Cisco IT Biztonsági portfólió

CBSW szeminárium, 2008. június 10.

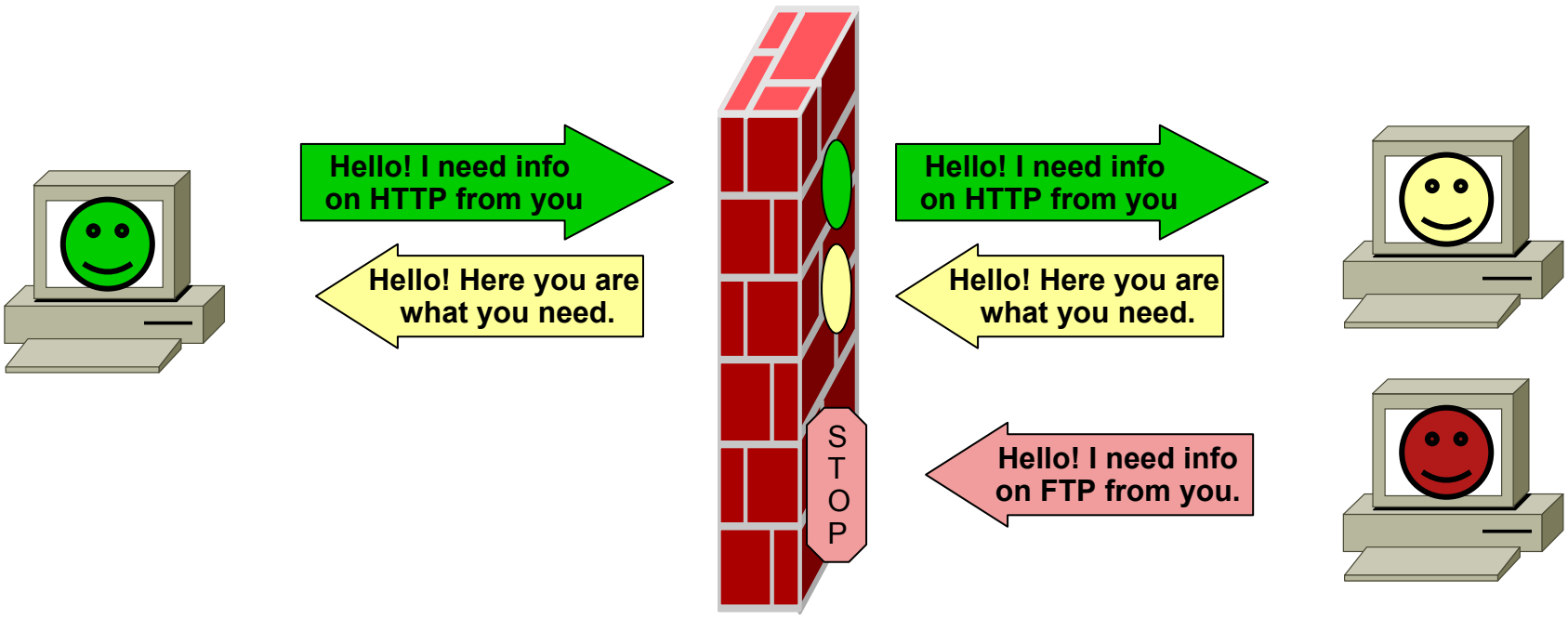
Segyik István, rendszermérnök

isegyik@cisco.com

Tartalom

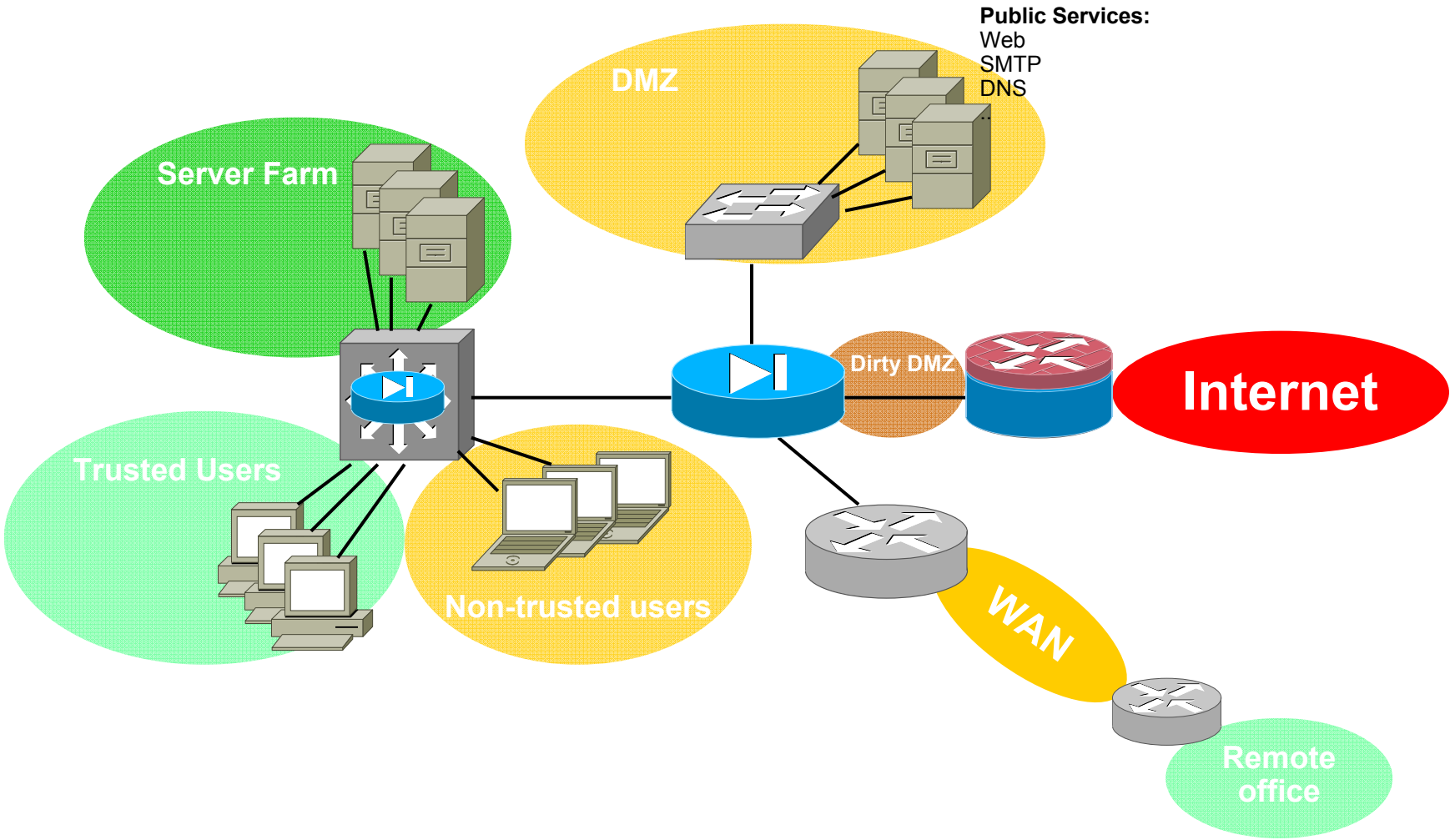
- Cisco Tűzfalak
- Cisco IPS-ek
- Application Level Gateway-ek (ALG)
- Cisco VPN megoldások
- Cisco Identity Management
- Beépített biztonság a Cisco infrastruktúrában
- Cisco Security Management
- Összefoglalás, kvíz

Alapvető Stateful inspection funkció?



Ez már nagyon kevés egy modern tűzfalban... ☹

Tűzfalak helye a hálózatban



Cisco Tűzfal megoldások - dióhéjban

- Cisco Security Appliance-ek és „tűzfalas” routerek sokkal többet nyújtanak szimpla stateful szűrésnél.
- Általános tűzfal termékek:

  Cisco ASA 5500 appliance-ek.

  Cisco router-ek Advanced Security vagy magasabb IOS-szel.

  Cisco Firewall Services modul Catalyst 6500 and 7600-hoz.
- Melyiket válasszuk?

?

ASA5500 series

- Inkább tűzfal, mint router...
- Nagyteljesítményű Stateful Packet Filtering extrákkal:

  Alkalmazás szintű protokol vizsgálat számos protokolra.

  Remote Access és Site-to-site VPN.

  Basic IPS alapesetben, Advanced IPS AIP-SSM modullal.

  Anti-x Web és SMTP ALG csomag CSC-SSM modullal.

- Miért is kell alkalmazás szintű protokol viszgálat:

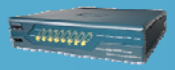
  Néhány alkalmazás egyáltalán nem- vagy csak nagy statikus réssel működne.

  Finomabb kontrol az alkalmazás felett: pl. Fájlcsere tiltása MSN-ben.

