Gerenciamento desonesto em uma rede Wireless unificada

Índice

Introdução

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. Consequentemente, um empregado que traga seu próprio Access point (Cisco ou não Cisco) em um Sem fio ou em uma infraestrutura ligada com fio bem-fixada e permita a acesso de usuários não autorizados a este de outra maneira a rede assegurada, pode facilmente comprometer uma rede segura.

A detecção desonesto permite que o administrador de rede monitore e elimine este interesse de segurança. Cisco unificou a arquitetura de rede fornece os métodos para a detecção desonesto que permitem uma solução desonesto completa da identificação e da retenção sem a necessidade para caro e duro-à-justificam redes e ferramentas de folha de prova.

Pré-requisitos

Requisitos

Este documento supõe que você é familiar com as configurações de controle básicas.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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

- Cisco unificou versão 7.0 running dos controladores (série de 2100, de 5500, 4400,WiSM, e NM-WLC)
- Controle e abastecimento do protocolo do ponto de acesso Wireless (CAPWAP) - regaços baseados - 1130AG, 1140, 3500, 1200, 1230AG, 1240AG, 1250, e regaços do 1260 Series

Convenções

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

Elimine as plantas pouco vigorozas a vista geral

Todo o dispositivo que compartilhar de seu espectro e não é controlado por você pode ser considerado um rogue. Um rogue torna-se perigoso nestas encenações:

- Quando setup para usar o mesmo SSID que sua rede (honeypot).
- Quando for detectado na rede ligada com fio igualmente.
- Os rogues ad hoc são igualmente uma ameaça grande.
- Setup por um estranho, a maioria de vezes, com intenção maliciosa.

Há três fases principal de Gerenciamento de dispositivo de rogue na solução da rede de Cisco Unified Wireless (UWN):

- Detecção – A varredura do Radio Resource Management (RRM) é usada para detectar a presença de dispositivos de rogue.
- Classificação – O protocolo de descoberta desonesto do lugar (RLDP), os detectores desonestos e o traçado da porta de switch estão usados para identificar se o dispositivo de rogue é conectado à rede ligada com fio. As regras desonestos da classificação igualmente ajudam em rogues de filtração nas categorias específicas baseadas em suas características.
- Mitigação – O fechamento da porta de switch, o lugar desonesto, e a retenção desonesto são usados em seguir para baixo seu local físico e para anular a ameaça do dispositivo de rogue.

Teoria da operação desonesto do Gerenciamento

Detecção desonesto

Um rogue é essencialmente todo o dispositivo que compartilhar de seu espectro, mas não está em seu controle. Isto inclui os Access point desonestos (AP), o roteador Wireless, os clientes do rogue, e redes ad-hoc desonestos. Cisco UWN usa um número de métodos para detectar dispositivos de rogue Wi-Fi-baseados incluir a exploração do fora-canal e capacidades dedicadas do modo de monitor. O Cisco Spectrum Expert pode igualmente ser usado para identificar os

dispositivos de rogue não baseados no protocolo do 802.11, tal como pontes de Bluetooth.

Exploração do Fora-canal

Esta operação é executada pelo modo local e pelo H−REAP (no modo conectado) AP e utiliza uma técnica decorte que permita a exploração do serviço de cliente e do canal usando o mesmo rádio. Indo fora canal por um período de 50ms cada 16 segundos, o AP, à revelia, gasta somente uma porcentagem pequena de seu tempo que não serve clientes. Também, note lá é um intervalo da mudança do canal 10ms que ocorra. No intervalo da varredura do padrão de 180 segundos, cada FCC 2.4Ghz canaliza (1−11) é feito a varredura pelo menos uma vez. Para outros domínios regulatório, tais como o ETSI, o AP estará fora do canal para uma porcentagem levemente mais alta do tempo. A lista de canais e de intervalo da varredura pode ser ajustada na configuração RRM. Isto limita o impacto no desempenho a um máximo de 1.5% e a inteligência está construída no algoritmo suspender a exploração quando os quadros prioritários de QoS, tais como a Voz, precisam de ser entregados.

Este gráfico é uma descrição do algoritmo da exploração do fora-canal para um modo local AP na banda de frequência 2.4GHz. Uma operação similar está sendo executada paralelamente no rádio 5GHz se o AP tem um presente. Cada quadrado vermelho representa o tempo passado no canal AP em casa, visto que cada quadrado azul representa a hora passada nos canais adjacentes para finalidades de varredura.

Varredura do modo de monitor

Esta operação é executada pelo modo de monitor e pelo modo de monitor adaptável AP do wIPS que utiliza 100% do momento do rádio para fazer a varredura de todos os canais em cada banda de frequência respectiva. Isto reserva uma velocidade maior da detecção e permite mais hora de ser gastado em cada canal individual. O modo de monitor AP é igualmente superior distante em detectar clientes desonestos porque têm mais visualização abrangente da atividade que ocorre em cada canal.

Este gráfico é uma descrição do algoritmo da exploração do fora-canal para um modo de monitor AP na banda de frequência 2.4GHz. Uma operação similar está sendo executada paralelamente no rádio 5GHz se o AP tem um presente.

Comparação do modo local e do modo de monitor

Um modo local AP racha seus ciclos entre clientes de WLAN do serviço e canais da exploração para ameaças. Em consequência, toma um modo local AP mais por muito tempo para dar um ciclo através de todos os canais, e passa menos tempo que recolhe dados em todo o canal particular de modo que as operações de cliente não sejam interrompidas. Consequentemente, o rogue e os tempos de detecção de ataque são mais longos (3 a 60 minutos) e uma escala menor sobre do - os ataques de ar podem ser detectados do que com um modo de monitor AP. Além disso, a detecção para o tráfego intermitente, tal como clientes desonestos, é muito menos determinística porque o AP tem que estar no canal do tráfego ao mesmo tempo que o tráfego está sendo transmitido ou recebido. Este transforma-se um exercício nas probabilidades. Um modo de monitor AP gasta tudo de seus ciclos que fazem a varredura dos canais que procuram rogues e sobre - os ataques de ar. Um modo de monitor AP pode simultaneamente ser usado para o wIPS adaptável, serviços (contexto-cientes) do lugar, e outros serviços do modo de monitor. Quando o modo de monitor AP é distribuído, os benefícios são uma mais baixa tempo-à-detecção. Quando o modo de monitor AP for configurado adicionalmente com wIPS adaptável, uma escala mais larga sobre do - as ameaças e os ataques de ar podem ser detectados.

