

KOCSIS TAMÁS (biztributor):

Mitől vállalati a Wi-Fi biztonsága?

D-Link

NETGEAR

TP-LINK

EnGenius

MikroTik

LINKSYS

ASUS

SMC
Networks

Biztonságos?

- ✓ Titkosítás
- ✓ Hitelesítés
- ✓ Forgalm szabályozás
- ✓ Átláthatóság
- ✓ Önvédelem

✓ 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!**

✓ 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

<input type="radio"/>	tkocsis	00:f4:b9:5d:1e:dd	10.0.0.111	rap-users	802.1x	biztributor-corporate	andris-rap
<input type="radio"/>	dnemes	a8:16:b2:ff:b2:47	10.0.0.53	rap-users	802.1x	biztributor-corporate	dnemes-rap

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

Példa a forgalomszabályozásra – II.

User Roles **System Roles** Policies Time Ranges Guest Access

Role Name

Firewall Policies

Name	Rule Count	Location	Action			
dhcp-acl	1		Edit	Delete	▲	▼
icmp-acl	1		Edit	Delete	▲	▼
http-acl	1		Edit	Delete	▲	▼
https-acl	1		Edit	Delete	▲	▼

Re-authentication Interval
1000 minutes (0 disables re-authentication. A positive value enables authentication 0 - 4096)

Role VLAN ID
99

Bandwidth Contract
Upstream: 2M (2mbps)
Downstream: 2M (2mbps)

VPN Dialer
Not Assigned

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 Type
---------	---------------	--------------	----------------	------------	-------	-------	------------

User Firewall State

Source IP	Source Port	Destination IP	Destination Port	Protocol	Status
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

Downstream: 2M (2mbps)

Change



Kocsis Tamás (biztributor):
Mitől vállalati a Wi-Fi biztonsága?

✓ Átláthatóság

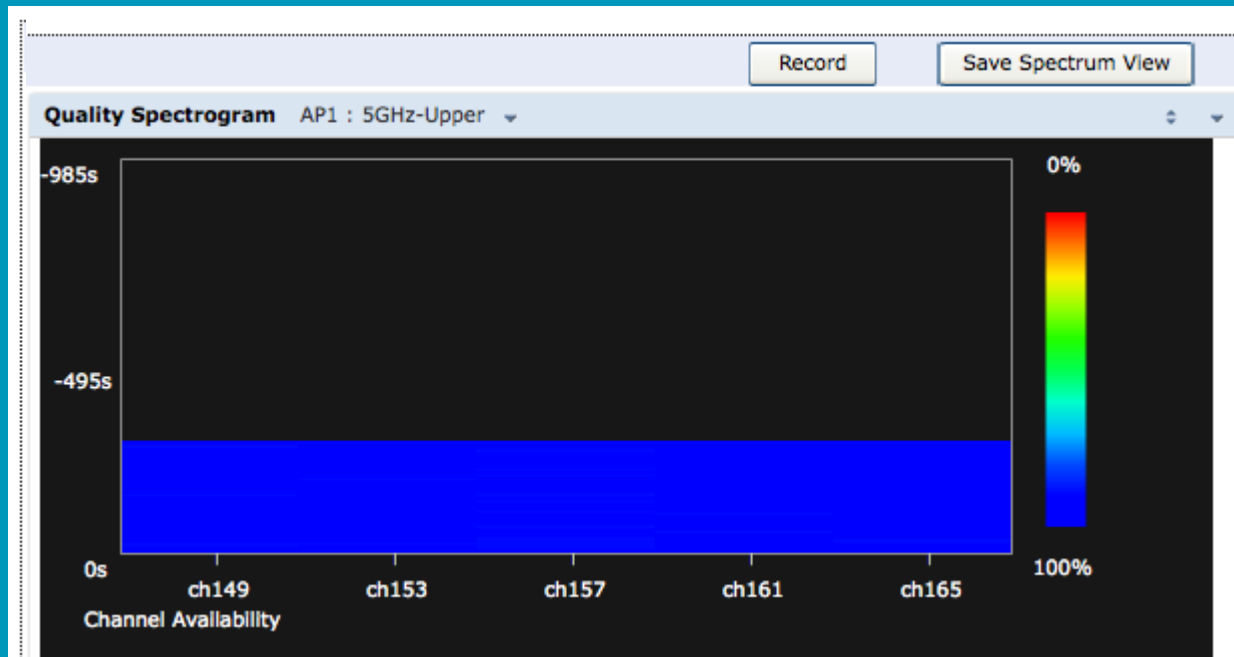
- ✓ Az átviteli közeg (L1) átláthatósága,
- ✓ Ha nem tudjuk mi történik a közegben, nem tekinthetjük biztonságosnak,
- ✓ Spektrum analízis, közegmonitoring
- ✓ Interferencia-elemzés,
- ✓ Zaj-zavar forrás azonosítás,
- ✓ Csatornák terheltségének elemzése,
- ✓ Anomáliák felfedése.

