A CISCO ÖNVÉDŐ HÁLÓZAT LEGÚJABB FEJLESZTÉSEI

ÁCS GYÖRGY
GACS@CISCO.COM

Networkshop 2006

Tartalom

IT BIZTONSÁG - TRENDEK

Trendek

- Karantén szolgáltatások
- Hosztok védelme
- Biztonsági riportok – törvényi előírások
- Integrált biztonsági megoldások

A CISCO ÖNVÉDŐ HÁLÓZATI KONCEPCIÓJA

Cisco önvédő hálózati stratégiája

ÖNVÉDŐ HÁLÓZAT

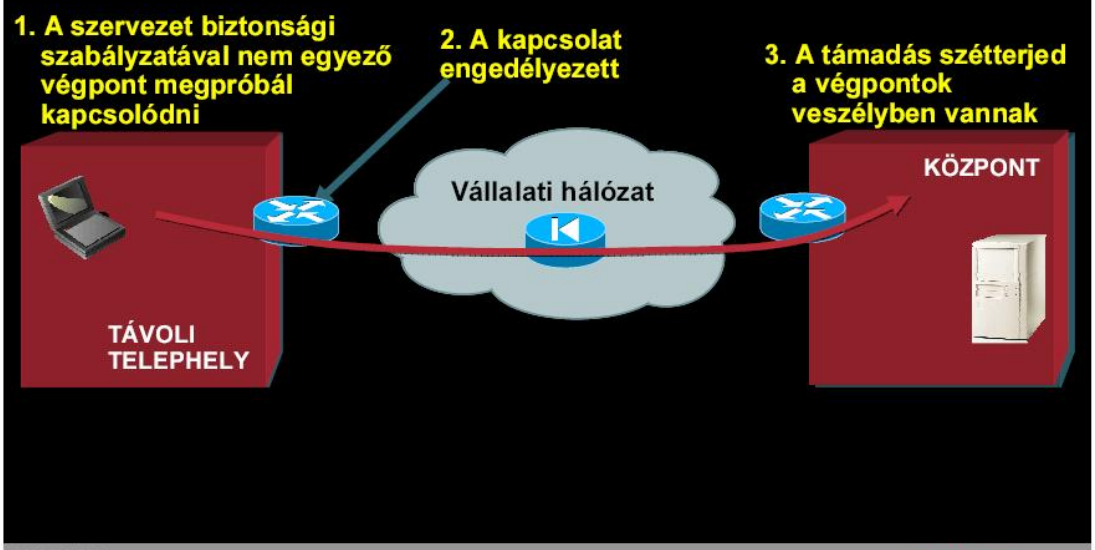
Cisco stratégia, nagy mértékben javítja a hálózat képességét, hogy azonosítsa és megelőzze a veszélyeket, és adaptálódjon

