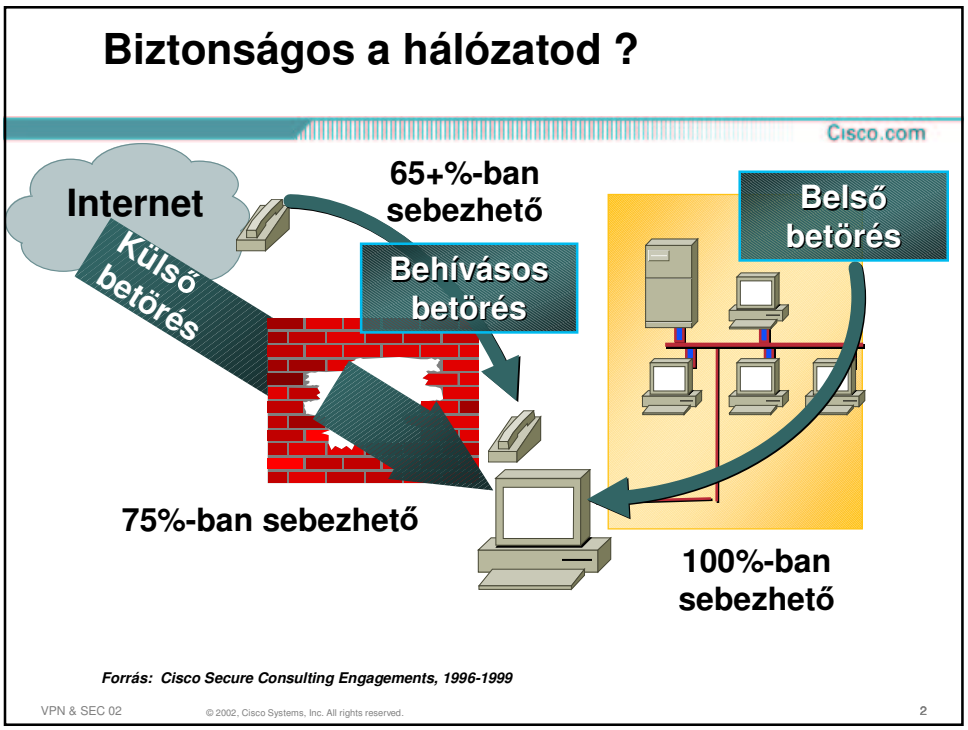
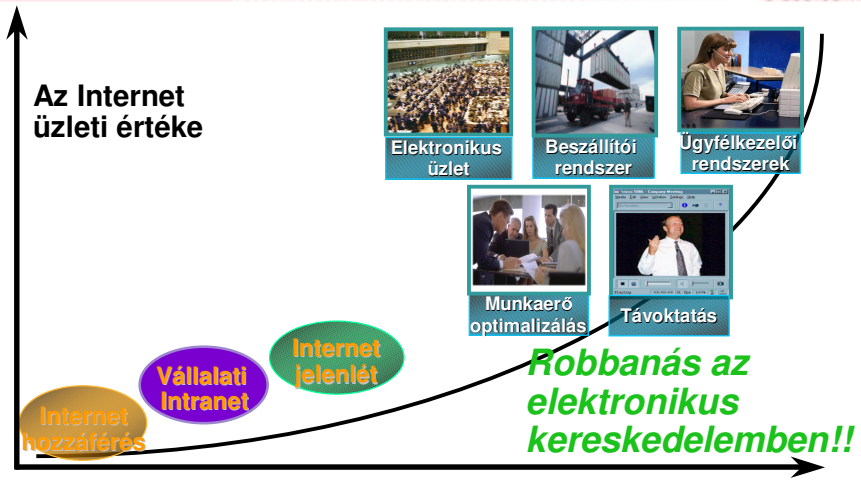


A hálózati biztonság dilemmája

Cisco.com



Hozzáférés kiszélesedett
Növekvő biztonsági veszélyek

Cisco.com

Cisco hálózatbiztonsági és VPN megoldások SAFE architektúra

Ács György

gacs@cisco.com

Networkshop 2002

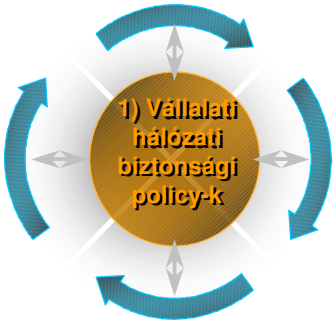
Napirend

- A Cisco hálózatbiztonsági stratégiája
- A Cisco biztonsági és VPN megoldásai
- Konklúzió

Átfogó hálózatbiztonsági megoldás

2) Biztonság kiépítése
Tűzfal, titkosítás, hitelesítés,..

