Adaptive wIPS ELM - Konfigurations- und Implementierungsleitfaden

Inhalt

Einleitung

Die Cisco Adaptive Wireless Intrusion Prevention System (wIPS)-Lösung verfügt über die Enhanced Local Mode (ELM)-Funktion, mit der Administratoren ihre bereitgestellten Access Points (APs) für umfassenden Schutz einsetzen können, ohne dass ein separates Overlay-Netzwerk erforderlich ist (Abbildung 1). Vor ELM und in der traditionellen adaptiven wIPS-Bereitstellung sind dedizierte MM-APs (Monitor Mode) erforderlich, um PCI-Compliance-Anforderungen zu erfüllen oder Schutz vor nicht autorisiertem Sicherheitszugriff, Eindringen und Angriffen zu bieten (Abbildung 2). ELM bietet ein vergleichbares Angebot, das die Implementierung von Wireless-Sicherheit vereinfacht und gleichzeitig die Investitions- und Betriebskosten senkt. Dieses Dokument konzentriert sich nur auf ELM und ändert keine bestehenden Vorteile der wIPS-Bereitstellung mit MM-APs.

Abbildung 1: Erweiterte AP-Bereitstellung im lokalen Modus

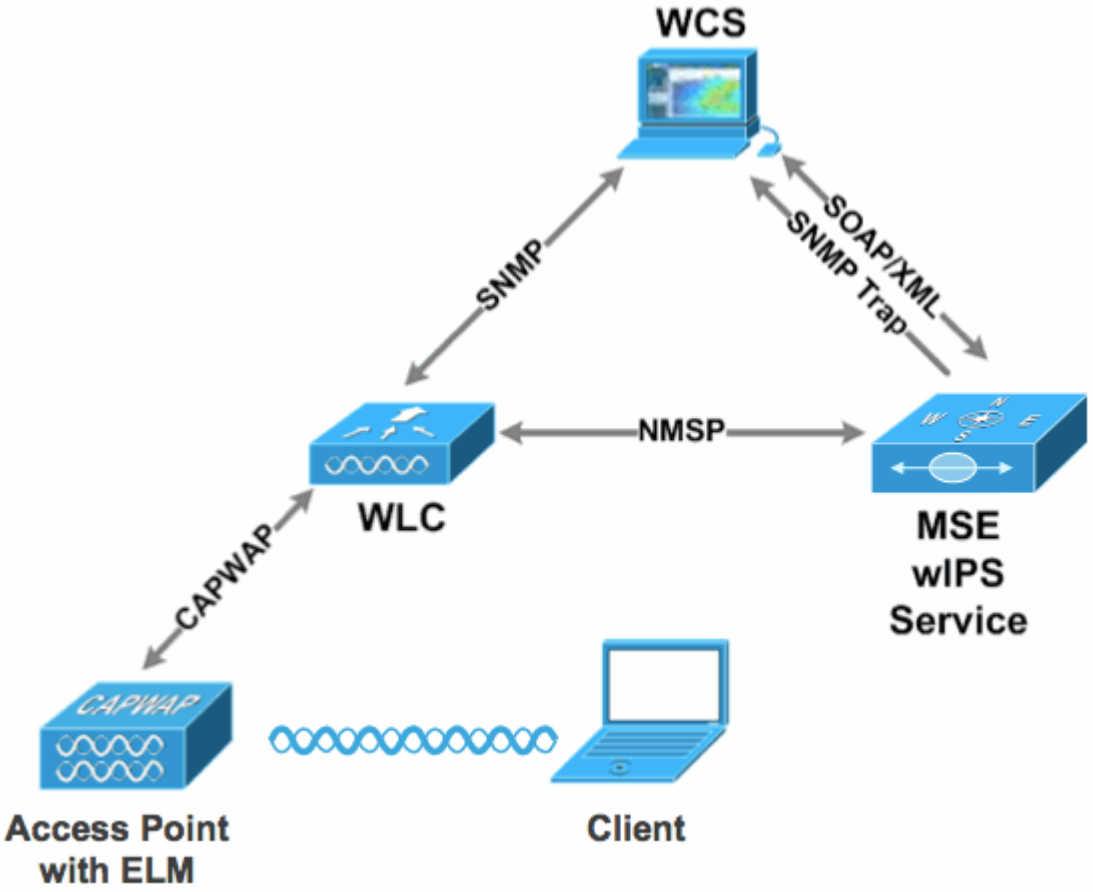
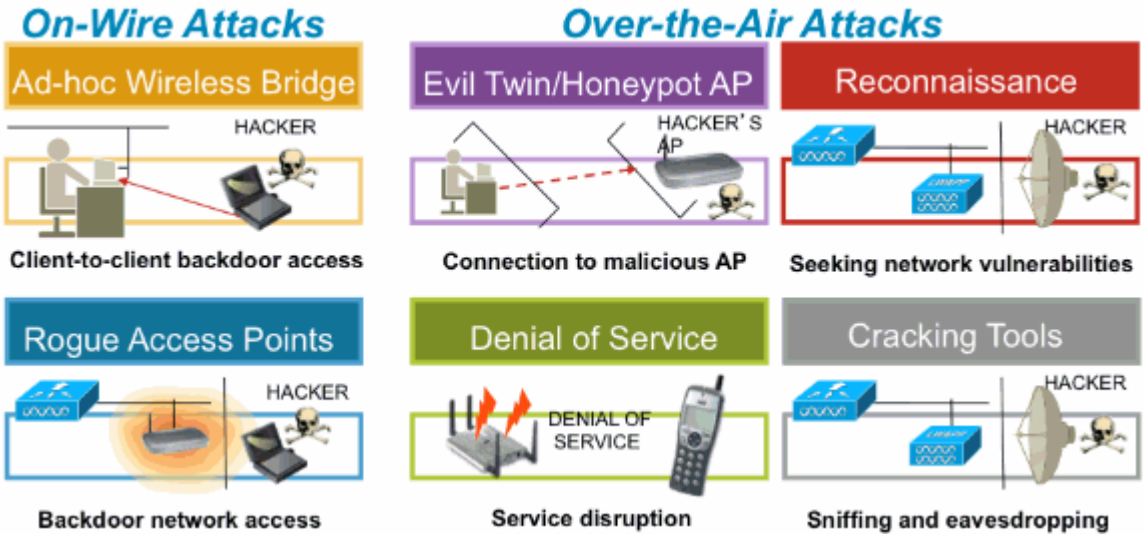


