Cisco Adaptive wIPS Enhanced Local Mode (ELM) Configuration and Deployment Guide

Document ID: 113027

Contents

Introduction
Prerequisites
Requirements
Components Used
Conventions
ELM wIPS Alarm Flow
Deployment Considerations for ELM
ELM vs Dedicated MM
On−Channel and Off−Channel Performance
ELM Across WAN Links
CleanAir Integration
ELM Features and Benefits
ELM Licensing
Configure ELM with WCS
Configuration from WLC
Attacks Detected in ELM
Troubleshoot ELM
Related Information

Introduction

The Cisco Adaptive Wireless Intrusion Prevention System (wIPS) solution adds the Enhanced Local Mode (ELM) feature, allowing administrators to use their deployed access points (APs) to provide comprehensive protection without the need for a separate overlay network (Figure 1). Prior to ELM and in the traditional Adaptive wIPS deployment, dedicated monitor mode (MM) APs are required to provide PCI Compliance needs or protection from unauthorized security access, penetration, and attacks (Figure 2). ELM effectively provides a comparable offering that eases wireless security implementation while lowering CapEx and OpEx costs. This document only focuses on ELM and does not modify any existing wIPS deployment benefits with MM APs.

Figure 1 − Enhanced Local Mode AP Deployment

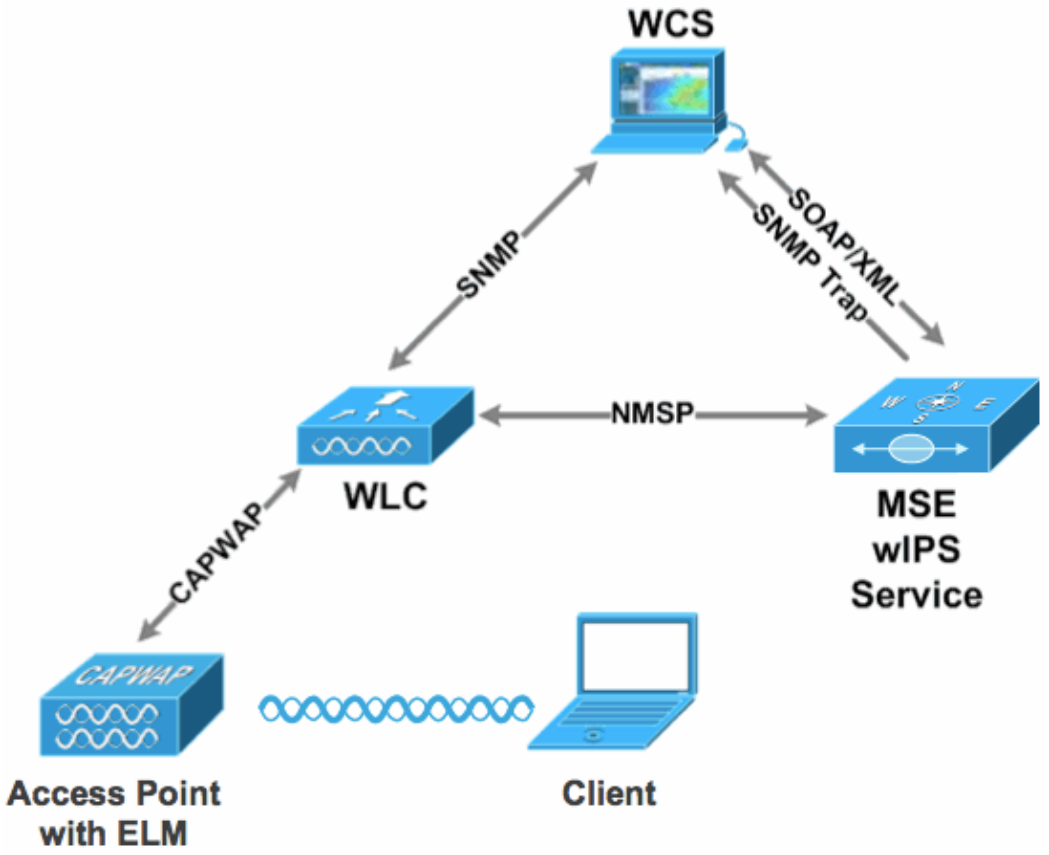
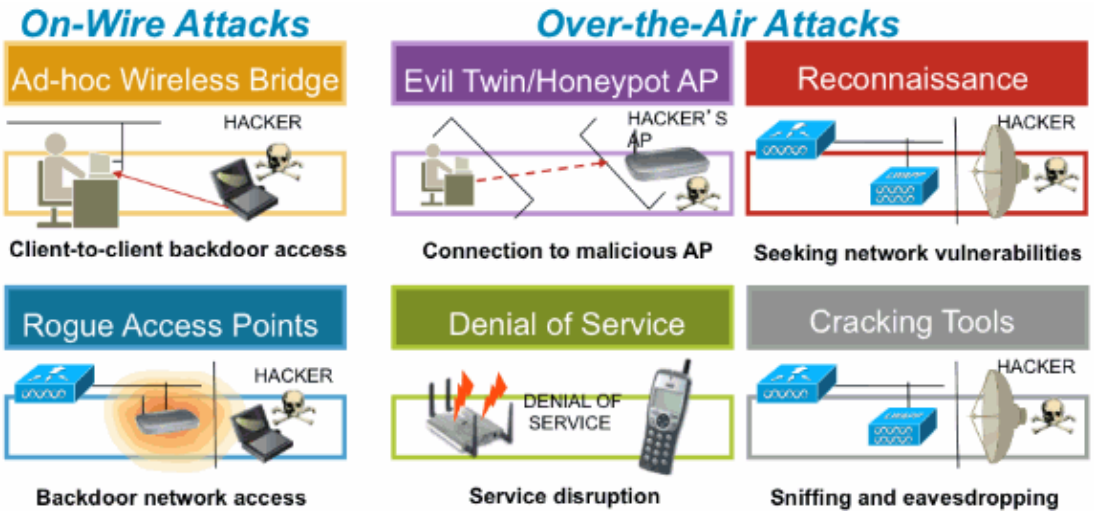


