4. fejezet: Tűzfaltechnológiák megvalósítása

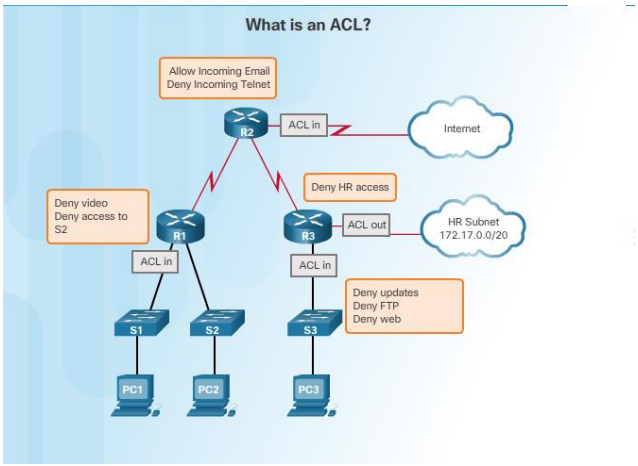
Mivel a hálózatok tovább növekedtek az idő múlásával, egyre inkább felhasználtak érzékeny adatok átvitelére és tárolására. Ez fokozta az erősebb biztonsági technológiák szükségességét, ami a tűzfal kialakulásához vezetett. A tűzfal kifejezés eredetileg egy tűzálló falra utal, amely általában kőből vagy fémből készült, ami megakadályozta, hogy a lángok elterjedjenek a csatlakoztatott szerkezetek között. A hálózatépítés világában a tűzfalak védett területeket különítenek el a nem védett területektől. Ez megakadályozza a jogosulatlan felhasználók számára a védett hálózati erőforrások elérését.

Kezdetben az alapvető hozzáférés-vezérlési listák (ACL-ek), beleértve a szabványos, kiterjesztett, számozott és megnevezett adatokat, az egyetlen eszköz a tűzfalvédelem biztosítására. Az egyéb tűzfaltechnológiák az 1990-es évek végén kezdtek érlelni. A tiltott tűzfalak táblákat használnak a végpontok közötti szakaszok valós idejű állapotának nyomon követésére. A tiltott tűzfalak figyelembe veszik a hálózatforgalom munkamenet-orientált jellegét. Az első állami tűzfalak használták a "TCP established" opciót az ACL-ek számára.

Ma már számos típusú tűzfal létezik, például a csomagszűrés, az állapotfájl, az alkalmazás átjáró, a proxy, a címfordítás, a gazdaalapú, átlátható és a hibrid tűzfalak. A modern hálózati kialakításnak gondosan meg kell határoznia egy vagy több tűzfal megfelelő elhelyezését az erőforrások védelme érdekében, amelyeket védeni kell, miközben lehetővé teszi a források biztonságos elérését, amelyeknek rendelkezésre kell állniuk.

Bevezetés az ACL-ekbe

Az ACL-eket széles körben használják a számítógépes hálózatokban és a hálózati biztonságban a hálózati támadások mérséklése és a hálózati forgalom ellenőrzése terén. A rendszergazdák használhatják az ACL-eket a hálózati eszközök forgalmának meghatározására és ellenőrzésére, hogy megfeleljenek az adott biztonsági követelményeknek. Az ACL-ek meghatározhatók az Open Systems Interconnection (OSI) 2., 3., 4. és 7. rétegéhez.



Történelmileg az ACL típusát a szám alapján lehet azonosítani. Például 200-299 körüli számozott ACL-eket használt az Ethernet típusú forgalom vezérlésére. A 700-799 számjegyű ACL azt jelezné, hogy a forgalom MAC-címek alapján osztályozható és ellenőrzött.

A forgalom osztályozása során a legelterjedtebb ACL-típusok IPv4 és IPv6 címeket, valamint a TCP (Transmission Control Protocol) és User Datagram Protocol (UDP) portszámokat használnak. A szabványos és kiterjesztett IPv4 ACL-ek nevezhetők vagy számozhatók. Az IPv6 ACL-eknek egy nevet kell használnia.

Protocol	Range
IP	1-99, 1300-1999
Extended IP	100-199, 2000-2699
Ethernet type code	200-299
DECnet and Extended DECnet	300-399
XNS	400-499
Extended XNS	500-599
AppleTalk	600-699
Ethernet address	700-799
IPX	800-899
Extended IPX	900-999
IPX SAP	1000-1099
Extended transparent bridging	1100-1199

Számozott és nevesített ACL-ek konfigurálása

Az ACL az engedéllyel vagy megtagadási nyilatkozatok sorozatos listája, más néven hozzáférési vezérlő bejegyzéseknek (ACE-k). Az ACE-k általában ACL-nyilatkozatoknak is nevezhetők. ACE-k létrehozhatók a forgalom szűrésére bizonyos kritériumok alapján, mint például: a forráscím, a célcím, a protokoll és a portszámok.

A szabványos ACL-ek a csomag IP-fejlécében lévő forrás IP-cím mezőjének megvizsgálásával illeszkednek a csomagokhoz. Ezek az ACL-ek csomagok szűrésére szolgálnak, amelyek kizárólag a 3. rétegbeli forrásadatokra épülnek. Számozott szabványos ACL konfigurálása.

Standard Numbered ACL Syntax

```
access-list {acl-#} {permit | deny | remark} source-addr [source-wildcard] [log]
```

Standard ACLs filter IP packets based on the source address only.

acl-#	This is a decimal number from 1 to 99, or 1300 to 1999.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
remark	Add a remark about entries in an IP access list to make the list easier to understand and scan.
source-addr	Number of the network or host from which the packet is being sent. There are two ways to specify the *source-addr* : • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.
source-wildcard	(Optional) 32-bit wildcard mask to be applied to the source. Places ones in the bit positions you want to ignore.
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message includes the ACL number, whether the packet was permitted or denied, the source address, and the number of packets. The message is generated for the first packet that matches, and then at five-minute intervals, including the number of packets permitted or denied in the prior five-minute interval.

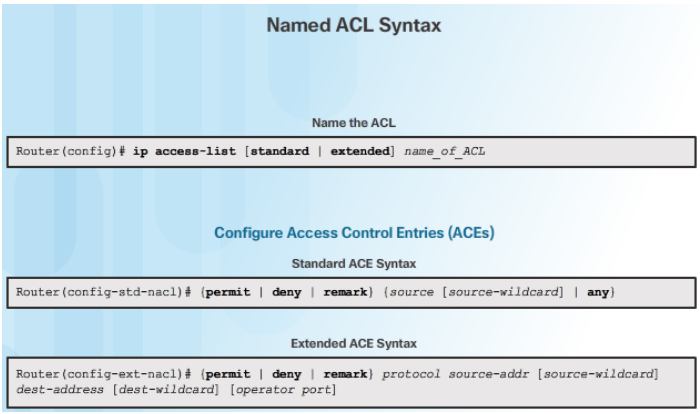
A kiterjesztett ACL-ek illeszkednek a 3. és 4. rétegbeli forrás- és célinformációk alapján. A 4. réteg lehet TCP és UDP port információ. A kiterjesztett ACL-ek nagyobb rugalmasságot és nagyobb hálózati hozzáférést biztosítanak, mint a hagyományos ACL-ek. A számozott kiterjesztett ACL konfigurálásához használja a parancsszintaxist.

Extended Numbered ACL Syntax

```
access-list acl-# {permit | deny | remark} protocol source-addr [source-wildcard]
dest-addr [dest-wildcard] [operator port] [established]
```

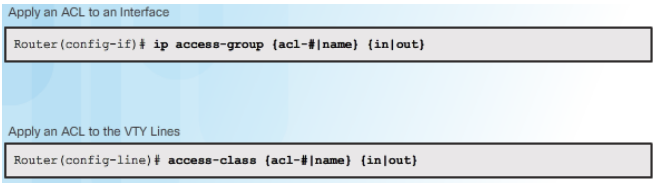
Parameter	Description
acl-#	Identifies the access list using a number in the range 100 to 199 (for an extended IP ACL) and 2000 to 2699 (expanded IP ACLs).
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
remark	Used to enter a remark or comment.
protocol	Name or number of an Internet protocol. Common keywords include **icmp**, **ip**, **tcp**, or **udp**. To match any Internet protocol (including ICMP, TCP, and UDP) use the **ip** keyword.
source-addr	Number of the network or host from which the packet is being sent.
source-wildcard	Wildcard bits to be applied to source.
destination-addr	Number of the network or host to which the packet is being sent.
destination-wildcard	Wildcard bits to be applied to the destination.
operator	(Optional) Compares source or destination ports. Possible operands include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range).
port	(Optional) The decimal number or name of a TCP or UDP port.
established	(Optional) For the TCP protocol only: Indicates an established connection.

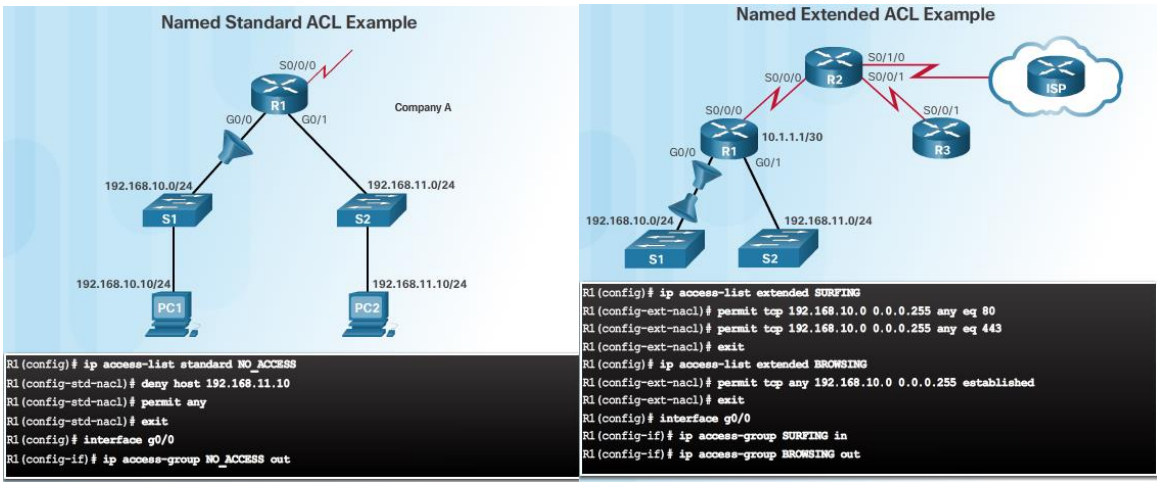
A szám használata helyett egy név használható az ACL konfigurálásához. Az elnevezett ACL-eket szabványos vagy kiterjesztettként kell megadni. Meghatározott szabvány vagy kiterjesztett ACL beállításához használja a parancssinta-parancsot.



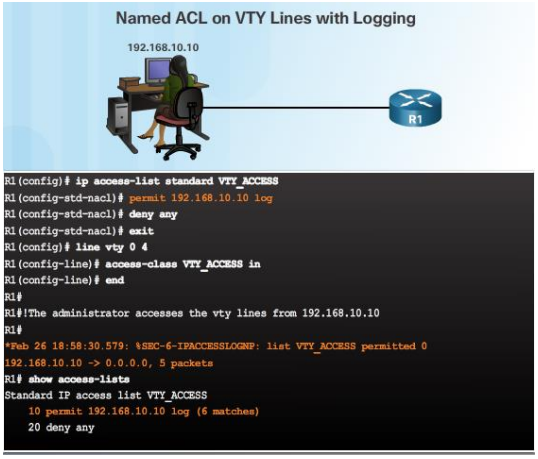
ACL alkalmazása

Az ACL létrehozása után a rendszergazda számos módon alkalmazhatja. Az 1. ábra a parancsszintaxist mutatja, hogy egy ACL-t alkalmazzon egy interfészre vagy a vty vonalakra. A 2. ábra a kimenő forgalomra vonatkozó megnevezett standard ACL-t mutatja. A 3. ábra két elnevezett kiterjesztett ACL-t mutat be. A SURFING ACL a bejövő forgalomra vonatkozik, és a BROWSING ACL a kimenő forgalomra vonatkozik. A 4. ábra a vty vonalakra vonatkozó bejövő forgalomra vonatkozó megnevezett standard ACL-t mutatja. A naplózás engedélyezve volt a naplóparaméterrel. Naplóüzenetek generálódnak az első csomagegyüttesen, majd öt perces időközönként az első csomagegyüttes után. A show access-list parancs segítségével megtekintheti, hogy hány csomag egyezik egy nyilatkozattal.





A Cisco router **log** paraméterének bekapcsolása vagy komoly váltása hatással van az eszköz teljesítményére. A naplófájl csak akkor használható, ha a hálózat támadás alatt áll, és a rendszergazda megpróbálja meghatározni, hogy ki a támadó.



Az ACL-eknek az interfészekhez és vonalakhoz való alkalmazása csak egyike a sok lehetséges felhasználásnak. Az ACL-ek szintén szerves részét képezik az egyéb biztonsági konfigurációknak, például a zónaalapú tűzfalaknak, a behatolás-megelőző rendszereknek és a virtuális magánhálózatoknak.

