14.A. Egy biztonsági szolgáltatásokat nyújtó cég munkatársaként egy kisvállalkozás hálózati biztonságának biztosítását, a támadások elhárítását kapta feladatként. Ismertesse a hálózati veszélyeket, támadási módszereket és az elhárítás biztonsági eszközeit!

14.1 Mutassa be a SOHO hálózatok biztonsági veszélyeit, és a támadási módszereket!

14.2 Ismertesse egy ISP üzemeltetési feladatait, és a biztonsági megfontolásokat!

14.3 Mutassa be az operációs rendszer és a konfigurációs állományok mentési lehetőségeit egy forgalomirányítón!

14.4 Ismertesse a hozzáférési listák szerepét a hálózat biztonságában és a forgalom szabályozásában!

-14.5 Határozza meg a tűzfalak szerepét a hálózat biztonságában!

Kulcsszavak, fogalmak:

- Az operációs rendszer és a konfigurációs állományok kezelése mentése egy forgalomirányítón
- Normál és kiterjesztett ACL-ek
- Konfigurációs parancsok, tűzfal, SNMP, Syslog

14.1 Mutassa be a SOHO hálózatok biztonsági veszélyeit, és a támadási módszereket!

Kis irodák hálózati elemei A kis irodai hálózat elemei a kis irodai router esetleg switch és a acces point. Ezek az eszközök legtöbbször integrálva vannak.

Kis irodai hálózatok fenyegetettsége és védelme

A kis irodai hálózatok hasonlóan a nagyvállalati hálózatokhoz különféle veszélyeknek vannak kitéve. Ebben a fejezetben áttekintjük a legfontosabbakat. Fizikai veszélyek (túlfeszültség és zavarvédelem)

A fizikai veszélyek általában a kis irodai hálózatunkat fizikailag veszélyeztető veszélyforrások. Ilyenek lehetnek:

- a különböző természeti veszélyforrások, földrengés árvíz stb.
- technikai veszélyforrások, kommunikációs és energiaellátási problémák stb.
- jogosulatlan fizikai hozzáférés, betörés ellenőrzés nélküli behatolás stb.
- elektromágneses veszélyek

Az ilyen jellegű támadások ellen is fel kell készíteni a kis irodánkat. A legtöbb esetben ezek a védekezi mechanizmusok automatikusak, pl. mert a bejárati ajtó védelmével és riasztó felszerelésével az iroda védelmén túl az informatikai rendszert is fizikailag megvédjük. Nagyon fontos a különböző elektromágneses veszélyek elleni védekezés, azért mert ezek elleni védekezés általában nem oldódik meg egyéb védelmi módok segítségével.

Feszültség – túlfeszültség Mindenekelőtt meg kell határoznunk milyen feszültségről is van szó: egy villamos berendezés kapcsán ugyanis számos feszültséget emlegethetünk: üzemi, maximális, próba, névleges stb. Mi itt kizárólag a tranziens, azaz rövididejű, nem ismétlődő, impulzusjellegű túlfeszültségekre korlátozzuk mondandónkat. Nem tartoznak tehát ide az üzemi jellegű túlfeszültségek, melyeknek mind keletkezési mechanizmusa, mind az ellenük való védekezés módja és eszköztára egészen más.

Villám vagy túlfeszültség ? Sokszor szinte egymás szinonimájaként használják a két szót a védelem kifejezés előtt, holott óriási különbség van a két terület között. A jól működő villámvédelem nem nyújt védelmet a túlfeszültség okozta károkkal szemben, s a túlfeszültségvédelem megléte nem befolyásolja a villámcsapás kockázatát. A két rendszer nem helyettesíti, hanem kiegészíti egymást. A félreértést az okozza, hogy a túlfeszültségek sok esetben a villámcsapás nyomán jelennek meg hálózatainkban. De vajon csak így keletkezhet túlfeszültség? Nem. Az EMC korábban már említett EMP részterülete tovább osztható a túlfeszültség keletkezési módja szerint.

Védekezés a logikai veszélyforrások ellen A pillanattól kezdve, ahogy a felhasználó bekapcsolja számítógépét, rengeteg veszély fenyegeti a rendszert, melyek forrásai az internet. Ezen veszélyforrások lehetnek akár kémprogram támadások, vírusok, trójai falovak, vagy akár hackerek is. Ezeket a veszélyforrásokat nevezzük logikai veszélyeknek.

Anti-virus megoldások A számítógépes vírus olyan program, amely saját másolatait helyezi el más, végrehajtható programokban vagy dokumentumokban. Többnyire rosszindulatú, más állományokat használhatatlanná, sőt teljesen tönkre is tehet. A vírusok manapság jellemzően pendrive vagy e-mail segítségével terjednek, az internetes böngészés mellett. A számítógépes vírusok működése hasonlít az élővilágban megfigyelhető vírus viselkedéséhez, mely az élő sejtekbe hatol be, hogy önmaga másolatait előállíthassa. Ha egy számítógépes vírus kerül egy másik programba, akkor ezt fertőződésnek nevezzük. A vírus csupán egyike a rosszindulatú szoftverek (malware) számos típusának. Ez megtévesztő lehet a számítógép-felhasználók számára, mivel mára lecsökkent a szűkebb értelemben vett számítógépes vírusok gyakorisága, az egyéb rosszindulatú szoftverekhez, mint például a férgekhez képest, amivel sokszor összetévesztik őket.

