KOCSIS TAMÁS
(biztributor):

Mitől vállalati a Wi-Fi biztonsága?

Biztonságos?

A vállalati Wi-Fi biztonsági vektorai

- ✓ Titkosítás
- ✓ Hitelesítés
- ✓ Forgalomszabályozás
- ✓ Átláthatóság
- ✓ Önvédelem

A vállalati Wi-Fi biztonsági vektorai - titkosítás

- **Titkosítás**
  - Nyitott közeghozzáférés (L1)
  - A csomagok hitelességének, sértetlenségének, bizalmasságának garantálása
  - WPA2-AES (CCMP)
  - A legtöbb eszköz tudja, WPA2-Personal/WPA2-Enterprise
  - **Nem a titkosításon van a hangsúly!**

A vállalati Wi-Fi biztonsági vektorai - hitelesítés

- **Hitelesítés**
  - **A PSK nem hitelesítés!**
  - Elvárt a WPA2-Enterprise, 802.1x hitelesítés
  - EAP-PEAP vs EAP-TLS
    - EAP-PEAP elterjedtebb, de sérülékenyebb (MSCHAP v2)
    - EAP-TLS jelenti az igazi biztonságot!
      - Gépen tárolt tanúsítványok,
      - Smartcardon tárolt tanúsítványok

○	tkocsis	00:f4:b9:5d:1e:dd	10.0.0.111	rap-users	802.1x	biztributor-corporate	andris-rap
○	dnemes	a8:16:b2:ff:b2:47	10.0.0.53	rap-users	802.1x	biztributor-corporate	dnemes-rap

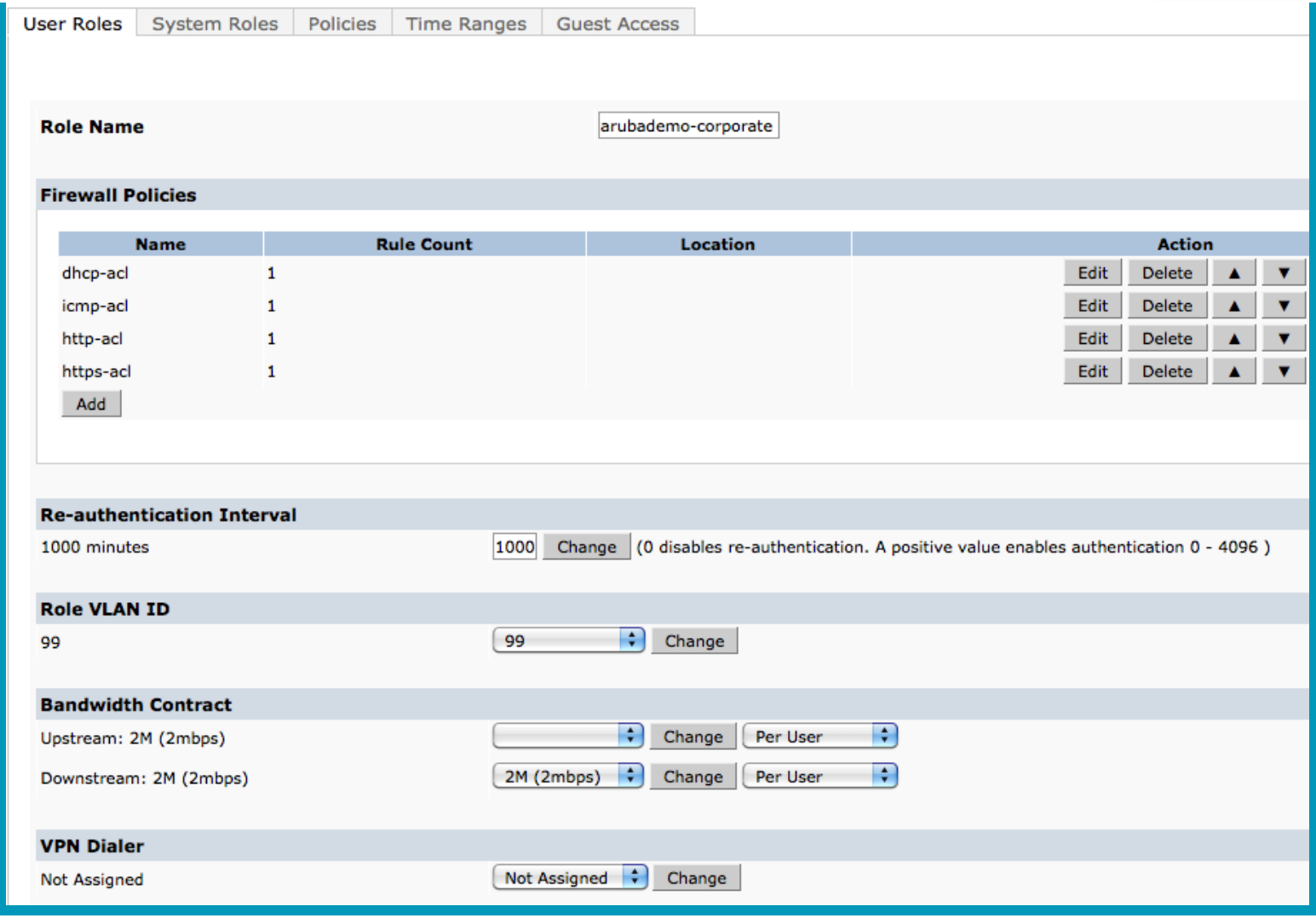
A vállalati Wi-Fi biztonsági vektorai - forgalomszabályozás