ASA 5500 modellek

Cisco ASA 5500 Platformok

- Nagy teljesítmény
- Feladatra optimalizált operációs rendszer
- HDD nélküli hardver
- Számos minősítés és díj
- Ergonómikus web interfész
- ...



ASA 5505

ASA 5510

ASA 5520

ASA 5540

ASA 5550

ASA 5580-20

ASA 5580-40

Teleworker | Branch | Internet Perem. | Belső szegmentáció | Data Center

Tűzfal a Cisco routerek-ben

- Advanced Security vagy magasabb IOS Feature set:
  - Stateful Inspection tűzfal alkalmazás vizsgálattal.
  - Remote Access és Site-to-site VPN-ek.
  - IOS Intrusion Prevention System közepes komplexitással és alacsony teljesítménnyel (dedikált IPS-ekhez képest).
  - Szeparált IPS hardvert alkalmazhatunk.
- ICSA és Common Criteria minősítések (ua., mint ASA).
- Grafikus felhasználói interfész (Router SDM).
- Majdnem minden routeren elérhető.

Valós IOS Firewall teljesítmény ISR routereken

Platform	76byte			TCPIMIX			1400 byte		
	pps	Mbps	CPU %	pps	Mbps	CPU %	pps	Mbps	CPU %
Cisco 1841	36,112	22	99%	35,528	102	99%	17,604	197	88%
Cisco 2801	36,112	22	99%	35,528	102	99%	17,604	197	88%
Cisco 2811	49,159	30	99%	48,048	138	99%	17,604	197	85%
Cisco 2821	87,474	53	99%	87,572	252	99%	84,445	946	99%
Cisco 2851	111,901	68	99%	109,498	315	99%	105,951	1,187	87%
Cisco 3825	156,666	95	99%	157,957	455	99%	157,783	1,767	99%
Cisco 3845	244,140	148	99%	243,927	703	99%	176,040	1,972	99%

Bizalmas, nem adható tovább harmadik személynek!

Firewall Services Module

- Cisco Catalyst 6500-as L3-as switch és 7600-as routerekbe.
- Teljesítmény:
  - 5 Gbps/modul,
  - 3 modul/eszköz.
- Gyors tűzfal VPN és IPS szolgáltatások nélkül.
- Alkalmazási területek:
  - Adatközpont (alternatíva ASA 5580-ra),
  - Belső szegmentáció.
- Általában hoszt rendszerrel együtt vagy utólagosan kerül értékesítésre.

ASA vagy Router?

- Attól függ...
- A legjobb mindkettő, néha szükséges is...
- Leegyszerűsítve:
  - •Amikor Site-to-Site VPN funkció nagyszámú telephellyel szempont, akkor ➲ ROUTER.
  - •Amikor Remote Access VPN sok felhasználóval szempont, akkor ➲ ASA.
  - •Amikor a nagy tűzfal teljesítmény a fő szempont, akkor ➲ ASA.

Tartalom

- Cisco Tűzfalak
- Cisco IPS-ek
- Application Level Gateway-ek (ALG)
- Cisco VPN megoldások
- Cisco Identity Management
- Beépített biztonság a Cisco infrastruktúrában
- Cisco Security Management
- Összefoglalás, kvíz

Network IPS (NIPS) típusok

- Mintázat alapú:

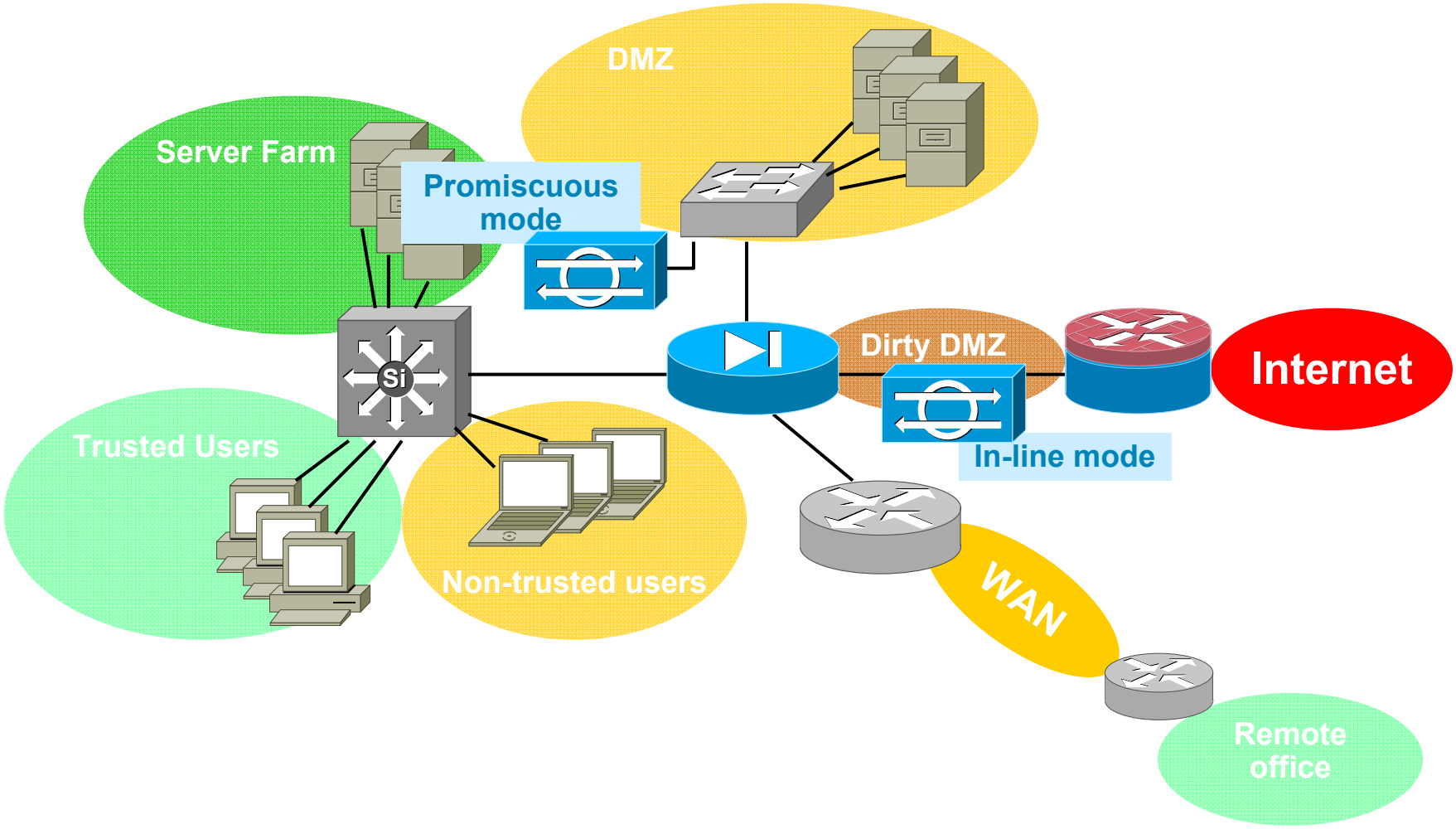
  Mintázatokkal előre definiált „ismert rosszindulatú tevékenységet” keres.
- Anomália alapú:

  Megtanulja a normális hálózati profilt és eltéréseket figyel.
- Policy alapú:

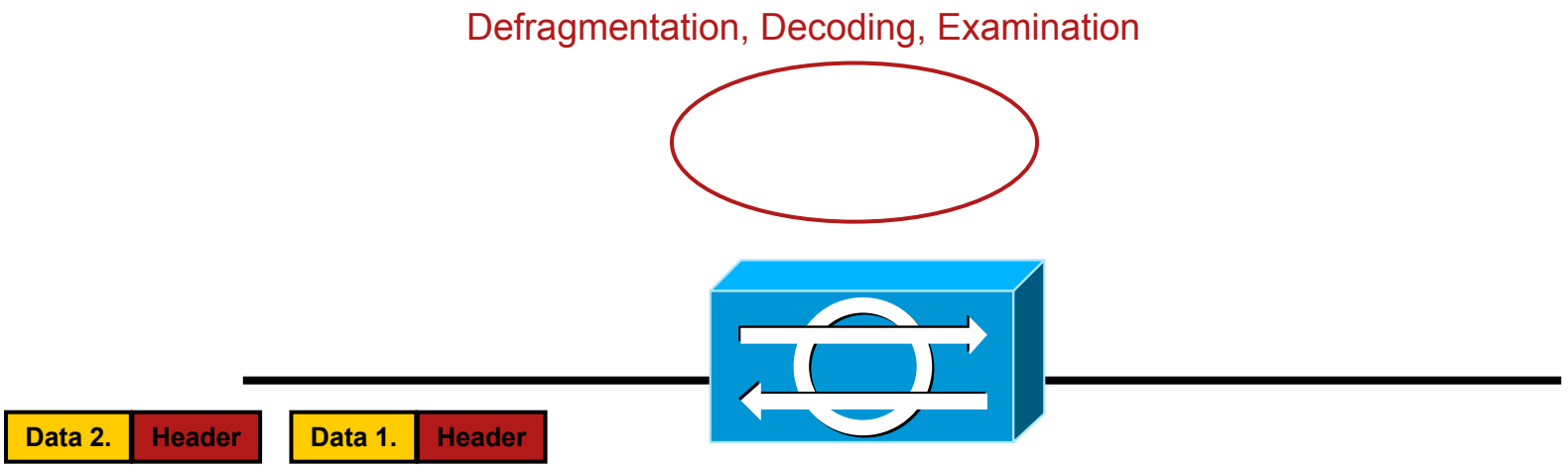
  Adminisztrátorok által készített szabályok döntik el, hogy mi a JÓ és mi a ROSSZ.
- Hibrid:

  Fentiek kombinációja.

