Exemplo de Configuração de MFP (Infrastructure Management Frame Protection, Proteção de Quadro de Gerenciamento de Infraestrutura) com WLC e LAP

Contents

Introduction

Este documento introduz uma nova característica de segurança em tecnologia wireless chamada Management Frame Protection (MFP). Este documento também descreve como configurar a MFP em dispositivos de infraestrutura, como Lightweight Access Points (LAPs) e Controllers de LAN Wireless (WLCs).

Prerequisites

Requirements

- Conhecimento de como configurar a WLC e o LAP para a operação básica
- Conhecimento básico dos quadros de gerenciamento IEEE 802.11

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 2000 Series WLC que executa o firmware versão 4.1
- LAP Cisco 1131AG
- Adaptador de cliente Cisco Aironet 802.11a/b/g que executa o firmware versão 3.6
- Cisco Aironet Desktop Utility versão 3.6

Observação: o MFP é compatível com a versão 4.0.155.5 da WLC e posterior, embora a versão 4.0.206.0 forneça o desempenho ideal com o MFP. O cliente MFP é compatível com a versão 4.1.171.0 e superior.

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

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

No 802.11, quadros de gerenciamento como (de)authentication, (dis)associação, beacons e probes são sempre não autenticados e não criptografados. Em outras palavras, os quadros de gerenciamento 802.11 são sempre enviados de maneira não segura, ao contrário do tráfego de dados, que são criptografados com protocolos como WPA, WPA2 ou, pelo menos, WEP, e assim por diante.

Isso permite que um invasor falsifique um quadro de gerenciamento do AP para atacar um cliente associado a um AP. Com os quadros de gerenciamento falsificados, um invasor pode executar estas ações:

- Execute uma negação de serviço (DOS) na WLAN
- Tente um homem no meio do ataque ao cliente quando ele se reconectar
- Executar um ataque de dicionário offline

O MFP supera esses obstáculos quando autentica quadros de gerenciamento 802.11 trocados na infraestrutura de rede sem fio.

Observação: este documento se concentra na **MFP da infraestrutura e do cliente**.

Observação: há certas restrições para alguns clientes sem fio se comunicarem com dispositivos de infraestrutura habilitados para MFP. O MFP adiciona um longo conjunto de elementos de informação a cada solicitação de sondagem ou beacon SSID. Alguns clientes sem fio, como PDAs, smartphones, scanners de código de barras e assim por diante, têm memória e CPU limitadas. Portanto, você não pode processar essas solicitações ou beacons. Como resultado, você não consegue ver o SSID completamente ou não consegue se associar a esses dispositivos

de infraestrutura, devido a um mal-entendido sobre os recursos do SSID. Esse problema não é específico do MFP. Isso também ocorre com qualquer SSID que tenha vários elementos de informação (IEs). É sempre aconselhável testar SSIDs *habilitados para* MFP no ambiente com todos os tipos de clientes disponíveis antes de implantá-los em tempo real.

Note:

Estes são os componentes do MFP de infraestrutura:

- **Proteção do quadro de gerenciamento** —Quando a proteção do quadro de gerenciamento está ativada, o AP adiciona o MIC IE (Message Integrity Check Information Elemento de Informação de Verificação da Integridade da Mensagem) a cada quadro de gerenciamento que transmite. Qualquer tentativa de copiar, alterar ou reproduzir o quadro invalida o MIC. Um AP, que é configurado para validar quadros MFP, recebe um quadro com MIC inválido, o relata ao WLC.
- **Validação do quadro de gerenciamento** — Quando a validação do quadro de gerenciamento está habilitada, o AP valida cada quadro de gerenciamento recebido de outros APs na rede. Garante que o MIC IE esteja presente (quando o originador estiver configurado para transmitir quadros MFP) e corresponda ao conteúdo do quadro de gerenciamento. Se receber qualquer quadro que não contenha um IE MIC válido de um BSSID que pertença a um AP, que está configurado para transmitir quadros MFP, ele reportará a discrepância ao sistema de gerenciamento de rede.**Observação:** para que os timestamps funcionem corretamente, todas as WLCs devem estar sincronizadas com o Network Time Protocol (NTP).
- **Relatórios de eventos** — O ponto de acesso notifica a WLC quando detecta uma anomalia. A WLC agrega os eventos anômalos e os relata através de armadilhas SNMP ao gerenciador de rede.