Figure 2 − Top Wireless Security Threats



Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

ELM Required Components and Minimum Code Versions

- Wireless LAN Controller (WLC) − Version 7.0.116.xx or later
- APs − Version 7.0.116.xx or later
- Wireless Control System (WCS) − Version 7.0.172.xx or later
- Mobility Services Engine − Version 7.0.201.xx or later

Supporting WLC Platforms

ELM is supported on WLC5508, WLC4400, WLC 2106,WLC2504, WiSM−1, and WiSM−2WLC platforms.

Supporting APs

ELM is supported on 11n APs including 3500, 1250, 1260, 1040, and 1140.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

ELM wIPS Alarm Flow

Attacks are only relevant when they occur on trusted infrastructure APs. The ELM APs will detect and communicate to the controller and correlate with the MSE for reporting with WCS management. Figure 3 provides the alarm flow from an administrator's point of view:

1. Attack launched against an infrastructure device ("trusted" AP)
2. Detected on ELM AP communicated through CAPWAP to WLC
3. Passed transparently to MSE via NMSP
4. Logged into wIPS Database on MSE Sent to WCS via SNMP trap
5. Displayed at WCS

Figure 3 − Threat Detection and Alarm Flow



Deployment Considerations for ELM

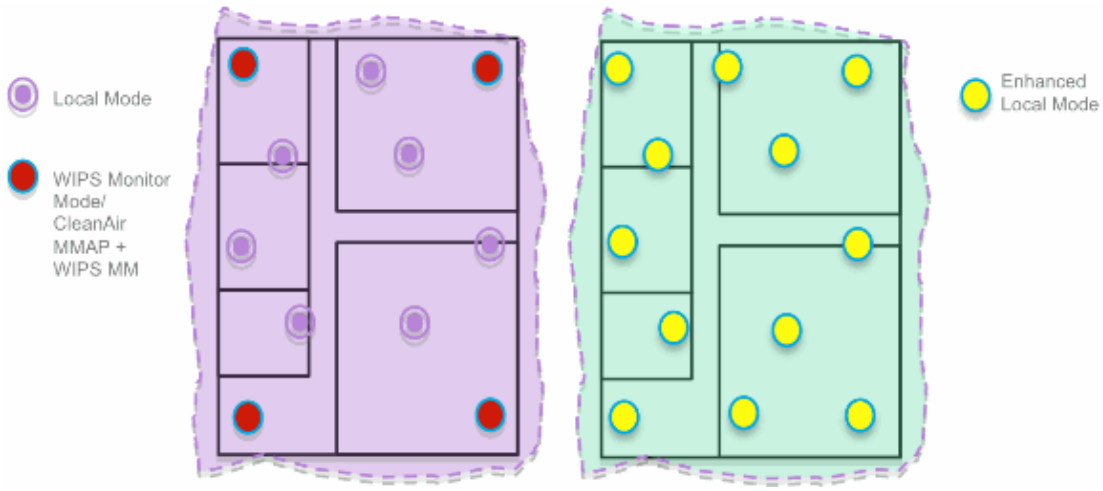
Cisco recommends that by enabling ELM on every AP on the network meet most customer security needs when a network overlay and/or costs are part of consideration. ELM primary feature operates effectively for on−channel attacks, without any compromise to the performance on data, voice and video clients, and services.

ELM vs Dedicated MM

Figure 4 provides a general contrast between the standard deployments of wIPS MM APs and ELM. In review, the typical coverage range for both modes suggests:

- Dedicated wIPS MM AP typically covers 15,000−35,000 square feet
- Client−serving AP will typically cover from 3,000−5,000 square feet

Figure 4 − Overlay of MM vs All ELM APs



In the traditional Adaptive wIPS deployment, Cisco recommends a ratio of 1 MM AP to every 5 local mode APs, which may also vary based on network design and expert guidance for best coverage. By considering ELM, the administrator simply enables the ELM software feature for all of the existing APs, effectively adding MM wIPS operations to local data−serving mode AP while maintaining performance.

On−Channel and Off−Channel Performance

A MM AP utilizes 100% of the radio s time for scanning all channels, as it does not serve any WLAN clients. The primary feature for ELM operates effectively for on−channel attacks, without any compromise to the performance on data, voice and video clients and services. The primary difference is in the local mode varying off−channel scanning; depending on the activity, off−channel scanning provides minimal dwell time to gather enough information available to classify and determine attack. An example may be with voice clients that are associated and where AP s RRM scanning is deferred until the voice client is dis−associated to make sure service is not affected. For this consideration, ELM detection during off−channel is considered best effort. Neighboring ELM APs operating on all, country or DCA channels increases effectiveness, hence the recommendation for enabling ELM on every local mode AP for maximum protection coverage. If the requirement is for dedicated scanning on all channels full−time, the recommendation will be to deploy MM APs.

These points review differences of local mode and MM APs:

- Local Mode AP − Serves WLAN clients with time slicing off−channel scanning, listens for 50ms on each channel, and features configurable scanning for all/country/DCA channels.
- Monitor Mode AP − Does not serve WLAN clients, dedicated to scanning only, listens for 1.2s on each channel, and scans all channels.

ELM Across WAN Links

Cisco has made great efforts in order to optimize features in challenging scenarios, such as deploying ELM APs across low bandwidth WAN links. The ELM feature involves pre−processing in determining attack signatures at the AP and is optimized to work over slow links. As best practices, it is recommended to test and measure the baseline to validate performance with ELM over WAN.