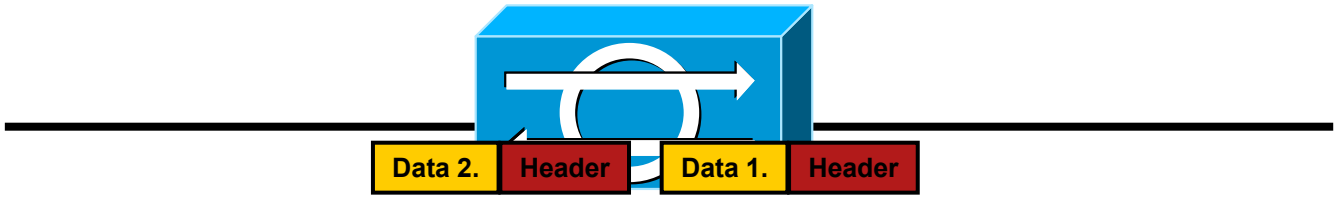
Network IPS telepítési módok



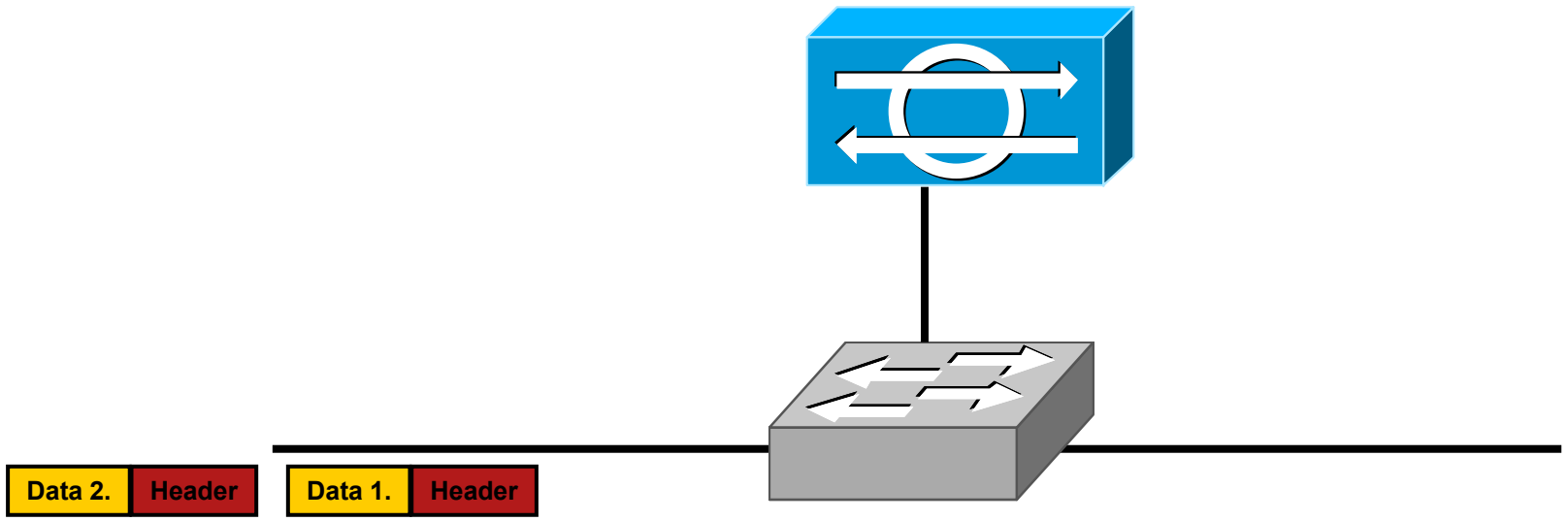
NIPS, in-line mód



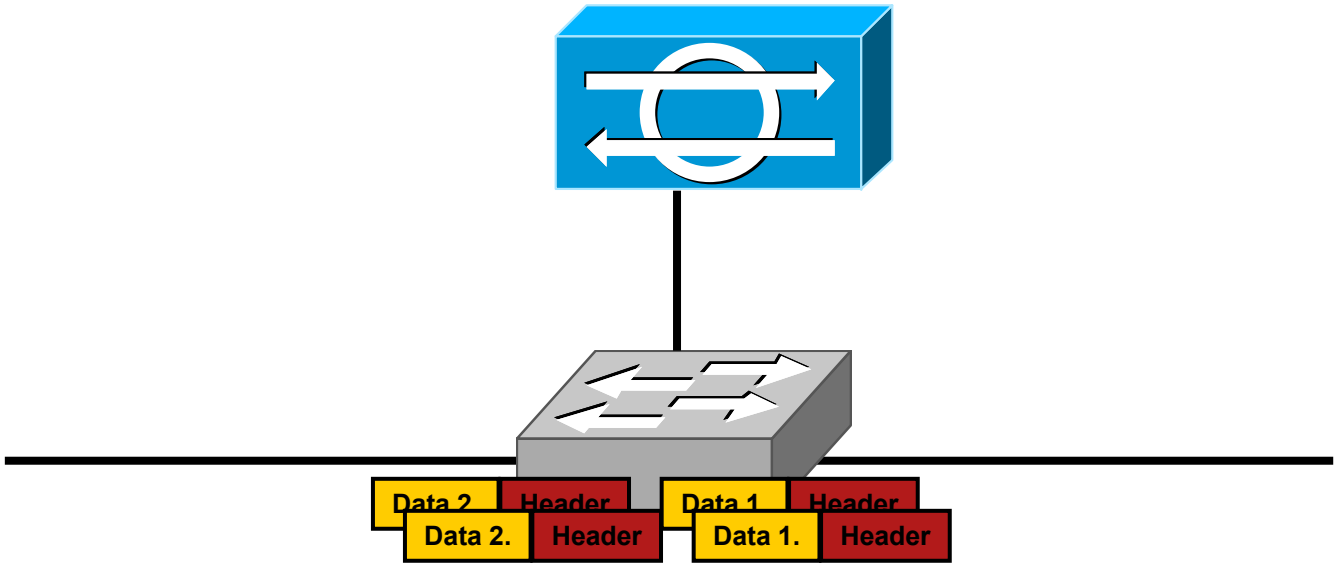
NIPS, in-line mód



NIPS „promiscuous” mód



NIPS „promiscuous” mód



NIPS In-line vs. Promiscuous mód

In-line	Promiscuous
• A valós forgalmat kezeli. • IPS be tud avatkozni egyedül, csomaeldobással. • Megállíthat egy csomagos ‘atomic’ támadásokat. • Meghibásodása hálózati leállással járhat. • Szűkkeresztmetszet lehet az átbocsájtóképessége.	• IPS csak másolatot kap. • IPS másik eszközön avatkozik be ACL-lel vagy TCP Reset-tel. • Nem tud megállítani ‘atomic’ támadásokat. • Nem okoz hálózati leállást az IPS hiba. • Nem okoz szűkkeresztmetszetet.

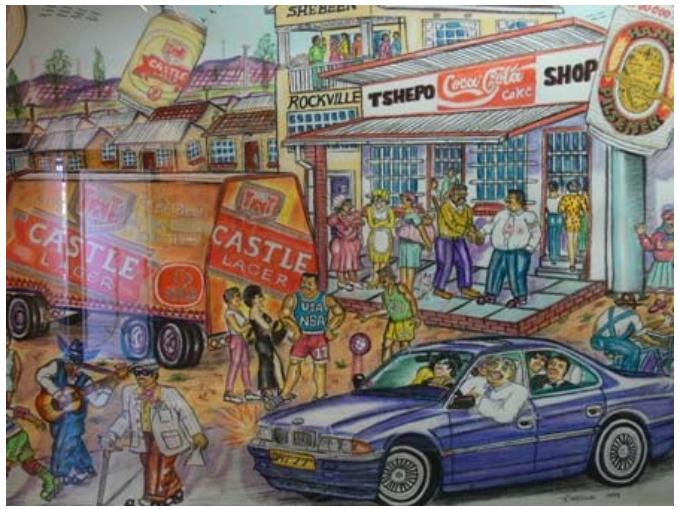
Cisco NIPS megoldások

- Dedikált erőforrással:
  - Dedikált eszközön vagy modulon.
  - In-line és Promiscuous mód.
  - Hardverek:
    - 4200-as dedikált szközök.
    - NM és AIM modulok ISR-ben.
    - SSM modulok ASA-ba.
  - Hibrid rendszer, de alapvetően mintázat alapú.
  - 65Mbps – 2Gbps.

