Filtrar o tráfego destinado aos dispositivos Cisco IOS XE WebUI usando uma lista de acesso

Contents

Introdução

Este documento descreve como configurar uma lista de acesso (ACL) em um dispositivo Cisco IOS XE para filtrar o tráfego destinado aos serviços da Web.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento foi criado para dispositivos corporativos que executam o software Cisco IOS® XE.

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 rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Background

Quando é necessário habilitar os Serviços Web HTTP para ter acesso à WebUI para gerenciar o dispositivo IOS XE ou para acesso de usuário webauth/convidado, os recursos de filtragem de

tráfego podem ser implementados para garantir que apenas os endereços IP necessários possam acessar a WebUI e que os usuários convidados possam continuar a integrar à rede.

Configurar

Configuração de Classe de Acesso ao Serviço HTTP

O método mais simples para definir o acesso pode ser feito através do suporte à classe de acesso IP no servidor Web HTTP. Neste exemplo de configuração, a sub-rede ipv4 192.168.10.0/24 é permitida, a sub-rede ipv6 fd00::/64 é permitida e todo o resto é negado. Existe um deny any any implícito no final da lista de acesso, mas você também pode adicionar um deny any any explícito, se desejar. No caso do controlador de LAN sem fio C9800, considere o acesso HTTP/HTTPS à interface de gerenciamento sem fio (WMI) e à porta de gerenciamento/serviço fora de banda.

Exemplo de IPv4

Etapa 1. Configurar uma ACL padrão e incluir os dispositivos/sub-redes confiáveis que têm permissão para acessar o dispositivo Cisco IOS XE sobre HTTP/HTTPS

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

Observação: esta ACL deve incluir apenas sub-redes confiáveis para ter acesso de administrador da Web ao dispositivo IOS XE. Ou seja, nenhuma sub-rede de convidado deve ser incluída nessa ACL. A não inclusão de sub-redes de convidados não interrompe a autenticação da Web, o acesso de convidados ou o redirecionamento da Web.

Etapa 2. Atribua a ACL padrão à classe de acesso do serviço Web HTTP.

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

Exemplo de IPv6

Etapa 1. Configurar uma ACL IPv6incluir os dispositivos/sub-redes confiáveis que têm permissão para acessar o dispositivo Cisco IOS XE sobre HTTP/HTTPS

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

Etapa 2. Atribua a ACL padrão ao recurso Serviço da Web HTTP.

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

Verificar

Verificar as entradas da 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
```

Verificar as entradas da ACL IPv6

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

P: Após aplicar a lista de acesso, obtenho uma resposta 403 em vez de nenhuma resposta. Por quê?

R: Esse é o comportamento esperado. A lista de acesso é projetada para limitar quem tem permissão para acessar o processo http/https. Uma resposta 403 indica que você está proibido de acessar esse recurso e é a resposta adequada nesse cenário, já que a lista de acesso é aplicada ao processo HTTP/HTTPS, ao contrário de uma lista de acesso no nível da interface. Se a lista de acesso tiver sido aplicada a uma interface em vez do processo HTTP/HTTPS, nenhuma resposta será a apropriada

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.