Cisco Biztonsági Megoldások

A Cisco önvédő hálózatának kiépítése

Tartalomjegyzék

A biztonság minden eddiginél fontosabb
A vállalat jó híre 2
A hatósági előírások betartása 2
A felelősség mérséklése 2
Hatékony vállalati működés 2
Alapkérdések 2
Az önvédő hálózat áttekintése 3

Cisco Security Agent
Áttekintés 4
A fő előnyök 5
Megfontolandó kérdések 5

Hálózati hozzáférés-szabályozás (NAC)
Áttekintés 6
NAC-készülék (Cisco Clean Access) 6
A fő előnyök 7
Megfontolandó kérdések 7

Cisco ASA 5500 sorozatú többfunkciós biztonsági berendezések
Áttekintés 10
A fő előnyök 11
Megfontolandó kérdések 11

Biztonsági WAN-útválasztócsomag
Áttekintés 12
A fő előnyök 13
Megfontolandó kérdések 13

Tűzfal (Cisco ASA 5500-as sorozatú tűzfalak, Cisco PIX, Cisco IOS, Cisco Catalyst 6500-as sorozatú szolgáltatásmodulok)
Áttekintés 14
A fő előnyök 15
Megfontolandó kérdések 15

Virtuális magánhálózatok (VPN)
Áttekintés 16
A fő előnyök 17
Megfontolandó kérdések 17

Behatolásmegelőző rendszerek (IPS)
Áttekintés 18
A fő előnyök 19
Megfontolandó kérdések 19

Megoldások a rendellenességek észlelésére és a veszélyek elhárítására
Áttekintés 20
A fő előnyök 21
Megfontolandó kérdések 21

Cisco Catalyst 6500 sorozatú biztonsági modulok
Áttekintés 22
A fő előnyök 23
Megfontolandó kérdések 23

Cisco Security Monitoring, Analysis, and Response System (MARS)
Áttekintés 24
A fő előnyök 25
Megfontolandó kérdések 25

Cisco Security Manager (CS-Manager)
Áttekintés 26
A fő előnyök 27
Megfontolandó kérdések 27

A biztonság minden eddiginél fontosabb

- A vállalat jó híre
- A hatósági előírások betartása
- A felelősség mérséklése
- Hatékony vállalati működés
- Alapkérdések
- Az önvédő hálózat áttekintése

A vállalat jó híre

Egyre több vásárló aggódik adatai biztonságáért. Ha egy vállalatnál veszélybe kerülhetnek a vevők személyes adatai, az rendkívül kedvezőtlenül befolyásolja az ügyfélkapcsolatokat és a vállalat jó hírét. És persze egy szervezet sem szeretné, ha rajta keresztül számítógépes károkozókkal fertőznék meg ügyfelei hálózatát vagy betörnének oda.

A hatósági előírások betartása

Minden vállalatra vonatkoznak bizonyos hatósági előírások, amelyek gyakran az ügyfelek adatainak titkosságára és védelmére vonatkoznak. Ezeknek az előírásoknak csak kellően szilárd és átgondolt biztonsági rendszerrel lehet megfelelni.

A felelősség mérséklése

A jogviták során a vállalatnak bizonyítania kell, hogy a rá bízott értékek, így az adatok védelme érdekében kellő gondossággal járt el. Ha ezt sikerül igazolnia, akkor általában jelentősen csökkenthető a kárfelelősség mértéke.

Hatékony vállalati működés

Minden vállalat tisztában van azzal, hogy egy egész napos leállás milyen jelentős veszteséget jelent. A férgek, a vírusok, a hackerek és még az alkalmazottak tevékenysége is mind veszélyeztethetik a vállalat működését, egyre gyakrabban okozva fennakadásokat abban.

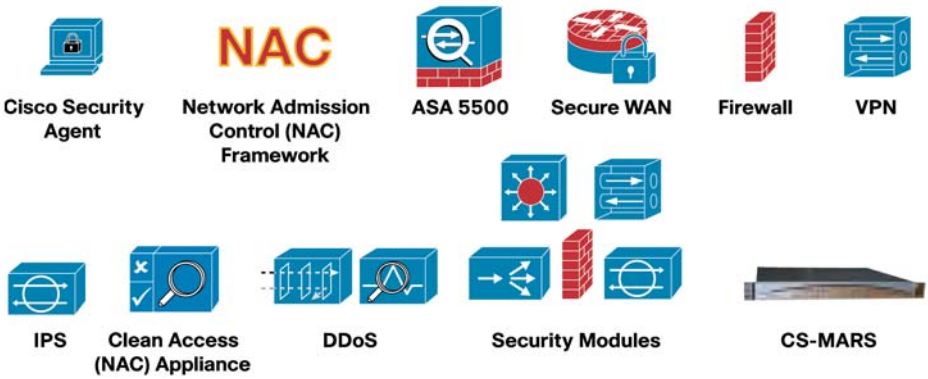
Alapkérdések

- Hogyan történik az elektronikus adatkommunikáció az ügyfelekkel?
- Hogyan tárolják a bizalmas ügyféladatokat?
- Előfordult-e már, hogy az üzleti tevékenységben fennakadást okozott valamilyen biztonsággal kapcsolatos esemény?
- Ha az ügyfelek, a hatóságok vagy az auditorok megkérnék, hogy mutassák be vállalatuk biztonsági tervét, mit tudnának felmutatni?
- Rendelkeznek olyan dokumentált vállalati biztonsági szabályzattal, amely egyértelműen meghatározza, hogy miként kell gondoskodni a vállalat értékeinek, köztük az adatoknak a védelméről?
- Érvényesíteni tudják ennek a szabályzatnak az előírásait?
- A hálózat minden hozzáférési pontja egyben kockázati pont is. Milyen tervvel rendelkeznek arra nézve, hogy minden hálózati belépési pontot kellően biztonságossá tegyenek?

Az önvédő hálózat áttekintése

A Cisco önvédő hálózat (Self-Defending Network) olyan hálózati biztonsági architektúra, amely átfogó, a végpontokig terjedő hálózati biztonságot kínál, ugyanakkor kikényszeríti az előírások betartását is. Amennyiben valamennyi hálózati belépési ponton garantált a megfelelő védelem és az előírások betartása, a vállalatok méretüktől függetlenül jelentősen csökkenthetik a kockázati tényezők számát, és jobban teljesíthetik a „kellő gondosság" elvárásait az adatok védelmét illetően. Ez az architektúra olyan megoldásokból áll, amelyeket a Cisco és sok más, ebben a fontos biztonsági kezdeményezésben résztvevő hardver- és szoftverszállító fejlesztett ki. A Cisco önvédő hálózat jól méretezhető, és tetszőleges nagyságú vállalat esetében alkalmazható. Az ügyfelek, a jogszabályalkotók és az auditáló cégek egyaránt az egész rendszerre kiterjedő védelmet várnak el. A Cisco ezt kínálja az önvédő hálózati megoldások széles választékával, amelyet eddig példa nélkül álló ágazati együttműködés és támogatás egészít ki.

1. ábra – A Cisco biztonsági megoldásainak vázlatos áttekintése



„BÁRKI EL TUD KÉSZÍTENI EGY STOPTÁBLÁT VAGY AKÁR EGY KÖZLEKEDÉSI LÁMPÁT IS. AHHOZ AZONBAN MÁR TELJESEN MÁS GONDOLKODÁSRA VAN SZÜKSÉG, HOGY EGY EGÉSZ VÁROSRA KITERJEDő FORGALOMIRÁNYÍTÓ RENDSZERT ALKOSSON MEG VALAKI."

