O wIPS adaptável de Cisco aumentou a configuração e o guia de distribuição do modo local (OLMO)

Índice

Introdução

A solução wireless adaptável do sistema da prevenção de intrusão de Cisco (wIPS) adiciona a característica aumentada do modo local (OLMO), permitindo que os administradores usem seus Access point distribuídos (AP) para fornecer a proteção detalhada sem a necessidade para uma rede de folha de prova separada (figura 1). Antes do OLMO e no desenvolvimento adaptável tradicional do wIPS, o modo de monitor dedicado (MM) AP é exigido para fornecer necessidades ou proteção da conformidade PCI de acesso de segurança, de penetração, e dos ataques desautorizados (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 focaliza somente no OLMO e não altera nenhuns benefícios existentes do desenvolvimento do wIPS com MM AP.

Figura 1 - Desenvolvimento aumentado do modo local AP

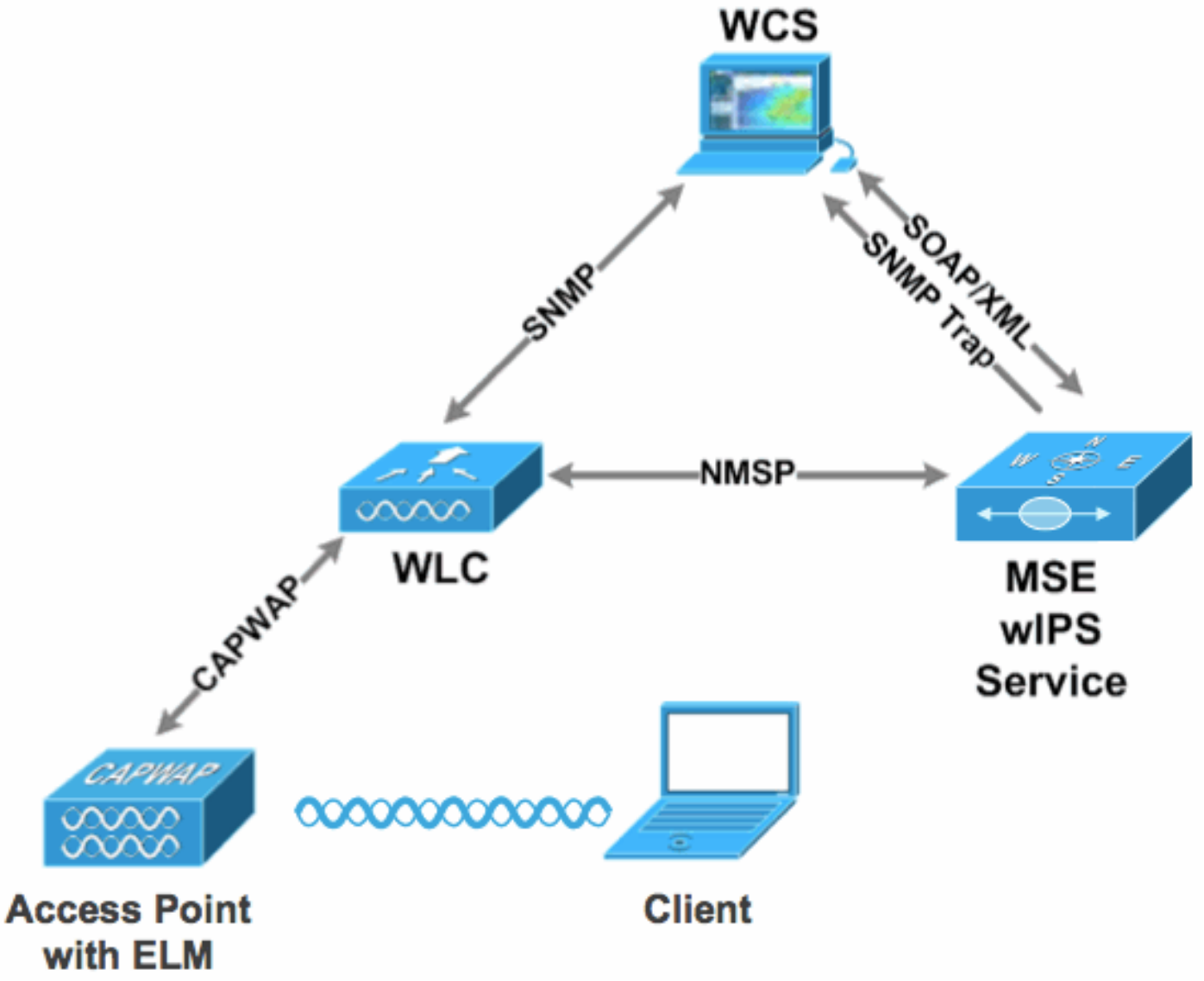
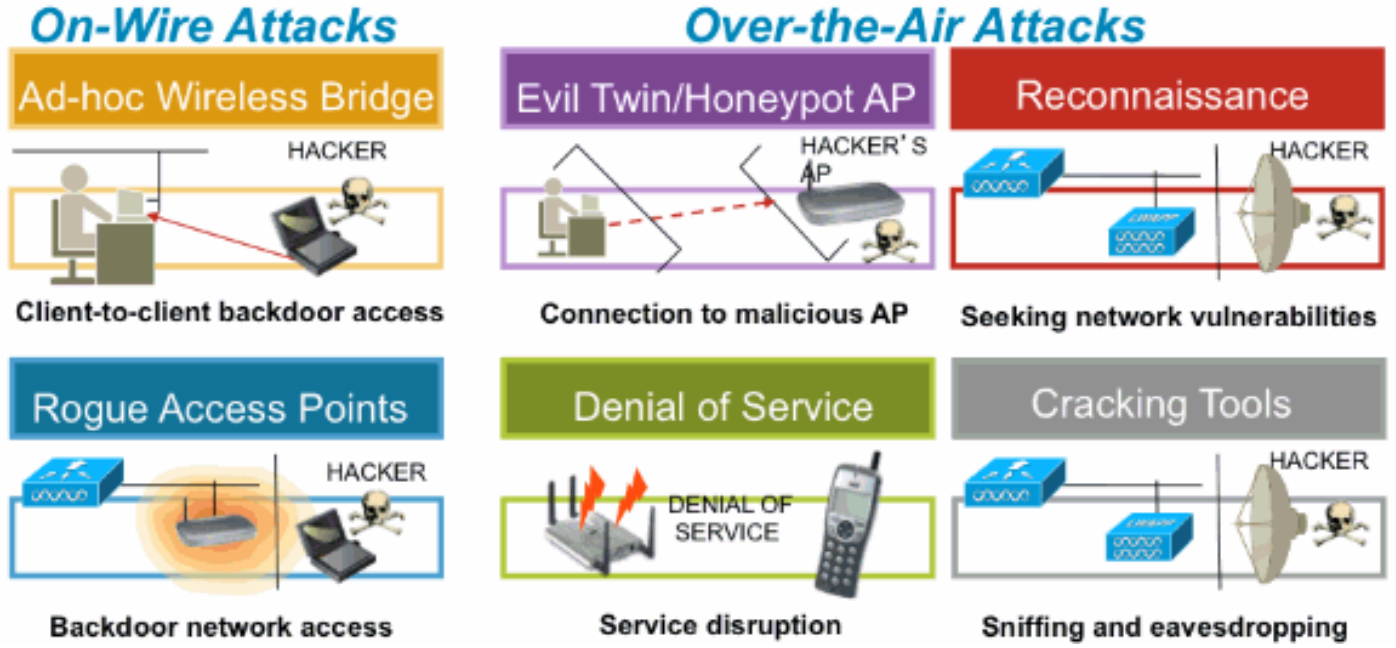


