

# Biztonság és vezeték nélküli hálózat?



**Turi János**

**Mérnök tanácsadó**

**Cisco Systems Magyarország Kft.**

**[jturi@cisco.com](mailto:jturi@cisco.com)**

# Amiről szó lesz - tervezés

## Mi az a CVD?

- Hogyan készül
- Mire használjuk

## Vezeték nélküli hálózat integrált biztonsági megoldásokkal

- Cisco Unified Wireless Network
- Cisco Security Agent
- Cisco NAC Appliance
- Cisco Firewall
- Cisco IPS

## A biztonság egy kicsit más szemszögből

# Cisco Validated Design (CVD)

[http://www.cisco.com/en/US/netsol/ns741/networking\\_solutions\\_program\\_home.html](http://www.cisco.com/en/US/netsol/ns741/networking_solutions_program_home.html)

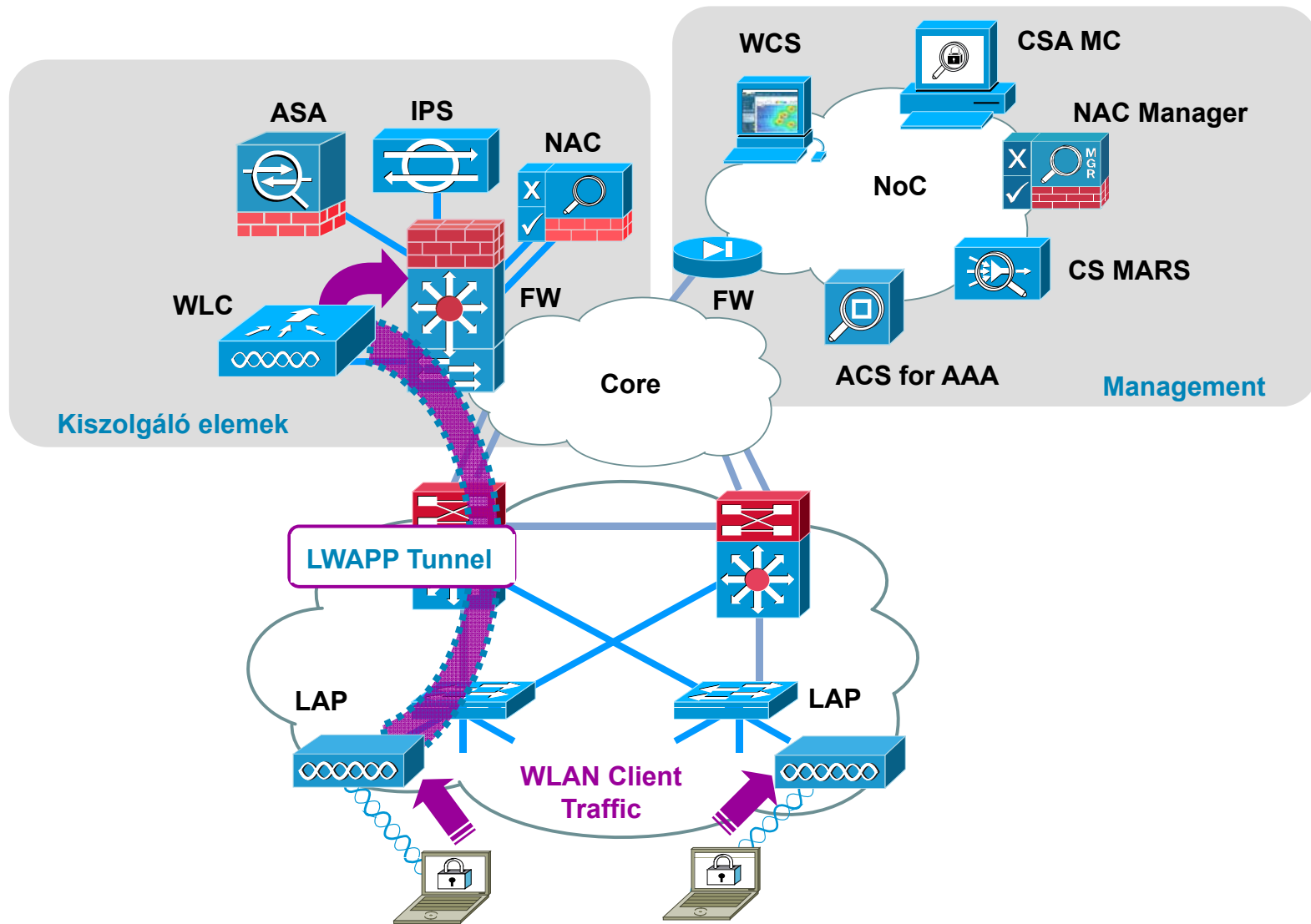
*Wireless and Network Security Integration Design Guide*