Identificação desonesto

Se a resposta ou as balizas da ponta de prova de um dispositivo de rogue são ouvidas pelo modo local, pelo modo H-REAP, ou pelo modo de monitor AP, a seguir esta informação está comunicada através de CAPWAP ao controlador do Wireless LAN (WLC) para processar. A fim impedir falsos positivos, um número de métodos são usados para assegurar-se de que outros AP com base em Cisco controlados não estejam identificados como um dispositivo de rogue. Estes métodos incluem atualizações do grupo da mobilidade, pacotes vizinhos RF, e a lista branca AP autônomos através do sistema de controle wireless (WCS).

Registros desonestos

Quando o base de dados do controlador dos dispositivos de rogue contiver somente o grupo atual de rogues detectados, o WCS igualmente inclui uma história do evento e registra os rogues que são vistos já não.

Detalhes desonestos

UM CAPWAP AP vai fora-canal para 50ms a fim escutar clientes desonestos, monitor para o ruído, e interferência do canal. Todos os clientes ou AP desonestos detectados são enviados ao controlador, que recolhe esta informação:

- O MAC address do rogue o AP
- Nome do rogue detectado AP
- O MAC address desonesto do cliente conectado
- Se os quadros estão protegidos com WPA ou WEP
- O preâmbulo
- A razão sinal-ruído (SNR)
- O indicador da intensidade de sinal do receptor (RSSI)
- Canal de detecção desonesto
- Rádio em que o rogue é detectado
- SSID desonesto (se o rogue SSID é transmitido)
- Endereço IP de Um ou Mais Servidores Cisco ICM NT desonesto
- Cronometre primeiro e último o rogue é relatado
- Largura do canal

Exportando eventos desonestos

A fim exportar eventos desonestos para um sistema de gerenciamento de rede (NMS) da terceira para arquivístico, o WLC permite receptores de armadilha de SNMP adicionais ser adicionado. Quando um rogue é detectado ou cancelado pelo controlador, uma armadilha que contém esta informação está comunicada a todos os receptores de armadilha de SNMP. Uma advertência com exportação de eventos através do SNMP é que se os controladores múltiplos detectam o mesmo rogue, os eventos duplicados estão considerados pelo NMS como a correlação é feita somente no WCS.

Intervalo desonesto do registro

Um rogue AP esteve adicionado uma vez aos registros do WLC, ele permanecerá lá até que se esteja visto já não. Após um intervalo configurável do usuário (um padrão de 1200 segundos), um rogue na categoria do **_unclassified_** é envelhecido para fora. Os rogues em outros estados tais como o **_Contained_** e o **_Friendly_** persistirão de modo que a classificação apropriada lhes esteja

aplicada se reaparecem.

Há um tamanho de base de dados máximo para registros desonestos que seja variável através das Plataformas do controlador:

- 21XX e WLCM - 125 rogues
- 44XX - 625 rogues
- WiSM - 1250 rogues
- 5508 - 2000 rogues

Classificação desonesto

Àrevelia, todos os rogues que são detectados por Cisco UWN são considerados não classificados. Como representado neste gráfico, os rogues podem ser classificados em um número de critérios que incluem o RSSI, o SSID, o tipo da Segurança, a rede de ligar/desligar, e o número de clientes:

Detector desonesto AP

Alvos desonestos do detector Um AP para correlacionar a informação desonesto ouvida sobre o ar com a informação ARP obtida da rede ligada com fio. Se um MAC address é ouvido sobre o ar como um rogue AP ou o cliente e igualmente ouvido na rede ligada com fio, a seguir o rogue está determinado estar na rede ligada com fio. Se o rogue é detectado para estar na rede ligada com fio, a seguir a severidade de alarme para esse rogue AP está levantada para o **_critical_**. Deve-se notar que um detector desonesto AP não é bem sucedido em identificar clientes desonestos atrás de um dispositivo usando o NAT.

Considerações da escalabilidade

Um detector desonesto AP pode detectar até 500 rogues e 500 clientes desonestos. Se o detector desonesto é colocado em um tronco com dispositivos de rogue demais, a seguir estes limites puderam ser excedidos, que causasse edições. A fim impedir que isto ocorra, mantenha o detector desonesto AP na distribuição ou na camada de acesso de sua rede.

RLDP

O alvo de RLDP é identificar se um rogue específico AP é conectado à infraestrutura ligada com fio. Esta característica usa essencialmente o AP unificado o mais próximo para conectar ao dispositivo de rogue como um cliente Wireless. Após a conexão como um cliente, um pacote está enviado com o endereço de destino do WLC para avaliar se o AP é conectado à rede ligada com fio. Se o rogue é detectado para estar na rede ligada com fio, a seguir a severidade de alarme para esse rogue AP está levantada para crítico.

O algoritmo de RLDP é alistado aqui:

1. Identifique o AP unificado o mais próximo aos valores de utilização desonestos da intensidade de sinal.
2. O AP conecta então ao rogue como um cliente de WLAN, tentando três associações antes de cronometrar para fora.
3. Se a associação é bem sucedida, o AP a seguir usa o DHCP para obter um endereço IP de Um ou Mais Servidores Cisco ICM NT.

4. Se um endereço IP de Um ou Mais Servidores Cisco ICM NT foi obtido, o AP (que atua como um cliente de WLAN) envia um pacote de UDP a cada um dos endereços IP de Um ou Mais Servidores Cisco ICM NT do controlador.
5. Se o controlador recebe mesmo um dos pacotes RLDP do cliente, esse rogue está marcado como o em-fio com uma severidade de crítico.

Nota: Os pacotes RLDP são incapazes de alcançar o controlador se as regras de filtragem são no lugar entre a rede de controlador e a rede onde o dispositivo de rogue está encontrado.

Advertências de RLDP

- Os trabalhos RLDP somente com o rogue aberto AP que transmite seu SSID com autenticação e criptografia desabilitaram.
- RLDP exige que o AP controlado que atua como um cliente pode obter um endereço IP de Um ou Mais Servidores Cisco ICM NT através do DHCP na rede desonesto
- RLDP manual pode ser usado para tentar e traço RLDP no épocas múltiplas desonestos.
- Durante o processo RLDP, o AP é incapaz de servir clientes. Isto impactará negativamente o desempenho e a Conectividade para o modo local AP.
- RLDP não tenta conectar a um rogue AP que opera-se em um canal 5GHz DF.