Abbildung 2: Wichtigste Wireless-Sicherheitsbedrohungen



Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Erforderliche ELM-Komponenten und Mindestcodeversionen

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

Unterstützende WLC-Plattformen

ELM wird auf den Plattformen WLC5508, WLC4400, WLC 2106, WLC2504, WiSM-1 und WiSM-2WLC unterstützt.

Unterstützende APs

ELM wird von 11n APs unterstützt, darunter 3500, 1250, 1260, 1040 und 1140.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

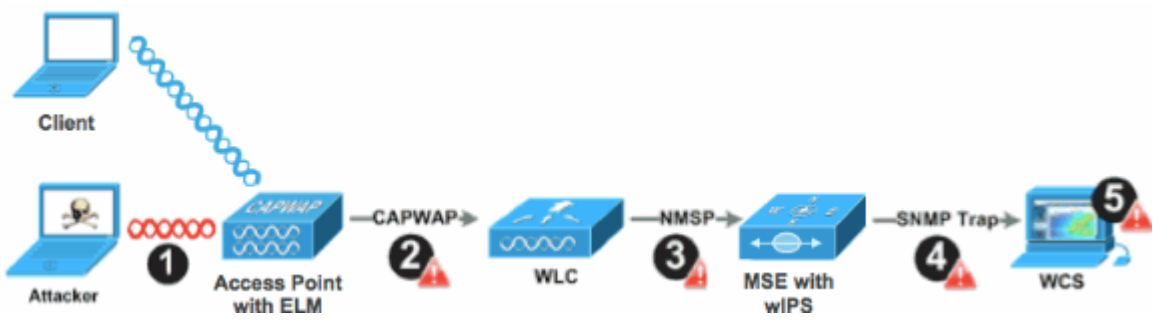
Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

ELM wIPS-Alarmablauf

Angriffe sind nur relevant, wenn sie auf vertrauenswürdigen Infrastruktur-APs stattfinden. Die ELM-APs erkennen den Controller und kommunizieren mit diesem und korrelieren mit der MSE, um Berichte an das WCS-Management zu senden. Abbildung 3 zeigt den Alarmverlauf aus Sicht eines Administrators:

1. Angriff auf ein Infrastrukturgerät ("vertrauenswürdiger" AP)
2. Erkennung am ELM-AP, der über CAPWAP an WLC übermittelt wurde
3. Transparente Weiterleitung an MSE über NMSP
4. Anmeldung bei wIPS-Datenbank auf MSE erfolgt über SNMP-Trap an WCS gesendet
5. Angezeigt bei WCS

