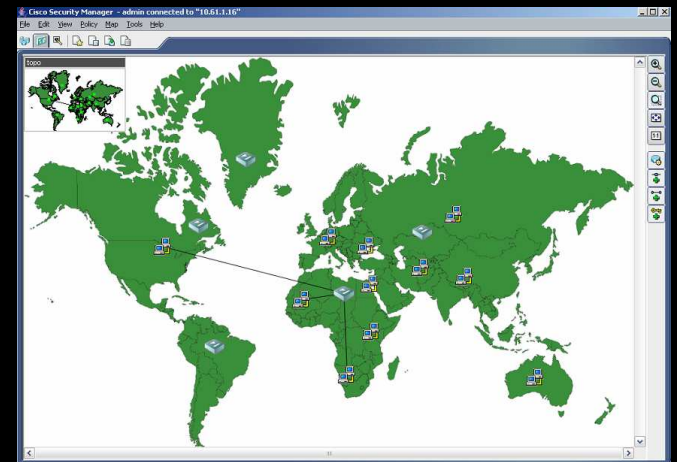




# Cisco Security Manager

**ÁCS GYÖRGY**  
**GACS@CISCO.COM**



# Tartalom

**Cisco security menedzsment  
alkalmazások**

**CSM főbb jellemzői**

**CSM - egyszerű policy  
konfigurálás**

**CSM - VPN konfigurálás**

**CSM – operátorok jogosultságai**

**Összefoglalás**



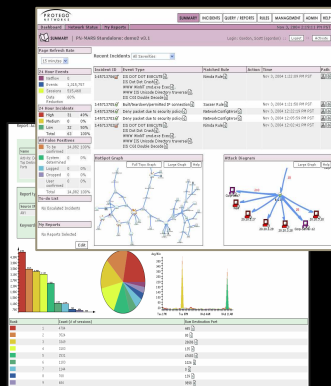
# CISCO SECURITY MENEDZSMENT ALKALMAZÁSOK



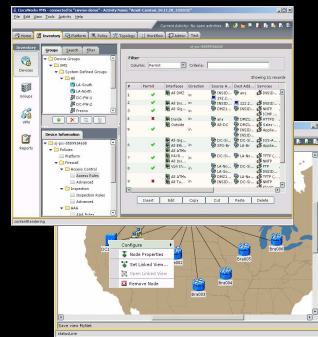
# Security menedzsment alkalmazások

Menedzsment

MARS



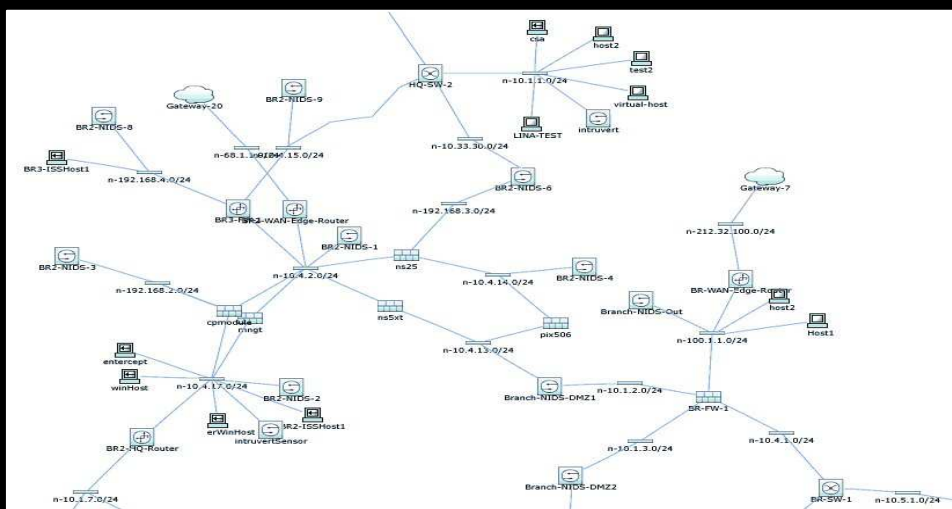
Security Manager



ACS



Hálózati eszközök



- Tűzfalak
- Integrált biztonsági megoldások (ASA)
- Host alapú IDS/IPS
- Routers (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

Device: pxnapuk.pbx.uk Policy: Static Route

Routing - Static Route

Interface	Network	Gateway	Metric	Tunneled
Inside	any	193.23.35.195/32	5	
Outside	157.147.0.0/16	193.23.35.213/32	2	
Outside	157.147.6.0/24	193.23.35.213/32	2	
Outside	157.147.72.0/21	193.23.35.213/32	2	
Outside	157.147.73.0/24	193.23.35.213/32	2	
Outside	157.147.74.0/24	193.23.35.213/32	2	
Outside	157.147.75.0/24	193.23.35.213/32	2	
Outside	157.147.76.0/24	193.23.35.213/32	2	
Outside	157.147.77.0/24	193.23.35.213/32	2	
Outside	157.147.78.0/24	193.23.35.213/32	2	
Outside	157.147.79.0/24	193.23.35.213/32	2	
Outside	157.147.108.0/24	193.23.35.213/32	2	
Outside	157.148.0.0/16	193.23.35.213/32	2	
Outside	157.148.128.0/19	193.23.35.213/32	2	
Outside	167.16.0.0/16	193.23.35.213/32	2	
Outside	172.17.192.0/24	193.23.35.218/32	2	
Outside	172.17.193.0/24	193.23.35.219/32	2	
Outside	172.17.194.0/24	193.23.35.213/32	1	
Outside	172.17.195.0/26	193.23.35.213/32	2	
Outside	172.17.195.64/26	193.23.35.213/32	2	
Outside	172.17.195.128/26	193.23.35.213/32	2	
Outside	172.17.195.192/26	193.23.35.213/32	2	

Save

**Eszköz választás**

**Policy választás**

**Aktuális beállítás**

# 3 nézet: Policy View

The screenshot shows the Cisco Security Manager interface. The left pane displays a tree view of policy groups, including 'Firewall', 'Access Rules', 'Inspection Rules', 'AAA Rules', 'Web Filter Rules (PIX/FWSM/ASA)', 'Web Filter Rules (IOS)', 'Transparent Rules', 'Settings', 'S2S VPN', and 'RA'. The 'Policies' pane shows a 'Worm Mitigation' policy. The main pane displays the 'Details' view for the 'Worm Mitigation' policy, showing a table of rules.