- IOS IPS:
  - ISR routeren fut (871-es vagy jobb).
  - Mindig in-line (fail-open lehetséges).
  - A router CPU-ját és memóriáját használja!
  - Limitált teljesítmény: Kb. 1-10 Mbps.
  - Mintázat alapú.

Cisco IPS szerviz szolgáltatások

- Dedikált- és IOS IPS-hez egyaránt.
- IPS-nek kevés haszna van enélkül.
- Az általános SmartNet szolgáltatásokon felül:
  - IPS mintázat frissítés előfizetés.
  - Cisco Security Alert Center riasztások.
  - Cisco Security Alert Center és IntelliShield „read-only” hozzáférés.



Hoszt IPS?

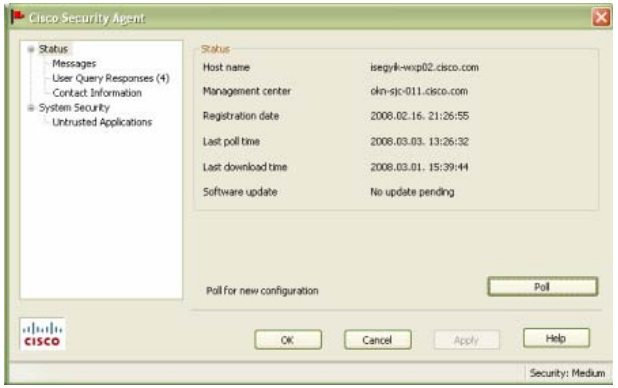
- A Hoszt IPS:
  - Szoftver „ügynök” egy hoszton.
  - A hosztra bízza a defregmentációt, kódolást és utána vizsgál tartalmat, kontextust stb.
  - Fregmentált-, több protokolt átfogó támadásokat is megtalálhat.
  - További extra funkciók jobb hoszt védelmet nyújthatnak.
- Hol érdemes használni?
  - Minimum minden kritikus hoszton ami titkosított forgalmat kezel.
  - Ajánlott minden kritikus munkaállomáson és szerveren.
  - A legjobb lenne miden hoszton alkalmazni.

Cisco Security Agent (CSA)

- CSA egy többfunkciós Agent szoftver.
- Átfogó hoszt védelem:
  - HIPS (Policy vagy szabályrendszer alapú),
  - Tűzfal protokol normalizációval,
  - Application Sandboxing és erőforrás kontrol,
  - Keylogger védelem,
  - QoS kontrol,
  - Adatvesztés- lopás megelőzés,
  - Szoftver leltár információk átadása más rendszereknek pl. NIPS-nek.

- Kliens-szerver architektúra, központi telepíthetőséggel-, frissíthetőséggel- és konfigurációval.
- Végfelhasználói interakció limitálható.

CSA a gyakorlatban



- Operációs rendszer „megerősítés”.
- Elengedhetetlen lesz IPv6 végleges bevezetésekor (amikor a titkosítás kötelező lesz).
- Nem plug-and-play.
- Általános vélemény:

‘A CSA-t relatíven nehéz implementálni, de az egyik legjobb proaktív hoszt védelmi megoldás a piacon’.

Tartalom

- Cisco Tűzfalak
- Cisco IPS-ek
- Application Level Gateway-ek (ALG)
- Cisco VPN megoldások
- Cisco Identity Management
- Beépített biztonság a Cisco infrastruktúrában
- Cisco Security Management
- Összefoglalás, kvíz

Rövid terminológia

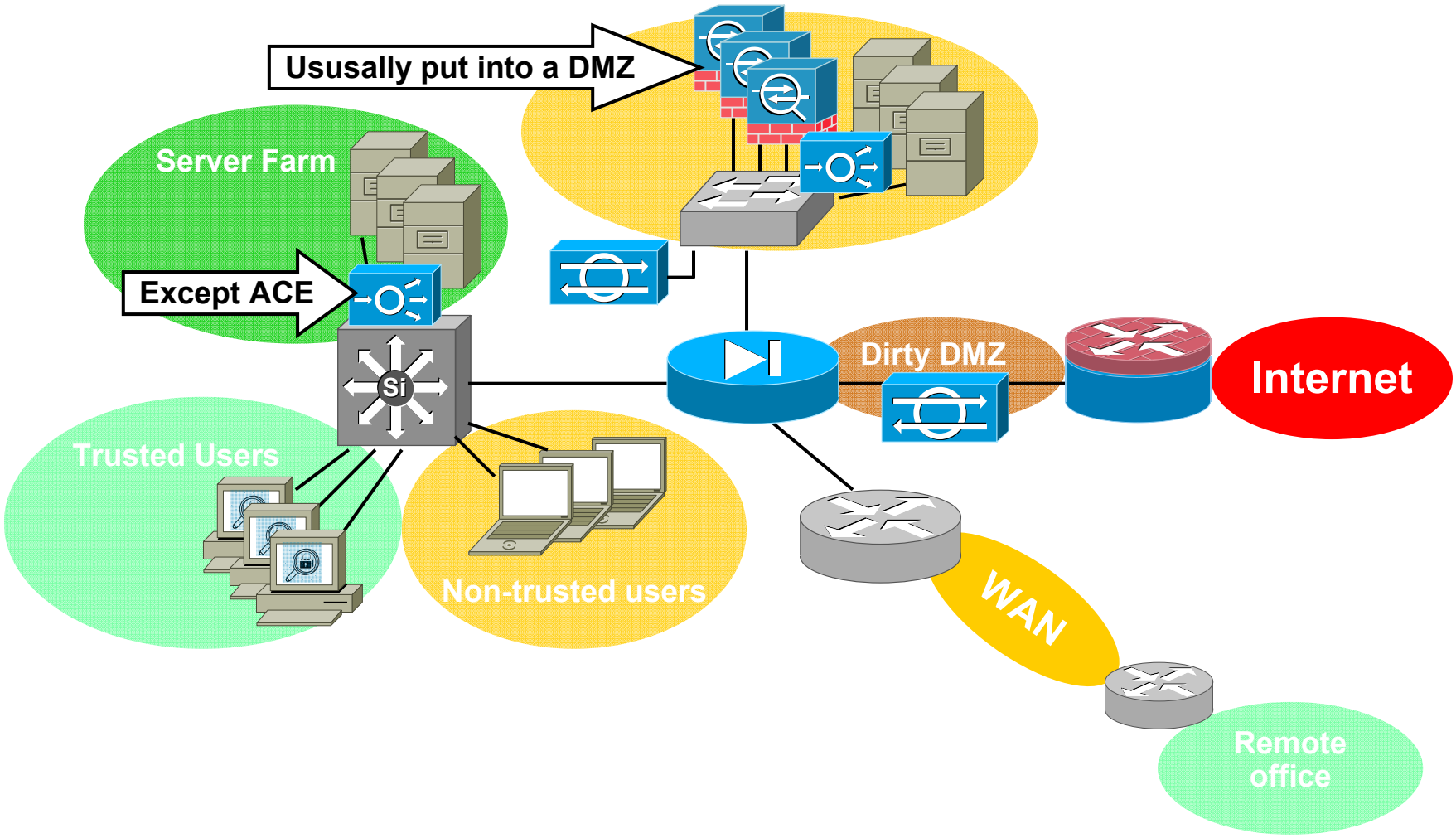
- Application Level Gateway (ALG):
  Speciális rendszer, amely egy-egy alkalmazás mély viszgálatával foglalkozik, gyakran proxy-ként működik.
- Mail sweeper:
  Internet peremzónába helyezett célrendszer, amely első védelmi vonalként helyezkedik el a tényleges postafiókokat kezelő szerver előtt.
- Web proxy:
  Speciális ALG, amely a belső hosztok számára teszi biztonságosabbá az Internet böngészését. Gyakran Cache funkciókkal is rendelkezik (gyorsít).
- Reverse Proxy:
  Speciális ALG, amely web szervereket véd kompromittáció ellen. Gyakran terhelésmegosztást is biztosít (teljesítményt javít).

Miért kellenek ALG-k?!

Mert egy-egy alkalmazásra nehéz fókuszálni másként:

- A tűzfalaknak a teljes IP címtartományban és minden TCP- és UDP porton kell dolgozniuk...
- Az IPS-ek a teljes címtartományban vizsgálják mind a 2x 65535 portot, defregmentálnak, korrelálnak...
- Igazán mély alkalmazás vizsgálathoz specifikus berendezés-, illetve szoftver kell.

