Guía de configuración e implementación de wIPS ELM adaptable

Contenido

Introducción

La solución Cisco Adaptive Wireless Intrusion Prevention System (wIPS) incorpora la función Enhanced Local Mode (ELM), que permite a los administradores utilizar sus puntos de acceso (AP) implementados para proporcionar una protección completa sin necesidad de una red superpuesta independiente (Figura 1). Antes del ELM y en la implementación wIPS adaptable tradicional, se necesitan puntos de acceso de modo de monitor dedicado (MM) para satisfacer las necesidades de cumplimiento de PCI o de protección contra el acceso de seguridad, la penetración y los ataques no autorizados (Figura 2). ELM proporciona con eficacia una oferta comparable que facilita la implementación de la seguridad inalámbrica a la vez que reduce los costes de CapEx y OpEx. Este documento solo se centra en el ELM y no modifica ninguna ventaja de implementación wIPS existente con los AP MM.

Figura 1: Implementación mejorada del punto de acceso de modo local

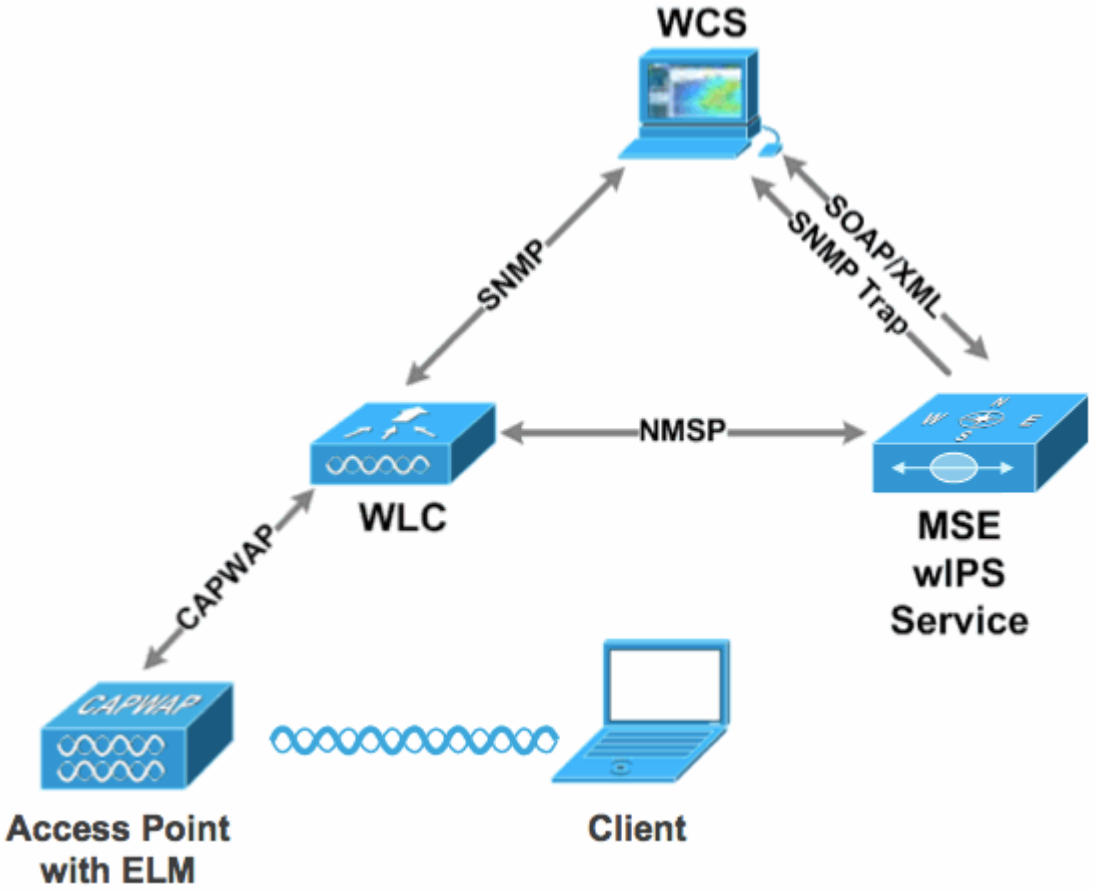
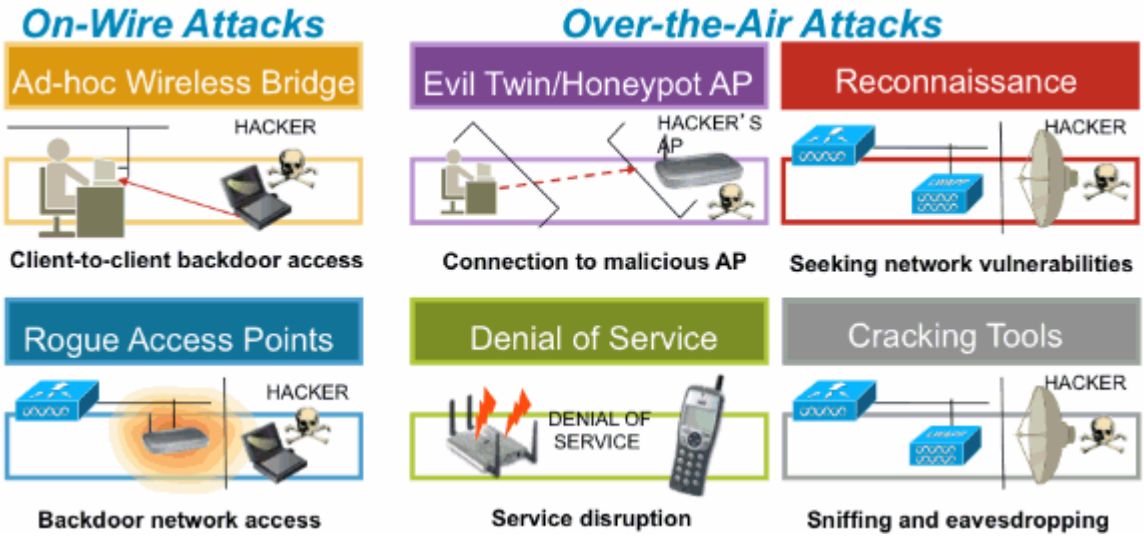


