Cisco Security Manager

ÁCS GYÖRGY
GACS@CISCO.COM

Tartalom

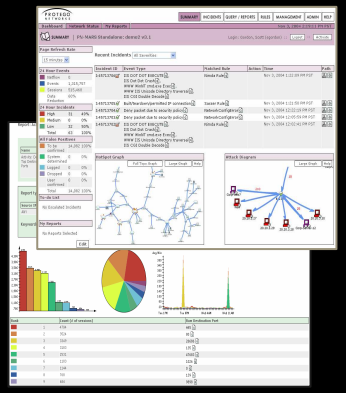
- Cisco security menedzsment alkalmazások
- CSM főbb jellemzői
- CSM - egyszerű policy konfigurálás
- CSM - VPN konfigurálás
- CSM – operátorok jogosultságai
- Összefoglalás

CISCO SECURITY MENEDZSMENT ALKALMAZÁSOK

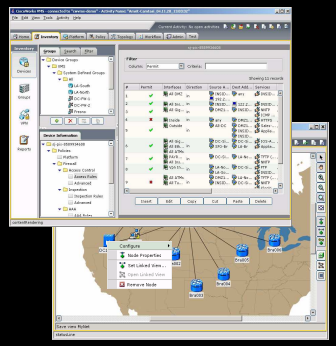
Security menedzsment alkalmazások

Menedzsment

MARS

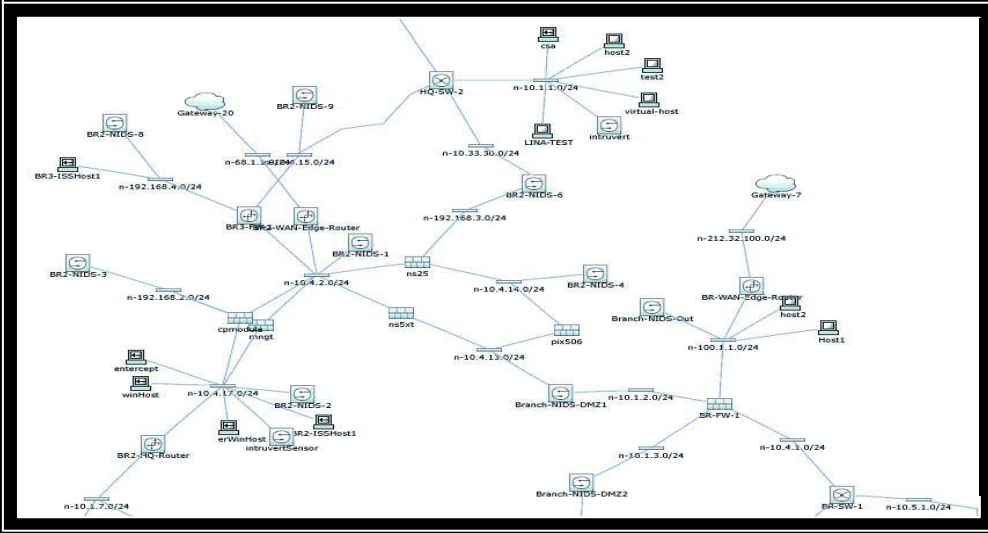


Security Manager



ACS

Hálózati eszközök



- Tűzfalak
- Integrált biztonsági megoldások (ASA)
- Hoszt alapú IDS/IPS
- Routerek (ISR) / Switch-ek
- Hálózat alapú IDS/IPS

