Esempio di acquisizione di ACL dello switch Nexus serie 7000

Sommario

Introduzione

L'acquisizione degli elenchi di controllo di accesso (ACL, Access Control List) consente di acquisire in modo selettivo il traffico su un'interfaccia o su una VLAN (Virtual Local Area Network). Quando si abilita l'opzione di acquisizione per una regola ACL, i pacchetti che soddisfano questa regola vengono inoltrati o eliminati in base all'azione di autorizzazione o di rifiuto specificata e possono inoltre essere copiati su una porta di destinazione alternativa per ulteriori analisi. È possibile applicare una regola ACL con l'opzione di acquisizione:

1. In una VLAN,
2. In direzione entrata su tutte le interfacce,
3. In direzione di uscita su tutte le interfacce di layer 3.

Questa funzionalità è supportata da Nexus 7000 NX-OS release 5.2 e successive. Questo documento offre un esempio come guida di riferimento rapido per la configurazione di questa funzionalità.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

hardware:

- Nexus 7000 con versione 5.2.x e successive.
- Scheda di linea serie M1.

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.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Esempio di configurazione di ACL

Di seguito è riportato un esempio di configurazione dell'acquisizione ACL applicata a una VLAN, nota anche come acquisizione VACL (Virtual LAN Access Control List). Dieci gigabit snifer designate potrebbero non essere fattibili per tutti gli scenari. L'acquisizione selettiva del traffico può essere molto utile in tali scenari, in particolare durante la risoluzione dei problemi quando i volumi di traffico sono elevati.

```
!! Global command required to enable ACL-capture feature (on default VDC)
hardware access-list capture

monitor session 1 type acl-capture
destination interface ethernet 2/1
no shut
exit
!!
ip access-list TEST_ACL
10 permit ip 216.113.153.0/27 any capture session 1
20 permit ip 198.113.153.0/24 any capture session 1
30 permit ip 47.113.0.0/16 any capture session 1
40 permit ip any any
!!
!! Note: Capture session ID matches with the monitor session ID
!!
vlan access-map VACL_TEST 10
match ip address TEST_ACL
action forward
statistics per-entry
!!
vlan filter VACL_TEST vlan-list 500
```

Èinoltre possibile controllare la programmazione TCAM (Ternary Content Indirissable Memory) dell'elenco degli accessi. Questo output è per la VLAN 500 per il modulo 1.

```
N7k2-VPC1# show system internal access-list vlan 500 input statistics

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

```
INSTANCE 0x0
--------------

Tcam 1 resource usage:
----------------------
Label_b = 0x802
Bank 0
------
IPv4 Class
Policies: VACL(VACL_TEST)
Netflow profile: 0
Netflow deny profile: 0
Entries:
[Index] Entry [Stats]
---------------------
[0006:0005:0005] permit ip 216.113.153.0/27 0.0.0.0/0 capture [0]
[0009:0008:0008] permit ip 198.113.153.0/24 0.0.0.0/0 capture [0]
[000b:000a:000a] permit ip 47.113.0.0/16 0.0.0.0/0 capture [0]
[000c:000b:000b] permit ip 0.0.0.0/0 0.0.0.0/0 [0]
[000d:000c:000c] deny ip 0.0.0.0/0 0.0.0.0/0 [0]
```

Avvertenze

1. Èpossibile attivare una sola sessione di acquisizione ACL alla volta nel sistema tra contesti di dispositivi virtuali (VDC).
2. I moduli Nexus serie 7000 F1 non supportano l'acquisizione di ACL.
3. I moduli Nexus serie 7000 F2 al momento non supportano l'acquisizione ACL, ma potrebbe trattarsi di un problema previsto nella roadmap.
4. L'acquisizione di ACL sui moduli Nexus serie 7000 M2 è supportata da Cisco NX-OS versione 6.1(1) e successive.
5. L'acquisizione di ACL sui moduli Nexus 7000 serie M1 è supportata con Cisco NX-OS versione 5.2(1) e successive.
6. L'acquisizione ACL non è compatibile con la registrazione ACL. Pertanto, se si hanno ACL con la parola chiave **log**, questi non funzionano dopo aver acquisito l'**elenco degli accessi all'hardware** a livello globale.
7. A causa del bug CSCug20139, l'esempio riportato in questo documento è documentato con una **sessione di acquisizione** per ACE anziché per ACL, finché il bug non viene risolto.

Informazioni correlate

- Cisco Nexus serie 7000 NX-OS Security Configuration Guide, versione 6.x, Esempi di configurazione per ACL IP
- Documentazione e supporto tecnico – Cisco Systems