Filtern von Datenverkehr für Cisco IOS XE-Geräte über die WebUI mithilfe einer Zugriffsliste

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie eine Zugriffsliste (ACL) auf einem Cisco IOS XE-Gerät konfigurieren, um den für die Webdienste bestimmten Datenverkehr zu filtern.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument wurde für Enterprise-Geräte mit Cisco IOS® XE-Software geschrieben.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrund

Wenn HTTP-Webdienste aktiviert sein müssen, damit sie über eine Web-Benutzeroberfläche auf das IOS XE-Gerät oder für den Webauthentifizierungs-/Gastbenutzerzugriff zugreifen können, können Funktionen zur Datenverkehrsfilterung implementiert werden, um sicherzustellen, dass nur

die erforderlichen IP-Adressen auf die WebUI zugreifen können und Gastbenutzer weiterhin an Bord des Netzwerks bleiben können.

Konfigurieren

Konfiguration der HTTP-Service-Zugriffsklasse

Die einfachste Methode zur Definition des Zugriffs ist die Unterstützung der IP Access Class auf dem HTTP-Webserver. In diesem Konfigurationsbeispiel ist das ipv4-Subnetz 192.168.10.0/24 zulässig, das ipv6-Subnetz fd00::/64 ist zulässig, und alles andere wird abgelehnt. Am Ende der Zugriffsliste gibt es eine implizite deny any, aber Sie können auch eine explizite deny any hinzufügen, wenn Sie möchten. Achten Sie beim Wireless LAN Controller C9800 darauf, den HTTP-/HTTPS-Zugriff auf die Wireless Management Interface (WMI) und den Out-of-Band-Management-/Service-Port zu berücksichtigen.

IPv4-Beispiel

Schritt 1: Konfigurieren einer Standard-ACL und Einschließen der vertrauenswürdigen Geräte/Subnetze, die über HTTP/HTTPS auf das Cisco IOS XE-Gerät zugreifen dürfen

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

Hinweis: Diese ACL darf nur vertrauenswürdige Subnetze enthalten, damit Web-Administratoren auf das IOS XE-Gerät zugreifen können. Das heißt, dass Gastsubnetze nicht in diese ACL eingeschlossen werden dürfen. Das Nichteinbeziehen von Gast-Subnetzen unterbricht nicht die Webauthentifizierung, den Gastzugriff oder die Webumleitung.

Schritt 2: Weisen Sie die Standard-ACL der HTTP-Webdienst-Zugriffsklasse zu.

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

IPv6-Beispiel

Schritt 1: Konfigurieren einer IPv6-ACLinklusive der vertrauenswürdigen Geräte/Subnetze, die über HTTP/HTTPS auf das Cisco IOS XE-Gerät zugreifen dürfen

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

Schritt 2: Weisen Sie die Standard-ACL der HTTP-Webdienstfunktion zu.

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

Überprüfung

Überprüfen der IPv4-ACL-Einträge

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

Überprüfen der IPv6-ACL-Einträge

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

F: Nach dem Anwenden der Zugriffsliste erhalte ich eine 403-Antwort, keine Antwort. Warum ist das so?

A: Dieses Verhalten wird erwartet. Die Zugriffsliste wurde entwickelt, um die Zugriffsrechte für den http/https-Prozess einzuschränken. Eine 403-Antwort weist darauf hin, dass Ihnen der Zugriff auf diese Ressource untersagt ist, und stellt in diesem Szenario die richtige Antwort dar, da die Zugriffsliste auf den HTTP/HTTPS-Prozess und nicht auf eine Zugriffsliste auf Schnittstellenebene angewendet wird. Wenn die Zugriffsliste auf eine Schnittstelle anstelle des HTTP/HTTPS-Prozesses angewendet wurde, ist keine Antwort angemessen.