Ejemplo de Configuración de Protección de Tramas de Administración de Infraestructura (MFP) con WLC y LAP

Contenido

Introducción

Este documento presenta una nueva función de seguridad inalámbrica llamada Management Frame Protection (MFP). Este documento también describe cómo configurar MFP en dispositivos de infraestructura como Lightweight Access Points (LAP) y Controladores de LAN inalámbricos (WLC).

Prerequisites

Requirements

- Conocimiento de cómo configurar el WLC y el LAP para el funcionamiento básico

- Conocimientos básicos de las tramas de administración IEEE 802.11

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- WLC de Cisco serie 2000 que ejecuta la versión 4.1 del firmware
- LAP 1131AG de Cisco
- Cisco Aironet 802.11a/b/g Client Adapter que ejecuta la versión 3.6 del firmware
- Cisco Aironet Desktop Utility versión 3.6

Nota: MFP es compatible con la versión 4.0.155.5 y posteriores del WLC, aunque la versión 4.0.206.0 proporciona el rendimiento óptimo con MFP. La MFP del cliente es compatible con la versión 4.1.171.0 y posteriores.

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.

Antecedentes

En 802.11, las tramas de administración como (des)autenticación, (dis)asociación, balizas y sondeos siempre están sin autenticar y sin cifrar. En otras palabras, las tramas de administración 802.11 siempre se envían de manera no segura, a diferencia del tráfico de datos, que se cifra con protocolos como WPA, WPA2 o, al menos, WEP, etc.

Esto permite que un atacante falsifique una trama de administración desde el AP para atacar a un cliente que está asociado a un AP. Con las tramas de administración simuladas, un atacante puede realizar estas acciones:

- Ejecute una denegación de servicio (DOS) en la WLAN
- Intentar un ataque de Man in the Middle contra el cliente cuando se vuelve a conectar
- Ejecutar un ataque de diccionario sin conexión

La MFP supera estos obstáculos cuando autentica tramas de administración 802.11 intercambiadas en la infraestructura de red inalámbrica.

Nota: Este documento se centra en la infraestructura y la MFP del cliente.

Nota: Existen ciertas restricciones para que algunos clientes inalámbricos se comuniquen con dispositivos de infraestructura habilitados para MFP. La función MFP agrega un conjunto largo de elementos de información a cada solicitud de sondeo o baliza SSID. Algunos clientes inalámbricos, como PDA, smartphones, escáneres de códigos de barras, etc., tienen memoria y CPU limitadas. Por lo tanto, no puede procesar estas solicitudes o indicadores. Como resultado, no puede ver el SSID por completo o no puede asociarse con estos dispositivos de infraestructura debido a un malentendido de las capacidades del SSID. Este problema no es específico de MFP. Esto también ocurre con cualquier SSID que tenga varios elementos de información (IE). Siempre es recomendable probar los SSID habilitados para MFP en el entorno con todos los tipos de clientes disponibles antes de implementarlos en tiempo real.

Nota:

Estos son los componentes de la MFP de infraestructura:

- Protección de trama de administración: cuando la protección de trama de administración está habilitada, el AP agrega el elemento de información de comprobación de integridad del mensaje (MIC IE) a cada trama de administración que transmite. Cualquier intento de copiar, alterar o reproducir la trama invalida el MIC. Un AP, que está configurado para validar tramas MFP recibe una trama con MIC inválida, informa al WLC.
- Validación de tramas de administración: cuando se habilita la validación de tramas de administración, el AP valida cada trama de administración que recibe de otros AP en la red. Asegura que el IE de MIC esté presente (cuando el originador está configurado para transmitir tramas MFP) y coincida con el contenido de la trama de administración. Si recibe cualquier trama que no contiene un IE de MIC válido de un BSSID que pertenece a un AP, que está configurado para transmitir tramas MFP, informa la discrepancia al sistema de administración de red.

  Nota: Para que las marcas de tiempo funcionen correctamente, todos los WLC deben estar sincronizados con el protocolo de tiempo de la red (NTP).
- Informe de eventos: el punto de acceso notifica al WLC cuando detecta una anomalía. El WLC agrega los eventos anómalos y los informa a través de las trampas SNMP al administrador de red.

Funcionalidad de MFP de infraestructura

Con MFP, todas las tramas de administración se trocean criptográficamente para crear una comprobación de integridad del mensaje (MIC). El MIC se añade al final del cuadro (antes de la Secuencia de comprobación de cuadro (FCS)).

- En una arquitectura inalámbrica centralizada, la MFP de infraestructura se habilita/inhabilita en el WLC (configuración global). La protección se puede inhabilitar selectivamente por WLAN, y la validación se puede inhabilitar selectivamente por AP.