INTEGRÁLT BIZTONSÁG	EGYÜTTMŰKÖDŐ BIZTONSÁGI RENDSZEREK	ADAPTÍV FENYEGETÉS ELHÁRÍTÁS

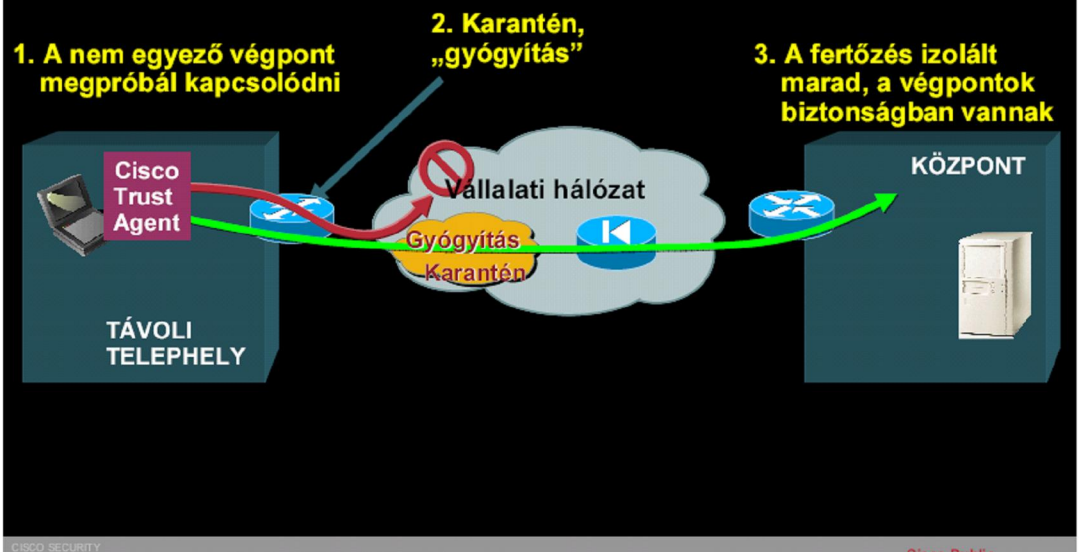
LEGÚJABB FEJLESZTÉSEK

ÖNVÉDŐ HÁLÓZATOK - 2. FÁZIS

Eddigi megoldások veszélye



Ahogy a Network Admission Control működik



Cisco Network Admission Control (NAC)

- A NAC a Cisco vezette iparági program, melynek célja az egyre inkább elterjedő biztonsági veszélyek (férgek, vírusok) által okozott károk csökkentése
- A NAC által az üzemeltetők a hálózati hozzáférést a hiteles végpontok (PDA, PC, szerver) számára engedélyezni tudják, míg a nem megfelelő eszközöket korlátozzák
- Ez a fejlesztés nagy mértékben javítja a hálózat képességét, hogy azonosítsa, megelőzze a veszélyeket és adaptálódjon hozzájuk

AhnLab, netForensics, SENFORCE, secure elements, infoexpress, CITADEL SECURITY SOFTWARE, BIGFIX

TREND MICRO, symantec., Network ASSOCIATES YOUR NETWORK. OUR BUSINESS., IBM, ca, Microsoft

Erős NAC Partner Program

http://www.cisco.com/en/US/partners/pr46/nac/partners.html

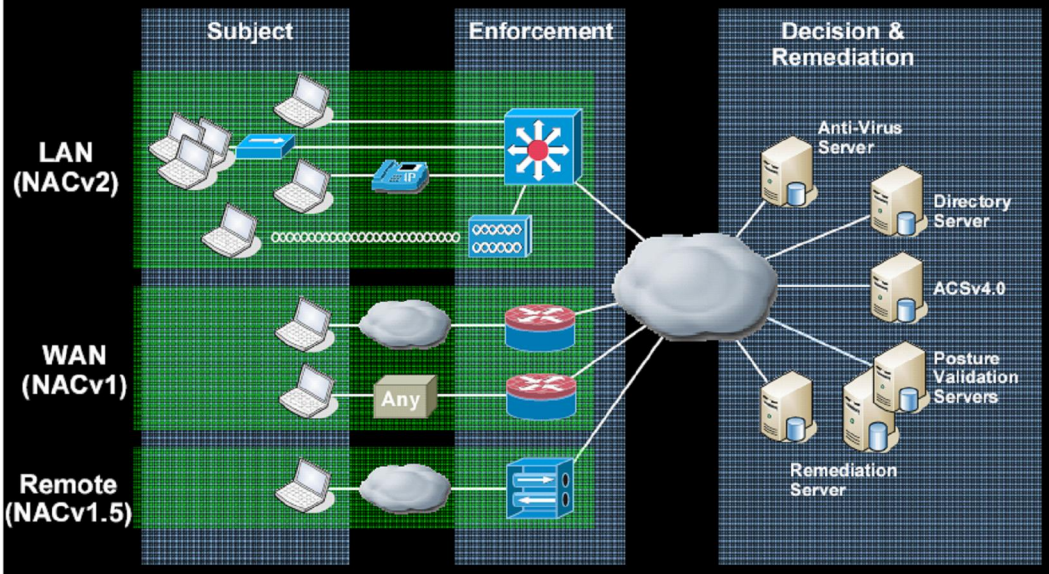
ANTI VIRUS: McAfee, ca, SOPHOS, AhnLab, symantec., F-SECURE, 金山在线 www.kingsoft.com, TREND MICRO, RISING 瑞星, NORMAN, Panda

REMEDIATION: altiris, BIGFIX, hp invent, IBM, iPass, LANDesk SOFTWARE, PATCHLINK

AUDIT: altiris, McAfee, QUALYS, symantec.