A CSM FŐBB JELLEMZŐI

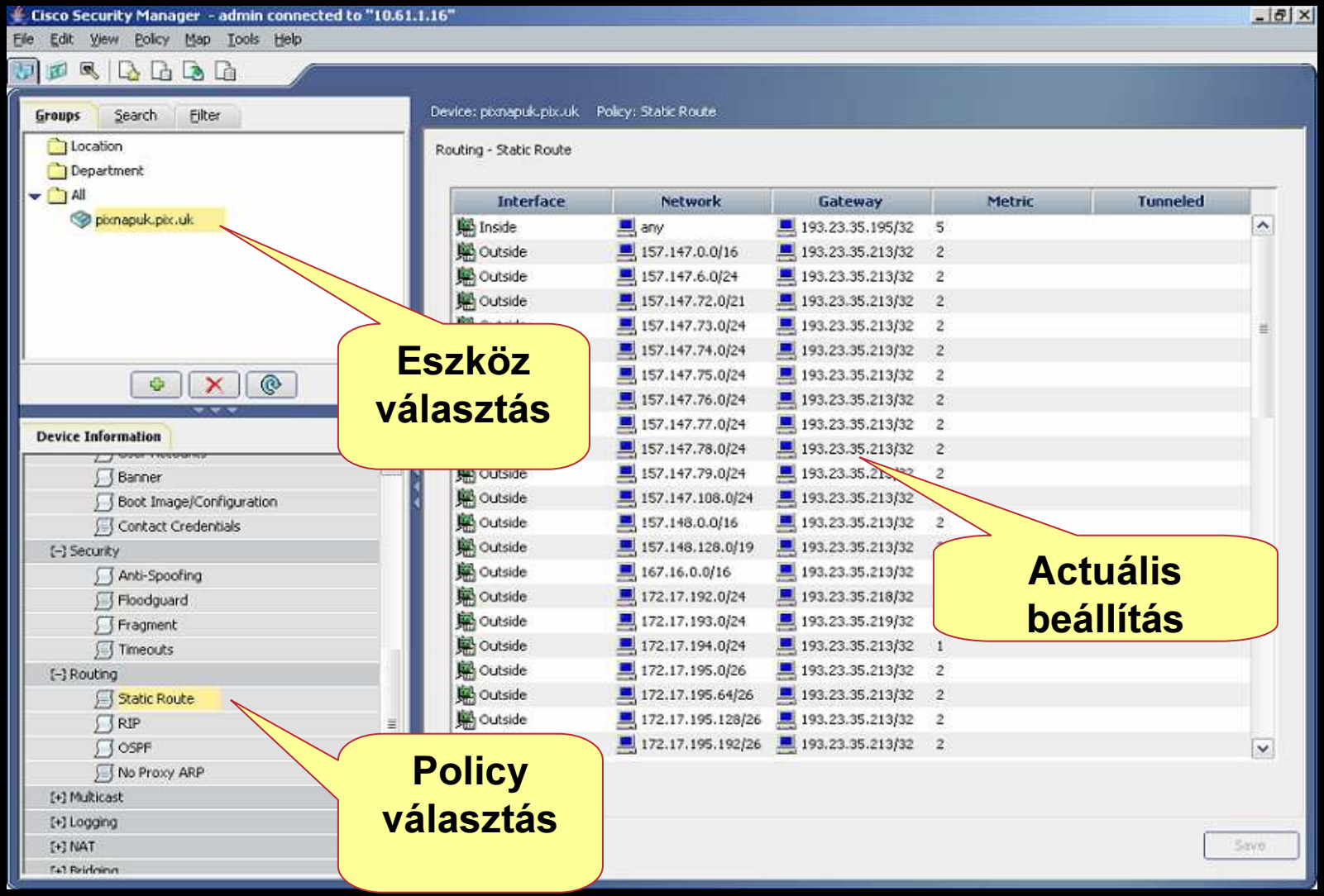
Cisco Security Manager 3.0

- ✓ **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.…**

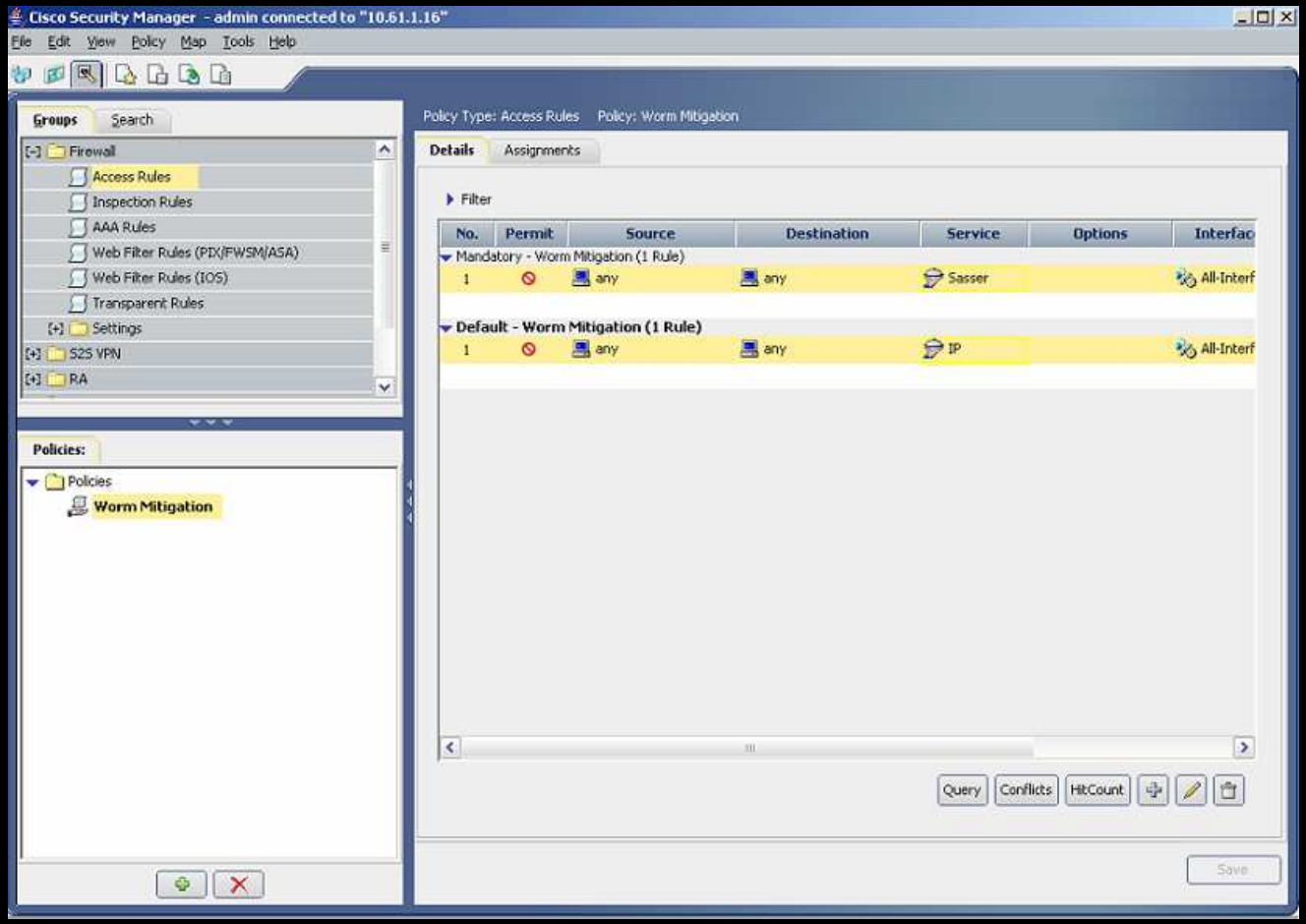
Az alkalmazás opcionális előnyei

- **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



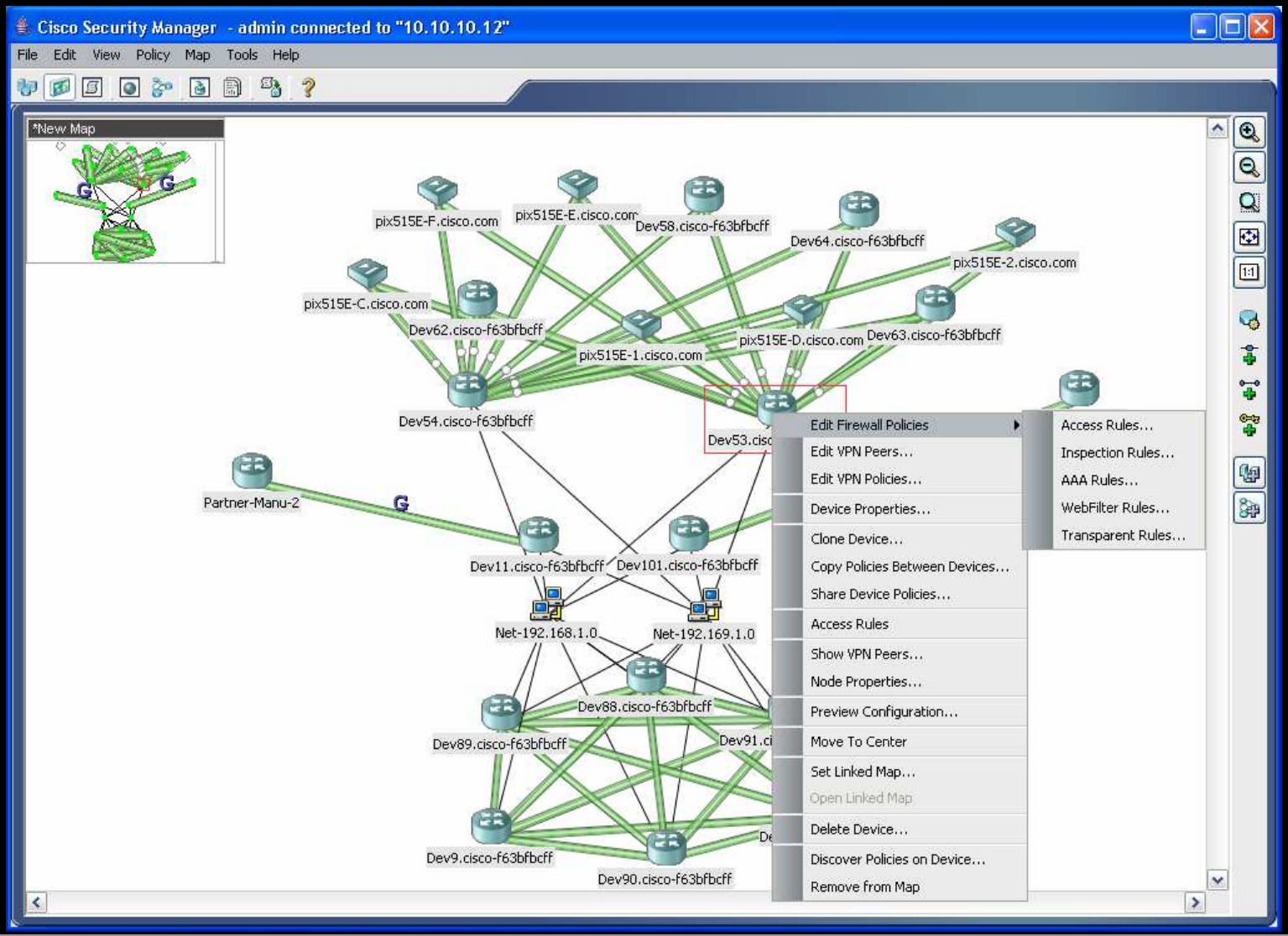
3 nézet: Policy View



Ebben a nézetben konfigurálhatók a skálázhatósági szolgáltatások:

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

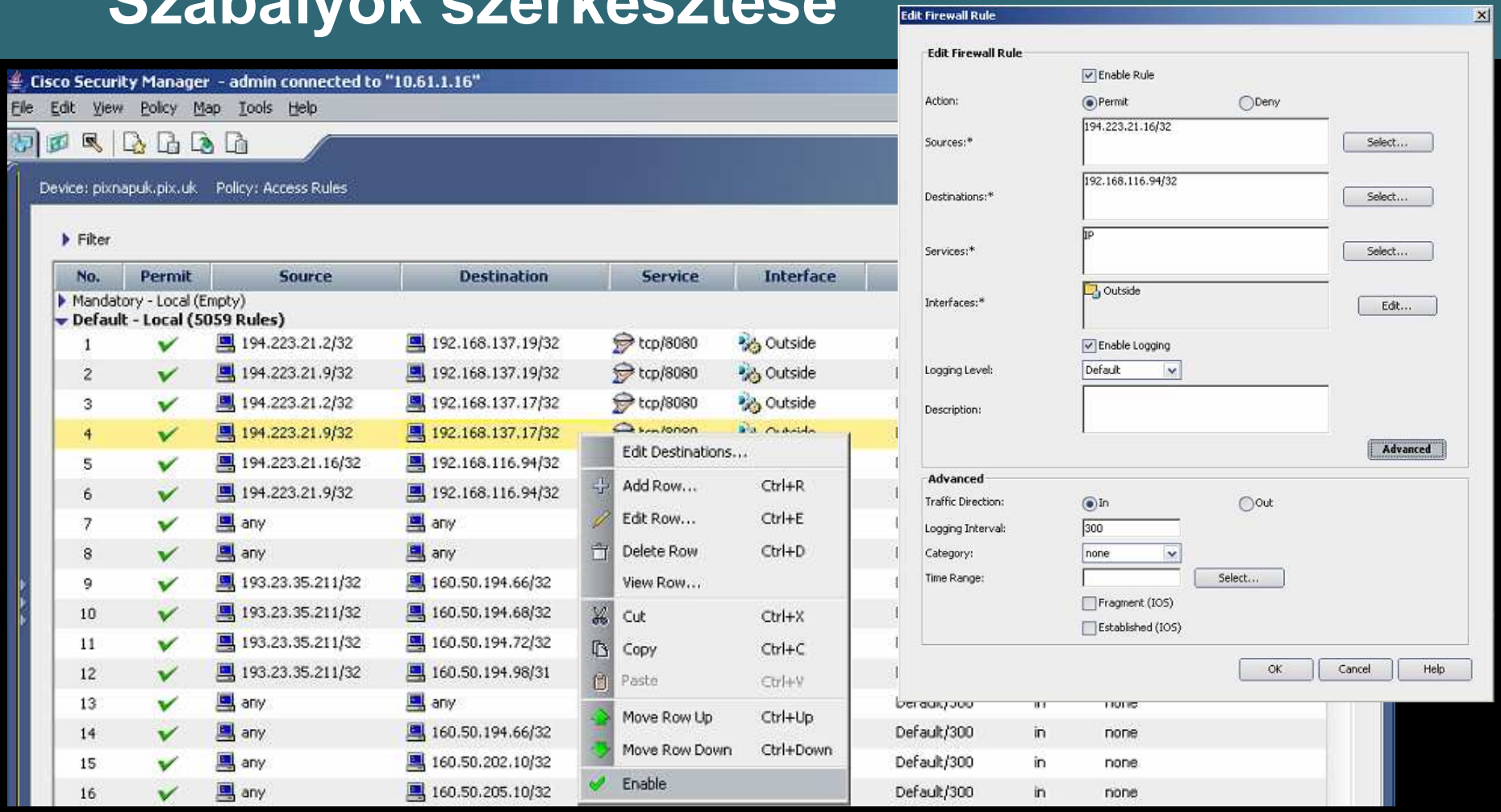
3 nézet: Map centric view



Tűzfal hozzáférési szabályok (ACL)

- **Könnyen áttekinthető szabály táblázat** minden eszközre
  - Egyszerű szabály másolás (ASA, PIX, FWSM, IOS)
- Támogatja az ACL opciókat (naplózás, időtartomány, megjegyzés, stb.)
- **Megtartja az ACL nevét** – csak a változtatott szabályt módosítja (insert-delete)
- Fejlett beállítások (turbo ACL, objektum csoportok)