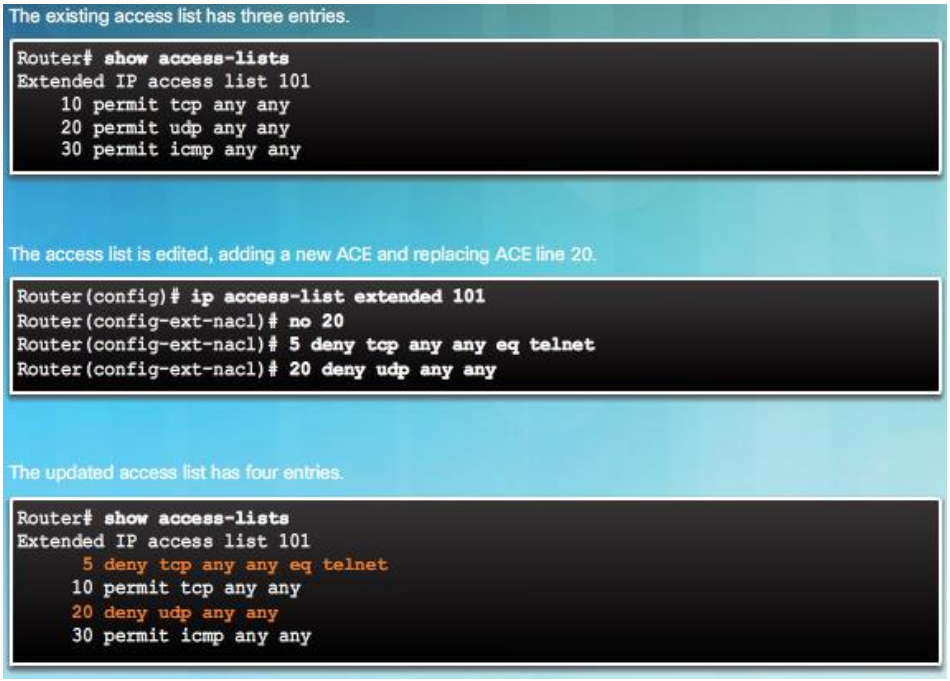
ACL konfigurációs irányelvek

Az ACL egy vagy több hozzáférési vezérlési tétel (ACE) vagy nyilatkozatból áll. ACL konfigurálásakor és alkalmazásakor vegye figyelembe az ábrán összegzett iránymutatásokat.

- Create an ACL globally and then apply it.
- Ensure the last statement is an implicit *deny any* or *deny any any*.
- Remember that statement order is important because ACLs are processed top-down. As soon as a statement is matched the ACL is exited.
- Ensure that the most specific statements are at the top of the list.
- Remember that only one ACL is allowed per interface, per protocol, per direction.
- Remember that new statements for an existing ACL are added to the bottom of the ACL by default.
- Remember that router generated packets are not filtered by outbound ACLs.
- Place standard ACLs as close to the destination as possible.
- Place extended ACLs as close to the source as possible.

Meglévő ACL-ek szerkesztése

Alapértelmezés szerint a sorszámozás 10 lépésben történik, és minden hozzáférési vezérlő bejegyzéshez (ACE) van rendelve egy ACL-en belül. Az ACL létrehozása és alkalmazása után szerkeszthető ezek a sorszámok. Használja a sorszámokat az egyes ACE-ek törléséhez vagy hozzáadásához különböző sorrendben, ahogy az az ábrán látható. Ha egy új bejegyzéshez nincs megadva egy sorszám, akkor az útválasztó automatikusan elhelyezi a bejegyzést a lista alján, és hozzárendel egy megfelelő sorszámot.



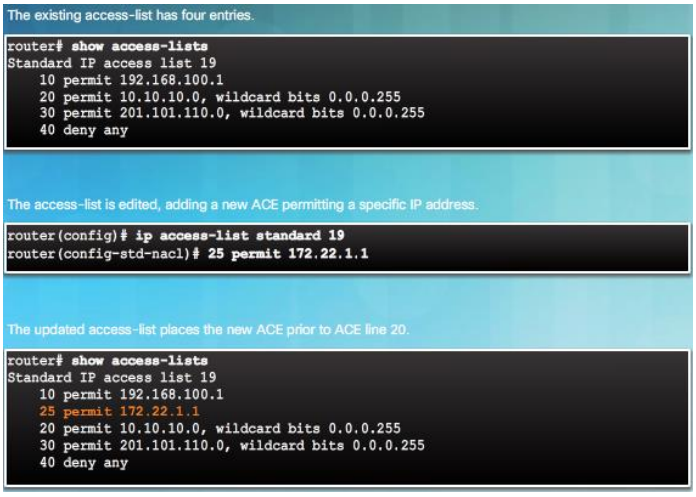
Sorszámok és standard ACL-ek

A szabványos hozzáférési listákon a Cisco IOS egy belső logikát alkalmaz az ACE-k konfigurálásához és az ACL-ek ellenőrzéséhez. A kiszolgálói nyilatkozatok (az adott IPv4-címekkel rendelkezők) először szerepelnek, de nem feltétlenül a bevitelük sorrendjében. Először is, az IOS a kiszolgálói állításokat egy adott sorrendben helyezik el, amelyet egy speciális hasítófunkció határoz meg. Az így kapott sorrend optimalizálja a host ACL bejegyzésének keresését. Nem feltétlenül az IPv4-címek sorrendje.

Az ábrán látható példa egy létező standard ACL 19 különböző bejegyzéseit mutatja be. A rendszergazda megpróbál hozzáadni egy bejegyzést a 19 hozzáférési listán, a 25-ös sorozatot használva, amely lehetővé teszi a 172.22.1.1 IP-címet. Annak ellenére, hogy a megadott sorszám nagyobb, mint a 10.10.10.0 hálózat szekvenciaszáma, a bejegyzést a 10.10.10.0 ACE előtt adják hozzá. Ez elsőbbséget ad a specifikus gazda utasításnak, nem pedig a hálózati vagy tartományi utasításnak.

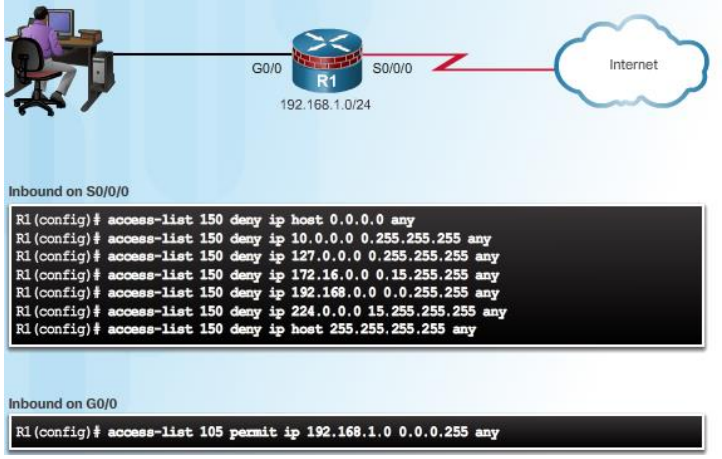
A szekvencia száma nem írja elő a feldolgozási megbízást egy standard ACL-ben. Azonban használható egy azonosítóként egy adott bejegyzés törléséhez.

Megjegyzés: Kezdetben a sorszámok jelzik a sorrendet, amelybe a kijelentéseket bevitték, nem pedig a nyilatkozatok feldolgozásának sorrendjét. Miután az útválasztó újratöltésre került, a sorozathoz tartozó hozzáférési listák sorszámozása új számozási sorrendbe kerül.



Antispoofing ACL-ekkel

Az ACL-ek számos hálózati fenyegetés enyhítésére használhatók, mint pl. IP-cím spoofing és denial of service (DoS) támadások. A legtöbb DoS támadás bizonyos típusú spoofingt használ. Az IP-cím spoofing felülbírálja a normál csomagkészítési folyamatot egy egyedi IP-fejléc beillesztésével egy másik forrás IP-címmel. A támadók elrejthetik identitásukat a forrás IP-cím meghamisításával.



Számos jól ismert IP-címosztály létezik, amelyet soha nem tekinthetõ forrás-IP-címnek a szervezet hálózatába való belépéshez. Például az ábrán az S0 / 0/0 interfész az internethez csatlakozik, és soha nem fogadja be a bejövő csomagokat a következő címekről:

Minden nulla cím

Broadcast címek

Helyi gazdanevek (127.0.0.0/8)

Fenntartott privát címek (RFC 1918)

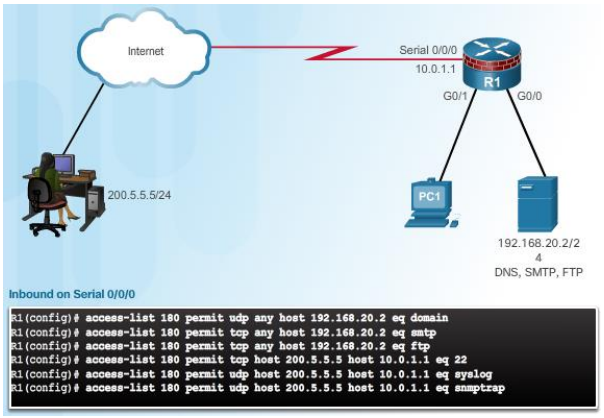
IP multicast címtartomány (224.0.0.0/4)

Egy 192.168.1.0/24 hálózat az R1 G0 / 0 interfészhez csatlakozik. Ez a felület csak olyan forrást tartalmazó csomagokat fogadhat el, amelyek forráshálózati címét az adott hálózatról. Az ábrán látható G0 / 0 ACL engedélyezi a bejövő csomagokat egy 192.168.1.0/24 hálózatból. Minden más eldobásra kerül.

A szükséges forgalom engedélyezése tűzfalon keresztül

A támadások mérséklésére szolgáló hatékony stratégia kifejezetten csak bizonyos típusú forgalom engedélyezését tűzfalon keresztül engedélyezi. Például a Domain Name System (DNS), az SMTP (Simple Mail Transfer Protocol) és az FTP szolgáltatás olyan szolgáltatások, amelyeket gyakran tűzfalon keresztül kell engedélyezni. Az is gyakori, hogy beállítson egy tűzfalat úgy, hogy lehetővé tegye a rendszergazdák számára a távoli hozzáférést a tűzfalon keresztül. A Secure Shell (SSH), a syslog és az egyszerű hálózati felügyeleti protokoll (SNMP) példák azoknak a szolgáltatásoknak, amelyeket a routernek tartalmaznia kell. Miközben sok ilyen szolgáltatás hasznos, azokat ellenőrizni és ellenőrizni kell. Ezeknek a szolgáltatásoknak a kihasználása biztonsági réseket okoz.

Az ábra egy minta topológiát mutat be lehetséges ACL konfigurációkkal, amelyek lehetővé teszik a Serial 0/0/0 interfészre vonatkozó speciális szolgáltatásokat.



Az ICMP visszaélések csökkentése

A hackerek az ICMP (Internet Control Message Protocol) echo csomagok (pings) segítségével felfedezhetik a védett hálózatok alhálózatát és házigazdáit, valamint DoS árvízkísérleteket generálhatnak. A hackerek az ICMP átirányítási üzeneteket használhatják a gazdagép-táblák megváltoztatására. Az ICMP echo és átirányító üzeneteket az útválasztónak be kell tartania.

Számos ICMP üzenet ajánlott a megfelelő hálózati működéshez, és engedélyezni kell a belső hálózathoz:

Echo válasz - Lehetővé teszi a felhasználók számára, hogy pingelítsék a külső hostokat.

Forráselhárítás - A küldő csökkenti az üzenetek forgalmát.

Nem érhető el - Olyan csomagok számára hozható létre, amelyeket egy ACL adminisztratív módon elutasít.

Számos ICMP üzenet szükséges a megfelelő hálózati működéshez, és engedélyezni kell a hálózatból való kilépést:

Echo - Lehetővé teszi a felhasználók számára a külső hostok pingelését.

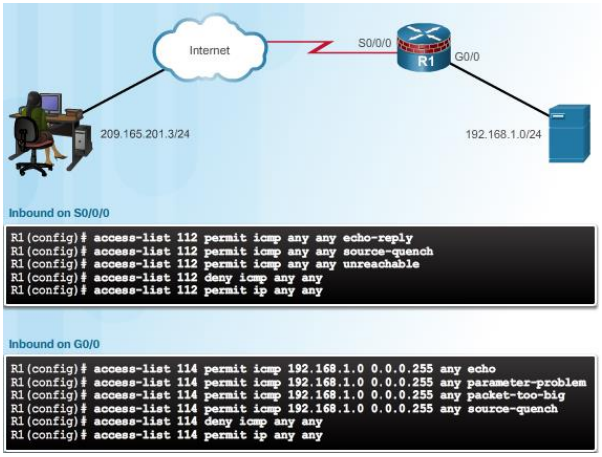
Paraméterprobléma - Tájékoztatja a csomag fejléc problémáit.

A csomag túl nagy - Lehetővé teszi a csomag maximális átviteli egység (MTU) felfedezését.

Forráselhárítás - Szükség esetén lecsökkenti a forgalmat.

Általános szabályként tiltsa le az összes többi ICMP üzenet típusú kimenetet.

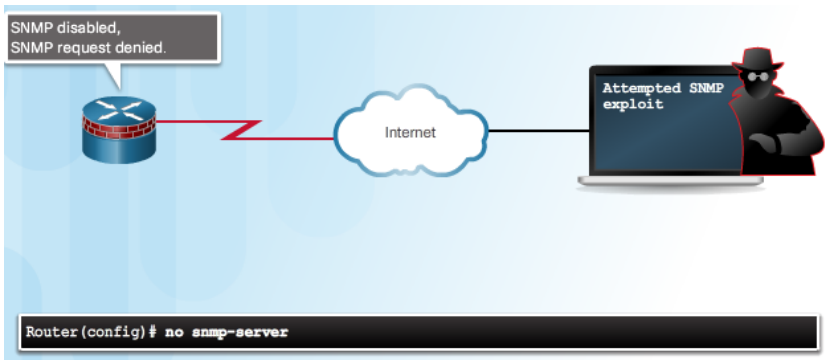
Az ACL-eket az IP cím spoofing blokkolására használják, szelektíven engedélyezik bizonyos szolgáltatásokat egy tűzfalon keresztül, és csak a szükséges ICMP üzeneteket engedélyezik. Az ábra egy minta topológiát és lehetséges ACL konfigurációkat mutat be, amelyek lehetővé teszik az egyedi ICMP szolgáltatásokat a G0 / 0 és az S0 / 0/0 interfészeken.