Figura 2 - Ameaças superiores da segurança Wireless



Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Componentes requeridos do OLMO e versões do código mínimo

- Controlador do Wireless LAN (WLC) - Versão 7.0.116.xx ou mais recente
- AP - Versão 7.0.116.xx ou mais recente
- Sistema de controle wireless (WCS) - Versão 7.0.172.xx ou mais recente
- Motor dos Serviços de mobilidade - Versão 7.0.201.xx ou mais recente

Plataformas de apoio WLC

O OLMO é apoiado em Plataformas WLC5508, WLC4400, WLC 2106,WLC2504, WiSM-1, e WiSM-2WLC.

AP de apoio

O OLMO é apoiado em 11n AP que inclui 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.

Convenções

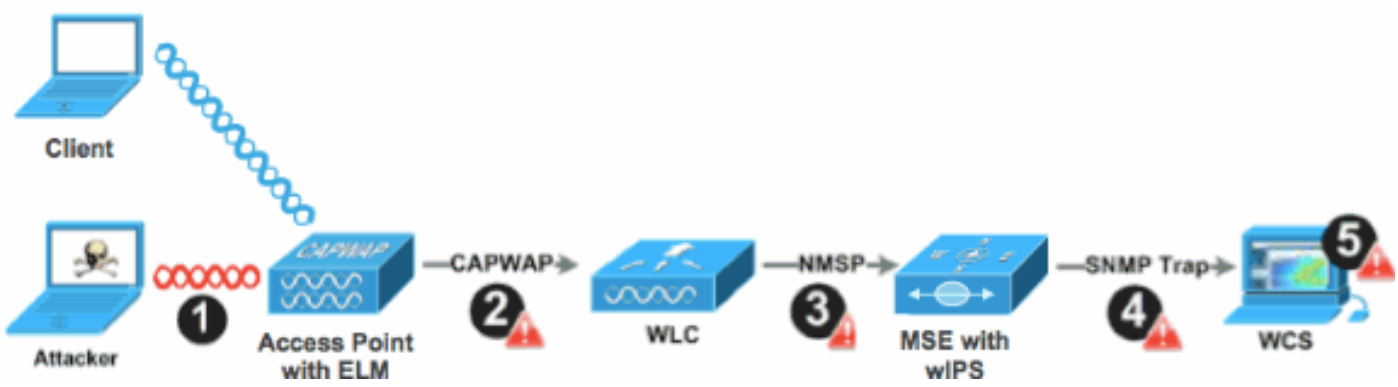
Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Fluxo do alarme do wIPS do OLMO

Os ataques são somente relevantes quando ocorrem na infraestrutura confiada AP. O OLMO AP detectará e comunicar-se-á ao controlador e correlacionar-se-á com o MSE para relatar com Gerenciamento WCS. Figura 3 fornece o fluxo do alarme do ponto de vista de um administrador:

1. Ataque lançado contra um dispositivo de infraestrutura (AP “confiado”)
2. Detectado no OLMO AP comunicado com CAPWAP ao WLC
3. Passado transparentemente a MSE através de NMSP
4. Registrado no base de dados do wIPS em MSE enviado ao WCS através da armadilha de SNMP
5. Indicado no WCS

