Políticas confiadas AP em um controlador do Wireless LAN

Índice

Introdução

Este documento descreve as políticas wireless *confiadas da* proteção *AP em um* controlador do Wireless LAN (WLC), define políticas confiadas AP, e fornece uma breve descrição de todas as políticas confiadas AP.

Pré-requisitos

Requisitos

Assegure-se de que você tenha uma compreensão básica de parâmetros de Segurança para LAN Wireless (tais como o SSID, criptografia, autenticação, e assim por diante).

Convenções

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

Políticas confiadas AP

As políticas confiadas AP são uns recursos de segurança no controlador que é projetado ser usado nas encenações onde os clientes têm uma rede autônoma paralela AP junto com o controlador. Nessa encenação, o AP autônomo pode ser marcado como o AP confiado no controlador, e o usuário pode definir políticas para estes os AP confiados (que devem usar

somente o WEP ou o WPA, nosso próprio SSID, preâmbulo curto, e assim por diante). Se qualquera um falha AP para encontrar estas políticas, o controlador levanta um alarme para o dispositivo de gerenciamento de rede (sistema de controle wireless) esse estados um AP confiado violou uma política configurada.

Que é um AP confiado?

Os AP confiados são os AP que não são parte de uma organização. Contudo, não causam uma ameaça de segurança à rede. Estes AP são chamados igualmente AP amigáveis. Diversas encenações existem onde você pôde querer configurar um AP como um AP confiado.

Por exemplo, você pôde ter categorias diferentes de AP em sua rede como:

- **AP que você possui que não executam LWAPP (talvez executam IO ou VxWorks)**
- LWAPP AP em que os empregados trazem (com o conhecimento do administrador)
- LWAPP AP usado para testar a rede existente
- O LWAPP AP esse vizinhos possui

Normalmente, os AP confiados são os AP que caem na **categoria 1**, que são os AP que você possui que não executam o LWAPP. Puderam ser os AP velhos que executam VxWorks ou IO. A fim assegurar-se de que estes AP não danifiquem a rede, determinadas características podem ser reforçadas, como SSID corretos e tipos do autenticação. Configurar as políticas confiadas AP no WLC, e certifique-se de que os AP confiados encontram estas políticas. Se não, você pode configurar o controlador para tomar diversas ações, tais como o aumento um alarme ao dispositivo de gerenciamento de rede (WCS).

Os AP conhecidos que pertencem aos vizinhos podem ser configurados como AP confiados.

Normalmente, MFP (proteção do quadro do Gerenciamento) deve impedir os AP que não são LWAPP legítimo AP de se juntar o WLC. Se os cartões NIC apoiam MFP, não estão permitidos aceitar deauthentications dos dispositivos diferentes dos AP reais. Refira a proteção do quadro do Gerenciamento da infraestrutura (MFP) com WLC e DOBRE o exemplo de configuração para obter mais informações sobre de MFP.

Se você tem os AP que executam VxWorks ou IO (como na categoria 1), nunca juntar-se-ão ao grupo LWAPP ou far-se-ão MFP, mas você pôde querer reforçar as políticas alistadas nessa página. Nesses casos, as políticas confiadas AP precisam de ser configuradas no controlador para os AP do interesse.

Geralmente, se você sabe sobre um rogue AP e identifica que não é uma ameaça a sua rede, você pode identificar que AP como um AP confiado conhecido.

Como configurar um AP como um AP confiado do WLC GUI?

Termine estas etapas a fim configurar um AP como um AP confiado:

1. O log no GUI do WLC com o HTTP ou os https entram.
2. Do menu principal do controlador, **Sem fio do** clique.
3. No menu situado no lado esquerdo da página theWireless, clique **AP desonestos**.A página do rogue AP alista todos os AP que são detectados como o rogue AP na rede.
4. Desta lista do rogue AP, encontre o AP que você quer configurado como o AP confiado que cai sob a categoria 1 (como explicado na seção anterior).Você pode encontrar os AP com os

