés- és rosszindulatú programok észlelési képességeivel:

* Következő generációs IPS (NGIPS)
* Fejlett rosszindulatú programok elleni védelem (AMP)
* Alkalmazásvezérlés és URL-szűrés

**Megjegyzés** : A „FirePOWER” az ASA-n futó Firepower szolgáltatásokra, míg a „Firepower” a Cisco Firepower sorozatú NGFW eszközökre utal.

20.1.5

## Videó – Cisco FTD: Veszélyközpontú NGFW

20.1.6

## A tűzfalak áttekintése a hálózattervezésben

Amikor a tűzfalhoz kapcsolódó hálózatokról beszélünk, néhány általános kifejezést figyelembe kell venni:

* **Hálózaton kívül** – Az a hálózat/zóna, amely kívül esik a tűzfal védelmén.
* **Hálózaton belüli** – A tűzfal mögött védett hálózat/zóna.
* **DMZ** – Demilitarizált zóna, amely lehetővé teszi a belső és külső felhasználók számára a védett hálózati erőforrásokhoz való hozzáférést.

A tűzfalak megvédik a belső hálózatokat a külső hálózaton lévő felhasználók jogosulatlan hozzáférésétől. Megvédik egymástól a belső hálózati felhasználókat is. Például a zónák létrehozásával az adminisztrátor elkülönítve tarthatja a könyvelési kiszolgálókat kiszolgáló hálózatot a szervezet többi hálózatától.

Az ábra azt szemlélteti, hogy ezek a zónák hogyan hatnak egymásra a megengedett forgalom szempontjából:

* A belső hálózatból kiinduló forgalom a külső hálózat felé megengedett.
* A belső hálózatról a DMZ hálózat felé induló forgalom megengedett.
* A külső hálózatról a DMZ hálózat felé induló forgalom szelektíven engedélyezett.

Az ábrán egy internet címkével ellátott külső hálózat látható, amely az a. az asa belső hálózathoz és adm z-hez is csatlakozik.

### Engedélyezett forgalom

G1/1 G1/2

G1/3

Internet kívül DMZ webszerver belül

Az alábbi ábra szemlélteti, hogyan működnek együtt ezek a zónák a tiltott forgalom esetén:

* A külső hálózatról a belső hálózatra menő forgalom megtagadva.
* A DMZ hálózatról a belső hálózatra menő forgalom megtagadva.

Az ábrán egy internet címkével ellátott külső hálózat látható, amely az a. az asa belső hálózathoz és adm z-hez is csatlakozik.

### Tiltott forgalom

G1/1 G1/2

G1/3

Internet kívül DMZ webszerver belül

A Cisco ISR-ek tűzfalszolgáltatásokat biztosíthatnak a zónaalapú házirend tűzfal (ZPF) vagy a régebbi környezetalapú hozzáférés-vezérlés (CBAC) használatával. Az ASA ugyanazokat a szolgáltatásokat nyújtja, de a konfiguráció jelentősen eltér a ZPF IOS útválasztó konfigurációjától.

Az ASA egy dedikált tűzfaleszköz. Alapértelmezés szerint a definiált belső interfészt megbízható hálózatként kezeli, minden meghatározott külső interfészt pedig nem megbízható hálózatként.

Minden interfészhez tartozik egy biztonsági szint. Ezek a biztonsági szintek lehetővé teszik az ASA számára, hogy biztonsági irányelveket hajtson végre. Például a belső felhasználók hozzáférhetnek a külső hálózatokhoz bizonyos címek alapján, hitelesítés vagy engedélyezés megkövetelésével, vagy külső URL-szűrő szerverrel egyeztetve.

**Megjegyzés** : A biztonsági szinteket néha megbízhatósági szinteknek is nevezik. Ebben a kurzusban a biztonsági szintek kifejezést fogjuk használni.

A külső felhasználók számára szükséges hálózati erőforrások, például egy web- vagy FTP-kiszolgáló, elhelyezhetők egy DMZ-ben. A tűzfal korlátozott hozzáférést tesz lehetővé a DMZ-hez, miközben megvédi a belső hálózatot a külső felhasználóktól.

20.1.7

## ASA tűzfal működési módok

Az ASA eszközökön két tűzfal interfész üzemmód áll rendelkezésre: irányított mód és transzparens mód.

Útirányított módban két vagy több interfész választja el a Layer 3 hálózatokat (azaz tartományokat). Az ábrán az ASA egy router ugrásnak tekinthető a hálózatban, és képes NAT-ot végrehajtani a csatlakoztatott hálózatok között. Az irányított mód több interfészt is támogat. Mindegyik interfész más alhálózaton található, és IP-címet igényel az adott alhálózaton. Az ASA szabályzatokat alkalmaz a tűzfalon áthaladó folyamokra.

**Megjegyzés** : Ennek a modulnak a középpontjában az irányított mód áll.

Az ábrán egy asa látható két 10.2.1.1 feliratú interfésszel a 10.2.1.0 / 24 hálózathoz és a 10.1.1.1 címkével a 10.1.1.0 / 24 hálózathoz csatlakoztatva

### Routed Mode

10.2.1.0/24 10.2.1.1 10.1.1.1

10.1.1.0/24

Az átlátszó módban lévő ASA-t gyakran „bump in the wire”-nek vagy „lopakodó tűzfalnak” nevezik, mivel az ASA úgy működik, mint egy Layer 2 eszköz, és nem tekintik router ugrásnak. Az alábbi ábrán az ASA-hoz csak felügyeleti célból van hozzárendelve IP-cím a helyi hálózaton. Ez a mód hasznos a hálózati konfiguráció leegyszerűsítéséhez, vagy ha a meglévő IP-címzés nem módosítható. A hátrányok közé tartozik azonban a dinamikus útválasztási protokollok, VPN-ek, QoS vagy DHCP Relay támogatásának hiánya.

Az ábrán egy 10.1.1.3 címû asa látható, amely a 10.1.1.0 / 2 hálózaton két .1 és .2 jelzésû útválasztó között található.

### Átlátszó mód

10.1.1.3 .1 .2

10.1.1.0/29

20.1.8

## ASA licenckövetelmények

A licenc meghatározza az adott ASA-n engedélyezett opciókat. A legtöbb ASA készülék előre telepítve van Base vagy Security Plus licenccel. Például a Cisco ASA 5506-X modell Base licenccel és a Security Plus licencre való frissítés lehetőségével érkezik. A Security Plus frissítési licenc lehetővé teszi a Cisco ASA 5506-X méretezését, hogy támogassa a nagyobb csatlakozási kapacitást és akár 50 IPsec VPN-felhasználót. Teljes körű DMZ-támogatást ad, és a VLAN trönkölés támogatásával integrálódik kapcsolt hálózati környezetekbe. Ezenkívül a Security Plus licenc lehetővé teszi a redundáns ISP-kapcsolatok és az állapot nélküli aktív/készenléti magas rendelkezésre állású szolgáltatások támogatását. Ez a funkció segít az üzletmenet folytonosságának biztosításában.

Az ASA további funkcióinak biztosítása érdekében további időalapú vagy opcionális licencek vásárolhatók. Például egy rendszergazda telepíthet egy Botnet Traffic Filter időalapú licencet, amely egy évig érvényes. Egy másik példa az, ha az ASA-nak kezelnie kell az egyidejű SSL VPN-felhasználók számának rövid távú megugrását. Ebben az esetben opcionális AnyConnect Premium licenc vásárolható.

Ha ezeket a további licenceket kombinálja az előre telepített licencekkel, akkor állandó licenc jön létre. Az állandó licenc ezután egy állandó aktiváló kulcs telepítésével aktiválódik az **activation-key** paranccsal. Az állandó aktiváló kulcs egyetlen kulcsban tartalmazza az összes licencelt szolgáltatást. A termék aktiváló kulcsa megvásárolható a Cisco-fiók képviselőjétől.

**Megjegyzés** : Csak egy állandó licenckulcs telepíthető. A telepítés után futó licencnek nevezzük.

Az ASA-eszköz licencinformációinak ellenőrzéséhez használja a **show activation-key** parancsot (lásd alább), vagy a **show version** parancsot.

NETSEC-ASA# **show activation-key**

Serial Number: JAD242301E6

Running Permanent Activation Key: 0x1e14e468 0x7c715e6b 0xcc71d1f4 0x9de81084 0x4e143eb6

Licensed features for this platform:

Maximum Physical Interfaces : Unlimited perpetual

Maximum VLANs : 5 perpetual

Inside Hosts : Unlimited perpetual

Failover : Disabled perpetual

Encryption-DES : Enabled perpetual

Encryption-3DES-AES : Enabled perpetual

Carrier : Disabled perpetual

AnyConnect Premium Peers : 2 perpetual

AnyConnect Essentials : Disabled perpetual

Other VPN Peers : 10 perpetual

Total VPN Peers : 12 perpetual

AnyConnect for Mobile : Disabled perpetual

AnyConnect for Cisco VPN Phone : Disabled perpetual

Advanced Endpoint Assessment : Disabled perpetual

Shared License : Disabled perpetual

Total TLS Proxy Sessions : 2 perpetual

Botnet Traffic Filter : Disabled perpetual

Cluster : Disabled perpetual

This platform has a Base license.

The flash permanent activation key is the SAME as the running permanent key.

NETSEC-ASA#

[20.0](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[20.2](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[The ASA 5506-X with FirePOWER Services](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                                                                                                        
*   

1. Introduction to the ASA
2. The ASA 5506-X with FirePOWER Services

# Az ASA 5506-X FirePOWER szolgáltatásokkal

20.2.1

## Az ASA 5506-X áttekintése

A Cisco ASA 5506-X egy teljes értékű biztonsági eszköz kisvállalkozások, fiókirodák és vállalati távmunkás környezetek számára. Nagy teljesítményű tűzfalat, SSL VPN-t, IPsec VPN-t és gazdag hálózati szolgáltatásokat kínál egy moduláris, plug-and-play készülékben.

Az ábra az ASA 5506-X előlapját mutatja.

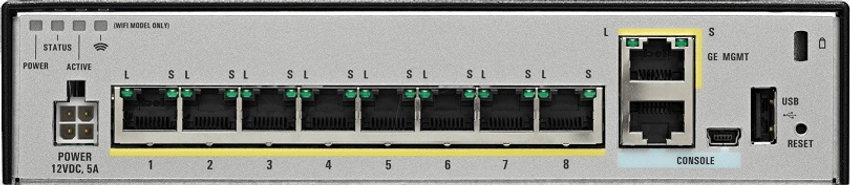
Az alábbi ábra a Cisco ASA 5506-X hátlapját mutatja be. Az alapértelmezett DRAM memória 4 GB, az alapértelmezett belső flash memória pedig 8 GB. Feladatátvételi konfigurációban a két egységnek azonos modellnek kell lennie, azonos hardverkonfigurációval, azonos számú és típusú interfésszel, valamint azonos mennyiségű RAM-mal. A feladatátvétel a Security Plus licenccel érhető el.

Az ábrán az ASA 5506-X hátlap látható

### ASA 5506-X hátlap

7 1 3 2 4 5

6



1. 12V-os tápcsatlakozó.
2. Négy állapotjelző LED a tápellátáshoz, az állapothoz, az aktívhoz és a WLAN-hoz.
3. 8-1 Gigabit Ethernet interfészek. Az L a kapcsolat állapotát, az S pedig a kapcsolat sebességét jelzi.
4. Gigabit Ethernet kezelőfelület.
5. A típusú USB port csatlakozó külső tárolóeszközhöz.
6. RJ45 és mini-USB konzol portok.
7. Reset pin. Ha három másodpercig megnyomja, az ASA újraindításkor visszaáll az alapértelmezett új állapotba. A vaku nem törlődik.

Az alábbi ábra a Cisco ASA 5506-X belső alkatrészeit mutatja.

**Megjegyzés:** Az irányított interfészeket és IP-címeket használó ASA 5506-X-től eltérően az ASA 5505 a Layer 2 switchekhez hasonló switchportokat és VLAN-okat használt.

Az ábra az ASA 5506-X belső komponenseit mutatja

### ASA 5506-X belső alkatrészek

1 2 3

4



1. 50 GB mSata szilárdtestalapú meghajtó
2. Kriptogyorsító CPU
3. Többmagos 1,25 GHz-es CPU
4. 4 GB DRAM

20.2.2

## ASA biztonsági szintek

Az ASA biztonsági szinteket rendel hozzá a belső és külső hálózatok megkülönböztetéséhez. A biztonsági szintek határozzák meg az interfész megbízhatóságának szintjét. Minél magasabb a szint, annál megbízhatóbb a felület. A biztonsági szintszámok 0-tól (nem megbízható) 100-ig (nagyon megbízható) terjednek. Minden működési interfészhez hozzá kell rendelni egy nevet és egy 0 (legalacsonyabb) és 100 (legmagasabb) közötti biztonsági szintet.

Ahogy az alábbi ábrán látható, a 100-as szintet a legbiztonságosabb hálózathoz kell hozzárendelni, például a belső hálózathoz. A 0. szint hozzárendelhető a külső hálózathoz, amely az internetre csatlakozik. A DMZ-ekhez és más hálózatokhoz 0 és 100 közötti biztonsági szint rendelhető. Ha a forgalom egy magasabb biztonsági szinttel rendelkező interfészről egy alacsonyabb biztonsági szintű interfészre kerül át, az kimenő forgalomnak minősül. Ezzel szemben az alacsonyabb biztonsági szintű interfészről egy magasabb biztonsági szintű interfészre mozgó forgalom bejövő forgalomnak minősül.

Az ábrán egy asa látható 3 interfésszel a külső, a belső és a dm z-hez csatlakoztatva. A külső interfész neve külső, 0-s biztonsági szinttel. A belső interfész neve belső 100-as biztonsági szinttel. A dmz interfész neve dmz 50-es biztonsági szinttel

### Biztonsági szint beállításai

G1/1 G1/3

G1/2

Hálózaton kívül   
Interfész neve: kívül   
Biztonsági szint: 0 Hálózaton belül   
Interfész neve: belül   
Biztonsági szint: 100 DMZ hálózat   
Interfész neve: dmz   
Biztonsági szint: 50 kívül Interneten belül A DMZ webszerveren

A biztonsági szintek segítenek a hálózati forgalom számos aspektusának szabályozásában, amint azt az alábbi táblázat mutatja.

| **Vonatkozás** | **Hatás** |
| --- | --- |
| Hálózati hozzáférés | Alapértelmezés szerint van egy implicit engedély a magasabb biztonsági interfészről egy alacsonyabb biztonsági interfészre (kimenő). A magasabb biztonsági interfészen lévő gazdagépek hozzáférhetnek az alacsonyabb biztonsági interfészen lévő gazdagépekhez. Ugyanahhoz a biztonsági szinthez több interfész is hozzárendelhető. Ha a kommunikáció engedélyezve van az azonos biztonsági szintű interfészeknél, akkor az interfészek közötti forgalomra implicit engedély vonatkozik. |
| Ellenőrző motorok | Néhány alkalmazás-ellenőrző motor a biztonsági szinttől függ. Ha az interfészek azonos biztonsági szinttel rendelkeznek, az ASA mindkét irányban ellenőrzi a forgalmat. |
| Alkalmazásszűrés | A HTTPS- és FTP-szűrés csak a magasabb szintről alacsonyabb szintű kimenő kapcsolatokra vonatkozik. Ha a kommunikáció engedélyezve van az azonos biztonsági szinttel rendelkező interfészeknél, a forgalom mindkét irányban szűrhető. |

A kimenő forgalom alapértelmezés szerint engedélyezett és ellenőrzött. A visszatérő forgalom az állapottartó csomagellenőrzés miatt engedélyezett. Például a belső felületen lévő belső felhasználók könnyen hozzáférhetnek a DMZ erőforrásaihoz. Megkötések nélkül, további házirend vagy további parancsok nélkül is kezdeményezhetnek csatlakozást az internethez. A külső hálózatról érkező és a DMZ-be vagy a belső hálózatba érkező forgalom azonban alapértelmezés szerint meg van tiltva. A belső hálózatról induló és a külső interfészen keresztül visszatérő forgalom megengedett lenne. Ez alól az alapértelmezett viselkedés alóli bármely kivételnek megköveteli az ACL konfigurálása, hogy kifejezetten engedélyezze a forgalmat egy alacsonyabb biztonsági szinttel rendelkező interfészről egy magasabb biztonsági szintű interfészre, például kívülről befelé.

20.2.3

## ASA 5506-X telepítési forgatókönyvek

Az ASA 5506-X-et általában élbiztonsági eszközként használják. Egy kisvállalkozást összeköt egy internetszolgáltató eszközzel, például DSL- vagy kábelmodemmel, hogy hozzáférjen az internethez. Több munkaállomás, hálózati nyomtató és IP-telefon összekapcsolására és védelmére használható.

Egy kis fióktelepen a közös telepítés magában foglal egy 100-as biztonsági szintű belső hálózatot és egy 0-s biztonsági szintű külső hálózatot, amint az az alábbi ábrán látható.

Az ábrán egy asa látható 6 gigabites ethernet interfésszel. az egyik interfész a külső hálózathoz csatlakozik, a többi pedig a belső hálózathoz csatlakozik.

### ASA bevezetése kis fióktelepeken

G1/2 G1/1 G1/3 G1/4 G1/5 G1/6

ASA 5506-X

Munkaállomások IP-telefonok belül hálózati nyomtatón kívül az interneten

A kisvállalkozásokban, amint az alább látható, az ASA 5506-X két különböző védett hálózati szegmenssel telepíthető. Az egyik szegmens a belső hálózat, amely munkaállomásokat és IP-telefonokat köt össze. A másik szegmens a DMZ, amely egy céges webszervert köt össze. A külső interfész az internethez való csatlakozásra szolgál.

Az ábra ugyanaz a topológia, mint az előző ábrán, egy további interfésszel, amely a webszervert tartalmazó admz-hez csatlakozik

### ASA bevezetése kisvállalkozásokban

G1/1 G1/2 G1/4 G1/5 G1/6

G1/7

IP-telefonok kívül a DMZ webszerver munkaállomásokon Interneten

Vállalati környezetben, amint az itt látható, az ASA 5506-X-et a távmunkások és az otthoni felhasználók használhatják, hogy VPN-en keresztül kapcsolódjanak egy központi helyhez.

Az ábrán egy asa látható a vállalati központban, amely az internetre csatlakozik, és két távoli asa, amely két különböző távmunkás hálózatot csatlakoztat a vállalati hálózathoz.

### ASA bevezetése vállalati környezetben

Vállalati központ ASA IPsec VPN IPsec VPN Internet ASA 5506-X ASA 5506-X munkaállomás munkaállomás IP telefon IP telefon távmunka 1 távmunka 2

[20.1](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[ASA Solutions](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[20.3](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Introduction to the ASA Summary](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                                                                                                           

1. Introduction to the ASA
2. Introduction to the ASA Summary

# Bevezetés az ASA összefoglalójába

20.3.1

## Mit tanultam ebben a modulban?

**ASA megoldások**   
A Cisco ASA FirePOWER Services termékcsaláddal dedikált tűzfalszolgáltatásokat kínál egyetlen eszközben. Ezek olyan NGFW eszközök, amelyek integrált fenyegetésvédelmet nyújtanak a teljes támadási kontinuumon. Az ASA-modell kiválasztása a szervezet követelményeitől függ, például a maximális átviteli sebességtől, a másodpercenkénti maximális kapcsolatoktól és a költségvetéstől. A Cisco ASAv az ASA készülékek erejét hozza el a virtuális tartományba. Amikor a tűzfalhoz csatlakoztatott hálózatokról beszélünk, néhány általános kifejezést figyelembe kell venni: külső hálózat, belső hálózat és DMZ.

Az ASA eszközökön két tűzfal interfész üzemmód áll rendelkezésre: irányított mód és transzparens mód. Routed módban két vagy több interfész választja el a Layer 3 hálózatokat, azaz tartományokat. Az átlátszó módban lévő ASA-t gyakran „bump in the wire”-nek vagy „lopakodó tűzfalnak” nevezik, mivel az ASA úgy működik, mint egy Layer 2 eszköz, és nem tekintik router ugrásnak. A fejlett ASA tűzfal szolgáltatásai közé tartozik az ASA virtualizáció, a magas szintű rendelkezésre állás feladatátvétellel, az identitástűzfal, valamint a fenyegetéskezelési és elszigetelési szolgáltatások. A legtöbb ASA készülék előre telepítve van Base vagy Security Plus licenccel.

**Az ASA 5506-X FirePOWER szolgáltatásokkal**   
A Cisco ASA 5506-X egy teljes értékű biztonsági eszköz kisvállalkozások, fiókirodák és vállalati távmunkás környezetek számára. Nagy teljesítményű tűzfalat, SSL VPN-t, IPsec VPN-t és gazdag hálózati szolgáltatásokat biztosít egy plug-and-play készülékben. Az ASA biztonsági szinteket rendel hozzá a belső és külső hálózatok megkülönböztetéséhez. A biztonsági szintszámok 0-tól (nem megbízható) 100-ig (nagyon megbízható) terjednek. A kimenő forgalom alapértelmezés szerint engedélyezett és ellenőrzött. A visszatérő forgalom az állapottartó csomagellenőrzés miatt engedélyezett. Az ASA 5506-X-et általában élbiztonsági eszközként használják. Egy kisvállalkozást összeköt egy internetszolgáltató eszközzel, például DSL- vagy kábelmodemmel, hogy hozzáférjen az internethez.

20.3.2

## 20. modul – Bevezetés az ASA kvízbe

Az űrlap teteje

1. Mi jellemzi az ASA biztonsági szinteket?

Az űrlap alja

Mi a két legnagyobb különbség a különböző ASA tűzfalmodellek között? (Válassz kettőt.)

Melyik állítás jellemzi a Cisco ASAv terméket?

Milyen két funkciónak kell egyeznie az ASA-eszközök között a feladatátvételi konfiguráció megvalósításához? (Válassz kettőt.)

Melyik szolgáltatás jellemző az ASA Security Plus frissítési licencére, és mely szolgáltatás biztosítja a fokozott rendelkezésre állást?

Mi a legmegbízhatóbb biztonsági szint, amely konfigurálható az ASA eszköz interfészén?

X készülék hátlapján található 8 Gigabit Ethernet portot Melyik két állítás írja le a Cisco ASA 5506 - ? (Válassz kettőt.)

Az ASA tűzfal melyik fejlett funkciója biztosít részletes hozzáférés-szabályozást az IP-címeknek a Windows Active Directory bejelentkezési adataihoz való társítása alapján?

Mi a két alapvető konfigurációs követelmény minden egyes működési interfészhez egy ASA 5506 - X eszközön? (Válassz kettőt.)

Mi az egyik hátránya a transzparens módú működésnek egy ASA-eszközön?

Milyen szolgáltatást ad a Cisco ASA 5500-hoz az ASA 5500 - X?

Melyik utasítás írja le az alapértelmezett hálózati hozzáférés-vezérlést egy ASA tűzfaleszközön?

[20.2](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[The ASA 5506-X with FirePOWER Services](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[21.0](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                                                                                                                             
* 

1. ASA Firewall Configuration
2. Introduction

# Bevezetés

21.0.1

## Miért vegyem ezt a modult?

A Cisco ASA 5506-X FirePOWER szolgáltatásokkal egy funkciókban gazdag biztonsági készülék, amely alkalmas kis- és közepes méretű üzleti hálózatokhoz. Az ASA 5506-X egy nagyon népszerű eszköz, amelyet számos szervezet használ, ami értékessé teszi az ezzel a biztonsági berendezéssel kapcsolatos ismereteket és készségeket a munkaerőpiacon. Ebben a modulban az eszköz funkcióinak széles skáláját állíthatja be, beleértve az ACL-eket, a DHCP-t, a NAT-ot, az AAA-t és a szolgáltatási szabályzatokat.

21.0.2

## Mit fogok tanulni ebben a modulban?

**Modul címe:** ASA Firewall Configuration

**Modul célja** : ASA tűzfalkonfiguráció megvalósítása.

| **téma címe** | **Téma Cél** |
| --- | --- |
| **Alapvető ASA tűzfal konfiguráció** | Ismertesse az ASA-5506-X FirePOWER szolgáltatásokkal való konfigurálását. |
| **Konfigurálja a felügyeleti beállításokat és szolgáltatásokat** | A felügyeleti beállítások és szolgáltatások konfigurálása ASA 5506-X tűzfalon. |
| **Tárgycsoportok** | Ismertesse az objektumcsoportok konfigurálását az ASA-n. |
| **ASA ACL-ek** | Használja a megfelelő parancsokat a hozzáférési listák objektumcsoportokkal történő konfigurálásához az ASA-n. |
| **NAT szolgáltatások ASA-n** | A megfelelő parancsokkal állítsa be az ASA-t a NAT szolgáltatások nyújtására. |
| **AAA** | Használja a megfelelő parancsokat a hozzáférés-vezérlés konfigurálásához a helyi adatbázis és az AAA-kiszolgáló használatával. |
| **Szolgáltatási szabályzatok az ASA-n** | Szolgáltatási szabályzatok konfigurálása egy ASA-n |
| **Az ASDM bemutatása (opcionális)** | **Megjegyzés** : Ez egy opcionális téma, amelyet nem értékelünk. |

[20.3](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Introduction to the ASA Summary](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[21.1](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Basic ASA Firewall Configuration](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                                                                                                                              
* 

1. ASA Firewall Configuration
2. Basic ASA Firewall Configuration

# Alapvető ASA tűzfal konfiguráció

21.1.1

## Alapvető ASA beállítások

Az ASA parancssori interfész (CLI) egy szabadalmaztatott operációs rendszer, amely a router IOS-éhez hasonló megjelenést és érzetet mutat. Az ASA parancssori felület például a Cisco IOS útválasztóhoz hasonló parancssorokat tartalmaz, amint az az ábrán látható. Az IOS CLI-hez hasonlóan az ASA CLI is felismeri a következőket:

* Parancsok és kulcsszavak rövidítése
* A Tab billentyű használata részleges parancs végrehajtásához
* ) használata **A súgó billentyű ( ?** egy parancs után további szintaxis megtekintéséhez

Az ábra az ASA, a user exec, a privileged exec, a global config és az interface config alapvető konfigurációs módjait mutatja.

ciscoasa> enablePassword: ciscoasa# ciscoasa# configure terminalciscoasa(config)# ciscoasa(config)# interface g1/1ciscoasa(config-if)# exitciscoasa(config)#

Felhasználói EXEC mód Kiváltságos EXEC mód Globális konfigurációs mód Interfész konfigurációs mód

Az ASA CLI-nek azonban különböző parancsai is vannak. A táblázat szembeállítja a gyakori IOS útválasztó és ASA parancsokat.

| **IOS Router parancs** | **Egyenértékű ASA-parancs** |
| --- | --- |
| **engedélyezése**  titkos jelszó | **jelszó engedélyezése**  jelszó |
| **sor vty 0 4**   **jelszó**  jelszó   **Belépés** | **passwd**  jelszó |
| **ip útvonal** | **útvonal**  if\_name |
| **ip interfész rövid megjelenítése** | **interfész ip rövid megjelenítése** |
| **mutasd az ip útvonalat** | **mutasd meg az útvonalat** |
| **ip nat fordítások megjelenítése** | **mutasd xlate** |
| **másolja a running-config startup-config** | **írj**  [  **memória**  ] |
| **startup-config törlése** | **írás törlés** |

Az ASA CLI parancsok az aktuális konfigurációs módtól függetlenül végrehajthatók. IOS parancs **A do** nem szükséges és nem ismerhető fel. A következő példák az ASA néhány egyedi funkcióját mutatják be.

az ábra az asa interfészt mutatja a jelszó titkosítás parancsával, amely elmagyarázza, hogy az asa cli parancsok az aktuális konfigurációs módtól függetlenül végrehajthatók. az ios do parancs nem kötelező és nem ismerhető fel. Megjelenik a help write parancs is, amely elmagyarázza, hogy az asa help parancs rövid parancsleírást és szintaxist biztosít bizonyos parancsokhoz. Megjelenik a Több megszakító, amely elmagyarázza, hogy a show parancs kimenetének megszakításához nyomja meg a q betűt. az ios control + c nem működik.

ciscoasa# conf tciscoasa(config)# show password encryption Password Encryption: DisabledMaster key hash: Not set(saved)ciscoasa(config)# ciscoasa(config)# help write USAGE: write erase|terminal|standby write net [<tftp\_ip>]:<filename> write [memory]DESCRIPTION:write Write config to net, flash, or terminal, or erase flash. Write without argument defaults to write memorySYNTAX:erase Clears the flash memory configurationterminal Display the current active configuration, not necessarily the saved configurationmem Save the active configuration to the flash, so that it will be the active configuration after a reloadstandby Save the active configuration on the active unit to the flash on the standby unit<--- More --->

Az ASA CLI parancsok az aktuális konfigurációs módtól függetlenül végrehajthatók. Az IOS do parancs nem szükséges és nem ismerhető fel. Az ASA help parancs egy rövid parancsleírást és szintaxist biztosít bizonyos parancsokhoz. A show parancs kimenetének megszakításához nyomja meg a Q betűt. Az IOS Ctrl+C nem működik.