Figura 2: Principales amenazas para la seguridad inalámbrica



Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Componentes requeridos del ELM y versiones de código mínimo

- Controlador de LAN inalámbrica (WLC): versión 7.0.116.xx o posterior
- AP - Versión 7.0.116.xx o posterior
- Wireless Control System (WCS), versión 7.0.172.xx o posterior
- Mobility Services Engine, versión 7.0.201.xx o posterior

Plataformas WLC compatibles

ELM es compatible con las plataformas WLC5508, WLC4400, WLC 2106, WLC2504, WiSM-1 y WiSM-2WLC.

AP compatibles

ELM es compatible con 11n AP, incluidos 3500, 1250, 1260, 1040 y 1140.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Convenciones

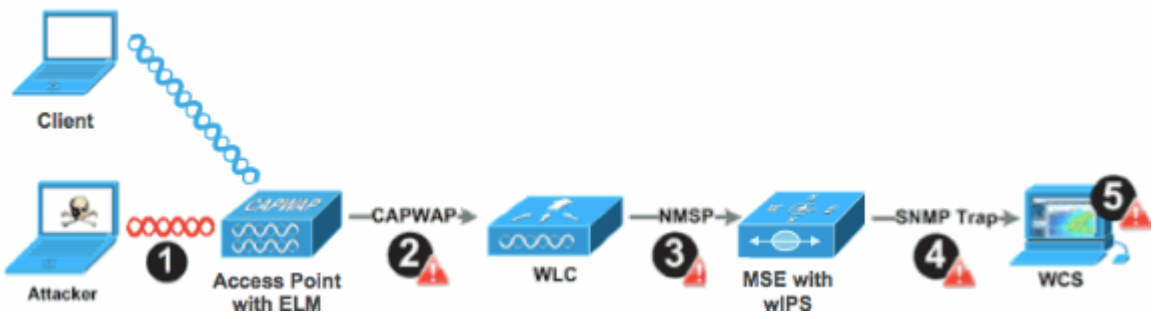
Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Flujo de alarmas wIPS de ELM

Los ataques solo son relevantes cuando se producen en puntos de acceso de infraestructura de confianza. Los AP del ELM detectarán y se comunicarán con el controlador y se correlacionarán con el MSE para informar con la administración del WCS. La Figura 3 proporciona el flujo de alarma desde el punto de vista de un administrador:

1. Ataque lanzado contra un dispositivo de infraestructura (punto de acceso "fiable")
2. Detectado en el AP del ELM comunicado a través de CAPWAP al WLC
3. Se pasa de forma transparente a MSE mediante NMSP
4. Conectado a la base de datos wIPS en MSE Enviado a WCS a través de una trampa SNMP
5. Mostrado en WCS