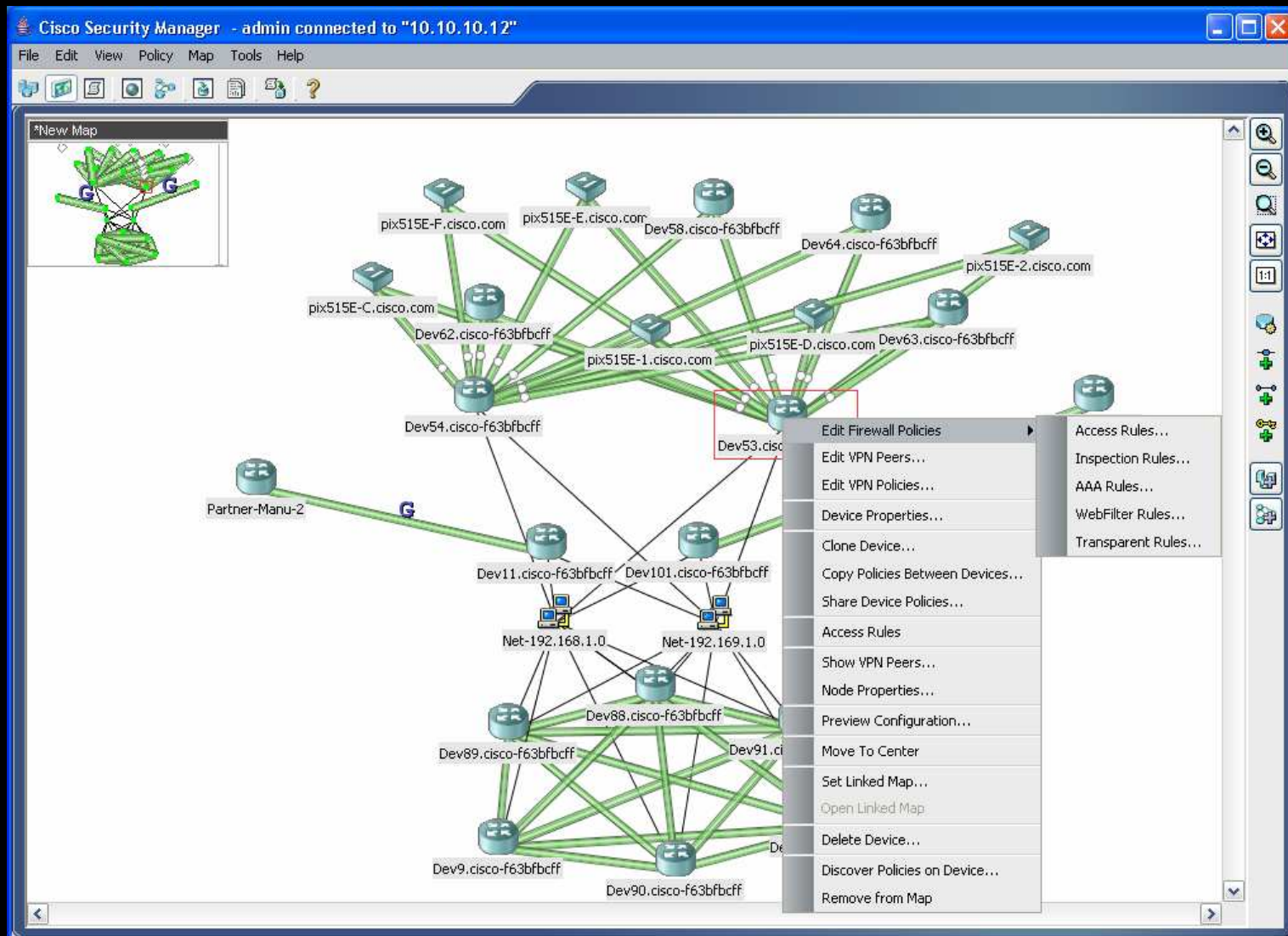
No.	Permit	Source	Destination	Service	Options	Interfac
Mandatory - Worm Mitigation (1 Rule)						
1		any	any	Sasser		All-Interf
Default - Worm Mitigation (1 Rule)						
1		any	any	IP		All-Interf

Buttons at the bottom: Query, Conflicts, HitCount, [Print], [Edit], [Delete], Save.