SNMP-kizsákmányolások enyhítése

A kezelési protokollok, például az SNMP, hasznosak a hálózati eszközök távfelügyeletéhez és kezeléséhez. Azonban mégis kihasználhatók. Ha az SNMP szükséges, az SNMP sérülékenységének kihasználása enyhíthető az interfész ACL-ek alkalmazásával az SNMP csomagok nem engedélyezett rendszerekből való szűrésére. Egy kizsákmányolás még mindig lehetséges, ha az SNMP csomag egy olyan címről származik, amelyet hamisított és az ACL engedélyezett.

Ezek a biztonsági intézkedések hasznosak, de a kizsákmányolás leghatékonyabb eszköze az, hogy letiltja az SNMP-kiszolgálót olyan IOS-eszközökön, amelyekre ez nem szükséges. Amint az az ábrán látható, használja a **no snmp-server** parancsot az SNMP letiltására a Cisco IOS eszközökön.



Bevezetés az IPv6 ACL-ekbe

Az utóbbi években számos hálózat elkezdte áttérni egy IPv6 környezetre. Az IPv6-ra való áttérés szükségességének része az IPv4-ben rejlő hiányosságok miatt. Az IPv4-t számos modern napi követelmény nélkül tervezték:

Biztonság - IP-biztonság (IPsec)

Eszköz barangolás - mobil IP

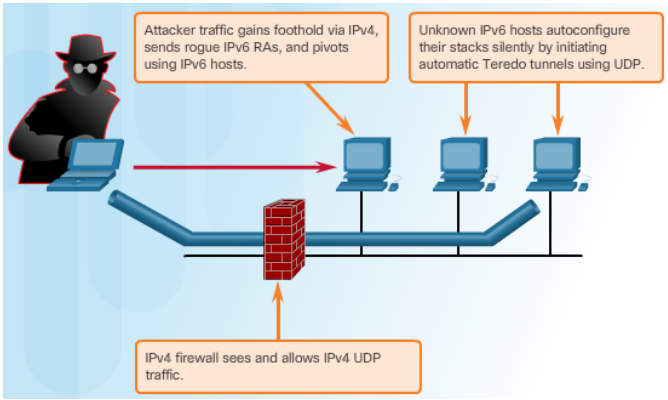
A szolgáltatás minősége - Resource Reservation Protocol (RSVP)

Cím skálázhatóság - DHCP, hálózati címfordítás (NAT), osztály nélküli interdomain útvonal (CIDR), változó hosszúságú alhálózati maszkolás (VLSM)

Sajnos, ahogy az IPv6 migráció folytatódik, az IPv6 támadások egyre terjedőben vannak. Az IPv4 nem fog eltűnni egyik napról a másikra. Az IPv4 együtt fog élni az IPv6-dal, majd fokozatosan helyettesíteni fog az IPv6-lel. Ez potenciális biztonsági lyukakat hoz létre. A biztonsági aggodalomra példa a támadók, akik az IPv4-t kihasználva kihasználják az IPv6-t kettős kötegben. A kettős stack egy olyan integrációs módszer, amelyben egy eszköz mind az IPv4, mind az IPv6 hálózatokon végrehajtást és kapcsolatot biztosít. Ennek eredményeként az eszköz két protokollkészletet tartalmaz.

A támadók olyan lopakodó támadásokat hajthatnak végre, amelyek bizalmi felhasználást eredményeznek a kettős halmozott állomás, a rogue Neighbor Discovery Protocol (NDP) üzenetek és az alagúttechnikák használatával. A Teredo alagút például IPv6 átmeneti technológia, amely automatikus IPv6-címkiosztást biztosít, amikor az IPv4 / IPv6-állomás az IPv4 hálózati címfordítás (NAT) eszközök mögött található. Ezt az IPv6 csomagok IPv4 UDP csomagokon belüli beágyazásával érheti el. A támadó megérzi az IPv4 hálózaton. A kompromittált gazda küld rogue router hirdetéseket, amelyek kettős halmozott állomásokat indítanak IPv6 cím megszerzéséhez. A támadó ezután használhatja ezt a lábat, hogy a hálózaton belül mozogjon vagy elforgatható. A támadó további gazdákat kompromittálhat, mielőtt a forgalmat a hálózaton keresztül visszahívja, amint az az ábrán látható.

Szükséges egy stratégia kidolgozása és végrehajtása az IPv6 infrastruktúrák és protokollok elleni támadások mérséklése érdekében. Ennek az enyhítési stratégiának magában kell foglalnia a szélezést különböző módszerek, például IPv6 ACL-ek használatával.



IPv6 ACL syntaxis

Az IPv6-ban az ACL-funkció hasonló az ACL-hez az IPv4-ben. Az IPv4 szabványos ACL-eknek azonban nincs ekvivalense, és minden IPv6 ACL-t névvel kell konfigurálni. Az IPv6 ACL-ek lehetővé teszik a forrás- és rendeltetési címek alapján történő szűrést, amelyek a bejövő és kimenő útválasztó egy adott felülethez érkeznek. Ugyancsak támogatják az IPv6 opcionális fejlécek és az opcionális, felső szintű protokolltípus-információk alapján a forgalom finom granulárisságára vonatkozó szűrést, hasonlóan az IPv4 kiterjesztett

ACL-ekhez. Az IPv6 ACL konfigurálásához használja az **ipv6 access-list** parancsot, hogy belépjen az IPv6 ACL konfigurációs üzemmódba. Ezután az ábrán látható szintaxist használja az egyes hozzáférési listák bejegyzésének konfigurálásához a forgalom engedélyezéséhez vagy megtagadásához. Adjon IPv6 ACL-t egy interfészhez az **ipv6 traffic-filter** paranccsal.

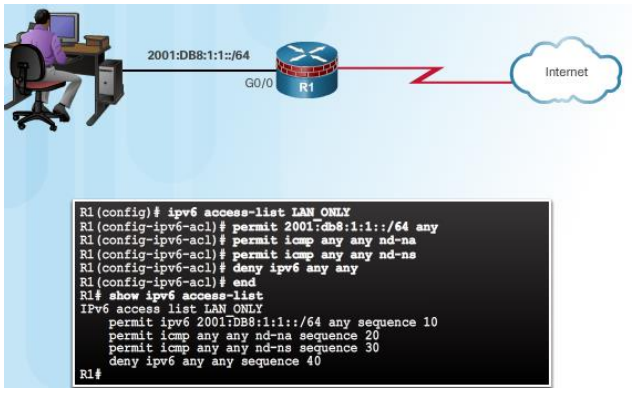
```
R1(config)# ipv6 access-list access-list-name
R1(config-ipv6-acl)# deny | permit protocol {source-ipv6-prefix/prefix-length | any | host
source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length | any |
host destination-ipv6-address} [operator [port-number]]
```

Parameter	Description
deny | **permit**	Specifies whether to deny or permit the packet.
protocol	Enter the name or number of an Internet protocol, or an integer representing an IPv6 protocol number.
source-ipv6-prefix/prefix-length *destination-ipv6-address*	The source or destination IPv6 network or class of networks for which to set deny or permit conditions.
any	Enter **any** as an abbreviation for the IPv6 prefix ::/0. This matches all addresses.
host	For **host** *source-ipv6-address* or *destination-ipv6-address*, enter the source or destination IPv6 host address for which to set deny or permit conditions.
operator	(Optional) An operand that compares the source or destination ports of the specified protocol. Operands are lt (less than), gt (greater than), eq (equal), neq (not equal), and range.
port-number	(Optional) A decimal number or the name of a TCP or UDP port for filtering TCP or UDP, respectively.

IPv6 ACL-ek konfigurálása

Az IPv6 ACL egy implicit **deny ipv6**-ot tartalmaz. Minden IPv6 ACL tartalmaz implicit engedélyszabályokat is, amelyek lehetővé teszik az IPv6 szomszédos felfedezését. Az IPv6 NDP-nek szüksége van az IPv6 hálózati réteg használatára szomszédos hirdetések és szomszédos ajánlatok (NSs) küldésére. Ha egy rendszergazda beállítja a **deny ipv6** bármelyik parancsát anélkül, hogy kifejezetten engedélyezi a szomszédos felfedezést, akkor az NDP letiltásra kerül.

Az ábrán az R1 engedélyezi a bejövő forgalmat G0 / 0-ban a 2001: DB8: 1: 1 :: / 64 hálózatból. Minden NA és NS csomag kifejezetten megengedett. A más IPv6-címről származó forgalmat kifejezetten megtagadják. Ha az adminisztrátor csak az első engedélykibocsátást állította be, az ACL-nek ugyanaz a hatása lesz. Jó gyakorlat azonban az implicit kifejezések dokumentálása azáltal, hogy kifejezetten konfigurálja őket.



Tűzfal meghatározása

A tűzfal fogalma eredetileg tűzálló falnak nevezett, amely általában kőből vagy fémből készült, ami megakadályozta a lángok terjedését a csatlakoztatott szerkezetekbe. Később a tűzfal kifejezést a fémlapra helyezték, amely a jármű vagy a légi jármű motortérét elválasztotta az utastérről. Végül a kifejezés számítógépes hálózatokhoz való alkalmazkodásra lett adaptálva: a tűzfal megakadályozza a nemkívánatos forgalmat a hálózaton belül előírt területek beírásával.

A tűzfalak különbözőek a különböző emberek és szervezetek számára, de az összes tűzfal közös tulajdonságokkal rendelkezik:

A tűzfalak ellenállnak a támadásoknak.

A tűzfalak az egyetlen tranzitpont a hálózatok között, mivel minden forgalom a tűzfalon keresztül áramlik.

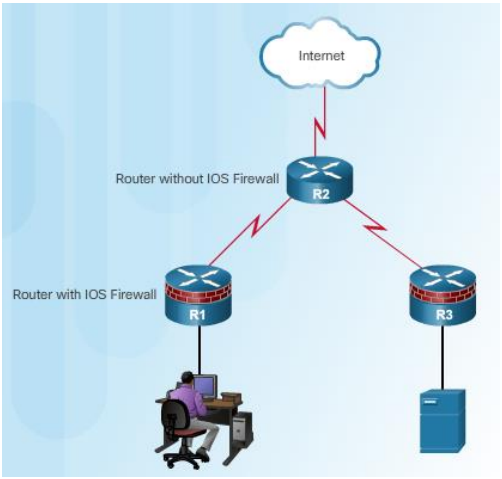
A tűzfalak érvényesítik a beléptetési házirendet.

1988-ban a Digital Equipment Corporation (DEC) létrehozta az első hálózati tűzfalat csomagszűrő tűzfal formájában. Ezek a korai tűzfalak ellenőrzött csomagokat láttak, hogy megfeleltek-e szabálysértéseknek, majd a csomagok továbbítását vagy eldobását választották. Ez a típusú csomagszűrés, azaz hontalan szűrés, függetlenül attól, hogy egy csomag része egy meglévő adatfolyamnak. Minden csomagot csak a csomag fejlécében lévő bizonyos paraméterek alapján szűrjük, ami hasonlít az ACL-ek csomagszűrésére.

1989-ben az AT & T Bell Laboratories kifejlesztette az első állami tűzfalat. A tiltott tűzfalak értékelik az adatfolyamokhoz való kapcsolódások állapotát a szűrőcsomagok számára. Az állapotos tűzfal képes megállapítani, hogy egy csomag létező adatfolyamhoz tartozik-e. A statikus szabályokat, például a csomagszűrő tűzfalakban, dinamikus szabályokkal egészítik ki valós időben, hogy meghatározzák ezeket az aktív áramlatokat. A tiltott tűzfalak segítenek csökkenteni a DoS támadásait, amelyek kihasználják az aktív kapcsolatokat egy hálózati eszközön keresztül.

Az eredeti tűzfalak nem önálló készülékek voltak. Ők voltak útválasztók vagy szerverek, amelyek szoftverfunkciókkal egészítették ki a tűzfal funkcióit. Idővel számos vállalat önálló tűzfalat fejlesztett ki. A dedikált tűzfal eszközök lehetővé tették a routerek és a kapcsolók számára a csomagok szűrésének intenzív és processzor-intenzív tevékenységét. A modern routerek, mint például az integrált szolgáltatás routerek (ISR-k), használhatók olyan kifinomult állapotú tűzfalaknak is, amelyek nem igényelnek dedikált tűzfalat.

A tűzfal olyan rendszer vagy rendszercsoport, amely a hálózatok közötti hozzáférés-vezérlési házirendet érvényesít, amint az az ábrán látható. Tartalmazhat olyan opciókat, mint például a csomagszűrő útválasztó, a két VLAN kapcsoló és több tűzfal-kiszolgáló.



A tűzfalak előnyei és korlátai

A tűzfal használatának számos előnye van egy hálózatban:

Megakadályozhatja az érzékeny gazdaállomások, erőforrások és alkalmazások kitettségét nem megbízható felhasználók számára.

Sanitize protokollfolyamat, amely megakadályozza a protokollhibák kihasználását.

A rosszindulatú adatok blokkolása a szerverekről és az ügyfelekről.

Csökkentse a biztonsági menedzsment bonyolultságát, ha a hálózati hozzáférés ellenőrzésének legtöbb részét a hálózat néhány tűzfalába terhelné.

A tűzfalak is tartalmaznak néhány korlátozást:

A rosszul konfigurált tűzfal komoly következményekkel járhat a hálózathoz, például egyetlen kiesési pontgá válik.

Számos alkalmazás adatai nem védhetők biztonságosan a tűzfalakon keresztül.

A felhasználók proaktív módon keressék meg a tűzfal körül kerülő eszközöket, hogy blokkolt anyagot kapjanak, ami felderíti a hálózatot potenciális támadásra.

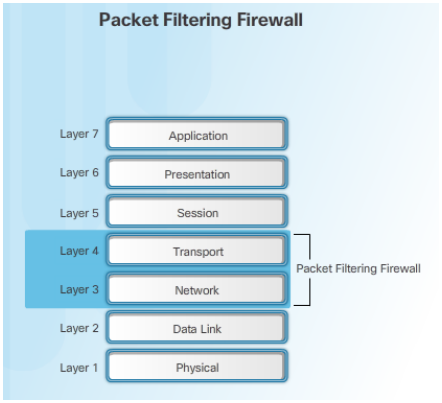
A hálózati teljesítmény lassulhat.