- La protección se puede desactivar en las WLAN que utilizan los dispositivos que no pueden hacer frente a IE adicionales.
- La validación debe estar inhabilitada en los AP que están sobrecargados o sobrecargados.

Cuando la MFP se habilita en una o más WLAN configuradas en el WLC, el WLC envía una llave única a cada radio en cada AP registrado. Las tramas de administración son enviadas por el AP a través de las WLAN habilitadas para MFP. Estos AP se etiquetan con un IE de MIC de protección de trama. Cualquier intento de alterar la trama invalida el mensaje, lo que hace que el AP receptor que está configurado para detectar tramas MFP informe la discrepancia al controlador WLAN.

Este es un proceso paso a paso de MFP mientras se implementa en un entorno de roaming:

1. Con la MFP globalmente habilitada, el WLC genera una llave única para cada AP/WLAN que se configura para la MFP. Los WLC se comunican dentro de sí mismos de modo que todos los WLC conocen las llaves para todos los AP/BSS en un dominio de la movilidad.

   Nota: Todos los controladores de un grupo de movilidad/RF deben tener MFP configurado de manera idéntica.

2. Cuando un AP recibe una trama protegida MFP para un BSS que no conoce, almacena en el búfer una copia de la trama y consulta al WLC para obtener la clave.
3. Si el BSSID no se conoce en el WLC, devuelve el mensaje "BSSID desconocido" al AP, y el AP descarta las tramas de administración recibidas de ese BSSID.
4. Si el BSSID se conoce en el WLC, pero el MFP se inhabilita en ese BSSID, el WLC devuelve un "BSSID inhabilitado". El AP asume entonces que todas las tramas de administración recibidas de ese BSSID no tienen un MIC MFP.
5. Si el BSSID es conocido y tiene MFP habilitado, el WLC devuelve la clave MFP al AP solicitante (sobre el túnel de administración LWAPP cifrado AES).
6. El AP almacena en caché las claves recibidas de esta manera. Esta clave se utiliza para validar o agregar MIC IE.

Funcionalidad de cliente MFP

La MFP del cliente protege a los clientes autenticados de tramas simuladas, lo que impide la eficacia de muchos de los ataques comunes contra las LAN inalámbricas. La mayoría de los ataques, como los ataques de desautenticación, vuelven a un rendimiento simplemente degradado cuando compiten con clientes válidos.

Específicamente, la MFP del cliente cifra las tramas de administración enviadas entre los puntos de acceso y los clientes CCXv5 para que ambos puedan tomar medidas preventivas y descartar las tramas de administración de clase 3 simuladas (es decir, las tramas de administración pasadas entre un punto de acceso y un cliente que está autenticado y asociado). La MFP del cliente aprovecha los mecanismos de seguridad definidos por IEEE 802.11i para proteger estos

tipos de tramas de gestión de unidifusión de clase 3: desasociación, desautenticación y acción de QoS (WMM). La MFP del cliente puede proteger una sesión de punto de acceso del cliente del tipo más común de ataque de denegación de servicio. Protege las tramas de administración de clase 3 con el mismo método de cifrado utilizado para las tramas de datos de la sesión. Si una trama recibida por el punto de acceso o el cliente falla en el descifrado, se descarta y el evento se informa al controlador.

Para utilizar la MFP del cliente, los clientes deben ser compatibles con la MFP CCXv5 y deben negociar WPA2 con TKIP o AES-CCMP. EAP o PSK se puede utilizar para obtener el PMK. CCKM y la gestión de movilidad del controlador se utilizan para distribuir claves de sesión entre puntos de acceso o itinerancia rápida de capa 2 y capa 3.

Para evitar ataques contra tramas de difusión, los puntos de acceso que admiten CCXv5 no emiten ninguna trama de administración de clase 3 de difusión (como desasociación, desautenticación o acción). Los clientes CCXv5 y los puntos de acceso deben descartar las tramas de administración de broadcast class 3.

La MFP del cliente complementa a la MFP de la infraestructura en lugar de reemplazarla porque la MFP de la infraestructura continúa detectando e informando de tramas unicast no válidas enviadas a clientes que no son compatibles con la MFP del cliente, así como de tramas de administración de clase 1 y 2 no válidas. La MFP de infraestructura se aplica solamente a las tramas de administración que no están protegidas por la MFP del cliente.

Componentes de MFP del cliente

La MFP del cliente consta de estos componentes:

- Generación y distribución de claves
- Protección y validación de tramas de gestión
- Informes de errores

Generación y distribución de claves

La MFP del cliente no utiliza los mecanismos de generación y distribución de claves que se derivaron para la MFP de infraestructura. En su lugar, la MFP del cliente aprovecha los mecanismos de seguridad definidos por IEEE 802.11i para proteger también las tramas de gestión de unidifusión de clase 3. Las estaciones deben admitir CCXv5 y deben negociar TKIP o AES-CCMP para utilizar la MFP del cliente. EAP o PSK se puede utilizar para obtener el PMK.