Figura 3 - Detecção da ameaça e fluxo do alarme



Considerações de desenvolvimento para o OLMO

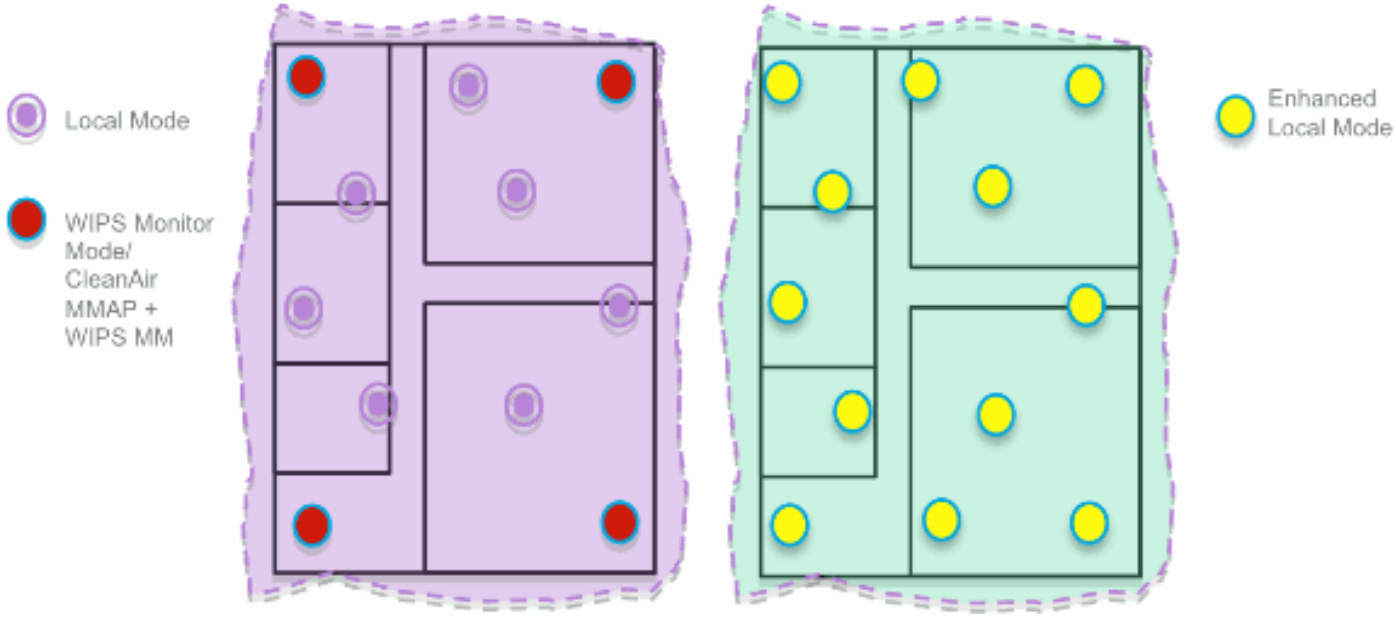
Cisco recomenda que permitindo o OLMO em cada AP na reunião da rede a maioria de Segurança do cliente precisa quando uma folha de prova e/ou os custos da rede são parte de consideração. A característica preliminar do OLMO opera-se eficazmente para ataques do em-canal, sem nenhum acordo ao desempenho em dados, clientes da Voz e do vídeo, e serviços.

OLMO contra MM dedicado

Figura 4 fornece um contraste geral entre as disposições padrão do wIPS MM AP e o OLMO. Na revisão, a escala de cobertura típica para ambos os modos sugere:

- O wIPS dedicado MM AP cobre tipicamente 15,000-35,000 pés quadrados
- o Cliente-serviço AP cobrirá tipicamente de 3,000-5,000 pés quadrados

Figura 4 - Folha de prova do MM contra todo o OLMO AP



No desenvolvimento adaptável tradicional do wIPS, Cisco recomenda uma relação de 1 MM AP a cada 5 modo local AP, que pode igualmente variar baseado no projeto de rede e na orientação do perito para a melhor cobertura. Considerando o OLMO, o administrador permite simplesmente os recursos de software do OLMO para todos os AP existentes, adicionando eficazmente operações do wIPS MM ao modo local AP do DATA-serviço ao manter o desempenho.

Em-canal e desempenho do Fora-canal

UM MM AP utiliza 100% do momento do rádio para fazer a varredura de todos os canais, porque não serve nenhuns clientes de WLAN. A característica preliminar para o OLMO opera-se eficazmente para ataques do em-canal, sem nenhum acordo ao desempenho em dados, Voz e clientes e serviços do vídeo. A diferença principal está na exploração de variação do fora-canal do modo local; segundo a atividade, a exploração do fora-canal fornece o tempo de interrupção mínimo recolher bastante informações disponíveis para classificar e determinar o ataque. Um exemplo pode ser com clientes da Voz que são associados e onde a exploração RRM do AP é adiada até que o cliente da Voz esteja dis-associado se certificar serviço não é afetada. Para esta consideração, a detecção do OLMO durante o fora-canal é considerada o melhor esforço. OLMO vizinho AP que opera-se em tudo, país ou de canais DCA eficácia dos aumentos, daqui a recomendação para permitir o OLMO em cada modo local AP para a cobertura da proteção máxima. Se a exigência é para exploração dedicada em todos os canais a tempo inteiro, a recomendação será distribuir MM AP.

Estes pontos reveem diferenças do modo local e do MM AP:

- Modo local AP - Os clientes de WLAN dos saques com exploração do fora-canal do corte de tempo, escutam 50ms em cada canal, e na exploração configurável das características para os canais tudo/country/DCA.
- Modo de monitor AP - Não serve os clientes de WLAN, dedicados à varredura somente, escuta 1.2s em cada canal, e faz a varredura de todos os canais.