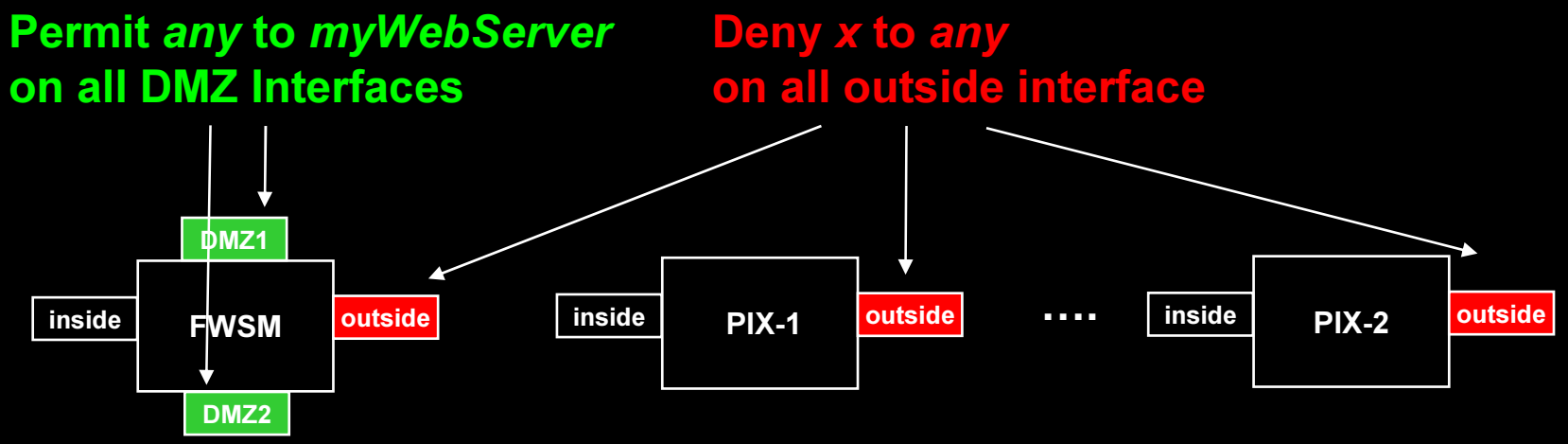
Szabályok szerkesztése



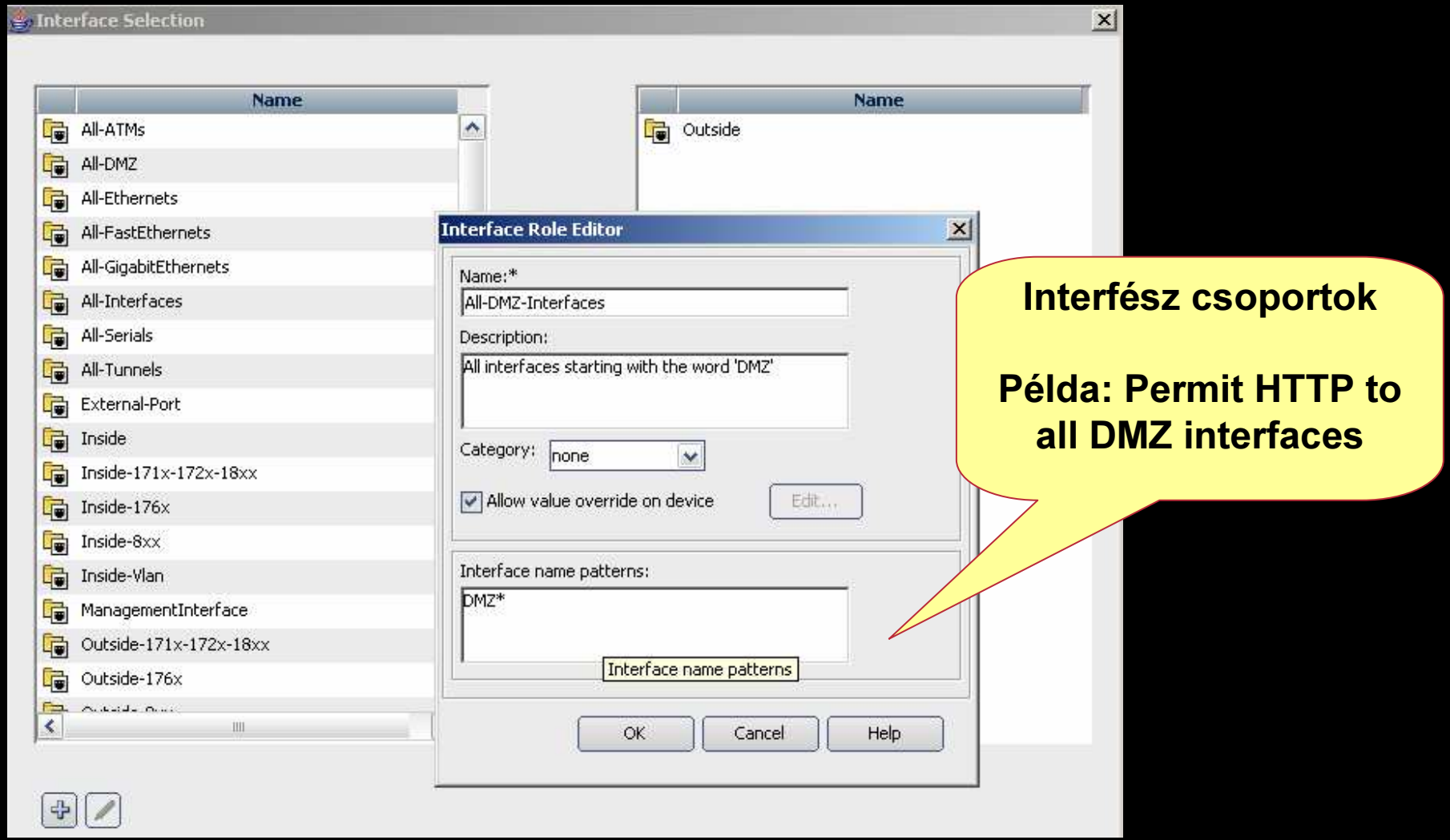
Right click, double click, enable/disable, change column width, column order, move up/down etc

Interfész szerepek

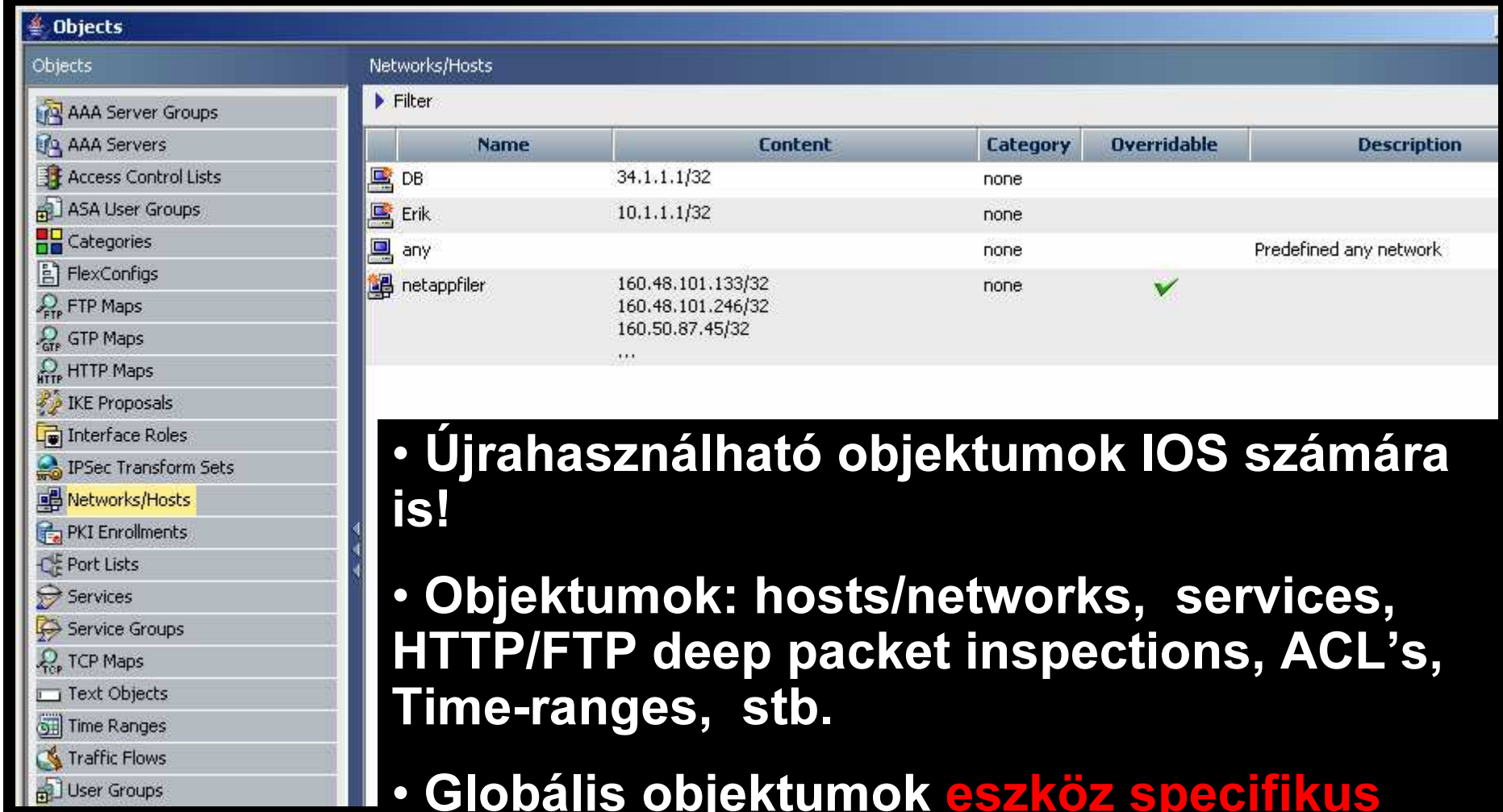
- Policy alkalmazható interfész csoportokra (zonákra) – skálázhatóság nő
  - “Interface Roles” készíthető, amelyik újrahasználható objektum interfész mintázattal (pl.: DMZ*, outside)
  - Az „interface roles” ugyanúgy használható egy szabályban, mint egy interfész
  - A config elkészítésénél az aktuális interfésznél figyelembe veszi az Interface role-t



Interfész szerepek (folyt.)



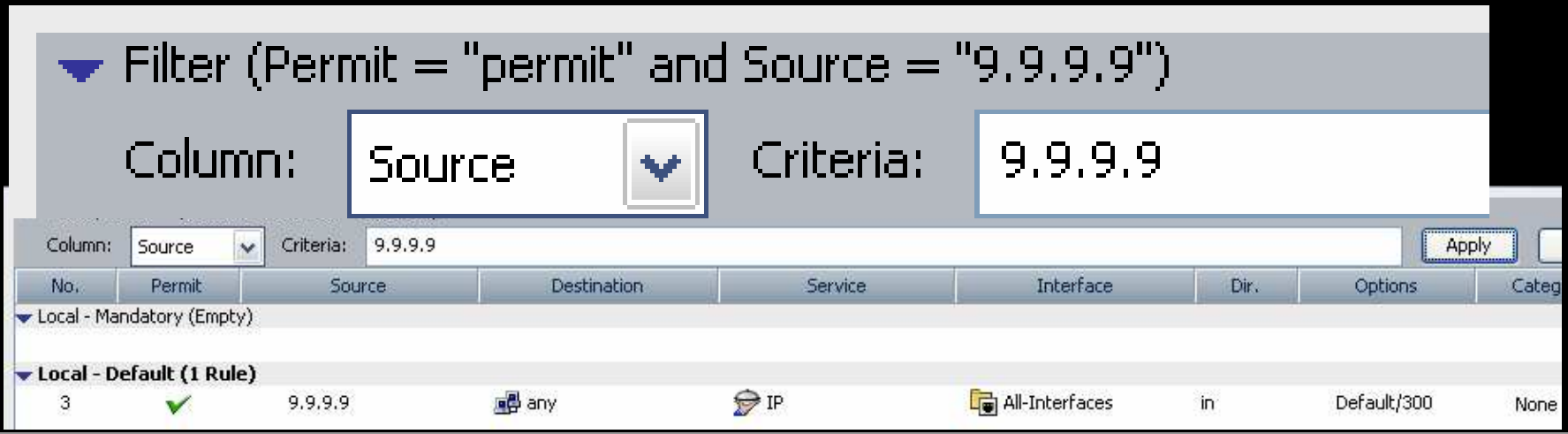
Policy objektum csoportok



- **Újrahasználható objektumok IOS számára is!**
- **Objektumok: hosts/networks, services, HTTP/FTP deep packet inspections, ACL's, Time-ranges, stb.**
- **Globális objektumok eszköz specifikus értékekkel!**

