Ejemplo de Configuración de Filtro ACL de Punto de Acceso

Contenido

Introducción

Este documento explica cómo configurar filtros basados en Listas de control de acceso (ACL) en Cisco Aironet Access Points (AP) mediante la interfaz de línea de comandos (CLI).

Prerequisites

Requirements

Cisco recomienda que tenga conocimientos básicos sobre estos temas:

- La configuración de una conexión inalámbrica con el uso de un Aironet AP y un Aironet 802.11 a/b/g Client Adapter
- Listas de control de acceso (ACL)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Aironet 1200 Series AP que ejecuta Cisco IOS® Software Release 12.3(7)JA1

- Adaptador de clientes Aironet 802.11a/b/g
- Software Aironet Desktop Utility (ADU) versión 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.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

Puede utilizar filtros en los AP para realizar estas tareas:

- Restringir el acceso a la red LAN inalámbrica (WLAN)
- Proporcione una capa adicional de seguridad inalámbrica

Puede utilizar diferentes tipos de filtros para filtrar el tráfico en función de:

- Protocolos específicos
- Dirección MAC del dispositivo cliente
- Dirección IP del dispositivo cliente

También puede activar filtros para restringir el tráfico de los usuarios en la LAN por cable. Los filtros de dirección IP y dirección MAC permiten o no permitir el reenvío de paquetes unidifusión y multidifusión que se envían a o desde direcciones IP o MAC específicas.

Los filtros basados en protocolo proporcionan una manera más granular de restringir el acceso a protocolos específicos a través de las interfaces Ethernet y de radio del AP. Puede utilizar cualquiera de estos métodos para configurar los filtros en los AP:

- GUI web
- CLI

Este documento explica cómo utilizar las ACL para configurar filtros a través de la CLI. Para obtener información sobre cómo configurar filtros a través de la GUI, consulte Configuración de Filtros.

Puede utilizar la CLI para configurar estos tipos de filtros basados en ACL en el AP:

- Filtros que utilizan ACL estándar
- Filtros que utilizan ACL extendidas
- Filtros que utilizan ACL de dirección MAC

Nota: El número de entradas permitidas en una ACL está limitado por la CPU del AP. Si hay un gran número de entradas que agregar a una ACL, por ejemplo, al filtrar una lista de direcciones MAC para los clientes, utilice un switch en la red que pueda realizar la tarea.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este

documento.

Use la herramienta Command Lookup Tool (clientes registrados solamente) para encontrar más información sobre los comandos usados en este documento.

Todas las configuraciones de este documento suponen que ya se ha establecido una conexión inalámbrica. Este documento se centra solamente en cómo utilizar la CLI para configurar filtros. Si no tiene una conexión inalámbrica básica, consulte Ejemplo de Configuración de Conexión LAN Inalámbrica Básica.

Filtros mediante listas de acceso estándar

Puede utilizar ACL estándar para permitir o denegar la entrada de dispositivos cliente en la red WLAN en función de la dirección IP del cliente. Las ACL estándar comparan la dirección de origen de los paquetes IP con las direcciones configuradas en la ACL para controlar el tráfico. Este tipo de ACL se puede hacer referencia como una ACL basada en dirección IP de origen.

El formato de sintaxis del comando de una ACL estándar es **access-list access-list-number {permit | deny} {host *ip-address* | *source-ip source-wildcard* | cualquier}**.

En Cisco IOS® Software Release 12.3(7)JA, el número de ACL puede ser cualquier número entre 1 y 99. Las ACL estándar también pueden utilizar el rango extendido de 1300 a 1999. Estos números adicionales son ACL IP ampliadas.

Cuando se configura una ACL estándar para denegar el acceso a un cliente, el cliente todavía se asocia al AP. Sin embargo, no hay comunicación de datos entre el AP y el cliente.

Este ejemplo muestra una ACL estándar configurada para filtrar la dirección IP del cliente 10.0.0.2 desde la interfaz inalámbrica (interfaz radio0). La dirección IP del AP es 10.0.0.1.

Después de esto, el cliente con la dirección IP 10.0.0.2 no puede enviar ni recibir datos a través de la red WLAN aunque el cliente esté asociado con el AP.