- Bárki számára hozzáférhető ajánlások
- Nem mindenre találuk benne megoldást – igyekszünk fejleszteni
- Cisco mérnökök által kipróbált megoldások – nincs zsákbamacska
  
- Követéséhez nem kell minden eszközzel rendelkezünk, elég ha elindulunk az úton. Így legalább látjuk, hol a vége

# Cisco Unified Wireless Network



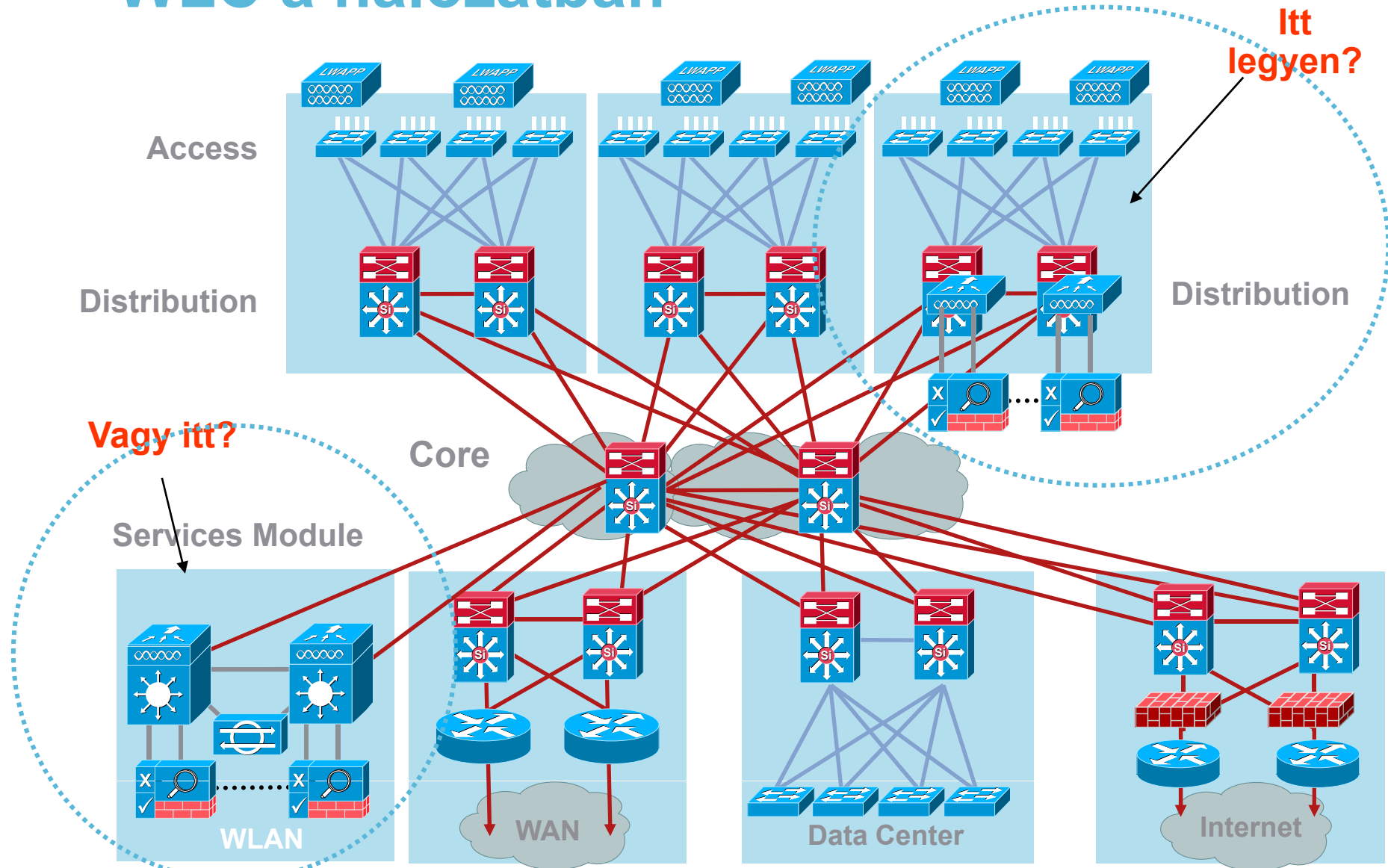
# Architektúrális megközelítés



# Wireless elemek

Cél	WLAN elemek	Hálózati elemek
Hálózati infrastruktúra megerősítése	LWAPP/CAPWAPP, Management Frame Protection, 802.1x	Megerősített hálózati elemek (redundancia)
Végpontok védelme	WPA2 nagyon ajánlott	CSA és Cisco Secure Service Client
Felhasználói azonosítás és hozzáférés szabályozása	WPA2, Client Exclusion a WLC-n	CSA, CSSC, NAC, Tűzfal
Titkosított kommunikáció	WPA2	
Hozzáférés szabályozás	ACL a WLC-n	Cisco Tűzfal
<b>Működtetés</b>		
Hálózat monitorozása, anomáliák és támadások detektálása	WLC, Wireless Control System, Adaptive wireless IPS	AAA, SNMP, Eszköz menedzsment és CS-MARS

