Exemple de configuration des fonctionnalités de sécurité de couche 2 sur les commutateurs Cisco Catalyst de couche 3 à configuration fixe

Contenu

Introduction

Ce document fournit une configuration d'échantillon pour certaines des fonctionnalités de sécurité de la couche 2, telles que la Sécurité de port, la surveillance DHCP, l'inspection dynamique de Protocole ARP (Address Resolution Protocol) et la protection de source IP, qui peut être mise en application sur des Commutateurs de configuration fixe de la couche 3 de Cisco Catalyst.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur la gamme Cisco Catalyst 3750 commutent avec la version 12.2(25)SEC2.

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 ces matériels :

- Commutateurs de la gamme Cisco Catalyst 3550
- Commutateurs de la gamme Cisco Catalyst 3560
- Commutateurs de la gamme Cisco Catalyst 3560-E
- Commutateurs de la gamme Cisco Catalyst 3750-E

Conventions

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

Informations générales

Semblable aux Routeurs, les Commutateurs de la couche 2 et de la couche 3 ont leurs propres ensembles de conditions requises de sécurité des réseaux. Les Commutateurs sont susceptibles de plusieurs des mêmes attaques de la couche 3 que des Routeurs. Cependant, les Commutateurs et la couche 2 du modèle de référence OSI sont sujets généralement à des attaques réseau dans différentes manières. Ceux-ci incluent :

- **Dépassement associatif de Tableau de mémoire (CAM)**Des tables associatives de mémoire (CAM) sont limitées dans la taille. Si assez d'entrées sont écrites dans la table de CAM avant que d'autres entrées soient expirées, la table de CAM remplit jusqu'au point qu'aucune nouvelle entrée ne peut être reçue. Typiquement, un intrus de réseau inonde le commutateur avec un grand nombre d'adresses de Contrôle d'accès au support (MAC) de source non valide jusqu'à la table de CAM se remplit. Quand cela se produit, le commutateur inonde tous les ports avec le trafic entrant parce qu'il ne peut pas trouver le numéro de port pour une adresse MAC particulière dans la table de CAM. Le commutateur, essentiellement, agit comme un hub. Si l'intrus ne met pas à jour la pléthore d'adresses MAC de source non valide, le commutateur chronomètre par la suite des entrées plus anciennes d'adresse MAC de la table de CAM et commence à agir comme un commutateur de nouveau. Les inondations de dépassement de table de CAM seulement trafiquent dans les gens du pays VLAN ainsi l'intrus voit seulement le trafic dans les gens du pays VLAN auxquels lui ou elle est connecté.L'attaque de dépassement de table de CAM peut être atténuée en configurant la Sécurité de port sur le commutateur. Cette option prévoit la spécification des adresses MAC sur un port de commutateur particulier ou la spécification du nombre d'adresses MAC qui peuvent être apprises par un port de commutateur. Quand une adresse MAC non valide est détectée sur le port, le commutateur peut bloquer l'adresse MAC offensante ou arrêter le port. La spécification des adresses MAC sur des ports de commutateur est une solution trop incontrôlable lointaine pour un environnement de production. Une limite du nombre d'adresses MAC sur un port de commutateur est maniable. Plus administrativement une

solution évolutive est l'implémentation de la Sécurité de port dynamique sur le commutateur. Afin d'implémenter la Sécurité de port dynamique, spécifiez un nombre maximal d'adresses MAC qui seront apprises.

- **Mystification d'adresse de Contrôle d'accès au support (MAC)**Les attaques de détournement de trafic de Contrôle d'accès au support (MAC) comportent l'utilisation d'une adresse MAC connue d'un autre hôte de tenter de faire la cible commuter les trames en avant destinées pour le serveur distant à l'attaquant de réseau. Quand une trame simple est envoyée avec l'adresse d'Ethernets de source de l'autre hôte, l'attaquant de réseau remplace l'entrée de table de CAM de sorte que les paquets de commutateur en avant destinés pour l'hôte à l'attaquant de réseau. Jusqu'à ce que l'hôte envoie le trafic, il ne reçoit aucun trafic. Quand l'hôte envoie le trafic, l'entrée de table de CAM est réécrite une fois de plus de sorte qu'elle se déplace de nouveau au port d'origine.Employez la caractéristique de Sécurité de port pour atténuer des attaques de détournement de trafic de MAC. La Sécurité de port fournit la capacité pour spécifier l'adresse MAC du système connecté à un port particulier. Ceci fournit également la capacité de spécifier une action de prendre si une violation de Sécurité de port se produit.
- **Charrier de Protocole ARP (Address Resolution Protocol)**L'ARP est utilisé pour tracer l'adressage IP aux adresses MAC dans un segment de réseau local où les hôtes du même sous-réseau résident. Normalement, un hôte envoie une demande d'ARP de diffusion de trouver l'adresse MAC d'un autre hôte avec une adresse IP particulière, et une réponse d'ARP provient l'hôte dont l'adresse apparie la demande. L'hôte demandeur cache alors cette réponse d'ARP. Dans le protocole ARP, une autre disposition est prise pour que des hôtes exécutent des réponses non sollicitées d'ARP. Les réponses non sollicitées d'ARP s'appellent Gratuitous ARP (GARP). GARP peut être exploité avec malveillance par un attaquant pour charrier l'identité d'une adresse IP sur un segment de RÉSEAU LOCAL. Ceci est typiquement utilisé pour charrier l'identité entre deux hôtes ou tous trafic à et d'une passerelle par défaut dans une attaque « homme-dans-le-moyenne ».Quand une réponse d'ARP est ouvrée, un attaquant de réseau peut faire son système sembler être la destination host recherchée par l'expéditeur. La réponse d'ARP fait enregistrer l'expéditeur l'adresse MAC du système de l'attaquant de réseau dans le cache d'ARP. Cette adresse MAC est également enregistrée par le commutateur dans sa table de CAM. De cette façon, l'attaquant de réseau a inséré l'adresse MAC de son système dans chacun des deux la table de CAM de commutateur et le cache d'ARP de l'expéditeur. Ceci permet à l'attaquant de réseau pour intercepter des trames destinées pour l'hôte que lui ou elle charrie.Des temporisateurs d'écrou de serrage dans le menu de configuration d'interface peuvent être utilisés pour atténuer des attaques de détournement de trafic d'ARP en plaçant la durée qu'une entrée restera dans le cache d'ARP. Cependant, les temporisateurs d'écrou de serrage sont seuls insuffisants. La modification du temps d'expiration de cache d'ARP sur tous les systèmes d'extrémité sont exigées aussi bien que les entrées statiques d'ARP. Une autre solution qui peut être utilisée pour atténuer le divers réseau basé sur ARP exploite, est l'utilisation de la surveillance DHCP avec l'inspection dynamique d'ARP. Ces caractéristiques de Catalyst valident des paquets d'ARP dans un réseau et permettent l'interception, se connectant, et jetant des paquets d'ARP avec l'adresse MAC non valide aux attaches d'adresse IP.Les filtres de surveillance DHCP ont fait confiance à des messages DHCP afin de fournir la Sécurité. Puis, ces messages sont utilisés pour construire et mettre à jour une table de corrélation de surveillance DHCP. La surveillance DHCP considère les messages DHCP qui proviennent de n'importe quel port d'utilisateur-revêtement qui n'est pas un port de serveur DHCP comme non approuvé. D'un point de vue de surveillance DHCP, ces ports non approuvés d'utilisateur-revêtement ne doivent pas