**Megjegyzés:** Minden ASA-modell konfigurálható és felügyelhető a CLI vagy az Adaptive Security Device Manager (ASDM) segítségével. Ennek a modulnak a középpontjában az ASA CLI áll. Az ASDM-et a modul végén található opcionális témakör tárgyalja.

21.1.2

## ASA alapértelmezett konfigurációja

Az ASA 5506-X FirePOWER Services szolgáltatással olyan alapértelmezett konfigurációval érkezik, amely a legtöbb esetben elegendő egy alapszintű SOHO-telepítéshez.

**Megjegyzés** : Az ASA visszaállítható a gyári alapértelmezett konfigurációjára a **configure gyári alapértelmezett** globális konfigurációs mód paranccsal.

Az alapértelmezett gazdagépnév a **ciscoasa** . Alapértelmezés szerint a privilegizált EXEC és a konzolvonal jelszavai nincsenek konfigurálva. Minden interfész leállt és névtelen. Az alapértelmezett konfiguráció részben látható a példában. Ezeket a beállításokat az alábbiak szerint módosíthatja:

* Manuálisan a CLI használatával
* Interaktívan a CLI Setup Initialization varázsló segítségével
* Az ASDM indítási varázsló használata

hostname ciscoasa

enable password 8Ry2YjIyt7RRXU24 encrypted

names

no mac-address auto

!

interface GigabitEthernet1/1

shutdown

no nameif

no security-level

no ip address

!

interface GigabitEthernet1/2

shutdown

no nameif

no security-level

no ip address

!

**<output omitted>**

interface Management1/1

management-only

shutdown

no nameif

no security-level

no ip address

!

ftp mode passive

pager lines 24

icmp unreachable rate-limit 1 burst-size 1

no asdm history enable

arp timeout 14400

no arp permit-nonconnected

arp rate-limit 16384

timeout xlate 3:00:00

timeout pat-xlate 0:00:30

timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02

**<output omitted>**

21.1.3

## ASA interaktív beállítási inicializálás varázsló

Az ASA interaktív beállítási inicializálási varázslót biztosít az eszköz kezdeti konfigurációjának egyszerűsítésére. A varázsló interaktív promptok segítségével irányítja a rendszergazdát az alapvető beállítások konfigurálásához.

A varázsló akkor jelenik meg, ha nincs indítási konfiguráció, vagy ha az indítási konfiguráció törlődik, és az ASA újraindul az **írástörlés** és **újratöltés** jogosultságokkal rendelkező EXEC parancsokkal.

Amikor az eszközt újraindítják, az ASA varázsló megjeleníti a „ **Tűzfal előzetes konfigurálása most interaktív promptokon keresztül [ igen ] ” üzenetet .** ” Az ASA alapértelmezett felhasználói EXEC mód parancssorának törléséhez és megjelenítéséhez írja be **a no** . Ellenkező esetben írja be **a yes-t** , vagy egyszerűen nyomja meg **az Entert** elfogadásához az alapértelmezett [ yes ] . Ez elindítja a varázslót, és az ASA interaktív módon irányítja a rendszergazdát az alapértelmezett beállítások konfigurálásához.

Az alábbiakban egy interaktív konfiguráció példáját mutatjuk be.

**Megjegyzés** : A biztonsági készülék zárójelben ( [ ] ) jeleníti meg az alapértelmezett értékeket, mielőtt felkéri a felhasználót azok elfogadására vagy módosítására. Az alapértelmezett bevitel elfogadásához nyomja meg **az Enter billentyűt** .

Pre-configure Firewall now through interactive prompts [yes]? **<Enter>**

Firewall Mode [Routed]: **<Enter>**

Enable password [<use current password>]: **cisco**

Allow password recovery [yes]? **<Enter>**

Clock (UTC):

Year [2021]:

Month [Feb]:

Day [9]:

Time [11:21:11]:

Management IP address: **192.168.1.1**

Management network mask: **255.255.255.0**

Host name: **NETSEC-ASA**

Domain name: **netsec.com**

IP address of host running Device Manager: **192.168.1.100**

The following configuration will be used:

Enable password: cisco

Allow password recovery: yes

Clock (UTC): 11:21:11 Feb 9 2021

Firewall Mode: Routed

Management IP address: 192.168.1.1

Management network mask: 255.255.255.0

Host name: NETSEC-ASA

Domain name: netsec.com

IP address of host running Device Manager: 192.168.1.100

Use this configuration and save to flash? [yes]**<Enter>**

A varázsló interaktív részének befejezése után a biztonsági készülék megjeleníti az új konfiguráció összegzését, és felkéri a felhasználót, hogy mentse vagy utasítsa el a beállításokat. válaszol **Ha igennel** , az elmenti a konfigurációt flash-re, és megjeleníti a konfigurált gazdagépnév promptot. válasz esetén **A nem** a Telepítés inicializálása varázsló újraindul az elejétől az új alapértelmezett beállításokként végrehajtott változtatásokkal. Ez lehetővé teszi a rendszergazdának, hogy kijavítsa a rosszul konfigurált beállítást.

Bár a varázsló biztosítja az alapvető konfigurációs beállításokat, a legtöbb rendszergazda inkább manuálisan konfigurálja az eszközt a CLI-parancsok használatával.

[21.0](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[21.2](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Configure Management Settings and Services](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                          
* 

1. ASA Firewall Configuration
2. Configure Management Settings and Services

# Konfigurálja a felügyeleti beállításokat és szolgáltatásokat

21.2.1

## Lépjen be a Globális konfigurációs módba

alapértelmezett ASA-felhasználói promptja **A ciscoasa >** akkor jelenik meg, ha egy ASA-konfigurációt törölnek, az eszközt újraindítják, és a felhasználó nem használja az interaktív telepítővarázslót.

A privilegizált EXEC módba való belépéshez használja az **enable** user EXEC mode parancsot. Kezdetben az ASA-ban nincs konfigurálva jelszó; ezért, amikor a rendszer kéri, hagyja üresen a jelszó engedélyezése mezőt, és nyomja meg **az Enter billentyűt** .

Az ASA dátumát és idejét manuálisan vagy a Network Time Protocol (NTP) használatával kell beállítani. A dátum és az idő beállításához használja a **clock set** privileged EXEC **parancsot.**

Lépjen be a globális konfigurációs módba a **configured terminál** privileged EXEC paranccsal. A globális konfigurációs mód első elérésekor megjelenik a Smart Call Home funkcióra vonatkozó üzenet. Ez lehetővé teszi a névtelen hibajelentés aktiválását a Ciscónak az eszköz állapotával és állapotával kapcsolatban. konfigurációs módban érhető el **A többi Smart Call Home funkció otthoni hívás** . Ezek a funkciók proaktív diagnosztikát és valós idejű riasztásokat kínálnak bizonyos Cisco-eszközökön, ami magasabb hálózati rendelkezésre állást és nagyobb működési hatékonyságot biztosít. A részvételhez cisco.com azonosító szükséges, és az ASA eszközt regisztrálni kell a Cisco SMARTnet szolgáltatási szerződés értelmében.

Keressen az interneten, ha többet szeretne megtudni a Cisco Smart Call Home szolgáltatásról.

Az alábbiakban egy példa látható a privilegizált EXEC és a globális konfigurációs módba való belépésre. Egy egyszerű konfigurációt kell megadni, és megjelenik a névtelen Smart Call Home prompt.

ciscoasa> **enable**

Password:

ciscoasa#

ciscoasa# **clock set 12:00:00 1 April 2020**

ciscoasa#

ciscoasa# **configure terminal**

ciscoasa(config)#

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* NOTICE \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Help to improve the ASA platform by enabling anonymous reporting,

which allows Cisco to securely receive minimal error and health

information from the device. To learn more about this feature,

please visit: http://www.cisco.com/go/smartcall

Would you like to enable anonymous error reporting to help improve

the product? [Y]es, [N]o, [A]sk later: A

You will be reminded again in 7 days.

If you would like to enable this feature, issue the command

"call-home reporting anonymous".

Please remember to save your configuration.

ciscoasa(config)#

21.2.2

## Konfigurálja az Alapbeállításokat

Az ASA-t alapvető felügyeleti beállításokkal kell konfigurálni. A táblázat a feladat végrehajtásához szükséges parancsokat jeleníti meg.

| **ASA parancs** | **Leírás** |
| --- | --- |
| **gazdagépnév**  neve | * Legfeljebb 63 karakter hosszúságú gazdagépnevet határoz meg. * A gazdagépnévnek betűvel vagy számjegygel kell kezdődnie és végződnie, és belső karakterként csak betűket, számokat vagy kötőjelet kell tartalmaznia. |
| **domain név**  név | Beállítja az alapértelmezett domain nevet. |
| **jelszó engedélyezése**  jelszó | * Beállítja a privilegizált EXEC mód engedélyezési jelszavát. * A jelszót 3–32 alfanumerikus és speciális karakterből álló kis- és nagybetűk megkülönböztető karakterláncaként állítja be (kérdőjel vagy szóköz nélkül). |
| **banner motd**  üzenet | Jogi értesítést biztosít, és úgy konfigurálja a rendszert, hogy az ASA-hoz való csatlakozáskor a napi üzenetet jelenítse meg. |
| **kulcs config-key password-encryption**   [ new-pass [ old-pass ]] | * A jelszót 8 és 128 karakter közé állítja. * A titkosítási kulcs létrehozására szolgál. |
| **jelszó titkosítás aes** | Engedélyezi a jelszavas titkosítást és titkosítja az összes felhasználói jelszót. |

A példa egy ASA 5506-X alapkonfigurációját jeleníti meg.

paranccsal történik **Az IOS CLI-hez hasonlóan a jogi értesítés a banner motd** . A parancs azonban némileg eltér az IOS verziótól. Egy többsoros szalaghirdetés konfigurálásához a **banner motd-t** többször meg kell adni. Sor(ok) eltávolításához használja a **no banner motd** message parancsot.

A privilegizált EXEC jelszó automatikusan titkosításra kerül az MD5 használatával. Az AES-t használó erősebb titkosítást azonban engedélyezni kell. Ehhez be kell állítani egy elsődleges jelszót, és engedélyezni kell az AES titkosítást.

ciscoasa(config)# **hostname NETSEC-ASA**

NETSEC-ASA(config)# **domain-name netsec.com**

NETSEC-ASA(config)# **enable password Cisco#123**

NETSEC-ASA(config)#

NETSEC-ASA(config)# **banner motd** -----------------------------------------------

NETSEC-ASA(config)# **banner motd Authorized access only!**

NETSEC-ASA(config)# **banner motd You have logged into a secure device.**

NETSEC-ASA(config)# **banner motd** -----------------------------------------------

NETSEC-ASA(config)# **banner motd**

NETSEC-ASA(config)# **exit**

NETSEC-ASA# **exit**

Logoff

---------------------------------------------------------

Authorized access only!

You have logged into a secure device.

---------------------------------------------------------

Type help or '?' for a list of available commands.

NETSEC-ASA>

A példa egy mintakonfigurációt jelenít meg az összes felhasználói jelszó titkosításához.

Az elsődleges jelmondat módosításához használja a **key config-key password-encryption** parancsot. A jelszótitkosítás megjelenítése paranccsal állapíthatja meg, hogy engedélyezve van-e a jelszavas **titkosítás** .

NETSEC-ASA> **enable**

Password: \*\*\*\*\*\*\*\*\*

NETSEC-ASA# **show password encryption**

Password Encryption: Disabled

Master key hash: Not set(saved)

NETSEC-ASA#

NETSEC-ASA# **configure terminal**

NETSEC-ASA(config)# **key config-key password-encryption cisco123**

NETSEC-ASA(config)# **password encryption aes**

NETSEC-ASA(config)# **exit**

NETSEC-ASA#

NETSEC-ASA# **show password encryption**

Password Encryption: Enabled

Master key hash: 0x45ebef8e 0x77a0f287 0x90247f80 0x2a184246 0xe85cbcc4(not saved)

NETSEC-ASA# **write**

Building configuration...

Cryptochecksum: c2cb4c42 66ed8038 c81a3d7f c5df996e

6781 bytes copied in 0.260 secs

[OK]

NETSEC-ASA#

21.2.3

## Szintaxis-ellenőrző – Az alapvető beállítások konfigurálása az ASA 5506-X-en

A Syntax Checker segítségével konfigurálja az ASA 5506-X alapbeállításait.

Lépjen be a globális konfigurációs módba, és adja meg a következő alapvető beállításokat:

* A gazdagép **neve NETSEC-ASA**
* A domain a **netsec.com**
* A jelszó engedélyezése **a Cisco#123**

**Megjegyzés** : A **banner motd** parancs kerül megadásra.

Az űrlap teteje

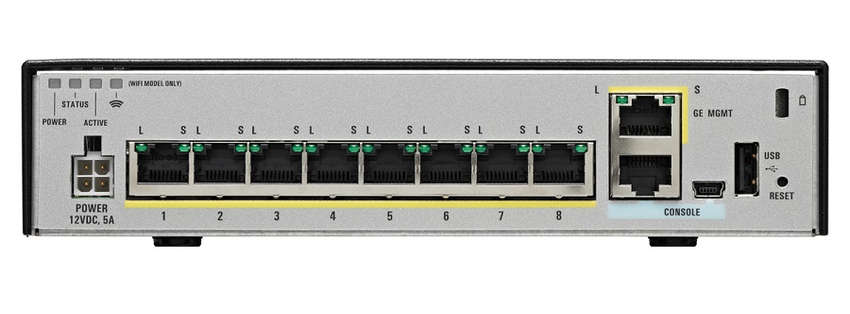
ciscoasa#

Az űrlap alja

21.2.4

## Interfészek konfigurálása

Az ASA-5506-X hátlapja az ábrán látható.



Az ASA-5506-X nyolc Gigabit Ethernet interfésszel rendelkezik, amelyek konfigurálhatók a különböző hálózatokról érkező forgalom továbbítására. A G1/1 interfész általában az internet vagy más külső hálózat külső interfészeként használatos. Alapértelmezés szerint úgy van beállítva, hogy IP-címét DHCP-n keresztül kapja meg, mivel feltételezhető, hogy az interfész olyan internetszolgáltatóhoz lesz konfigurálva, amely DHCP-t használ a csatolt interfészek címzésére.

A fennmaradó interfészek, G1/2-G1/8, belső hálózatokhoz vagy DMZ-ekhez rendelhetők. Ezenkívül egy Gigabit Ethernet port ( **az ábrán GE MGMT** felirattal ) az ASA Fire POWER modul sávon belüli kezelésére szolgál. A konfigurálás során Management1/1-nek van kijelölve. Az ASA FirePOWER modul konfigurálása túlmutat a kurzus keretein.

A 9.7-es és újabb szoftververziókban az egyes portok hídcsoportokká kombinálhatók, amelyek kapcsolóportként működnek ugyanazon a logikai hálózaton. Ily módon több eszköz közvetlenül csatlakoztatható az ASA 5506-X-hez a DMZ-ben és a logikai hálózatokon belül. Ez úgy történik, hogy konfigurálja a portokat az áthidalt virtuális felületeken (BVI). A BVI ezután névvel, biztonsági szinttel, IP-címmel és maszkkal, valamint egyéb beállításokkal konfigurálódik. Az eszközök különböző fizikai interfészeken való engedélyezéséhez az **azonos biztonsági forgalom engedélyezése interfész** globális konfigurációs parancsot kell konfigurálni. A BVI-k használatának hátránya, hogy sok parancsot, például **a no shutdown** parancsot az egyes interfészeken kell konfigurálni. Ezenkívül, ha hozzáférési listát kell használni a BVI-n, a listát minden fizikai interfészhez külön-külön kell csoportosítani.

Az interfész IP-címe a következő opciók egyikével konfigurálható:

* **Manuálisan** – Általában IP-cím és maszk hozzárendelésére szolgál az interfészhez.
* **DHCP** – Akkor használatos, amikor egy interfész egy DHCP-szolgáltatásokat nyújtó upstream eszközhöz csatlakozik. Az interfész lehet egy DHCP-kliens, és az IP-címét és a DHCP-vel kapcsolatos információkat az upstream eszközről fedezheti fel.
* **PPPoE** – Akkor használatos, amikor egy interfész egy upstream DSL-eszközhöz csatlakozik, amely pont-pont kapcsolatot biztosít Ethernet szolgáltatásokon keresztül. Az interfész lehet egy PPPoE kliens, és az IP-címét egy upstream PPPoE DSL-eszközről fedezheti fel.

A táblázat felsorolja azokat a parancsokat, amelyekkel IP-címet lehet konfigurálni egy interfészen.

|  |  |  |
| --- | --- | --- |
| **Konfiguráláshoz** | **ASA parancs** | **Leírás** |
| **Manuálisan** | **ip-cím**  ip-add hálózati maszk | IP-címet rendel az interfészhez. |
| **DHCP használata** | **ip cím dhcp** | Az interfész IP-cím konfigurációt kér az upstream eszköztől. |
|  | **ip cím dhcp setroute** | Az interfész kérésére és az alapértelmezett útvonal telepítésére szolgál az upstream eszközhöz. |
| **PPP0E használatával** | **ip cím pppoe** | Interfész konfigurációs mód parancs, amely IP-címet kér az upstream eszköztől. |
|  | **ip cím pppoe setroute** | Ugyanez a parancs, de kér és telepít egy alapértelmezett útvonalat az upstream eszközhöz. |

Minden interfésznek 0 (legalacsonyabb) és 100 (legmagasabb) közötti biztonsági szinttel kell rendelkeznie. Például a legbiztonságosabb hálózatát, például a belső gazdagép hálózatát a 100-as szinthez kell rendelnie. Míg az internethez csatlakoztatott külső hálózat lehet 0. Más hálózatok, például a DMZ-k lehetnek ezek között. Az interfészeket ugyanahhoz a biztonsági szinthez rendelheti.

A példa egy mintakonfigurációt jelenít meg. Figyelje meg, hogyan vannak az alapértelmezett biztonsági szint értékek hozzárendelve a belső és a külső interfészekhez. Vegye figyelembe, hogy a DMZ interfészhez ugyanaz a biztonsági szint van hozzárendelve, mint a külső nem megbízható hálózaté. Ezért a **biztonsági szint** parancsára valójában csak akkor van szükség, ha a rendszergazda úgy dönt, hogy módosítja ezeket az értékeket. Minden más interfészhez biztonsági szint értéket kell rendelni.

A biztonsági szint alapértelmezett viselkedése az, hogy hallgatólagosan engedélyezi a forgalmat egy magasabb biztonsági interfészről egy alacsonyabb biztonsági interfész kimenő felé. A forgalom implicit módon engedélyezett az azonos biztonsági szintű interfészek között, ha az ASA úgy van konfigurálva, hogy globálisan engedélyezze ezt a viselkedést. Az alacsonyabb biztonsági szinttel rendelkező interfészekről érkező forgalom implicit módon meg van tiltva a magasabb biztonsági szintű interfészek felé.

A példában a külső interfész manuálisan van konfigurálva egy IP-címmel. Sok internetszolgáltató azonban DHCP-t használ az ügyfélhálózatok címeinek megadására. Ebben az esetben használja az **ip address dhcp** parancsot a külső interfész konfigurálásához.

Az alábbi parancsok az alapvető interfész paraméterek konfigurálására szolgálnak.

| **ASA parancs** | **Leírás** |
| --- | --- |
| **nameif**  if\_name | * Legfeljebb 48 karakter hosszúságú szöveges karakterlánc segítségével nevezi el a felületet. * A név nem különbözteti meg a kis- és nagybetűket. * Megváltoztathatja a nevet, ha újból beírja ezt a parancsot egy új értékkel. * **Ne** írja be a **nem** űrlapot, mert ez a parancs az összes, erre a névre utaló parancs törlését okozza. |
| **biztonsági szintű**  érték | Beállítja a biztonsági szintet, ahol a szám egy 0 (legalacsonyabb) és 100 (legmagasabb) közötti egész szám. |
| **nincs leállás** | Aktiválja a felületet. |

Az ábra az INSIDE hálózatot, a DMZ hálózatot és a KÜLSŐ hálózatot összekötő ASA minta topológiáját mutatja. egy internetes gazdaszámítógép csatlakozik az internethez, amely kívülről van megjelölve. az internet egy asa 5506-x-hez csatlakozik g1/1-en keresztül 209.165.200.225 / 30-as hálózattal. Az asa egy [www.example.com](http://www.example.com) nevű szerverhez csatlakozik a dmz-ben g1/3-on keresztül, 192.168-as hálózati címmel. .2.0 / 24. az asa a belső hálózatra is csatlakozik 192.168.1.0 / 24 hálózattal g1/2-n keresztül.

G1/1 192.168.2.0 /24 209.165.200.225 /30 G1/3

G1/2

Internet KÍVÜL ASA 5506-X BELÜL   
192.168.1.0 /24 www.example.com DMZ Internet Host

NETSEC-ASA(config)# **interface g1/1**

NETSEC-ASA(config-if)# **nameif OUTSIDE**

INFO: Security level for "OUTSIDE" set to 0 by default.

NETSEC-ASA(config-if)# **security-level 0**

NETSEC-ASA(config-if)# **ip address 209.165.200.225 255.255.255.252**

NETSEC-ASA(config-if)# **no shutdown**

NETSEC-ASA(config-if)# **interface g1/2**

NETSEC-ASA(config-if)# **nameif INSIDE**

INFO: Security level for "INSIDE" set to 100 by default.

NETSEC-ASA(config-if)# **security-level 100**

NETSEC-ASA(config-if)# **ip address 192.168.1.1 255.255.255.0**

NETSEC-ASA(config-if)# **no shutdown**

NETSEC-ASA(config-if)# **interface g1/3**

NETSEC-ASA(config-if)# **nameif DMZ**

INFO: Security level for "DMZ" set to 0 by default.

NETSEC-ASA(config-if)# **security-level 50**

NETSEC-ASA(config-if)# **ip address 192.168.2.1 255.255.255.0**

NETSEC-ASA(config-if)# **no shutdown**

NETSEC-ASA(config-if)# **exit**

NETSEC-ASA(config)#

Ellenőrizze az interfész címét és állapotát a **show interface ip short** paranccsal az alábbiak szerint. Vegye figyelembe, hogy a **show** parancsot nem kell beírni User EXEC módban.

NETSEC-ASA(config-if)# **show interface ip brief**

Interface IP-Address OK? Method Status Protocol

Virtual0 127.1.0.1 YES unset up up

GigabitEthernet1/1 209.165.200.225 YES manual down down

GigabitEthernet1/2 192.168.1.1 YES manual up up

GigabitEthernet1/3 192.168.2.1 YES manual up up

GigabitEthernet1/4 unassigned YES unset administratively down down

GigabitEthernet1/5 unassigned YES unset administratively down down

GigabitEthernet1/6 unassigned YES unset administratively down down

GigabitEthernet1/7 unassigned YES unset administratively down down

GigabitEthernet1/8 unassigned YES unset administratively down down

Internal-Control1/1 unassigned YES unset down down

Internal-Data1/1 unassigned YES unset down down

Internal-Data1/2 unassigned YES unset down down

Internal-Data1/3 unassigned YES unset up up

Internal-Data1/4 169.254.1.1 YES unset up up

Management1/1 unassigned YES unset administratively down down

NETSEC-ASA(config-if)#

21.2.5

## Szintaxis-ellenőrző – ASA 5506-X külső, belső és DMZ interfészek konfigurálása

A Syntax Checker segítségével konfigurálhatja az ASA 5506-X külső, belső és DMZ interfészeit.

Configure the OUTSIDE interface.

* Enter interface configuration mode for **g1/1**.
* Name the interface **OUTSIDE**.
* Configure level **0** for security.
* Configure the IP address **209.165.200.225 255.255.255.252**.
* Activate the interface.

NETSEC-ASA(config)#interface g1/1

NETSEC-ASA(config-if)#nameif OUTSIDE

INFO: Security level for "OUTSIDE" set to 0 by default.