OLMO através dos links MACILENTOS

Cisco fez grandes esforços a fim aperfeiçoar características em encenações desafiantes, tais como o OLMO de distribuição AP através dos links de WAN da largura de banda baixa. A característica do OLMO envolve PRE-processar em determinar assinaturas do ataque no AP e é aperfeiçoada para trabalhar sobre enlaces lentos. Como melhores prática, recomenda-se testar e medir a linha de base para validar o desempenho com o OLMO sobre WAN.

Integração de CleanAir

A característica do OLMO felicita altamente operações de CleanAir com o desempenho similar e benefícios ao desenvolvimento de MM AP com estes benefícios espectro-cientes existentes de CleanAir:

- Inteligência dedicada do silicone-nível RF
- Espectro-ciente, auto-cura, e auto-aperfeiçoando
- Ameaça do canal e detecção e mitigação não padronizadas de interferência
- Não detecção do Wi-fi tal como Bluetooth, a micro-ondas, os telefones sem fio, etc.
- Detecte e encontre ataques DOS da camada RF tais como jammer RF

Recursos e benefício do OLMO

- Exploração adaptável do wIPS nos dados que servem o local e o H-REAP AP
- Proteção sem exigir uma rede de folha de prova separada
- Disponível como uma transferência livre SW para clientes existentes do wIPS
- Conformidade dos apoios PCI para o Sem fio LAN

- 802.11 e detecção de ataque non-802.11 completos
- Adiciona capacidades do forense e do relatório
- Integra com Gerenciamento existente CUWM e WLAN
- Flexibilidade ajustar MM integrado ou dedicado AP
- PRE-processar em AP minimiza o regresso dos dados (isto é, trabalha sobre muito enlaces de largura de banda baixa)
- Baixo impacto nos dados do serviço

Licenciar do OLMO

O wIPS do OLMO adiciona uma licença nova a pedir:

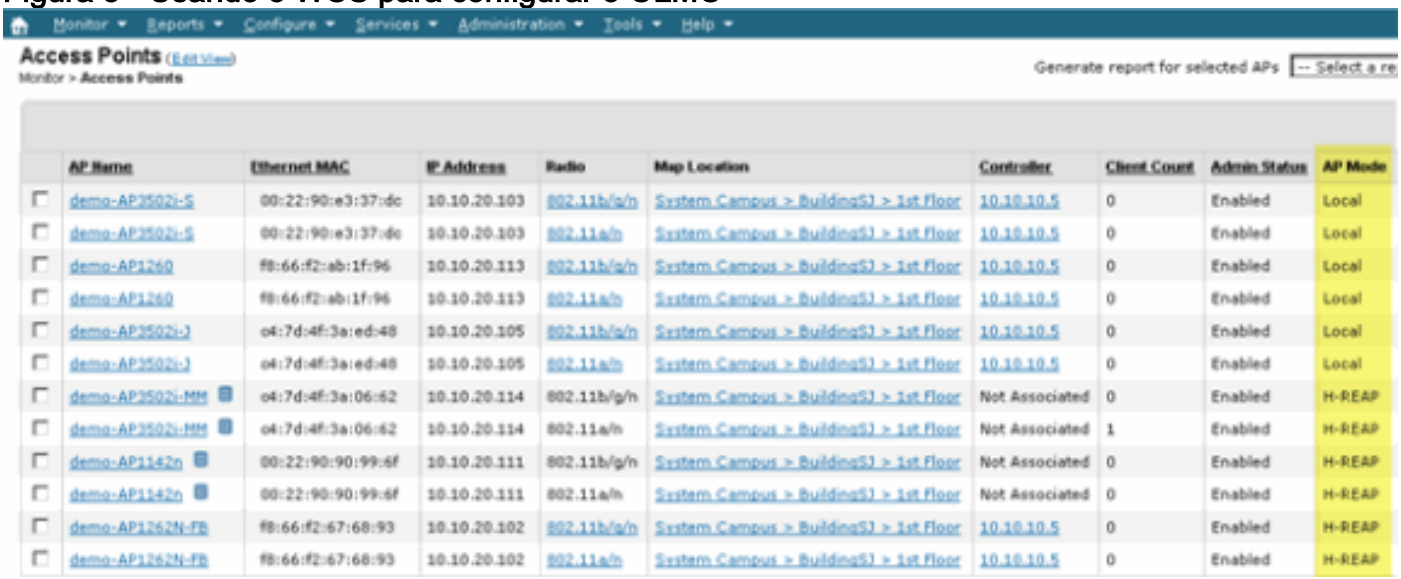
- Ar-LM-WIPS-Xx - Licença do wIPS do OLMO de Cisco
- Ar-WIPS-AP-xx - Licença do wIPS do Cisco Wireless

Notas adicionais licenciar do OLMO:

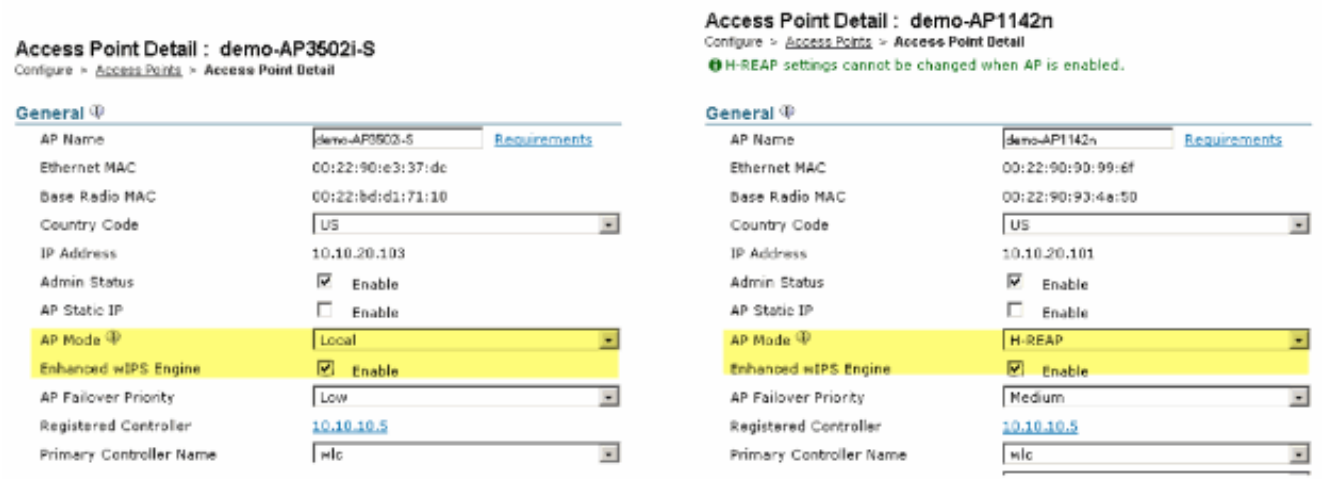
- Se a licença SKU do wIPS MM AP é instalada já, aquelas licenças podem igualmente ser usadas para o OLMO AP.
- as licenças do wIPS e as licenças do OLMO contam junto para os limites da licença da plataforma para o motor do wIPS; 2000 AP em 3310, e 3000 AP em 335x, respectivamente.
- A licença de avaliação incluirá 10 AP para o wIPS e 10 para o OLMO por um período de até 60 dias. Antes do OLMO, a licença de avaliação permitiu a até 20 o wIPS MM AP. O requisito mínimo das versões de software que apoiam o OLMO deve ser cumprido.

Configurar o OLMO com WCS

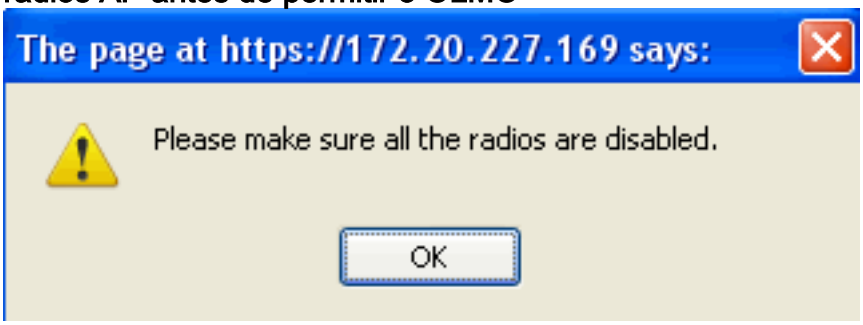
Figura 5 - Usando o WCS para configurar o OLMO



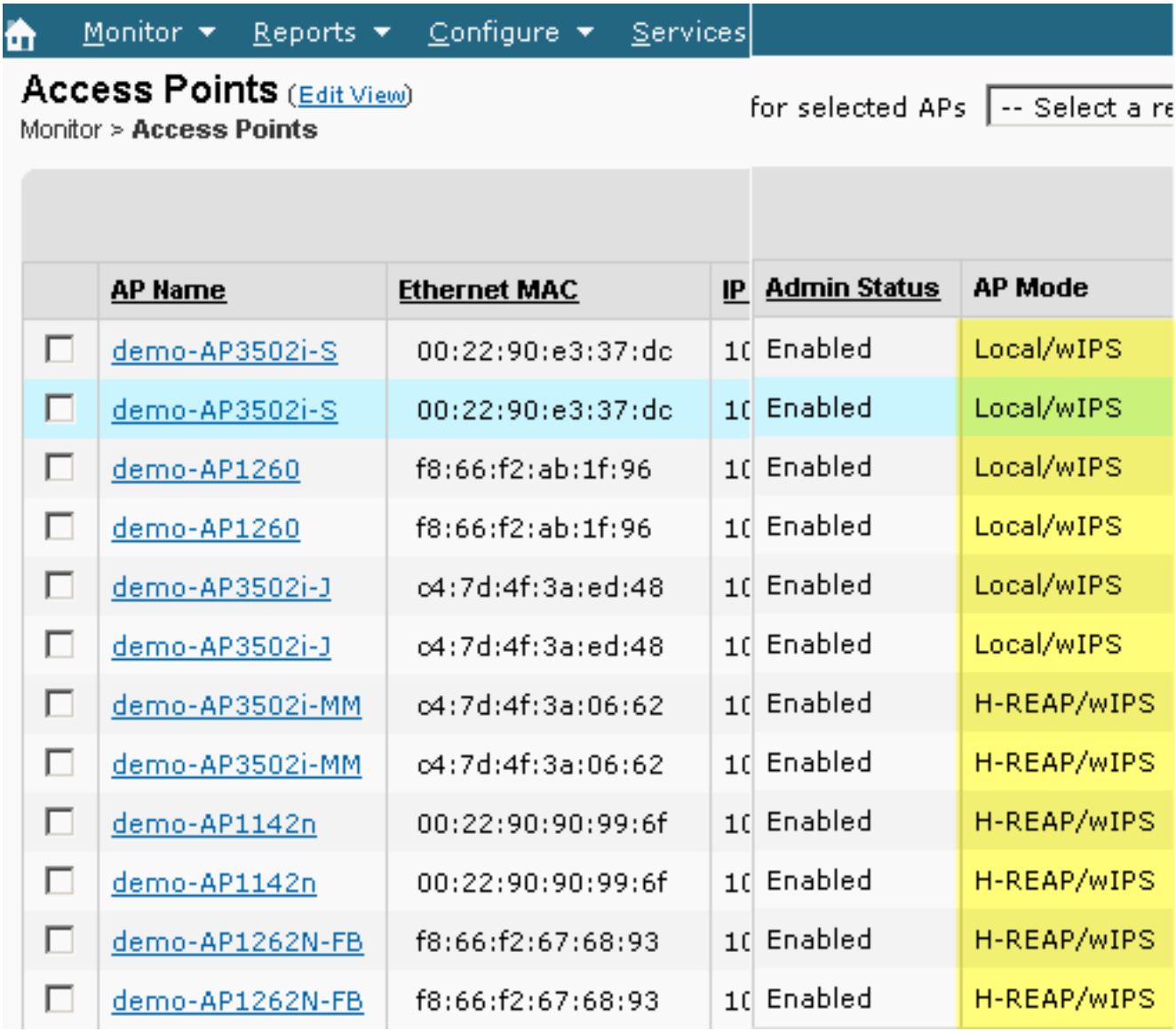
1. Do WCS, desabilite os rádios 802.11b/g e 802.11a do AP antes de permitir “o motor aumentado do wIPS.”**Nota:** Todos os clientes associados estarão desligados, e não se juntarão até que os rádios estejam permitidos.
2. Configurar um AP, ou use um gabarito de configuração WCS para o peso leve múltiplo AP. Veja a figura 6.**Figura 6 - Permita o modo aumentado do sub do motor do wIPS (OLMO)**