- ✓ **Forgalomszabályozás (ki, honnan, hova, mivel?)**
  - ✓ Felhasználó-alapú
  - ✓ Wireless firewall
    - ✓ L2-L7 védelem
    - ✓ Csomagirányítás
    - ✓ Forgalomszabályozás
    - ✓ QoS
    - ✓ Priorizálások

Példa a forgalomszabályozásra – I.

	IPv4	IPv6
Monitor Ping Attack (per sec)		
Monitor TCP SYN Attack rate (per sec)		
Monitor IP Session Attack (per sec)		
Monitor/Police CP Attack rate (per sec)		
Deny Inter User Bridging	☑	☑
Deny Inter User Traffic	☐	
Deny All IP Fragments	☐	☐
Enforce TCP Handshake Before Allowing Data	☑	☑
Prohibit IP Spoofing	☑	☐
Prohibit RST Replay Attack	☐	☐
Log ICMP Errors	☐	
Stateful SIP Processing	☑	
Allow Tri-session with DNAT	☐	
Session Mirror Destination	IP Address: / Port:	IP Address: / Port:
Session Idle Timeout (sec)		
Disable FTP server	☐	
GRE Call ID Processing	☐	
Per-packet Logging	☐	☐
Broadcast-filter ARP	☐	
Prohibit ARP Spoofing	☑	
Session VOIP Timeout (sec)		
Stateful H.323 Processing	☑	
Stateful SCCP Processing	☑	

Példa a forgalomszabályozásra – II.



Példa a forgalomszabályozásra - III.

Authentication State

General	
Profile	biztributor-HQ-corporate
Username	dnemes
User Role	authenticated
Age	0 days 05:51:00
Authenticated	Yes
Authentication Status	successful

Idle Timeout

Mobility State

Host Information

RoamingStatus	Home VLAN	Home Network	DHCP Status
None found.			

Trail Information

AP Name	Controller IP	Current VLAN	Roaming Status	Start Date	ESSID	BSSID	Radio Ty

User Firewall State

Source IP	Source Port	Destination IP	Destination Port	Protocol	Stat
10.0.0.57	51736	205.251.205.217	80	TCP	Allow
10.0.0.57	51737	205.251.205.217	80	TCP	Allow
10.0.0.57	51738	205.251.205.217	80	TCP	Allow
10.0.0.57	51739	205.251.205.217	80	TCP	Allow
10.0.0.57	51734	205.251.205.217	80	TCP	Allow
10.0.0.57	51735	205.251.205.217	80	TCP	Allow