Figura 3: Detección de amenazas y flujo de alarmas



Consideraciones de implementación para ELM

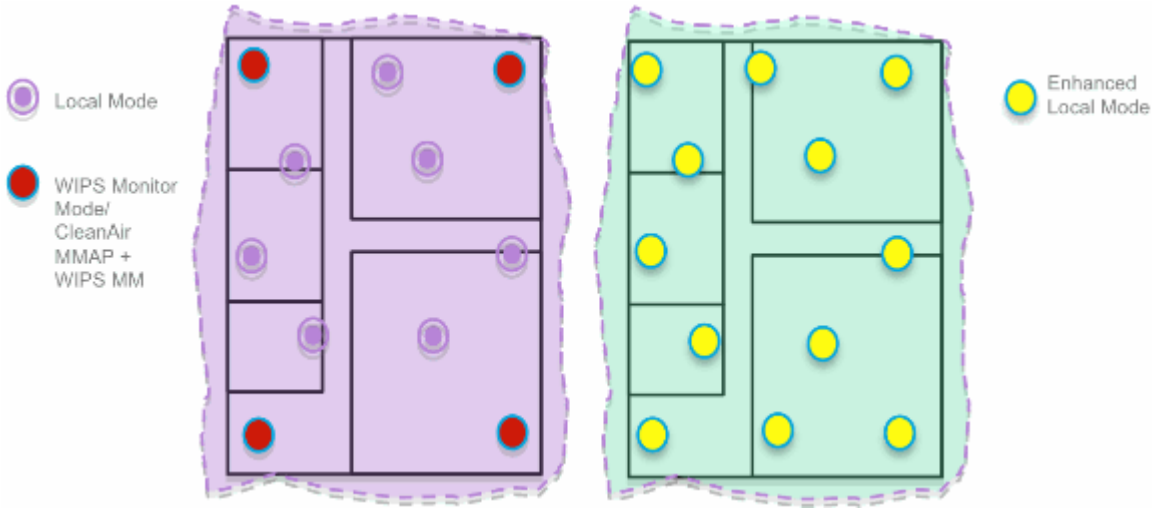
Cisco recomienda que, al habilitar el ELM en cada punto de acceso de la red, se satisfagan la mayoría de las necesidades de seguridad de los clientes cuando se tenga en cuenta una superposición o los costes de la red. La función principal del ELM funciona de forma eficaz para los ataques en el canal, sin poner en peligro el rendimiento de los clientes y servicios de datos, voz y vídeo.

ELM frente a MM dedicado

La figura 4 proporciona un contraste general entre las implementaciones estándar de AP MM wIPS y ELM. En revisión, el rango de cobertura típico para ambos modos sugiere:

- El punto de acceso MM wIPS dedicado cubre normalmente entre 15 000 y 35 000 pies cuadrados
- El punto de acceso de servicio al cliente normalmente cubrirá de 3000 a 5000 pies cuadrados

Figura 4: Superposición de MM frente a todos los AP de ELM



En la implementación wIPS adaptable tradicional, Cisco recomienda una proporción de 1 MM AP por cada 5 AP de modo local, que también puede variar en función del diseño de la red y de la orientación de los expertos para obtener una mejor cobertura. Al considerar el ELM, el administrador simplemente habilita la función del software del ELM para todos los AP existentes, agregando eficazmente las operaciones del wIPS del MM al AP local del modo de servicio de datos mientras que mantiene el rendimiento.

Rendimiento dentro y fuera del canal

Un AP MM utiliza el 100% del tiempo de la radio para escanear todos los canales, ya que no sirve a ningún cliente WLAN. La función principal de ELM funciona de forma eficaz para los ataques en el canal, sin poner en peligro el rendimiento de los clientes y servicios de datos, voz y vídeo. La diferencia principal radica en el modo local, que varía en función del análisis fuera del canal; en función de la actividad, el análisis fuera del canal proporciona un tiempo de permanencia mínimo para recopilar la información suficiente disponible para clasificar y determinar el ataque. Un ejemplo puede ser con los clientes de voz que están asociados y donde el escaneo RRM del AP se aplaza hasta que el cliente de voz se desasocie para asegurarse de que el servicio no se vea afectado. A este respecto, se considera que la detección del ELM fuera del canal es el mejor esfuerzo. Los AP de ELM vecinos que funcionan en todos los canales, país o DCA aumentan la eficacia, de ahí la recomendación de habilitar el ELM en cada AP de modo local para una cobertura de protección máxima. Si el requisito es para el escaneo dedicado en todos los canales a tiempo

completo, la recomendación será implementar APs MM.

Estos puntos revisan las diferencias del modo local y los AP MM:

- AP de modo local: sirve a los clientes WLAN con exploración fuera del canal dividida en el tiempo, escucha durante 50 ms en cada canal y ofrece exploración configurable para todos los canales/país/DCA.
- AP de modo monitor: no sirve a clientes WLAN, dedicados únicamente al escaneo, escucha 1.2 s en cada canal y escanea todos los canales.