Funcionalidade de MFP de infraestrutura

Com o MFP, todos os quadros de gerenciamento são criptografados com hash para criar um MIC (Message Integrity Check). O MIC é adicionado ao final do quadro (antes da FCS (Frame Check Sequence)).

- Em uma arquitetura sem fio centralizada, o MFP da infraestrutura é ativado/desativado na WLC (configuração global). A proteção pode ser desativada seletivamente por WLAN, e a validação pode ser desativada seletivamente por AP.
- A proteção pode ser desativada nas WLANs usadas por dispositivos que não podem lidar com IEs extras.
- A validação deve ser desabilitada em APs sobrecarregados ou sobrecarregados.

Quando o MFP é ativado em uma ou mais WLANs configuradas na WLC, a WLC envia uma chave exclusiva para cada rádio em cada AP registrado. Os quadros de gerenciamento são enviados pelo AP através das WLANs habilitadas para MFP. Esses APs são rotulados com um MIC IE de proteção de quadro. Qualquer tentativa de alterar o quadro invalida a mensagem, o que faz com que o AP receptor que está configurado para detectar quadros MFP comunique a discrepância com o controlador WLAN.

Este é um processo passo a passo do MFP enquanto é implementado em um ambiente de roaming:

1. Com o MFP ativado globalmente, a WLC gera uma chave exclusiva para cada AP/WLAN configurado para MFP. As WLCs se comunicam entre si para que todas as WLCs saibam as chaves de todos os APs/BSSs em um domínio de mobilidade.**Observação:** todos os controladores em um grupo de RF/mobilidade devem ter o MFP configurado de forma idêntica.
2. Quando um AP recebe um quadro protegido MFP para um BSS que não conhece, ele coloca em buffer uma cópia do quadro e consulta a WLC para obter a chave.
3. Se o BSSID não for conhecido na WLC, ele retornará a mensagem "BSSID desconhecido" para o AP, e o AP descartará os quadros de gerenciamento recebidos desse BSSID.
4. Se o BSSID for conhecido na WLC, mas o MFP for desabilitado nesse BSSID, a WLC retornará um "BSSID Desabilitado". O AP então assume que todos os quadros de gerenciamento recebidos desse BSSID não têm um MFP MIC.
5. Se o BSSID for conhecido e tiver o MFP ativado, o WLC retornará a Chave MFP para o AP solicitante (sobre o túnel de gerenciamento do LWAPP criptografado por AES).
6. As chaves de cache AP recebidas dessa maneira. Essa chave é usada para validar ou adicionar MIC IE.

Funcionalidade MFP do cliente

O cliente MFP protege os clientes autenticados contra quadros falsificados, o que evita a eficácia de muitos dos ataques comuns contra LANs sem fio. A maioria dos ataques, como ataques de desautenticação, reverte para um desempenho simplesmente degradado quando se deparam com clientes válidos.

Especificamente, o MFP do cliente criptografa quadros de gerenciamento enviados entre pontos de acesso e clientes CCXv5, de modo que tanto os pontos de acesso quanto os clientes possam tomar medidas preventivas e descartar quadros de gerenciamento de classe 3 falsificados (ou seja, quadros de gerenciamento passados entre um ponto de acesso e um cliente autenticado e associado). O MFP do cliente aproveita os mecanismos de segurança definidos pelo IEEE 802.11i para proteger esses tipos de quadros de gerenciamento unicast classe 3: ação de desassociação, desautenticação e QoS (WMM). O MFP do cliente pode proteger uma sessão de ponto de acesso do cliente do tipo mais comum de ataque de negação de serviço. Ele protege os quadros de gerenciamento de classe 3 com o mesmo método de criptografia usado para os quadros de dados da sessão. Se um quadro recebido pelo ponto de acesso ou cliente falha na descriptografia, ele é descartado e o evento é relatado ao controlador.

Para usar o MFP do cliente, os clientes devem suportar o CCXv5 MFP e devem negociar o WPA2 com TKIP ou AES-CCMP. EAP ou PSK podem ser usados para obter o PMK. O CCKM e o gerenciamento de mobilidade do controlador são usados para distribuir chaves de sessão entre pontos de acesso ou o roaming rápido de Camada 2 e Camada 3.

Para evitar ataques contra quadros de broadcast, os pontos de acesso que suportam CCXv5 não emitem nenhum quadro de gerenciamento de classe 3 de broadcast (como desassociação, desautenticação ou ação). Os clientes e pontos de acesso do CCXv5 devem descartar quadros de gerenciamento de classe 3 de broadcast.

