Résoudre la suppression de paquets IPv6 complète lorsqu'une liste de contrôle d'accès IPv6 est utilisée

Table des matières

Introduction

Ce document décrit qu'une liste de contrôle d'accès IPv6 avec un préfixe de zéro dans une ACE peut correspondre à tous les paquets IPv6 et à sa solution de contournement.

Conditions préalables

Exigences

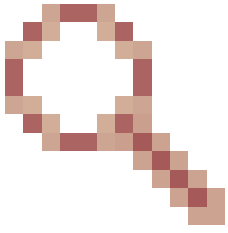
Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration de la liste de contrôle d'accès IPv6 sur les routeurs Cisco IOS® XR
- Programmation matérielle ACL sur les routeurs Cisco IOS® XR

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- La liste de contrôle d'accès IPv6 est appliquée avec le niveau de compression 2 ou 3



- Version de Cisco IOS® XR sans correction du bogue Cisco ID CSCwe08250

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.

Informations générales

L'adresse IPv6 ::/128 est réservée à l'adresse non spécifiée dans le document RFC(Request For Comments) 4291. Il ne doit jamais être attribué à un noeud. Il est donc recommandé de refuser cette adresse dans le filtrage de connexion IPv6.

Problème

Une liste de contrôle d'accès IPv6 incluant une entrée de contrôle d'accès (ACE) de ::/128 peut correspondre à n'importe quel paquet IPv6 sur l'interface à laquelle elle s'applique.

Un exemple de cette observation en laboratoire est présenté ci-dessous.

Configuration d'une liste de contrôle d'accès IPv6 avec ::/128 correspondant respectivement à l'adresse source et à l'adresse de destination IPv6 :

```
ipv6 access-list PREFIX_ALL_ZERO
 10 remark ** HOST MASK **
 11 deny ipv6 any host :: log
 12 deny ipv6 host :: any log
```

Envoi du trafic PING (Packet Internet ou Inter-Network Groper) vers une adresse de destination IPv6 non nulle :

```
RP/0/RP0/CPU0:router#ping fd00:4860:1:1::150 count 100 timeout 0
Thu Sep 14 12:30:23.412 UTC
pings with timeout=0 may result in system instability and
control protocol flaps resulting in traffic impact.
Do you really want to continue[confirm with only 'y' or 'n'] [y/n] :y
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to FD00:4860:1:1::150, timeout is 0 seconds:
....................................................................................................
Success rate is 0 percent (0/100)
```

Le paquet a été abandonné par ACE11 :

RP/0/RP0/CPU0:router#show access-lists ipv6 PREFIX_ALL_ZERO hardware ingress lo
Thu Sep 14 12:30:46.346 UTC
ipv6 access-list PREFIX_ALL_ZERO
11 deny ipv6 any host :: log (100 matches)
12 deny ipv6 host :: any log

Lors de la suppression de l'ACE 11, les abandons passent à l'ACE 12 :

RP/0/RP0/CPU0:router#clear access-list ipv6 PREFIX_ALL_ZERO hardware ingress location 0/RP0/CPU0

Thu Sep 14 12:31:34.899 UTC

RP/0/RP0/CPU0:router#ping fd00:4860:1:1::150 count 100 timeout 0

Thu Sep 14 12:31:39.482 UTC

pings with timeout=0 may result in system instability and

control protocol flaps resulting in traffic impact.

Do you really want to continue[confirm with only 'y' or 'n'] [y/n] :y

Type escape sequence to abort.

Sending 100, 100-byte ICMP Echos to FD00:4860:1:1::150, timeout is 0 seconds:

.....

Success rate is 0 percent (0/100)

