Biztonság és vezeték nélküli hálózat?

Turi János

Mérnök tanácsadó
Cisco Systems Magyarország Kft.
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)

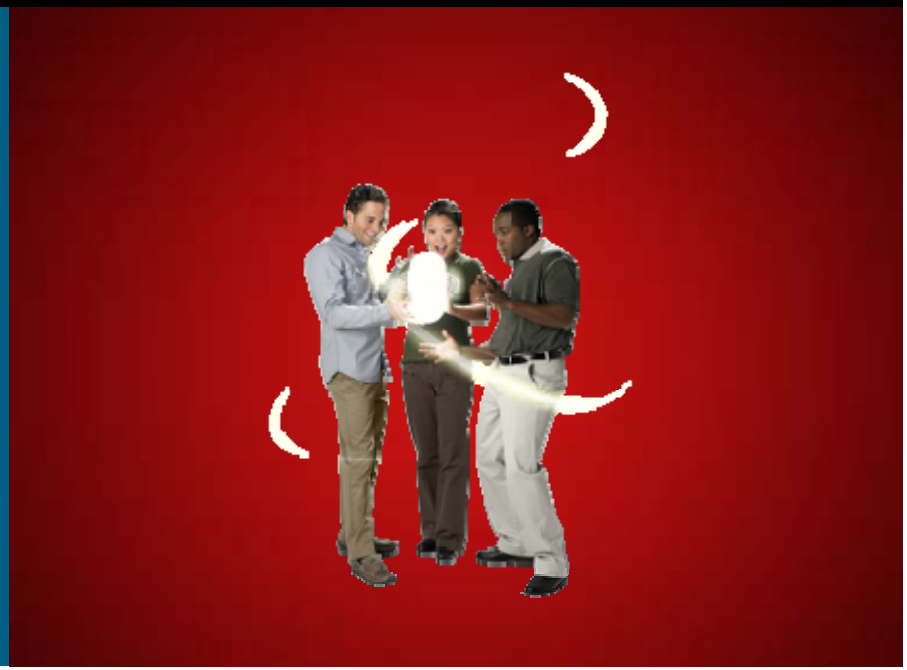
http://www.cisco.com/en/US/netsol/ns741/networking_solutions_program_home.html

Wireless and Network Security Integration Design Guide

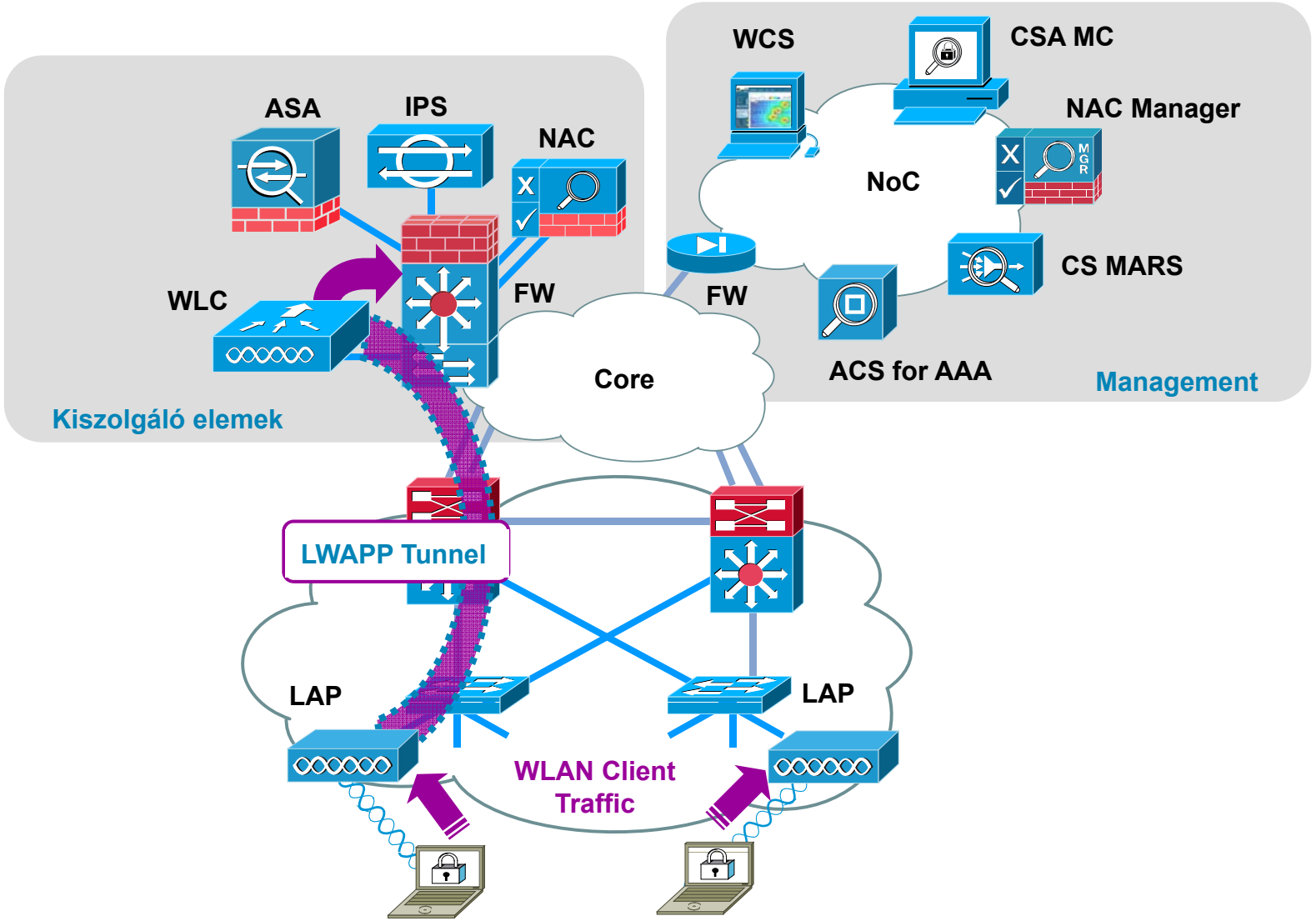
- Bárki számára hozzáférhető ajánlások
- Nem mindenre találuk benne megoldást – igyekszünk fejleszteni
- Cisco mérnökök által kipróbált megoldások – nincs zsákbamacska