O MFP do cliente complementa o MFP da infraestrutura em vez de substituí-lo porque o MFP da infraestrutura continua a detectar e relatar quadros unicast inválidos enviados a clientes que não têm capacidade para MFP do cliente, bem como quadros de gerenciamento inválidos das classes 1 e 2. O MFP da infraestrutura é aplicado somente a quadros de gerenciamento que não estão

protegidos pelo MFP do cliente.

Componentes MFP do cliente

O MFP do cliente consiste nestes componentes:

- Geração e distribuição de chaves
- Proteção e validação de quadros de gerenciamento
- Relatórios de erros

Geração e distribuição de chaves

O MFP do cliente não usa os mecanismos de geração e distribuição de chaves que foram derivados para o MFP de infraestrutura. Em vez disso, o cliente MFP aproveita os mecanismos de segurança definidos pelo IEEE 802.11i para também proteger quadros de gerenciamento unicast de classe 3. As estações devem suportar CCXv5 e devem negociar TKIP ou AES-CCMP para usar o MFP do cliente. EAP ou PSK podem ser usados para obter o PMK.

Proteção de quadros de gerenciamento

Os quadros de gerenciamento unicast classe 3 são protegidos com a aplicação de AES-CCMP ou TKIP de forma semelhante à usada para quadros de dados. Partes do cabeçalho do quadro são copiadas no componente de payload criptografado de cada quadro para maior proteção, conforme discutido nas próximas seções.

Estes tipos de quadros estão protegidos:

- Desassociação
- Desautenticação
- Quadros de ação de QoS (WMM)

Os quadros de dados protegidos por AES-CCMP e TKIP incluem um contador de sequência nos campos IV, que é usado para impedir a detecção de repetição. O contador de transmissão atual é usado para quadros de dados e gerenciamento, mas um novo contador de recebimento é usado para quadros de gerenciamento. Os contadores de recepção são testados para garantir que cada quadro tenha um número maior que o último quadro recebido (para garantir que os quadros sejam únicos e não tenham sido reproduzidos), portanto, não importa que esse esquema faça com que os valores recebidos sejam não sequenciais.

Relatórios de erros

Os mecanismos de relatório MFP-1 são usados para relatar erros de desencapsulamento de quadros de gerenciamento detectados por pontos de acesso. Ou seja, a WLC coleta estatísticas de erro de validação de MFP e encaminha periodicamente informações coladas para o WCS.

Os erros de violação de MFP detectados por estações clientes são tratados pelo recurso CCXv5 Roaming e Real Time Diagnostics e não estão no escopo deste documento.

Proteção de Quadro de Gerenciamento de Broadcast

Para evitar ataques que usam quadros de broadcast, os APs que suportam CCXv5 não

transmitem nenhum quadro de gerenciamento de classe 3 de broadcast (ou seja, desassoc, deauth ou ação), exceto quadros de desautenticação/desassociação de contenção de invasão. As estações cliente com capacidade para CCXv5 devem descartar quadros de gerenciamento de classe 3 de broadcast. Supõe-se que as sessões de MFP estejam em uma rede adequadamente segura (autenticação forte mais TKIP ou CCMP), de modo que o desrespeito por broadcasts de contenção não autorizados não seja um problema.

Da mesma forma, os APs descartam quadros de gerenciamento de broadcast de entrada. Não há suporte para nenhum quadro de gerenciamento de broadcast de entrada no momento, portanto, não é necessário alterar o código para isso.

Plataformas suportadas

Essas plataformas são suportadas:

- Controladores WLAN200621064400WiSM3750 com controlador 440x incorporado28/26/37/38xx Roteadores
- Pontos de acesso LWAPPAP 1000AP 1100, 1130AP 1200, 1240, 1250AP 1310
- Software clienteADU 3.6.4 e superior
- Sistemas de Gerenciamento de RedeWCS

O AP LWAPP de malha 1500 não é suportado nesta versão.

Modos suportados

Os access points baseados em LWAPP que operam nesses modos suportam o MFP do cliente:

Modos de ponto de acesso suportados	
Modo	**Suporte MFP do cliente**
Local	Yes
Monitor	No
Farejador	No
Detector de Rogue	No
REAP híbrido	Yes
REAP	No
Raiz da Bridge	Yes
WGB	No

Suporte a células mistas

As estações clientes que não têm capacidade para CCXv5 podem se associar a uma WLAN MFP-2. Os pontos de acesso controlam quais clientes são compatíveis com MFP-2 e quais não são para determinar se as medidas de segurança MFP-2 são aplicadas aos quadros de gerenciamento unicast de saída e esperadas nos quadros de gerenciamento unicast de entrada.