# WLC a hálózatban

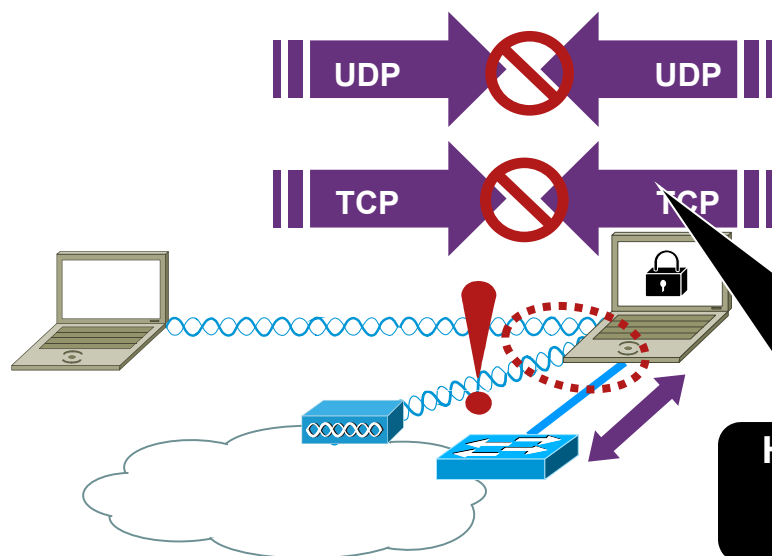


# Cisco Security Agent - CSA

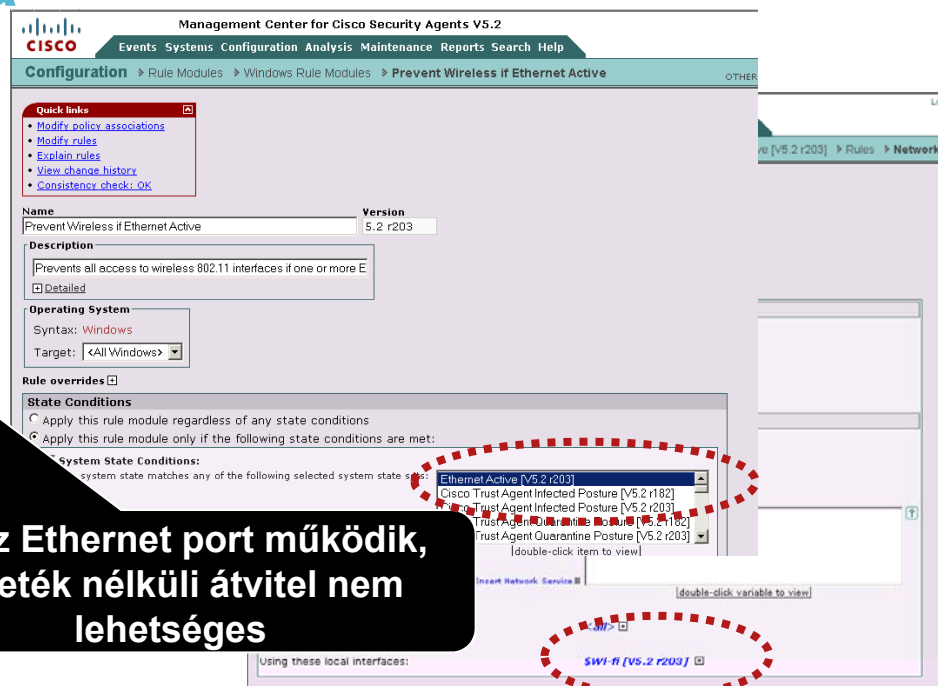




# CSA vezetékes és vezeték nélküli hálózat együttes használatára

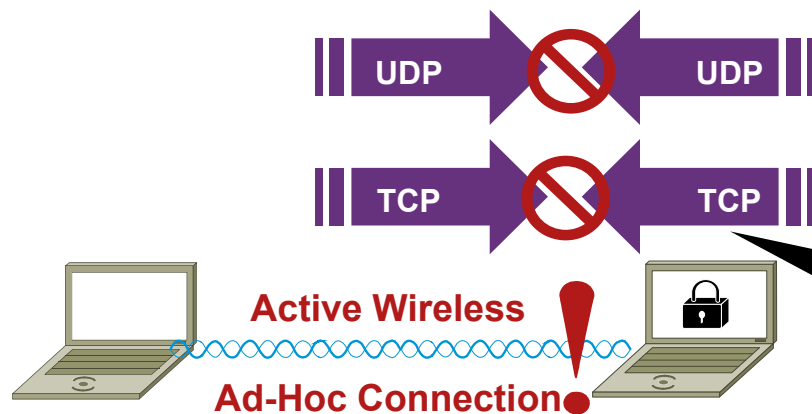


**Ha az Ethernet port működik, vezeték nélküli átvitel nem lehetséges**

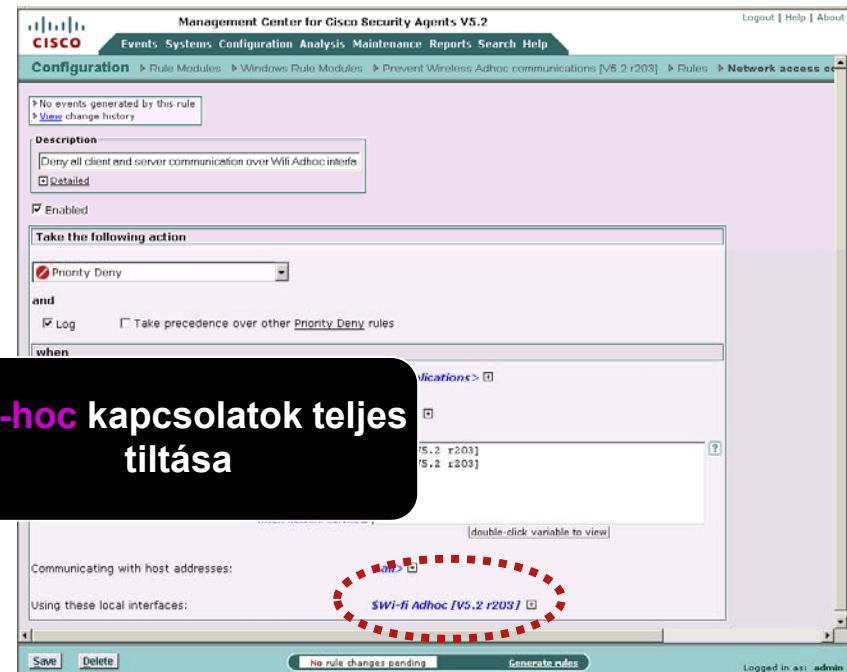


- Több egyidejű hálózati kapcsolat (vezetékes és vezeték nélküli) tiltására 5.2-es CSA verziótól
- Cisco Secure Service Client használatával is elérhető ugyanez

# CSA Ad-Hoc kapcsolatok megakadályozása



Ad-hoc kapcsolatok teljes tiltása



- Csak engedélyezett hozzáférések legyenek a belső hálózathoz
  - Egyidőben a hálózat oldaláról is érdemes figyelni ezekre a kapcsolatokra
- Wireless IDS/IPS szolgáltatás