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

Cisco Security Manager - admin connected to "10.61.1.16"

File Edit View Policy Map Tools Help

Device: pixnapuk.pix.uk Policy: Access Rules

Filter

No.	Permit	Source	Destination	Service	Interface
Mandatory - Local (Empty)					
Default - Local (5059 Rules)					
1	✓	194.223.21.2/32	192.168.137.19/32	tcp/8080	Outside
2	✓	194.223.21.9/32	192.168.137.19/32	tcp/8080	Outside
3	✓	194.223.21.2/32	192.168.137.17/32	tcp/8080	Outside
4	✓	194.223.21.9/32	192.168.137.17/32	tcp/8080	Outside
5	✓	194.223.21.16/32	192.168.116.94/32	tcp/8080	Outside
6	✓	194.223.21.9/32	192.168.116.94/32	tcp/8080	Outside
7	✓	any	any	any	any
8	✓	any	any	any	any
9	✓	193.23.35.211/32	160.50.194.66/32	any	any
10	✓	193.23.35.211/32	160.50.194.68/32	any	any
11	✓	193.23.35.211/32	160.50.194.72/32	any	any
12	✓	193.23.35.211/32	160.50.194.98/31	any	any
13	✓	any	any	any	any
14	✓	any	160.50.194.66/32	any	any
15	✓	any	160.50.202.10/32	any	any
16	✓	any	160.50.205.10/32	any	any

- Edit Destinations...
- Add Row... Ctrl+R
- Edit Row... Ctrl+E
- Delete Row Ctrl+D
- View Row...
- Cut Ctrl+X
- Copy Ctrl+C
- Paste Ctrl+V
- Move Row Up Ctrl+Up
- Move Row Down Ctrl+Down
- Enable

Edit Firewall Rule

Enable Rule

Action:  Permit  Deny

Sources:\* 194.223.21.16/32 [Select...]

Destinations:\* 192.168.116.94/32 [Select...]

Services:\* ip [Select...]

Interfaces:\* Outside [Edit...]

Enable Logging

Logging Level: Default [v]

Description:

Advanced

Traffic Direction:  In  Out

Logging Interval: 300

Category: none [v]

Time Range: [Select...]

Fragment (IOS)

Established (IOS)

OK Cancel Help

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

# Interfész szerepek

- Policy alkalmazható **interfész csoportokra (zonákra)** – skálázhatóság nő

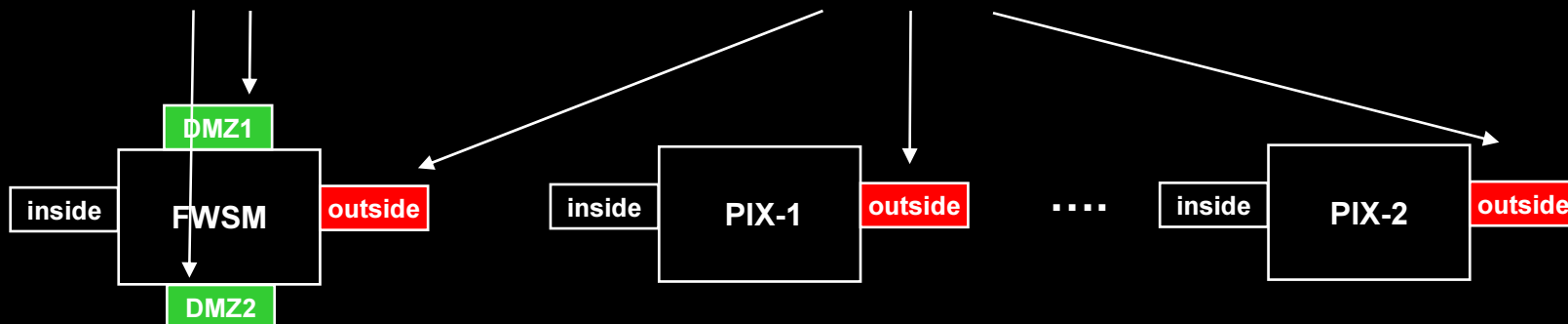
“Interface Roles” készíthető, amelyik újrahasználható objektum interfész mintázattal (pl.: DMZ\*, outside)

Az „interface roles” ugyanúgy használható egy szabályban, mint egy interfész

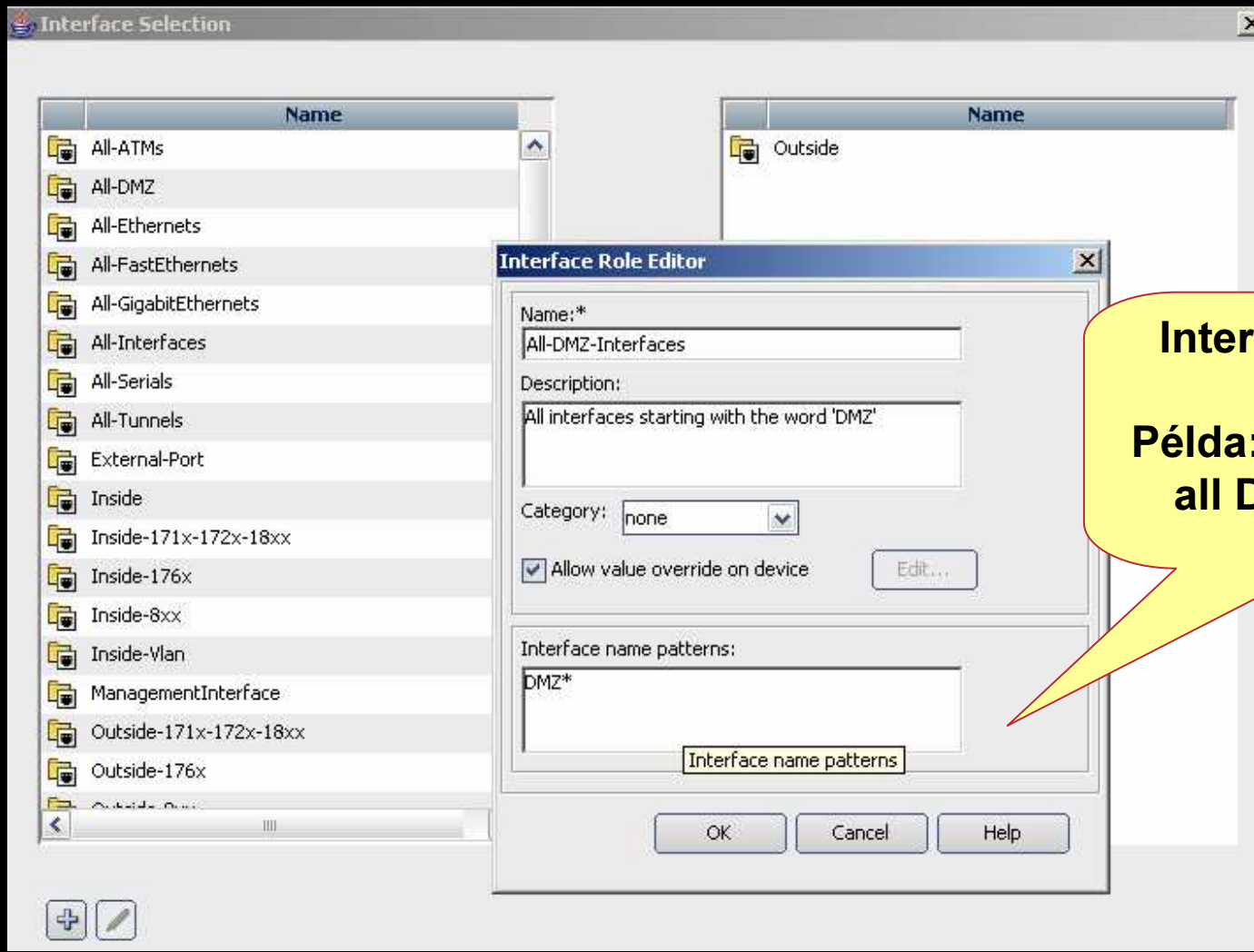
A config elkészítésénél az aktuális interfésznél figyelembe veszi az Interface role-t