ALG-k helye a hálózatban



Cisco ALG-k: Anti-X (CSC) modul ASA-ba

- Két hardver (SSM modul) verzió különböző teljesítménnyel.
- Cisco Specifikus Linux OS, TrendMicro InterScan Enterprise.
- Főbb funkciók:
  - Anti-Virus, Anti-SPAM, Anti-Phishing, E-Mail-re,
  - Anti-Virus, Anti-Phishing és dinamikus URL szűrés Web forgalomra.
- Skálázható n x 100 felhasználóra.
- HDD nélküli kialakítás:
  - ☺ Jó, mert kompakt és kisebb a meghibásodási esély,
  - ☹ Nem jó, mert egyenlőre nincs karantén funkció.
- A TrendMicro-s online frissítés előfizetés külön vásárolandó a SmartNet-től, de nem kell a Trend-től megvenni, Cisco is árulja

Cisco ALG-k: Ironport C-series E-Mail security

- Az Ironportot a Cisco tavaly vette meg: www.ironport.com.
- A C-series appliance az E-Mail (SMTP) ALG megoldásuk.
- Főbb paraméterek:
  - OEM, szerver kategóriás hardver.
  - Specializált BSD alapú UNIX OS: AsyncOS for E-mail security.
  - Anti-Virus (több motorral), Anti-SPAM, reputation filtering SenderBase-zek, egyéni viszgálati szabályok. Best in class...
  - Skálázhatóság: 100 to n x 10000 felhasználó per appliance. Cluster-ezhető (plusz párhuzamos feldolgozás ...).
- Dell alapú hardver és nagyon kedvező Sales és Support modell.
- Az Ironport saját terméktámogatási központot üzemeltet.

Cisco ALG-k: Ironport S-series Web security

- Web proxy az Internetet böngésző felhasználók (és a cég üzleteinek védelmére).
- Főbb funkciók:
  - Anti-virus több motorral.
  - Dinamikus URL szűrés.
  - Reputation filtering Senderbase-zel (www.senderbase.org).
  - Proxy és cache-elés.
  - TCP L4 protokol vizsgálat (65535 portra), worm call-home, misuse megelőzés.
  - HTTPs protokol vizsgálat Man-In-The-Middle (MITM) módszerrel.
- Skálázhatóság n x 1000 felhasználó per appliance.

Cisco ALG-k: Application Control Engine (ACE)

- Reverse HTTP (Web) proxy web szerverek védelmére.
- Jól pozícionálható amikor szükséges:
  - Szerver terhelésmegosztás.
  - Szerver védelem.
- Fontosabb biztonsági funkciók:
  - Proxy. Valós szerverek teljes megszemélyes
  - Nagy teljesítményű- nem állapottartó szűrés
  - IP és TCP megfelelőség ellenőrzés.
  - SSL off-load.

- Elérhető Catalyst 6500 és dedikált berendezés formátumban.
- SSL és Clear-text átbocsájtóképesség alapján licencelve.

Cisco ALG-k: a többi...

- CUBE:
  - A ‘Cisco Unified Border Element’ rövidítése.
  - IOS funkció, routeren futhat.
  - Külön licenc köteles.
  - SIP-, H.323 és MGCP jelzésrendszert, illetve RTP médiát kezel.
  - Proxy, megfelelőség ellenőrzés, NAT-tal kapcsolatos funkciók elsősorban biztonságos IP fővanalak létesítéséhez.
- Unified Mobile Communicator Proxy Server:
  - Kötelező amennyiben a Mobile Communicator-t asználjuk.
  - Megvédi és elrejti a belső Mob. Comm. Server-t.

Tartalom

- Cisco Tűzfalak
- Cisco IPS-ek
- Application Level Gateway-ek (ALG)
- Cisco VPN megoldások
- Cisco Identity Management
- Beépített biztonság a Cisco infrastruktúrában
- Cisco Security Management
- Összefoglalás, kvíz

Fontosabb rövidítések

- Virtual Private Network (VPN):
  Biztonságos kommunikáció egy publikus médián.
- IPSec:
  Tunneling, Encrpyption és Integrity Checking technológia IP hálózatok felett.
- Dynamic Multipoint VPN (DMVPN):
  NHRP protokolt alkalmazó-, Cisco specifikus IPSec kiterjesztés. Lehetővé teszi távoli telephelyek közötti direkt IPSec csatorna kiépítést dinamikusan, amikor szükség van rá.
- Generic Encrypted Tunnel (GET) VPN:
  Speciális IPSec transport mód megvalósítás központi kulcs menedzsmettel. Lehetővé teszi a fix tunnel-ek nélküli teljes hurkolt kommunikációt. MPLS VPN hálózatok titkosítására ajánljuk.

Important terms and abbreviations

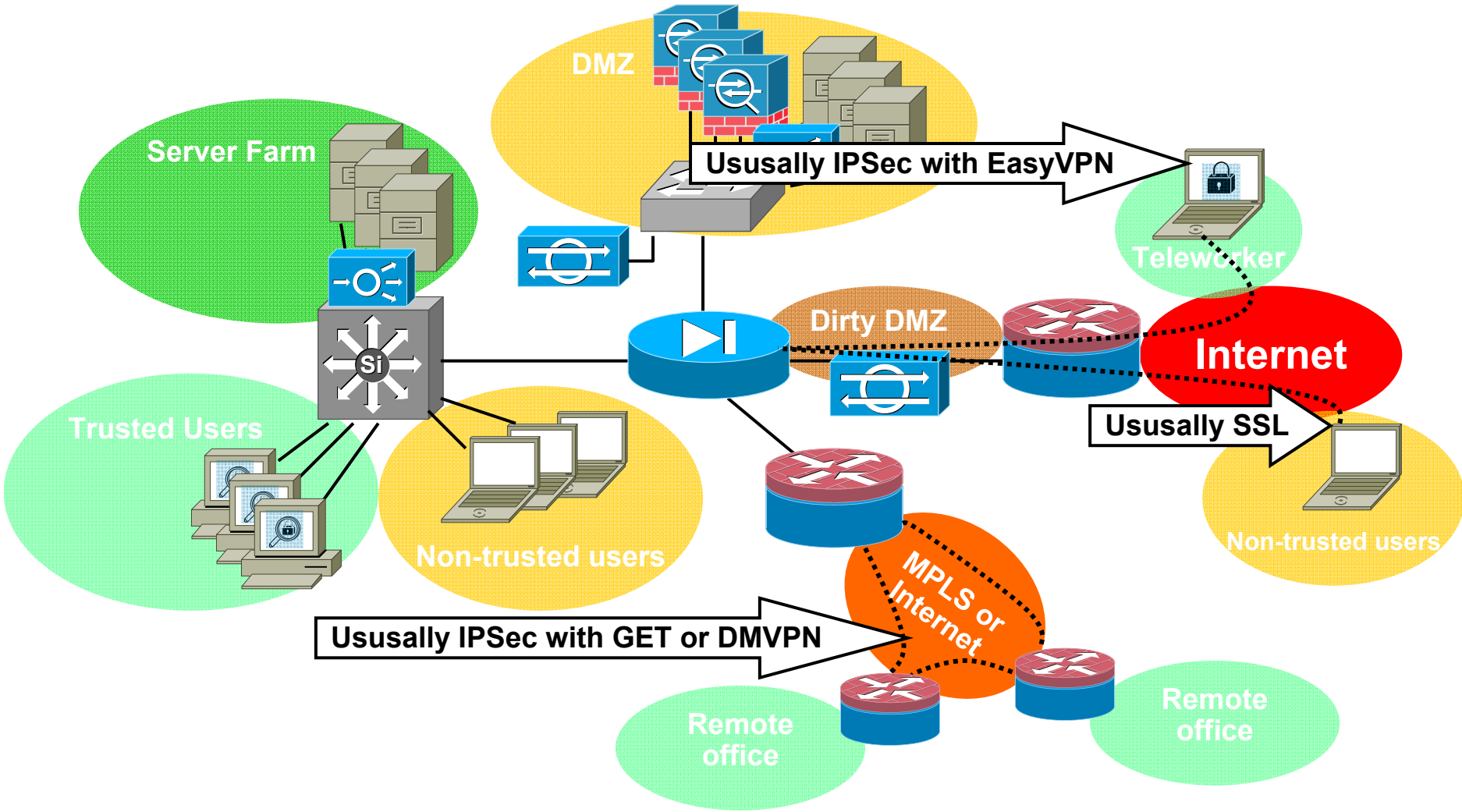
- WebVPN:

  SSL vagy TLS VPN-nek is nevezett VPN megoldás mobil- és otthoni felhasználók részére. A böngésző titkosítási motorját használja, illetve a speciális kiterjesztéseket is a böngészőben futtatja.
  Kliens nélküli módban is használható.

