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 caractéristique de capture-port VACL sur 6000/6500 de cela de Cisco Catalyst exécute le logiciel Catalyst OS, se rapportent à la capture VACL pour l'analyse du trafic granulaire avec Cisco Catalyst 6000/6500 logiciel courant de 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 configurer le pour en savoir plus de Listes d'accès IP.
- RÉSEAU LOCAL virtuel : référez-vous au Virtual LAN/VLAN Trunking Protocol (VLAN/VTP) - Pour en savoir plus d'introduction.

Composants utilisés

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

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.

Produits connexes

Cette configuration peut également être utilisée avec Cisco Catalyst 6000/gamme 6500 de Commutateurs qui exécutent le Logiciel Cisco IOS version 12.1(13)E et plus tard.

Conventions

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

Informations générales

ENVERGURE basée par VLAN

Les copies d'ENVERGURE (analyseur commuté de port) trafiquent d'un ou plusieurs ports de source de n'importe quel VLAN ou d'un ou plusieurs VLAN à une destination port pour l'analyse. Le SPAN local prend en charge des ports de source, la source VLAN, et les destinations port sur la même gamme Catalyst 6500 commutent.

Une source VLAN est un VLAN surveillé pour l'analyse de trafic réseau. l'ENVERGURE basée sur VLAN (VSPAN) utilise un VLAN comme source d'ENVERGURE. Tous les ports dans la source VLAN deviennent des ports de source. Un port de source est un port surveillé pour l'analyse de trafic réseau. Des ports de joncteur réseau peuvent être configurés comme ports de source et être mélangés aux ports de source de nontrunk, mais l'ENVERGURE ne copie pas l'encapsulation d'un port de joncteur réseau de source.

Pour des sessions VSPAN avec le d'entrée et le de sortie configurés, deux paquets sont expédiés de la destination port si les paquets obtiennent en fonction le même VLAN (un que le trafic entrant du port d'entrée et un comme trafic en sortie du port de sortie).

Les moniteurs VSPAN seulement trafiquent que des feuilles ou entrent dans des ports de la couche 2 dans le VLAN.

- Si vous configurez un VLAN comme source d'entrée et le trafic obtient conduit dans le VLAN surveillé, le trafic routé n'est pas surveillé parce qu'il n'apparaît jamais comme trafic entrant

qui entre dans un port de la couche 2 dans le VLAN.
- Si vous configurez un VLAN comme source de sortie et le trafic obtient conduit hors du VLAN surveillé, le trafic routé n'est pas surveillé parce qu'il n'apparaît jamais comme trafic en sortie qui quitte un port de la couche 2 dans le VLAN.

Pour plus d'informations sur la source VLAN, référez-vous aux caractéristiques de la source VLAN.

ACL VLAN

VACLs peut fournir le contrôle d'accès pour tous les paquets qui pont dans un VLAN ou dans qui sont conduits ou hors d'un VLAN ou d'une interface WAN pour la capture VACL. À la différence du Cisco IOS régulier standard ou de l'ACLs étendu qui sont configurés sur des interfaces de routeur seulement et sont appliqués sur des paquets routés seulement, VACLs s'appliquent à tous les paquets et peuvent être appliqués à n'importe quel VLAN ou interface WAN. VACLs sont traités dans le matériel. Cisco IOS ACLs d'utilisation de VACLs. VACLs ignorent tous les champs d'ACL de Cisco IOS qui ne sont pas pris en charge dans le matériel.

Vous pouvez configurer VACLs pour l'IP, l'IPX, et le trafic de MAC-couche. VACLs s'est appliqué au trafic IP de support d'interfaces WAN seulement pour la capture VACL.

Quand vous configurez un VACL et vous appliquez l'à un VLAN, tous les paquets qui écrivent le VLAN sont vérifiés contre ce VACL. Si vous vous appliquez un VACL au VLAN et un ACL à une interface conduite dans le VLAN, un paquet qui entre dans le VLAN est d'abord vérifié contre le VACL et, si permis, est ensuite vérifié contre l'ACL en entrée avant qu'il soit manipulé par l'interface conduite. Quand le paquet est conduit à un autre VLAN, il est d'abord vérifié contre l'ACL de sortie qui est appliqué à l'interface conduite, et, si permis, le VACL configuré pour le VLAN de destination est appliqué. Si un VACL est configuré pour un type de paquet et un paquet de ce type n'apparie pas le VACL, l'action par défaut est refusent. Ce sont les instructions pour l'option de capture dans VACL.

- Le port de capture ne peut pas être un port atmosphère.
- Le port de capture doit être dans l'état d'expédition de spanning-tree pour le VLAN.
- Le commutateur n'a aucune restriction sur le nombre de ports de capture.
- Le port de capture capture seulement des paquets permis par l'ACL configuré.
- Les ports de capture transmettent seulement le trafic qui appartient au port VLAN de capture. Configurez le port de capture comme joncteur réseau qui porte les VLAN exigés afin de capturer le trafic qui va à beaucoup de VLAN.

Attention : La combinaison incorrecte d'ACLs peut perturber la circulation. Exercez l'attention supplémentaire tandis que vous configurez l'ACLs dans votre périphérique.

Note: VACL n'est pas pris en charge avec l'IPv6 sur une gamme Catalyst 6000 commute. En d'autres termes, l'ACL VLAN réorientent et l'IPv6 ne sont pas compatible ainsi l'ACL ne peut pas être utilisé au trafic de match ipv6.