**Permit any to myWebServer  
on all DMZ Interfaces**

**Deny x to any  
on all outside interface**



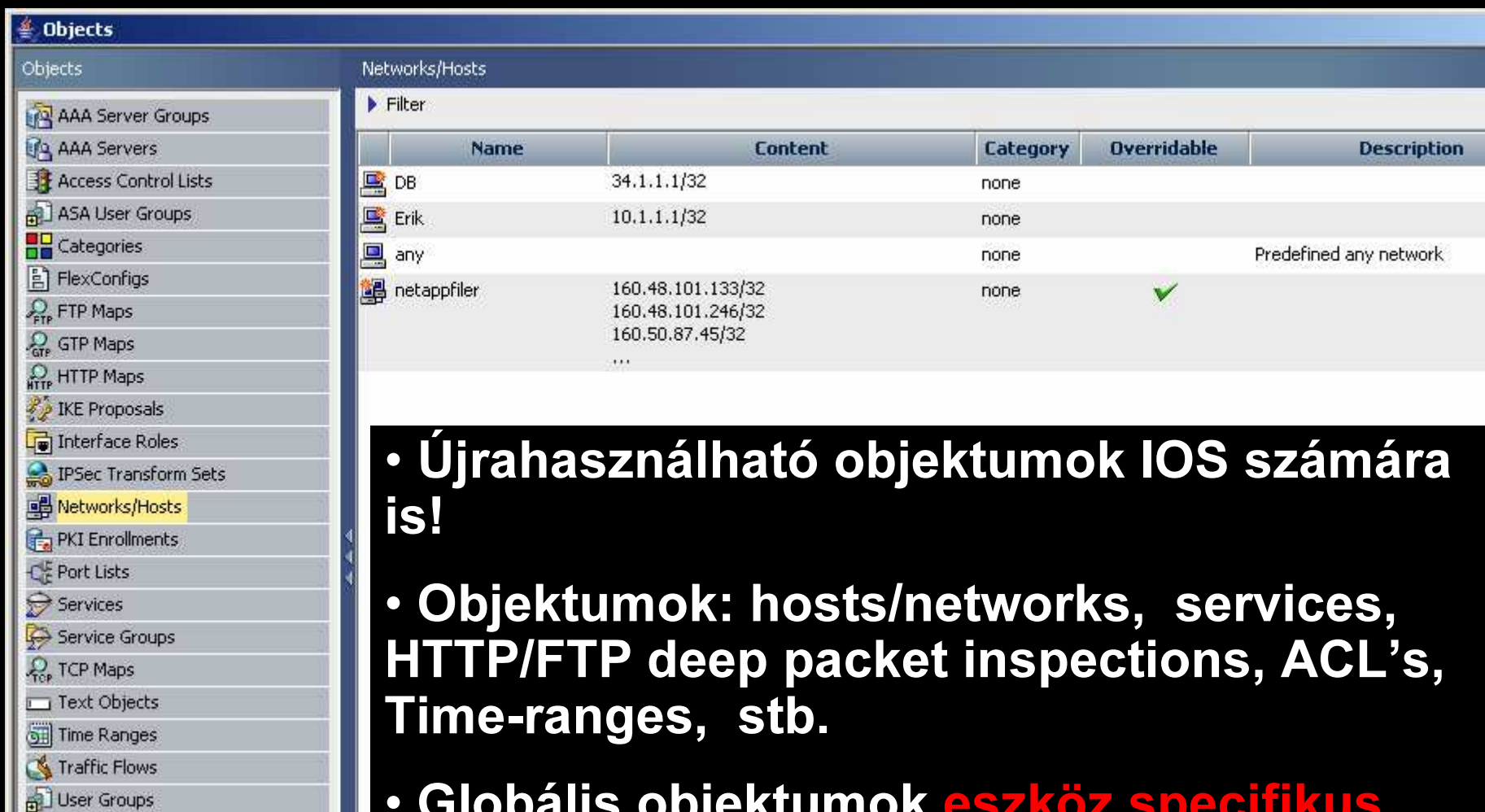
# Interfész szerepek (folyt.)



**Interfész csoportok**

**Példa: Permit HTTP to all DMZ interfaces**

# Policy objektum csoportok



The screenshot shows the Cisco Security Manager Objects console. The left pane displays a tree view of object categories, with 'Networks/Hosts' selected. The right pane shows a table of objects in this category.

