

A hálózati biztonság dilemmája

Cisco.com



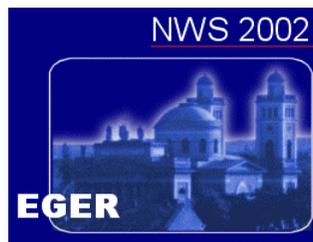
VPN & SEC 02

© 2002, Cisco Systems, Inc. All rights reserved.

3

Cisco hálózatbiztonsági és VPN megoldások SAFE architektúra

Ács György
gacs@cisco.com



Networkshop 2002

Session Number
VPN & SEC 02

© 2002, Cisco Systems, Inc. All rights reserved.

4

Napirend

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

Cisco.com

5

Átfogó hálózatbiztonsági megoldás

Cisco.com

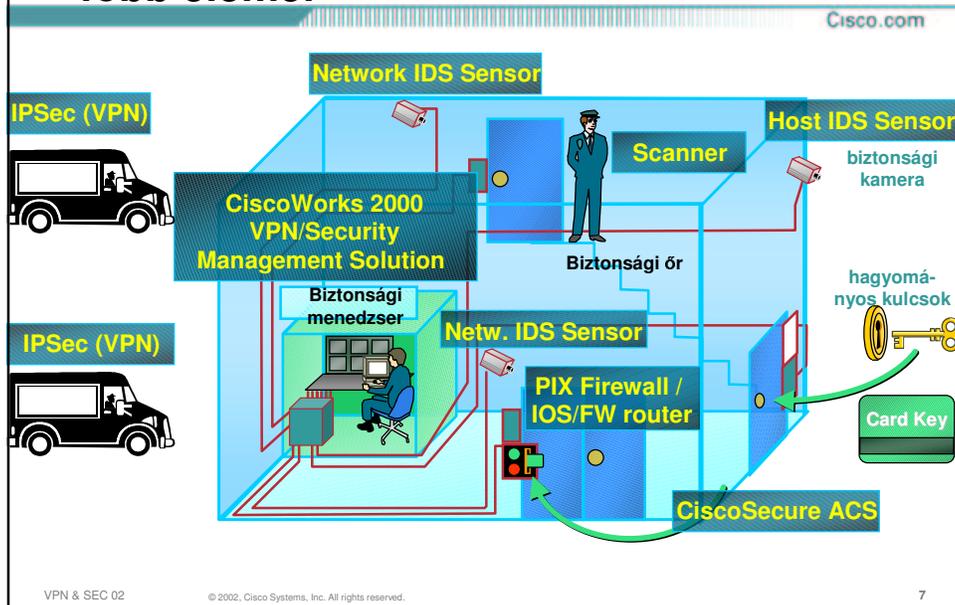


VPN & SEC 02

© 2002, Cisco Systems, Inc. All rights reserved.

6

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



VPN

Cisco VPN Concentrators
Cisco PIX™ Firewalls

Peremzóna biztosítás



Tűzfalak

Cisco PIX™ Firewalls

Biztonsági monitorozás



Betörés detektálók

Cisco IDS Appliances

Azonosítás



Autentikáció

Cisco Access Control Server

Biztonsági menedzsment



Policy

Cisco Works—VPN Mgmt Solution
Cisco Secure Policy Manager
Web Device Managers

Cisco IOS VPN

Cisco IOS Firewall

Cisco IOS IDS



VPN & SEC 02

© 2002, Cisco Systems, Inc. All rights reserved.

9

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



VPN & SEC 02

© 2002, Cisco Systems, Inc. All rights reserved.

10

AAA architektúra

Cisco.com

The diagram illustrates the AAA architecture. On the left, two user types are shown: 'Dial-In felhasználó' (Dial-in user) connected to a 'Public Network' and 'Internet felhasználó' (Internet user) connected to the 'Internet'. Both networks connect to a 'NAS' (Network Access Server) represented by a yellow triangle. The 'NAS' connects to a 'Gateway Router' (blue circle) and a 'Firewall' (red brick wall). The 'Gateway Router' connects to the 'Internet'. The 'Firewall' connects to a 'Campus' (blue oval). The 'Campus' connects to an 'AAA Server' (grey server rack). Bidirectional arrows between the NAS and AAA Server are labeled 'TACACS+' and 'RADIUS'. A box next to the AAA Server lists 'ID/User Profile' three times.