CleanAir Integration

The ELM feature highly compliments CleanAir operations with similar performance and benefits to deployment of MM APs with these existing CleanAir spectrum−aware benefits:

- Dedicated silicon−level RF intelligence
- Spectrum−aware, self−healing, and self−optimizing
- Non−standard channel threat and interference detection and mitigation
- Non Wi−Fi detection such as Bluetooth, microwave, cordless phones, etc.
- Detect and locate RF layer DOS attacks such as RF jammers

ELM Features and Benefits

- Adaptive wIPS scanning in data serving local and H−REAP APs
- Protection without requiring a separate overlay network
- Available as a free SW download for existing wIPS customers
- Supports PCI compliance for the wireless LANs
- Full 802.11 and non−802.11 attack detection
- Adds forensics and reporting capabilities
- Integrates with existing CUWM and WLAN management
- Flexibility to set integrated or dedicated MM APs
- Pre−processing at APs minimize data backhaul (that is, works over very low bandwidth links)
- Low impact on the serving data

ELM Licensing

ELM wIPS adds a new license to the ordering:

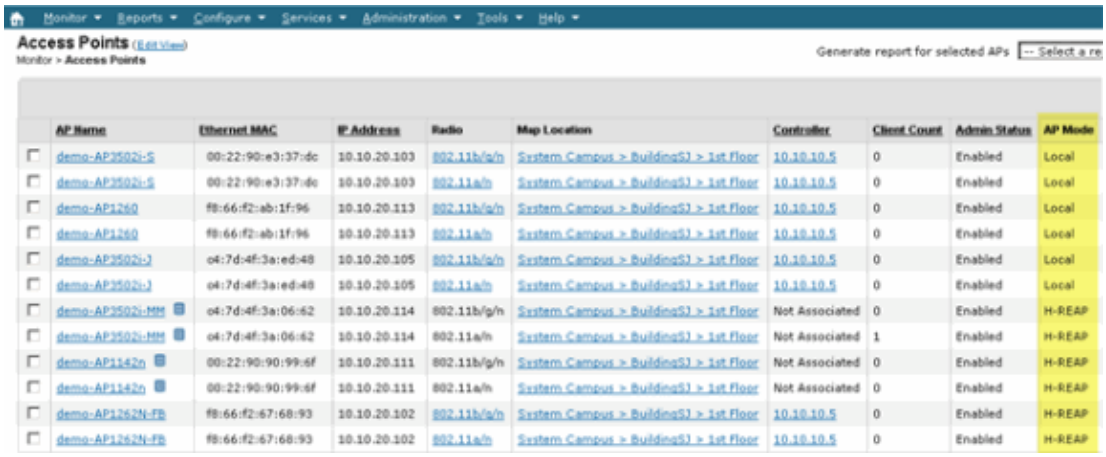
- AIR−LM−WIPS−xx − Cisco ELM wIPS License
- AIR−WIPS−AP−xx − Cisco Wireless wIPS License

Additional ELM licensing notes:

- If wIPS MM AP license SKU(s) are already installed, those licenses can also be used for ELM APs.
- wIPS licenses and ELM licenses together count towards the platform license limits for wIPS engine; 2000 APs on 3310, and 3000 APs on 335x, respectively.
- The evaluation license will include 10 APs for wIPS and 10 for ELM for a period of up to 60 days. Prior to ELM, the evaluation license allowed up to 20 wIPS MM APs. Minimum requirement of software versions supporting ELM must be met.