NETSEC-ASA(config-if)#security-level 0

NETSEC-ASA(config-if)#ip address 209.165.200.225 255.255.255.252

NETSEC-ASA(config-if)#no shutdown

NETSEC-ASA(config-if)#exit

Configure the INSIDE interface.

* Enter interface configuration mode for **g1/2**.
* Name the interface **INSIDE**.
* Configure level **100** for security.
* Configure the IP address **192.168.1.1 255.255.255.0**.
* Activate the interface.
* Exit interface configuration mode.

NETSEC-ASA(config)#interface g1/2

NETSEC-ASA(config-if)#nameif INSIDE

INFO: Security level for "INSIDE" set to 100 by default.

NETSEC-ASA(config-if)#security-level 100

NETSEC-ASA(config-if)#ip address 192.168.1.1 255.255.255.0

NETSEC-ASA(config-if)#no shutdown

NETSEC-ASA(config-if)#exit

Configure the DMZ interface.

* Enter interface configuration mode for **g1/3**.
* Name the interface **DMZ**.
* Configure level **50** for security.
* Configure the IP address **192.168.2.1 255.255.255.0**.
* Activate the interface.
* Exit interface configuration mode.

NETSEC-ASA(config)#interface g1/3

NETSEC-ASA(config-if)#nameif DMZ

INFO: Security level for "DMZ" set to 0 by default.

NETSEC-ASA(config-if)#security-level 50

NETSEC-ASA(config-if)#ip address 192.168.2.1 255.255.255.0

NETSEC-ASA(config-if)#no shutdown

NETSEC-ASA(config-if)#exit

Display brief output to verify the interfaces are up.

NETSEC-ASA(config)#show interface ip brief

show interface ip brief

Interface IP-Address OK? Method Status Protocol

Virtual0 127.1.0.1 YES unset up up

GigabitEthernet1/1 209.165.200.225 YES manual up up

GigabitEthernet1/2 192.168.1.1 YES manual up up

GigabitEthernet1/3 192.168.2.1 YES manual up up

GigabitEthernet1/4 unassigned YES unset administratively down down

GigabitEthernet1/5 unassigned YES unset administratively down down

GigabitEthernet1/6 unassigned YES unset administratively down down

GigabitEthernet1/7 unassigned YES unset administratively down down

GigabitEthernet1/8 unassigned YES unset administratively down down

Internal-Control1/1 unassigned YES unset down down

Internal-Data1/1 unassigned YES unset down down

Internal-Data1/2 unassigned YES unset down down

Internal-Data1/3 unassigned YES unset up up

Internal-Data1/4 169.254.1.1 YES unset up up

Management1/1 unassigned YES unset administratively down down

NETSEC-ASA(config)#

You have successfully configured inside, outside, and DMZ interfaces on the ASA 5506-X.

21.2.6

## Konfiguráljon egy alapértelmezett statikus útvonalat

Ha egy ASA DHCP-kliensként van konfigurálva, akkor képes fogadni és telepíteni egy alapértelmezett útvonalat az upstream eszközről. Ellenkező esetben egy alapértelmezett statikus útvonalat kell beállítani a **route** interface-name **0.0.0.0 0.0.0.0** next-hop-ip-address paranccsal. Az útvonal bejegyzés ellenőrzéséhez használja a **show route** parancsot.

A példa egy alapértelmezett statikus útvonal konfigurációját és ellenőrzését mutatja be.

NETSEC-ASA(config)# **route OUTSIDE 0.0.0.0 0.0.0.0 209.165.200.226**

NETSEC-ASA(config)#

NETSEC-ASA(config)# **show route | begin Gateway**

Gateway of last resort is 209.165.200.226 to network 0.0.0.0

S\* 0.0.0.0 0.0.0.0 [1/0] via 209.165.200.226, OUTSIDE

C 192.168.1.0 255.255.255.0 is directly connected, INSIDE

L 192.168.1.1 255.255.255.255 is directly connected, INSIDE

C 192.168.2.0 255.255.255.0 is directly connected, DMZ

L 192.168.2.1 255.255.255.255 is directly connected, DMZ

C 209.165.200.224 255.255.255.252 is directly connected, OUTSIDE

L 209.165.200.225 255.255.255.255 is directly connected, OUTSIDE

NETSEC-ASA(config)#

21.2.7

## Szintaxis-ellenőrző – Alapértelmezett statikus útvonal konfigurálása az ASA 5506-X-en

Használja a Szintaxis-ellenőrzőt egy alapértelmezett statikus útvonal konfigurálásához az ASA 5506-X-en.

Configure a default route to the **OUTSIDE** interface using **209.165.200.226** as the next-hop IP address.

NETSEC-ASA(config)#route OUTSIDE 0.0.0.0 0.0.0.0 209.165.200.226

Pipe the route table output to begin at the word **Gateway**.

NETSEC-ASA(config)# útvonal megjelenítése | kezdődik a Gateway

Az utolsó lehetőség átjárója a 209.165.200.226 a 0.0.0.0 hálózathoz

S\* 0.0.0.0 0.0.0.0 [1/0] keresztül 209.165.200.226, KÍVÜL

C 192.168.1.0 255.255.255.0 közvetlenül csatlakozik, BELÜL

L 192.168.1.1 255.255.255.255 közvetlenül csatlakozik, BELÜL

C 192.168.2.0 255.255.255.0 közvetlenül csatlakozik, DMZ

L 192.168.2.1 255.255.255.255 közvetlenül csatlakozik, DMZ

C 209.165.200.224 255.255.255.252 közvetlenül csatlakozik, KÍVÜL

L 209.165.200.225 255.255.255.255 közvetlenül csatlakozik, KÍVÜL

NETSEC-ASA(config)#

Sikeresen konfigurált egy alapértelmezett statikus útvonalat egy ASA 5506-X-en.

21.2.8

## A távelérési szolgáltatások konfigurálása

Telnet vagy SSH szükséges az ASA 5506-X távoli, CLI használatával történő kezeléséhez. A Telnet szolgáltatás engedélyezéséhez használja a táblázatban felsorolt ​​parancsokat.

**Megjegyzés** : Az **aaa hitelesítési telnet konzol LOCAL** parancs felülírja a **jelszó** paranccsal beállított jelszót, és hitelesíti a Telnet hozzáférést a helyi adatbázishoz képest.

| **ASA parancs** | **Leírás** |
| --- | --- |
| {  **passwd**  |  **jelszó**  } jelszó | Legfeljebb 80 karakter hosszúságú bejelentkezési jelszót állít be Telnethez. |
| **telnet**  { ipv4\_maszk hozzáadása | ipv6\_add  ***/***  előtag } if\_name | * Azonosítja, hogy melyik gazdagépen vagy hálózaton belül tud Telnetet kötni az ASA interfészhez. * használja a **clear configure telnet parancsot** A Telnet kapcsolat eltávolításához |
| **telnet időtúllépési**  percek | * Alapértelmezés szerint az öt percig tétlenül hagyott Telnet szekciókat az ASA lezárja. * A parancs megváltoztatja az alapértelmezett öt perces végrehajtási időt. |
| **aaa hitelesítés telnet konzol HELYI** | * A Telnet beállítása úgy, hogy a hitelesítéshez a helyi adatbázisra hivatkozzon. * A LOCAL kulcsszó megkülönbözteti a kis- és nagybetűket, és egy előre meghatározott szervercímke. |
| **törölje a telnet konfigurációját** | Eltávolítja a Telnet kapcsolatot a konfigurációból. |

A példában szereplő konfiguráció engedélyezi a Telnetet egy ASA 5506-X rendszeren. A példában csak a 192.168.1.3 IP-című belső gazdagép férhet hozzá az ASA-hoz. Az ASA bezárja a Telnet szekciót, ha három percig tétlen marad.

NETSEC-ASA(config)# **password cisco**

NETSEC-ASA(config)# **telnet 192.168.1.3 255.255.255.255 INSIDE**

NETSEC-ASA(config)# **telnet timeout 3**

NETSEC-ASA(config)#

NETSEC-ASA(config)# **show run telnet**

telnet 192.168.1.3 255.255.255.255 INSIDE

telnet timeout 3

NETSEC-ASA(config)#

A Telnet kommunikáció mindent egyszerű szövegben küld, beleértve a jelszavakat is. Az SSH-forgalom egy alagútban van titkosítva, amely segít megvédeni a jelszavakat és más érzékeny konfigurációs parancsokat a lehallgatástól. Ezért biztonsági okokból a távoli hozzáférést mindig engedélyezni kell az SSH használatával. Az SSH-hozzáférés engedélyezéséhez használja a táblázatban felsorolt ​​parancsokat. Az SSH konfiguráció ellenőrzéséhez használja a **show ssh** parancsot.

| **ASA parancs** | **Leírás** |
| --- | --- |
| **felhasználónév**  név  **jelszó**  jelszó | Létrehoz egy helyi adatbázis bejegyzést. |
| **aaa hitelesítés ssh konzol HELYI** | * Beállítja az SSH-t úgy, hogy a hitelesítéshez a helyi adatbázisra hivatkozzon. * A **LOCAL** kulcsszó megkülönbözteti a kis- és nagybetűket, és egy előre meghatározott szervercímke. |
| **titkosítási kulcs generál rsa modulus**  modulus\_size | * Létrehozza az SSH-titkosításhoz szükséges RSA-kulcsot. * A modulus\_size (bitekben) 512, 768, 1024, 2048, 3072 vagy 4096 lehet. * Legalább 2048-as érték ajánlott. |
| **ssh**  { ip\_address mask | ipv6\_cím  ***/***  előtag } if\_name | * Azonosítja, hogy melyik gazdagépen vagy hálózaton belül tud SSH-t küldeni az ASA interfészre. * A konfigurációban több parancs is szerepelhet. * Ha az if\_name nincs megadva, az SSH a külső interfész kivételével minden interfészen engedélyezve van. * Az SSH-kapcsolat eltávolításához használja a clear configure ssh parancsot. |
| **ssh verzió**  verziószám | * (Opcionális) Alapértelmezés szerint az ASA engedélyezi az SSH 1-es verzióját (kevésbé biztonságos) és a 2-es verziót (biztonságosabb). * Írja be ezt a parancsot, ha a kapcsolatokat egy adott verzióra szeretné korlátozni. |
| **ssh időtúllépési**  percek | Módosítja az alapértelmezett öt perces végrehajtási időtúllépést. |
| **törölje az ssh beállítását** | Eltávolítja az SSH-kapcsolatot a konfigurációból. |

A példában az SSH-hozzáférés engedélyezett az ASA 5506-X-en. Az AAA hitelesítés engedélyezve van, és a helyi felhasználói adatbázisra hivatkozik. Az RSA titkosítási kulcsot 2048 bitből állítják elő. Két belső és egy külső gazdagép hozzáférhet az ASA-hoz, és az SSH 2-es verziója engedélyezett.

NETSEC-ASA(config)# **username ADMIN password class**

NETSEC-ASA(config)# **aaa authentication ssh console LOCAL**

NETSEC-ASA(config)# **crypto key generate rsa modulus 2048**

WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.

Do you really want to replace them? [yes/no]: **y**

Keypair generation process begin. Please wait...

NETSEC-ASA(config)# **ssh 192.168.1.3 255.255.255.255 INSIDE**

NETSEC-ASA(config)# **ssh 192.168.1.4 255.255.255.255 INSIDE**

NETSEC-ASA(config)# **ssh 172.16.1.3 255.255.255.255 OUTSIDE**

NETSEC-ASA(config)# **ssh version 2**

NETSEC-ASA(config)# **show ssh**

Timeout: 5 minutes

Version allowed: 2

Cipher encryption algorithms enabled: aes256-ctr aes256-cbc aes192-ctraes192-cbc aes128-ctr aes128-cbc

Cipher integrity algorithms enabled: hmac-sha2-256

Hosts allowed to ssh into the system:

172.16.1.3 255.255.255.255 OUTSIDE

192.168.1.3 255.255.255.255 INSIDE

192.168.1.4 255.255.255.255 INSIDE

NETSEC-ASA(config)#

21.2.9

## Szintaxis-ellenőrző – SSH távoli hozzáférés engedélyezése a helyi adatbázis használatához ASA 5506-X-en

A Syntax Checker segítségével engedélyezheti az SSH távoli hozzáférést a helyi adatbázis használatával egy ASA 5506-X rendszeren.

Enable SSH using the following requirements:

* Configure the user **ADMIN** to use the password **class**.
* Configure SSH to refer to the local database for authentication.
* Generate an RSA key with a modulus of **2048**.
* Reply **y** to the prompt "Do you really want to replace them?"

NETSEC-ASA(config)#username ADMIN password class

NETSEC-ASA(config)#aaa authentication ssh console LOCAL

NETSEC-ASA(config)#crypto key generate rsa modulus 2048

WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.

Do you really want to replace them? [yes/no]:y

Keypair generation process begin. Please wait...

* Allow the 192.168.1.3 and 192.168.1.4 hosts to SSH to the **INSIDE** interface.
* Allow the 172.16.1.3 host to SSH to the **OUTSIDE** interface.
* Configure SSH to use version 2

NETSEC-ASA(config)#ssh 192.168.1.3 255.255.255.255 INSIDE

NETSEC-ASA(config)#ssh 192.168.1.4 255.255.255.255 INSIDE

NETSEC-ASA(config)#ssh 172.16.1.3 255.255.255.255 OUTSIDE

NETSEC-ASA(config)#ssh version 2

Enter the show ssh command to verify your configuration.

NETSEC-ASA(config)#show ssh

Idle Timeout: 5 minutes

Version allowed: 2

Cipher encryption algorithms enabled: aes256-ctr aes256-cbc aes192-ctr aes192-cbc aes128-ctr aes128-cbc

Cipher integrity algorithms enabled: hmac-sha2-256

Hosts allowed to ssh into the system:

172.16.1.3 255.255.255.255 OUTSIDE

192.168.1.3 255.255.255.255 INSIDE

192.168.1.4 255.255.255.255 INSIDE

NETSEC-ASA(config)#

You have successfully enabled SSH remote access to use the local database on an ASA 5506-X.

21.2.10

## Opcionális labor – Az ASA alapbeállításainak konfigurálása a CLI segítségével

Ebben a laborban a következő célokat kell teljesítenie:

* 1. rész: Alapvető eszközbeállítások konfigurálása
* 2. rész: Nyissa meg az ASA konzolt, és használja a CLI beállítási módot az alapvető beállítások konfigurálásához
* 3. rész: Alapvető ASA-beállítások és interfészbiztonsági szintek konfigurálása

21.2.11

## Konfigurálja a Network Time Protocol Services szolgáltatást

A Network Time Protocol (NTP) szolgáltatások engedélyezhetők az ASA-n, hogy lekérjék a dátumot és az időt az NTP-kiszolgálótól. Az NTP engedélyezéséhez használja a táblázatban felsorolt ​​globális konfigurációs mód parancsokat.

Az NTP konfigurációjának és állapotának ellenőrzéséhez használja a **show ntp status** és **a show ntp Associations** parancsokat.

| **ASA parancs** | **Leírás** |
| --- | --- |
| **ntp hitelesítés** | Lehetővé teszi a hitelesítést NTP-kiszolgálóval. |
| **ntp megbízható kulcs**  kulcs\_azonosítója | A hitelesítési kulcs azonosítóját megbízható kulcsként határozza meg, amely az NTP-kiszolgálóval történő hitelesítéshez szükséges. |
| **ntp hitelesítési kulcs**  kulcs\_azonosító  **md5**  kulcs | Kulcsot állít be az NTP-kiszolgálóval történő hitelesítéshez. |
| **ntp szerver**  IP-címe  **[kulcs**  kulcsazonosítója  **]** | Egy NTP-kiszolgálót azonosít. |

A példa bemutatja, hogyan engedélyezhető az NTP hitelesítéssel egy ASA 5506-X rendszeren. A konfiguráció feltételezi, hogy az NTP-kiszolgáló hitelesítési kulccsal van konfigurálva.

NETSEC-ASA(config)# **ntp authenticate**

NETSEC-ASA(config)# **ntp trusted-key 1**

NETSEC-ASA(config)# **ntp authentication-key 1 sha-256 cisco123**

NETSEC-ASA(config)# **ntp server 192.168.1.254**

NETSEC-ASA(config)#

21.2.12

## Szintaxis-ellenőrző – Engedélyezze az NTP-t hitelesítéssel az ASA 5506-X rendszeren

A Syntax Checker segítségével engedélyezze az NTP-t, és konfigurálja a hitelesítést az ASA 5506-X-en.

Implement the following requirements to enable NTP:

* Enable authentication with an NTP server.
* Set the authentication key to **1**.
* The key uses SHA-256 and the key **cisco123**.
* Specify NTP to use the server at **192.168.1.254**

NETSEC-ASA(config)# ntp hitelesítés

NETSEC-ASA(config)# ntp megbízható kulcs 1

NETSEC-ASA(config)# ntp hitelesítési kulcs 1 sha-256 cisco123

NETSEC-ASA(config)# ntp szerver 192.168.1.254

NETSEC-ASA(config)#

Sikeresen engedélyezte az NTP-t hitelesítéssel egy ASA 5506-X-en.

21.2.13

## Konfigurálja a DHCP-szolgáltatásokat

Az ASA beállítható DHCP-kiszolgálóként, amely IP-címeket és DHCP-vel kapcsolatos információkat biztosít a gazdagépeknek. Az ASA DHCP-kiszolgálóként való engedélyezéséhez és a gazdagépek DHCP-szolgáltatásainak biztosításához használja a táblázatban felsorolt ​​parancsokat.

| **ASA parancs** | **Leírás** |
| --- | --- |
| **dhcpd cím**  IP\_cím1 [ - IP\_cím2 ] if\_name | * Létrehoz egy DHCP-címkészletet, amelyben az IP\_cím1 a készlet kezdete, az IP\_cím2 pedig a készlet vége, kötőjellel elválasztva. * A címkészletnek ugyanazon az alhálózaton kell lennie, mint az ASA interfésznek. |
| **dhcpd dns**  dns1 [ dns2 ] | (Opcionális) Megadja a DNS-kiszolgáló(k) IP-címét. |
| **dhcpd lease**  lease\_length | * (Opcionális) Módosítja az ügyfélnek adott bérleti hosszt, amely másodpercben az az idő, ameddig az ügyfél használhatja a hozzárendelt IP-címét a bérlet lejárta előtt. * A lease\_length alapértelmezett értéke 3600 másodperc (1 óra), de lehet 0 és 1 048 575 másodperc közötti érték is. |
| **dhcpd domain**  domain\_name | (Opcionális) Megadja az ügyfélhez rendelt tartománynevet. |
| **dhcpd engedélyezése**  if\_name | Engedélyezi a DHCP-kiszolgáló szolgáltatást (démont) az ASA felületén (általában a belső interfészen). |

A példa lehetővé teszi a DHCP szolgáltatást az ASA 5506-X belső klienseinek.

**Megjegyzés** : Ha az ASA külső interfész DHCP-kliensként volt konfigurálva, akkor a **dhcpd auto \_ config OUTSIDE** globális konfigurációs mód parancs használható a DHCP által megszerzett információk átadására a belső DHCP-klienseknek.

A DHCP beállítások ellenőrzéséhez használja a következő parancsokat:

* **show dhcpd state** - Megjeleníti az aktuális DHCP állapotot a belső és külső interfészek számára.
* **show dhcpd kötés** – Megjeleníti a belső felhasználók aktuális DHCP-kötéseit.
* **dhcpd statisztikák megjelenítése** – Megjeleníti az aktuális DHCP statisztikákat.

A DHCP-összerendelések vagy statisztikák törléséhez használja a **dhcpd kötés törlése** vagy **a dhcpd statisztikák törlése** parancsot.

NETSEC-ASA(config)# **dhcpd address 10.0.0.1-10.0.1.255 INSIDE**

Warning, DHCP pool range is limited to 256 addresses, set address range as: 10.0.0.1-10.0.1.0

Address range subnet 10.0.0.1 or 10.0.1.0 is not the same as INSIDE interface subnet 192.168.1.1

NETSEC-ASA(config)# **dhcpd address 192.168.1.10-192.168.1.250 INSIDE**

NETSEC-ASA(config)# **dhcpd lease 1800**

NETSEC-ASA(config)#

21.2.14

## Szintaxis-ellenőrző – A DHCP-szolgáltatások konfigurálása

A Syntax Checker segítségével engedélyezheti a DHCP-szolgáltatásokat az ASA 5506-X-en.

A DHCP szolgáltatások konfigurálásához hajtsa végre a következő követelményeket:

* Hozzon létre egy belső címkészletet **192.168.1.10** és **192.168.1.250** között az **INSIDE** felületen.
* Állítsa be a bérlet hosszát 30 percre ( **1800** ).

NETSEC-ASA(config)# dhcpd cím 192.168.1.10-192.168.1.250 BELÜL

NETSEC-ASA(config)# dhcpd lease 1800

NETSEC-ASA(config)#

Sikeresen konfigurálta a DHCP-szolgáltatásokat egy ASA 5506-X-en.

[21.1](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Basic ASA Firewall Configuration](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[21.3](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Object Groups](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                              
* 

1. ASA Firewall Configuration
2. Object Groups

# Tárgycsoportok

21.3.1

## Bevezetés az objektumokba és tárgycsoportokba

Az objektumok újrafelhasználható összetevők, amelyek konfigurációkban használhatók. Az objektumok definiálhatók és használhatók a Cisco ASA konfigurációkban a soron belüli IP-címek, szolgáltatások, nevek stb. helyén. Az objektumok megkönnyítik a konfigurációk karbantartását, mivel egy objektum egy helyen módosítható, és a változás minden más helyen megjelenik, amely hivatkozik rá. Objektumok nélkül minden jellemző paramétereit egyszeri helyett módosítani kellene. Például, ha egy hálózati objektum meghatároz egy IP-címet és alhálózati maszkot, és meg akarja változtatni a címet, akkor csak az objektumdefinícióban kell módosítania, nem minden olyan szolgáltatásban, amely erre az IP-címre hivatkozik. Ennek az az előnye, hogy egy objektum módosításakor a változás automatikusan érvényesül minden olyan szabályra, amely a megadott objektumot használja. Ezért az objektumok megkönnyítik a konfigurációk karbantartását.

Kétféle objektum konfigurálható:

* **Hálózati objektum** – A hálózati objektum tartalmazhat egy gazdagépet, egy hálózati IP-címet, egy IP-címtartományt vagy egy teljesen minősített tartománynevet (FQDN). paranccsal van konfigurálva **Egy hálózati objektum az objektum hálózati** .
* **Szolgáltatásobjektum** – Protokollt és opcionális forrás- és/vagy célportot tartalmaz. paranccsal van konfigurálva **A szolgáltatás objektum az objektum szolgáltatás** .

**Megjegyzés** : A NAT 8.3-as és újabb verzióiban a NAT konfigurálásához hálózati objektum szükséges.

A hálózati objektumcsoportok több hálózati objektumot, valamint soron belüli hálózatokat vagy gazdagépeket is tartalmazhatnak. A hálózati objektumcsoportok IPv4- és IPv6-címek keverékét is tartalmazhatják. Az objektumok szükség esetén csatolhatók vagy leválaszthatók egy vagy több objektumcsoportról, így biztosítva, hogy az objektumok ne duplikálódjanak, hanem szükség esetén újra felhasználhatók legyenek. Ezek az objektumok NAT-ban, hozzáférési listákban és objektumcsoportokban használhatók. A hálózati objektumok a NAT konfigurálásának létfontosságú részét képezik, és nagymértékben leegyszerűsíthetik az ACL-eket.

Az ASA támogatja az objektumokat és objektumcsoportokat, amint azt a következő példa kimenete mutatja.

NETSEC-ASA(config)# **object ?**

configure mode commands/options:

network Specifies a host, subnet or range IP addresses

service Specifies a protocol/port

NETSEC-ASA(config)#

NETSEC-ASA(config)# **object-group ?**

configure mode commands/options:

icmp-type Specifies a group of ICMP types, such as echo

network Specifies a group of host or subnet IP addresses

protocol Specifies a group of protocols, such as TCP, etc

security Specifies identity attributes such as security-group

service Specifies a group of TCP/UDP ports/services

user Specifies single user, local or import user group

NETSEC-ASA(config)#

21.3.2

## Hálózati objektumok konfigurálása

Hálózati objektum létrehozásához használja az **objektum hálózati** objektumnév globális konfigurációs mód parancsát. A prompt hálózati objektum konfigurációs módra vált.

A hálózati objektumok a következőkből állhatnak:

* **host** – gazdagép címe
* **fqdn** – egy teljesen minősített domain név
* **tartomány** - IP-címek tartománya
* **alhálózat** - egy teljes IP-hálózat vagy alhálózat

A hálózati objektum konfigurációs módban elérhető parancsok a táblázatban láthatók.

A hálózati objektum értékének eltávolításához használja **no** ezen parancsok egyikének formáját. Az összes hálózati objektum törléséhez használja a **clear config object network** parancsot. Ez a parancs törli **az összes** hálózati objektumot.

| **ASA parancs** | **Leírás** |
| --- | --- |
| **attribútum attribútum**  -ügynök attribútum-típus attribútum-érték | Egy vagy több virtuális géphez kapcsolódó forgalom szűrésére szolgál. |
| **leírás** | Adja meg az objektum legfeljebb 200 karakter hosszúságú leírását. |
| **fqdn** | Teljesen minősített domain név, például egy gazdagép neve, például www.example.com. Adja meg a v4-et a cím IPv4-re való korlátozásához, a v6-ot pedig az IPv6-hoz. Ha nem ad meg címtípust, akkor a rendszer IPv4-et feltételez. |
| **gazdagép**  ip-címe | Egyetlen gazdagép IPv4 vagy IPv6 címe. |
| **tartomány**  kezdete\_hozzáadása vége\_hozzáadása | Címek tartománya. Megadhat IPv4 vagy IPv6 tartományokat. Ne használjon maszkokat vagy előtagokat. |
| **alhálózat**  { ipv4\_add ipv4\_mask | ipv6\_add  ***/***  ipv6\_prefix } | Hálózati alhálózatot rendel a megnevezett objektumhoz. |

A példa egy minta **hálózati objektum** konfigurációt jelenít meg. Az ellenőrzéshez használja a **show running-config object** parancsot. konfigurációja **Figyelje meg, hogy a tartomány** előző konfigurációját **felülírja a gazdagép** .