endereços MAC alistados na página desonesto AP. Se o AP desejado não está nesta página, clique **em seguida** a fim identificar o AP da página seguinte.
5. Uma vez que o AP desejado é ficado situado da lista do rogue AP, clique o **botão Edit** que corresponde ao AP, que o toma à página do detalhe do AP.Nos detalhes página do rogue AP, você pode encontrar a informação detalhada sobre este AP (como se esse AP conectado à rede ligada com fio, assim como o status atual do AP e assim por diante).
6. A fim configurar este AP como um AP confiado, para selecionar **interno conhecido da** lista de drop-down do status de atualização, e o clique **aplica-se**.Quando você atualiza o estado AP a *interno conhecido*, este AP está configurado como o AP confiado desta rede.
7. Repita estas etapas para todos os AP que você quer configurar como AP confiados.

Verifique a configuração confiada AP

Termine estas etapas a fim verificar que o AP está configurado corretamente como o AP confiado do controlador GUI:

1. Clique o **Sem fio**.
2. No menu situado no lado esquerdo da página theWireless, clique o **rogue conhecido AP**.O AP desejado deve aparecer na página desonesto conhecida AP com o estado alistado como *sabido*.

Compreendendo ajustes confiados da política AP

O WLC tem estas políticas confiadas AP:

- Política de criptografia reforçada
- Política reforçada do preâmbulo
- Tipo de rádio reforçado política
- Valide o SSID
- Alerta se o AP confiado falta
- Intervalo da expiração para entradas confiadas AP (segundos)

Política de criptografia reforçada

Esta política é usada para definir o tipo de criptografia que o AP confiado deve usar. Você pode configurar qualquens um tipos de criptografia sob a política de criptografia reforçada:

- Nenhum
- Abrir
- WEP
- WPA/802.11i

O WLC verifica se o tipo de criptografia configurado no AP confiado combina o tipo de criptografia configurado “no ajuste da **política de criptografia reforçada**”. Se o AP confiado não usa o tipo de criptografia designado, o WLC levanta um alarme para o sistema de administração a fim tomar ações apropriadas.

Política reforçada do preâmbulo

O preâmbulo de rádio (chamado às vezes um encabeçamento) é uma seção dos dados na cabeça de um pacote que contenha a informação que os dispositivos Wireless precisam quando enviam e recebem pacotes. Os preâmbulos **curtos** melhoram o desempenho da taxa de transferência de dados, assim que são permitidos à revelia. Contudo, alguns dispositivos Wireless, tais como telefones de SpectraLink NetLink, exigem preâmbulos **longos**. Você pode configurar qualqueras um opções do preâmbulo sob a política reforçada do preâmbulo:

- Nenhum
- Curto
- Por muito tempo

O WLC verifica se o tipo do preâmbulo configurado no AP confiado combina o tipo do preâmbulo configurado “no ajuste da **política reforçada do preâmbulo**”. Se o AP confiado não usa o tipo especificado do preâmbulo, o WLC levanta um alarme para o sistema de administração a fim tomar ações apropriadas.

Tipo de rádio reforçado política

Esta política é usada para definir o tipo de rádio que o AP confiado deve usar. Você pode configurar qualquens um tipos do rádio sob o tipo de rádio reforçado política:

- Nenhum
- 802.11b somente
- 802.11a somente
- 802.11b/g somente

O WLC verifica se o tipo de rádio configurado no AP confiado combina o tipo de rádio configurado “no ajuste do **tipo política de rádio reforçada**”. Se o uso confiado de APdoes não os rádios especificados, o WLC levanta um alarme para o sistema de administração a fim tomar ações apropriadas.

Valide o SSID

Você pode configurar o controlador para validar AP confiados SSID contra os SSID configurados no controlador. Se os AP confiados SSID combinam um do controlador SSID, o controlador levanta um alarme.

Alerta se o AP confiado falta

Se esta política é permitida, o WLC alerta o sistema de administração se o AP confiado falta da lista desonesto conhecida AP.

Intervalo da expiração para entradas confiadas AP (segundos)

Este valor de timeout da expiração especifica o número de segundos antes do AP confiado é considerado expirado e nivelado da entrada WLC. Você pode especificar este valor de timeout nos segundos (120 - 3600 segundos).

Como configurar confiou políticas AP no WLC?