Complete estos pasos para crear una ACL estándar a través de la CLI:

1. Inicie sesión en el AP a través de la CLI.Utilice el puerto de la consola o utilice Telnet para acceder a la ACL a través de la interfaz Ethernet o la interfaz inalámbrica.
2. Ingrese al modo de configuración global en el AP:
   ```
   AP#configure terminal
   ```
3. Ejecute estos comandos para crear la ACL estándar:
   ```
   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. Ejecute estos comandos para aplicar esta ACL a la interfaz de radio:
   ```
   AP<config>#interface Dot11Radio 0
   AP<config-if>#ip access-group 25 in
   !--- Apply the standard ACL to the radio interface 0.
   ```

También puede crear una ACL denominada estándar (NACL). La NACL utiliza un nombre en lugar de un número para definir la ACL.

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

Ejecute estos comandos para utilizar NACL estándar para denegar el acceso del host 10.0.0.2 a la red 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 utilizan listas de acceso extendidas

Las ACL extendidas comparan las direcciones de origen y destino de los paquetes IP con las direcciones configuradas en la ACL para controlar el tráfico. Las ACL extendidas también proporcionan un medio para filtrar el tráfico basado en protocolos específicos. Esto proporciona un control más granular para la implementación de filtros en una red WLAN.

Las ACL extendidas permiten que un cliente acceda a algunos recursos de la red mientras que el cliente no puede acceder a los otros recursos. Por ejemplo, puede implementar un filtro que permita el tráfico DHCP y Telnet al cliente mientras restringe el resto del tráfico.

Esta es la sintaxis del comando de las ACL extendidas:

Nota: Este comando se ajusta a cuatro líneas por consideraciones espaciales.

```
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]
```

En Cisco IOS Software Release 12.3(7)JA, las ACL extendidas pueden utilizar números en el rango de 100 a 199. Las ACL extendidas también pueden utilizar números en el rango de 2000 a 2699. Este es el rango ampliado para las ACL extendidas.

Nota: La palabra clave **log** al final de las entradas de ACL individuales muestra:

- número y nombre de ACL
- Si el paquete fue permitido o denegado
- Información específica del puerto

Las ACL extendidas también pueden utilizar nombres en lugar de números. Esta es la sintaxis para crear NACL extendidas:

```
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 ejemplo de configuración utiliza NACL extendidas. El requisito es que la NACL extendida debe permitir el acceso Telnet a los clientes. Debe restringir todos los demás protocolos en la red WLAN. Además, los clientes utilizan DHCP para obtener la dirección IP. Debe crear una ACL extendida que:

- Permite el tráfico DHCP y Telnet
- Niega todos los demás tipos de tráfico

Una vez que esta ACL extendida se aplica a la interfaz de radio, los clientes se asocian con el AP y obtienen una dirección IP del servidor DHCP. Los clientes también pueden utilizar Telnet. Se deniegan todos los demás tipos de tráfico.

Complete estos pasos para crear una ACL extendida en el AP:

1. Inicie sesión en el AP a través de la CLI.Utilice el puerto de consola o Telnet para acceder a la ACL a través de la interfaz Ethernet o la interfaz inalámbrica.
2. Ingrese al modo de configuración global en el AP:
   ```
   AP#configure terminal
   ```
3. Ejecute estos comandos para crear la ACL extendida:
   ```
   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. Ejecute estos comandos para aplicar la ACL a la interfaz de radio:
   ```
   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 que utilizan ACL basadas en MAC

Puede utilizar filtros basados en direcciones MAC para filtrar los dispositivos cliente según la dirección MAC codificada. Cuando a un cliente se le niega el acceso a través de un filtro basado en MAC, el cliente no puede asociarse con el AP. Los filtros de direcciones MAC permiten o no permitir el reenvío de paquetes unidifusión y multidifusión enviados desde o dirigidos a direcciones MAC específicas.

Esta es la sintaxis del comando para crear una ACL basada en dirección MAC en el AP:

Nota: Este comando se ha ajustado a dos líneas debido a consideraciones espaciales.

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

En Cisco IOS Software Release 12.3(7)JA, las ACL de dirección MAC pueden utilizar números en el rango de 700 a 799 como número de ACL. También pueden utilizar números en el rango ampliado de 1100 a 1199.