– Bruce Schneier: Beyond Fear (A félelmen túl)

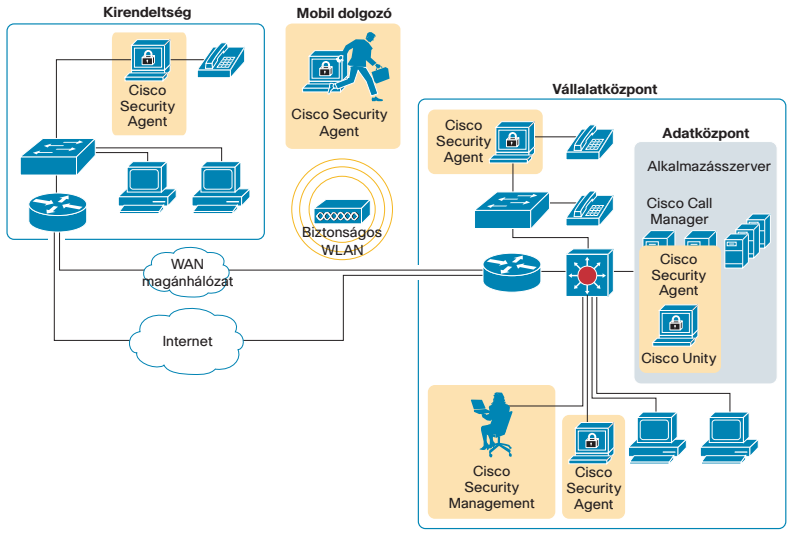
Cisco Security Agent

- Áttekintés
- A fő előnyök
- Megfontolandó kérdések

Áttekintés

- A Cisco Security Agent olyan munkaállomás és kiszolgáló alapú szoftver, amely egyaránt képes kivédeni az ismert és az ismeretlen támadásokat, vagyis azokat is, amelyek ellen a vírusdefiníciókon alapuló vagy hasonló technológiák nem nyújtanak védelmet
- Felismeri a támadó szándékú tevékenységet, és ismeretlen férgek, vírusok, kémprogramok és egyéb biztonsági veszélyforrások ellen is azonnali védelmet biztosít
- Ártalmatlanítja a károkozókat, megőrzi a rendszer épségét, és a támadásokat a hálózaton kívül tartja; emellett a gyenge pontok feltárásával képes felhívni a szakemberek figyelmét a telepítendő programjavításokra
- Intelligens módon feltérképezi a számítógépeken futó szoftvereket, az alkalmazások viselkedését, a vírusvédelem naprakészségét, valamint a telepített gyorsjavítások és szervizcsomagok körét
- Támogatja a vállalati biztonsági előírások érvényesítését (pl. érzékeny adatfájlok, MP3-fájlok és azonnali üzenetküldés korlátozása)
- Az adatlopás megelőzésére vonatkozó szabályok korlátozzák a személyes azonosítók cserélhető háttértárakra történő másolását, amely az identitáslopás egy leggyakoribb módja

2. ábra – Alkalmazási területek



A fő előnyök

- Védelem az ismeretlen támadásokkal szemben
  - Képes megállítani az olyan új és ismeretlen támadásokat, amelyek rosszindulatú tevékenységet kísérelnek meg, és nem szerepelnek a vírusvédelem támadásazonosító-adatbázisában
- Elkerülhetővé teszi a programjavítások kapkodó és áttekinthetetlen telepítését
  - Elegendő időt biztosít a szervezeteknek ahhoz, hogy teszteljék az új programjavításokat, és kiszűrjék azokat, amelyet nem működnek jól együtt az alkalmazásokkal. Csökkentheti a végpontokon telepítendő frissítések számát.
- Szoros együttműködés a hálózati hozzáférés-szabályozási (NAC) keretrendszerrel
  - A biztonsági szabályok betartásának ellenőrzéséhez átadja az operációs rendszer szintű azonosító adatokat a NAC keretrendszerének
- Felhasználó által definiált biztonsági szabályok
  - A felhasználó szervezet által meghatározott hálózathasználati házirend érvényesítésének elsődleges szintjeként szolgál (MP3-fájlok, adatlopás megelőzése, azonnali üzenetküldés, előírásos hálózati viselkedés stb.)
- A Cisco Security Agent személyi tűzfalként is funkcionálhat

Megfontolandó kérdések

- Megzavarta-e már vállalatának működését valamilyen internetes támadás, mint például vírusok, férgek, kémprogramok vagy hackerek?
- Alkalmaznak-e elektronikus adatkommunikációt az ügyfelekkel? Teljesen biztos-e abban, hogy vállalatának rendszere nem válhat az ügyfelek hálózatát megfertőző veszély forrásává?
- Kívánják-e a vállalat egészében ellenőrzés alatt tartani az érzékeny adatokat tartalmazó fájlok, az MP3-fájlok, az azonnali üzenetküldés stb. használatát, és érvényesíteni az erre vonatkozó előírásokat?
- Előfordult már, hogy ha bejutott a hálózatba egy vírus, a fertőzés terjedésének sebessége miatt nem tudták az új programjavításokat megfelelően bevizsgálni és jóváhagyni?
- Úgy véli, hogy vállalata egy esetleges jogvita során egyértelműen bizonyítani tudja, hogy kellő gondossággal jár el a kritikus fontosságú és bizalmas adatok védelme, illetve a munkavállalók viselkedésének ellenőrzése tekintetében?
- A személyes adatokat tároló kiszolgálók esetében le kívánják-e tiltani a fizikai adathordozókra (pl. lemezekre vagy USB-kulcsokra) történő fájlmásolást?

Hálózati hozzáférés-szabályozás (NAC)

- Áttekintés
- NAC-készülék (Cisco Clean Access)
  - Áttekintés
  - A fő előnyök
  - Megfontolandó kérdések

Áttekintés

- Hálózati hozzáférés-szabályozáson (Network Admission Control – NAC) a Cisco Systems vezetésével létrejött ágazati kezdeményezés eredményeként megszületett technológiák és megoldások összességét értjük. Az NAC a hálózati infrastruktúrán keresztül valamennyi hálózati hozzáférést igénylő készülék esetében érvényesíti a biztonsági előírásokat, így jelentősen korlátozza a vírusok, férgek és kémprogramok által okozható károkat.
- A NAC csak az előírásoknak maradéktalanul megfelelő és megbízható végpontok (pl. PC-k, szerverek, PDA-k) csatlakozását engedélyezi, és korlátozhatja a nem megfelelő eszközök hálózati hozzáférését
- NAC-készülék
  - A Cisco Clean Access termékcsaláddal bevezetett NAC-készülékek (NAC Appliance) gyorsan rendszerbe állítható megoldások önálló végpont-kiértékeléssel, szabálykezeléssel és kockázatelhárítással

NAC-készülék (Cisco Clean Access)

Áttekintés

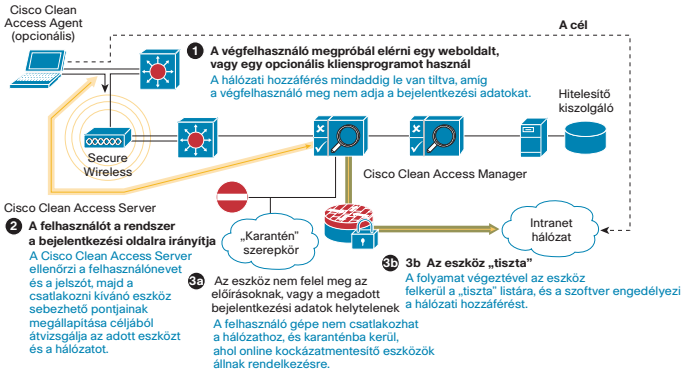
A Cisco Clean Access egy olyan egyszerűen üzembe helyezhető termék, amely automatikusan képes a hálózathoz kapcsolódni szándékozó fertőzött vagy kockázatot jelentő eszközök észlelésére, izolálására és fertőzésmentesítésére. A program megvizsgálja, hogy a hálózatba kötött eszközök, mint például laptopok, PDA-k vagy éppen játékkonzolok megfelelnek-e a hálózat biztonsági előírásainak. Amennyiben szükséges, a rendszer az eszköz csatlakozásának engedélyezése előtt kiküszöböli az esetleges sebezhető pontokat.

A Cisco Clean Access a legelterjedtebb hálózati hozzáférés-szabályozási termék, amely jelenleg több mint 300 rendszer 2,5 millió végfelhasználójának nyújt támogatást. A szoftver bármekkora szervezetben képes egyszerre többféle hozzáférési módot támogatni, beleértve a vezeték nélküli vagy távoli elérést, illetve a LAN-ról, WAN-ról vagy vendégként történő hozzáférést.