- Cisco Easy VPN:

  Cisco specifikus IPSec kiterjesztés amely célja a konfiguráció és kulcs menedzsment egyszerűsítése.
  Főleg távoli és otthoni felhasználók számára ajánlott.
  Kliens alapú-, így főleg IT által menedzselt gépeken használjuk.
  Routerek között is működik.

VPN alkalmazása a hálózaton



Cisco VPN megoldások

- A VPN 3000-es sorozat nyugdíjazása óta nincs dedikált eszköz!
- Cisco IOS router-ek.
- Cisco ASA-k.
- Cisco (IPSec) VPN Client szoftver (PC-s kliens).
- Cisco AnyConnect (SSL) szoftver (PC-s kliens).

Router vagy ASA?

Router

- Közepes ár/teljesítmény.
- Nagyon rugalmas routing.
- DMVPN és GET VPN branch-branch kommunikációra.
- Limitált SSL VPN támogatás.
- Inkább site-to-site VPN-ekhez ajánljuk...

ASA

- Kedvező ár/teljesítmény.
- Limitált routing.
- Statikus branch-branch direct tunnel-ek.
- Egyik legrugalmasabb SSL VPN eszköz a piacon!
- Inkább mobil- és otthoni felhasználós VPN-ekhez...

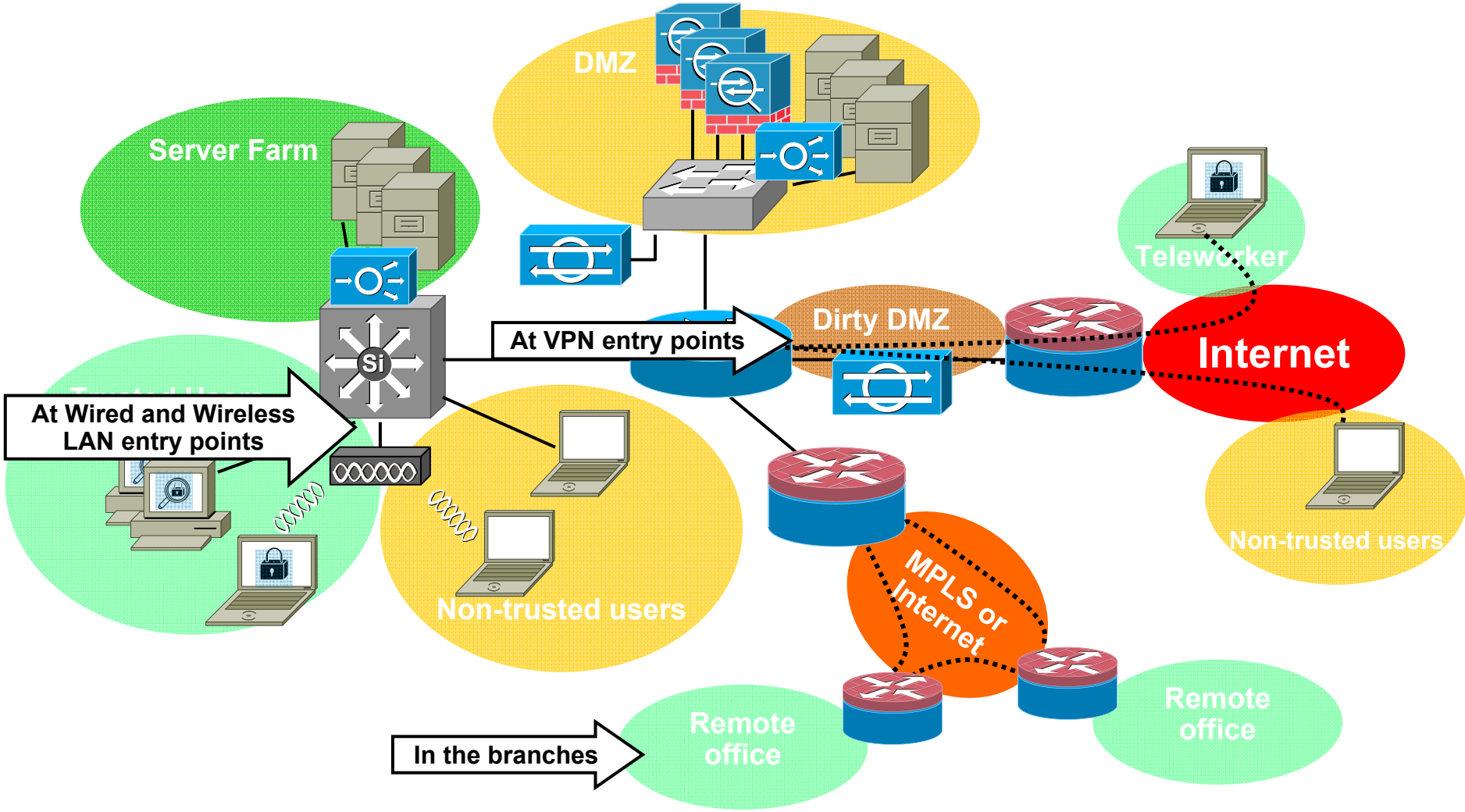
SSL vagy Easy (IPSec) VPN Remote Access-hez?

SSL VPN	Easy (IPsec) VPN
• Lehet kliens nélküli. • SSL(TLS) és DTLS transport és titkosítás. • Licenc köteles. • Nem IT által menedzselt PC-k esetén ideális.	• Mindig kliens alapú. • IPSec Cisco specifikus kiterjesztésekkel. • Jelenleg ingyenes. • IT által menedzselt kliensek és iPhone esetén ideális.

Tartalom

- Cisco Tűzfalak
- Cisco IPS-ek
- Application Level Gateway-ek (ALG)
- Cisco VPN megoldások
- Cisco Identity Management
- Beépített biztonság a Cisco infrastruktúrában
- Cisco Security Management
- Összefoglalás, kvíz

Hol van szükségünk AAA és NAC szabályok érvényesítésére?

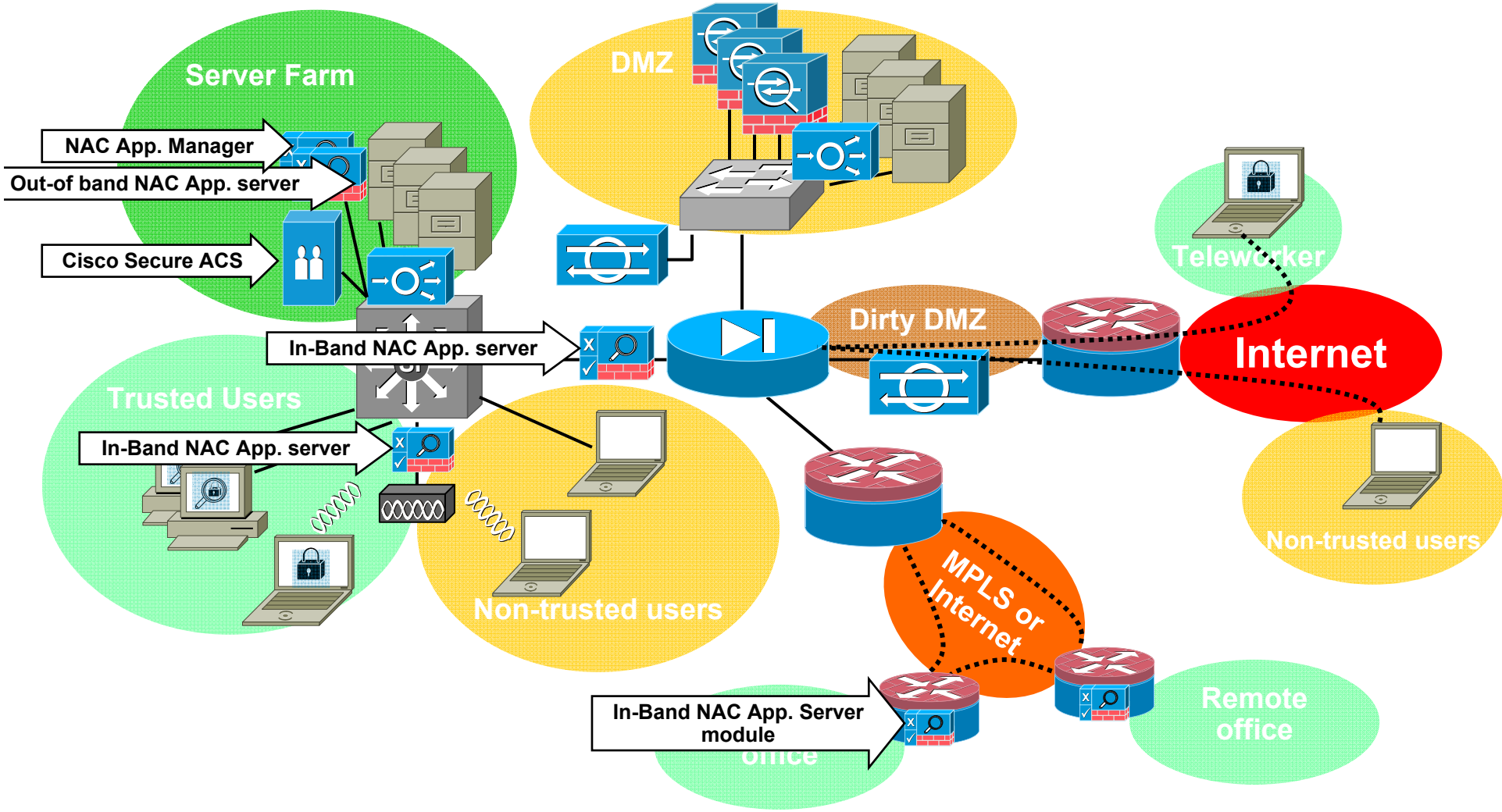


AAA és NAC komponensek a Cisco portfólióban

- Szabály érvényesítési pontok:
  - Tűzfalak,
  - Router-ek,
  - LAN switch-ek,
  - Wireless Controller-ek,
  - NAC Appliances Server-ek.