NetSec-ASA(config)# **object network EXAMPLE-1**

NetSec-ASA(config-network-object)# **host 192.168.1.3**

NetSec-ASA(config-network-object)# **exit**

NetSec-ASA(config)# **show run object**

object network EXAMPLE-1

host 192.168.1.3

NetSec-ASA(config)# **object network EXAMPLE-1**

NetSec-ASA(config-network-object)# **range 192.168.1.10 192.168.1.20**

NetSec-ASA(config-network-object)# **exit**

NetSec-ASA(config)# **show run object**

object network EXAMPLE-1

range 192.168.1.10 192.168.1.20

NetSec-ASA(config)#

21.3.3

## Szervizobjektumok konfigurálása

Szolgáltatásobjektum létrehozásához használja az **objektum szolgáltatásobjektum** -név globális konfigurációs mód parancsot. A prompt szolgáltatásobjektum konfigurációs módra vált. A szolgáltatásobjektum tartalmazhat protokollt, ICMP-t, ICMPv6-ot, TCP-t vagy UDP-portot (vagy porttartományokat).

A példa az elérhető szolgáltatási lehetőségeket mutatja be.

NETSEC-ASA(config)# **object service EXAMPLE-2**

NETSEC-ASA(config-service-object)#

NETSEC-ASA(config-service-object)# **service ?**

service-object mode commands/options:

<0-255> Enter protocol number (0 - 255)

ah

eigrp

esp

gre

icmp

icmp6

igmp

igrp

ip

ipinip

ipsec

nos

ospf

pcp

pim

pptp

sctp

snp

tcp

udp

configure mode commands/options:

call-home Enable or disable Smart Call-Home

internal Advanced settings (use only under Cisco supervision)

password-recovery Password recovery configuration

resetinbound Send reset to a denied inbound TCP packet

resetoutbound Send reset to a denied outbound TCP packet

resetoutside Send reset to a denied TCP packet to outside interface

sw-reset-button Configure software reset button

NETSEC-ASA(config-service-object)#

A táblázat áttekintést nyújt a rendelkezésre álló általános szolgáltatási lehetőségekről. Az opcionális kulcsszavak a forrásport vagy a célport, vagy mindkettő azonosítására szolgálnak. Az olyan operátorok, mint **az eq** (egyenlő), **a neq** (nem egyenlő), **az lt** (kisebb, mint), **a gt** (nagyobb, mint) és **a range** , támogatják a port konfigurálását egy adott protokollhoz. Ha nincs megadva operátor, az alapértelmezett operátor az **eq** .

A szolgáltatásobjektum eltávolításához használja a **no** parancs formáját. Az összes szolgáltatásobjektum törléséhez használja a **clear config object service** parancsot.

| **ASA parancs** | **Leírás** |
| --- | --- |
| **szolgáltatási**  protokoll | Megadja az IP protokoll nevét vagy számát. |
| **szolgáltatás tcp**  [  **forrás**  operátor port ]  [  **cél**  operátor port ] | Megadja, hogy a szolgáltatásobjektum a TCP protokollhoz való. |
| **service udp**  [  **forrás**  operátor port ]  [  **cél**  operátor port ] | Megadja, hogy a szolgáltatásobjektum az UDP protokollhoz való. |
| **szolgáltatás icmp**  [ icmp-type [ icmp\_code ]] | Megadja, hogy a szolgáltatásobjektum az ICMP protokollhoz való. |
| **szolgáltatás icmp6**  [ icmp-type [ icmp\_code ]] | Megadja, hogy a szolgáltatásobjektum az ICMPv6 protokollhoz való. |

A példa egy minta szolgáltatásobjektum konfigurációt jelenít meg. Egy szolgáltatásobjektum neve csak egy protokollhoz és porthoz (vagy portokhoz) társítható. Ha egy meglévő szolgáltatásobjektum más protokollal és porttal van konfigurálva, az új konfiguráció lecseréli a meglévő protokollt és portot az újakra.

Az ellenőrzéshez használja a **show running-config object service** parancsot.

NETSEC-ASA(config)# **object service SERV-1**

NETSEC-ASA(config-service-object)# **service tcp destination eq ftp**

NETSEC-ASA(config-service-object)# **service tcp destination eq www**

NETSEC-ASA(config-service-object)# **exit**

NETSEC-ASA(config)# **show run object service**

object service SERV-1

service tcp destination eq www

NETSEC-ASA(config)#

21.3.4

## Tárgycsoportok

Az objektumok csoportosíthatók objektumcsoport létrehozásához. Hasonló objektumok csoportosításával egy objektumcsoport használható a hozzáférés-vezérlési bejegyzésben (ACE), ahelyett, hogy minden egyes objektumhoz külön kellene megadni egy ACE-t.

**Megjegyzés** : Protokoll objektumcsoport is létrehozható. Ez azonban nem ajánlott, helyette egy szolgáltatásobjektum-csoportot kell használni.

Az alábbi irányelvek és korlátozások vonatkoznak az objektumcsoportokra:

* Az objektumok és objektumcsoportok ugyanazon a névteren osztoznak.
* Az objektumcsoportoknak egyedi névvel kell rendelkezniük.
* Egy objektumcsoportot nem lehet eltávolítani vagy kiüríteni, ha parancsban használják.
* Az ASA nem támogatja az IPv6 beágyazott objektumcsoportokat.

Ötféle objektumcsoport létezik.

* **Hálózat** – A hálózati alapú objektumcsoport IP-gazda-, alhálózat- vagy hálózati címek listáját határozza meg.
* **Felhasználó** – Helyileg létrehozott, valamint importált Active Directory felhasználói csoportok definiálhatók az identitástűzfalat támogató szolgáltatásokhoz.
* **Szolgáltatás** – A szolgáltatás alapú objektumcsoport a TCP, UDP vagy TCP és UDP portok objektumba történő csoportosítására szolgál. Az ASA lehetővé teszi egy szolgáltatásobjektum-csoport létrehozását, amely TCP-szolgáltatásokat, UDP-szolgáltatásokat, ICMP-típusú szolgáltatásokat és bármilyen protokollt, például ESP-t, GRE-t és TCP-t tartalmazhat.
* **ICMP-típus** – Az ICMP protokoll egyedi típusokat használ a vezérlőüzenetek küldésére (RFC 792). Az ICMP típusú objektumcsoport csoportosíthatja a szervezet biztonsági igényeinek kielégítéséhez szükséges típusokat, például létrehozhat egy ECHO nevű objektumcsoportot a visszhang és az echo-reply csoportosításához.
* **Biztonság** – A biztonsági csoport objektumcsoportja használható a Cisco TrustSec-et támogató szolgáltatásokban, ha a csoportot egy kiterjesztett ACL-be foglalják, ami viszont egy hozzáférési szabályban használható.

21.3.5

## Állítsa be a közös objektumcsoportokat

Hálózati objektumcsoport konfigurálásához használja az **objektumcsoport hálózat** grp-name globális konfigurációs mód parancsát. A parancs beírása után adjon hozzá hálózati objektumokat a hálózati csoporthoz a **network-object** és **a group-object** parancsokkal.

**Megjegyzés** : A hálózati objektumcsoport nem használható a NAT megvalósítására. A NAT megvalósításához hálózati objektum szükséges.

ICMP-objektumcsoport konfigurálásához használja az **objektumcsoport icmp-type** grp-name globális konfigurációs mód parancsát. A parancs beírása után adjon hozzá ICMP objektumokat az ICMP objektumcsoporthoz az **icmp-object** és **a group-object** parancsokkal.

A példa egy minta hálózati objektumcsoport konfigurációt jelenít meg.

NETSEC-ASA(config)# **object-group network ADMIN-HOST**

NETSEC-ASA(config-network-object-group)# **description Administrative hosts**

NETSEC-ASA(config-network-object-group)# **network-object host 192.168.1.3**

NETSEC-ASA(config-network-object-group)# **network-object host 192.168.1.4**

NETSEC-ASA(config-network-object-group)# **exit**

NETSEC-ASA(config)# **object-group network ALL-HOSTS**

NETSEC-ASA(config-network-object-group)# **description All inside hosts**

NETSEC-ASA(config-network-object-group)# **network-object 192.168.1.32 255.255.255.240**

NETSEC-ASA(config-network-object-group)# **group-object ADMIN-HOST**

NETSEC-ASA(config-network-object-group)# **exit**

NETSEC-ASA(config)# **show run object-group**

object-group network ADMIN-HOST

description Administrative host IP addresses

network-object host 192.168.1.3

network-object host 192.168.1.4

object-group network ALL-HOSTS

network-object 192.168.1.32 255.255.255.240

group-object ADMIN-HOST

NETSEC-ASA(config)#

A példa egy minta ICMP-típusú objektumcsoport konfigurációt jelenít meg.

NETSEC-ASA(config)# **object-group icmp-type ICMP-ALLOWED**

NETSEC-ASA(config-icmp-object-group)# **icmp-object echo**

NETSEC-ASA(config-icmp-object-group)# **icmp-object time-exceeded**

NETSEC-ASA(config-icmp-object-group)# **exit**

NETSEC-ASA(config)# **show running-config object-group id ICMP-ALLOWED**

object-group icmp-type ICMP-ALLOWED

icmp-object echo

icmp-object time-exceeded

NETSEC-ASA(config)#

Szolgáltatásobjektum-csoport konfigurálásához használja az **objektumcsoport szolgáltatás** grp-name globális konfigurációs mód parancsát. A szolgáltatásobjektum-csoport TCP-szolgáltatások, UDP-szolgáltatások, ICMP-típusú szolgáltatások és bármilyen protokoll keverékét határozhatja meg. parancs bevitele után **Az objektumcsoport szolgáltatás** adjon hozzá szolgáltatásobjektumokat a szolgáltatáscsoporthoz a **service-object** és **a group-object** parancsok segítségével.

Szolgáltatásobjektum-csoport TCP, UDP vagy TCP és UDP számára történő beállításához adja meg a beállítást a **objektumcsoport szolgáltatásban** grp-name [ **tcp** | **udp** | **tcp-udp** ] globális konfigurációs mód parancsot. Ha **a tcp** , **udp** vagy **tcp-udp** opcionálisan meg van adva a parancssorban, a szolgáltatás a TCP/UDP port specifikációiból egy szabványos szolgáltatásobjektum csoportot határoz meg, például "eq smtp" és "range 2000 2010". A parancs beírása után adjon hozzá portobjektumokat a szolgáltatáscsoporthoz a **port-object** és **group-object** parancsokkal.

Az összes objektumcsoport konfigurációból való eltávolításához használja a **Clear configure object-group** globális konfigurációs mód parancsot.

A csoportobjektum-konfigurációk ellenőrzéséhez használja a **show running-config object-group** parancsot.

Az ACL-ek és a NAT konfigurálásakor gyakorlati példákat mutatunk be az objektumcsoportokra. Az ASA nem támogatja az IPv6 beágyazott objektumcsoportokat.

A példa egy minta szolgáltatásobjektum-csoport konfigurációt jelenít meg.

NETSEC-ASA(config)# **object-group service SERVICES-1**

NETSEC-ASA(config-service-object-group)# **service-object tcp destination eq www**

NETSEC-ASA(config-service-object-group)# **service-object tcp destination eq https**

NETSEC-ASA(config-service-object-group)# **service-object tcp destination eq pop3**

NETSEC-ASA(config-service-object-group)# **service-object udp destination eq ntp**

NETSEC-ASA(config-service-object-group)# **exit**

NETSEC-ASA(config)#

NETSEC-ASA(config)# **object-group service SERVICES-2 tcp**

NETSEC-ASA(config-service-object-group)# **port-object eq www**

NETSEC-ASA(config-service-object-group)# **port-object eq smtp**

NETSEC-ASA(config-service-object-group)# **exit**

NETSEC-ASA(config)#

NETSEC-ASA(config)# **object-group service SERVICES-3 tcp**

NETSEC-ASA(config-service-object-group)# **group-object SERVICES-2**

NETSEC-ASA(config-service-object-group)# **port-object eq ftp**

NETSEC-ASA(config-service-object-group)# **port-object range 2000 2005**

NETSEC-ASA(config-service-object-group)# **exit**

NETSEC-ASA(config)#

21.3.6

## Ellenőrizze, hogy megértette – Tárgycsoportok

Az űrlap teteje

Ellenőrizze, hogy megértette-e az objektumcsoportok típusait, és válassza ki a megfelelő választ a következő kérdésekre.

1. Melyik típusú objektumcsoport tartalmazhat szolgáltatásokat, például TCP-t és UDP-t, és tartalmazhat bármilyen protokollt, például ESP-t vagy GRE-t?

Az űrlap alja

Melyik típusú objektumcsoport használ egyedi típusokat a vezérlőüzenetek küldésére?

Milyen típusú objektumcsoport használható a hozzáférés szabályozására az identitástűzfallal?

Milyen típusú objektumcsoportot használnak a Cisco TrustSec-et támogató szolgáltatások azáltal, hogy a csoportot egy kiterjesztett ACL-be foglalják, amely viszont egy hozzáférési szabályban használható?

Melyik típusú objektumcsoport már nem ajánlott, és le kell cserélni szolgáltatási objektumcsoportra?

Melyik típusú objektumcsoport határoz meg egy teljes tartománynév-címet, gazdagépet, alhálózatot vagy IP-címtartományt?

[21.2](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Configure Management Settings and Services](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[21.4](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[ASA ACLs](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                     
* 

1. ASA Firewall Configuration
2. ASA ACLs

# ASA ACL-ek

21.4.1

## ASA ACL-ek

A Cisco ASA 5506-X alapvető forgalomszűrési képességeket biztosít az ACL-ekkel. Az ACL-ek szabályozzák a hozzáférést a hálózaton azáltal, hogy megakadályozzák a meghatározott forgalom belépését vagy kilépését. Ezen túlmenően, az ACL használható annak a forgalomnak a kiválasztására, amelyre egy szolgáltatás vonatkozni fog, ezáltal egy megfelelő szolgáltatást hajthat végre, nem pedig vezérlőszolgáltatást.

Sok hasonlóság van az ASA ACL-ek és az IOS ACL-ek között. Például mindkettő ACE-kből áll, amelyeket felülről lefelé, egymás után dolgoznak fel, és **van egy implicit tagadás** alul . Ezenkívül továbbra is érvényes az a szabály, hogy interfészenként, protokollonként és irányonként csak egy ACL.

Az ASA ACL-ek abban különböznek az IOS ACL-ektől, hogy helyettesítő karaktermaszk (pl. 0.0.0.255) helyett hálózati maszkot (pl. 255.255.255.0) használnak. Szintén a legtöbb ASA ACL neve számozás helyett.

Ezek a hasonlóságok az ASA ACL-ek és az IOS ACL-ek között:

* Az ACL-ek egy vagy több ACE-ből állnak. Az ACE-ket protokollra, forrás- és cél IP-címre, hálózatra vagy a forrás- és célportra alkalmazzák.
* Az ACL-ek feldolgozása egymás után felülről lefelé történik.
* A feltételek egyezése az ACL-ből való kilépést okozza.
* Az alján van egy implicit tagadás.
* Megjegyzések ACE vagy ACL szerint adhatók hozzá.
* Interfészenként, protokollonként és irányonként csak egy hozzáférési lista alkalmazható.
* Az ACL-ek az időtartományok alapján engedélyezhetők/letilthatók.

Ezek a különbségek az ASA ACL-ek és az IOS ACL-ek között:

* Az ASA hálózati maszkot (pl. 255.255.255.0) használ, nem helyettesítő karakteres maszkot (pl. 0.0.0.255).
* Az ACL-ek számozás helyett mindig el vannak nevezve.
* Alapértelmezés szerint az interfész biztonsági szintjei hozzáférés-vezérlést alkalmaznak konfigurált ACL nélkül.

21.4.2

## Az ASA ACL szűrés típusai

A biztonsági berendezések ACL-jei nem csak a készüléken áthaladó csomagok szűrésére használhatók, hanem a készüléknek szánt csomagok szűrésére is.

* **Átmenő forgalom szűrése** – A biztonsági berendezésen áthaladó forgalom az egyik interfészről a másikra. A konfiguráció két lépésben történik. Az első lépés az ACL beállítása. A második lépés az ACL alkalmazása egy interfészre.
* **A dobozba szállított forgalom szűrése** – Felügyeleti hozzáférési szabályként is ismert, a dobozba szállított forgalom szűrése az ASA-nál végződő forgalomra vonatkozik. Az ASA vezérlősíkjára szánt forgalom szűrésére készültek. Egy lépésben fejeződnek be, de a hozzáférés-szabályozás megvalósításához további szabályokra van szükség.

Az ASA-eszközök az interfész biztonsági szintje miatt különböznek útválasztóiktól. Alapértelmezés szerint a biztonsági szintek hozzáférés-vezérlést alkalmaznak konfigurált ACL nélkül. Például egy biztonságosabb interfészről, például a 100-as biztonsági szintről érkező forgalom hozzáférhet a kevésbé biztonságos interfészekhez, például a 0. szinthez. A kevésbé biztonságos interfészről érkező forgalom blokkolva van a biztonságosabb interfészekhez való hozzáférésben.

Például egy 100-as biztonsági szinttel rendelkező belső hálózatról származó gazdagép hozzáférhet a külső interfészhez 0-s biztonsági szinttel, az alábbiak szerint.

Az ábrán egy asa látható 3 interfésszel a külső, a belső és a dm z-hez csatlakoztatva. A külső interfész neve külső, 0-s biztonsági szinttel. A belső interfész neve belső 100-as biztonsági szinttel. A dmz interfész neve dmz 50-es biztonsági szinttel

G1/1 G1/3

G1/2

A biztonságosabb interfészek hozzáférhetnek a kevésbé biztonságos interfészekhez. Biztonsági kívül DMZ-n szint: 50 Webszerver Biztonsági szint: 100 Internetes biztonsági szint: 0

A 0-s biztonsági szintű külső interfészről származó gazdagép azonban nem férhet hozzá a belső magasabb szintű interfészhez, amint az alább látható. A kevésbé biztonságos interfészek blokkolva vannak a biztonságosabb interfészek elérésében. Szükség esetén az ACL-t kifejezetten be kell állítani, hogy lehetővé tegye az alacsonyabb biztonsági szintről a magasabb biztonsági szintre irányuló forgalmat.

Az ábrán egy asa látható 3 interfésszel a külső, a belső és a dm z-hez csatlakoztatva. A külső interfész neve külső, 0-s biztonsági szinttel. A belső interfész neve belső 100-as biztonsági szinttel. A dmz interfész neve dmz 50-es biztonsági szinttel

G1/1 G1/3

G1/2

A kevésbé biztonságos interfészek blokkolva vannak a biztonságosabb interfészek elérésében. Biztonsági kívül DMZ-n szint: 50 Webszerver Biztonsági szint: 100 Internetes biztonsági szint: 0

Az azonos biztonsági szintekkel rendelkező interfészek közötti kapcsolódás engedélyezéséhez az **azonos biztonsági forgalom engedélyezése interfész** globális konfigurációs mód parancsra van szükség. Ha engedélyezni szeretné, hogy a forgalom ugyanarra az interfészre lépjen be és kilépjen, például amikor a titkosított forgalom belép egy interfészbe, majd ugyanazon az interfészen kódolatlanul továbbítódik, használja az **azonos biztonsági forgalom engedély interfészen belüli** globális konfigurációs mód parancsát.

21.4.3

## Az ASA ACL-ek típusai

Az ASA ötféle hozzáférési listát támogat:

* **Kiterjesztett hozzáférési lista** – Az ACL leggyakoribb típusa. Egy vagy több ACE-t tartalmaz a forrás- és célcímek és protokollok, portok (TCP vagy UDP esetén) vagy az ICMP típusának (ICMP esetén) megadásához. A forgalom szűrésére és a forgalom azonosítására szolgálnak, amelyet különféle szolgáltatásokkal kell kezelni.
* **Szabványos hozzáférési lista** – Az IOS-től eltérően, ahol a szabványos ACL azonosítja a forrás gazdagépet/hálózatot, az ASA szabványos ACL-ek a cél IP-címek azonosítására szolgálnak. Általában csak OSPF-útvonalakhoz használják, és az OSPF-újraelosztáshoz használható útvonaltérképekben. A szabványos hozzáférési listák nem alkalmazhatók a forgalmat irányító interfészekre.
* **EtherType hozzáférési lista** – EtherType ACL csak akkor konfigurálható, ha a biztonsági készülék transzparens módban fut.
* **Webtípus hozzáférési lista** – Az ügyfél nélküli SSL VPN-forgalom szűrésére szolgál. Ezek az ACL-ek megtagadhatják a hozzáférést URL-ek vagy célcímek alapján.
* **IPv6 hozzáférési lista** – Annak meghatározására szolgál, hogy melyik IPv6-forgalmat kell blokkolni, és melyik forgalmat továbbítani kell az útválasztó interfészén.

Használja a **help access-list** privilegizált EXEC parancsot az ASA platformon támogatott összes ACL szintaxisának megjelenítéséhez.

**Megjegyzés** : Ennek a modulnak a középpontjában a kiterjesztett ACL-ek állnak.

Az alábbi táblázatok példákat adnak a kiterjesztett, szabványos és IPv6 ACL-ek használatára.

A táblázat példákat tartalmaz a kiterjesztett ACL-ek használatára.

| **ACL használat** | **Leírás** |
| --- | --- |
| Az IP-forgalom hálózati hozzáférésének szabályozása | Az ASA nem engedélyez semmilyen forgalmat egy alacsonyabb biztonsági interfészről egy magasabb biztonsági interfészre, kivéve, ha ezt egy kiterjesztett hozzáférési lista kifejezetten engedélyezi. |
| Határozza meg a forgalmat az AAA szabályok szerint | Az AAA szabályok hozzáférési listákat használnak a forgalom azonosítására. |
| Határozza meg a NAT címeit | A NAT házirend lehetővé teszi a helyi forgalom azonosítását a címfordításhoz a forrás- és célcímek kiterjesztett hozzáférési listában történő megadásával. |
| Hozzon létre VPN hozzáférést | A kiterjesztett hozzáférési lista a VPN-parancsokban használható. |
| Forgalom azonosítása a moduláris irányelv-keretrendszerhez (MPF) | * A hozzáférési listák használhatók a forgalom azonosítására egy osztálytérképen, amelyet az MPF-et támogató szolgáltatásokhoz használnak. * Az MPF-et támogató funkciók közé tartozik a TCP, az általános csatlakozási beállítások és az ellenőrzés. |

A táblázat példákat tartalmaz a szabványos ACL-ek használatára.

| **ACL használat** | **Leírás** |
| --- | --- |
| Határozza meg az OSPF célhálózatát az útvonaltérképeken | * A normál hozzáférési listák csak a célcímet tartalmazzák. * Használható az OSPF útvonalak újraelosztásának szabályozására. |
| VPN szűrők | A LAN-LAN (L2L), a Cisco VPN Client és a Cisco AnyConnect Secure Mobility Client forgalom szűrése. |

A táblázat példát mutat az IPv6 ACL-ek használatára.

| **ACL használat** | **Leírás** |
| --- | --- |
| Az IPv6 hálózatok hálózati hozzáférésének szabályozása | Használható hozzáférési listák hozzáadására és alkalmazására az IPv6-hálózatok forgalmának szabályozására. |

21.4.4

## Szintaxis az ASA ACL konfigurálásához

Az ASA ACL konfigurációs szintaxis beállításai kissé túlterheltek lehetnek, figyelembe véve a támogatott paraméterek számát, amint **help access-list** az a példában látható parancs kimenetének részleges kimenetén is látható. Ezek a paraméterek nemcsak teljes körű ellenőrzést biztosítanak az adminisztrátornak arról, hogy mit kell ellenőrizni, hanem teljes naplózási képességet is biztosítanak a forgalom későbbi elemzéséhez.

NETSEC-ASA(config)# **help access-list**

USAGE:

Extended access list:

Use this to configure policy for IP traffic through the firewall

[no] access-list <id> [line <line\_num>] [extended] {deny | permit}

{<protocol> | object-group {<service\_obj\_grp\_id> |

<protocol\_obj\_grp\_id>} | object <service\_object\_name>}

[user-group [<domain\_nickname>\\]<user\_group\_name> |

user [<domain\_nickname>\]<user\_name> |

object-group-user < object\_group\_user\_name>]

[security-group {name <sgname> | tag <sgt>} |

object-group-security <security\_obj\_grp\_id>]

{host <sip> | <sip> <smask> | <sip-prefix> |

interface <ifc> | any | any4 | any6

object-group <network\_obj\_grp\_id> |

object <network\_obj\_name>}

[<operator> <port> [<port>] |

object-group <service\_obj\_grp\_id>]

[security-group {name <sgname> | tag <sgt>} |

object-group-security <security\_obj\_grp\_id>]

{host <dip> | <dip> <dmask> | <dip-prefix> |

interface <ifc> | any | any4 |any6

object-group <network\_obj\_grp\_id> |

object <network\_obj\_name>}

[<operator> <port> [<port>] |

object-group <service\_obj\_grp\_id>]

- More -

Az ACL-ekkel számos lehetőség használható. A legtöbb igényre azonban a szintaxis egy hasznosabb és tömörebb változata látható alább.

Az ábra a help access-list parancs részleges kimenetét mutatja a CLI-ben. Az elemeket a továbbiakban ismertetjük.

access-list id extended {deny | permit} protocol {source\_addr source\_mask | any | host src\_host | interface src\_if\_name} [operator port [port]] {dest\_addr dest\_mask} | any | host dst\_host | interface dst\_if\_name}[operator port [port]]

ACL név, de lehet szám is. Példák: IP, TCP, UDP forrásforgalom a szűréshez.   
Ez lehet egy hálózati objektumcsoport is. Az interfész opció a dobozba szállított forgalom szűrésére szolgál. Az operátor lehet lt (kisebb, mint), gt (nagyobb, mint), eq (egyenlő), neq (nem egyenlő) operandusok és egy befogadó tartományhoz tartozó tartomány. A port lehet portszám vagy TCP vagy UDP port neve. Ez egy szolgáltatásobjektum-csoport is lehet. Szűrendő célforgalom.   
Ez lehet egy hálózati objektumcsoport. Az interfész opció a dobozba szállított forgalom szűrésére szolgál.

Az IOS és az ASA ACL-ek hasonló elemekkel rendelkeznek, de egyes lehetőségek az ASA-tól függően változnak. A táblázat az ASA ACL elemeit írja le.