Traçado da porta de switch

O traçado da porta de switch é uma técnica de mitigação do rogue AP executada primeiramente na liberação 5.1. Embora o traçado da porta de switch seja iniciado no WCS, utiliza o CDP e a informação de SNMP para seguir para baixo um rogue a uma porta específica na rede. Para que o traçado da porta de switch seja executado, todo o Switches na rede deve ser adicionado ao WCS com credenciais SNMP. Embora as credenciais de leitura apenas trabalhem identificando a porta o rogue está ligada, credenciais de leitura/gravação permite que o WCS igualmente feche a porta para baixo, assim contendo a ameaça. Neste tempo, esta característica trabalha somente com switch Cisco que executam IO com o CDP permitido, e o CDP deve igualmente ser permitido nos AP controlados.

O algoritmo para o traçado da porta de switch é alistado aqui:

- O WCS encontra o AP o mais próximo, que detecta o rogue AP sobre - areja, e recupera seus vizinhos de CDP.
- O WCS usa então o SNMP para examinar a tabela CAM dentro do switch confinante, procurando um fósforo positivo para identificar o lugar dos rogues.
- Um fósforo positivo é baseado no MAC address exato do rogue, +1/−1 o MAC address desonesto, algum elimina as plantas pouco vigorozas endereços MAC de cliente, ou um fósforo OUI baseado na informação do vendedor inerente em um MAC address.
- Se um fósforo positivo não é encontrado no interruptor o mais próximo, o WCS continua a procurar switch confinante até dois saltos afastado (à revelia).

Regras desonestos da classificação

As regras desonestos da classificação, introduzidas na liberação 5.0, permitem que você defina um conjunto de condição que marcam um rogue como malicioso ou amigável. Estas regras são configuradas no WCS ou no WLC, mas estão executadas sempre no controlador enquanto os rogues novos são descobertos.

Leia a classificação desonesto baseada regra do documento nos controladores do Wireless LAN (WLC) e no sistema de controle wireless (WCS) para obter mais informações sobre das regras

desonestos nos WLC.

Elimine as plantas pouco vigorozas a mitigação

Elimine as plantas pouco vigorozas a retenção

A retenção é um método da utilização sobre - os pacotes do ar para interromper temporariamente o serviço em um dispositivo de rogue até que possa fisicamente ser removida. A retenção trabalha por pacotes da de-autenticação da falsificação com o endereço de origem falsificado do rogue AP de modo que todos os clientes associados sejam retrocedidos fora.

Detalhes desonestos da retenção

Uma retenção iniciada em um rogue AP sem clientes usará somente os quadros da de-autenticação enviados ao endereço de broadcast:

Uma retenção iniciada em um rogue AP com clientes usará os quadros da de-autenticação enviados ao endereço de broadcast e ao endereço de cliente:

Os pacotes da retenção são enviados a nível da potência do AP controlado e na mais baixa taxa de dados permitida.

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

Nota: Da liberação 6.0, uma retenção executada pelo modo de NON-monitor AP é enviada em um intervalo de 500ms em vez do intervalo 100ms usado pelo modo de monitor AP.

- Um dispositivo de rogue individual pode ser contido por 1 a 4 AP controlados que trabalham na junção para abrandar temporariamente a ameaça.
- A retenção pode ser executada usando o modo local, o modo de monitor e o modo AP H-REAP (conectado). Para o modo local de H-REAP AP, um máximo de três dispositivos de rogue pelo rádio pode ser contido. Para o modo de monitor AP, um máximo de seis dispositivos de rogue pelo rádio pode ser contido.

Auto-retenção

Além do que manualmente o início da retenção em um dispositivo de rogue através de WCS ou do WLC GUI, há igualmente a capacidade para lançar automaticamente a retenção sob determinadas encenações. Esta configuração é encontrada sob o **general na** seção **desonesto das políticas da** relação WCS ou de controlador. Cada um destas características é desabilitada à revelia e deve somente ser permitida de anular as ameaças as mais prejudiciais.

- Rogue no fio - Se um dispositivo de rogue é identificado para ser anexado à rede ligada com fio, a seguir está colocado automaticamente sob a retenção.
- Usando nosso SSID - Se um dispositivo de rogue está usando um SSID que seja o mesmo que aquele configurado no controlador, é contido automaticamente. Esta característica aponta endereçar um ataque do mel-potenciômetro antes que cause dano.
- Cliente válido no rogue AP - Se um cliente alistado no ACS é encontrado para ser associado com um dispositivo de rogue, a retenção está lançada contra esse cliente somente, impedindo que associe a todo o AP NON-controlado.
- Rogue ad hoc AP - Se uma rede ad-hoc é descoberta, está contida automaticamente.

Advertências desonestos da retenção

- Porque a retenção usa uma parcela do momento do rádio do AP controlado de enviar os quadros da de-autenticação, o desempenho a ambos os clientes dos dados e da Voz é impactado negativamente por até 20%. Para clientes dos dados, o impacto é throughput reduzido. Para clientes da Voz, a retenção pode causar interrupções nas conversações e na Qualidade de voz reduzida.
- A retenção pode ter implicações legais quando lançada contra redes de vizinhança. Assegure-se de que o dispositivo de rogue esteja dentro de sua rede e levante um risco de segurança antes que você lance a retenção.

Fechamento da porta de switch

Uma vez que uma porta de switch é seguida usando o SPT, há uma opção para desabilitar essa porta no WCS. O administrador tem que fazer este exercício manualmente. Uma opção está disponível para permitir a porta de switch com o WCS se o rogue é removido fisicamente da rede.

Configurar o Gerenciamento desonesto

Configurar a detecção desonesto

A detecção desonesto é permitida no controlador à revelia.

Para encontrar detalhes desonestos em um controlador que usa a interface gráfica, vá ao **monitor** > aos **rogues**.

Nesta página, a classificação diferente para rogues está disponível:

- **AP amigáveis** – Aps que são marcados como amigável pelo administrador.
- **AP maliciosos** – Aps que são identificados como RLDP de utilização malicioso ou o detector desonesto AP.
- **AP não classificados** – Os AP desonestos serão mostrados à revelia como lista não classificada no controlador.
- **Clientes do rogue** – Clientes conectados para eliminar as plantas pouco vigorozas AP.
- **Rogues ad hoc** – Clientes desonestos ad hoc.
- **O AP desonesto ignora a lista** – Aps alistados com o WCS.

Nota: Se o WLC e o AP autônomo são controlados pelo mesmo WCS, o WLC estará alistando automaticamente este AP autônomo no rogue AP ignora a lista. Não há nenhuma configuração adicional exigida no WLC para permitir esta característica.