- Klines szoftverek (supplicants):
  - Cisco Secure Services Client,
  - Cisco NAC Appliance Agent.
- Szabályrendszer menedzsment:
  - Cisco Sec. Acc. Control Serv.,
  - NAC Appliance Manager.
  - NAC Appliance Profiler
  - NAC Appliance Guest server
- Lehetséges3rd party kiegészítések:
  - One Time Password systems,
  - Two factor auth. systems.

Hová helyezzük a NAC és AAA komponenseket?



Cisco Secure Access Control Server (CSACS)

- AAA szerver RADIUS és TACACS+ „interfészekkel”.
- Extra funkciók:
  - Clustering terhelésmegosztás és redundancia végett.
  - Külső felhasználói adatbázis szinkronizáció: LDAP, Active Directory, Windows NT user adatbázis, SQL, flat file ...
  - Cisco NAC integráció.
  - Adminisztrátori-, akár parancs szintű authorizáció (TACACS+ kompatibilis) eszközökre.
  - Felhasználónkénti hozzáférés authorizáció Cisco NAD-okon.
  - Együttműködés a legtöbb elterjedt kétfaktoros authentikációs és One Time Password rendszerrel.
  - ...
- Megvásárolhtó Appliance és Softver-only „kiszerelésben”.

Cisco Network Admission Control (NAC)

- A NAC segít megoldani, hogy:
  - Csak megfelelő OS-sel és patch-ekkel rendelkező hosztok jelentkezhessenek be.
  - A bejelentkező hosztok megfelelő anti-vírus szoftverrel és friss vírusleíró adatbázissal rendelkeznek.
  - Aktív vírusfertőzés esetén karanténba tegyük a hosztot automatikusan.
  - Meggátolni hacker-eket abban, hogy telefonnak, nyomtatónak... adják ki magukat a 802.1x kikerülése céljából.

Cisco Network Admission Control (NAC)

- Főbb komponensek:
  - NAC Appliance Server-ek: hoszt vizsgálat, szabály érvényesítés.
  - NAC Appliance Profiler: telefonok, nyomtatók stb. ellenőrzése.
  - NAC Appliance Manager: központi NAC Server és szabályrendszer adminisztráció.

Tartalom

- Cisco Tűzfalak
- Cisco IPS-ek
- Application Level Gateway-ek (ALG)
- Cisco VPN megoldások
- Cisco Identity Management
- Beépített biztonság a Cisco infrastruktúrában
- Cisco Security Management
- Összefoglalás, kvíz

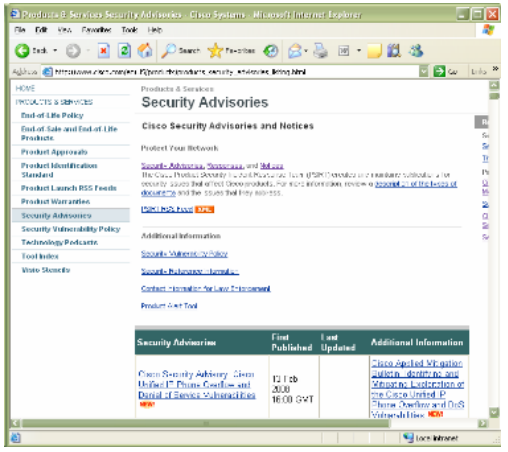
Beépített biztonsági mehanizmusok

- Fizikai:
  - Külső- vagy belső redundáns táp sok eszköz esetén.
  - Kensington lock csatolás nem rack-be szerelt eszközökön.
  - Általában masszív kiépítés.
  - Alaposan tervezett, túlméretezett hűtés.

- Technikai:
  - Titkosított adminisztráció (SSH, HTTPS).
  - Role Based Access Control.
  - TACACS+ adminisztrátor authorizáció.
  - Backplane Control Policies CPU-t célzó DoS ellen.
  - Kiterjedt naplózás és jelentéskészítés.
  - Kifinomult debug-olás.

Sebezhetőségek kezelése

- A Cisco rendszeresen teszteli a termékeit és az ügyfelektől is fogad információkat.
- Sebezhetőség esetén PSIRT riasztást ad ki és elérhetővé teszi a javítást.
- A PSIRT riasztásokra történő előfizetéshez és a javítások letöltéséhez SmartNet szükséges.



Tartalom

- Cisco Tűzfalak
- Cisco IPS-ek
- Application Level Gateway-ek (ALG)
- Cisco VPN megoldások
- Cisco Identity Management
- Beépített biztonság a Cisco infrastruktúrában
- Cisco Security Management
- Összefoglalás, kvíz

Követelmények és Megoldások

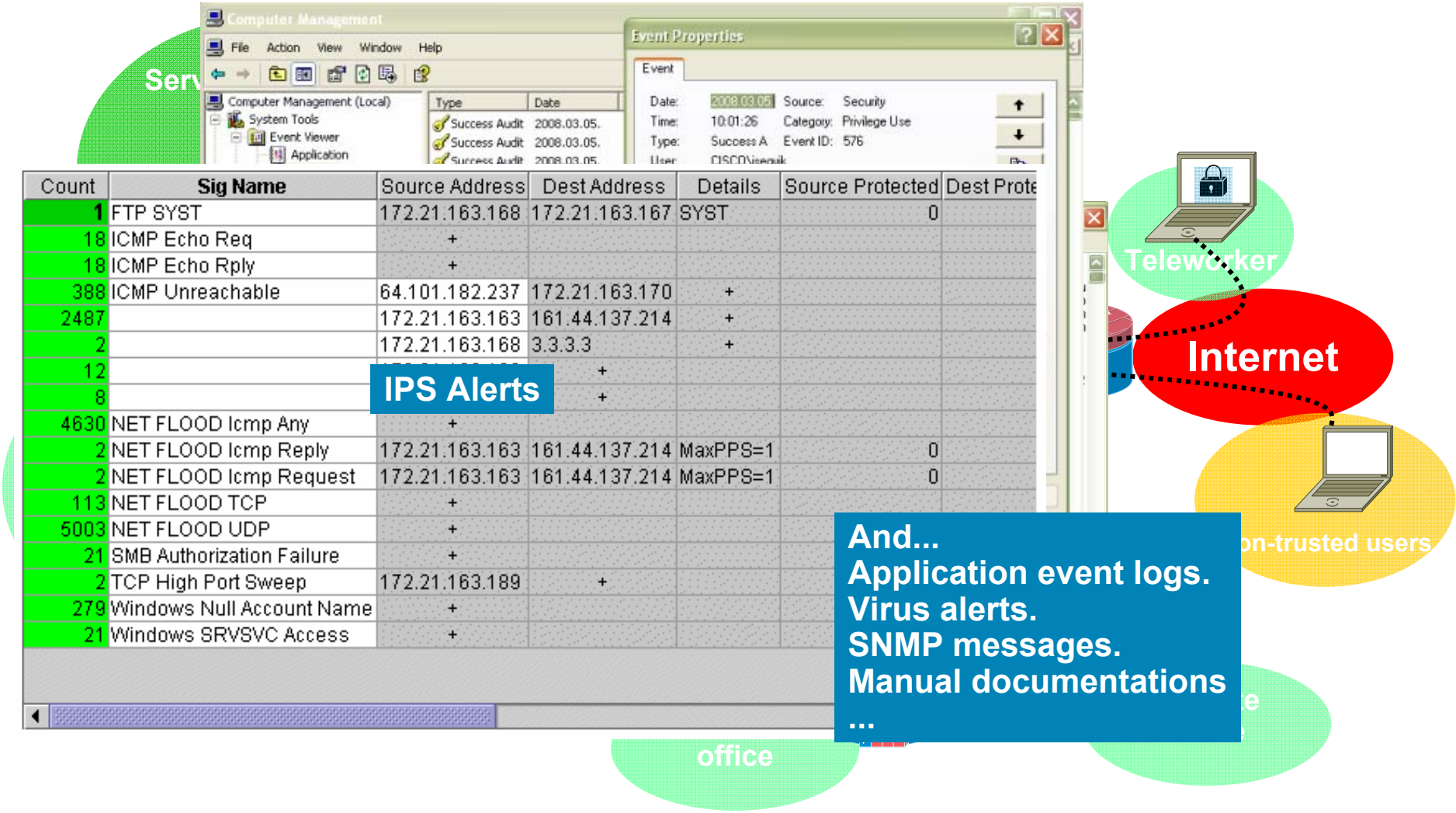
- Telepítés, leltár, üzemeltetés.
- Napi működés, Betörési kísérletek kezelése.
- Vírus-, Támadás- és Sebezhetőségi riasztások kezelése.
- Cisco Security Manager
- Cisco Monitoring Analysis and Response System (MARS).
- Intellishield Alert Center, IPS SmartNet services.

