Exemple de configuration de journalisation des listes de contrôle d'accès optimisées pour les commutateurs des gammes Nexus 7000 et 7700

Contenu

Introduction
Conditions préalables
Conditions requises
Components Used
Informations générales
Configuration
Diagramme du réseau
Configurations
Vérification
Dépannage
Notes de configuration
Journalisation détaillée des listes de contrôle d’accès
Description des commandes OAL globales
Description des commandes de journalisation
Directives et limitations

Introduction

Ce document décrit comment configurer la journalisation OAL (Optimized Access Control List) sur les commutateurs Cisco Nexus 7000 et 7700.

Conditions préalables

Conditions requises

Cisco vous recommande de connaître les configurations Nexus avec les listes de contrôle d'accès de base avant de tenter la configuration décrite dans ce document.

Components Used

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

logiciel suivantes :

- Cisco Nexus 7000 Series Switches
- Cisco Nexus 7700 Series Switches

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

Les listes de contrôle d’accès activées pour la journalisation fournissent des informations sur le trafic lorsqu’il traverse le réseau ou est abandonné par des périphériques réseau. Malheureusement, la journalisation des listes de contrôle d’accès peut être gourmande en CPU et affecter négativement d’autres fonctions du périphérique réseau. Afin de réduire les cycles CPU, le commutateur Cisco Nexus 7000 utilise des OAL.

L'utilisation des listes de contrôle d'accès fournit la prise en charge matérielle de la journalisation des listes de contrôle d'accès. L'OAL autorise ou supprime les paquets dans le matériel et utilise une routine optimisée afin d'envoyer des informations au superviseur afin qu'il puisse générer les messages de journalisation. Par exemple, lorsqu'un paquet atteint une liste de contrôle d'accès avec journalisation activée lors de son transfert dans le matériel, une copie du paquet est créée dans le matériel et le paquet est pointé vers le superviseur pour journalisation conformément à l'intervalle de temps configuré.

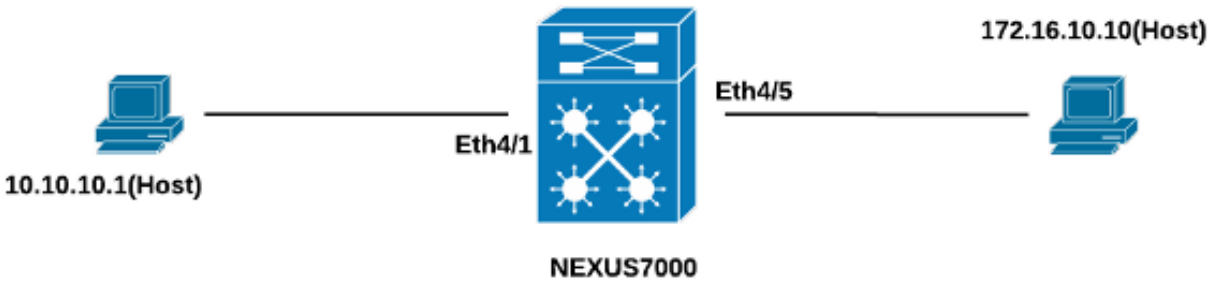
Configuration

Cette section fournit des informations que vous pouvez utiliser afin de configurer le commutateur Nexus pour l'utilisation des OAL.

Dans l'exemple décrit dans cette section, il y a un hôte à l'adresse IP 10.10.10.1 qui envoie du trafic à un autre hôte à l'adresse IP 172.16.10.10 via une interface Nexus 7000, qui a une liste de contrôle d'accès avec journalisation configurée.

Diagramme du réseau

La connexion entre les hôtes et le commutateur de la gamme Nexus 7000 se produit conformément à cette topologie :



Configurations

Complétez ces étapes afin de configurer le commutateur pour l'utilisation des OAL :

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. Appliquer cette configuration à la journalisation :

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

   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 la liste de contrôle d'accès afin d'activer la journalisation. Les entrées doivent être configurées avec le mot clé **log** activé, comme indiqué dans 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 la liste de contrôle d'accès que vous avez configurée à l'étape précédente à l'interface requise :

   ```
   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)#
```

Vérification

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

Dans l'exemple utilisé dans ce document, la requête ping est lancée de l'hôte à l'adresse IP 10.10.10.1 vers l'hôte à l'adresse IP 172.16.10.1. Entrez la commande **show logging ip access-list cache** dans l'interface de ligne de commande afin de vérifier le flux de trafic :

```
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 la journalisation toutes les 300 secondes, car il s'agit de l'intervalle de temps 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
```

Dépannage

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

Notes de configuration

Cette section fournit des informations supplémentaires sur la configuration décrite dans ce document.

Journalisation détaillée des listes de contrôle d'accès

Dans Nexus Operating System (NX-OS) Versions 6.2(6) et ultérieures, une journalisation *détaillée* des listes de contrôle d'accès est disponible. La fonction enregistre ces informations :

- Adresses IP de source et de destination
- Ports source et de destination
- Interface source
- Protocol
- Nom ACL
- Action ACL (autorisation ou refus)
- Interface appliquée
- Nombre de paquets

Entrez la commande **logging ip access-list detail** dans l'interface de ligne de commande afin d'activer la journalisation détaillée. 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 un exemple de sortie de journalisation après l'activation de la journalisation détaillée :

```
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
```

Description des commandes OAL globales

Cette section décrit les commandes OAL globales utilisées pour configurer le commutateur Nexus 7000 pour l'utilisation des OAL.

