Rogue Classification

Unmodified Rules

Anti-MiFi:

# of discovering APs:	At least 0
Signal strength:	25 to 100 dBm
SSIDs:	Match MiFi, MiFi*, mifi, mifi*
Classification:	suspected-rogue
Confidence level:	100%
Enabled:	No

New Rule:

# of discovering APs:	At least 0
Signal strength:	25 to 100 dBm
SSIDs:	Match N/A
Classification:	suspected-rogue
Confidence level:	25%
Enabled:	No

SHE-HULK:

# of discovering APs:	At least 0
Signal strength:	10 to 100 dBm
SSIDs:	Match SHE-HULK
Classification:	suspected-rogue
Confidence level:	100%
Enabled:	No

Policy default

Assigned AP Groups:
A Building,
C Building,
CFCC RAP Group,
CFCC Special Event,
CFCC Special Event North,
default,
DT Air Monitors,
F Building,
G Building,
K, P, X & Art Gallery,
K, X and Art Gallery,
L Building,
N Building,
NA Building,
NA IDS / WIPS Test Grp,
NB Building,
NB IDS / WIPS Test Grp,
NC Air Monitors,
NC Building,
ND Building,
NoAuthApGroup,
R Building,
S Building,
T Building,
US Building 1st Floor,
US Building 2nd Floor,
US Building 3rd Floor,
US Building 4th Floor,
US Building 5th Floor,
W buildings

Infrastructure

Infrastructure: All Aruba APs

Intrusion detection

Detection level for infrastructure: Medium

- ✔ Detect AP Spoofing
- Detect AP Impersonation
- Detect Adhoc Networks
- Detect Valid SSID Misuse
- ✔ Detect Adhoc Network Using Valid SSID
- ✔ Detect Windows Bridge
- Detect Wireless Bridge
- Detect 802.11n 40MHz Intolerance Setting
- Detect Active 802.11n Greenfield Mode
- Detect AP Flood Attack
- Detect Client Flood Attack
- Detect Bad WEP
- ✔ IDS Signature:Deauth-Broadcast
- ✔ IDS Signature:Disassoc-Broadcast
- IDS Signature:Netstumbler Generic
- IDS Signature:Netstumbler Version 3.3.0.x
- IDS Signature:Wellenreiter
- ✔ Detect Misconfigured AP
- ✔ Privacy
- ✔ Require WPA
- Detect CTS Rate Anomaly
- Detect RTS Rate Anomaly
- Detect Invalid Address Combination
- Detect Malformed Frame - HT IE
- Detect Malformed Frame - Assoc Request
- Detect Malformed Frame - Auth
- ✔ Detect Malformed Frame - Large Duration
- Detect Overflow IE
- Detect Overflow EAPOL Key
- Detect Beacon Wrong Channel
- Detect Devices with an Invalid MAC OUI

Detection level for clients: Medium

- ✔ Detect Disconnect Station Attack
- Detect EAP Rate Anomaly
- Detect Rate Anomalies
- ✔ Detect Omerta Attack
- ✔ Detect FATA-Jack Attack
- ✔ Detect Block ACK DoS
- Detect ChopChop Attack
- Detect TKIP replay Attack
- ✔ Detect Hotspotter Attack
- ✔ Detect Valid Client Misassociation
- ✔ Detect Unencrypted Valid Clients
- IDS Signature:AirJack
- IDS Signature:ASLEAP
- IDS Signature:Null Probe Resonse
- ✔ Detect Power Save DoS Attack

Protection

Protection level for infrastructure: Off

- Protect Misconfigured AP
- Protect From Adhoc Networks
- Protect SSID
- Protect 802.11n High Throughput Devices
- Protect 40MHz 802.11n High Throughput Devices
- Protect from AP Impersonation
- Rogue Containment
- Suspected Rogue Containment
- Suspected Rogue Confidence level > 90
- Suspected Rogue Confidence level > 80

Protection level for clients: Off

- Protect Valid Stations
- Protect Windows Bridge