Abbildung 3: Erkennung von Sicherheitsrisiken und Alarmverlauf



Überlegungen zur Bereitstellung von ELM

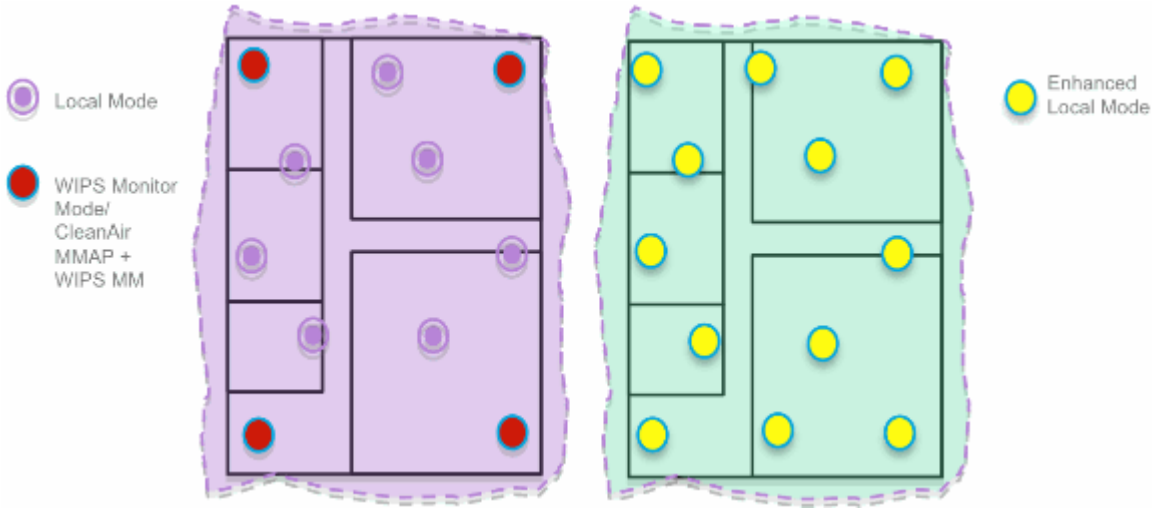
Cisco empfiehlt, dass durch die Aktivierung von ELM auf jedem AP im Netzwerk die meisten Sicherheitsanforderungen der Kunden erfüllt werden, wenn ein Netzwerk-Overlay und/oder Kosten in Betracht gezogen werden. Die primäre ELM-Funktion kann effektiv für On-Channel-Angriffe eingesetzt werden, ohne dass die Leistung von Daten-, Sprach- und Video-Clients und Services beeinträchtigt wird.

ELM und dediziertes MM

Abbildung 4 zeigt einen allgemeinen Kontrast zwischen den Standardbereitstellungen von wIPS MM APs und ELM. Der typische Abdeckungsbereich für beide Modi lässt sich wie folgt zusammenfassen:

- Dedizierter wIPS MM AP deckt in der Regel 15.000-35.000 Quadratfuß ab
- Client-bedienende AP deckt in der Regel zwischen 3.000 und 5.000 Quadratfuß ab

Abbildung 4: Overlay von MM und allen ELM-APs



Für die herkömmliche adaptive wIPS-Bereitstellung empfiehlt Cisco ein Verhältnis von 1 MM AP zu 5 APs im lokalen Modus, das je nach Netzwerkdesign und fachkundiger Unterstützung variieren kann, um eine optimale Abdeckung zu gewährleisten. Durch die Berücksichtigung von ELM aktiviert der Administrator einfach die ELM-Softwarefunktion für alle vorhandenen APs und fügt MM wIPS-Operationen effektiv zum lokalen Datenbereitstellungsmodus AP hinzu, während die Leistung aufrechterhalten wird.

On-Channel- und Off-Channel-Leistung

Ein MM-AP verbraucht 100 % der Funkzeit zum Scannen aller Kanäle, da er keine WLAN-Clients bedient. Die primäre Funktion von ELM ist effektiv für On-Channel-Angriffe, ohne die Leistung von Daten-, Sprach- und Video-Clients und -Services zu beeinträchtigen. Der Hauptunterschied besteht darin, dass bei der Abtastung außerhalb des Kanals im lokalen Modus variiert wird. Je nach Aktivität ermöglicht die Abtastung außerhalb des Kanals eine minimale Verweilzeit, um genügend verfügbare Informationen zur Klassifizierung und Bestimmung des Angriffs zu sammeln. Ein Beispiel hierfür sind zugewiesene Sprach-Clients, bei denen das RRM-Scanning des Access Points zurückgestellt wird, bis die Verknüpfung des Sprach-Clients aufgehoben wird, um sicherzustellen, dass der Service nicht beeinträchtigt wird. Aus diesem Grund gilt die ELM-Erkennung außerhalb des Kanals als bestmöglicher Ansatz. Benachbarte ELM-APs, die auf allen, Landes- oder DCA-Kanälen betrieben werden, erhöhen die Effektivität. Daher wird empfohlen, ELM für eine maximale Schutzabdeckung auf jedem lokalen Modus-AP zu aktivieren. Wenn dedizierte

Scans auf allen Kanälen in Vollzeit erforderlich sind, wird empfohlen, MM-APs bereitzustellen.

Diese Punkte zeigen die Unterschiede zwischen dem lokalen Modus und den MM-APs auf:

- AP im lokalen Modus - Bietet WLAN-Clients Zeitaufteilung für Off-Channel-Scanning, hört 50 ms auf jedem Kanal ab und bietet konfigurierbare Scanfunktionen für alle Kanäle/Länder/DCA.
- AP im Überwachungsmodus - Keine WLAN-Clients, die nur für Scans vorgesehen sind, lauschen 1,2 Sekunden auf jedem Kanal und scannen alle Kanäle.

ELM über WAN-Links

Cisco hat große Anstrengungen unternommen, um die Funktionen in anspruchsvollen Szenarien zu optimieren, wie z. B. bei der Bereitstellung von ELM APs über WAN-Verbindungen mit niedriger Bandbreite. Die ELM-Funktion beinhaltet eine Vorverarbeitung zur Bestimmung von Angriffssignaturen am WAP und ist für langsame Verbindungen optimiert. Als Best Practices wird empfohlen, die Baseline zu testen und zu messen, um die Leistung mit ELM über WAN zu validieren.