NAC Framework egy architektúra alapú hozzáférés vezérlő megoldás, ami egyaránt képes együttműködni a már telepített Cisco hálózati megoldásokkal és amás gyártók biztonsági és felügyeleti megoldásaival.

A NAC Framework lehetőséget kínál, hogy felügyelje a távolról kezdeményezett vagy a helyi hálózati hozzáféréseket egyránt, kikényszerítse a végpontok biztonsági előírását és ezzel meggátolva a károkozók terjedését.

3. ábra – Alkalmazási területek



A fő előnyök

- Jelentős mértékben növeli a hálózat biztonságát
  - Gondoskodik arról, hogy a végpontok (mobil és asztali számítógépek, PDA-k, szerverek) megfeleljenek a biztonsági előírásoknak
  - Proaktív védelmet biztosít a férgek, vírusok, kémprogramok és rosszindulatú szoftverek ellen
  - A megelőzésre és nem a válaszlépésre helyezi a hangsúlyt
- Kibővíti a meglévő informatikai eszközök felhasználási körét
  - A több gyártótól származó vírusvédelmi, biztonsági és felügyeleti szoftverek széles körével képes együttműködni
  - Növeli a hálózati infrastruktúrába történt beruházások értékét
- A vállalat egészében megnövelt, rugalmasabb védelmet biztost
  - Átfogó hozzáférés-szabályozást biztosít valamennyi hozzáférési mód esetében (LAN, WAN, vezeték nélküli, VPN)
  - Megakadályozza, hogy az előírásoknak nem megfelelő vagy visszaélésre lehetőséget adó végpontok kihatással legyenek a hálózat rendelkezésre állására
- Csökkenti a működési költségeket
  - Mérsékli az előírásoknak nem megfelelő, visszaélésekre lehetőséget adó és fertőzött rendszerek beazonosításával és javításával kapcsolatos kiadásokat

Megfontolandó kérdések

- Előfordult-e már, hogy a vállalat működésében zavart okozott valamilyen féreg vagy vírus elterjedése?
- Szükség van-e a felügyelet nélküli számítógépek csatlakozásának ellenőrzésére, mint például vendégfelhasználók, külső szakértők és alvállalkozók esetében?
- Szükséges-e a vezeték nélküli hálózat felhasználóazonosításának szigorítása?
- Működik-e hálózatukon Cisco virtuális magánhálózat?
  - Az NAC Appliance ellenőrzési funkciói a rendszert egyszeri bejelentkezéssel használó távoli elérésű felhasználókra is kiterjeszthetők
  - A Cisco Clean Access kiváló lehetőséget kínál a vezeték nélküli hálózatok biztonságának növelésére

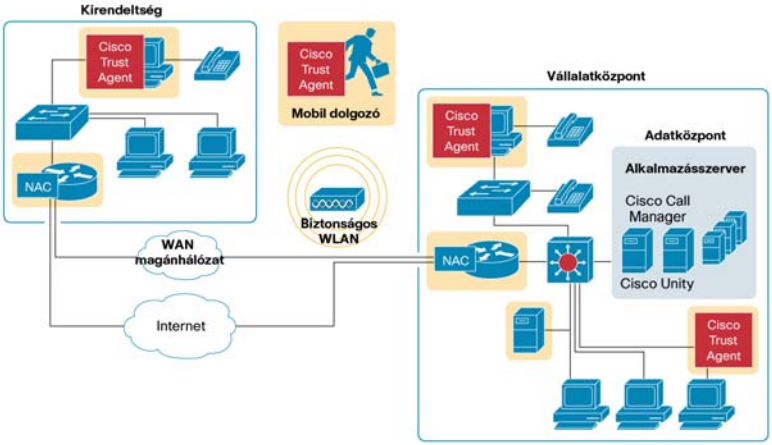
NAC Framework

Áttekintés

- NAC Framework egy architektúra alapú hozzáférés vezérlő megoldás, ami egyaránt képes együttműködni a már telepített Cisco hálózati megoldásokkal és amás gyártók biztonsági és felügyeleti megoldásaival.

- A NAC Framework lehetőséget kínál, hogy felügyelje a távolról kezdeményezett vagy a helyi hálózati hozzáféréseket egyránt, kikényszerítse a végpontok biztonsági előírásait és ezzel meggátolva a károkozók terjedését.

4. Ábra - Alkalmazási területek



Fő előnyök:

- Megelőzi a végpontok ismert és ismeretlen (day-zero) károkozók általi megfertőződését és a fertőzés elterjedését a hálózaton

- Tökéletesíti a károkozót azonosítását, és az elterjedésük megelőzésével megnöveli a hálózat hozzáférhetőségét, rugalmasságát és termelékenységét

- Felhasználja és megvédi a jelenlegi Cisco hálózatot és végponti biztonsági befektetéseket

- Teljes láthatóságot kínál, hogy ki és mi kapcsolódik a hálózati erőforrásokhoz

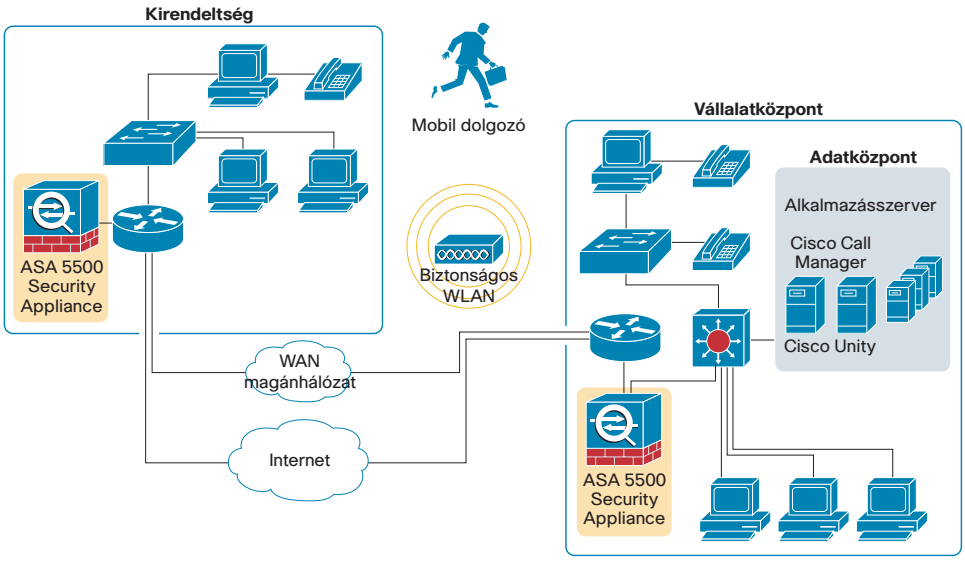
- Csökkenti a végpontok megfelelősségének elérési idejét és a ügyfélszolgálati hívásokat, ezáltal az üzemeltetési költségeket

- Hozzáférés felügyelet az összes végpont összes hozzáférési metódusára, beleértve a LAN, vezeték nélküli, távolis és WAN hozzáférést

Áttekintés

- A Cisco ASA 5500-as sorozat berendezései egyetlen, egyszerűen használható készülékben egyesítik a tűzfal, a virtuális magánhálózat (VPN), a behatolás-megelőzés és a hálózati vírusvédelem funkcióit
- Immár professzionális védelmet biztosíthat vállalata hálózatának, ugyanakkor jelentősen csökkentheti a költségeket és a megoldás bonyolultsági szintjét, hiszen több biztonsági funkció egyetlen nagyteljesítményű készülékben egyesíthető
- Nincs szükség többé kompromisszumokra, ha a távoli helyszínek védelméről van szó

