# Filtrer le trafic destiné aux périphériques Cisco IOS XE WebUI à l'aide d'une liste d'accès

## Table des matières



## Introduction

Ce document décrit comment configurer une liste de contrôle d'accès (ACL) sur un périphérique Cisco IOS XE pour filtrer le trafic destiné aux services Web.

## Conditions préalables

### Exigences

Aucune exigence spécifique n'est associée à ce document.

### Composants utilisés

Ce document est écrit pour les périphériques d'entreprise exécutant le logiciel Cisco IOS® XE.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

### Fond

Lorsque les services Web HTTP doivent être activés pour avoir un accès WebUI pour gérer le périphérique IOS XE ou pour un accès utilisateur webauth/invité, des fonctionnalités de filtrage du trafic peuvent être implémentées pour garantir que seules les adresses IP nécessaires peuvent accéder à l'interface WebUI et que les utilisateurs invités peuvent continuer à s'intégrer au réseau.

# Configurer

## Configuration de classe d'accès au service HTTP

La méthode la plus simple pour définir l'accès peut être effectuée via la prise en charge de la classe d'accès IP sur le serveur Web HTTP.  Dans cet exemple de configuration, le sous-réseau ipv4 192.168.10.0/24 est autorisé, le sous-réseau ipv6 fd00::/64 est autorisé et tout le reste est refusé.  Il y a un deny any any implicite à la fin de la liste d'accès, mais vous pouvez aussi ajouter un deny any any explicite si vous le souhaitez. Dans le cas du contrôleur LAN sans fil C9800, veillez à prendre en compte l'accès HTTP/HTTPS à l'interface de gestion sans fil (WMI) et au port de gestion/service hors bande.

## Exemple d'IPv4

Étape 1. Configurez une liste de contrôle d'accès standard et incluez les périphériques/sous-réseaux approuvés qui sont autorisés à accéder au périphérique Cisco IOS XE via HTTP/HTTPS

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

---

Remarque : cette liste de contrôle d'accès doit inclure uniquement les sous-réseaux approuvés pour avoir un accès administrateur Web au périphérique IOS XE. En d'autres termes, aucun sous-réseau invité ne doit être inclus dans cette liste de contrôle d'accès. L'exclusion des sous-réseaux invités n'interrompt pas l'authentification Web, l'accès invité ou la redirection Web.

---

Étape 2. Attribuez la liste de contrôle d'accès standard à la classe access-class du service Web HTTP.

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

## Exemple d'IPv6

Étape 1. Configurer une liste de contrôle d'accès IPv6Incluez les périphériques/sous-réseaux approuvés qui sont autorisés à accéder au périphérique Cisco IOS XE via HTTP/HTTPS

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

Étape 2. Attribuez la liste de contrôle d'accès standard à la fonctionnalité HTTP Web Service.

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

# Vérifier

Vérifiez les entrées de la liste de contrôle d'accès 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
```

Vérifiez les entrées de la liste de contrôle d'accès IPv6

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

# Q : Après avoir appliqué la liste d'accès, j'obtiens une réponse 403 au lieu de aucune réponse.  Pourquoi ?

R : C'est un comportement normal.  La liste de contrôle d'accès est conçue pour limiter les personnes autorisées à accéder au processus http/https.  Une réponse 403 indique que vous n'avez pas le droit d'accéder à cette ressource et est la réponse appropriée dans ce scénario, car la liste de contrôle d'accès est appliquée au processus HTTP/HTTPS par opposition à une liste de contrôle d'accès de niveau interface.  Si la liste de contrôle d’accès a été appliquée à une interface au lieu du processus HTTP/HTTPS, aucune réponse ne serait appropriée

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.