Upstream: 2M (2mbps) Change Per Role

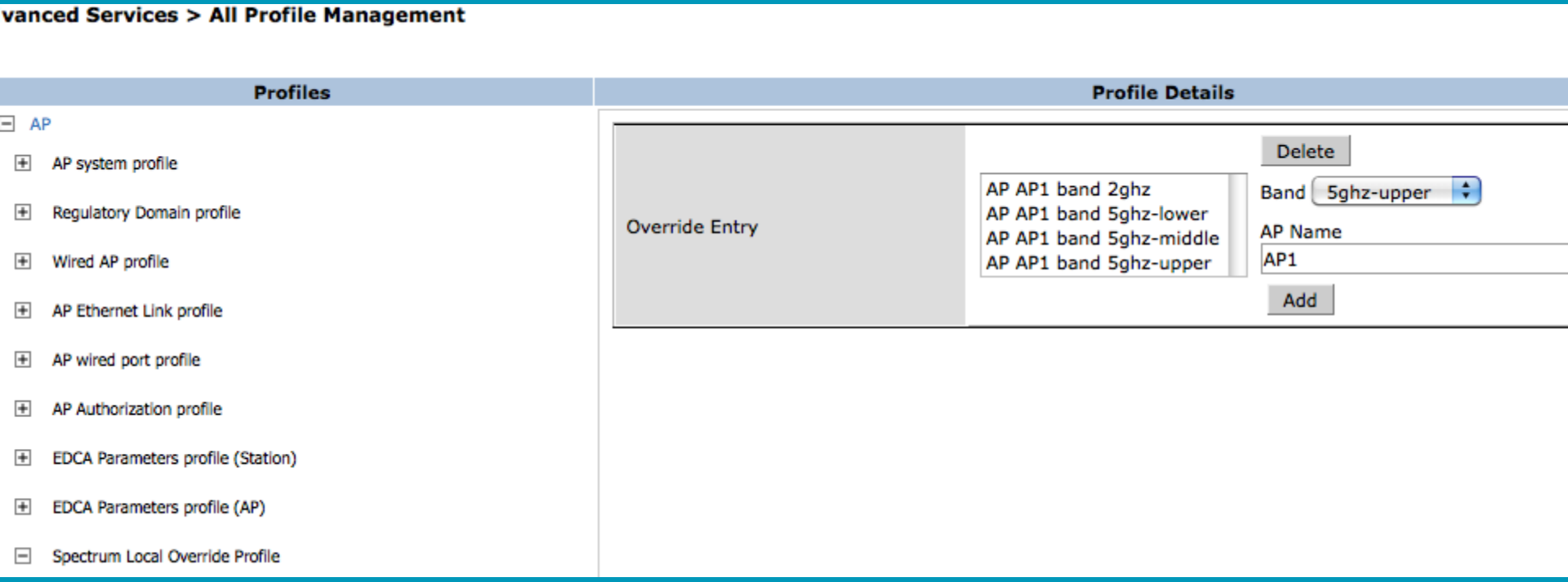
Downstream: 2M (2mbps) Change Per Role

A vállalati Wi-Fi biztonsági vektorai - átláthatóság

- **Átláthatóság**
  - Az átviteli közeg (L1) átláthatósága,
  - Ha nem tudjuk mi történik a közegben, nem tekinthetjük biztonságosnak,
  - Spektrum analízis, közegmonitoring
  - Interferencia-elemzés,
  - Zaj-zavar forrás azonosítás,
  - Csatornák terheltségének elemzése,
  - Anomáliák felfedése.

