Capture de VACL pour l'analyse du trafic granulaire avec Cisco Catalyst 6000/6500 exécutant le logiciel CatOS

Contenu

Introduction

Ce document fournit un exemple de configuration pour l'utilisation de la fonction de port de capture VACL (VLAN Access Control List) pour l'analyse du trafic réseau de manière plus précise. Ce document indique également l'avantage de l'utilisation des ports de capture VACL par rapport à l'utilisation de l'analyseur de ports commutés (SPAN) basé sur VLAN (VSPAN).

Afin de configurer la fonctionnalité VACL Capture Port sur Cisco Catalyst 6000/6500 qui exécute le logiciel Cisco IOS®, référez-vous à Capture VACL pour une analyse granulaire du trafic avec Cisco Catalyst 6000/6500 exécutant le logiciel Cisco IOS.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- LAN virtuel : reportez-vous à VLAN/VLAN Trunking Protocol (VLAN/VTP) - Introduction pour plus d'informations.
- Listes d'accès : reportez-vous à Configuration du contrôle d'accès pour plus d'informations.

Components Used

Les informations de ce document sont basées sur le commutateur de la gamme Cisco Catalyst 6506 qui exécute Catalyst OS version 8.1(2).

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.

Produits connexes

Cette configuration peut également être utilisée avec les commutateurs de la gamme Cisco Catalyst 6000 / 6500 qui exécutent Catalyst OS version 6.3 et ultérieures.

Conventions

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

Informations générales

SPAN basé sur VLAN

SPAN copie le trafic d'un ou de plusieurs ports sources dans un VLAN ou d'un ou plusieurs VLAN vers un port de destination pour analyse. La fonctionnalité SPAN locale prend en charge les ports source, les VLAN source et les ports de destination sur le même commutateur de la gamme Catalyst 6500.

Un port source est un port surveillé pour l'analyse du trafic réseau. Un VLAN source est un VLAN surveillé pour l'analyse du trafic réseau. La fonctionnalité VSPAN (VLAN-based SPAN) analyse le trafic réseau dans un ou plusieurs VLAN. Vous pouvez configurer VSPAN en tant que SPAN d'entrée, SPAN de sortie ou les deux. Tous les ports des VLAN source deviennent les ports source opérationnels de la session VSPAN. Les ports de destination, s'ils appartiennent à l'un des VLAN source d'administration, sont exclus de la source opérationnelle. Si vous ajoutez ou supprimez les ports des VLAN source d'administration, les sources opérationnelles sont modifiées en conséquence.

Instructions pour les sessions VSPAN :

- Les ports d’agrégation sont inclus comme ports source pour les sessions VSPAN, mais seuls les VLAN qui figurent dans la liste source Admin sont surveillés si ces VLAN sont actifs pour l’agrégation.
- Pour les sessions VSPAN avec SPAN d'entrée et de sortie configurées, le système fonctionne en fonction du type de moteur de supervision que vous avez :WS-X6K-SUP1A-PFC, WS-X6K-SUP1A-MSFC, WS-X6K-S1A-MSFC2, WS-X6K-S2-PFC2, WS-X6K-S1A-MSFC2, WS-

SUP720, WS-SUP32-GE-3B - Deux paquets sont transférés par le Port de destination SPAN si les paquets sont commutés sur le même VLAN.WS-X6K-SUP1-2GE, WS-X6K-SUP1A-2GE : un seul paquet est transféré par le port de destination SPAN.

- Un port intrabande n'est pas inclus comme source opérationnelle pour les sessions VSPAN.
- Lorsqu'un VLAN est effacé, il est supprimé de la liste source pour les sessions VSPAN.
- Une session VSPAN est désactivée si la liste VLAN source Admin est vide.
- Les VLAN inactifs ne sont pas autorisés pour la configuration VSPAN.
- Une session VSPAN est inactive si l'un des VLAN source devient les VLAN RSPAN.

Référez-vous à Caractéristiques du VLAN source pour plus d'informations sur les VLAN source.

ACL VLAN

Les VACL peuvent accéder au contrôle de tout le trafic. Vous pouvez configurer les VACL sur le commutateur pour qu'elles s'appliquent à tous les paquets qui sont acheminés à destination ou en provenance d'un VLAN ou qui sont pontés au sein d'un VLAN. Les VACL sont strictement destinées au filtrage des paquets de sécurité et à la redirection du trafic vers des ports de commutation physiques spécifiques. Contrairement aux listes de contrôle d'accès Cisco IOS, les listes de contrôle d'accès virtuelles ne sont pas définies par direction (entrée ou sortie).

