Resolver detecção e mitigação de invasores em uma rede sem fio unificada

Contents

Introduction

Este documento descreve a detecção e a mitigação de invasores em redes sem fio da Cisco.

As redes wireless estendem redes com fio e aumentam a produtividade dos trabalhadores e acessam às informações. Contudo, uma rede wireless não autorizada apresenta uma camada adicional de preocupação de segurança. Além disso, ela é colocada na segurança das portas em redes com fio, tendo as redes wireless como uma extensão simples de redes com fio. Portanto, um funcionário que traz seu próprio ponto de acesso (Cisco ou não Cisco) para uma infraestrutura com ou sem fio bem protegida e permite que usuários não autorizados acessem essa rede protegida de outra forma, pode facilmente comprometer uma rede segura.

A detecção de invasores permite que o administrador de rede monitore e elimine essa preocupação de segurança. A Cisco Unified Network Architecture fornece métodos para detecção de invasores que permitem uma solução completa de identificação e contenção de invasores sem a necessidade de redes e ferramentas de sobreposição caras e difíceis de justificar.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Controladores De Lan Sem Fio Da Cisco.
- Infraestrutura Cisco Prime.

Componentes Utilizados

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

- Cisco Unified Wireless Lan Controllers (5520, 8540 e 3504 Series) que executa a versão 8.8.120.0.
- APs Wave 2 séries 1832, 1852, 2802 e 3802.
- APs Wave 1 séries 3700, 2700 e 1700.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Visão geral do invasor

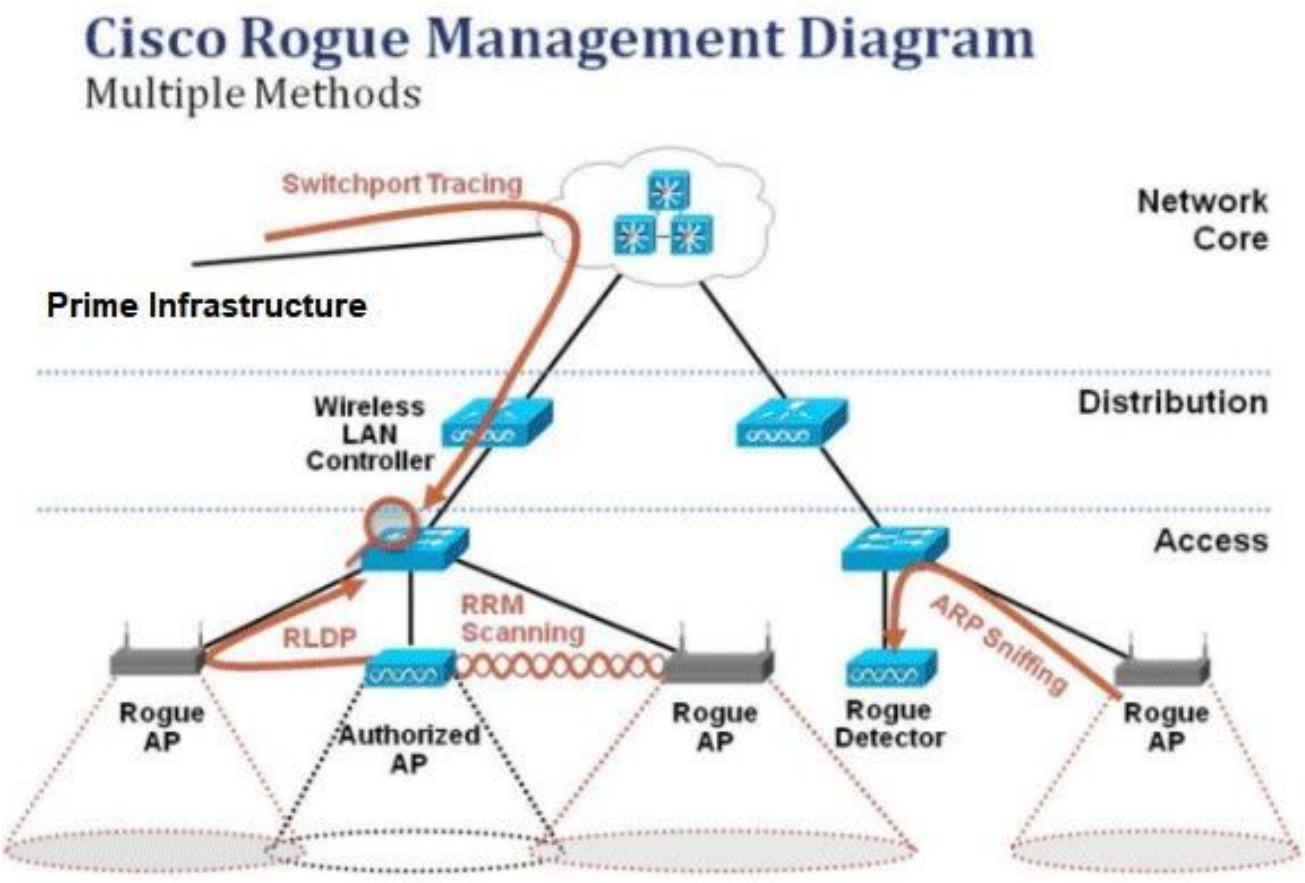
Qualquer dispositivo que compartilhe seu espectro e não seja gerenciado por você pode ser considerado invasor. Um invasor se torna perigoso nestes cenários:

- Quando configurado para usar o mesmo Service Set Identifier (SSID) da sua rede (honeypot).
- Quando detectado na rede com fio.
- Invasores ad-hoc.
- Configuração feita por um estranho, na maioria das vezes, com intenção mal-intencionada.

A prática recomendada é usar a detecção de invasores para minimizar os riscos de segurança, por exemplo, em um ambiente corporativo. No entanto, há determinados cenários em que a detecção de invasores não é necessária, por exemplo, na implantação do Office Extend Access Point (OEAP), em toda a cidade e em ambientes externos. Com o uso de APs de malha externos para detectar invasores, você obteria pouco valor e usaria recursos para analisar. Por fim, é essencial avaliar (ou evitar completamente) a contenção automática desonesta, pois há possíveis problemas legais e responsabilidades se você deixar a operação automaticamente.

Há três fases principais de gerenciamento de dispositivos invasores na solução Cisco Unified Wireless Network (UWN):

- Detecção - Uma varredura de RRM (Radio Resource Management, gerenciamento de recursos de rádio) é usada para detectar a presença de dispositivos invasores.
- Classificação - RLDP (Rogue Location Discovery Protocol), detectores de invasores (somente APs Wave 1) e rastreamentos de porta de switch são usados para identificar se o dispositivo invasor está conectado à rede com fio. As regras de classificação de invasores também ajudam na filtragem de invasores em categorias específicas com base em suas características.
- Mitigação - O desligamento da porta do switch, a localização do invasor e a contenção do invasor são usados para rastrear sua localização física e anular a ameaça do dispositivo invasor.

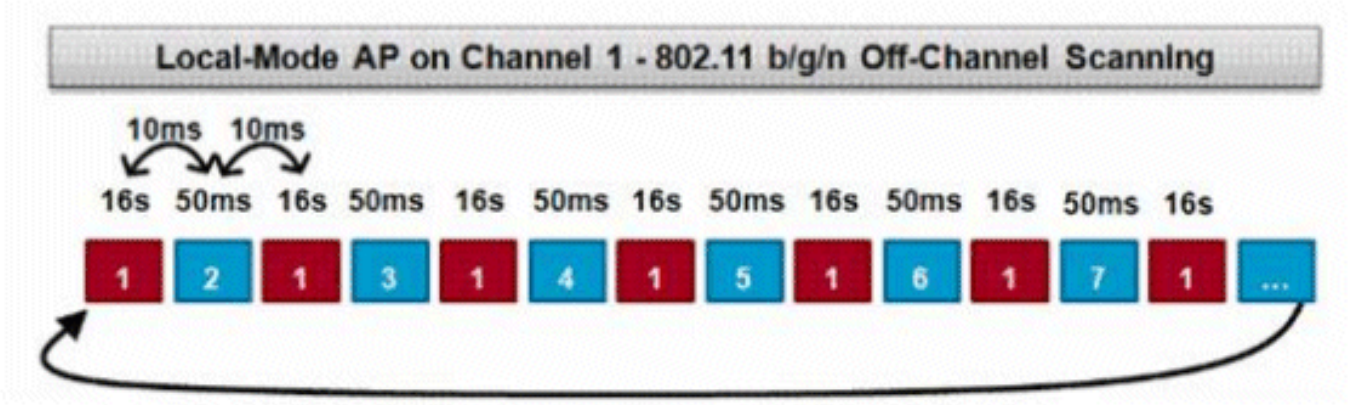


Detecção de invasor

Um invasor é essencialmente qualquer dispositivo que compartilha seu espectro, mas não está no seu controle. Isso inclui pontos de acesso não autorizados, roteador sem fio, clientes não autorizados e redes ad-hoc não autorizadas. O Cisco UWN usa vários métodos para detectar dispositivos invasores baseados em Wi-Fi, como verificação fora do canal e recursos de modo de monitor dedicado. O Cisco Spectrum Expert também pode ser usado para identificar dispositivos invasores não baseados no protocolo 802.11, como bridges Bluetooth.

Verificação fora do canal

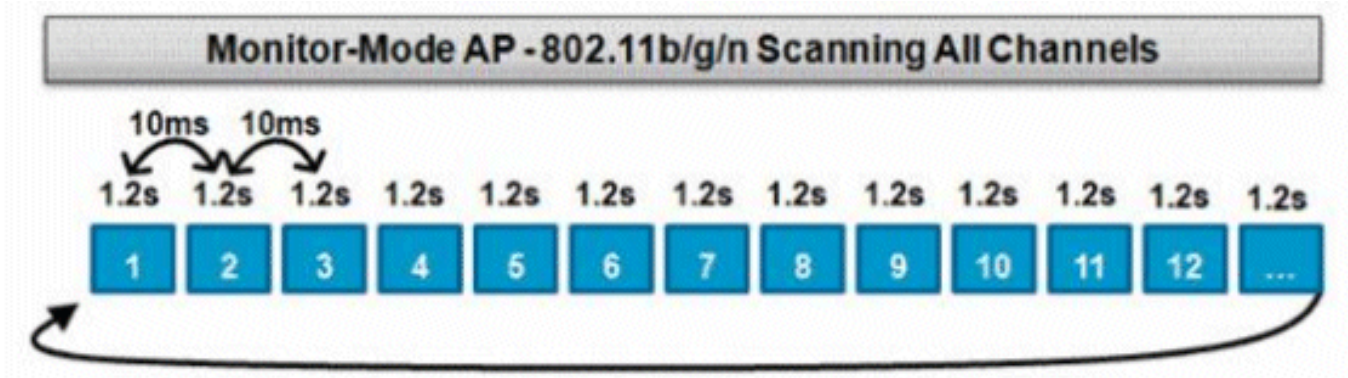
Essa operação é realizada por APs nos modos Local e Flex-Connect (no modo conectado) e utiliza uma técnica de divisão de tempo que permite o atendimento ao cliente e a verificação de canal com o uso do mesmo rádio. Com a mudança para fora do canal por um período de 50 ms a cada 16 segundos, o AP, por padrão, gasta apenas uma pequena porcentagem de seu tempo para não atender aos clientes. Além disso, observe que ocorre um intervalo de alteração de canal de 10 ms. No intervalo de verificação padrão de 180 segundos, cada canal FCC de 2,4 Ghz (1−11) é verificado pelo menos uma vez. Para outros domínios regulatórios, como ETSI, o AP fica fora do canal por uma porcentagem de tempo ligeiramente maior. A lista de canais e o intervalo de verificação podem ser ajustados na configuração do RRM. Isso limita o impacto no desempenho a um máximo de 1,5% e a inteligência é integrada no algoritmo para suspender a verificação quando quadros de QoS de alta prioridade, como voz, precisam ser entregues.



Esta figura é uma representação do algoritmo de varredura off-channel para um AP de modo local na faixa de frequência de 2,4 GHz. Uma operação semelhante é feita em paralelo no rádio de 5 GHz se o AP tiver um presente. Cada quadrado vermelho representa o tempo gasto no canal inicial dos APs, enquanto cada quadrado azul representa o tempo gasto nos canais adjacentes para fins de verificação.

Verificação do modo de monitor

Essa operação é realizada pelos APs do modo de monitor do Modo de Monitor e Adaptive wIPS, que utilizam 100% do tempo de rádio para examinar todos os canais em cada banda de frequência respectiva. Isso permite maior velocidade de detecção e permite que mais tempo seja gasto em cada canal individual. Os APs do modo de monitoramento também são muito superiores na detecção de clientes invasores, pois têm uma visão mais abrangente da atividade que ocorre em cada canal.



Esta figura é uma representação do algoritmo de varredura off-channel para um AP no modo de monitor na faixa de frequência de 2,4 GHz. Uma operação semelhante é feita em paralelo no rádio de 5 GHz se o AP tiver um presente.

Comparação dos modos local e monitor

Um AP do modo local divide seus ciclos entre o serviço de clientes WLAN e a verificação de canais para ameaças. Como resultado, um AP de modo local leva mais tempo para percorrer todos os canais e gasta menos tempo na coleta de dados em qualquer canal específico para que as operações do cliente não sejam interrompidas. Consequentemente, os tempos de detecção de invasores e ataques são maiores (3 a 60 minutos) e uma faixa menor de ataques pelo ar pode ser detectada do que com um AP de modo de monitor.

Além disso, a detecção de tráfego em surtos, como clientes invasores, é muito menos

determinística porque o AP precisa estar no canal do tráfego ao mesmo tempo em que o tráfego é transmitido ou recebido. Isso se torna um exercício de probabilidades. Um AP no modo de monitor gasta todos os seus ciclos na verificação de canais para procurar invasores e ataques pelo ar. Um AP do modo de monitor pode ser usado simultaneamente para wIPS adaptativo, serviços de localização (contextuais) e outros serviços do modo de monitor.

Quando os APs do modo de monitoramento são implantados, os benefícios são menor tempo de detecção. Quando os APs do modo de monitor são configurados adicionalmente com o Adaptive wIPS, uma gama mais ampla de ameaças e ataques pelo ar pode ser detectada.

APs do modo local	APs do modo de monitor
Atende clientes com verificação de divisão de tempo fora do canal	Varredura dedicada
Escuta 50 ms em cada canal	Escuta 1.2s em cada canal
Configurável para varredura: • Todos os canais • Canais do país (padrão) • Canais DCA	Verifica todos os canais

Identificação de invasor

Se a resposta da sonda ou os beacons de um dispositivo invasor forem ouvidos por APs locais, de conexão flexível ou do modo de monitor, essas informações serão comunicadas via CAPWAP à controladora Wireless LAN (WLC) do processo. Para evitar falsos positivos, vários métodos são usados para garantir que outros APs baseados na Cisco não sejam identificados como um dispositivo invasor. Esses métodos incluem atualizações de grupos de mobilidade, pacotes de vizinhos de RF e APs amigáveis de lista permitida via Prime Infrastructure (PI).

Registros invasores

Enquanto o banco de dados do controlador de dispositivos invasores contém apenas o conjunto atual de invasores detectados, o PI também inclui um histórico de eventos e registra invasores que não são mais vistos.

Detalhes do invasor

Um AP CAPWAP fica fora do canal por 50 ms para ouvir clientes não autorizados, monitorar quanto a ruído e interferência de canal. Todos os APs ou clientes invasores detectados são enviados para a controladora, que reúne estas informações:

- O endereço MAC do AP invasor
- Nome do AP detectado como invasor
- O endereço MAC do(s) cliente(s) conectado(s) invasor(es)
- Política de segurança
- O preâmbulo
- A razão sinal/ruído (SNR)
- O indicador de intensidade do sinal receptor (RSSI)
- Canal de detecção de invasor
- Rádio no qual o invasor é detectado
- SSID invasor (se o SSID invasor for transmitido)

- Endereço IP invasor
- Primeira e última vez que o invasor é relatado
- Largura de canal

Para exportar eventos não autorizados

Para exportar eventos não autorizados para um Network Management System (NMS) de terceiros para arquivamento, a WLC permite que receptores de interceptação SNMP adicionais sejam adicionados. Quando um invasor é detectado ou removido pelo controlador, uma interceptação (trapping) que contém essas informações é comunicada a todos os receptores de interceptação (trap) SNMP. Uma advertência com a exportação de eventos via SNMP é que se vários controladores detectarem o mesmo invasor, eventos duplicados serão vistos pelo NMS como correlação somente é feita no PI.

Tempo Limite de Registro Invasor

Depois que um AP invasor tiver sido adicionado aos registros da WLC, ele permanecerá lá até que não seja mais visto. Após um tempo limite configurável pelo usuário (padrão de 1200 segundos), um invasor na_unclassification_category é desativado.

Os invasores em outros estados, como_Contained_e_Friendly_, persistem para que a classificação apropriada seja aplicada a eles se eles reaparecerem.

