Exemplo de configuração do filtro ACL do ponto de acesso

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Conventions](#)
[Informações de Apoio](#)
[Configurar](#)
[Filtros usando listas de acesso padrão](#)
[Filtros que usam listas de acesso estendidas](#)
[Filtros usando ACLs baseadas em MAC](#)
[Filtros usando ACLs baseadas em tempo](#)
[Verificar](#)
[Troubleshoot](#)
[Informações Relacionadas](#)

Introduction

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).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento básico sobre estes tópicos:

- A configuração de uma conexão sem fio com o uso de um AP Aironet e um Adaptador de Cliente Aironet 802.11 a/b/g
- ACLs

Componentes Utilizados

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

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

- Software Aironet Desktop Utility (ADU) versão 2.5

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. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Informações de Apoio

Você pode usar filtros em APs para executar estas tarefas:

- Restringir o acesso à rede LAN sem fio (WLAN)
- Forneça uma camada adicional de segurança sem fio

Você pode usar diferentes tipos de filtros para filtrar o tráfego com base em:

- Protocolos específicos
- Endereço MAC do dispositivo cliente
- Endereço IP do dispositivo cliente

Você também pode ativar filtros para restringir o tráfego dos usuários na LAN com fio. Os filtros de endereços IP e MAC permitem ou não permitem o encaminhamento de pacotes unicast e multicast enviados de ou para endereços IP ou MAC específicos.

Os filtros baseados em protocolo fornecem uma maneira mais granular de restringir o acesso a protocolos específicos através das interfaces Ethernet e de rádio do AP. Você pode usar qualquer um destes métodos para configurar os filtros nos APs:

- GUI da Web
- CLI

Este documento explica como usar ACLs para configurar filtros através da CLI. Para obter informações sobre como configurar filtros através da GUI, consulte Configuração de Filtros.

Você pode usar a CLI para configurar esses tipos de filtros baseados em ACL no AP:

- Filtros que usam ACLs padrão
- Filtros que usam ACLs estendidas
- Filtros que usam ACLs de endereços MAC

Observação: o número de entradas permitidas em uma ACL é limitado pela CPU do AP. Se houver um grande número de entradas a serem adicionadas a uma ACL, por exemplo, ao filtrar uma lista de endereços MAC para os clientes, use um switch na rede que possa 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 presumem que uma conexão sem fio já está estabelecida. Este documento concentra-se apenas em como usar a CLI para configurar filtros. Se você não tiver uma conexão sem fio básica, consulte Exemplo de Configuração Básica de Conexão de LAN Sem Fio.

Filtros usando listas de acesso padrão

Você pode usar ACLs padrão para permitir ou não permitir a entrada de dispositivos clientes na rede WLAN com base no endereço IP do cliente. As ACLs padrão comparam o endereço de origem dos pacotes IP com os endereços configurados na ACL para controlar o tráfego. Esse tipo de ACL pode ser chamado de ACL baseada em endereço IP origem.

O formato de sintaxe de comando de uma ACL padrão é **access-list access-list-number {permit | deny} {host *ip-address* | *source-ip source-wildcard* | qualquer**.

No Cisco IOS® Software Release 12.3(7)JA, o número da ACL pode ser qualquer número de 1 a 99. As ACLs padrão também podem usar o intervalo estendido de 1300 a 1999. Esses números adicionais são ACLs IP expandidas.

Quando uma ACL padrão é configurada para negar acesso a um cliente, o cliente ainda se associa ao AP. No entanto, não há comunicação de dados entre o AP e o cliente.

Este exemplo mostra uma ACL padrão configurada para filtrar o endereço IP do cliente 10.0.0.2 da interface sem fio (interface radio0). O endereço IP do AP é 10.0.0.1.

Depois disso, o cliente com endereço IP 10.0.0.2 não pode enviar ou receber dados pela rede WLAN mesmo que o cliente esteja associado ao AP.

