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

Contenu

Introduction

Ce document fournit une configuration d'échantillon pour l'usage de la liste de contrôle d'accès VLAN (ACL) (VACL) fonctionnalité de port de capture pour l'analyse de trafic réseau d'une manière plus granulaire. Ce document énonce également l'avantage de l'utilisation de capture-port VACL par opposition à l'utilisation basée sur VLAN du Fonction Switched Port Analyzer (SPAN) (VSPAN).

Afin de configurer le VACL capturez la fonctionnalité de port sur 6000/6500 de cela de Cisco Catalyst exécute le logiciel de Cisco IOS®, se rapportent à la capture VACL pour l'analyse du trafic granulaire avec Cisco Catalyst 6000/6500 logiciel de Cisco IOS d'exécution.

Conditions préalables

Conditions requises

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

- RÉSEAU LOCAL virtuel — Référez-vous au Virtual LAN/VLAN Trunking Protocol (VLAN/VTP) - Pour en savoir plus d'introduction.
- Listes d'accès — Référez-vous à configurer le pour en savoir plus de contrôle d'accès.

Composants utilisés

Les informations dans ce document sont basées sur la gamme Cisco Catalyst 6506 commutent que la version Catalyst OS de passages 8.1(2).

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 la version Catalyst OS 6.3 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 sur VLAN

Les copies d'ENVERGURE 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.

Un port de source est un port surveillé pour l'analyse de trafic réseau. Une source VLAN est un VLAN surveillé pour l'analyse de trafic réseau. l'ENVERGURE basée sur VLAN (VSPAN) est analyse du trafic réseau dans un ou plusieurs VLAN. Vous pouvez configurer le VSPAN comme ENVERGURE d'entrée, ENVERGURE de sortie, ou chacun des deux. Tous les ports dans la source VLAN deviennent les ports opérationnels de source pour la session VSPAN. Les destinations port, si elles appartiennent à la source administrative l'une des VLAN, sont exclues de la source opérationnelle. Si vous ajoutez ou enlevez les ports de la source administrative VLAN, les sources opérationnelles sont modifiées en conséquence.

Instructions pour des sessions VSPAN :

- Les ports de joncteur réseau sont inclus comme ports de source pour les sessions VSPAN, mais seulement les VLAN qui sont dans la liste d'origine d'admin sont surveillés si ces VLAN sont en activité pour le joncteur réseau.
- Pour les sessions VSPAN avec le d'entrée et l'ENVERGURE de sortie configurés, le système fonctionne basé sur le type d'engine de superviseur 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 expédiés par la destination port d'ENVERGURE si les paquets obtiennent en fonction le même VLAN.WS-X6K-SUP1-2GE, WS-X6K-SUP1A-2GE — Seulement un paquet est expédié par la destination port d'ENVERGURE.

- Un port intrabande n'est pas inclus en tant que source opérationnelle pour les sessions VSPAN.
- Quand un VLAN est effacé, il est retiré de la liste d'origine pour les sessions VSPAN.
- Une session VSPAN est désactivée si la liste de la source VLAN d'admin est vide.
- On ne permet pas les VLAN inactifs pour la configuration VSPAN.
- Une session VSPAN est rendue inactive si la source l'une des VLAN deviennent le RSPAN VLAN.

Référez-vous aux caractéristiques de la source VLAN pour plus d'informations sur la source VLAN.

ACL VLAN

Le VACLs peut contrôle d'accès tout le trafic. Vous pouvez configurer le VACLs sur le commutateur pour s'appliquer à tous les paquets dans lesquels sont conduits ou hors d'un VLAN ou pont dans un VLAN. Le VACLs sont strictement pour le filtrage des paquets de Sécurité et le trafic de réorientation aux ports de commutateur physiques spécifiques. À la différence du Cisco IOS ACLs, le VACLs ne sont pas définis par la direction (entrée ou sortie).

Vous pouvez configurer le VACLs sur les adresses de la couche 3 pour l'IP et l'IPX. Tous autres protocoles sont accès contrôlé par les adresses MAC et EtherType utilisant le MAC VACLs. Le trafic IP et le trafic IPX ne sont pas accès contrôlé par le MAC VACLs. Tous autres types de trafic (AppleTalk, DECNet, et ainsi de suite) sont classifiés comme trafic de MAC. Le MAC VACLs sont utilisés au contrôle d'accès ce trafic.

As pris en charge dans VACLs

VACL contient un liste dans un certain ordre des entrées de contrôle d'accès (as). Chaque VACL peut contenir des as de seulement un type. Chaque ACE contient un certain nombre de champs qui sont appariés contre le contenu d'un paquet. Chaque champ peut avoir un masque de bits associé pour indiquer quels bits sont appropriés. Une action est associée avec chaque ACE qui décrit ce que le système devrait faire avec le paquet quand une correspondance se produit. L'action est personne à charge de caractéristique. Types du support trois de Commutateurs de gamme Catalyst 6500 d'as dans le matériel :

- As IP
- As IPX
- As d'Ethernets

Ce tableau présente les paramètres qui sont associés avec chaque type d'ACE :

ACE tapent	TCP ou UDP	ICMP	L'autre IP	IPX	Ethernets
Paramètres de la couche	Port de source	-	-	-	-
	Opérateur de	-	-	-	-

4	port de source				
	Destination port	-	-	-	-
	Opérateur de destination port	Code d'ICMP	-	-	-
	S/O	Type ICMP	S/O	-	-
Paramètres de la couche 3	Octet de tos IP	Octet de tos IP	Octet de tos IP	-	-
	Adresse source IP	Adresse source IP	Adresse source IP	Réseau de 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	L'autre Protocol	Type de paquet IPX	-
Paramètres de la couche 2	-	-	-	-	EtherType
	-	-	-	-	Adresse source d'Ethernets
	-	-	-	-	Adresse de destination d'Ethernets

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 résumé des

fonctionnalités et limites.
- 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. Cependant, 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'as qui peuvent être créés 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.

