Exemple de capture des listes de contrôle d'accès des commutateurs de la gamme Nexus 7000

Contenu

Introduction

La capture de liste de contrôle d'accès (ACL) vous permet de capturer sélectivement le trafic sur une interface ou un réseau local virtuel (VLAN). Lorsque vous activez l'option de capture pour une règle ACL, les paquets qui correspondent à cette règle sont transférés ou abandonnés en fonction de l'action d'autorisation ou de refus spécifiée et peuvent également être copiés vers un autre port de destination pour une analyse plus approfondie. Une règle ACL avec l'option de capture peut être appliquée :

1. Dans un VLAN,
2. Dans la direction d'entrée sur toutes les interfaces,
3. Dans la direction de sortie sur toutes les interfaces de couche 3.

Cette fonctionnalité est prise en charge depuis Nexus 7000 NX-OS version 5.2 et ultérieure. Ce document fournit un exemple de guide de référence rapide sur la façon de configurer cette fonctionnalité.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

- Nexus 7000 avec les versions 5.2.x et ultérieures.
- Carte de ligne de la gamme M1.

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Exemple de configuration d’ACL

Voici un exemple de configuration de la capture ACL appliquée à un VLAN, également appelé capture VACL (Virtual LAN Access Control List). Dix snifeurs gigabits désignés peuvent ne pas être réalisables pour tous les paysages. La capture sélective du trafic peut s'avérer très utile dans de tels environnements, notamment lors du dépannage lorsque les volumes de trafic sont élevés.

```
!! 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
```

Vous pouvez également vérifier la programmation TCAM (ternary content Addressable Memory) de la liste d'accès. Ce résultat correspond au VLAN 500 pour le module 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]
```

Cavates

1. Une seule session de capture de liste de contrôle d'accès peut être active à un moment donné dans le système à travers les contextes de périphériques virtuels (VDC).
2. Les modules de la gamme Nexus 7000 F1 ne prennent pas en charge la capture des listes de contrôle d'accès.
3. Les modules de la gamme Nexus 7000 F2 ne prennent pas actuellement en charge la capture des listes de contrôle d'accès, mais cela peut se trouver dans la feuille de route.
4. La capture des listes de contrôle d'accès sur les modules Nexus 7000 M2 est prise en charge avec Cisco NX-OS version 6.1(1) et ultérieure.
5. La capture des listes de contrôle d'accès sur les modules Nexus 7000 M1 est prise en charge avec Cisco NX-OS version 5.2(1) et ultérieure.
6. La capture des listes de contrôle d'accès n'est pas compatible avec la journalisation des listes de contrôle d'accès. Par conséquent, si vous avez des listes de contrôle d'accès avec un mot clé **log**, elles ne fonctionnent pas après que vous ayez entré globalement **la capture de liste d'accès matérielle**.
7. En raison du bogue CSCug20139, l'exemple de ce document est documenté avec une **session de capture** par ACE au lieu de par ACL, jusqu'à ce que le bogue soit résolu.

Informations connexes

- Guide de configuration de la sécurité NX-OS de la gamme Cisco Nexus 7000, version 6.x, exemples de configuration pour les listes de contrôle d'accès IP
- Support et documentation techniques - Cisco Systems