Do CLI:

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

Rogue on wire Auto-Contain....................... Disabled
Rogue using our SSID Auto-Contain................ Disabled
Valid client on rogue AP Auto-Contain............ Disabled
Rogue AP timeout................................. 1200

MAC Address        Classification     # APs # Clients Last Heard
-----------------  -----------------  -----  ---------  ----------------------
00:14:1b:5b:1f:90  Unclassified       1      0          Thu Jun 10 19:04:51 2010
```

```
00:14:1b:5b:1f:91  Unclassified      1     0         Thu Jun 10 18:58:51 2010
00:14:1b:5b:1f:92  Unclassified      1     0         Thu Jun 10 18:49:50 2010
00:14:1b:5b:1f:93  Unclassified      1     0         Thu Jun 10 18:55:51 2010
00:14:1b:5b:1f:96  Unclassified      1     0         Thu Jun 10 18:58:51 2010
00:17:df:a9:08:00  Unclassified      1     0         Thu Jun 10 18:49:50 2010
00:17:df:a9:08:10  Unclassified      1     0         Thu Jun 10 18:55:51 2010
00:17:df:a9:08:11  Unclassified      1     0         Thu Jun 10 19:04:51 2010
00:17:df:a9:08:12  Unclassified      1     0         Thu Jun 10 18:49:50 2010
00:17:df:a9:08:16  Unclassified      1     0         Thu Jun 10 19:04:51 2010
```

Clique uma entrada desonesto particular a fim obter os detalhes desse rogue.

Do CLI:

```
(Cisco Controller) >show rogue ap detailed 00:14:1b:5b:1f:90

Rogue BSSID..................................... 00:14:1b:5b:1f:90
Is Rogue on Wired Network....................... No
Classification.................................. Unclassified
Manual Contained................................ No
State........................................... Alert
First Time Rogue was Reported................... Thu Jun 10 18:37:50 2010
Last Time Rogue was Reported.................... Thu Jun 10 19:04:51 2010
Reported By
    AP 1
        MAC Address............................. 00:24:97:8a:09:30
        Name.................................... AP_5500
        Radio Type.............................. 802.11g
        SSID.................................... doob
        Channel................................. 6
        RSSI.................................... -51 dBm
        SNR..................................... 27 dB
        Encryption.............................. Disabled
        ShortPreamble........................... Enabled
        WPA Support............................. Disabled
        Last reported by this AP................ Thu Jun 10 19:04:51 2010
```

Configurar a exploração do canal para a detecção desonesto

Para um modo locais/Hreap/modo de monitor AP há uma opção sob a configuração RRM que permite que o usuário escolha que canal é feito a varredura para rogues. Segundo a configuração, o AP faz a varredura de todo o canal/canal do país channel/DCA para rogues.

Para configurar isto do GUI, vá ao **Sem fio** > ao **802.11a/802.11b** > ao **RRM** > ao **general**.

Do 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
```

Para configurar estas opções, vá à **Segurança > políticas wireless da proteção > políticas > general do rogue**.

1. Mude o intervalo para o rogue AP.
2. Permita a detecção de redes desonestos ad hoc.

Do 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 a classificação desonesto

Classifique manualmente um rogue AP

Para classificar um rogue AP como amigável, malicioso, ou não classificado, ir ao **monitor** > ao **rogue** > **AP não classificados**, e clicar o nome particular do rogue AP. Escolha a opção da lista de drop-down.

Do 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 using rogue APs.
```

Para remover manualmente uma entrada do rogue da lista desonesto, para ir ao **monitor** > ao **rogue** > os **AP não classificados**, e o clique **removem**.

Para configurar um rogue AP como um AP amigável, ir à **Segurança** > **políticas wireless da proteção** > **políticas do rogue** > **rogues amigáveis** e adicionar o MAC address desonesto.

As entradas desonestos amigáveis adicionadas podem ser verificadas do **monitor** > dos **rogues** > página **desonesto amigável**.

Configurar um detector desonesto AP

Para configurar o AP como um detector desonesto usando o GUI, vá ao **Sem fio** > **todos os AP**. Escolha o nome AP e mude o modo AP.

Do CLI:

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

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

Configurar o Switchport para um detector desonesto AP

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

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

Nota: O VLAN nativo nesta configuração é uma que tem a conectividade IP ao WLC.

Configurar RLDP

Para configurar RLDP no GUI do controlador, vá à **Segurança** > **políticas wireless da proteção** > **políticas** > **general do rogue**.

Modo de monitor AP – Permite que somente os AP no modo de monitor participem em RLDP.

Todos os AP – O Local/Hreap/modo de monitor AP participam no processo RLDP.

Deficiente – RLDP não é provocado automaticamente. Contudo, o usuário pode provocar RLDP manualmente para um endereço MAC particular com o CLI.

Nota: O modo de monitor AP obterá a preferência sobre o local/Hreap AP para RLDP de execução se ambos eles estão detectando um rogue particular acima de -85dbm RSSI.

Do 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

RLDP scheduling and triggering manually is configurable only through Command
    prompt

To Initiate RLDP manually:

(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).
For Scheduling RLDP

Note: RLDP scheduling and option to configure RLDP retries are two options
    introduced in 7.0 through CLI

RLDP Scheduling :

(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 ?

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



RLDP retries can be configured using the command

(Cisco Controller) >config rogue ap rldp retries ?

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

Para configurar a validação AAA para clientes desonestos, vá à **Segurança > políticas wireless da proteção > políticas > general do rogue**.

Permitir esta opção certifica-se que o endereço do rogue client/AP está verificado com o servidor AAA antes do classificar como malicioso.

Do CLI:

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

disable         Disables use of AAA/local database to detect valid mac addresses.
enable          Enables use of AAA/local database to detect valid mac addresses.
```

Para validar um cliente desonesto particular é um rogue prendido, há uma opção para verificar a alcançabilidade desse rogue particular do controlador (se o controlador pode detectar o endereço IP cliente desonesto). Esta opção pode ser alcançada na página desonesto do detalhe do cliente e está disponível somente através da interface gráfica.

Para configurar o traçado da porta de switch, refira o White Paper do Gerenciamento do rogue do documento (clientes registrados somente).

Configurar a mitigação desonesto

Configurar a retenção manual:

A fim conter manualmente um rogue AP, vá ao **monitor** > aos **rogues > não classificado**.

Do CLI:

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

aaa             Configures to validate if a rogue client is a valid client using
                    AAA/local database.
alert           Configure the rogue client to the alarm state.
contain         Start containing a rogue client.

(Cisco Controller) >config rogue client contain 01:22:33:44:55:66 ?

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

Nota: Um rogue particular pode ser contido usando 1-4 AP. À revelia, o controlador usa um AP contendo um cliente. Se dois AP podem detectar um rogue particular, o AP com o RSSI o mais alto contém o cliente apesar do modo AP.

Para configurar a auto retenção, vá à **Segurança > políticas wireless da proteção > políticas > general do rogue**, e permita todas as opções aplicáveis para sua rede.