Vírusok működése Bár a számítógépes vírusok lehetnek kártékonyak (például adatokat semmisítenek meg), a vírusok bizonyos fajtái azonban csupán zavaróak. Némely vírus késleltetve fejti csak ki hatását, például csak egy bizonyos számú gazdaprogram megfertőzése után. A vírusok kártékony hatásának legenyhébbje az ellenőrizetlen reprodukciójuk, mely túlterhelheti a számítógépes erőforrásokat, lelassítja a gép működését, elfogyasztja a szabad helyet a merevlemezen. Súlyosabb ártalom, ha a vírus fontos fájlokat töröl a gépről, akár az operációs rendszert megbénítva, hasonlóképp törölhet célzottan dokumentumfájlokat, videofájlokat, programokat. A legsúlyosabb kár a merevlemez teljes tartalmának megsemmisítése vagy elérhetetlenné tétele,[1] vagy a számítógép valamelyik elektronikus alkatrészének szélsőséges túlterhelése révén műszaki meghibásodás, sérülés előidézése. Napjainkban, az internet térhódításával vírusok már valamivel kevésbé gyakoriak, mint a hálózaton terjedő férgek. Az antivírus szoftverek, melyeket eredetileg a számítógépes vírusok elleni védelemre fejlesztettek ki, mára már képesek a férgek és más veszélyes szoftverek, mint például a kémprogramok (spyware) elleni védelemre is. 2008-ban a Google elindított egy vírus elleni kampányt úgy, hogy megpróbálja elkapni a vírusterjesztő oldalakat, és azt a keresési találatokban vírusos oldalként megjeleníti.
A legtöbb fajta vírusprogram és a legtöbb vírusfertőzés a PC-ken leginkább elterjedt operációs rendszert, a Microsoft Windowst használó számítógépeken figyelhető meg. Sajnálatos jellegzetesség, hogy a vírusok terjedését sokszor csak megkönnyítik az operációs rendszerek és felhasználói programok által kényelmi szolgáltatásnak szánt megoldások. Azok, amikor a program nem terheli a felhasználót esetleg nem érthető kérdésekkel, hanem automatikusan hajt végre műveletsorokat, a program által optimálisnak tartott útvonalon. („Csak egy kattintás...”) Amikor a meghajtóba helyezünk egy DVD-t, akkor automatikusan elindul a rajta levő telepítőprogram, automatikusan megnyílik rajta a fotóalbum vagy a videofájl, a behelyezett pendrive-on levő programok esetében ugyanígy, a megnézett e-mail mellékletei automatikusan megnyílnak, a gépünkre bejegyzett (és bárki által átírható) című kezdőhonlap nyílik meg a böngésző elindításakor, a rendszer külön engedély nélkül letölti és telepíti a Flash-lejátszó program vagy a Java rendszer központi magjának legfrissebb változatát és így tovább. Nem beszélve azokról a biztonsági résekről, amelyek az operációs rendszer vagy a böngésző „túlokosításának” következményeként létrejött speciális, de hozzáértő által a gép védelmeinek kijátszására is kihasználható kerülőutakat jelentik, ezeket a programok gyártói sűrű egymásutánban kibocsátott frissítésekkel, „foltokkal” (patch) próbálják lezárni, utólag, amikor valaki felismer és közzétesz a rendszer szövevényes szerkezetében egy ilyen kerülőutat. A rutinos felhasználó tisztában van ezekkel az eshetőségekkel, és csak annyi automatizmust enged meg a saját rendszerének, amennyinek a kockázatát még elfogadhatónak tartja.

Vírusok fajtái

- **Fájlvírusok:** csak úgy tudnak szaporodni, hogy egy program állomány belsejébe másolják be magukat.
- **Bootvírusok**: a floppy vagy merevlemez boot-területeinek egyikébe írják be magukat. Akkor fertőződnek, ha fertőzött lemezről indul a gép.
- **Makróvírusok**: sok manapság használatos program, mint pl a Word, Excel lehetővé teszik, hogy sablonjaik makrókat tartalmazzanak. A makróvírusok így ilyen dokumentumhoz hozzákapcsolódó öninduló makrók, amik reprodukálódnak, s más dokumentum-állományokhoz fűzik magukat. Fő terjedésük: e-mailek csatolt állományaival.
- **Mailvírusok:** e-mailekkel terjednek, a levélkiszolgálókat és levelezőprogramokat használják ki terjedésükhöz. Ezek legtöbbször a levelek csatolt állományaival terjednek, de napjainkban már előfordulnak a levéltörzsben speciális karakterekként elrejtve, amik rákényszerítik a levelezőprogramot vagy a levelezőszervert egy speciális feladat végrehajtására.

Egyéb rosszindulatú kódok

- **Trójai falovak**: nem szaporodnak, de a gépbe bekerülve ott valamilyen rendellenességet okoznak, pl. PC-k és a hálózati forgalom lelassítása.
- **Kémvírusok:** kárt nem okoznak, hanem információkat szolgáltatnak az adott gépről és a hálózatról Interneten keresztül.
- **Férgek:** „csak" szaporodnak, s emiatt lecsökkentik a háttértár szabad területét, súlyos rendszerhibákat okoznak

A tűzfal célja a annak biztosítása, hogy a hálózaton keresztül egy adott számítógépbe ne történhessen illetéktelen behatolás. Szoftver- és hardverkomponensekből áll. Hardverkomponensei olyan hálózatfelosztó eszközök, mint a router vagy a proxy. A szoftverkomponensek ezeknek az alkalmazási rendszerei tűzfalszoftverekkel, beleértve ezek csomag- vagy proxyszűrőit is. A tűzfalak általában folyamatosan jegyzik a forgalom bizonyos adatait, a bejelentkező gépek és felhasználók azonosítóit, a rendkívüli és kétes eseményeket, továbbá riasztásokat is adhatnak. A tűzfal megpróbálja a privát hálózatot ill. a hálózati szegmenst a nemkívánt támadásoktól megóvni. Szabályozza a különböző megbízhatósági szintekkel rendelkező számítógép-hálózatok közti forgalmat. Tipikus példa erre az internet, ami semmilyen megbízhatósággal nem rendelkezik és egy belső hálózat, ami egy magasabb megbízhatósági szintű zóna. Egy közepes megbízhatósági szintű zóna az ún. „határhálózat" vagy demilitarizált zóna (DMZ), amit az internet és a megbízható belső hálózat között alakítanak ki. Megfelelő beállítás nélkül egy tűzfal gyakranértelmetlenné válik. A biztonsági szabványok „alapértelmezett-letiltás" tűzfal-szabálycsoportot határoznak meg, amelyben csakis azok a hálózatok vannak engedélyezve, amiket már külsőleg engedélyeztünk. Sajnos egy ilyen beállításhoz részletesen ismerni kell a hálózati eszközöket és azokat a végpontokat, amik a vállalat mindennapi működéséhez szükségesek. Sok vállalatnál hiányzik ez az ismeret, és ezért egy „alapértelmezett-engedélyezés" szabályt alkalmaznak, amiben minden forgalom engedélyezve van, amíg konkrétan nem blokkolják. Az ilyen beállítások kéretlen hálózati kapcsolatokat és rendszer veszélyeket okoznak. A szabálymegszegéseket leszámítva, egy tűzfal funkciója nem abból áll, hogy veszélyeket felismerjen és akadályozzon. Főleg abból áll, hogy a meghatározott kommunikációs kapcsolatokat engedélyezze, a forrás- vagy célcímek és a használt szolgáltatások alapján. A támadások felkutatásáért az ún. behatolás-felismerő rendszerek a felelősek, amelyet akár a tűzfalra is lehet telepíteni, de ezek nem tartoznak a tűzfalhoz.