Configure ELM with WCS

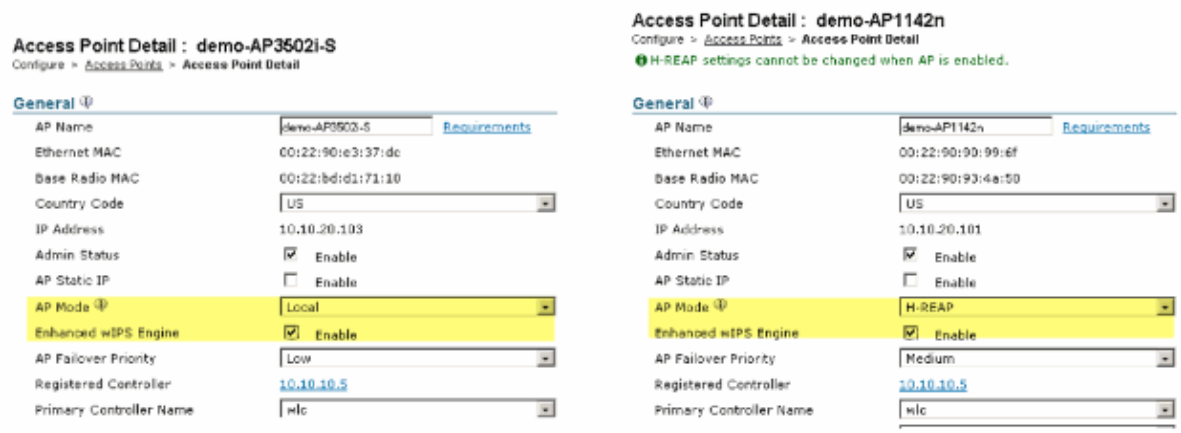
Figure 5 − Using WCS to Configure ELM



1. From WCS, disable both 802.11b/g and 802.11a radios of the AP before enabling Enhanced wIPS Engine.

   Note: All associated clients will be disconnected, and will not join until the radios are enabled.
2. Configure one AP, or use a WCS configuration template for multiple lightweight APs. See Figure 6.

Figure 6 − Enable Enhanced wIPS Engine (ELM) sub mode

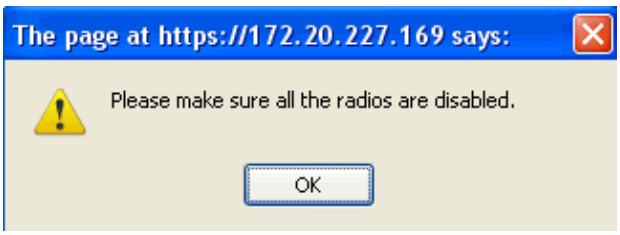


3. Choose **Enhanced wIPS Engine**, and click **Save**.

   a. Enabling Enhanced wIPS Engine will not cause the AP to reboot.
   b. H−REAP is supported; enable the same way as for local mode AP.

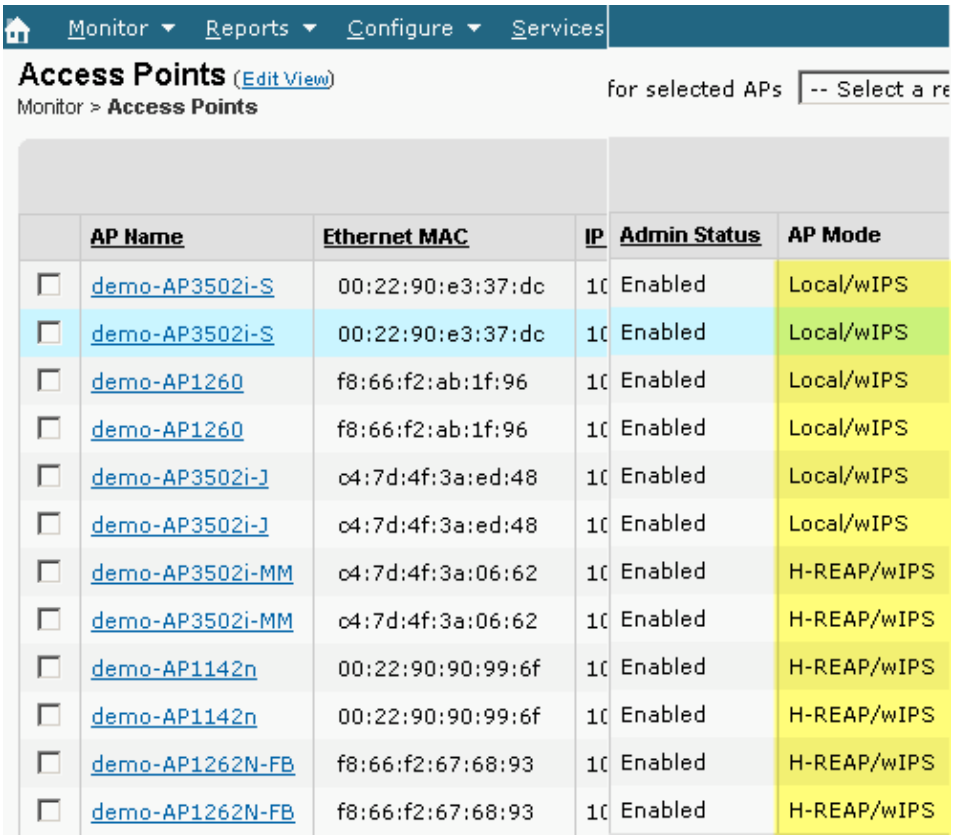
Note: If either of the radios of this AP is enabled, WCS will ignore the configuration and throw the error in Figure 7.