Do CLI:

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

alert           Stop Auto-Containment, generate a trap upon detection of the
                    adhoc rogue.
auto-contain    Automatically containing adhoc rogue.
contain         Start containing 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! Using this feature may have legal consequences
         Do you want to continue(y/n) :y
```

Troubleshooting

Se o rogue não é detectado:

- Verifique que a detecção do rogue está permitida no AP usando este comando. À revelia, a detecção desonesto é permitida no AP.`(Cisco_Controller) >show ap config general Managed_AP`

```
Cisco AP Identifier.............................. 2
Cisco AP Name.................................... Managed_AP
Country code..................................... US  - United States
Regulatory Domain allowed by Country............. 802.11bg:-A     802.11a:-A
AP Country code.................................. US  - United States
AP Regulatory Domain............................. 802.11bg:-A    802.11a:-A
Switch Port Number .............................. 2
MAC Address...................................... 00:1d:a1:cc:0e:9e
IP Address Configuration......................... DHCP
IP Address....................................... 10.8.99.104
IP NetMask....................................... 255.255.255.0
Gateway IP Addr.................................. 10.8.99.1
CAPWAP Path MTU.................................. 1485
Telnet State..................................... Enabled
Ssh State........................................ Disabled
Cisco AP Location................................ india-banaglore
Cisco AP Group Name.............................. default-group
Primary Cisco Switch Name........................ Cisco_e9:d9:23
Primary Cisco Switch IP Address.................. 10.44.81.20
Secondary Cisco Switch Name.....................
Secondary Cisco Switch IP Address................ Not Configured
Tertiary Cisco Switch Name.....................
Tertiary Cisco Switch IP Address................. Not Configured
Administrative State ............................ ADMIN_ENABLED
Operation State ................................. REGISTERED
Mirroring Mode .................................. Disabled
AP Mode ......................................... Local
Public Safety ................................... Disabled
AP SubMode ...................................... Not Configured
Remote AP Debug ................................. Disabled
Logging trap severity level ..................... informational
Logging syslog facility ......................... kern
S/W  Version ..................................... 7.0.98.0
Boot  Version .................................... 12.3.7.1
Mini IOS Version ................................ 3.0.51.0
Stats Reporting Period .......................... 209
LED State........................................ Enabled
PoE Pre-Standard Switch.......................... Enabled
PoE Power Injector MAC Addr...................... Override
Power Type/Mode.................................. Power injector / Normal mode
Number Of Slots.................................. 2
AP Model......................................... AIR-LAP1242AG-A-K9
AP Image......................................... C1240-K9W8-M
IOS Version...................................... 12.4(23c)JA
Reset Button..................................... Enabled
AP Serial Number................................. FTX1137B22V
```

```
AP Certificate Type..............................Manufacture Installed
AP User Mode.....................................AUTOMATIC
AP User Name.....................................Not Configured
AP Dot1x User Mode...............................GLOBAL
AP Dot1x User Name...............................Cisco12
Cisco AP system logging host.....................255.255.255.255
AP Up Time.......................................13 days, 15 h 01 m 33 s
AP LWAPP Up Time.................................13 days, 15 h 00 m 40 s
Join Date and Time...............................Tue Jun  1 10:36:38 2010

Join Taken Time..................................0 days, 00 h 00 m 52 s
Ethernet Port Duplex.............................Auto
Ethernet Port Speed..............................Auto
AP Link Latency..................................Enabled
 Current Delay..................................0 ms
 Maximum Delay..................................56 ms
 Minimum Delay..................................2 ms
 Last updated (based on AP Up Time).............13 days, 15 h 00 m 44 s
Rogue Detection..................................Enabled
AP TCP MSS Adjust................................Disabled
```

A detecção desonesto pode ser permitida em um AP usando 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 modo local AP faz a varredura somente dos canais do país channels/DCA segundo a configuração. Se o rogue está em qualquer outro canal, o controlador não pode identificar o rogue se você não tem o modo de monitor AP 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 AP Coverage Interval.................. 180 seconds
  802.11a AP Load Interval...................... 60 seconds
  802.11a AP Noise Interval..................... 180 seconds
  802.11a AP Signal Strength Interval........... 60 seconds
```

- O AP desonesto não pode transmitir o SSID.
- Certifique-se que o MAC address do rogue o AP não está adicionado no WCS direto listado desonesto amigável do lista ou o branco.
- As balizas do rogue AP não podem ser alcançáveis ao AP que detecta rogues. Isto pode ser verificado capturando o pacote usando um sniffer perto do rogue dedetecção.
- Um modo local AP pode tomar até os minutos 9 para detectar um rogue (3 ciclos 180x3).
- Cisco AP não pode detectar rogues em frequências como o canal da segurança pública (4.9 gigahertz).
- Cisco AP não pode detectar rogues trabalhar em FHSS (espectro de propagação do salto de frequência).

Útil debuga

```
(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 AP Coverage Interval.................. 180 seconds
  802.11a AP Load Interval...................... 60 seconds
  802.11a AP Noise Interval..................... 180 seconds
```

```
  802.11a AP Signal Strength Interval..... 60 seconds
```