Protección de marcos de gestión

Las tramas de administración de unidifusión clase 3 están protegidas con la aplicación de AES-CCMP o TKIP de una manera similar a la que ya se utiliza para las tramas de datos. Partes del encabezado de trama se copian en el componente de carga útil cifrada de cada trama para una mayor protección, como se describe en las siguientes secciones.

Estos tipos de trama están protegidos:

- Desasociación
- Desautenticación
- Tramas de acción de QoS (WMM)

Las tramas de datos protegidas por AES-CCMP y TKIP incluyen un contador de secuencia en los campos IV, que se utiliza para evitar la detección de reproducción. El contador de transmisión actual se utiliza para las tramas de datos y de administración, pero se utiliza un nuevo contador de recepción para las tramas de administración. Los contadores de recepción se prueban para asegurarse de que cada trama tenga un número mayor que la última trama recibida (para asegurarse de que las tramas son únicas y no se han reproducido), por lo que no importa que este esquema haga que los valores recibidos sean no secuenciales.

Informes de errores

Los mecanismos de generación de informes MFP-1 se utilizan para notificar los errores de desencapsulación de tramas de administración detectados por los puntos de acceso. Es decir, el WLC recopila las estadísticas de error de validación de MFP y reenvía periódicamente la información recopilada al WCS.

Los errores de violación de MFP detectados por las estaciones cliente son manejados por la función Roaming and Real Time Diagnostics de CCXv5 y no están en el alcance de este documento.

Protección de tramas de Broadcast Management

Para evitar ataques que utilizan tramas de broadcast, los AP que soportan CCXv5 no transmiten ninguna trama de administración de clase de broadcast 3 (es decir, disassoc, deauth o action) excepto para tramas de desautenticación/desasociación de contención rogue. Las estaciones cliente compatibles con CCXv5 deben descartar las tramas de administración de clase 3 de difusión. Se supone que las sesiones de MFP están en una red correctamente protegida (autenticación fuerte más TKIP o CCMP), por lo que no se tienen en cuenta las transmisiones de contención no autorizadas.

De manera similar, los AP descartan las tramas de administración de broadcast entrante. Actualmente no se admiten tramas de administración de difusión entrante, por lo que no se requieren cambios de código para esto.

Plataformas Soportadas

Estas plataformas son compatibles:

- Controladores WLAN
    - 2006

    - 2106
    - 4400
    - WiSM
    - 3750 con controlador 440x integrado
    - 26/28/37/38xx Routers
- Puntos de acceso LWAPP
    - AP 1000
    - AP 1100 y 1130
    - AP 1200, 1240 y 1250
    - AP 1310
- Software cliente
    - ADU 3.6.4 y superior
- Sistemas de administración de la red
    - WCS

El AP 1500 Mesh LWAPP no se soporta en esta versión.

Modos admitidos

Los puntos de acceso basados en LWAPP que funcionan en estos modos no soportan la MFP del cliente:

Modos de punto de acceso admitidos	
Modo	Compatibilidad con MFP del cliente
Local	Yes
Monitor	No
Rastreador	No
Detector de acceso no deseado	No
COSECHA HÍBRIDA	Yes
COSECHA	No
Raíz del puente	Yes

WGB	No

Compatibilidad con celdas mixtas

Las estaciones cliente que no son compatibles con CCXv5 pueden asociarse con una WLAN MFP-2. Los puntos de acceso realizan un seguimiento de qué clientes son compatibles con MFP-2 y cuáles no para determinar si las medidas de seguridad de MFP-2 se aplican a las tramas de administración de unidifusión saliente y se esperan en las tramas de administración de unidifusión entrante.