- Követéséhez nem kell minden eszközzel rendelkeznünk, elég ha elindulunk az úton. Így legalább látjuk, hol a vége

Cisco Unified Wireless Network



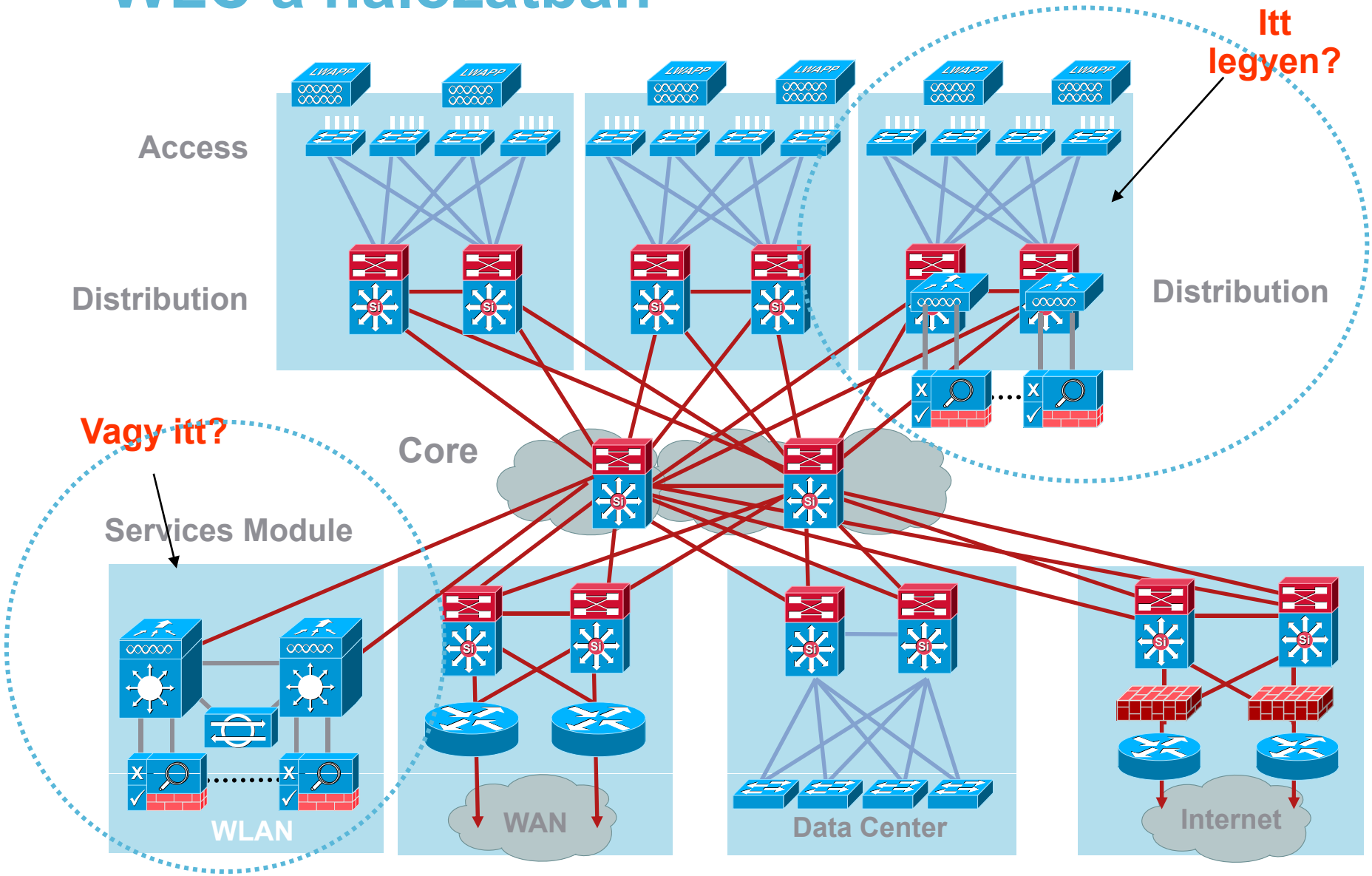
Architektúrális megközelítés



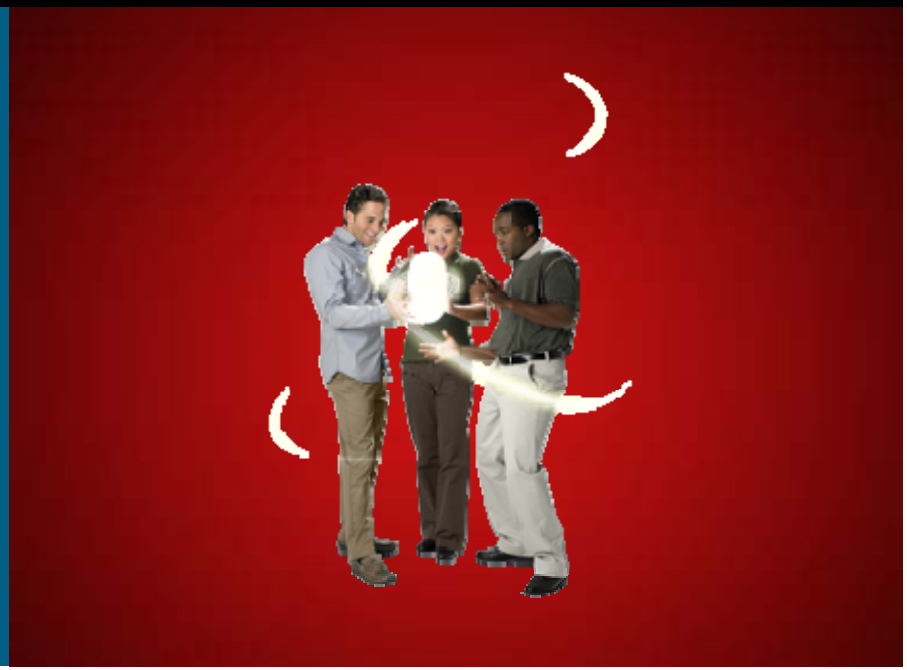
Wireless elemek

Cél	WLAN elemek	Hálózati elemek
Hálózati infrastuktúra 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
Működtetés		
Hálózat monitorozása, anomáliák és támadások detektálása	WLC, Wireless Control System, Adaptive wireless IPS	AAA, SNMP, Eszköz menedzsment és CS-MARS