Name	Content	Category	Overridable	Description
DB	34.1.1.1/32	none		
Erik	10.1.1.1/32	none		
any		none		Predefined any network
netappfiler	160.48.101.133/32 160.48.101.246/32 160.50.87.45/32 ...	none	✓	

- 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

Device: 3725-nac.cisco.com Policy: Access Rules

Filter (none)  
Column: Permit Criteria: permit Apply

No.	Permit	Source	Destination	Service	Interface	Dir.	Options	Cat
Local - Mandatory (Empty)								
Local - Default (4 Rules)								
1	✓	any	any	IP	FastEthernet0/0 FastEthernet0/1	in	Default/300	No
2	✗	any	any	IP	All-Interfaces	in	Default/300	No
3	✓	9.9.9.9	any	IP	All-Interfaces	in	Default/300	No
4	✗	30.1.1.1	any	IP	All-Interfaces	in	Default/300	No

- Gyors keresés és változtatás a szabály táblázatban

Filter (Permit = "permit" and Source = "9.9.9.9")

Column: Source Criteria: 9.9.9.9 Apply

No.	Permit	Source	Destination	Service	Interface	Dir.	Options	Categ
Local - Mandatory (Empty)								
Local - Default (1 Rule)								
3	✓	9.9.9.9	any	IP	All-Interfaces	in	Default/300	None

# Policy lekérdezés - Policy Query

## 1. Lekérdezés

**Rule Types**

AAA Rules     Access Rules

**Enabled and/or Disabled Rules**

Enabled Rules     Disabled Rules

**Actions**

Permit     Deny

Source Addresses:

Destination Addresses:

Interfaces:

Services:

## 2. Lekérdezés eredménye

**Access Rule Results**

**FirewallRule Matches**

FirewallRule

Match Status	Scope	Rule No.	Permit	Source...	Dest Addresses	Services	Options
Partial Match	Local	1	✓	any	MyServer	HTTP	Default...

Kereszthivatkozás (double click a szabályon)

## 3. Szabály tábla (kiemeli az egyező szabályt)

#	Permit	Source Addresses	Dest Address...	Services	Options
▼ Global Security Policy (1 Rule)					
1	✗	any	any	Sqlnet V2	Default/0
▼ Local (2 Rules)					
1	✓	any	MyServer	HTTP	Default/0
2	✓	any	EngNet	IP	Default/0

# ACL Hitcount – találat számláló

Hit Count Query Results

Hit Count Query Results

Info

Select Device: 3725-nac.cis... Refresh Hit Count 0 Days 0:hrs 0:min 24:sec

Selected Access Rules

Rule	HitCount	Permit	Source	Destination	Service	Interface	Dir.	Options	Category
Local - Default_1	1123131	✓	any	any	IP	FastEthernet0/0	in	Default/300	None

Choose: Expande...

Rule	Permit	Hit Count	Service	Interfaces	Direction	Source Addresses	Source Port	Dest Addresses	Destination Port	ACL Name
Local - Default_1	✓	1123131	ip	FastEthernet0/0 FastEthernet0/1	in in	0.0.0.0/0.0.0.0		0.0.0.0/0.0.0.0		CSM_FW_...

OK

HitCount !