CLIENT SECURITY: Aranda, BELARC, Check Point, INTERNET SECURITY SYSTEMS, phoenix, SENFORCE, TRUST DIGITAL, BindView, CITADEL, elemental security, PREDATORWATCH, StillSecure, ENDFORCE, intel, SYGATE, BLUECAT NETWORKS, PREVENTSYS, symantec., NEW BOUNDARY, CONSENTRY, Safend, VERDASYS, FIBERLINK, IPSWAT, CA MASS, CREDANT, TriGeo, tenebril, vmware, ECUTEL, infoexpress, secure elements, WEBSENSE

NAC keretrendszer – megvalósítási esetek



ANTI-X ÉS SSL VPN SZOLGÁLTATÁSOK

ASA

- Többfunkciós biztonsági megoldás:
  - Tűzfal, VPN, IPS, Antivírus, SSL VPN, ...
- Új hardver platform (alaplapi titkosító chip)
- ASA OS nagyon hasonló a PIX OS v7-hez
  - Különbségek:
    - SSL VPN
    - IPS, antivírus/ SPAM / URL szűrő modulok
    - hardver adta különbségek (failover, USB)

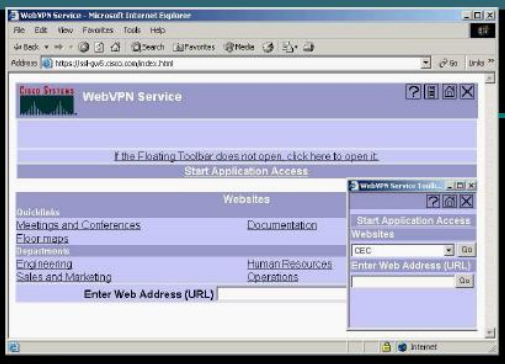
Content Security and Control SSM - ASA
Termék leírás

- Funkciója: tartalom vezérlés, veszély elhárítás az internet bejáratnál, piac-vezető technológia:
  - átfogó antivírus, anti-spyware,
  - file blocking,
  - anti-spam, anti-phishing,
  - URL blocking és filtering (munkaidő, azon túl -> kategóriánként),
  - tartalom szűrő szolgáltatások
- díjnyertes anti-vírus technológia a Trend Micro's InterScan security suite alapján
- Teljes védelem átfogó vírus és malware adatbázis

Modellek:
CSC-SSM-10 - 500 felhasználó
CSC-SSM-20 - 1000 felhasználó

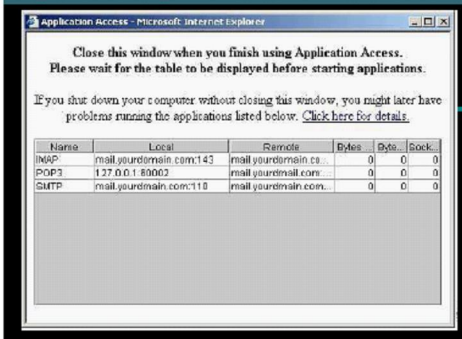
Trend Micro Certifications

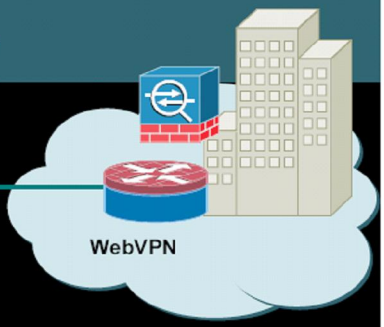
Kliens nélküli hozzáférés
Testreszabható távoli alkalmazás hozzáférés