5. ábra – Alkalmazási területek



A fő előnyök

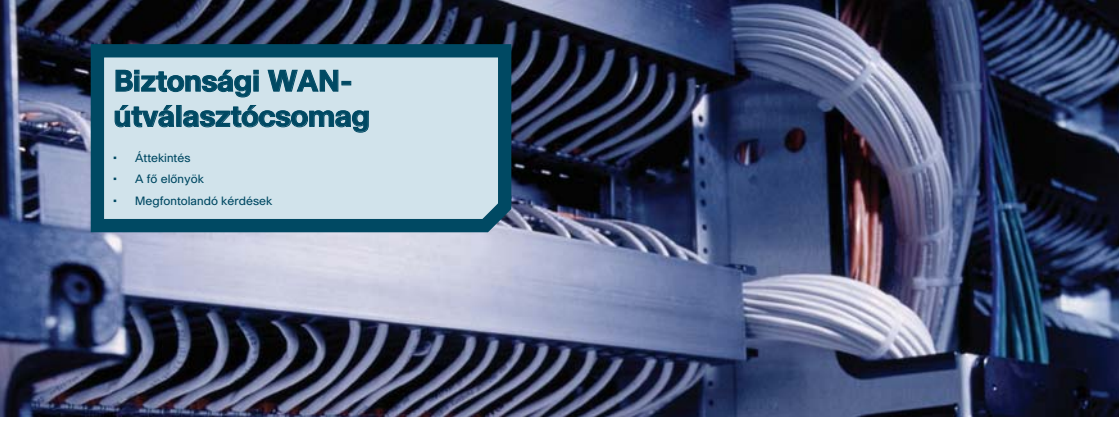
- Jelentősen csökkenti a hálózati felügyelet költségét és összetettségét, mivel egyidejűleg működik tűzfalként, virtuális magánhálózatként, behatolásmegelőző rendszerként és hálózati vírusvédelmi eszközként
- Egyetlen tűzfal áráért nagy teljesítményt kínál számos biztonsági szolgáltatással
- Az új veszélyforrásokat is sikerrel felismeri és kivédi
- A Cisco önvédő hálózatának funkcióit a távoli helyszíneken is elérhetővé teszi
- A Cisco PIX® tűzfallal megegyező felügyeleti kezelőfelületnek köszönhetően gyorsan bevezethető

Megfontolandó kérdések

Szeretné csökkenteni a hálózati biztonsághoz kapcsolódó kiadásokat és a feladatok összetettségét?

Még mindig gondot okoznak a férgek és vírusok?

- Szeretné, ha további biztonsági szolgáltatások lennének elérhetők a távoli helyszíneken?
- Korszerűsíteni vagy bővíteni kívánja meglévő biztonsági rendszerét?
- Vonzónak találja-e az ötletet, hogy egyetlen készülékben olyan sokoldalú biztonsági szolgáltatások találhatók meg, mint a tűzfal, behatolásmegelőzés, hálózati vírusvédelem és a távoli felhasználóazonosítás?

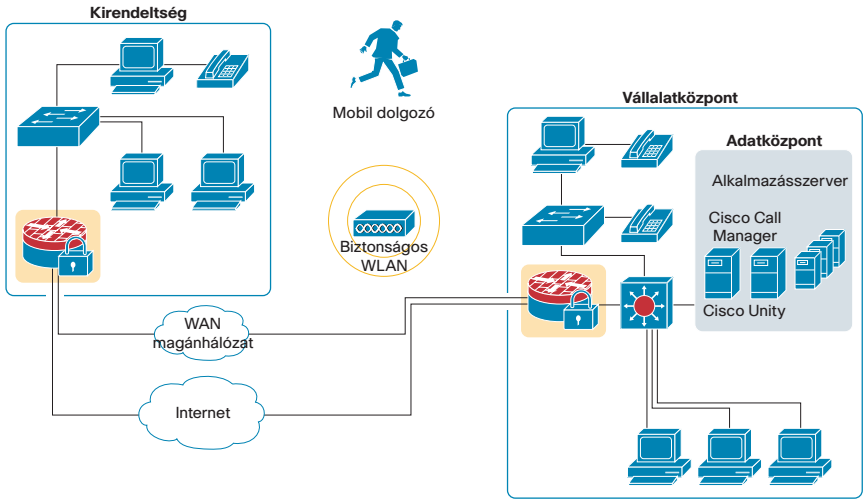


Biztonsági WAN-útválasztócsomag

- Áttekintés
- A fő előnyök
- Megfontolandó kérdések

Áttekintés

- A Cisco biztonsági WAN-útválasztócsomag a fiókirodai útválasztókat egy sor igen fontos biztonsági funkcióval ruházza fel, mindezt minimális többletköltség mellett, kiváló megtérülést kínálva
- A csomag a következő új funkciókkal bővíti a fiókirodai útválasztókat: telephelyek közötti VPN, távoli elérésű VPN, állapottartó tűzfal, alkalmazás szintű tűzfal, URL-szűrés, közvetlenül a forgalom útvonalába telepíthető behatolásmegelőzés, hálózati hozzáférés-szabályozás és biztonságos felügyelet
- Napjainkban a fiókirodáknak ugyanolyan biztonságosnak kell lenniük, mint a vállalati központoknak. A Cisco Secure WAN-csomag vonzó és gazdaságos megoldást kínál, mivel nem kell később külön időt és pénzt fordítani ezeknek a fontos szolgáltatásoknak a bevezetésére.
- Az új Cisco routerek integrált szolgáltatásai jól kihasználják a WAN-hálózatok biztonságát szolgáló funkciókészletet



6. ábra – Alkalmazási területek

A fő előnyök

Integrált szolgáltatásokat nyújtó útválasztók

870, 1800, 2800 és 3800

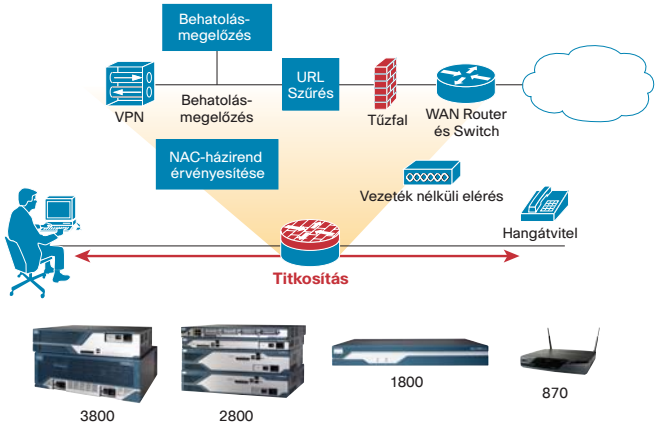
Magas szintű biztonsági szolgáltatások sebességcsökkenés nélkül

- A biztonsági szabályok érvényesítése (NAC)
- Állapottartó és alkalmazás szintű vizsgálatokat végző tűzfal
- Titkosítás (IPSec)
- Behatolásmegelőzés (Cisco IOS® IPS)
- Telephelyek közötti és távoli VPN
- Biztonságos felügyelet