ELM a través de enlaces WAN

Cisco ha realizado grandes esfuerzos para optimizar las funciones en situaciones desafiantes, como la implementación de AP de ELM a través de enlaces WAN de ancho de banda bajo. La función del ELM implica un procesamiento previo para determinar las firmas de ataque en el AP y está optimizada para funcionar en links lentos. Como prácticas recomendadas, se recomienda probar y medir la línea de base para validar el rendimiento con ELM sobre WAN.

Integración de CleanAir

La función ELM complementa enormemente las operaciones de CleanAir con un rendimiento y unas ventajas similares a los de la implementación de puntos de acceso MAP con estas ventajas existentes de CleanAir con reconocimiento del espectro:

- Inteligencia de radiofrecuencia dedicada a nivel de silicio
- Detección del espectro, reparación y optimización automáticas
- Mitigación y detección de interferencias y amenazas de canal no estándar
- Detección de dispositivos que no sean Wi-Fi, como Bluetooth, microondas, teléfonos inalámbricos, etc.
- Detecte y localice ataques DOS de capa de RF, como bloqueadores de RF

Características y ventajas del ELM

- Análisis wIPS adaptable en los datos que sirven a los puntos de acceso locales y H-REAP
- Protección sin necesidad de una red superpuesta independiente
- Disponible como descarga de software gratuita para clientes existentes de wIPS
- Admite compatibilidad con PCI para las redes LAN inalámbricas
- Detección completa de ataques conforme a 802.11 y 802.11 no relacionados
- Añade funciones de diagnóstico y de generación de informes
- Se integra con la gestión existente de CUWM y WLAN
- Flexibilidad para establecer puntos de acceso MM integrados o dedicados

- El preprocesamiento en los puntos de acceso minimiza la red de retorno de datos (es decir, funciona en enlaces de ancho de banda muy bajo)
- Bajo impacto en los datos de servicio

Licencias del ELM

ELM wIPS agrega una nueva licencia al pedido:

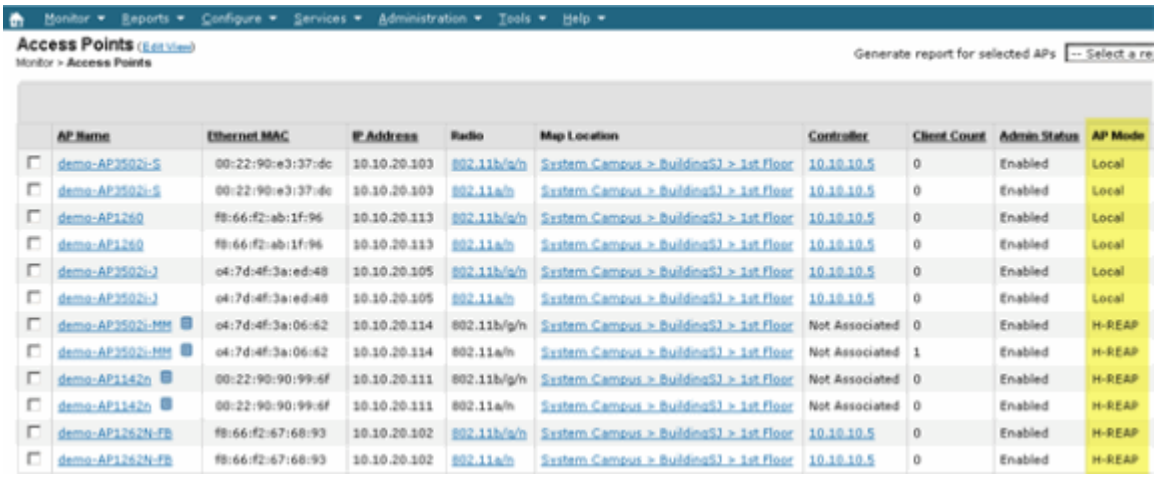
- AIR-LM-WIPS-xx: licencia wIPS del ELM de Cisco
- AIR-WIPS-AP-xx: licencia inalámbrica wIPS de Cisco

Notas de licencia del ELM adicionales:

- Si las SKU de licencias de AP MM wIPS ya están instaladas, dichas licencias también se pueden utilizar para los AP de ELM.
- Las licencias wIPS y las licencias ELM cuentan conjuntamente para los límites de licencia de plataforma para el motor wIPS; 2000 AP en 3310 y 3000 AP en 335x, respectivamente.
- La licencia de evaluación incluirá 10 puntos de acceso para wIPS y 10 para ELM durante un período de hasta 60 días. Antes del ELM, la licencia de evaluación permitía hasta 20 puntos de acceso wIPS MM. Se deben cumplir los requisitos mínimos de las versiones de software compatibles con ELM.

