Ejemplo de Configuración de Filtro ACL de Punto de Acceso

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Convenciones
Antecedentes
Configurar
Filtros usando las listas de acceso estándar
Filtros usando las listas de acceso ampliadas
Filtros usando los ACL MAC basados
Filtros usando el time basado ACL
Verificación
Troubleshooting
Información Relacionada

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).

prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento básico de estos temas:

- La configuración de una conexión de red inalámbrica con el uso de un Aironet AP y de un adaptador del cliente del a/b/g del 802.11 del Aironet
- ACL

Componentes Utilizados

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

- 1200 Series AP del Aironet que funcionan con el Software Release 12.3(7)JA1 de Cisco

IOS®
- Adaptador del cliente del Aironet 802.11a/b/g
- Utilidad Aironet Desktop Software Release 2.5 (ADU)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

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

Antecedentes

Usted puede utilizar los filtros en los AP para realizar estas tareas:

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

Usted puede utilizar diversos tipos de filtros al filtrar tráfico basado encendido:

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

Usted puede también permitir a los filtros para restringir el tráfico de los usuarios en el LAN cableado. Los filtros de la dirección IP y de la dirección MAC permiten o rechazan la expedición del unicast y de los paquetes de multidifusión que se envían a o desde el IP o las direcciones MAC específico.

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

- Red GUI
- CLI

Este documento explica cómo utilizar los ACL para configurar los filtros con el CLI. Para la información sobre cómo configurar los filtros con el GUI, refiera a configurar los filtros.

Usted puede utilizar el CLI para configurar estos tipos de filtros ACL-basados en el AP:

- Filtros que utilizan los ACL estándar
- Filtros que utilizan los ACL ampliados
- Filtros que utilizan la dirección MAC ACL

Nota: El número de entradas permitidas en un ACL es limitado por el CPU del AP. Si hay un gran número de entradas a agregar a un ACL, por ejemplo al filtrar una lista de direcciones MAC para los clientes, utilice un Switch en la red que puede 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 en este documento asumen que una conexión de red inalámbrica está establecida ya. Este documento se centra solamente en cómo utilizar el CLI para configurar los filtros. Si usted no tiene una conexión de los elementos básicos de red inalámbrica, refiera al ejemplo de configuración de la conexión LAN de los elementos básicos de red inalámbrica.

Filtros usando las listas de acceso estándar

Usted puede utilizar los ACL estándar para permitir o para rechazar la entrada de los dispositivos del cliente en la red WLAN basada en la dirección IP del cliente. Los ACL estándar comparan a la dirección de origen de los paquetes del IP a los direccionamientos que se configuran en el tráfico de control ACL para. Este tipo de ACL puede ser referido como direccionamiento basado ACL IP de la fuente.

El formato de sintaxis del comando de una ACL estándar es **access-list access-list-number {permit | niegue} {***IP address del* **host |** *source comodín fuente-IP* **| ningunos}**.

En el Software Release 12.3(7)JA de Cisco IOS®, el número ACL puede ser cualquier número a partir de la 1 a 99. Los ACL estándar pueden también utilizar el alcance extendido de 1300 a 1999. Estos números adicionales son IP ampliado ACL.

Cuando un ACL estándar se configura para negar 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 un ACL estándar que se configure para filtrar el dirección IP del cliente 10.0.0.2 de la interfaz inalámbrica (interfaz radio0). La dirección IP del AP es 10.0.0.1.

Después de que se haga esto, el cliente con la dirección IP 10.0.0.2 no puede enviar o recibir los datos a través de la red WLAN aunque asocian al cliente al AP.

Complete estos pasos para crear un ACL estándar con el CLI:

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

Usted puede también crear un estándar ACL mencionado (NACL). El NACL utiliza un nombre en vez de un número para definir el ACL.