Conclua estes passos para criar uma ACL padrão através da CLI:

1. Faça login no AP através da CLI.Use a porta do console ou use Telnet para acessar a ACL através da interface Ethernet ou da interface sem fio.
2. Entre no modo de configuração global no AP:
   ```
   AP#configure terminal
   ```
3. Execute estes comandos para criar a ACL padrão:
   ```
   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. Execute estes comandos para aplicar esta 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 também pode criar uma ACL nomeada padrão (NACL). O NACL usa um nome em vez de um número para definir a ACL.

```
AP#configure terminal
AP<config>#ip access-list standard name
```

```
AP<config>#permit | deny {host ip-address | source-ip [source-wildcard] | any} log
```

Execute estes comandos para usar NACLs padrão para negar ao host 10.0.0.2 o acesso à rede 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 que usam listas de acesso estendidas

As ACLs estendidas comparam os endereços origem e destino dos pacotes IP com os endereços configurados na ACL para controlar o tráfego. As ACLs estendidas também fornecem um meio de filtrar o tráfego com base em protocolos específicos. Isso fornece um controle mais granular para a implementação de filtros em uma rede WLAN.

As ACLs estendidas permitem que um cliente acesse alguns recursos na rede enquanto ele não pode acessar os outros recursos. Por exemplo, você pode implementar um filtro que permita o tráfego DHCP e Telnet para o cliente enquanto ele restringe todo o tráfego restante.

Esta é a sintaxe do comando das ACLs estendidas:

Observação: este comando é empacotado para quatro linhas devido a 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, as ACLs estendidas podem usar números na faixa de 100 a 199. As ACLs estendidas também podem usar números no intervalo de 2000 a 2699. Este é o intervalo expandido para ACLs estendidas.

Observação: a palavra-chave **log** no final das entradas ACL individuais mostra:

- Número e nome da ACL
- Se o pacote foi permitido ou negado
- Informações específicas da porta

As ACLs estendidas também podem usar nomes em vez de números. Esta é a sintaxe para criar NACLs estendidas:

```
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 estendidas. O requisito é que a NACL estendida deve permitir acesso Telnet aos clientes. Você deve restringir todos os outros protocolos na rede WLAN. Além disso, os clientes usam DHCP para obter o endereço IP. Você deve criar uma ACL estendida que:

- Permite tráfego DHCP e Telnet
- Nega todos os outros tipos de tráfego

Quando essa ACL estendida é aplicada à interface de rádio, os clientes se associam ao AP e obtêm um endereço IP do servidor DHCP. Os clientes também podem usar Telnet. Todos os outros tipos de tráfego são negados.

Conclua estes passos para criar uma ACL estendida no AP:

1. Faça login no AP através da CLI.Use a porta do console ou Telnet para acessar a ACL através da interface Ethernet ou da interface sem fio.
2. Entre no modo de configuração global no AP:
   ```
   AP#configure terminal
   ```
3. Execute estes comandos para criar a ACL estendida:
   ```
   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. Execute estes comandos para aplicar a 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 ACLs baseadas em MAC

Você pode usar filtros baseados em endereços MAC para filtrar dispositivos clientes com base no endereço MAC codificado. Quando um cliente tem acesso negado por meio de um filtro baseado em MAC, ele não pode se associar ao AP. Os filtros de endereços MAC permitem ou não permitem o encaminhamento de pacotes unicast e multicast enviados de ou endereçados a endereços MAC específicos.

Esta é a sintaxe do comando para criar uma ACL baseada em endereço MAC no AP:

Observação: este comando foi empacotado para duas linhas devido a 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, as ACLs de endereços MAC podem usar números no

intervalo de 700 a 799 como o número da ACL. Eles também podem usar números na faixa expandida de 1100 a 1199.

Este exemplo ilustra como configurar um filtro baseado em MAC através da CLI, para filtrar o cliente com um endereço MAC de **0040.96a5.b5d4**:

1. Faça login no AP através da CLI.Use a porta do console ou Telnet para acessar a ACL através da interface Ethernet ou da interface sem fio.
2. Entre no modo de configuração global na CLI do AP:
   ```
   AP#configure terminal
   ```
3. Crie um endereço MAC ACL 700.Essa ACL não permite que o cliente 0040.96a5.b5d4 se associe ao 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 para aplicar esta ACL baseada em MAC à interface de rádio:

   ```
   dot11 association mac-list 700