Configuración del ELM con WCS

Figura 5: Uso de WCS para configurar el ELM

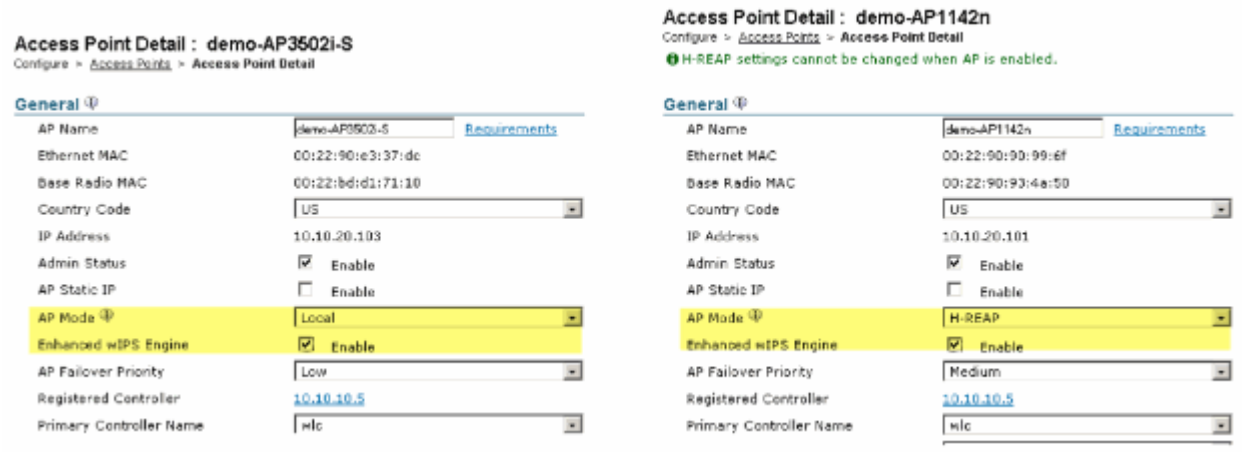


1. Desde WCS, desactive las radios 802.11b/g y 802.11a del punto de acceso antes de activar el "motor wIPS mejorado".

   Nota: se desconectarán todos los clientes asociados y no se unirán hasta que se habiliten las radios.

2. Configure un AP o utilice una plantilla de configuración de WCS para varios AP ligeros. Consulte la Figura 6.

   Figura 6: Submodo Habilitar motor wIPS mejorado (ELM)



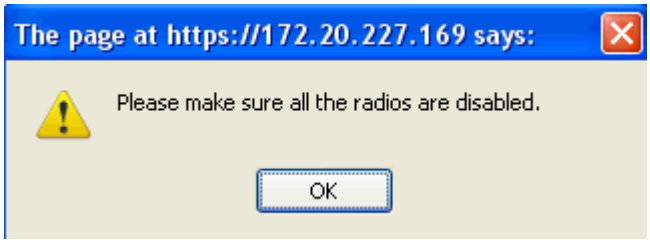
3. Elija **Enhanced wIPS Engine** y haga clic en **Save**.

    a. La activación del motor wIPS mejorado no hará que el AP se reinicie.

    b. H-REAP es compatible; habilite de la misma manera que para el AP de modo local.