CSM szabály szűrés – rule filtering

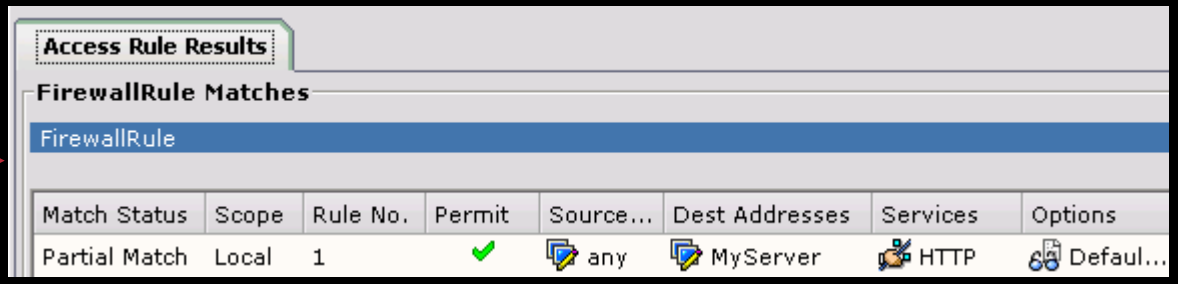
- **Gyors keresés és változtatás a szabály táblázatban**



Policy lekérdezés - Policy Query

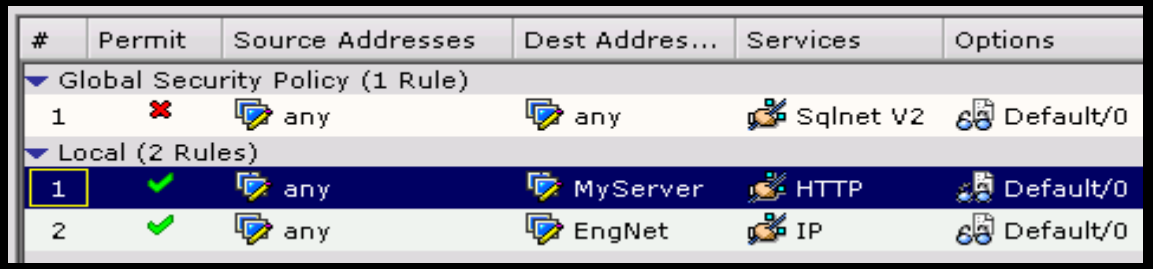
1. Lekérdezés

2. Lekérdezés eredménye

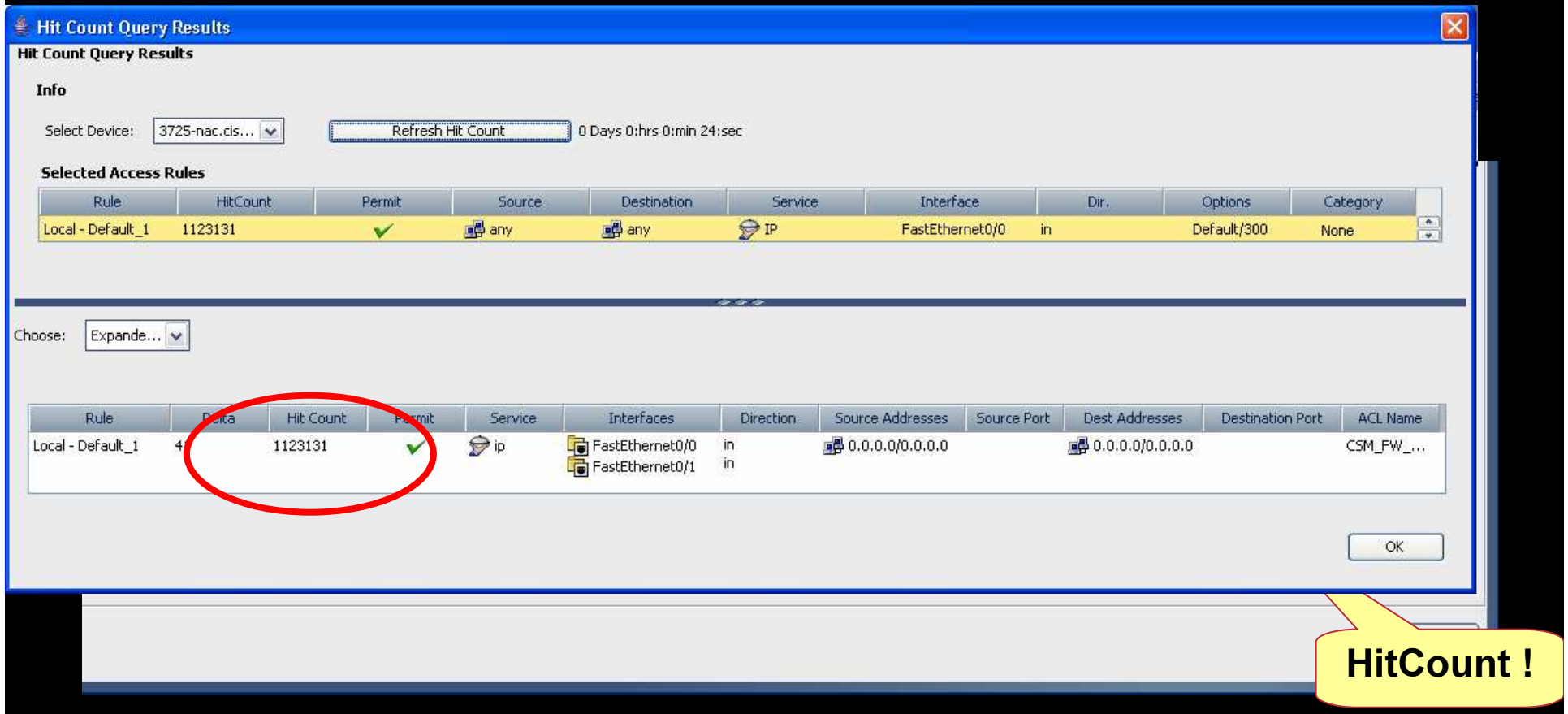


Kereszthivatkozás (double click a szabályon)

3. Szabály tábla (kiemeli az egyező szabályt)



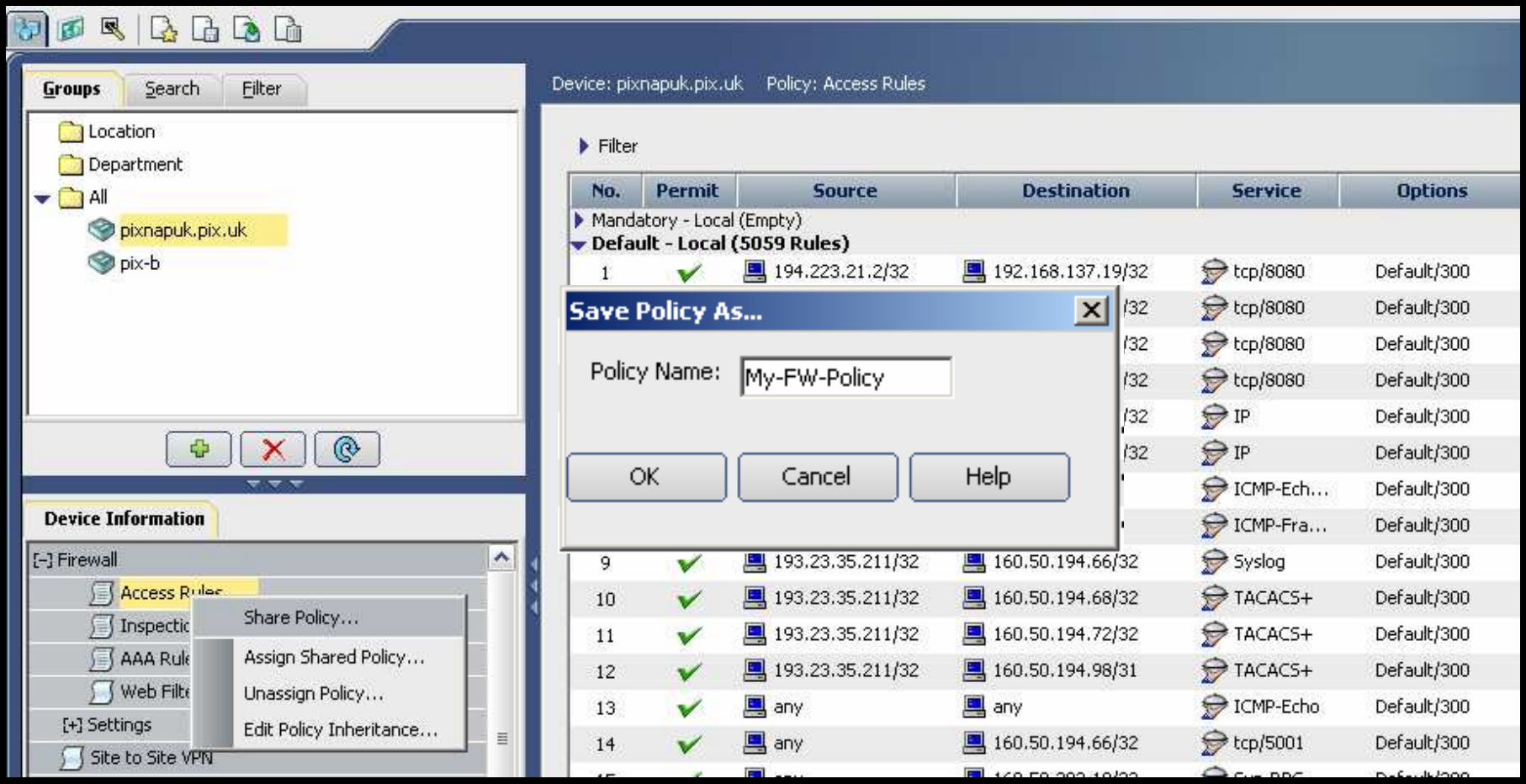
ACL Hitcount – találat számláló



A CSM ellenőrzi, hogy a szabály működik-e! Valósítsunk meg egy szabályt, és nézzük, hogy lesz-e találat!