Este ejemplo ilustra cómo configurar un filtro basado en MAC a través de la CLI, para filtrar el cliente con una dirección MAC de **0040.96a5.b5d4**:

1. Inicie sesión en el AP a través de la CLI.Utilice el puerto de consola o Telnet para acceder a la ACL a través de la interfaz Ethernet o la interfaz inalámbrica.
2. Ingrese el modo de configuración global en la CLI de AP:
   ```
   AP#configure terminal
   ```
3. Cree una dirección MAC ACL 700.Esta ACL no permite que el cliente 0040.96a5.b5d4 se asocie con el 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. Ejecute este comando para aplicar esta ACL basada en MAC a la interfaz de radio:

   ```
   dot11 association mac-list 700

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

Después de configurar este filtro en el AP, el cliente con esta dirección MAC, que previamente estaba asociado al AP, se desasocia. La consola AP envía este mensaje:

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

Filtros que utilizan ACL basadas en tiempo

Las ACL basadas en tiempo son ACL que se pueden habilitar o inhabilitar durante un período de tiempo específico. Esta capacidad proporciona solidez y flexibilidad para definir políticas de control de acceso que permiten o niegan determinados tipos de tráfico.

Este ejemplo ilustra cómo configurar una ACL basada en tiempo a través de la CLI, donde se permite la conexión Telnet desde el interior a la red externa en días laborables durante el horario laboral:

Nota: Una ACL basada en tiempo se puede definir en el puerto Fast Ethernet o en el puerto de radio del AP Aironet, según sus requerimientos. Nunca se aplica en la interfaz virtual de grupo de puentes (BVI).

1. Inicie sesión en el AP a través de la CLI.Utilice el puerto de consola o Telnet para acceder a la ACL a través de la interfaz Ethernet o la interfaz inalámbrica.
2. Ingrese el modo de configuración global en la CLI de AP:
   ```
   AP#configure terminal
   ```
3. Cree un rango de tiempo. Para ello, ejecute este comando en el modo de configuración 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. Cree una 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.
```

   Esta ACL permite una sesión Telnet al AP los días laborables.

5. Ejecute este comando para aplicar esta ACL basada en tiempo a la interfaz Ethernet:

```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in

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

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Use esta sección para resolver problemas de configuración.

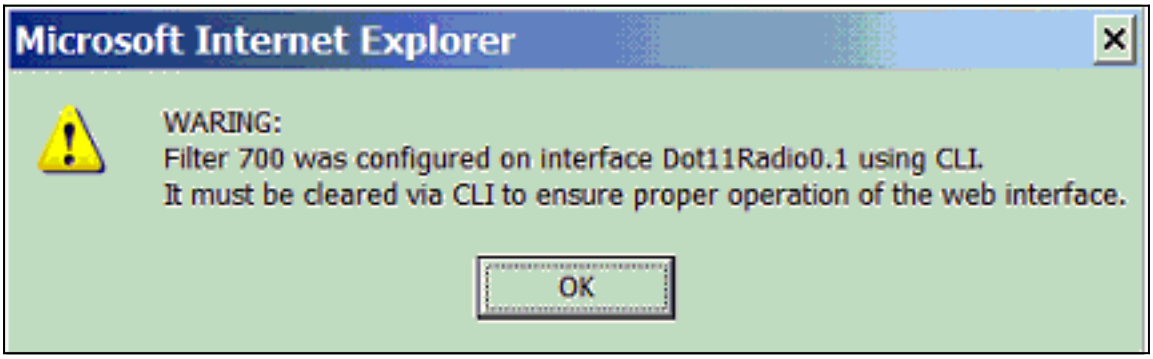
Complete estos pasos para quitar una ACL de una interfaz:

1. Vaya al modo de configuración de la interfaz.
2. Ingrese **no** delante del **comando ip access-group**, como muestra este ejemplo:

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

También puede utilizar el *nombre* ***show access-list | number*** para resolver problemas de su configuración. El comando **show ip access-list** proporciona un conteo de paquetes que muestra qué entrada ACL se está ejecutando.

Evite el uso de las interfaces CLI y del navegador web para configurar el dispositivo inalámbrico. Si configura el dispositivo inalámbrico con la CLI, la interfaz del navegador web puede mostrar una interpretación incorrecta de la configuración. Sin embargo, la inexactitud no significa necesariamente que el dispositivo inalámbrico esté mal configurado. Por ejemplo, si configura las ACL con la CLI, la interfaz del navegador web puede mostrar este mensaje:



Si ve este mensaje, use la CLI para eliminar las ACL y utilice la interfaz del navegador web para reconfigurarlas.

Información Relacionada

- Configuración de filtros
- Página de Soporte de Red Inalámbrica
- Soporte Técnico y Documentación - Cisco Systems