- Bárhonnan hozzáférhetőek a cég felajánlott erőforrásai
- Web tartalom transzformáció > kompatibilitás a HTML és a JavaScript weblapokkal
- Egységes és hatékony alkalmazás megvalósítás – teljesen kliens nélküli Citrix támogatás
- Alkalmazások: Intranet (HTML és JavaScript), Citrix, Windows File Share (CIFS)
- Többféle browser támogatás – sokféle kapcsolat

Kliens nélküli hozzáférés
Port Forwarding Application Helper

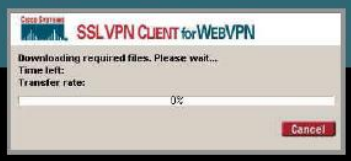




Java-based alkalmazás „helper” kiegészíti a kliens nélküli hozzáférést , kapcsolatot biztosít nem webes alkalmazásokhoz applications

- POP, SMTP vagy IMAP e-mail
- Instant messaging
- Calendar
- Kliens kezdeményezte TCP alapú alkalmazások, mint pl.: telnet

Cisco SSL VPN Client
Teljes hálózati hozzáférés



Szolgáltatás	Előny
IPsec - szerű alkalmazás hozzáférés "web-pushed" kliens segítségével	Teljes hálózati hozzáférés
Csak központi konfiguráció	Alacsony működési költség
Kompatibilis a Cisco softphone-nal - VoIP támogatás	Multimédia - adat, hang
A kliens maradhat a kapcsolat végén az adott gépen, vagy törölhető	Nagyobb biztonság – kapcsolat után nincs nyoma a kliensnek
Kevesebb, mint 250KB	Gyors kliens letöltési idő
Nincs szükség újra indításra	Egyszerűbb, kényelmesebb

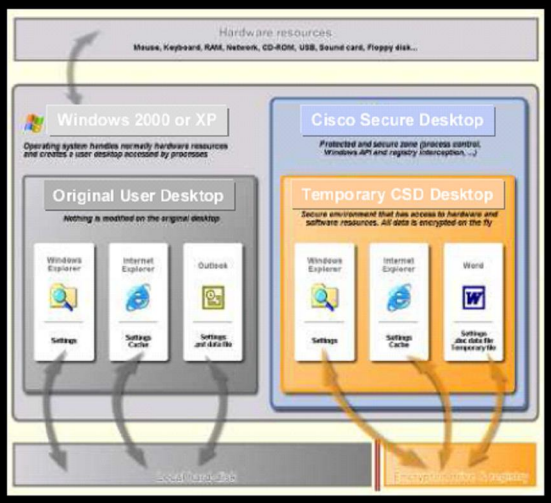
Nagy biztonságú VPN
Cisco Secure Desktop: átfogó végponti biztonság az SSL VPN számára

Teljes kapcsolat előtti kiértékelés:
- Hely kiértékelés – managed vagy unmanaged desktop?
- Security posture assessment – AV operational/up-to-date, personal firewall operational, malware present?

Átfogó kapcsolat alatti védelem:
- Adat „sandbox" és titkosítás véd minden kapcsolatot
- Malware detektálás a Microsoft free anti-spyware software segítségével

Kapcsolat uáni tisztítás
- Encrypted partition overwrite (not just deletion) using DoD algorithm
- Cache, history and cookie overwrite
- File download and email attachment overwrite
- Auto-complete password overwrite