# NAC Appliance és Tűzfal

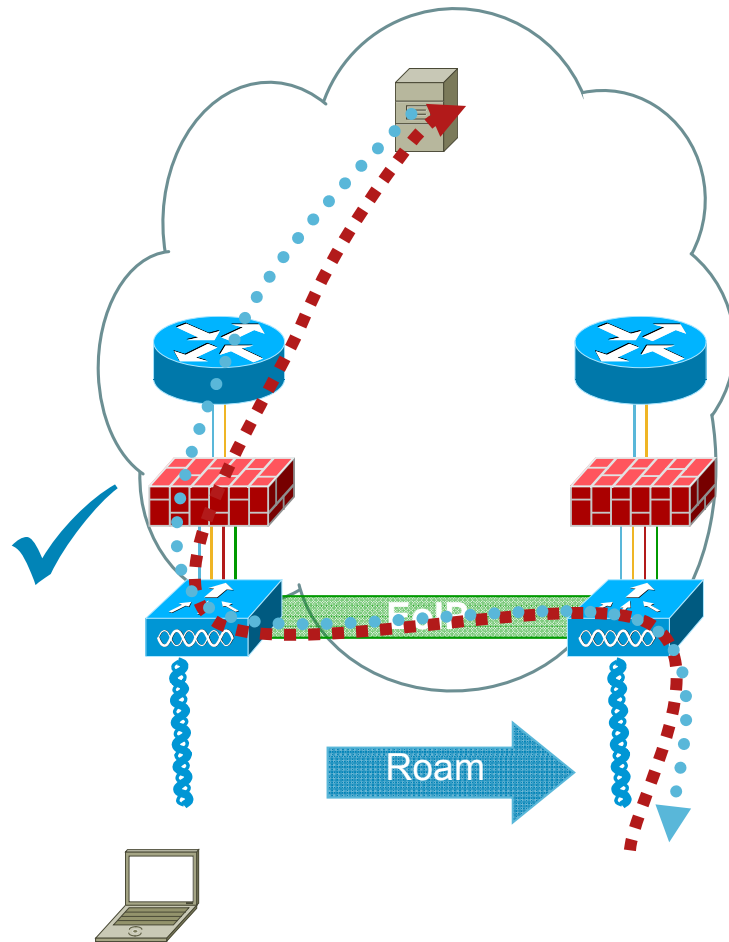


# NAC: Négy fő funkció

Használatával a hálózat kényszerítheti ki, hogy a felhasználók megfeleljenek a feltételeknek