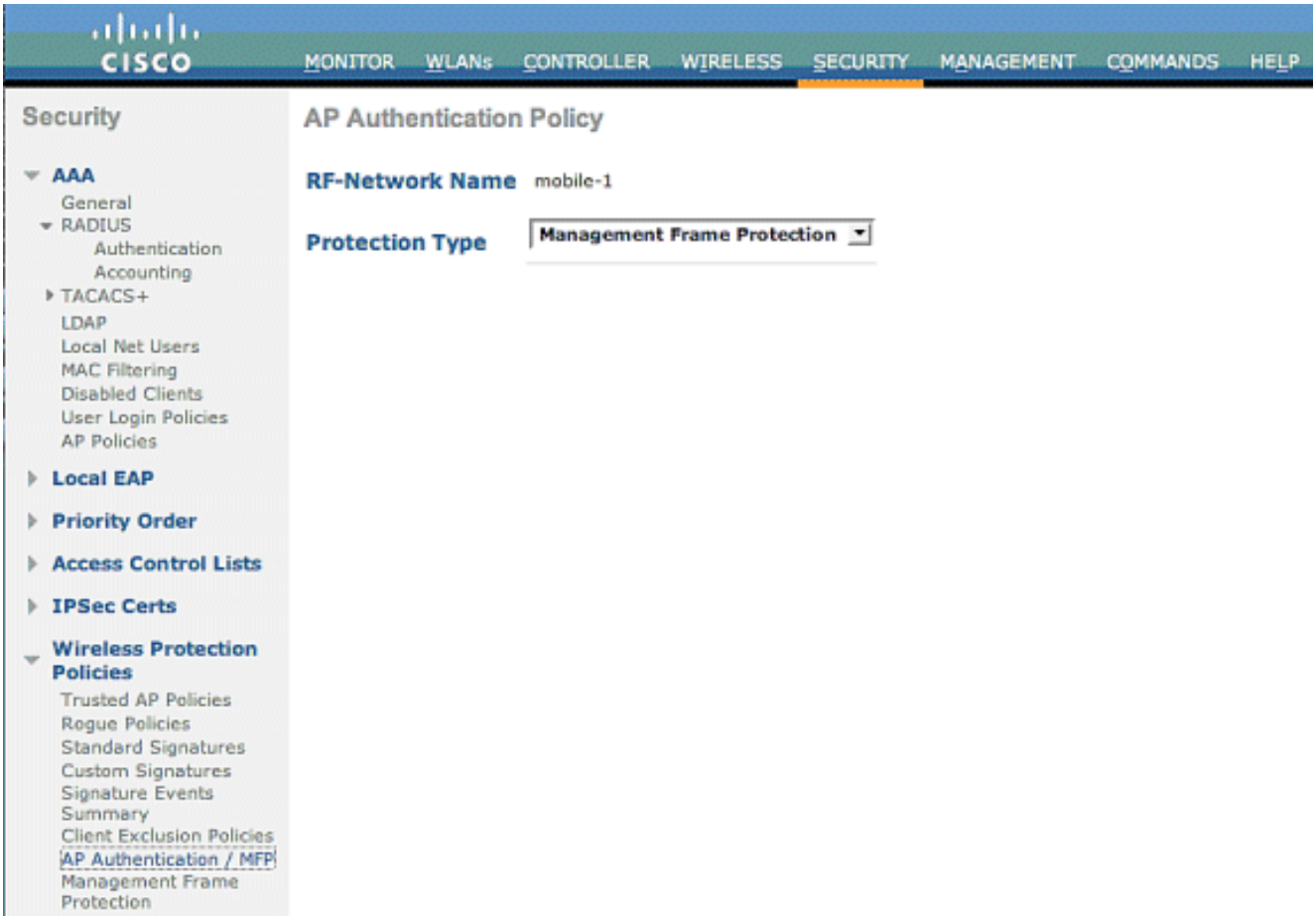
Configurar

Configurar o MFP em um controlador

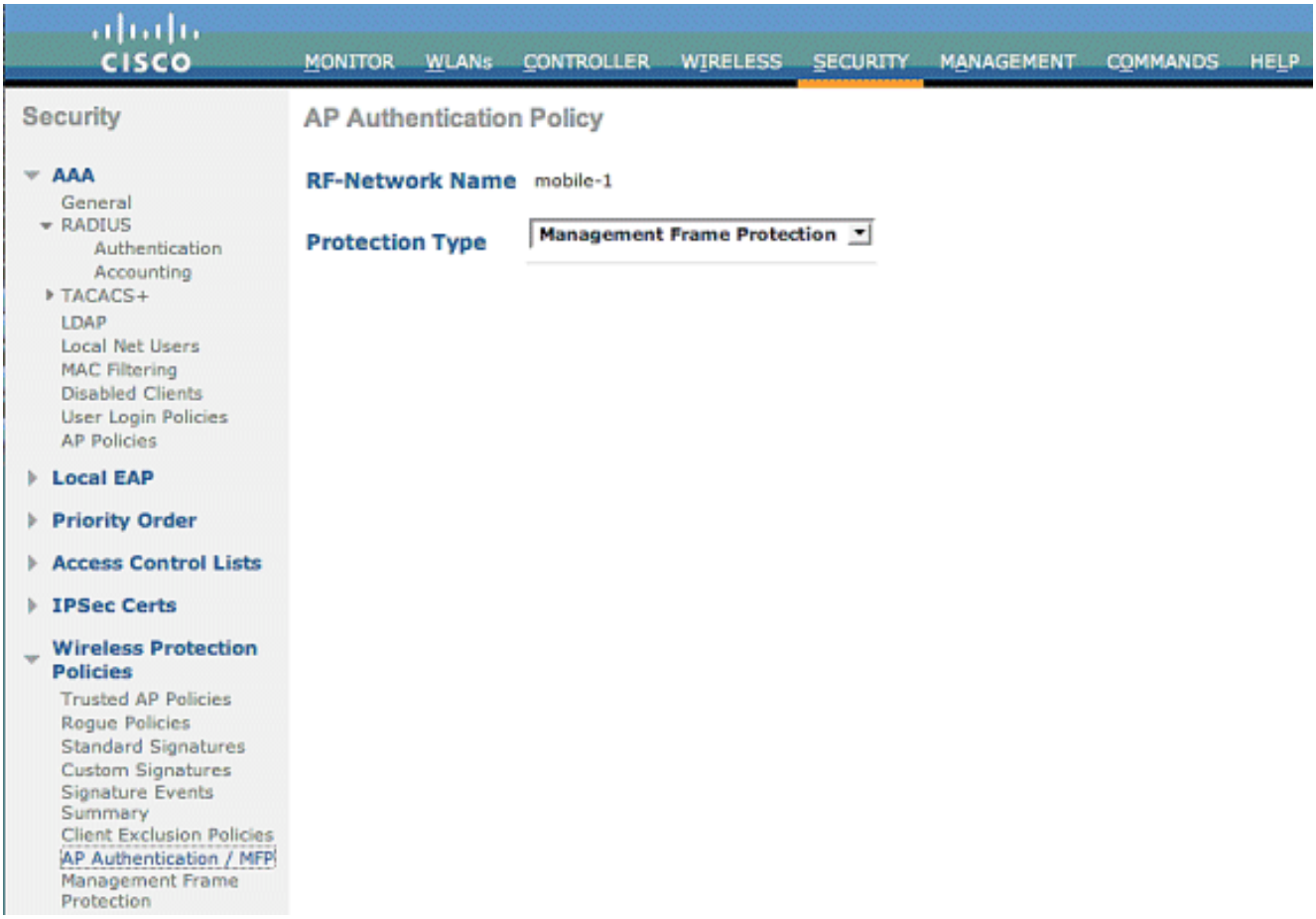
Você pode configurar globalmente o MFP em um controlador. Ao fazê-lo, a **proteção e validação do quadro de gestão são ativadas por predefinição para cada ponto de acesso associado**, e a autenticação do ponto de acesso é desativada automaticamente.

Execute estas etapas para configurar o MFP globalmente em um controlador.

1. No controller GUI, clique em **Security**. Na tela resultante, clique em **Autenticação de AP/MFP** em **Políticas de proteção sem fio**.