Desktop Guest jogosultsággal is működik, nem kell admin jogosultság



CISCO SECURITY MANAGEMENT SUITE

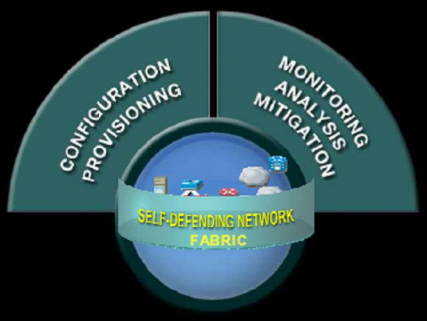
Menedzsment alkalmazások

Cisco® Security Manager

Egyszerűsített policy adminisztráció

Végponttól végponting terjedő konfiguráció

Hálózati széles vagy eszköz specifikus



Cisco® Security Mars

Gyors veszély azonosítás és enyhítés

Topológia tudása

Adat korreláció

ACS

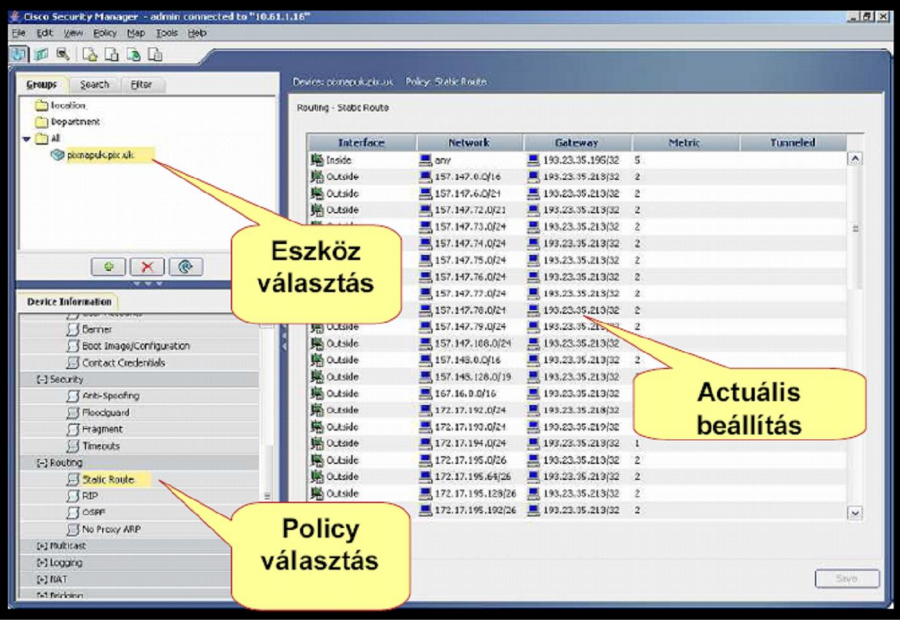
Cisco Security Manager 3.0

- ✓ **Feladata:**
  - **Kliens/szerver alkalmazás** a tűzfalak és a VPN menedzselésére - Cisco platformok támogatása
  - **Könnyű, áttekinthető kezelhetőség** + skálázhatóság
  - **Bővíthetőség:** CiscoWorks integráció, később IPS és más biztonsági technológiák vagy biztonsági menedzsment alkalmazások, mint például a CS-MARS
- ✓ **Támogatott termékek**
  - PIX és ASA biztonsági megoldások, IOS Firewall, FWSM Service Modules, VPN Service Module és ISR VPN (8xx – 72xx),
- ✓ **Támogatott technológiák**
  - **Teljes szolgáltatás lefedettség az appliance-ekre,** mint például a ASA/Pix/FWSM/VPNSM
  - Biztonsági szolgáltatások az IOS eszközökön : ACL-ek, NAT, SSH/SSL, HTTPS, High Availability, Dial Backup, PKI, Certificates, **NAC,** stb.…