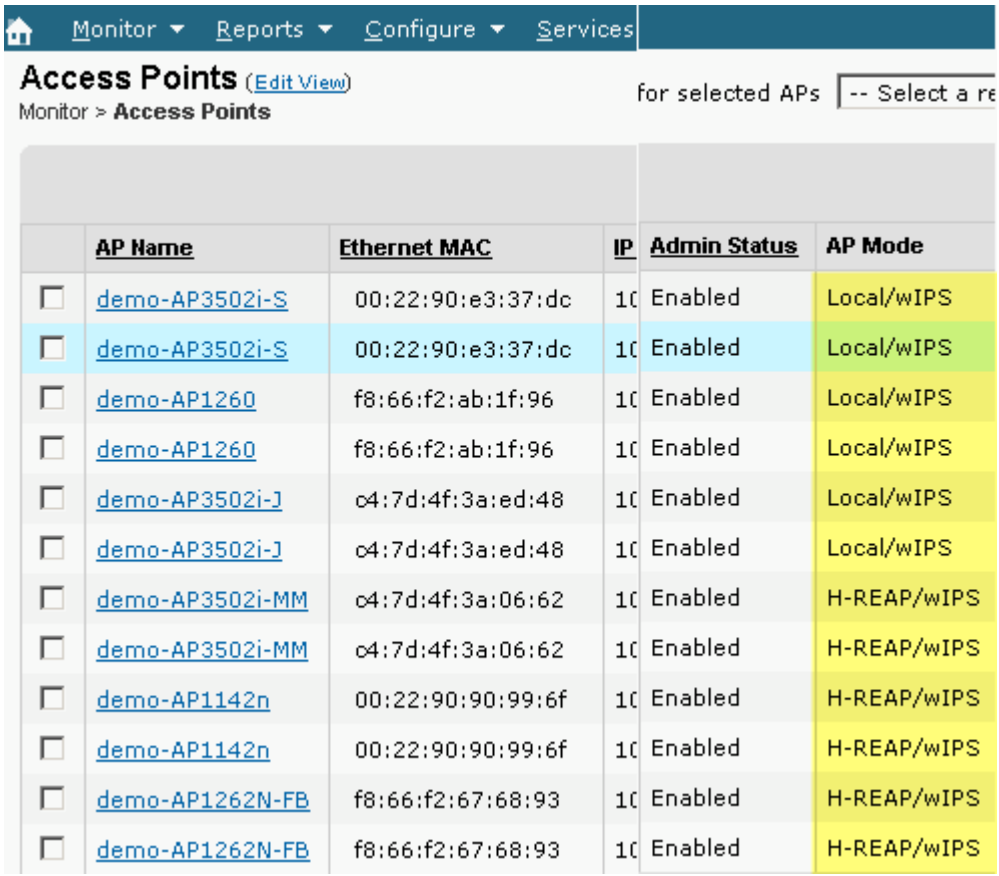
    Nota: Si cualquiera de las radios de este AP está habilitada, WCS ignorará la configuración y producirá el error en la Figura 7.

    Figura 7: Recordatorio de WCS para desactivar las radios AP antes de activar el ELM



4. El éxito de la configuración se puede verificar observando el cambio en el modo AP de "Local o H-REAP" a **Local/wIPS** o **H-REAP/wIPS**. Consulte la Figura 8.

    Figura 8: WCS muestra el modo AP para incluir wIPS con H-REAP o local

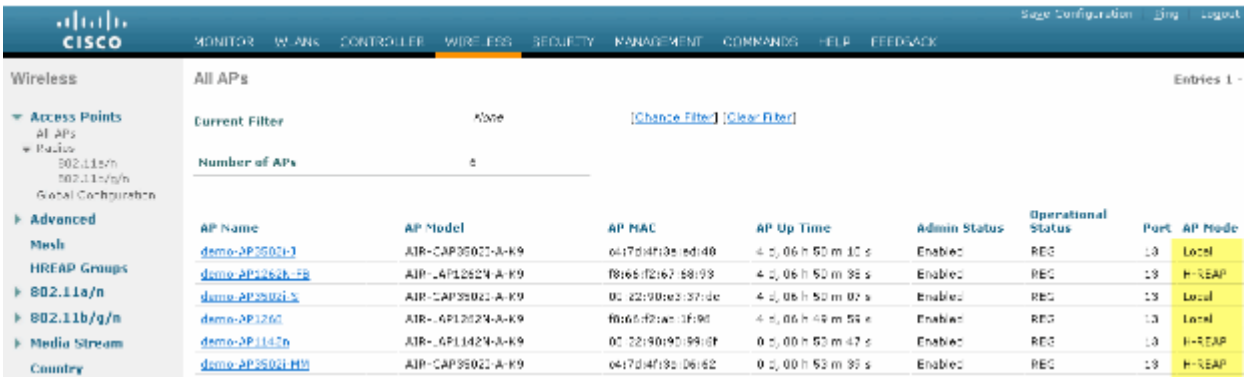


5. Active las radios que estaban desactivadas en el paso 1.
6. Cree el perfil wIPS y envíelo al controlador para que se complete la configuración.

   Nota: Para obtener información de configuración completa sobre wIPS, consulte la Guía de implementación de wIPS adaptable de Cisco.