Figure 7 − WCS Reminder to Disable AP Radios before Enabling ELM



4. Configuration success can be verified by observing the change in AP Mode from Local or H−REAP to **Local/wIPS** or **H−REAP/wIPS**. See Figure 8.

Figure 8 − WCS Displaying AP Mode to Include wIPS with Local and/or H−REAP

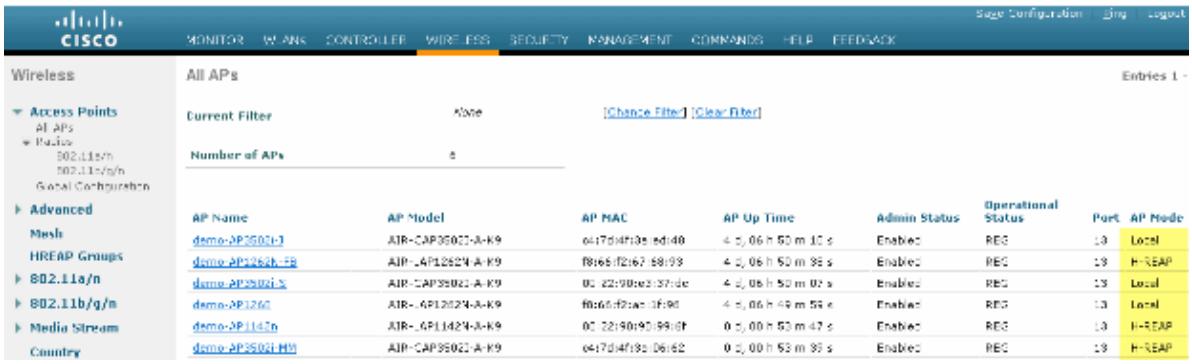


5. Enable the radios that where disabled in Step 1.
6. Create the wIPS profile and push it to the controller in order for the configuration to complete.

Note: For complete configuration information on wIPS, refer to the Cisco Adaptive wIPS Deployment Guide.