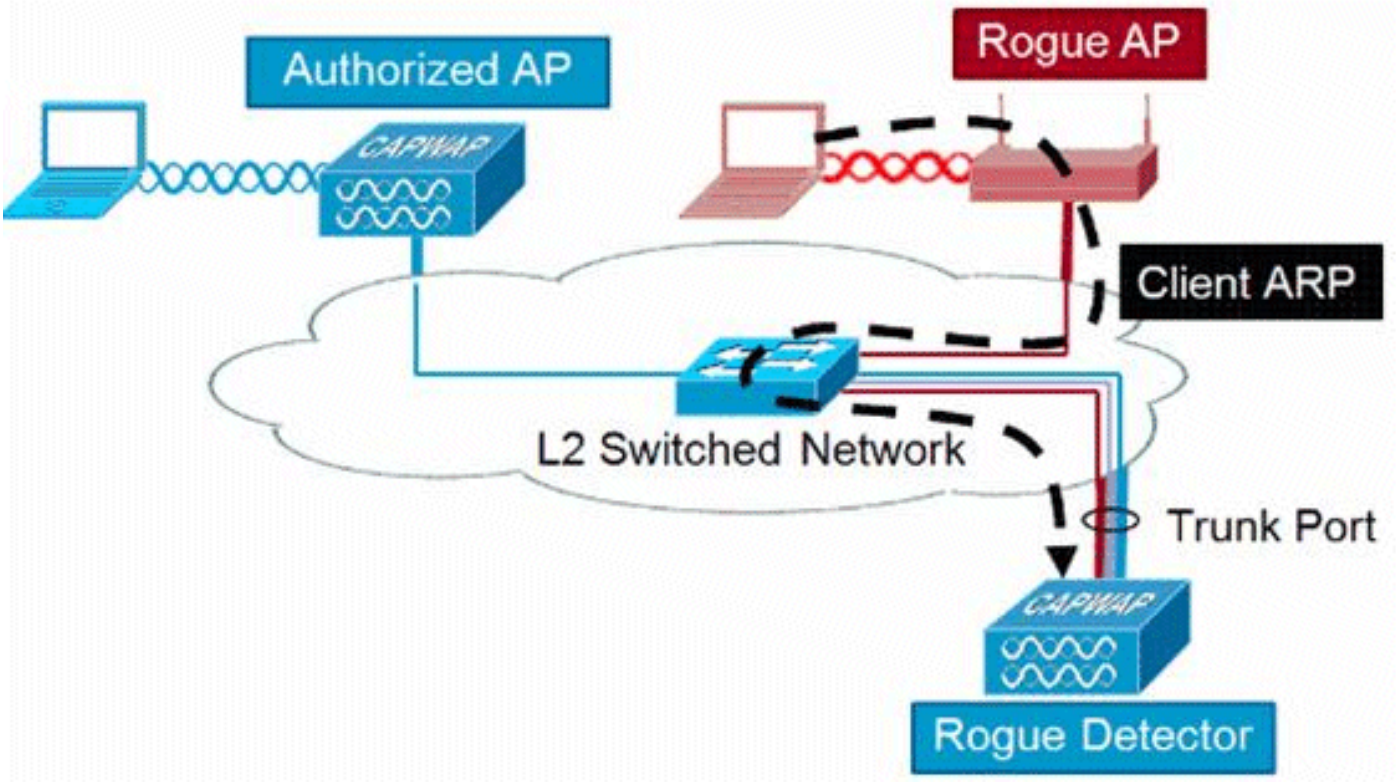
Há um tamanho máximo de banco de dados para registros invasores que é variável nas plataformas do controlador:

- 3504 - Detecção e contenção de até 600 APs invasores e 1500 clientes invasores
- 5520 - Detecção e contenção de até 24000 APs invasores e 32000 clientes invasores
- 8540 - Detecção e contenção de até 24000 APs invasores e 32000 clientes invasores

Rogue Detector AP

Um AP detector de invasor tem como objetivo correlacionar informações invasoras ouvidas pelo ar com informações ARP obtidas da rede com fio. Se um endereço MAC for ouvido no ar como um AP invasor ou cliente e também for ouvido na rede com fio, o invasor será determinado como estando na rede com fio. Se for detectado que o invasor está na rede com fio, a gravidade do alarme para esse AP invasor será elevada para_critical_. Um AP detector invasor não é bem-sucedido na identificação de clientes invasores atrás de um dispositivo que usa NAT.

Essa abordagem é usada quando o AP invasor tem alguma forma de autenticação, seja WEP ou WPA. Quando uma forma de autenticação é configurada no AP invasor, o AP leve não pode se associar porque não conhece o método de autenticação e as credenciais configuradas no AP invasor.



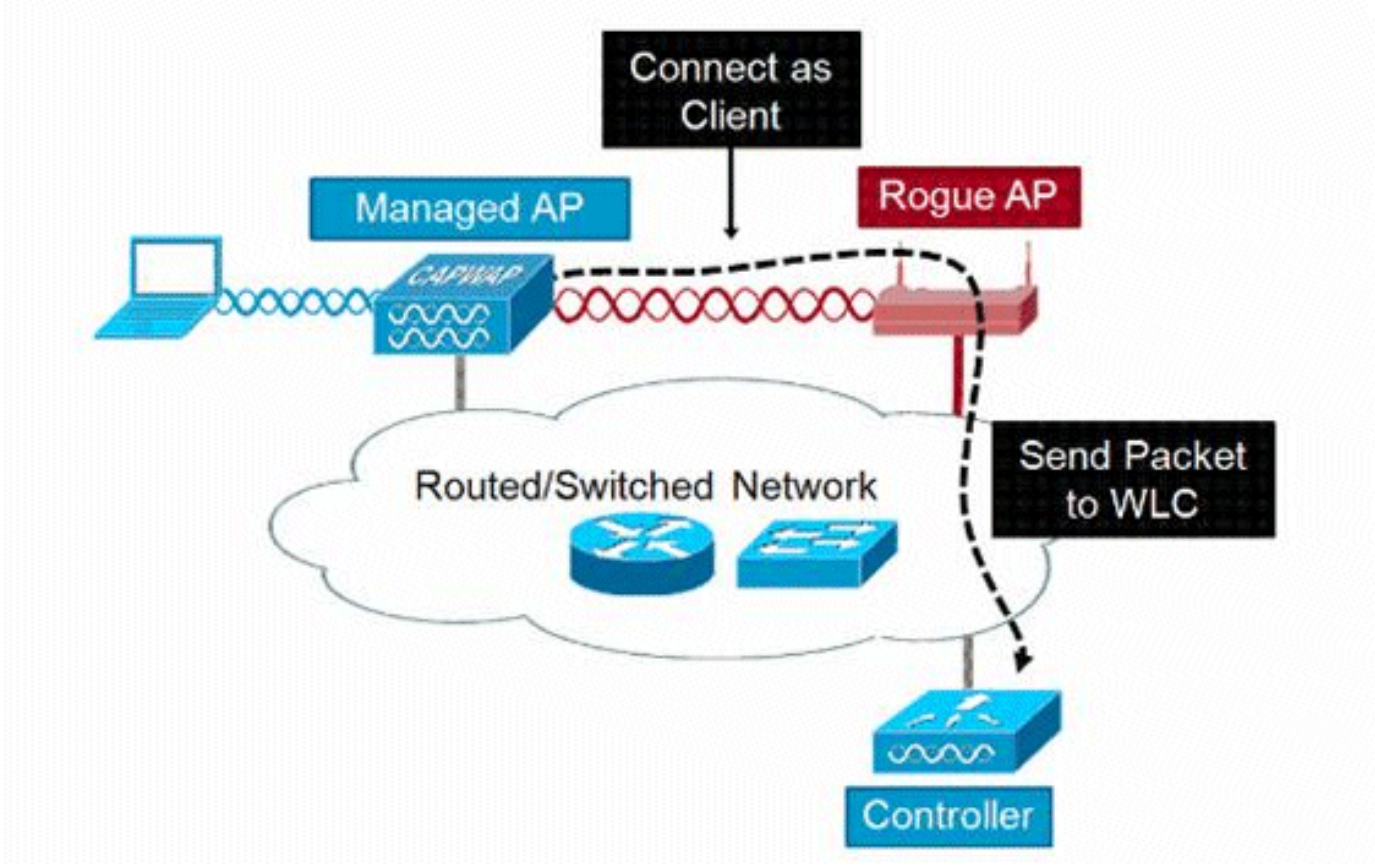
Note: Somente APs Wave 1 podem ser configurados como Rogue Detectors.

Considerações sobre escalabilidade

Um AP detector invasor pode detectar até 500 invasores e 500 clientes invasores. Se o detector de invasor for colocado em um tronco com muitos dispositivos invasores, esses limites serão excedidos, o que causa problemas. Para evitar que isso ocorra, mantenha os APs do detector invasores na camada de distribuição ou de acesso da rede.

RLDP

O objetivo do RLDP é identificar se um AP invasor específico está conectado à infraestrutura com fio. Esse recurso usa essencialmente o AP mais próximo para se conectar ao dispositivo invasor como um cliente sem fio. Após a conexão como um cliente, um pacote é enviado com o endereço destino da WLC para avaliar se o AP está conectado à rede com fio. Se for detectado que o invasor está na rede com fio, a gravidade do alarme desse AP invasor será elevada para crítica.



O algoritmo de RLDP está listado aqui:

1. Identificar o AP Unificado mais próximo do invasor pelo uso de valores de intensidade de sinal.
2. O AP conecta-se ao invasor como um cliente WLAN, tenta três associações antes que ele expire.
3. Se a associação for bem-sucedida, o AP usará DHCP para obter um endereço IP.
4. Se um endereço IP foi obtido, o AP (que atua como um cliente WLAN) envia um pacote UDP para cada um dos endereços IP do controlador.
5. Se o controlador receber até mesmo um dos pacotes RLDP do cliente, esse invasor será marcado como on-wire com uma gravidade de crítico.

Note: Os pacotes RLDP não conseguirão alcançar o controlador se as regras de filtro estiverem em vigor entre a rede do controlador e a rede onde o dispositivo invasor está localizado.

Avisos do RLDP

- O RLDP só funciona com APs invasores abertos que transmitem seu SSID com autenticação e criptografia desativadas.
- O RLDP exige que o AP Gerenciado que atua como um cliente possa obter um endereço IP através do DHCP na rede invasora
- O RLDP manual pode ser usado para tentar e rastrear o RLDP em um invasor várias vezes.
- No processo RLDP, o AP é incapaz de servir clientes. Isso afeta negativamente o desempenho e a conectividade para APs de modo local.

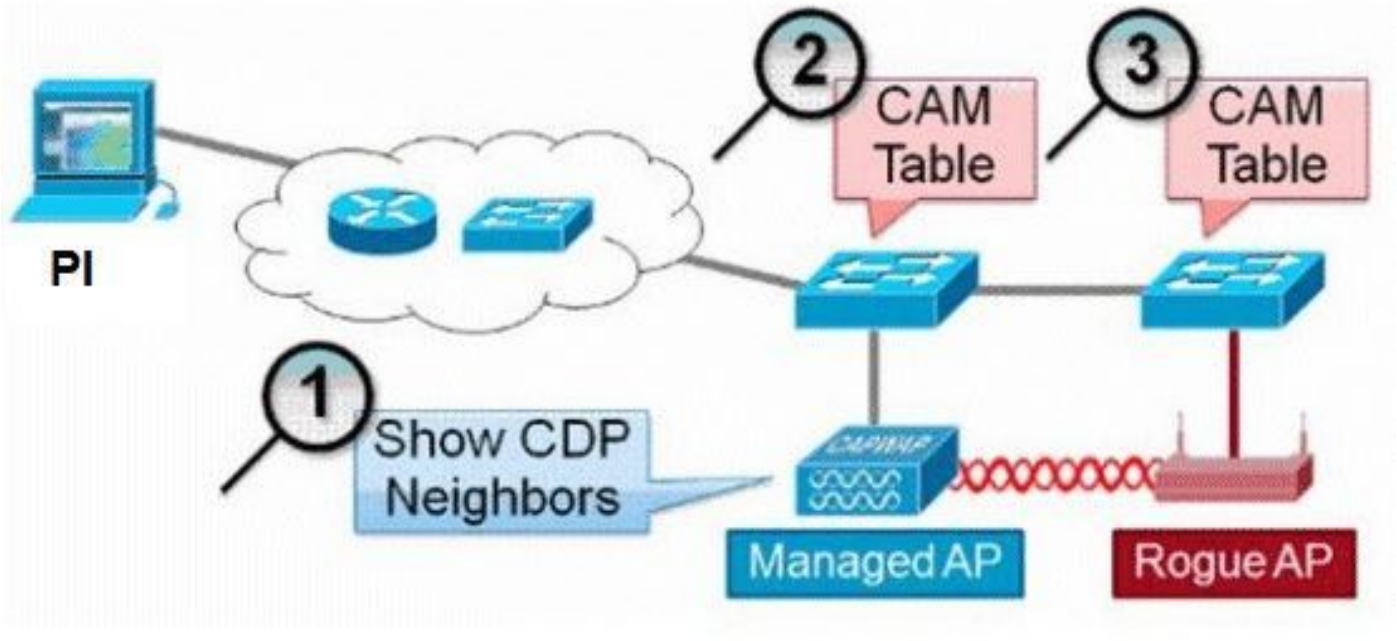
- O RLDP não tenta se conectar a um AP invasor que opera em um canal DFS de 5 GHz.

Rastreamentos de porta do switch

O rastreamento de porta de switch é uma técnica de mitigação de AP invasor. Embora o rastreamento de porta do switch seja iniciado no PI, ele utiliza informações CDP e SNMP para rastrear um invasor até uma porta específica na rede.

Para que o rastreamento de porta do switch seja executado, todos os switches na rede devem ser adicionados ao PI com credenciais SNMP. Embora as credenciais somente leitura funcionem para identificar a porta em que o invasor está, as credenciais de leitura e gravação permitem que o PI também desligue a porta, portanto, ela contém a ameaça.

Neste momento, esse recurso funciona apenas com switches Cisco que executam o Cisco IOS® com CDP ativado, e o CDP também deve ser ativado nos APs gerenciados.



O algoritmo para o rastreamento de porta do switch está listado aqui:

1. O PI encontra o AP mais próximo, que detecta o AP invasor pelo ar e recupera seus vizinhos CDP.
2. Em seguida, o PI usa o SNMP para examinar a tabela CAM dentro do switch vizinho; ele procura uma correspondência positiva para identificar o local não autorizado.
3. Uma correspondência positiva é baseada no endereço MAC invasor exato, +1/−1 no endereço MAC invasor, em qualquer endereço MAC cliente invasor ou em uma correspondência OUI baseada nas informações do fornecedor inerentes a um endereço MAC.
4. Se uma correspondência positiva não for encontrada no switch mais próximo, o PI continuará a pesquisa nos switches vizinhos a até dois saltos de distância (por padrão).

Wired-Side Tracing Techniques
Comparison

	How it Works	What It Detects	Accuracy
Switchport Tracing	1. AP hears rogue over air 2. Detecting AP advises of nearby switches 3. Trace starts on nearby switches 4. Results reported in order of probability 5. Administrator may disable port	•Open APs •Secured APs •NAT APs	•Moderate
RLDP	1. AP hears rogue over air 2. Detecting AP connects as client to rogue AP 3. Detecting AP sends RLDP packet 4. If RLDP packet seen at WLC, then on wire	•Open APs •NAT APs	•100%
Rogue Detector	1. Place detector AP on trunk 2. Detector receives all rogue MACs from WLC 3. Detector AP matches rogue MACs from wired-side ARPs	•Open APs •Secured APs •NAT APs	•High

Classificação de invasor

Por padrão, todos os invasores detectados pelo Cisco UWN são considerados Não classificados. Como mostrado neste gráfico, os invasores podem ser classificados em vários critérios que incluem RSSI, SSID, tipo de segurança, rede ativa/desativa e número de clientes:

Regras de classificação não autorizadas

As regras de classificação de invasor permitem definir um conjunto de condições que marcam um invasor como mal-intencionado ou amigável. Essas regras são configuradas no PI ou no WLC, mas sempre são executadas no controlador quando novos invasores são descobertos.

Leia o documento Classificação de invasores com base em regras em controladoras Wireless LAN (WLC) e infraestrutura Prime (PI)para obter mais informações sobre regras invasoras nas WLCs.

Fatos HA

Se você mover manualmente qualquer dispositivo invasor para o estado contido (qualquer classe) ou amigável, essas informações serão armazenadas na memória flash do Cisco WLC em standby; no entanto, o banco de dados não é atualizado. Quando ocorre o switchover HA, a lista de invasores da memória flash do Cisco WLC em espera anteriormente é carregada.

Em um cenário de Alta Disponibilidade, se o nível de segurança de detecção de invasor estiver definido como Alto ou Crítico, o temporizador de invasor no controlador em espera começará somente após a detecção de invasor gastar o tempo de estabilização, que é de 300 segundos. Portanto, as configurações ativas no controlador em standby são refletidas somente após 300 segundos.

Fatos sobre Flex-Connect

Um AP FlexConnect (com detecção de invasor ativada) no modo conectado obtém a lista de contenção do controlador. Se o SSID de contenção automática e o adhoc de contenção automática estiverem definidos no controlador, essas configurações serão definidas para todos os APs FlexConnect no modo conectado e o AP o armazenará na memória.

Quando o AP FlexConnect muda para um modo autônomo, as próximas tarefas são executadas:

- A contenção definida pelo controlador continua.
- Se o AP FlexConnect detectar qualquer AP invasor que tenha o mesmo SSID do SSID inferior (SSID configurado no controlador ao qual o AP FlexConnect está conectado), a contenção será iniciada se o SSID de contenção automática tiver sido ativado no controlador antes de ele passar para o modo autônomo.
- Se o AP FlexConnect detectar qualquer invasor adhoc, a contenção será iniciada se o adhoc de contenção automática tiver sido ativado no controlador quando ele estava no modo conectado.