# Tűzfal és Roaming

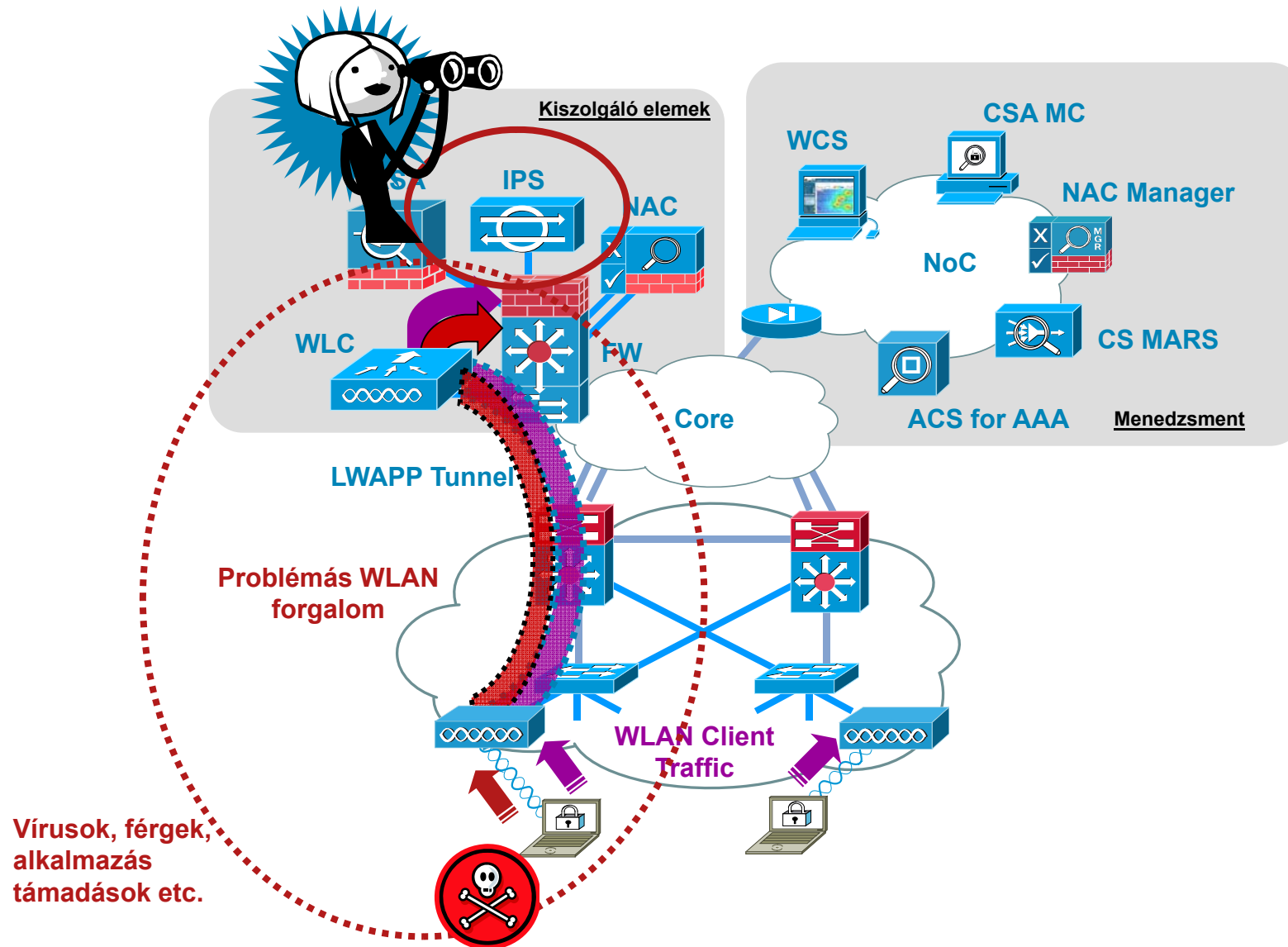


- A kliens kezdeményezi
- A forgalom ezután egy tunnelben halad az új és a régi WLC között
- A forgalom ugyanazon a tűzfalon halad keresztül

