Les Commutateurs de Nexus 7000 et de gamme 7700 ont optimalisé l'exemple de configuration de journalisation d'ACL

Contenu

Introduction

Ce document décrit comment configurer la liste de contrôle d'accès optimalisée (ACL) se connectant (OAL) sur les Commutateurs de gammes 7000 et 7700 de Cisco Nexus.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance des configurations de Nexus avec ACLs de base avant que vous tentiez la configuration qui est décrite dans ce document.

[Composants utilisés](#)

Les informations contenues dans ce document sont basées sur les versions de matériel et de

logiciel suivantes :

- Commutateurs de la gamme Cisco Nexus 7000
- Commutateurs de gamme 7700 de Cisco Nexus

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Le logging enabled ACLs fournissent la vue dans le trafic pendant qu'il traverse le réseau ou est relâché par des périphériques de réseau. Malheureusement, se connecter d'ACL peut être CPU intensive et peut négativement affecter d'autres fonctions du périphérique de réseau. Afin de réduire des cycles CPU, la gamme 7000 de Cisco Nexus commute des utilisations OALs.

L'utilisation d'OALs fournit le support matériel pour se connecter d'ACL. Les autorisations OAL ou les paquets de baisses dans le matériel et emploie une routine optimisée afin d'envoyer les informations au superviseur de sorte qu'elles puissent générer les messages de journalisation. Par exemple, quand un paquet frappe un ACL avec le logging enabled tandis qu'il est expédié dans le matériel, une copie du paquet est créée dans le matériel et le paquet est donné un coup de volée au superviseur pour l'accord logging on avec l'intervalle de temps qui est configuré.

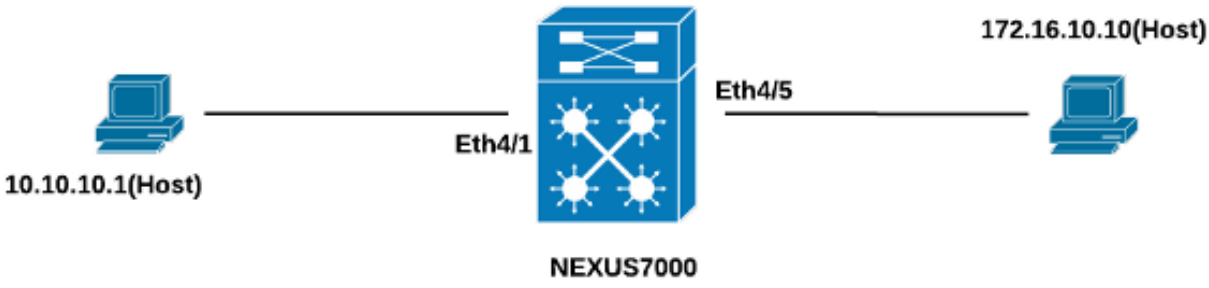
Configurez

Cette section fournit les informations que vous pouvez employer afin de configurer le commutateur de Nexus pour l'usage d'OALs.

Dans l'exemple qui est décrit dans cette section, il y a un serveur à l'IP address 10.10.10.1 qui envoie le trafic à un autre serveur à l'IP address 172.16.10.10 par la gamme d'un Nexus 7000 relient, qui a un ACL avec se connecter configuré.

Diagramme du réseau

La connexion entre les serveurs et le commutateur de gamme de Nexus 7000 se produit selon cette topologie :



Configurations

Terminez-vous ces étapes afin de configurer le commutateur pour l'usage d'OALs :

1. Configurez ces commandes globales afin d'activer OAL :
   ```
   logging ip access-list cache entries 8000
   logging ip access-list cache interval 300
   logging ip access-list cache threshold 0
   ```
   Voici un exemple :
   ```
   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. Appliquez cette configuration pour se connecter :
   ```
   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
   ```
   Voici un exemple :
   ```
   Nexus-7000(config)# logging level acllog 5
   Nexus-7000(config)# acllog match-log-level  5
   Nexus-7000(config)# logging logfile acllog 5
   ```
3. Configurez l'ACL afin d'activer se connecter. Les entrées doivent être configurées avec le **mot clé de journal** activé, suivant les indications de cet exemple :
   ```
   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. Appliquez l'ACL que vous avez configuré dans l'étape précédente à l'interface priée :
   ```
   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)#
   ```

Vérifiez

Utilisez les informations qui sont fournies dans cette section afin de vérifier que votre configuration fonctionne correctement.

Dans l'exemple qui est utilisé dans ce document, le ping est initié de l'hôte à l'adresse IP

10.10.10.1 à l'hôte à l'adresse IP 172.16.10.1. Sélectionnez la commande de **show logging ip access-list cache** dans le CLI afin de vérifier la circulation :

```
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#
```

Vous pouvez voir se connecter toutes les 300 secondes, comme c'est le délai par défaut :

```
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
```

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Notes de configuration

Cette section fournit les informations complémentaires au sujet de la configuration qui est décrite dans ce document.

Se connecter détaillé d'ACL

Dans des versions 6.2(6) et ultérieures du système d'exploitation de Nexus (NX-OS), se connecter *détaillé d'*ACL est disponible. La caractéristique se connecte ces informations :

- Adresses IP de source et de destination
- Source et destinations port
- Interface de source
- Protocol
- Nom d'ACL
- Action d'ACL (l'autorisation ou refusent)
- Interface appliquée
- Compte de paquet

Sélectionnez la commande **détaillée par ip access-list se connectante** dans le CLI afin d'activer se

connecter détaillé. Voici un exemple :

```
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)#
```

Voici une sortie de journalisation d'exemple après que se connecter détaillé soit activé :

```
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)#
```

Descriptions globales de commande OAL

Cette section décrit les commandes globales OAL qui sont utilisées afin de configurer la gamme de Nexus 7000 commutent pour l'usage d'OALs.

