Risoluzione dei problemi di perdita di pacchetti con ACL su piattaforma Nexus

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi di perdita di pacchetti utilizzando gli Access Control Lists (ACL) sulla piattaforma Nexus.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

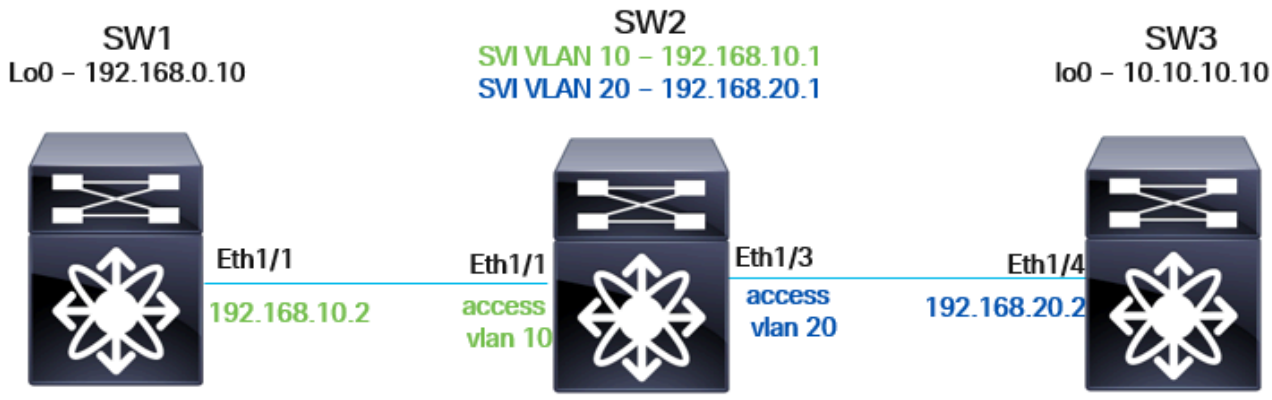
- Piattaforma NXOS
- Access Control Lists

Componente utilizzato

N9K1	N9K-C93108TC-EX	9.3(10)
N9K2	N9K-C93108TC-EX	9.3(10)
N9K3	N9K-C93108TC-EX	9.3(10)

Le informazioni discusse in questo documento fanno riferimento a dispositivi Nexus usati in un ambiente di emulazione. Tutti i dispositivi menzionati nel documento sono stati avviati senza alcuna configurazione preesistente. Se si utilizza una rete live, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Topologia



Breve panoramica sugli elenchi di controllo di accesso e sulle relative funzionalità

Un ACL viene usato essenzialmente per filtrare il traffico in base a una serie di regole e criteri ordinati (ad esempio, filtri basati sugli indirizzi IP di origine/destinazione). Queste regole determinano se i pacchetti soddisfano determinate condizioni per decidere se essere autorizzati o rifiutati. In parole più semplici, l'ACL definisce se i pacchetti di rete possono passare attraverso la rete o essere rifiutati sulla base delle regole impostate all'interno. Se i pacchetti soddisfano le condizioni previste dalle norme di autorizzazione, devono essere elaborati dal commutatore Nexus. Al contrario, se i pacchetti soddisfano le condizioni di rifiuto, essi vengono scartati.

Una delle caratteristiche principali degli ACL è la capacità di fornire contatori statistici per il flusso del pacchetto. Questi contatori rilevano il numero di pacchetti che soddisfano le regole ACL, una

funzione molto utile per risolvere eventuali problemi di perdita dei pacchetti.

Ad esempio, se un dispositivo invia un certo numero di pacchetti, ma riceve meno del previsto, i contatori statistici dell'ACL possono aiutare a isolare il punto in cui i pacchetti vengono scartati all'interno della rete.

PACL e RACL

L'implementazione degli ACL può variare a seconda che vengano applicati alle interfacce di layer 2 (PACL), di layer 3 (RACL) o alle VLAN (VACL). Di seguito è riportato un breve confronto tra questi metodi:

- PACL (Port Access Control List): L'ACL viene applicato a un'interfaccia di porta switch di layer 2 (L2).
- RACL (Router Access Control List): L'ACL viene applicato a un'interfaccia di routing di layer 3 (L3).

Tipo ACL	Interfaccia	Azione	Direzione applicata
PACL	L2	Interfacce Switchport Se l'ACL viene applicato a un'interfaccia trunk, filtra il traffico di tutte le VLAN consentite sul trunk.	Solo in entrata: il traffico che arriva all'interfaccia.
RACL	L3	Sottointerfacce SVI, Physical L3 e L3	Sia in entrata che in uscita: il traffico in entrata filtra il traffico in entrata e in uscita che esce dall'interfaccia.