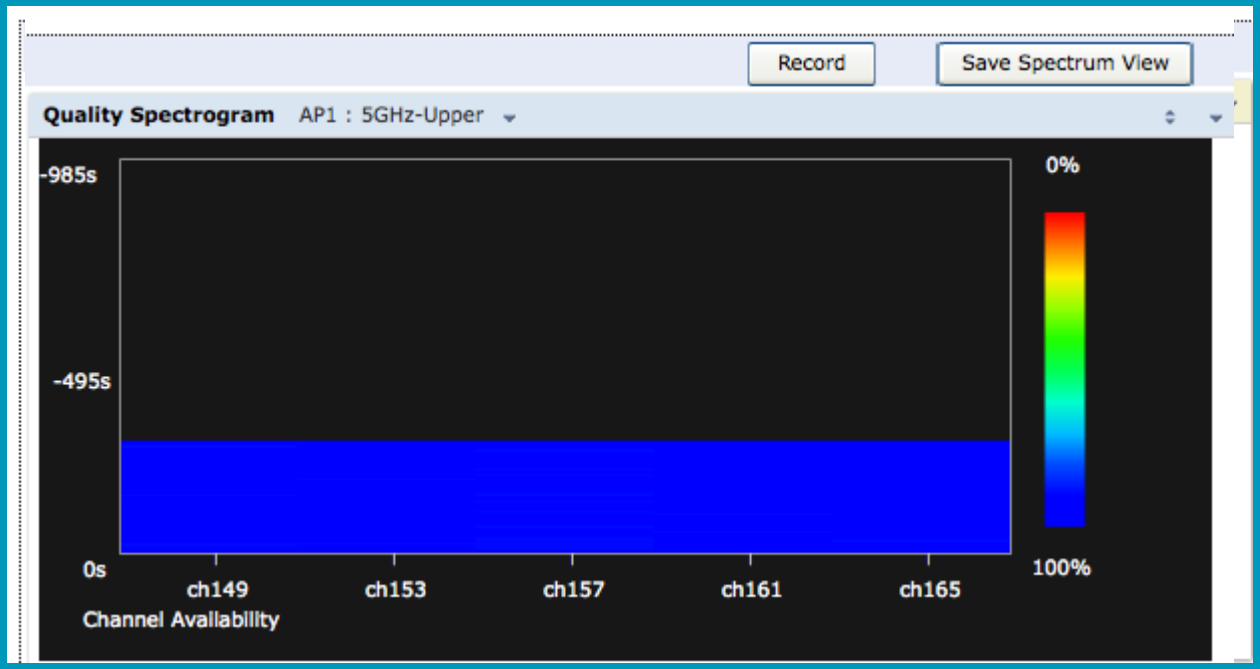
Példa at átláthatóságra – I.

- ✓ Teljes spektrumkép monitorozás



Példa az átláthatóságra – II.

- ✓ Quality spectogram 2.4 és 5Ghz



Példa az átláthatóságra – III.