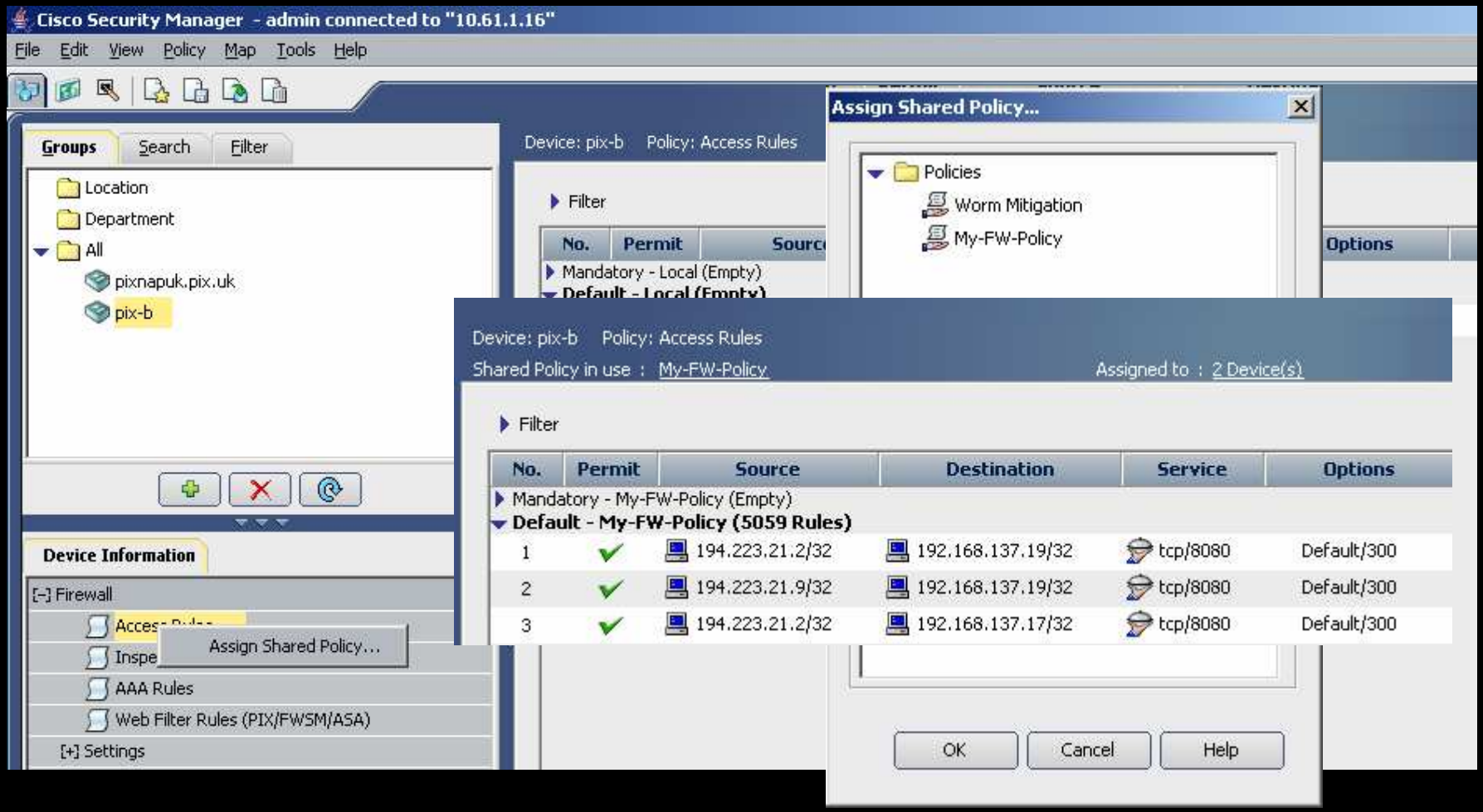
CSM – EGYSZERŰ POLICY KONFIGURÁLÁS

1. lépés: eszköz policy megosztása



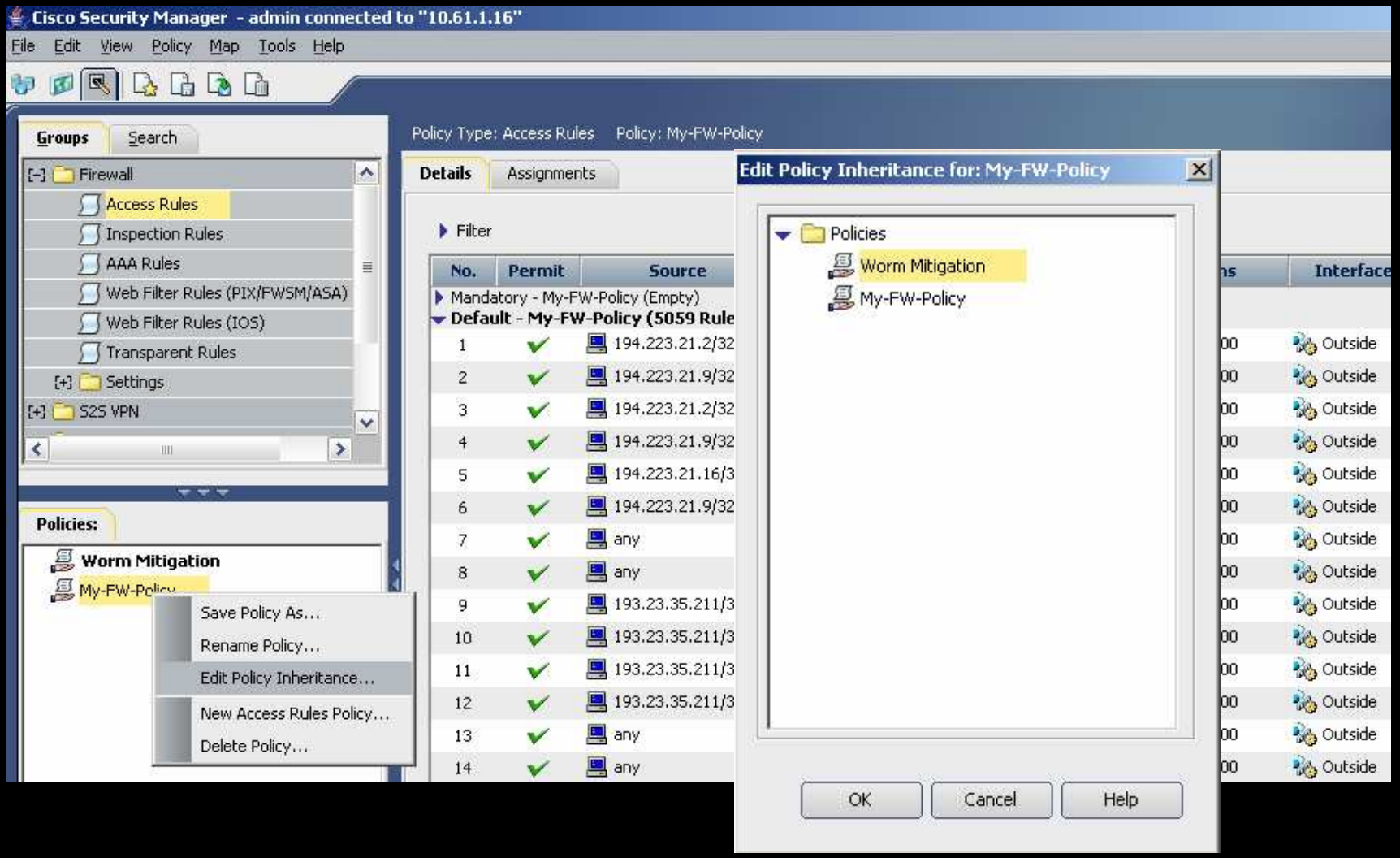
- **Vegyünk egy eszköz policy-t/beállítást és mentsük el – a megosztáshoz**