CleanAir-Integration

Die ELM-Funktion ergänzt CleanAir-Vorgänge mit ähnlicher Leistung und ähnlichen Vorteilen wie die Bereitstellung von MM-APs durch die folgenden spektrumsbezogenen Vorteile von CleanAir:

- Dedizierte RF-Intelligenz auf Chip-Ebene
- Spektrumerkennung, Selbstreparatur und Selbstoptimierung
- Erkennung und Behebung von Channel-Bedrohungen und -Interferenzen (nicht standardkonform)
- Keine Wi-Fi-Erkennung wie Bluetooth, Mikrowelle, schnurlose Telefone usw.
- Erkennung und Lokalisierung von DOS-Angriffen auf der Funkschicht, z. B. von Funkstörern

ELM - Funktionen und Vorteile

- Adaptives wIPS-Scanning von Daten für lokale und H-REAPs
- Schutz ohne separates Overlay-Netzwerk
- Verfügbar als kostenloser Software-Download für bestehende wIPS-Kunden
- Unterstützt PCI-Konformität für WLANs
- Vollständige Erkennung von 802.11- und Nicht-802.11-Angriffen
- Zusätzliche Forensik- und Berichterstellungsfunktionen
- Integration mit vorhandenem CUWM- und WLAN-Management
- Flexibilität zum Einrichten integrierter oder dedizierter MM-APs
- Die Vorverarbeitung an den APs minimiert das Daten-Backhaul (d. h. es funktioniert über Verbindungen mit sehr niedriger Bandbreite).

- Geringe Auswirkungen auf die bereitstellenden Daten

ELM-Lizenzierung

ELM wIPS fügt der Bestellung eine neue Lizenz hinzu:

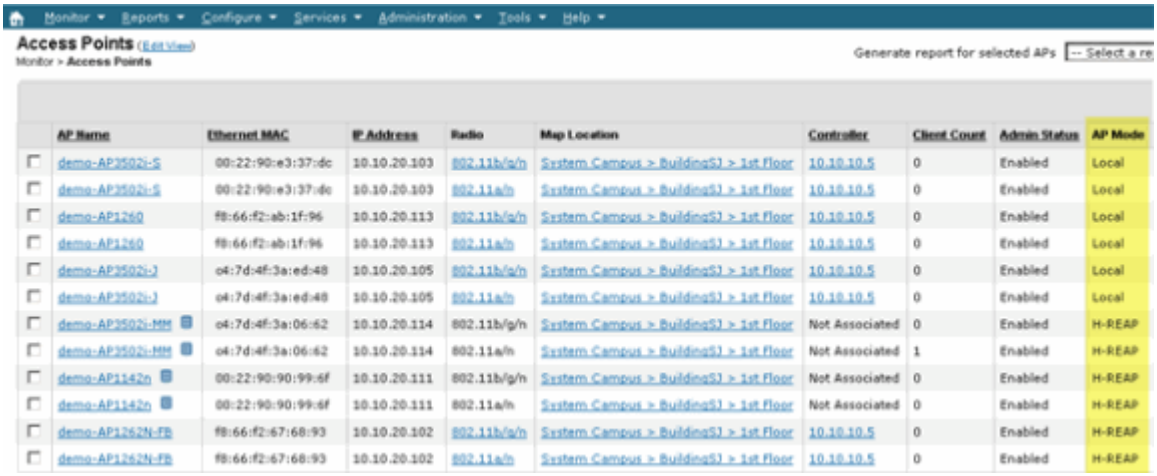
- AIR-LM-WIPS-xx - Cisco ELM wIPS-Lizenz
- AIR-WIPS-AP-xx - Cisco Wireless wIPS-Lizenz

Zusätzliche ELM-Lizenzhinweise:

- Wenn bereits wIPS MM AP-Lizenz-SKUs installiert sind, können diese Lizenzen auch für ELM APs verwendet werden.
- wIPS- und ELM-Lizenzen werden zusammen auf die Plattformlizenzlimits für die wIPS-Engine angerechnet; 2.000 APs auf dem 3310 bzw. 3.000 APs auf dem 335x.
- Die Testlizenz umfasst 10 APs für wIPS und 10 APs für einen Zeitraum von bis zu 60 Tagen für ELM. Vor der ELM-Testlizenz waren bis zu 20 WIPS-MM-APs zulässig. Die Mindestanforderung an Softwareversionen, die ELM unterstützen, muss erfüllt werden.