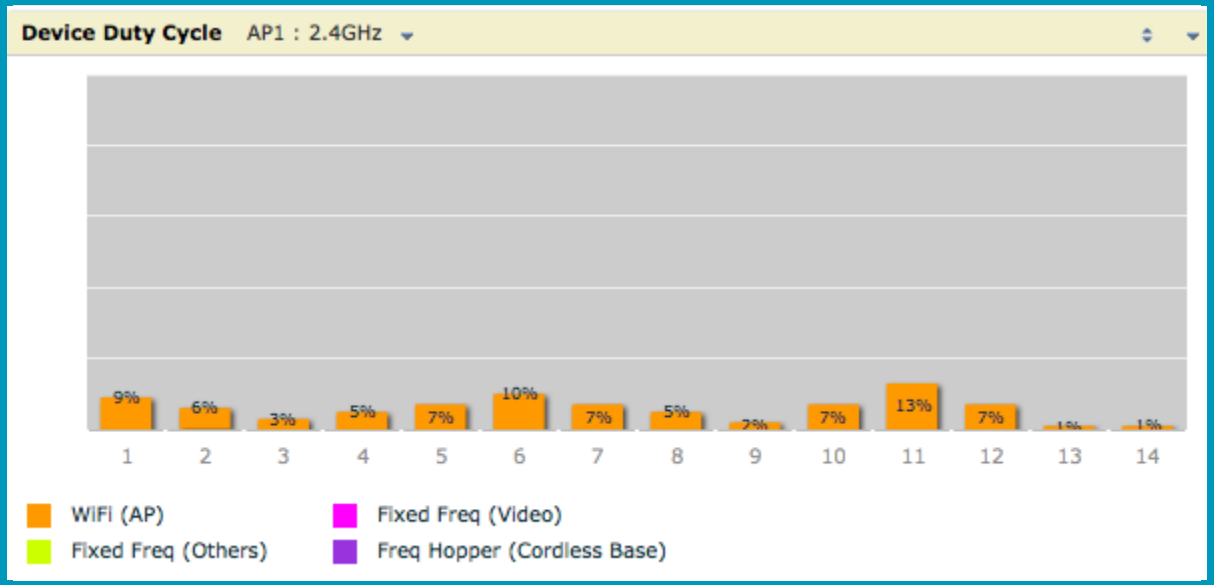
- ✓ Utilization és summary

Channel Summary Table (14) AP1 : 2.4GHz

Chan	Valid APs	Not Valid APs	Non Wi-Fi Devices	Center Freq. (GHz)	Channel Util. (%)	Max AP Power (dBm)	Max Interference (dBm)	SINR (dB)
1	0	5	0	2.412	11	-26	-	26
2	0	6	0	2.417	10	-	-	0
3	0	8	0	2.422	10	-	-	0
4	0	8	0	2.427	12	-	-	0
5	0	4	0	2.432	17	-87	-	87
6	0	4	0	2.437	20	-24	-	24
7	0	4	0	2.442	18	-	-	0
8	0	9	0	2.447	16	-	-	0
9	0	8	0	2.452	15	-87	-	87
10	0	7	0	2.457	17	-	-	0

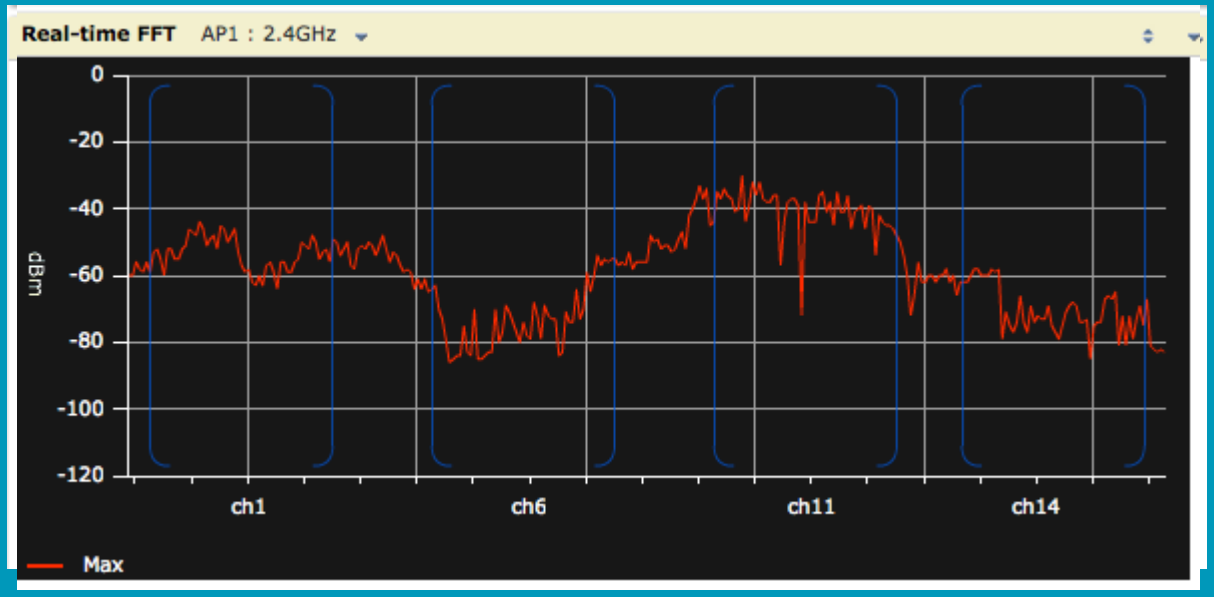
Példa az átláthatóságra – IV.

- ✓ Eszköz-csatorna eloszlások, stb.



Példa az átláthatóságra – V.

- ✓ Interferencia elemzés, FFT, stb.