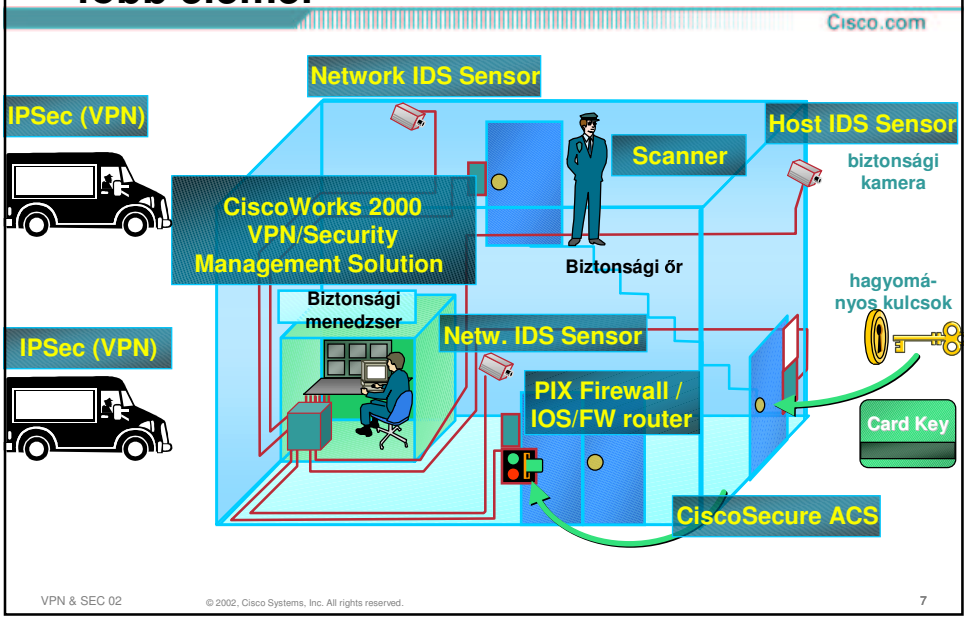
5) Menedzselés és továbbfejlesztés
Hálózat működtetése és hálózati biztonsági szakértők



3) Monitorozás és beavatkozás
betörés detektálása (Intrusion Detection System, IDS)

4) Ellenőrzés
Sebezhetőség felderítése

A Cisco SAFE hálózat főbb elemei



Napirend

- A Cisco hálózatbiztonsági stratégiája
- A Cisco biztonsági és VPN megoldásai
- Konklúzió

A Cisco biztonsági megoldásai

Cisco.com

Biztonságos kapcsolat	Peremzóna biztosítás	Biztonsági monitorozás	Azonosítás	Biztonsági menedzsment
				
VPN	Tűzfalak	Betörés detektálók	Autentikáció	Policy
Cisco VPN Concentrators Cisco PIX™ Firewalls	Cisco PIX™ Firewalls	Cisco IDS Appliances	Cisco Access Control Server	Cisco Works—VPN Mgmt Solution Cisco Secure Policy Manager Web Device Managers
Cisco IOS VPN	Cisco IOS Firewall	Cisco IOS IDS		

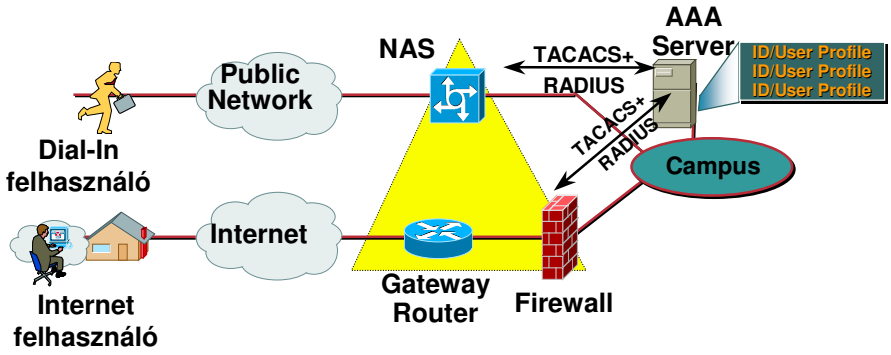
Hiteles azonosítás

Cisco.com

- **A felhasználók, szolgáltatások és erőforrások pontos azonosítása**
  - **AAA szerver, RADIUS, TACACS+, Kerberos,**
  - **OTP, MS-login,**
  - **digitális aláírások,**
  - **címtár szolgáltatások**
  - **Cisco Secure ACS**
  - **3rd party CA szerverek**