Quando o AP FlexConnect autônomo volta para o modo conectado, estas tarefas são executadas:

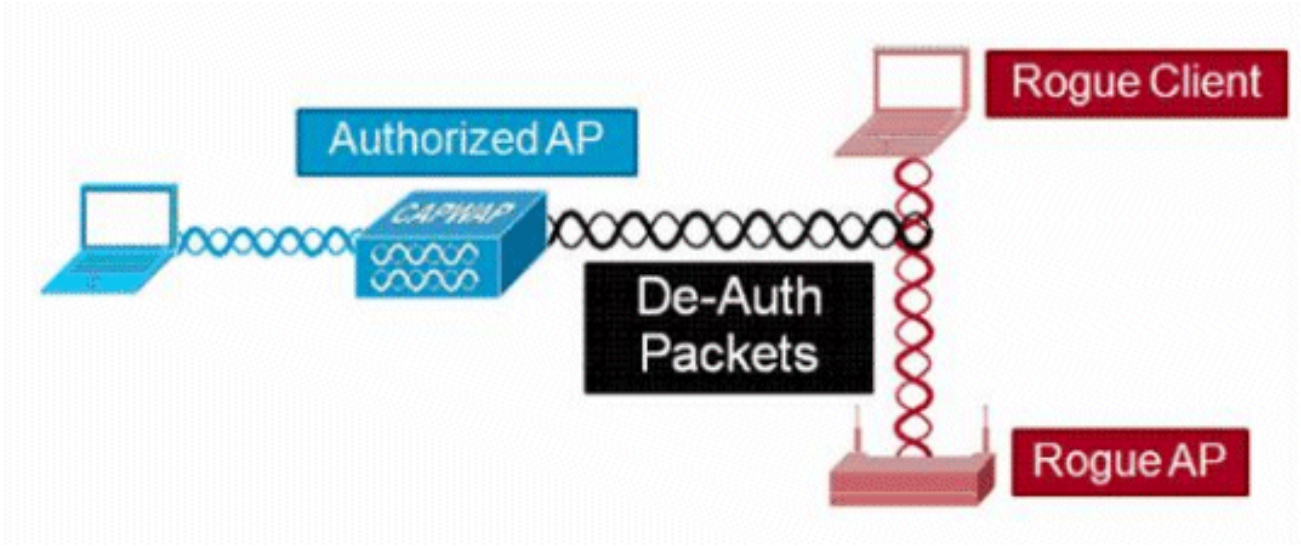
- Toda a contenção é limpa.
- A contenção iniciada pelo controlador assume o controle.

Atenuação de invasores

Contenção de invasores

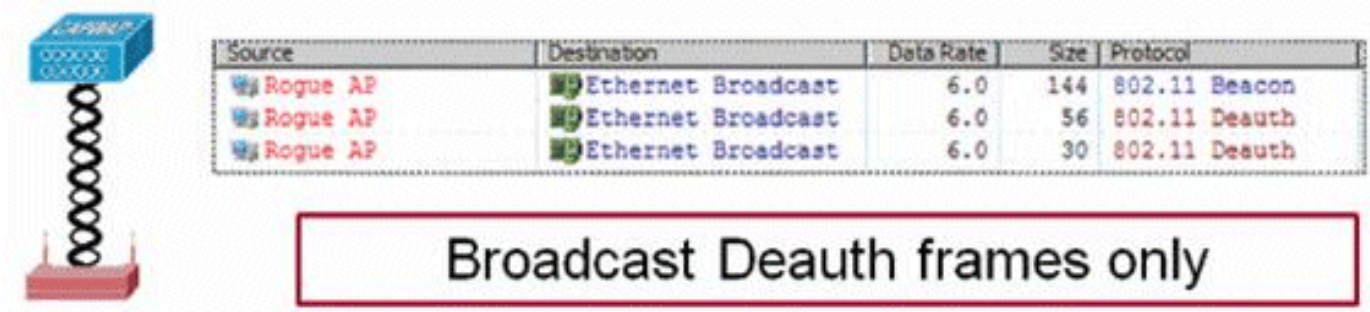
A contenção é um método que usa pacotes over-the-air para interromper temporariamente o

serviço em um dispositivo invasor até que ele possa ser fisicamente removido. A contenção funciona com o spoof de pacotes de desautenticação com o endereço de origem falsificado do AP invasor de modo que todos os clientes associados sejam iniciados.

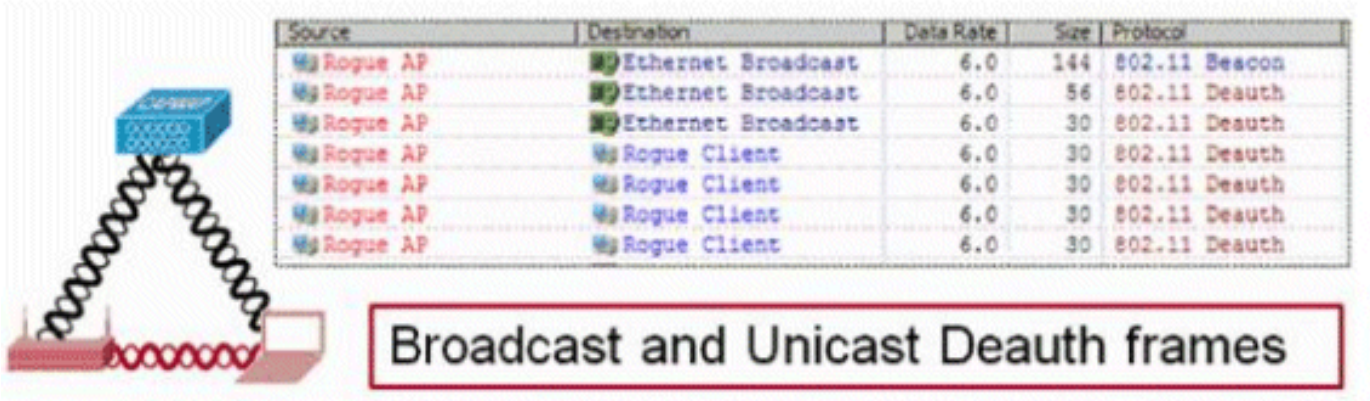


Detalhes de contenção invasor

Uma contenção iniciada em um AP invasor sem clientes usa apenas quadros de desautenticação enviados ao endereço de broadcast:

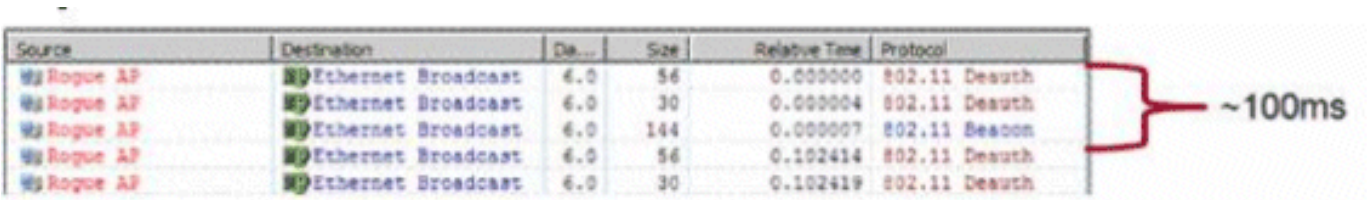


Uma contenção iniciada em um AP invasor com cliente(s) usa quadros de desautenticação enviados ao endereço de broadcast e ao endereço do cliente(s):



Os pacotes de contenção são enviados no nível de potência do AP gerenciado e na menor taxa de dados ativada.

A contenção envia um mínimo de 2 pacotes a cada 100 ms:



> **Note**: Uma contenção executada por APs no modo não monitor é enviada em um intervalo de 500 ms em vez do intervalo de 100 ms usado por APs no modo monitor.

- Um dispositivo invasor individual pode ser contido por 1 a 4 APs gerenciados que trabalham em conjunto para mitigar a ameaça temporariamente.
- A contenção pode ser realizada pelo uso de APs de modo local, modo de monitor e modo de conexão flexível (conectado). Para o modo local de APs de conexão flexível, um máximo de três dispositivos invasores por rádio pode ser contido. Para APs do modo de monitor, um máximo de seis dispositivos invasores por rádio pode ser contido.

Contenção automática

Além do início manual da contenção em um dispositivo invasor através do PI ou da GUI da WLC, também há a capacidade de iniciar automaticamente a contenção em determinados cenários. Essa configuração é encontrada na seção Generalin theRogue Policies do PI ou da interface do controlador. Cada um desses recursos é desativado por padrão e deve ser ativado apenas para anular as ameaças que causam mais danos.

- Rogue on Wire - Se um dispositivo invasor for identificado para ser conectado à rede com fio, ele será automaticamente colocado sob contenção.
- Uso de nosso SSID - Se um dispositivo invasor usa um SSID que é o mesmo que o configurado no controlador, ele é automaticamente contido. Este recurso tem como objetivo abordar um ataque de pote de mel antes que ele cause danos.
- Cliente válido no AP Invasor - Se um cliente listado no servidor Radius/AAA for identificado como associado a um dispositivo invasor, a contenção será iniciada somente nesse cliente, ela impedirá a associação a qualquer AP não gerenciado.
- AP invasor ad-hoc - Se uma rede ad-hoc for descoberta, ela será automaticamente contida.

Avisos de contenção invasores

- Como a contenção usa uma parte do tempo de rádio do AP gerenciado para enviar os quadros de desautenticação, o desempenho para os clientes de dados e voz é afetado negativamente por até 20%. Para clientes de dados, o impacto é o throughput reduzido. Para clientes de voz, a contenção pode causar interrupções nas conversações e reduzir a qualidade de voz.
- A contenção pode ter implicações legais quando lançada contra redes vizinhas. Certifique-se de que o dispositivo invasor esteja na rede e represente um risco de segurança antes de iniciar a contenção.

Porta do switch fechada

Quando uma porta do switch é rastreada pelo uso de SPT, há uma opção para desativar essa porta no PI. O administrador precisa fazer este exercício manualmente. Uma opção está disponível para ativar a porta do switch através do PI se o invasor for fisicamente removido da rede.

Configurar

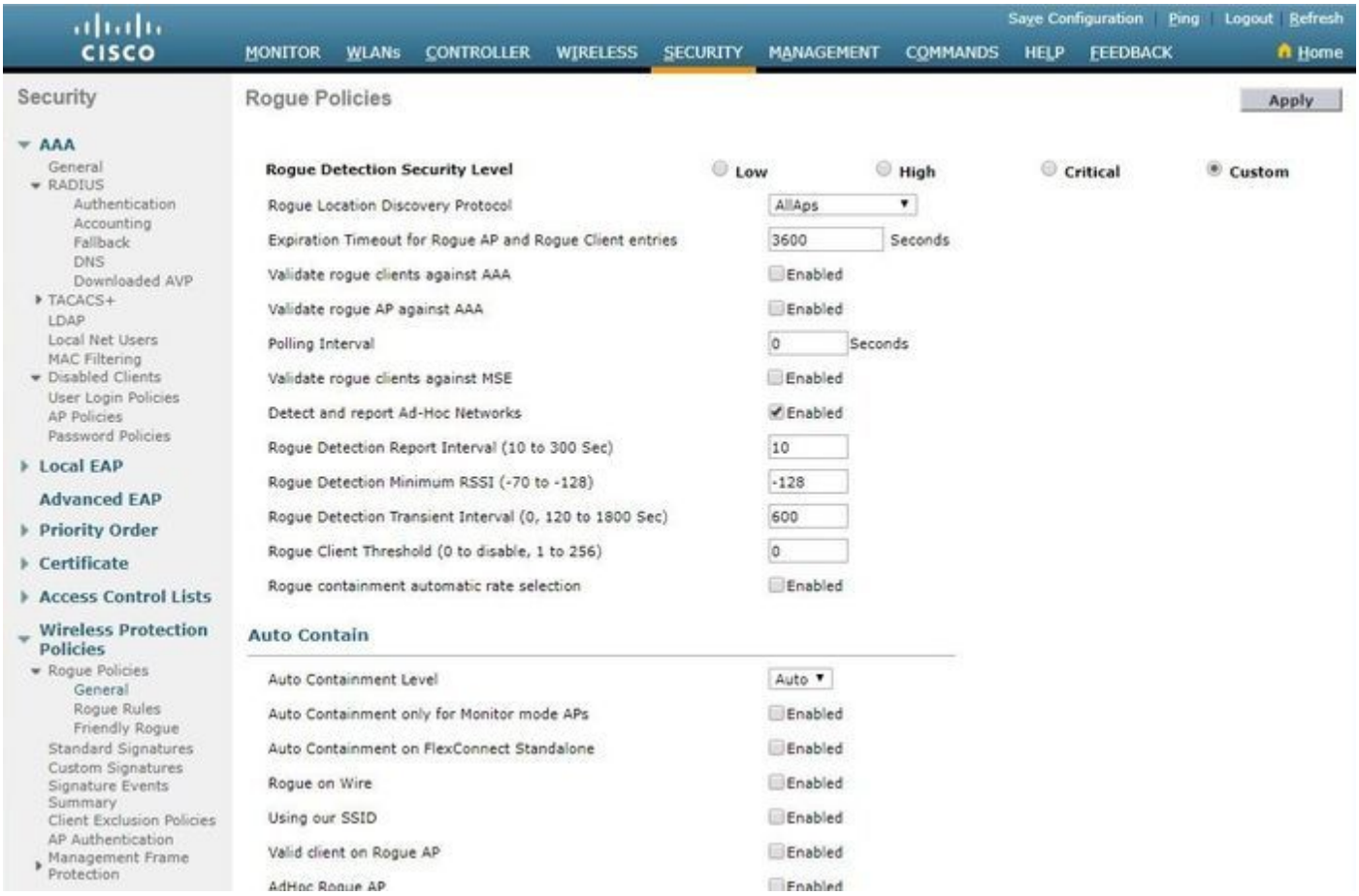
Configurar detecção de invasor

A detecção de invasor é habilitada no controlador por padrão.

Para configurar várias opções, navegue **para Segurança > Políticas de proteção sem fio > Políticas invasoras > Geral**. Como exemplo:

Etapa 1. Alterar o tempo limite para APs invasores.

Etapa 2. Habilitar a detecção de redes invasoras ad-hoc.



Na CLI:

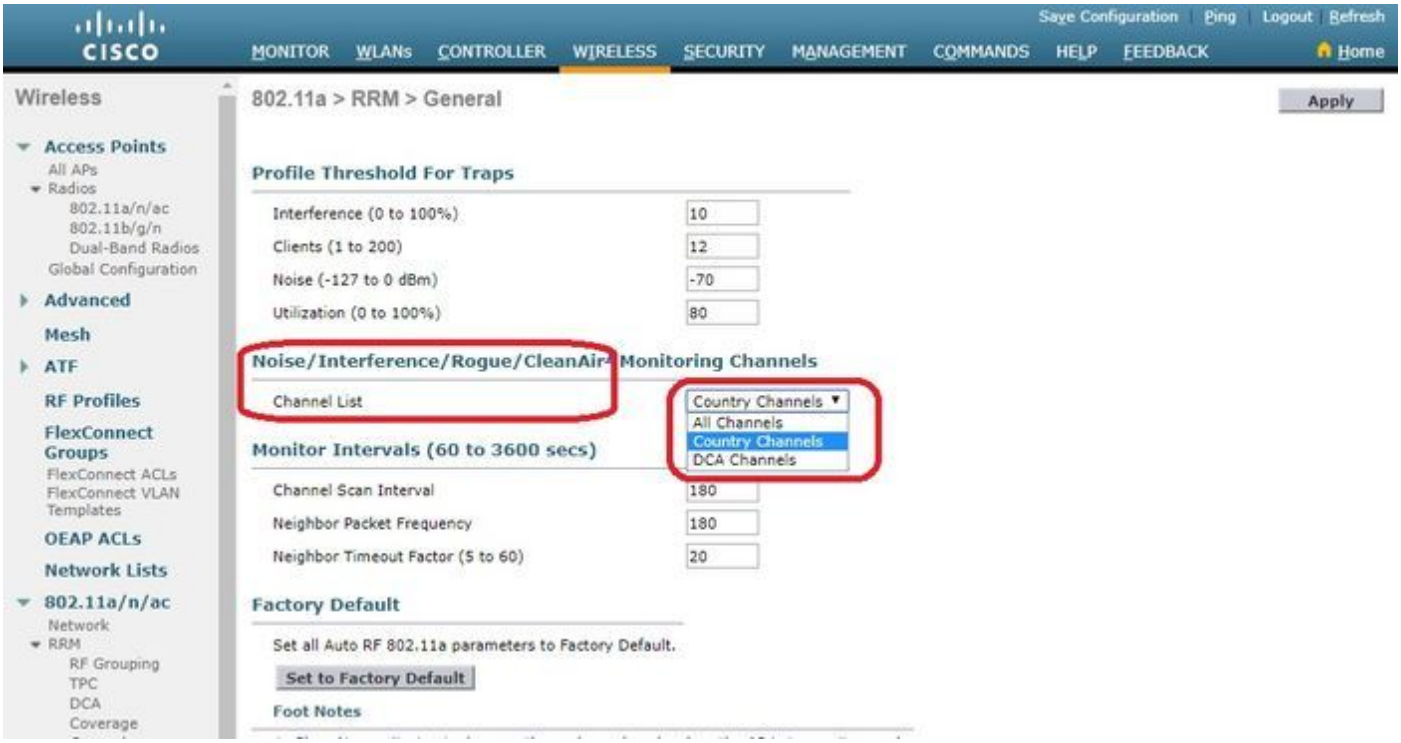
```
(Cisco Controller) >config rogue ap timeout ?

<seconds>      The number of seconds<240 - 3600> before rogue entries are flushed
```

```
(Cisco Controller) >config rogue adhoc enable/disable
```

Configurar verificação de canal para detecção de invasor

Para um AP de modo local/Flex-Connect/Monitor, há uma opção na configuração do RRM que permite que o usuário escolha quais canais são verificados quanto a invasores. Depende da configuração, o AP verifica se há invasores em todos os canais/países/canais de DCA.