A jogosulatlan forgalom alagutatható vagy elrejthető a tűzfalon keresztül történő törvényes forgalomként.

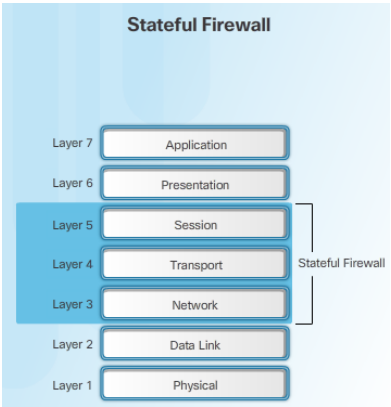
Tűzfal típusok

A tűzfal rendszer számos különböző eszközből és komponensből állhat. Az egyik elem a forgalomszűrés, ami a legtöbb ember általában tűzfalat hív. A következő három tűzfal szerepel ebben a fejezetben:

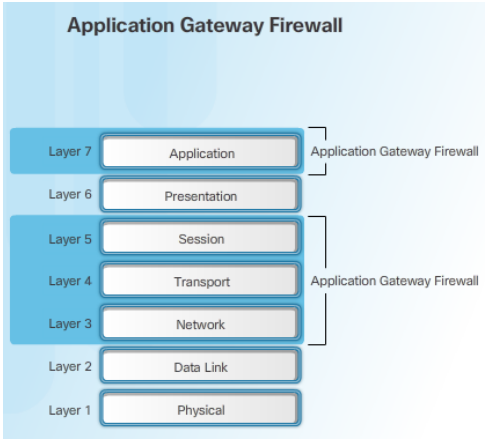
- Csomagszűrő tűzfal - Általában olyan útválasztó, amely képes bizonyos csomagtartalmak szűrésére, mint például a 3. réteg, néha a 4. réteg információi.



- Állapotfigyelő tűzfal - figyelemmel kíséri a kapcsolatok állapotát, függetlenül attól, hogy a kapcsolat egy iniciációban, adatátvitelben vagy befejezési állapotban van-e.



- Alkalmazás rétegbeli tűzfal (proxy tűzfal) - Az OSI referenciamodell 3., 4., 5. és 7. rétegében lévő információk szűrése. A tűzfal vezérlése és szűrése legtöbbször szoftveres. Ha az ügyfélnek hozzáférést kell biztosítania egy távoli kiszolgálóhoz, akkor csatlakozik egy proxykiszolgálóhoz. A proxykiszolgáló az ügyfél nevében kapcsolódik a távoli kiszolgálóhoz. Ezért a kiszolgáló csak egy kapcsolatot lát a proxykiszolgálóról.



A tűzfalak megvalósításának egyéb módjai a következők:

Host-alapú (szerver és személyi) tűzfal - PC vagy szerver tűzfallal működő szoftveren.

Transzparens tűzfal - Az IP-forgalmat áthidaló interfészek között szűrődik.

Hibrid tűzfal - A különböző tűzfal típusok kombinációja. Például egy alkalmazás-ellenőrző tűzfal kombinálja az állapotos tűzfalat egy alkalmazás átjáró tűzfalával.

A csomagszűrő tűzfal előnyei és korlátai

A csomagszűrő tűzfalak általában egy útválasztó tűzfal részét képezik, amely lehetővé teszi vagy megtagadja a forgalmat a 3. réteg és a 4. rétegbeli információk alapján. Ezek olyan hontalan tűzfalak, amelyek egyszerű politikai táblázatot használnak, amely a konkrét kritériumok alapján szűri a forgalmat, amint az az ábrán látható. Például az SMTP-kiszolgálók alapértelmezés szerint a 25. portot hallgatják. A rendszergazda beállíthatja a csomagszűrő tűzfalat, hogy blokkolja a 25. portot egy adott munkaállomásról, hogy megakadályozza az e-mail vírus közvetítését.

A csomagszűrő tűzfal használatának számos előnye van:

A csomagszűrők egyszerűen engedélyezik vagy tiltják a szabálykészleteket.

A csomagszűrők kis mértékben befolyásolják a hálózati teljesítményt.

A csomagszűrők egyszerűen megvalósíthatók, és a legtöbb útválasztó támogatja azokat.

A csomagszűrők biztosítják a kezdeti biztonsági szintet a hálózati rétegben.

A csomagszűrők jóval alacsonyabb költséggel végeznek szinte minden feladatot egy csúcskategóriás tűzfalon.

A csomagszűrők nem jelentenek komplett tűzfal megoldást, ám ezek a tűzfal biztonsági elemei fontos elemei. A csomagszűrő tűzfal használatának számos hátránya van:

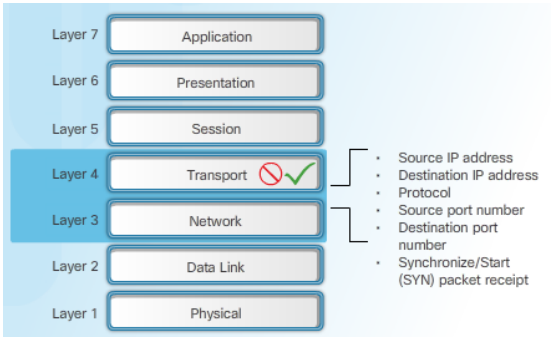
A csomagszűrők érzékenyek az IP spoofelésre. A hackerek tetszőleges csomagokat küldhetnek, amelyek megfelelnek az ACL kritériumoknak, és áthaladnak a szűrőn.

A csomagszűrők nem képesek megbízhatóan szűrni a töredezett csomagokat. Mivel a töredezett IP csomagok hordozzák a TCP fejlécet az első töredékben, és csomagszűrők szűrik a TCP fejléc információit, az összes fragmens az első fragmens után feltétel nélkül átadódik. A csomagszűrők használatára vonatkozó döntések feltételezik, hogy az első töredék szűrője pontosan érvényesíti a házirendet.

A csomagszűrők olyan komplex ACL-eket használnak, amelyeket nehéz megvalósítani és karbantartani.

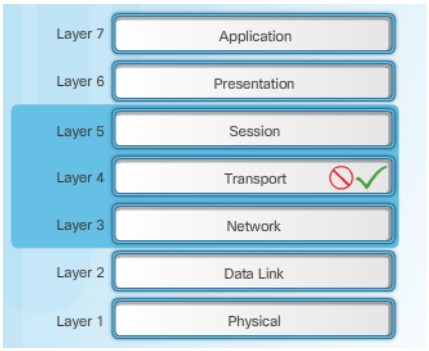
A csomagszűrők nem tudják dinamikusan szűrni bizonyos szolgáltatásokat. Például a dinamikus port-tárgyalásokat használó munkamenetek nehezen szűrhetők, anélkül, hogy a portok teljes skálájához hozzáférést nyitnának.

A csomagszűrők hontalanok. Minden egyes csomagot külön-külön vizsgálnak, nem pedig egy kapcsolat állapotában.

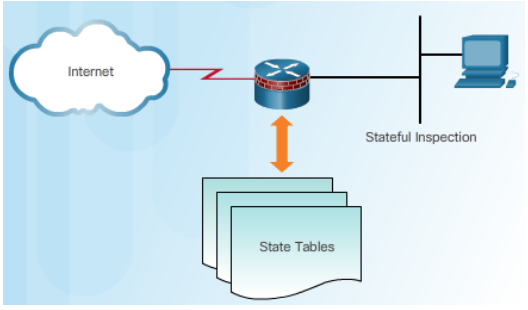


Állapotfigyelő tűzfalak

Az állapotfigyelő tűzfalak a legváltozatosabb és leggyakoribb tűzfaltechnológiák. A tiltott tűzfalak statikus csomagszűrést biztosítanak az állami táblában tárolt kapcsolati információk felhasználásával. A tiltott szűrés olyan tűzfal-architektúra, amely a hálózati rétegbe van besorolva. Azt is elemzi a forgalmat az OSI 4. rétegben és az 5. rétegben.

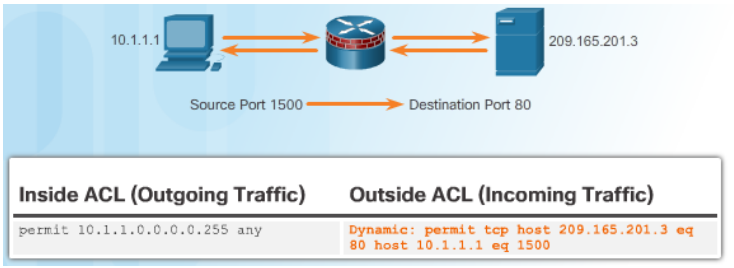


A statikus csomagszűrést használó, hontalan tűzfalaktól eltérően az állapotfüggetlen szűrés nyomon követi a tűzfal összes felületét átlépő valamennyi kapcsolatot, és megerősíti, hogy azok érvényesek. A tiltott tűzfalak egy állami táblát használnak a tényleges kommunikációs folyamat nyomon követésére. A tűzfal az információkat a 3. rétegbeli csomagok és a 4. rétegbeli szegmens fejlécében vizsgálja. A tűzfal például a TCP fejlécet a szinkronizálásra (SYN), az alaphelyzetbe állításra (RST), a visszaigazolásra (ACK), a befejezésre (FIN) és más vezérlő kódokra nézve meghatározza a kapcsolat állapotát.



Minden alkalommal, amikor a bejövő vagy a kimenő kapcsolatokhoz TCP vagy UDP kapcsolatot hoz létre, az állapotos tűzfal naplózza az adatokat egy adott táblázatban az adott adatfolyamhoz. Például a képen a 10.1.1.1 gazda weboldalt kér a kiszolgálótól 209.165.201.3 cím alatt. Az állapotfüggetlen csomagszűrő tűzfal megőrzi bizonyos részleteket azáltal, hogy megmenti a kérés állapotát az állami táblában. Ebben a példában

a router dinamikusan hozzáadta a 209.165.201.3 kiszolgálótól, a 80-as porton lévő, és a 1500-as porton lévő 10.1.1.1 kiszolgálóra szánt 209.165.201.3 kiszolgálóhoz tartozó beléptetési vezérlő bejegyzést.



Megjegyzés: Ez az, ahogyan az IOS tűzfal korábbi verziói végrehajtották az állapotos viselkedést. Az újabb Cisco IOS tűzfal implementációk a fejezetben később tárgyalt zónaalapú megközelítést alkalmazzák.

Az állapotfigyelő tűzfalak előnyei és hátrányai

Számos előnnyel jár, ha egy hálózati tűzfalakat használ:

Az állami tűzfalakat gyakran használják elsődleges védelmi eszközként a nemkívánatos, felesleges vagy nemkívánatos forgalom szűrésével.

Az állami tűzfalak megerősítik a csomagszűrést, mivel szigorúbb védelmet biztosítanak a biztonság érdekében.

A tiltott tűzfalak javítják a teljesítményt a csomagszűrőkön vagy proxykiszolgálókon.

A tiltott tűzfalak védekeznek a hamisítás és a DoS támadások ellen annak meghatározásával, hogy a csomagok egy meglévő kapcsolathoz tartoznak-e vagy nem engedélyezett forrásból származnak-e.

A tiltott tűzfalak több naplózési információt nyújtanak, mint a csomagszűrő tűzfal.

A tiltott tűzfalak szintén korlátozásokat tartalmaznak:

A tiltott tűzfalak nem akadályozhatják az alkalmazásréteg támadásait, mert nem vizsgálják a HTTP kapcsolat tényleges tartalmát.

Nem minden protokoll állapít meg. Például, az UDP és az ICMP nem hoz létre kapcsolati adatokat egy állami tábla számára, és ezért nem szerez be annyi támogatást a szűréshez.

Nehéz nyomon követni azokat a kapcsolatokat, amelyek dinamikus kikötői tárgyalásokat használnak. Egyes alkalmazások több kapcsolatot nyitnak meg. Ehhez egy teljesen új portkészlet szükséges, amelyet meg kell nyitni ahhoz, hogy ez a második kapcsolat.

A tiltott tűzfalak nem támogatják a felhasználói hitelesítést.

Benefits	Limitations
Primary means of defense	No Application Layer inspection
Strong packet filtering	Limited tracking of stateless protocols
Improved performance over packet filters	Difficult to defend against dynamic port negotiation
Defends against spoofing and DoS attacks	No authentication support
Richer data log	

Következő generációs tűzfalak

A következő generációs tűzfal több fontos tényezőn túlmutat az állapotos tűzfalon:

Az alkalmazáson belüli granuláris azonosítás, láthatóság és viselkedésvezérlés

A webes és webes alkalmazások korlátozása a webhely jó hírneve alapján

Proaktív védelem az internetes fenyegetések ellen

A felhasználó, eszköz, szerepkör, alkalmazástípus és fenyegetésprofil alapú irányelvek végrehajtása

A NAT, a VPN és a statikus protokoll-ellenőrzés (SPI) teljesítménye

Integrált behatolásvédelmi rendszer (IPS) használata

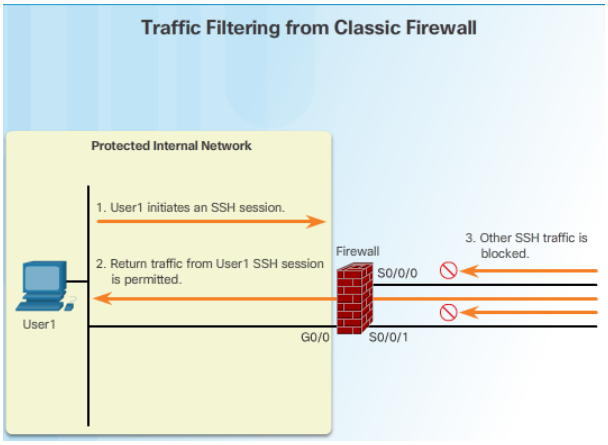
2014 augusztusában a Cisco bejelentette a Sourcefire FirePOWER szolgáltatásainak integrálását a Cisco Adaptive Security Appliance (ASA) rendszerbe. A Cisco ASA és a FirePOWER szolgáltatásokat a Cisco ASA Next-Generation tűzfalának is nevezik, mivel adaptív, fenyegetésközpontú tűzfal. Úgy tervezték, hogy védelmet nyújtson az egész támadási kontinuumban, amely magában foglalja a támadások előtt, alatt és után is.