✓ Teljes spektrumkép monitorozás

Advanced Services > All Profile Management

Profiles	Profile Details
<ul style="list-style-type: none">AP<ul style="list-style-type: none">AP system profileRegulatory Domain profileWired AP profileAP Ethernet Link profileAP wired port profileAP Authorization profileEDCA Parameters profile (Station)EDCA Parameters profile (AP)Spectrum Local Override Profile	<div data-bbox="755 511 1186 758">Override Entry</div> <div data-bbox="1205 511 1534 696"><ul style="list-style-type: none">AP AP1 band 2ghzAP AP1 band 5ghz-lowerAP AP1 band 5ghz-middleAP AP1 band 5ghz-upper</div> <div data-bbox="1553 525 1823 739"><p>Delete</p><p>Band <input type="text" value="5ghz-upper"/></p><p>AP Name <input type="text" value="AP1"/></p><p>Add</p></div>

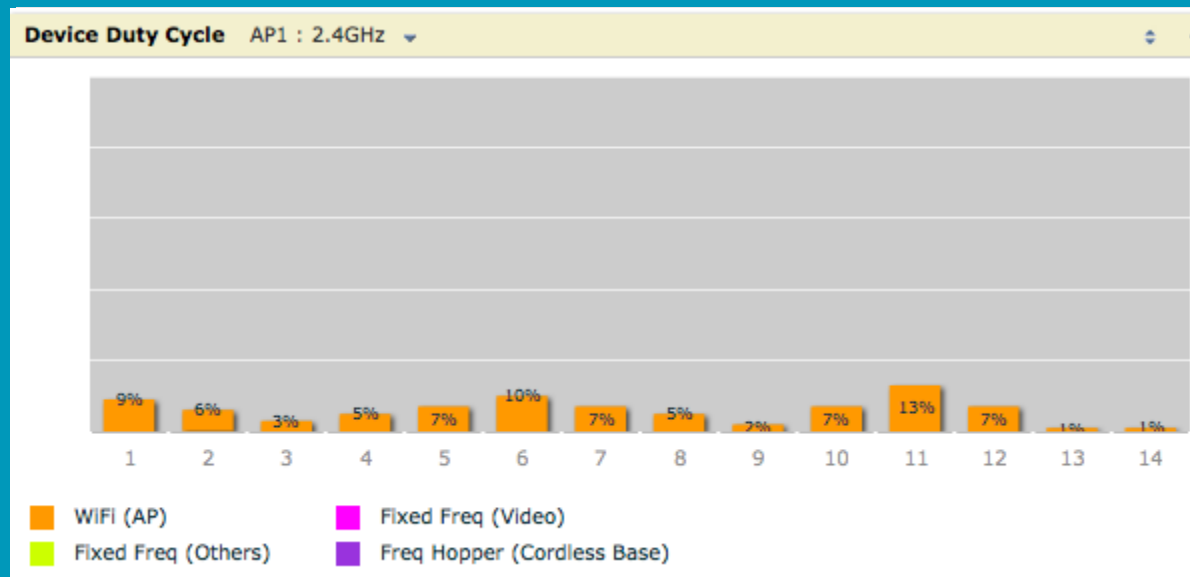
- ✓ Quality spectrogram 2.4 és 5Ghz



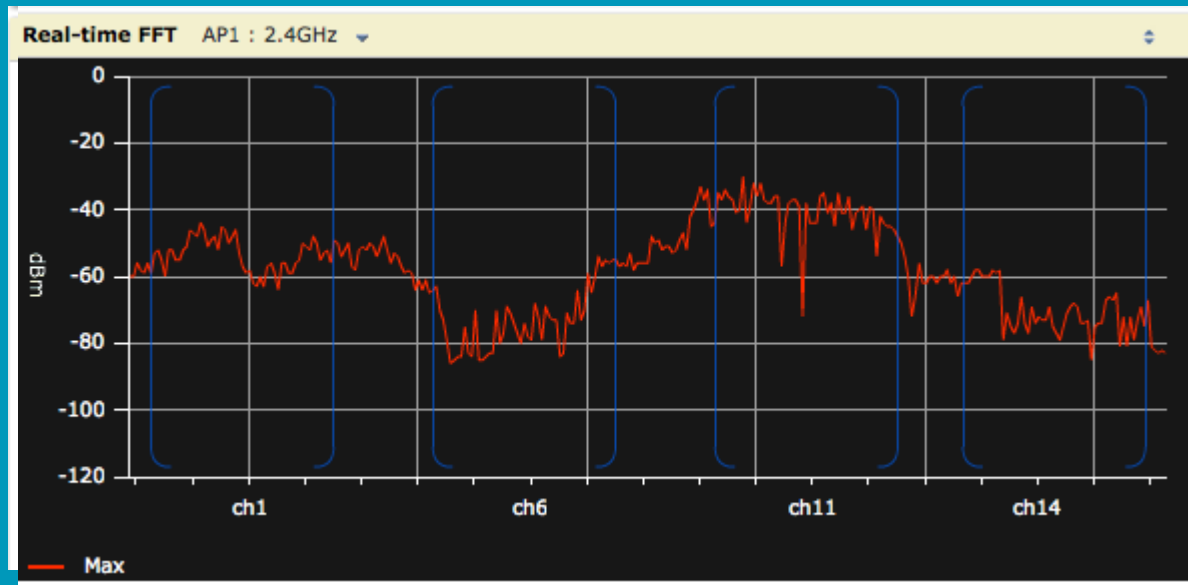
✓ Utilization és summary

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

- ✓ Eszköz-csatorna eloszlások, stb.



- ✓ Interferencia elemzés, FFT, stb.



✓ 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.

✓ SNR based (unconnected Rogue)

Define Rogue Classification Rules

You can optionally define Rogue Classification rules using the table below.

Rogue Classification Rules (edited)						
Rule name	# of Discovering APs	SNR(dB)	SSID	Classification	Confidence	Enabled
Tavoli APK	At Least 2	81 - 100	Is Not: arubademo-corp...	neighbor	--	✓
Kozeli Szomszedok	At Least 2	75 - 80	arubademo-corporate	neighbor	--	✓
Talan Rogue	At Least 2	30 - 74	arubademo-guest	suspected-rogue	100%	
			arubademo-phone			