Para configurar isso na GUI, navegue **para Wireless > 802.11a/802.11b > RRM > General,** conforme mostrado na imagem.



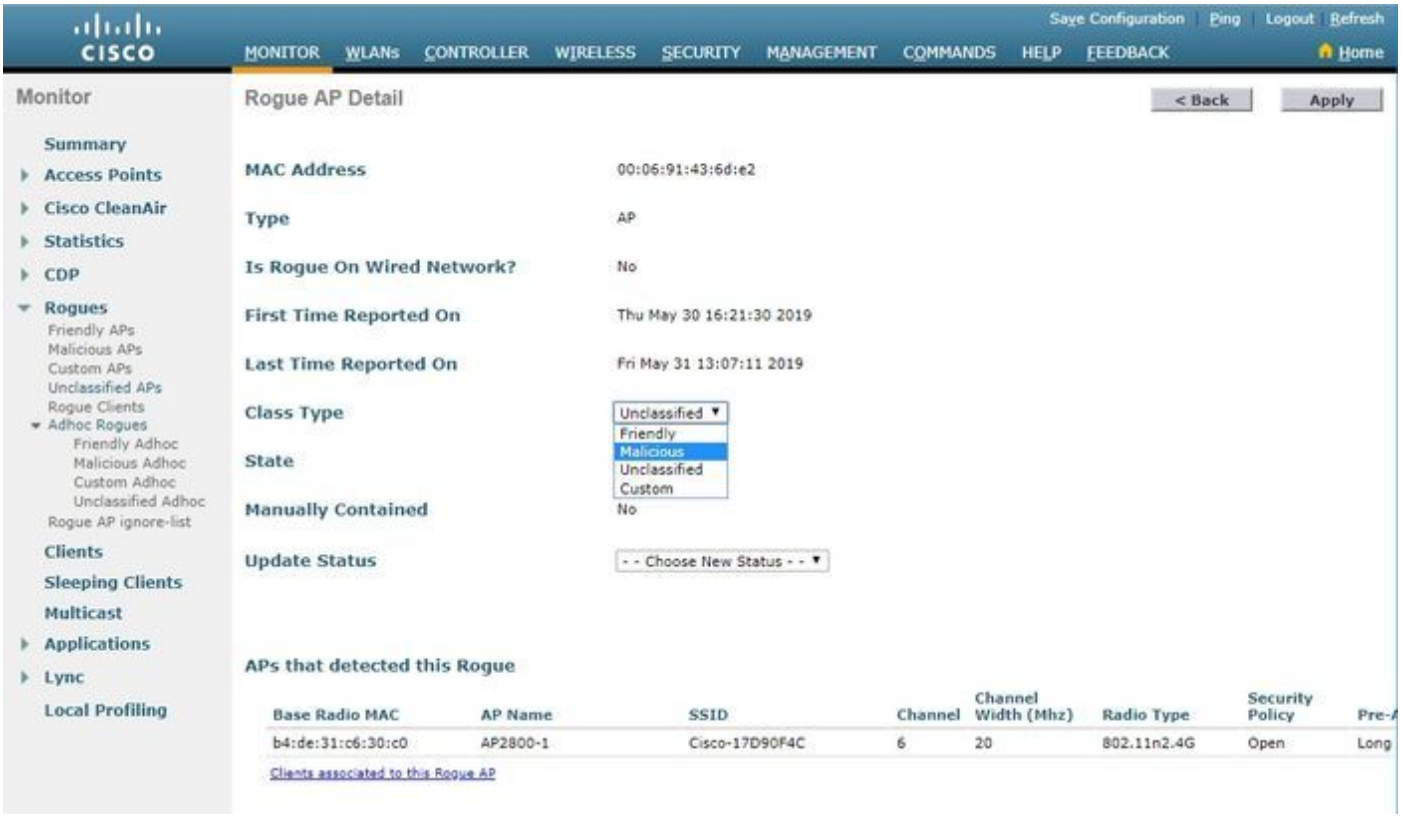
Na CLI:

```
(Cisco Controller) >config advanced 802.11a monitor channel-list ?

all             Monitor all channels
country         Monitor channels used in configured country code
dca             Monitor channels used by automatic channel assignment
```

Configurar classificação de invasor

Classificar manualmente um AP invasor

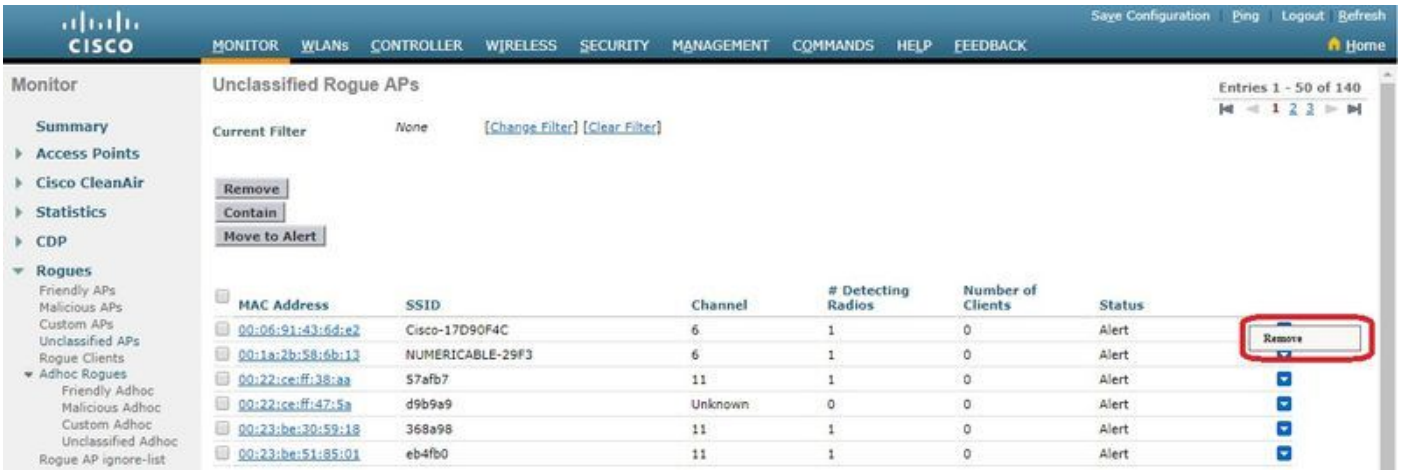
Para classificar um AP invasor como amigável, mal-intencionado ou não classificado, navegue **para Monitor > Invasor >** APs **não classificados** e clique no nome do AP invasor específico. Escolha a opção na lista suspensa, conforme mostrado na imagem.



Na CLI:

```
(Cisco Controller) >config rogue ap ?

classify        Configures rogue access points classification.
friendly        Configures friendly AP devices.
rldp            Configures Rogue Location Discovery Protocol.
ssid            Configures policy for rogue APs advertsing our SSID.
timeout         Configures the expiration time for rogue entries, in seconds.
valid-client    Configures policy for valid clients which use rogue APs.
```

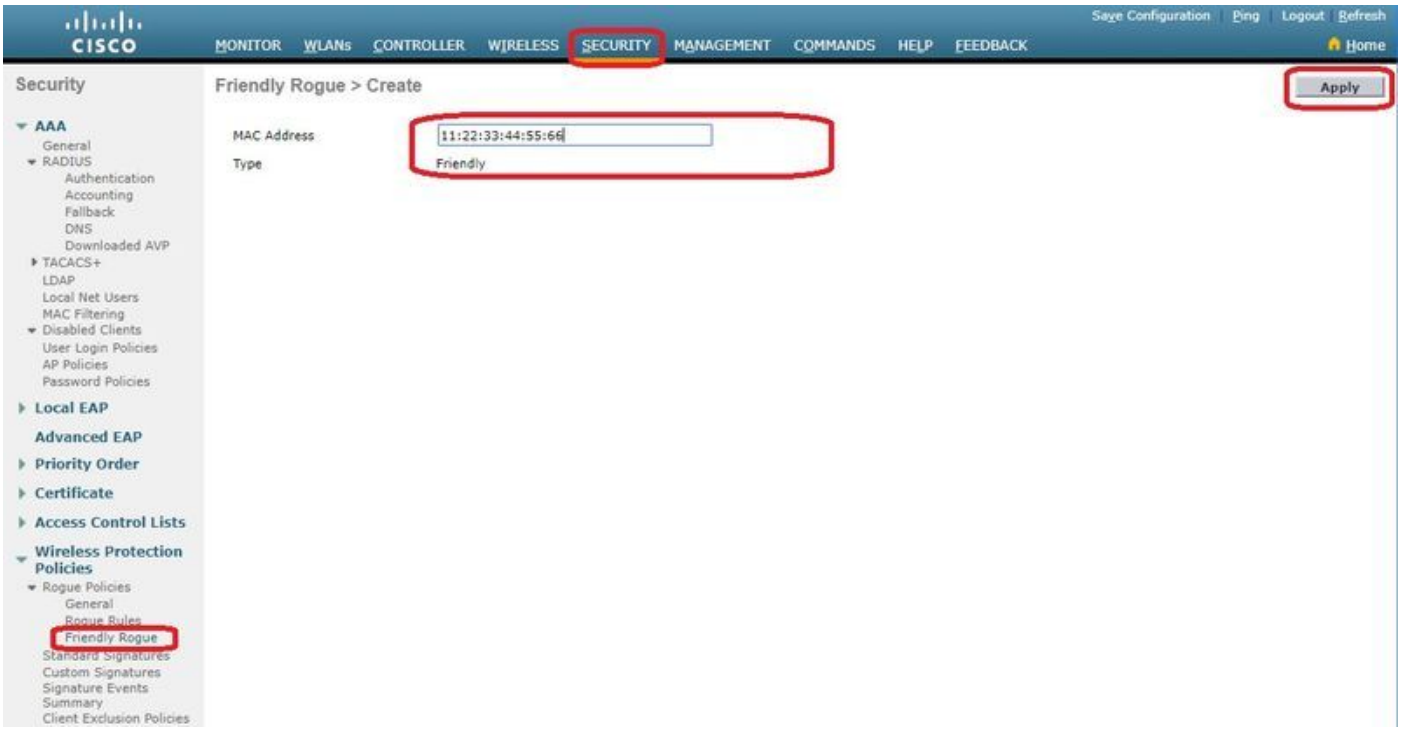
Para remover uma entrada de invasor manualmente da lista de invasores, navegue **para Monitor > Invasor >** APs **não classificados** e **clique em Remover**, como mostrado na imagem.



Para configurar um AP invasor como um AP amigável, navegue **paraSegurança > Políticas de proteção sem fio > Políticas invasoras >** Rogues **amigáveise** adicione o endereço MAC invasor.

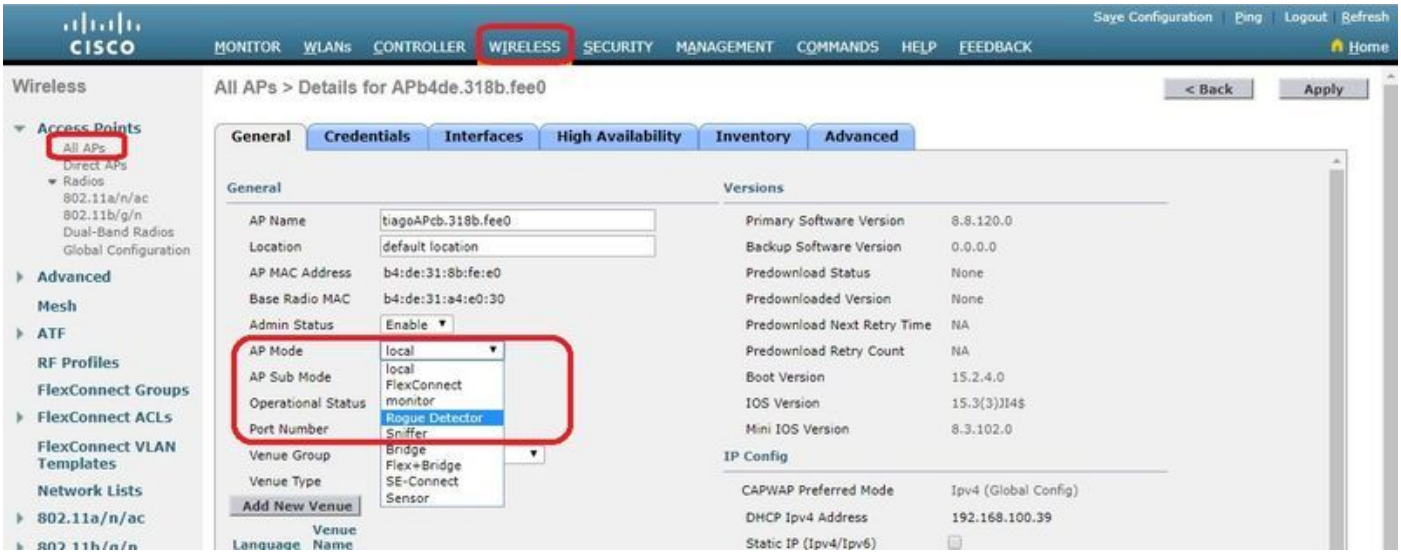
As entradas invasoras amigáveis adicionadas podem ser verificadas **emMonitor > Invasores >**

Roguepage **Amigável**, como mostrado na imagem.



Configurar um AP de Detector Invasor

Para configurar o AP como um detector invasor através da GUI, navegue para Wireless > All APs. Escolha o nome do AP e altere o modo do AP como mostrado na imagem.



Na CLI:

```
(Cisco Controller) >config ap mode rogue AP_Managed

Changing the AP's mode cause the AP to reboot.
Are you sure you want to continue? (y/n) y
```

Configurar a porta de switch para um AP de detector de invasor

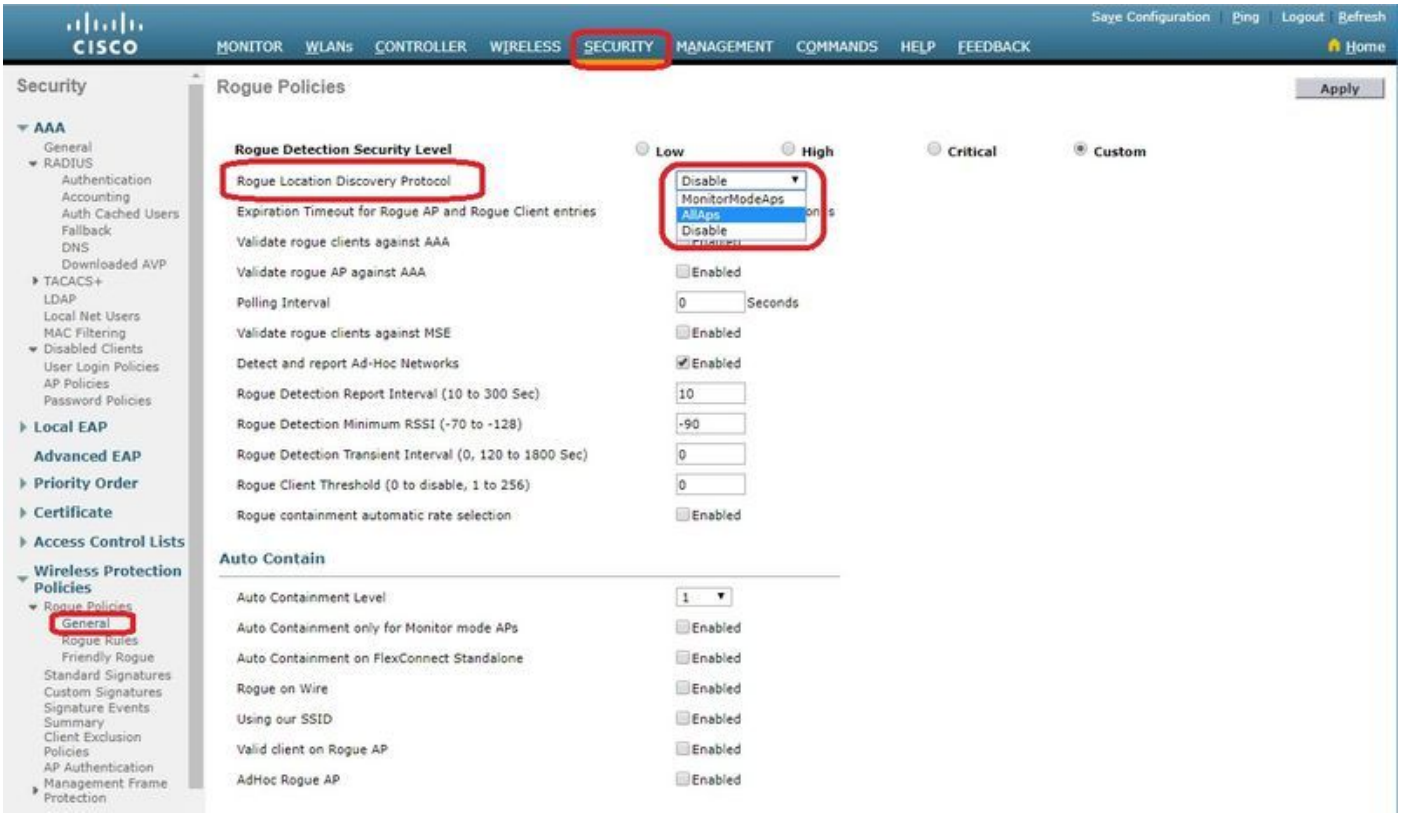
```
interface GigabitEthernet1/0/5
description Rogue Detector
```

```
switchport trunk native vlan 100
switchport mode trunk
```

Note: A VLAN nativa nessa configuração é aquela que tem conectividade IP com a WLC.