A klasszikus tűzfal bemutatása

A Cisco IOS Classic tűzfal, amely korábbi nevén környezetalapú hozzáférés-vezérlés (CBAC), a Cisco IOS 12.0-as verziója előtt hozzáadott állapotfájl-tűzfal funkció. A Classic Firewall négy fő funkciót kínál: a forgalomszűrés (az ábrán látható), a forgalom ellenőrzése, a behatolásérzékelés és az ellenőrzések és figyelmeztetések generálása. A Classic Firewall a beágyazott NAT és Port Address Translation (PAT) információkat támogató kapcsolatokat is megvizsgálhatja, és elvégezheti a szükséges címfordítást. A klasszikus tűzfal blokkolja a P2P (peer-to-peer) kapcsolatokat, például a Gnutella és KaZaA alkalmazások által használt eszközöket. Az azonnali üzenetküldési forgalom, például a Yahoo !, AOL és az MSN blokkolható.

A Classic Firewall azonban csak a rendszergazda által meghatározott protokollok szűrését biztosítja. Ha egy protokoll nincs megadva, a meglévő ACL-k meghatározzák, hogy miként szűri meg ezt a protokollt, és nem hoz létre ideiglenes megnyitást. Ezenkívül a Classic Firewall csak a tűzfalon áthaladó támadások felderítését és védelmét szolgálja. Általában nem védi meg a védett hálózatból származó támadások ellen, kivéve, ha a forgalom belső routeren keresztül érkezik a Cisco IOS tűzfal engedélyezve.

A Cisco IOS Software Classic Firewall továbbra is fennmarad a belátható jövőben, de nem fog jelentősen bővíteni az új funkciókat. Ehelyett a Cisco IOS szoftver állapotfelmérési tűzfalának stratégiai fejlesztési irányát a zóna-alapú tűzfal (ZPF) hajtja végre.



Klasszikus tűzfal üzemeltetés

A Classic Firewall ideiglenes megnyitásokat hoz létre az ACL-ben, hogy lehetővé tegye a visszatérő forgalom engedélyezését. Ezek a bejegyzések úgy jönnek létre, hogy ellenőrzött forgalom elhagyja a hálózatot, és eltávolításra kerülnek, amikor a kapcsolat megszakad, vagy a kapcsolat alapjárati időtúllépési ideje elérik.

Tegyük fel például, hogy a felhasználó kezdeményez egy kimenő SSH kapcsolatot egy védett hálózatról egy külső hálózatra, és a Classic Firewall lehetővé teszi az SSH forgalom ellenőrzését. Tételezzük fel továbbá, hogy a külső interfészen egy ACL-t alkalmaznak, amely megakadályozza, hogy az SSH forgalom a védett hálózatba lépjen. Ez a kapcsolat egy többszörös műveleten megy keresztül, amely ideiglenes megnyitást hoz létre a tűzfalon, amint az az ábrán látható:

1. Amikor a forgalom először létrejön és átmegy az útválasztón, a bejövő ACL feldolgozása megtörténik. Ha az ACL tagadja ezt a kapcsolatot, akkor a csomagot le kell dobni. Ha az ACL lehetővé teszi a kapcsolatot, a Classic Firewall ellenőrzési szabályokat vizsgálják.

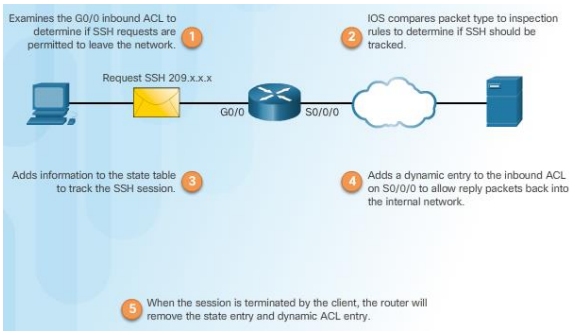
2. A Classic Firewall ellenőrzési szabályai alapján a Cisco IOS szoftver ellenőrizheti a kapcsolatot. Ha az SSH forgalom nem ellenőrzött, akkor a csomag engedélyezett, és nem gyűjtenek más adatokat. Ellenkező esetben a kapcsolat a következő lépéshez vezet.

3. A csatlakozási információkat összehasonlítjuk az állami táblában szereplő bejegyzésekkel. Ha a kapcsolat jelenleg nem létezik, a bejegyzés hozzáadásra kerül. Ha létezik, a kapcsolat alapjárati időzítője visszaáll.

4. Ha új bejegyzést ad hozzá, akkor egy dinamikus ACL bejegyzést adnak hozzá, hogy az ugyanazon SSH-kapcsolat részét képező SSH-forgalom visszatérő legyen. Ez az ideiglenes nyitás csak addig aktív, amíg a munkamenet nyitva van. Ezek a dinamikus ACL bejegyzések nem mentve az NVRAM-ba.

5. Amikor a munkamenet befejeződik, az állapot táblázatból és a dinamikus ACL bejegyzésből származó dinamikus információ eltávolításra kerül.

A klasszikus tűzfal úgy is konfigurálható, hogy két irányba ellenőrizze a forgalmat: be és ki. Ez akkor hasznos, ha megvédi a hálózat két részének védelmét, ahol mindkét fél bizonyos kapcsolatokat kezdeményez, és lehetővé teszi, hogy a visszatérő forgalom elérje a forrását.



Klasszikus tűzfalbeállítás

Tekintsük az ábrán látható topológiát. A rendszergazda engedélyezi az SSH munkameneteket a 10.0.0.0 és a 172.30.0.0 hálózatok között. Azonban csak a 10.0.0.0 hálózatból érkező gazda engedélyezi az SSH munkamenetek kezdeményezését. Minden egyéb hozzáférést megtagad. Négy lépésben állíthatja be ezt a házirendet Classic tűzfal használatával.

1. lépés: Válassza ki a belső és külső interfészeket.

Ebben a példában a G0 / 0 a belső felület és a G0 / 1 a külső felület.

2. lépés: Állítsa be az ACL-eket minden egyes interfészhez.

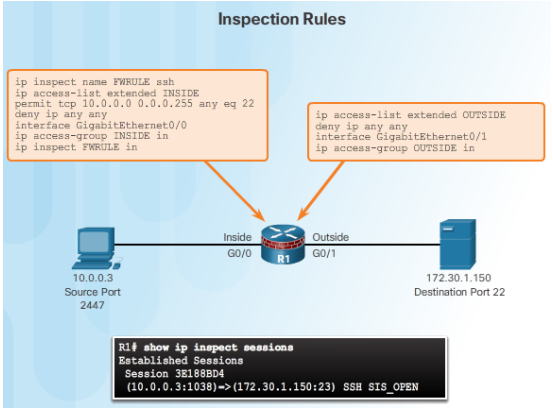
Az INSIDE ACL csak SSH forgalom engedélyezését teszi lehetővé a 10.0.0.0 hálózatból. A G0 / 0 interfészre vonatkozik. Amíg az ellenőrzési szabály nincs beállítva, az OUTSIDE ACL megtagadja a bejövő forgalmat a 172.30.0.0 hálózatból. A G0 / 1 interfészre vonatkozik.

3. lépés: Határozza meg az ellenőrzési szabályokat.

Az FWRULE ellenőrzési szabály meghatározza, hogy a forgalom ellenőrizni fogják az SSH kapcsolatokat. Ez az ellenőrzési szabálynak nincs hatása addig, amíg egy felületre nem kerül. Annak ellenére, hogy az SSH kapcsolat engedélyezett a G0 / 0 interfészen, és a 172.30.0.0 hálózaton fog működni, az SSH forgalom G0 / 1-be való beérkezése továbbra is megtagadható.

4. lépés: Ellenőrzési szabály alkalmazása egy interfészre.

Ha a FWRULE-t a bejövő forgalomra a G0 / 0 interfészen alkalmazzák, a Classic Firewall konfiguráció dinamikusan hozzáad egy bejegyzést, amely lehetővé teszi a bejövő SSH forgalom megteremtését a két gép között. Ez ellenőrizhető a show ip vizsgálati sessions paranccsal.

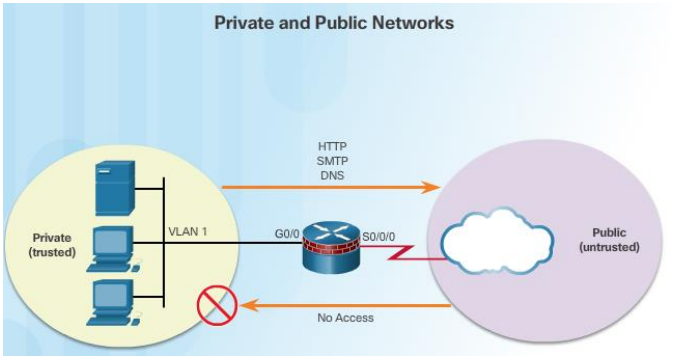


Külső és belső hálózatok

A tűzfal tervezése elsősorban olyan eszközök interfészeiről szól, amelyek lehetővé teszik vagy megtagadják a forgalmat a forrás, a cél és a forgalom típusától függően. Egyes tervezések olyan egyszerűek, mint a külső hálózat és a belső hálózat kijelölése, amelyeket két tűzfalon lévő interfész határoz meg. Amint az ábrán látható, a nyilvános hálózat (vagy a külső hálózat) nem megbízható, és a privát hálózat (vagy belső hálózat) megbízható. Jellemzően egy két interfésszel rendelkező tűzfal a következőképpen konfigurálható:

A magánhálózatból származó forgalom engedélyezett és ellenőrzött, mivel a közhálózat felé halad. Engedélyezett a nyilvános hálózatból visszatérő és a magánhálózattól származó forgalomhoz kapcsolódó ellenőrzött forgalom.

A nyilvános hálózatból származó és a magánhálózathoz való közlekedés általában tiltott.



Demilitarizált Zónák

A demilitarizált zóna (DMZ) egy tűzfal kialakítás, ahol jellemzően egy belső interfész csatlakozik a magánhálózathoz, egy nyilvános hálózathoz csatlakozó külső interfész és egy DMZ interfész, amint az az ábrán látható.

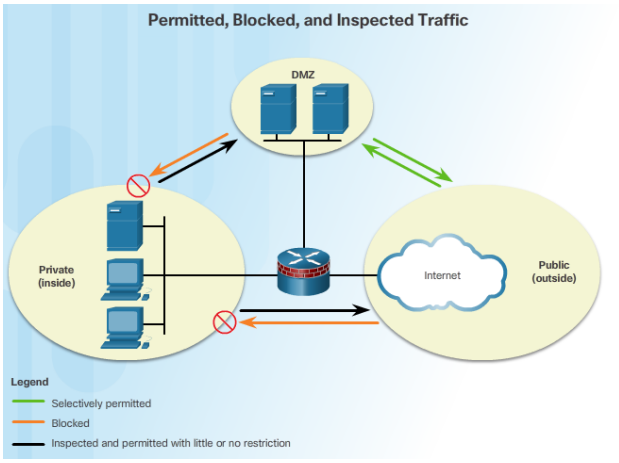
A magánhálózatból származó forgalom ellenőrzése a nyilvános vagy a DMZ hálózat felé halad. Ez a forgalom korlátozott vagy kevéssé korlátozható. A DMZ-től vagy a nyilvános hálózattól a magánhálózathoz visszatérő ellenőrzött forgalom engedélyezett.

A DMZ hálózatból érkező forgalom és a magánhálózaton való utazás általában blokkolva van.

A DMZ-hálózatból származó és a nyilvános hálózathoz közlekedő forgalom szelektíven engedélyezett a szolgáltatási követelmények alapján.

A nyilvános hálózatból származó és a DMZ felé közlekedő forgalom szelektíven engedélyezett és ellenőrzött. Ez a típusú forgalom jellemzően e-mail, DNS, HTTP vagy HTTPS forgalom. Dinamikusan engedélyezik a DMZ és a nyilvános hálózat forgalmának visszaforgatását.

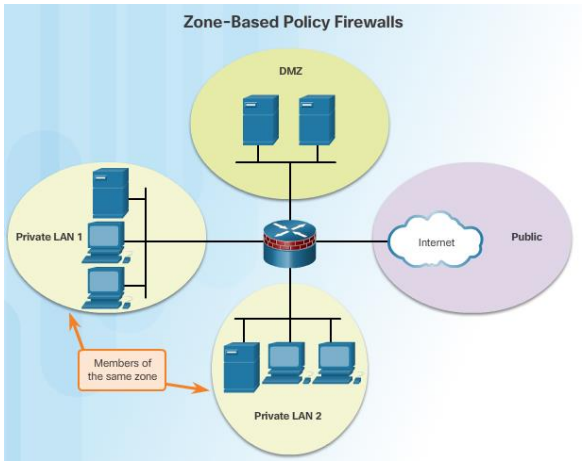
A nyilvános hálózatból érkező és a magánhálózaton közlekedő forgalom blokkolva van.



ZPF-ek

A ZPF-ek a zónák fogalmát használják további rugalmasság biztosítására. A zóna egy vagy több interfész csoportja, amelyek hasonló funkciókat vagy jellemzőket tartalmaznak. A Zónák segítenek megadni, hogy hol legyen a Cisco IOS tűzfal alkalmazása. Az ábrán a LAN 1 és a LAN 2 biztonsági szabályai hasonlóak, és tűzfal-konfigurációk zónájaként csoportosíthatók. Alapértelmezés szerint az ugyanazon zónában lévő kapcsolódási pontok közötti forgalom nem tartozik szabályzathoz és szabadon halad. Azonban minden zóna-zónás forgalom blokkolva van. Annak érdekében, hogy lehetővé tegye a zónák közötti forgalmat, a forgalmat engedélyező vagy ellenőrző irányelveket kell beállítani.