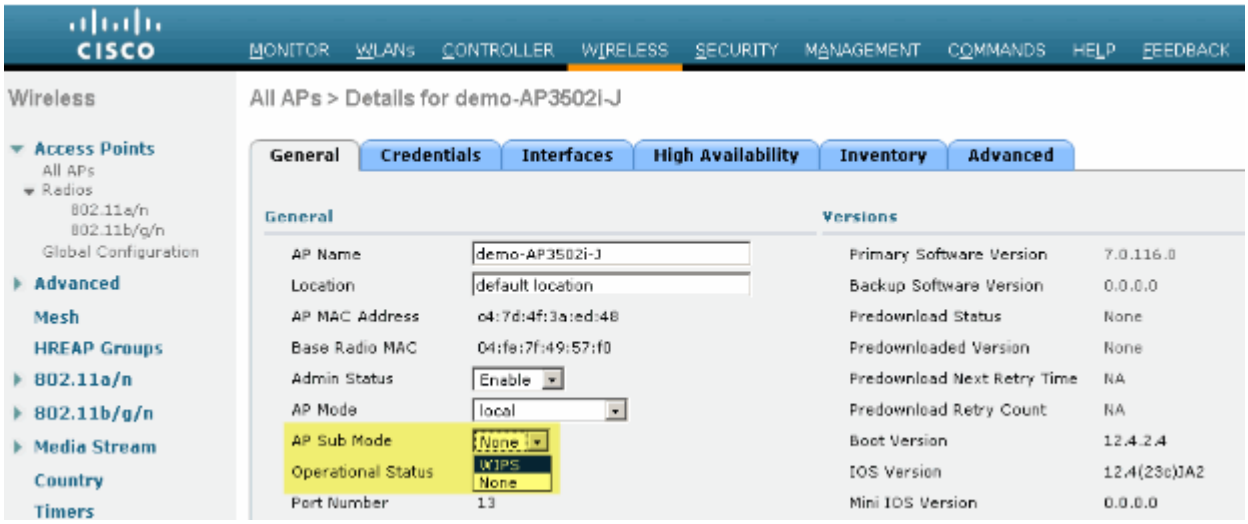
Configuración desde el WLC

Figura 9: Configuración del ELM con el WLC



1. Elija un AP de la pestaña **Wireless**.

Figura 10: WLC cambia el submodo AP para incluir el ELM wIPS



2. En el menú desplegable AP Sub Mode, elija **wIPS** (Figura 10).

3. Aplique y, a continuación, guarde la configuración.

Nota: Para que la funcionalidad del ELM funcione, se requieren MSE y WCS con las licencias wIPS. El cambio del submodo AP del WLC solamente no habilitará el ELM.

Ataques detectados en el ELM

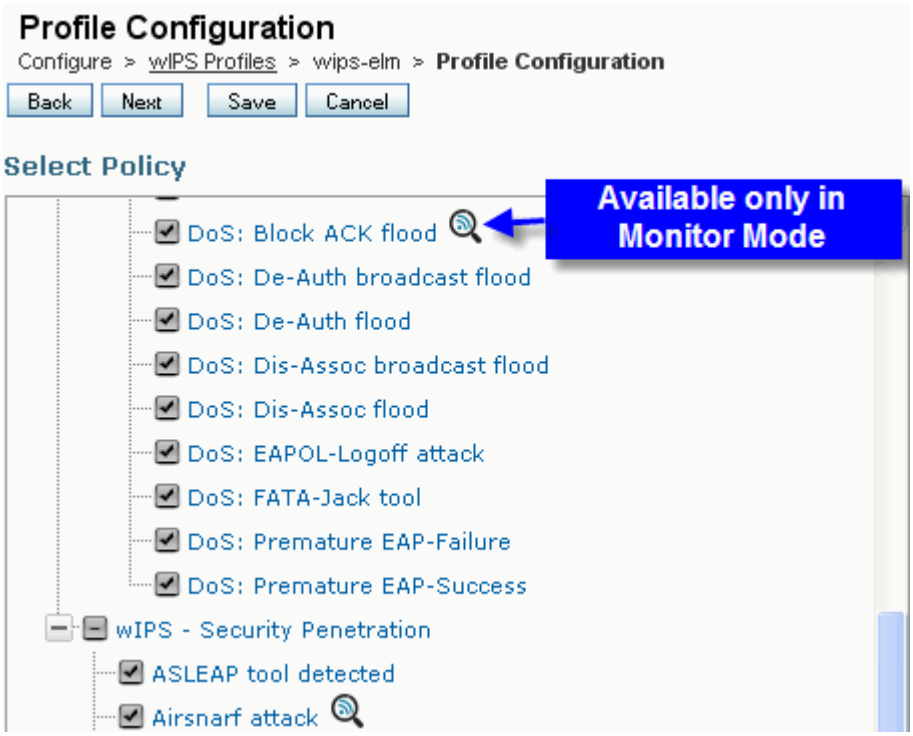
Tabla 1: Matriz de compatibilidad de firmas wIPS

Ataques detectados	ELM	MM
Ataque DoS contra AP		
Inundación de asociación	S	S
Desbordamiento de tabla de asociación	S	S
Inundación de autenticación	S	S
Ataque EAPOL-Start	S	S
PS-Poll flood	S	S
Inundación de solicitud de sondeo	N	S
Asociación no autenticada	S	S
Ataque DoS contra la infraestructura		
inundación CTS	N	S
Aprovechamiento de la tecnología de la Universidad de Queensland	N	S
Interferencia de RF	S	S
inundación RTS	N	S
Ataque de operador virtual	N	S
Ataque DoS contra la estación		
Ataque de fallo de autenticación	S	S
Bloquear inundación ACK	N	S