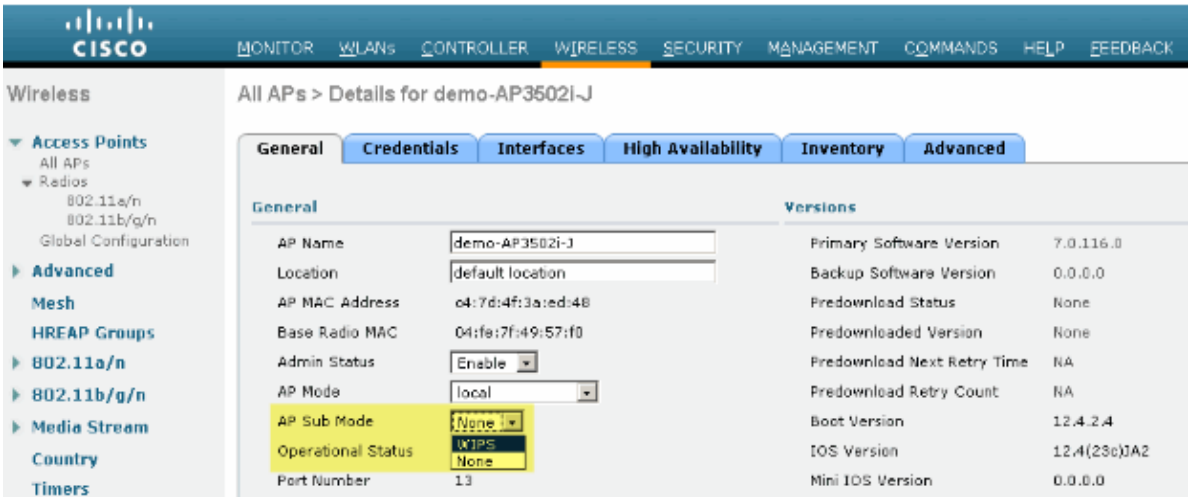
Configuration from WLC

Figure 9 − Configure ELM with WLC



1. Choose an AP from the **Wireless** tab.

Figure 10 − WLC Changing AP sub mode to Include wIPS ELM



2. From the AP Sub Mode drop−down menu, choose **wIPS** (Figure 10).
3. Apply, and then save the configuration.

Note: For ELM functionality to work, MSE and WCS are required with wIPS licensing. Changing the AP sub mode from WLC alone will not enable ELM.

Attacks Detected in ELM

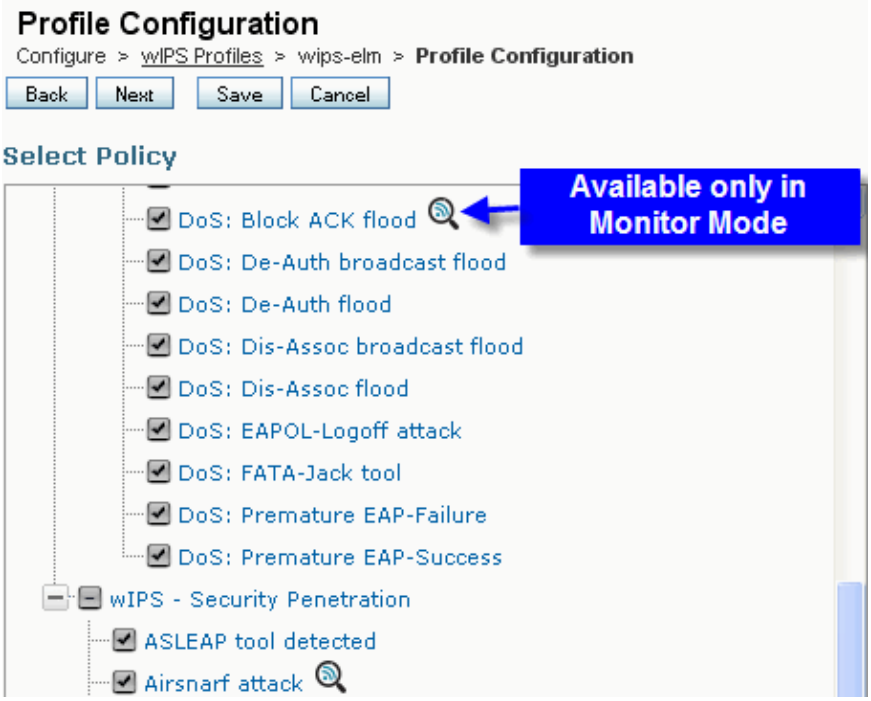
Table 1 − wIPS Signatures Support Matrix

Attacks Detected	ELM	MM
DoS Attack Against AP		
Association Flood	Y	Y
Association Table Overflow	Y	Y
Authentication Flood	Y	Y
EAPOL−Start attack	Y	Y
PS−Poll flood	Y	Y
Probe request flood	N	Y
Unauthenticated association	Y	Y
DoS Attack Against Infrastructure		
CTS flood	N	Y
Queensland University of Technology Exploit	N	Y
RF jamming	Y	Y
RTS flood	N	Y
Virtual Carrier attack	N	Y
DoS Attack Against Station		
Authentication−failure attack	Y	Y
Block ACK flood	N	Y
De−Auth broadcast flood	Y	Y
De−Auth flood	Y	Y

