Guia de implantação e configuração adaptável do wIPS ELM

Contents

Introdução

A solução Cisco Adaptive Wireless Intrusion Prevention System (wIPS) adiciona o recurso Enhanced Local Mode (ELM), permitindo que os administradores usem seus access points (APs) implantados para fornecer proteção abrangente sem a necessidade de uma rede de sobreposição separada (Figura 1). Antes do ELM e na implantação tradicional Adaptive wIPS, os APs MM (modo de monitor dedicado) são necessários para fornecer as necessidades de conformidade com PCI ou proteção contra acesso de segurança, penetração e ataques não autorizados (Figura 2). O ELM fornece efetivamente uma oferta comparável que facilita a implementação de segurança wireless ao passo que reduz as despesas de CapEx e OpEx. Este documento se concentra apenas no ELM e não modifica nenhum benefício de implantação do wIPS existente com APs MM.

Figura 1 - Implantação do AP no modo local aprimorado

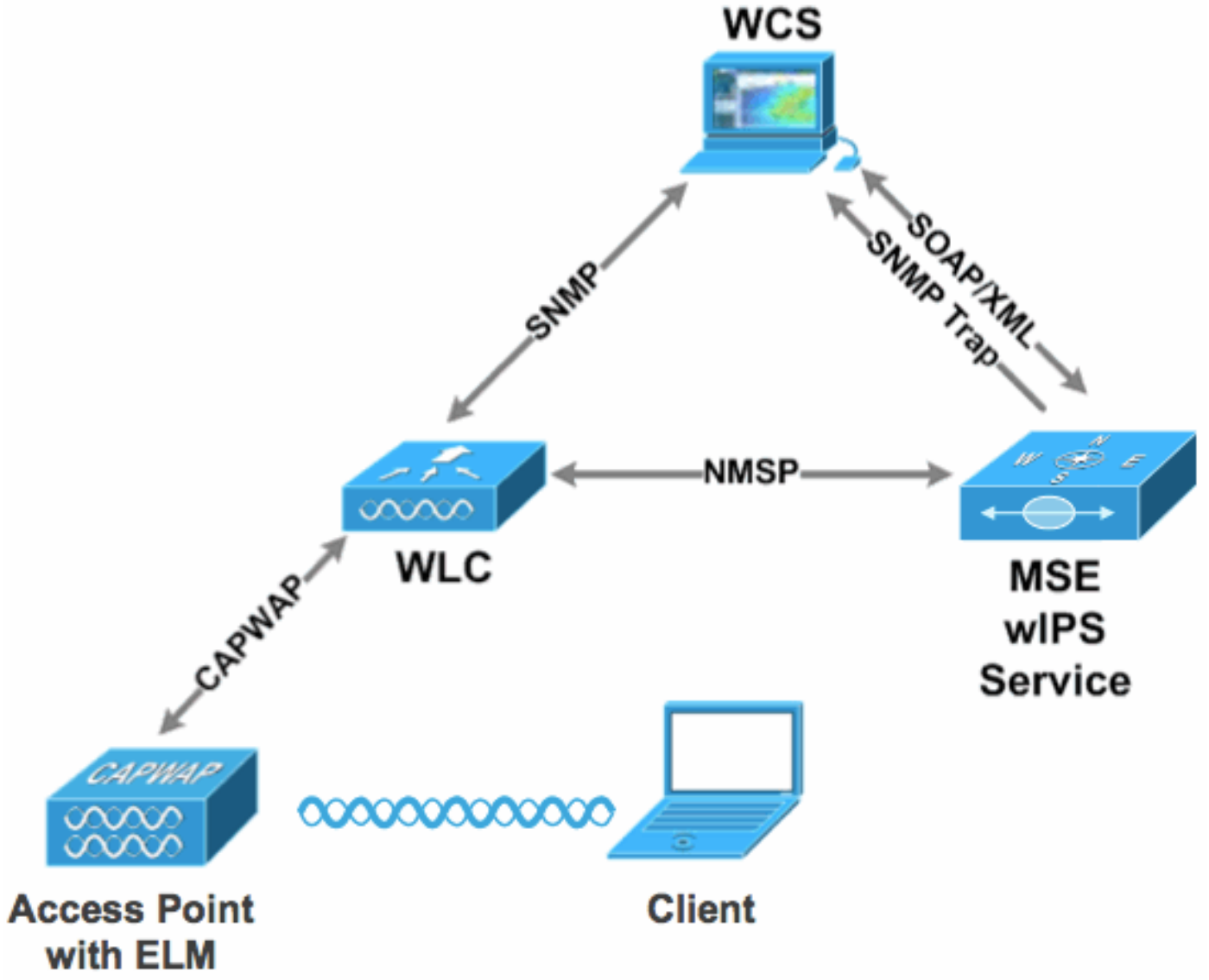
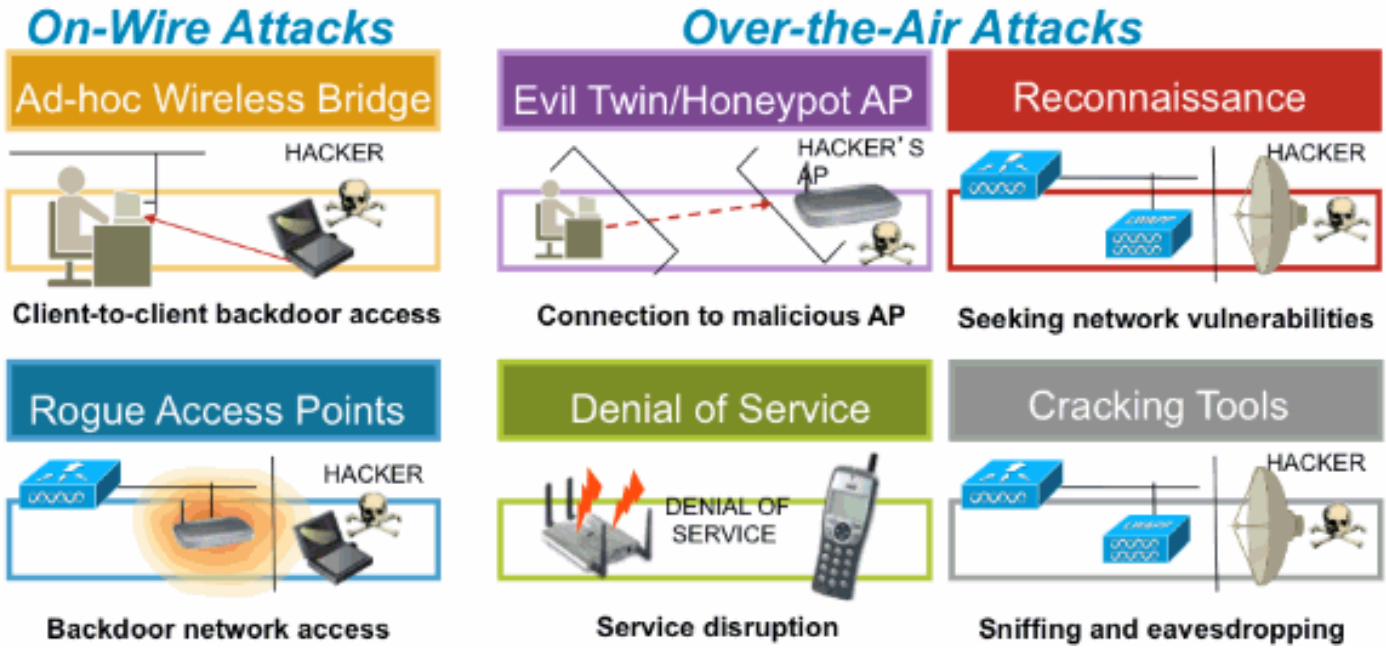