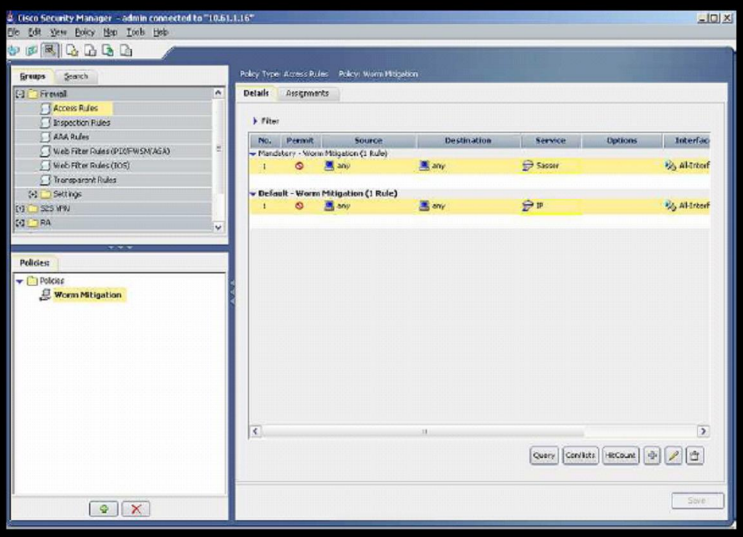
Az alkalmazás opcionális előnyei

- **Egységes felhasználói tapasztalat és szolgáltatás halmaz – heterogén eszköz család környezetben is**
- **Komplex feladatok leegyszerűsített megvalósítása grafikus felhasználói interfész segítségével**
- **Non workflow és workflow modellek és RBAC (Role Based Access Control) illetve felhasználói típusok - jogosultságok és szolgáltatások + rollback**
- **Többféle nézet – a különböző megközelítési módok közül a felhasználó választhat**
  - Policy-based megközelítés
  - Device-based megközelítés
  - Map-based megközelítés

3 nézet: Device view



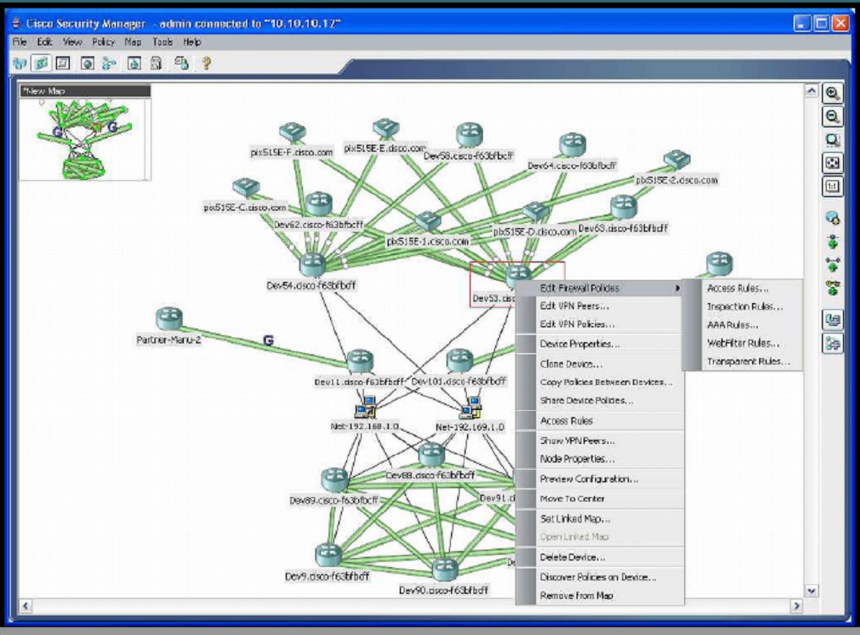
3 nézet: Policy View



Ebben a nézetben konfigurálhatók a skálázhatósági szolgáltatások:

- Policy Inheritance (örökítés)
- Policy Assignment (csatolás)
- Policy Sharing (megosztás)

3 nézet: Map centric view

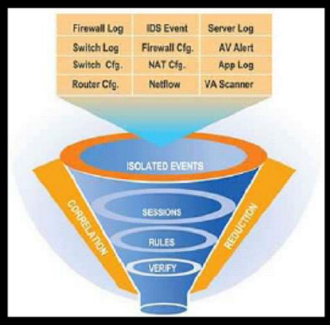


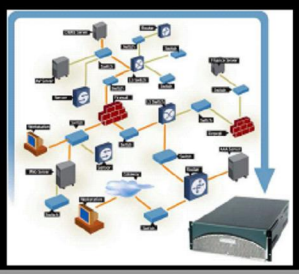
Biztonsági incidensek kezelése

- Támadások mindig lesznek -> elő kellene készülni
- Sokféle hálózati és biztonsági eszköz -> gigantikus mennyiségű napló -> valódi esemény?
- Válaszreakció?
- Törvényi előírások: Sarbanes-Oxley, Mo.: PSZÁF