   !--- Apply the MAC-based ACL.
   ```

Depois de configurar esse filtro no AP, o cliente com esse endereço MAC, que foi associado anteriormente ao AP, é desassociado. O console do AP envia esta mensagem:

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

Filtros usando ACLs baseadas em tempo

As ACLs com base no tempo são ACLs que podem ser ativadas ou desativadas por um período de tempo específico. Esse recurso oferece robustez e flexibilidade para definir políticas de controle de acesso que permitem ou negam certos tipos de tráfego.

Este exemplo ilustra como configurar uma ACL com base no tempo através da CLI, onde a conexão Telnet é permitida de dentro para fora da rede nos dias úteis durante o horário comercial:

Observação: uma ACL baseada em tempo pode ser definida na porta Fast Ethernet ou na porta de rádio do AP Aironet, com base em seus requisitos. Ele nunca é aplicado na BVI (Bridge Group Virtual Interface, interface virtual do grupo de bridge).

1. Faça login no AP através da CLI.Use a porta do console ou Telnet para acessar a ACL através da interface Ethernet ou da interface sem fio.
2. Entre no modo de configuração global na CLI do AP:
   ```
   AP#configure terminal
   ```
3. Crie um intervalo de tempo. Para fazer isso, 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. Criar uma 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.
```

   Essa ACL permite uma sessão Telnet para o AP em dias úteis.
5. Execute este comando para aplicar esta ACL baseada em tempo 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.

Troubleshoot

Use esta seção para resolver problemas de configuração.

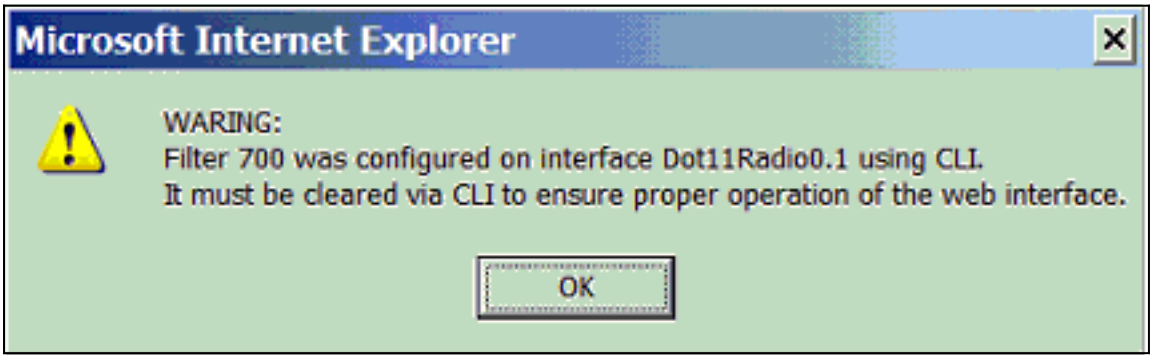
Conclua estes passos para remover uma ACL de uma interface:

1. Entre no modo configuração de interface.
2. Digite **no** na frente do comando **ip access-group**, como mostrado neste exemplo:

```
interface interface
no ip access-group {access-list-name | access-list-number} {in | out}
```

Você também pode usar o *nome* ***show access-list | number*** para solucionar problemas de sua configuração. O comando **show ip access-list** fornece uma contagem de pacotes que mostra qual entrada da ACL está sendo atingida.

Evite o uso da CLI e das interfaces do navegador da Web para configurar o dispositivo sem fio. Se você configurar o dispositivo sem fio com a CLI, a interface do navegador da Web poderá exibir uma interpretação imprecisa da configuração. No entanto, a imprecisão não significa necessariamente que o dispositivo sem fio esteja configurado incorretamente. Por exemplo, se você configurar ACLs com a CLI, a interface do navegador da Web poderá exibir esta mensagem:



Se essa mensagem for exibida, use a CLI para excluir as ACLs e use a interface do navegador da Web para reconfigurá-las.

Informações Relacionadas

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