Obiettivo

È necessario verificare che tutti i pacchetti inviati vengano ricevuti correttamente.

Spiegazione topologia

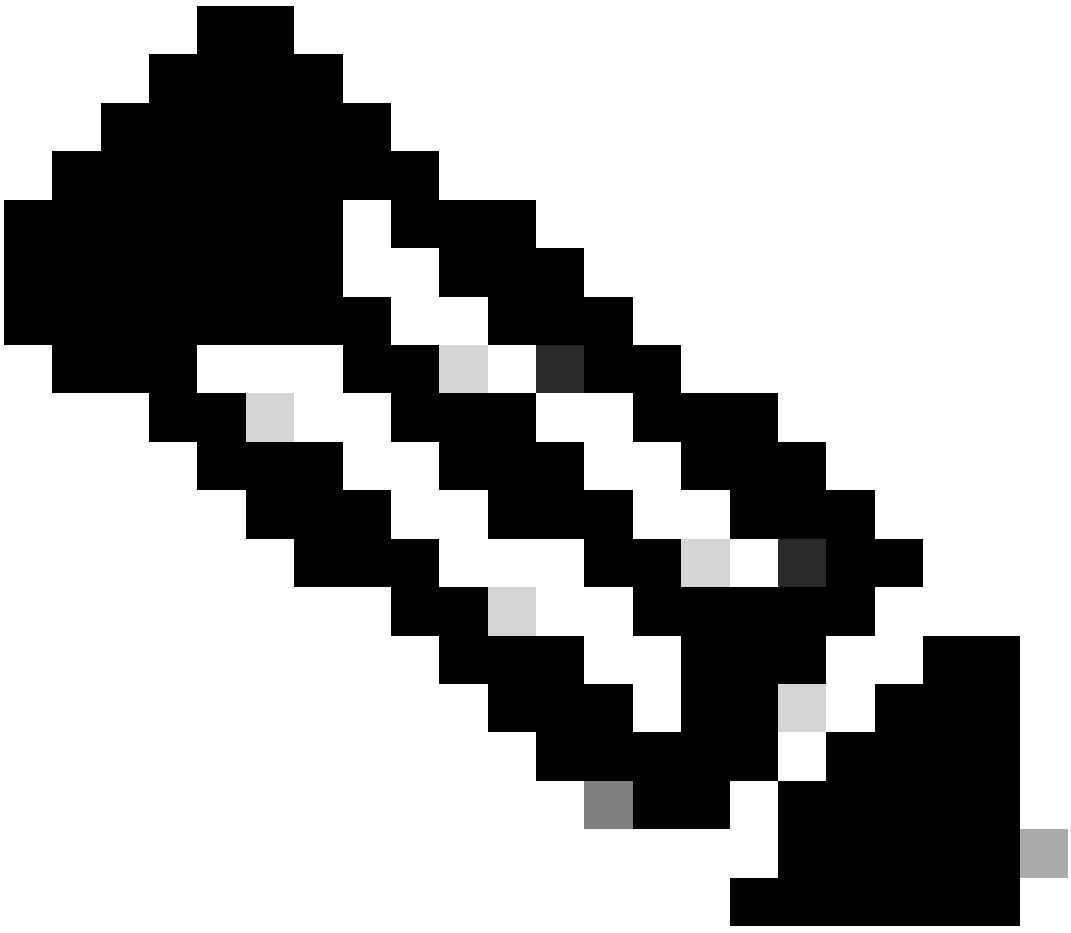
- N9K-1 ha una connettività L3 con N9K-2. L'interfaccia Eth1/1 su N9K-1 è configurata come interfaccia L3 instradata, mentre Eth1/1 di N9K-2 è un'interfaccia L2 switchport, contrassegnata con VLAN 10.
- N9K-2 ha anche una connettività L3 con N9K-3. L'interfaccia Eth1/3 su N9K-2 è

un'interfaccia switchport L2 etichettata con VLAN 20, e l'interfaccia Eth1/4 di N9K-3 è configurata come un'interfaccia instradata L3.
- Configurazione loopback: Sia N9K-1 che N9K-2 hanno l'interfaccia Lo0 configurata. Queste interfacce Lo0 devono essere utilizzate per inviare pacchetti ping ICMP tra i due dispositivi.

Risoluzione dei problemi

Trovare i passaggi dettagliati del processo per la configurazione e la verifica di RACL e PACL sui dispositivi N9K. Durante questo processo, gli Access Control List delle porte e i Control List dei router vengono esaminati per analizzare il flusso dei pacchetti e determinare se tutti i pacchetti vengono trasmessi e ricevuti correttamente.