3. Escolha o **motor aumentado do wIPS**, e clique a **salvaguarda**.Permitir o motor aumentado do wIPS não fará com que o AP recarregue.H-REAP é apoiado; permita a mesma maneira que para o modo local AP.**Nota:** Se qualquer um dos rádios deste AP é permitido, o WCS ignorará a configuração e jogará o erro na figura 7.**Figura 7 - Lembrete WCS para desabilitar rádios AP antes de permitir o OLMO**



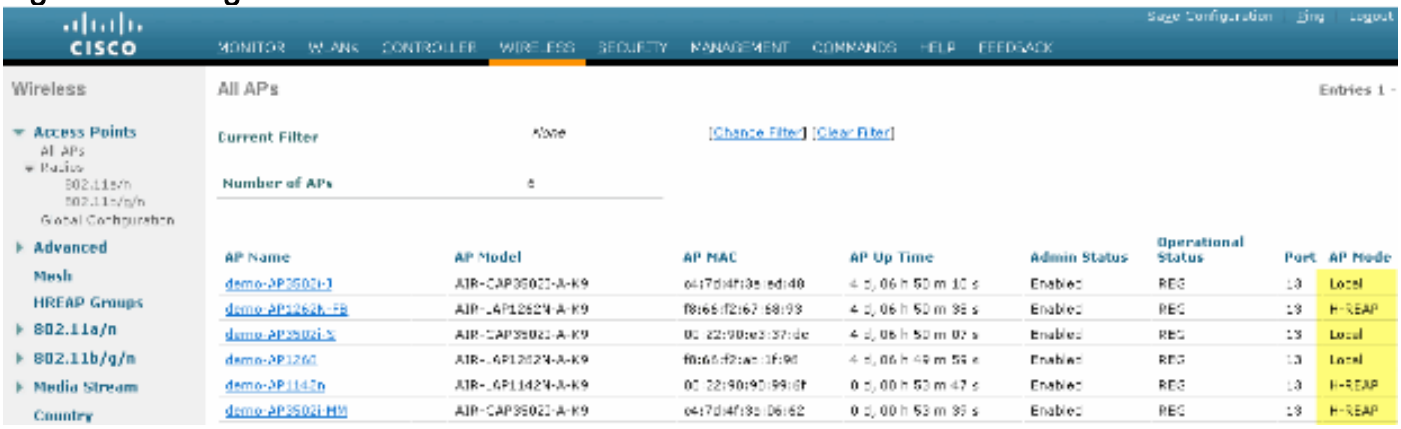
4. O sucesso da configuração pode ser verificado observando a mudança no modo AP do “Local ou do H-REAP” ao **Local/wIPS** ou ao **H-REAP/wIPS**. Veja figura 8.**Figura 8 - WCS que indica o modo AP para incluir o wIPS com Local e/ou H-REAP**



5. Permita os rádios que onde desabilitado em etapa 1.
6. Crie o perfil do wIPS e empurre-o para o controlador para que a configuração termine.**Nota:** Para a informação de configuração completa no wIPS, refira o guia de distribuição adaptável do wIPS de Cisco.