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

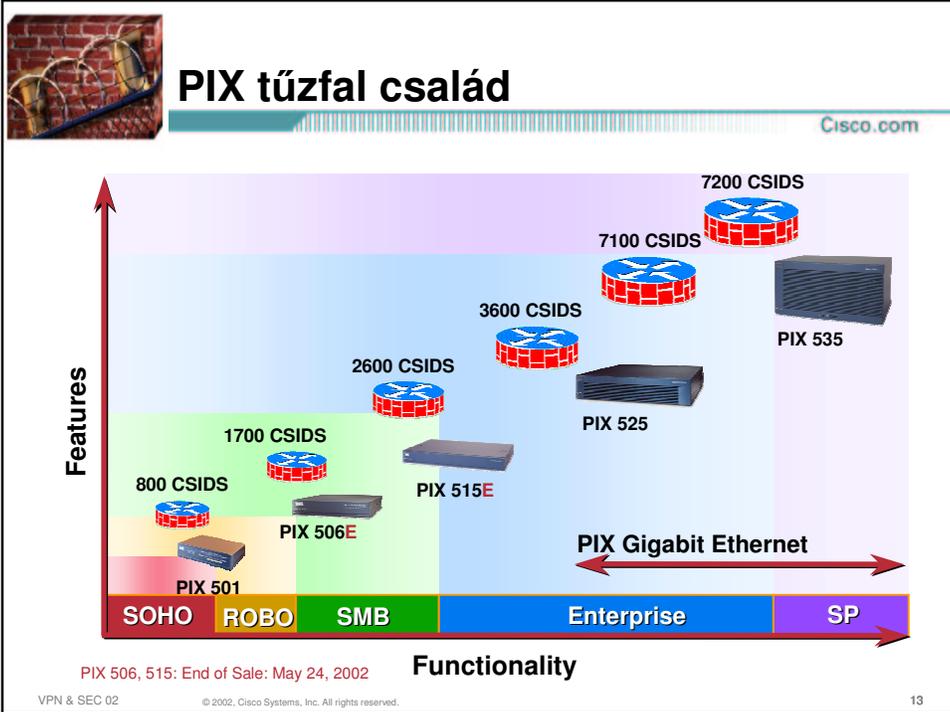
VPN & SEC 02 © 2002, Cisco Systems, Inc. All rights reserved. 11

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**

VPN & SEC 02 © 2002, Cisco Systems, Inc. All rights reserved. 12



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 rendelkezésreállítás**
 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

VPN & SEC 02 © 2002, Cisco Systems, Inc. All rights reserved. 14

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 & SEC 02

© 2002, Cisco Systems, Inc. All rights reserved.

15



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!

VPN & SEC 02

© 2002, Cisco Systems, Inc. All rights reserved.

16

Cisco VPN 3002 Hardware VPN Client

Cisco.com

The diagram illustrates three deployment scenarios for the Cisco VPN 3002 Hardware VPN Client:

- Single User:** A single computer is connected to a Cisco 3002 device, which is connected to a Cable Modem. The Cable Modem connects to the Internet cloud.
- Home Office:** Multiple computers are connected to a Cisco 3002 device, which is connected to a DSL modem. The DSL modem connects to the Internet cloud.
- Small Office:** Multiple computers are connected to a Cisco 3002 device, which is connected to a DSL modem. The DSL modem connects to the Internet cloud.

The Internet cloud is connected to a Cisco VPN 30xx router, which is labeled as a Cisco VPN Client.

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

VPN & SEC 02 © 2002, Cisco Systems, Inc. All rights reserved. 17

Cisco Site-to-Site VPN megoldások

Cisco.com

The diagram illustrates four Cisco Site-to-Site VPN solutions connecting different office types through the Internet:

- Remote Office:** Connected to the Internet cloud.
- Regional Office:** Connected to the Internet cloud.
- Small Office/Home Office:** Connected to the Internet cloud.
- Main Office:** Connected to the Internet cloud.

Each office type is associated with a specific Cisco router series:

- 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.