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

# CSM – EGYSZERŰ POLICY KONFIGURÁLÁS



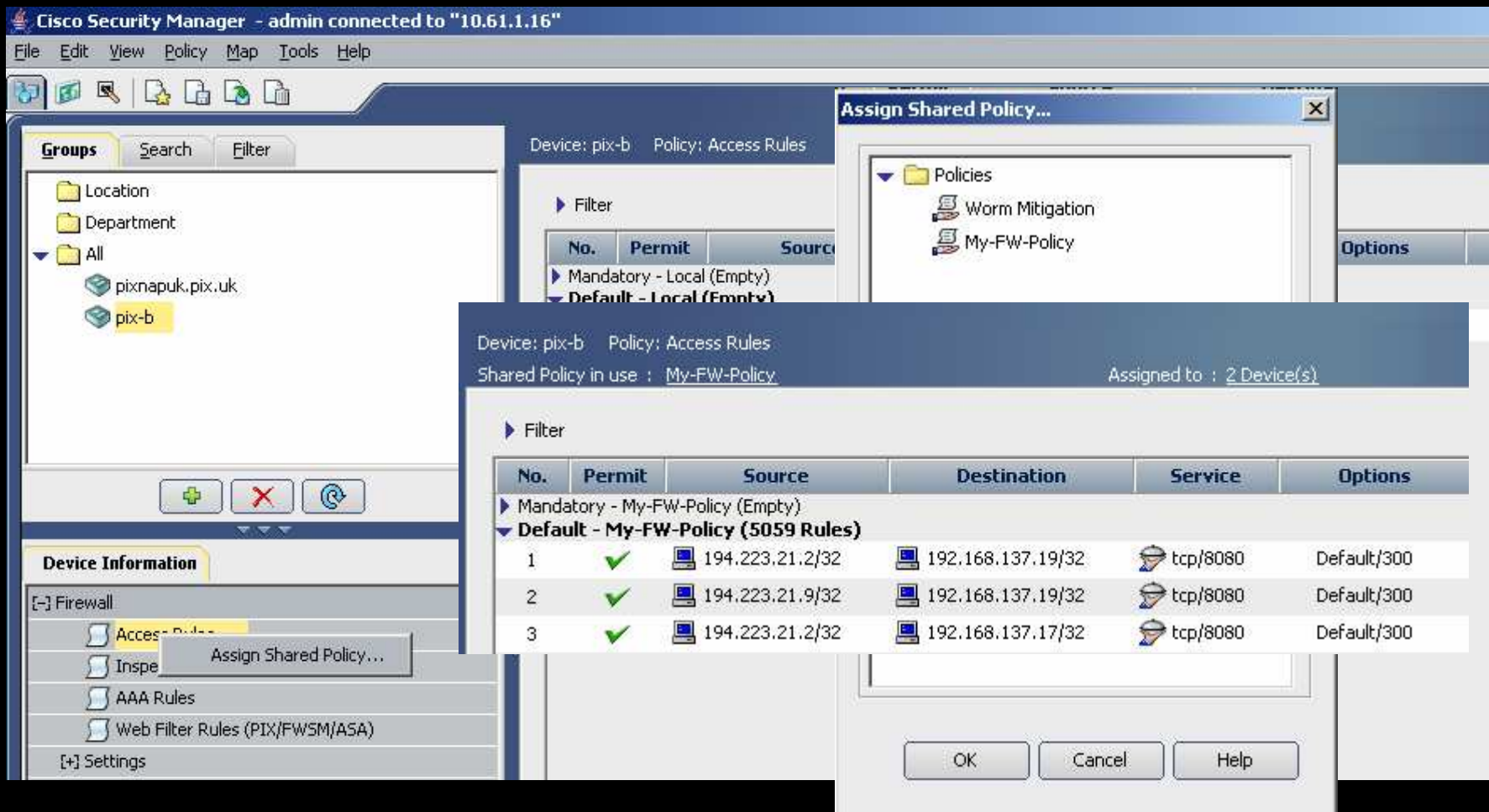
# 1. lépés: eszköz policy megosztása

The screenshot shows the Cisco Firepower Management Center interface. On the left, a tree view shows the hierarchy: Groups > All > pixnapuk.pix.uk. The main area displays 'Device: pixnapuk.pix.uk' and 'Policy: Access Rules'. A table of rules is visible, with a 'Save Policy As...' dialog box overlaid on it. The dialog box has a text field for 'Policy Name' containing 'My-FW-Policy' and buttons for 'OK', 'Cancel', and 'Help'. The table below the dialog shows the following rules:

No.	Permit	Source	Destination	Service	Options
1	✓	194.223.21.2/32	192.168.137.19/32	tcp/8080	Default/300
9	✓	193.23.35.211/32	160.50.194.66/32	Syslog	Default/300
10	✓	193.23.35.211/32	160.50.194.68/32	TACACS+	Default/300
11	✓	193.23.35.211/32	160.50.194.72/32	TACACS+	Default/300
12	✓	193.23.35.211/32	160.50.194.98/31	TACACS+	Default/300
13	✓	any	any	ICMP-Echo	Default/300
14	✓	any	160.50.194.66/32	tcp/5001	Default/300

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

## 2. lépés : újra használjuk a megosztott policy-t



Device: pix-b Policy: Access Rules

Shared Policy in use : My-FW-Policy Assigned to : 2 Device(s)

No.	Permit	Source	Destination	Service	Options
Mandatory - My-FW-Policy (Empty)					
Default - My-FW-Policy (5059 Rules)					
1	✓	194.223.21.2/32	192.168.137.19/32	tcp/8080	Default/300
2	✓	194.223.21.9/32	192.168.137.19/32	tcp/8080	Default/300
3	✓	194.223.21.2/32	192.168.137.17/32	tcp/8080	Default/300

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

# VAGY: használjuk a megosztott policy-t örökítésre

The screenshot displays the Cisco Security Manager web interface. The main window shows the 'Policy Type: Access Rules' and 'Policy: My-FW-Policy'. A context menu is open over the 'My-FW-Policy' entry in the 'Policies' list, with 'Edit Policy Inheritance...' selected. An 'Edit Policy Inheritance for: My-FW-Policy' dialog box is open, showing a tree view of policies with 'Worm Mitigation' and 'My-FW-Policy' listed. In the background, a table lists 14 rules under the 'Default - My-FW-Policy (5059 Rule)'.

No.	Permit	Source
Mandatory - My-FW-Policy (Empty)		
Default - My-FW-Policy (5059 Rule)		
1	✓	194.223.21.2/32
2	✓	194.223.21.9/32
3	✓	194.223.21.2/32
4	✓	194.223.21.9/32
5	✓	194.223.21.16/3
6	✓	194.223.21.9/32
7	✓	any
8	✓	any
9	✓	193.23.35.211/3
10	✓	193.23.35.211/3
11	✓	193.23.35.211/3
12	✓	193.23.35.211/3
13	✓	any
14	✓	any

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

The screenshot shows the Cisco Security Manager interface. The left pane displays a tree view of 'Groups' including Firewall, Access Rules, Inspection Rules, AAA Rules, Web Filter Rules (PIX/FWSM/ASA), Web Filter Rules (IOS), Transparent Rules, Settings, and S2S VPN. The 'Policies' pane shows 'Worm Mitigation' and 'My-FW-Policy'. The main pane shows the 'Details' view for 'My-FW-Policy' (Access Rules). The table below shows the rules configuration:

No.	Permit	Source	Destination	Service	Options	Interface
Mandatory - Worm Mitigation (1 Rule)						
1	⊘	any	any	Sasser		All-Interfa...
Mandatory - My-FW-Policy (Empty)						
Default - My-FW-Policy (5059 Rules)						
1	✓	194.223.21.2/32	192.168.137.19/32	tcp/8080	Default/300	Outside
2	✓	194.223.21.9/32	192.168.137.19/32	tcp/8080	Default/300	Outside
3	✓	194.223.21.2/32	192.168.137.17/32	tcp/8080	Default/300	Outside
4	✓	194.223.21.9/32	192.168.137.17/32	tcp/8080	Default/300	Outside
5	✓	194.223.21.16/32	192.168.116.94/32	IP	Default/300	Outside
6	✓	194.223.21.9/32	192.168.116.94/32	IP	Default/300	Outside

- 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!