Monitoring, Analysis, and Response System (MARS)
Új generációs SIM/STM

- A hálózatban **már meglévő** minden eszközben jelenlévő biztonsági szolgáltatásokat használja ki
- A vállalat egészén keletkező adatokat **korrelálja**
  - NIDS, tűzfalak, routerek, switch-ek, CSA
  - Syslog, SNMP, RDEP, SDEE, NetFlow, végpont esemény logok, több gyártó támogatása
- Gyorsan **lokalizálja és enyhíti** a támadásokat

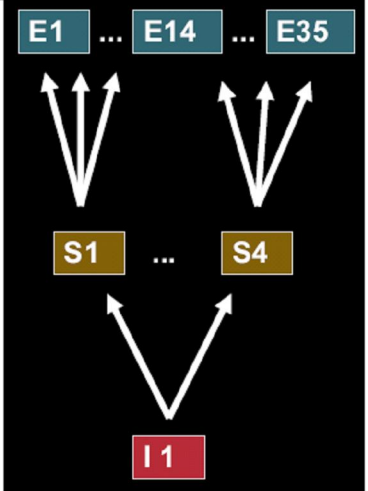




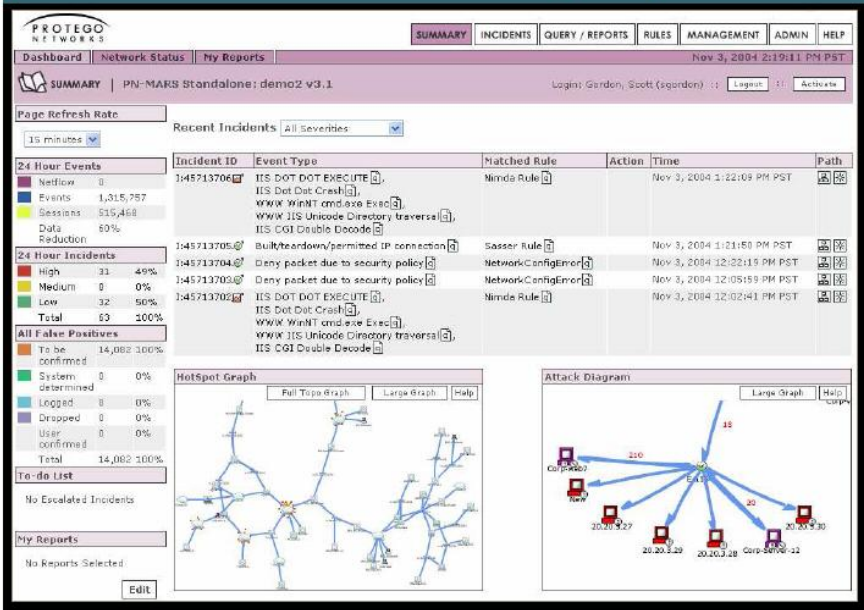
- Főbb jellemzők
  - Meghatározza az ***incidenseket*** az üzenetek, események és a kapcsolatok alapján
  - Az incidens ***topológiájának birtokában*** lehetőség van ábrázolásra és visszajátszásra
  - **Enyhítés** L2 és L3 „lezárópontokon”
  - A teljes vállalaton keresztüli hatékony **skálázhatóság** a valós idejű használatra