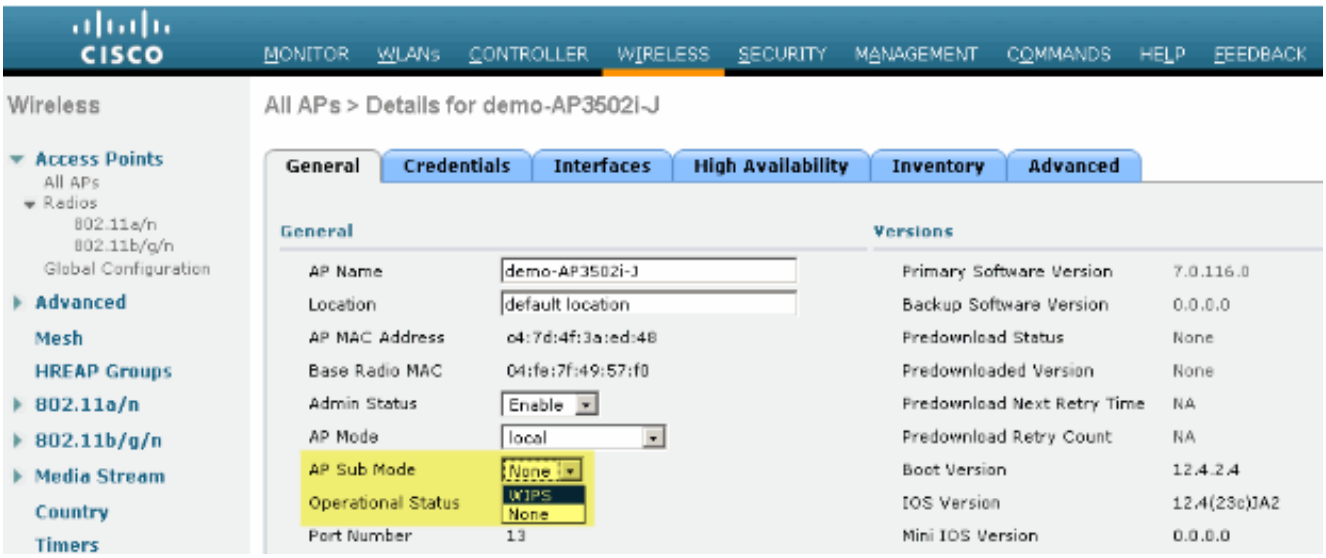
Configuração do WLC

Figura 9 - Configurar o OLMO com WLC



1. Escolha um AP da aba **wireless**.**Figura 10 - WLC que muda o modo do sub AP para incluir o**

OLMO do wIPS



2. Do menu suspenso do modo do sub AP, escolha o **wIPS** (figura 10).
3. Aplique, e salvar então a configuração.

Nota: Para que a funcionalidade do OLMO trabalhe, MSE e o WCS são exigidos com licenciar do wIPS. Mudar o modo do sub AP do WLC apenas não permitirá o OLMO.

Ataques detectados no OLMO

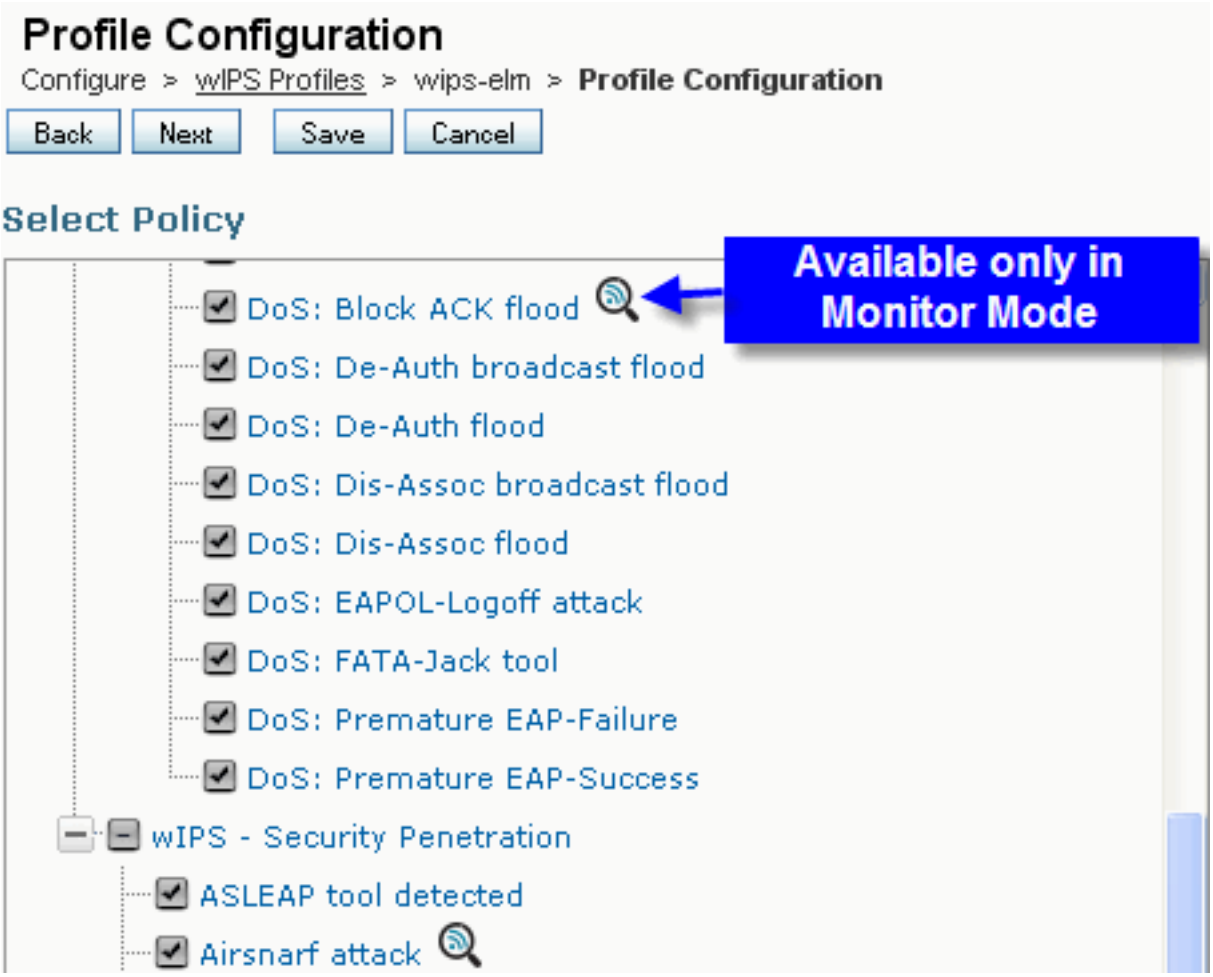
Tabela 1 - matriz de suporte das assinaturas do wIPS