Egyéb elérhető szolgáltatások

- IP-kommunikáció (hang és videó)
- Biztonságos vezeték nélküli elérés

7. ábra –



Megfontolandó kérdések

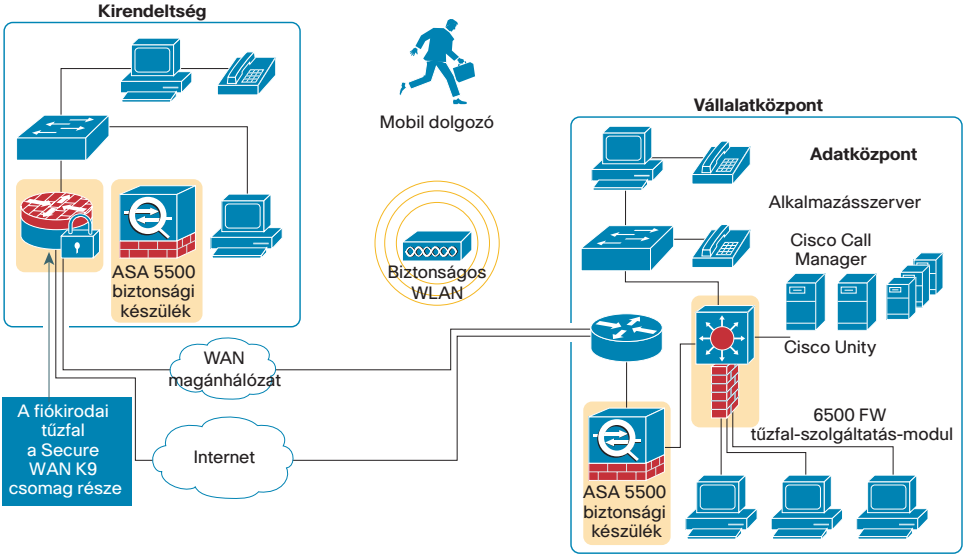
- Ugyanakkora hangsúlyt fektetnek vállalatánál a távoli helyszínek védelmére, mint a központéra?
- Szeretné, ha a Cisco útválasztókra fordított beruházásaik egyben hozzájárulnának a hálózat biztonságához is?
- Szeretné, ha a sokféle készülék helyett egyetlen platform gondoskodna az útválasztásról, a kapcsolásról, a vezeték nélküli és a hangátvitelről, valamint a biztonságról is?
- Ha még nincs kiforrott biztonsági stratégiájuk, akkor nem gondolja, hogy az elkövetkezendő egy-másfél évben a fenti WAN-biztonsági funkciók közül legalább egyre, de akár mindre szükségük lehet? Ha a válasz igen, akkor a jövőben jóval költségesebb lenne ezeket az új funkciókat bevezetni, hiszen egy meglévő rendszert kellene bővíteni, és az összes útválasztóval egyenként foglalkozni kellene.

Tűzfal (Cisco ASA 5500-as sorozatú tűzfalak, Cisco PIX, Cisco IOS, Cisco Catalyst 6500-as sorozatú szolgáltatásmodulok)

- Áttekintés
- A fő előnyök
- Megfontolandó kérdések

Áttekintés

- A tűzfal védelmet biztosít a hálózat erőforrásainak a belső és külső hálózati felhasználókkal szemben
- A Cisco tűzfalmegoldásai integrált hálózatbiztonsági szolgáltatásokat kínálnak, például állapottartó csomagvizsgálatot, protokoll- és alkalmazásvizsgálatot, in-line behatolásmegelőzést, valamint a multimédiás és hangátvitel védelmét
- A Cisco többféle tűzfalmegoldást kínál, köztük a fiókirodáknak szánt, a Cisco IOS szoftveren alapuló tűzfalat, a Cisco ASA 5500-as sorozatú készülékeket, a Cisco PIX biztonsági készülékeket, illetve a rugalmasabb méretezhetőséget igénylő környezetekhez a Cisco Catalyst® 6500-as sorozatú tűzfal-szolgáltatásmodult (FWSM)



8. ábra – Alkalmazási területek:

A fő előnyök

- A kisvállalati és irodai környezetektől a nagyvállalati rendszerekig egységes felhasználói és hálózati jogosultságkezelést biztosító, következetesen végigvitt identitáskezelő és azonosítási szolgáltatások
- Egységes kezelőfelület a könnyebb központi és távoli felügyelet érdekében
- A dinamikus útválasztás támogatása a hatékony útvonalkiosztásnak köszönhetően nagyobb hálózati megbízhatóságot és teljesítményt eredményez
- Valamennyi tűzfalmegoldást a Cisco Security Manager (CSM) felügyeli
- Kimagasló megbízhatóság (nincs beépített merevlemez, nem nyílt operációs rendszerrel működik)
- Állapottartó vizsgálatokat végző tűzfal az alkalmazások hálózati viselkedésének kiterjedt ismeretével

Megfontolandó kérdések

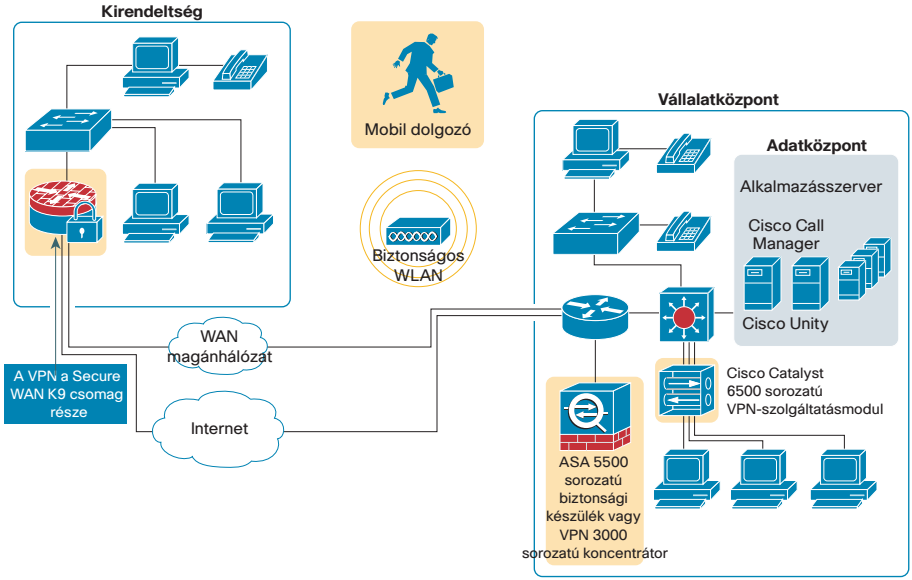
- Úgy véli, hogy az üzleti követelményeknek megfelelő, részletes tűzfalstratégiával rendelkeznek?
- Milyen végfelhasználóknak és alkalmazásoknak kell hozzáférniük a vállalat hálózatához (alkalmazottak, beszállítók, ügyfelek, hang- és videoátviteli szolgáltatások, internetes tartalom)?
- Több különböző felügyeleti megoldás használatára kényszerülnek a biztonsági infrastruktúra felügyeletéhez?
- Előnyös lenne-e a vállalata számára egy olyan átfogó tűzfal-megoldáscsalád, amely a fiókirodáktól kezdve a központ alaphálózatáig a hálózat valamennyi elemére kiterjedne?
- Úgy véli, hogy meglévő, nem Cisco gyártmányú tűzfalaik karbantartása túl magas költségekkel jár?

Virtuális magánhálózatok (VPN)

- Áttekintés
- A fő előnyök
- Megfontolandó kérdések

Áttekintés

- A virtuális magánhálózatok (VPN-ek) gyors, megbízható és biztonságos kapcsolatot kínálnak a távoli helyszínek és a mobil dolgozók számára. A Cisco egy sor olyan VPN-megoldással rendelkezik, amelyek költséghatékony és kiválóan felügyelhető távoli elérést biztosítanak.
- Ezek együttesen az ágazat legátfogóbb VPN-termékcsaládját képviselik
- A Cisco VPN-megoldásai a dedikált VPN-titkosító processzoroknak köszönhetően késleltetés nélküli (vezetéksebességű) átbocsátást biztosítanak
- A Cisco VPN-megoldásokat kínáló termékei a következők:
  - **Dedikált készülékek** – ASA 5500 sorozatú készülékek és VPN 3000 sorozatú koncentrátorok
  - **Integrált megoldás** – Cisco IOS alapú útválasztó
  - Cisco Catalyst 6500 sorozatú VPN-szolgáltatásmodulok



9. ábra – Alkalmazási területek

A fő előnyök

- A távoli felhasználók hatékonyabb munkavégzése a vállalati erőforrások és alkalmazások biztonságos távoli elérésével
- IPSec és SSL VPN-kapcsolatok támogatása egyetlen készülékkel (ASA 5500, VPN 3000, Catalyst 6500, ISR-útválasztók)
  - Az SSL VPN része a Cisco Secure Desktop, amely a nem védett eszközökről is garantáltan biztonságos távoli elérést biztosít
- A vállalati hálózati erőforrások interneten keresztül elérhetővé válásával a vállalatok jelentősen csökkenthetik vállalati magánhálózataik kiépítésének költségeit
- A VPN révén a vállalati hálózat szinte bármely internetes hotspoton keresztül elérhető, ami számottevően fokozza a mobil dolgozók hatékonyságát
- A Cisco VPN-megoldásai mindkét alábbi igénynek megfelelnek:
  - Távoli elérés (mobil felhasználók)
  - Telephelyek közötti kapcsolat költséges WAN vagy bérelt vonalak nélkül