AAA architektúra

Cisco.com

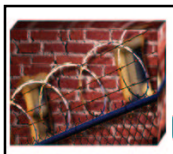


- **Authentication (azonosítás):** Ki vagy?
- **Authorization (jogosultság):** Mit csinálhatsz?
- **Accounting (naplózás):** Mit csináltál?

Peremzóna biztosítás

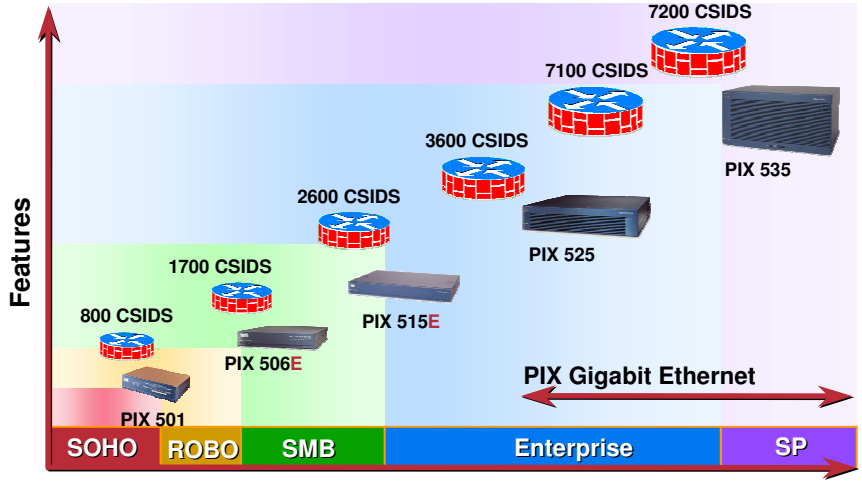
Cisco.com

- **Kritikus hálózati alkalmazások, adatok és szolgáltatások hozzáférésvezérlése**
  - Access control listák, tűzfal technológiák, tartalomszűrés, hitelesítés
  - Cisco Secure PIX tűzfal,
  - Cisco Secure Integrated Services

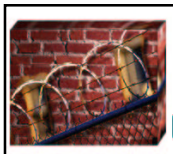


PIX tűzfal család

Cisco.com



PIX 506, 515: End of Sale: May 24, 2002



Cisco Secure PIX Firewall

Piac-vezető

Cisco.com

- Dedikált tűzfal megoldás integrált hardver és szoftver
  - Nincsenek szoftver installáció/karbantartási kockázatok
  - Kis költségű
  - Önálló és nem 'Hardened' OS
- Hibrid tervezés
  - Adaptive Security Algorithm (ASA)
  - Cut-through proxy
  - IDS

- Nagy rendelkezésreállású
  - Flash-ből fut
  - STATEFUL failover
- Nagy teljesítmény
  - 250-500,000 párhuzamos kapcsolatig
  - 1.7 Gbps teljesítmény
  - 100Mbit/s 3DES- HW
- Installációk
  - >100,000 PIX Firewall

Biztonságos kommunikáció

Cisco.com

- **Biztonságos, hitelesített kommunikáció**
  - VPN, IPSec, titkosítás,
  - DES, 3DES, IKE,
  - digitális aláírás
  - Cisco IOS IPSec, PIX IPSec, Cisco Secure VPN Concentrator