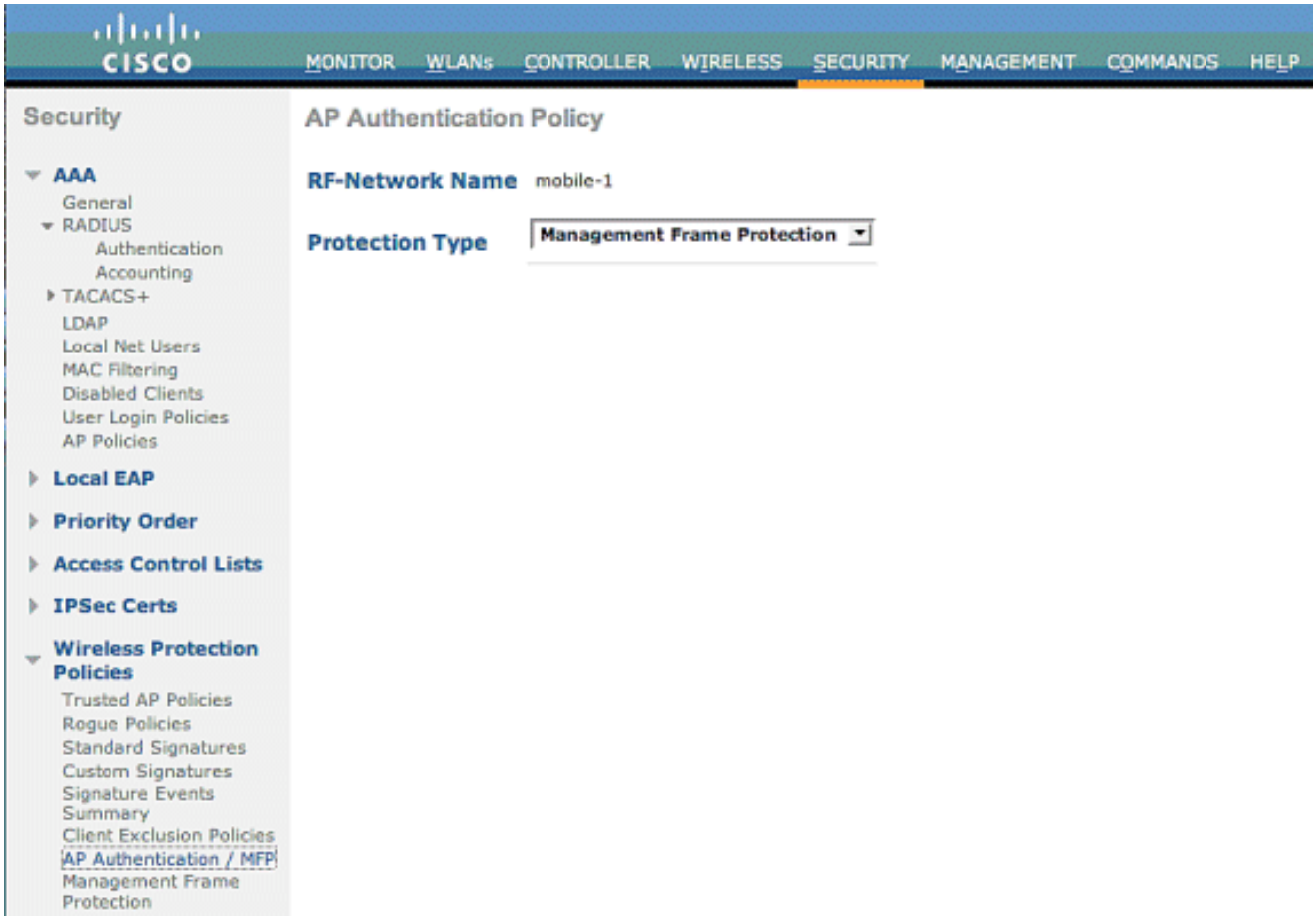
Configurar

Configuración de MFP en un controlador

Puede configurar globalmente la MFP en un controlador. Al hacerlo, la protección de tramas de administración y la validación se habilitan de forma predeterminada para cada punto de acceso unido, y la autenticación del punto de acceso se inhabilita automáticamente.

