Esempio di configurazione della registrazione di ACL ottimizzata sugli switch Nexus serie 7000 e 7700

Sommario

Introduzione

In questo documento viene descritto come configurare la registrazione OAL (Optimized Access Control List) sugli switch Cisco Nexus serie 7000 e 7700.

Prerequisiti

Requisiti

Cisco consiglia di conoscere le configurazioni Nexus con ACL di base prima di provare la configurazione descritta in questo documento.

Componenti usati

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

- Cisco Nexus serie 7000 switch
- Cisco Nexus serie 7700 switch

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

Gli ACL con registrazione abilitata forniscono informazioni dettagliate sul traffico che attraversa la rete o che viene scartato dai dispositivi di rete. La registrazione ACL può richiedere molte risorse della CPU e influire negativamente su altre funzioni del dispositivo di rete. Per ridurre i cicli della CPU, lo switch Cisco Nexus serie 7000 utilizza gli OAL.

L'uso degli OAL fornisce supporto hardware per la registrazione degli ACL. L'OAL autorizza o scarta i pacchetti nell'hardware e usa una routine ottimizzata per inviare informazioni al Supervisor in modo che possa generare i messaggi di logging. Ad esempio, quando un pacchetto raggiunge un ACL con registrazione abilitata mentre viene inoltrato nell'hardware, viene creata una copia del pacchetto nell'hardware e il pacchetto viene inviato al Supervisor per la registrazione in base all'intervallo di tempo configurato.

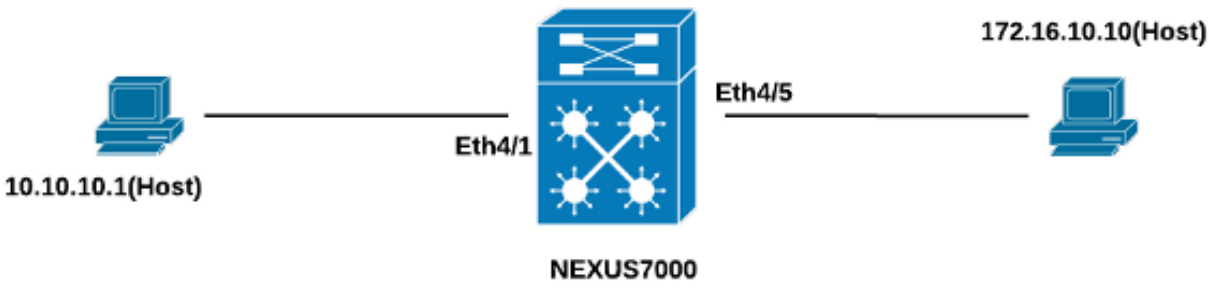
Configurazione

In questa sezione vengono fornite informazioni che è possibile utilizzare per configurare lo switch Nexus per l'utilizzo degli OAL.

Nell'esempio descritto in questa sezione, è presente un host all'indirizzo IP 10.10.10.1 che invia il traffico a un altro host all'indirizzo IP 172.16.10.10 tramite un'interfaccia Nexus serie 7000, con un ACL con registrazione configurata.

Esempio di rete

La connessione tra gli host e lo switch Nexus serie 7000 viene effettuata in base alla seguente topologia:



Configurazioni

Per configurare lo switch per l'utilizzo degli OAL, attenersi alla seguente procedura:

1. Configurare questi comandi globali per abilitare OAL:

   ```
   logging ip access-list cache entries 8000
   logging ip access-list cache interval 300
   logging ip access-list cache threshold 0
   ```

   Di seguito è riportato un esempio:

   ```
   Nexus-7000# conf t
   Enter configuration commands, one per line.  End with CNTL/Z.
   Nexus-7000(config)#logging ip access-list cache entries 8000
   Nexus-7000(config)#logging ip access-list cache interval 300
   Nexus-7000(config)#logging ip access-list cache threshold 0
   ```

2. Applica questa configurazione per la registrazione:

   ```
   logging level acllog <number>
   acllog match-log-level <number>
   logging logfile [name] <number>
   ```

   Di seguito è riportato un esempio:

   ```
   Nexus-7000(config)# logging level acllog 5
   Nexus-7000(config)# acllog match-log-level  5
   Nexus-7000(config)# logging logfile acllog 5
   ```

3. Configurare l'ACL per abilitare la registrazione. Le voci devono essere configurate con la parola chiave **log** abilitata, come mostrato nell'esempio seguente:

   ```
   Nexus-7000(config)# ip access-list test1
   Nexus-7000(config-acl)# 10 permit ip 10.10.10.1/32 172.16.10.10/32 log
   Nexus-7000(config-acl)# 20 deny ip any any log
   Nexus-7000(config-acl)#
   Nexus-7000(config-acl)#show ip access-lists test1 IP access list test1
   10 permit ip 10.10.10.1/32 172.16.10.10/32 log
   20 deny ip any any log
   Nexus-7000(config-acl)#
   ```