Dis−Assoc broadcast flood	Y	Y
Dis−Assoc flood	Y	Y
EAPOL−Logoff attack	Y	Y
FATA−Jack tool	Y	Y
Premature EAP−Failure	Y	Y
Premature EAP−Success	Y	Y
Security Penetration Attacks		
ASLEAP tool detected	Y	Y
Airsnarf attack	N	Y
ChopChop attack	Y	Y
Day−Zero attack by WLAN security anomaly	N	Y
Day−Zero attack by device security anomaly	N	Y
Device probing for APs	Y	Y
Dictionary attack on EAP methods	Y	Y
EAP attack against 802.1x authentication	Y	Y
Fake APs detected	Y	Y
Fake DHCP server detected	N	Y
FAST WEP crack tool detected	Y	Y
Fragmentation attack	Y	Y
Honeypot AP detected	Y	Y
Hotspotter tool detected	N	Y
Improper broadcast frames	N	Y
Malformed 802.11 packets detected	Y	Y
Man in the middle attack	Y	Y
Netstumbler detected	Y	Y
Netstumbler victim detected	Y	Y
PSPF violation detected	Y	Y
Soft AP or host AP detected	Y	Y
Spoofed MAC address detected	Y	Y
Suspicious after−hours traffic detected	Y	Y
Unauthorized association by vendor list	N	Y
Unauthorized association detected	Y	Y
Wellenreiter detected	Y	Y

Note: Adding CleanAir will also enable detection of non−802.11 attacks.

Figure 11 − WCS wIPS Profile View



In Figure 11, configure the wIPS profile from WCS, the icon indicates that the attack will be detected only when AP is in MM, while only best effort when in ELM.

Troubleshoot ELM

Check these items:

- Make sure NTP is configured.
- Make sure MSE time setting is in UTC.
- If the device group is not working, use overlay profile SSID with Any. Reboot the AP.
- Make sure licensing is configured (Currently ELM APs are using KAM licenses)
- If wIPS profiles are changed too often, synchronize the MSE−Controller again. Make sure the profile is active on WLC.
- Make sure WLC is part of MSE using MSE CLIs:

    1. SSH or telnet to your MSE.
    2. Execute **/opt/mse/wips/bin/wips_cli** − This console can be used to access to following commands to gather information regarding the state of the adaptive wIPS system.
    3. **show wlc all** Issue inside the wIPS console. This command is used to verify the controllers that are actively communicating with the wIPS service on the MSE. See Figure 12.

    Figure 12 − MSE CLI Verifying WLC Active with MSE wIPS Services

```
wIPS>show wlc all

WLC MAC              Profile             Profile
Status                  IP
Onx Status Status
-----------------------------------------------
-----------------------------------------------
----
00:21:55:06:F2:80    WCS-Default         Policy
active on controller     172.20.226.197
Active
```

- Make sure alarms are getting detected on MSE using MSE CLIs.

- **show alarm list** − Issue inside the wIPS console. This command is used to list the alarms currently contained within the wIPS service database. The key field is the unique hash key assigned to the specific alarm. The Type field is the type of alarm. This chart in Figure 13 shows a list of alarm IDs and descriptions:

Figure 13 − MSE CLI show alarm list Command

```
wIPS>show alarm list

Key        Type  Src MAC
LastTime              Active          First Time
-------------------------------------------
-------------------------------------------
89         89    00:00:00:00:00:00     2008/09/04
18:19:26  2008/09/07 02:16:58   1
65631      95    00:00:00:00:00:00     2008/09/04
17:18:31  2008/09/04 17:18:31   0
1989183    99    00:1A:1E:80:5C:40     2008/09/04
18:19:44  2008/09/04 18:19:44   0
```

The First Time and Last Time fields signify the timestamps when the alarm was detected; these are stored in UTC time. The Active field highlights if the alarm is currently detected.

- Clear the MSE Database.

- If you run into a situation where the MSE database is corrupt, or no other troubleshooting methods will work, it may be best to clear the database and start over.

Figure 14 − MSE services Command

```
1. /etc/init.d/msed stop
2. Remove the database using the command 'rm
/opt/mse/locserver/db/linux/server−eng.db'
3. /etc/init.d/msed start
```

Related Information

- **Cisco Wireless LAN Controller Configuration Guide, Release 7.0.116.0**
- **Cisco Wireless Control System Configuration Guide, Release 7.0.172.0**
- **Technical Support & Documentation − Cisco Systems**

Contacts & Feedback | Help | Site Map
© 2014 − 2015 Cisco Systems, Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.

Updated: Jan 14, 2015 Document ID: 113027