Filterverkeer bestemd voor Cisco IOS XE-apparaten - WebUI met toegangslijst

Inhoud

Inleiding

Dit document beschrijft hoe u een toegangslijst (ACL) op een Cisco IOS XE-apparaat kunt configureren om verkeer te filteren dat bestemd is voor de webservices.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document wordt geschreven voor Enterprise-apparaten waarop Cisco IOS® XE-software wordt uitgevoerd.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrond

Wanneer HTTP Web Services ingeschakeld moeten worden om webUI-toegang te hebben om het IOS XE-apparaat te beheren of voor webauth/guest user access, kunnen verkeersfiltering-functies

worden geïmplementeerd om ervoor te zorgen dat alleen de noodzakelijke IP-adressen toegang tot de WebUI kunnen krijgen en dat gastgebruikers aan boord van het netwerk kunnen blijven.

Configureren

Configuratie van HTTP-serviceklasse

De eenvoudigste methode om toegang te definiëren kan worden uitgevoerd via de ondersteuning van IP Access Class op de HTTP-webserver. In dit configuratievoorbeeld is ipv4-subnetnummer 192.168.10.0/24 toegestaan, ipv6-subnetnummer fd00::/64 is toegestaan en alle andere zaken worden geweigerd. Er is impliciet ontkennen om het even welk aan het eind van de toegang-lijst maar u kunt ook toevoegen uitdrukkelijk om het even welk om het even welk als u wenst ontkennen. Zorg er in het geval van de C9800 draadloze LAN-controller voor dat u HTTP/HTTPS-toegang tot de Wireless Management Interface (WMI) en out-of-band beheer/service-poort in overweging neemt.

IPv4-voorbeeld

Stap 1. Configureer een standaard ACL en neem de vertrouwde apparaten/subnetten op die toegang mogen hebben tot het Cisco IOS XE-apparaat via HTTP/HTTPS

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

Opmerking: deze ACL moet alleen subnetten bevatten die zijn vertrouwd met webbeheertoegang tot het IOS XE-apparaat. Namelijk om het even welke gastsubnets moeten niet in deze ACL worden omvat. Niet inbegrepen gast subnets breekt web audio, gast toegang, of web redirect niet.

Stap 2. Wijs de standaard ACL toe aan de HTTP Web Service access-klasse.

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

IPv6-voorbeeld

Stap 1. IPv6-ACL configureren: deze bevat de vertrouwde apparaten/subnetten die toegang hebben tot het Cisco IOS XE-apparaat via HTTP/HTTPS

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

Stap 2. Wijs de standaard ACL toe aan de HTTP-webservicefunctie.

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

Verifiëren

Controleer de IPv4 ACL-vermeldingen

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

Controleer de IPv6 ACL-vermeldingen

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

Q: Na het toepassen van de toegang-lijst krijg ik een 403 reactie in plaats van geen reactie. Waarom?

A: Dit is het verwachte gedrag. De toegangslijst is bedoeld om te beperken wie toegang heeft tot het http/https-proces. Een 403-antwoord geeft aan dat het u verboden is om toegang te krijgen tot deze bron en is de juiste respons in dit scenario omdat de toegangslijst wordt toegepast op het HTTP/HTTPS-proces in plaats van een toegangslijst op interfaceniveau. Als de toegangslijst is toegepast op een interface in plaats van het HTTP/HTTPS-proces, dan is geen reactie de juiste

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.