Megfontolandó kérdések

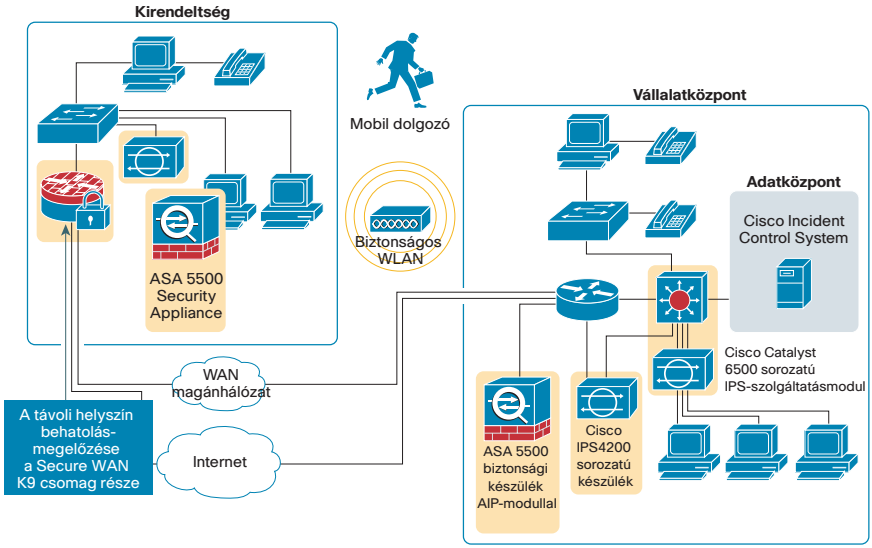
- A szervezetnél vannak-e olyan mobil dolgozók, akiknek el kell érniük a vállalati hálózatot?
- Szeretné, ha mind az IPSec, mind az SSL alapú VPN-eket egyetlen platformról működtethetnék?
- Tudta-e, hogy a Gartner piackutató a következő adatokat jelentette a VPN-eket használó vállalatokról:
  - 85 százalékuk szerint a VPN bevezetésével nőtt a hálózati biztonság, és gyorsabbá vált a hálózati elérés.
  - Majdnem 90 százalékuk költségmegtakarítást ért el. A beruházás átlagos megtérülése 18 hónap alatt 54 százalék.
  - Több mint 70 százalékuk szerint a VPN-ek hatékonyabbá tették az ügyfelekkel és a partnerekkel folytatott kommunikációt.
  - Több mint 75 százalékuk szerint a VPN-ek megkönnyítik az informatikusok számára a távoli felhasználók támogatását.
  - Átlagosan heti 3 munkaórát takarítottak meg alkalmazottanként.
- Vállalatának távoli felhasználói gyorsabb és megbízhatóbb kapcsolatot igényelnek?

Behatolásmegelőző rendszerek (IPS)

- Áttekintés
- A fő előnyök
- Megfontolandó kérdések

Áttekintés

- A Cisco behatolásmegelőző rendszere (IPS) közvetlenül a forgalom útvonalába telepíthető (in-line) „deep packet inspection” technológián alapuló megoldást kínál, amely a hálózati támadások széles körének hatékony kivédését és az adatok és a hálózati infrastruktúra védelmét teszi lehetővé.
- A Cisco IPS-termékek hatékony behatolásmegelőző képességeinek négy fő eleme:
  1. A veszélyforrások pontos észlelése
  2. A veszélyforrások intelligens elemzése
  3. Egyszerű felügyelhetőség
  4. Rugalmas alkalmazási lehetőségek
- A Cisco Incident Control System (ICS) rendszere kiterjeszti a behatolásmegelőző rendszer képességeit, és a támadásazonosítóknak a Trend Micro szolgáltatásain keresztüli gyors frissítésével a hálózat szintjén tartóztatja fel a támadások járványszerű terjedését



10. ábra – Alkalmazási területek

A fő előnyök

- Hatékony megelőzés a potenciális veszélyforrások átfogó észlelésével
- A veszélyforrások intelligens elemzése jelentősen csökkenti a téves riasztások számát
- A böngésző alapú felügyelet nagyban leegyszerűsíti a beavatkozást, ugyanakkor hatékony elemző eszközöket biztosít
- Rugalmas alkalmazási lehetőségek, például:
  - IPS 4200 sorozatú készülékek
  - ASA 5500 sorozatú készülékek integrált AIP-modulokkal
  - Integrált behatolásmegelőzéssel rendelkező útválasztók
  - IDSM-2 modulok a Cisco Catalyst 6500 sorozatú termékhez
- A Cisco ICS az IPS, az útválasztók és a kapcsolók infrastruktúráját használva hálózati szinten akadályozza meg a féreg- és vírusfertőzéseket

Megfontolandó kérdések

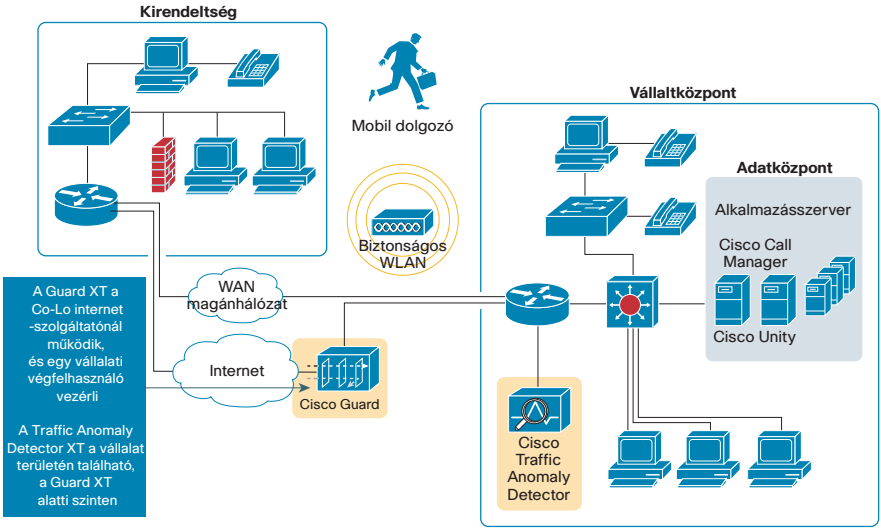
- Úgy véli, hogy részletes stratégiával rendelkeznek a hálózati behatolások észlelésére és elemzésére?
- Be tudná-e mutatni az auditoroknak, hogy összvállalati szinten egységes megközelítést és módszereket alkalmaznak a hálózat védelmére?
- Érte már pénzügyi veszteség a vállalatot hálózati fennakadás miatt?
- A jelenlegi IPS-megoldásnál bosszantónak tartja-e a hamis riasztásokat?
- Szeretné a féreg- és vírusfertőzéseket még a hálózat szintjén megállítani, mielőtt a munkaállomásokat is elérnék?