Configurar RLDP

Para configurar o RLDP na GUI do controlador, navegue **para Segurança > Políticas de proteção sem fio > Políticas invasoras > Geral**.



Monitor Mode APs- Permite que apenas APs no modo de monitor participem do RLDP.

Todos os APs - APs no modo Local/Flex-Connect/Monitor participam do processo RLDP.

Disabled- O RLDP não é acionado automaticamente. No entanto, o usuário pode acionar o RLDP manualmente para um endereço MAC específico por meio da CLI.

Note: O AP do modo de monitor tem preferência sobre o AP local/Flex-Connect para executar RLDP se ambos detectarem um invasor específico em excesso de -85dbm RSSI.

Na CLI:

```
(Cisco Controller) >config rogue ap rldp enable ?

alarm-only Enables RLDP and alarm if rogue is detected
auto-contain Enables RLDP, alarm and auto-contain if rogue is detected.

(Cisco Controller) >config rogue ap rldp enable alarm-only ?

monitor-ap-only Perform RLDP only on monitor AP
```

O agendamento e o disparo manual do RLDP são configuráveis somente através do prompt de comando. Para iniciar o RLDP manualmente:

```
(Cisco Controller) >config rogue ap rldp initiate ?

<MAC addr> Enter the MAC address of the rogue AP (e.g. 01:01:01:01:01:01).
```

Para programação do RLDP:

```
(Cisco Controller) >config rogue ap rldp schedule ?

add             Enter the days when RLDP scheduling to be done.
delete          Enter the days when RLDP scheduling needs to be deleted.
enable          Configure to enable RLDP scheduling.
disable         Configure to disable RLDP scheduling.


(Cisco Controller) >config rogue ap rldp schedule add ?

fri             Configure Friday for RLDP scheduling.
sat             Configure Saturday for RLDP scheduling.
sun             Configure Sunday for RLDP scheduling.
mon             Configure Monday for RLDP scheduling.
tue             Configure Tuesday for RLDP scheduling.
wed             Configure Wednesday for RLDP scheduling.
thu             Configure Thursday for RLDP scheduling.
```

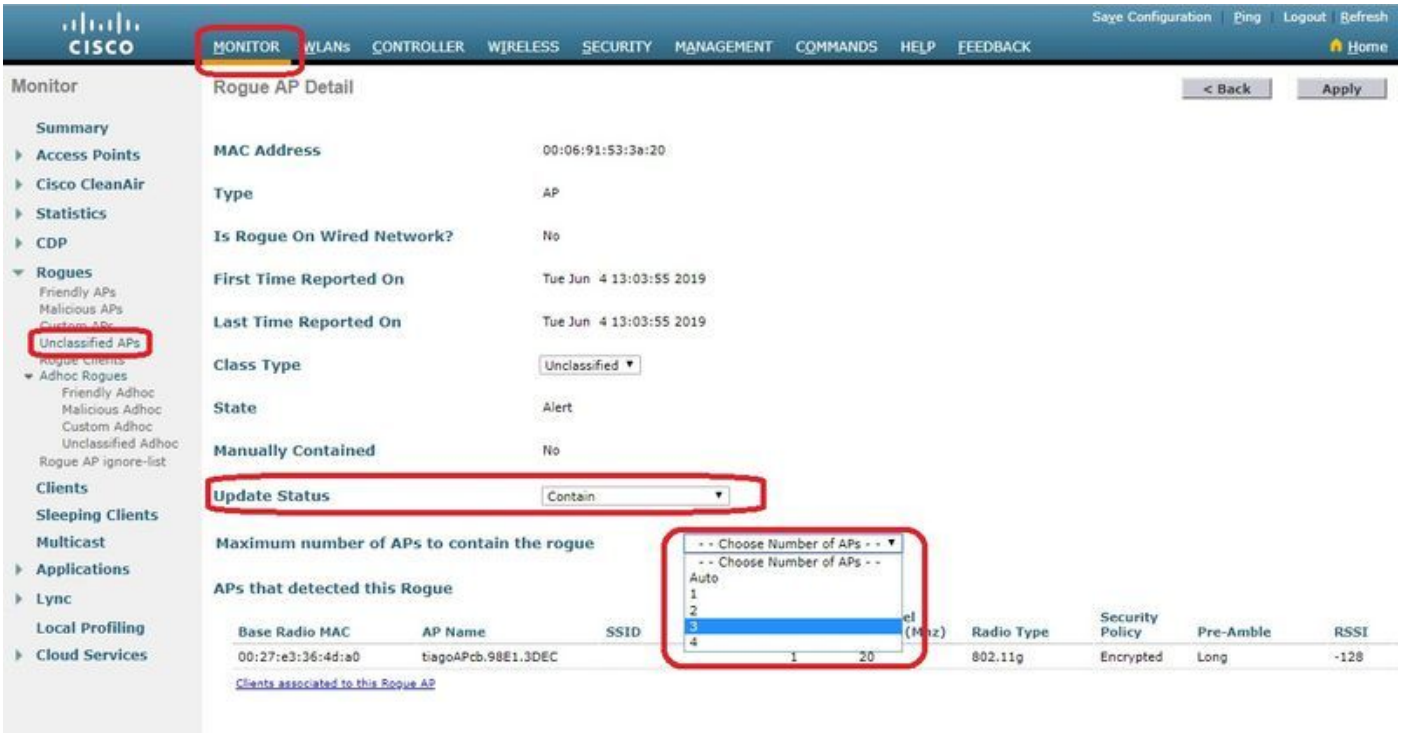
As tentativas de RLDP podem ser configuradas com o comando:

```
(Cisco Controller) >config rogue ap rldp retries ?

<count>         Enter the no.of times(1 - 5) RLDP to be tried per Rogue AP.
```

Configurar a mitigação de invasores

Configurar Contenção Manual

Para conter um AP invasor manualmente, navegue **para Monitor > Invasores > Não classificado**, conforme mostrado na imagem.



Na CLI:

```
(Cisco Controller) >config rogue client ?

aaa Configures to validate if a rogue client is a valid client which uses AAA/local database.
alert Configure the rogue client to the alarm state.
contain Start to contain a rogue client.
delete Delete rogue Client
mse Configures to validate if a rogue client is a valid client which uses MSE.

(Cisco Controller) >config rogue client contain 11:22:33:44:55:66 ?

<num of APs> Enter the maximum number of Cisco APs to actively contain the rogue client [1-4].
```

> **Note**: Um invasor específico pode ser contido com 1 a 4 APs. Por padrão, o controlador usa um AP para conter um cliente. Se dois APs são capazes de detectar um invasor específico, o AP com o RSSI mais alto contém o cliente, independentemente do modo do AP.

Contenção automática

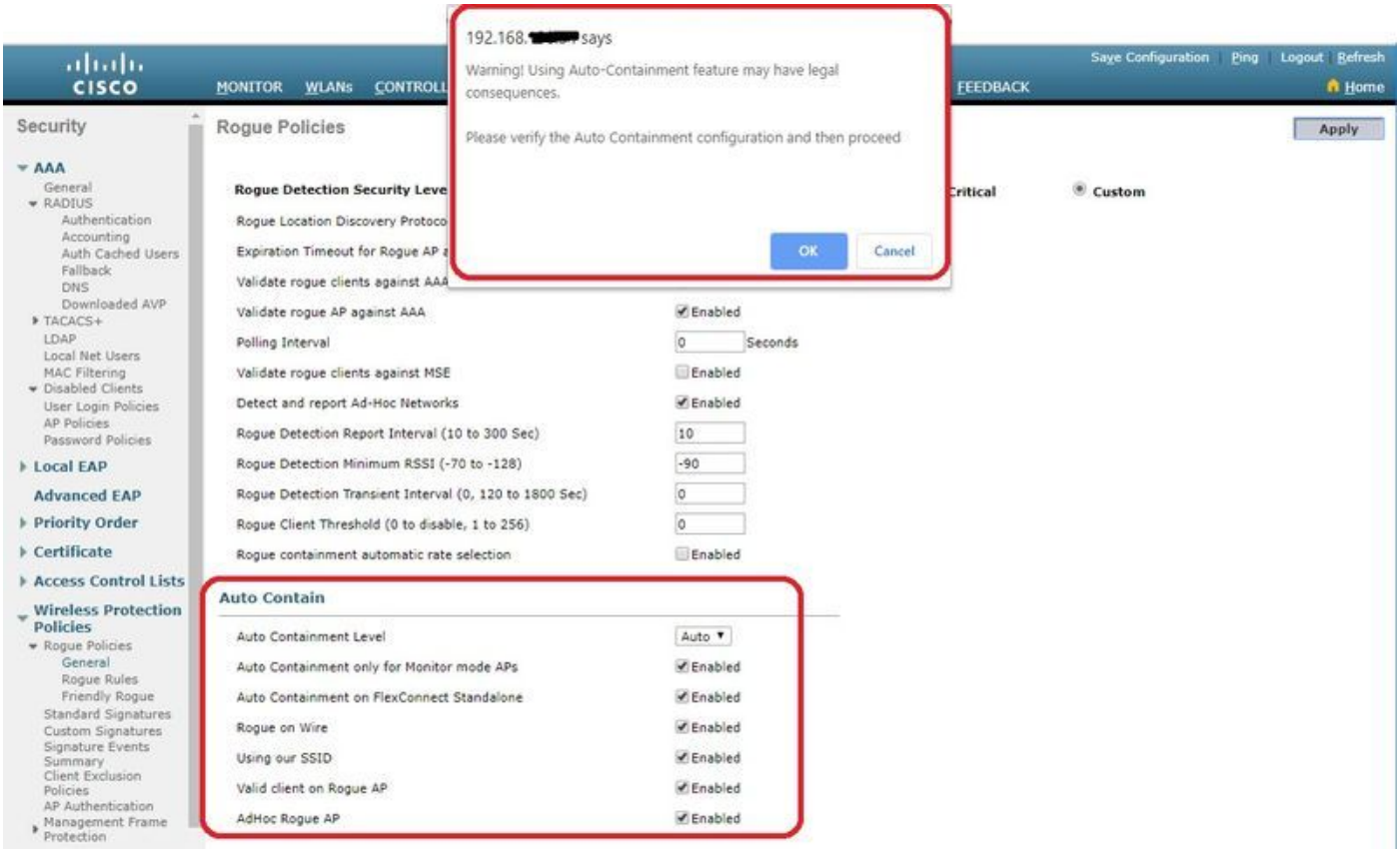
Para configurar a contenção automática, vá **paraSecurity>Wireless Protection Policies>Rogue Policies>General** e ative todas as opções aplicáveis para sua rede.

Se você quiser que o Cisco WLC contenha automaticamente determinados dispositivos invasores, marque essas caixas. Caso contrário, deixe as caixas de seleção desmarcadas, que é o valor padrão.

> **aviso:** Quando você ativa qualquer um desses parâmetros, a mensagem aparece:"O uso desse recurso tem consequências legais. Deseja continuar?" As frequências de 2,4 e 5 GHz na banda Industrial, Scientific e Medical (ISM) são abertas ao público e podem ser usadas sem licença. Como tal, a contenção de dispositivos na rede de outra parte pode ter consequências legais.

Estes são os parâmetros de contenção automática:

Parâmetro	Descrição
Nível de contenção automática	Lista suspensa na qual você pode escolher o nível de contenção automática invasor de 1 a Você pode escolher até quatro APs para contenção automática quando um invasor for mo para um estado contido por meio de qualquer uma das políticas de contenção automática. Você também pode escolher Automático para seleção automática do número de APs usad para contenção automática. O Cisco WLC escolhe o número necessário de APs com base RSSI para uma contenção eficaz. O valor de RSSI associado a cada nível de contenção é o seguinte: • 1 — 0 a -55 dBm • 2 — -75 a -55 dBm • 3 — -85 a -75 dBm • 4 — Inferior a -85 dBm
Contenção automática somente para APs no modo Monitor	Marque a caixa que você pode selecionar para ativar os APs do modo de monitor para contenção automática. O padrão é o estado desativado.
Contenção automática no FlexConnect independente	Marque a caixa que você pode selecionar para ativar a contenção automática em APs FlexConnect no modo autônomo. O padrão é o estado desativado. Quando os APs FlexConnect estão no modo autônomo, você pode habilitar somente as políticas de conter automática Use our SSID or AdHoc Rogue AP. A contenção pára depois que o AP autôno conecta novamente ao Cisco WLC.
Rogue no fio	Marque a caixa que você habilita para conter automaticamente os invasores detectados na com fio. O padrão é o estado desativado.
Use nosso SSID	Marque a caixa que você habilita para conter automaticamente os invasores que anuncian SSID da sua rede. Se você deixar esse parâmetro desmarcado, o Cisco WLC gerará um a apenas quando um invasor for detectado. O padrão é o estado desativado.
Cliente válido no AP Invasor	Caixa de seleção que você ativa para conter automaticamente um ponto de acesso não autorizado ao qual os clientes confiáveis estão associados. Se você deixar esse parâmetro desmarcado, o Cisco WLC gerará um alarme apenas quando um invasor for detectado. O padrão é o estado desativado.
AP invasor ad-hoc	Marque a caixa que você habilita para conter automaticamente redes ad-hoc detectadas p Cisco WLC. Se você deixar esse parâmetro desmarcado, o Cisco WLC gerará um alarme apenas quando tal rede for detectada. O padrão é o estado desativado.



Clique em Apply para enviar dados para o Cisco WLC, mas os dados não são preservados durante um ciclo de energia; esses parâmetros são armazenados temporariamente na RAM volátil.

Na CLI:

```
(Cisco Controller) >config rogue adhoc ?

alert           Stop Auto-Containment, generate a trap upon detection of the
                    adhoc rogue.
auto-contain    Automatically contain adhoc rogue.
contain         Start to contain adhoc rogue.
disable         Disable detection and reporting of Ad-Hoc rogues.
enable          Enable detection and reporting of Ad-Hoc rogues.
external        Acknowledge presence of a adhoc rogue.

(Cisco Controller) >config rogue adhoc auto-contain ?
(Cisco Controller) >config rogue adhoc auto-contain
 Warning! Use of this feature has legal consequences
        Do you want to continue(y/n) :y
```

Com infraestrutura Prime

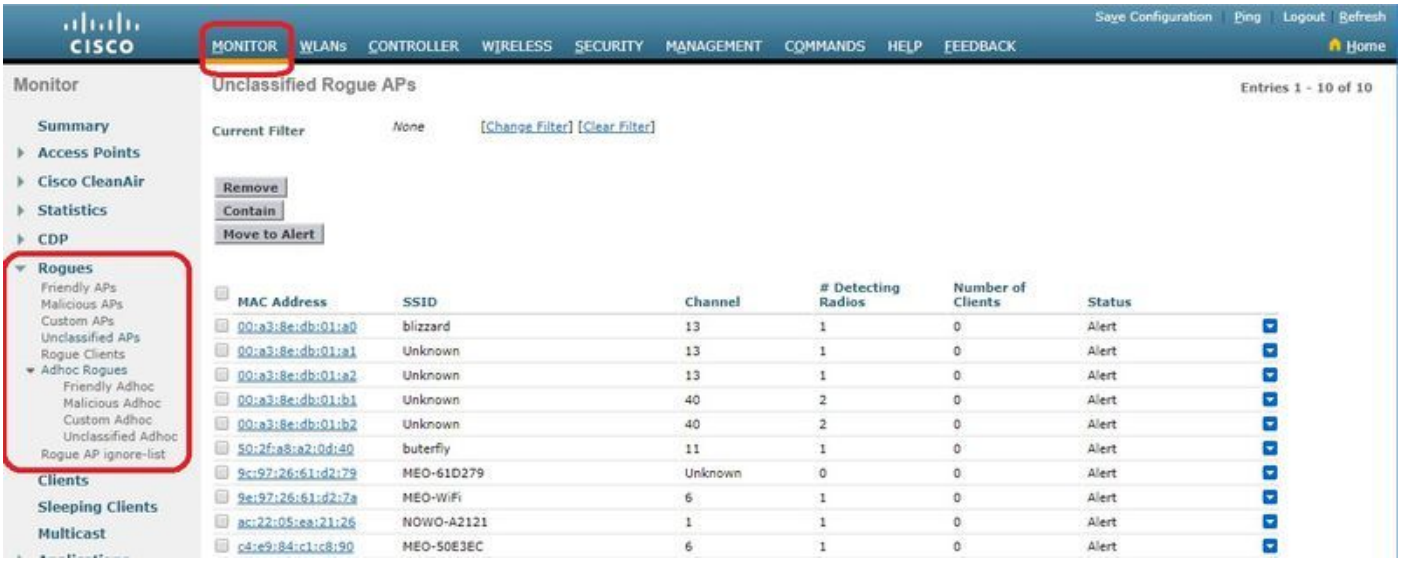
O Cisco Prime Infrastructure pode ser usado para configurar e monitorar um ou mais controladores e APs associados. O Cisco PI tem ferramentas para facilitar o monitoramento e o controle de grandes sistemas. Quando você usa o Cisco PI em sua solução sem fio da Cisco, os controladores determinam periodicamente o cliente, o ponto de acesso não autorizado, o cliente de ponto de acesso não autorizado, a localização da etiqueta da ID de radiofrequência (RFID) e armazenam os locais no banco de dados Cisco PI.