VPN & SEC 02 © 2002, Cisco Systems, Inc. All rights reserved. 18

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

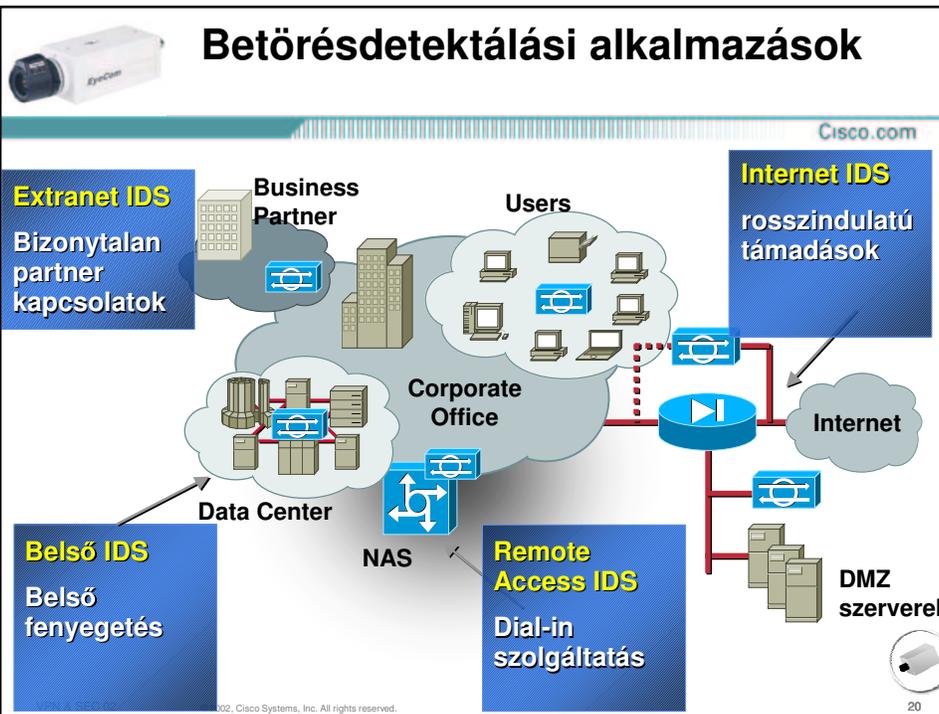
Cisco Secure Intrusion Detection System



VPN & SEC 02

© 2002, Cisco Systems, Inc. All rights reserved.

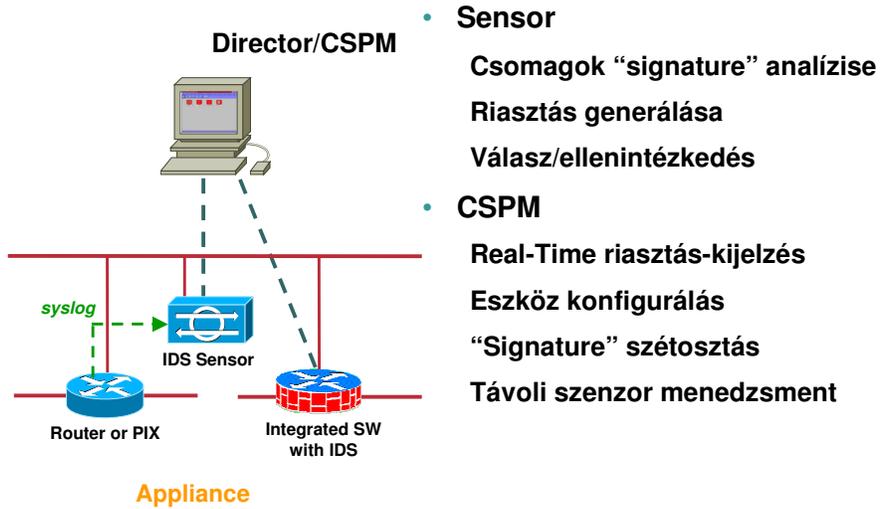
19





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

VPN & SEC 02

© 2002, Cisco Systems, Inc. All rights reserved.

21



Cisco IDS Host Sensor

Cisco.com

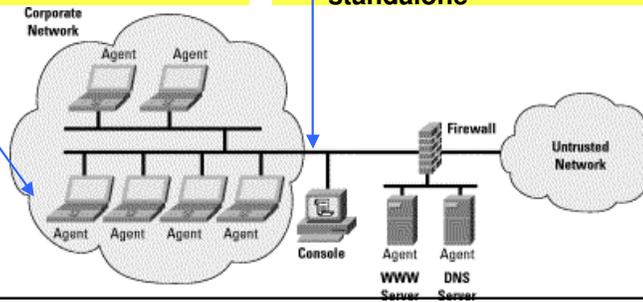
- **Kliens/Szerver Architektúra**
- OS-szintű technológia lehetővé teszi, hogy a gyanús kéréseket OS hívás előtt szűrjük

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



VPN & SEC 02

22



Cisco Secure Scanner

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

A hálózat feltérképezése

Passzív sebességanalízis

Aktív sebességanalízis

Megjelenítés & Reportkészítés

The screenshot shows a web browser displaying a 'Network Vulnerability Assessment Report'. The report title is 'Network Vulnerability Assessment Report' and it is dated 'Wed Feb 03 16:11:59 CST 1999'. A 'TABLE OF CONTENTS' section lists various report parts like 'Executive Summary', 'NetScan Process Overview', 'Host Discovery', 'Vulnerability Findings', 'Appendices', and 'Appendix A Configuration Information'. To the right, a network diagram shows several servers, with some labeled 'Active' and others 'Inactive'. Below the diagram, there are labels for 'SMB Redbutton' and 'Anonymous FTP'.