Figura 2 - Principais ameaças à segurança sem fio



Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Componentes obrigatórios do ELM e versões de código mínimas

- Controladora Wireless LAN (WLC) - Versão 7.0.116.xx ou posterior
- APs - Versão 7.0.116.xx ou posterior
- Wireless Control System (WCS) - Versão 7.0.172.xx ou posterior
- Mobility Services Engine - Versão 7.0.201.xx ou posterior

Suporte a plataformas WLC

O ELM é suportado nas plataformas WLC5508, WLC4400, WLC 2106, WLC2504, WiSM-1 e WiSM-2WLC.

Suporte a APs

O ELM é suportado em APs 11n, incluindo 3500, 1250, 1260, 1040 e 1140.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Conventions

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

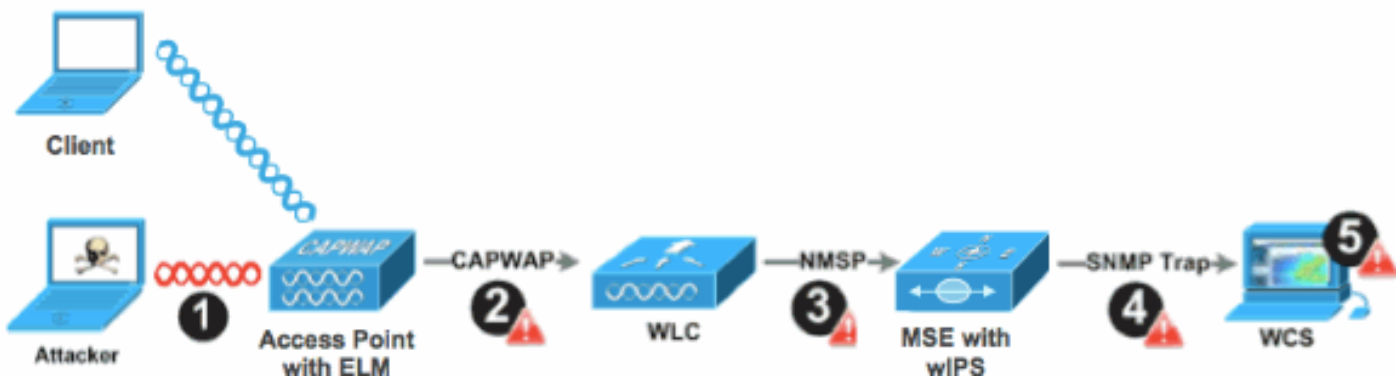
Fluxo de alarme do ELM wIPS

Os ataques só são relevantes quando ocorrem em APs de infraestrutura confiáveis. Os APs ELM detectarão e se comunicarão com a controladora e se correlacionarão com o MSE para gerar relatórios com o gerenciamento do WCS. A Figura 3 fornece o fluxo de alarme do ponto de vista de um administrador:

1. Ataque iniciado contra um dispositivo de infraestrutura (AP "confiável")
2. Detectado em AP ELM comunicado através de CAPWAP para WLC

3. Transmitido de forma transparente para o MSE via NMSP
4. Conectado ao banco de dados wIPS no MSE Enviado ao WCS via interceptação SNMP
5. Exibido no WCS