Passaggio 1. Configurare RACL sulle interfacce L3 di N9K-1 (Eth1/1), N9K-2 (SVI 10, SVI 20) e N9K-3 (Eth1/14)



Nota: Per osservare il flusso del pacchetto in uscita, è necessaria una configurazione ACL

aggiuntiva sull'unità N9K-2. Poiché N9K-2 non dispone di interfacce con routing fisico L3 (dispone invece di interfacce con switchport SVI e L2), PACL supporta solo il traffico in entrata.

Per acquisire le corrispondenze dei pacchetti in uscita, è possibile creare un nuovo ACL da applicare alle interfacce L3.

L'ACL deve essere applicato a N9K-1, N9K-2 e N9K-3.

```
ip access-list TAC-IN
statistics per-entry
10 permit ip 192.168.20.2/32 192.168.0.10/32
20 permit ip 192.168.0.10/32 192.168.20.2/32
30 permit ip any any


ip access-list TAC-OUT
statistics per-entry
10 permit ip 192.168.20.2/32 192.168.0.10/32
20 permit ip 192.168.0.10/32 192.168.20.2/32
30 permit ip any any


***N9K-1***
interface Ethernet1/1
description ***Link-to-N9K-2***
ip access-group TAC-IN in
ip access-group TAC-OUT out
ip address 192.168.10.2/30
no shutdown



***N9K-2***

interface Vlan10
no shutdown
ip access-group TAC-IN-SVI in
ip access-group TAC-OUT-SVI out
ip address 192.168.10.1/30

interface Vlan20
no shutdown
ip access-group TAC-IN-SVI in
ip access-group TAC-OUT-SVI out
ip address 192.168.20.1/30

***N9K-3***

interface Ethernet1/4
description ***Link-to-N9K-2***
ip access-group TAC-IN in
ip access-group TAC-OUT out
ip address 192.168.20.2/30
no shutdown
```

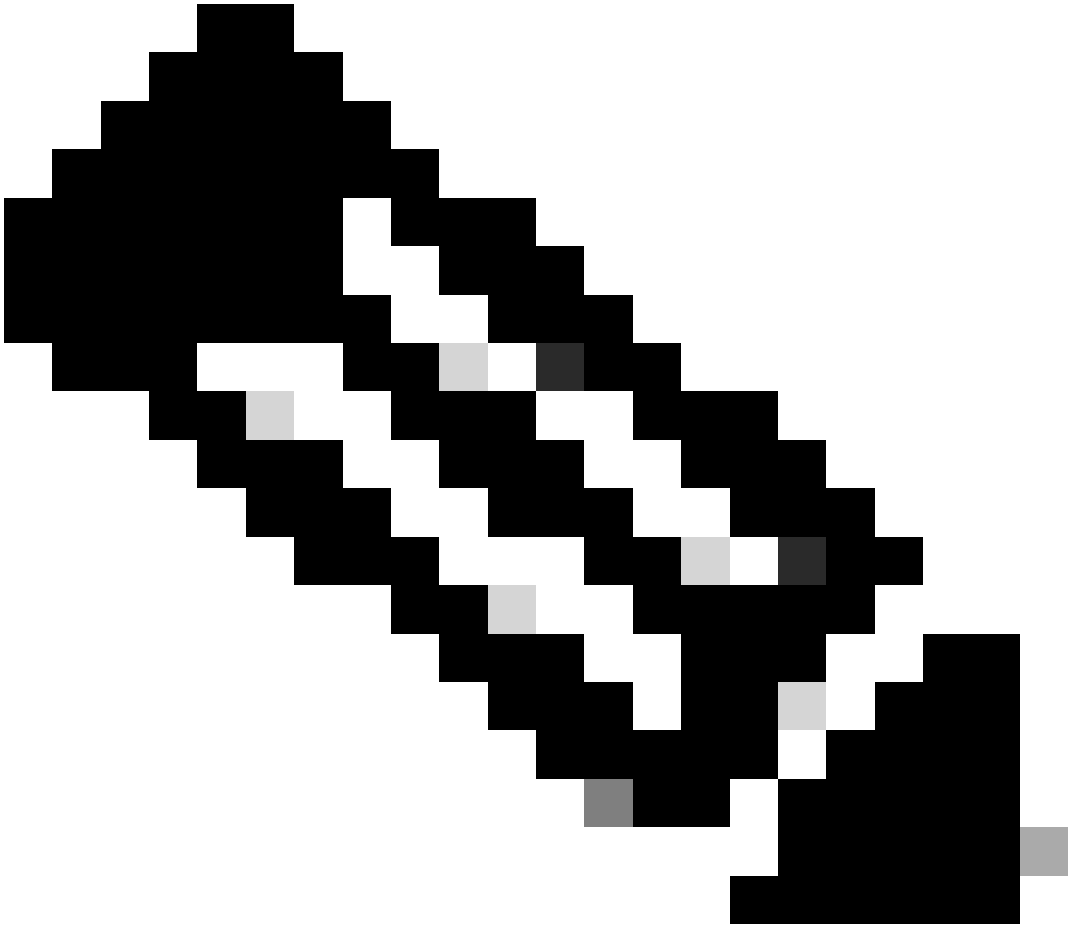
Passaggio 2. Configurare PACL sulle interfacce Switchport L2 di N9K-2

