Exemplo de configuração do filtro ACL do ponto de acesso

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Convenções
Informações de Apoio
Configurar
Filtros usando lista de acesso padrão
Filtros usando listas de acesso extendida
Filtros usando ACL com base em MAC
Filtros usando ACL com base no período
Verificar
Troubleshooting
Informações Relacionadas

Introdução

Este documento explica como configurar os filtros com base na lista de controle de acesso (ACL) em Pontos de Acesso (APs) do Cisco Aironet usando a interface de linha de comando (CLI).

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento básico destes assuntos:

- A configuração de uma conexão Wireless com uso de Aironet AP e um adaptador cliente do a/b/g do 802.11 de Aironet
- ACL

Componentes Utilizados

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

- 1200 Series AP de Aironet que executa o Software Release 12.3(7)JA1 de Cisco IOS®
- Adaptador cliente de Aironet 802.11a/b/g

- Software Release 2.5 do utilitário de Desktop de Aironet (ADU)

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

Convenções

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

Informações de Apoio

Você pode usar filtros em AP para executar estas tarefas:

- Restrinja o acesso à rede do Wireless LAN (WLAN)
- Forneça uma camada adicional de segurança Wireless

Você pode usar tipos diferentes de filtros ao filtrar tráfego baseado sobre:

- Protocolos específicos
- MAC address do dispositivo do cliente
- Endereço IP de Um ou Mais Servidores Cisco ICM NT do dispositivo do cliente

Você pode igualmente permitir filtros de restringir o tráfego dos usuários no LAN ligado com fio. Os filtros do endereço IP de Um ou Mais Servidores Cisco ICM NT e do MAC address permitem ou recusam a transmissão do unicast e dos pacotes de transmissão múltipla que são enviados a ou dos endereços específicos IP ou MAC.

Os filtros com base nos protocolos fornecem uma maneira mais granulada de restringir o acesso aos protocolos específicos através dos Ethernet e das interfaces de rádio do AP. Você pode usar qualquer um destes métodos para configurar os filtros nos AP:

- Web GUI
- CLI

Este documento explica como usar ACL para configurar filtros com o CLI. Para obter informações sobre de como configurar filtros com o GUI, refira configurar filtros.

Você pode usar o CLI para configurar estes tipos de filtros ACL-baseados no AP:

- Filtros que usam o padrão ACL
- Filtros que usam ACL extendido
- Filtros que usam o MAC address ACL

Nota: O número de entradas permitidas em um ACL é limitado pelo CPU do AP. Se há um grande número entradas a adicionar a um ACL, por exemplo ao filtrar uma lista de endereços MAC para os clientes, use um interruptor na rede que pode executar a tarefa.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste

documento.

Use a ferramenta Command Lookup Tool (apenas para clientes registrados) para obter mais informações sobre os comandos usados neste documento.

Todas as configurações neste documento supõem que uma conexão Wireless está estabelecida já. Este documento focaliza somente em como usar o CLI a fim configurar filtros. Se você não tem uma conexão da tecnologia Wireless básica, refira o exemplo de configuração da conexão de LAN da tecnologia Wireless básica.

Filtros usando lista de acesso padrão

Você pode usar o padrão ACL para permitir ou recusar a entrada dos dispositivos do cliente na rede de WLAN baseada no endereço IP de Um ou Mais Servidores Cisco ICM NT do cliente. O padrão ACL compara o endereço de origem dos pacotes IP aos endereços que são configurados no tráfego de controle ACL. Este tipo de ACL pode ser referido como um IP ACL com base em endereço da fonte.

O formato de sintaxe de comando de um padrão ACL é *access-list-number da* **lista de acesso {licença | negue}** {*IP address do* **host |** *widlcard de origem fonte-IP* **| alguns}**.

No Software Release 12.3(7)JA de Cisco IOS®, o número ACL pode ser qualquer número de 1 a 99. O padrão ACL pode igualmente usar o intervalo estendido de 1300 a 1999. Estes números adicionais são IP expandido ACL.

Quando um padrão ACL é configurado para negar o acesso a um cliente, o cliente ainda associa ao AP. Contudo, não há nenhuma comunicação de dados entre o AP e o cliente.