Csomagszűrés Az adatcsomagok egyszerű szűrése a cél-port, valamint forrás- és célcím, egy a tűzfal-adminisztrátor által már definiált szabályrendszer alapján történik. Ez minden hálózati-tűzfal alapfunkciója. A vizsgálat eredményeképp a csomagokat megsemmisíti vagy továbbítja. A fejlett tűzfalak csendben dobják el a csomagokat, azaz az érintett kapcsolat egyszerűen nem jön létre/megszakad, de nincs konkrét visszajelzés. Ez egy gyors és univerzális megoldás, viszont jelentős háttérismeretet, a hálózati és alkalmazási protokollok ismeretét igényli. Ez a tűzfalak leggyakrabban használt fajtája, ezekkel az alapvető szűrésekkel rendelkezik manapság a legtöbb router, és vállalati switchek.

Állapot szerinti szűrés Ez a csomagszűrés egy kibővített formája, ami a 7. OSI-rétegen egy rövid vizsgálatot hajt végre, hogy minden hálózati-csomagról egyfajta állapottáblát hozzon létre. Ezáltal felismeri ez a tűzfal a csomagok közti összefüggéseket és az aktív kapcsolathoz tartozó munkafolyamatokat leállíthatja. Így sikerül ennek felismerni egy kapcsolat felépítése után, hogy a belső kliens a külső célrendszerrel mikor kommunikál, és csak akkor engedélyezi a válaszadást. Amikor a célrendszer olyan adatokat küld, melyeket a belső kliens nem kért, akkor a tűzfal már önmaga blokkolja az átvitelt a kliens és a célrendszer között fennálló kapcsolatnál. Ez különbözteti meg ezt a tűzfalat egy szokásos csomagszűréstől. Egy proxy-val ellentétben a kapcsolat itt önmagában nem befolyásolt.

Alkalmazásszintű tűzfal Egy alkalmazásszintű tűzfal a tisztán csak a forgalomhoz tartozó, mint a forrás, cél és szolgáltatás adatokon kívül a hálózati csomagok tartalmát is figyeli. Ez lehetővé teszi az ún. dedikált proxy-k alkalmazását is, amik egy specializált tartalomszűrést vagy egy Malware-szkennelést is lehetővé tesznek. Egy népszerű félreértéssel ellentétben egy alkalmazásszintű tűzfal alapszintű feladata nem abból áll, hogy meghatározott alkalmazások (programok) hálózathoz való hozzáférését engedélyezze vagy megtiltsa. Egyébként egy áramkör szintű proxy-t lehet egy ilyen tűzfalra létesíteni, ami egy protokollfüggetlen port- és címszűrés mellett egy lehetséges hitelesítés a kapcsolat felépítésének támogatásához. E nélkül egy alkalmazás számára nem lehetséges egy külső hálózattal (internettel) történő kommunikálás.

Proxy / Anonymous proxy Az alkalmazás-szintű tűzfal integrált proxyt használ, ami a munkamenetének helytállósága alapján építi fel a kliensekkel és a célrendszerekkel a kapcsolatot. A szervernek csak a proxy IP-címe lesz látható mint feladó, nem pedig a kliensé. Így a helyi hálózat struktúrája nem lesz felismerhető az Internet felől. Tehát megakadályozza a közvetlen kommunikációt a külső és a védett hálózat között. Közvetítő szerepet játszik a kettő között: a belülről érkező kéréseket feldolgozza, majd azokkal azonos értelmű kérést küld a külső szerver felé, az azokra érkező válaszokat pedig ugyanilyen módon továbbítja a belső hálózat felé. Elég biztonságosnak mondható és általában egyszerűen konfigurálható. Hátránya viszont, hogy kizárólag olyan kommunikációra használható, melynek értelmezésére képes. Magukba foglalhatnak tartalmi gyorsítótárat, így néhány esetben jelentős mértékben csökkenthetik a kifelé irányuló forgalmat. Minden magasabb kommunikációs protokollnak (HTTP, FTP, DNS, SMTP, POP3, MS-RPC, stb.) van egy saját, dedikált proxy-ja. Egyetlen alkalmazás-szintű tűzfalon több dedikált proxy is futhat egyszerre. Anonim proxy: Az eredeti webező identitásának elrejtésére, a webszerver és a böngésző közti kommunikációba harmadik félként beépül olyan módon, hogy valójában ő tölti le a kiszolgálóról a kliens által kért weblapokat. Ezeket továbbítja, így a tényleges kliens identitása (IP címe) a szerver elől rejtve marad.

Tartalomszűrés Egy tűzfal a tartalomszűrő használatával egy kapcsolat hasznos adatait kiértékelni, ill. az áthaladó adatokat ellenőrizni tudja. Hálózati címfordítás (angolul Network Address Translation, NAT) Lehetővé teszi belső hálózatra kötött saját nyilvános IP cím nélküli gépek közvetlen kommunikációját tetszőleges protokollokon keresztül külső gépekkel. Vagyis, hogy több számítógépet egy routeren keresztül kössünk az internetre. Az elsődleges cél ez esetben az, hogy egy nyilvános IP-címen keresztül több privát IP-című (privát címtartomány: RFC 1918) számítógép csatlakozhasson az internethez. A belső gépekről érkező csomagok feladójaként saját magát tünteti fel a tűzfal (így elrejthető a védett host igazi címe), a válaszcsomagok is hozzá kerülnek továbbításra, amiket – a célállomás címének módosítása után – a belső hálózaton elhelyezkedő eredeti feladó részére továbbít. Egy proxy-val ellentétben itt a csomagokat csak továbbküldik és nem analizálják a tartalmukat.