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

Publique estos comandos para utilizar NACLs estándar para negar el acceso de 10.0.0.2 del host

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 usando las listas de acceso ampliadas

Los ACL ampliados comparan a las direcciones de origen y de destino de los paquetes del IP a los direccionamientos que se configuran en el tráfico de control ACL para. Los ACL ampliados también proporcionan los medios al filtrar tráfico basado en los protocolos específicos. Esto proporciona un control más granular para la implementación de los filtros en una red WLAN.

Los ACL ampliados permiten que un cliente acceda algunos recursos en la red mientras que el cliente no puede acceder los otros recursos. Por ejemplo, usted puede implementar un filtro que permita el DHCP y el tráfico telnet al cliente mientras que restringe el resto del tráfico.

Ésta es la sintaxis de los comandos de los ACL ampliados:

Nota: Este comando se envuelve a cuatro líneas debido a las 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 el Cisco IOS Software Release 12.3(7)JA, los ACL ampliados pueden utilizar los números en el rango de 100 a 199. Los ACL ampliados pueden también utilizar los números en el rango de 2000 a 2699. Éste es el rango ampliado para los ACL ampliados.

Nota: La palabra clave del **registro** en el extremo de las entradas ACL individuales muestra:

- Número y nombre ACL
- Si el paquete fue permitido o negado
- Información del específico portuario