Az egyetlen kivétel ez alól az alapértelmezettől megtilt minden házirendet az útválasztó saját zónája. Az önzónák maguk a routerek, és magukban foglalják az összes router interfész IP címét. Az önzónát magában foglaló házirend-konfigurációk a forgalomirányítóra szánt forgalomra vonatkoznak és azokról származnak. Alapértelmezés szerint az ilyen típusú forgalomra nincs irányelv. Az önzónákra vonatkozó irányelvek kidolgozása során figyelembe veendő forgalom magában foglalja az irányítási síkot és az irányítószámos forgalmat, például az SSH-t, az SNMP-t és az útválasztási protokollokat.



Réteges védelem

A réteges védelem különböző típusú tűzfalakat használ, amelyek rétegekben vannak kombinálva, hogy mélyebbre növelhessék a szervezet biztonságát. További információkért kattintson az 1. ábra minden egyes rétegére. A rétegek és a rétegek között érvényesíthetők a házirendek. Ezek az irányelvek végrehajtási pontjai meghatározzák, hogy a forgalom továbbításra vagy eldobásra kerül-e. Például a nem megbízható hálózatból érkező forgalom először találkozik egy csomagszűrővel az élű útválasztón. Ha a házirend megengedi, a forgalom megy át a védett tűzfal vagy bástyás gazda rendszerhez, amely több szabályt alkalmaz a forgalomra és elvetette a gyanús csomagokat. A bástya fogadó egy edzett számítógép, amely jellemzően a DMZ-ben van. Ezután a forgalom egy belső szűrő útválasztóhoz vezet. A forgalom a belső célállomásra csak akkor kerül át, ha sikeresen átadta az összes végrehajtási pontot a külső forgalomirányító és a belső hálózat között. Ezt a fajta DMZ beállítást szűrő alhálózati konfigurációnak nevezik.

A réteges védelmi megközelítés nem minden, ami a biztonságos belső hálózat biztosításához szükséges. A hálózati rendszergazdának számos tényezőt kell figyelembe vennie egy teljes mélyreható védelem megalkotásakor:

A tűzfalak általában nem akadályozzák meg a hálózaton vagy zónán belüli házigazdákból származó behatolást.

A tűzfalak nem védenek a gazember hozzáférési pontok telepítése ellen.

A tűzfalak nem helyettesítik a támadás vagy a hardverhiba következtében fellépő mentési és katasztrófa-helyreállítási mechanizmusokat.

A tűzfalak nem helyettesíthetik a tájékozott adminisztrátorokat és felhasználókat.

Az ábrán bemutatott legjobb gyakorlatok részleges listája kiindulópontként szolgálhat egy tűzfal biztonsági házirendhez.

A ZPF előnyei

A Cisco IOS tűzfal két konfigurációs modellje létezik:

Klasszikus tűzfal - A hagyományos konfigurációs modell, amelyben a tűzfal házirendjét a felületeken alkalmazzák.

ZPF - Az új konfigurációs mód, amelyben a kapcsolódási pontok a biztonsági zónákhoz vannak hozzárendelve, és a zónák közötti forgalomra a tűzfalra vonatkozó szabályokat alkalmazzák.

Amint az az ábrán látható, ha egy privát zónához további interfészt adunk hozzá, a privát zóna új kezelőfelületéhez csatlakoztatott gazdák át tudják adni a forgalmat az ugyanazon a zónán lévő meglévő felületen lévő összes gazda számára.

A hálózatbiztonsági szakemberek ZPF-modellre való áttérésének elsődleges oka a szerkezet és a könnyű használat. A strukturált megközelítés hasznos a dokumentációhoz és a kommunikációhoz. A könnyű használat miatt a hálózatbiztonsági implementációk elérhetőbbek a biztonsági szakemberek nagyobb közösségéhez.

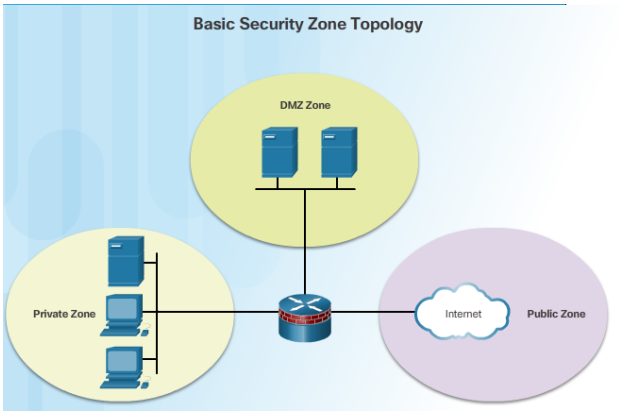
A ZPF számos előnye van:

Nem függ az ACL-ektől.

Az útválasztó biztonsági pozíciója tilos, kivéve, ha kifejezetten engedélyezett.

A házirendeket könnyű olvashatóság és hibaelhárítás a Cisco Common Classification Policy Language (C3PL) segítségével. A C3PL strukturált módszer az események, feltételek és műveletek alapján létrehozott forgalmi irányelvek létrehozására. A skálázhatóságot biztosítja, ha egy szabályzat befolyásolja az adott forgalmat, ahelyett, hogy több ACL-t és ellenőrzési műveletet igényelne.

A klasszikus tűzfal vagy ZPF végrehajtásakor fontos megjegyezni, hogy mindkét konfigurációs modell egyidejűleg engedélyezhető egy útválasztón. A modelleket azonban nem lehet egyetlen felületen kombinálni. Például egy interfész nem konfigurálható egyszerre biztonsági zóna tagként és IP-ellenőrzés céljából.



ZPF tervezés

A közös ZPF tervek LAN-to-Internet, amint az az 1. ábrán látható. A 2. és a 3. ábrán látható a nyilvános szerverekkel ellátott tűzfal. A 4. ábrán redundáns tűzfalak láthatók. A komplex tűzfalak az 5. ábrán láthatók.

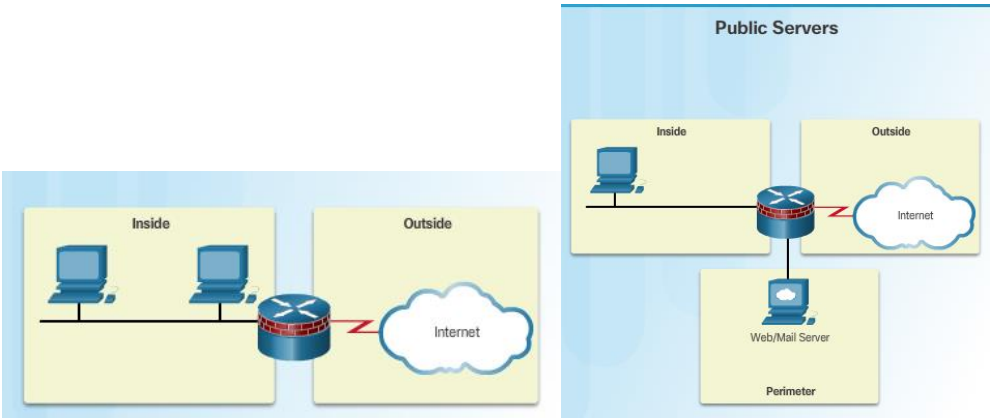
A ZPF-k tervezése számos lépést tartalmaz:

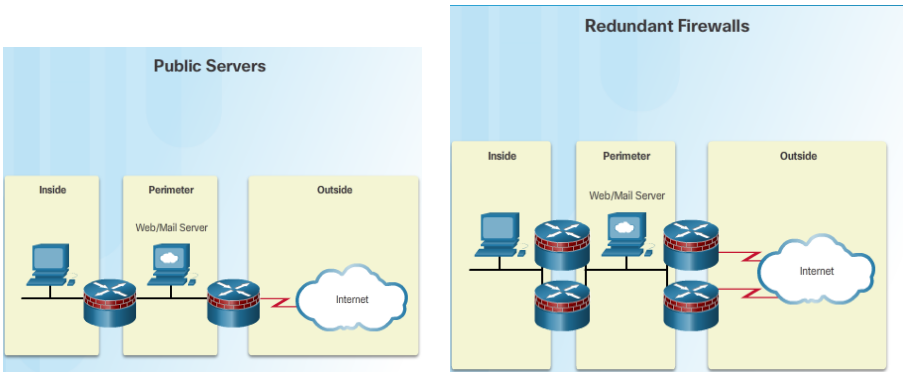
1. lépés. Határozza meg a zónákat - Az adminisztrátor a hálózat zónákra való szétválasztására összpontosít. Például a nyilvános hálózat egy zóna lenne, és a belső hálózat egy másik zóna lenne.

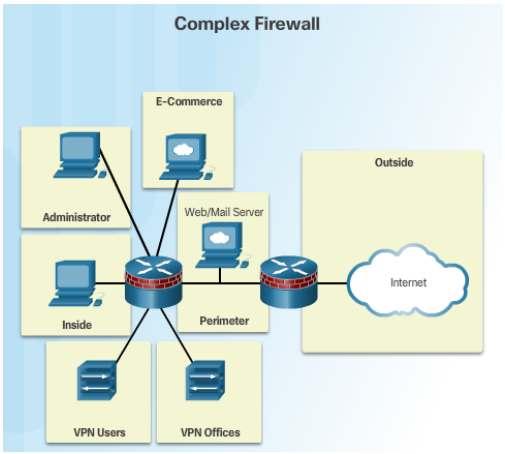
2. lépés: Zónák közötti házirendek létrehozása - Minden "forrás-cél" zónához (például a belső hálózattól a külső internethez) hozzon létre olyan munkameneteket, amelyeket a forrászónákban a célzónákban lévő kiszolgálók kérhetnek. Ezek a munkamenetek leggyakrabban TCP és UDP munkamenetek, de lehetnek ICMP-munkamenetek is, például ICMP echo. Az olyan forgalom esetében, amely nem a munkamenetek fogalmán alapul, a rendszergazdanak egyirányú forgalmi forrást kell meghatároznia a forrásról a célra, és fordítva.

3. lépés: Tervezze meg a fizikai infrastruktúrát - Miután a zónákat azonosították, és a közlekedési követelmények dokumentáltak, az adminisztrátornak meg kell terveznie a fizikai infrastruktúrát. Az adminisztrátornak figyelembe kell vennie a biztonsági és rendelkezésre állási követelményeket a fizikai infrastruktúra megtervezésekor. Ez magában foglalja az eszközök számának a legmegbízhatóbb és legkevésbé biztonságos zónák közötti meghatározását és a redundáns eszközök meghatározását.

4. lépés: A zónákon belüli részegységek azonosítása és a forgalmi követelmények összevonása - Az egyes tűzfal eszközön belül a rendszergazda azonosítja az interfészekhez kapcsolódó zónasorokat, és egyesíti a zónák forgalmi követelményeit. Például több zóna közvetve csatlakozhat egy tűzfal egyetlen felületéhez. Ez egy eszköz-specifikus interzone politikát eredményezne. Bár fontos szempont, a végrehajtó övezetek alcsoportjai túlmutatnak a tanterv területén.







ZPF műveletek

A Cisco IOS ZPF három lehetséges lépést tehet:

Inspect - Cisco IOS állapotfelmérő csomagellenőrzést hajt végre.

Drop - Hasonlóan egy ACL-ben szereplő tiltó nyilatkozathoz. Egy napló opció áll rendelkezésre az elutasított csomagok naplózására.

Pass - Hasonlóan egy engedélyezési nyilatkozathoz egy ACL-ben. A lépés művelet nem követi a forgalomban lévő kapcsolatok vagy munkamenetek állapotát.

A tranzitforgalom szabályai

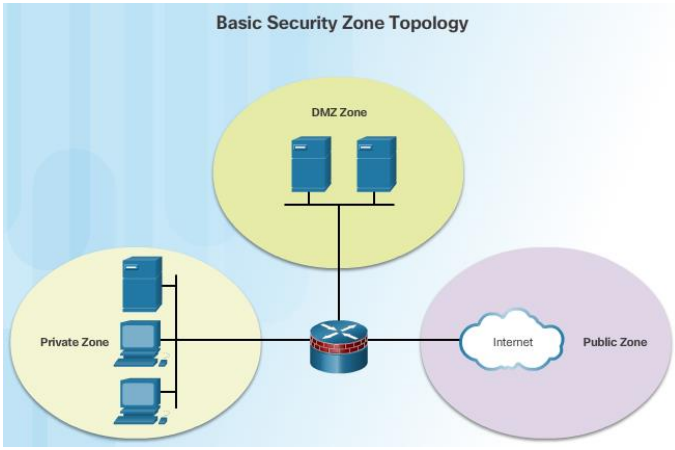
Az útválasztó interfészeken átmenő forgalmat számos, az interfész viselkedését szabályozó szabály vonatkozik. Az átmenő forgalom példája az 1. ábrán látható topológiára vonatkozik. A szabályok attól függnek, hogy a be- és kimeneti interfészek ugyanabban a zónában vannak-e, mint a 2. ábrán látható:

Ha egyik felület sem a zóna tagja, akkor a kapott művelet a forgalom átadását eredményezi.

Ha mindkét interfész ugyanazon a zónán belül van, akkor az így létrejövő művelet a forgalom átadását eredményezi.

Ha egy felület egy zónaelem, de a másik nem, akkor az eredményes művelet a forgalmat leállítja függetlenül attól, hogy létezik-e zónapár.

Ha mindkét interfész ugyanarra a zónapárra és egy házirendre vonatkozik, akkor a követendő művelet a házirend által meghatározott módon ellenőrzi, engedélyezi vagy letiltja.