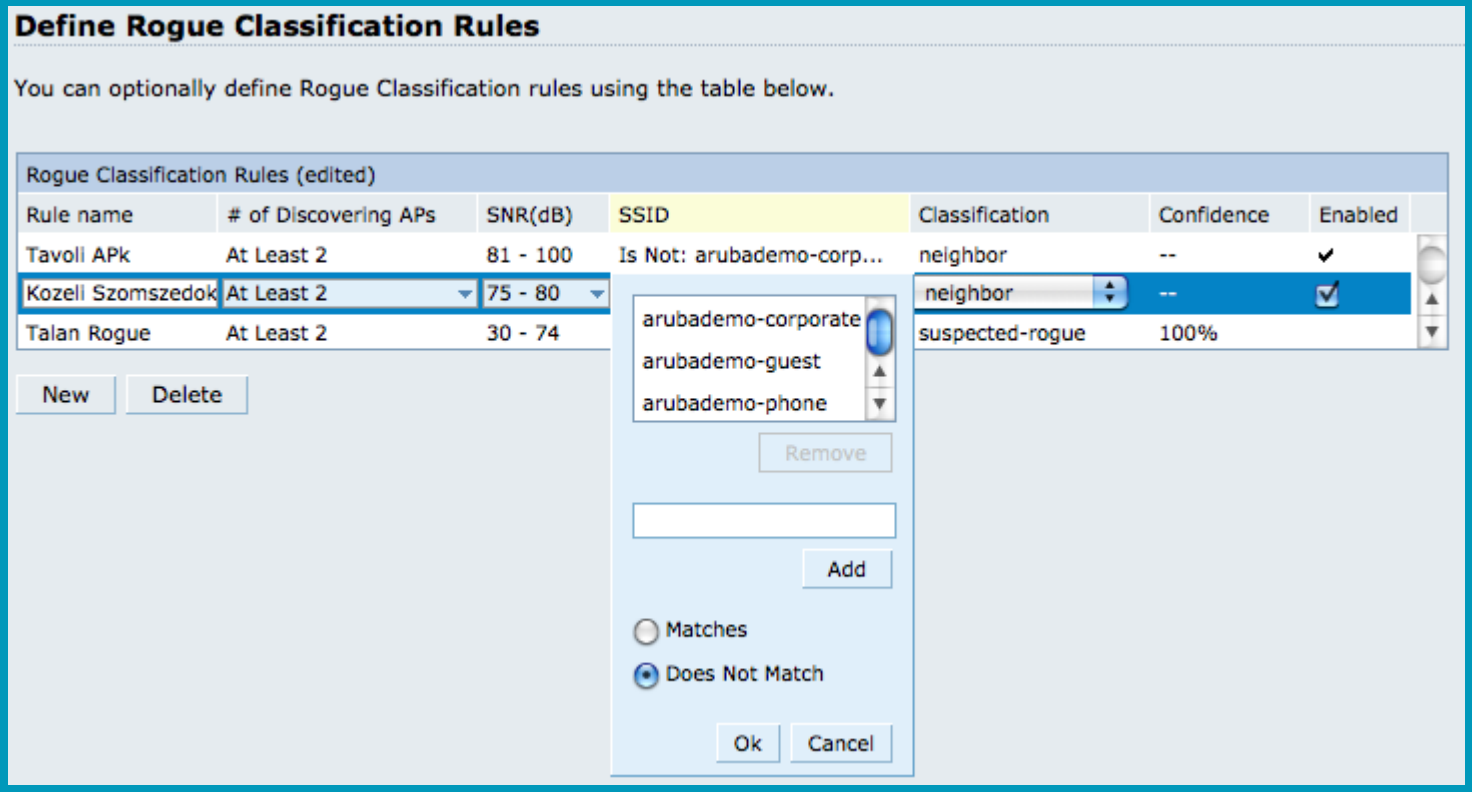


A vállalati Wi-Fi biztonsági vektorai - Önvédelem

- **Önvédelem**
  - Az átviteli közeg (L1) védelme,
  - Ha nem tudjuk mi történik a közegben, nem tekinthetjük biztonságosnak,
  - **Wireless IPS**
    - Infrastruktúra-védelem,
      - Rogue devices (Rogue, brideg, ad-hoc, soft AP),
      - Spoofing,
      - Impersonation
      - Közegmanipulációk, stb.
    - Kliens-védelem,
    - Anomáliák felfedése.