Figura 3 - Detecção de ameaças e fluxo de alarme



Considerações de implantação para ELM

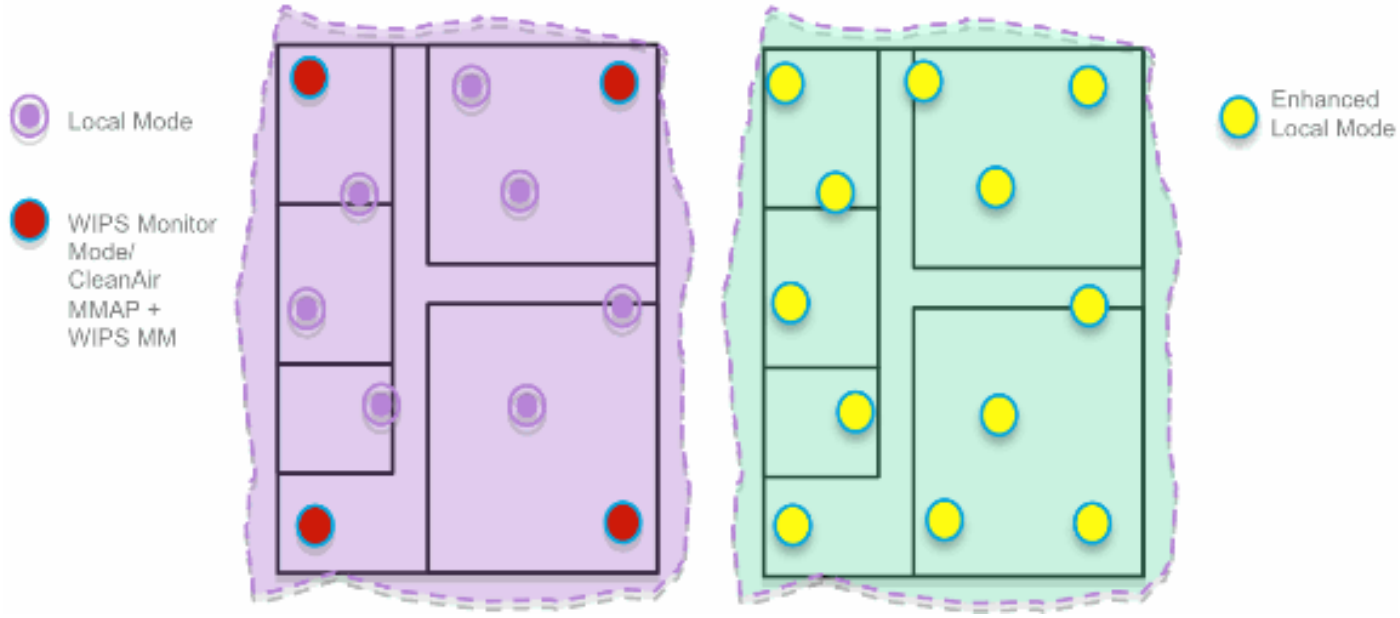
A Cisco recomenda que, ao habilitar o ELM em cada AP na rede, você atenda à maioria das necessidades de segurança do cliente quando uma sobreposição de rede e/ou custos fizerem parte da consideração. O recurso principal do ELM opera com eficiência para ataques no canal, sem comprometer o desempenho em dados, clientes de voz e vídeo e serviços.

ELM versus MM dedicado

A Figura 4 fornece um contraste geral entre as implantações padrão de APs MM wIPS e ELM. Em revisão, o intervalo de cobertura típico para ambos os modos sugere:

- O AP wIPS MM dedicado normalmente cobre de 15.000 a 35.000 pés quadrados
- O AP de atendimento ao cliente normalmente cobre de 3.000 a 5.000 pés quadrados

Figura 4 - Sobreposição de MM vs Todos os APs ELM



Na implantação Adaptive wIPS tradicional, a Cisco recomenda uma proporção de AP de 1 MM para cada 5 APs de modo local, que também podem variar com base no projeto de rede e orientação especializada para melhor cobertura. Ao considerar o ELM, o administrador simplesmente ativa o recurso de software ELM para todos os APs existentes, adicionando efetivamente as operações do MM wIPS ao AP do modo de servidor de dados local enquanto mantém o desempenho.

Desempenho no canal e fora do canal

Um AP MM utiliza 100% do tempo do rádio para a varredura de todos os canais, já que ele não atende a nenhum cliente WLAN. O principal recurso do ELM opera efetivamente para ataques no canal, sem nenhum comprometimento do desempenho em clientes e serviços de dados, voz e vídeo. A principal diferença está no modo local que varia a varredura fora do canal; dependendo da atividade, a varredura fora do canal oferece tempo de permanência mínimo para reunir informações suficientes disponíveis para classificar e determinar ataques. Um exemplo pode ser com clientes de voz que estão associados e onde a verificação de RRM do AP é adiada até que o cliente de voz seja desassociado para garantir que o serviço não seja afetado. Por isso, a detecção do ELM durante o canal externo é considerada o melhor esforço. Os APs ELM vizinhos que operam em todos os canais, países ou DCA aumentam a eficácia, portanto, a recomendação para ativar o ELM em todos os APs de modo local para cobertura de proteção máxima. Se o requisito for a varredura dedicada em todos os canais em tempo integral, a recomendação será implantar APs MM.

Estes pontos revisam as diferenças do modo local e dos APs MM:

- AP no modo local - atende clientes de WLAN com verificação fora do canal de divisão de tempo, escuta 50 ms em cada canal e apresenta verificação configurável para todos os canais/país/DCA.
- AP no modo de monitor - Não atende clientes WLAN, dedicados apenas à verificação, escuta 1.2s em cada canal e examina todos os canais.

ELM em links WAN

A Cisco fez grandes esforços para otimizar recursos em cenários desafiadores, como a implantação de APs ELM em links WAN de baixa largura de banda. O recurso ELM envolve o pré-processamento na determinação de assinaturas de ataque no AP e é otimizado para funcionar em links lentos. Como práticas recomendadas, é recomendável testar e medir a linha de base para validar o desempenho com ELM sobre WAN.

Integração com o CleanAir

O recurso ELM complementa altamente as operações da CleanAir com desempenho e benefícios semelhantes à implantação de APs MM com os seguintes benefícios existentes sensíveis ao espectro da CleanAir:

- Inteligência RF dedicada em nível de silício
- Detecção de espectro, autorrecuperação e auto-otimização
- Detecção e mitigação de interferência e ameaças de canal fora do padrão
- Detecção sem Wi-Fi, como Bluetooth, micro-ondas, telefones sem fio, etc.
- Detectar e localizar ataques DOS da camada de RF, como bloqueadores de RF

Recursos e benefícios do ELM

- Varredura wIPS adaptável em dados que servem APs locais e H-REAP
- Proteção sem exigir uma rede de sobreposição separada
- Disponível como download gratuito de software para clientes de wIPS existentes
- Suporta conformidade PCI para LANs sem fio
- Detecção completa de ataques de 802.11 e não-802.11
- Adiciona recursos de computação forense e de geração de relatórios
- Integra-se com o gerenciamento CUWM e WLAN existente
- Flexibilidade para definir APs MM integrados ou dedicados
- O pré-processamento nos APs minimiza o backhaul de dados (isto é, funciona em links com largura de banda muito baixa)
- Baixo impacto nos dados de serviço

Licenciamento ELM

O ELM wIPS adiciona uma nova licença ao pedido:

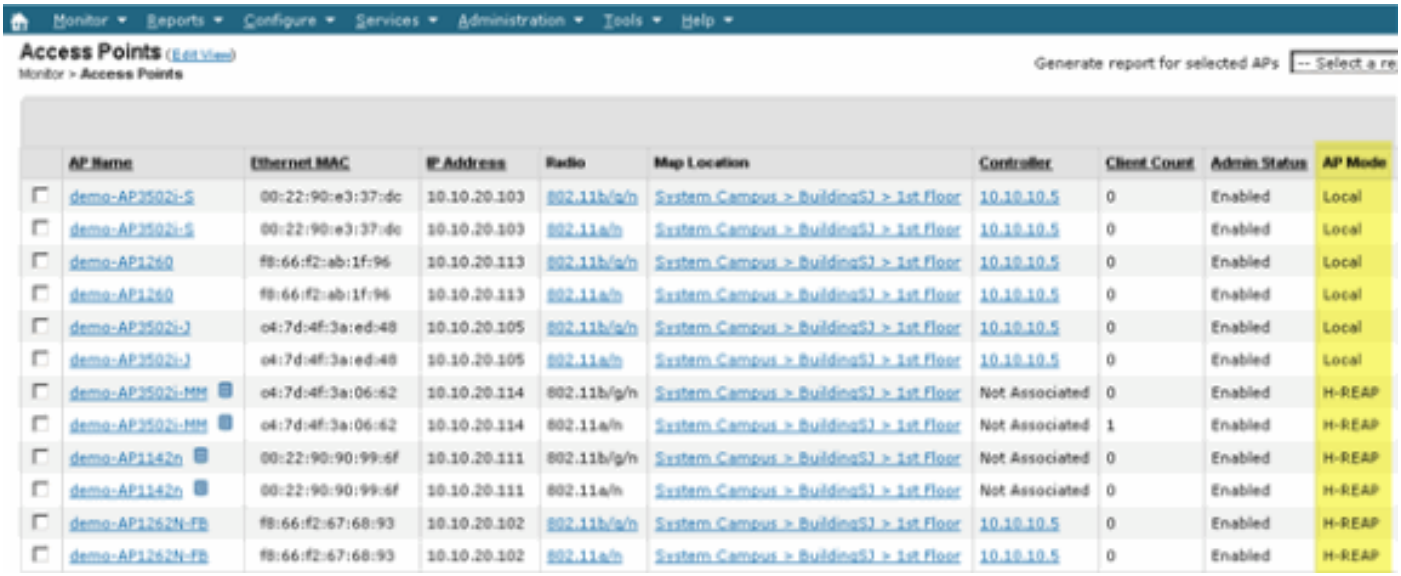
- AIR-LM-WIPS-xx - Licença do Cisco ELM wIPS
- AIR-WIPS-AP-xx - Licença Cisco Wireless wIPS

Observações adicionais sobre o licenciamento do ELM:

- Se as SKUs de licença do AP MM wIPS já estiverem instaladas, essas licenças também poderão ser usadas para APs ELM.
- As licenças wIPS e ELM juntas contam para os limites de licença de plataforma para o mecanismo wIPS; 2.000 APs no 3310 e 3.000 APs no 335x, respectivamente.
- A licença de avaliação incluirá 10 APs para wIPS e 10 para ELM por um período de até 60 dias. Antes do ELM, a licença de avaliação permitia até 20 APs wIPS MM. O requisito mínimo de versões de software que suportam o ELM deve ser atendido.

Configurar ELM com WCS

Figura 5 - Uso do WCS para configurar o ELM

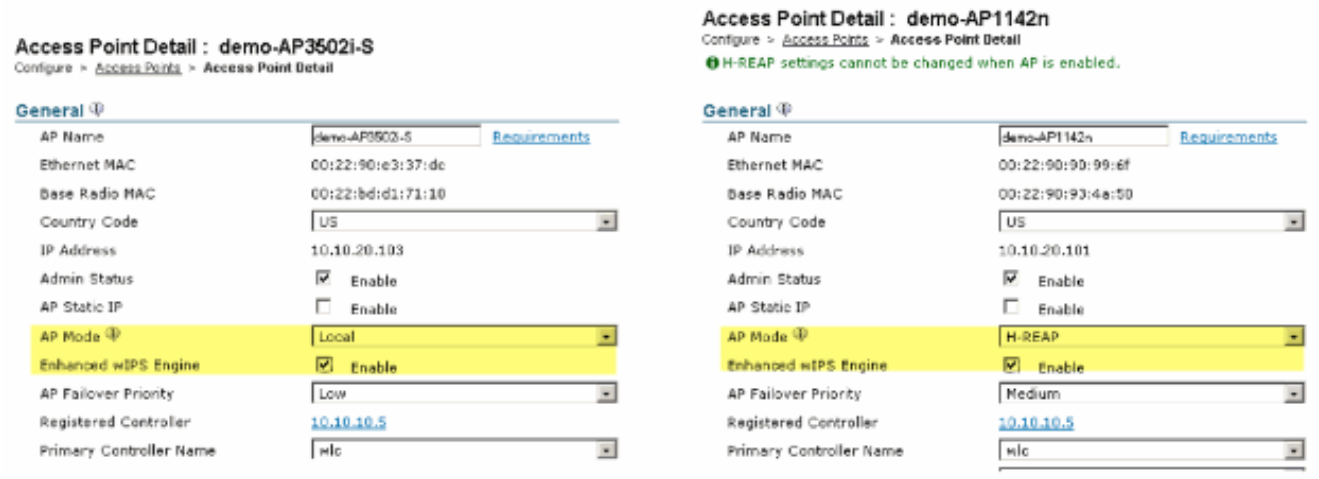


1. No WCS, desabilite os rádios 802.11b/g e 802.11a do AP antes de habilitar o "Enhanced wIPS Engine".

   Observação: todos os clientes associados serão desconectados e não ingressarão até que os rádios sejam habilitados.