ELM mit WCS konfigurieren

Abbildung 5: Konfigurieren von ELM mit WCS

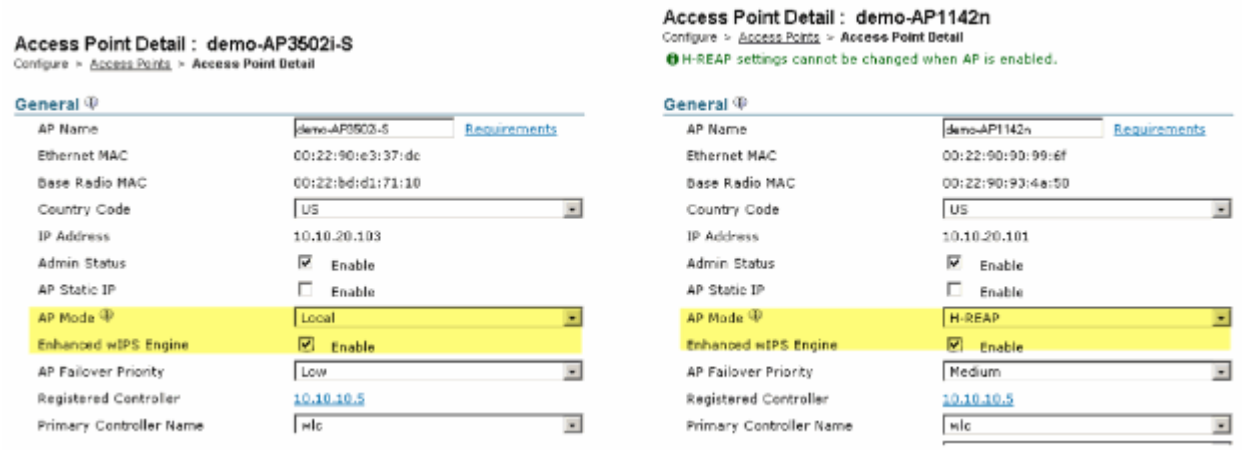


1. Deaktivieren Sie in WCS die 802.11b/g- und 802.11a-Funkmodule des AP, bevor Sie die "Enhanced wIPS Engine" aktivieren.

   Hinweis: Alle verbundenen Clients werden getrennt und treten erst bei, wenn die Funkmodule aktiviert sind.

2. Konfigurieren Sie einen AP, oder verwenden Sie eine WCS-Konfigurationsvorlage für mehrere Lightweight APs. Siehe Abbildung 6.

   Abbildung 6: Aktivieren des Enhanced wIPS Engine (ELM)-Untermodus



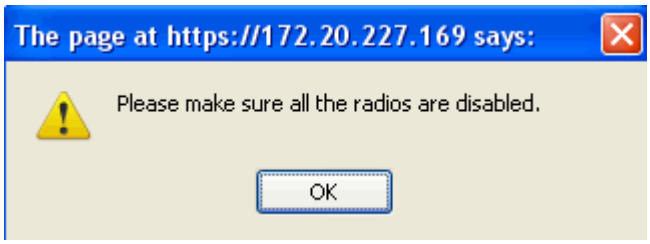
3. Wählen Sie **Enhanced wIPS Engine aus**, und klicken Sie auf **Save**.

   a. Die Aktivierung der erweiterten wIPS-Engine führt nicht zum Neustart des Access Points.

   b. H-REAP wird unterstützt. Aktivieren Sie dieses ebenso wie für den AP im lokalen Modus.

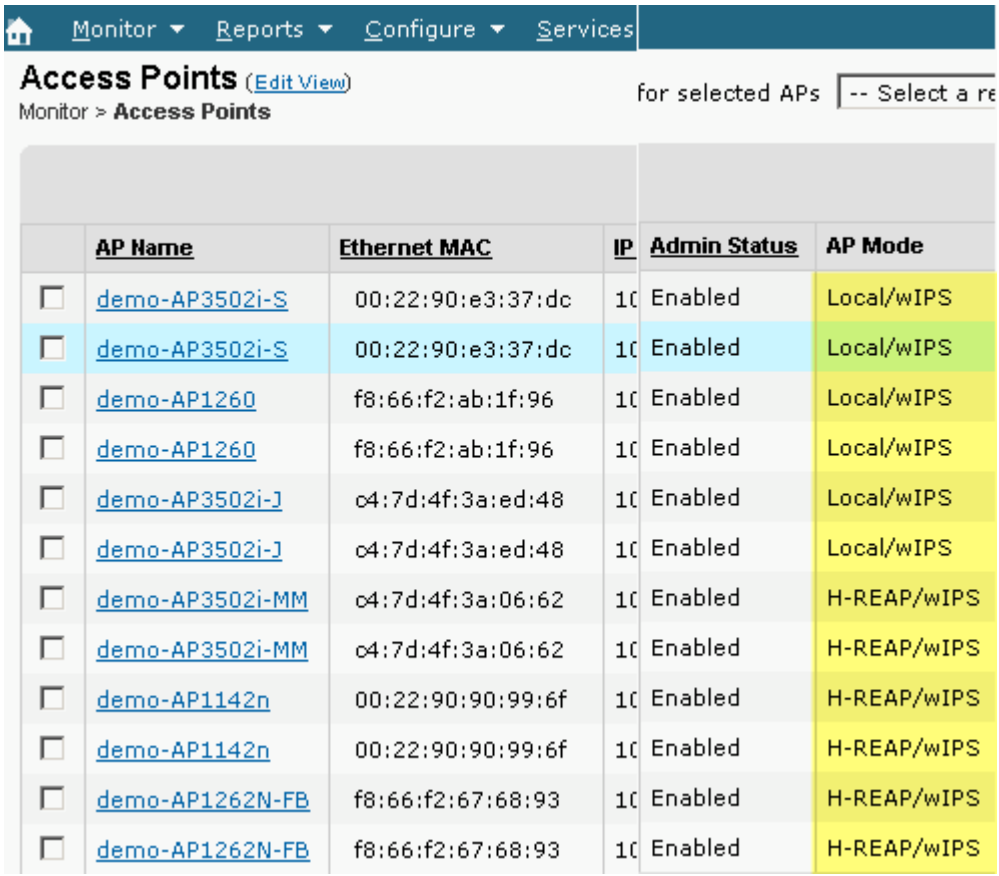
   Hinweis: Wenn eines der Funkmodule dieses Access Points aktiviert ist, ignoriert WCS die Konfiguration und löst den Fehler in Abbildung 7 aus.