Commande	Description
Logging ip access-list cache de Switch(config)# {{number_of_entries d'entrées} | {secondes d'intervalle} | {number_of_packets de rate-limit} | {number_of_packets de seuil}}	Cette commande place les paramètres globaux OAL.
Switch(config)# aucun logging ip access-list cache {entrées | intervalle | rate-limit | seuil}	Cette commande retourne les paramètres globaux OAL aux valeur défaut.
entrées num_entries	Ces paramètres spécifient le nombre maximal d'entrées de journal sont cachées en logiciel. La plage est de 0 à 1,048,576. La valeur défaut est 8,000 entrées.
intervalle secondes	Ces paramètres spécifient l'intervalle de temps maximum avant qu entrée soit envoyée à un Syslog. La plage est de 5 à 86,400. La va par défaut est de 300 secondes.
seuil num_packets	Ces paramètres spécifient le nombre de correspondances de paqu (hit) avant qu'une entrée soit envoyée à un Syslog. La plage est de 1,000,000. La valeur par défaut est les paquets 0 (la limitation de d est éteinte), ainsi il signifie que le log système n'est pas déclenché le nombre de correspondances de paquet.

> Remarque: *Le forme no de* ces commandes CLI retourne seulement les paramètres aux valeurs par défaut s'ils ont été changés ; il ne retire pas la configuration, car le commutateur de gamme de Nexus 7000 a seulement l'option d'OAL.

Se connecter des descriptions de commande

Cette section décrit les commandes se connectantes qui sont utilisées afin de configurer la gamme de Nexus 7000 commutent pour l'usage d'OALs.

Commande	Description
nombre de niveau de correspondance-log d'acllog de switch(config)#	Cette commande spécifie le niveau se connectant qui doit être apparié que des entrées soient ouvertes une session le log d'ACL (acllog). La p est de 0 à 7. Le par défaut est valeur est 6.

Exemple : niveau 3 de correspondance-log d'acllog de switch(config)#	
Switch(config)# aucun nombre de niveau de correspondance-log d'acllog Exemple : switch(config)# aucun niveau 6 de correspondance-log d'acllog	Cette commande retourne le niveau se connectant à la valeur par défau
Switch(config)# se connectant le niveau d'importance de niveau d'installation Exemple : switch(config)# se connectant l'acllog de niveau 3	Ce messages de journalisation de commandes enables de l'installation spécifiée qui ont le niveau d'importance spécifié ou plus élevé. Dans l'exemple qui est utilisé dans ce document, le niveau d'*acllog* est placé tandis que la valeur par défaut est 2.
Switch(config)# aucun niveau se connectant [niveau d'importance d'installation] Exemple : switch(config)# aucun acllog de niveau se connectant 3	Cette commande remet à l'état initial le niveau d'importance se connect pour l'installation spécifiée à son niveau par défaut. Si vous ne spécifiez une installation et une sévérité nivelez, le périphérique remet à l'état initial tous les équipements à leurs niveaux par défaut. Dans l'exemple qui est utilisé dans ce document, l'a est retourné au (2) par défaut.
Niveau d'importance de fichier journal-nom de logging logfile de Switch(config)# [octets de taille] Exemple : acllog 3 de logging logfile de switch(config)#	Cette commande configure le nom du fichier journal qui est utilisé afin d'enregistrer les messages système et le niveau d'importance minimum avant de se connecter se produit. Vous pouvez sur option spécifier une de fichier maximum. Le niveau d'importance par défaut est 5, et le volu fichier par défaut est 10,485,760.
Switch(config)# aucun logging logfile [niveau d'importance de fichier journal-nom [octets de taille]] Exemple : switch(config)# aucun acllog 3 de logging logfile	Cette commande désactive se connecter au fichier journal.

> Remarque: Pour que les messages de log soient entrés dans les logs, le niveau se connectant pour l'installation de log d'ACL (acllog) et le niveau d'importance se connectant pour le fichier journal doivent être supérieur ou égal à la configuration *correspondance correspondance log de* log d'ACL.

Instructions et limites

Voici quelques importantes instructions et limites que vous devriez considérer avant que vous appliquiez la configuration qui est décrite dans ce document :

- Le Nexus 7000 et les Commutateurs de gamme 7700 prennent en charge seulement OAL.
- Se connecter d'ACL ne fonctionne pas avec la configuration de capture d'ACL.
- L'option de *log* dans le de sortie ACLs n'est pas prise en charge pour des paquets de multidiffusion.
- Le support se connectant détaillé n'est pas disponible pour des paquets d'IPv6.

- Le niveau se connectant pour l'installation d'*acllog* et la sévérité de *logging logfile* doit être configuré tels qu'ils sont supérieur ou égal à la configuration *correspondance correspondance log d'acllog*.

- N'utilisez pas l'ordre de **capture de liste d'accès de matériel** tandis qu'OAL est utilisé. Quand cette commande est utilisée à côté d'OAL, et de vous capture d'ACL d'enable, un message d'avertissement apparaît afin de vous informer que se connecter d'ACL est désactivé pour tous les contextes de périphérique virtuel (VDCs). Quand vous désactivez la capture d'ACL, se connecter d'ACL est activé. Pour que ce de processus fonctionne correctement, débronchement avec l'utilisation de l'**aucun** ordre de **capture de liste d'accès de matériel**.