VPN megoldások - választás

Cisco.com

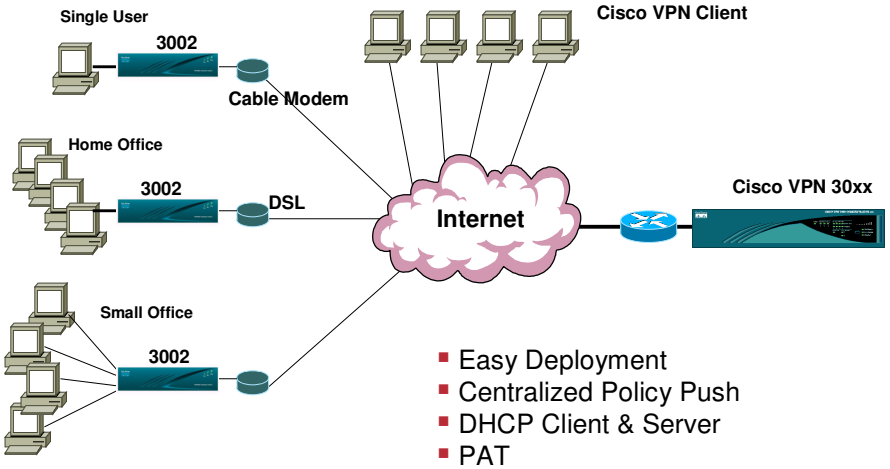
A Cisco nyújtja a legszélesebb VPN megoldás halmazt!

Customer Type	Remote Access	Site-to-Site	Firewall-based
Large Enterprise, SP	3060, 3080 Concentrators	7100,7200 Routers	PIX Firewall 525, 535
Medium Enterprise	3030 Concentrator	7100, 3600 Routers	PIX Firewall 515
Small Business/ Branch Office	3015, 3005 Concentrators	3600, 2600, 1700 Routers	PIX Firewall 515 PIX Firewall 506
SOHO Market	VPN 3000 Client 3002 Hardware Client	800, 900 Routers	PIX Firewall 506

Kielégít bármilyen VPN követelményt!

Cisco VPN 3002 Hardware VPN Client

Cisco.com



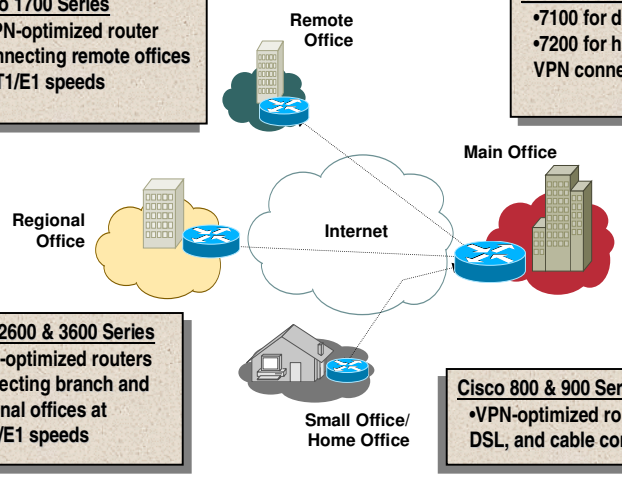
- Easy Deployment
- Centralized Policy Push
- DHCP Client & Server
- PAT
- Client & Network Extension modes

Cisco Site-to-Site VPN megoldások

Cisco.com

Cisco 1700 Series
•VPN-optimized router connecting remote offices at T1/E1 speeds

Cisco 7100 & 7200 Series
•7100 for dedicated VPN head-end
•7200 for hybrid private WAN + VPN connectivity



Cisco 2600 & 3600 Series
•VPN-optimized routers connecting branch and regional offices at nxT1/E1 speeds

Cisco 800 & 900 Series
•VPN-optimized routers for ISDN, DSL, and cable connectivity

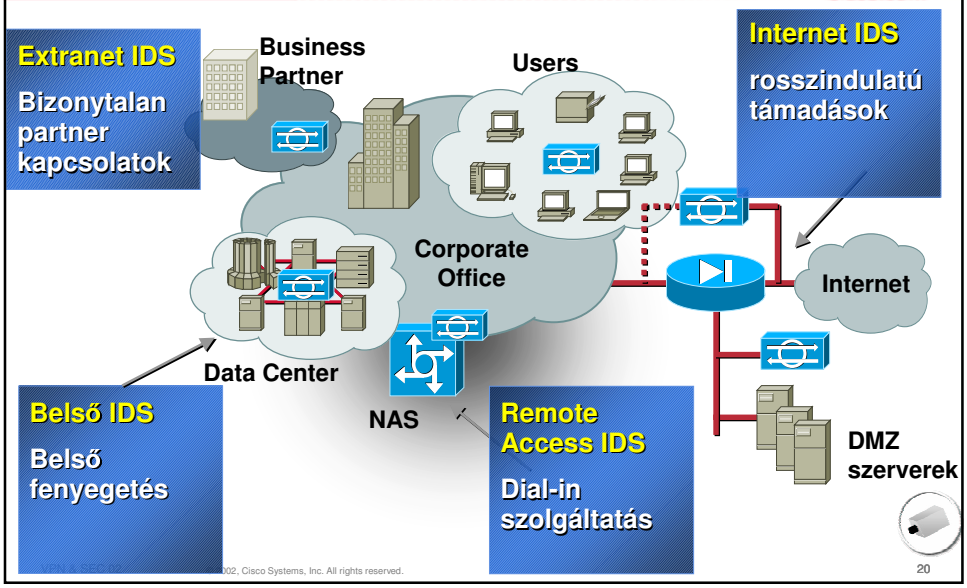
Hálózati biztonság monitorozása - betörés detektálása, IDS