New Delete

Remove

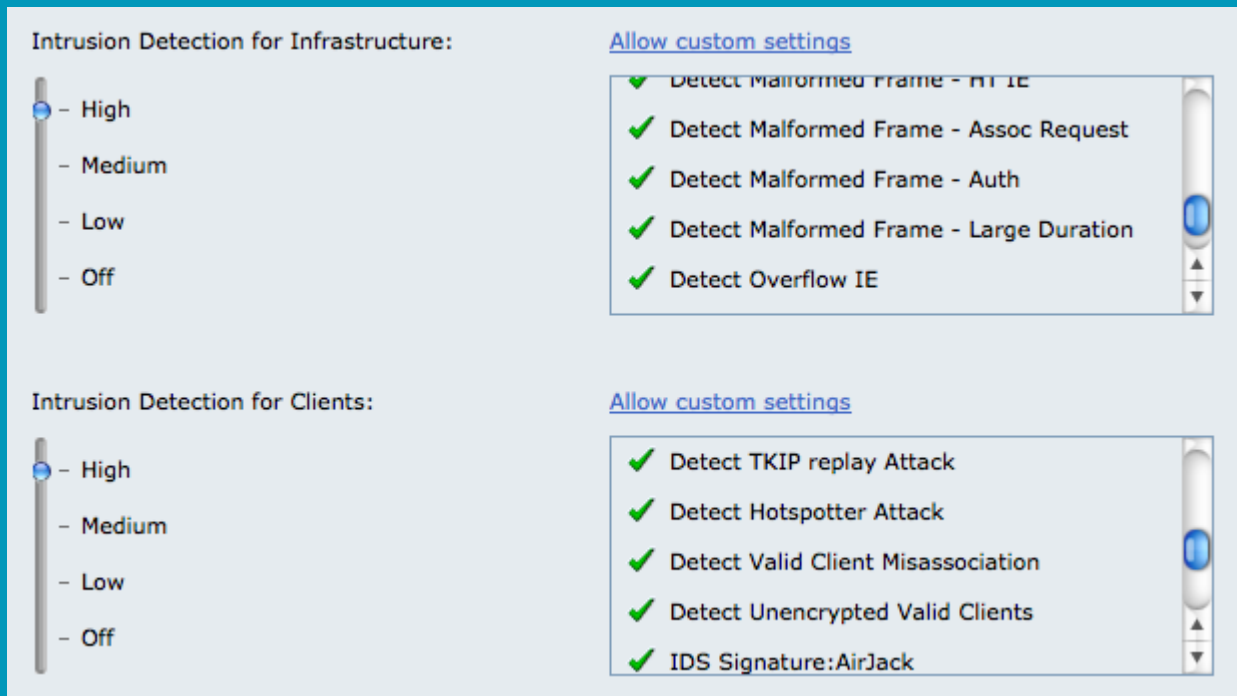
Add

Matches

Does Not Match

Ok Cancel

✓ RF&Security anomália detektálás



Intrusion Detection for Infrastructure:

– High
– Medium
– Low
– Off

[Allow custom settings](#)