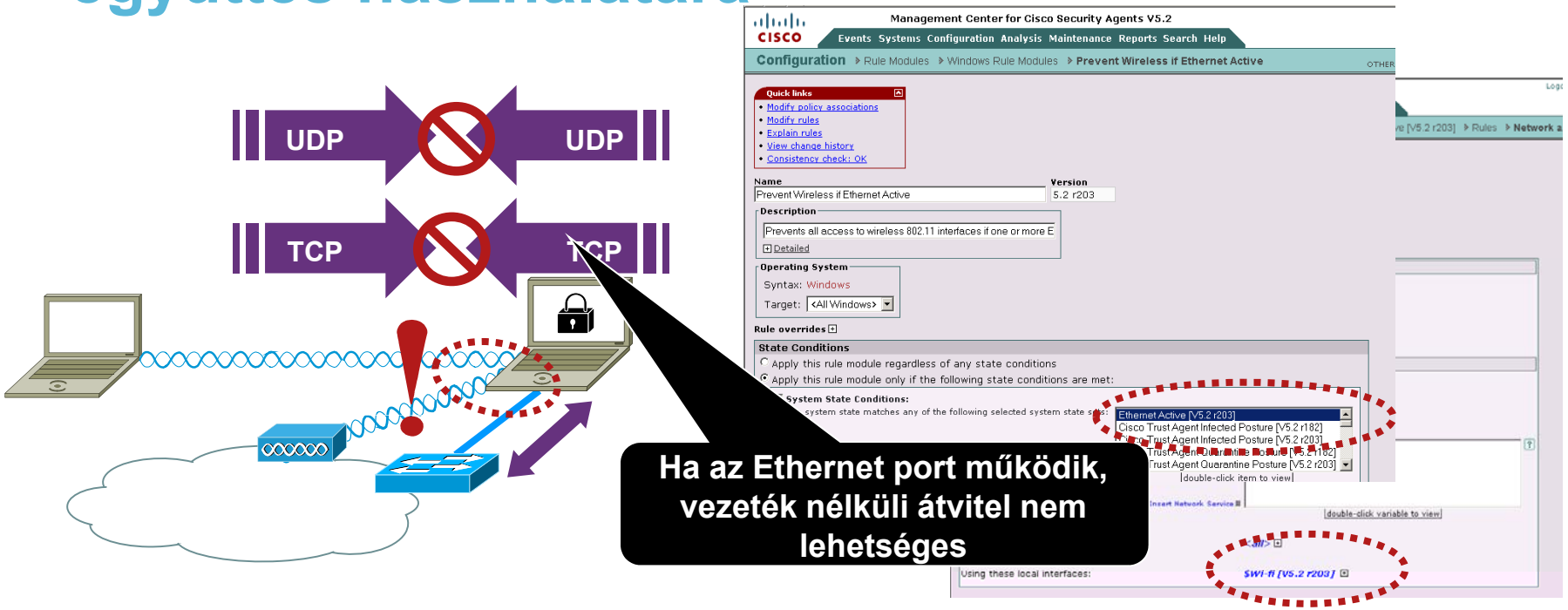
WLC a hálózatban



Cisco Security Agent - CSA

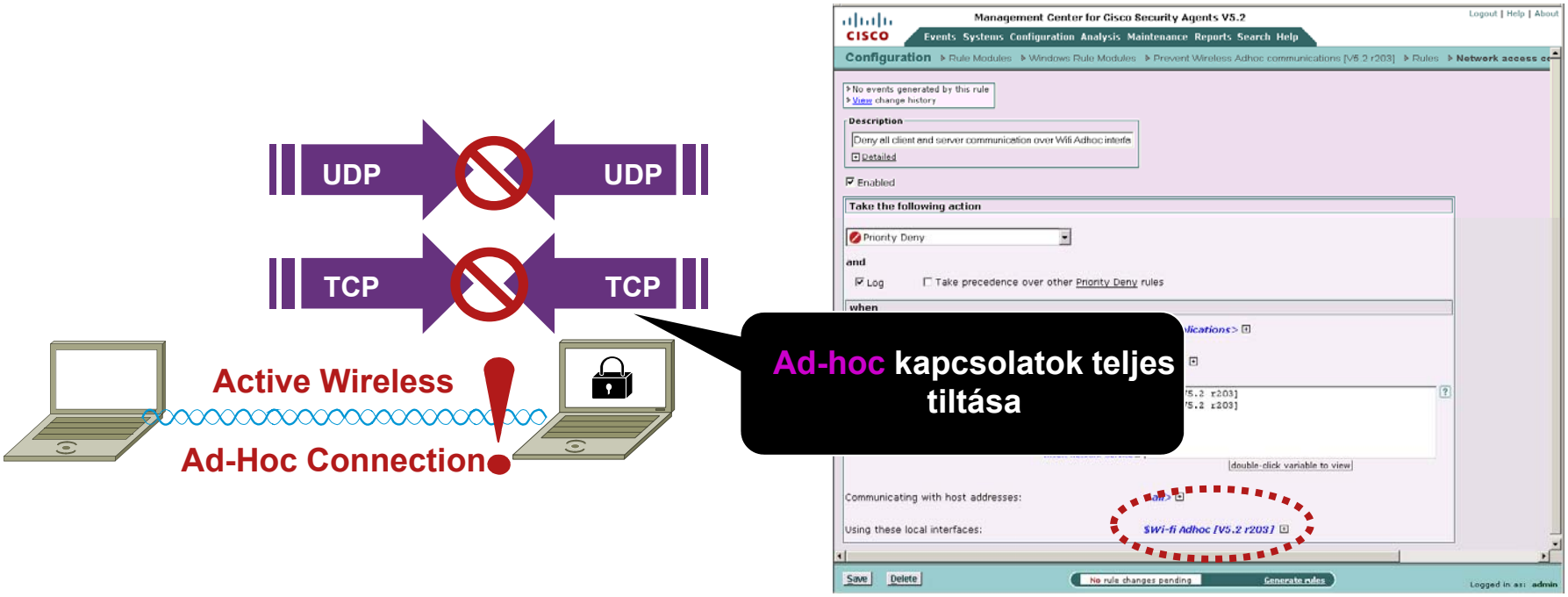


CSA vezetékes és vezeték nélküli hálózat együttes használatára



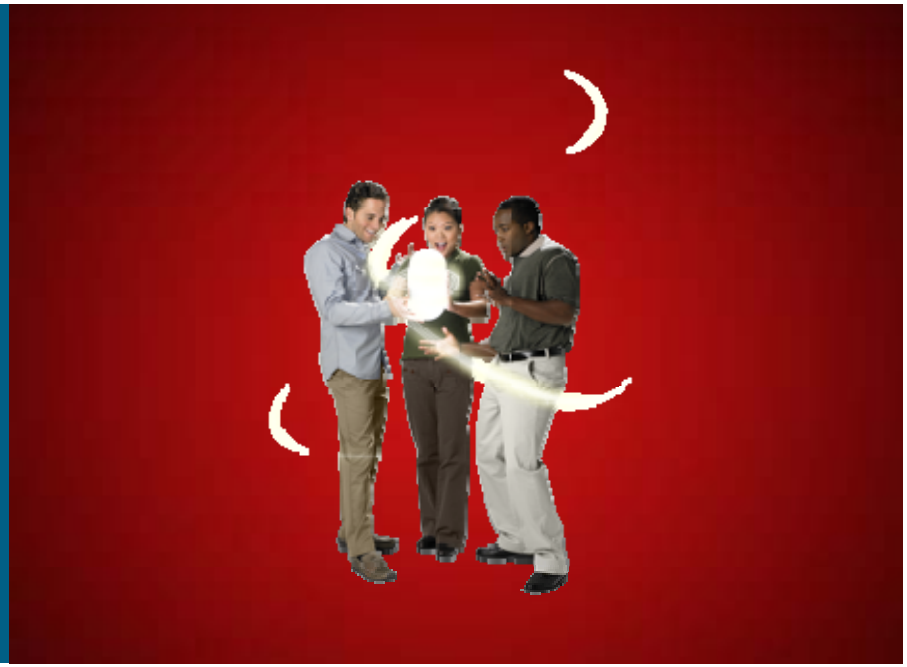