Los ACL ampliados pueden también utilizar los nombres en vez de los números. Éste es el sintaxis para crear NACLs extendido:

```
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 NACLs extendido. El requisito es que el NACL extendido debe permitir el acceso de Telnet a los clientes. Usted debe restringir el resto de los protocolos en la red WLAN. También, los clientes utilizan el DHCP para conseguir la dirección IP. Usted debe crear un ACL ampliado eso:

- Permite el DHCP y el tráfico de Telnet
- Niega el resto de los tipos de tráfico

Una vez que este ACL ampliado se aplica a la interfaz radio, los clientes se asocian al AP y consiguen una dirección IP del servidor DHCP. Los clientes pueden también utilizar Telnet. Niegan el resto de los tipos de tráfico.

Complete estos pasos para crear un ACL ampliado en el AP:

1. Inicie sesión al AP con el CLI.Utilice el puerto de la consola o Telnet para acceder el ACL a través de la interfaz de Ethernet o de la interfaz inalámbrica.
2. Ingrese al modo de configuración global en el AP:`AP#configure terminal`
3. Publique estos comandos para crear el ACL ampliado:`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. Publique estos comandos para aplicar el ACL a la interfaz 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 usando los ACL MAC basados

Usted puede utilizar los filtros del direccionamiento basado MAC para filtrar los dispositivos del cliente basados en la dirección MAC cifrada dura. Cuando niegan un cliente el acceso a través de un filtro MAC basado, el cliente no puede asociarse al AP. Los filtros de la dirección MAC permiten o rechazan la expedición del unicast y de los paquetes de multidifusión enviados de o dirigidos a las direcciones MAC específicas.

Ésta es la sintaxis de los comandos para crear un direccionamiento basado ACL MAC en el AP:

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

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

En el Cisco IOS Software Release 12.3(7)JA, la dirección MAC ACL puede utilizar los números en el rango de 700 a 799 como el número ACL. Pueden también utilizar los números en el rango ampliado de 1100 a 1199.

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

1. Login al AP con el CLI.Utilice el puerto de la consola o Telnet para acceder el ACL a través de la interfaz de Ethernet o de la interfaz inalámbrica.
2. Ingrese al modo de configuración global en el AP CLI:`AP#configure terminal`
3. Cree una dirección MAC ACL 700.Este ACL no permite que el cliente 0040.96a5.b5d4 se asocie al 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. Publique este comando para aplicar este ACL MAC basado a la interfaz radio:
   `dot11 association mac-list 700 !--- Apply the MAC-based ACL.`

Después de que usted configure este filtro en el AP, desasocian al cliente con esta dirección MAC, que fue asociada previamente al AP. La consola AP envía este mensaje:

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

Filtros usando el time basado ACL

El time basado ACL es los ACL que se pueden habilitar o inhabilitar por un período de tiempo específico. Esta capacidad proporciona la robustez y la flexibilidad de definir las directivas del control de acceso esas cualquier ciertas clases del permit or deny de tráfico.

Este ejemplo ilustra cómo configurar un ACL basado en la hora con el CLI, donde la conexión Telnet se permite del interior a la red externa el los días laborables durante las horas hábiles:

Nota: Un ACL basado en la hora se puede definir en el puerto Fast Ethernet o en el puerto de radio del Aironet AP, sobre la base de sus requisitos. Nunca se aplica en el (BVI) del Interfaz Virtual de Bridge Group.

1. Login al AP con el CLI.Utilice el puerto de la consola o Telnet para acceder el ACL a través de la interfaz de Ethernet o de la interfaz inalámbrica.
2. Ingrese al modo de configuración global en el AP CLI:`AP#configure terminal`
3. Cree un rango de tiempo. Para hacer esto, publique 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 un 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 a una sesión telnet al AP el los días laborables.
5. Publique este comando para aplicar este ACL basado en la hora a la interfaz de 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.

Troubleshooting

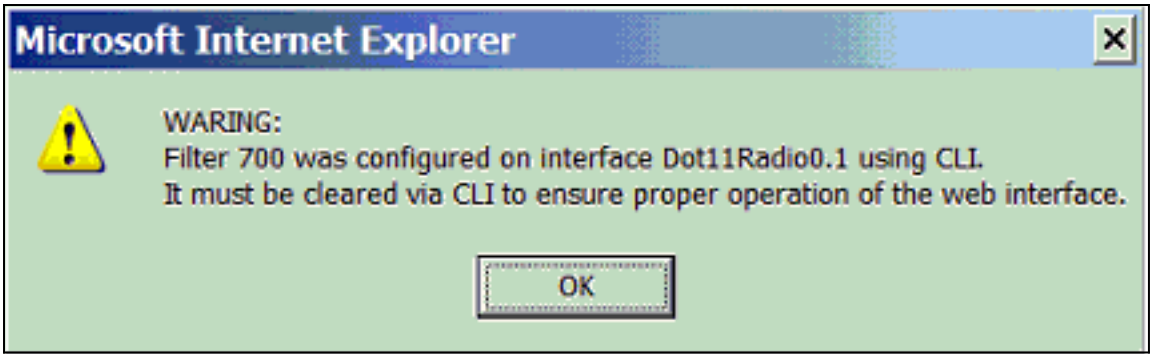
Use esta sección para resolver problemas de configuración.

Complete estos pasos para quitar un ACL de una interfaz:

1. Entre el modo de configuración de la interfaz.
2. Ingrese **no** delante del **comando ip access-group**, como este ejemplo muestra:
   interface *interface* **no ip access-group {***access-list-name* **|** *access-list-number***} {in | out}**

Usted puede también utilizar el *nombre de la* **lista de acceso de la demostración |** *comando number* para resolver problemas su configuración. **El comando show ip access-list** proporciona una cuenta de paquetes que las demostraciones que la entrada ACL se está golpeando.

Evite el uso del CLI y de las interfaces del buscador Web de configurar el dispositivo de red inalámbrica. Si usted configura el dispositivo de red inalámbrica con el CLI, la interfaz del buscador Web puede visualizar una interpretación inexacta de la configuración. Sin embargo, la inexactitud no significa necesariamente que el dispositivo de red inalámbrica está configurado mal. Por ejemplo, si usted configura los ACL con el CLI, la interfaz del buscador Web puede visualizar este mensaje:



Si usted ve este mensaje, utilice el CLI para borrar los ACL y utilizar la interfaz del buscador Web para configurarlos de nuevo.

Información Relacionada

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