O Cisco Prime Infrastructure suporta classificação baseada em regras e usa as regras de classificação configuradas no controlador. O controlador envia armadilhas para o Cisco Prime Infrastructure após estes eventos:

- Se um ponto de acesso desconhecido passar para o estado Amigável pela primeira vez, o controlador enviará uma interceptação à Cisco Prime Infrastructure somente se o estado invasor for Alerta. Ele não enviará uma armadilha se theroguestate for **Internal** ou External.
- Se arogueentry for removida após o tempo limite expirar, o controlador enviará uma interceptação para o Cisco Prime Infrastructureforrogueaccess points que são categorizados como Malicioso (Alerta, Ameaça) ou Não classificado (Alerta). O controlador não removerogueentries com oseroguestates: **Contido, Contido Pendente**, **Interno e Externo.**

Verificar

Para encontrar detalhes de invasor em um controlador na interface gráfica, navegue **para Monitor > Invasores**, conforme mostrado na imagem.

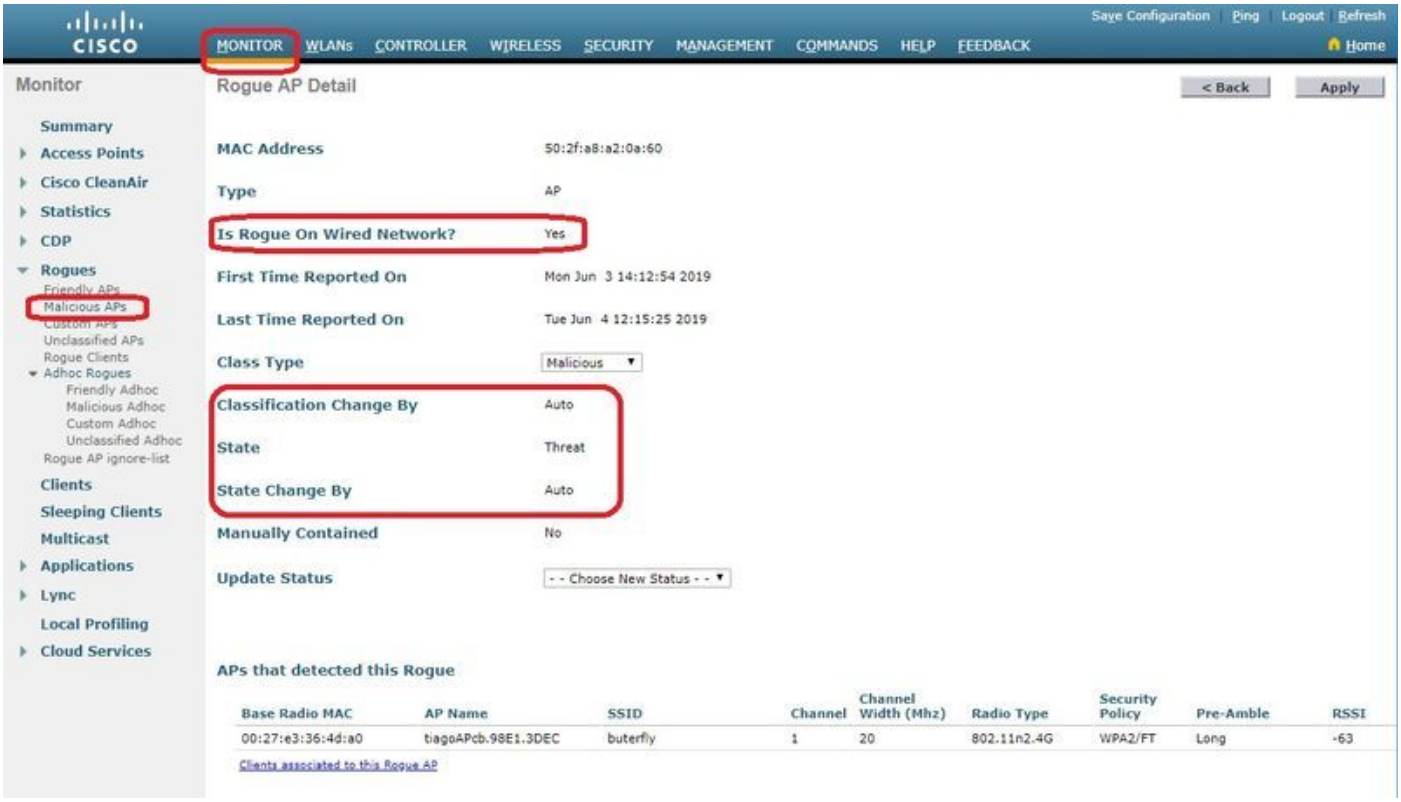


Nesta página, estão disponíveis classificações diferentes para invasores:

- APs amigáveis - APs marcados como amigáveis pelo administrador.
- APs mal-intencionados - APs que são identificados como mal-intencionados por meio de RLDP ou AP detector de invasores.
- APs personalizados - APs classificados como personalizados por regras não autorizadas.
- APs não classificados - Por padrão, os APs invasores são mostrados como uma lista não classificada no controlador.
- Clientes invasores - Clientes conectados a APs invasores.
- Invasores Adhoc - Clientes Invasores Adhoc.
- Lista de ignorar AP não autorizado - Conforme listado através do PI.

> **Note**: Se a WLC e o AP autônomo forem gerenciados pelo mesmo PI, a WLC listará automaticamente esse AP autônomo na lista de ignorar APs invasores. Não há configuração adicional necessária na WLC para ativar esse recurso.

Clique em uma entrada não autorizada específica para obter os detalhes dessa entrada não autorizada. Aqui está um exemplo de um invasor detectado em uma rede com fio:



Na CLI:

```
(Cisco Controller) >show rogue ap summary

Rogue Detection Security Level..................... custom
Rogue Pending Time.............................. 180 secs
Rogue on wire Auto-Contain...................... Disabled
Rogue uses our SSID Auto-Contain................ Disabled
Valid client on rogue AP Auto-Contain............ Disabled
Rogue AP timeout................................ 1200
Rogue Detection Report Interval................. 10
Rogue Detection Min Rssi........................ -90
Rogue Detection Transient Interval.............. 0
Rogue Detection Client Num Threshold............ 0
Validate rogue AP against AAA................... Enabled
Rogue AP AAA validation interval................ 0 secs
Total Rogues(AP+Ad-hoc) supported............... 600
Total Rogues classified......................... 12

MAC Address       Class        State                #Det #Rogue  #Highest RSSI     #RSSI
#Channel        #Second Highest   #RSSI  #Channel
                                                    Aps  Clients  det-Ap
RSSI Det-Ap
----------------- ------------ -------------------- ---- ------- ----------------- ------ ------
--------- ----------------- ------ ---------------
00:a3:8e:db:01:a0 Unclassified Alert                1    0       00:27:e3:36:4d:a0 -16    13
00:a3:8e:db:01:a1 Unclassified Alert                1    0       00:27:e3:36:4d:a0 -16    13
00:a3:8e:db:01:a2 Unclassified Alert                1    0       00:27:e3:36:4d:a0 -16    13
00:a3:8e:db:01:b0 Malicious    Threat               2    1       00:27:e3:36:4d:a0 -27    40
00:27:e3:36:4d:a0 -37    40
00:a3:8e:db:01:b1 Unclassified Alert                2    0       00:27:e3:36:4d:a0 -28    40
00:27:e3:36:4d:a0 -36    40
00:a3:8e:db:01:b2 Unclassified Alert                2    0       00:27:e3:36:4d:a0 -28    40
00:27:e3:36:4d:a0 -37    40
50:2f:a8:a2:0a:60 Malicious    Threat               1    2       00:27:e3:36:4d:a0 -66    1
50:2f:a8:a2:0d:40 Unclassified Alert                1    0       00:27:e3:36:4d:a0 -65    11
```

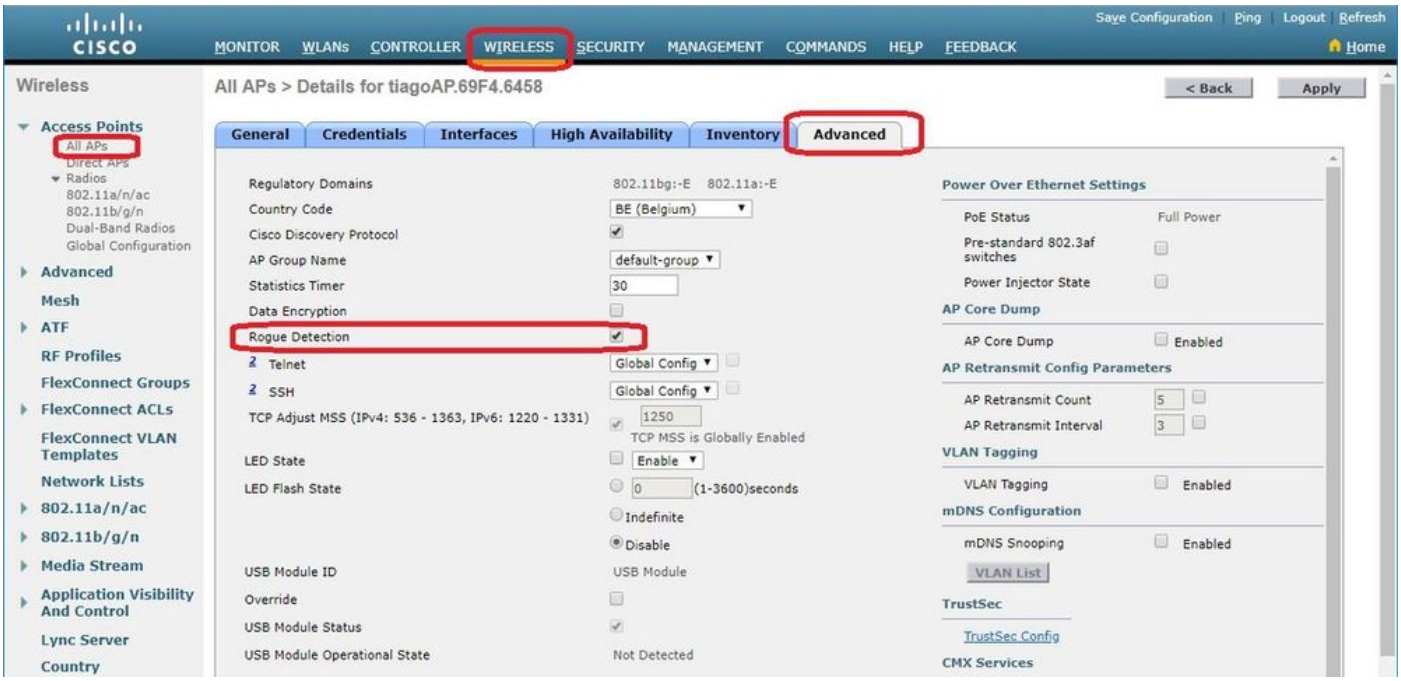
```
9c:97:26:61:d2:79 Unclassified Alert                1    0       00:27:e3:36:4d:a0 -89    6
ac:22:05:ea:21:26 Unclassified Alert                1    0       00:27:e3:36:4d:a0 -89    (1,5)
c4:e9:84:c1:c8:90 Unclassified Alert                1    0       00:27:e3:36:4d:a0 -89    (6,2)
d4:28:d5:da:e0:d4 Unclassified Alert                1    0       00:27:e3:36:4d:a0 -85    13
```

```
(Cisco Controller) >show rogue ap detailed 50:2f:a8:a2:0a:60

Rogue BSSID..................................... 50:2f:a8:a2:0a:60
Is Rogue on Wired Network....................... Yes
Classification.................................. Malicious
Classification change by........................ Auto
Manual Contained................................ No
State........................................... Threat
State change by................................. Auto
First Time Rogue was Reported................... Tue Jun  4 13:06:55 2019
Last Time Rogue was Reported.................... Wed Jun  5 08:25:57 2019
Reported By
    AP 1
        MAC Address............................. 00:27:e3:36:4d:a0
        Name.................................... tiagoAPcb.98E1.3DEC
        Radio Type.............................. 802.11n2.4G
        SSID.................................... buterfly
        Channel................................. 1
        RSSI.................................... -64 dBm
        SNR..................................... 29 dB
        Security Policy......................... WPA2/FT
        ShortPreamble........................... Disabled
        Last reported by this AP................ Wed Jun  5 08:25:57 2019
```

Troubleshoot

Se O Invasor Não For Detectado

Verifique se a detecção de invasor está habilitada no AP. Na GUI:



Na CLI:

```
(Cisco Controller) >show ap config general tiagoAPcb.98E1.3DEC

Cisco AP Identifier.............................. 13
Cisco AP Name.................................... tiagoAPcb.98E1.3DEC
[...]
Administrative State ............................ ADMIN_ENABLED
Operation State ................................. REGISTERED
Mirroring Mode .................................. Disabled
AP Mode ......................................... Local
Public Safety ................................... Disabled
AP SubMode ...................................... Not Configured
Rogue Detection ................................. Enabled
Remote AP Debug ................................. Disabled
Logging trap severity level ..................... informational
KPI not configured .............................
Logging syslog facility ......................... kern
S/W  Version .................................... 8.8.120.0
Boot  Version ................................... 1.1.2.4
[...]
Power Type/Mode.................................. PoE/Full Power
Number Of Slots.................................. 3
AP Model......................................... AIR-AP3802I-I-K9
AP Image......................................... AP3G3-K9W8-M
Cisco IOS Version..................................... 8.8.120.0
Reset Button..................................... Enabled
AP Serial Number................................. FGL2114A4SU
[...]
```

A detecção de invasor pode ser habilitada em um AP com este comando:

```
(Cisco Controller) >config rogue detection enable ?
all            Applies the configuration to all connected APs.
<Cisco AP>     Enter the name of the Cisco AP.
```

Um AP no modo local verifica apenas canais do país/canais de DCA e depende da configuração. Se o invasor estiver em qualquer outro canal, a controladora não poderá identificar o invasor se você não tiver APs no modo de monitor na rede. Execute esse comando para verificar:

```
(Cisco Controller) >show advanced 802.11a monitor

Default 802.11a AP monitoring
  802.11a Monitor Mode........................... enable
  802.11a Monitor Mode for Mesh AP Backhaul...... disable
  802.11a Monitor Channels....................... Country channels
  802.11a RRM Neighbor Discover Type............. Transparent
  802.11a RRM Neighbor RSSI Normalization........ Enabled
  802.11a AP Coverage Interval................... 90 seconds
  802.11a AP Load Interval....................... 60 seconds
  802.11a AP Monitor Measurement Interval........ 180 seconds
  802.11a AP Neighbor Timeout Factor............. 20
  802.11a AP Report Measurement Interval......... 180 seconds
```

- O AP invasor não transmite o SSID.
- Certifique-se de que o endereço MAC do AP não seja adicionado à lista de invasores amigáveis ou permitido listado através do PI.
- Os beacons do AP não são alcançáveis para o AP que detectou invasores. Isso pode ser verificado pela captura dos pacotes com um sniffer próximo ao invasor do detector de AP.

- Um AP de modo local pode levar até 9 minutos para detectar um invasor (3 ciclos 180x3).
- Os APs Cisco não são capazes de detectar invasores em frequências como o canal de segurança pública (4,9 Ghz).
- Os APs Cisco não são capazes de detectar invasores que funcionam no FHSS (Frequency Hopping Spread Spectrum, Espectro espalhado com salto de frequência).