- Több egyidejű hálózati kapcsolat (vezetékes és vezeték nélküli) tiltására 5.2-es CSA verziótól
- Cisco Secure Service Client használatával is elérhető ugyanez

CSA Ad-Hoc kapcsolatok megakadályozása



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

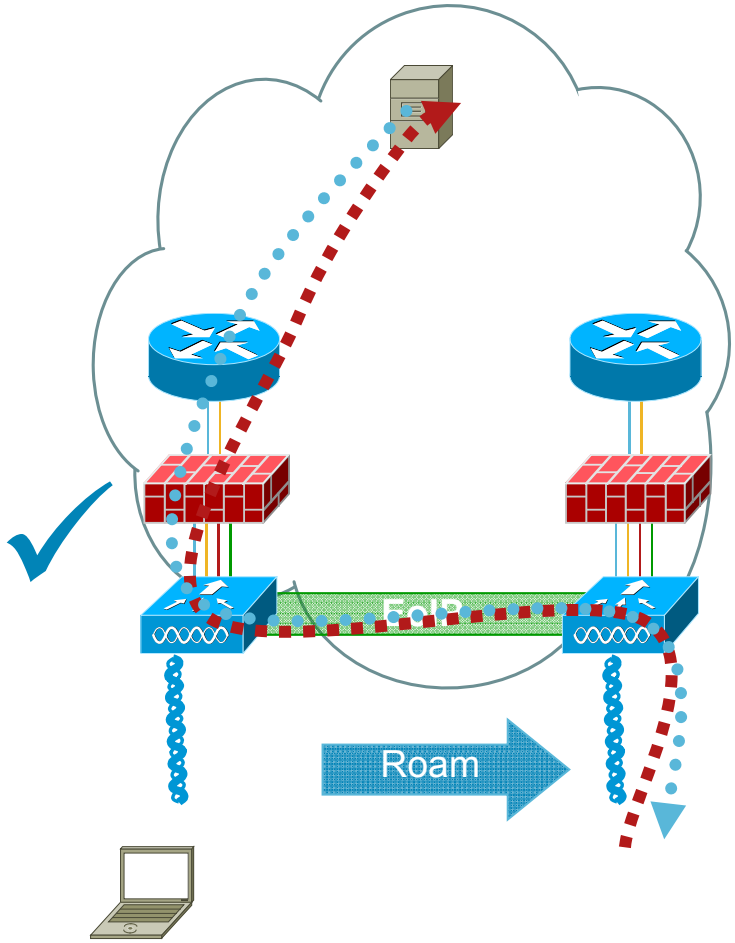
NAC Appliance és Tűzfal



NAC: Négy fő funkció

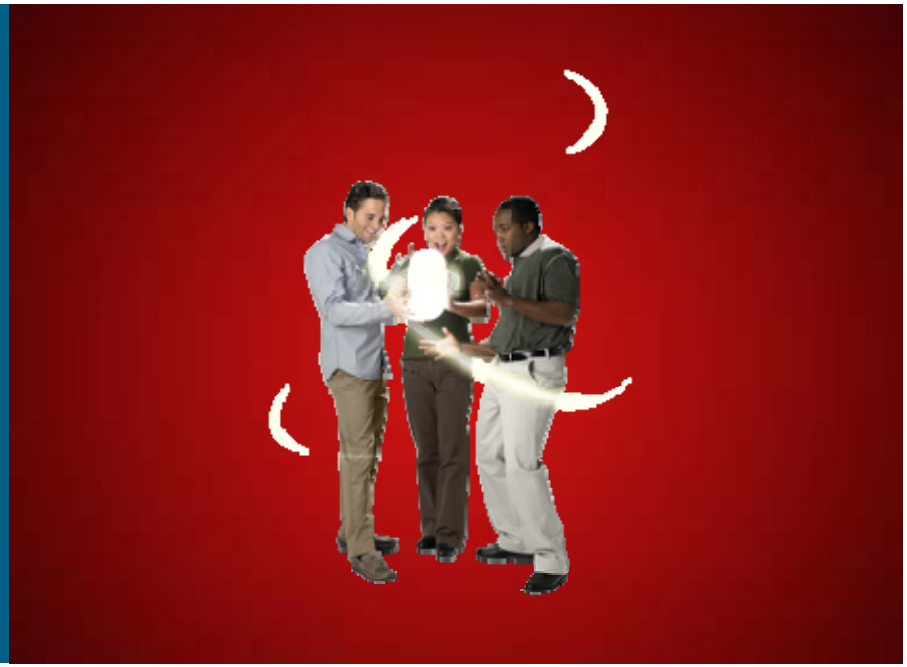
Használatával a hálózat kényszerítheti ki, hogy a felhasználók megfeleljenek a feltételeknek