Vous pouvez configurer les VACL sur les adresses de couche 3 pour IP et IPX. Tous les autres protocoles sont contrôlés par les adresses MAC et EtherType à l'aide des VACL MAC. Le trafic IP et le trafic IPX ne sont pas contrôlés par les VACL MAC. Tous les autres types de trafic (AppleTalk, DECnet, etc.) sont classés comme trafic MAC. Les VACL MAC sont utilisées pour contrôler ce trafic.

ACE pris en charge dans les VACL

La VACL contient une liste ordonnée d'entrées de contrôle d'accès (ACE). Chaque VACL peut contenir des ACE d'un seul type. Chaque ACE contient un certain nombre de champs qui correspondent au contenu d'un paquet. Chaque champ peut avoir un masque de bit associé pour indiquer quels bits sont pertinents. Une action est associée à chaque ACE qui décrit ce que le système doit faire avec le paquet lorsqu'une correspondance se produit. L'action dépend de la fonction. Les commutateurs de la gamme Catalyst 6500 prennent en charge trois types d'ACE dans le matériel :

- ACE IP
- ACE IPX
- ACE Ethernet

Ce tableau répertorie les paramètres associés à chaque type ACE :

Type ACE	TCP ou UDP	ICMP	Autre IP	IPX	Ethernet
Paramètres de couche 4	Port source	-	-	-	-
	Opérateur de port source	-	-	-	-
	Destination Port (port de	-	-	-	-

	destination)				
	Opérateur de port de destination	Code ICMP	-	-	-
	S/O	Type ICMP	S/O	-	-
Paramètres de couche 3	Octet ToS IP	Octet ToS IP	Octet ToS IP	-	-
	Adresse IP source	Adresse IP source	Adresse IP source	Réseau source IPX	-
	Adresse de destination IP	Adresse de destination IP	Adresse de destination IP	Réseau de destination IP	-
	-	-	-	Noeud de destination IP	-
	TCP ou UDP	ICMP	Autre protocole	Type de paquet IPX	-
Paramètres de couche 2	-	-	-	-	TypeÉther
	-	-	-	-	Adresse source Ethernet
	-	-	-	-	Adresse de destination Ethernet

Avantages de l'utilisation de VACL par rapport à l'utilisation de VSPAN

L'utilisation de VSPAN pour l'analyse du trafic présente plusieurs limites :

- Tout le trafic de couche 2 qui circule dans un VLAN est capturé. Cela augmente la quantité de données à analyser.
- Le nombre de sessions SPAN pouvant être configurées sur les commutateurs de la gamme Catalyst 6500 est limité. Référez-vous à Récapitulatif des fonctionnalités et limitations pour plus d'informations.
- Un port de destination reçoit des copies du trafic envoyé et reçu pour tous les ports sources surveillés. Si un port de destination est surabonné, il peut devenir saturé. Cet encombrement peut affecter le transfert du trafic sur un ou plusieurs des ports sources.

La fonctionnalité VACL Capture Port peut aider à surmonter certaines de ces limitations. Les listes

de contrôle d’accès virtuel ne sont pas conçues pour surveiller le trafic. Cependant, avec une large gamme de fonctionnalités permettant de classer le trafic, la fonctionnalité Capture Port a été introduite afin de simplifier l'analyse du trafic réseau. Voici les avantages de l'utilisation des ports de capture VACL par rapport à VSPAN :

- Analyse granulaire du traficLes VACL peuvent correspondre en fonction de l'adresse IP source, de l'adresse IP de destination, du type de protocole de couche 4, des ports de couche 4 source et de destination, ainsi que d'autres informations. Cette fonctionnalité rend les VACL très utiles pour l'identification et le filtrage granulaires du trafic.
- Nombre de sessionsLes VACL sont appliquées au matériel. Le nombre d'ACE pouvant être créés dépend de la TCAM disponible dans les commutateurs.
- Surabonnement au port de destinationL'identification granulaire du trafic réduit le nombre de trames à transférer au port de destination et réduit ainsi la probabilité de surabonnement.
- PerformancesLes VACL sont appliquées au matériel. Il n'y a aucune pénalité en termes de performances pour l'application de VACL à un VLAN sur les commutateurs de la gamme Cisco Catalyst 6500.

Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

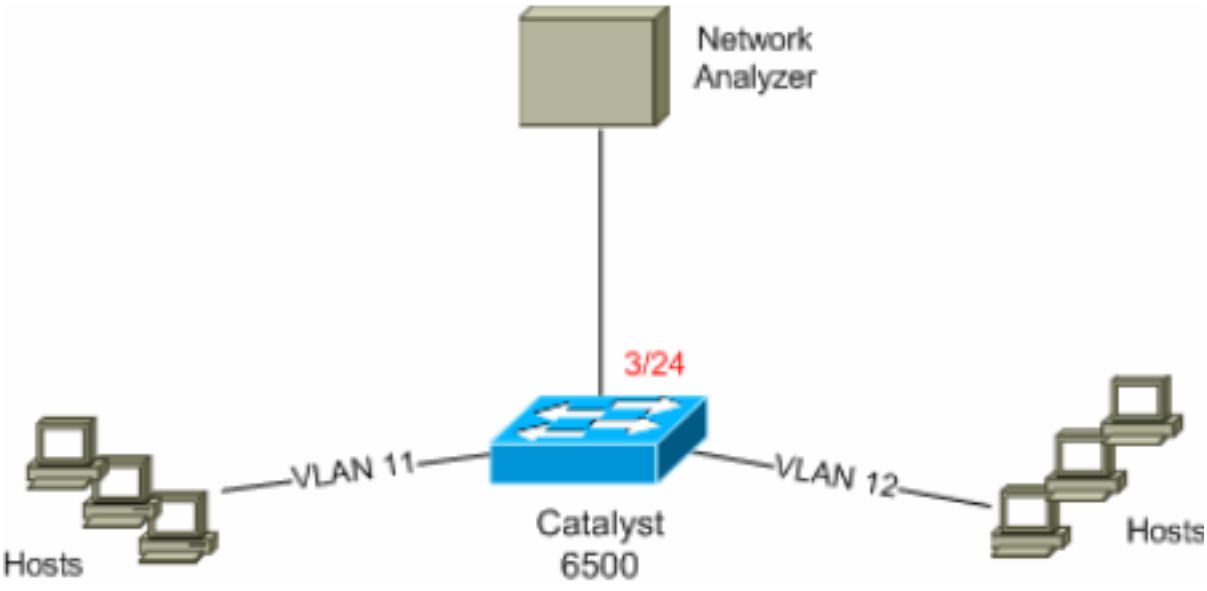
Ce document utilise les configurations suivantes :

- Configuration avec SPAN basé sur VLAN
- Configuration avec VACL

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configuration avec SPAN basé sur VLAN

Cet exemple de configuration répertorie les étapes requises pour capturer tout le trafic de couche 2 qui circule dans VLAN 11 et VLAN 12 et les envoyer au périphérique Network Analyzer.

1. Spécifiez le trafic intéressant.Dans cet exemple, c'est le trafic qui circule dans VLAN 100 et VLAN 200.
```
6K-CatOS> (enable) set span 11-12 3/24
!--- where 11-12 specifies the range of source VLANs and 3/24 specify the destination port.

2007 Jul 12 21:45:43 %SYS-5-SPAN_CFGSTATECHG:local span session inactive for des
tination port 3/24

Destination     : Port 3/24
Admin Source    : VLAN 11-12
Oper Source     : Port 3/11-12,16/1
Direction       : transmit/receive
Incoming Packets: disabled
Learning        : enabled
Multicast       : enabled
Filter          : -
Status          : active

6K-CatOS> (enable) 2007 Jul 12 21:45:43 %SYS-5-SPAN_CFGSTATECHG:local span sessi
on active for destination port 3/24
```
   Avec cela, tout le trafic de couche 2 qui appartient aux VLAN 11 et 12 est copié et envoyé au port 3/24.
2. Vérifiez votre configuration SPAN à l'aide de la commande **show span all**.
```
6K-CatOS> (enable) show span all

Destination     : Port 3/24
Admin Source    : VLAN 11-12
Oper Source     : Port 3/11-12,16/1
Direction       : transmit/receive
Incoming Packets: disabled
Learning        : enabled
Multicast       : enabled
Filter          : -
Status          : active


Total local span sessions:  1

No remote span session configured
6K-CatOS> (enable)
```

Configuration avec VACL

Dans cet exemple de configuration, l'administrateur réseau a plusieurs besoins :

- Le trafic HTTP d'une plage d'hôtes (10.12.12.128/25) dans le VLAN 12 vers un serveur spécifique (10.11.11.100) dans le VLAN 11 doit être capturé.
- Le trafic UDP (Multicast User Datagram Protocol) dans la direction de transmission destinée à l'adresse de groupe 239.0.0.100 doit être capturé à partir du VLAN 11.