**Megjegyzés** : Az összes ACL szintaxis magyarázata túlmutat ennek a modulnak a hatókörén, és nem vizsgáljuk tovább.

| **Elem** | **Leírás** |
| --- | --- |
| ACL azonosító | Az ACL neve. Bármilyen alfanumerikus név lehet, legfeljebb 241 karakter. |
| Akció | Lehet **engedélyezni** vagy **megtagadni** . |
| Protokollszám – Forrás | Lehet az összes forgalom IP-címe, vagy a név/IP protokollszám (0-250), beleértve az icmp-t (1), a tcp-t (6), az udp-t (17), vagy egy protokollobjektum-csoportot. |
| Forrás | * Azonosítja a forrást, és lehet **bármilyen** , gazdagép, hálózat vagy hálózati objektumcsoport. * A dobozba szállított forgalom szűréséhez az interfész kulcsszót használjuk az ASA forrásfelületének megadására. |
| Forrás port üzemeltetője | * (Opcionális) Az operandus a forrásporttal együtt használatos. * Az érvényes operandusok közé tartozik **az lt** (kisebb, mint), **a gt** (nagyobb, mint), **az eq** (egyenlő), **a neq** (nem egyenlő) és **a tartomány** egy befogadó tartományhoz. |
| Forrás port | (Opcionális) Lehet a tényleges TCP- vagy UDP-portszám, portnevek kiválasztása vagy szolgáltatásobjektum-csoport. |
| Rendeltetési hely | * lehet . **Azonosítja a célt, és a forráshoz hasonlóan bármely** , gazdagép, hálózat vagy hálózati objektumcsoport * A dobozba szállított forgalomszűréshez az interfész kulcsszót használjuk az ASA célfelületének megadására. |
| A célkikötő üzemeltetője | * (Opcionális) Az operandus a célporttal együtt használatos. * Az érvényes operandusok megegyeznek a forrásport operandusokkal. |
| Célkikötő | (Opcionális) Lehet a tényleges TCP- vagy UDP-portszám, portnevek kiválasztása vagy szolgáltatásobjektum-csoport. |
| Napló | Beállíthat elemeket a rendszernaplóhoz, beleértve a súlyossági szintet és a naplózási intervallumot. |
| Időtartományban | (Opcionális) Adja meg az ACE időtartományát. |

21.4.5

## Szintaxis az ASA ACL alkalmazásához

Az ACL konfigurálása után a következő lépés az interfészre történő alkalmazása bejövő vagy kimenő irányban. Az ACL alkalmazása globális konfigurációs módban történik.

használó interfészre történő alkalmazásához . **A példa megjeleníti a parancs szintaxisát és paraméterleírását az ACL-nek az access-group** parancs szintaxisát

ciscoasa(config)#  **access-group**  id {  **in**  |  **out**  }  **interfész**  if\_name [  **felhasználónkénti felülbírálás**  |  **irányítósík**  ]

| **Szintaxis** | **Leírás** |
| --- | --- |
| **hozzáférési csoport** | Az ACL interfészre történő alkalmazására használt kulcsszó. |
| id | Az interfészre alkalmazandó tényleges ACL neve. |
| **ban ben** | Az ACL kiszűri a bejövő csomagokat. |
| **ki** | Az ACL kiszűri a kimenő csomagokat. |
| **felület** | Kulcsszó annak a felületnek a megadásához, amelyre az ACL-t alkalmazni kell. |
| if\_name | Annak az interfésznek a neve, amelyre ACL-t kell alkalmazni. |
| **felhasználónkénti felülbírálás** | Lehetőség, amely lehetővé teszi a letölthető ACL-ek felülbírálását az interfész ACL-jén. |
| **irányító-sík** | Kulcsszó annak meghatározására, hogy az alkalmazott ACL elemzi-e az ASA-nak szánt forgalmat kezelési célból. |

Az ACL-ek ellenőrzéséhez használja a **show access-list** és **show running-config access-list** parancsokat.

A konfigurált ACL törléséhez használja a **clear configure access-list** id parancsot.

21.4.6

## ASA ACL példák

Kattintson az alábbi négy ASA ACL-példára rövid magyarázatokkal.

NETSEC-ASA(config)# **access-list ACL-IN extended permit ip any any**

NETSEC-ASA(config)# **access group ACL-IN in interface INSIDE**

* Az ACL lehetővé teszi, hogy a belső hálózaton lévő összes gazdagép átmenjen az ASA-n.
* Alapértelmezés szerint az összes többi forgalom le van tiltva, hacsak nincs kifejezetten engedélyezve.

21.4.7

## ACL-ek és objektumcsoportok

Tekintsük az ábrán látható mintatopológiát, amelyben két megbízható távoli gazdagép, a PC1 és a PC2 hozzáférését engedélyezni kell a két belső web- és e-mail-kiszolgálóhoz. Minden egyéb, az ASA-n áthaladó forgalmat meg kell szüntetni és naplózni kell.

Az ábra egy ACL-referenciatopológiát mutat be, amelyben a két megbízható távoli gazdagép hozzáférését engedélyezni kell a belső kiszolgálókhoz az alábbi asa-konfiguráció miatt.

.131 .132 209.165.202.128/27 G1/2 G1/3 G1/1 209.165.200.224/27 209.165.201.1 209.165.201.2 PC1

PC2

Web és e-mail szerver Web és e-mail kiszolgáló kívül Interneten az

Az alábbi példában látható ACL-hez két ACE-re van szükség minden PC-hez a feladat végrehajtásához. Az implicit **megtagad minden** ledobást, és naplózza azokat a csomagokat, amelyek nem egyeznek az e-mailekkel vagy a webszolgáltatásokkal. Ahogy a példában is látható, az ACL-eket mindig alaposan dokumentálni kell a **megjegyzés** paranccsal.

NETSEC-ASA(config)# **access-list ACL-IN remark Permit PC-1 -> Server A for HTTP / SMTP**

NETSEC-ASA(config)# **access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.131 eq http**

NETSEC-ASA(config)# **access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.131 eq smtp**

NETSEC-ASA(config)# **access-list ACL-IN remark Permit PC-1 -> Server B for HTTP / SMTP**

NETSEC-ASA(config)# **access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.132 eq http**

NETSEC-ASA(config)# **access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.132 eq smtp**

NETSEC-ASA(config)# **access-list ACL-IN remark Permit PC-2 -> Server A for HTTP / SMTP**

NETSEC-ASA(config)# **access-list ACL-IN extended permit tcp host 209.165.201.2 host 209.165.202.131 eq http**

NETSEC-ASA(config)# **access-list ACL-IN extended permit tcp host 209.165.201.2 host 209.165.202.131 eq smtp**

NETSEC-ASA(config)# **access-list ACL-IN remark Permit PC-2 -> Server B for HTTP / SMTP**

NETSEC-ASA(config)# **access-list ACL-IN extended permit tcp host 209.165.201.2 host 209.165.202.132 eq http**

NETSEC-ASA(config)# **access-list ACL-IN extended permit tcp host 209.165.201.2 host 209.165.202.132 eq smtp**

NETSEC-ASA(config)# **access-list ACL-IN extended deny ip any any log**

NETSEC-ASA(config)# **access-group ACL-IN in interface OUTSIDE**

Az ACL szintaxis ellenőrzéséhez használja a **show running-config access-list** és **a show access-list** parancsokat a példában látható módon.

NETSEC-ASA(config)# **show running-config access-list**

access-list ACL-IN remark Permit PC-1 -> Server A for HTTP / SMTP

access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.131 eq www

access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.131 eq smtp

access-list ACL-IN remark Permit PC-1 -> Server B for HTTP / SMTP

access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.132 eq www

access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.132 eq smtp

access-list ACL-IN remark Permit PC-2 -> Server A for HTTP / SMTP

access-list ACL-IN extended permit tcp host 209.165.201.2 host 209.165.202.131 eq www

access-list ACL-IN extended permit tcp host 209.165.201.2 host 209.165.202.131 eq smtp

access-list ACL-IN remark Permit PC-2 -> Server B for HTTP / SMTP

access-list ACL-IN extended permit tcp host 209.165.201.2 host 209.165.202.132 eq www

access-list ACL-IN extended permit tcp host 209.165.201.2 host 209.165.202.132 eq smtp

access-list ACL-IN extended deny ip any any log

NETSEC-ASA(config)#

NETSEC-ASA(config)# **show access-list ACL-IN brief**

access-list ACL-IN; 9 elements; name hash: 0x44d1c580

NETSEC-ASA(config)#

21.4.8

## ACL objektumcsoportok példái használatával

Az objektumcsoportosítás a hasonló elemek csoportosításának módja az ACE-k számának csökkentése érdekében. Hasonló objektumok csoportosításával az objektumcsoportok használhatók az ACL-ben, ahelyett, hogy minden objektumhoz külön kellene megadni az ACE-t. Objektumcsoportosítás nélkül a biztonsági berendezés konfigurációja több ezer ACE-sort tartalmazhat, amelyek kezelése nehézkessé válhat.

A példa egy tömörített ACL-szintaxist jelenít meg az ezen az oldalon található objektumcsoport-példával.

A biztonsági berendezés a szorzótényező szabályt követi az ACE-k meghatározásakor. Például, ha két külső gazdagépnek kell hozzáférnie két belső kiszolgálóhoz, amely HTTP- és SMTP-szolgáltatásokat futtat, az ASA-nak nyolc gazdagép alapú ACE-je lesz. Ezeket a következőképpen kell kiszámítani:

ACE-k száma = (2 külső gazdagép) x (2 belső szerver) x (2 szolgáltatás) = 8

Az objektumok csoportosítása a hálózati objektumokat egy csoportba, a külső gazdagépeket pedig egy másik csoportba fürtheti, amint azt a következő szintaxis mutatja. A biztonsági készülék mindkét TCP-szolgáltatást egy szolgáltatásobjektum-csoportba is kombinálhatja.

ciscoasa(config)#  **access-list**  id  **extended**  {  **deny**  |  **engedély** ​ ​ **​**  ​ **​**  ​ **​**  ​

Vegyük például a referencia topológiát az alábbi ábrán. Az előző oldalon található kiterjesztett ACL-példában ez a topológia összesen kilenc ACL ACE-t, a nyolc engedélyezési ACE-t és az implicit megtagadó ACE-t igényelt. A következő objektumok létrehozása megkönnyítheti a tényleges ACL-t egyetlen ACE-vé. Például a következő objektumcsoportok jönnek létre:

* nevű hálózati objektumcsoport **NET-HOSTS** – Két külső gazdagépet azonosít.
* nevű hálózati objektumcsoport **SERVERS** – Azonosítja az e-mail- és webszolgáltatásokat nyújtó kiszolgálókat.
* szolgáltatásobjektum csoport **HTTP-SMTP** – Az SMTP és HTTP protokollokat azonosítja.

Az ábra egy ACL hivatkozási topológiát mutat, amely ugyanazt az eredményt éri el, mint az előző oldalon lévő kiterjesztett ACL objektumcsoportok használatával. Az asa-n ennek végrehajtásához szükséges konfiguráció a következő.

.131 .132 209.165.202.128/27 G1/2 G1/3 G1/1 209.165.200.224/27 209.165.201.1 209.165.201.2 PC1

PC2

Web és   
E-mail szerver Web és   
E-mail szerver kívül Interneten az

A példa azt a konfigurációt jeleníti meg, amely ugyanazt az eredményt éri el, mint az előző oldalon lévő kiterjesztett ACL objektumcsoportok használatával.

**Megjegyzés** A korábbi **ACL-IN** paranccsal eltávolítottuk **ACE utasításokat a no access-list** .

NETSEC-ASA(config)# **object-group network NET-HOSTS**

NETSEC-ASA(config-network-object-group)# **description OG matches PC-A and PC-B**

NETSEC-ASA(config-network-object-group)# **network-object host 209.165.201.1**

NETSEC-ASA(config-network-object-group)# **network-object host 209.165.201.2**

NETSEC-ASA(config-network-object-group)# **exit**

NETSEC-ASA(config)#

NETSEC-ASA(config)# **object-group network SERVERS**

NETSEC-ASA(config-network-object-group)# **description OG matches Web / Email Servers**

NETSEC-ASA(config-network-object-group)# **network-object host 209.165.202.131**

NETSEC-ASA(config-network-object-group)# **network-object host 209.165.202.132**

NETSEC-ASA(config-network-object-group)# **exit**

NETSEC-ASA(config)#

NETSEC-ASA(config)# **object-group service HTTP-SMTP tcp**

NETSEC-ASA(config-service-object-group)# **description OG matches SMTP / WEB traffic**

NETSEC-ASA(config-service-object-group)# **port-object eq smtp**

NETSEC-ASA(config-service-object-group)# **port-object eq www**

NETSEC-ASA(config-service-object-group)# **exit**

NETSEC-ASA(config)#

NETSEC-ASA(config)# **access-list ACL-IN remark Only permit PC-A / PC-B -> Internal Servers**

NETSEC-ASA(config)# **access-list ACL-IN extended permit tcp object-group NET-HOSTS object-group SERVERS object-group HTTP-SMTP**

Az objektumcsoportok konfigurálása után bármely ACL-ben és több ACL-ben is használhatók. Egyetlen ACE használható arra, hogy a megbízható gazdagépek meghatározott szolgáltatási kérelmeket küldjenek belső kiszolgálók csoportjának.

Bár az objektumcsoportok konfigurálása unalmasnak tűnhet, az az előnye, hogy ezek az objektumok más ASA-parancsokban újra felhasználhatók, és könnyen módosíthatók. Például, ha egy új belső levelezőkiszolgálót kell hozzáadni, akkor csak a SERVERS objektumcsoportot kell szerkeszteni.

**Megjegyzés** : Az objektumcsoportok más objektumcsoportokba is beágyazhatók.

A példa a végső ACL konfigurációt jeleníti meg a futó konfigurációban.

NETSEC-ASA(config)# **show running-config access-list**

access-list ACL-IN remark Only permit PC-A / PC-B -> Internal Servers

access-list ACL-IN extended permit tcp object-group NET-HOSTS object-group SERVERS object-group HTTP-SMTP

21.4.9

## Szintaxis-ellenőrző – ASA ACL konfigurálása objektumcsoportok használatával

Használja a Szintaxis-ellenőrzőt az ASA ACL objektumcsoportok használatával történő beállításához.

Configure a network object group named **NET-HOSTS** to match hosts 209.165.201.1 and 209.165.201.2. Then exit network object configuration mode.

NETSEC-ASA(config)#object-group network NET-HOSTS

NETSEC-ASA(config-network-object-group)# description OG matches PC-A and PC-B

NETSEC-ASA(config-network-object-group)#network-object host 209.165.201.1

NETSEC-ASA(config-network-object-group)#network-object host 209.165.201.2

NETSEC-ASA(config-network-object-group)#exit

Configure a network object group named **SERVERS** to match hosts 209.165.202.131 and 209.165.202.132. Then exit network object configuration mode.

NETSEC-ASA(config)#object-group network SERVERS

NETSEC-ASA(config-network-object-group)# description OG matches Web / Email Servers

NETSEC-ASA(config-network-object-group)#network-object host 209.165.202.131

NETSEC-ASA(config-network-object-group)#network-object host 209.165.202.132

NETSEC-ASA(config-network-object-group)#exit

Konfiguráljon egy **match nevű tcp** szolgáltatásobjektum csoportot, **HTTP-SMTP** hogy megfeleljen az **smtp** portnak, majd egyeztesse a **www** porttal. Lépjen ki a hálózati objektum konfigurációs módból.

NETSEC-ASA(config)# objektumcsoport szolgáltatás HTTP-SMTP tcp

NETSEC-ASA(config-service-object-group)# leírása Az OG megfelel az SMTP/WEB forgalomnak

NETSEC-ASA(config-service-object-group)# port-object eq smtp

NETSEC-ASA(config-service-object-group)# port-object eq www

NETSEC-ASA(config-service-object-group)# kilépés

NETSEC-ASA(config)#

NETSEC-ASA(config)# access-list ACL-IN megjegyzés Csak PC-A / PC-B engedélyezése -> Belső szerverek

Az ACL-IN-re vonatkozó megjegyzést már konfigurálták. Most állítsa be **az ACL-IN-t,** hogy engedélyezze **a tcp-t** ról **a NET-HOSTS-** a **a SZERVEREKRE** használatával . **HTTP-SMTP** szolgáltatási szabályzat

NETSEC-ASA(config)# hozzáférési lista ACL-IN kiterjesztett engedély tcp objektumcsoport NET-HOSTS objektumcsoport SZERVEREK objektumcsoport HTTP-SMTP

Jelenítse meg az ACL-IN-t a futó konfigurációban.

NETSEC-ASA(config)# a futó-konfiguráció hozzáférési listája megjelenítése

access-list ACL-IN megjegyzés Csak PC-A / PC-B -> Belső szerverek engedélyezése

hozzáférési lista ACL-IN kiterjesztett engedély tcp objektumcsoport NET-HOSTS objektumcsoport SZERVEREK objektumcsoport HTTP-SMTP

Sikeresen konfigurált egy ACL-t az ASA 5506-X objektumcsoportjaival.

[21.3](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Object Groups](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[21.5](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[NAT Services on an ASA](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                         
* 

1. ASA Firewall Configuration
2. NAT Services on an ASA

# NAT szolgáltatások ASA-n

21.5.1

## ASA NAT áttekintése

Az IOS útválasztókhoz hasonlóan az ASA is támogatja a hálózati címfordítást (NAT). A NAT-ot általában arra használják, hogy a privát IP-címeket nyilvános IP-címekké alakítsák.

A NAT a következő módszerek egyikével telepíthető:

**A NAT-on belül** – A tipikus NAT-telepítési módszer az, amikor egy magasabb biztonságú interfészről származó állomás forgalommal rendelkezik egy alacsonyabb biztonságú interfészre, és az ASA a belső gazdagépcímet globális címre fordítja. Az ASA ezután visszaállítja az eredeti belső IP-címet a visszatérő forgalomhoz.

**NAT-on kívül** – Ez a módszer akkor használatos, ha le kell fordítani az alacsonyabb biztonsági szintű interfészről érkező forgalmat, amely a magasabb szintű biztonságú interfészen lévő gazdagépnek van szánva. Ez a módszer hasznos lehet annak érdekében, hogy a belső hálózaton kívül található vállalati gazdagép ismert belső IP-címről származóként jelenjen meg.

**Kétirányú NAT** – Azt jelzi, hogy a NAT-on belül és a NAT-on kívül egyaránt használatban van.

Az ábra szemlélteti a NAT-on belüli és a NAT-on kívüli áramlást.

Az ábra ugyanaz a topológia, mint az előző ábra. Az asa konfigurációja a következő.

G1/3 G1/2 G1/1 192.168.2.0/24 .3 192.168.1.0/27 .3 209.165.200.224/27 209.165.201.2

PC2

DMZ belül Interneten on belül NAT- kívül NAT-on kívül NAT- on kívül kívül   
NAT

A Cisco ASA a következő általános NAT-típusokat támogatja:

* **Dinamikus PAT** – Ez egy több az egyhez fordítás. Ezt túlterheléses NAT-nak is nevezik. Általában a privát címek belső készlete, amely túlterheli a külső interfészt vagy külső címet.
* **Statikus NAT** – Ez egy-egy fordítás. Általában egy külső cím hozzárendelése egy belső szerverhez.
* **Házirend NAT** – A házirend-alapú NAT egy szabálykészleten alapul. Ezek a szabályok meghatározhatják, hogy csak bizonyos forráscímek legyenek lefordítva, amelyek meghatározott célcímekhez és/vagy adott portokhoz vannak szánva.
* **Identity NAT** – A valódi cím statikusan lefordítva önmagára, lényegében megkerülve a NAT-ot. Érdemes lehet így konfigurálni a NAT-ot, ha címek nagy csoportját szeretné lefordítani, de ezután a címek egy kisebb részhalmazát szeretné mentesíteni.

nak nevezik, **Az ilyen típusú NAT-okat hálózati objektum-NAT-** mivel a konfigurációhoz hálózati objektumokat kell konfigurálni.

**Megjegyzés** : Egy másik ASA NAT szolgáltatás a Twice-NAT. A kétszeres NAT egyetlen szabályban ( **nat** parancs) azonosítja a forrás- és a célcímet is. A kétszeres NAT-ot a távoli hozzáférésű IPsec és SSL VPN-ek konfigurálásakor használják. A Twice-NAT túlmutat a modul hatókörén, és nem vizsgálják tovább.

21.5.2

## Dinamikus NAT konfigurálása

A hálózati objektum dinamikus NAT beállításához két hálózati objektum szükséges:

* Egy hálózati objektum, amely azonosítja a nyilvános IP-címek azon készletét, amelybe a belső címeket lefordítják. Ezek azonosítása **tartomány** vagy **alhálózati** hálózati objektum parancsokkal történik.
* A második hálózati objektum azonosítja a lefordítandó belső címeket, majd összekapcsolja a két objektumot. segítségével azonosítja . **Ezeket a tartomány** vagy **alhálózati** hálózati objektum parancsok

kötjük össze **A két hálózati objektumot ezután a nat** [ ( valós \_ if \_ name,mapped \_ if \_ name ) ] **dynamic** mapped \_ obj [ **interface** [ **ipv6** ] ] [ **dns** ] hálózati objektum paranccsal . A valódi \_ if \_ név a prenat interfész. A leképezett \_ if \_ név a postnat felület. Figyelje meg, hogy a parancs szintaxisában nincs szóköz a vessző után.

Az ábra például a dinamikus NAT, dinamikus PAT és statikus NAT konfigurálásához használt NAT hivatkozási topológiát jeleníti meg.

Ebben a dinamikus NAT-példában a 192.168.1.0/27 hálózat belső gazdagépei dinamikusan lesznek hozzárendelve nyilvános IP-címek tartományához 209.165.200.240 és 209.165.200.248 között.

Az ábra ugyanaz a topológia, mint az előző ábra. Az asa konfigurációja a következő.

G1/3 G1/2 G1/1 192.168.2.0/24 .3 192.168.1.0/27 .3 209.165.200.224/27 209.165.201.2

PC2

DMZ belül Interneten on belül NAT- kívül NAT-on kívül NAT- on kívül kívül   
NAT

A példa egy dinamikus NAT-konfiguráció mintát jelenít meg a feladat végrehajtásához. A **PUBLIC** hálózati objektum azonosítja a nyilvános IP-címeket, amelyekre le kell fordítani, míg a **DYNAMIC-NAT** objektum a lefordítandó belső címeket, és **paranccsal a PUBLIC** hálózati objektumhoz **a NAt** van kötve .

NETSEC-ASA(config)# **object network PUBLIC**

NETSEC-ASA(config-network-object)# **range 209.165.200.240 209.165.200.248**

NETSEC-ASA(config-network-object)# **exit**

NETSEC-ASA(config)#

NETSEC-ASA(config)# **object network DYNAMIC-NAT**

NETSEC-ASA(config-network-object)# **subnet 192.168.1.0 255.255.255.224**

NETSEC-ASA(config-network-object)# **nat (INSIDE,OUTSIDE) dynamic PUBLIC**

NETSEC-ASA(config-network-object)# **end**

NETSEC-ASA#

Ha engedélyezni szeretné a belső gazdagépeknek a külső gazdagépek ping-elését, akkor egy házirend-leképezés segítségével engedélyezheti az ICMP-üzenetek visszatérését a külső interfészen keresztül. A példa azt a konfigurációt mutatja be, amely lehetővé teszi az ICMP-forgalom visszatérését a külső gazdagépektől az **OUTSIDE** interfészen keresztül.

NETSEC-ASA(config)# **policy-map global\_policy**

NETSEC-ASA(config-pmap)# **class inspection\_default**

NETSEC-ASA(config-pmap-c)# **access-list ICMPACL extended permit icmp any any**

NETSEC-ASA(config)# **access-group ICMPACL in interface OUTSIDE**

NETSEC-ASA(config)#

Miután a belső gazdagép megpingelte a külső gazdagépet, ellenőrizze a hálózati cím fordítását a **show xlate** paranccsal a példában látható módon. További információk gyűjthetők a **show nat** és **a show nat detail** parancsokkal.

NETSEC-ASA(config)# **show xlate**

1 in use, 1 most used

Flags: D - DNS, e - extended, I - identity, I - dynamic, r - portmap,

s - static, T - twice, N - net-to-net

NAT from INSIDE:192.168.1.3 to OUTSIDE:209.165.200.242 flags I idle 0:00:02 timeout 3:00:00

NETSEC-ASA(config)#

NETSEC-ASA(config)# **show nat**

Auto NAT Policies (Section 2)

1 (INSIDE) to (OUTSIDE) source dynamic DYNAMIC-NAT PUBLIC

translate\_hits = 1, ntranslated\_hits = 1

NETSEC-ASA(config)#

NETSEC-ASA(config)# **show nat detail**

Auto NAT Policies (Section 2)

1 (INSIDE) to (OUTSIDE) source dynamic DYNAMIC-NAT PUBLIC

translate\_hits = 1, ntranslated\_hits = 1

Source - Origin: 192.168.1.0/27, Translated: 209.165.200.240-209.165.200.248

NETSEC-ASA(config)#

21.5.3

## Szintaxis-ellenőrző – Dinamikus NAT konfigurálása az ASA 5506-X rendszeren

A Syntax Checker segítségével konfigurálja a dinamikus NAT-ot egy ASA 5506-X-en.

Dynamic NAT configuration on a ASA requires the following:

* A network object defining the pool of public IP addresses.
* A network object defining the internal IP address to be translated.
* Binding the network objects together to begin the translation.

Create a network object **PUBLIC**, and then assign it the IP address pool from **209.165.200.240** to **209.165.200.248**. Exit network object configuration mode.

NETSEC-ASA(config)#object network PUBLIC

NETSEC-ASA(config-network-object)#range 209.165.200.240 209.165.200.248

NETSEC-ASA(config-network-object)#exit

* Create a network object **DYNAMIC-NAT**
* Assign it the subnet 192.168.1.0 255.255.255.224.
* Use the **nat** command to specify the **INSIDE** and **OUTSIDE** interface and bind the **PUBLIC** network object for dynamic IP addresses.
* Exit network object configuration mode.

NETSEC-ASA(config)#object network DYNAMIC-NAT

NETSEC-ASA(config-network-object)#subnet 192.168.1.0 255.255.255.224

NETSEC-ASA(config-network-object)#nat (INSIDE,OUTSIDE) dynamic PUBLIC

NETSEC-ASA(config-network-object)#exit

Complete the following to allow inside hosts to ping outside hosts:

* Enter policy map configuration mode for **global\_policy**.
* Enter class configuration mode for the **inspection\_default** class.
* In class configuration mode, configure an ACL named **ICMPACL**. The ACL should allow all ICMP traffic.
* Assign the ACL to match inbound traffic entering the **OUTSIDE** interface.