Példa az önvédelemre – I.

- ✓ SNR based (unconnected Rogue)

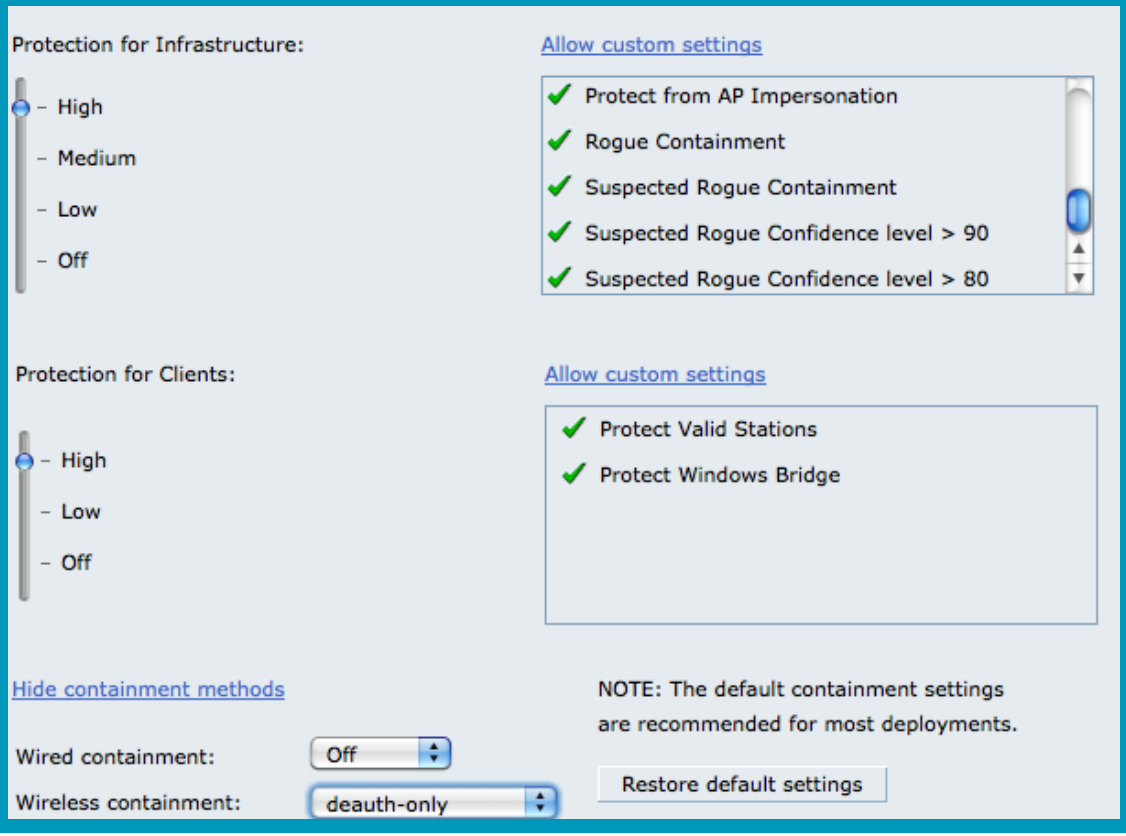


Példa az önvédelemre – II.

- ✓ RF&Security anomália detektálás

Példa az önvédelemre – III.

- ✓ Infrastruktúra és kliens védelem



Példa az önvédelemre – IV.

- ✓ Rogue detektálás, teljes környezet monitoring

Discovered APs & Clients — Summary | Details

AP Classification	Active APs	Associated Clients
Rogue	1	7
Suspected Rogue	2	3
Interfering	18	1
Neighbor	0	0
Valid	0	0
Manually Contained	0	0
Total	21	11

Events

Containment	Infrastructure	
	Client	
	Total	
Detection	Low	
	Med	
	High	
	Total	

Discovered Access Points: AP Classification = Rogue, Active = Yes

Locate | Contain M

BSSID	Band	PHY Type	SSID	Channel	Clients	AP Classification: Rogue	Encryption	Marked to Contain
00:1a:1e:81:26:60	2.4 GHz	g-HT40	biztributor-corporate	11	7	Rogue	WPA2	No

Példa az önvédelemre – V.