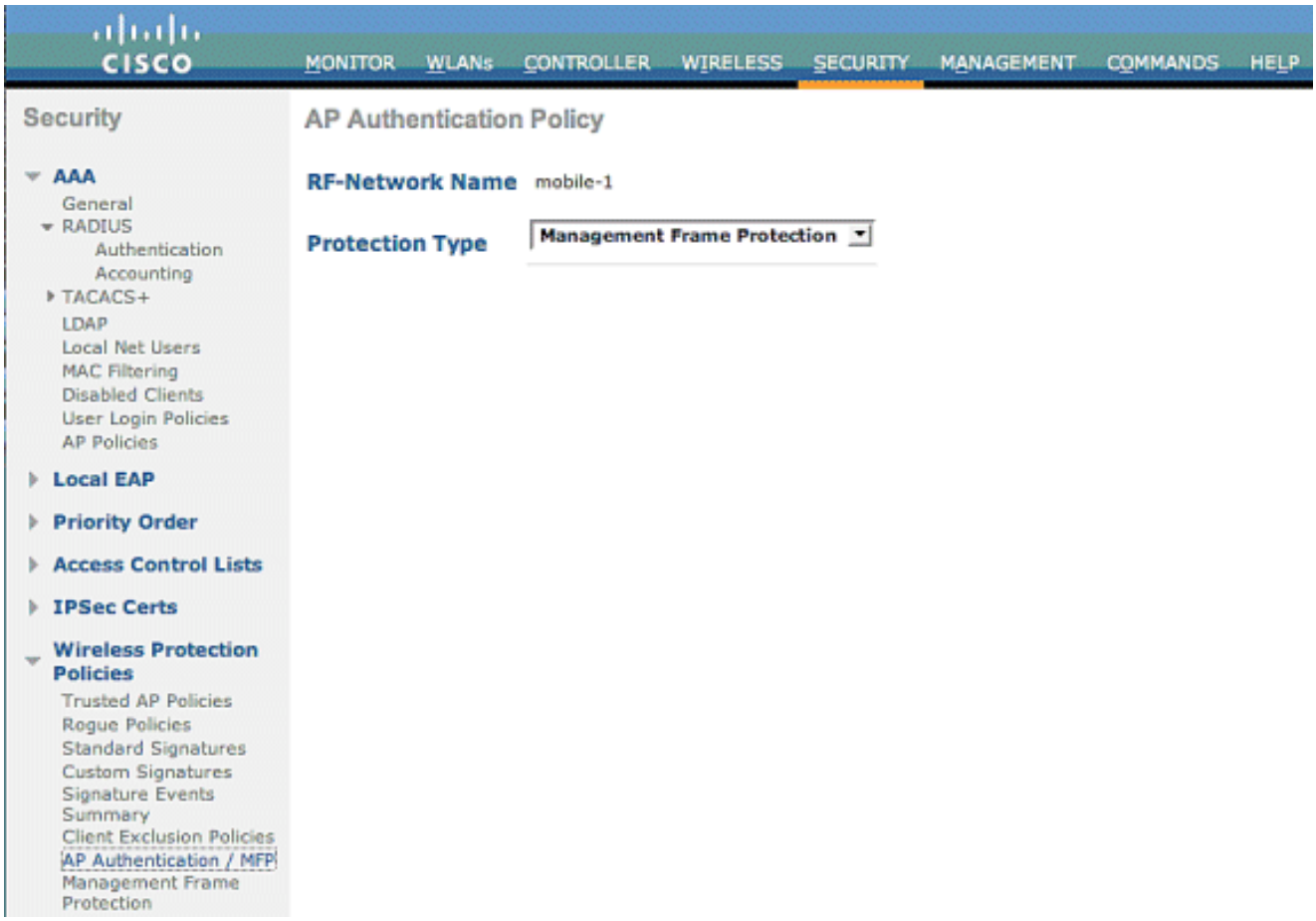
Realice estos pasos para configurar MFP globalmente en un controlador.

1. En la GUI del controlador, haga clic en Security. En la pantalla resultante, haga clic en Autenticación AP/MFP bajo Políticas de protección inalámbrica.



2. En la Política de autenticación de AP, elija Management Frame Protection en el menú

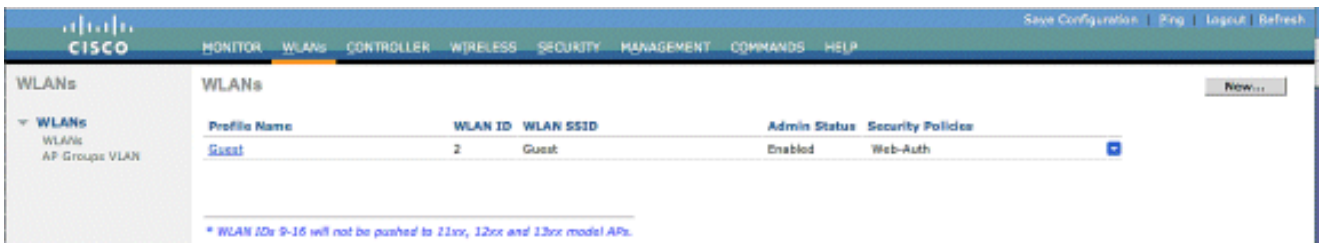
desplegable Protection Type y haga clic en Apply.



