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

Contenu

Introduction

Ce document fournit un exemple de configuration pour l'utilisation de la fonctionnalité de port de capture VLAN ACL (VACL) pour l'analyse du trafic réseau d'une manière plus granulaire. Ce document présente également l'avantage qu'il y a à utiliser le port de capture VACL par rapport à l'utilisation du SPAN basé sur un VLAN (VSPAN).

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

Conditions préalables

Conditions requises

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

- Listes d'accès IP : référez-vous à Configuration des listes d'accès IP pour plus d'informations.
- Réseau local virtuel: référez-vous à VLAN/VLAN Trunking Protocol (VLAN/VTP) - Introduction pour plus d'informations.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes : Commutateur de la gamme Cisco Catalyst 6506 qui exécute le logiciel Cisco IOS® version 12.2(18)SXF8.

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 le logiciel Cisco IOS version 12.1(13)E et ultérieure.

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 (Switched Port ANalyzer) copie le trafic d'un ou 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 VLAN source est un VLAN surveillé pour l'analyse du trafic réseau. Le VLAN SPAN (VSPAN) utilise un VLAN comme source SPAN. Tous les ports des VLAN source deviennent des ports source. Un port source est un port surveillé pour l'analyse du trafic réseau. Les ports agrégés peuvent être configurés en tant que ports source et mélangés avec des ports source non agrégés, mais SPAN ne copie pas l'encapsulation à partir d'un port agrégé source.

Pour les sessions VSPAN configurées à la fois en entrée et en sortie, deux paquets sont transférés du port de destination si les paquets sont commutés sur le même VLAN (un comme trafic d'entrée depuis le port d'entrée et un comme trafic de sortie depuis le port de sortie).

VSPAN surveille uniquement le trafic qui quitte ou entre des ports de couche 2 dans le VLAN.

- Si vous configurez un VLAN comme source d'entrée et que le trafic est acheminé vers le VLAN surveillé, le trafic routé n'est pas surveillé car il n'apparaît jamais comme trafic d'entrée qui entre dans un port de couche 2 dans le VLAN.
- Si vous configurez un VLAN comme source de sortie et que le trafic est acheminé hors du

VLAN surveillé, le trafic routé n'est pas surveillé car il n'apparaît jamais comme trafic de sortie qui laisse un port de couche 2 dans le VLAN.

Pour plus d'informations sur les VLAN source, référez-vous à Caractéristiques du VLAN source.

ACL VLAN

Les VACL peuvent fournir un contrôle d'accès pour tous les paquets qui sont pontés au sein d'un VLAN ou qui sont routés vers ou depuis un VLAN ou une interface WAN pour la capture de VACL. Contrairement aux listes de contrôle d'accès standard ou étendues de Cisco IOS configurées sur des interfaces de routeur uniquement et appliquées sur des paquets routés uniquement, les listes de contrôle d'accès virtuelles s'appliquent à tous les paquets et peuvent être appliquées à n'importe quelle interface VLAN ou WAN. Les VACL sont traitées dans le matériel. Les VACL utilisent les ACL Cisco IOS. Les VACL ignorent tous les champs ACL Cisco IOS qui ne sont pas pris en charge dans le matériel.

Vous pouvez configurer des VACL pour le trafic IP, IPX et de couche MAC. Les VACL appliquées aux interfaces WAN prennent uniquement en charge le trafic IP pour la capture VACL.

Lorsque vous configurez une VACL et l'appliquez à un VLAN, tous les paquets qui entrent dans le VLAN sont vérifiés par rapport à cette VACL. Si vous appliquez une VACL au VLAN et une ACL à une interface routée dans le VLAN, un paquet qui entre dans le VLAN est d'abord vérifié par rapport à la VACL et, si cela est autorisé, est ensuite vérifié par rapport à la liste de contrôle d'accès d'entrée avant d'être traité par l'interface routée. Lorsque le paquet est routé vers un autre VLAN, il est d'abord vérifié par rapport à la liste de contrôle d'accès de sortie qui est appliquée à l'interface routée et, si cela est autorisé, la liste de contrôle d'accès configurée pour le VLAN de destination est appliquée. Si une VACL est configurée pour un type de paquet et qu'un paquet de ce type ne correspond pas à la VACL, l'action par défaut est deny. Voici les directives relatives à l'option de capture dans VACL.