2. Configure um AP ou use um modelo de configuração do WCS para vários APs leves. Consulte a Figura 6.

   Figura 6 - Ativar o submodo do Mecanismo Avançado de wIPS (ELM)



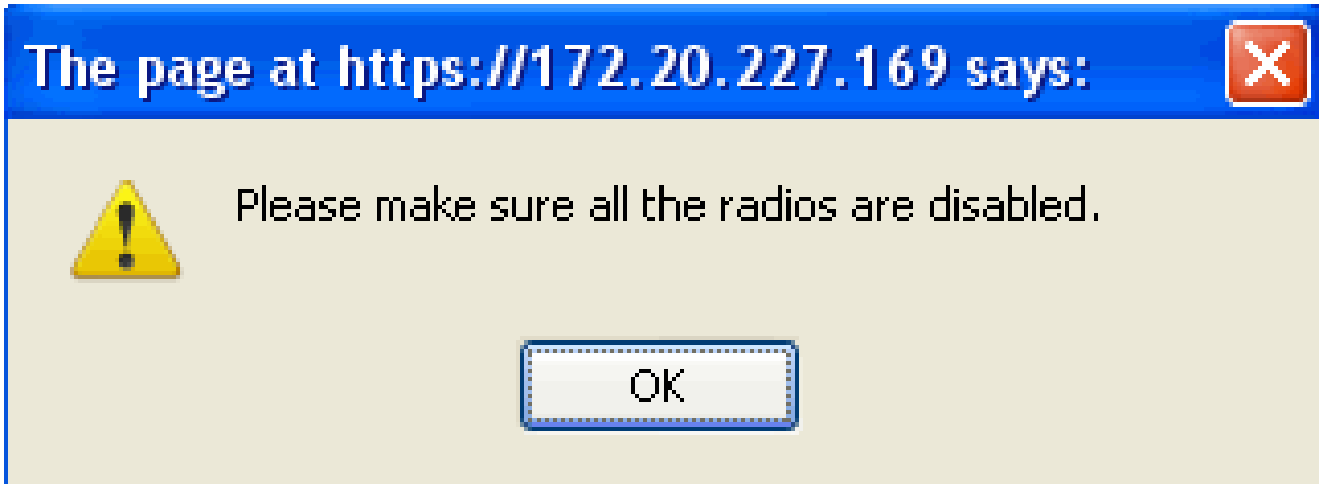
3. Escolha Enhanced wIPS Engine e clique em Save.

    a. Habilitar o mecanismo wIPS aprimorado não fará com que o AP seja reinicializado.

    b. H-REAP é suportado; habilite da mesma maneira que para AP de modo local.

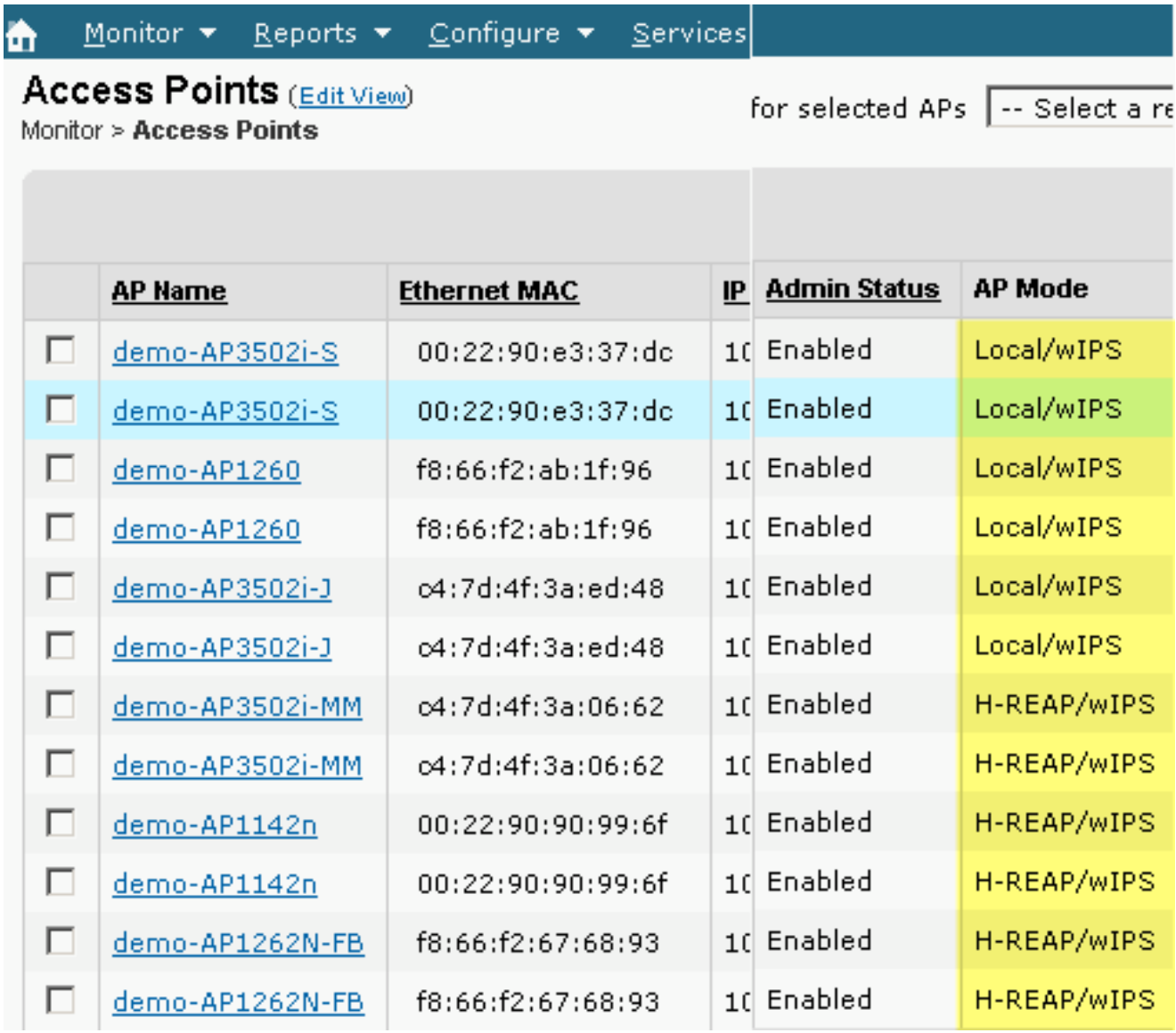
    Observação: se qualquer um dos rádios desse AP estiver habilitado, o WCS ignorará a configuração e lançará o erro na Figura 7.

    Figura 7 - Lembrete do WCS para desativar rádios AP antes de ativar o ELM



4. O sucesso da configuração pode ser verificado observando-se a mudança no modo AP de "Local ou H-REAP" para Local/wIPS ou H-REAP/wIPS. Consulte a Figura 8.