1. Définissez le trafic intéressant à l'aide des listes de contrôle d'accès de sécurité. N'oubliez pas de mentionner la **capture** par mot clé pour tous les ACE définis.
```
6K-CatOS> (enable) set security acl ip HttpUdp_Acl permit tcp 10.12.12.128 0.0.0.127 host
10.11.11.100 eq www capture
!--- Command wrapped to the second line. HttpUdp_Acl editbuffer modified. Use 'commit'
```

```
command to apply changes. 6K-CatOS> (enable) set security acl ip HttpUdp_Acl permit udp any
host 239.0.0.100 capture
HttpUdp_Acl editbuffer modified. Use 'commit' command to apply changes.
```

2. Vérifiez si la configuration ACE est correcte et dans le bon ordre.

```
6K-CatOS> (enable) show security acl info HttpUdp_Acl editbuffer
set security acl ip HttpUdp_Acl
-------------------------------------------------
1. permit tcp 10.12.12.128 0.0.0.127 host 10.11.11.100 eq 80 capture
2. permit udp any host 239.0.0.100 capture
ACL HttpUdp_Acl Status: Not Committed
6K-CatOS> (enable)
```

3. Validez la liste de contrôle d'accès sur le matériel.

```
6K-CatOS> (enable) commit security acl HttpUdp_Acl
ACL commit in progress.

ACL 'HttpUdp_Acl' successfully committed.
6K-CatOS> (enable)
```

4. Vérifiez l'état de la liste de contrôle d'accès.

```
6K-CatOS> (enable) show security acl info HttpUdp_Acl editbuffer
set security acl ip HttpUdp_Acl
-------------------------------------------------
1. permit tcp 10.12.12.128 0.0.0.127 host 10.11.11.100 eq 80 capture
2. permit udp any host 239.0.0.100 capture
ACL HttpUdp_Acl Status: Committed
6K-CatOS> (enable)
```

5. Appliquez la carte d'accès VLAN aux VLAN appropriés.

```
6K-CatOS> (enable) set security acl map HttpUdp_Acl ?
  <vlans>                    Vlan(s) to be mapped to ACL
6K-CatOS> (enable) set security acl map HttpUdp_Acl 11
Mapping in progress.

ACL HttpUdp_Acl successfully mapped to VLAN 11.
6K-CatOS> (enable)
```

6. Vérifiez le mappage de la liste de contrôle d'accès au VLAN.

```
6K-CatOS> (enable) show security acl map HttpUdp_Acl
ACL HttpUdp_Acl is mapped to VLANs:
11
6K-CatOS> (enable)
```

7. Configurez le port de capture.

```
6K-CatOS> (enable) set vlan 11 3/24
VLAN  Mod/Ports
---- ----------------------
11    3/11,3/24
6K-CatOS> (enable)


6K-CatOS> (enable) set security acl capture-ports 3/24
Successfully set 3/24 to capture ACL traffic.
6K-CatOS> (enable)
```

Remarque : si une liste de contrôle d'accès est mappée à plusieurs VLAN, le port de capture doit être configuré pour tous ces VLAN. Afin que le port de capture autorise plusieurs VLAN, configurez le port en tant que trunk et autorisez uniquement les VLAN mappés à la liste de contrôle d'accès. Par exemple, si la liste de contrôle d'accès est mappée aux VLAN 11 et 12, complétez la configuration.

```
6K-CatOS> (enable) clear trunk 3/24 1-10,13-1005,1025-4094
6K-CatOS> (enable) set trunk 3/24 on dot1q 11-12
6K-CatOS> (enable) set security acl capture-ports 3/24
```

8. Vérifiez la configuration du port de capture.

```
6K-CatOS> (enable) show security acl capture-ports
ACL Capture Ports: 3/24
6K-CatOS> (enable)
```

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

- **show security acl info** : affiche le contenu de la VACL actuellement configurée ou la dernière validée pour la mémoire NVRAM et le matériel.
```
6K-CatOS> (enable) show security acl info HttpUdp_Acl
set security acl ip HttpUdp_Acl
---------------------------------------------
1. permit tcp 10.12.12.128 0.0.0.127 host 10.11.11.100 eq 80 capture
2. permit udp any host 239.0.0.100 capture
6K-CatOS> (enable)
```
- **show security acl map** : affiche le mappage ACL vers VLAN ou ACL vers port pour une ACL, un port ou un VLAN spécifique.
```
6K-CatOS> (enable) show security acl map all
ACL Name                        Type Vlans
------------------------------- ---- -----
HttpUdp_Acl                        IP   11
6K-CatOS> (enable)
```
- **show security acl capture-ports** : affiche la liste des ports de capture.
```
6K-CatOS> (enable) show security acl capture-ports
ACL Capture Ports: 3/24
6K-CatOS> (enable)
```

Dépannage

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

Informations connexes

- Capture de VACL pour l'analyse du trafic granulaire avec Cisco Catalyst 6000/6500 exécutant le logiciel Cisco IOS
- Configuration du contrôle d'accès - Guide de configuration du logiciel de la gamme Catalyst 6500, 8.6
- Pages de support pour les produits LAN
- Page de support sur la commutation LAN
- Support et documentation techniques - Cisco Systems