Este exemplo mostra um padrão ACL que seja configurado para filtrar o endereço IP cliente 10.0.0.2 da relação wireless (relação radio0). O endereço IP de Um ou Mais Servidores Cisco ICM NT do AP é 10.0.0.1.

Depois que isto é feito, o cliente com endereço IP 10.0.0.2 não pode enviar ou receber dados através da rede de WLAN mesmo que o cliente seja associado ao AP.

Termine estas etapas a fim criar um padrão ACL com o CLI:

1. Entre ao AP com o CLI.Use a porta de Console ou use o telnet a fim alcançar o ACL através da interface Ethernet ou da relação wireless.
2. Incorpore o modo de configuração global no AP:`AP#configure terminal`
3. Emita estes comandos a fim criar o padrão ACL:`AP<config>#access-list 25 deny host 10.0.0.2 !--- Create a standard ACL 25 to deny access to the !--- client with IP address 10.0.0.2. AP<config>#access-list 25 permit any !--- Allow all other hosts to access the network.`
4. Emita estes comandos a fim aplicar este ACL à interface de rádio:`AP<config>#interface Dot11Radio 0 AP<config-if>#ip access-group 25 in !--- Apply the standard ACL to the radio interface 0.`

Você pode igualmente criar um ACL nomeado padrão (NACL). O NACL usa um nome em vez de um número para definir o ACL.

`AP#configure terminal AP<config>#ip access-list standard name AP<config>#permit | deny {host ip-address | source-ip [source-wildcard] | any} log`

Emita estes comandos a fim usar NACLs padrão para negar o acesso de 10.0.0.2 do host à rede

de WLAN:

```
AP#configure terminal AP<config>#ip access-list standard TEST !--- Create a standard NACL TEST.
AP<config-std-nacl>#deny host 10.0.0.2 !--- Disallow the client with IP address 10.0.0.2 !---
access to the network. AP<config-std-nacl>#permit any !--- Allow all other hosts to access the
network. AP<config-std-nacl>#exit !--- Exit to global configuration mode. AP<config>#interface
Dot11Radio 0 !--- Enter dot11 radio0 interface mode. AP<config-if>#ip access-group TEST in !---
Apply the standard NACL to the radio interface.
```

Filtros usando listas de acesso extendida

Os ACL extendido comparam os endereços de rementente e destinatário dos pacotes IP aos endereços que são configurados no tráfego de controle ACL. Os ACL extendido igualmente fornecem meios ao filtrar tráfego baseado em protocolos específicos. Isto fornece um controle mais granulado para a aplicação dos filtros em uma rede de WLAN.

Os ACL extendido permitem que um cliente alcance alguns recursos na rede quando o cliente não puder alcançar os outros recursos. Por exemplo, você pode executar um filtro que permita o DHCP e o tráfego do telnet ao cliente quando restringir todo tráfego restante.

Esta é a sintaxe de comando dos ACL extendido:

Nota: Este comando é envolvido a quatro linhas devido às considerações espaciais.

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny | permit} protocol
source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [log |
log-input] [time-range time-range-name]
```

No Cisco IOS Software Release 12.3(7)JA, os ACL extendido podem usar números na escala de 100 a 199. Os ACL extendido podem igualmente usar números na escala de 2000 a 2699. Esta é a escala expandida para ACL extendido.

Nota: A palavra-chave do **log na** extremidade das entradas ACL individuais mostra:

- Número e nome ACL
- Se o pacote esteve permitido ou negado
- Informação do específico de porta

Os ACL extendido podem igualmente usar nomes em vez dos números. Esta é a sintaxe para criar NACLs prolongado:

```
ip access-list extended name {deny | permit} protocol source source-wildcard destination
destination-wildcard [precedence precedence] [tos tos] [log | log-input] [time-range time-range-
name]
```

Este exemplo de configuração usa NACLs prolongado. A exigência é que o NACL prolongado deve permitir o acesso do telnet aos clientes. Você deve restringir todos protocolos restantes na rede de WLAN. Também, os clientes usam o DHCP a fim obter o endereço IP de Um ou Mais Servidores Cisco ICM NT. Você deve criar um ACL extendido isso:

- Permite o tráfego DHCP e de telnet
- Nega todos tipos de tráfego restantes

Uma vez que este ACL extendido é aplicado à interface de rádio, os clientes associam com o AP e obtêm um endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor DHCP. Os clientes podem igualmente usar o telnet. Todos tipos de tráfego restantes são negados.

Termine estas etapas a fim criar um ACL extendido no AP:

1. Entre ao AP com o CLI.Use a porta de Console ou o telnet a fim alcançar o ACL através da interface Ethernet ou da relação wireless.
2. Incorpore o modo de configuração global no AP:`AP#configure terminal`
3. Emita estes comandos a fim criar o ACL extendido:`AP<config>#ip access-list extended Allow_DHCP_Telnet !--- Create an extended ACL Allow_DHCP_Telnet. AP<config-extd-nacl>#permit tcp any any eq telnet !--- Allow Telnet traffic. AP<config-extd-nacl>#permit udp any any eq bootpc !--- Allow DHCP traffic. AP<config-extd-nacl>#permit udp any any eq bootps !--- Allow DHCP traffic. AP<config-extd-nacl>#deny ip any any !--- Deny all other traffic types. AP<config-extd-nacl>#exit !--- Return to global configuration mode.`
4. Emita estes comandos a fim aplicar o ACL à interface de rádio:`AP<config>#interface Dot11Radio 0 AP<config-if>#ip access-group Allow_DHCP_Telnet in !--- Apply the extended ACL Allow_DHCP_Telnet !--- to the radio0 interface.`

Filtros usando ACL com base em MAC

Você pode usar filtros com base em endereço MAC a fim filtrar os dispositivos do cliente baseados no MAC address codificado duro. Quando um cliente é negado o acesso através de um filtro com base em MAC, o cliente não pode associar com o AP. Os filtros do MAC address permitem ou recusam a transmissão do unicast e dos pacotes de transmissão múltipla enviados de ou endereçados aos endereços específicos MAC.

Esta é a sintaxe de comando para criar um MAC ACL com base em endereço no AP:

Nota: Este comando foi envolvido a duas linhas devido às considerações espaciais.

access-list *access-list-number* **{permit | deny}** *48-bit-hardware-address 48-bit-hardware-address-mask*

No Cisco IOS Software Release 12.3(7)JA, o MAC address ACL pode usar números na escala de 700 a 799 como o número ACL. Podem igualmente usar números na escala expandida de 1100 a 1199.

Este exemplo ilustra como configurar um filtro com base em MAC com o CLI, a fim filtrar o cliente com um MAC address de **0040.96a5.b5d4**:

1. Início de uma sessão ao AP com o CLI.Use a porta de Console ou o telnet a fim alcançar o ACL através da interface Ethernet ou da relação wireless.
2. Incorpore o modo de configuração global no AP CLI:`AP#configure terminal`
3. Crie um MAC address ACL 700.Este ACL não permite que o cliente 0040.96a5.b5d4 associe com o AP.
   `access-list 700 deny 0040.96a5.b5d4 0000.0000.0000 !--- This ACL denies all traffic to and from !--- the client with MAC address 0040.96a5.b5d4.`
4. Emita este comando a fim aplicar este ACL com base em MAC à interface de rádio:
   `dot11 association mac-list 700 !--- Apply the MAC-based ACL.`

Depois que você configura este filtro no AP, o cliente com este MAC address, que foi associado previamente ao AP, está dissociado. O console AP envia esta mensagem:

```
AccessPoint# *Mar 1 01:42:36.743: %DOT11-6-DISASSOC: Interface
 Dot11Radio0, Deauthenticating Station 0040.96a5.b5d4
```

Filtros usando ACL com base no período

Os ACL com base no período são os ACL que podem ser permitidos ou desabilitado por um período de tempo específico. Esta capacidade fornece o vigor e a flexibilidade definir as políticas do controle de acesso essas um ou outro determinados tipos do permit or deny do tráfego.

Este exemplo ilustra como configurar um ACL baseado no período com o CLI, onde a conexão Telnet é permitida do interior à rede externa em dias úteis durante horas de negócio:

Nota: Um ACL baseado no período pode ser definido na porta de Ethernet rápida ou na porta de rádio de Aironet AP, com base em suas exigências. É aplicado nunca no Bridge Group Virtual Interface (BVI).

1. Início de uma sessão ao AP com o CLI.Use a porta de Console ou o telnet a fim alcançar o ACL através da interface Ethernet ou da relação wireless.
2. Incorpore o modo de configuração global no AP CLI:`AP#configure terminal`
3. Crie um intervalo de tempo. Para fazer isto, emita este comando no modo de configuração global:`AP<config>#time-range Test !--- Create a time-range with name Test. AP(config-time-range)# periodic weekdays 7:00 to 19:00 !--- Allows access to users during weekdays from 7:00 to 19:00 hrs.`
4. Crie um ACL 101:`AP<config># ip access-list extended 101 AP<config-ext-nacl>#permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq telnet time-range Test !--- This ACL permits Telnet traffic to and from !--- the network for the specified time-range Test.` Este ACL permite uma sessão de Telnet ao AP em dias úteis.
5. Emita este comando a fim aplicar este ACL baseado no período à interface Ethernet: `interface Ethernet0/0 ip address 10.1.1.1 255.255.255.0 ip access-group 101 in !--- Apply the time-based ACL.`

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

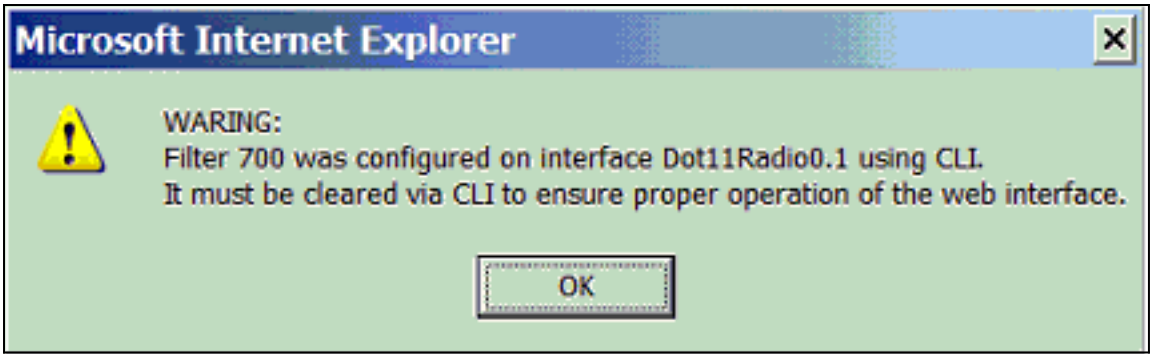
Use esta seção para resolver problemas de configuração.

Termine estas etapas a fim remover um ACL de uma relação:

1. Entre no modo de configuração da interface.
2. Entre **não** na frente do **comando ip access-group**, como este exemplo mostra: `interface interface no ip access-group {access-list-name | access-list-number} {in | out}`

Você pode igualmente usar o *nome da* **lista de acesso da mostra |** *comando number* a fim pesquisar defeitos sua configuração. **O comando show ip access-list** fornece um contagem de pacote de informação que as mostras que a entrada ACL está sendo batida.

Evite o uso do CLI e das interfaces do navegador da Web configurar o dispositivo Wireless. Se você configura o dispositivo Wireless com o CLI, a interface do navegador da Web pode indicar uma interpretação impreciso da configuração. Contudo, a irregularidade não significa necessariamente que o dispositivo Wireless está desconfigurado. Por exemplo, se você configura ACL com o CLI, a interface do navegador da Web pode indicar esta mensagem:



Se você vê esta mensagem, use o CLI a fim suprimir dos ACL e usar a interface do navegador da Web para reconfigurá-los.

Informações Relacionadas

- Configurando filtros
- Página de Suporte Wireless
- Suporte Técnico e Documentação - Cisco Systems