Filtrado de Tráfico Destinado a WebUI de Dispositivos Cisco IOS XE Usando una Lista de Acceso

Contenido

Introducción

Este documento describe cómo configurar una lista de acceso (ACL) en un dispositivo Cisco IOS XE para filtrar el tráfico destinado a los servicios web.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento está escrito para dispositivos empresariales que ejecutan el software Cisco IOS® XE.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Background

Cuando se requiere que los servicios web HTTP estén habilitados para tener acceso a la interfaz de usuario web para administrar el dispositivo IOS XE o para el acceso de usuario invitado/autenticación web, se pueden implementar características de filtrado de tráfico para garantizar que solo las direcciones IP necesarias puedan acceder a la interfaz de usuario web y que los usuarios invitados puedan continuar incorporándose a la red.

Configurar

Configuración de la Clase de Acceso al Servicio HTTP

El método más sencillo para definir el acceso se puede realizar a través de la compatibilidad con la clase de acceso IP en el servidor Web HTTP. En este ejemplo de configuración, se permite la subred ipv4 192.168.10.0/24, se permite la subred ipv6 fd00::/64 y se deniega todo lo demás. Hay una negación implícita any any al final de la lista de acceso, pero también puede agregar una negación explícita any any si lo desea. En el caso del controlador de LAN inalámbrica C9800, asegúrese de considerar el acceso HTTP/HTTPS a la interfaz de administración inalámbrica (WMI) y al puerto de administración/servicio fuera de banda.

Ejemplo de IPv4

Paso 1. Configure una ACL estándar e incluya los dispositivos/subredes de confianza que pueden acceder al dispositivo Cisco IOS XE a través de HTTP/HTTPS

```
ip access-list standard restrict_ipv4_webui
permit 192.168.10.0 0.0.0.255
```

Nota: Esta ACL solo debe incluir subredes de confianza para tener acceso de administrador web al dispositivo IOS XE. Es decir, cualquier subred de invitado no debe incluirse en esta ACL. Al no incluir subredes de invitados, no se interrumpe la autenticación Web, el acceso de invitados ni la redirección Web.

Paso 2. Asigne la ACL estándar a la clase de acceso del servicio Web HTTP.

```
ip http access-class ipv4 restrict_ipv4_webui
```

Ejemplo de IPv6

Paso 1. Configure una ACL IPv6 para incluir los dispositivos/subredes de confianza que pueden acceder al dispositivo Cisco IOS XE a través de HTTP/HTTPS

```
ipv6 access-list restrict_ipv6_webui
permit fd00::/64 any
```

Paso 2. Asigne la ACL estándar a la función de servicio web HTTP.

```
ip http access-class ipv6 restrict_ipv6_webui
```

Verificación

Compruebe las entradas de ACL IPv4

```
show ip access-list restrict_ipv4_webui
Standard IP access list restrict_ipv4_webui
10 permit 192.168.10.0 0.0.0.255
```

Compruebe las entradas de ACL IPv6

```
show ipv6 access restrict_ipv4_webui
IPv6 access list restrict_ipv6_webui
permit ipv6 FD00::/64 any sequence 10
```

P: Después de aplicar la lista de acceso, obtengo una respuesta 403 en lugar de ninguna respuesta. ¿Por qué?

R: Este es el comportamiento esperado. La lista de acceso está diseñada para limitar quién tiene permiso para acceder al proceso http/https. Una respuesta 403 indica que tiene prohibido acceder a este recurso y es la respuesta correcta en este escenario ya que la lista de acceso se aplica al proceso HTTP/HTTPS en lugar de una lista de acceso de nivel de interfaz. Si la lista de acceso se aplicó a una interfaz en lugar del proceso HTTP/HTTPS, entonces ninguna respuesta sería la apropiada

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).