Tűzfal és Roaming

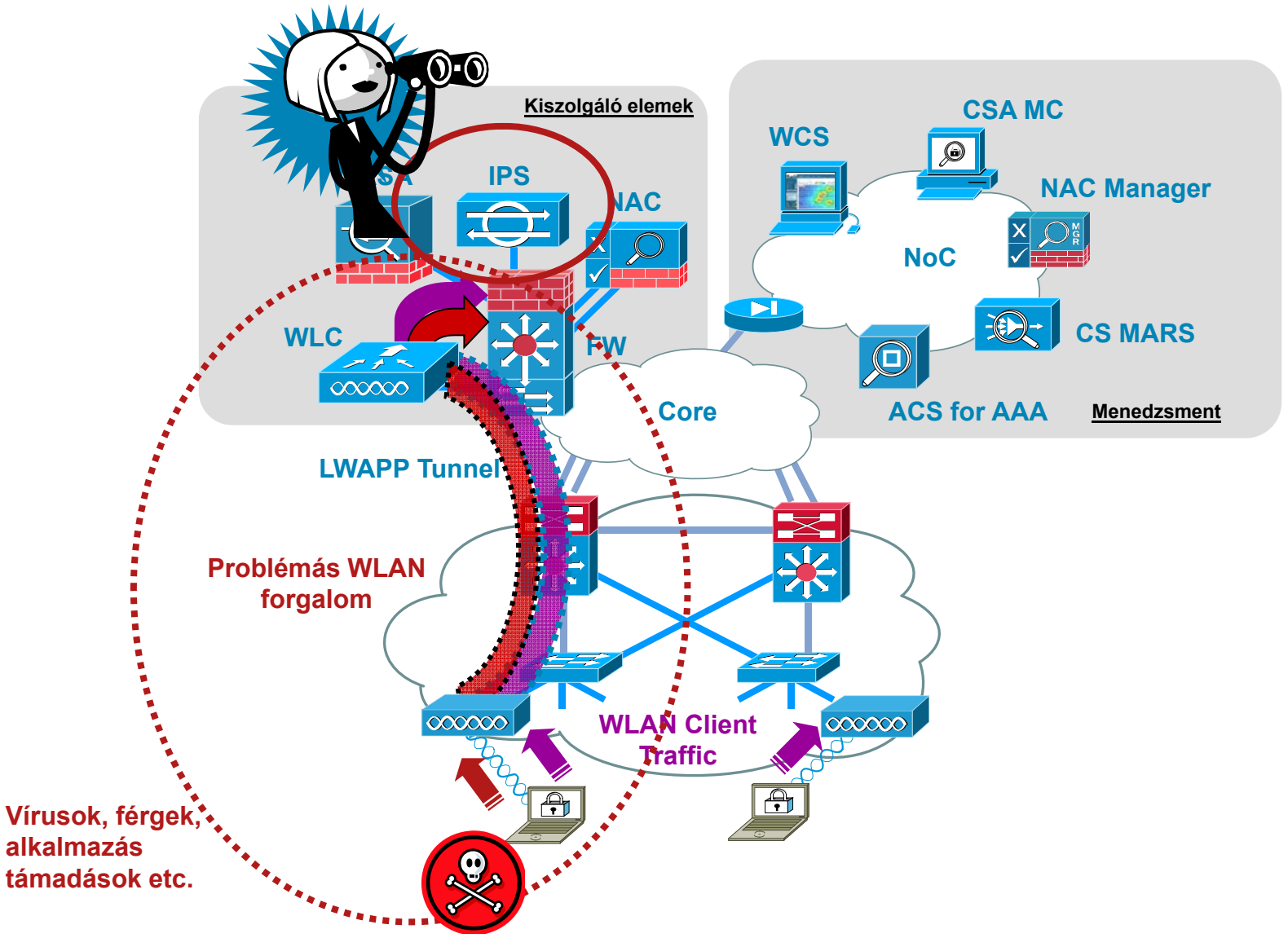


- A kliens kezdeményezi
- A forgalom ezután egy tunnel-ben halad az új és a régi WLC között
- A forgalom ugyazanon a tűzfalon halad keresztül