2. lépés : újra használjuk a megosztott policy-t

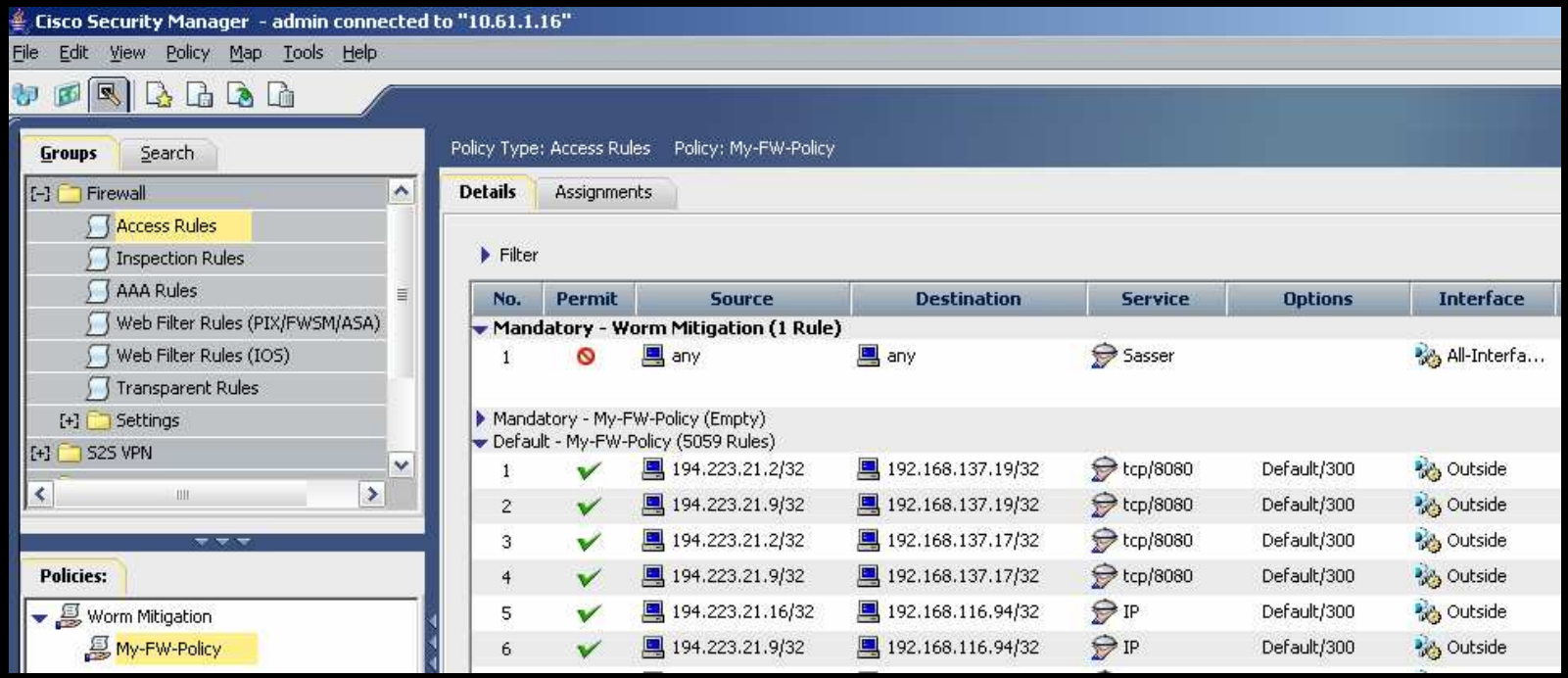


- **Válasszuk ki a policy-t és csatoljuk a második eszközhöz (Pix-B)**

VAGY: használjuk a megosztott policy-t örökítésre

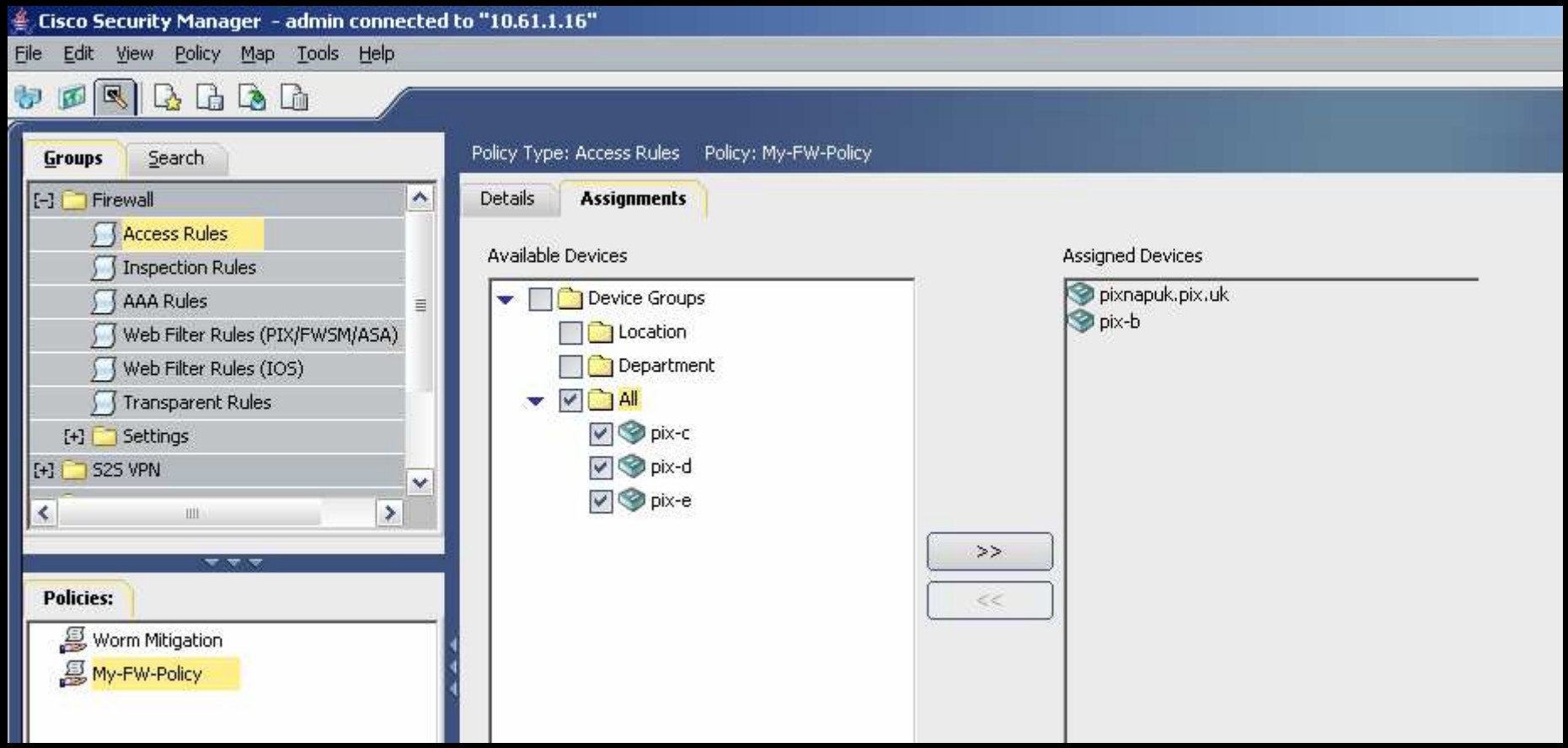


VAGY: használjuk a megosztott policy-t örökítésre (folyt.)



- Most a ‘Worm Mitigation’ policy mindig része a ‘My-FW-Policy’-nak
- A „Mandatory rules” az eszköz specifikus policy-k előtt vannak
- A „Default rules” az eszköz specifikus policy-k mögött vannak

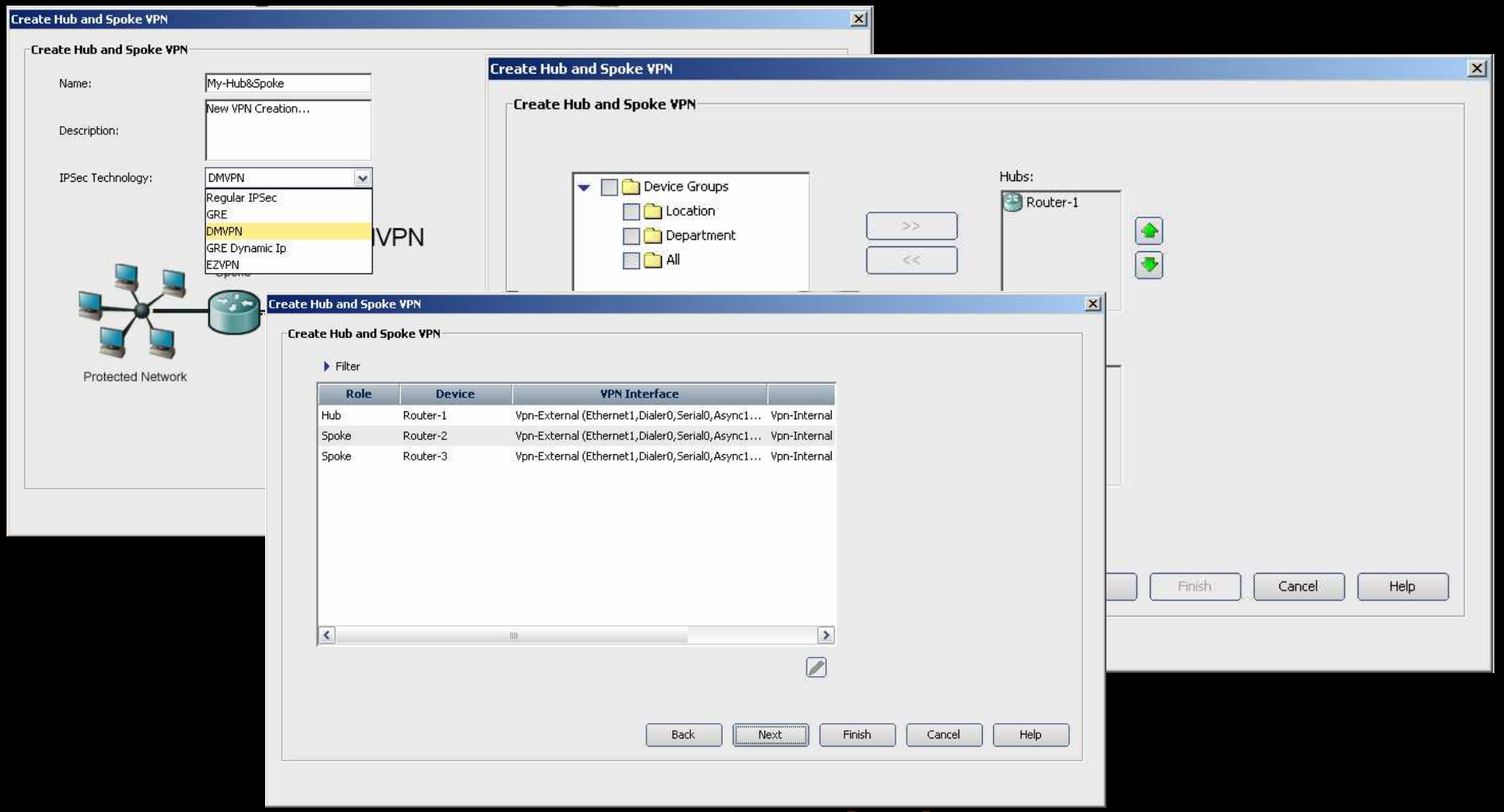
VAGY a Policy View-ban: A policy-t akár több 100 eszközhöz csatolhatjuk egyszerre!



Használjuk az eszköz csoportokat arra, hogy gyorsan tudjunk megosztott policy-t több száz eszközhöz rendelni -> sok telephelyes ügyfél