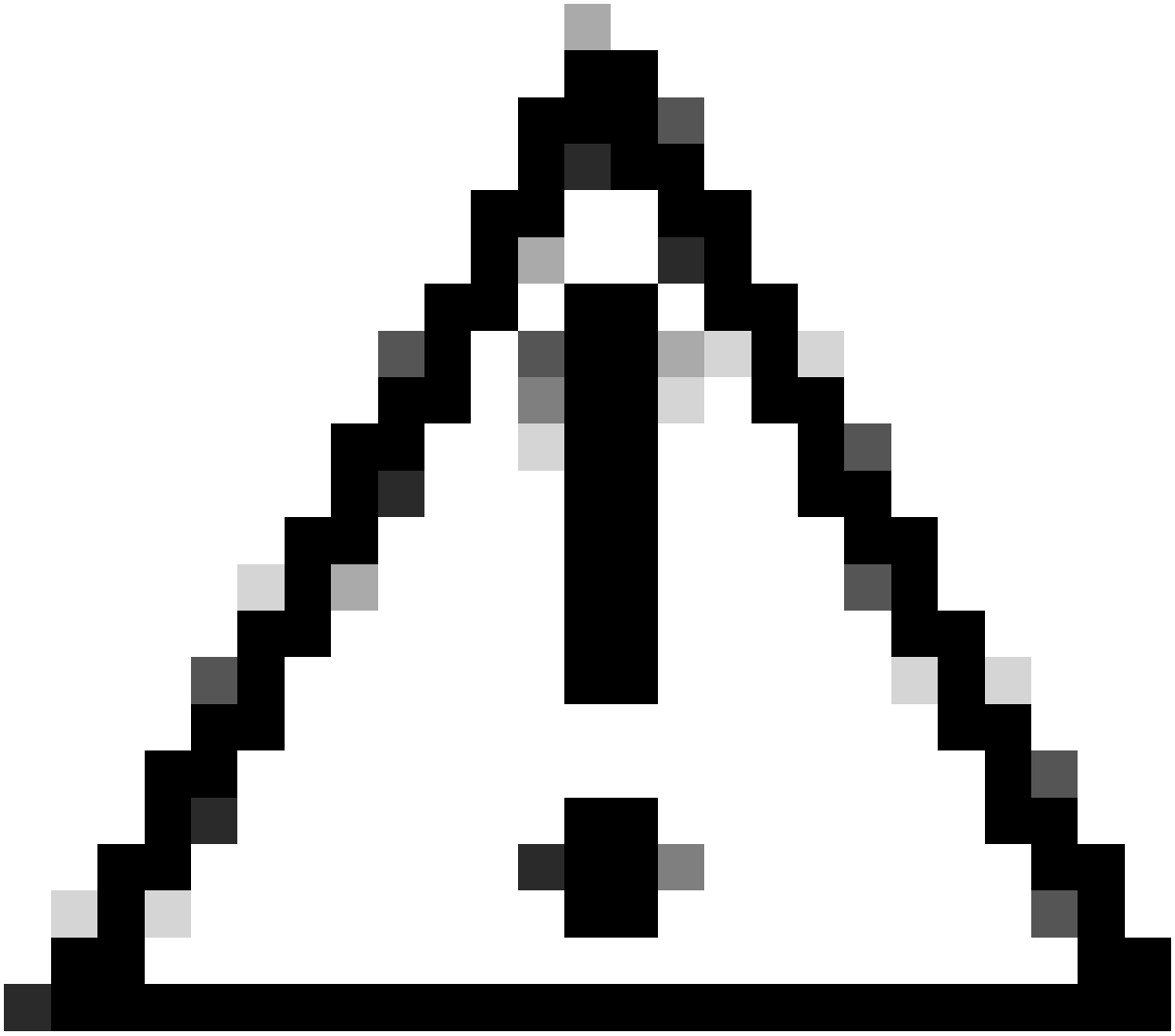
RP/0/RP0/CPU0:router#show access-lists ipv6 PREFIX_ALL_ZERO hardware ingress location 0/RP0/CPU0

Thu Sep 14 12:31:45.229 UTC

ipv6 access-list PREFIX_ALL_ZERO

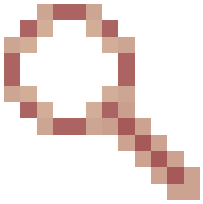
12 deny ipv6 host :: any log (100 matches)

Ces ACE sont supposés supprimer uniquement les paquets dont l'adresse source ou de destination est composée uniquement de zéros.
Cependant, tout le trafic, même avec la source ou la destination pas tous les zéros, était abandonné.



Attention : ce comportement de non-concordance est appliqué à la longueur de la marque de sous-réseau IPv6 comprise entre /1 et /128 pour une entrée de données ACE, et pas seulement /128 dans l'exemple.

Solution



La version de Cisco IOS® XR avec le correctif de l'ID de bogue Cisco CSCwe08250 corrige ce comportement incorrect.

Sur un routeur Cisco IOS® XR s'exécutant sans ce correctif, il existe une solution de contournement :

- Utilisez des listes de contrôle d'accès hybrides et déplacez l'::/<x> de la liste de contrôle

d'accès vers un groupe d'objets réseau pour faire correspondre l'adresse source ou de destination avec tous les zéros.

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.