TCAM Scolpendo

A seconda del tipo di ACL, può essere richiesta l'intaglio TCAM. Per ulteriori informazioni, fare riferimento a:

Informazioni su come eseguire il carve Nexus 9000 TCAM Space

Per applicare il PACL alle interfacce fisiche L2, è necessario configurare un gruppo di accesso alla porta ip ....
Tuttavia, è necessario anche configurare la regione TCAM.



Nota: Alcune righe sono state rimosse per mantenere l'output pulito.

```
N9K-C93180YC-2# conf
Enter configuration commands, one per line. End with CNTL/Z.
```

```
N9K-C93180YC-2(config)# int e1/2
N9K-C93180YC-2(config-if)# ip port access-group TAC-IN in
ERROR: TCAM region is not configured. Please configure TCAM region Ingress PACL [ing-ifacl] and retry t
N9K-C93180YC-2(config-if)#
```

Procedura per la configurazione della regione TCAM

Passaggio 1. Modifiche della regione TCAM

Valutare quale area può fornire spazio libero, in quanto può variare in base all'ambiente.

```
N9K-C93180YC-2# show system internal access-list globals

slot 1
=======



LOU Threshold Value : 5

------------------------------------------------------------------------------------
INSTANCE 0 TCAM Region Information:
------------------------------------------------------------------------------------
Ingress:
--------
Region TID Base Size Width
------------------------------------------------------------------------------------
NAT 13 0 0 1
Ingress PACL 1 0 0 1 >>>>>>> Size of 0
Ingress VACL 2 0 0 1
Ingress RACL 3 0 1792 1
Ingress RBACL 4 0 0 1
Ingress L2 QOS 5 1792 256 1
Ingress L3/VLAN QOS 6 2048 512 1 >>>>>> Size of 512
Ingress SUP 7 2560 512 1
Ingress L2 SPAN ACL 8 3072 256 1
Ingress L3/VLAN SPAN ACL 9 3328 256 1
Ingress FSTAT 10 0 0 1
SPAN 12 3584 512 1
Ingress REDIRECT 14 0 0 1
Ingress NBM 30 0 0 1
Ingress Flow-redirect 39 0 0 1
Ingress RACL Lite 42 0 0 1
Ingress PACL IPv4 Lite 41 0 0 1
Ingress PACL IPv6 Lite 43 0 0 1
Ingress CNTACL 44 0 0 1
Mcast NAT 46 0 0 1
Ingress DACL 47 0 0 1
Ingress PACL Super Bridge 49 0 0 1
Ingress Storm Control 50 0 0 1
Ingress VACL Redirect 51 0 0 1
Egress Netflow L3 56 0 0 1
```

```
55 0 0 1
--------------------------------------------------------------------------------
Total configured size: 4096
Remaining free size: 0
Note: Ingress SUP region includes Redirect region
```

Metodo alternativo per la verifica.

```
N9K-C93180YC-2# sh hardware access-list tcam region
NAT ACL[nat] size = 0
Ingress PACL [ing-ifacl] size = 0 >>>>>>> Size of 0
VACL [vacl] size = 0
Ingress RACL [ing-racl] size = 1792
Ingress L2 QOS [ing-l2-qos] size = 256
Ingress L3/VLAN QOS [ing-l3-vlan-qos] size = 512 >>>>>> Size of 512
Ingress SUP [ing-sup] size = 512
Ingress L2 SPAN filter [ing-l2-span-filter] size = 256
Ingress L3 SPAN filter [ing-l3-span-filter] size = 256
Ingress FSTAT [ing-fstat] size = 0
span [span] size = 512
Egress RACL [egr-racl] size = 1792
Egress SUP [egr-sup] size = 256
Ingress Redirect [ing-redirect] size = 0
Egress L2 QOS [egr-l2-qos] size = 0
Egress L3/VLAN QOS [egr-l3-vlan-qos] size = 0
Ingress Netflow/Analytics [ing-netflow] size = 0
Ingress NBM [ing-nbm] size = 0
TCP NAT ACL[tcp-nat] size = 0
Egress sup control plane[egr-copp] size = 0
Ingress Flow Redirect [ing-flow-redirect] size = 0
Ingress CNTACL [ing-cntacl] size = 0
Egress CNTACL [egr-cntacl] size = 0
MCAST NAT ACL[mcast-nat] size = 0
Ingress DACL [ing-dacl] size = 0
Ingress PACL Super Bridge [ing-pacl-sb] size = 0
Ingress Storm Control [ing-storm-control] size = 0
Ingress VACL redirect [ing-vacl-nh] size = 0
Egress PACL [egr-ifacl] size = 0
Egress Netflow [egr-netflow] size = 0
N9K-C93180YC-2#
```