NETSEC-ASA(config)#policy-map global\_policy

NETSEC-ASA(config-pmap)#class inspection\_default

NETSEC-ASA(config-pmap-c)#access-list ICMPACL extended permit icmp any any

NETSEC-ASA(config)#access-group ICMPACL in interface OUTSIDE

Assume host 192.168.1.3 has sent traffic to the outside. Enter the **show xlate** command to verify the internal private IP address was translated to a public IP address.

NETSEC-ASA(config)#show xlate

1 in use, 1 most used

Flags: D - DNS, e - extended, I - identity, I - dynamic, r - portmap,

s - static, T - twice, N - net-to-net

NAT from INSIDE:192.168.1.3 to OUTSIDE:209.165.200.242 flags I idle 0:00:02 timeout 3:00:00

NETSEC-ASA(config)#

You have successfully configured dynamic NAT on an ASA 5506-X.

21.5.4

## Dinamikus PAT konfigurálása

Ennek a konfigurációnak egy változata a dinamikus PAT. Ekkor az ASA interfész IP-címe helyett egy tényleges külső IP-cím van konfigurálva és túlterhelve.

Csak egy hálózati objektum szükséges a külső interfész túlterheléséhez. Ha engedélyezni szeretné, hogy a belső gazdagépek túlterheljék a külső címet, használja **a nat** [ ( valós \_ if \_ name,mapped \_ if \_ name ) ] **dinamikus interfész** parancsot.

A példa egy dinamikus PAT konfigurációt jelenít meg ugyanazon referencia topológiához.

NETSEC-ASA(config)# **object network INSIDE-NET**

NETSEC-ASA(config-network-object)# **subnet 192.168.1.0 255.255.255.224**

NETSEC-ASA(config-network-object)# **nat (INSIDE,OUTSIDE) dynamic interface**

NETSEC-ASA(config-network-object)# **end**

NETSEC-ASA#

Miután a belső gazdagép pingelte a külső gazdagépet, ellenőrizze a hálózati cím fordítását a **show xlate** paranccsal. A példa az eredményül kapott fordítást jeleníti meg.

NETSEC-ASA# **show xlate**

1 in use, 1 most used

Flags: D - DNS, e - extended, I - identity, I - dynamic, r - portmap,

s - static, T - twice, N - net-to-net

ICMP PAT from INSIDE:192.168.1.3/1 to OUTSIDE:209.165.200.226/1 flags ri idle

0:00:02 timeout 0:00:30

NETSEC-ASA#

21.5.5

## Állítsa be a statikus NAT-ot

A statikus NAT akkor van beállítva, ha egy belső cím egy külső címre van leképezve. Például a statikus NAT akkor használható, ha a kiszolgálónak kívülről elérhetőnek kell lennie.

A statikus NAT beállításához használja a **nat** [ ( valódi \_ ha \_ név,leképezett \_ ha \_ név ) ] **static** mapped-inline-host-ip hálózati objektum parancsot.

Az ábra a DMZ interfész és a statikus NAT konfigurálásához használt NAT hivatkozási topológiát mutatja.

Az ábra a dmz asa hálózati topológián kívüli hivatkozást mutatja. Az asa konfiguráció következik.

.3 G1/3 G1/2 G1/1 192.168.1.0/27 209.165.200.224/27 209.165.201

192.168.2.3

DMZ kívül az Interneten

Az alábbi példa a statikus NAT engedélyezéséhez használt konfigurációt mutatja be. Ebben a példában a külső gazdagépek a 192.168.2.3 IP-címmel érhetik el a belső szervert a 209.165.200.227 külső IP-cím használatával.

A sikeres fordításhoz ACL-re van szükség.

NETSEC-ASA(config)# **object network DMZ-SERVER**

NETSEC-ASA(config-network-object)# **host 192.168.2.3**

NETSEC-ASA(config-network-object)# **nat (DMZ,OUTSIDE) static 209.165.200.227**

NETSEC-ASA(config-network-object)# **exit**

NETSEC-ASA(config)#

NETSEC-ASA(config)# **access-list OUTSIDE-DMZ extended permit ip any host 192.168.2.3**

NETSEC-ASA(config)# **access-group OUTSIDE-DMZ in interface OUTSIDE**

NETSEC-ASA(config)#

NETSEC-ASA(config)# **policy-map global\_policy**

NETSEC-ASA(config-pmap)# **class inspection\_default**

NETSEC-ASA(config-pmap-c)# **access-list ICMPACL extended permit icmp any any**

NETSEC-ASA(config)# **access-group ICMPACL in interface DMZ**

NETSEC-ASA(config)#

Használja a **show xlate** és **show nat detail** parancsokat a fordítások ellenőrzéséhez, ahogy a példában is látható. szükség lehet a **clear nat counters parancs használatára.** A NAT tesztelésekor

NETSEC-ASA(config)# **show xlate**

2 in use, 2 most used

Flags: D - DNS, e - extended, I - identity, I - dynamic, r - portmap,

s - static, T - twice, N - net-to-net

NAT from DMZ:192.168.2.3 to OUTSIDE:209.165.200.227

flags s idle 0:00:21 timeout 0:00:00

NAT from INSIDE:192.168.1.3 to OUTSIDE:209.165.200.242 flags I idle 0:09:06 timeout

3:00:00

NETSEC-ASA(config)#

NETSEC-ASA(config)# **show nat detail**

Auto NAT Policies (Section 2)

1 (DMZ) to (OUTSIDE) source static DMZ-SERVER 209.165.200.227

translate\_hits = 1, ntranslated\_hits = 1

Source - Origin: 192.168.2.3/32, Translated: 209.165.200.227/32

2 (INSIDE) to (OUTSIDE) source dynamic DYNAMIC-NAT PUBLIC

translate\_hits = 1, ntranslated\_hits = 1

Source - Origin: 192.168.1.0/27, Translated: 209.165.200.240-209.165.200.248

NETSEC-ASA(config)#

21.5.6

## Szintaxis-ellenőrző – Állítsa be a statikus NAT-ot egy ASA 5506-X-en

A szintaxis-ellenőrző segítségével állítsa be a statikus NAT-ot egy ASA 5506-X-en.

To configure static NAT, you create a network object for the host you want to map to a public IP address.

* Create a network object **DMZ-SERVER**.
* Assign 192.168.2.3 to the network object.
* Use the **nat** command to statically assign 209.165.200.227 for packets coming in the **DMZ** interface and exiting the **OUTSIDE** interface.
* Exit network object configuration mode.

NETSEC-ASA(config)#object network DMZ-SERVER

NETSEC-ASA(config-network-object)#host 192.168.2.3

NETSEC-ASA(config-network-object)#nat (DMZ,OUTSIDE) static 209.165.200.227

NETSEC-ASA(config-network-object)#exit

* Configure an ACL **OUTSIDE-DMZ** that will permit any traffic to destination 192.168.2.3.
* Apply the ACL for inbound traffic on the **OUTSIDE** interface.

NETSEC-ASA(config)# hozzáférési lista KÍVÜLI DMZ kiterjesztett engedély ip bármely gazdagépen 192.168.2.3

NETSEC-ASA(config)# hozzáférési csoport OUTSIDE-DMZ az OUTSIDE felületen

NETSEC-ASA(config)# policy-map global\_policy

NETSEC-ASA(config-pmap)# osztály ellenőrzési\_alapértelmezett

NETSEC-ASA(config-pmap-c)# hozzáférési lista ICMPACL kiterjesztett engedély icmp bármely tetszőleges

ACL **Az ICMPACL** már konfigurálva van. felületre érkező bejövő forgalomhoz **Rendelje hozzá az ACL-t a DMZ** .

NETSEC-ASA(config)# hozzáférési csoport ICMPACL a DMZ interfészben

Tegyük fel, hogy a 209.165.200.242-es külső gazdagép forgalmat küldött a 192.168.2.3-as DMZ-kiszolgálóra. A **show xlat** paranccsal ellenőrizze, hogy a belső privát IP-cím nyilvános IP-címre lett-e lefordítva. Figyeljük meg, hogy az **s** zászló azt jelzi, hogy a fordítás statikus volt.

NETSEC-ASA(config)# xlate megjelenítése

2 használatban van, 2 leggyakrabban használt

Jelzők: D - DNS, e - kiterjesztett, I - azonosság, I - dinamikus, r - porttérkép,

s - statikus, T - kétszer, N - net-net

NAT DMZ:192.168.2.3-tól OUTSIDE-ig:209.165.200.227

zászlók s tétlen 0:00:21 időtúllépés 0:00:00

NAT INSIDE:192.168.1.3-tól OUTSIDE:209.165.200.242-ig I tétlen 0:09:06 időtúllépés

3:00:00

NETSEC-ASA(config)#

Sikeresen konfigurálta a statikus NAT-ot egy ASA 5506-X-en.

[21.4](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[ASA ACLs](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[21.6](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[AAA](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                           
* 

1. ASA Firewall Configuration
2. AAA

# AAA

21.6.1

## AAA Review

A hitelesítés, engedélyezés és elszámolás (AAA) további szintű védelmet és felhasználói felügyeletet biztosít. Csak AAA használatával hitelesített és jogosult felhasználók csatlakozhatnak az ASA-n keresztül.

A hitelesítés használható önmagában vagy felhatalmazással és elszámolással. Az engedélyezéshez először mindig a felhasználó hitelesítése szükséges. A könyvelés önmagában, vagy hitelesítéssel és felhatalmazással is használható.

Az AAA fogalmilag hasonló a hitelkártya használatához, amint az az ábrán látható. A hitelesítés érvényes felhasználói hitelesítő adatok megkövetelésével szabályozza a hozzáférést, amelyek általában felhasználónév és jelszó. Az ASA képes hitelesíteni az összes adminisztrációs kapcsolatot az ASA-val, beleértve a Telnetet, az SSH-t, a konzolt, az ASDM-et a HTTPS használatával és a privilegizált EXEC-et.

Az engedélyezés felhasználónként szabályozza a hozzáférést a felhasználók hitelesítése után. Az engedélyezés szabályozza az egyes hitelesített felhasználók számára elérhető szolgáltatásokat és parancsokat. Engedélyezett engedélyezés nélkül a hitelesítés önmagában ugyanazt a hozzáférést biztosítaná a szolgáltatásokhoz minden hitelesített felhasználó számára. Az ASA engedélyezheti a felügyeleti parancsokat, a hálózati hozzáférést és a VPN hozzáférést.

A könyvelés nyomon követi az ASA-n áthaladó forgalmat, lehetővé téve az adminisztrátorok számára a felhasználói tevékenységek nyilvántartását. A könyvelési információk magukban foglalják a munkamenet kezdési és leállítási idejét, a felhasználóneveket, az ASA-n átmenő bájtok számát a munkamenethez, a használt szolgáltatást és az egyes munkamenetek időtartamát.

Az ábrán egy hitelkártya látható a hitelkártya-kivonat mellett. A hitelkártyán lévő számok körül egy téglalap található, amelyen a következő szöveg található: Hitelesítés Ki vagy? A második téglalap a hitelkeret körül van a hitelkártya-kivonaton, és a következő szöveggel: Engedélyezés Mennyit tud költeni? A harmadik téglalap a hitelkártya-összesítő tranzakciós része körül van, és a Számvitel szöveggel. Mit költött rá?



**Hitelesítés**   
  
Ki vagy te? **Engedélyezés**   
  
Mennyit tudsz költeni? **Könyvelés**   
  
mire költötted?

21.6.2

## Helyi adatbázis és szerverek

A Cisco ASA beállítható úgy, hogy a hitelesítéshez helyi felhasználói adatbázist vagy külső kiszolgálót használjon, vagy mindkettőt.

A helyi AAA helyi adatbázist használ a hitelesítéshez. Ez a módszer helyileg tárolja a felhasználóneveket és jelszavakat az ASA-n, és a felhasználók hitelesítik a helyi adatbázist. A helyi AAA ideális kis hálózatokhoz, amelyekhez nincs szükség dedikált AAA-kiszolgálóra.

**Megjegyzés** : Az ISR-rel ellentétben az ASA-eszközök nem támogatják a helyi hitelesítést AAA használata nélkül.

használja a **felhasználónév** jelszó **jelszó** parancsot [ **privilege** priv-level ] Helyi felhasználói fiókok létrehozásához . Ha törölni szeretne egy felhasználót a helyi adatbázisból, használja a **clear config username** [ name ] parancsot. Az összes felhasználói fiók megtekintéséhez használja a **show running-config username** parancsot.

A kiszolgáló alapú AAA hitelesítés sokkal skálázhatóbb módszer, mint a helyi AAA hitelesítés. A kiszolgáló alapú AAA hitelesítés külső adatbázis-kiszolgálót használ a RADIUS vagy TACACS+ protokollok kihasználásával. Ha több hálózati eszköz van, a szerver alapú AAA megfelelőbb.

A TACACS+ vagy RADIUS szerver konfigurálásához használja a táblázatban felsorolt ​​parancsokat.

| **ASA parancs** | **Leírás** |
| --- | --- |
| **aaa-szerver**  szerver-címke  **protokoll**  protokoll | Létrehoz egy TACACS+ vagy RADIUS AAA kiszolgálócsoportot. |
| **aaa-szerver**  szerver-címke [  **(**  if\_name  **)**  ]  **host**  { szerver-ip | név } [ kulcs ] | * Beállít egy AAA-kiszolgálót egy AAA-kiszolgálócsoport részeként. * Beállítja az AAA-kiszolgáló paramétereit is, amelyek gazdagép-specifikusak. |

Az összes AAA-kiszolgáló konfiguráció törléséhez használja a **clear config aaa-server** parancsot. Az összes felhasználói fiók megtekintéséhez használja a **show running-config aaa-server** parancsot.

A példa egy AAA TACACS+ szerver konfigurációját mutatja be egy ASA 5506-X-en.

NETSEC-ASA(config)# **username Admin password class privilege 15**

NETSEC-ASA(config)# **show run username**

username Admin password \*\*\*\*\* pbkdf2 privilege 15

NETSEC-ASA(config)# **aaa-server TACACS-SVR protocol tacacs+**

NETSEC-ASA(config-aaa-server-group)# **aaa-server TACACS-SVR (DMZ) host 192.168.2.3**

NETSEC-ASA(config-aaa-server-host)# **exit**

NETSEC-ASA(config)# **show run aaa-server**

aaa-server TACACS-SVR protocol tacacs+

aaa-server TACACS-SVR (DMZ) host 192.168.2.3

NETSEC-ASA(config)#

21.6.3

## AAA konfiguráció

Az ASA CLI-t konzolon ( **soros** paranccsal elérő felhasználók hitelesítéséhez **), SSH-n, HTTPS-en (ASDM) vagy Telnet-kapcsolaton keresztül elérő felhasználók hitelesítéséhez, illetve a privilegizált EXEC módhoz az enable** használja az **aaa hitelesítés engedélyezése konzol** parancsot a globális konfigurációban. mód. A parancs szintaxisa a következő:

ciscoasa(config)#  **aaa hitelesítés**  {  **serial**  |  **engedélyezése**  |  **telnet**  |  **ssh**  |  **http**  }  **konzol**  {  **HELYI**  | szervercsoport [  **HELYI**  ]}

Az összes AAA paraméter törléséhez használja a **clear config aaa** parancsot. Az összes felhasználói fiók megtekintéséhez használja a **show running-config username** parancsot.

A példa egy minta AAA-konfigurációt tartalmaz, amelyet ezután ellenőriznek és tesztelnek.

NETSEC-ASA(config)# **aaa authentication serial console TACACS-SVR LOCAL**

NETSEC-ASA(config)# **aaa authentication ssh console TACACS-SVR LOCAL**

NETSEC-ASA(config)# **aaa authentication http console TACACS-SVR LOCAL**

NETSEC-ASA(config)# **aaa authentication telnet console TACACS-SVR LOCAL**

NETSEC-ASA(config)# **aaa authentication enable console TACACS-SVR LOCAL**

NETSEC-ASA(config)#

NETSEC-ASA(config)# **show run aaa**

aaa authentication serial console TACACS-SVR LOCAL

aaa authentication ssh console TACACS-SVR LOCAL

aaa authentication http console TACACS-SVR LOCAL

aaa authentication telnet console TACACS-SVR LOCAL

aaa authentication enable console TACACS-SVR LOCAL

aaa authentication login-history

NETSEC-ASA(config)# **exit**

NETSEC-ASA# **exit**

Logoff

Username: **Admin**

Password: **\*\*\*\*\***

-----------------------------------------------

Authorized access only!

You have logged into a secure device.

-----------------------------------------------

User Admin logged in to NETSEC-ASA

Logins over the last 2 days: 4. Last login: 10:14:48 UTC Feb 11 2021 from console

Failed logins since the last login: 0.

Type help or '?' for a list of available commands.

NETSEC-ASA>

21.6.4

## Szintaxis-ellenőrző – Konfigurálja az AAA-t egy ASA 5506-X-en

A Syntax Checker segítségével konfigurálja és ellenőrizze az AAA szolgáltatásokat egy ASA 5506-X-en.

Configure privilege level 15 for the user **Admin** with the password **class**.

NETSEC-ASA(config)#username Admin password class privilege 15

NETSEC-ASA(config)# show run username

username Admin password \*\*\*\*\* pbkdf2 privilege 15

* Name the AAA server **TACACS-SVR** and configure it to use **tacacs+**.
* Associate the server to the DMZ interface and specify the IP address 192.168.2.3.
* Exit AAA server host configuration mode.

NETSEC-ASA(config)#aaa-server TACACS-SVR protocol tacacs+

NETSEC-ASA(config-aaa-server-group)#aaa-server TACACS-SVR (DMZ) host 192.168.2.3

NETSEC-ASA(config-aaa-server-host)#exit

NETSEC-ASA(config)# show run aaa-server

aaa-server TACACS-SVR protocol tacacs+

aaa-server TACACS-SVR (DMZ) host 192.168.2.3

NETSEC-ASA(config)#

Configure AAA to use the LOCAL TACACS-SVR to authenticate users over a console (serial) connection. SSH, HTTP, and Telnet will be configured for you. Then configure AAA to authenticate users that attempt to access privilege EXEC mode.

NETSEC-ASA(config)#aaa authentication serial console TACACS-SVR LOCAL

NETSEC-ASA(config)# aaa authentication ssh console TACACS-SVR LOCAL

NETSEC-ASA(config)# aaa authentication http console TACACS-SVR LOCAL

NETSEC-ASA(config)# aaa authentication telnet console TACACS-SVR LOCAL

NETSEC-ASA(config)#aaa authentication enable console TACACS-SVR LOCAL

Use the **show run aaa** command to verify the AAA configuration.

NETSEC-ASA(config)#show run aaa

aaa hitelesítési soros konzol TACACS-SVR LOCAL

aaa hitelesítés ssh konzol TACACS-SVR LOCAL

aaa hitelesítési http konzol TACACS-SVR LOCAL

aaa hitelesítési telnet konzol TACACS-SVR LOCAL

aaa hitelesítés engedélyezése konzol TACACS-SVR LOCAL

aaa hitelesítés bejelentkezési előzményei

NETSEC-ASA(config)#

írja be **kétszer az exit parancsot** A NETSEC-ASA-ból való kijelentkezéshez . Ezután jelentkezzen be újra a felhasználó **Admin** és jelszó **osztályával** .

**Megjegyzés** megjelenítése helyett : A Syntax Checker a jelszót fogja megjeleníteni a \* \* \* \* \* .

NETSEC-ASA(config)# kilépés

NETSEC-ASA# kilépés

Kijelentkezés

Felhasználónév: Admin

Jelszó: osztály

-----------------------------------------------

Csak engedélyezett hozzáférés!

Biztonságos eszközre jelentkezett be.

-----------------------------------------------

Felhasználói rendszergazda bejelentkezett a NETSEC-ASA-ba

Bejelentkezések az elmúlt 2 napban: 4. Utolsó bejelentkezés: 10:14:48 UTC 2021. február 11. a konzolról

Sikertelen bejelentkezések az utolsó bejelentkezés óta: 0.

Írja be a help vagy a "?" az elérhető parancsok listájához.

NETSEC-ASA>

Sikeresen konfigurálta a statikus NAT-ot egy ASA 5506-X-en.

[21.5](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[NAT Services on an ASA](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[21.7](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Service Policies on an ASA](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                               
* 

1. ASA Firewall Configuration
2. Service Policies on an ASA

# Szolgáltatási szabályzatok az ASA-n

21.7.1

## Az MPF áttekintése

A Modular Policy Framework (MPF) konfigurációja szabályokat határoz meg a tűzfalfunkciók, például a forgalomellenőrzés és a QoS alkalmazására az ASA-n áthaladó forgalomra. Az MPF lehetővé teszi a forgalmi áramlások részletes osztályozását, ami lehetővé teszi a különböző fejlett házirendek alkalmazását a különböző folyamokra. Az MPF a hardvermodulokkal együtt a forgalom aprólékos átirányítására szolgál az ASA-ból a Cisco MPF-et használó modulokhoz. Az MPF a forgalom fejlett alkalmazási rétegbeli vizsgálatára használható az 5–7. rétegek szerinti osztályozással. Sebességkorlátozás és QoS szolgáltatások MPF használatával is megvalósíthatók.

A Cisco MPF három konfigurációs objektumot használ a moduláris, objektumorientált, hierarchikus házirendek meghatározásához.

Kattintson az alábbiakra, ha többet szeretne megtudni az MPF-ben használt három konfigurációs objektumról.

Mit keresünk?

* A forgalom osztályozása.
* Azonosítsa a forgalmat, amelyen MPF-t kell végrehajtani.
* Hozzon létre 3. és 4. rétegbeli osztálytérképeket, amelyek több egyezési feltételt is tartalmazhatnak.

ciscoasa(config)# **class-map** class-name

Bár az MPF szintaxis hasonló az ISR IOS Cisco Modular QoS CLI (MQC) szintaxisához vagy a Cisco Common Classification Policy Language (C3PL) szintaxisához, a konfigurálható paraméterek eltérőek. Az ASA platform több konfigurálható műveletet biztosít, mint a Cisco IOS ZPF ISR-je. Az ASA támogatja a Layer 5-Layer 7 ellenőrzéseket az alkalmazás-specifikus paraméterek kritériumainak gazdagabb készletével. Az ASA MPF funkció például használható HTTP URL-ek és kérési módszerek egyeztetésére, megakadályozhatja, hogy a felhasználók meghatározott időpontokban bizonyos webhelyeken szörfözzenek, vagy akár zenét (MP3) és videofájlokat töltsenek le HTTP/FTP-n vagy HTTPS/SFTP-n keresztül. .

Négy lépésből áll az MPF konfigurálása ASA-n:

**1. lépés** (Opcionális) Konfigurálja a kiterjesztett ACL-eket, hogy azonosítsa a részletes forgalmat, amelyre kifejezetten hivatkozni lehet az osztálytérképen. Az ACL-ek például használhatók a TCP-forgalom, az UDP-forgalom, a HTTP-forgalom vagy az összes forgalom egy adott szerverhez való egyeztetésére.

**2. lépés:** Állítsa be az osztálytérképet a forgalom azonosítására.

**3. lépés:** Állítsa be a házirend-leképezést, hogy műveleteket alkalmazzon ezekre az osztályleképezésekre.

**4. lépés:** Konfiguráljon egy szolgáltatási szabályzatot a házirend-leképezés csatolásához egy interfészhez.

21.7.2

## Osztálytérképek konfigurálása

Az osztálytérképek úgy vannak beállítva, hogy azonosítsák a 3. és 4. rétegbeli forgalmat (más néven 3/4. réteg). Osztálytérkép létrehozásához és az osztálytérkép konfigurációs módba lépéséhez használja az **osztálytérkép** osztálytérkép-név globális konfigurációs mód parancsát. Az „class-default” nevek és minden olyan név, amely „ \_ belső” vagy „ \_ default” karakterrel kezdődik, le van foglalva. Az osztálytérkép nevének egyedinek kell lennie, és legfeljebb 40 karakter hosszúságú lehet. A névnek is leíró jellegűnek kell lennie.

**Megjegyzés** parancs egy változata **: Az osztályleképezés** az ASA-hoz rendelt forgalom kezeléséhez használatos. Ebben az esetben használja a **class-map type management** class-map-name parancsot.

Osztálytérkép konfigurációs módban az osztályleképezés célját magyarázó leírást a **leírás** paranccsal kell konfigurálni.

Ezután az egyező forgalmat a **Match any** (összes forgalommal megegyezik) vagy az **access-list** access-list-name parancsokkal kell azonosítani, hogy megfeleljen a kiterjesztett hozzáférési lista által meghatározott forgalomnak.

**Megjegyzés** : Ha nincs másképp megadva, csak egy **match** parancsot tartalmazzon az osztálytérképben.

A példa egy minta osztálytérkép-konfigurációt ad.

NETSEC-ASA(config)# **access-list UDP permit udp any any**

NETSEC-ASA(config)# **access-list TCP permit tcp any any**

NETSEC-ASA(config)# **access-list SERVER permit ip any host 10.1.1.1**

NETSEC-ASA(config)#

NETSEC-ASA(config)# **class-map ALL-TCP**

NETSEC-ASA(config-cmap)# **description This class-map matches all TCP traffic**

NETSEC-ASA(config-cmap)# **match access-list TCP**

NETSEC-ASA(config-cmap)# **exit**

NETSEC-ASA(config)#

NETSEC-ASA(config)# **class-map ALL-UDP**

NETSEC-ASA(config-cmap)# **description This class-map matches all UDP traffic**

NETSEC-ASA(config-cmap)# **match access-list UDP**

NETSEC-ASA(config-cmap)# **exit**

NETSEC-ASA(config)#

NETSEC-ASA(config)# **class-map ALL-HTTP**

NETSEC-ASA(config-cmap)# **description This class-map matches all HTTP traffic**

NETSEC-ASA(config-cmap)# **match port TCP eq http**

NETSEC-ASA(config-cmap)# **exit**

NETSEC-ASA(config)#

NETSEC-ASA(config)# **class-map TO-SERVER**

NETSEC-ASA(config-cmap)# **description Class map matches traffic 10.1.1.1**

NETSEC-ASA(config-cmap)# **match access-list SERVER**

NETSEC-ASA(config-cmap)# **exit**

NETSEC-ASA(config)#

Az ASA automatikusan meghatároz egy alapértelmezett 3/4-es rétegbeli osztályleképezést is, amelyet a konfigurációban **az osztálytérkép-ellenőrzés \_ default** azonosít . Ezen az osztálytérképen az **alapértelmezett-ellenőrzési forgalom egyezése** található , amely megegyezik az összes ellenőrzés alapértelmezett portjával. Ha házirend-leképezésben használjuk, ez az osztályleképezés biztosítja, hogy minden egyes csomagra a megfelelő ellenőrzés kerüljön alkalmazásra, a forgalom célportja alapján. Például amikor a 69-es port UDP-forgalma eléri az ASA-t, az ASA alkalmazza a TFTP-ellenőrzést. Csak ebben az esetben több ellenőrzés konfigurálható ugyanahhoz az osztálytérképhez. Általában az ASA nem a portszámot használja annak meghatározásához, hogy melyik ellenőrzést kell alkalmazni. Ez rugalmasságot biztosít a nem szabványos kikötők ellenőrzéséhez.