14.2 Ismertesse egy ISP üzemeltetési feladatait, és a biztonsági megfontolásokat!

ISP és ISP szolgáltatások Függetlenül attól, hogy egy magánszemély vagy vállalat milyen eszköz segítségével kapcsolódik az

internethez, az eszköznek internetszolgáltatóhoz (ISP - Internet service provider) kell csatlakoznia. Az ISP egy vállalat vagy szervezet, amely az előfizetők számára az internet hozzáférést biztosítja. Előfizető lehet vállalat, magánszemély, kormányzati testület vagy akár egy másik ISP.
Az internet kapcsolat biztosítása mellett egy ISP további szolgáltatásokat is nyújthat az előfizetők számára, beleértve:
· Eszköztárolás (Equipment co-location) - A vállalatok kérhetik néhány vagy az összes hálózati eszközüknek az ISP területén történő tárolását.
· Webes tárhely szolgáltatás - Az ISP biztosítja a kiszolgálót és az alkalmazást a vállalat weboldalainak tárolásához.
· FTP - Az ISP biztosítja a kiszolgálót és az alkalmazást a vállalat FTP oldalainak tárolásához.
· Alkalmazások és médiaszolgáltatások - Az ISP bocsájtja rendelkezésre a kiszolgálót és a szoftvert egy vállalatnak, hogy az biztosíthasson média adatfolyam, mint például a zene és a video, vagy alkalmazásokat, mint például az on-line adatbázisok.
· IP alapú hangtovábbítás - Az egymástól fizikailag távol eső telephelyek közötti kommunikációra használva, az IP alapú hangátvitel költségmegtakarítással jár.
· IP alapú hangtovábbítás - sok vállalat nem rendelkezik olyan szakértelemmel, amely egy nagy belső hálózat karbantartásához kell. Számos internetszolgáltató nyújt fizetett technikai támogatást.
· Szolgáltatási pont (POP - Point of Presence) - Egy vállalat egy megjelenési ponton keresztül, különböző elérési technológiát használva kapcsolódhat az internetszolgáltatóhoz.

14.3 Mutassa be az operációs rendszer és a konfigurációs állományok mentési lehetőségeit egy forgalomirányítón!

Hosztnév: A routernek beállítható egy címkenév, mely alapján a későbbiekben megkülönböztethető lesz a router más routerektől. Mindenképp javaslom megadását.
- Enable secret: Titkosított belépési jelszó megadása. A későbbi alfejezetben részletesen foglalkozunk vele, annyiban tér el az „enable password" bejelentkezési jelszótól, hogy titkosítási algoritmust használ, tehát nem visszafejthető formátumban tárolja a jelszót.
- Enable password: titkosítatlan állapotban tárolja a begépelt bejelentkezési jelszót
Virtual terminal password: A router távoli felügyeleti módban való elérhetőségéhez szükséges megadni egy jelszót. Ezt a jelszót a routert távolról telnet alkalmazással való elérése esetén kell alkalmazni. Fontos, hogy a VTY rövidítéssel is használt telnet jelszó megadása önmagában kevés! Szükséges az enable bejelentkezési jelszó megadása is!
Konfigurációs fájlok kezelése Többször esett szó arról, hogy a router a betöltési folyamata utolsó lépéseként indító konfigurációt tölt be. Ez a startup-config nevű állomány, melyet az NVRAM-ban tárol De mi a helyzet akkor, amikor konfigurálunk egy routert vagy amikor külső erőforrásról kell áttölteni egy konfigurációt? A konfigurációknak két fajtáját különböztetjük meg:
- startup-config - indító konfiguráció (NVRAM)
- running-config - futó konfiguráció (RAM) Ez utóbbi, a running-config, az éppen aktuálisan terminálról vagy távolról (telnet) szerkesztett konfigurációt tárolja a router ideiglenesen a RAM-ban. Amennyiben nem gondoskodunk annak mentéséről, a router áramtalanítását követően elvész a szerkesztett konfiguráció, és marad egy korábbi mentett indító konfiguráció formájában
Konfiguráció mentése Az aktuális (futó) konfiguráció NVRAM-ba történő elmentésének parancsa:
Router#copy running-config startup-config
Felhasználói EXEC (User EXEC) : Ebben az üzemmódban elsősorban néhány konfigurációs lekérdezést tudunk elvégezni. Ez a rendszergazdai feladatokhoz kevés.
- Privilegizált EXEC (Privileged EXEC): A rendszergazdai feladatok ellátására megfelelő jogosultsági szint, beállításokat tudunk ellenőrizni és módosítani. Ebbe a módba az enable paranccsal léphetünk be, illetve a disable paranccsal léphetünk ki.
- Globális konfigurációs mód (Global Conf. Mode) : A router konfigurációjának módosításához globális konfigurációs módban kell belépni. A globális konfigurációs mód parancsai olyan beállítások megadására alkalmasak, amelyek a teljes rendszerre vonatkoznak. Globális konfigurációs módba lépés parancsa: Router#configure terminal.
- Speciális konfigurációs módok : A globális konfig módból (rövidítve) további almódokat választhatunk, melyek kifejezetten egy adott célt szolgálnak:
 Interfész mód: ebben a módban lehet a router interfészeit beállítani.
 Alinterfész mód: vannak esetek, amikor interfészek további alinterfészeit kell tudtunk beállítani (VLAN-ban).
 Vonali mód: vonali kapcsolat beállítására szolgál (telnet, konzolport).
 Router - forgalomirányító mód: dinamikus útválasztási beállításokat lehet itt kezdeményezni.

Konzoljelszó:
```
PECS(config)#line console 0
PECS(config-line)#password cisco
PECS(config-line)#login
PECS(config-line)#
```

ENABLE jelszó:
```
PECS(config)#enable password pecs
```

ENABLE biztonságos jelszó:
```
PECS(config)#enable secret pecs
```

Virtuális terminál jelszó (5 db):
```
PECS(config)#line vty 0 4
PECS(config-line)#password cisco
PECS(config-line)#login
```