Ataques detectados	OLMO	MM
Ataque DoS contra o AP		
Inundação da associação	Y	Y
Excesso da tabela de associação	Y	Y
Inundação da autenticação	Y	Y
Ataque do EAPOL-início	Y	Y
Inundação da PS-votação	Y	Y
Inundação do pedido da ponta de prova	N	Y
Associação não-autenticado	Y	Y
Ataque DoS contra a infraestrutura		
Inundação CTS	N	Y
Façanha da Universidade Tecnológica de Queensland	N	Y
Bloqueio RF	Y	Y
Inundação RTS	N	Y
Ataque virtual do portador	N	Y
Ataque DoS contra a estação		
Ataque da falha de autenticação	Y	Y
Inundação do bloco ACK	N	Y
Inundação da transmissão do De-AUTH	Y	Y
Inundação do De-AUTH	Y	Y
Inundação da transmissão Dis-Assoc	Y	Y

Inundação Dis-Assoc	Y	Y
Ataque do EAPOL-fazer logoff	Y	Y
Ferramenta de FATA-Jack	Y	Y
EAP-falha prematura	Y	Y
EAP-sucesso prematuro	Y	Y
Ataques da penetração da Segurança		
Ferramenta ASLEAP detectada	Y	Y
Ataque de Airsnarf	N	Y
Ataque de ChopChop	Y	Y
Ataque de dia-Zero pela anomalia da Segurança de WLAN	N	Y
Ataque de dia-Zero pela anomalia da segurança do dispositivo	N	Y
Dispositivo que sonda para AP	Y	Y
Ataque do dicionário em métodos de EAP	Y	Y
Ataque EAP contra a autenticação do 802.1x	Y	Y
Falsificação AP detectada	Y	Y
Servidor DHCP falsificado detectado	N	Y
Ferramenta RÁPIDA da quebra WEP detectada	Y	Y
Ataque de fragmentação	Y	Y
Honeypot AP detectado	Y	Y
Ferramenta de Hotspotter detectada	N	Y
Frames de transmissão impróprios	N	Y
Pacotes deformados do 802.11 detectados	Y	Y
Homem no ataque médio	Y	Y
Netstumbler detectou	Y	Y
Vítima de Netstumbler detectada	Y	Y
Violação PSPF detectada	Y	Y
AP macio ou host AP detectado	Y	Y
MAC address falsificado detectado	Y	Y
Suspeito após o tráfego das horas detectado	Y	Y
Associação desautorizada pela lista do vendedor	N	Y
Associação desautorizada detectada	Y	Y
Wellenreiter detectou	Y	Y

Nota: Adicionar CleanAir igualmente permitirá a detecção dos ataques non-802.11.

Figura 11 - Opinião do perfil do wIPS WCS



Em figura 11, configurar o perfil do wIPS do WCS, o ícone indica que o ataque estará detectado somente quando o AP está no MM, quando somente o melhor esforço quando no OLMO.

Pesquise defeitos o OLMO

Verifique estes artigos:

- Certifique-se que o NTP está configurado.
- Certifique-se que configuração de tempo MSE está no UTC.
- Se o grupo do dispositivo não está trabalhando, use o perfil SSID da folha de prova com alguns. Recarregue o AP.
- Licenciar Make sure é configurado (atualmente o OLMO AP está usando licenças KAM)
- Se os perfis do wIPS são mudados demasiado frequentemente, sincronize o MSE-controlador outra vez. Certifique-se que o perfil é ativo no WLC.
- Certifique-se que o WLC é parte de MSE usando MSE CLI:SSH ou telnet a seu MSE.Execute **/opt/mse/wips/bin/wips_cli** - Este console pode ser usado para alcançar aos comandos seguintes recolher a informação em relação ao estado do sistema adaptável do wIPS.**mostre o wlc todo** – Emita dentro do console do wIPS. Este comando é usado verificar os controladores que se estão comunicando ativamente com o serviço do wIPS no MSE. Veja figura 12.**Figura 12 - MSE CLI que verifica o Active WLC com serviços do wIPS MSE**`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`

- Certifique-se que os alarmes estão obtendo detectaram em MSE usando MSE CLI.**mostre a lista do alarme** - Emita dentro do console do wIPS. Este comando é usado alistar os alarmes contidos atualmente dentro do base de dados do serviço do wIPS. O campo chave é a chave original da mistura atribuída ao alarme específico. O tipo campo é o tipo de alarme. Esta carta em figura 13 mostra uma lista do alarme ID e das descrições:**Figura 13 - Comando list do alarme da mostra MSE CLI**`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` A primeira vez que e os campos da última vez significam os timestamps em que o alarme esteve detectado; estes são armazenados no tempo UTC. O campo ativo destaca se o alarme é detectado atualmente.
- Cancele o base de dados MSE.Se você é executado em uma situação onde o base de dados MSE seja corrompido, ou nenhum outros métodos de Troubleshooting trabalhará, pode ser o melhor cancelar o base de dados e começá-lo sobre.**Figura 14 - MSE presta serviços de manutenção ao comando**`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

- Manual de configuração do controlador de LAN do Cisco Wireless, liberação 7.0.116.0
- Manual de configuração do Sistema de controle sem fio da Cisco, liberação 7.0.172.0
- Suporte Técnico e Documentação - Cisco Systems