Inundación de difusión de desautenticación	S	S
Inundación De-Auth	S	S
Inundación de broadcast Dis-Assoc	S	S
Inundación Dis-Assoc	S	S
Ataque de cierre de sesión de EAPOL	S	S
herramienta FATA-Jack	S	S
Falla de EAP prematuro	S	S
Éxito de EAP prematuro	S	S
Ataques de penetración de seguridad		
Herramienta ASLEAP detectada	S	S
ataque Airsnarf	N	S
Ataque ChopChop	S	S
Ataque de día cero por anomalía en la seguridad de WLAN	N	S
Ataque de día cero por anomalía en la seguridad de los dispositivos	N	S
Sondeo de dispositivos para puntos de acceso	S	S
Ataque de diccionario en métodos EAP	S	S
Ataque EAP contra la autenticación 802.1x	S	S
AP falsos detectados	S	S
Se ha detectado un servidor DHCP falso	N	S
Herramienta de descifrado FAST WEP detectada	S	S
Ataque de fragmentación	S	S
Punto de acceso Honeypot detectado	S	S
Herramienta Hotspotter detectada	N	S
Tramas de broadcast inadecuadas	N	S
Paquetes 802.11 mal formados detectados	S	S
Hombre en medio del ataque	S	S
Netstumbler detectado	S	S
Víctima de Netstumbler detectada	S	S
Infracción de PSPF detectada	S	S
AP de software o AP de host detectado	S	S
Dirección MAC falsa detectada	S	S
Se ha detectado tráfico sospechoso fuera del horario de oficina	S	S
Asociación no autorizada por lista de proveedores	N	S
Asociación no autorizada detectada	S	S
Wellenreiter detectado	S	S

Nota: si agrega CleanAir, también podrá detectar ataques que no sean de tipo 802.11.

Figura 11: Vista del perfil de wIPS de WCS



En la Figura 11, configure el perfil wIPS desde WCS, el icono indica que el ataque será detectado solamente cuando el AP esté en MM, mientras que el mejor esfuerzo solamente cuando esté en el ELM.

Solucionar problemas de ELM

Compruebe estos elementos:

- Asegúrese de que NTP está configurado.
- Asegúrese de que la configuración de la hora MSE está en UTC.
- Si el grupo de dispositivos no funciona, utilice SSID de perfil de superposición con Any. Reinicie el AP.
- Asegúrese de que la licencia está configurada (actualmente los AP del ELM utilizan licencias KAM)
- Si los perfiles wIPS se cambian con demasiada frecuencia, vuelva a sincronizar el controlador MSE. Asegúrese de que el perfil esté activo en el WLC.
- Asegúrese de que el WLC sea parte de MSE usando las CLI de MSE:

    1. SSH o telnet a su MSE.
    2. Execute **/opt/mse/wips/bin/wips_cli**: esta consola se puede utilizar para acceder a los siguientes comandos con el fin de recopilar información sobre el estado del sistema wIPS adaptativo.
    3. **show wlc all** - Problema dentro de la consola wIPS. Este comando se utiliza para verificar los controladores que se comunican activamente con el servicio wIPS en MSE. Consulte la Figura 12.

Figura 12: Verificación de WLC activo con servicios wIPS de MSE CLI

```
<#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
```

- Asegúrese de que se detectan alarmas en MSE mediante CLI de MSE.
    - **show alarm list -** Problema dentro de la consola wIPS. Este comando se utiliza para enumerar las alarmas que contiene actualmente la base de datos del servicio wIPS. El campo key es la llave hash única asignada a la alarma específica. El campo Tipo es el tipo de alarma. Este gráfico de la Figura 13 muestra una lista de ID de alarma y descripciones:

    Figura 13 - Comando show alarm list de MSE CLI

    ```
    <#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
    ```

    Los campos First Time (Primera vez) y Last Time (Última hora) indican las marcas de hora en que se detectó la alarma; se almacenan en la hora UTC. El campo Activo se resalta si la alarma se ha detectado en ese momento.

- Borre la base de datos MSE.
    - Si se encuentra con una situación en la que la base de datos de MSE está dañada o no funciona ningún otro método de solución de problemas, puede ser mejor borrar la base de datos y empezar de nuevo.

Figura 14: Comando 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
```

Información Relacionada

- **Guía de Configuración de Cisco Wireless LAN Controller, Versión 7.0.116.0**
- **Guía de Configuración de Cisco Wireless Control System, Versión 7.0.172.0**
- **Soporte Técnico y Documentación - Cisco Systems**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).