debug dot11 rogue enable

```
(Cisco_Controller) >*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12
    Looking for Rogue 00:27:0d:8d:14:12 in known AP table
*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12 Rogue AP 00:27:0d:8d:14:12
    is not found either in AP list or neighbor, known or Mobility group AP lists
*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12 Change state from 0 to 1
    for rogue AP 00:27:0d:8d:14:12
*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12 rg change state Rogue AP:
    00:27:0d:8d:14:12

*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12 New RSSI report from AP
    00:1b:0d:d4:54:20  rssi -74, snr -9 wepMode 129
*apfRogueTask: Jun 15 01:45:09.010: 00:27:0d:8d:14:12 rg send new rssi -74
*apfRogueTask: Jun 15 01:45:09.010: 00:27:0d:8d:14:12 Updated AP report
    00:1b:0d:d4:54:20  rssi -74, snr -9
*apfRogueTask: Jun 15 01:45:09.010: 00:27:0d:8d:14:12 Manual Contained Flag = 0

*apfRogueTask: Jun 15 01:45:09.010: 00:27:0d:8d:14:12 rg new Rogue AP:
    00:27:0d:8d:14:12

*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Found Rogue AP:
    00:24:97:2d:bf:90 on slot 0

*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Added Rogue AP:
    00:24:97:2d:bf:90

*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Looking for Rogue
    00:24:97:2d:bf:90 in known AP table
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Rogue AP 00:24:97:2d:bf:90
    is not found either in AP list or neighbor, known or Mobility group AP lists
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Change state from 0 to 1
    for rogue AP 00:24:97:2d:bf:90
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 rg change state Rogue AP:
    00:24:97:2d:bf:90

*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 New RSSI report from AP
    00:1b:0d:d4:54:20  rssi -56, snr 34 wepMode 129
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 rg send new rssi -56
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Updated AP report
    00:1b:0d:d4:54:20  rssi -56, snr 34
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Manual Contained Flag = 0

*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 rg new Rogue AP:
    00:24:97:2d:bf:90

*apfRogueTask: Jun 15 01:45:09.010: 9c:af:ca:0f:bd:40 Found Rogue AP:
    9c:af:ca:0f:bd:40 on slot 0

*apfRogueTask: Jun 15 01:45:09.010: 9c:af:ca:0f:bd:40 Added Rogue AP:
    9c:af:ca:0f:bd:40

*apfRogueTask: Jun 15 01:45:09.010: 9c:af:ca:0f:bd:40 Looking for Rogue
    9c:af:ca:0f:bd:40 in known AP table
*apfRogueTask: Jun 15 01:45:09.010: 9c:af:ca:0f:bd:40 Rogue AP 9c:af:ca:0f:bd:40
    is not found eithe*apfRogueTask: Jun 15 01:45:09.011: 00:25:45:a2:e1:62
    Updated AP report 00:1b:0d:d4:54:20  rssi -73, snr 24
*apfRogueTask: Jun 15 01:45:09.012: 00:25:45:a2:e1:62 Manual Contained Flag = 0

*apfRogueTask: Jun 15 01:45:09.012: 00:25:45:a2:e1:62 rg new Rogue AP:
    00:25:45:a2:e1:62
```

```
*apfRogueTask: Jun 15 01:45:09.012: 00:24:c4:ad:c0:40 Found Rogue AP:
    00:24:c4:ad:c0:40 on slot 0

*apfRogueTask: Jun 15 01:45:09.012: 00:24:c4:ad:c0:40 Added Rogue AP:
    00:24:c4:ad:c0:40
```

Logs previstos da armadilha

Um rogue é detectado uma vez

debug dot11 rogue enable

```
(Cisco_Controller) >*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12
    Looking for Rogue 00:27:0d:8d:14:12 in known AP table
*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12 Rogue AP 00:27:0d:8d:14:12
    is not found either in AP list or neighbor, known or Mobility group AP lists
*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12 Change state from 0 to 1
    for rogue AP 00:27:0d:8d:14:12
*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12 rg change state Rogue AP:
    00:27:0d:8d:14:12

*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12 New RSSI report from AP
    00:1b:0d:d4:54:20  rssi -74, snr -9 wepMode 129
*apfRogueTask: Jun 15 01:45:09.010: 00:27:0d:8d:14:12 rg send new rssi -74
*apfRogueTask: Jun 15 01:45:09.010: 00:27:0d:8d:14:12 Updated AP report
    00:1b:0d:d4:54:20  rssi -74, snr -9
*apfRogueTask: Jun 15 01:45:09.010: 00:27:0d:8d:14:12 Manual Contained Flag = 0

*apfRogueTask: Jun 15 01:45:09.010: 00:27:0d:8d:14:12 rg new Rogue AP:
    00:27:0d:8d:14:12

*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Found Rogue AP:
    00:24:97:2d:bf:90 on slot 0

*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Added Rogue AP:
    00:24:97:2d:bf:90

*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Looking for Rogue
    00:24:97:2d:bf:90 in known AP table
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Rogue AP 00:24:97:2d:bf:90
    is not found either in AP list or neighbor, known or Mobility group AP lists
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Change state from 0 to 1
    for rogue AP 00:24:97:2d:bf:90
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 rg change state Rogue AP:
    00:24:97:2d:bf:90

*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 New RSSI report from AP
    00:1b:0d:d4:54:20  rssi -56, snr 34 wepMode 129
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 rg send new rssi -56
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Updated AP report
    00:1b:0d:d4:54:20  rssi -56, snr 34
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Manual Contained Flag = 0

*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 rg new Rogue AP:
    00:24:97:2d:bf:90

*apfRogueTask: Jun 15 01:45:09.010: 9c:af:ca:0f:bd:40 Found Rogue AP:
    9c:af:ca:0f:bd:40 on slot 0

*apfRogueTask: Jun 15 01:45:09.010: 9c:af:ca:0f:bd:40 Added Rogue AP:
    9c:af:ca:0f:bd:40
```

```
*apfRogueTask: Jun 15 01:45:09.010: 9c:af:ca:0f:bd:40 Looking for Rogue
    9c:af:ca:0f:bd:40 in known AP table
*apfRogueTask: Jun 15 01:45:09.010: 9c:af:ca:0f:bd:40 Rogue AP 9c:af:ca:0f:bd:40
    is not found eithe*apfRogueTask: Jun 15 01:45:09.011: 00:25:45:a2:e1:62
    Updated AP report 00:1b:0d:d4:54:20  rssi -73, snr 24
*apfRogueTask: Jun 15 01:45:09.012: 00:25:45:a2:e1:62 Manual Contained Flag = 0

*apfRogueTask: Jun 15 01:45:09.012: 00:25:45:a2:e1:62 rg new Rogue AP:
    00:25:45:a2:e1:62

*apfRogueTask: Jun 15 01:45:09.012: 00:24:c4:ad:c0:40 Found Rogue AP:
    00:24:c4:ad:c0:40 on slot 0

*apfRogueTask: Jun 15 01:45:09.012: 00:24:c4:ad:c0:40 Added Rogue AP:
    00:24:c4:ad:c0:40
```