Avantages d'utilisation VACL au-dessus d'utilisation VSPAN

Il y a plusieurs limites d'utilisation VSPAN pour l'analyse du trafic :

- Tout le trafic de la couche 2 qui entre dans un VLAN est capturé. Ceci augmente la quantité de données à analyser.

- Le nombre de sessions d'ENVERGURE qui peuvent être configurées sur les Commutateurs de gamme Catalyst 6500 est limité. Référez-vous au pour en savoir plus de limites de SPAN local et de session RSPAN.
- 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 de port de capture VACL peut aider à surmonter certaines de ces limites. VACLs ne sont pas principalement conçus pour surveiller le trafic, mais, avec un large éventail de capacité pour classifier le trafic, la fonctionnalité de port de capture a été introduite de sorte que l'analyse de trafic réseau puisse devenir beaucoup plus simple. Ce sont les avantages de l'utilisation de port de capture VACL au-dessus du VSPAN :

- Analyse du trafic granulaireVACLs peut s'assortir basé sur l'adresse IP source, adresse IP de destination, pose des ports de type de protocole 4, de source et de couche 4 de destination, et d'autres informations. Cette capacité rend VACLs très utile pour l'identification et le filtrage granulaires du trafic.
- Nombre de sessionsVACLs sont imposés dans le matériel ; le nombre d'entrées de contrôle d'accès (ACE) qui peuvent être créées dépend du TCAM disponible dans les Commutateurs.
- Surabonnement de destination portL'identification granulaire du trafic réduit le nombre de trames à expédier à la destination port et réduit de ce fait la probabilité de leur surabonnement.
- ReprésentationVACLs sont imposés dans le matériel ; il n'y a aucune baisse de performances pour l'application de VACLs à un VLAN sur le Commutateurs de la gamme Cisco Catalyst 6500

Configurez

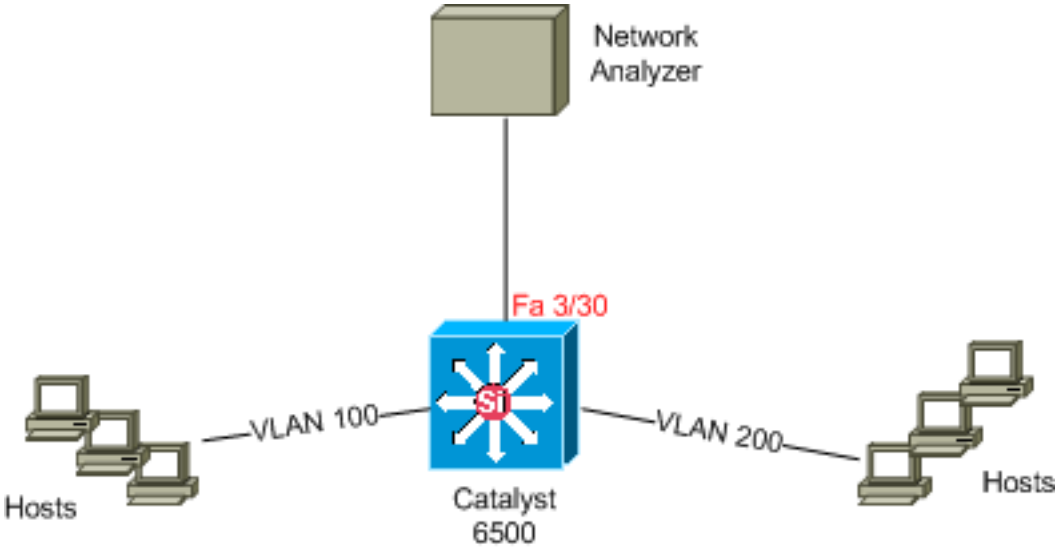
Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

- Configurer avec l'ENVERGURE basée par VLAN
- Configurer avec VACL

Note: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour trouver plus d'informations sur les commandes utilisées dans ce document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configuration avec l'ENVERGURE basée sur VLAN

Cet exemple de configuration répertorie l'étape nécessaire pour capturer tout le trafic de la couche 2 que les écoulements dans VLAN 100 et VLAN 200 et leur envoient au périphérique d'analyseur de réseau.

1. Spécifiez le trafic intéressant. Dans notre exemple, c'est le trafic qui entre 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 la destination port pour le trafic capturé.

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

Avec ceci, tout le trafic de la couche 2 qui appartient à VLAN 100 et à VLAN 200 est copié et envoyé pour mettre en communication Fa3/30. Si la destination port fait partie du même VLAN dont le trafic est surveillé, le trafic qui sort de la destination port n'est pas capturé.

Vérifiez votre configuration d'ENVERGURE avec la commande de **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, il y a de plusieurs conditions requises de l'administrateur réseau :

- Le trafic http d'une plage des hôtes (10.20.20.128/25) dans VLAN 200 à un serveur spécifique (10.10.10.101) dans les besoins VLAN 100 d'être capturé.
- Le trafic de Protocole UDP (User Datagram Protocol) de Multidiffusion dans la direction de transmission destiné pour l'adresse de groupe 239.0.0.100 doit être capturé de VLAN 100.

1. Définissez le trafic intéressant à caputured et être envoyé à l'analyse.
```
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 un ACL d'umberlla pour tracer 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
```

Vérifiez

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 VLAN Access.

```
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 au sujet des vlans filters.

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

Dépannez

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
- Support de 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