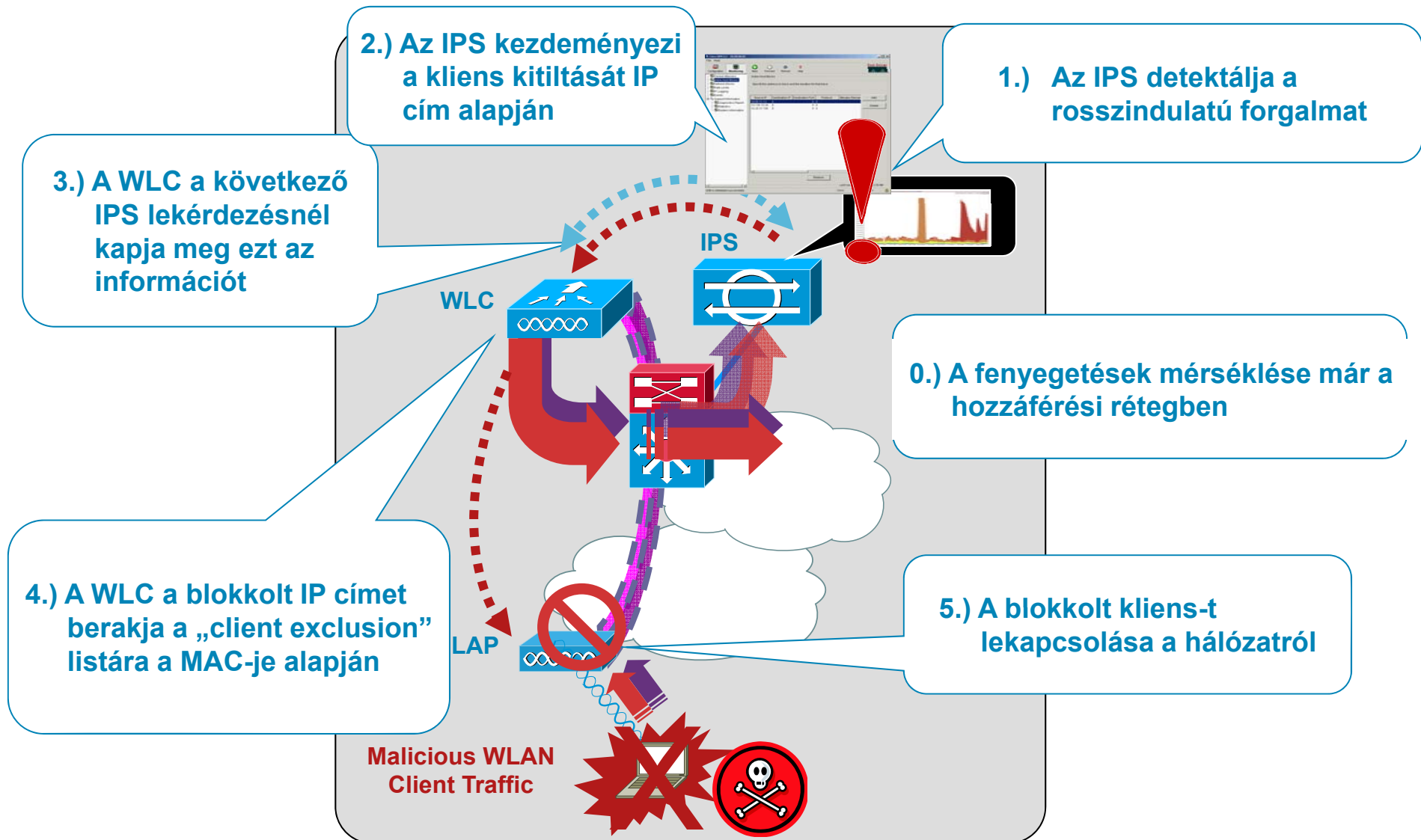
# Cisco IPS



# Cisco IPS elhelyezkedése a hálózatban



# Cisco WLC and IPS Integration for Automated Threat Mitigation





# Biztonság – kicsit más szemszögből is



Cisco Spectrum Expert - WCS Compatible - Playing: Instant Replay

File View Tools Help Thu Apr 16 12:49:40 871 KB

Active Devices Spectrum Spectrum [2] Devices Channel Summary

Bluetooth [1]  
Bluetooth Paging/Inquiry Device(s)

Wi-Fi Ad Hoc(s) [1]  
WIRELESS (Ch 11)

Wi-Fi APs (In-Network) [3]  
(00:17:DF:A3:D9:91) (Ch 36)  
SZTE-KONF (Ch 1)  
SZTE-KONF (Ch 6)