4. Applicare l'ACL configurato nel passaggio precedente all'interfaccia richiesta:

   ```
   Nexus-7000# conf t
   Enter configuration commands, one per line. End with CNTL/Z.
   Nexus-7000(config)# int ethernet 4/1
   Nexus-7000(config-if)# ip access-group test1 in
   Nexus-7000(config-if)# ip access-group test1 out
   Nexus-7000(config-if)#
   Nexus-7000(config-if)# show run int ethernet 4/1
   !Command: show running-config interface Ethernet4/1
   !Time: Mon Jun 30 16:30:38 2014
   version 6.2(6)
   interface Ethernet4/1
    ip access-group test1 in
    ip access-group test1 out
    ip address 10.10.10.2/24
    no shutdown
   Nexus-7000(config-if)#
   ```

Verifica

Per verificare che la configurazione funzioni correttamente, consultare le informazioni contenute in questa sezione.

Nell'esempio utilizzato in questo documento, il ping viene avviato dall'host all'indirizzo IP 10.10.10.1 all'host all'indirizzo IP 172.16.10.1. Immettere il comando **show logging ip access-list cache** nella CLI per verificare il flusso del traffico:

```
Nexus-7000# show logging ip access-list cache
Src IP Dst IP S-Port D-Port Src Intf Protocol Hits
------------------------------------------------------------
10.10.10.1 172.16.10.10 0 0 Ethernet4/1 (1)ICMP 368
Number of cache entries: 1
------------------------------------------------------------
Nexus-7000#
Nexus-7000# show logging ip access-list status Max flow = 8000
Alert interval = 300
Threshold value = 0
Nexus-7000#
```

Èpossibile visualizzare la registrazione ogni 300 secondi, poiché questo è l'intervallo di tempo predefinito:

```
Nexus-7000# show logging logfile
2014 Jun 29 19:19:01 Nexus-7000 %SYSLOG-1-SYSTEM_MSG : Logging logfile (acllog)
cleared by user
2014 Jun 29 19:20:57 Nexus-7000 %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configured from vty by
admin on console0
2014 Jun 29 19:21:18 Nexus-7000 %ACLLOG-5-ACLLOG_FLOW_INTERVAL: Src IP: 10.1 0.10.1,
Dst IP: 172.16.10.10, Src Port: 0, Dst Port: 0, Src Intf: Ethernet4/1, Pro tocol:
"ICMP"(1), Hit-count = 2589
2014 Jun 29 19:26:18 Nexus-7000 %ACLLOG-5-ACLLOG_FLOW_INTERVAL: Src IP: 10.1 0.10.1,
Dst IP: 172.16.10.10, Src Port: 0, Dst Port: 0, Src Intf: Ethernet4/1, Pro tocol:
"ICMP"(1), Hit-count = 4561
```

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Note sulla configurazione

In questa sezione vengono fornite ulteriori informazioni sulla configurazione descritta in questo documento.

Registrazione ACL dettagliata

In Nexus Operating System (NX-OS) versione 6.2(6) e successive, è disponibile la registrazione *dettagliata* degli ACL. La funzionalità registra le seguenti informazioni:

- Indirizzi IP di origine e di destinazione
- Porte di origine e di destinazione

- Source interface
- Protocollo
- Nome ACL
- Azione ACL (consenti o nega)
- Interfaccia applicata
- Numero pacchetti

Immettere il comando **logging ip access-list detail** nella CLI per abilitare la registrazione dettagliata. Di seguito è riportato un esempio:

```
Nexus-7000(config)# logging ip access-list detailed
ACL Log detailed Logging feature is enabled. Hit-count of existing ACL Flow entry will
be reset to zero and will contain Hit Count per ACL type Flow.
Nexus-7000(config)#
```

Di seguito è riportato un esempio di output di registrazione dopo l'attivazione della registrazione dettagliata:

```
2014 Jul 18 02:20:38 Nexus7k-1-oal %ACLLOG-6-ACLLOG_FLOW_INTERVAL: Src IP: 10.10.10.1,
Dst IP: 172.16.10.10, Src Port: 0, Dst Port: 0, Src Intf: Ethernet4/5, Protocol:
"ICMP"(1), ACL Name: test1, ACE Action: Permit, Appl Intf: Ethernet4/5, Hit-count: 69
```

Descrizioni dei comandi OAL globali

In questa sezione vengono descritti i comandi OAL globali utilizzati per configurare lo switch Nexus serie 7000 per l'utilizzo degli OAL.