- ✓ Rogue detektálás, teljes környezet monitoring

Discovered APs & Clients Summary Details

AP Classification	Active APs	Associated Clients
Rogue	1	7
Suspected Rogue	2	3
Interfering	18	1
Neighbor	0	0
Valid	0	0
Manually Contained	0	0
Total	21	11

Events

		Las
Containment	Infrastructure	
	Client	
	Total	
Detection	Low	
	Med	
	High	
	Total	

Discovered Clients: AP Classification = Rogue, Active = Yes

Locate

MAC	Band	PHY Type	BSSID	SSID	Client Classification	AP Classification Rogue	Events	Channel
00:19:d2:33:f2:f3	2.4 GHz	g	00:1a:1e:81:26:60	biztributor-corporate	Interfering	Rogue	1	11
00:22:fa:ee:53:7c	2.4 GHz	g-HT	00:1a:1e:81:26:60	biztributor-corporate	Interfering	Rogue	1	11
78:e4:00:12:a9:8f	2.4 GHz	g-HT	00:1a:1e:81:26:60	biztributor-corporate	Interfering	Rogue	1	11
c0:cb:38:7c:89:3a	2.4 GHz	g-HT	00:1a:1e:81:26:60	biztributor-corporate	Interfering	Rogue	1	11
c4:46:19:30:96:d2	2.4 GHz	g-HT	00:1a:1e:81:26:60	biztributor-corporate	Interfering	Rogue	1	11
e0:f8:47:19:74:f8	2.4 GHz	g-HT	00:1a:1e:81:26:60	biztributor-corporate	Interfering	Rogue	5	11
e8:39:df:44:a7:25	2.4 GHz	g-HT	00:1a:1e:81:26:60	biztributor-corporate	Interfering	Rogue	1	11

Példa az önvédelemre – VI.

- ✓ „wKlicsko” lecsap – offenzív védelem

Events: Target Type = Infrastructure, Feature Type = Containment

Level	Last Seen	Type	Target	Target Type: Infrastructure	Occurrences	Details
High	14:27:43 Feb 2, 2012	Tarpit Containment	00:1a:1e:81:26:60	Infrastructure	535	Channel:11; Channel:12; Src-MAC:00:1a:
High	14:26:26 Feb 2, 2012	AP Deauth Containment	00:1a:1e:81:26:60	Infrastructure	9	SSID:biztributor-corporate; Channel:11; M
High	14:25:45 Feb 2, 2012	AP Deauth Containment	00:1a:1e:81:26:70	Infrastructure	6	SSID:biztributor-corporate; Channel:116;
High	14:25:45 Feb 2, 2012	Tarpit Containment	00:1a:1e:81:26:70	Infrastructure	16	Channel:11
High	14:10:11 Feb 2, 2012	Tarpit Containment	74:ea:3a:c1:ff:e0	Infrastructure	132	Channel:4;
High	14:07:15 Feb 2, 2012	AP Deauth Containment	74:ea:3a:c1:ff:e0	Infrastructure	1	SSID:rogu
High	14:04:01 Feb 2, 2012	AP Deauth Containment	00:1a:1e:81:26:63	Infrastructure	1	SSID:biztri

És az új vektor: BYOD

- ✓ Megjelenik egy új vektor, az eszköz maga

Bring Your Own Device

Block Your Own Device

IBWIW (BYOD fokozása)

És az új vektor: BYOD

- **BYOD**
  - Rendszeridegen eszköz, amely hozzáfér a vállalati hálózathoz,
  - Beléptetés a hálózatba,
  - Kontroll,
  - Szeparálás

Nem a titkosítás...

- ✓ A vállalati Wi-Fi biztonsága NEM a titkosításon múlik!

Nem a titkosítás...

- ✓ A forgalmat kell szabályozni és a környezetet kell átláthatóvá tenni!

Kérdések?

köszönöm a figyelmet!

tkocsis@biztributor.hu