Configuración de MFP en WLAN

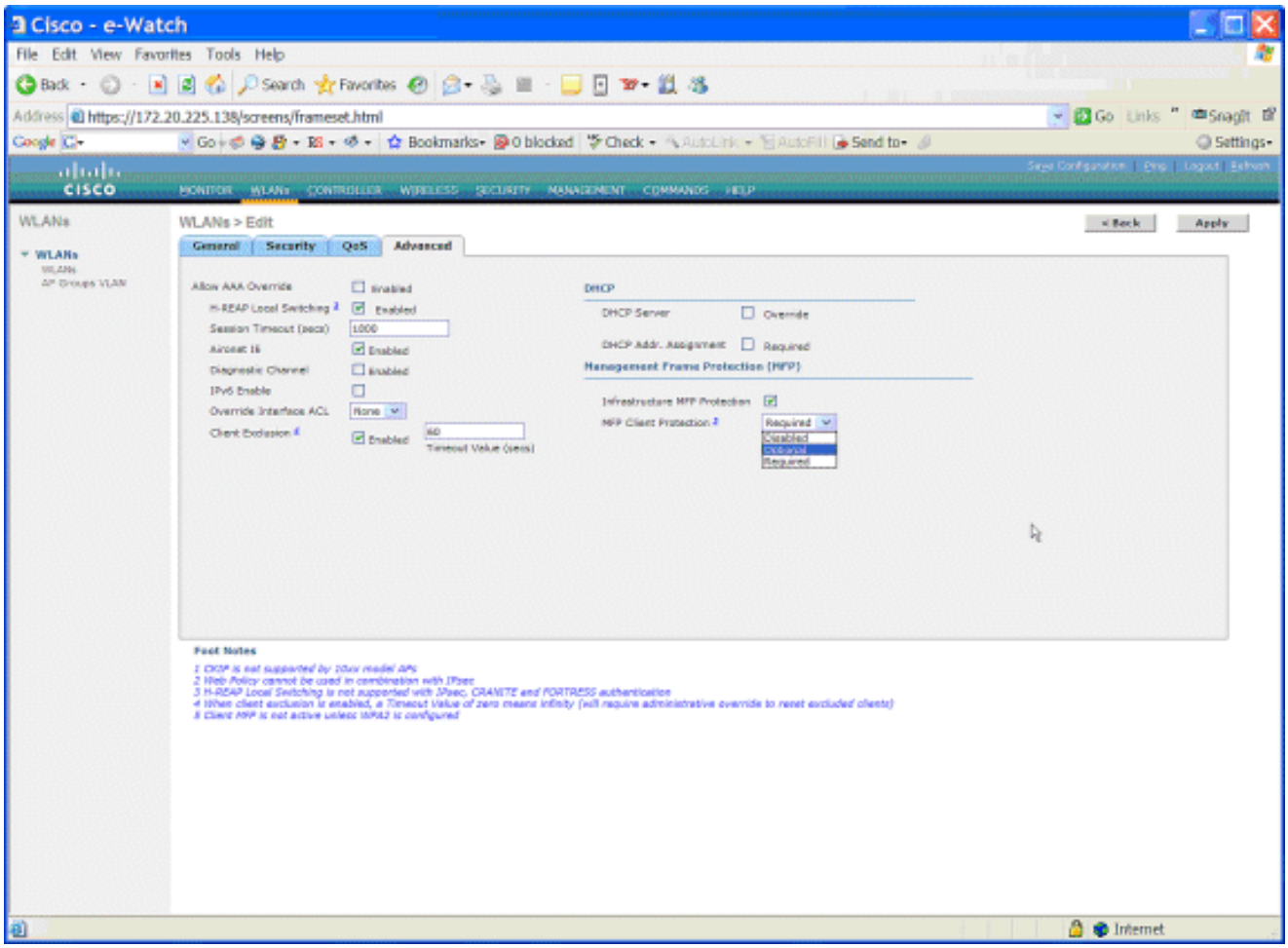
También puede habilitar/inhabilitar la protección de la MFP de la infraestructura y la MFP del cliente en cada WLAN configurada en el WLC. Ambas están habilitadas de forma predeterminada mediante la protección de MFP de infraestructura, que solo está activa si está habilitada globalmente, y la MFP de cliente solo está activa si la WLAN está configurada con seguridad WPA2. Siga estos pasos para habilitar MFP en una WLAN:

1. Desde el WLC GUI, haga clic en WLANs y haga clic en Nuevo para crear un nuevo WLAN.



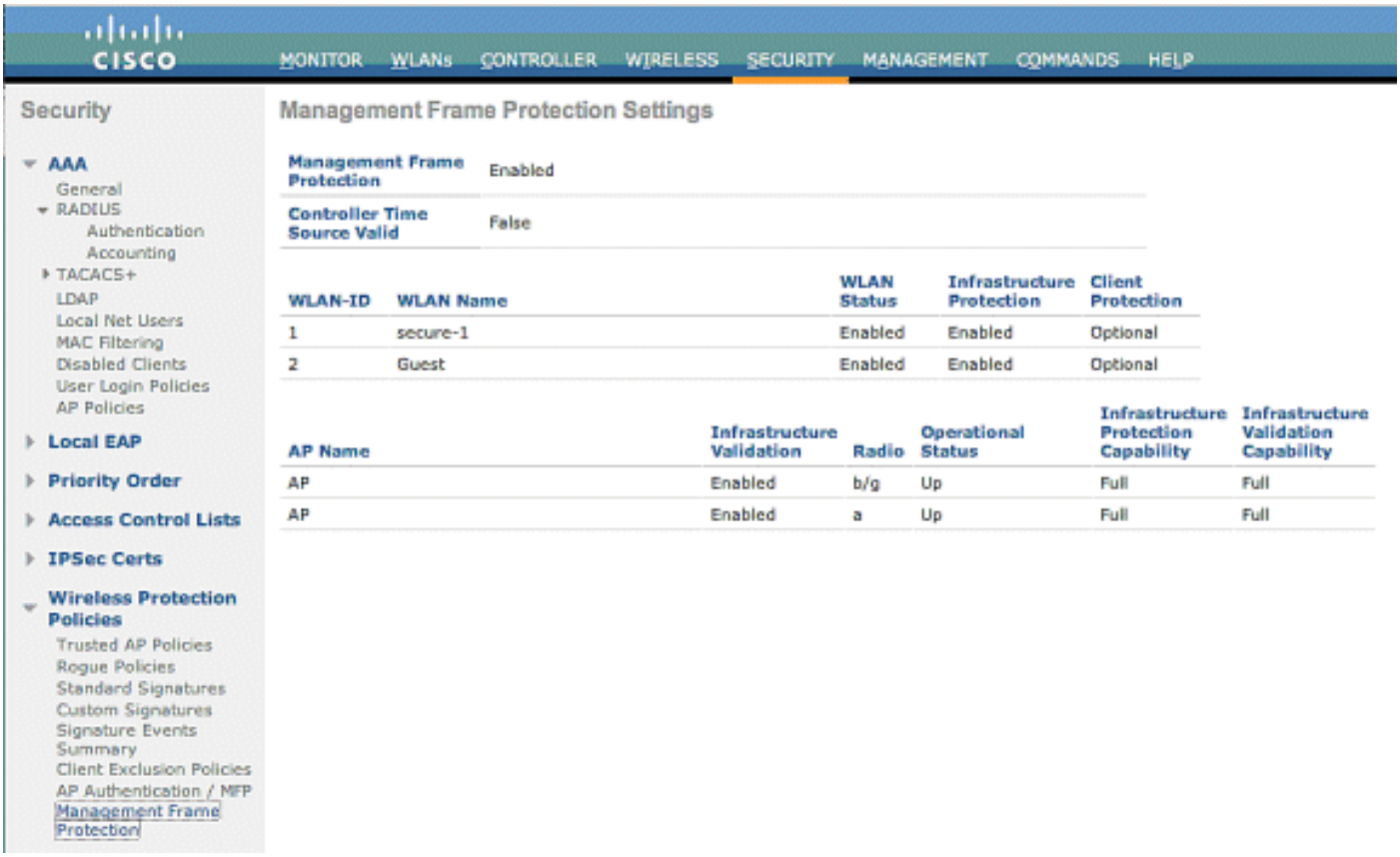
2. En la página de edición de WLANs, vaya a la ficha Advanced y marque la casilla de verificación Infrastructure MFP Protection para habilitar la MFP de infraestructura en esta WLAN. Para inhabilitar la protección MFP de infraestructura para esta WLAN, desmarque esta casilla de verificación. Para habilitar la MFP del cliente, elija la opción requerida u opcional del menú desplegable. Si elige Cliente MFP= Obligatorio, asegúrese de que todos sus clientes tengan soporte para MFP-2 o no puedan conectarse. Si elige la opción

opcional, tanto los clientes con MFP como los que no lo tienen activado pueden conectarse a la misma WLAN.



Verificación

Para verificar las configuraciones MFP desde la GUI, haga clic en Management Frame Protection bajo Wireless Protection Policies desde la página Security. De este modo accederá a la página Configuración de MFP.



En la página MFP Settings (Parámetros de MFP), puede ver la configuración de MFP en el WLC, el LAP y la WLAN. Esto es un ejemplo.

- El campo Management Frame Protection muestra si MFP está habilitado globalmente para el WLC.
- El campo Válido de Origen de Tiempo del Controlador indica si la hora del WLC se establece localmente (mediante la entrada manual de la hora) o a través de una fuente externa (como un servidor NTP). Si la hora la establece un origen externo, el valor de este campo es "True". Si la hora se establece localmente, el valor es "False". La fuente de tiempo se utiliza para validar las tramas de administración entre los puntos de acceso de los diversos WLC que también tienen la movilidad configurada.

  Nota: Si MFP está habilitado en todos los WLC en un grupo de movilidad/RF, siempre se recomienda que utilice un servidor NTP para establecer la hora del WLC en un grupo de movilidad.
- El campo MFP Protection muestra si MFP está habilitado para WLANs individuales.
- El campo MFP Validation muestra si MFP está habilitado para puntos de acceso individuales.