The screenshot displays the Cisco Security Manager web interface. At the top, it shows the user is connected to '10.61.1.16'. The main area is titled 'Policy Type: Access Rules' and 'Policy: My-FW-Policy'. On the left, a 'Groups' sidebar lists various rule categories like 'Firewall', 'Access Rules', 'Inspection Rules', etc. Below this is a 'Policies' section with 'My-FW-Policy' selected. The central 'Assignments' pane is split into two columns: 'Available Devices' and 'Assigned Devices'. Under 'Available Devices', a tree view shows 'All' selected, with sub-items 'pix-c', 'pix-d', and 'pix-e' checked. The 'Assigned Devices' column shows 'pixnapuk.pix.uk' and 'pix-b' already assigned. Navigation buttons '>>' and '<<' are visible between the columns.

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

# CSM – VPN KONFIGURÁCIÓ



# VPN menedzsment - bevezetés

**Create Hub and Spoke VPN**

Name: My-Hub&Spoke  
Description: New VPN Creation...  
IPsec Technology: DMVPN

Protected Network

**Create Hub and Spoke VPN**

Device Groups: Device Groups, Location, Department, All  
Hubs: Router-1

**Create Hub and Spoke VPN**

Role	Device	VPN Interface
Hub	Router-1	Vpn-External (Ethernet1,Dialer0,Serial0,Async1... Vpn-Internal
Spoke	Router-2	Vpn-External (Ethernet1,Dialer0,Serial0,Async1... Vpn-Internal
Spoke	Router-3	Vpn-External (Ethernet1,Dialer0,Serial0,Async1... Vpn-Internal

- **3 klick - VPN konfiguráció!**

# VPN - változtatás a default-okhoz képest

The screenshot displays the Cisco VPN configuration interface for a 'Site to site VPN'. The interface is divided into several sections:

- Groups:** A search bar and a list of VPN Topologies. The 'My-Hub&Spoke' topology is selected and highlighted.
- Policy Types:** A list of policy types for the selected topology. The 'Preshared Key' policy type is selected and highlighted.
- VPN: My-Hub&Spoke Policy: Preshared Key:** The main configuration area, which is further divided into:
  - Key Specification:** This section contains two radio buttons: 'User Defined' (unselected) and 'Auto Generated' (selected). The 'User Defined' option has a 'Key:' text box. The 'Auto Generated' option has a 'Key Length:' text box containing the value '24'. Below this are two checkboxes: 'Same Key for All Tunnels' (unselected) and 'Regenerate Key (Only in Next Deployment)' (checked). A note below states: 'Note: This check is deselected once the key is regenerated.'
  - Negotiation Method:** This section contains a 'Main Mode Address Type' label and three radio buttons: 'Peer Address' (selected), 'Subnet(x.x.x.x/y)' (unselected), and 'Wildcard (0.0.0.0)' (unselected). The 'Subnet' option has an associated text box.

# CSM – OPERÁTOROK JOGOSULTSÁGAI



# Workflow: Setup

The screenshot displays the 'Security Manager Administration' web interface. On the left is a navigation tree with the following structure:

- System
  - Device Communication
    - General
    - Device Parameters
    - Token Management
  - Groups
  - Licensing
- Preferences
  - Config Archive
  - CSM GUI Timeout
  - Deployment
  - Discovery
  - FlexConfig
  - Logs
  - Policy
  - Policy Management
  - Workflow**
  - Application Security
  - Take Over Changes

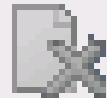
The main content area is titled 'Workflow' and contains the following sections:

- Workflow Control**
  - Enable Workflow
  - Require Activity Approval
  - Require Deployment Approval
- Default Approvers**
  - Activity Approval Email:
  - Job Approval Email:
- Workflow History**
  - Keep Activity for:  days
  - Keep Job for:  days
- Default Deployment**
  - Default Deployment Method:
  - Directory:

At the bottom of the page are three buttons: , , and .

# Workflow: New buttons

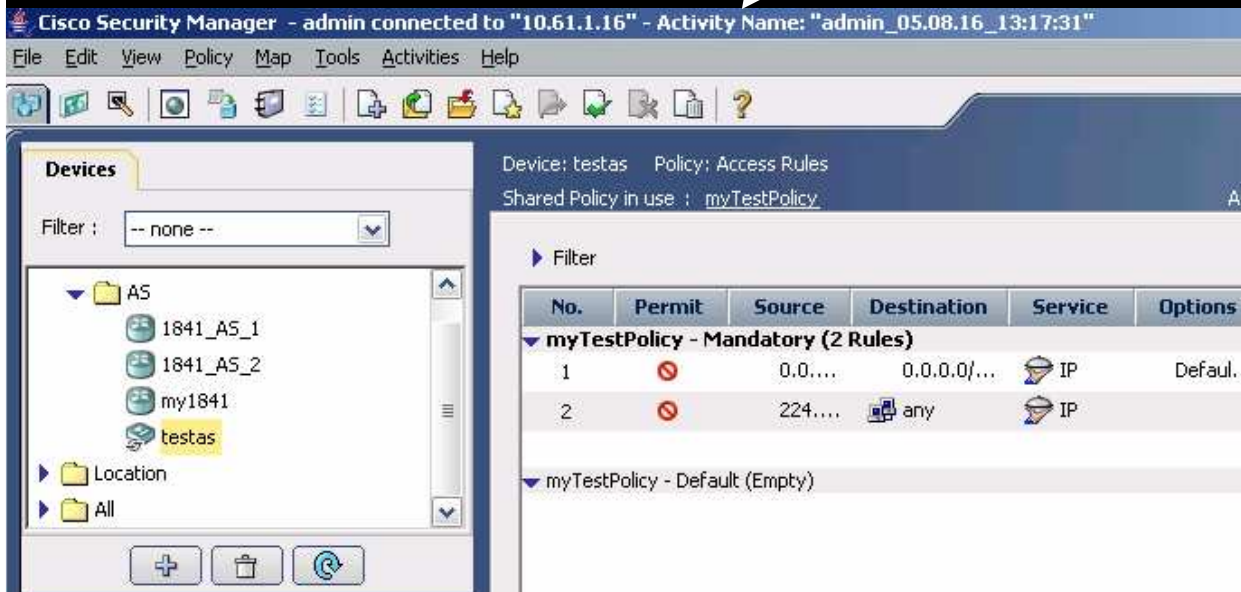
create



discard

open close validate submit approve reject

Több operátor  
együttműködése:  
Policy locking!