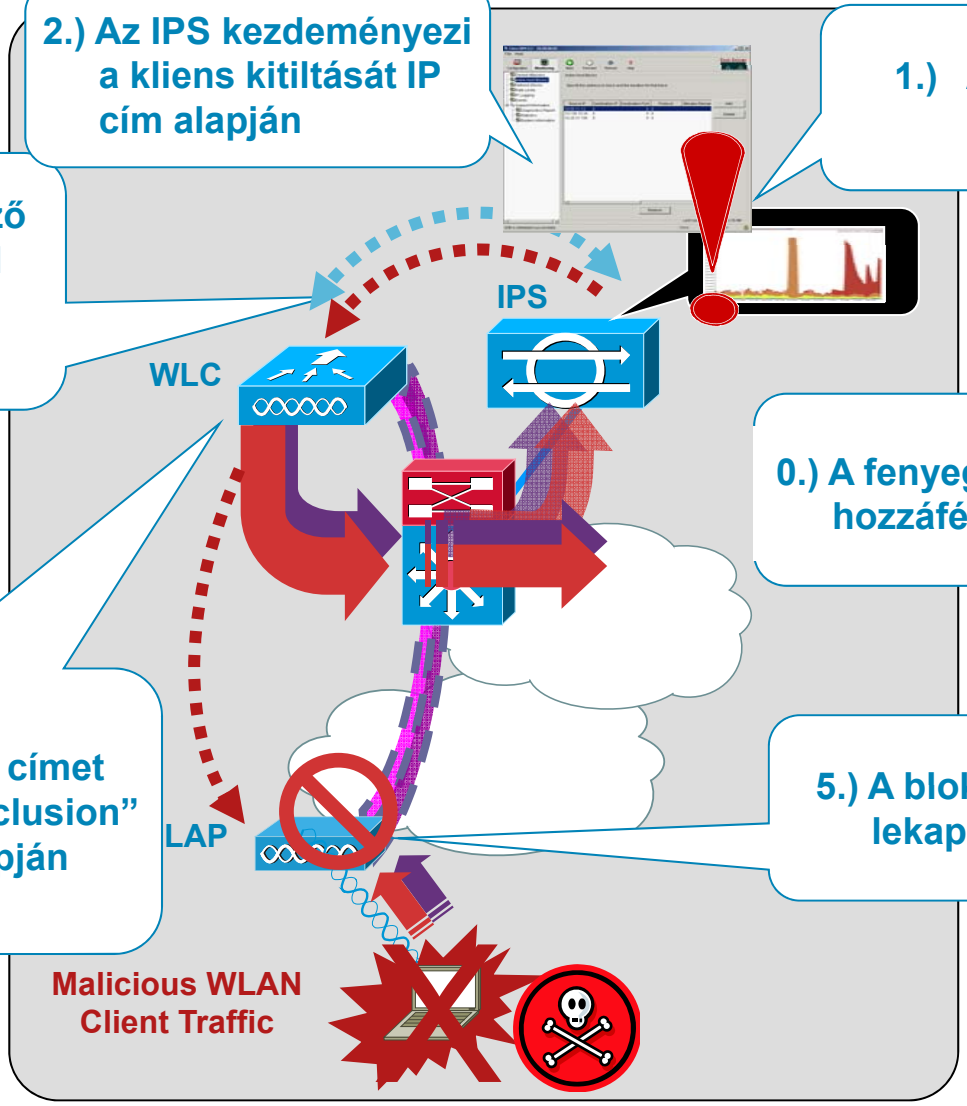
Cisco IPS



Cisco IPS elhelyezkedése a hálózatban



Cisco WLC and IPS Integration for Automated Threat Mitigation



2.) Az IPS kezdeményezi a kliens kitiltását IP cím alapján

1.) Az IPS detektálja a rosszindulatú forgalmat

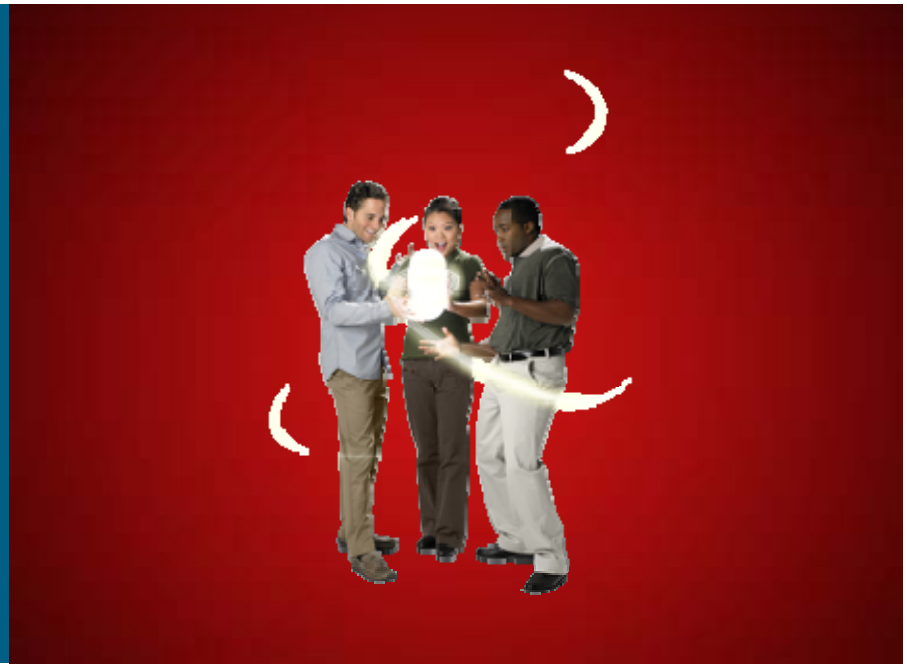
3.) A WLC a következő IPS lekérdezésnél kapja meg ezt az információt