Commande	Description
Switch(config)# logging ip access-list cache {{entry number_of_entry} | {interval seconds} | {rate-limit number_of_packets} | {nombre_seuil_paquets}	Cette commande définit les paramètres globaux OAL.
Switch(config)# no logging ip access-list cache {entrées | intervalle | taux limite | seuil}	Cette commande rétablit les paramètres globaux OAL par défaut.
entrées nombre_entrées	Ces paramètres spécifient le nombre maximal d'entrées de journal qui s mises en cache dans le logiciel. La vitesse est comprise entre 0 et 1,048,576. La valeur par défaut est 8 000 entrées.

intervalle secondes	Ces paramètres spécifient l'intervalle de temps maximal avant l'envoi d'entrée à un syslog. La vitesse est comprise entre 5 et 86,400. La valeur défaut est de 300 secondes.
seuil num_packets	Ces paramètres spécifient le nombre de correspondances de paquets avant l'envoi d'une entrée à un syslog. La vitesse est comprise entre 0 1,000,000. La valeur par défaut est 0 paquet (la limitation de débit est désactivée), ce qui signifie que le journal système n'est pas déclenché nombre de correspondances de paquets.

Note: La forme *no* de ces commandes CLI rétablit les paramètres par défaut uniquement s'ils ont été modifiés ; il ne supprime pas la configuration, car le commutateur de la gamme Nexus 7000 n'a que l'option OAL.

Description des commandes de journalisation

Cette section décrit les commandes de journalisation utilisées afin de configurer le commutateur Nexus 7000 pour l'utilisation d'OAL.

Commande	Description
switch(config)# acllog match-log-level number Exemple : switch(config)# acllog match-log- niveau 3	Cette commande spécifie le niveau de journalisation qui doit être mis en correspondance avant que les entrées soient enregistrées dans le journal listes de contrôle d'accès (acllog). La vitesse est comprise entre 0 et 7. La valeur par défaut est 6.
Switch(config)# no acllog match-log-level number Exemple : switch(config)# no acllog match-log- niveau 6	Cette commande rétablit le niveau de journalisation sur le paramètre par (6).
Switch(config)# logging level, installation niveau de gravité Exemple : switch(config)# logging level acllog 3	Cette commande active la journalisation des messages de l'installation spécifiée qui ont le niveau de gravité spécifié ou supérieur. Dans l'exemple utilisé dans ce document, le niveau *acllog* est défini sur 3, alors que le paramètre par défaut est 2.
Switch(config)# no logging level [niveau de gravité de l'installation] Exemple : switch(config)# no logging level acllog 3	Cette commande réinitialise le niveau de gravité de journalisation de l'installation spécifiée à son niveau par défaut. Si vous ne spécifiez pas d'installation et de gravité , le périphérique réinitialise toutes les installations à leurs niveaux par défa Dans l'exemple utilisé dans ce document, l'acllog est rétabli à la valeur pa défaut (2).
Switch(config)# logging logfile nom_fichier_journal niveau_gravité [taille octets] Exemple : switch(config)# logging logfile acllog 3	Cette commande configure le nom du fichier journal utilisé pour stocker le messages système et le niveau de gravité minimal avant la journalisation. pouvez éventuellement spécifier une taille de fichier maximale. Le niveau gravité par défaut est 5 et la taille de fichier par défaut est 10 485 760.
Switch(config)# no logging logfile [logfile-name séverlevel [size bytes]] Exemple : switch(config)# no logging logfile acllog 3	Cette commande désactive la journalisation dans le fichier journal.

Note: Pour que les messages du journal soient entrés dans les journaux, le niveau de journalisation de la fonction de journalisation de la liste de contrôle d'accès (acllog) et le niveau de gravité de la journalisation du fichier journal doivent être supérieurs ou égaux au

paramètre de niveau *match-log de la* liste de contrôle d'accès.

Directives et limitations

Voici quelques directives et limitations importantes que vous devez prendre en compte avant d'appliquer la configuration décrite dans ce document :

- Les commutateurs des gammes Nexus 7000 et 7700 ne prennent en charge que la fonctionnalité OAL.
- La journalisation des listes de contrôle d’accès ne fonctionne pas avec la fonction de capture des listes de contrôle d’accès.
- L'option *log* dans les listes de contrôle d'accès de sortie n'est pas prise en charge pour les paquets de multidiffusion.
- La journalisation détaillée n'est pas disponible pour les paquets IPv6.
- Le niveau de journalisation pour la fonction *acllog* et la gravité du *journal* de journalisation doivent être configurés de manière à être supérieur ou égal au paramètre de *niveau de journal de correspondance acllog*.
- N'utilisez pas la commande **hardware access-list capture** tant qu'OAL est utilisé. Lorsque cette commande est utilisée avec OAL et que vous activez la capture des listes de contrôle d'accès, un message d'avertissement s'affiche afin de vous informer que la journalisation des listes de contrôle d'accès est désactivée pour tous les contextes de périphériques virtuels (VDC). Lorsque vous désactivez la capture des listes de contrôle d'accès, la journalisation des listes de contrôle d'accès est activée. Pour que ce processus fonctionne correctement, désactivez avec l'utilisation de la commande **no hardware access-list capture**.