Jelszóbiztonság beállítása:
```
PECS(config)#service password-encryption
```

14.4 Ismertesse a hozzáférési listák szerepét a hálózat biztonságában és a forgalom szabályozásában!

A hozzáférés-vezérlési listák A forgalomszűrés egyik legáltalánosabb módja a hozzáférés-vezérlési listák (Access Control List, ACL) használata. Az ACL-ek használatával a hálózatba belépő és az onnan távozó forgalom ellenőrizhető és szűrhető. Méretét tekintve az ACL lehet egy adott forrásból érkező forgalmat engedélyező vagy tiltó egyetlen parancs, de lehet több száz parancsból álló lista is, ami különböző forrásból érkező csomagok átengedéséről vagy tiltásáról dönt. Az ACL elsődlegesen az engedélyezni vagy elutasítani kívánt csomagtípusok azonosítására használható. **Az ACL által azonosított forgalom az alábbi célokra is felhasználható:**
 A belső állomások meghatározása címfordításhoz
 A speciális funkciókhoz (pl. a szolgáltatásminőség /QoS - Quality of Service/, sorba állítás) tartozó forgalom azonosítása és csoportosítása
 A forgalomirányítási frissítések tartalmi korlátozása
 A hibakeresési üzenetek korlátozása
 A forgalomirányítók virtuális terminálról történő elérésének szabályozása

Az ACL-ek használatából eredő potenciális problémák:
 Az összes csomag ellenőrzése komoly terhelést jelent a forgalomirányító számára, így kevesebb idő jut a csomagtovábbításra.
 A rosszul megtervezett ACL-ek még nagyobb terhelést okoznak, ami zavart okozhat a hálózat használatában.
 A nem megfelelően elhelyezett ACL-ek blokkolhatják az engedélyezni kívánt, és engedélyezhetik a blokkolni kívánt forgalmat.

Az ACL típusok és használatuk A hozzáférési listák létrehozásakor a hálózati rendszergazda számos lehetőség közül választhat, a szükséges ACL típusát mindig a tervezési irányelvek összetettsége határozza meg. 8. Forgalomszűrés hozzáférési listák használatával

Normál ACL A normál ACL (Standard ACL) a legegyszerűbb a három típusból. Normál IP ACL létrehozásakor az ACL a csomag forrás IP-címének alapján végzi a szűrést. A normál ACL a teljes (pl. IP) protokollműködés alapján engedélyezi vagy tiltja a forgalmat. Ha például egy normál ACL nem engedélyezi egy hálózati állomás IP forgalmát, akkor az állomásról érkező összes szolgáltatást tiltja. Ez az ACL-típus egy adott felhasználó vagy LAN számára engedélyezheti az összes szolgáltatás elérését a forgalomirányítón keresztül, míg az összes többi IP-cím

esetén tiltja a hozzáférést. A normál ACL-ek a hozzájuk rendelt azonosítási szám alapján azonosíthatók. Az IP-forgalom engedélyezését vagy tiltását végző hozzáférési listák azonosítási száma 1 és 99, illetve 1300 és 1999 közötti lehet.

Kiterjesztett ACL A kiterjesztett ACL (Extended ACL) nem csupán a forrás IP-cím, hanem a cél IP-cím, a protokoll és a portszámok alapján is szűrhet. A kiterjesztett ACL-ek használata sokkal elterjedtebb, mint a normál ACL-eké, mivel specifikusabbak és jobb ellenőrzést tesznek lehetővé. A kiterjesztett ACL-ek azonosítási száma 100 és 199, illetve 2000 és 2699 közötti lehet.

Nevesített ACL A nevesített ACL (Named ACL, NACL) olyan normál vagy kiterjesztett hozzáférési lista, amelyre szám helyett egy beszédes névvel hivatkozunk. A nevesített ACL-ek beállítása a forgalomirányító NACL üzemmódjában történik.

Az IOS hozzáférési listák típusai

ACL típus	ACL parancs/utasítás	Utasítás célja
Normál	`Router(config)#access-list 1 permit host 172.16.2.88`	• Egy bizonyos IP-címet engedélyez.
Kiterjesztett	`Router(config)#access-list 100 deny tcp 172.16.2.0 0.0.0.255 any eq telnet`	• Tiltja a 172.16.2.0/24 alhálózat számára bármely más állomás elérését, amennyiben telnetkapcsolatot próbálnak létesíteni.
Nevesített	`Router(config)#ip access-list standard permit-ip` `Router(config-ext-nacl)#permit host 192.168.5.47`	• Létrehoz egy permit-ip nevű normál hozzáférési listát. • Engedélyezi a hozzáférést a 192.168.5.47 IP-címről. • Az első parancs a forgalomirányítót NACL konfigurációs almódba helyezi.

A normál és a kiterjesztett ACL-ek elhelyezése

A megfelelően megtervezett hozzáférési listák pozitív hatással vannak a hálózati teljesítményre és rendelkezésre állásra. Tervezzünk meg a hozzáférési listák létrehozását és elhelyezését a maximális hatás érdekében!

A tervezés az alábbi lépésekből áll:

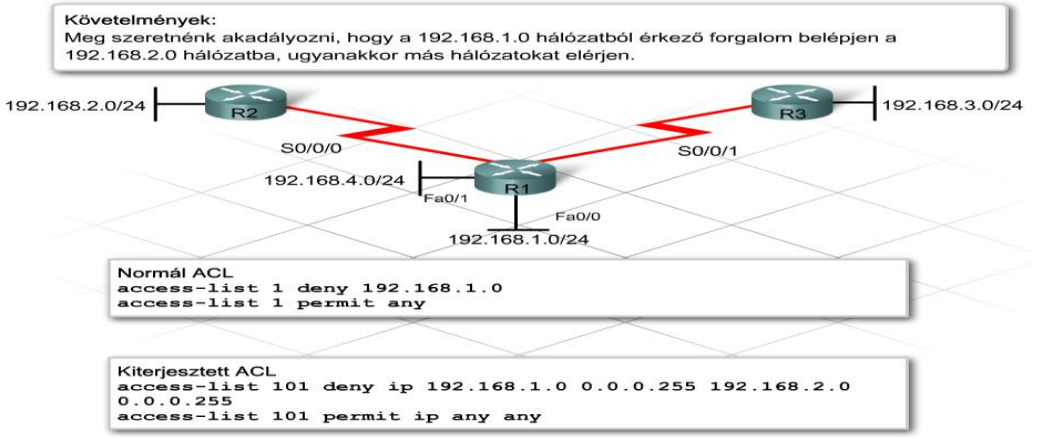
1. A forgalomszűrési igények meghatározása.
2. Az igényeknek leginkább megfelelő ACL típusának kiválasztása.
3. Annak a forgalomirányítónak és interfésznek a kiválasztása, amelyhez az ACL-t rendeljük.
4. A forgalomszűrés irányának meghatározása

1 lépés: A forgalomszűrési igények meghatározása Gyűjtsük össze a forgalomszűrési igényeket az érintettektől, a vállalat minden osztályáról! A fenti –felhasználói igényeken, forgalomtípuson, terheltségen és biztonsági szempontokon alapuló –igények vállalatonként eltérőek lehetnek.