Control Panel

Tree View  
List View

Devices Historic Range:  
Last 10 Minutes

Channel Selection:  
All Channels

Devices: Last 10 Minutes, All Channels

Device	Signal Strength (dBm)	Duty Cycle (%)	Discovery Time	On Time	Channels Affected	Network ID	D
Bluetooth [5]							
Bluetooth Paging/Inquiry Device(s)	-59.5		Thu Apr 16 12:49...	00:00:30	N/A	21:06:8B	
Bluetooth Paging/Inquiry Device(s)	-66.3		Thu Apr 16 12:42...	00:02:45 (Down)	N/A	F8:22:C1	
Bluetooth Paging/Inquiry Device(s)	-63.2		Thu Apr 16 12:38...	00:02:09 (Down)	N/A	F8:22:C1	
Piconet 39 [1]							
Device 1	-76.7	1	Thu Apr 16 12:38...	00:01:44 (Down)	3..14	DE:B2:F2	
Piconet 40 [1]							
Device 1	-73.2	1	Thu Apr 16 12:42...	00:00:30 (Down)	7..10	DE:B2:F2	
Wi-Fi Ad Hoc(s) [1]							
WIRELESS (Ch 11)	-89.0		Thu Apr 16 12:09...	00:40:00	8..13	02:1D:E0:03:FE:29	02:1D:
Wi-Fi APs (In-Network) [63]							
(00:17:DF:A3:D9:91) (Ch 36)	-51.0		Thu Apr 16 12:47...	00:02:00	34..38	00:17:DF:A3:D9:91	00:17:
SZTE-KONF (Ch 1)	-61.0		Thu Apr 16 12:48...	00:00:30	1..4	00:40:96:A4:97:7E	00:40:
SZTE-KONF (Ch 1)	-59.0		Thu Apr 16 12:48...	00:00:10 (Down)	1..4	00:40:96:A4:97:7E	00:40:
SZTE-KONF (Ch 1)	-62.0		Thu Apr 16 12:48...	00:00:09 (Down)	1..4	00:40:96:A4:97:7E	00:40:
SZTE-KONF (Ch 1)	-60.0		Thu Apr 16 12:48...	00:00:10 (Down)	1..4	00:40:96:A4:97:7E	00:40:
SZTE-KONF (Ch 1)	-63.0		Thu Apr 16 12:48...	00:00:09 (Down)	1..4	00:40:96:A4:97:7E	00:40:
SZTE-KONF (Ch 1)	-62.0		Thu Apr 16 12:48...	00:00:09 (Down)	1..4	00:40:96:A4:97:7E	00:40:
SZTE-KONF (Ch 1)	-62.0		Thu Apr 16 12:47...	00:00:10 (Down)	1..4	00:40:96:A4:97:7E	00:40:
SZTE-KONF (Ch 1)	-61.0		Thu Apr 16 12:47...	00:00:09 (Down)	1..4	00:40:96:A4:97:7E	00:40:
SZTE-KONF (Ch 1)	-61.0		Thu Apr 16 12:47...	00:00:09 (Down)	1..4	00:40:96:A4:97:7E	00:40:
SZTE-KONF (Ch 1)	-61.0		Thu Apr 16 12:47...	00:00:10 (Down)	1..4	00:40:96:A4:97:7E	00:40:
SZTE-KONF (Ch 1)	-62.0		Thu Apr 16 12:47...	00:00:09 (Down)	1..4	00:40:96:A4:97:7E	00:40:
SZTE-KONF (Ch 1)	-63.0		Thu Apr 16 12:47...	00:00:09 (Down)	1..4	00:40:96:A4:97:7E	00:40:
SZTE-KONF (Ch 1)	-64.0		Thu Apr 16 12:47...	00:00:10 (Down)	1..4	00:40:96:A4:97:7E	00:40:
SZTE-KONF (Ch 1)	-60.0		Thu Apr 16 12:46...	00:00:09 (Down)	1..4	00:40:96:A4:97:7E	00:40:
SZTE-KONF (Ch 1)	-61.0		Thu Apr 16 12:46...	00:00:10 (Down)	1..4	00:40:96:A4:97:7E	00:40:
SZTE-KONF (Ch 1)	-61.0		Thu Apr 16 12:46...	00:00:09 (Down)	1..4	00:40:96:A4:97:7E	00:40:
SZTE-KONF (Ch 1)	-62.0		Thu Apr 16 12:46...	00:00:09 (Down)	1..4	00:40:96:A4:97:7E	00:40:
SZTE-KONF (Ch 1)	-61.0		Thu Apr 16 12:46...	00:00:10 (Down)	1..4	00:40:96:A4:97:7E	00:40:
SZTE-KONF (Ch 1)	-62.0		Thu Apr 16 12:46...	00:00:09 (Down)	1..4	00:40:96:A4:97:7E	00:40:
SZTE-KONF (Ch 1)	-62.0		Thu Apr 16 12:45...	00:00:09 (Down)	1..4	00:40:96:A4:97:7E	00:40:
SZTE-KONF (Ch 1)	-64.0		Thu Apr 16 12:45...	00:00:10 (Down)	1..4	00:40:96:A4:97:7E	00:40:
SZTE-KONF (Ch 1)	-64.0		Thu Apr 16 12:45...	00:00:09 (Down)	1..4	00:40:96:A4:97:7E	00:40:
SZTE-KONF (Ch 1)	-63.0		Thu Apr 16 12:45...	00:00:10 (Down)	1..4	00:40:96:A4:97:7E	00:40:
SZTE-KONF (Ch 1)	-64.0		Thu Apr 16 12:45...	00:00:09 (Down)	1..4	00:40:96:A4:97:7E	00:40:
SZTE-KONF (Ch 1)	-63.0		Thu Apr 16 12:45...	00:00:09 (Down)	1..4	00:40:96:A4:97:7E	00:40:
SZTE-KONF (Ch 1)	-63.0		Thu Apr 16 12:44...	00:00:10 (Down)	1..4	00:40:96:A4:97:7E	00:40:

For Help, press F1

Monitored: 2.40-2.50, 5.15-5.35, 5.47-5.72 Playing External Antenna UpTime: 3 Hours, 15 Mins Wi-Fi

Start 4 W... 2 In... 2 Mi... Reszl... GIB s... Cisco... Inbox... NetBr... 68% 12:51

# Kérdések



