

Los de volledige IPv6 Packet Drop op waar IPv6 ACL in gebruik is

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Probleem](#)

[Oplossing](#)

Inleiding

Dit document beschrijft dat een IPv6 ACL met een prefix alles-nul in een ACE alle IPv6-pakketten en de tijdelijke oplossing kan matchen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Configuratie van IPv6 ACL (toegangscontrolelijst) op Cisco IOS® XR-routers
- ACL-hardwareprogrammering op Cisco IOS® XR-routers

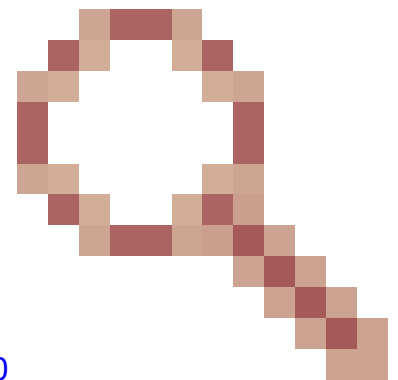
Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- IPv6-ACL wordt toegepast met compressieniveau 2 of 3

- Cisco IOS® XR release zonder fix van Cisco bug-id [CSCwe08250](#)

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.

Achtergrondinformatie

IPv6-adres::/128 is in RFC(request for comments) 4291 gereserveerd voor niet-gespecificeerd adres. Het moet nooit worden toegewezen aan een knooppunt, dus het is de beste praktijk om dit adres te ontkennen in de IPv6 Bogon filtering.

Probleem

Een IPv6 ACL met een ACE (Access Control Entry) van::/128 kan elk IPv6-pakket op de interface waarop het van toepassing was, matchen.

Een voorbeeld van deze observatie in het lab wordt hieronder getoond.

Een IPv6-ACL configureren met::/128 overeenkomende IPv6-bron- en doeladres:

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

Het verzenden van verkeer van PING (Packet Internet of Inter-Network Groper) naar een niet-nul IPv6-bestemmingsadres:

```
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)
```

Het pakket is door ACE11 laten vallen:

```
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
```

Bij het verwijderen van de ACE 11, druppels verplaatsen naar ACE 12:

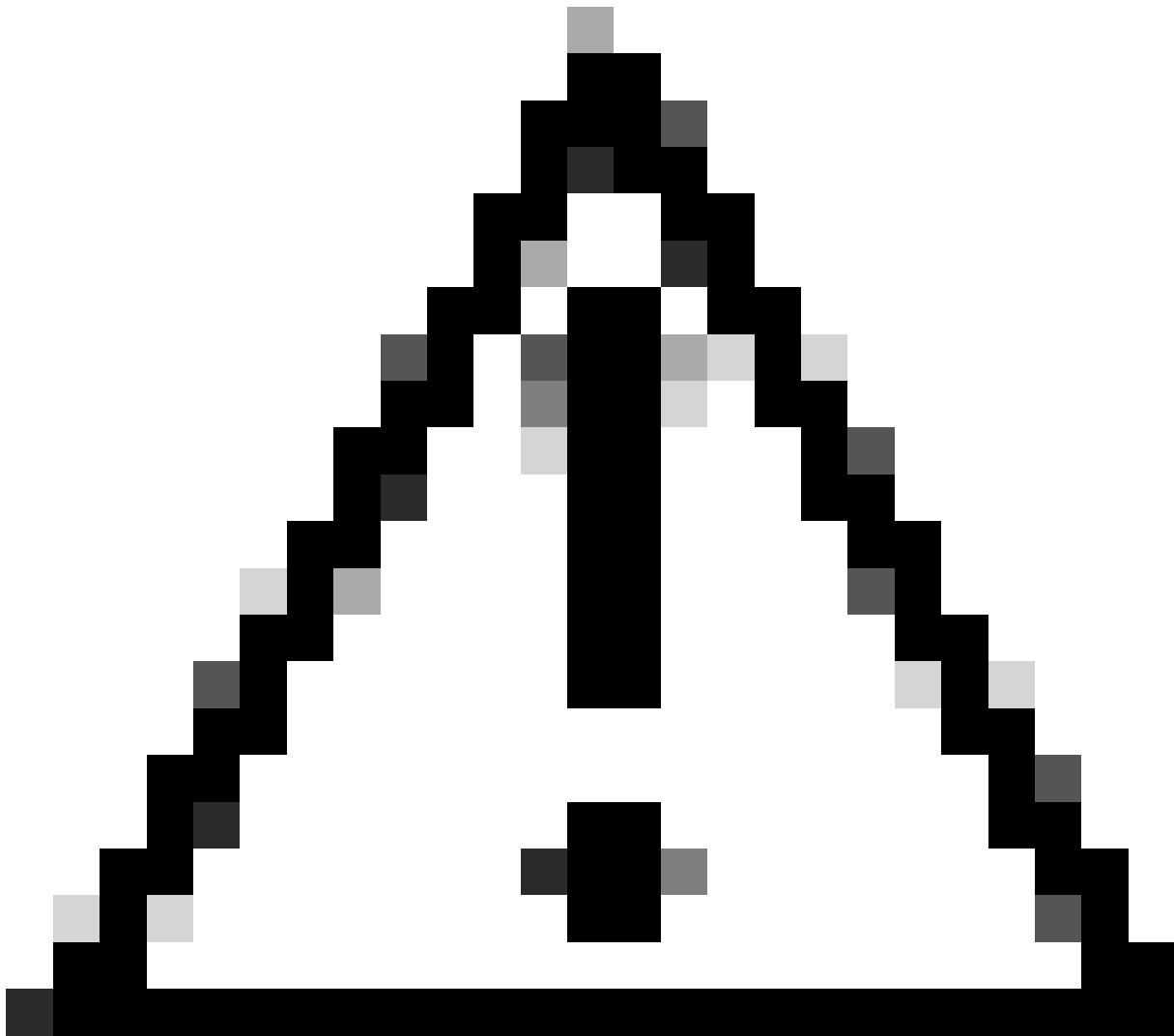
```
RP/0/RP0/CPU0:router#clear access-list ipv6 PREFIX_ALL_ZERO hardware ingress location 0/RP0/CPU0
Thu Sep 14 12:31:34.899 UTC
```

```
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)
```

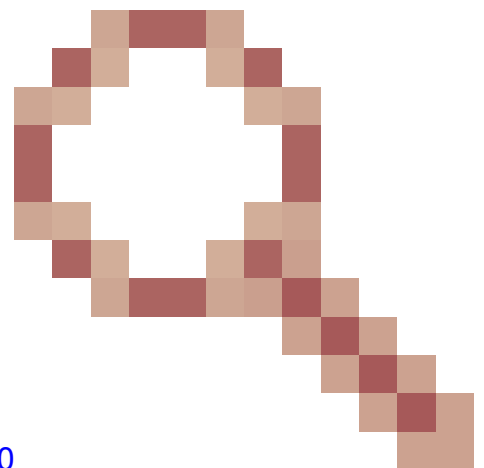
Deze ACE's worden verondersteld om alleen pakketten te laten vallen met bron- of doeladres dat allemaal nullen zijn.

Echter, al het verkeer, zelfs met bron of bestemming niet alle nullen, werd gedropt.



Waarschuwing: dit foutieve gedrag wordt toegepast op de IPv6-subnetmarklengte van /1 tot /128 voor een ACE, niet alleen op de /128 in het voorbeeld.

Oplossing



corrigeert dit verkeerde gedrag.

Op een router van Cisco IOS® XR die zonder die moeilijke situatie loopt, bestaat een tijdelijke oplossing:

- Gebruik hybride ACL's en verplaats de `:/<x>` van de ACL naar een netwerk object-groep om bron- of doeladres aan te passen aan alle nullen.

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.