2. lépés: Az igényeknek leginkább megfelelő ACL típusának kiválasztása Mindig a helyzetnek megfelelő szűrési igényeken múlik, hogy normál vagy kiterjesztett ACL-t használunk. Az ACL típusának kiválasztása hatással lehet az ACL rugalmasságára csakúgy, mint a forgalomirányító teljesítményére és a hálózati kapcsolat sávszélességére. A normál ACL létrehozása és alkalmazása egyszerű. A normál ACL viszont kizárólag a forráscím alapján képes szűrni, tekintet nélkül a forgalom típusára és céljára. A több hálózatba vezető útvonalak esetében egy, a forráshoz túl közel elhelyezett ACL akaratlanul is letilthatja az engedélyezni kívánt forgalmat is. Ezért fontos, hogy a normál ACL-eket a célhoz a lehető legközelebb helyezzük el! Ha a szűrési igények jóval összetettebbek, használjunk kiterjesztett ACL-t! A kiterjesztett ACL precizebb szelekciót biztosít, mint a normál ACL. Forrás- és célcím szerinti szűrésre egyaránt képes. Szükség esetén a hálózati és szállítási réteg protokolljai és a portszámok alapján is szűrhet. Ez a megnövelt szűrési részletesség lehetővé teszi a hálózati rendszergazda számára a biztonsági terv igényeinek megfelelő ACL-ek létrehozását. A kiterjesztett ACL-t mindig a forráscímhez közel helyezzük el! Ha az ACL mind a forrás-, mind a célcímet megvizsgálja, akkor bizonyos célhálózatba szánt csomagokat még azelőtt letilthat, hogy azok elhagynák a forrás-forgalomirányítót. A csomagok szűrése még a hálózaton történő áthaladásuk előtt történik, ami segít a sávszélesség megőrzésében.

3. lépés: A megfelelő forgalomirányító és interfész meghatározása, amelyhez az ACL-t rendeljük Helyezzük az ACL-eket a hozzáférési vagy az elosztási réteg forgalomirányítóira! A hálózati rendszergazdának megfelelő jogosultságokkal kell rendelkeznie a fenti forgalomirányítók vezérléséhez és a biztonsági irányelvek alkalmazásához. Az a hálózati rendszergazda, aki nem rendelkezik hozzáféréssel a forgalomirányítóhoz, az ACL-t sem képes ott beállítani. A megfelelő interfész kiválasztásához a szűrési igényeket, az ACL típusát és a forgalomirányító hálózaton belüli pozícióját egyaránt figyelembe kell venni. A forgalom szűrését még azelőtt célszerű elvégezni, hogy az elérne egy alacsonyabb sávszélességű soros összeköttetést. Az interfész kiválasztása a forgalomirányító kijelölését követően már általában egyértelmű.

4. lépés: A forgalomszűrés irányának meghatározása Szemléljük a forgalom áramlását a forgalomirányító szemszögéből azért, hogy az ACL alkalmazásának irányát meg tudjuk határozni! Bejövő forgalom a forgalomirányító valamely interfészére kívülről érkező forgalom. A forgalomirányító összeveti a beérkező csomagot az ACL-lel, mielőtt megkeresné a célhálózatot az irányítótáblában. Az itt elutasított csomagok megspórolják az irányítótáblában történő keresés költségét. Emiatt a befelé szűrő hozzáférési lista jóval hatékonyabb a forgalomirányító számára, mint a kifelé szűrő hozzáférési lista. A kimenő forgalom a forgalomirányítón belül áramlik, majd onnan valamelyik interfészen keresztül távozik. A kimenő csomagra vonatkozóan a forgalomirányító már elvégezte az irányítási keresést, és a csomagot a megfelelő interfészre kapcsolta. A csomag összevetése az ACL-lel közvetlenül a forgalomirányítóról való távozás előtt történik.



14.B. A munka keretében Ön a kisvállalkozás telephelyén helyszíni kockázatfelmérést végzett. Az elvégzett munkáról számlát kell kiállítania. A számla kitöltése után jelezte csak a megrendelő, hogy nem áll módjában készpénzes számlát befogadni, ezért a készpénzes számlát sztornóznia kell, majd a munkahelyén számlázó szoftver segítségével átutalás számlát kell kiállítania.
- Töltsön ki egy készpénzes számlát, nevezze meg a részeit! - Sztornózza a készpénzes számlát!
- Milyen szolgáltatásokat nyújt egy számlázó szoftver?
- Mi a különbség a géppel kiállított számla és az elektronikus számla között?

Kulcsszavak, fogalmak:
- teljesítés ideje, számla kibocsátás kelte, fizetési határidő (átutalásos számla)
- számla sorszáma, számlakiállító neve, címe, adószáma, vevő neve, címe
- értékesített termék/szolgáltatás megnevezése, mennyisége, nettó, számla nettó értéke, az ÁFA százaléka és értéke
- vevő törzs, szolgáltatások és termékek nyilvántartása a számlázó programban
- az elektronikus számla fogalma, elektronikus aláírás, beleegyező nyilatkozat

Számla kötelező tartalmi elemei Minden számlán az alábbi adatokat kötelező feltüntetni:
- számla kibocsátás kelte - számla sorszáma, amely a számlát egyértelműen azonosítja
- számlakiállító neve, címe, adószáma - vevő neve, címe - értékesített termék/szolgáltatás megnevezése, mennyisége, nettó egységára (adó nélküli értéke) - számla nettó értéke (adó nélküli értéke) - az ÁFA százaléka és értéke

- Számla kelte: A számlán a számla keltének mindig annak a napnak kell lennie, amikor Ön a számlát kiállítja. A számla kelte elméleti esetben tehát sem múltbéli, sem jövőbeli dátum nem lehet. Sokan azonban tévhiteken alapulva trükköznek a számla kelte dátumozásánál és múltbéli időpontot adnak meg, pedig a számla keltének semmilyen jelentősége nincs, így teljesen felesleges ezzel bárkinek csalni. Könyvelés és ÁFA bevallás szempontjából a számla teljesítésének időpontja a mérvadó, ami pedig lehet múltbéli és jövőbeli dátum is. Amennyiben ez sem győzte meg, úgy jó ha tudja, hogy a számla szigorú számadású bizonylat, így a számla kelte sosem lehet korábbi, mint a legutóbbi kiállított számla keltének dátuma.