Megoldások a rendellenességek észlelésére és a veszélyek elhárítására

- Áttekintés
- A fő előnyök
- Megfontolandó kérdések

Áttekintés

- A Cisco rendellenességeket érzékelő és elhárító megoldásai nemcsak észlelik az elosztott elárasztásos (DDoS) támadásokat, hanem valós időben azonosítják és blokkolják a rosszindulatú forgalmat anélkül, hogy befolyásolnák a jogosult, feladatkritikus tranzakciókat
- Ennek eredményeként a megtámadott szervezetek továbbra is működőképesek maradnak, így a kritikus fontosságú vállalati eszközök és adatok állandóan megfelelő védelem alatt állnak



11. ábra – Alkalmazási területek

A fő előnyök

- Választ ad a hálózati és adatközponti erőforrások biztonságos rendelkezésre állásának igényére
- A jogosultnak tűnő, de rosszindulatú tranzakciófolyamot megállítva megakadályozza, hogy az befolyásolja a hálózat üzleti rendelkezésre állását
- Magasabb szintű, átfogó biztonságot nyújt
- Lehetővé teszi, hogy a tűzfal, a tartalomvizsgálat és a behatolásmegelőzés egymást kiegészítő biztonságos hozzáférés- és adatvédelmi funkciókat lássanak el
- Választható termékek:
  - Cisco Guard XT és Traffic Anomaly Detector XT dedikált készülékek
  - Cisco Catalyst 6500 sorozatú Guard és Traffic Anomaly Detector szolgáltatási modulok

Megfontolandó kérdések

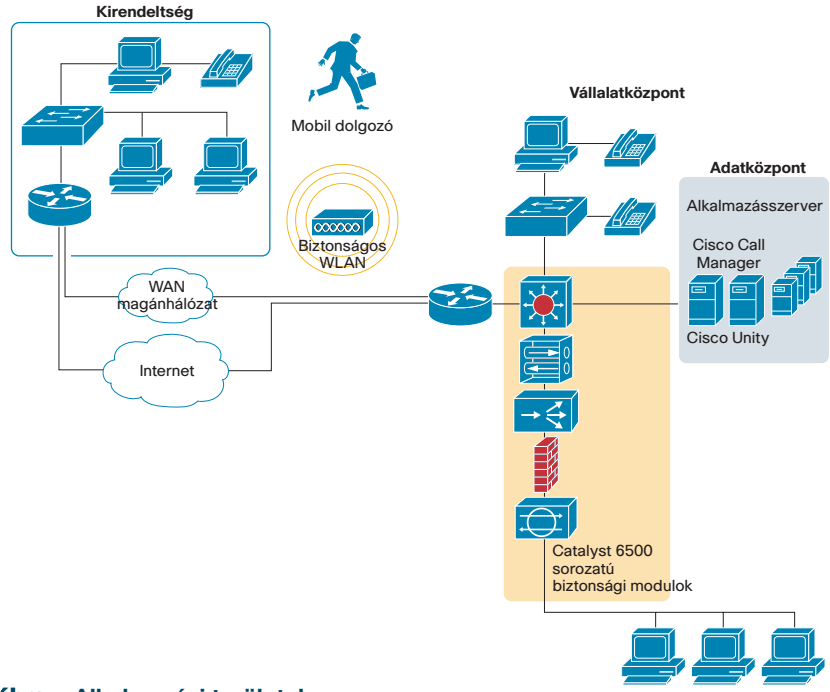
- Kedvezőtlenül érintené vállalatát, ha webhelyük elosztott elárasztásos támadás (DDoS) célpontjává válna?
- Felkészült arra a szervezete, hogy észlelje és elhárítsa a legkülönbözőbb DDoS-támadásokat?
- Biztosítani tudják-e a folyamatos működést úgy, hogy a jogos tranzakcióknak engedélyezik a vállalati webhely elérését, míg a jogosulatlan tranzakciókat más helyre irányítják?
- Tudja-e, hogy a Cisco rendellenességet érzékelő és elhárító megoldásait felügyelt szolgáltatásként is lehet kínálni olyan ügyfeleknek, akik nem engedhetik meg, hogy saját DDoS-védelmet alakíthassanak ki?

Cisco Catalyst 6500 sorozatú biztonsági modulok

- Áttekintés
- A fő előnyök
- Megfontolandó kérdések

Áttekintés

- A Cisco olyan integrált hálózati biztonsági szolgáltatásokat kínál a Cisco Catalyst 6500 sorozatú kapcsolók sokoldalú biztonsági moduljaival, mint például a tűzfal, az IPS, az IPSec és SSL alapú VPN-ek, az SSL-gyorsítás, illetve a DDoS-védelem és a gigabites hálózatelemzési modul
- Ezek a biztonsági modulok integrált, nagy rendelkezésre állású, alkalmazkodó védelmű és jól méretezhető biztonsági megoldást kínálnak mind a hálózati kapcsolat, mind a hálózati szolgáltatások és alkalmazások terén



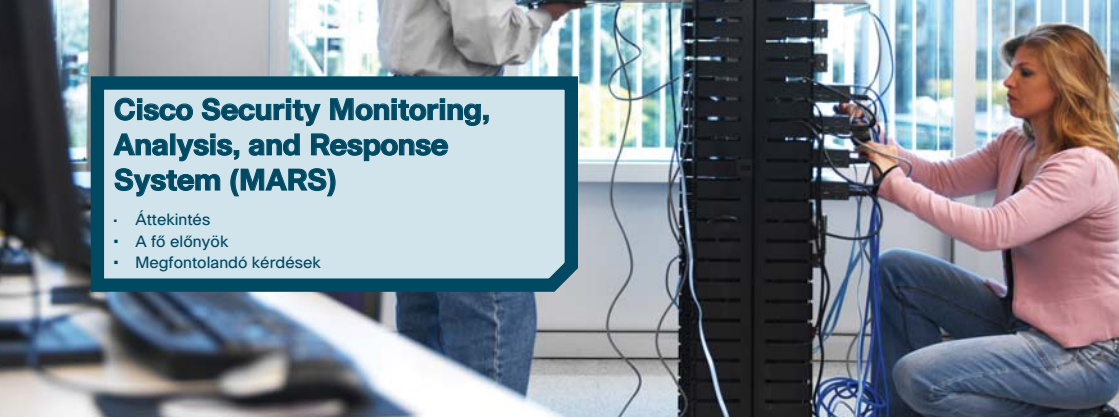
12. ábra – Alkalmazási területek

A fő előnyök

- Használja ki a Cisco Catalyst 6500 sorozatú kapcsolókban rejlő lehetőségeket!
- Szorosan integrált infrastruktúrabiztonsági megoldások
- A legnagyobb teljesítményű biztonsági megoldások, amelyek több gigabites teljesítményt garantálnak egyetlen Cisco Catalyst 6500 sorozatú kapcsolón belül
- Alkalmazás szintű betekintés az infrastruktúrába
- Kulcsfontosságú platform az új technológiák együttműködéséhez (pl. alkalmazások hálózati együttműködése)

Megfontolandó kérdések

- VPN-szolgáltatásmodul
  - Az ágazati előírások betartása céljából hogyan tervezik megvalósítani a teljes hálózatra kiterjedő nagyteljesítményű titkosítást?
  - Gondolt már arra, hogy a VPN-technológiát használják olyan biztonságos vezeték nélküli hálózat kialakítására, amelyben a biztonság nem befolyásolja kedvezőtlenül a teljesítményt?
- Tűzfalas szolgáltatásmodul
  - A leginkább javasolt biztonsági stratégiák a végpontokhoz lehető legközelebb kívánják megoldani a szabályérvényesítést, és nagyobb fokú szegmentálást kínálnak a hálózatok között. Az Önök stratégiája illeszkedik ehhez az elképzeléshez?
- Web-VPN szolgáltatásmodul
  - Szeretné, ha Catalyst 6500 sorozatú kapcsolója nagy teljesítményű SSL VPN-kapcsolatokat is biztosítana?
- SSL-szolgáltatásmodul
  - A kapcsolatok száma és a tanúsítványok kezelése szempontjából hogyan méretezik a webszerverfarmok SSL-teljesítményét?
- Hálózatelemző modul
  - Milyen stratégia alapján elemzik a hálózati forgalmat, hogy támadás esetén beazonosíthassák az ismeretlen veszélyforrásokat?
- Behatolásészlelő rendszermodul
  - Hogyan tervezik beazonosítani és blokkolni azokat a rosszindulatú támadásokat, amelyek már bejutottak az alaphálózatba?