   Abbildung 7: WCS-Erinnerung zum Deaktivieren von AP-Funkmodulen vor dem Aktivieren von ELM



4. Die erfolgreiche Konfiguration kann durch Beobachtung der Änderung des AP-Modus von "Local or H-REAP" zu "**Local/wIPS**" oder "**H-REAP/wIPS**" überprüft werden. Siehe Abbildung 8.

   Abbildung 8: WCS zeigt AP-Modus für wIPS mit lokalem und/oder H-REAP an



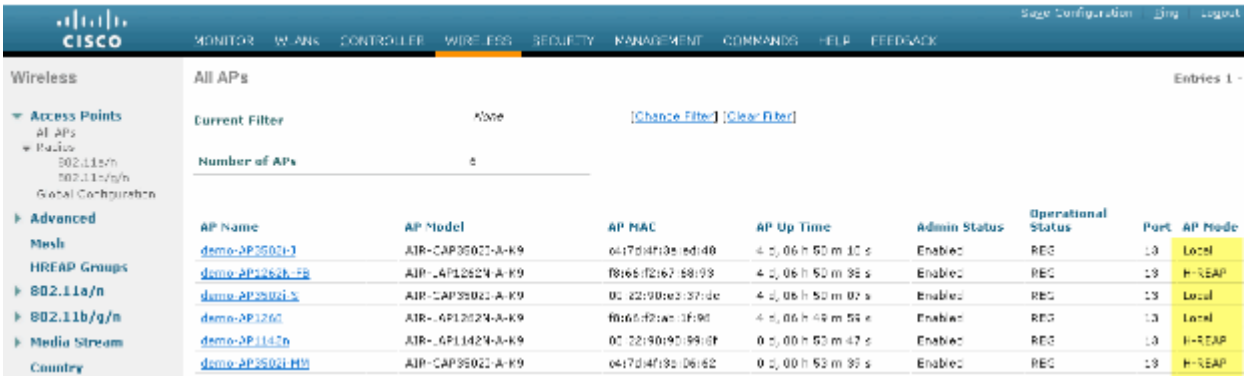
5. Aktivieren Sie die Funkmodule, die in Schritt 1 deaktiviert wurden.

6. Erstellen Sie das wIPS-Profil, und schieben Sie es auf den Controller, damit die Konfiguration abgeschlossen werden kann.

   Hinweis: Vollständige Konfigurationsinformationen zu wIPS finden Sie im Cisco Adaptive wIPS Deployment Guide.