Passaggio 2. Ridurre le dimensioni dell'area

Ridurre le dimensioni della regione allocata per ing-l3-vlan-qos. (Questo varia a seconda dell'ambiente).

N9K-C93180YC-2(config)# elenco accessi hardware regione tcam ing-l3-vlan-qos 256 **>>>** Riduzione dell'allocazione da 512 a 256.
Salvare la configurazione e ricaricare il sistema per rendere effettiva la configurazione.

Passaggio 3. Aumentare la regione TCAM per ing-ifacl

N9K-C93180YC-2(config)# elenco accessi hardware regione tcam ing-ifacl 256

Salvare la configurazione e ricaricare il sistema per rendere effettiva la configurazione.

N9K-C93180YC-2(config)#

Passaggio 4. Salvataggio della configurazione

```
N9K-C93180YC-2(config)# copy running-config startup-config
[########################################] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
N9K-C93180YC-2(config)#
```

Passaggio 5. Ricarica

```
N9K-C93180YC-2(config)# reload
This command will reboot the system. (y/n)? [n] y
```

Verifica post-ricaricamento

Dopo il riavvio, verificare che le modifiche siano state applicate.

```
N9K-C93180YC-2# sh system internal access-list globals

slot 1
=======
```

```
-------------------------------------------------------------------------------
INSTANCE 0 TCAM Region Information:
-------------------------------------------------------------------------------
Ingress:
--------
Region TID Base Size Width
-------------------------------------------------------------------------------
NAT 13 0 0 1
Ingress PACL 1 0 256 1 >>> The size value is now 256.
Ingress VACL 2 0 0 1
Ingress RACL 3 256 1792 1
Ingress RBACL 4 0 0 1
Ingress L2 QOS 5 2048 256 1
Ingress L3/VLAN QOS 6 2304 256 1 >>> The size value is now 256.
Ingress SUP 7 2560 512 1
Ingress L2 SPAN ACL 8 3072 256 1
Ingress L3/VLAN SPAN ACL 9 3328 256 1
Ingress FSTAT 10 0 0 1
SPAN 12 3584 512 1
Ingress REDIRECT 14 0 0 1
Ingress NBM 30 0 0 1
Ingress Flow-redirect 39 0 0 1
Ingress RACL Lite 42 0 0 1
Ingress PACL IPv4 Lite 41 0 0 1
Ingress PACL IPv6 Lite 43 0 0 1
Ingress CNTACL 44 0 0 1
Mcast NAT 46 0 0 1
Ingress DACL 47 0 0 1
Ingress PACL Super Bridge 49 0 0 1
Ingress Storm Control 50 0 0 1
Ingress VACL Redirect 51 0 0 1
Egress Netflow L3 56 0 0 1
55 0 0 1
-------------------------------------------------------------------------------
Total configured size: 4096
Remaining free size: 0
Note: Ingress SUP region includes Redirect region
```

Metodo alternativo per la verifica.

```
N9K-C9318OYC-2# sh hardware access-list tcam region
NAT ACL[nat] size = 0
```

```
Ingress PACL [ing-ifacl] size = 256 >>> The size value is now 256.
VACL [vacl] size = 0
Ingress RACL [ing-racl] size = 1792
Ingress L2 QOS [ing-l2-qos] size = 256
Ingress L3/VLAN QOS [ing-l3-vlan-qos] size = 256 >>> The size value is now 256.
Ingress SUP [ing-sup] size = 512
Ingress L2 SPAN filter [ing-l2-span-filter] size = 256
Ingress L3 SPAN filter [ing-l3-span-filter] size = 256
Ingress FSTAT [ing-fstat] size = 0
span [span] size = 512
Egress RACL [egr-racl] size = 1792
Egress SUP [egr-sup] size = 256
Ingress Redirect [ing-redirect] size = 0
Egress L2 QOS [egr-l2-qos] size = 0
Egress L3/VLAN QOS [egr-l3-vlan-qos] size = 0
Ingress Netflow/Analytics [ing-netflow] size = 0
Ingress NBM [ing-nbm] size = 0
TCP NAT ACL[tcp-nat] size = 0
Egress sup control plane[egr-copp] size = 0
Ingress Flow Redirect [ing-flow-redirect] size = 0
Ingress CNTACL [ing-cntacl] size = 0
Egress CNTACL [egr-cntacl] size = 0
MCAST NAT ACL[mcast-nat] size = 0
Ingress DACL [ing-dacl] size = 0
Ingress PACL Super Bridge [ing-pacl-sb] size = 0
Ingress Storm Control [ing-storm-control] size = 0
Ingress VACL redirect [ing-vacl-nh] size = 0
Egress PACL [egr-ifacl] size = 0
Egress Netflow [egr-netflow] size = 0
N9K-C93180YC-2#
```