Debugs úteis

```
(Cisco Controller) >debug client
```

```
        (If rogue mac is known)
(Cisco Controller) >debug client 50:2f:a8:a2:0a:60

(Cisco Controller) >*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Found Rogue AP:
50:2f:a8:a2:0a:60 on slot 0

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 New RSSI report from AP
00:27:e3:36:4d:a0  rssi -55, snr 39 wepMode 81 wpaMode 86, detectinglradtypes :20
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue SSID timestmap set to 1559724417.
Detecting lrad: 00:27:e3:36:4d:a0
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60  SYNC for Channel (new/old : 1/0) or
channel width (new/old :0/0) change detected on  Detecting lrad: 00:27:e3:36:4d:a0
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 rg changed rssi prev -64, new -55
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Updated AP report 00:27:e3:36:4d:a0
rssi -55, snr 39
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue detected by AP: 00:27:e3:36:4d:a0
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 RadioType: 3 lradInfo->containSlotId = 2
ReceiveSlotId = 0 ReceiveBandId = 0

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue before Rule Classification : Class
malicious, Change by Auto State Threat Change by Auto

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue doesnt qualify for rule
classification : Class malicious, Change by Auto State Threat Change by Auto

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Manual Contained Flag = 0, trustlevel =
7

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 ssidLen = 8 min = 8 50:2f:a8:a2:0a:60

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 This rogue does not use my ssid. Rogue
ssid=buterfly

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60  Rogue AP: 50:2f:a8:a2:0a:60 autocontain
= 2 Mode = 7

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Checking Impersonation source
50:2f:a8:a2:0a:60 detected by 00:27:e3:36:4d:a0, FailCnt 0, mode 7, apAuthEnabled on mac 0,
ptype 318505456 mfp_supported 1
*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Known AP 0 mfp global 0 AP Auth Global 0
mfp Impersonation 0 ids flags 2

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue Client ssid: buterfly

*apfRogueTask_2: Jun 05 08:46:57.111: 50:2f:a8:a2:0a:60 Rogue Client ssid: buterfly
```

(Cisco Controller) >**debug dot11 rogue enable**

(Cisco Controller) >*emWeb: Jun 05 08:39:46.828:
Debugging session started on Jun 05 08:39:46.828 for WLC AIR-CT3504-K9   Version :8.8.120.0 SN :FCW2245M09Y Hostname tiagoWLCcb
*iappSocketTask: Jun 05 08:39:57.104: 00:27:e3:36:4d:a0 Posting Rogue AP Iapp Report from AP for processing Payload version:c1, slot:0 , Total Entries:5, num entries this packet:5 Entry index :0, pakLen:285

*apfRogueTask_2: Jun 05 08:39:57.104: 00:27:e3:36:4d:a0 fakeAp check: slot=0, entryIndex=0, (Radio_upTime-now)=152838
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid b0:72:bf:93:e0:d7 src b0:72:bf:93:e0:d7 channel 1 rssi -59 ssid SMA1930072865
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid 50:2f:a8:a2:0a:60 src 50:2f:a8:a2:0a:60 channel 1 rssi -63 ssid buterfly
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid 00:a3:8e:db:01:a1 src 00:a3:8e:db:01:a1 channel 13 rssi -16 ssid
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid 00:a3:8e:db:01:b0 src a4:c3:f0:cf:db:18 channel 40 rssi -26 ssid blizzard
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 New RSSI report from AP 00:27:e3:36:4d:a0 rssi -28, snr 61 wepMode 81 wpaMode 82, detectinglradtypes :30
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 entries 5 slotId 0 bssid 00:a3:8e:db:01:b2 src 00:a3:8e:db:01:b2 channel 40 rssi -28 ssid
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Found Rogue AP: 00:a3:8e:db:01:a1 on slot 0

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue SSID timestmap expired. last update at 0 Detecting lrad: 00:27:e3:36:4d:a0
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 fakeAp check: knownApCount=0, totalNumOfRogueEntries=5, #entriesThisPkt=5, #totalEntries=5
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 New RSSI report from AP 00:27:e3:36:4d:a0 rssi -16, snr 76 wepMode 81 wpaMode 82, detectinglradtypes :28
*apfRogueTask_2: Jun 05 08:39:57.105: 00:27:e3:36:4d:a0 fakeAp check: avgNumOfRogues[0]/10=4, rogueAlarmInitiated[0]=0
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 SYNC for Channel (new/old : 40/0) or channel width (new/old :0/0) change detected on Detecting lrad: 00:27:e3:36:4d:a0
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue SSID timestmap expired. last update at 0 Detecting lrad: 00:27:e3:36:4d:a0
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 rg changed rssi prev -28, new -28
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 SYNC for Channel (new/old : 13/0) or channel width (new/old :0/0) change detected on Detecting lrad: 00:27:e3:36:4d:a0
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Updated AP report 00:27:e3:36:4d:a0 rssi -28, snr 61
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Updated AP report 00:27:e3:36:4d:a0 rssi -16, snr 76
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 RadioType: 3 lradInfo->containSlotId = 1 ReceiveSlotId = 0 ReceiveBandId = 1

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue before Rule Classification : Class unclassified, Change by Default State Alert Change by Default

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Created rogue client table for Rogue AP at 0xfff0617238

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue is Rule candidate for : Class Change by Default State Change by Default

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Added Rogue AP: b0:72:bf:93:e0:d7

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Applying Rogue rule to this MAC

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Looking for Rogue b0:72:bf:93:e0:d7 in

known AP table
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue AP b0:72:bf:93:e0:d7 is not found either in AP list or neighbor, known or Mobility group AP lists
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue After Rule Classification : Class unclassified, Change by Default State Alert Change by Default

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Manual Contained Flag = 0, trustlevel = 2

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Scheduled pending Time 184 and expiry time 1200 for rogue AP b0:72:bf:93:e0:d7
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 ssidLen = 0 min = 0 00:a3:8e:db:01:b2

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Change state from 0 to 1 for rogue AP b0:72:bf:93:e0:d7
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 This rogue does not use my ssid. Rogue ssid=

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rg change state Rogue AP: b0:72:bf:93:e0:d7

*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Rogue AP: 00:a3:8e:db:01:b2 autocontain = 2 Mode = 2

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue detected by AP: 00:27:e3:36:4d:a0
*apfRogueTask_1: Jun 05 08:39:57.105: 00:a3:8e:db:01:b2 Checking Impersonation source 00:a3:8e:db:01:b2 detected by 00:27:e3:36:4d:a0, FailCnt 0, mode 2, apAuthEnabled on mac 0, ptype -155740480 mfp_supported 1
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 RadioType: 3 lradInfo->containSlotId = 2 ReceiveSlotId = 0 ReceiveBandId = 0

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 New RSSI report from AP 00:27:e3:36:4d:a0 rssi -59, snr 36 wepMode 81 wpaMode 83, detectinglradtypes :20
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue is Rule candidate for : Class Change by Default State Change by Default

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Send Rogue Info Notificaiton for AP report 00:27:e3:36:4d:a0 Rogue ssid change from   to SMA1930072865
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Applying Rogue rule to this MAC

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue SSID timestmap set to 1559723997. Detecting lrad: 00:27:e3:36:4d:a0
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rg send new rssi -59
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Rogue After Rule Classification : Class unclassified, Change by Default State Alert Change by Default

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Updated AP report 00:27:e3:36:4d:a0 rssi -59, snr 36
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Manual Contained Flag = 0, trustlevel = 2

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue detected by AP: 00:27:e3:36:4d:a0
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 ssidLen = 0 min = 0 00:a3:8e:db:01:a1

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 RadioType: 3 lradInfo->containSlotId = 2 ReceiveSlotId = 0 ReceiveBandId = 0

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 This rogue does not use my ssid. Rogue ssid=

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue before Rule Classification : Class unconfigured, Change by Default State Pending Change by Default

```
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1  Rogue AP: 00:a3:8e:db:01:a1 autocontain
= 2 Mode = 2

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue state is pending or lrad, cannot
apply rogue rule

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue doesnt qualify for rule
classification : Class unconfigured, Change by Default State Pending Change by Default

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Checking Impersonation source
00:a3:8e:db:01:a1 detected by 00:27:e3:36:4d:a0, FailCnt 0, mode 2, apAuthEnabled on mac 0,
ptype -155740480 mfp_supported 1
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Manual Contained Flag = 0, trustlevel =
1

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:a1 Known AP 0 mfp global 0 AP Auth Global 0
mfp Impersonation 0 ids flags 6

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Checking Impersonation source
b0:72:bf:93:e0:d7 detected by 00:27:e3:36:4d:a0, FailCnt 0, mode 1, apAuthEnabled on mac 0,
ptype 318505456 mfp_supported 1
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Known AP 0 mfp global 0 AP Auth Global 0
mfp Impersonation 0 ids flags 2

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Found Rogue AP: 00:a3:8e:db:01:b0 on
slot 0

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rg new Rogue AP: b0:72:bf:93:e0:d7

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 New RSSI report from AP
00:27:e3:36:4d:a0  rssi -26, snr 61 wepMode 81 wpaMode 82, detectinglradtypes :32
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Rogue SSID timestmap set to 1559723997.
Detecting lrad: 00:27:e3:36:4d:a0
*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 New RSSI report from AP
00:27:e3:36:4d:a0  rssi -63, snr 5 wepMode 81 wpaMode 86, detectinglradtypes :20
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0  SYNC for Channel (new/old : 40/0) or
channel width (new/old :0/0) change detected on  Detecting lrad: 00:27:e3:36:4d:a0
*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue SSID timestmap set to 1559723997.
Detecting lrad: 00:27:e3:36:4d:a0
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 rg changed rssi prev -28, new -26
*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60  SYNC for Channel (new/old : 1/0) or
channel width (new/old :0/0) change detected on  Detecting lrad: 00:27:e3:36:4d:a0
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Updated AP report 00:27:e3:36:4d:a0
rssi -26, snr 61
*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 rg changed rssi prev -65, new -63
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Rogue detected by AP: 00:27:e3:36:4d:a0
*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Updated AP report 00:27:e3:36:4d:a0
rssi -63, snr 5
*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 RadioType: 3 lradInfo->containSlotId = 1
ReceiveSlotId = 0 ReceiveBandId = 1

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue detected by AP: 00:27:e3:36:4d:a0
*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 RadioType: 3 lradInfo->containSlotId = 2
ReceiveSlotId = 0 ReceiveBandId = 0

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Manual Contained Flag = 0, trustlevel =
7

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue before Rule Classification : Class
malicious, Change by Auto State Threat Change by Auto

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 ssidLen = 8 min = 8 00:a3:8e:db:01:b0

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Manual Contained Flag = 0, trustlevel =
```

7

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 This rogue does not use my ssid. Rogue ssid=blizzard

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 ssidLen = 8 min = 8 50:2f:a8:a2:0a:60

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Rogue AP: 00:a3:8e:db:01:b0 autocontain = 2 Mode = 7

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 This rogue does not use my ssid. Rogue ssid=buterfly

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue AP: 50:2f:a8:a2:0a:60 autocontain = 2 Mode = 7

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Known AP 0 mfp global 0 AP Auth Global 0 mfp Impersonation 0 ids flags 2

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Checking Impersonation source 50:2f:a8:a2:0a:60 detected by 00:27:e3:36:4d:a0, FailCnt 0, mode 7, apAuthEnabled on mac 0, ptype 318505456 mfp_supported 1
*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Known AP 0 mfp global 0 AP Auth Global 0 mfp Impersonation 0 ids flags 2

*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 APF processing Rogue Client: on slot 0

*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 Rogue Client IPv6 addr: Not known

*apfRogueTask_2: Jun 05 08:39:57.105: b4:82:fe:54:b3:14 APF processing Rogue Client: on slot 0

*apfRogueTask_3: Jun 05 08:39:57.105: 00:a3:8e:db:01:b0 Rogue Client ssid: blizzard

*apfRogueTask_2: Jun 05 08:39:57.105: b4:82:fe:54:b3:14 Rogue Client IPv6 addr: Not known

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue Client ssid: buterfly

*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 New AP report 00:27:e3:36:4d:a0 rssi -37, snr 50
*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 rgc change from -38 RSSI -37
*apfRogueTask_2: Jun 05 08:39:57.105: b4:82:fe:54:b3:14 rgc change from -39 RSSI -39
*apfRogueTask_3: Jun 05 08:39:57.105: a4:c3:f0:cf:db:18 Updated AP report 00:27:e3:36:4d:a0 rssi -37, snr 50
*apfRogueTask_2: Jun 05 08:39:57.105: b4:82:fe:54:b3:14 Updated AP report 00:27:e3:36:4d:a0 rssi -39, snr 43
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 APF processing Rogue Client: on slot 0

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue Client IPv6 addr: Not known

*apfRogueTask_2: Jun 05 08:39:57.105: 50:2f:a8:a2:0a:60 Rogue Client ssid: buterfly

*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 New AP report 00:27:e3:36:4d:a0 rssi -62, snr 32
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rgc change from -61 RSSI -62
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Updated AP report 00:27:e3:36:4d:a0 rssi -62, snr 32
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Looking for Rogue b0:72:bf:93:e0:d7 in known AP table
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Rogue AP b0:72:bf:93:e0:d7 is not found either in AP list or neighbor, known or Mobility group AP lists
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 Change state from 1 to 2 for rogue AP b0:72:bf:93:e0:d7
*apfRogueTask_2: Jun 05 08:39:57.105: b0:72:bf:93:e0:d7 rg change state Rogue AP: b0:72:bf:93:e0:d7

```
*apfRogueTask_2: Jun 05 08:39:57.106: b0:72:bf:93:e0:d7 rg change state Rogue AP:
b0:72:bf:93:e0:d7

*apfRogueTask_2: Jun 05 08:39:57.106: b0:72:bf:93:e0:d7 Deleting Rogue AP: b0:72:bf:93:e0:d7

*apfRogueTask_2: Jun 05 08:39:57.106: b0:72:bf:93:e0:d7 Freed rogue client table for Rogue AP at
0xfff0617238

*apfRogueTask_2: Jun 05 08:39:57.106: b0:72:bf:93:e0:d7 rg delete for Rogue AP:
b0:72:bf:93:e0:d7
```

Logs de interceptações esperados

Quando um invasor é detectado/removido da lista de invasores:

0	Qua Jun 5 09:01:57 2019	Cliente invasor: b4:c0:f5:2b:4f:90 é **detectado** por 1 APs Rogue Client Bssid: a6:b1:e9:f0:e Estado: Alerta, Último AP detectável :00:27:e3:36:4d:a0 Rogue Client gateway mac 00:00:00:02:02:02.
1	Qua Jun 5 09:00:39 2019	AP invasor: 9c:97:26:61:d2:79 **removido** do MAC do Rádio Base : 00:27:e3:36:4d:a0 Interf no:0(802.11n(2.4 GHz))
2	Qua Jun 5 08:53:39 2019	AP invasor: 7c:b7:33:c0:51:14 **removido** do MAC do Rádio Base : 00:27:e3:36:4d:a0 Interf no:0(802.11n(2.4 GHz))
3	Qua Jun 5 08:52:27 2019	Cliente invasor: fc:3f:7c:5f:b1:1b é **detectado** por 1 APs Rogue Client Bssid: 50:2f:a8:a2:0a Estado: Alerta, Último AP detectável :00:27:e3:36:4d:a0 Rogue Client gateway mac 00:26:44:73:c5:1d.
4	Qua Jun 5 08:52:17 2019	AP invasor: d4:28:d5:da:e0:d4 **removido** do MAC de Rádio Base : 00:27:e3:36:4d:a0 Interf no:0(802.11n(2.4 GHz))

Recomendações

1. Configure a verificação de canal para todos os canais se você suspeitar de possíveis invasores na rede.
2. O número e a localização de APs de detectores invasores podem variar de um por andar a um por prédio e depende do layout da rede com fio. É aconselhável ter pelo menos um AP detector invasor em cada andar de um prédio. Como um AP detector invasor exige um tronco para todos os domínios de broadcast de rede da camada 2 que devem ser monitorados, a colocação depende do layout lógico da rede.

Se o invasor não estiver classificado

Verifique se as regras não autorizadas estão configuradas corretamente.

Debugs úteis

```
(Cisco Controller) >debug dot11 rogue rule enable
```

```
(Cisco Controller) >*emWeb: Jun 05 09:12:27.095:
Debugging session started on Jun 05 09:12:27.095 for WLC AIR-CT3504-K9 Version :8.8.120.0 SN
:FCW2245M09Y Hostname tiagoWLCcb

(Cisco Controller) >
*apfRogueTask_1: Jun 05 09:12:57.135: 00:a3:8e:db:01:a0 Rogue Rule Classify Params: rssi=-16,
maxRssiLrad = 00:27:e3:36:4d:a0 ,client=0, duration=154623, wep=1, ssid=blizzard slotId = 0
channel = 13 snr = 76 dot11physupport =
*apfRogueTask_3: Jun 05 09:12:57.135: 00:a3:8e:db:01:a1 Rogue Rule Classify Params: rssi=-15,
maxRssiLrad = 00:27:e3:36:4d:a0 ,client=0, duration=154683, wep=1, ssid= slotId = 0 channel = 13
snr = 77 dot11physupport = 3

*apfRogueTask_1: Jun 05 09:12:57.135: ac:22:05:ea:21:26 Rogue Rule Classify Params: rssi=-89,
maxRssiLrad = 00:27:e3:36:4d:a0 ,client=0, duration=5790, wep=1, ssid=NOWO-A2121 slotId = 0
channel = 1 snr = 4 dot11physupport = 3

*apfRogueTask_1: Jun 05 09:13:27.135: ac:22:05:ea:21:26 Rogue Rule Classify Params: rssi=-89,
maxRssiLrad = 00:27:e3:36:4d:a0 ,client=0, duration=5820, wep=1, ssid=NOWO-A2121 slotId = 0
channel = 1 snr = 4 dot11physupport = 3
*apfRogueTask_3: Jun 05 09:13:27.135: 50:2f:a8:a2:0d:40 Rogue Rule Classify Params: rssi=-62,
maxRssiLrad = 00:27:e3:36:4d:a0 ,client=0, duration=154353, wep=1, ssid=buterfly slotId = 0
channel = 11 snr = 30 dot11physupport =
*apfRogueTask_3: Jun 05 09:13:27.135: 50:2f:a8:a2:0d:40 Rogue Classification:malicious,
RuleName:TestRule, Rogue State:Containment Pending

*apfRogueTask_3: Jun 05 09:13:27.136: 00:a3:8e:db:01:a1 Rogue Rule Classify Params: rssi=-15,
maxRssiLrad = 00:27:e3:36:4d:a0 ,client=0, duration=154713, wep=1, ssid= slotId = 0 channel = 13
snr = 77 dot11physupport = 3

*apfRogueTask_1: Jun 05 09:13:57.136: 00:a3:8e:db:01:a0 Rogue Rule Classify Params: rssi=-16,
maxRssiLrad = 00:27:e3:36:4d:a0 ,client=0, duration=154683, wep=1, ssid=blizzard slotId = 0
channel = 13 snr = 76 dot11physupport =
*apfRogueTask_3: Jun 05 09:13:57.136: 50:2f:a8:a2:0d:40 Rogue Classification:malicious,
RuleName:TestRule, Rogue State:Containment Pending

*apfRogueTask_3: Jun 05 09:13:57.136: 00:a3:8e:db:01:a1 Rogue Rule Classify Params: rssi=-15,
maxRssiLrad = 00:27:e3:36:4d:a0 ,client=0, duration=154743, wep=1, ssid= slotId = 0 channel = 13
snr = 77 dot11physupport = 3
```

Recomendações

Se você tiver entradas invasoras conhecidas, adicione-as à lista amigável ou habilite a validação com AAA e verifique se as entradas conhecidas do cliente estão no banco de dados de Autenticação, Autorização e Contabilização (AAA).

