Risolvere il problema del pacchetto IPv6 completo se è in uso un ACL IPv6

Sommario

Introduzione

Prerequisiti

- Requisiti
- Componenti usati

Premesse

Problema

Soluzione

Introduzione

In questo documento viene descritto che un ACL IPv6 con un prefisso "all-zero" in un ACE può corrispondere a tutti i pacchetti IPv6 e alla relativa soluzione alternativa.

Prerequisiti

Requisiti

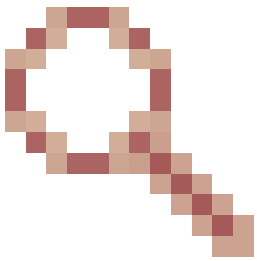
Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione di ACL (Access Control List) IPv6 sui router Cisco IOS® XR
- Programmazione hardware ACL su router Cisco IOS® XR

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- L'ACL IPv6 viene applicato con il livello di compressione 2 o 3



- Cisco IOS® XR versione senza correzione dell'ID bug Cisco CSCwe08250

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Premesse

Indirizzo IPv6 ::/128 è riservato per gli indirizzi non specificati nella RFC(Request For Comments) 4291. Non deve mai essere assegnato ad alcun nodo, pertanto è consigliabile negare questo indirizzo nel filtro Bogon IPv6.

Problema

Un ACL IPv6 che include una voce ACE (Access Control Entry) di ::/128 può corrispondere a qualsiasi pacchetto IPv6 nell'interfaccia a cui è applicato.

Di seguito è riportato un esempio di questa osservazione nel laboratorio.

Configurazione di un ACL IPv6 con ::/128 corrispondente all'indirizzo di origine e di destinazione IPv6, rispettivamente:

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

Invio del traffico PING (Packet Internet or Inter-Network Groper) a un indirizzo di destinazione IPv6 diverso da zero:

```
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)
```

Il pacchetto è stato scartato da 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

Quando si rimuove la voce ACE 11, le eliminazioni vengono spostate nella voce 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)

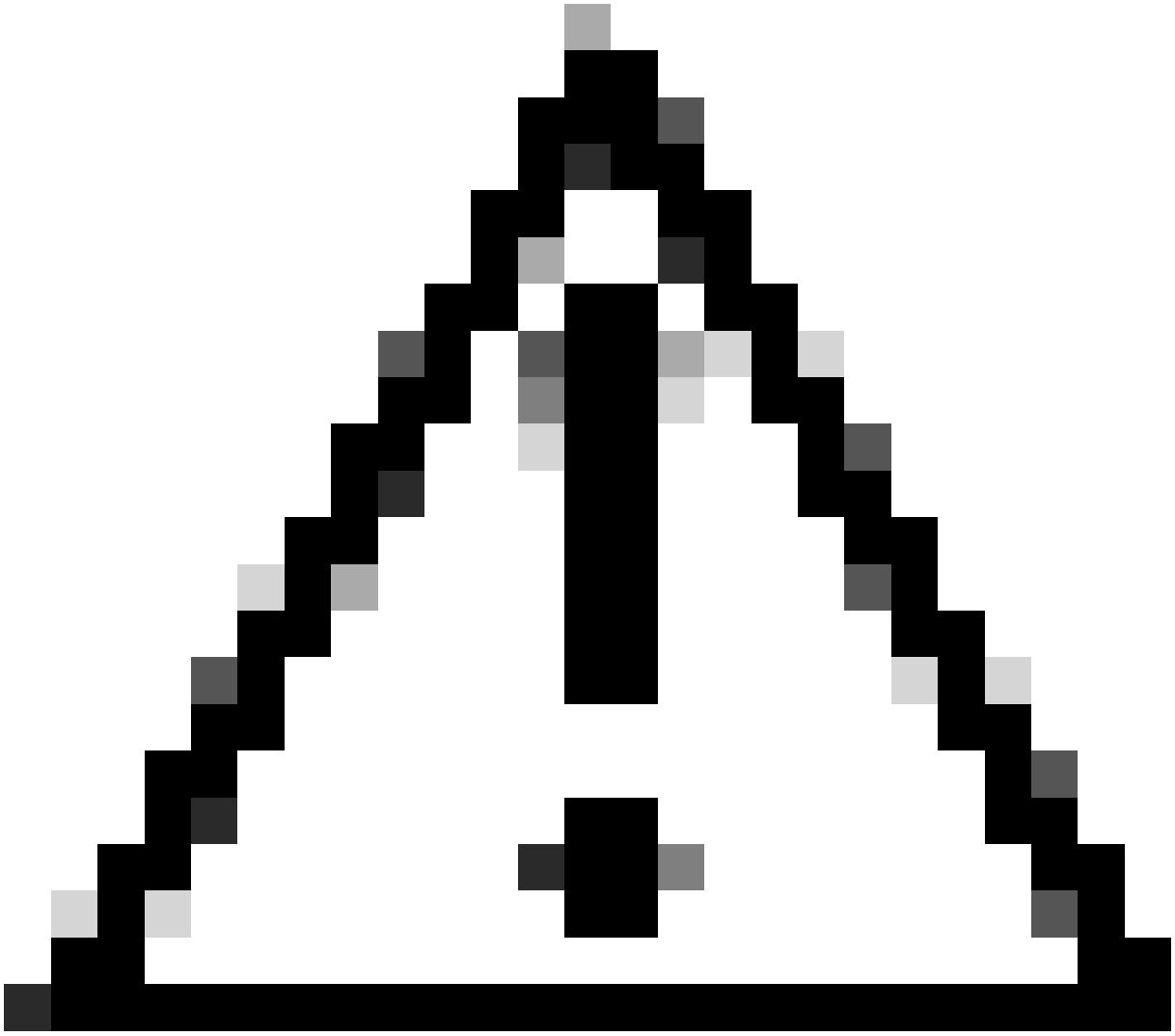
RP/0/RP0/CPU0:router#show access-lists ipv6 PREFIX_ALL_ZERO hardware ingress location 0/RP0/CPU0

Thu Sep 14 12:31:45.229 UTC

ipv6 access-list PREFIX_ALL_ZERO

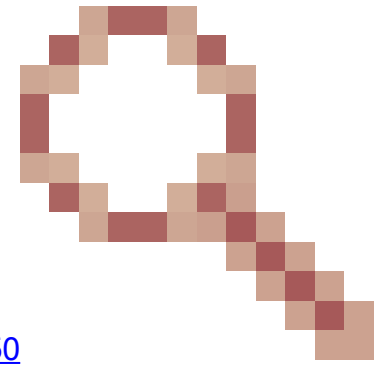
12 deny ipv6 host :: any log (100 matches)

Questi ACE devono eliminare solo i pacchetti con l'indirizzo di origine o di destinazione composto da tutti zero.
Tuttavia, tutto il traffico, anche con gli zeri di origine o di destinazione non tutti, veniva interrotto.



Attenzione: questo comportamento di mancata corrispondenza viene applicato alla lunghezza del contrassegno della subnet IPv6 da /1 a /128 per una voce ACE, non solo alla voce /128 nell'esempio.

Soluzione



Cisco IOS® XR release con la correzione dell'ID bug Cisco CSCwe08250 corregge questo comportamento errato.

Su un router Cisco IOS® XR in esecuzione senza tale correzione, è disponibile una soluzione:

- Usare ACL ibridi e spostare ::/<x> dall'ACL in un object group di rete per far corrispondere l'indirizzo di origine o di destinazione con tutti gli zeri.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).