    Figura 8 - WCS exibindo o modo AP para incluir wIPS com local e/ou H-REAP

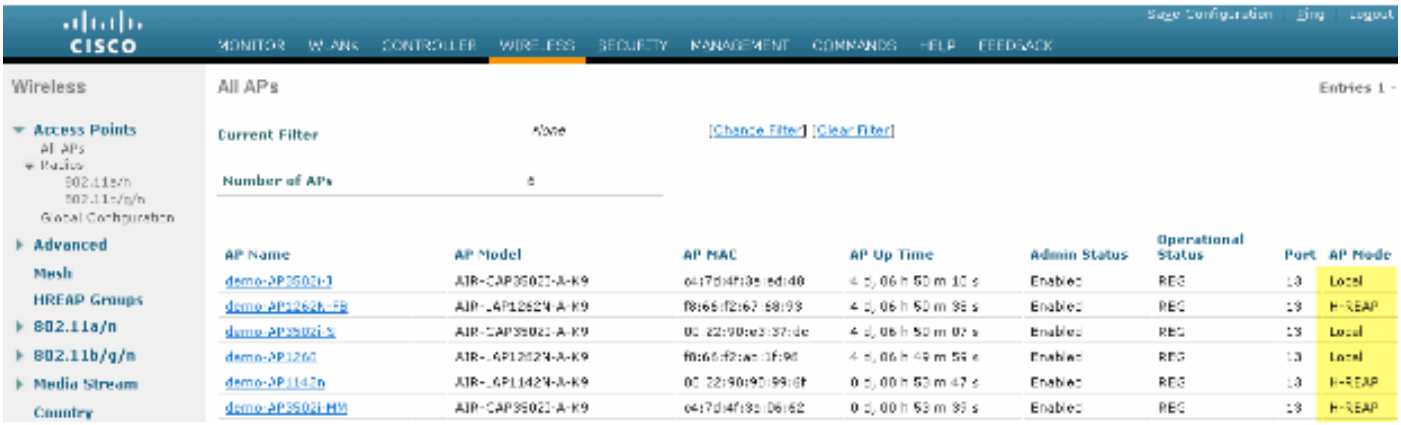


5. Ative os rádios que foram desativados na Etapa 1.
6. Crie o perfil wIPS e envie-o ao controlador para que a configuração seja concluída.

   Observação: para obter informações de configuração completas sobre o wIPS, consulte o Guia de implantação do Cisco Adaptive wIPS.

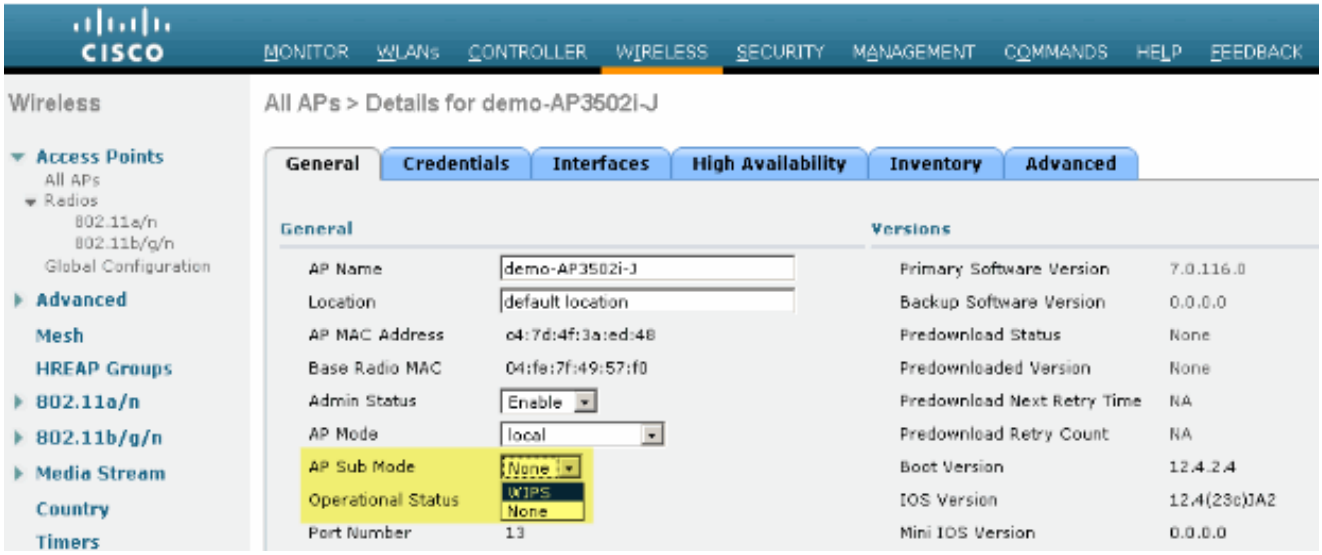
Configuração do WLC

Figura 9 - Configurar o ELM com WLC



1. Escolha um AP na guia Wireless.

   Figura 10 - WLC alterando o submodo do AP para incluir wIPS ELM



2. No menu suspenso AP Sub Mode, escolha wIPS (Figura 10).

3. Aplique e salve a configuração.

Observação: para que a funcionalidade do ELM funcione, o MSE e o WCS são necessários com o licenciamento wIPS. Alterar o submodo do AP apenas da WLC não habilitará o ELM.