O RLDP não localiza invasores

- Se o invasor estiver no canal DFS, o RLDP não funcionará.
- O RLDP funciona apenas se a WLAN invasora estiver aberta e o DHCP estiver disponível.
- Se o AP do modo local serve ao cliente no canal DFS, ele não participa do processo RLDP.
- O RLDP não é suportado nos APs das séries 1800i, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800 e 3800.

Debugs úteis

```
(Cisco Controller) >debug dot11 rldp enable

!--- RLDP not available when AP used to contain only has invalid channel for the AP country code
```

*apfRLDP: Jun 05 12:24:41.291: 50:2f:a8:a2:0a:61 Received request to detect Rogue
*apfRLDP: Jun 05 12:24:41.291: 50:2f:a8:a2:0a:61 Entering apfFindClosestLrad
*apfRLDP: Jun 05 12:24:41.292: Rogue detected slot :0 Rogue contains SlotId :2
*apfRLDP: Jun 05 12:24:41.292: 50:2f:a8:a2:0a:61 **Invalid channel 1 for the country IL for AP 00:27:e3:36:4d:a0**
*apfRLDP: Jun 05 12:24:41.292: 50:2f:a8:a2:0a:61 Cannot find any AP to perform RLDP operation
*apfRLDP: Jun 05 12:24:41.292: 50:2f:a8:a2:0a:61 Exiting apfFindClosestLrad
*apfRLDP: Jun 05 12:24:41.292: Waiting for ARLDP request

!--- ROGUE detected on DFS channel

*apfRLDP: Jun 05 12:43:16.659: 50:2f:a8:a2:0d:4e Received request to detect Rogue
*apfRLDP: Jun 05 12:43:16.659: 50:2f:a8:a2:0d:4e Entering apfFindClosestLrad
*apfRLDP: Jun 05 12:43:16.660: Rogue detected slot :1 Rogue contains SlotId :1
*apfRLDP: Jun 05 12:43:16.660: 50:2f:a8:a2:0d:4e **Our AP 00:27:e3:36:4d:a0 detected this rogue on a DFS Channel 100**
*apfRLDP: Jun 05 12:43:16.660: 50:2f:a8:a2:0d:4e Cannot find any AP to perform RLDP operation
*apfRLDP: Jun 05 12:43:16.660: 50:2f:a8:a2:0d:4e Exiting apfFindClosestLrad
*apfRLDP: Jun 05 12:43:16.660: Waiting for ARLDP request

!--- RLDP is not supported on AP model 1800i, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800, and 3800 Series APs

*apfRLDP: Jun 05 12:52:41.980: 9e:97:26:a2:a1:1a Received request to detect Rogue
*apfRLDP: Jun 05 12:52:41.980: 9e:97:26:a2:a1:1a Entering apfFindClosestLrad
*apfRLDP: Jun 05 12:52:41.980: 9e:97:26:a2:a1:1a **Skipping RLDP on AP 94:d4:69:f5:f7:e0 AP Model: AIR-AP1852I-E-K9**
*apfRLDP: Jun 05 12:52:41.980: 9e:97:26:a2:a1:1a Cannot find any AP to perform RLDP operation
*apfRLDP: Jun 05 12:52:41.980: 9e:97:26:a2:a1:1a Exiting apfFindClosestLrad
*apfRLDP: Jun 05 12:52:41.980: Waiting for ARLDP request

!--- Association TO ROGUE AP
*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 Received request to detect Rogue *apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 Entering apfFindClosestLrad *apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 Skipping RLDP on AP 94:d4:69:f5:f7:e0 AP Model: AIR-AP1852I-E-K9 *apfRLDP: Jun 05 15:02:49.602: Rogue detected slot :0 Rogue contains SlotId :0 *apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 **Monitor Mode AP found b4:de:31:a4:e0:30 with RSSI -61**
*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 found closest monitor AP b4:de:31:a4:e0:30 slot = 0, channel = 1

*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 Exiting apfFindClosestLrad
*apfRLDP: Jun 05 15:02:49.602: 50:2f:a8:a2:0a:61 Found RAD: 0xffd682b5b8, slotId = 0, Type=1

*apfRLDP: Jun 05 15:02:50.102: 50:2f:a8:a2:0a:61 AP b4:de:31:a4:e0:30 Client b4:de:31:a4:e0:31 Slot = 0
*apfRLDP: Jun 05 15:02:50.102: 50:2f:a8:a2:0a:61 WARNING!!!!! mscb already exists!

*apfRLDP: Jun 05 15:02:50.102: b4:de:31:a4:e0:31 In rldpSendAddMobile:724 setting Central switched to TRUE
*apfRLDP: Jun 05 15:02:50.302: 50:2f:a8:a2:0a:61 **rldp started association, attempt 1**
*apfRLDP: Jun 05 15:02:55.346: 50:2f:a8:a2:0a:61 RLDP could not finish the association in time. RLDP State(2)

*apfRLDP: Jun 05 15:02:55.346: 50:2f:a8:a2:0a:61 rldp started association, attempt 2
*apfRLDP: Jun 05 15:03:00.390: 50:2f:a8:a2:0a:61 RLDP could not finish the association in time. RLDP State(2)

*apfRLDP: Jun 05 15:03:00.390: 50:2f:a8:a2:0a:61 rldp started association, attempt 3
*apfOpenDtlSocket: Jun 05 15:03:00.608: apfRoguePreamble = 0 mobile b4:de:31:a4:e0:31.
*apfOpenDtlSocket: Jun 05 15:03:00.808: **50:2f:a8:a2:0a:61 RLDP state RLDP_ASSOC_DONE** (3).

*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61 **Successfully associated with rogue: 50:2F:A8:A2:0A:61**

```
!--- Attempt to get ip from ROGUE

*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61 Starting dhcp
*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61 Initializing RLDP DHCP for rogue
50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61 RLDP DHCPSTATE_INIT for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31 BOOTP[rldp] op: REQUEST

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31       htype: Ethernet

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31        hlen: 6

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31        hops: 1

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31         xid: 0x3da1f13

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31        secs: 0

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31       flags: 0x0

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31       hw_addr: B4:DE:31:A4:E0:31

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31     client IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31         my IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31     server IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31    gateway IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31   options:

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31        DHCP message: 1 DISCOVER

*apfRLDP: Jun 05 15:03:00.870: DHCP option: 39/57.2: (2)

*apfRLDP: Jun 05 15:03:00.870:      [0000] 02 40

*apfRLDP: Jun 05 15:03:00.870: b4:de:31:a4:e0:31          host name: RLDP

*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61 Sending DHCP packet through rogue AP
50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:00.870: 50:2f:a8:a2:0a:61 RLDP DHCP SELECTING for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:10.877: 50:2f:a8:a2:0a:61 Initializing RLDP DHCP for rogue
50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:10.877: 50:2f:a8:a2:0a:61 RLDP DHCPSTATE_INIT for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31 BOOTP[rldp] op: REQUEST

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31       htype: Ethernet

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31        hlen: 6

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31        hops: 1

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31         xid: 0x3da1f13

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31        secs: 0

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31       flags: 0x0

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31       hw_addr: B4:DE:31:A4:E0:31

*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31     client IP: 0.0.0.0
```

```
*apfRLDP: Jun 05 15:03:10.877: b4:de:31:a4:e0:31          my IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31      server IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31     gateway IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31   options:

*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31         DHCP message: 1 DISCOVER

*apfRLDP: Jun 05 15:03:10.878: DHCP option: 39/57.2: (2)

*apfRLDP: Jun 05 15:03:10.878:      [0000] 02 40

*apfRLDP: Jun 05 15:03:10.878: b4:de:31:a4:e0:31           host name: RLDP

*apfRLDP: Jun 05 15:03:10.878: 50:2f:a8:a2:0a:61 Sending DHCP packet through rogue AP
50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:10.878: 50:2f:a8:a2:0a:61 RLDP DHCP SELECTING for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:20.885: 50:2f:a8:a2:0a:61 Initializing RLDP DHCP for rogue
50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:20.885: 50:2f:a8:a2:0a:61 RLDP DHCPSTATE_INIT for rogue 50:2f:a8:a2:0a:61
*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31 BOOTP[rldp] op: REQUEST

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31        htype: Ethernet

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31         hlen: 6

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31         hops: 1

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31          xid: 0x3da1f13

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31         secs: 0

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31        flags: 0x0

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31        hw_addr: B4:DE:31:A4:E0:31

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31      client IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31          my IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31      server IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31     gateway IP: 0.0.0.0

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31   options:

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31         DHCP message: 1 DISCOVER

*apfRLDP: Jun 05 15:03:20.885: DHCP option: 39/57.2: (2)

*apfRLDP: Jun 05 15:03:20.885:      [0000] 02 40

*apfRLDP: Jun 05 15:03:20.885: b4:de:31:a4:e0:31           host name: RLDP

*apfRLDP: Jun 05 15:03:20.885: 50:2f:a8:a2:0a:61 Sending DHCP packet through rogue AP
50:2f:a8:a2:0a:61

!--- RLDP DHCP fails as there is no DHCP server providing IP address
*apfRLDP: Jun 05 15:03:20.885: 50:2f:a8:a2:0a:61 RLDP DHCP FAILED state for rogue
50:2f:a8:a2:0a:61 *apfRLDP: Jun 05 15:03:20.885: 50:2f:a8:a2:0a:61 DHCP failed *apfRLDP: Jun 05
15:03:20.885: Waiting for ARLDP request
```

Recomendações

1. Inicie o RLDP manualmente em entradas invasoras suspeitas.
2. Programe o RLDP periodicamente.
3. O RLDP pode ser implantado em APs no modo local ou de monitor. Para implantações mais escaláveis e para eliminar qualquer impacto no serviço do cliente, o RLDP deve ser implantado em APs no modo de monitor quando possível. No entanto, essa recomendação requer que uma sobreposição de AP no modo de monitor seja implantada com uma proporção típica de 1 AP no modo de monitor para cada 5 APs no modo local. Os APs no modo de monitor wIPS adaptativo também podem ser utilizados para essa tarefa.

Rogue Detector AP

A entrada de invasor em um detector de invasor pode ser vista com esse comando no console do AP. Para invasores com fio, o sinalizador se move para definir o status.

```
tiagoAP.6d09.eff0#show capwap rm rogue detector
 LWAPP Rogue Detector Mode
  Current Rogue Table:
  Rogue hindex = 0: MAC 502f.a8a2.0a61, flag = 0, unusedCount = 1
  Rogue hindex = 0: MAC 502f.a8a2.0a60, flag = 0, unusedCount = 1
  Rogue hindex = 7: MAC 502f.a8a2.0d41, flag = 0, unusedCount = 1
  Rogue hindex = 7: MAC 502f.a8a2.0d40, flag = 0, unusedCount = 1

!--- once rogue is detected on wire, the flag is set to 1
```

Comandos de depuração úteis em um console AP

```
Rogue_Detector#debug capwap rm rogue detector

*Jun 05 08:37:59.747: ROGUE_DET: Received a rogue table update of length 170
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1ac4
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1ac5
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1aca
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acb
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acc
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acd
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acf
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0024.1431.e9ef
*Jun 05 08:37:59.747: ROGUE_DET: Got wired mac 0024.148a.ca2b
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.148a.ca2d
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.148a.ca2f
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.3570
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.3574
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.357b
*Jun 05 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.357c
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.357d
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.357f
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3dcd
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3ff0
*Jun 05 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3ff2
*Jun 05 08:37:59.774: ROGUE_DET: Got wired mac 0040.96b9.4aec
*Jun 05 08:37:59.774: ROGUE_DET: Got wired mac 0040.96b9.4b77
*Jun 05 08:37:59.774: ROGUE_DET: Flushing rogue entry 0040.96b9.4794
```

```
*Jun 05 08:37:59.774: ROGUE_DET: Flushing rogue entry 0022.0c97.af80
*Jun 05 08:37:59.775: ROGUE_DET: Flushing rogue entry 0024.9789.5710
*Jun 05 08:38:19.325: ROGUE_DET: Got ARP src 001d.a1cc.0e9e
*Jun 05 08:38:19.325: ROGUE_DET: Got wired mac 001d.a1cc.0e9e
*Jun 05 08:39:19.323: ROGUE_DET: Got ARP src 001d.a1cc.0e9e
*Jun 05 08:39:19.324: ROGUE_DET: Got wired mac 001d.a1cc.0e9e
```

Contenção de invasores

Depurações esperadas

```
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Updated AP report b4:de:31:a4:e0:30 rssi
-33, snr 59
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Looking for Rogue 00:a3:8e:db:01:b0 in
known AP table
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue AP 00:a3:8e:db:01:b0 is not found
either in AP list or neighbor, known or Mobility group AP lists
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue in same state as before : 6
ContainmentLevel : 4 level 4

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue detected by AP: b4:de:31:a4:e0:30
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 RadioType: 2 lradInfo->containSlotId = 1
ReceiveSlotId = 1 ReceiveBandId = 1

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue before Rule Classification : Class
malicious, Change by Auto State Contained Change by Auto

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue doesnt qualify for rule
classification : Class malicious, Change by Auto State Contained Change by Auto

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Manual Contained Flag = 0, trustlevel =
6

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue AP: 00:a3:8e:db:01:b0 autocontain
= 1 Mode = 6

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 apfRogueMode : 6
apfRogueContainmentLevel : 4 lineNumber : 8225 apfRogueManualContained : 0 function :
apfUpdateRogueContainmentState

*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Trying Containment on 1 band for rogue
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Skipping xor radio for 1 band and cont
slotid 1
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Found 0 channels to try containment for
rogue
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Trying Containment on 2 band for rogue
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue detected on detected slot 0
contains slot 1 for detecting lrad 00:27:e3:36:4d:a0.
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Found 1 channels to try containment for
rogue
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 RSSI SORTED AP MAC 00:27:e3:36:4d:a0
RSSI = -28
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 RSSI SORTED AP MAC 00:27:e3:36:4d:a0
RSSI = -31
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 RSSI SORTED AP MAC b4:de:31:a4:e0:30
RSSI = -33
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Detecting AP MAC 00:27:e3:36:4d:a0 RSSI
= -28 totClientsDetected = 2
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Detecting AP MAC 00:27:e3:36:4d:a0 RSSI
= -31 totClientsDetected = 2
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Detecting AP MAC b4:de:31:a4:e0:30 RSSI
= -33 totClientsDetected = 1
```

```
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue already contained by AP
00:27:e3:36:4d:a0. Containment mode 1
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue already contained by AP
00:27:e3:36:4d:a0. Containment mode 1
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Rogue already contained by AP
b4:de:31:a4:e0:30. Containment mode 1
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Contains rogue with 3 container
AP(s).Requested containment level : 4
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Checking Impersonation source
00:a3:8e:db:01:b0 detected by b4:de:31:a4:e0:30, FailCnt 0, mode 6, apAuthEnabled on mac 0,
ptype 318505456 mfp_supported 1
*apfRogueTask_3: Jun 06 13:25:11.840: 00:a3:8e:db:01:b0 Known AP 0 mfp global 0 AP Auth Global 0
mfp Impersonation 0 ids flags 3
```

Recomendações

1. O AP do modo local/Flex-Connect pode conter 3 dispositivos por vez por rádio e o AP do modo de monitor pode conter 6 dispositivos por rádio. Como resultado, certifique-se de que o AP não contenha o número máximo de dispositivos permitidos. Neste cenário, o cliente está em um estado de contenção pendente.
2. Verifique as regras de contenção automática.

Conclusão

A detecção e contenção de invasores na solução de controlador centralizado da Cisco é o método mais eficaz e menos invasivo do setor. A flexibilidade fornecida ao administrador de rede permite uma adequação mais personalizada que pode acomodar qualquer requisito de rede.

Informações Relacionadas

- Guia de configuração do Cisco Wireless Controller Release 8.8 - Gerenciamento invasor
- Práticas recomendadas de configuração da controladora Wireless LAN (WLC) da Cisco
- Guia de implantação do WLC 3504 versão 8.5
- Guia de implantação do Cisco 5520 Wireless LAN Controller
- Notas de versão para Cisco Wireless Controllers e Lightweight Access Points, Cisco Wireless Versão 8.8.120.0

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.