Az osztálytérkép konfigurációjával kapcsolatos információk megjelenítéséhez használja a **show running-config class-map** parancsot.

Az összes osztályleképezés eltávolításához használja a **clear configure class-map** parancsot globális konfigurációs módban.

21.7.3

## Szabályzat meghatározása és aktiválása

A házirend-térképek az osztálytérképek műveletekkel való összekapcsolására szolgálnak. Használja a **policy-map** policy-map-name globális konfigurációs mód parancsot, hogy műveleteket alkalmazzon a 3. és 4. rétegbeli forgalomra. Az irányelvtérkép nevének egyedinek kell lennie, és legfeljebb 40 karakter hosszúságúnak kell lennie. A névnek is leíró jellegűnek kell lennie.

A config-pmap házirend-leképezés konfigurációs módban használja a következő parancsokat:

* **leírás** - Leíró szöveg hozzáadása.
* **osztály** osztálytérkép-név – Határozzon meg egy adott osztálytérképet, amelyen műveleteket hajthat végre.

A szabályzatleképezések maximális száma 64. Egy szabályzattérképen több ¾ rétegű osztályleképezés is szerepelhet, és egy vagy több jellemzőtípusból több művelet is hozzárendelhető minden osztálytérképhez.

**Megjegyzés** : A konfiguráció tartalmaz egy alapértelmezett Layer ¾ házirend-leképezést, amelyet az ASA használ az alapértelmezett globális házirendben. hívják **Globális \_ házirendnek** , és az alapértelmezett ellenőrzési forgalmat ellenőrzi. Csak egy globális politika létezhet. Ezért a globális szabályzat módosításához vagy szerkessze, vagy cserélje ki.

Ez a három leggyakoribb parancs, amely házirend-térkép konfigurációs módban érhető el:

* **kapcsolat beállítása** – Beállítja a kapcsolati értékeket.
* **inspect** – Protokoll-ellenőrző szervereket biztosít.
* **rendőrség** – Meghatározza a forgalom mértékét ebben az osztályban.

A műveletek a szolgáltatástól függően kétirányú vagy egyirányú forgalomra vonatkoznak.

A szabályzatleképezés konfigurációjával kapcsolatos információk megjelenítéséhez használja a **show running-config policy-map** parancsot.

Az összes házirend-leképezés eltávolításához használja a **clear configure policy-map** parancsot globális konfigurációs módban.

**Konfigurálja a szolgáltatási házirendet**

Ha globálisan szeretné aktiválni a házirend-leképezést az összes felületen vagy egy célzott felületen, használja a **service-policy** policy-map-name [ **global** | **interface** intf ] globális konfigurációs mód parancs, amely lehetővé teszi házirendek készletét az interfészen.

A példa a házirend-leképezést konfigurálja. A kapcsolódó szolgáltatási szabályzatot globálisan alkalmazzák.

NETSEC-ASA(config)# **access-list TFTP-TRAFFIC permit udp any any eq 69**

NETSEC-ASA(config)#

NETSEC-ASA(config)# **class-map CLASS-TFTP**

NETSEC-ASA(config-cmap)# **match access-list TFTP-TRAFFIC**

NETSEC-ASA(config-cmap)# **exit**

NETSEC-ASA(config)#

NETSEC-ASA(config)# **policy-map POLICY-TFTP**

NETSEC-ASA(config-pmap)# **class CLASS-TFTP**

NETSEC-ASA(config-pmap-c)# **inspect tftp**

NETSEC-ASA(config-pmap-c)# **exit**

NETSEC-ASA(config-pmap)# **exit**

NETSEC-ASA(config)#

NETSEC-ASA(config)# **service-policy POLICY-TFTP global**

NETSEC-ASA(config)#

21.7.4

## Szintaxis-ellenőrző – Házirend meghatározása és aktiválása az ASA 5506-X-en

A Syntax Checker segítségével határozzon meg és aktiváljon házirendet az ASA 5506-X-en.

Configure an ACL named **TFTP-TRAFFIC** to allow all inbound and outbound TFTP traffic. Use the port number instead of the keyword.

NETSEC-ASA(config)#access-list TFTP-TRAFFIC permit udp any any eq 69

Configure a class named **CLASS-TFTP** to match the **TFTP-TRAFFIC** ACL. Then exit class map configuration mode.

NETSEC-ASA(config)# class-map CLASS-TFTP

A NETSEC-ASA(config-cmap)# megfelel a hozzáférési lista TFTP-TRAFFIC

NETSEC-ASA(config-cmap)# kilépés

TP nevű házirendet **Állítsa be a POLICY-TF** használatához **a CLASS-TFTP** a TFTP-forgalom ellenőrzéséhez. A globális konfigurációs módba való visszatéréshez kétszer nyomja meg az Enter exit gombot.

NETSEC-ASA(config)# policy-map POLICY-TFTP

NETSEC-ASA(config-pmap)# osztály CLASS-TFTP

NETSEC-ASA(config-pmap-c)# vizsgálja meg a tftp-t

NETSEC-ASA(config-pmap-c)# kilépés

NETSEC-ASA(config-pmap)# kilépés

használja **Állítsa be a szolgáltatási házirendet úgy, hogy a POLICY-TFTP-t** az összes forgalomhoz (globális).

NETSEC-ASA(config)# service-policy POLICY-TFTP globális

Sikeresen definiált és aktivált egy házirendet egy ASA 5506-X-en.

21.7.5

## Packet Tracer – Az ASA alapbeállításai és a tűzfal konfigurálása a CLI segítségével

Ebben az átfogó Packet Tracer tevékenységben a következő célokat éri el:

* Ellenőrizze a kapcsolatot, és fedezze fel az ASA-t.
* Konfigurálja az alapvető ASA-beállításokat és az interfész biztonsági szintjeit a CLI segítségével.
* Konfigurálja az útválasztást, a címfordítást és az ellenőrzési szabályzatot a CLI segítségével.
* Konfigurálja a DHCP-t, az AAA-t és az SSH-t.
* Konfiguráljon DMZ-t, statikus NAT-ot és ACL-eket.

[Konfigurálja az ASA alapbeállításait és a tűzfalat a parancssori felület segítségével](https://contenthub.netacad.com/courses/netsec/_common/21.7.5-packet-tracer---configure-asa-basic-settings-and-firewall-using-the-cli.pka)

21.7.6

## Opcionális labor – ASA hálózati szolgáltatások, útválasztás és DMZ konfigurálása ACL-ekkel a CLI használatával

Ebben az átfogó laborban a következő célokat fog teljesíteni:

* 1. rész: Alapvető eszközbeállítások konfigurálása
* 2. rész: Útválasztás, címfordítás és ellenőrzési házirend konfigurálása a CLI használatával
* 3. rész: DHCP, AAA és SSH konfigurálása
* 4. rész: DMZ, statikus NAT és ACL-ek konfigurálása

[21.6](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[AAA](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[21.8](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[ASA Firewall Configuration Summary](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                               
* 

1. ASA Firewall Configuration
2. ASA Firewall Configuration Summary

# ASA tűzfal konfigurációs összefoglaló

21.8.1

## Mit tanultam ebben a modulban?

**Alapvető ASA tűzfal konfiguráció**   
Az ASA parancssori interfész (CLI) egy szabadalmaztatott operációs rendszer, amely a router IOS-éhez hasonló megjelenést és érzetet mutat. Például az ASA parancssori felület a Cisco IOS útválasztókhoz hasonló parancssorokat tartalmaz. Az IOS CLI-hez hasonlóan az ASA CLI is támogatja a parancsok és kulcsszavak rövidítését, a Tab billentyű használatát a részleges parancsok végrehajtásához, valamint a parancs után a súgó ( **?** ) használatát a további szintaxis megtekintéséhez. Sok parancs hasonló az IOS más verzióiban lévő parancsokhoz, de sok különbség is létezik.

Az ASA 5506-X FirePOWER Services szolgáltatással olyan alapértelmezett konfigurációval érkezik, amely a legtöbb esetben elegendő egy alapszintű SOHO-telepítéshez. A konfigurációs módosításokat manuálisan is elvégezheti a CLI használatával, interaktívan a CLI beállítási inicializálási varázslójával és az Adaptive Security Device Manager (ASDM) telepítővarázslójával.

Az ASA visszaállítható a gyári alapértelmezett konfigurációjára a **configure gyári alapértelmezett** globális konfigurációs mód paranccsal.

**Konfigurálja a felügyeleti szolgáltatásokat és beállításokat**   
Az ASA 5506-X úgy konfigurálható, hogy privilegizált EXEC módba lép az enable paranccsal, majd a konfigurálási terminál használatával lépjen be a globális konfigurációs módba. Amikor először lép be a globális konfigurációs módba, felkínálja a lehetőséget, hogy részt vegyen a Cisco Smart Call Home programban. Ha a jóváhagyott és egyéb feltételek teljesülnek, az ASA kommunikál a Ciscóval, hogy proaktív diagnosztikát és valós idejű riasztásokat küldjön és fogadjon.

A privilegizált EXEC jelszó automatikusan titkosításra kerül az MD5 használatával. Az AES-t használó erősebb titkosítást azonban engedélyezni kell. Ehhez be kell állítani egy elsődleges jelszót, és engedélyezni kell az AES titkosítást. Az elsődleges jelszó módosításához használja a **key config-key password-encryption** parancsot.

Az ASA 5506-X nyolc Gigabit Ethernet interfésszel rendelkezik, amelyek konfigurálhatók a forgalom továbbítására különböző Layer 3 hálózatokon. A G1/1 interfész gyakran az ISP külső interfészeként van konfigurálva. Az interfészek alapkonfigurációja magában foglalja az IP-címzést, az elnevezést és a biztonsági szint beállítását. Az interfészek csoportosíthatók áthidalt virtuális interfészekként (BVI). A BVI konfigurálható egyetlen névvel és IP-címmel, bár előfordulhat, hogy más beállításokat is konfigurálni kell az egyes összetevő-interfészeken. Az interfészek címekkel manuálisan, DHCP-vel vagy PPPoE-n keresztül konfigurálhatók. Ha az interfész DHCP-vel van konfigurálva, az ASA-n automatikusan beállítható egy alapértelmezett útvonal egy upstream eszközről. Ellenkező esetben az alapértelmezett útvonalat kézzel kell konfigurálni.

A távoli felügyelethez az ASA beállítható úgy, hogy fogadjon Telneten vagy SSH-n keresztüli kapcsolatokat. Az SSH erősen preferált. Az engedélyezés a helyi felhasználói adatbázisból történhet.

Más hálózati szolgáltatások, például az NTP és a DHCP konfigurálhatók az ASA-n. Az ASA beállítható úgy, hogy fogadja az NTP-információkat a hitelesített kiszolgálóktól. A DHCP-szolgáltatásokat úgy is be lehet állítani, hogy címeket adjanak a belső gazdagépeknek.

**Tárgycsoportok**   
Az objektumok újrafelhasználható összetevők, amelyek konfigurációkban használhatók. Az objektumok definiálhatók és használhatók a Cisco ASA konfigurációkban a soron belüli IP-címek, szolgáltatások, nevek stb. helyén. Az objektumok megkönnyítik a konfigurációk karbantartását, mivel egy objektum egy helyen módosítható, és a változás minden más helyen megjelenik, amely hivatkozik rá. Például létrehozható egy hálózati objektum egy syslog szerver IP-címének tárolására. Ha a kiszolgáló címe megváltozik, az objektum módosítható, és ez a változás minden olyan konfigurációs parancsban megjelenik, amely az objektumra hivatkozik. Kétféle objektum létezik, hálózati objektumok és szolgáltatásobjektumok. A hálózati objektumok tartalmazhatnak gazdagépcímeket, alhálózatokat, címtartományokat és FQDN-eket. A szolgáltatásobjektumok különböző hálózati szolgáltatásokra és protokollokra hivatkozhatnak. Az objektumcsoportok egymáshoz kapcsolódó objektumok gyűjteményei. A hálózati objektumcsoportok olyan konfigurációkban is használhatók, mint az ACL és a NAT. Ötféle objektumcsoport létezik. Ahol az objektumok csak egy értéket tartalmazhatnak, az objektumcsoportok több értéket is tartalmazhatnak, beleértve a soron belüli értékeket, valamint a korábban létrehozott objektumokat.

**ASA ACL-ek**   
A Cisco ASA 5506-X alapvető forgalomszűrési képességeket biztosít az ACL-ekkel. Az ACL-ek szabályozzák a hozzáférést a hálózaton azáltal, hogy megakadályozzák a meghatározott forgalom belépését vagy kilépését. Ezen túlmenően, az ACL használható annak a forgalomnak a kiválasztására, amelyre egy szolgáltatás vonatkozni fog, ezáltal egy megfelelő szolgáltatást hajthat végre, nem pedig vezérlőszolgáltatást. Az ASA ACL-ek abban különböznek az IOS ACL-ektől, hogy helyettesítő karaktermaszk (pl. 0.0.0.255) helyett hálózati maszkot (pl. 255.255.255.0) használnak. Ötféle ASA ACL létezik, beleértve az ismert szabványos és kiterjesztett típusokat. Minden ASA ACL el van nevezve. Az ASA szabvány és a kiterjesztett ACL szintaxis hasonló az ISR-eknél használthoz. Az ASA ACL-eket interfésszel kell csoportosítani ahhoz, hogy életbe léphessenek. Az objektumcsoportok az ASA ACL-ekkel együtt használhatók a listában szükséges ACE-k számának korlátozására.

**NAT szolgáltatások ASA-n**   
A NAT az ASA-kon konfigurálható, ahogy az útválasztók esetében is történik. Az ASA-k esetében három telepítési módszer létezik. Az első a belső NAT, amelyet a biztonságos hálózatokon belüli címek kevésbé biztonságos hálózatokon lévő külső címekre történő fordítására használnak. A NAT-on kívül az alacsonyabb biztonságú hálózatról érkező forgalom magasabb biztonságú hálózatra fordítódik. Ez arra szolgál, hogy a belső vállalati gazdagépeket elérhetővé tegye a külső felhasználók számára. A kétirányú NAT együtt használja mind a belső, mind a külső NAT-ot. Az ASA négyféle NAT-ot támogat, a dinamikus NAT-ot túlterheléssel, a statikus NAT-ot, a házirend-NAT-ot és az identitás-NAT-ot. A NAT konfigurálásához hálózati objektumokat kell használni. A fordítás során használandó IP-címek és a lefordítható belső IP-címek készleteinek ábrázolására szolgálnak.

**AAA**   
A Cisco ASA-k beállíthatók úgy, hogy hitelesítsék a hozzáférést egy helyi felhasználói adatbázis vagy egy külső kiszolgáló segítségével a hitelesítéshez, vagy mindkettőhöz. Az ISR-rel ellentétben az ASA-eszközök nem támogatják a helyi hitelesítést AAA használata nélkül. A kiszolgáló alapú AAA hitelesítés külső adatbázis-kiszolgálót használ a RADIUS vagy TACACS+ protokollok kihasználásával.

Az ASA CLI-t konzolon, SSH-n, HTTPS-en (ASDM) vagy Telnet-kapcsolaton keresztül elérő felhasználók hitelesítéséhez, illetve a privilegizált EXEC módhoz az **enable** paranccsal elérő felhasználók hitelesítéséhez használja az **aaa hitelesítés engedélyezése konzol** parancsot globális konfigurációs módban.

**Szolgáltatási szabályzatok az ASA-n**   
A Modular Policy Framework (MPF) konfigurációja szabályokat határoz meg a tűzfalfunkciók, például a forgalomellenőrzés és a QoS alkalmazására az ASA-n áthaladó forgalomra. Az MPF lehetővé teszi a forgalmi áramlások részletes osztályozását, hogy különböző speciális irányelveket alkalmazhasson a különböző folyamokra. A Cisco MPF három konfigurációs objektumot használ a moduláris, objektumorientált, hierarchikus házirendek meghatározásához. Az osztálytérképek az MPF által feldolgozott forgalom azonosítására szolgálnak. A házirend-térképek határozzák meg, hogy mi történik az azonosított forgalommal. A szolgáltatási szabályzatok meghatározzák, hogy mely felületekre kell alkalmazni a házirend-térképet.

Az ASA támogatja a Layer 5-Layer 7 ellenőrzéseket az alkalmazás-specifikus paraméterek kritériumainak gazdagabb készletével. Az ASA MPF funkció például használható HTTP URL-ek és kérési módszerek egyeztetésére, megakadályozhatja, hogy a felhasználók meghatározott időpontokban bizonyos webhelyeken szörfözzenek, vagy akár zenét (MP3) és videofájlokat töltsenek le HTTP/FTP-n vagy HTTPS/SFTP-n keresztül. .

21.8.2

## 21. modul – ASA tűzfal konfigurációs kvíz

Az űrlap teteje

1. Melyik két állítás igaz az ASA szabványos ACL-ekre? (Válassz kettőt.)

Az űrlap alja

Ha egy ASA-n dinamikus NAT-ot állítanak be, milyen két paramétert kell megadniuk a hálózati objektumoknak? (Válassz kettőt.)

Melyik parancsot használják az ASA-n a jelszavas titkosítás engedélyezéséhez és az összes felhasználói jelszó titkosításához?

Milyen típusú NAT használható olyan ASA-n, ahol a 10.0.1.0/24 belső címeket csak akkor kell lefordítani, ha az ezekről a címekről érkező forgalom a 198.133.219.0/24 hálózatra irányul?

A hálózati rendszergazda objektumcsoportokat telepített az ACL-ek könnyebb megvalósítása és megértése érdekében. Melyik két objektum lenne egy szolgáltatásobjektum-csoport része? (Válassz kettőt.)

Mi a különbség az ASA IPv4 ACL és az IOS IPv4 ACL között?

Which object or object group is required to implement NAT on an ASA 5506-X device?

Which statement describes a feature of AAA in an ASA device?

What type of ACL is designed for use in the configuration of an ASA to support filtering for clientless SSL VPNs?

Egy hálózati technikus megpróbálja megoldani az ASA NAT-konfigurációjával kapcsolatos problémákat. A technikus pinget generál egy belső gazdagépről egy külső gazdagépre. Melyik parancs ellenőrzi, hogy a címeket lefordítják-e az ASA?

Melyik két típusú objektum konfigurálható egy ASA-eszközön? (Válassz kettőt.)

Melyik opció sorolja fel a négy lépést a moduláris házirend-keretrendszer ASA-n történő konfigurálásához?

Melyik állítás igaz az ASA CLI és az IOS CLI parancsaira?

[21.7](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Service Policies on an ASA](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[21.9](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Introduction to ASDM (Optional)](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                   

1. ASA Firewall Configuration
2. Introduction to ASDM (Optional)

# Az ASDM bemutatása (opcionális)

21.9.1

## Az ASDM áttekintése

A Cisco ASA konfigurálható és felügyelhető a parancssori felület (CLI) vagy a grafikus felhasználói felület (GUI) Adaptive Security Device Manager (ASDM) használatával. A CLI gyors, de több időt igényel a tanulás. Az ASDM intuitív és leegyszerűsíti az ASA konfigurációját.

A Cisco ASDM egy Java-alapú grafikus felhasználói felület, amely megkönnyíti a Cisco ASA-k beállítását, konfigurálását, figyelését és hibaelhárítását. Az alkalmazás elrejti a parancsok összetettségét az adminisztrátorok elől, és egyszerűsített konfigurációkat tesz lehetővé anélkül, hogy az ASA CLI széleskörű ismeretére lenne szükség. SSL-lel működik, hogy biztonságos kommunikációt biztosítson az ASA-val. Gyors konfigurációs varázslókat, valamint naplózási és megfigyelési funkciókat is biztosít, amelyek nem érhetők el a CLI használatával.

Az ASA 5506-X-hez mellékelt Cisco ASA FirePOWER modul fejlett funkcióinak eléréséhez a Firepower Management Center (FMC) használata javasolt.

**Megjegyzés** : A Cisco Adaptive Security Manager (ASDM) használatához Java telepítése szükséges az ASA ASDM konfigurációjához használt gazdagépen. Az Oracle Java License változásai miatt többé nem szükséges Java futtatókörnyezet (JRE) letöltése és telepítése az ASDM laborok futtatásához.

21.9.2

## Készüljön fel az ASDM-re

Az ASDM-hez való hozzáférés engedélyezéséhez az ASA-nak minimális konfigurációra van szüksége. Pontosabban, az ASDM az ASA webszerverhez vezető Secure Socket Layer (SSL) webböngészőkapcsolaton keresztül érhető el. Az SSL titkosítja az ügyfél és az ASA webszerver közötti forgalmat.

Az ASA-nak legalább egy felügyeleti interfész konfigurálása szükséges az ASDM futtatásához. A felügyeleti felület az ASA modelljétől függ. Az ASA 5506-X-en a felügyeleti interfész bármilyen belső interfész lehet (G1/2 - G1/8).

Pontosabban, az ASDM-hozzáférés előkészítéséhez egy ASA 5506-X-en a következőket kell konfigurálni, ahogy a példában is látható:

* **Fizikai porton belül kiválasztva** – végezze el a porton az alapkonfigurációt, beleértve a felügyeleti IP-címet és a biztonsági szintet
* **Az ASA webszerver engedélyezése** – Engedélyezze az ASA HTTP szervert.
* **Hozzáférés engedélyezése az ASA webszerverhez** – Alapértelmezés szerint az ASA zárt házirendben működik; ezért minden kapcsolat a HTTP szerverrel meg van tiltva. Be kell állítani egy hálózati utasítást, amely meghatározza, hogy mely gazdagépek hozzáférhetnek a HTTP-kiszolgálóhoz.

A példa a kiválasztott belső interfész (G1/2) felügyeletet 192.168.1.1 IP-címmel konfigurálja. Engedélyezi az interfészt, engedélyezi az ASA HTTP szervert, és lehetővé teszi a hozzáférést a 192.168.1.0/24 hálózat bármely belső gazdagépéről.

Az ASA konfigurálása után ellenőrizze a csatlakozást úgy, hogy pingelje le az engedélyezett gazdagéptől.

ciscoasa# **conf t**

ciscoasa(config)# **interface g1/2**

ciscoasa(config-if)# **ip address 192.168.1.1 255.255.255.0**

ciscoasa(config-if)# **nameif INSIDE**

INFO: Security level for "INSIDE" set to 100 by default.

ciscoasa(config-if)# **no shutdown**

ciscoasa(config)# **exit**

ciscoasa(config)#

ciscoasa(config)# **http server enable**

ciscoasa(config)# **http 192.168.1.0 255.255.255.0 inside**

ciscoasa(config)#

21.9.3

## Szintaxis-ellenőrző – Konfiguráljon egy ASA 5506-X-et az ASDM-hozzáféréshez

A Syntax Checker segítségével konfiguráljon egy ASA 5506-X-et az ASDM-hozzáféréshez.

Konfigurálja az INSIDE interfészt.

* interfész konfigurációs módjába **Lépjen be a g1/2** .
* Nevezze el az interfészt **INSIDE** .
* Konfigurálja a 192.168.1.1 255.255.255.0 IP-címet.
* Aktiválja a felületet.
* Lépjen ki az interfész konfigurációs módból.

ciscoasa(config)# interfész g1/2

ciscoasa(config-if)# IP-cím 192.168.1.1 255.255.255.0

ciscoasa(config-if)# nameif INSIDE

INFO: Az "INSIDE" biztonsági szintje alapértelmezés szerint 100.

ciscoasa(config-if)# nincs leállítás

ciscoasa(config-if)# kilépés

* Engedélyezze az ASA-t HTTP-kiszolgálóként.
* Konfigurálja a 192.168.1.0/24 hálózat bármely gazdagépét a HTTP-kiszolgáló eléréséhez az **INSIDE** interfészen.

ciscoasa(config)# http szerver engedélyezése

ciscoasa(config)# http 192.168.1.0 255.255.255.0 BELSŐ

Sikeresen konfigurált egy ASA 5506-X-et az ASDM-hozzáféréshez.

21.9.4

## Indítsa el az ASDM-et

Az ASDM elindításához adja meg az ASA felügyeleti IP-címét egy webböngészőben egy engedélyezett gazdagépről. Az engedélyezett gazdagépnek egy böngészőn keresztül kapcsolatot kell létesítenie a belső interfész IP-címével a HTTPS protokoll használatával.

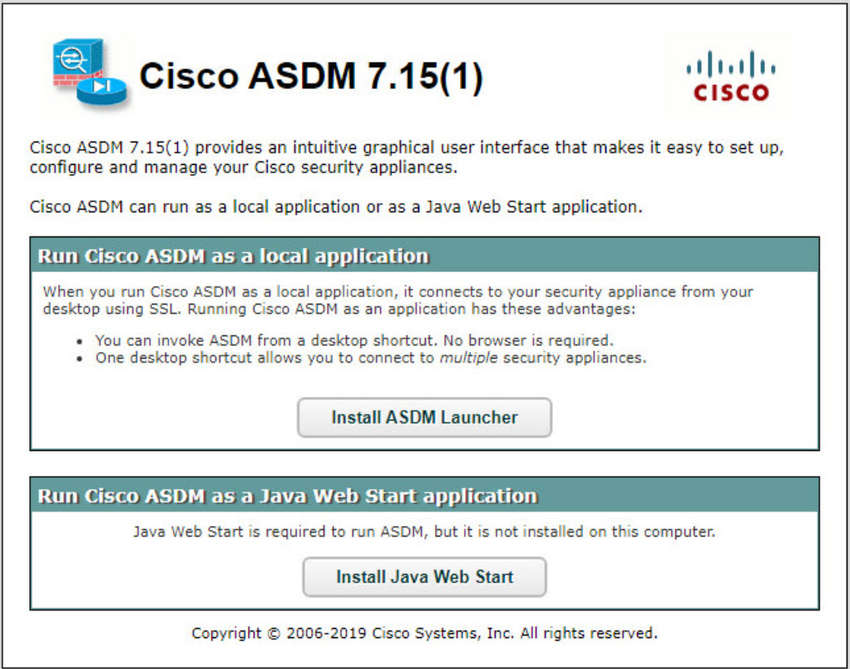
Kattintson a gombra a kezdeti biztonsági tanúsítvány figyelmeztetésének figyelmen kívül hagyásához és az ASDM ablak elindításához.