Configurazione del gruppo di accesso alla porta IP

Configurare il gruppo di accesso alla porta ip sulle interfacce fisiche L2.

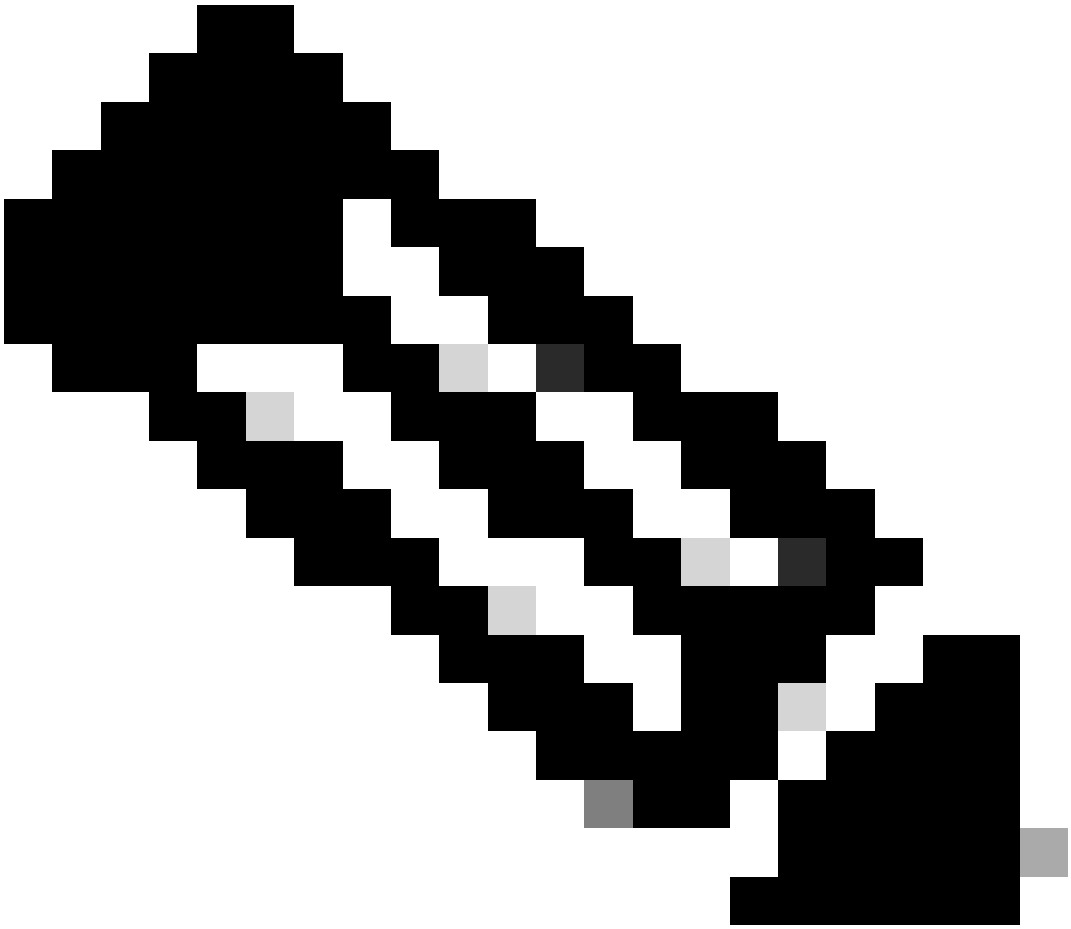
```
N9K-C93180YC-2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
N9K-C93180YC-2(config)# int e1/2,e1/51
N9K-C93180YC-2(config-if-range)# ip port access-group TAC-IN in
N9K-C93180YC-2(config-if-range)# ip port access-group TAC-OUT out
Port ACL is only supported on ingress direction >>>>>>>>
N9K-C93180YC-2(config-if-range)#
```

```
interface Ethernet1/1
description ***Link-to-N9K-1***
switchport
switchport access vlan 10
ip port access-group TAC-IN in >>> Inboud only
no shutdown
```

```
interface Ethernet1/3
description ***Link-to-N9K-3***
switchport
switchport access vlan 20
ip port access-group TAC-IN in >>> Inboud only
no shutdown
```