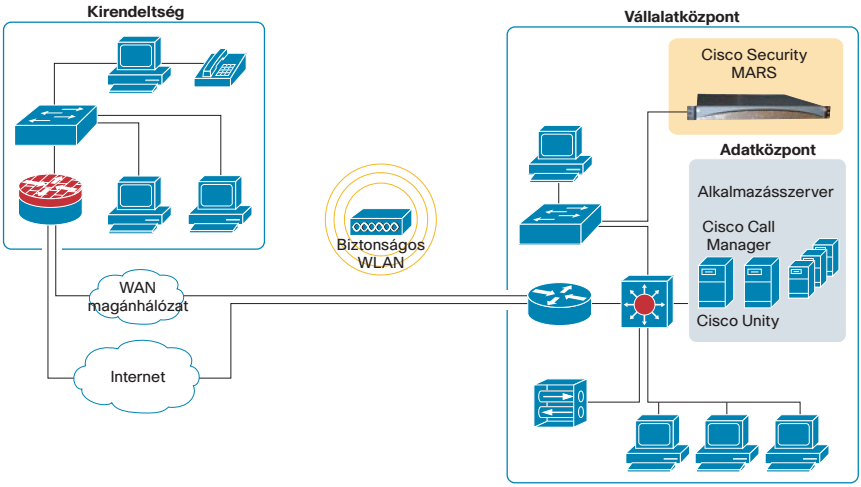


Cisco Security Monitoring, Analysis, and Response System (MARS)

- Áttekintés
- A fő előnyök
- Megfontolandó kérdések

Áttekintés

- A Cisco Security MARS a veszélyforrások kezelésére, megfigyelésére és elhárítására használt nagy teljesítményű, jól méretezhető készülékcsalád, amelynek segítségével az ügyfelek hatékonyabban kihasználhatják hálózati és a biztonsági eszközeiket
- A Cisco Security MARS a biztonsági események hagyományos figyelését és az automatikus elhárító funkciókkal rendelkező hálózati intelligenciát egyesíti
- A Cisco Security MARS a Cisco Security Management Suite biztonságfelügyeleti csomag része, amely a Cisco önvédő hálózat biztonsági szabályainak adminisztrációját és átfogó érvényesítését teszi lehetővé.



13. ábra – Alkalmazási területek

A fő előnyök

- Kiszűri a számos különböző hálózati összetevőn (Cisco és más gyártmányú termékeken) áthaladó adatokat, megkeresi köztük az összefüggéseket, majd elhárítja az esetleges támadásokat
- Képes megállítani a folyamatban lévő támadásokat, és felfedni a támadás útvonalát
- A dedikált készülék egyszerűen és pillanatok alatt üzembe helyezhető
- Kiváló teljesítmény: másodpercenként akár 10 000 eseményt is képes kezelni

Megfontolandó kérdések

- Vállalata maximálisan kihasználja meglévő biztonsági eseményfigyelő infrastruktúrájának lehetőségeit?
  – Rendelkeznek-e egyáltalán ilyen infrastruktúrával?
- Észreveszik, ha hálózatukon támadás van terjedőben?
- Szeretnék, ha hálózatukban az ismert és az ismeretlen támadásokat egyaránt el tudnák hárítani?
- Mikor nézték meg utoljára a tűzfal vagy az IDS naplófájljait?
- Rendszeresen be kell számolniuk a vezetőségnek a biztonsági helyzet napi alakulásáról?
- Hogyan akadályozzák meg, hogy a biztonságot érintő események fennakadást okozzanak a vállalat működésében?
- Hogyan gondoskodnak a kulcsfontosságú kiszolgálók és szolgáltatások előírásosságáról?

Cisco Security Manager

- Áttekintés
- A fő előnyök
- Megfontolandó kérdések

Áttekintés

- A Cisco Security Manager a kategóriájában legjobb vállalati szintű megoldás a tűzfalak, virtuális magánhálózatok és behatolásmegelőző rendszerek biztonsági házirendjeinek kezelésére
- A Cisco következő eszközeinek biztonsági konfigurálását támogatja: a biztonsági funkciókészlettel rendelkező IOS szoftvert tartalmazó Cisco útválasztók, a Cisco ASA 5500-as sorozatú adaptív biztonsági berendezések, a Cisco PIX biztonsági készülékek, a Cisco IPS 4200 sorozatú behatolásészlelők és a Cisco Catalyst 6500-as sorozatú tűzfal-szolgáltatásmodulok
- A Cisco Security Manager sokoldalú, de igen könnyen kezelhető funkcióival kiválóan alkalmas a kisebb és nagyobb hálózatok hatékony felügyeletére egyaránt
- A Cisco Security Manager a Cisco Security Management Suite biztonságfelügyeleti csomag része, amely a Cisco önvédő hálózat biztonsági szabályainak adminisztrációját és átfogó érvényesítését teszi lehetővé

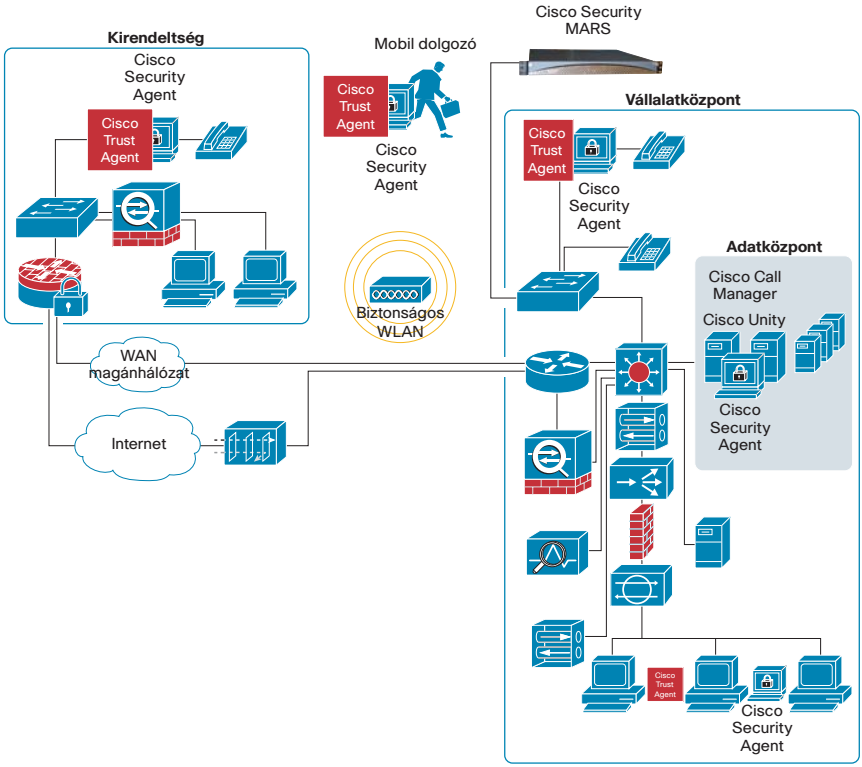
A fő előnyök

- Rugalmas méretezhetőség házirend alapú felügyelettel
- Gyorsabb reagálás a jelentkező veszélyekre: az új biztonsági szabályokat pár egyszerű lépésben lehet akár egyszerre több ezer eszközhöz definiálni és hozzárendelni
- Funkciógazdag grafikus felület a könnyű kezelhetőség érdekében
- Központilag előírhatók olyan közös biztonsági házirendek, amelyeket az új eszközök automatikusan átvesznek, így a vállalat biztonsági házirendje a hálózat egészében következetesen érvényesül
- Egyetlen közös tűzfalszabály-táblázatot lehet létrehozni az összes érintett Cisco eszköz számára
- A VPN-varázslóval pár egyszerű lépésben, könnyen konfigurálhatók a telephelyek közti, csillag vagy hálós topológiájú, illetve extranetes VPN-ek

Megfontolandó kérdések

- Egyre több pénzbe és időbe kerül a hálózat adminisztrációja és üzemeltetése?
- Szükség lenne egy közös felügyeleti alkalmazásra az összes Cisco tűzfal, VPN vagy IPS-rendszer biztonsági konfigurálásához?
- Új veszélyek jelentkezése esetén szeretnék gyorsabban beállítani a megfelelő biztonsági szabályokat az összes érintett eszközön?
- Egyre nehezebb képzett szakembereket találni az újabb és újabb biztonsági berendezések üzemeltetéséhez?
- Ha megfelelő felügyeleti megoldásokat találnának, hatékonyabban szervezhetnék jelenlegi szakembergárdájuk munkáját?

14. ábra –Átfogó megoldás a Cisco önvédő hálózattal



Cisco Systems Magyarország Kft.
1123 Budapest, Csörsz u. 45. Telefon: (1) 225 4600 Fax: (1) 225 4611 www.cisco.hu