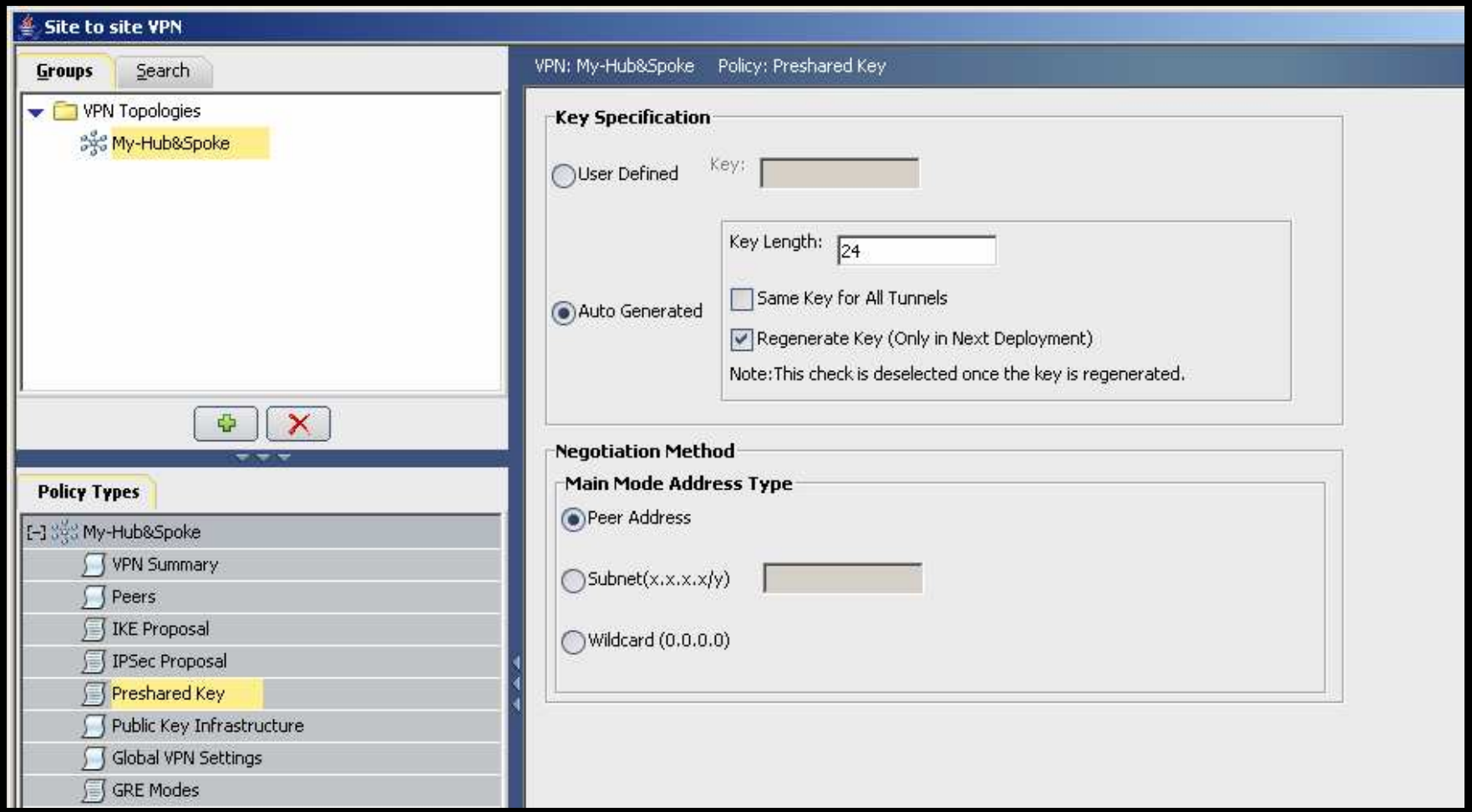
CSM – VPN KONFIGURÁCIÓ

VPN menedzsment - bevezetés



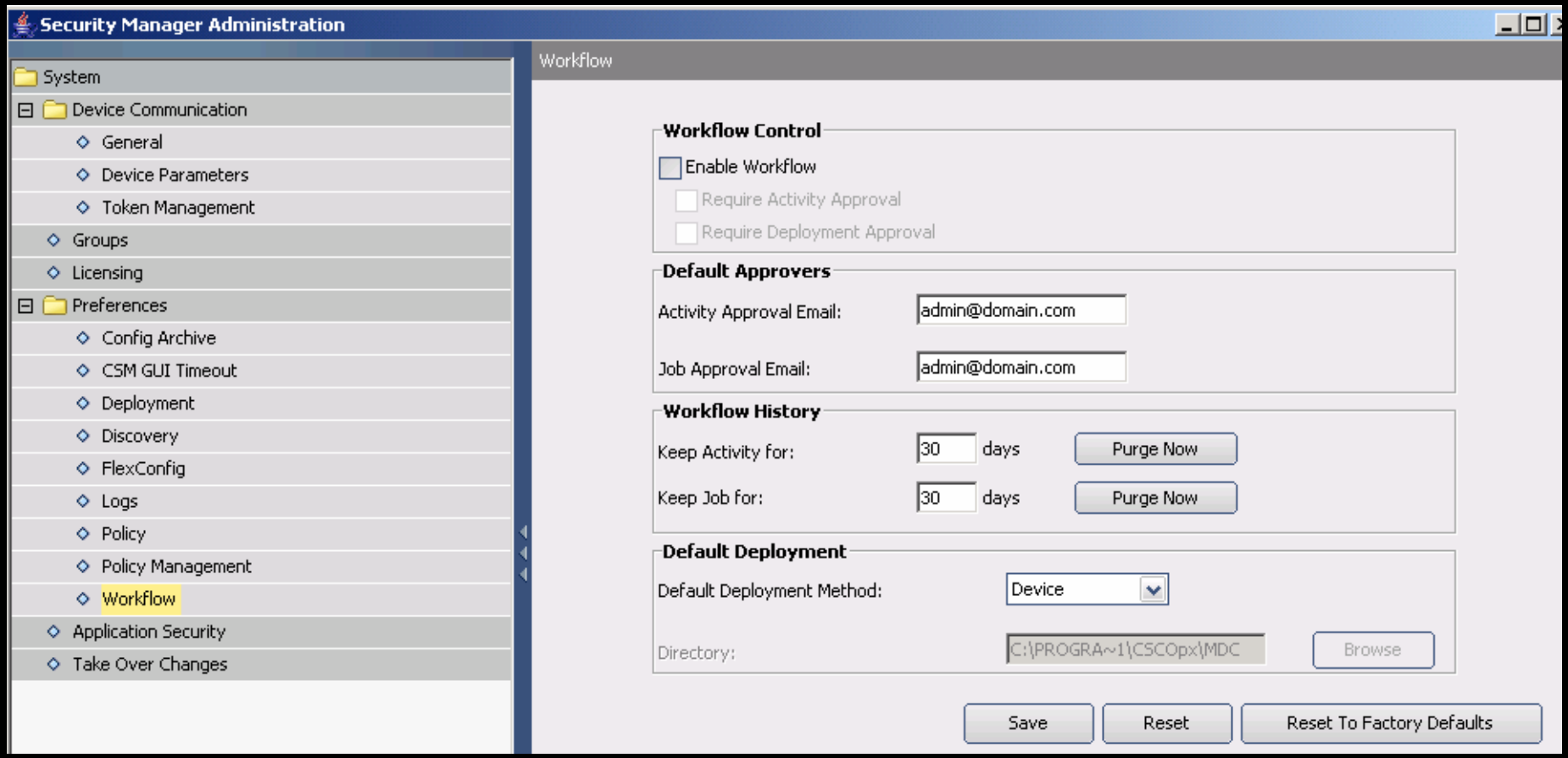
- **3 klick - VPN konfiguráció!**

VPN - változtatás a default-okhoz képest

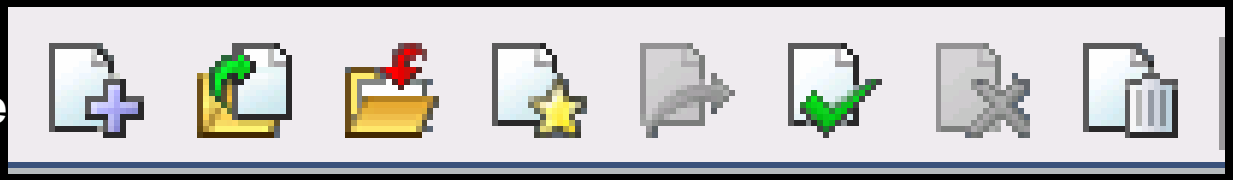


CSM – OPERÁTOROK JOGOSULTSÁGAI

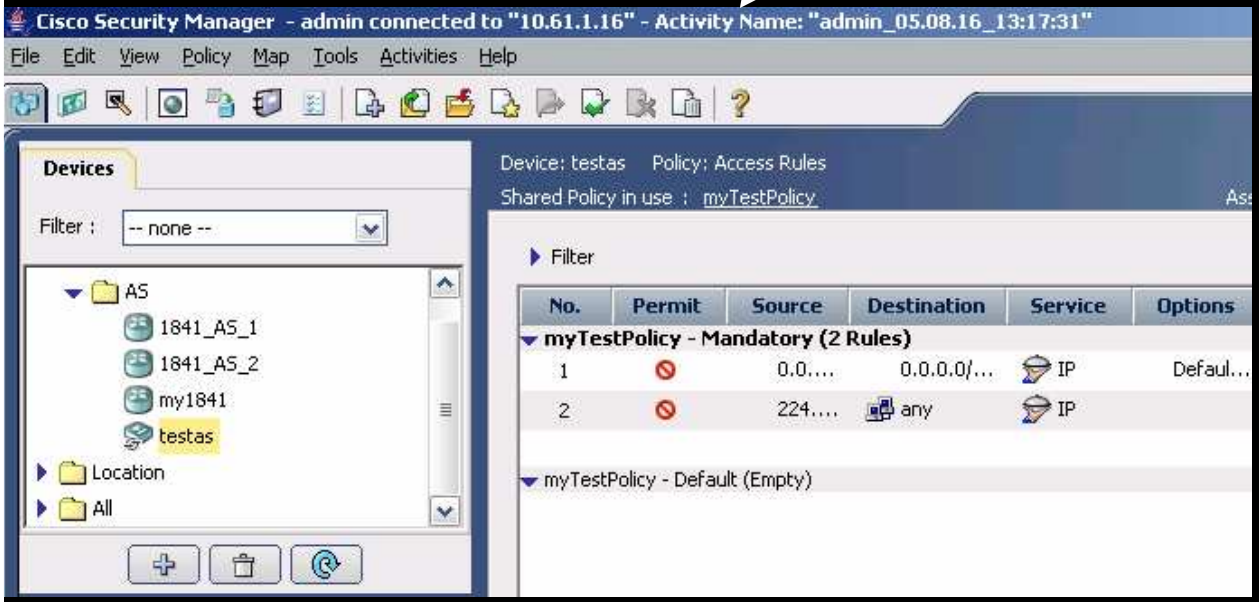
Workflow: Setup



Workflow: New buttons

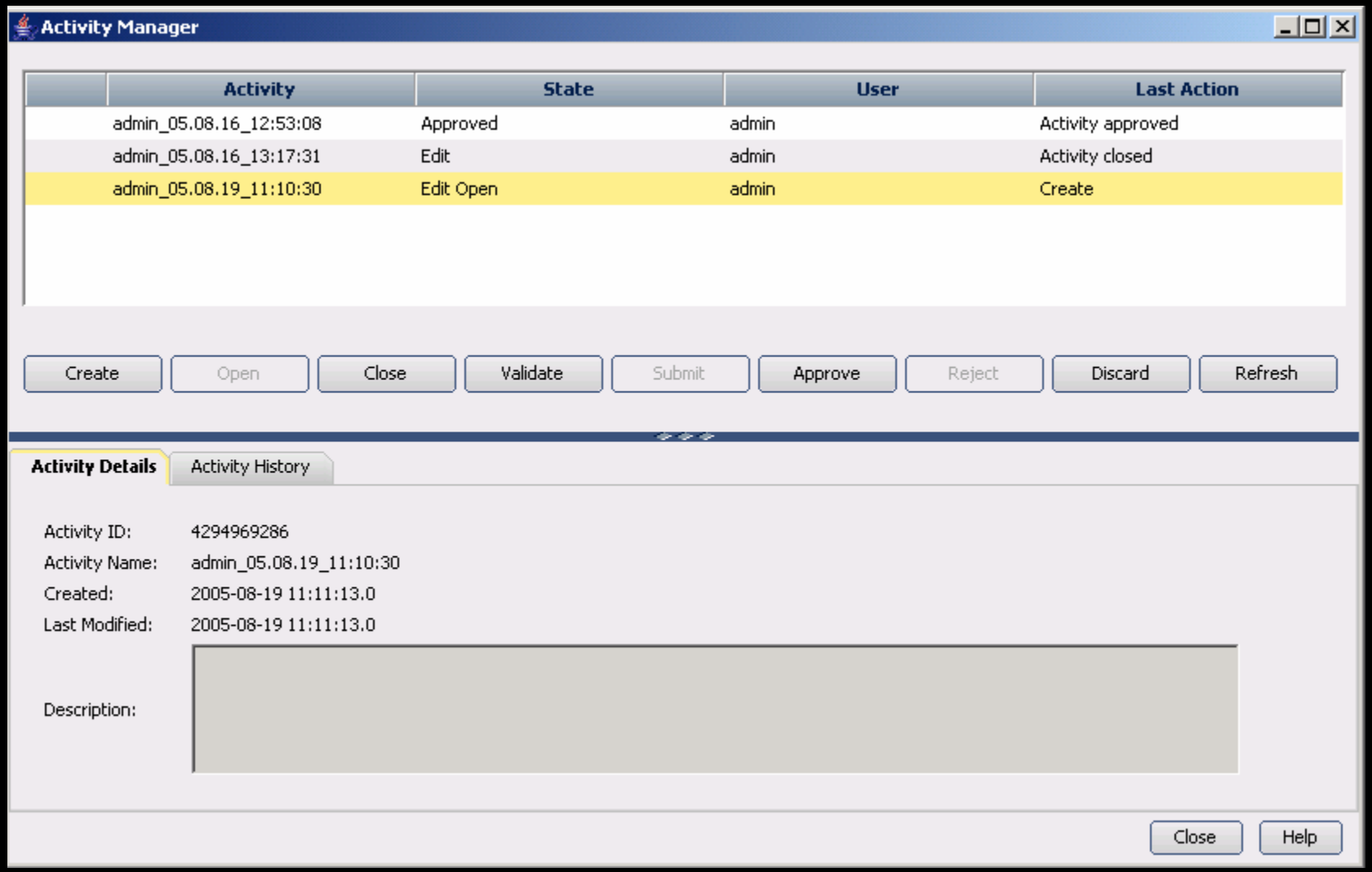
create  discard

open close validate submit approve reject

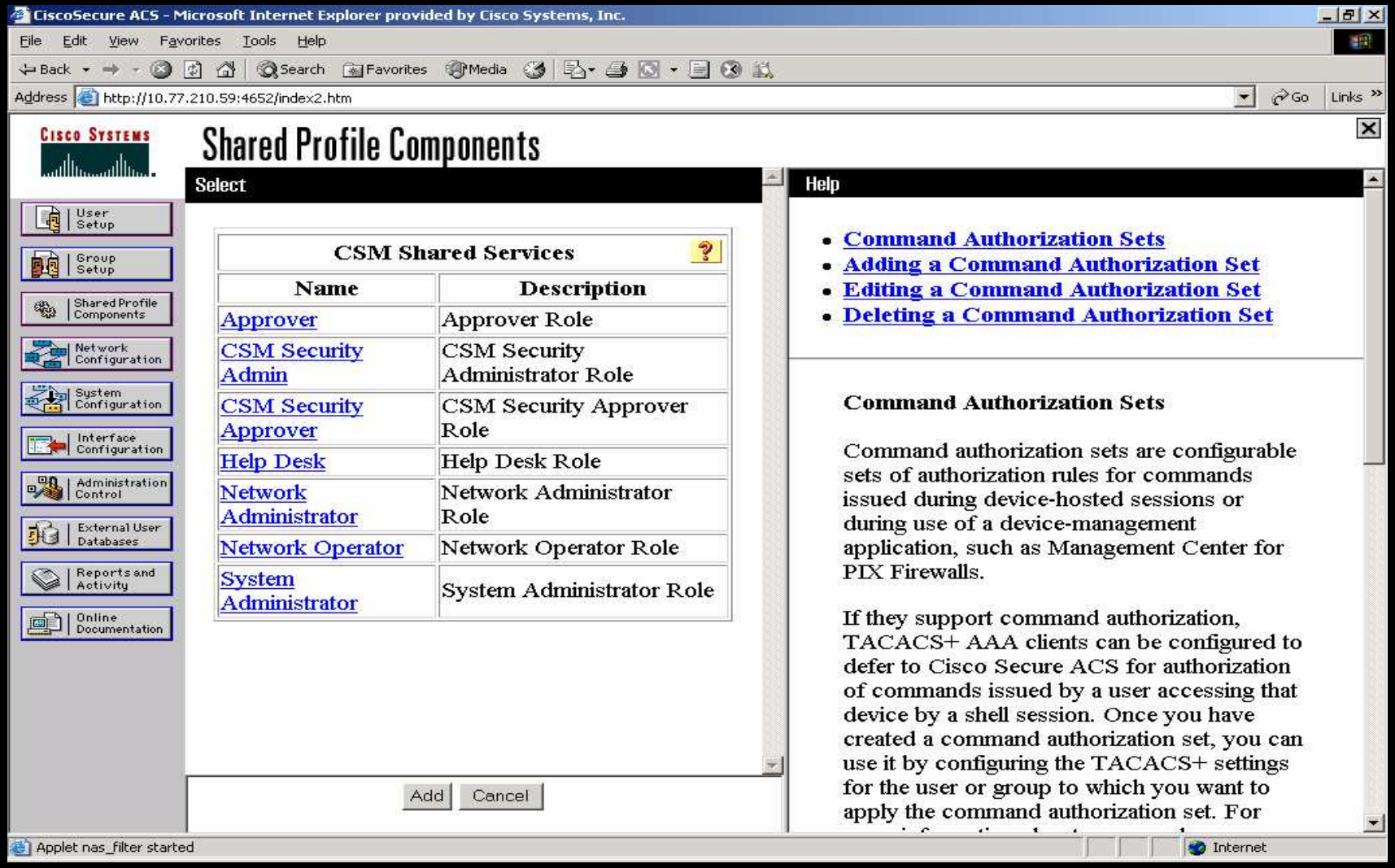


Több operátor együttműködése: Policy locking!

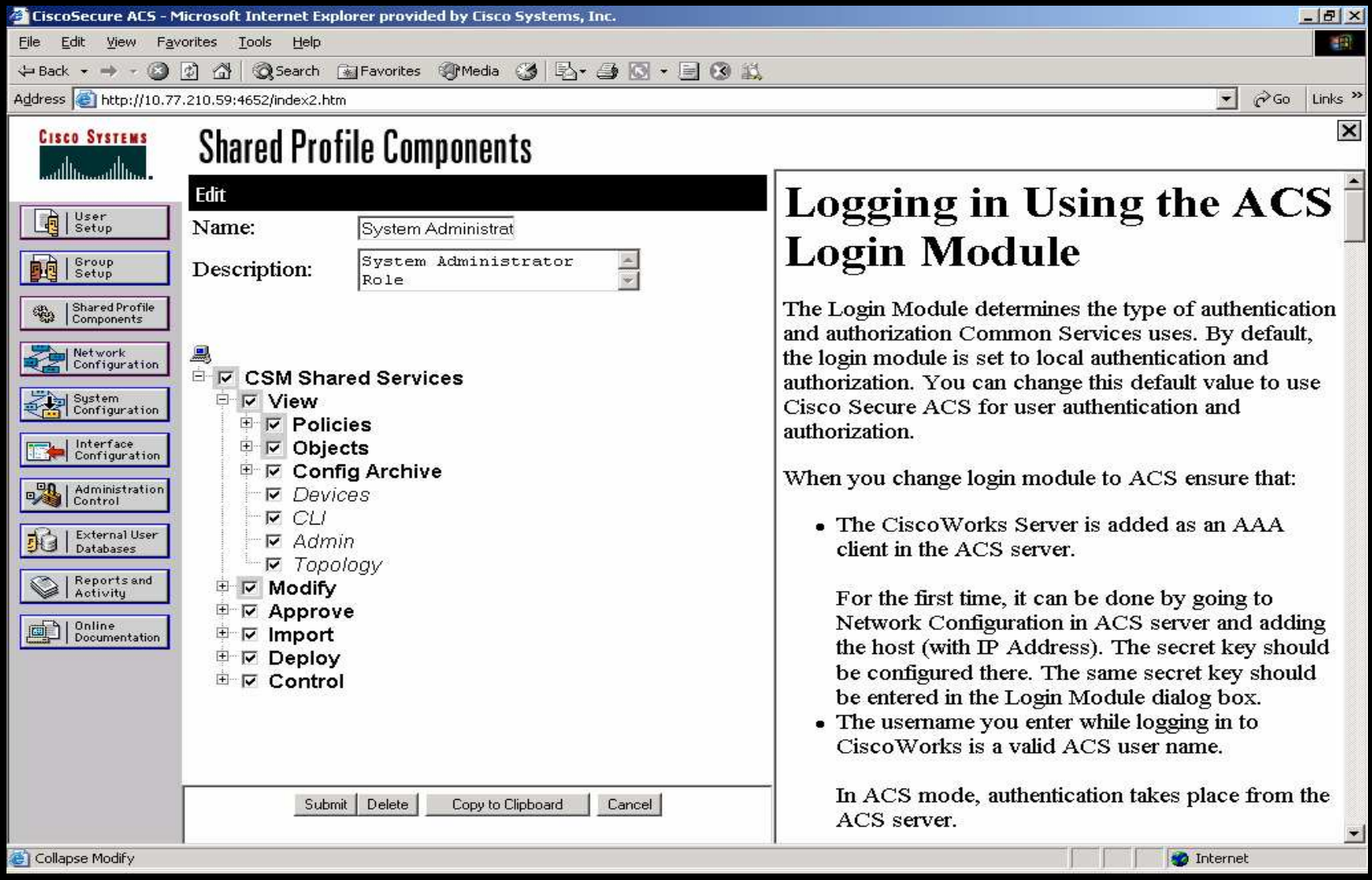
Approve/Reject aktivitások az activity manager-ben



RBAC -- 8 szerep – konfigurálható jogosultságok



RBAC -- 8 szerep – konfigurálható jogosultságok



ÖSSZEFOGLALÁS

Összefoglalás

A Cisco Security Manager segít ...

- **A feladatokat gyorsabban lehet végrehajtani :**
  - A szabály tábla sok szolgáltatást nyújt
  - Policy megosztás: konfigáljunk egyszer, alkalmazzuk sokszor
  - Újra használható objektumok, interfész szerepek
- **A feladatokat ügyesebben lehet végrehajtani:**
  - Rule Conflict Detection, Policy Query
  - ACL HitCount
- **Egyszerű migráció - IOS <-> ASA <-> FWSM**
- **Gyors migráció a nem virtualizáltból a virtualizáltba**
- **Összetett VPN konfiguráció - 3 egyszerű lépésben**

Összefoglalás

- Sok ügyfeles szolgáltatások
  - RBAC
  - Workflow
  - Eszközök klónozása = nagy mennyiségű fiókirodai telepítés
- Flow (nem eszköz) szintű alkalmazás specifikus szabály
- Az elvárt feltételek már a 3.0-ban támogatottak, később még további szolgáltatások is jönnek...
- Nagyon versenyképes ár

KÉRDÉSEK ÉS VÁLASZOK