# Approve/Reject aktivitások az activity manager-ben

The screenshot displays the 'Activity Manager' application window. At the top, there is a table with the following columns: Activity, State, User, and Last Action. The table contains three rows of activity data. The third row is highlighted in yellow. Below the table is a row of buttons: Create, Open, Close, Validate, Submit, Approve, Reject, Discard, and Refresh. Below the buttons is a tabbed interface with 'Activity Details' selected. The 'Activity Details' section shows the following information:

Activity	State	User	Last Action
admin_05.08.16_12:53:08	Approved	admin	Activity approved
admin_05.08.16_13:17:31	Edit	admin	Activity closed
admin_05.08.19_11:10:30	Edit Open	admin	Create

**Activity Details** | Activity History

Activity ID: 4294969286  
Activity Name: admin\_05.08.19\_11:10:30  
Created: 2005-08-19 11:11:13.0  
Last Modified: 2005-08-19 11:11:13.0

Description:

Buttons: Close, Help

# RBAC -- 8 szerep – konfigurálható jogosultságok

The screenshot shows the CiscoSecure ACS web interface in Microsoft Internet Explorer. The main content area is titled "Shared Profile Components" and features a "Select" tab. Below this tab is a table of "CSM Shared Services". The table has two columns: "Name" and "Description". The roles listed are: Approver (Approver Role), CSM Security Admin (CSM Security Administrator Role), CSM Security Approver (CSM Security Approver Role), Help Desk (Help Desk Role), Network Administrator (Network Administrator Role), Network Operator (Network Operator Role), and System Administrator (System Administrator Role). At the bottom of the table are "Add" and "Cancel" buttons. To the right of the table is a "Help" panel with a list of links: "Command Authorization Sets", "Adding a Command Authorization Set", "Editing a Command Authorization Set", and "Deleting a Command Authorization Set". Below the links is a section titled "Command Authorization Sets" with a paragraph explaining that these sets are configurable authorization rules for commands issued during device-hosted sessions or during use of a device-management application, such as Management Center for PIX Firewalls. It also states that if devices support command authorization, TACACS+ AAA clients can be configured to defer to Cisco Secure ACS for authorization of commands issued by a user accessing that device by a shell session.

Name	Description
<a href="#">Approver</a>	Approver Role
<a href="#">CSM Security Admin</a>	CSM Security Administrator Role
<a href="#">CSM Security Approver</a>	CSM Security Approver Role
<a href="#">Help Desk</a>	Help Desk Role
<a href="#">Network Administrator</a>	Network Administrator Role
<a href="#">Network Operator</a>	Network Operator Role
<a href="#">System Administrator</a>	System Administrator Role

- [Command Authorization Sets](#)
- [Adding a Command Authorization Set](#)
- [Editing a Command Authorization Set](#)
- [Deleting a Command Authorization Set](#)

**Command Authorization Sets**

Command authorization sets are configurable sets of authorization rules for commands issued during device-hosted sessions or during use of a device-management application, such as Management Center for PIX Firewalls.

If they support command authorization, TACACS+ AAA clients can be configured to defer to Cisco Secure ACS for authorization of commands issued by a user accessing that device by a shell session. Once you have created a command authorization set, you can use it by configuring the TACACS+ settings for the user or group to which you want to apply the command authorization set. For

# RBAC -- 8 szerep – konfigurálható jogosultságok

The screenshot shows the CiscoSecure ACS web interface in Microsoft Internet Explorer. The browser address bar shows `http://10.77.210.59:4652/index2.htm`. The page title is "Shared Profile Components". On the left, there is a navigation menu with icons for User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled "Edit" and shows the configuration for a role named "System Administrator". The "Description" is "System Administrator Role". Below this, there is a tree view of permissions under "CSM Shared Services". The tree view shows the following permissions checked:

- CSM Shared Services
  - View
    - Policies
    - Objects
    - Config Archive
      - Devices
      - CLI
      - Admin
      - Topology
  - Modify
  - Approve
  - Import
  - Deploy
  - Control

At the bottom of the configuration area, there are buttons for "Submit", "Delete", "Copy to Clipboard", and "Cancel".

## Logging in Using the ACS Login Module

The Login Module determines the type of authentication and authorization Common Services uses. By default, the login module is set to local authentication and authorization. You can change this default value to use Cisco Secure ACS for user authentication and authorization.

When you change login module to ACS ensure that:

- The CiscoWorks Server is added as an AAA client in the ACS server.

For the first time, it can be done by going to Network Configuration in ACS server and adding the host (with IP Address). The secret key should be configured there. The same secret key should be entered in the Login Module dialog box.

- The username you enter while logging in to CiscoWorks is a valid ACS user name.

In ACS mode, authentication takes place from the ACS server.

# ÖSSZEFOGLALÁS



# Összefoglalás

## A Cisco Security Manager segít ...

- **A feladatokat gyorsabban lehet végrehajtani :**

A szabály tábla sok szolgáltatást nyújt

Policy megosztás: konfiguráljunk 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



# CISCO SYSTEMS