Passaggio 3. Loopback

N9K-1 utilizza il suo Loopback0 (Lo0) come origine, mentre N9K-3 può utilizzare il suo Loopback0 (Lo0) come destinazione.
La configurazione corrente delle interfacce di loopback utilizzate a scopo di test viene descritta in dettaglio nel modo seguente.



Nota: La connettività di layer 3 con un protocollo di routing è stata configurata in precedenza.

```
***N9K-1***
interface loopback0
ip address 192.168.0.10/32
```

```
***N9K-3***
interface loopback0
ip address 10.10.10.10/30
```

Passaggio 4. Generare il traffico e inviare un ping da N9K-3 utilizzando l'indirizzo IP di origine 192.168.20.2 a Lo0 192.168.0.10 di N9K-1

```
N9K-3# ping 192.168.0.10 source 192.168.20.2
PING 192.168.0.10 (192.168.0.10) from 192.168.20.2: 56 data bytes
64 bytes from 192.168.0.10: icmp_seq=0 ttl=253 time=1.163 ms
64 bytes from 192.168.0.10: icmp_seq=1 ttl=253 time=0.738 ms
64 bytes from 192.168.0.10: icmp_seq=2 ttl=253 time=0.706 ms
64 bytes from 192.168.0.10: icmp_seq=3 ttl=253 time=0.668 ms
64 bytes from 192.168.0.10: icmp_seq=4 ttl=253 time=0.692 ms

--- 192.168.0.10 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.668/0.793/1.163 ms
N9K-3#
```

Passaggio 5. Verifica delle informazioni statistiche PACL e RACL su N9K-1, N9K-2 e N9K-3

- Poiché i pacchetti ICMP sono originari del N9K-3, è necessario verificare che i cinque pacchetti di richiesta ICMP siano stati ricevuti dal N9K-2.
- Verifica PACL su N9K-2: Si prevede di ricevere cinque pacchetti provenienti da 192.168.20.2 (Eth1/4 di N9K-3), con la destinazione Lo0 di N9K-1 (192.168.0.10).

```
N9K-2# show ip access-lists TAC-IN
IP access list TAC-IN
statistics per-entry
10 permit ip 192.168.20.2/32 192.168.0.10/32 [match=5] >>>
20 permit ip 192.168.0.10/32 192.168.20.2/32 [match=0]
30 permit ip any any [match=0]
```

Configurazione correlata su Eth1/3 di N9K-2.

```
interface Ethernet1/3
description ***Link-to-N9K-3***
switchport
switchport access vlan 20
ip port access-group TAC-IN in >>> PACL
no shutdown
```

- Su N9K-2, il RACL segnala 5 pacchetti di richiesta ICMP che lasciano N9K-2 e che vengono inoltrati a N9K-1.
- Poiché PACL non supporta la direzione in uscita, è essenziale verificare l'altro ACL (TAC-OUT-SVI) configurato sulla SVI per la VLAN 10, ossia configurato come ACL (poiché la direzione in uscita è supportata sui RACL). La VLAN 10 fornisce la connettività tra N9K-2 e N9K-1.

```
N9K-2# show ip access-lists TAC-OUT-SVI

IP access list TAC-OUT-SVI
statistics per-entry
10 permit ip 192.168.20.2/32 192.168.0.10/32 [match=5] >>>
20 permit ip 192.168.0.10/32 192.168.20.2/32 [match=0]
30 permit ip any any [match=0]
```

```
configuration associated:


interface Vlan10
no shutdown
ip access-group TAC-IN-SVI in
ip access-group TAC-OUT-SVI out >>>>
ip address 192.168.10.1/30
```

In base ai risultati precedenti, viene confermata l'assenza di perdite di pacchetti con la richiesta ICMP inviata da N9K-3.