- ✓ Detect Malformed Frame - HT IE
- ✓ Detect Malformed Frame - Assoc Request
- ✓ Detect Malformed Frame - Auth
- ✓ Detect Malformed Frame - Large Duration
- ✓ Detect Overflow IE

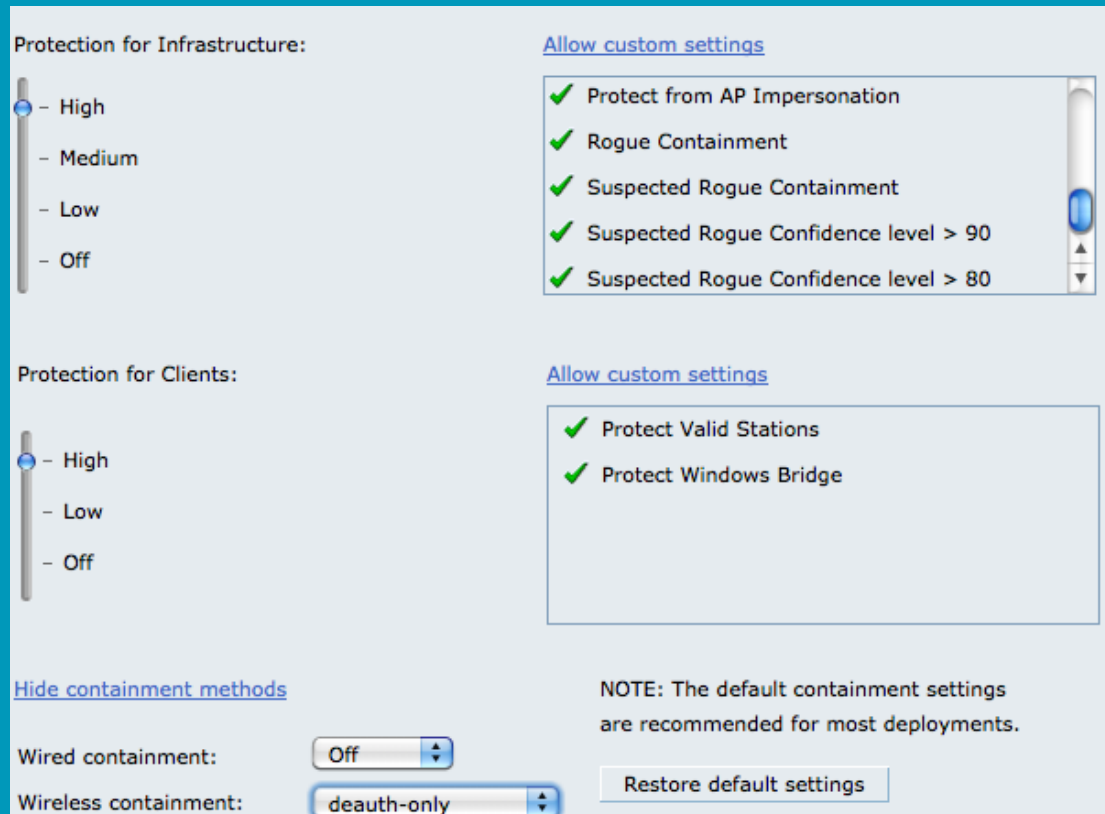
Intrusion Detection for Clients:

– High
– Medium
– Low
– Off

[Allow custom settings](#)

- ✓ Detect TKIP replay Attack
- ✓ Detect Hotspotter Attack
- ✓ Detect Valid Client Misassociation
- ✓ Detect Unencrypted Valid Clients
- ✓ IDS Signature:AirJack

✓ Infrastruktúra és kliens védelem



The screenshot shows the configuration interface for protection settings, divided into two main sections: "Protection for Infrastructure" and "Protection for Clients".

Protection for Infrastructure:

- Protection level: High (selected)
- Options: High, Medium, Low, Off
- Link: [Allow custom settings](#)
- Enabled features (all checked):
 - Protect from AP Impersonation
 - Rogue Containment
 - Suspected Rogue Containment
 - Suspected Rogue Confidence level > 90
 - Suspected Rogue Confidence level > 80

Protection for Clients:

- Protection level: High (selected)
- Options: High, Low, Off
- Link: [Allow custom settings](#)
- Enabled features (all checked):
 - Protect Valid Stations
 - Protect Windows Bridge

Wired/Wireless Containment:

- Wired containment: Off
- Wireless containment: deauth-only

Additional Information:

- Link: [Hide containment methods](#)
- NOTE: The default containment settings are recommended for most deployments.
- Button: Restore default settings

✓ Rogue detektálás, teljes környezet monitoring

Discovered APs & Clients

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

Events

Containment	📶 Infrastructure
	👤 Client
	Total
Detection	● Low
	● Med
	● High
	Total

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

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

✓ Rogue detektálás, teljes környezet monitoring

Discovered APs & Clients

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

Events

- Containment
 - Infrastructure
 - Client
 - Total
- Detection
 - Low
 - Med
 - High
 - Total

Discovered Clients: AP Classification = Rogue, Active = Yes

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

✓ „wKlicsko” lecsap – offenzív védelem

Events: Target Type = Infrastructure, Feature Type = Containment

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



- ✓ Megjelenik egy új vektor, az eszköz maga

Bring Your Own Device



Block Your Own Device



I
Buy
What
I
Want

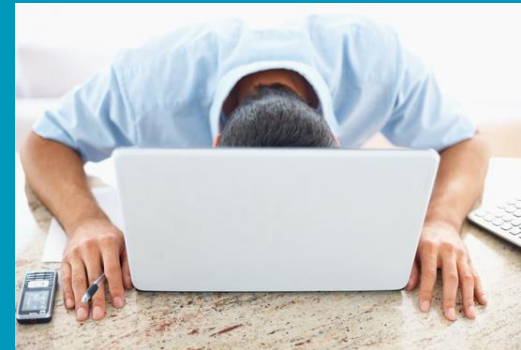


CAPISCE?



✓ BYOD

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



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

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

Kérdések?

köszönöm a figyelmet!

tkocsis@biztributor.hu