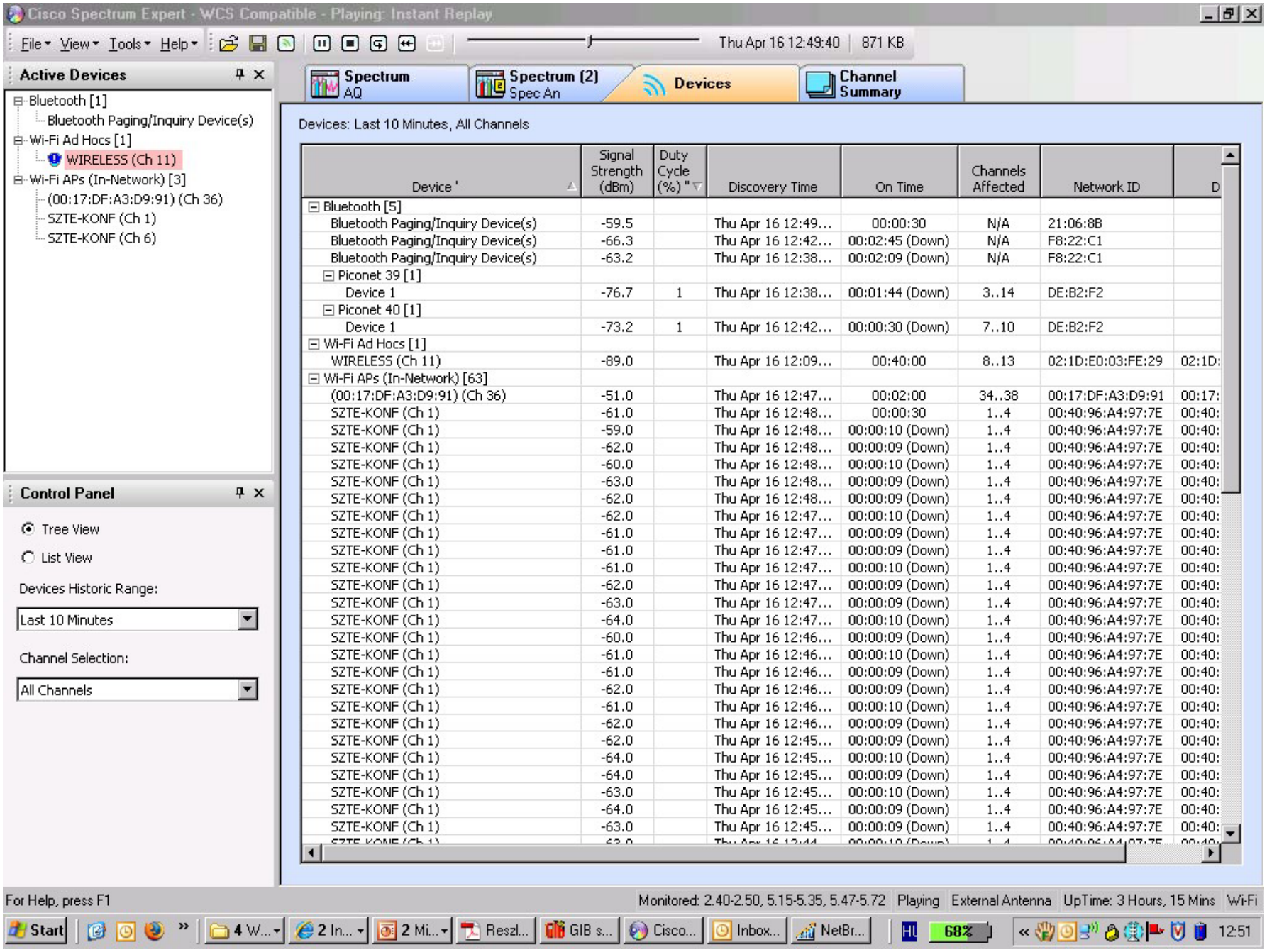
0.) A fenyegetések mérséklése már a hozzáférési rétegben

4.) A WLC a blokkolt IP címet berakja a „client exclusion” listára a MAC-je alapján

5.) A blokkolt kliens-t lekapcsolása a hálózatról

Biztonság – kicsit más szemszögből is





Kérdések