- Il passaggio successivo consiste nel passare al dispositivo successivo (destinazione N9K-1) e verificare che venga ricevuto lo stesso numero di pacchetti di richieste ICMP da N9K-3.
- Le statistiche RACL indicano che N9K-2 sta inviando 5 pacchetti di richiesta ICMP provenienti da N9K-3.

```
N9K-1# show ip access-lists TAC-IN
IP access list TAC-IN
statistics per-entry
10 permit ip 192.168.20.2/32 192.168.0.10/32 [match=5] >>>>
20 permit ip 192.168.0.10/32 192.168.20.2/32 [match=0]
30 permit ip any any [match=0]
```

Configurazione correlata su Eth1/1 di N9K-1.

```
interface Ethernet1/1
description ***Link-to-N9K-2***
ip access-group TAC-IN in >>> RACL
ip access-group TAC-OUT out
ip address 192.168.10.2/30
no shutdown
```

- Sulla base delle informazioni, viene confermato che non vi è alcuna perdita di pacchetto (richiesta ICMP) da N9K-3 a Lo0 192.168.0.10 su N9K-2.
- Il passaggio successivo è tenere traccia dei pacchetti di risposta ICMP provenienti da N9K-1 Lo0 192.168.0.10 e destinati a N9K-3 a 192.168.20.2.
- Quindi, è necessario procedere fino al N9K-2 e verificare se sta ricevendo i cinque pacchetti di risposta ICMP da 192.168.0.10 a 192.168.20.2.
- Per tenere traccia dei pacchetti di risposta ICMP da N9K-1, è necessario verificare il PACL (TAC-IN) configurato su Eth1/1.

```
N9K-2# show ip access-lists TAC-IN
IP access list TAC-IN
statistics per-entry
10 permit ip 192.168.20.2/32 192.168.0.10/32 [match=0]
20 permit ip 192.168.0.10/32 192.168.20.2/32 [match=5] >>> 5 icmp reply comming from 192.168.0.10 to 19
30 permit ip any any [match=0]
```

```
interface Ethernet1/1
description ***Link-to-N9K-1***
switchport
switchport access vlan 10
ip port access-group TAC-IN in >>> PACL (Inboud direction only)
no shutdown
```

- In base alle informazioni fornite in precedenza, si conferma che non vi è alcuna perdita di pacchetti sul traffico tra i N9K-1 e N9K-2.
- Il passaggio successivo è quello di verificare che il protocollo N9K-2 stia inviando correttamente i pacchetti di risposta ICMP al protocollo N9K-3. Poiché il protocollo PACL non supporta la direzione in uscita, è necessario verificare l'altro ACL (TAC-OUT-SVI) configurato sulla SVI per la VLAN 20, che è configurata come ACL (la direzione in uscita è supportata sui RAC). La VLAN 20 fornisce la connettività tra N9K-2 e N9K-3.

```
N9K-2# show ip access-lists TAC-OUT-SVI
IP access list TAC-OUT-SVI
statistics per-entry
10 permit ip 192.168.20.2/32 192.168.0.10/32 [match=0]
```

```
20 permit ip 192.168.0.10/32 192.168.20.2/32 [match=5] >>> 5 ICMP reply packets are being sent out to N
```

Configurazione correlata:

```
interface Vlan10
no shutdown
ip access-group TAC-IN-SVI in
ip access-group TAC-OUT-SVI out >>> RACL outboud direccion
ip address 192.168.20.1/30
```

In base ai contatori ACL degli output di cui sopra, è confermato che N9K-1 sta inviando correttamente i cinque pacchetti di risposta ICMP a N9K-2.

- Non si verificano perdite di pacchetti da N9K-2 a N9K-3.

- Il passaggio finale è quello di procedere all'origine del traffico, N9K-3, e verificare se sta ricevendo i cinque pacchetti di risposta ICMP.
- È confermato che i cinque pacchetti ICMP stanno violando l'ACL TAC-IN per le risposte ICMP provenienti da N9K-1 Lo0 (192.168.0.10).
  Per ulteriori indagini, è necessario rivedere il RACL (TAC-IN) configurato su Eth1/4.

```
N9K-3# sh ip access-lists TAC-IN

IP access list TAC-IN
statistics per-entry
10 permit ip 192.168.20.2/32 192.168.0.10/32 [match=0]
20 permit ip 192.168.0.10/32 192.168.20.2/32 [match=5] >>> 5 icmp replies comming from Lo0 N9K-1
30 permit ip any any [match=0]
```

Configurazione correlata:

```
interface Ethernet1/4
description ***Link-to-N9K-2***
ip access-group TAC-IN in >>>
ip access-group TAC-OUT out
ip address 192.168.20.2/30
no shutdown
```

- Utilizzando le procedure di risoluzione dei problemi descritte in precedenza, il percorso in entrata e in uscita del pacchetto è stato convalidato hop per hop tra l'origine e la destinazione.

Nell'esempio, è stato confermato che non vi è alcuna perdita di pacchetti perché tutti i 5 pacchetti

ICMP sono stati ricevuti e inoltrati correttamente su ciascun dispositivo.

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).