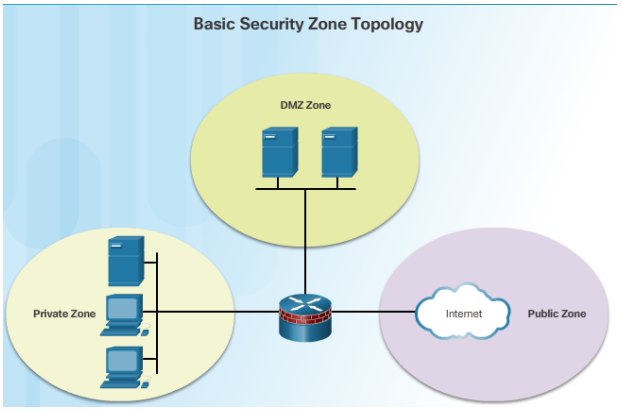


Transit Traffic: Pass, Drop or Inspect?

Source Interface Member of Zone?	Destination Interface Member of Zone?	Zone-Pair Exists?	Policy Exists?	Result
NO	NO	N/A	N/A	PASS
YES	NO	N/A	N/A	DROP
NO	YES	N/A	N/A	DROP
YES (private)	YES (private)	N/A	N/A	PASS
YES (private)	YES (public)	NO	N/A	DROP
YES (private)	YES (public)	YES	NO	PASS
YES (private)	YES (public)	YES	YES	INSPECT

A saját zónák forgalmának szabályai

Az sajátzónák maguk a routerek, és magukban foglalják az útválasztó interfészekhez rendelt összes IP-címet. A ZPF szabályai eltérnek az önzónában. Az önzónás forgalmi példáját lásd:



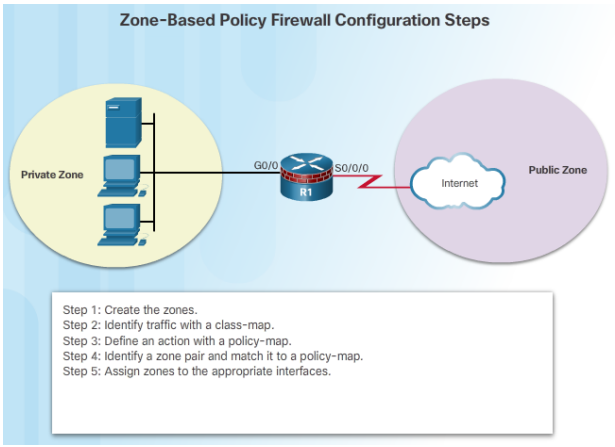
A szabályok attól függnek, hogy az útválasztó a forgalom forrása vagy rendeltetési helye. Ha az útválasztó a forrás vagy a célállomás, akkor az összes forgalom engedélyezett. Az egyetlen kivétel, ha a forrás és a cél egy olyan zónapár, amely egy adott szolgáltatási irányelvvel rendelkezik. Ebben az esetben a házirend érvényes az összes forgalomra.

Self Zone Traffic: Pass, Drop or Inspect?

Source Interface Member of Zone?	Destination Interface Member of Zone?	Zone-Pair Exists?	Policy Exists?	Result
YES (self zone)	YES	NO	N/A	PASS
YES (self zone)	YES	YES	NO	PASS
YES (self zone)	YES	YES	YES	INSPECT
YES	YES (self zone)	NO	N/A	PASS
YES	YES (self zone)	YES	NO	PASS
YES	YES (self zone)	YES	YES	INSPECT

ZPF beállítása

Az ábrán látható topológia és lépések a továbbiakban a ZPF konfigurációjának bemutatására használatosak. A lépések sorrendje nem szükséges. Bizonyos konfigurációkat azonban sorrendben kell elvégezni. Például egy osztály-térképet kell beállítania, mielőtt hozzárendelne egy osztály-térképet egy irányelv-térképhez. Hasonlóképpen nem rendelhet hozzá egy irányelvcsomagot zópartihoz, amíg nem állította be a házirendet. Ha megpróbál konfigurálni egy olyan részt, amely a konfiguráció egy másik részére támaszkodik, még nem konfigurálva, az útválasztó hibaüzenettel válaszol.



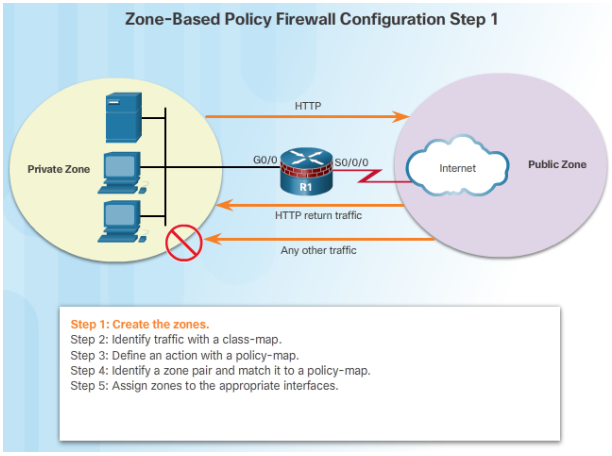
Zónák létrehozása

Az első lépés a zónák létrehozása. Azonban a zónák létrehozása előtt válaszoljon néhány kérdésre:

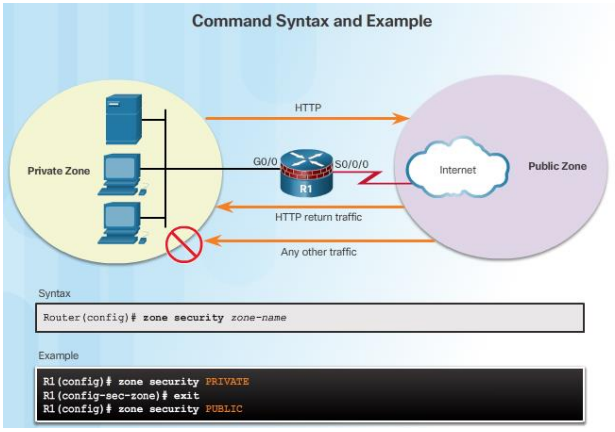
Milyen interfészeket kell bevonni a zónákba?

Mi lesz az egyes zónák neve?

Milyen forgalom szükséges a zónák között és milyen irányban?

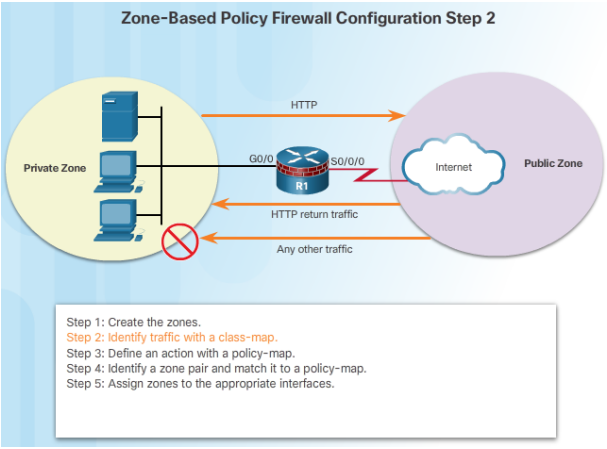


A példa topológiájában két interfésszel, két zónával és egy irányban haladva közlekedünk. A nyilvános övezetből származó forgalom nem engedélyezett. Hozzon létre zónákat a tűzfalhoz a zóna biztonsági parancs segítségével.

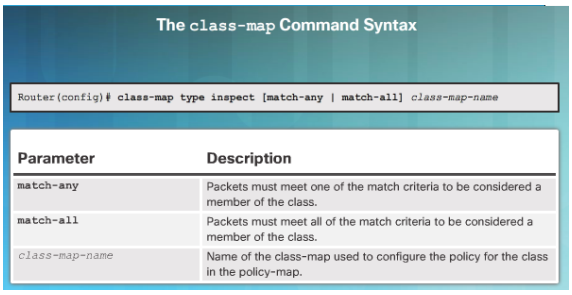


A forgalom azonosítása

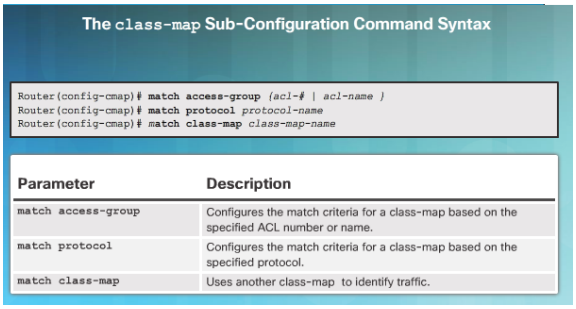
A második lépés az osztály-térkép használata a forgalom azonosításához. Az osztály a csomagok egy sor azonosításának egyik módja annak tartalmán alapuló "match" feltételek mellett. Általában egy olyan osztályt definiál, amely lehetővé teheti, hogy egy tevékenységet alkalmazzon az azonosított forgalomra, amely tükrözi a házirendet. Egy osztály osztálytérképekkel van meghatározva.



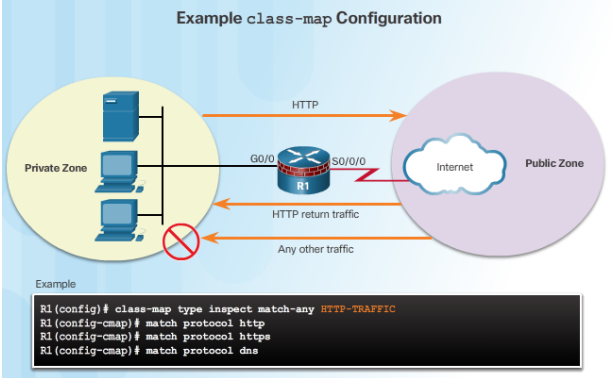
A 2. ábra az osztály-térkép parancs szintaxisa. Számos osztálytérkép létezik. A ZPF konfigurációhoz használja az ellenőrző kulcsszót egy osztály-térkép meghatározásához. Határozza meg, miként értékelik a csomagok értékét, ha több egyezési kritérium létezik. A csomagoknak meg kell felelniük az egyezési kritériumnak (a mérkőzés bármelyikének) vagy az összes egyezési kritériumnak (match-all), hogy az osztály tagja legyen.



A 3. ábra az osztály-térkép alkonfigurációs üzemmódban a meccsnyilatkozatok szintaxisát mutatja. Egy ACL-re, egy konkrét protokollra vagy akár egy másik osztály-térképre vonatkozó forgalom egyeztetése.



A 4. ábrán bemutatott topológiában a HTTP forgalom megengedhető, hogy átkerül az R1-re a PUBLIC zónára. HTTP-forgalom engedélyezésekor ajánlatos kifejezetten HTTPS és DNS protokollokat is tartalmazni. A forgalom a HTTP-TRAFFIC osztály tagjává válik.



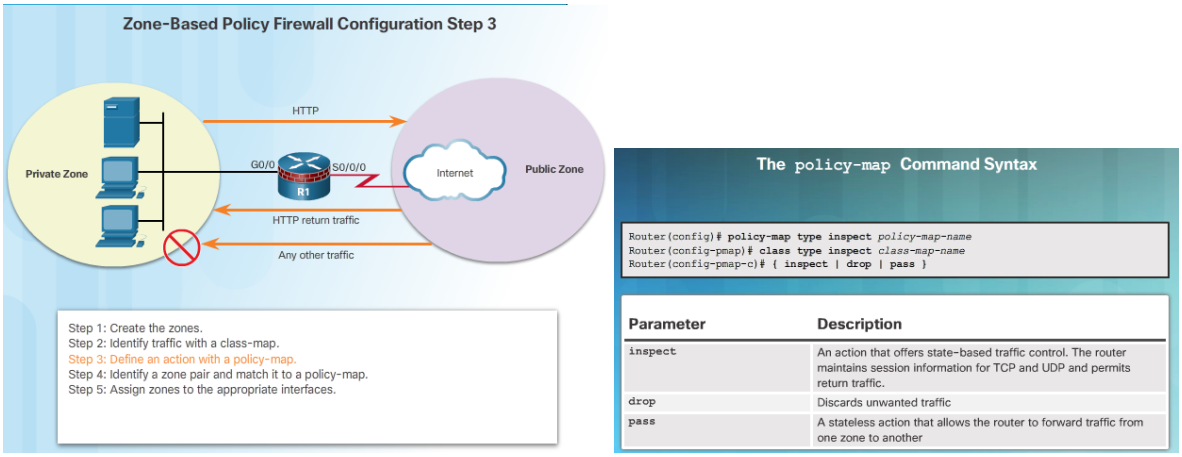
Egy cselekvés meghatározása

A harmadik lépés, amint az az 1. ábrán látható, egy politikai térképet használ annak meghatározására, hogy milyen lépéseket kell tenni az osztályhoz tartozó forgalom számára. A 2. ábra a parancssinta szintaxisát mutatja be egy irányelv-térkép konfigurálásához. Egy művelet egy konkrét funkció. Általában egy forgalmi osztályhoz kapcsolódik. Például az ellenőrzések, a cseppek és a továbbítások műveletek.