Ataques detectados no ELM

Tabela 1 - Matriz de suporte de assinaturas wIPS

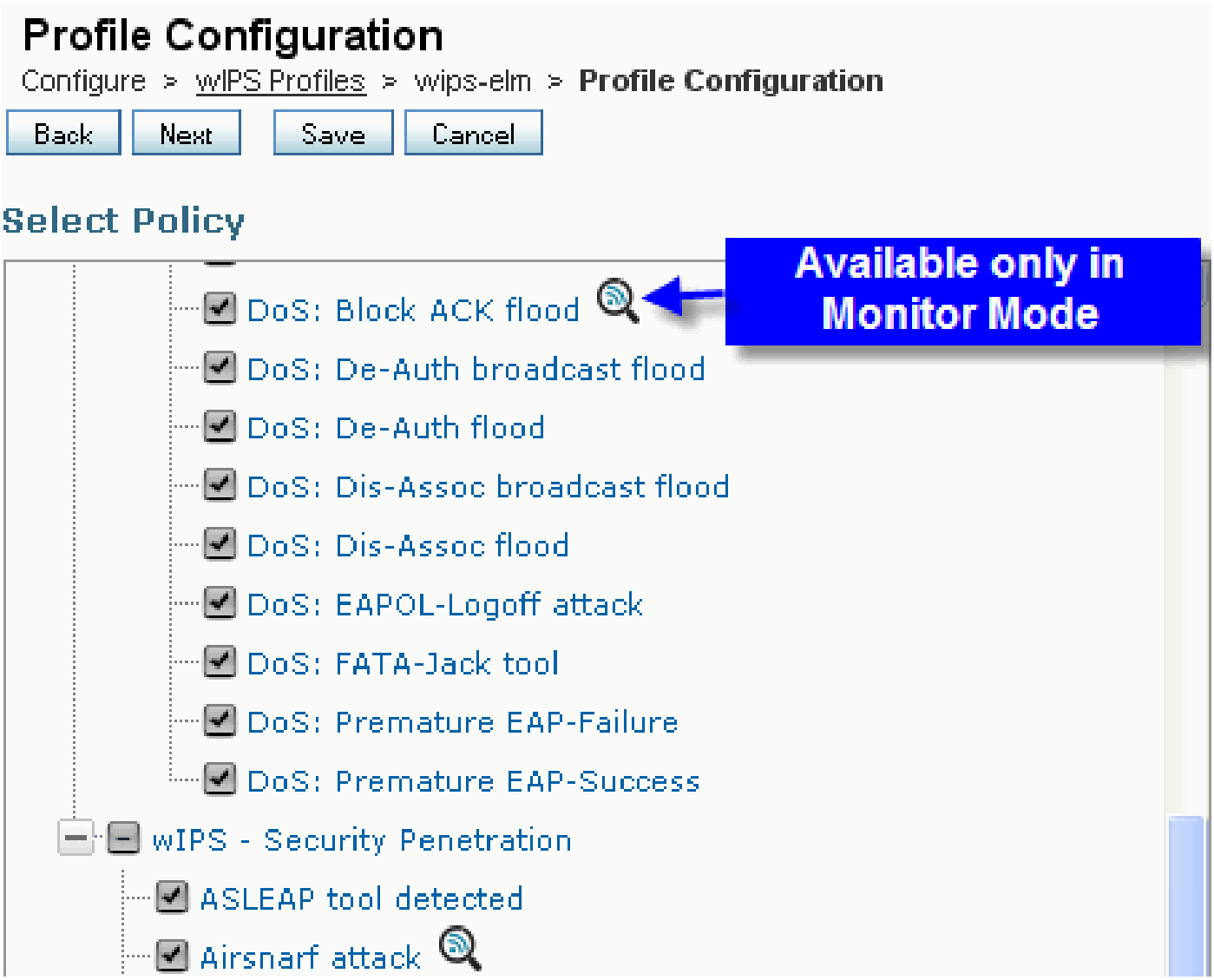
Ataques detectados	ELM	MM
Ataque DoS contra AP		
Inundação de Associação	Y	Y
Estouro da Tabela de Associação	Y	Y
Inundação de Autenticação	Y	Y
Ataque EAPOL-Start	Y	Y

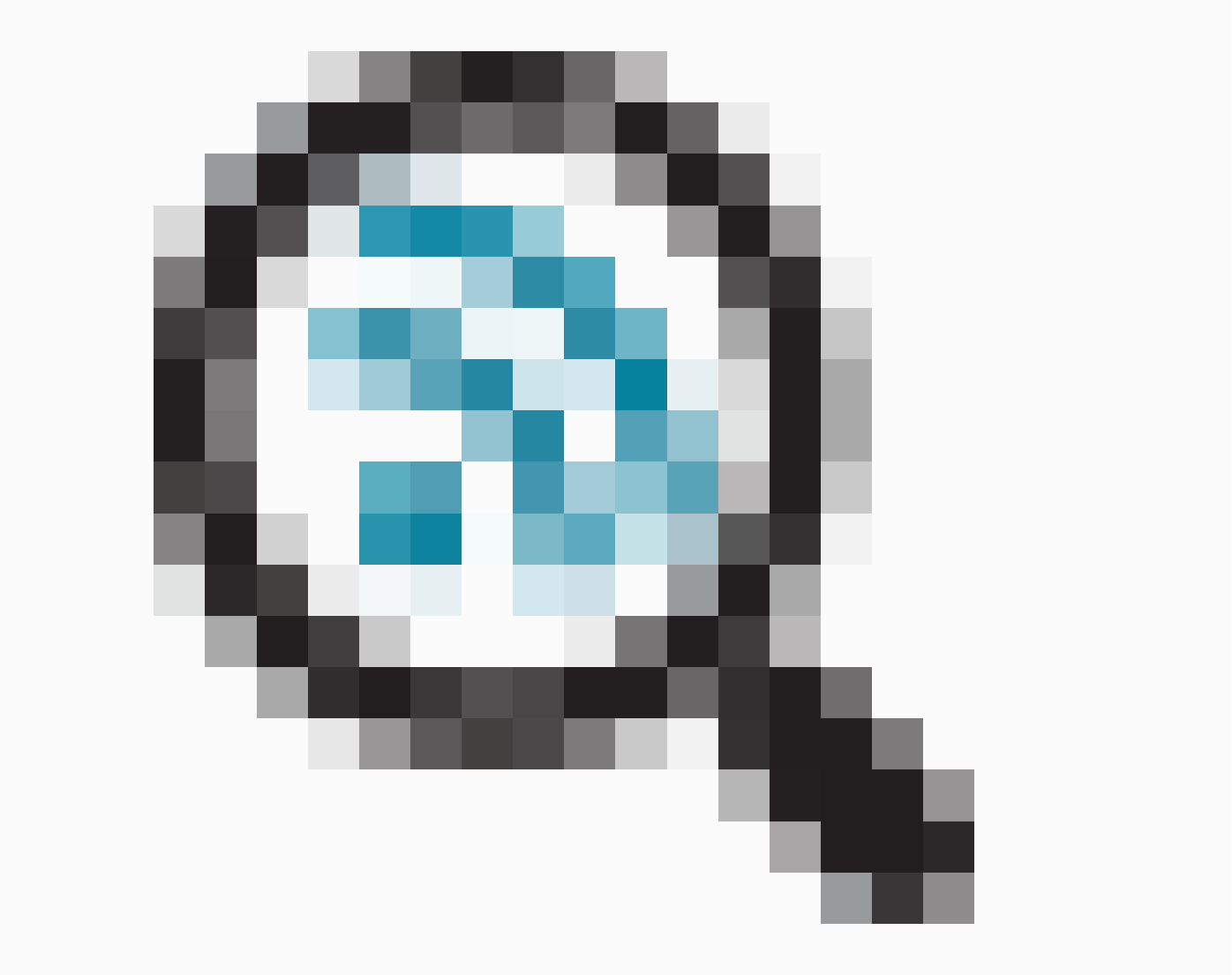
Inundação de PS-Poll	Y	Y
Inundação de solicitação de sondagem	N	Y
Associação não autenticada	Y	Y
Ataque de DoS contra a infraestrutura		
inundação de CTS	N	Y
Exploração da Universidade de Tecnologia de Queensland	N	Y
interferência de RF	Y	Y
inundação de RTS	N	Y
Ataque de portadora virtual	N	Y
Ataque de DoS contra estação		
Ataque de falha de autenticação	Y	Y
Inundação ACK de bloco	N	Y
Inundação de transmissão de De-Auth	Y	Y
Inundação de De-Auth	Y	Y
Inundação de broadcast Dis-Assoc	Y	Y
inundação de Dis-Assoc	Y	Y
Ataque EAPOL-Logoff	Y	Y
ferramenta de conector FATA	Y	Y
Falha prematura de EAP	Y	Y
EAP-Êxito Prematuro	Y	Y
Ataques de penetração de segurança		
ferramenta ASLEAP detectada	Y	Y
Ataque Airsnarf	N	Y
Ataque ChopChop	Y	Y
Ataque de dia zero por anomalia na segurança da WLAN	N	Y
Ataque de dia zero por anomalia na segurança do dispositivo	N	Y
Sondagem de dispositivos para APs	Y	Y
Ataque de dicionário em métodos EAP	Y	Y
Ataque de EAP contra a autenticação 802.1x	Y	Y
APs falsos detectados	Y	Y
Servidor DHCP falso detectado	N	Y