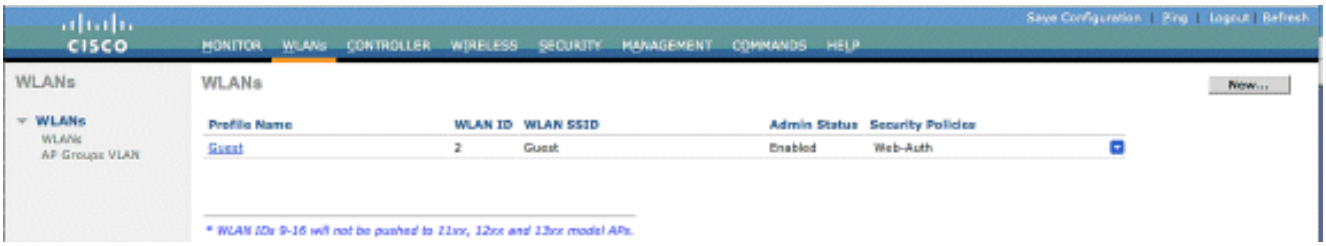
2. Na Política de autenticação do AP, escolha **Proteção de quadro de gerenciamento** no menu suspenso **Tipo de proteção** e clique em **Aplicar**.



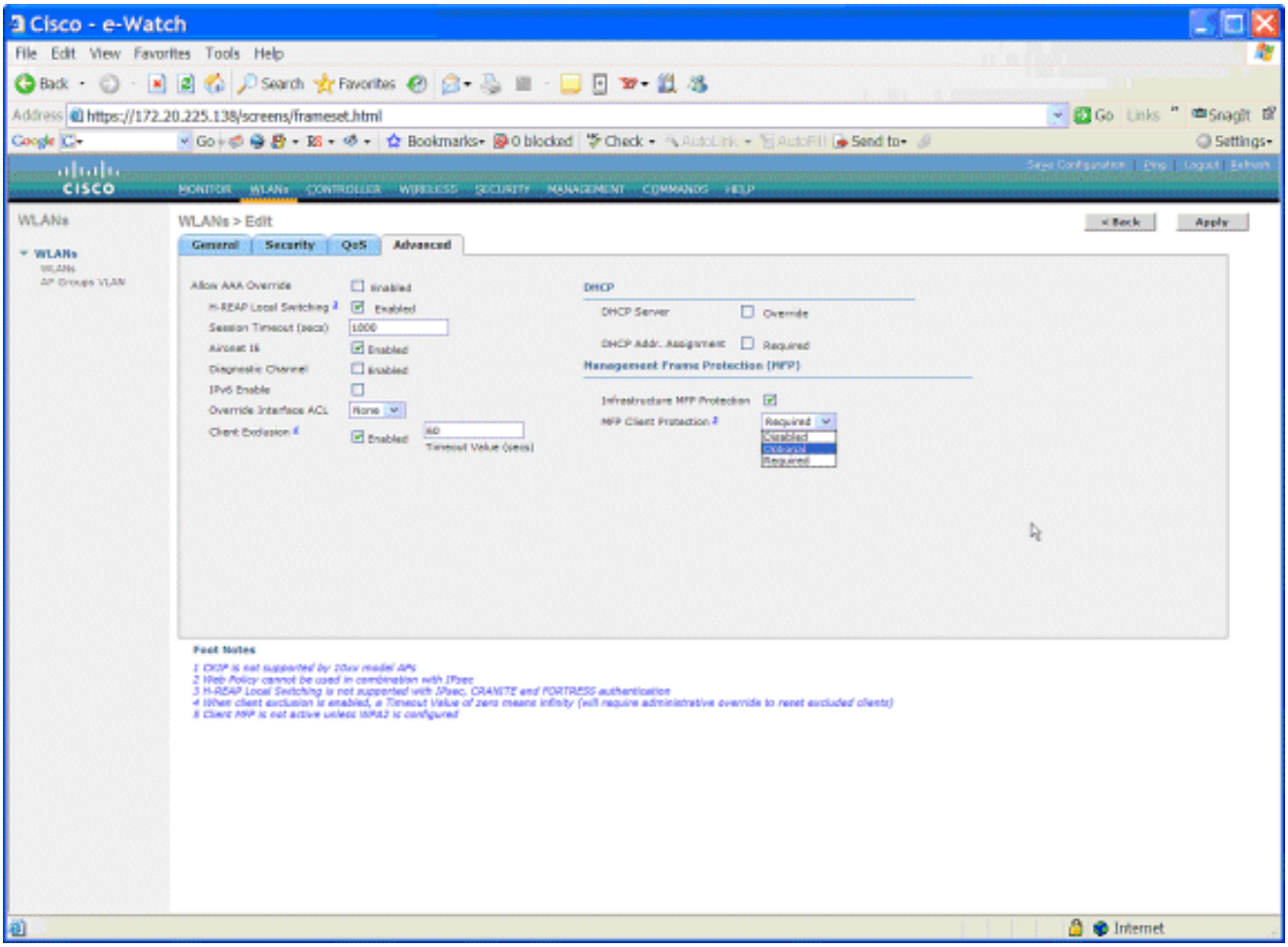
Configurar MFP na WLAN

Você também pode habilitar/desabilitar a proteção MFP da infraestrutura e o MFP do cliente em cada WLAN configurada na WLC. Ambos são ativados por padrão através da proteção MFP de infraestrutura, que só é ativa se globalmente habilitada, e o MFP do cliente só é ativo se a WLAN estiver configurada com segurança WPA2. Siga estas etapas para ativar o MFP em uma WLAN:

1. Na GUI da WLC, clique em **WLANs** e clique em **New** para criar uma nova WLAN.

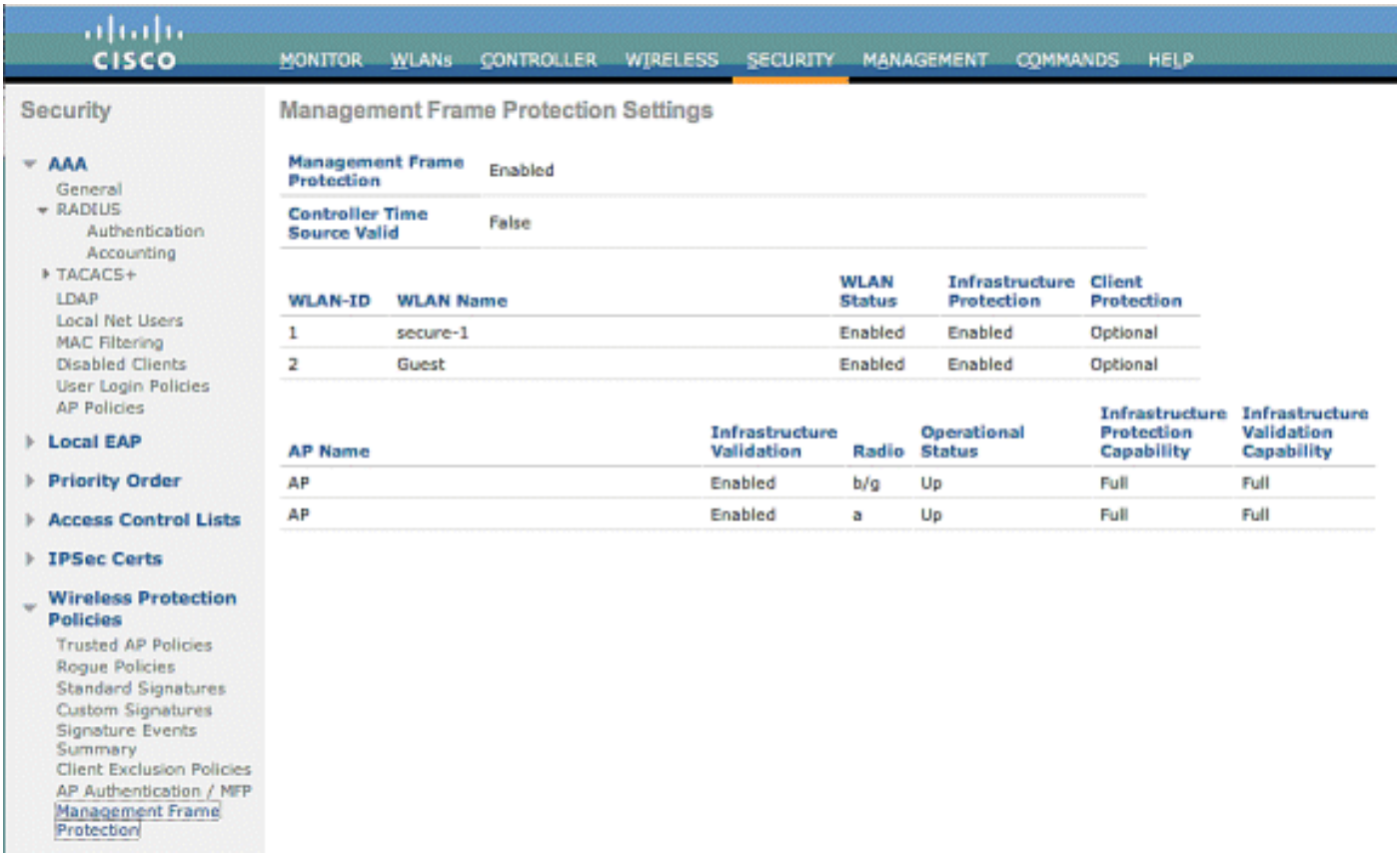


2. Na página de edição de WLANs, vá para a guia *Avançado* e marque a caixa de seleção **Proteção MFP de infraestrutura** para ativar o MFP de infraestrutura nesta WLAN. Para desabilitar a proteção de MFP de infraestrutura para esta WLAN, desmarque essa caixa de seleção. Para habilitar o MFP do cliente, escolha a opção necessária ou opcional no menu suspenso. Se você escolher Cliente MFP= Obrigatório, verifique se todos os seus clientes têm suporte para MFP-2 ou se eles não conseguem se conectar. Se você escolher opcional, os clientes habilitados para MFP e não para MFP podem se conectar na mesma WLAN.



Verificar

Para verificar as configurações de MFP na GUI, clique em **Proteção de Quadro de Gerenciamento** em Políticas de Proteção Sem Fio na página Segurança. Isso o leva à página Configurações de MFP.



Na página Configurações de MFP, você pode ver a configuração de MFP na WLC, LAP e WLAN. Este é um exemplo.

- O campo Management Frame Protection mostra se o MFP está ativado globalmente para o WLC.
- O campo Controller Time Source Valid indica se o tempo da WLC é definido localmente (pela entrada manual do tempo) ou através de uma fonte externa (como um servidor NTP). Se a hora for definida por uma fonte externa, o valor desse campo será "Verdadeiro". Se a hora for definida localmente, o valor será "Falso". A origem de tempo é usada para validar quadros de gerenciamento entre pontos de acesso de diferentes WLCs que também têm mobilidade configurada.**Observação:** se o MFP estiver habilitado em todas as WLCs em um grupo de RF/mobilidade, é sempre recomendável que você use um servidor NTP para definir o tempo do WLC em um grupo de mobilidade.
- O campo **Proteção MFP** mostra se o MFP está habilitado para WLANs individuais.
- O campo **Validação de MFP** mostra se o MFP está habilitado para pontos de acesso individuais.