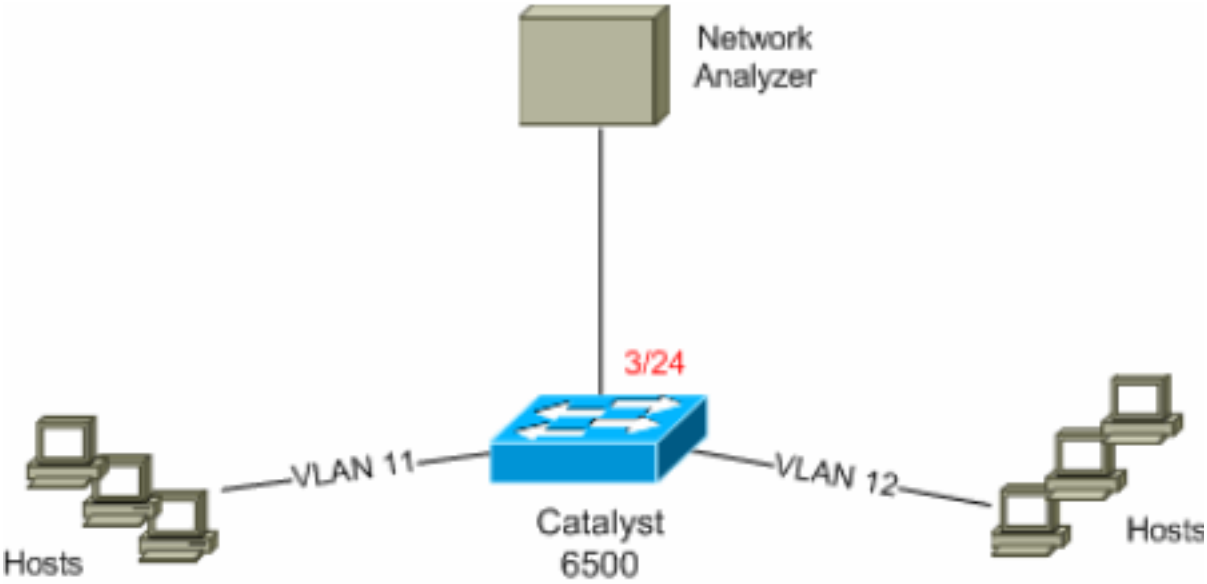
Ce document utilise les configurations suivantes :

- Configuration avec l'ENVERGURE basée sur VLAN
- Configuration avec VACL

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

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 le VLAN 11 et le VLAN 12 et leur envoient au périphérique d'analyseur de réseau.

1. Spécifiez le trafic intéressant.Dans cet exemple, c'est le trafic qui entre 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 ceci, tout le trafic de la couche 2 qui appartient au VLAN 11 et au VLAN 12 sont copiés et envoyés au port 3/24.
2. Vérifiez votre configuration d'ENVERGURE avec le **show span toute la** commande.`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, il y a de plusieurs conditions requises de l'administrateur réseau :

- Le trafic http d'une plage des hôtes (10.12.12.128/25) dans le VLAN 12 à un serveur spécifique (10.11.11.100) dans le VLAN 11 doit 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 du VLAN 11.

1. Définissez le trafic intéressant utilisant la Sécurité ACLs. Souvenez-vous pour mentionner la **capture de** mot clé pour tous les as 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 d'ACE est correcte et dans la commande appropriée.`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. Commettez l'ACL au 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 l'ACL.`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 l'ACL au mappage 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 un ACL est tracé aux VLAN multiples, alors le port de capture doit être configuré à tous ces VLAN. Afin de faire le port de capture permettre des VLAN multiples, configurer le port comme joncteur réseau et permettre seulement les VLAN tracés à l'ACL. Par exemple, si l'ACL est tracé à VLAN 11 et 12, puis terminez-vous 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 des ports de capture.`6K-CatOS> (enable) **show security acl capture-ports** ACL Capture Ports: 3/24 6K-CatOS> (enable)`

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** .

- **affichez les informations d'acl de Sécurité** — Affiche le contenu des VACL qui sont actuellement configurés ou pour la dernière fois commis à NVRAM et à 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)`
- **affichez la carte d'acl de Sécurité** — Affiche l'Acl-à-VLAN ou le mappage d'Acl-à-port pour un 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)`
- **affichez les capture-ports d'acl de Sécurité** — Affiche la liste de ports de capture.`6K-CatOS> (enable) **show security acl capture-ports** ACL Capture Ports: 3/24 6K-CatOS> (enable)`

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 Cisco IOS
- Configuration du contrôle d'accès - Guide de configuration du logiciel de 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