Termine estas etapas a fim configurar políticas confiadas AP no WLC com o GUI:

Nota: Todas as políticas confiadas AP residem na mesma página WLC.

1. Do menu principal WLC GUI, **Segurança do** clique.
2. Do menu situado no lado esquerdo da página da Segurança, o clique **confiou as políticas AP** alistadas sob a direção wireless das políticas da proteção.
3. Nas políticas confiadas AP pagine, selecione o tipo de criptografia desejado (nenhuns, abrem, WEP, WPA/802.11i) da lista de drop-down reforçada da política de criptografia.
4. Selecione o tipo desejado do preâmbulo (nenhum, curto, longo) do tipo reforçado lista de drop-down do preâmbulo da política.
5. Selecione o tipo de rádio desejado (nenhum, 802.11b somente, 802.11a somente, 802.11b/g somente) do tipo de rádio reforçado lista de drop-down da política.
6. Verifique ou desmarcar a caixa de verificação **permitida SSID da validação** a fim permitir ou desabilitar o ajuste da validação SSID.
7. Verifique ou desmarcar o **alerta se o AP confiado é** caixa de verificação **permitida faltante** a fim permitir ou desabilitar o alerta se o AP confiado é ajuste faltante.
8. Incorpore um valor (nos segundos) para o **intervalo da expiração para a** opção **confiada das entradas AP**.
9. Clique em Apply.

Nota: A fim configurar estes ajustes do WLC CLI, você pode usar o comando confiar-**ap dos wps da configuração** com a opção apropriada da política.

```
Cisco Controller) >config wps trusted-ap ? encryption Configures the trusted AP encryption
policy to be enforced. missing-ap Configures alert of missing trusted AP. preamble Configures
the trusted AP preamble policy to be enforced. radio Configures the trusted AP radio policy to
be enforced. timeout Configures the expiration time for trusted APs, in seconds.
```

Mensagem de alerta confiado da violação da política AP

Está aqui um exemplo do mensagem de alerta confiado da violação da política AP mostrado pelo controlador.

```
Thu Nov 16 12:39:12 2006  [WARNING] apf_rogue.c 1905: Possible AP
impersonation of xx:xx:xx:xx:xx:xx, using source address of
00:16:35:9e:6f:3a, detected by 00:17:df:7d:e1:70 on slot 0
 Thu Nov 16 12:39:12 2006  [SECURITY] apf_rogue.c 1490: Trusted AP Policy failed for AP
xx:xx:xx:xx:xx:xx - invalid SSID 'SSID1' Thu Nov 16 12:39:12 2006 [SECURITY] apf_rogue.c 1457:
Trusted AP Policy failed for AP xx:xx:xx:xx:xx:xx - invalid encryption type Thu Nov 16 12:39:12
2006 Previous message occurred 6 times
```

Observe os Mensagens de Erro destacados aqui. Estes Mensagens de Erro indicam que o SSID e o tipo de criptografia configurados no AP confiado não combinam o ajuste confiado da política AP.

O mesmo mensagem de alerta pode ser considerado do WLC GUI. A fim ver esta mensagem, vá ao menu principal WLC GUI, e clique o **monitor**. Na seção a mais recente das armadilhas da página do monitor, clique a **vista toda** a fim ver todos os alertas recentes no WLC.

Nas armadilhas as mais recentes página, você pode identificar o controlador que gerencie o mensagem de alerta confiado da violação da política AP segundo as indicações desta imagem:

Informações Relacionadas

- Manual de configuração do controlador de LAN do Cisco Wireless, liberação 5.2 - Permitindo

a detecção do Access point do vermelho em grupos RF
- Manual de configuração do controlador de LAN do Cisco Wireless, liberação 4.0 - Configurando soluções da Segurança
- Detecção desonesto sob redes Wireless unificadas
- Projeto e guia de distribuição do telefone de SpectraLink
- Exemplo de Configuração de Conexão de LAN Wireless Básica
- Conectividade deTroubleshooting em uma Rede Wireless LAN
- Autenticação em exemplos de configuração dos controladores do Wireless LAN
- Suporte Técnico e Documentação - Cisco Systems