CS-MARS terminológiák

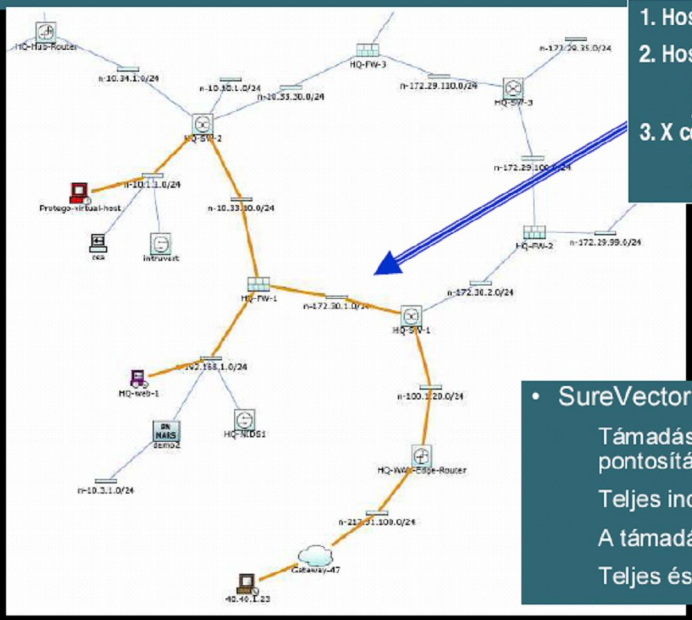
Események	Nyers üzenetek (pl.: IDS és tűzfal naplók), amelyeket a CS-MARS-nak küldenek a riportoló eszközök
Session-ök (kapcsolatok)	Olyan eseményből álló sorozat, melyeknek a végponti információi megegyeznek: Cél/Forrás IP cím Cél/Forrás Port és protokoll
Incidensek	Olyan kapcsolatokból álló sorozat, melyek egy definiált szabályra egyeznek



CS-MARS – analízis egy lapon



CS-MARS - a végpontok összekötése

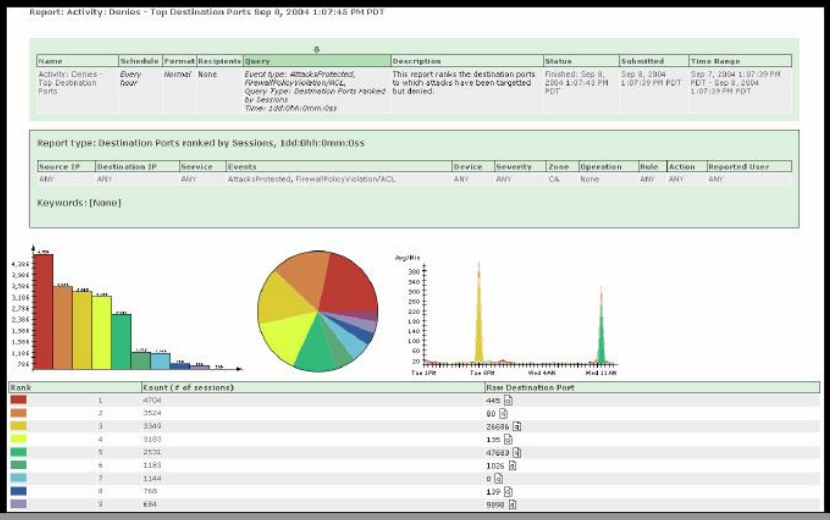


1. Host A port szkenneli X célt
2. Host A Buffer Overflow támadja X-et, ahol X NAT eszköz mögött van és X sérülékeny az adott támadásra
3. X cél jelszó támadást hajt végre Y cél ellen, ami egy NAT mögött lévő eszköz

- SureVector™ analízis
  - Támadási útvonal bemutatása és pontosítása
  - Teljes incidens és esemény részletezés
  - A támadás pontos forrásának kiderítése
  - Teljes és pontos történet

CS-MARS megfelelőségi riportok

A leggyakrabban használt riportok (beépített) – testreszabási lehetőség
Intuitív keretrendszer (nincs SQL konfigurálási igény)



KÉRDÉSEK ÉS VÁLASZOK

ÖSSZEFOGLALÁS

Összefoglalás

Témák:

- **IT biztonsági trendek**
- **Legújabb megoldások:**
  - **Önvédő hálózatok – 2. fázis**
  - **Anti-x és SSL VPN szolgáltatások**
  - **Cisco Security Management Suite**

További információ

NAC

www.cisco.com/go/nac

ASA

www.cisco.com/go/asa

CS Manager

www.cisco.com/go/csmanager

MARS

www.cisco.com/go/mars

Cisco SAFE Blueprints

www.cisco.com/go/safe