Estos comandos show pueden ser útiles:

- show wps summary: utilice este comando para ver un resumen de las políticas de protección inalámbrica actuales (que incluye MFP) del WLC.

- show wps mfp summary: para ver la configuración de MFP global actual del WLC, ingrese este comando.
- show ap config general AP_name : para ver el estado actual de la MFP para un punto de acceso determinado, ingrese este comando.

Este es un ejemplo del resultado del comando show ap config general AP_name:

<#root>

```
(Cisco Controller) >

show ap config general AP


Cisco AP Identifier.............................. 4
Cisco AP Name.................................... AP
Country code..................................... US  - United States
Regulatory Domain allowed by Country............. 802.11bg:-AB    802.11a:-AB
AP Country code.................................. US  - United States
AP Regulatory Domain............................. 802.11bg:-A    802.11a:-A
Switch Port Number .............................. 29
MAC Address...................................... 00:19:2f:7e:3a:30
IP Address Configuration......................... DHCP
IP Address....................................... 172.20.225.142
IP NetMask....................................... 255.255.255.248
Gateway IP Addr.................................. 172.20.225.137
Cisco AP Location................................ default location
Cisco AP Group Name.............................. default-group
Primary Cisco Switch.............................
Secondary Cisco Switch..........................
Tertiary Cisco Switch...........................
Administrative State ............................ ADMIN_ENABLED
Operation State ................................. REGISTERED
Mirroring Mode .................................. Disabled
AP Mode ......................................... H-Reap
Public Safety ................................... Global: Disabled, Local: Disabled
Remote AP Debug ................................. Disabled
S/W  Version .................................... 4.1.169.24
Boot  Version ................................... 12.3.7.1
Mini IOS Version ................................ 3.0.51.0
Stats Reporting Period .......................... 180
LED State........................................ Enabled
PoE Pre-Standard Switch.......................... Disabled
PoE Power Injector MAC Addr...................... Disabled
Number Of Slots.................................. 2
AP Model......................................... AIR-LAP1242AG-A-K9
IOS Version...................................... 12.4(20070414:021809)
Reset Button..................................... Enabled
AP Serial Number................................. FTX1035B3QX
AP Certificate Type.............................. Manufacture Installed
H-REAP Vlan mode :............................... Disabled
Management Frame Protection Validation........... Enabled
Console Login Name..............................
Console Login State.............................. Unknown
Ethernet Port Duplex............................. Auto
Ethernet Port Speed.............................. Auto
```

Este es un ejemplo del resultado del comando show wps mfp summary:

```
<#root>

(Cisco Controller) >

show wps mfp summary


Global MFP state..................................... enabled

Controller Time Source Valid..................... false


                                    WLAN       Infra.      Client
WLAN ID  WLAN Name                  Status     Protection  Protection

-------  -------------------------  ---------  ----------  ----------
1        secure-1                   Enabled    Enabled     Optional
2        Guest                      Enabled    Enabled     Optional but inactive (WPA2 not configured)

                     Infra.             Operational     --Infra. Capability--
AP Name              Validation  Radio  State           Protection  Validation

-------------------  ----------  -----  --------------  ----------  ----------
AP                   Enabled     b/g    Up              Full        Full
```

Estos comandos debug pueden ser útiles;

- debug wps mfp lwapp—Muestra información de depuración para mensajes MFP.
- debug wps mfp detail—Muestra información de depuración detallada para los mensajes MFP.
- debug wps mfp report: muestra información de depuración para los informes de MFP.
- debug wps mfp mm—Muestra información de depuración para mensajes de movilidad MFP (entre controladores).

Nota: También hay varios sniffers gratuitos de paquetes inalámbricos disponibles en Internet, que se pueden utilizar para capturar y analizar las tramas de administración 802.11. Algunos ejemplos de rastreadores de paquetes son Omnipeek y Wireshark.

Información Relacionada

- Configuración de Soluciones de Seguridad: Guía de Configuración de WLC

- Configuración de soluciones de seguridad en WCS
- Ejemplo de Configuración de Autenticación de EAP con Controladores de WLAN (WLC)
- Ejemplo de configuración de ACL en controladores de LAN inalámbricas
- Ejemplo de configuración de autenticación web externa con controladores de LAN inalámbrica
- Ejemplo de Configuración de Asignación de VLAN Dinámica con Servidor RADIUS y Controlador de LAN Inalámbrica
- Cisco Secure Services Client con autenticación EAP-FAST
- PREGUNTAS FRECUENTES DEL WLC
- Página de Soporte de Red Inalámbrica
- 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).