Uma entrada do rogue é removida uma vez da lista desonesto

debug dot11 rogue enable

```
(Cisco_Controller) >*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12
    Looking for Rogue 00:27:0d:8d:14:12 in known AP table
*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12 Rogue AP 00:27:0d:8d:14:12
    is not found either in AP list or neighbor, known or Mobility group AP lists
*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12 Change state from 0 to 1
    for rogue AP 00:27:0d:8d:14:12
*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12 rg change state Rogue AP:
    00:27:0d:8d:14:12

*apfRogueTask: Jun 15 01:45:09.009: 00:27:0d:8d:14:12 New RSSI report from AP
    00:1b:0d:d4:54:20  rssi -74, snr -9 wepMode 129
*apfRogueTask: Jun 15 01:45:09.010: 00:27:0d:8d:14:12 rg send new rssi -74
*apfRogueTask: Jun 15 01:45:09.010: 00:27:0d:8d:14:12 Updated AP report
    00:1b:0d:d4:54:20  rssi -74, snr -9
*apfRogueTask: Jun 15 01:45:09.010: 00:27:0d:8d:14:12 Manual Contained Flag = 0

*apfRogueTask: Jun 15 01:45:09.010: 00:27:0d:8d:14:12 rg new Rogue AP:
    00:27:0d:8d:14:12

*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Found Rogue AP:
    00:24:97:2d:bf:90 on slot 0

*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Added Rogue AP:
    00:24:97:2d:bf:90

*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Looking for Rogue
    00:24:97:2d:bf:90 in known AP table
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Rogue AP 00:24:97:2d:bf:90
    is not found either in AP list or neighbor, known or Mobility group AP lists
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Change state from 0 to 1
    for rogue AP 00:24:97:2d:bf:90
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 rg change state Rogue AP:
    00:24:97:2d:bf:90

*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 New RSSI report from AP
    00:1b:0d:d4:54:20  rssi -56, snr 34 wepMode 129
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 rg send new rssi -56
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Updated AP report
    00:1b:0d:d4:54:20  rssi -56, snr 34
*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 Manual Contained Flag = 0

*apfRogueTask: Jun 15 01:45:09.010: 00:24:97:2d:bf:90 rg new Rogue AP:
```

```
    00:24:97:2d:bf:90

*apfRogueTask: Jun 15 01:45:09.010: 9c:af:ca:0f:bd:40 Found Rogue AP:
    9c:af:ca:0f:bd:40 on slot 0

*apfRogueTask: Jun 15 01:45:09.010: 9c:af:ca:0f:bd:40 Added Rogue AP:
    9c:af:ca:0f:bd:40

*apfRogueTask: Jun 15 01:45:09.010: 9c:af:ca:0f:bd:40 Looking for Rogue
    9c:af:ca:0f:bd:40 in known AP table
*apfRogueTask: Jun 15 01:45:09.010: 9c:af:ca:0f:bd:40 Rogue AP 9c:af:ca:0f:bd:40
    is not found eithe*apfRogueTask: Jun 15 01:45:09.011: 00:25:45:a2:e1:62
    Updated AP report 00:1b:0d:d4:54:20  rssi -73, snr 24
*apfRogueTask: Jun 15 01:45:09.012: 00:25:45:a2:e1:62 Manual Contained Flag = 0

*apfRogueTask: Jun 15 01:45:09.012: 00:25:45:a2:e1:62 rg new Rogue AP:
    00:25:45:a2:e1:62

*apfRogueTask: Jun 15 01:45:09.012: 00:24:c4:ad:c0:40 Found Rogue AP:
    00:24:c4:ad:c0:40 on slot 0

*apfRogueTask: Jun 15 01:45:09.012: 00:24:c4:ad:c0:40 Added Rogue AP:
    00:24:c4:ad:c0:40
```

Recomendações

1. Configurar o canal que faz a varredura para todos os canais se você suspeita rogues potenciais em sua rede
2. Segundo a disposição da rede ligada com fio, o número e o lugar do detector desonesto AP podem variar de um pelo assoalho a um pela construção. É aconselhável ter pelo menos um detector desonesto AP em cada assoalho de uma construção. Porque um detector desonesto AP exige um tronco a todos os domínios do broadcast de rede da camada 2 que devem ser monitorados, a colocação é dependente da disposição lógica da rede.

Se o rogue não está obtendo classificado

- Verifique que as regras desonestos estão configuradas corretamente.
- Se o rogue está no canal DF, RLDP não trabalha.
- RLDP trabalha somente se o WLAN do rogue está aberto e o DHCP está disponível.
- Se o modo local AP está servindo o cliente no canal DF, não participará no processo RLDP.

Útil debuga

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

Received Request to detect rogue: 00:1A:1E:85:21:B0
00:1a:1e:85:21:b0 found closest monitor AP 00:17:df:a7:20:d0slot =1 channel = 44
Found RAD: 0x158f1ea0, slotId = 1
rldp started association, attempt 1
Successfully associated with rogue: 00:1A:1E:85:21:B0

!--- ASSOCIATING TO ROGUE AP Starting dhcp 00:1a:1e:85:21:b0 RLDP DHCP SELECTING for rogue
00:1a:1e:85:21:b0 00:1a:1e:85:21:b0 Initializing RLDP DHCP for rogue 00:1a:1e:85:21:b0
.00:1a:1e:85:21:b0 RLDP DHCPSTATE_INIT for rogue 00:1a:1e:85:21:b0 00:1a:1e:85:21:b0 RLDP
DHCPSTATE_REQUESTING sending for rogue 00:1a:1e:85:21:b0 00:1a:1e:85:21:b0 Sending DHCP packet
through rogue AP 00:1a:1e:85:21:b0 00:1a:1e:85:21:b0 RLDP DHCP REQUEST RECV for rogue
00:1a:1e:85:21:b0 00:1a:1e:85:21:b0 RLDP DHCP REQUEST received for rogue 00:1a:1e:85:21:b0
00:1a:1e:85:21:b0 RLDP DHCP BOUND state for rogue 00:1a:1e:85:21:b0 Returning IP 172.20.226.246,
netmask 255.255.255.192, gw 172.20.226.193 !--- GETTING IP FROM ROGUE Found Gateway MacAddr:
```

```
00:1D:70:F0:D4:C1 Send ARLDP to 172.20.226.198 (00:1D:70:F0:D4:C1) (gateway) Sending ARLDP
packet to 00:1d:70:f0:d4:c1 from 00:17:df:a7:20:de Send ARLDP to 172.20.226.197
(00:1F:9E:9B:29:80) Sending ARLDP packet to 00:1f:9e:9b:29:80 from 00:17:df:a7:20:de Send ARLDP
to 0.0.0.0 (00:1D:70:F0:D4:C1) (gateway) Sending ARLDP packet to 00:1d:70:f0:d4:c1 from
00:17:df:a7:20:de !--- SENDING ARLDP PACKET Received 32 byte ARLDP message from:
172.20.226.24642 Packet Dump: sourceIp: 172.20.226.246 destIp: 172.20.226.197 Rogue Mac:
00:1A:1E:85:21:B0 !--- RECEIVING ARLDP PACKET security: 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00
```

Recomendações

1. RLDP iniciado manualmente em entradas desonestos suspeitos.
2. Programação RLDP periodicamente.
3. Se você conheceu entradas desonestos, adicionar-las na lista amigável ou permita-o a validação com AAA e certifique-se que entradas do cliente conhecido está lá no base de dados AAA.
4. RLDP pode ser distribuído no local ou no modo de monitor AP. Para a maioria de disposições escaláveis, e para eliminar todo o impacto no serviço de cliente, RLDP deve ser distribuído no modo de monitor AP quando possível. Contudo, esta recomendação exige que um modo de monitor AP overlay esteja distribuído com uma relação típica como 1 modo de monitor AP para cada 5 modo local AP. Os AP no modo de monitor adaptável do wIPS podem igualmente ser leveraged para esta tarefa.

Detector desonesto AP

A entrada do rogue em um detector desonesto pode ser considerada usar este comando no console AP. Para rogues prendidos, a bandeira será ajustada.