Megjelenik a kezdeti ASDM ablak, az ábrán látható módon. Két lehetőséget kínál a számítógép felkészítésére az ASDM GUI elérésére:

* **Futtassa a Cisco ASDM-et helyi alkalmazásként** – Ez biztosítja az **ASDM-indító telepítése** opciót, amellyel a gazdagép asztaláról SSL használatával csatlakozhat az ASA-hoz. Ennek az az előnye, hogy egy alkalmazással több ASA-eszköz is kezelhető, és nincs szükség webböngészőre az ASDM elindításához.
* **Futtassa a Cisco ASDM-et Java Web Start alkalmazásként** – Ez biztosítja a **Java Web Start telepítése** opciót, amely lehetővé teszi a böngésző számára az ASDM elindítását. A kapcsolat létrehozásához webböngésző szükséges. Az ASDM nincs telepítve a helyi gazdagépen.

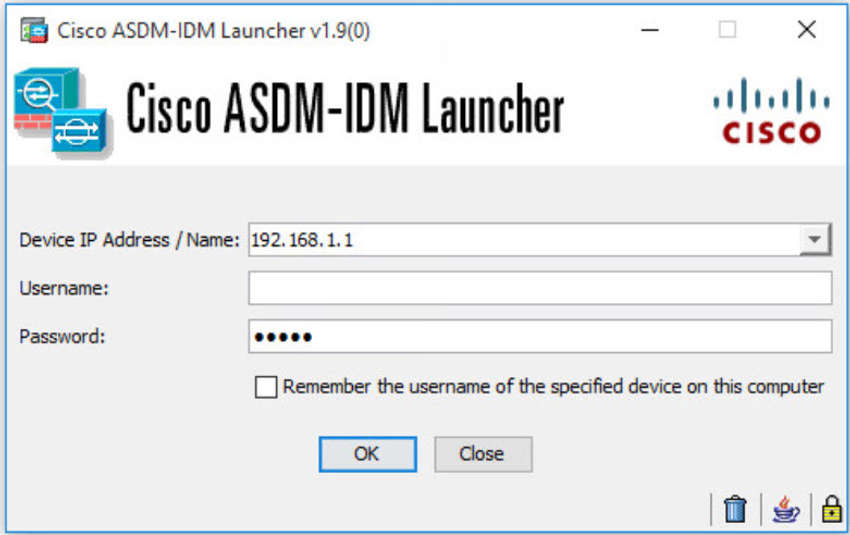
Egy opció kiválasztása után megkezdődik a telepítési folyamat. **Megjegyzés:** A számítógépen a Java futtatókörnyezet egy verziója szükséges ahhoz, hogy bármelyik beállítás működjön.

### ASDM kezdeti indítási ablak



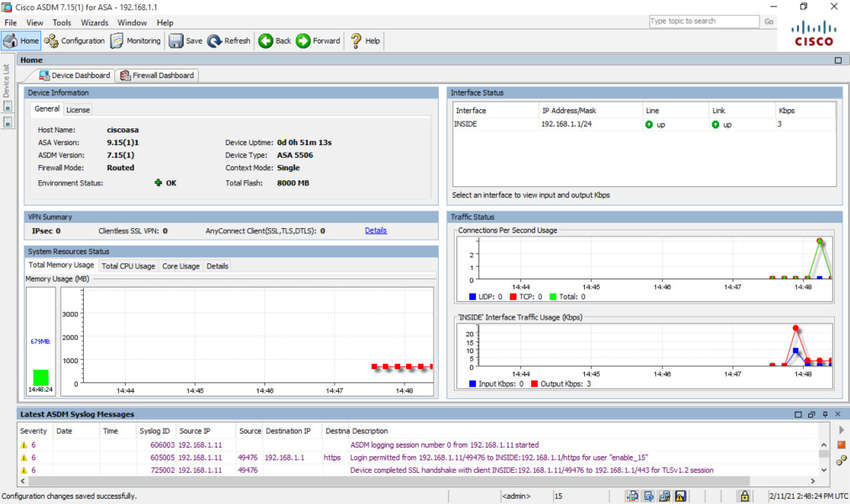
Ebben a példában **az ASDM Launcher telepítése** van kiválasztva. Az alkalmazástelepítő letölti a számítógépére. Futtassa a telepítőt, és kövesse az utasításokat a szoftver telepítéséhez. Amikor a telepítés befejeződött, megjelenik a Cisco ASDM-IDM Launcher ablak, ahogy az ábrán látható. Adja meg az engedélyezési jelszót, majd kattintson az OK gombra.

### Hitelesítés az ASDM használatához



Végül megjelenik az ASDM kezdőlapja, az ábrán látható módon.

### ASDM honlap



21.9.5

## Lab – Az ASA alapbeállításai és a tűzfal konfigurálása ASDM használatával

Ebben a laborban a következő célokat kell teljesítenie:

[21.8](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[ASA Firewall Configuration Summary](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[22.0](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                          

1. Network Security Testing
2. Introduction

# Bevezetés

22.0.1

## Miért vegyem ezt a modult?

A hálózatok támadás alatt állnak. Hogyan tesztelheti a hálózatát? Milyen eszközök állnak rendelkezésre a teszteléshez? Olvassa tovább, ha többet szeretne megtudni a tesztelési technikák típusairól és a rendelkezésre álló eszközökről.

22.0.2

## Mit fogok tanulni ebben a modulban?

**Modul címe:** Hálózatbiztonsági tesztelés

**A modul célja** : Ismertesse a hálózatbiztonsági teszteléshez használt különféle technikákat és eszközöket.

| **téma címe** | **Téma Cél** |
| --- | --- |
| **Hálózatbiztonsági tesztelési technikák** | Ismertesse a hálózatbiztonsági tesztelés során használt technikákat. |
| **Hálózatbiztonsági tesztelőeszközök** | Ismertesse a hálózatbiztonsági teszteléshez használt eszközöket! |

[21.9](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Introduction to ASDM (Optional)](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[22.1](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Network Security Testing Techniques](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                            

1. Network Security Testing
2. Network Security Testing Techniques

# Hálózatbiztonsági tesztelési technikák

22.1.1

## Hadműveletek biztonsági biztosítása

A működési biztonság azokra a napi gyakorlatokra vonatkozik, amelyek a biztonságos rendszer első üzembe helyezéséhez, majd későbbi karbantartásához szükségesek. Minden hálózat sebezhető a támadásokkal szemben, ha a hálózat tervezése, megvalósítása, üzemeltetése és karbantartása nem tartja be a működési biztonsági gyakorlatot.

A működési biztonság a hálózat tervezési és megvalósítási folyamatával kezdődik. Ezekben a fázisokban az operatív csapat elemzi a terveket, azonosítja a kockázatokat és a sebezhetőségeket, és elvégzi a szükséges módosításokat. A tényleges üzemeltetési feladatok a hálózat felállítása után kezdődnek, és magukban foglalják a környezet folyamatos karbantartását. Ezek a tevékenységek lehetővé teszik a környezet, a rendszerek és az alkalmazások megfelelő és biztonságos működését.

Egyes biztonsági tesztelési technikák túlnyomórészt manuálisak, mások pedig nagymértékben automatizáltak. A tesztelés típusától függetlenül a biztonsági tesztelést beállító és lebonyolító személyzetnek jelentős biztonsági és hálózati ismeretekkel kell rendelkeznie a következő területeken:

* Operációs rendszer
* Alapvető programozás
* Hálózati protokollok, például TCP/IP
* Hálózati sérülékenységek és kockázatcsökkentés
* Készülék keményedés
* Tűzfalak
* IPS-ek

22.1.2

## A hálózati biztonság tesztelése és értékelése

A műveleti biztonsági megoldások hatékonysága anélkül tesztelhető, hogy megvárnánk a valós fenyegetés bekövetkeztét. A hálózati biztonsági tesztelés ezt lehetővé teszi. A hálózati biztonsági tesztelést a hálózaton végzik el, hogy megbizonyosodjon arról, hogy az összes biztonsági megvalósítás a várt módon működik. A hálózatbiztonsági tesztelésre jellemzően a bevezetés és az üzemeltetés szakaszában, a rendszer fejlesztése, telepítése és integrálása után kerül sor.

A biztonsági tesztelés betekintést nyújt különféle adminisztratív feladatokba, például kockázatelemzésbe és készenléti tervezésbe. Fontos a biztonsági tesztelés eredményeinek dokumentálása és elérhetővé tétele az egyéb informatikai területeken dolgozó munkatársak számára.

A megvalósítás szakaszában biztonsági tesztelést hajtanak végre a hálózat meghatározott részein. Miután a hálózat teljesen integrálódott és működőképes, biztonsági tesztet és értékelést (ST&E) hajtanak végre. Az ST&E egy működő hálózaton elhelyezett védelmi intézkedések vizsgálata.

Az ST&E céljai a következők:

* Fedezze fel azokat a tervezési, megvalósítási és működési hibákat, amelyek a biztonsági szabályzat megsértéséhez vezethetnek.
* Határozza meg a biztonsági mechanizmusok, biztosítékok és eszköztulajdonságok megfelelőségét a biztonsági politika érvényesítéséhez.
* Mérje fel a rendszerdokumentáció és a megvalósítás közötti összhang mértékét.

A teszteket rendszeresen meg kell ismételni, és minden alkalommal, amikor a rendszerben változás történik. Azon biztonsági rendszerek esetében, amelyek védik a kritikus információkat vagy védik az állandó fenyegetésnek kitett gazdagépeket, gyakrabban kell biztonsági tesztelést végezni.

22.1.3

## A hálózati tesztek típusai

A hálózat működése után hozzá kell férnie a biztonsági állapotához. Számos biztonsági teszt elvégezhető a hálózat működési állapotának felmérésére:

* **Behatolási tesztelés –** A hálózati penetrációs tesztek vagy tolltesztek rosszindulatú forrásokból származó támadásokat szimulálnak. A cél a támadás megvalósíthatóságának és lehetséges következményeinek meghatározása, ha bekövetkezne. Egyes tollteszteknél előfordulhat, hogy be kell lépni az ügyfél helyiségeibe, és szociális mérnöki készségeket kell használni az általános biztonsági testtartás tesztelésére.
* **Hálózati szkennelés –** Tartalmaz olyan szoftvert, amely képes pingelni a számítógépeket, megkeresni a figyelő TCP-portokat, és megjeleníteni, hogy milyen típusú erőforrások állnak rendelkezésre a hálózaton. Egyes szkennelőszoftverek felhasználóneveket, csoportokat és megosztott erőforrásokat is képesek észlelni. A hálózati rendszergazdák ezt az információt felhasználhatják hálózataik megerősítésére.
* **Sebezhetőség-ellenőrzés –** Ide tartozik a szoftver, amely képes észlelni a tesztelt rendszerek lehetséges gyengeségeit. Ezek a hiányosságok magukban foglalhatják a hibás konfigurációt, az üres vagy alapértelmezett jelszavakat, vagy a DoS-támadások lehetséges célpontjait. Egyes szoftverek lehetővé teszik a rendszergazdák számára, hogy megpróbálják összeomlani a rendszert az azonosított biztonsági résen keresztül.
* **Jelszó feltörése –** Ez magában foglalja a módosítandó gyenge jelszavak tesztelésére és észlelésére használt szoftvereket. A jelszószabályzatnak tartalmaznia kell a gyenge jelszavak elkerülésére vonatkozó iránymutatásokat.
* **Napló áttekintése –** A rendszergazdáknak át kell tekinteniük a biztonsági naplókat a lehetséges biztonsági fenyegetések azonosítása érdekében. A hosszadalmas naplófájlok átvizsgálására szolgáló szűrőszoftvert kell használni a rendellenes tevékenység kivizsgálásához.
* **Integritás-ellenőrzők –** Az integritás-ellenőrző rendszer észleli a rendszerben bekövetkezett változásokat, és jelentést készít azokról. A figyelés nagy része a fájlrendszerre összpontosul. Néhány ellenőrző rendszer azonban jelentést készíthet a bejelentkezési és kijelentkezési tevékenységekről.
* **Vírusfelderítés –** A számítógépes vírusok és egyéb rosszindulatú programok azonosítására és eltávolítására vírus- vagy kártevőirtó szoftvert kell használni.

**Megjegyzés** : Az egyéb tesztek, köztük a Wardialing és a Wardriving, örököltnek minősülnek, de figyelembe kell venni őket a hálózati tesztelés során.

22.1.4

## Hálózati teszteredmények alkalmazása

A hálózatbiztonsági tesztek eredményei többféleképpen felhasználhatók:

* Mérséklő tevékenységek meghatározása az azonosított sebezhetőségek kezelésére
* Összehasonlítási alapként a szervezet előrehaladásának nyomon követésére a biztonsági követelmények teljesítésében
* A rendszerbiztonsági követelmények megvalósítási állapotának felmérése
* Költség-haszon elemzés elvégzése a hálózat biztonságának javítása érdekében
* Más tevékenységek, például kockázatértékelés, tanúsítás és engedélyezés (C&A), valamint a teljesítmény javítására irányuló erőfeszítések fokozása
* Referenciapontként a korrekciós intézkedésekhez

[22.0](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Introduction](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[22.2](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Network Security Testing Tools](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                               

1. Network Security Testing
2. Network Security Testing Tools

# Hálózatbiztonsági tesztelőeszközök

22.2.1

## Hálózati tesztelési eszközök

Számos eszköz áll rendelkezésre a rendszerek és hálózatok biztonságának tesztelésére. Ezen eszközök némelyike ​​nyílt forráskódú, míg mások kereskedelmi eszközök, amelyekhez licenc szükséges.

A hálózati teszteléshez használható szoftvereszközök a következők:

* **Nmap/Zenmap –** A hálózaton lévő számítógépek és szolgáltatásaik felderítésére szolgál, így a hálózat térképének létrehozására.
* **SuperScan** – Ez a portellenőrző szoftver a nyitott TCP- és UDP-portok észlelésére, az ezeken a portokon futó szolgáltatások meghatározására, valamint lekérdezések futtatására szolgál, mint például a whois, ping, traceroute és gazdagépnév-keresések.
* **SIEM (Security Information Event Management)** – Ez a technológia, amelyet a vállalati szervezetekben használnak a biztonsági események valós idejű jelentésére és hosszú távú elemzésére.
* **GFI LANguard** – Ez egy hálózati és biztonsági szkenner, amely észleli a sebezhetőségeket.
* **Tripwire** – Ez az eszköz felméri és érvényesíti az IT-konfigurációkat a belső szabályzatok, megfelelőségi szabványok és a legjobb biztonsági gyakorlatok alapján.
* **Nessus** – Ez egy sebezhetőséget vizsgáló szoftver, amely a távoli hozzáférésre, a hibás konfigurációkra és a TCP/IP-verem DoS-re összpontosít.
* **L0phtCrack** - Ez egy jelszó-auditáló és -helyreállító alkalmazás.
* **Metasploit** – Ez az eszköz a sebezhetőségekről nyújt információkat, valamint segítséget nyújt a behatolási teszteléshez és az IDS aláírások fejlesztéséhez.

**Megjegyzés** : A hálózati tesztelő eszközök gyors ütemben fejlődnek. Az előző lista örökölt eszközöket tartalmaz, és célja, hogy megismertesse a rendelkezésre álló különböző típusú eszközöket.

22.2.2

## Nmap és Zenmap

Az Nmap egy gyakran használt, alacsony szintű szkenner, amely a nyilvánosság számára elérhető. Számos kiváló tulajdonsággal rendelkezik, amelyek használhatók hálózati feltérképezéshez és felderítéshez.

Az Nmap alapvető funkciói lehetővé teszik a felhasználó számára, hogy több feladatot is végrehajtson, az alábbiak szerint:

* **Klasszikus TCP és UDP port-ellenőrzés** – Különféle szolgáltatásokat keres egy gazdagépen.
* **Klasszikus TCP- és UDP-portsöprés** – Ez ugyanazt a szolgáltatást keresi több gazdagépen.
* **Stealth TCP- és UDP-port-ellenőrzések és -sweep-ek** – Ez hasonló a klasszikus vizsgálatokhoz és sweep-ekhez, de a célállomás vagy az IPS nehezebben észlelhető.
* **Az operációs rendszer távoli azonosítása** – Ezt az operációs rendszer ujjlenyomatának is nevezik.

Az Nmap fejlett funkciói közé tartozik a protokoll-ellenőrzés, az úgynevezett Layer 3 port scan. Ez a szolgáltatás azonosítja a 3. rétegbeli protokoll támogatását egy gazdagépen. Az azonosítható protokollok közé tartozik például a GRE és az OSPF.

Míg az Nmap használható biztonsági tesztelésre, rosszindulatú célokra is használható. Az Nmap rendelkezik egy további funkcióval, amely lehetővé teszi, hogy a célállomással azonos LAN-on lévő csali gazdagépeket használjon, hogy elfedje a vizsgálat forrását.

Az Nmap nem rendelkezik alkalmazásréteg-funkciókkal, és UNIX, Linux, Windows és OS X rendszeren fut. Mind a konzolos, mind a grafikus verzió elérhető. Az Nmap program és a Zenmap GUI letölthető az internetről.

22.2.3

## SuperScan

A SuperScan egy Microsoft Windows portellenőrző eszköz. A Windows legtöbb verzióján fut, és rendszergazdai jogosultságokat igényel.

A SuperScan 4-es verziója számos hasznos funkcióval rendelkezik:

* Állítható szkennelési sebesség
* Korlátlan IP-tartomány támogatása
* Továbbfejlesztett gazdagép-észlelés több ICMP-módszerrel
* TCP SYN szkennelés
* UDP szkennelés (két módszer)
* Egyszerű HTML jelentéskészítés
* Forrás port szkennelés
* Gyors gazdagépnév felbontás
* Kiterjedt szalaghirdetési lehetőség
* Hatalmas beépített portlista-leíró adatbázis
* IP és port szkennelés sorrendjének randomizálása
* Hasznos eszközök válogatása, mint például a ping, a traceroute és a whois
* Kiterjedt Windows hosztfelsorolási lehetőség

Az olyan eszközök, mint az Nmap és a SuperScan, hatékony penetrációs tesztelést biztosíthatnak a hálózaton, és meghatározhatják a hálózati sebezhetőségeket, miközben segítik a lehetséges támadási mechanizmusok előrejelzését. A hálózati tesztelés azonban nem tud minden biztonsági problémára felkészíteni a hálózati rendszergazdát.

22.2.4

## SIEM

A Security Information Event Management (SIEM) egy olyan technológia, amelyet a vállalati szervezetek valós idejű jelentések készítésére és a biztonsági események hosszú távú elemzésére használnak. A SIEM két korábban különálló termékből fejlődött ki: a Security Information Management (SIM) és a Security Event Management (SEM) termékből. A SIEM megvalósítható szoftverként, integrálva a Cisco Identity Services Engine-hez (ISE) vagy felügyelt szolgáltatásként.

A SIEM egyesíti a SIM és a SEM alapvető funkcióit, hogy biztosítsa:

* **Korreláció** – Megvizsgálja a különböző rendszerekből vagy alkalmazásokból származó naplókat és eseményeket, felgyorsítja a biztonsági fenyegetések észlelését és reagálását.
* **Összesítés** – Az összesítés csökkenti az eseményadatok mennyiségét a duplikált eseményrekordok konszolidálásával.
* **Törvényszéki elemzés** – A naplók és eseményrekordok forrásokból való keresésének képessége a szervezeten belül teljesebb információkkal szolgál a törvényszéki elemzéshez.
* **Megőrzés** – A jelentés a korrelált és összesített eseményadatokat jeleníti meg valós idejű megfigyelésben és hosszú távú összefoglalókban.

A SIEM részleteket közöl a gyanús tevékenység forrásáról, többek között:

* Felhasználói adatok (név, hitelesítési állapot, hely, jogosultsági csoport, karantén állapota)
* Eszközinformációk (gyártó, modell, operációs rendszer verziója, MAC-cím, hálózati csatlakozási mód, hely)
* Testtartási információk (az eszköz megfelelése a vállalati biztonsági szabályzatnak, víruskereső verzió, operációs rendszer javítások, mobileszköz-kezelési szabályzatnak való megfelelés)

Ezen információk felhasználásával a hálózati biztonsági mérnökök gyorsan és pontosan felmérhetik bármely biztonsági esemény jelentőségét, és megválaszolhatják a kritikus kérdéseket:

* Ki kapcsolódik ehhez az eseményhez?
* Fontos felhasználó, aki hozzáfér a szellemi tulajdonhoz vagy érzékeny információkhoz?
* Jogosult-e a felhasználó hozzáférni ehhez az erőforráshoz?
* Hozzáfér-e a felhasználó más érzékeny forrásokhoz?
* Milyen készüléket használnak?
* Ez az esemény potenciális megfelelési problémát jelent?

22.2.5

## Ellenőrizze, hogy megértette-e a hálózati biztonsági tesztelőeszközöket

Az űrlap teteje

Ellenőrizze, hogy megértette-e a hálózati biztonsági tesztelési eszközöket, és válassza ki a megfelelő választ a következő kérdésekre.

1. Melyik eszköz nyújt információt a sebezhetőségekről, és segíti a penetrációs tesztelést és az IDS aláírások fejlesztését?

Az űrlap alja

Melyik eszköz fedezi fel a számítógépeket és a szolgáltatásokat a számítógépes hálózaton, és így készíti el a hálózat térképét?

Melyik eszköz a sebezhetőség-ellenőrző szoftver, amely a távoli hozzáférésre, a hibás konfigurációkra és a TCP/IP-verem DoS-re összpontosít?

[22.1](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Network Security Testing Techniques](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[22.3](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Network Security Testing Summary](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

# Hálózati biztonság

v 1.0

[Skip to content](https://contenthub.netacad.com/netsec/11.0.1?lng=en#chunks-container)

1.                                                                                                                                                                                                                                                                                                                                                                                                 
2. Network Security Testing
3. Network Security Testing Summary

# Hálózatbiztonsági tesztelés összefoglalója

22.3.1

## Mit tanultam ebben a modulban?

**Hálózatbiztonsági tesztelési technikák**   
A működési biztonság a hálózat tervezési és megvalósítási folyamatával kezdődik. Ezekben a fázisokban az operatív csapat elemzi a terveket, azonosítja a kockázatokat és a sebezhetőségeket, és elvégzi a szükséges módosításokat. A tényleges üzemeltetési feladatok a hálózat felállítása után kezdődnek, és magukban foglalják a környezet folyamatos karbantartását. A biztonsági tesztelést beállító és lebonyolító személyzetnek jelentős biztonsági és hálózati ismeretekkel kell rendelkeznie ezeken a területeken: eszközök keményítése, tűzfalak, IPS-ek, operációs rendszerek, alapvető programozás, hálózati protokollok, például TCP/IP, valamint hálózati sebezhetőségek és kockázatcsökkentés. Az ST&E egy működő hálózaton elhelyezett védelmi intézkedések vizsgálata. Számos biztonsági teszt elvégezhető a hálózat működési állapotának felmérésére, ideértve a következőket: behatolási tesztelés, hálózati vizsgálat, sebezhetőségi vizsgálat, jelszavak feltörése, naplók áttekintése, integritás-ellenőrzés és vírusérzékelés.

**Hálózatbiztonsági tesztelőeszközök**   
Számos eszköz áll rendelkezésre a rendszerek és hálózatok biztonságának tesztelésére: Nmap/Zenmap, SuperScan, SIEM, GFI LANguard, Tripwire, Nessus, L0phtCrack és Metasploit. Az Nmap és a Zenmap (annak grafikus felülete) általánosan használt és ingyenes alacsony szintű szkennerek. A SuperScan egy ingyenes Microsoft Windows portellenőrző eszköz is. A Security Information Event Management (SIEM) egy olyan technológia, amelyet a vállalati szervezetek valós idejű jelentések készítésére és a biztonsági események hosszú távú elemzésére használnak. A SIEM-ek korrelációt, összesítést, kriminalisztikai elemzést és megőrzést biztosítanak.

22.3.2

## 22. modul – Hálózatbiztonsági tesztelési kvíz

Az űrlap teteje

1. A biztonsági elemzők minden nap időt töltenek azzal, hogy megvizsgálják a különböző rendszerek és alkalmazások naplóit és eseményeit, hogy gyorsan észleljék a biztonsági fenyegetéseket. A biztonsági információs eseménykezelő (SIEM) technológia milyen funkcióját képviseli ez a művelet?

Az űrlap alja

Melyik hálózati biztonsági eszköz képes észlelni a nyitott TCP- és UDP-portokat a Microsoft Windows legtöbb verziójában?

Egy biztonsági technikus egy új műveleti biztonsági javaslatot értékel, amelynek célja az összes kiszolgálóhoz való hozzáférés korlátozása. Milyen előnyökkel jár a hálózatbiztonsági tesztelés alkalmazása az új javaslat értékelésére?

Milyen információkat nyújt a SIEM hálózatbiztonsági felügyeleti eszköz a hálózati rendszergazdáknak?

Melyik hálózati leolvasó eszköz rendelkezik olyan fejlett funkciókkal, amelyek lehetővé teszik csali gazdagépek használatát a vizsgálat forrásának elfedésére?

Új személy csatlakozott egy gyártóüzem biztonsági műveleti csapatához. Mi a közös felelősségi kör ennek a személynek?

Melyik biztonsági teszt alkalmas a rendszer gyengeségeinek, például a hibás konfiguráció, az alapértelmezett jelszavak és a lehetséges DoS-célok észlelésére?

Milyen típusú hálózati biztonsági tesztet használnának a hálózati rendszergazdák a hálózati rendszerek változásainak észlelésére és jelentésére?

Melyik hálózati biztonsági eszköz teszi lehetővé a rendszergazdák számára a gyenge jelszavak tesztelését és észlelését?

Milyen két feladatot lehet végrehajtani az Nmap és a Zenmap hálózati eszközökkel? (Válassz kettőt.)

Milyen típusú biztonsági tesztek használnak szimulált támadásokat a valós fenyegetés lehetséges következményeinek meghatározására?

Milyen funkciókat biztosít a Tripwire hálózati biztonsági eszköz?

[22.2](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)

[Network Security Testing Tools](https://contenthub.netacad.com/netsec/11.0.1?lng=en" \l "/netsec/undefined.1)