Cisco.com

- Ismert és gyanús hálózati betörések azonosítása és beavatkozás
  - Passzív, válogatás nélküli monitorozás, adatbázis a gyanús/veszélyes viselkedési formákról, kommunikációs infrastruktúráról, access control - változtatás
  - Cisco Secure Intrusion Detection System

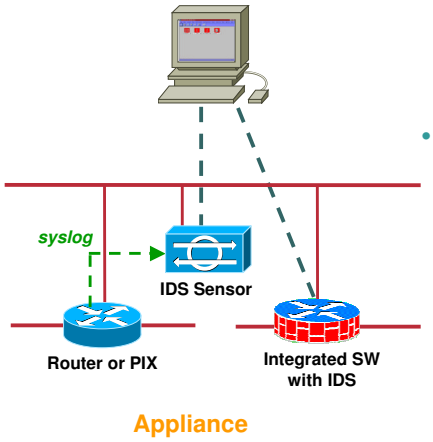
Betörésdetektálási alkalmazások

Cisco.com



Cisco Secure IDS felépítése

Cisco.com



- **Sensor**
  - Csomagok “signature” analízise
  - Riasztás generálása
  - Válasz/ellenintézkedés
- **CSPM**
  - Real-Time riasztás-kijelzés
  - Eszköz konfigurálás
  - “Signature” szétosztás
  - Távoli szenzor menedzsment

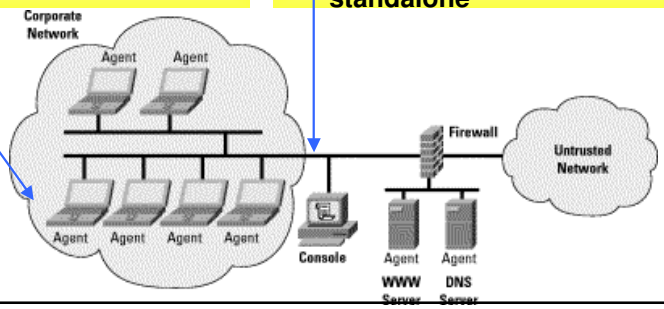
Cisco IDS Host Sensor

Cisco.com

- Kliens/Szerver Architektúra
- OS-szintű technológia lehetővé teszi, hogy a gyanús kéréseket OS hívás előtt szűrjük

Agent-ek (Warning Mode or Prevention Mode)
- Microsoft WinNT /2k
- Solaris Ultrasparc

Console (skálázható 1000 „agent” per console)
- Microsoft WinNT/2k
- CW2k VMS 2.0 (preferred) or standalone



Cisco Secure Scanner

- EVAL változat:
- www.cisco.com/go/scanner
- (5 IP cím, teljes értékű)