```
Rogue_Detector_5500#show capwap rm rogue detector
 CAPWAP Rogue Detector Mode
  Current Rogue Table:
  Rogue hindex = 0: MAC 0023.ebdc.1ac6, flag = 0, unusedCount = 1
  Rogue hindex = 2: MAC 0023.04c9.72b9, flag = 1, unusedCount = 1

!--- once the flag is set, rogue is detected on wire Rogue hindex = 2: MAC 0023.ebdc.1ac4, flag
= 0, unusedCount = 1 Rogue hindex = 3: MAC 0026.cb4d.6e20, flag = 0, unusedCount = 1 Rogue
hindex = 4: MAC 0026.cb9f.841f, flag = 0, unusedCount = 1 Rogue hindex = 4: MAC 0023.04c9.72bf,
flag = 0, unusedCount = 1 Rogue hindex = 4: MAC 0023.ebdc.1ac2, flag = 0, unusedCount = 1 Rogue
hindex = 4: MAC 001c.0f80.d450, flag = 0, unusedCount = 1 Rogue hindex = 6: MAC 0023.04c9.72bd,
flag = 0, unusedCount = 1
```

Comandos debug úteis em um console AP

```
Rogue_Detector#debug capwap rm rogue detector

*Jun 18 08:37:59.747: ROGUE_DET: Received a rogue table update of length 170
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1ac4
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1ac5
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1aca
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acb
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acc
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acd
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acf
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0024.1431.e9ef
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0024.148a.ca2b
*Jun 18 08:37:59.748: ROGUE_DET: Got wired mac 0024.148a.ca2d
*Jun 18 08:37:59.748: ROGUE_DET: Got wired mac 0024.148a.ca2f
*Jun 18 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.3570
*Jun 18 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.3574
*Jun 18 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.357b
*Jun 18 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.357c
```

```
*Jun 18 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.357d
*Jun 18 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.357f
*Jun 18 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3dcd
*Jun 18 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3ff0
*Jun 18 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3ff2
*Jun 18 08:37:59.774: ROGUE_DET: Got wired mac 0040.96b9.4aec
*Jun 18 08:37:59.774: ROGUE_DET: Got wired mac 0040.96b9.4b77
*Jun 18 08:37:59.774: ROGUE_DET: Flushing rogue entry 0040.96b9.4794
*Jun 18 08:37:59.774: ROGUE_DET: Flushing rogue entry 0022.0c97.af80
*Jun 18 08:37:59.775: ROGUE_DET: Flushing rogue entry 0024.9789.5710
*Jun 18 08:38:19.325: ROGUE_DET: Got ARP src 001d.a1cc.0e9e
*Jun 18 08:38:19.325: ROGUE_DET: Got wired mac 001d.a1cc.0e9e
*Jun 18 08:39:19.323: ROGUE_DET: Got ARP src 001d.a1cc.0e9e
*Jun 18 08:39:19.324: ROGUE_DET: Got wired mac 001d.a1cc.0e9e
```

Se desonesto a retenção não ocorre:

1. O modo AP local/Hreap pode conter 3 dispositivos de cada vez pelo rádio, e o modo de monitor AP pode conter os dispositivos 6 pelo rádio. Em consequência, certifique-se que o AP já está contendo o número máximo de dispositivos permitidos. Nesta encenação, o cliente está em um estado pendente da retenção.
2. Verifique auto regras da retenção.

Logs previstos da armadilha

```
Rogue_Detector#debug capwap rm rogue detector

*Jun 18 08:37:59.747: ROGUE_DET: Received a rogue table update of length 170
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1ac4
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1ac5
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1aca
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acb
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acc
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acd
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0023.ebdc.1acf
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0024.1431.e9ef
*Jun 18 08:37:59.747: ROGUE_DET: Got wired mac 0024.148a.ca2b
*Jun 18 08:37:59.748: ROGUE_DET: Got wired mac 0024.148a.ca2d
*Jun 18 08:37:59.748: ROGUE_DET: Got wired mac 0024.148a.ca2f
*Jun 18 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.3570
*Jun 18 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.3574
*Jun 18 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.357b
*Jun 18 08:37:59.748: ROGUE_DET: Got wired mac 0024.14e8.357c
*Jun 18 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.357d
*Jun 18 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.357f
*Jun 18 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3dcd
*Jun 18 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3ff0
*Jun 18 08:37:59.749: ROGUE_DET: Got wired mac 0024.14e8.3ff2
*Jun 18 08:37:59.774: ROGUE_DET: Got wired mac 0040.96b9.4aec
*Jun 18 08:37:59.774: ROGUE_DET: Got wired mac 0040.96b9.4b77
*Jun 18 08:37:59.774: ROGUE_DET: Flushing rogue entry 0040.96b9.4794
*Jun 18 08:37:59.774: ROGUE_DET: Flushing rogue entry 0022.0c97.af80
*Jun 18 08:37:59.775: ROGUE_DET: Flushing rogue entry 0024.9789.5710
*Jun 18 08:38:19.325: ROGUE_DET: Got ARP src 001d.a1cc.0e9e
*Jun 18 08:38:19.325: ROGUE_DET: Got wired mac 001d.a1cc.0e9e
*Jun 18 08:39:19.323: ROGUE_DET: Got ARP src 001d.a1cc.0e9e
*Jun 18 08:39:19.324: ROGUE_DET: Got wired mac 001d.a1cc.0e9e
```

Conclusão

A detecção desonesto e a retenção dentro da solução centralizada Cisco do controlador são método o mais eficaz e menos o mais intrusivo na indústria. A flexibilidade fornecida ao administrador de rede permite um ajuste mais personalizado que possa acomodar todos os requisitos de rede.

Informações Relacionadas

- Classificação desonesto baseada regra nos controladores do Wireless LAN (WLC) e no sistema de controle wireless (WCS)
- Detecção desonesto sob redes Wireless unificadas
- White Paper desonesto do Gerenciamento (clientes registrados somente)
- Manual de configuração do controlador de LAN do Cisco Wireless, liberação 7.0
- Suporte Técnico e Documentação - Cisco Systems