A biztonság menedzselése

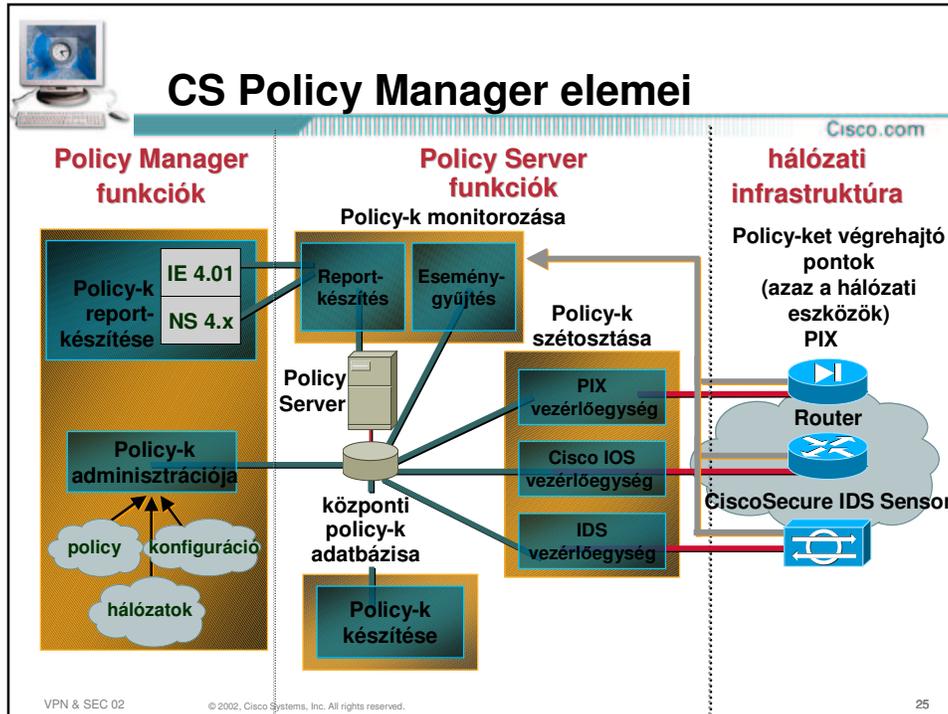
Cisco.com

- Integrált vezérlés a hálózati erőforrások számára

A Cisco tűzfalak, IPSec titkosítás és a VPN-ek biztonsági menedzselése, biztonsági policy-k ellenőrzése

CiscoWorks 2000
VPN/Security Management Solution
Cisco Secure Policy Manager





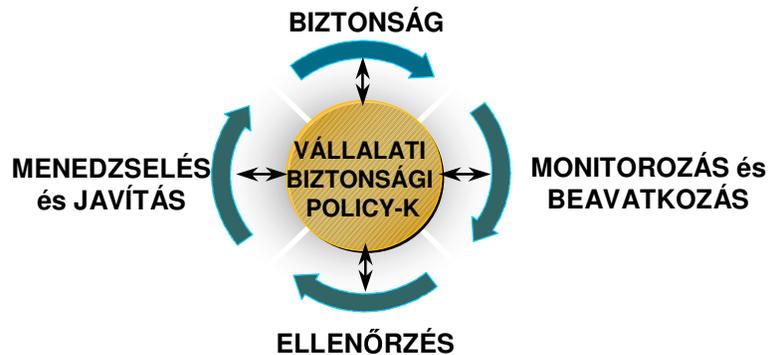
Napirend

- 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*



VPN & SEC 02

© 2002, Cisco Systems, Inc. All rights reserved.

27

További információ...

Cisco.com



www.cisco.com/go/security

VPN & SEC 02

© 2002, Cisco Systems, Inc. All rights reserved.

CISCO SYSTEMS



EMPOWERING THE
INTERNET GENERATION