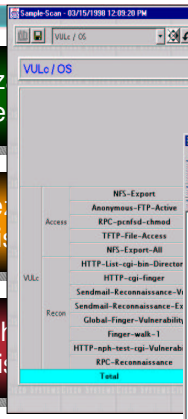
A hálóz
feltérképe

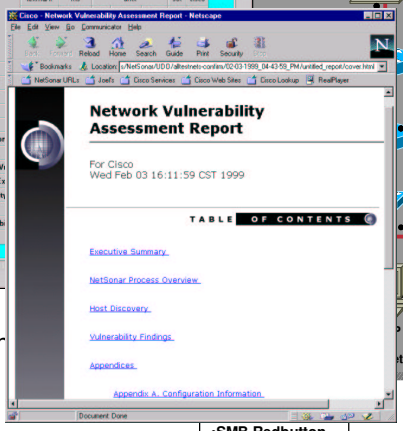
Passzív sebe
analízi

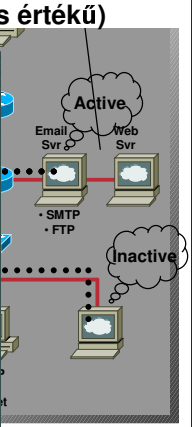
Aktív sebezh
analízi

Megjelenítés &
Reportkészítés

Jeler





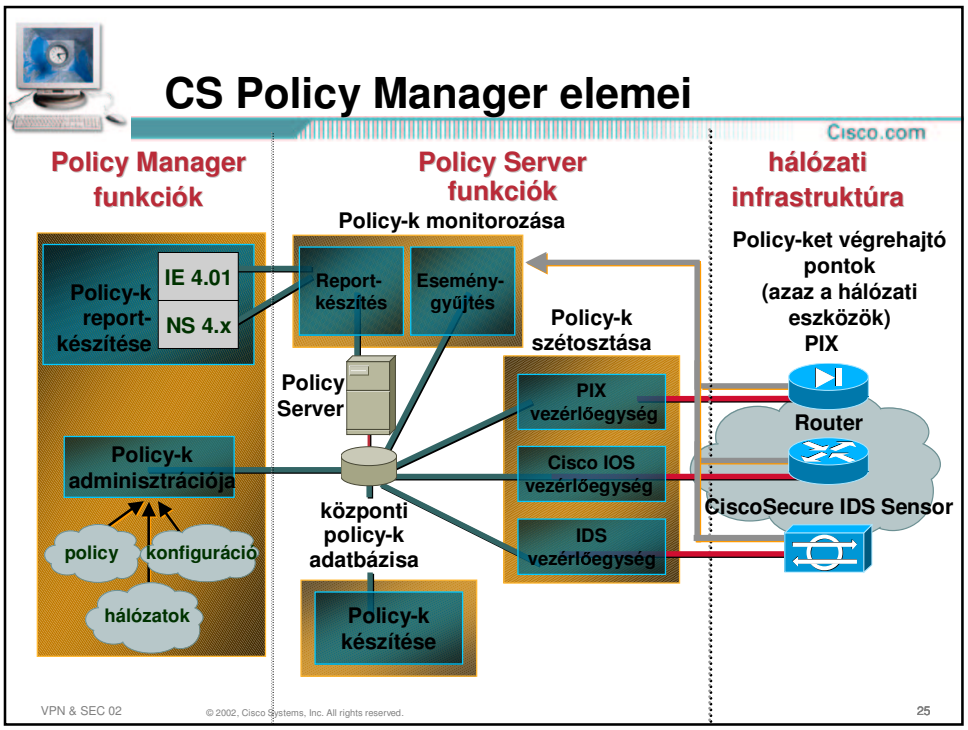


•SMB Redbutton
•Anonymous FTP

A biztonság menedzselése

Cisco.com

- **Integrált vezérlés a hálózati erőforrások számára**
  - **A Cisco tűzfalak, IPSec titkosítás és a VPN-ek biztonsági menedzsmentje, biztonsági policy-k ellenőrzése**
  - **CiscoWorks 2000 VPN/Security Management Solution**
  - **Cisco Secure Policy Manager**



Napirend

- A Cisco hálózatbiztonsági stratégiája
- A Cisco biztonsági és VPN megoldásai
- Konklúzió

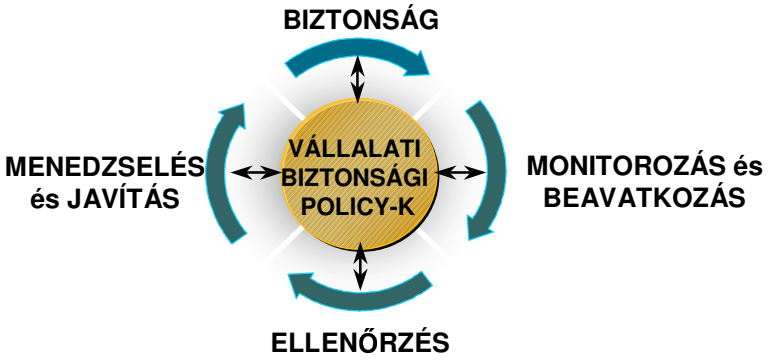
Az “új világ” biztonsági filozófiája

Cisco.com

A biztonság fenntartása

folyamatos, többszintű folyamat,

melyet mindig tovább kell fejleszteni



További információ...

Cisco.com

www.cisco.com/go/security