- Számla sorszáma: Azonos cégnév alatt tilos azonos sorszámmal számlát kiállítani! Amennyiben Ön több számítógépen, egymástól teljesen függetlenül (nem hálózatba kötve) számítógéppel állítja ki számláit, úgy minden gépen/telephelyen állítsa be a számlázó programban a számla sorszámozása előtt feltüntetendő előtagot! (pl. egyik telephelyen A2014/00001, másik telephelyen B2014/00001). Az előtag beállításával tud arról gondoskodni, hogy a különböző gépeken/telephelyeken kiállított számlák külön tartományban kapják a sorszámot, így teljes biztonsággal elkerülheti, hogy azonos cégnév alatt azonos sorszámmal állítson ki számlát. A számla sorszáma bármilyen formátumú lehet (tehát még az évet sem kötelező tartalmaznia), lényeg, hogy cégen belül egyedileg azonosítsa a számlát.

- Számla módosítása: Már kiállított (sorszámmal rendelkező) számla tartalmilag nem módosítható! Két lehetősége van a javításra: 1. A számla érvénytelenítéséhez állítson ki érvénytelenítő (storno) számlát, majd állítson ki egy új számlát a kívánt tartalommal, így összesen három számla keletkezik: rossz, rossz stornója, jó számla. 2. A számlát egy lépésből helyesbítheti, ha egy új (helyesbítő) számlát állít ki, ami tartalmilag hivatkozik az elrontott számlára, így összesen csak két számla keletkezik: rossz és a helyesbítő. További információk >>

- Számla aláírása: A számla aláírás és pecsét nélkül is érvényes! Ez a szabály teszi egyébként lehetővé azt is, hogy a számlát egyszerűen akár e-mailben is átküldheti a vevőnek, a vevő így kinyomtathatja azt, Ön pedig megspórolhatja a postaköltséget. További információk >>

- Számla nyelve: A számlát a magyar nyelven kívül bármilyen élő idegen nyelven is kiállíthatja, de ilyenkor javasolt a magyar fordítás feltüntetése (kétnyelvű számla). Az adóhatóság az angol, német vagy francia nyelven kiállított számlákat is elfogadja, de ha ettől eltérő idegen nyelvet használ, akkor egy ellenőrzés során kérhetik Öntől a számla fordítóiroda által elvégzett hiteles fordítását.

- Egyszerűsített számla: A számla egyszerűsített adattartalommal is kiállítható, de csak akkor, ha a gazdasági esemény a számla kiállításkor megvalósul (pl. készpénzes vagy bankkártyás fizetés esetén). Ilyenkor a számlán a bruttó végösszeget kell feltüntetni és az ÁFA összeg helyett a bruttó összeg ÁFA tartalmát kell százalékosan meghatározni (figyelem, ez nem egyenlő az alkalmazott ÁFA kulcs százalékával!).

- Elektronikus számla: Papír használata nélkül is kiállíthat számlákat, de az ilyen elektronikus számlák esetében kötelező a számlákat minősített elektronikus aláírással ellátni vagy a számlákat egy speciális elektronikus adatcsere-rendszerben (EDI) létrehozni és továbbítani. Nagyon fontos, hogy az elektronikus számlázás alkalmazása esetén a vevő előzetes (jellemzően írásos) beleegyezése szükséges.

- Milyen szolgáltatásokat nyújt egy számlázó szoftver?
A rEVOL Express SzámlaVarázslóval akár több tömböt, több céget vagy több telephelyet is kezelhet. Videónkban bemutatjuk mennyire egyszerűen tud több tömböt kezelni a számlázó programban.

Egyszerű számlázás A rEVOL Express SzámlaVarázslóval csupán néhány gombnyomással, egyszerűen, könnyedén és gyorsan készítheti el számláit, így partnereinek saját cégemblémával ellátott, igényes kinézetű számlát nyújthat át.

Számlaismétlés Sűrűn előforduló számláit nem szükséges hónapról hónapra újra rögzítenie. Visszatérő partnereinek, akiknek rendszeresen ugyanazt a terméket vagy szolgáltatást értékesíti számlaismétléssel gyorsabban számlázhat. Elegendő a terméket és partnert egyszer rögzíteni, ezeket a program megjegyzi, és a következő alkalommal felkínálja Önnek, így csak ki kell választania.

Előlegszámla A kereskedelemben gyakran előfordul, hogy vásárláskor nem fizetik ki a teljes vételárat. Erre nyújt megoldást az előlegszámla. A végleges számla kiállításakor beilleszthető a korábban készített előlegszámlát, vagyis a vevőnek ilyenkor már csak a különbözetet kell fizetnie. Egy végleges számlához akár több előlegszámlát is hozzárendelhet.

Sztornó és helyesbítő számla A számla kiállításakor számtalan hibázási lehetőség van. Előfordul, hogy már a számlázáskor feltűnik a hiba, de sokszor a vevő küldi vissza azt. A számlázó programmal egyszerűen készíthet sztornó és helyesbítő számlákat is. A két fogalom között az alapvető különbség, hogy sztornózásra akkor van lehetőség, ha megvan a számla eredeti példánya, mert időben kiderült a hiba, vagy mert a vevő visszaküldte azt. Helyesbítés esetén a vevőnél marad az eredeti, utólag javított számla.

Vonalkód kezelés és keresés Az egyes termékekhez cikkszám mellett egyedi vonalkódot is rögzíthet. Bizonylat kiállításánál Megnevezés, Cikkszám vagy akár Vonalkód alapján is kereshet.

Hasznos kimutatások és elemzések A programba rögzített adatok és számlák alapján hasznos kimutatásokat és elemzéseket készíthet, amelyek támogatják a vállalkozása mindennapjait érintő fontos döntések meghozatalát és a bevallások készítését.

Komplex ármeghatározás A komplex ármeghatározásnak köszönhetően rugalmasan kezelheti a kedvezményeket és egy termékhez akár több árat is rendelhet. Részesítse különleges kedvezményben rendszeres vevőit, vagy akár kínálhatja termékeit extra kedvezménnyel az első vásárlás alkalmával!