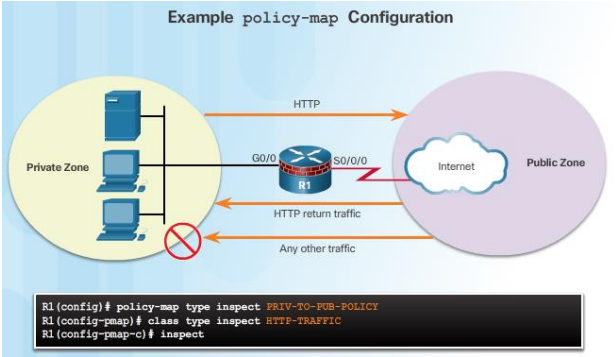
inspect - Ez a tevékenység állami forgalomirányítást kínál. Például ha a PRIVATE zónából a PUBLIC zónába közlekedő forgalom ellenőrzése megtörtént, az útválasztó fenntartja a kapcsolat vagy a munkamenet-információkat a TCP és az UDP forgalom számára. Az útválasztó ezután lehetővé teszi a PUBLIC zóna házigazdáknak küldött visszaforgalmat, válaszul a PRIVATE zóna csatlakozási kérelmére.

drop - Ez az alapértelmezett művelet az összes forgalom számára. Ugyanúgy, mint az összes ACL végét jelző implicit megtagadás, az IOS mindegyik irányítási térképének végén kifejezett cseppet alkalmaz. Az osztály osztály-alapértelmezettként van felsorolva a politika-térkép-konfiguráció utolsó szakaszában. A szakpolitikai térképen belüli egyéb osztálytérképek is beállíthatók a nem kívánt forgalom kiszűrésére. Az ACL-lel ellentétben a forgalom csendben csökken, és az ICMP elérhetetlen üzenetek nem kerülnek a forgalom forrásába.

pass - Ez a művelet lehetővé teszi az útválasztó számára az egyik zónából a másikba irányuló forgalmat. A lépés művelet nem követi a kapcsolatok állapotát. A passz csak lehetővé teszi a forgalmat egy irányba. Megfelelő szabályzatot kell alkalmazni, hogy a forgalmi forgalom ellentétes irányú legyen. A passzív művelet ideális a kiszámítható viselkedésű biztonságos protokollokhoz, például IPsec-hez. Azonban a legtöbb alkalmazásforgalmat jobban kezelik a ZPF-ben a vizsgálati művelettel.

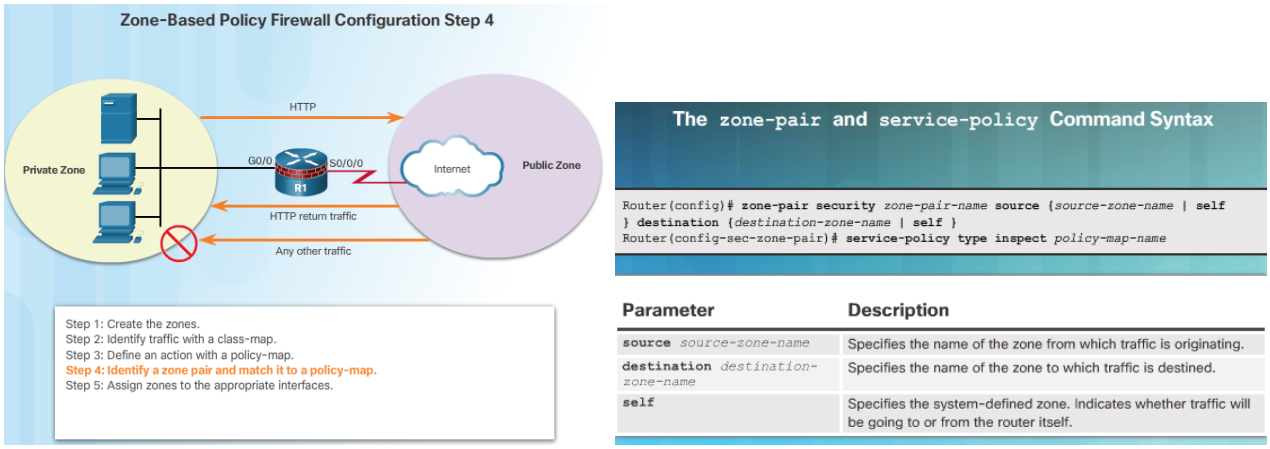


A 3. ábra egy policy map konfiguráció példáját mutatja. Az előző lépésben konfigurált HTTP-TRAFFIC osztály egy új, PRIV-TO-PUB-POLICY nevű házirend-mappához kapcsolódik. A harmadik **inspect** parancs konfigurálja az R1-et, hogy fenntartsa az összes olyan forgalomra vonatkozó állapotinformációt, amely a HTTP-TRAFFIC .

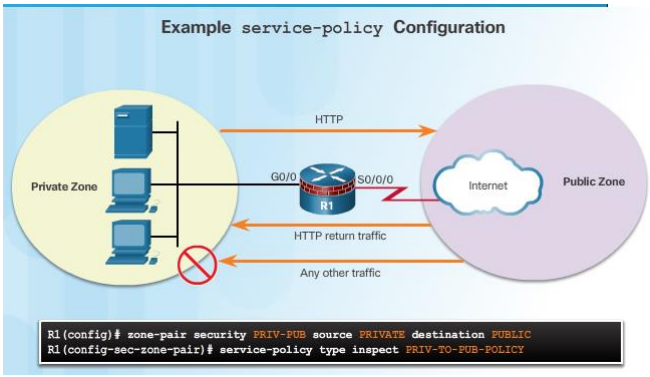


Zóna párosítás és egyezés házirend

A negyedik lépés, amint az az 1. ábrán látható, egy zónapár azonosítása és a zónapár hozzárendelése egy szabályzathoz. A 2. ábra a parancsszintaxist mutatja. Hozzon létre egy zóna-párt a **zone-pair security** paranccsal. Ezután használja a **service-policy type inspect** parancsot, hogy csatoljon egy irányelv-térképet és a kapcsolódó műveletet a zóna-párhoz.



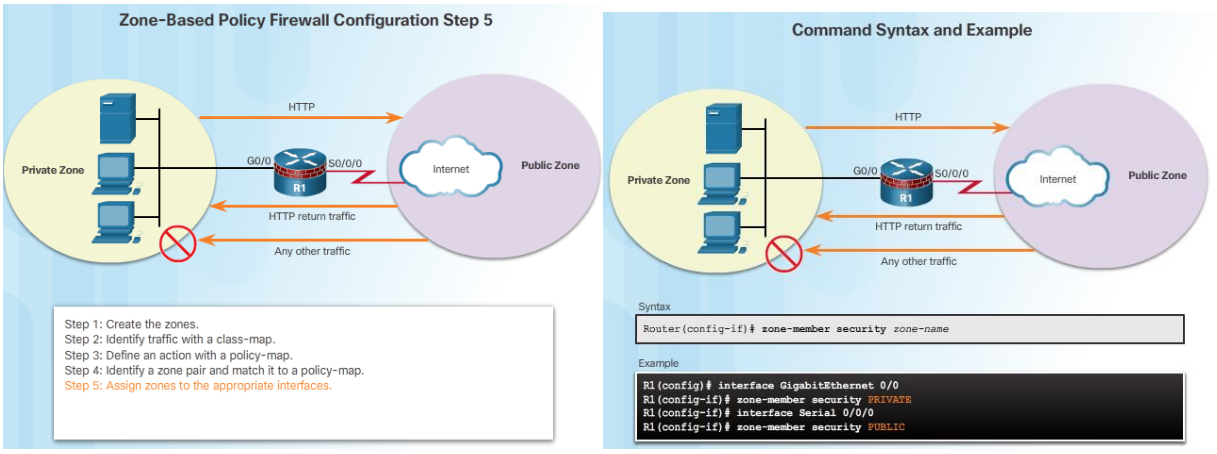
A 3. ábra egy zóna-párt konfiguráció példáját mutatja. A PRIV-PUB nevű zónapár létrehozása a PRIVATE, amely a forrás zónához van rendelve, és a PUBLIC rendeltetési zónához van hozzárendelve. Ezután az előző lépésben létrehozott irányelvmappa kapcsolódik a zónapárhoz.



Miután a tűzfal házirendjét konfigurálta, a rendszergazda a **zone-pair security** parancs használatával alkalmazza a zónák közötti forgalmat. A házirend alkalmazása egy zónapárhoz rendelt. A zónapárnak meg kell adnia a forrás zónát, a célzónát és a forrás- és rendeltetési zónák közötti forgalom kezelését.

Zónák hozzárendelése az interfészekhez

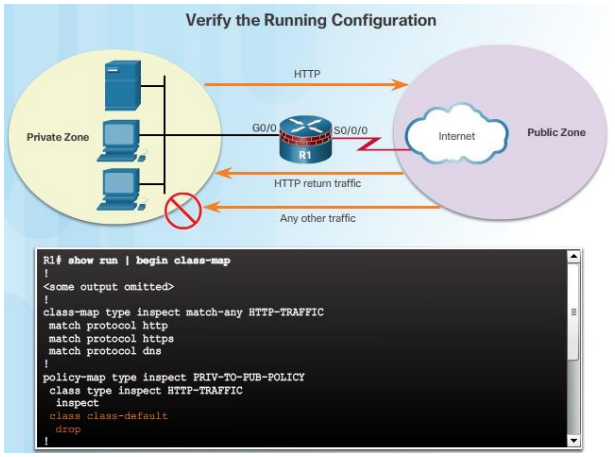
Az ötödik lépés, amint az az 1. ábrán látható, zónákat rendel a megfelelő interfészekhez. Ha egy zónát egy interfészhez társít, azonnal alkalmazni fogja a zónához társított szolgáltatáspolitikát. Ha a zónához még nincs beállítva szolgáltatási irányelv, akkor az összes tranzitforgalom leesik. Használja a zóna tag biztonsági parancsot, amint az a 2. ábrán látható, hogy egy zónát hozzon létre egy interfészhez. A példában a GigabitEthernet 0/0 a PRIVATE zónához van rendelve, a Serial 0/0/0 pedig a PUBLIC zónához van hozzárendelve.



A szolgáltatáspolitika mostantól aktív. HTTP, HTTPS és DNS-forgalmat a PRIVATE zónából, és a PUBLIC zónához kerülnek ellenőrzésre. A PUBLIC zónából származó és a PRIVATE zónához rendelt forgalom csak akkor engedélyezett, ha az a PRIVATE zóna házigazdái által eredetileg kezdeményezett munkák része.

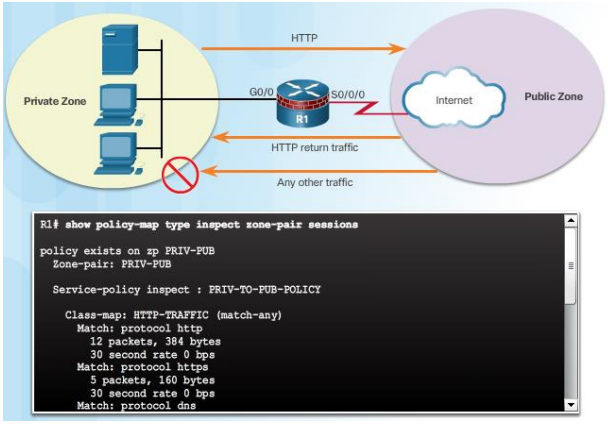
A ZPF konfiguráció ellenőrzése

Ellenőrizze a ZPF konfigurációt a futó konfiguráció megtekintésével. Vegye figyelembe, hogy először az osztály-térkép szerepel. Ezután a policy térkép használja az osztály-térképet. Vegye észre a kiemelt class class-default értéket is, amely minden olyan forgalmat eldob, amely nem tagja a HTTP-TRAFFIC osztálynak.

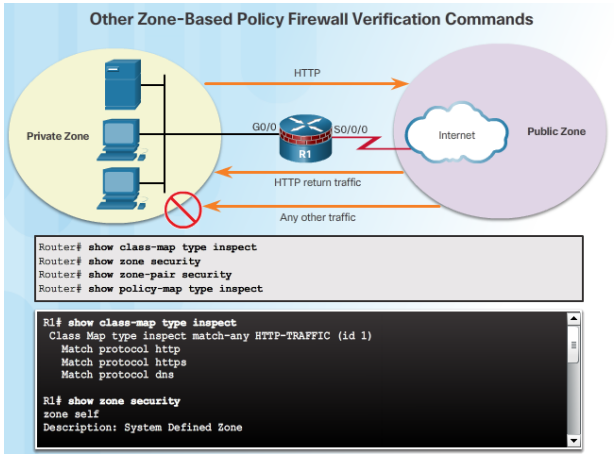


A zóna konfigurációk követi a zónabemutatóval, a zóna párosítással és a szolgáltatásparaméterek zónapárral való összekapcsolását. Végül az interfészek hozzárendelt zónák.

A 2. ábra a ZPF konfiguráció tesztelése után a hitelesítési adatokat mutatja. A 192.168.1.3 PRIVÁT-zóna állomás HTTPS-munkamenetet hozott létre egy 10.1.1.2-es webszerverrel. A parancs kimenetében további észrevétel található, hogy négy csomag megfelelt az class class-default-nak. Ezt az ellenőrzési információt úgy hozta létre, hogy a gazdagép 192.168.1.3-vel pingezte a webszervert a 10.1.1.2-ben.



A 3. ábrán további ellenőrző parancsok láthatók, amelyek lehetővé teszik a ZPF konfiguráció meghatározott részeinek megtekintését.



ZPF konfigurációs szempontok

Amikor egy ZPF-t konfigurál a CLI-vel, akkor számos tényezőre van szükség:

Az útválasztó soha nem szűri a forgalmat az ugyanazon zónában lévő interfészek között.

Egy interfész nem tartozhat több zónához. Biztonsági zónák egységeinek létrehozásához adja meg az új zónát és a megfelelő térkép- és zópárokat.

A ZPF egyidejűleg létezhetnek a Classic Firewall-mal, bár nem használhatók ugyanazon a felületen. Távolítsa el az **ip inspect** interfészkonfigurációs parancsot a **zone-member security** parancs alkalmazása előtt.

A forgalom soha nem léphet át egy zónához rendelt interfész és egy zóna hozzárendelés nélküli interfész között. A **zone-member** konfigurációs parancs alkalmazása mindig a szolgáltatás ideiglenes megszakítását eredményezi, amíg a másik zóna-tag nincs beállítva.

Az alapértelmezett inter zóna-irányelv az, hogy az összes forgalmat elhagyja, hacsak a zónapárra konfigurált szolgáltatáspolitika másképp nem rendelkezik.

A **zone-member** parancs nem védi magát az útválasztót (a forgalomirányítóról érkező forgalmat nem érinti), hacsak a zóna-párok az előre definiált saját zónával vannak konfigurálva.