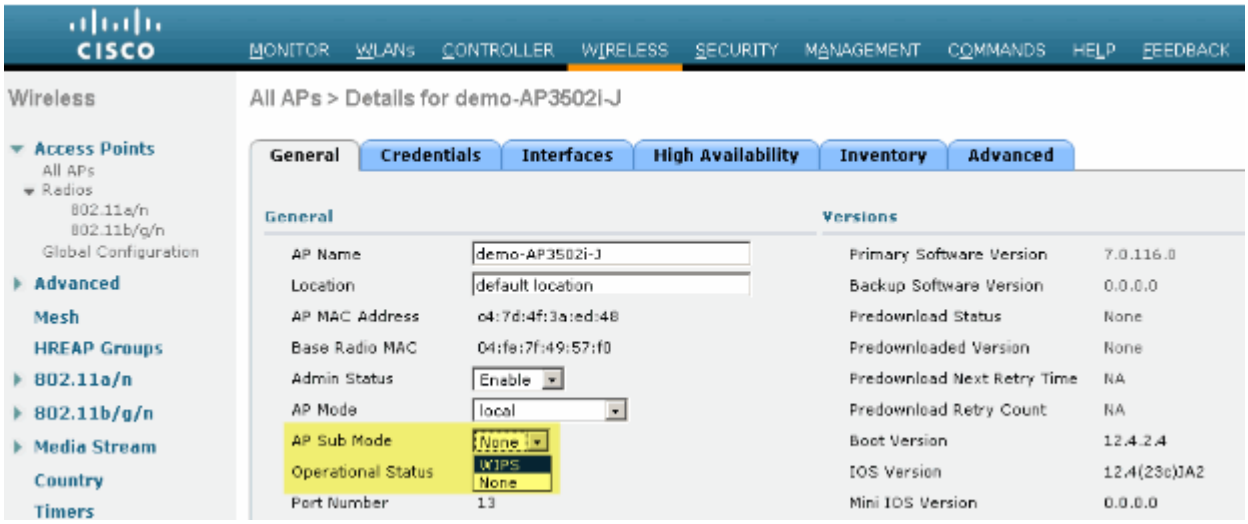
Konfiguration von WLC

Abbildung 9: Konfigurieren von ELM mit WLC



1. Wählen Sie auf der Registerkarte **Wireless** einen Access Point aus.

Abbildung 10: WLC Ändern des AP-Submodus in Include wIPS ELM



2. Wählen Sie aus dem Dropdown-Menü AP Sub Mode (AP-Untermodus) die Option **wIPS** aus (Abbildung 10).

3. Übernehmen Sie die Konfiguration, und speichern Sie sie.

Hinweis: Damit die ELM-Funktionalität funktioniert, sind MSE und WCS mit wIPS-Lizenzierung erforderlich. Durch eine Änderung des AP-Submodus von WLC allein wird ELM nicht aktiviert.

In ELM erkannte Angriffe

Tabelle 1: Unterstützungsmatrix für wIPS-Signaturen

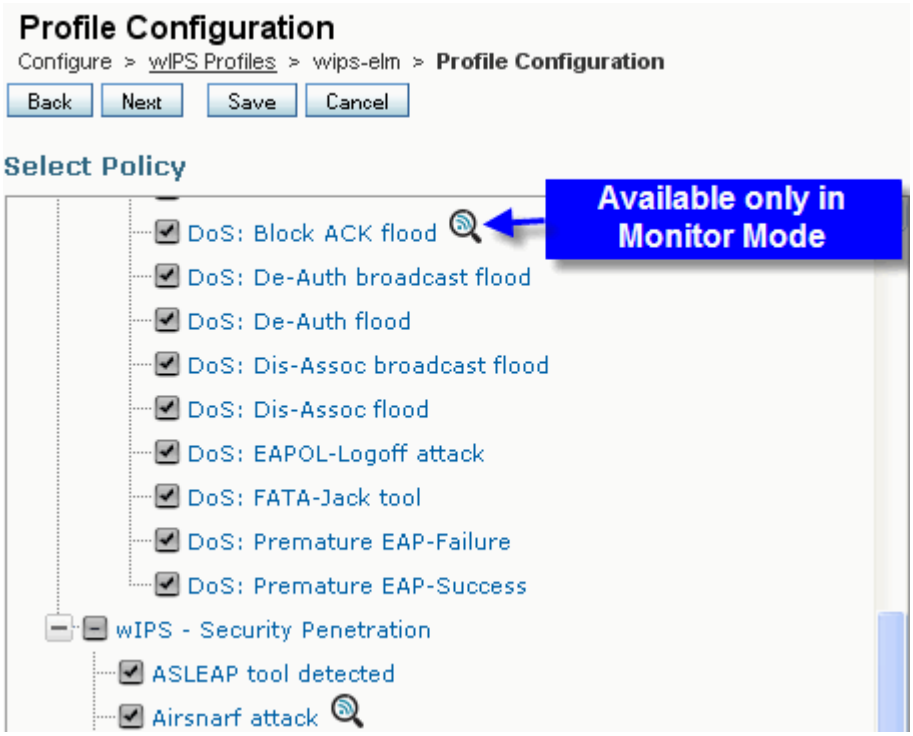
Erkannte Angriffe	ELM	MM
DoS-Angriff gegen AP		
Vereinsflut	Y	Y
Überlauf der Zuordnungstabelle	Y	Y
Authentifizierungs-Flood	Y	Y
EAPOL-Start-Angriff	Y	Y
PS-Umfrage Flut	Y	Y
Flutwelle der Anfrage	N	Y
Nicht authentifizierte Zuordnung	Y	Y
DoS-Angriff auf Infrastruktur		
CTS-Flood	N	Y
Technologischer Exploit der Universität Queensland	N	Y
HF-Störsender	Y	Y
RTS-Flood	N	Y
Virtual Carrier-Angriff	N	Y
DoS-Angriff auf Station		
Authentifizierungsfehler-Angriff	Y	Y