Jogosultságok A SzámlaVarázsló programban lehetőség van az adott funkciókhoz jogosultságokat beállítani, így munkatársai csak a számukra szükséges menüpontokat tudják használni, csak az engedélyezett riportokat tudják elkészíteni és meghatározott adatokhoz férhetnek hozzá.

Több cég kezelése Egy SzámlaVarázsló programban akár több céget is kezelhet, a különböző felhasználókhoz rendelt jogosultságok beállításával mindenki csak a számára szükséges adatokat és információkat láthatja.

Hálózat A rEVOL Express SzámlaVarázsló programot hálózatba is kötheti, így még több munkatársa használhatja, ezáltal a munkavégzés még gyorsabb és még hatékonyabb lehet.

Igény szerint bővíthető A SzámlaVarázsló modul igény szerint további modulokkal bővíthető, így számlázását összekötheti a készletkezeléssel, a pénzügyek nyilvántartásával, webáruházával, e-számlákat készíthet vagy egyszerűen elküldheti a könyvelőnek szánt adatokat.

Az elektronikus számla egy olyan számla (bizonylat), ami – az adott ország által meghatározott és elfogadott – elektronikus jelek formájában tartalmazza a számla adatokat. A 2013. január 1-jén hatályba lépő 2010/45/EU irányelv FOGALMA szerint e-számlának minősül az a számla, amelyet elektronikus formában bocsátottak ki és fogadtak be. Azonban mind az említett irányelv, (és az azt átültető magyar áfatörvény) kimondja, hogy ugyanakkor az e-számlának teljesítenie kell az alábbi alapelveket: megbízható módon biztosítani kell a számla eredetének hitelességét, adattartalma sértetlenségét és olvashatóságát.

Az elektronikus számla olyan nem papír alapú számla, amely egy eredeti példányban készül, és egyszerűen fájlmásolás útján sokszorosítható. Az áfatörvény 175. § (1) bekezdése alapján számlát elektronikus úton kibocsátani kizárólag abban az esetben lehet, ha a számla és az abban foglalt adattartalom sértetlensége, valamint eredetiségének hitelessége és olvashatósága biztosított. Az elektronikus számla és adattartalmának sértetlensége azt jelenti, hogy a számla megegyezik az eredetileg kibocsátottal, a számlára utólag semmiféle változtatást, módosítást nem vezethetnek. Az elektronikus számla eredetének hitelessége alatt az értendő, hogy technikai eszközök segítségével egyértelműen azonosítható a számlát kibocsátó, és minden kétséget kizáróan megállapítható, hogy a számlát a számlán szereplő adóalany bocsátotta ki.

Minősített szolgáltató által kibocsátott elektronikus aláírás a számla hitelességét és eredetiségét hivatott igazolni. Az elektronikus számla és az elektronikus aláírás ebben az esetben elválaszthatatlanok egymástól. Egy elektronikus aláírás csak egy számlához tartozik és fordítva. Ha egy aláírt számlán bármilyen apró változtatás történik, akkor az aláírás már nem rendelhető hozzá, így az elveszíti a hitelességét.
Az elektronikus aláírás nyilvános kulcsú titkosítással, más néven aszimmetrikus kulcspárú (RSA) titkosítással valósul meg.

E-számla megjelenése Az elektronikus számla kibocsátási formátumára semmilyen jogszabályi előírás nincsen. Lehet képfájl (jpg), szöveges fájl (txt) vagy PDF állomány, akár többfajta kimenet is megvalósítható.
A 46/2007. PM rendelet az elektronikus számla fájlformátumát határozza meg és nem a kibocsátás formátumát. Ez azt jelenti, hogy az elektronikus számla kibocsátható bármilyen formátumban, de a fájlformátuma kizárólag az állami adóhatóság által közleményben közzétett formátumnak megfelelő lehet. Az elektronikus számla tehát kibocsátható például PDF formátumban a könnyebb megjelenítés érdekében, azonban a fájl formátuma kizárólag a hatályos jogszabályi előírásoknak megfelelő lehet pl. txt fájl.

Az elektronikus számlázás során az adóhatóság által elfogadott fájlformátumok:
txt formátum (szövegfájl)
bármilyen más olyan ún. print fájl formátum, amely nem tartalmaz formázott szöveget, illetve karaktereket, továbbá nem találhatók a fájlban – a soremelésen és az oldalkezdet jelzésén kívül – utasítások, és a fájl tartalma (a fájlban szereplő szöveg, illetve karakterek) egyértelműen megfeleltethető a kinyomtatott adatoknak (a fájlban szereplő karakterek sorozata, tulajdonsága a papírra történő kinyomtatással sem változik),
.csv fájlformátum,
.dbf fájlformátum,
.mdb fájlformátum,
.xls (Excel) fájlformátum,
.xml fájlformátum.
.....
AZ ELEKTRONIKUS SZÁMLA ÉS A SZÁMÍTÓGÉPPEL KIÁLLÍTOTT SZÁMLA KÖZTI KÜLÖNBSÉG
A számítógéppel előállított, de fokozott biztonságú elektronikus aláírással és időbélyegzővel nem rendelkező számla nem elektronikus számla. A piacon többször fedezhető fel az a számlázási gyakorlat, amely szerint a számítógéppel előállított számlát egyszerűen e-mailben továbbítják az ügyfél részére.
Az APEH a kérdések tisztázása érdekében állásfoglalást adott ki (az állásfoglalás elérhetősége: http://www.apeh.hu/adoinfo/afa/szgep_szla_emailen.html), amely szerint:
A számítógéppel kiállított számla papír alapú előállításától eltekinteni semmilyen esetben nem lehet
A számítógépen előállított számla minden példányát papír alapon ki kell nyomtatni
Jelenleg nincs lehetőség arra, hogy a számítógéppel előállított számlát a vevőnek pusztán elektronikus formában továbbítsák
A fentiekből következik, hogy az elektronikus úton továbbított, és a kibocsátó helyett a befogadó által kinyomtatott számlák adóigazgatási célra nem alkalmasak
Tehát amennyiben az elektronikusan előállított számla nem lett fokozott biztonságú elektronikus aláírással és minősített szolgáltató által kibocsátott időbélyegzővel hitelesítve, úgy az nem tekinthető elektronikus számlának.