Ferramenta de trinca FAST WEP detectada	Y	Y
Ataque de fragmentação	Y	Y
AP Honeypot detectado	Y	Y
Ferramenta Hotspotter detectada	N	Y
Quadros de broadcast inadequados	N	Y
Pacotes 802.11 malformados detectados	Y	Y
Homem no meio do ataque	Y	Y
Netstumbler detectado	Y	Y
Vítima do Netstumbler detectada	Y	Y
Violação de PSPF detectada	Y	Y
AP soft ou AP host detectado	Y	Y
Endereço MAC falsificado detectado	Y	Y
Detectado tráfego suspeito fora do horário comercial	Y	Y
Associação não autorizada por lista de fornecedores	N	Y
Associação não autorizada detectada	Y	Y
Wellenreiter detectado	Y	Y

Observação: adicionar o CleanAir também permitirá a detecção de ataques não relacionados ao 802.11.

Figura 11 - Exibição do perfil do WCS wIPS


Profile Configuration
Configure > wIPS Profiles > wips-elm > Profile Configuration
Back
Next
Save
Cancel
Select Policy
Available only in Monitor Mode
DoS: Block ACK flood
DoS: De-Auth broadcast flood
DoS: De-Auth flood
DoS: Dis-Assoc broadcast flood
DoS: Dis-Assoc flood
DoS: EAPOL-Logoff attack
DoS: FATA-Jack tool
DoS: Premature EAP-Failure
DoS: Premature EAP-Success
wIPS - Security Penetration
ASLEAP tool detected
Airsnarf attack



Na Figura 11, configure o perfil wIPS do WCS, o ícone indica que o ataque será detectado somente quando o AP estiver em MM, enquanto apenas o melhor esforço quando estiver no ELM.

Identificar e Solucionar Problemas do ELM

Verifique estes itens:

- Verifique se o NTP está configurado.
- Verifique se a configuração de hora do MSE está em UTC.
- Se o grupo de dispositivos não estiver funcionando, use a sobreposição de perfil SSID com Qualquer. Reinicialize o AP.
- Certifique-se de que o licenciamento esteja configurado (no momento, os APs ELM estão usando licenças KAM)
- Se os perfis wIPS forem alterados com muita frequência, sincronize o Controlador MSE novamente. Verifique se o perfil está ativo no WLC.
- Certifique-se de que a WLC faça parte do MSE usando CLIs do MSE:

1. SSH ou telnet para o MSE.
2. Execute /opt/mse/wips/bin/wips_cli - Este console pode ser usado para acessar os seguintes comandos para coletar informações sobre o estado do sistema wIPS adaptativo.
3. show wlc all - Problema dentro do console wIPS. Esse comando é usado para verificar os controladores que estão se comunicando ativamente com o serviço wIPS no MSE. Consulte a Figura 12.

   Figura 12 - Verificação da WLC do MSE ativa com os serviços wIPS do MSE

```
<#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
```

- Verifique se os alarmes estão sendo detectados no MSE usando CLIs do MSE.
  - show alarm list - Problema dentro do console do wIPS. Esse comando é usado para listar os alarmes contidos atualmente no banco de dados do serviço wIPS. O campo de chave é a chave de hash exclusiva atribuída ao alarme específico. O campo Tipo é o tipo de alarme. Este gráfico na Figura 13 mostra uma lista de IDs de alarme e descrições:

    Figura 13 - Comando show alarm list do 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
```

Os campos Primeira e Última Hora significam os timestamps quando o alarme foi detectado; eles são armazenados em hora UTC. O campo Ativo será realçado se o alarme for detectado no momento.

- Limpe o banco de dados do MSE.
  - Se você se deparar com uma situação em que o banco de dados do MSE esteja corrompido ou nenhum outro método de solução de problemas funcionará, talvez seja melhor limpar o banco de dados e recomeçar.

    Figura 14 - Comando de serviços do MSE

```
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
```

Informações Relacionadas

- Guia de configuração do Cisco Wireless LAN Controller Release 7.0.116.0
- Guia de configuração do Cisco Wireless Control System, versão 7.0.172.0
- 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.