- Le port de capture ne peut pas être un port ATM.
- Le port de capture doit être à l'état de transmission Spanning Tree pour le VLAN.
- Le commutateur n'a aucune restriction sur le nombre de ports de capture.
- Le port de capture capture capture uniquement les paquets autorisés par la liste de contrôle d'accès configurée.
- Les ports de capture transmettent uniquement le trafic qui appartient au VLAN du port de capture. Configurez le port de capture en tant que trunk qui transporte les VLAN requis afin de capturer le trafic qui va à de nombreux VLAN.

Attention : Une combinaison incorrecte de listes de contrôle d'accès peut perturber le flux de trafic. Faites preuve d'une plus grande prudence lors de la configuration des listes de contrôle d'accès dans votre périphérique.

Remarque : la VACL n'est pas prise en charge avec IPv6 sur un commutateur de la gamme Catalyst 6000. En d'autres termes, la redirection des listes de contrôle d'accès VLAN et IPv6 ne sont pas compatibles, de sorte que les listes de contrôle d'accès ne peuvent pas être utilisées pour correspondre au trafic IPv6.

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 Limites de session SPAN et RSPAN locales 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 VACL ne sont pas principalement conçues pour surveiller le trafic, mais, 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 dans le matériel ; le nombre d'entrées de contrôle d'accès (ACE) qui peuvent être créées dépend du 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 dans le 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

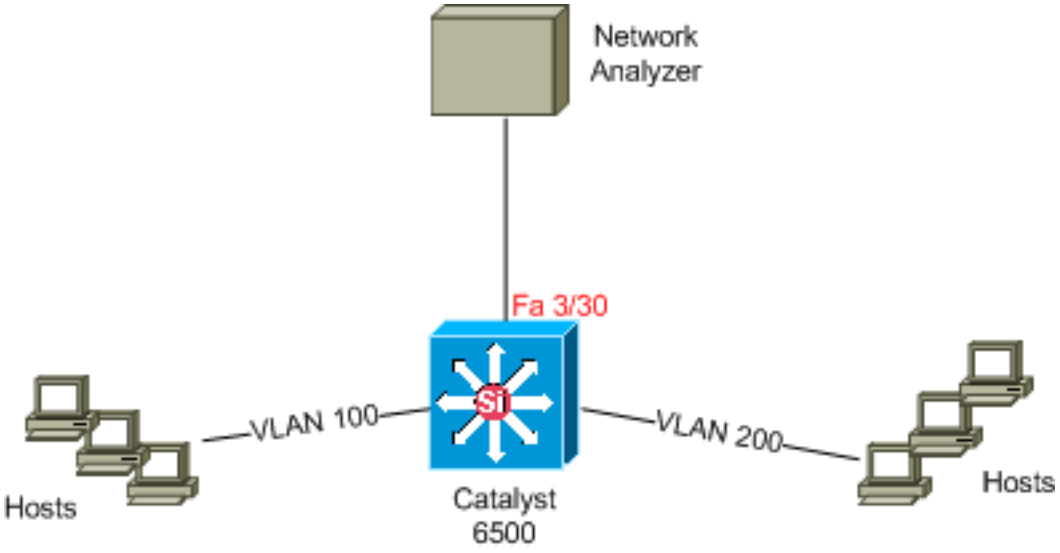
Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

- Configuration avec SPAN basé sur VLAN
- Configuration avec VACL

Remarque : Utilisez l'outil de recherche de commandes (clients inscrits seulement) pour en savoir plus sur les commandes figurant dans le présent document.

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 100 et VLAN 200 et les envoyer au périphérique Network Analyzer.

1. Spécifiez le trafic intéressant. Dans notre exemple, c'est le trafic qui circule dans VLAN 100 et VLAN 200.

```
Cat6K-IOS#conf t
Cat6K-IOS(config)#monitor session 50 source vlan 100 , 200 ?
  ,     Specify another range of VLANs
  -     Specify a range of VLANs
  both  Monitor received and transmitted traffic
  rx    Monitor received traffic only
  tx    Monitor transmitted traffic only
  <cr>

 !--- Default is to monitor both received and transmitted traffic

Cat6K-IOS(config)#monitor session 50 source vlan 100 , 200
Cat6K-IOS(config)#
```

2. Spécifiez le port de destination pour le trafic capturé.

```
Cat6K-IOS(config)#monitor session 50 destination interface Fa3/30
Cat6K-IOS(config)#
```

Avec cela, tout le trafic de couche 2 qui appartient aux VLAN 100 et 200 est copié et envoyé au port Fa3/30. Si le port de destination fait partie du même VLAN dont le trafic est surveillé, le trafic qui sort du port de destination n'est pas capturé.