Cisco Security Manager

- Segít...:
  - Nagyszámú eszköz gyors telepítése-, automatikus- időzített konfigurációja.
  - Automatikus Tűzfal- és IPS szabályok telepítése több eszközre.
  - VPN konfiguráció, topológia ábrán Drag&Drop módon.
  - Központi IPS mintázat és ASA OS upgrade.
  - Szoftver és hardver leltár.
  - Audit, jelentés készítés hisztorikus audit információkból.
- Windows alapú kliens-szerver alkalmazás.

Security felhasználói interfész

Biztonsági naplók feldolgozása



Count	Sig Name	Source Address	Dest Address	Details	Source Protected	Dest Prote
1	FTP SYST	172.21.163.168	172.21.163.167	SYST	0	
18	ICMP Echo Req	+				
18	ICMP Echo Rply	+				
388	ICMP Unreachable	64.101.182.237	172.21.163.170	+		
2487		172.21.163.163	161.44.137.214	+		
2		172.21.163.168	3.3.3.3	+		
12			+			
8			+			
4630	NET FLOOD Icmp Any	+				
2	NET FLOOD Icmp Reply	172.21.163.163	161.44.137.214	MaxPPS=1	0	
2	NET FLOOD Icmp Request	172.21.163.163	161.44.137.214	MaxPPS=1	0	
113	NET FLOOD TCP	+				
5003	NET FLOOD UDP	+				
21	SMB Authorization Failure	+				
2	TCP High Port Sweep	172.21.163.189	+			
279	Windows Null Account Name	+				
21	Windows SRVSVC Access	+				

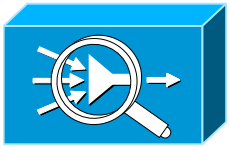
Biztonsági naplók feldolgozása

- Nyers biztonsági információk valósidejű feldolgozása meghaladja az emberi képességeket:
  - •Túl nagy mennyiség.
  - •Sokféle rendszer, eltérő formátumok, nehéz mindenben kompetensnek lenni.
- Hasonló helyzet, mint az F-22-es esetében. Számítógép segíti a manőverezést, az ember fizikai tűrőképessége limitál egyedül.

Biztonsági naplók feldolgozása

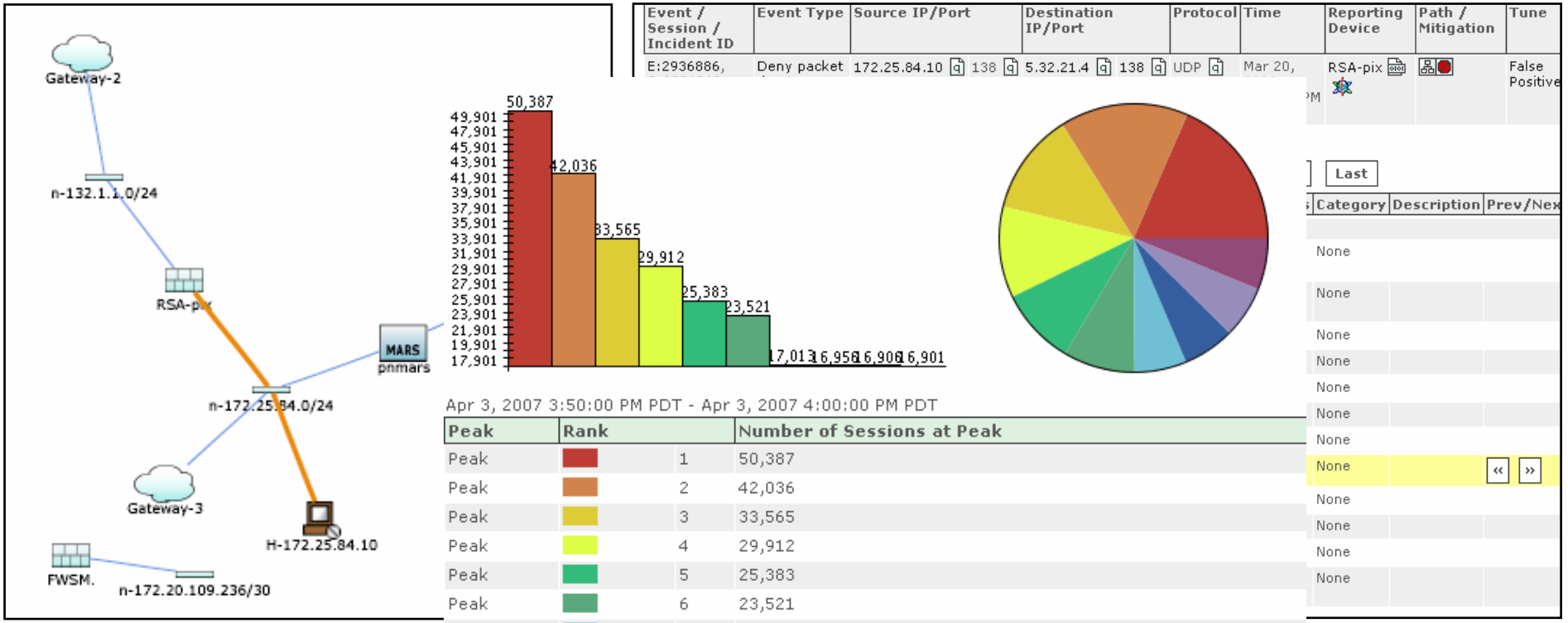
- Egy másik példa: próbáljunk elolvasni 100 oldalt egy idegen nyelven íródott könyvben
- ... EGY másodperc alatt.

Cisco Security Monitoring Analysis and Response System: CS-MARS



- Fontosabb funkciók:
  - Gyűjti és tárolja a nyers napló bejegyzéseket és riasztásokat Cisco és más gyártók eszközeitől és szoftvereitől.
  - Normalizál-, Session-ökre bont- és korrelál majd incidensek formájában jeleníti meg az információkat.
  - Felfedezi a hálózati topológiát és vizualizálja a támadási irány(oka)t.
  - Felkínál elhárítási terveket, amelyeket gombnyomásra végre is hajt.
  - Beépített „Biztonsági operátor help-desk” rendszer.
  - Audit és jelentés készítés.
- Appliance modellben vásárolható Linux OS-sel.

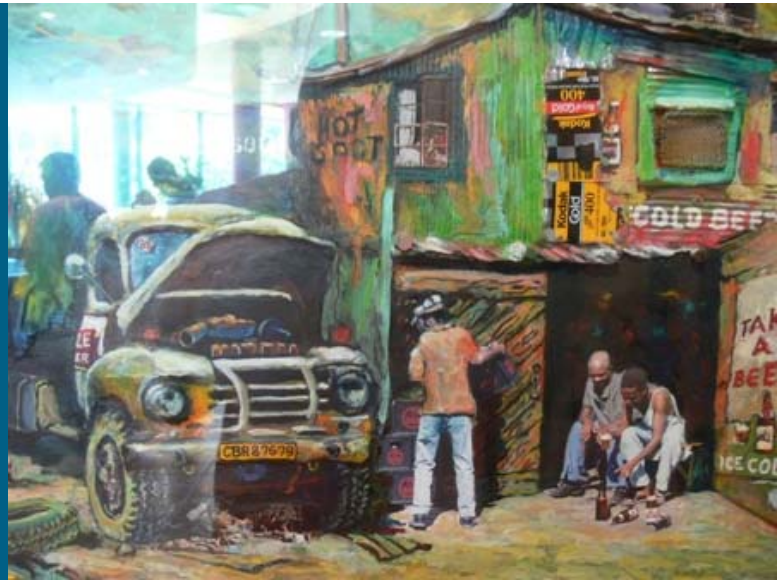
CS-MARS felhasználói interfész



MARS-ról még egy kicsit...

- Egy majdnem mindenhol létező problémára jelent megoldást.
- Érdemes pilot rendszert telepíteni... Általában megveszi az ügyfél, ha egyébként van rá pénzügyi kerete.
- Árak: 7.500 – 150.000 USD teljesítménytől függően.

Összefoglaló, Quiz



Quiz