Block ACK Flood	N	Y
De-Auth-Sendeflut	Y	Y
De-Auth-Flut	Y	Y
Dis-Assoc-Broadcast-Flood	Y	Y
Dis-Assoc-Flut	Y	Y
EAPOL-Logoff-Angriff	Y	Y
FATA-Jack-Tool	Y	Y
Vorzeitiger EAP-Ausfall	Y	Y
Vorzeitiger EAP-Erfolg	Y	Y
Eindringungsangriffe auf das Netzwerk		
ASLEAP-Tool erkannt	Y	Y
Luftangriff	N	Y
ChopChop-Angriff	Y	Y
Day-Zero-Angriff durch WLAN-Sicherheitsanomalien	N	Y
Day-Zero-Angriff nach Gerätesicherheitsanomalien	N	Y
Geräteerkennung für APs	Y	Y
Wörterbuchangriff auf EAP-Methoden	Y	Y
EAP-Angriff auf 802.1x-Authentifizierung	Y	Y
Gefälschte APs erkannt	Y	Y
Gefälschter DHCP-Server erkannt	N	Y
FAST WEP-Cracktool erkannt	Y	Y
Fragmentierungsangriff	Y	Y
Honeypot-AP erkannt	Y	Y
Hotspotter-Tool erkannt	N	Y
Unzulässige Broadcastrahmen	N	Y
802.11-Pakete mit Fehlern erkannt	Y	Y
Mann im Mittelangriff	Y	Y
Netstumbler erkannt	Y	Y
Netstumbler-Opfer entdeckt	Y	Y
PSPF-Verletzung erkannt	Y	Y
Soft-AP oder Host-AP erkannt	Y	Y
Gefälschte MAC-Adresse erkannt	Y	Y
Verdächtiger Datenverkehr nach Geschäftsschluss erkannt	Y	Y
Nicht autorisierte Zuordnung nach Anbieterliste	N	Y
Nicht autorisierte Zuordnung erkannt	Y	Y

Wellenreiter erkannt	Y	Y

Hinweis: Durch Hinzufügen von CleanAir können auch nicht 802.11-konforme Angriffe erkannt werden.

Abbildung 11: WCS-wIPS-Profilansicht



In Abbildung 11, Konfigurieren des wIPS-Profils von WCS, zeigt das Symbol an, dass der Angriff nur erkannt wird, wenn der Access Point in MM ist, während nur bestmögliche Leistung, wenn der Access Point in ELM ist.

ELM-Fehlerbehebung

Überprüfen Sie diese Punkte:

- Vergewissern Sie sich, dass das NTP konfiguriert ist.
- Stellen Sie sicher, dass die MSE-Zeiteinstellung in UTC festgelegt ist.
- Wenn die Gerätegruppe nicht funktioniert, verwenden Sie die SSID des Overlay-Profils mit Any (Beliebig). Starten Sie den Access Point neu.
- Stellen Sie sicher, dass die Lizenzierung konfiguriert ist (derzeit verwenden ELM APs KAM-Lizenzen).
- Wenn wIPS-Profile zu häufig geändert werden, synchronisieren Sie den MSE-Controller erneut. Stellen Sie sicher, dass das Profil auf dem WLC aktiv ist.
- Stellen Sie mithilfe der MSE-CLIs sicher, dass der WLC Teil der MSE ist:

    1. SSH oder Telnet an Ihre MSE senden.
    2. Execute/**opt/mse/wips/bin/wips_cli** - Diese Konsole kann verwendet werden, um auf die folgenden Befehle zuzugreifen und Informationen zum Status des adaptiven wIPS-Systems zu

sammeln.

3. **show wlc all** - Problem in der wIPS-Konsole. Mit diesem Befehl werden die Controller überprüft, die aktiv mit dem wIPS-Service auf der MSE kommunizieren. Siehe Abbildung 12.

   Abbildung 12: MSE-CLI zur Überprüfung des aktiven WLC mit MSE wIPS-Services

```
<#root>

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
```

- Stellen Sie mithilfe von MSE-CLIs sicher, dass auf der MSE Alarme erkannt werden.
  - **show alarm list** - Problem in der wIPS-Konsole. Mit diesem Befehl werden die derzeit in der wIPS-Dienstdatenbank enthaltenen Alarme aufgelistet. Das Schlüsselfeld ist der eindeutige Hashschlüssel, der dem jeweiligen Alarm zugewiesen ist. Das Feld Typ gibt den Typ des Alarms an. Das Diagramm in Abbildung 13 zeigt eine Liste der Alarm-IDs und -Beschreibungen:

    Abbildung 13: Befehl "MSE CLI show alarm list"

```
<#root>

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
```

    Die Felder "First Time" (Erstes Datum) und "Last Time" (Letztes Datum) geben die Zeitstempel an, nach denen der Alarm erkannt wurde. Diese werden in UTC-Zeit gespeichert. Das Feld Active (Aktiv) hebt hervor, ob der Alarm derzeit erkannt wird.

- Löschen der MSE-Datenbank
    - Wenn die MSE-Datenbank beschädigt ist oder keine andere Fehlerbehebungsmethode funktioniert, ist es möglicherweise am besten, die Datenbank zu löschen und von vorne zu beginnen.

      Abbildung 14: Befehl "MSE services"

```
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
```

Zugehörige Informationen

- **Konfigurationsleitfaden für Cisco Wireless LAN Controller, Version 7.0.116.0**
- **Konfigurationsanleitung für das Cisco Wireless Control System, Version 7.0.172.0**
- **Technischer Support und Dokumentation für Cisco Systeme**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.