Comando	Descrizione
Switch(config)# registrazione cache elenco accessi ip {{entry_number_of_entries} | {secondi intervallo} | {rate-limit_number_of_packets} | {threshold_number_of_packets}	Questo comando imposta i parametri globali OAL.
Switch(config)# senza log ip access-list cache {entries intervallo | | limite di tasso | soglia}	Con questo comando vengono ripristinate le impostazioni predefinit parametri globali OAL.
voci num_voci	Questi parametri specificano il numero massimo di voci di log memorizzate nella cache del software. L'intervallo è compreso tra 0 1.048.576. Il valore predefinito è 8.000 voci.
intervallo secondi	Questi parametri specificano l'intervallo di tempo massimo prima ch voce venga inviata a un syslog. L'intervallo è compreso tra 5 e 86.4 valore predefinito è 300 secondi.
soglia num_pacchetti	Questi parametri specificano il numero di corrispondenze di pacche (accessi) prima che una voce venga inviata a un syslog. L'intervallo compreso tra 0 e 1.000.000. Il valore predefinito è 0 pacchetti (la limitazione della velocità è disattivata), quindi il registro di sistema n viene attivato dal numero di corrispondenze dei pacchetti.

Nota: la forma *no* di questi comandi CLI ripristina le impostazioni predefinite dei parametri solo se sono stati modificati; la configurazione non viene rimossa, in quanto lo switch Nexus serie 7000 ha solo l'opzione OAL.

Descrizioni dei comandi di registrazione

In questa sezione vengono descritti i comandi di log utilizzati per configurare lo switch Nexus serie 7000 per l'utilizzo degli OAL.

Comando	Descrizione
switch(config)# acllog corrisp-log-numero livello Esempio: switch(config)# aclog match-log-level 3	Questo comando specifica il livello di registrazione che deve corrispond prima che le voci vengano registrate nel log ACL (acllog). L'intervallo è compreso tra 0 e 7. Il valore predefinito è 6.
Switch(config)# no acllog match-log-level numero Esempio: switch(config)# no aclog match-log-level 6	Con questo comando viene ripristinato il livello di registrazione predefini
Livello di gravità della funzione di registrazione Switch(config)# Esempio: switch(config)# livello di log acl 3	Questo comando abilita la registrazione dei messaggi provenienti dalla struttura specificata con il livello di gravità specificato o superiore. Nell'esempio utilizzato in questo documento, il livello *acllog* è impostato mentre l'impostazione predefinita è 2.
Switch(config)# senza livello di registrazione [livello di gravità della struttura] Esempio: switch(config)# nessun acl del livello di registrazione 3	Con questo comando viene ripristinato il livello predefinito di gravità dell registrazione per la struttura specificata. Se non si specifica una struttur una gravità , il dispositivo ripristina tutti i livelli predefiniti. Nell'esempio utilizzato nel documento, viene ripristinato il valore predefinito (2).
Switch(config)# livello di gravità del nome del file di log del file di log [size byte] Esempio: switch(config)# log file registro acl 3	Con questo comando viene configurato il nome del file di log utilizzato p archiviare i messaggi di sistema e il livello di gravità minimo prima dell'esecuzione della registrazione. Se lo si desidera, è possibile specific una dimensione massima del file. Il livello di gravità predefinito è 5 e le dimensioni predefinite del file sono 10.485.760.
Switch(config)# no logging fileregistro [logfile-name livello di gravità [size byte] Esempio: switch(config)# nessun file di log acl 3	Questo comando disattiva la registrazione nel file di registro.

> **Nota:** Affinché i messaggi vengano immessi nei log, il livello di log per la funzione di log ACL (acllog) e il livello di gravità della registrazione per il file di log devono essere maggiori o uguali all'impostazione *match-log*-level del log ACL.

Linee guida e limitazioni

Di seguito sono riportate alcune importanti linee guida e limitazioni che è necessario considerare prima di applicare la configurazione descritta in questo documento:

- Gli switch Nexus serie 7000 e 7700 supportano solo OAL.
- La registrazione ACL non funziona con la funzione di acquisizione ACL.
- L'opzione *log* negli ACL in uscita non è supportata per i pacchetti multicast.

- Il supporto della registrazione dettagliata non è disponibile per i pacchetti IPv6.
- Il livello di log per la funzionalità *acllog* e la gravità del *file di log* devono essere configurati in modo che siano maggiori o uguali all'impostazione *acllog match-log-level*.
- Non utilizzare il comando **hardware access-list capture** mentre OAL è in uso. Quando questo comando viene utilizzato insieme a OAL e si abilita l'acquisizione ACL, viene visualizzato un messaggio di avviso per informare che la registrazione ACL è disabilitata per tutti i contesti dei dispositivi virtuali (VDC). Quando si disabilita l'acquisizione ACL, la registrazione ACL viene abilitata. per il corretto funzionamento del processo, disabilitarlo usando il comando **no hardware access-list capture**.