Esses comandos show podem ser úteis:

- **show wps summary** —Use este comando para ver um resumo das políticas de proteção sem fio atuais (que inclui MFP) da WLC.
- **show wps mfp summary** — Para ver a configuração de MFP global atual da WLC, insira este comando.
- **show ap config general** *AP_name* —Para ver o estado atual do MFP para um ponto de acesso específico, insira este comando.

Este é um exemplo da saída do comando **show ap config general** *AP_name*:

```
(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 é um exemplo da saída do comando **show wps mfp summary**:

```
(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
```

Esses comandos debug podem ser úteis;

- **debug wps mfp lwapp** — Mostra informações de depuração para mensagens MFP.
- **debug wps mfp detail** — Mostra informações detalhadas de depuração para mensagens MFP.
- **debug wps mfp report** —Mostra informações de depuração para relatórios MFP.
- **debug wps mfp mm** — Mostra informações de depuração para mensagens de mobilidade MFP (entre controladores).

Observação: também há vários sniffers de pacote sem fio disponíveis na Internet, que podem ser usados para capturar e analisar os quadros de gerenciamento 802.11. Alguns exemplos de sniffers de pacotes são o Omnipeek e o Wireshark.

Informações Relacionadas

- Configuração de soluções de segurança: Guia de configuração de WLC
- Configurando soluções de segurança no WCS
- Exemplo de Configuração de Autenticação EAP com Controladores WLAN (WLC)
- Exemplo de configuração de ACLs em Wireless LAN Controller
- Exemplo de configuração de autenticação de web externa com Wireless LAN Controllers
- "Atribuição da VLAN dinâmica com um exemplo de configuração do servidor RADIUS e do controlador LAN sem fio
- Cisco Secure Services Client com autenticação EAP-FAST
- Perguntas frequentes sobre WLC
- Página de Suporte Wireless
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.