Vérifiez votre configuration SPAN à l'aide de la commande **show monitor**.

```
Cat6K-IOS#show monitor detail
Session 50
----------
Type               : Local Session
Source Ports       :
    RX Only        : None
    TX Only        : None
    Both           : None
Source VLANs       :
    RX Only        : None
    TX Only        : None
```

```
    Both          : 100,200
Source RSPAN VLAN : None
Destination Ports : Fa3/30
Filter VLANs      : None
Dest RSPAN VLAN   : None
```

Configuration avec VACL

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

- Le trafic HTTP d'une plage d'hôtes (10.20.20.128/25) dans VLAN 200 vers un serveur spécifique (10.10.10.101) dans VLAN 100 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 100.

1. Définissez le trafic intéressant à capturer et à analyser.
```
Cat6K-IOS(config)#ip access-list extended HTTP_UDP_TRAFFIC
Cat6K-IOS(config-ext-nacl)#permit tcp 10.20.20.128 0.0.0.127 host 10.10.10.101 eq www
Cat6K-IOS(config-ext-nacl)#permit udp any host 239.0.0.100
Cat6K-IOS(config-ext-nacl)#exit
```
2. Définissez une liste de contrôle d'accès umberlla pour mapper tout autre trafic.
```
Cat6K-IOS(config)#ip access-list extended ALL_TRAFFIC
Cat6K-IOS(config-ext-nacl)#permit ip any any
Cat6K-IOS(config-ext-nacl)#exit
```
3. Définissez la carte d'accès VLAN.
```
Cat6K-IOS(config)#vlan access-map HTTP_UDP_MAP 10
Cat6K-IOS(config-access-map)#match ip address HTTP_UDP_TRAFFIC
Cat6K-IOS(config-access-map)#action forward capture
Cat6K-IOS(config)#vlan access-map HTTP_UDP_MAP 20
Cat6K-IOS(config-access-map)#match ip address ALL_TRAFFIC
Cat6K-IOS(config-access-map)#action forward
Cat6K-IOS(config-access-map)#exit
```
4. Appliquez la carte d'accès VLAN aux VLAN appropriés.
```
Cat6K-IOS(config)#vlan filter HTTP_UDP_MAP vlan-list 100
!--- Here 100 is the ID of VLAN on which the VACL is applied.
```
5. Configurez le port de capture.
```
Cat6K-IOS(config)#int fa3/30
Cat6K-IOS(config-if)#switchport capture allowed vlan ?
  WORD    VLAN IDs of the allowed VLANs when this po
  add     add VLANs to the current list
  all     all VLANs
  except  all VLANs except the following
  remove  remove VLANs from the current list

Cat6K-IOS(config-if)#switchport capture allowed vlan 100
Cat6K-IOS(config-if)#switchport capture
Cat6K-IOS(config-if)#exit
```

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 vlan access-map** — Affiche le contenu des cartes d'accès VLAN.

```
Cat6K-IOS#show vlan access-map HTTP_UDP_MAP
Vlan access-map "HTTP_UDP_MAP"  10
        match: ip address HTTP_UDP_TRAFFIC
        action: forward capture
Vlan access-map "HTTP_UDP_MAP"  20
        match: ip address ALL_TRAFFIC
        action: forward
```

- **show vlan filter** — Affiche des informations sur les filtres VLAN.

```
Cat6K-IOS#show vlan filter
VLAN Map HTTP_UDP_MAP:
        Configured on VLANs:  100
            Active on VLANs:  100
```

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 CatOS
- Prise en charge des commutateurs de la gamme Cisco Catalyst 6500
- Support pour les produits LAN
- Prise en charge de la technologie de commutation LAN
- Support et documentation techniques - Cisco Systems