envoyer des réponses de type de serveur DHCP, telles que DHCPOFFER, DHCPACK, ou DHCPNAK. La table de corrélation de surveillance DHCP contient l'adresse MAC, l'adresse IP, la durée de bail, le type contraignant, le nombre VLAN, et les informations d'interface qui correspondent aux interfaces non approuvées locales d'un commutateur. La table de corrélation de surveillance DHCP ne contient pas des informations sur des hôtes interconnectés avec une interface de confiance. Une interface non approuvée est une interface configurée pour recevoir des messages de l'extérieur du réseau ou du Pare-feu. Une interface de confiance est une interface qui est configurée aux messages uniquement récepteurs du réseau. La table de corrélation de surveillance DHCP peut contenir l'adresse MAC dynamique et statique aux attaches d'adresse IP.L'inspection dynamique d'ARP détermine la validité d'un paquet d'ARP basé sur l'adresse MAC valide aux attaches d'adresse IP enregistrées dans une base de données de surveillance DHCP. Supplémentaire, l'inspection dynamique d'ARP peut valider des paquets d'ARP basés sur le Listes de contrôle d'accès (ACL) utilisateur-configurable. Ceci tient compte de l'inspection des paquets d'ARP pour les hôtes qui utilisent les adresses IP statiquement configurées. L'inspection dynamique d'ARP tient compte de l'usage du par-port et des listes de contrôle d'accès VLAN (PACLs) de limiter des paquets d'ARP pour les adresses IP spécifiques aux adresses MAC spécifiques.

- **Famine du protocole DHCP (DHCP)**Une attaque de famine DHCP fonctionne à côté de l'émission des requêtes DHCP avec les adresses MAC charriées. Si assez de demandes sont envoyées, l'attaquant de réseau peut épuiser l'espace d'adressage disponible aux serveurs DHCP pendant une période. L'attaquant de réseau peut alors installer un serveur DHCP escroc sur son système et répondre à de nouvelles requêtes DHCP des clients sur le réseau. Avec le placement d'un serveur DHCP escroc sur le réseau, un attaquant de réseau peut fournir à des clients des adresses et toute autre information réseau. Puisque les réponses DHCP incluent typiquement la passerelle par défaut et les informations de serveur de DNS, l'attaquant de réseau peut fournir son propre système en tant que la passerelle par défaut et serveur DNS. Ceci a comme conséquence une attaque homme-dans-le-moyenne. Cependant, l'échappement de toutes les adresses DHCP n'est pas exigé pour introduire un serveur DHCP escroc.Des fonctionnalités supplémentaires dans la famille de commutateurs Catalyst, telle que la surveillance DHCP, peuvent être utilisées pour aider à garder contre une attaque de famine DHCP. La surveillance DHCP est une fonctionnalité de sécurité que les messages DHCP non approuvés et les constructions de filtres et met à jour une table de corrélation de surveillance DHCP. La table de corrélation contient les informations telles que l'adresse MAC, l'adresse IP, la durée de bail, le type contraignant, le nombre VLAN et les informations d'interface qui correspondent aux interfaces non approuvées locales d'un commutateur. Les messages non approuvés sont ceux reçus de l'extérieur du réseau ou du Pare-feu. Les interfaces commutateur non approuvées sont ceux qui sont configurées pour recevoir de tels messages de l'extérieur du réseau ou du Pare-feu.D'autres fonctions de commutateur de Catalyst, telles que la protection de source IP, peuvent assurer la défense supplémentaire contre des attaques telles que la famine et l'usurpation d'adresse IP DHCP. Semblable à la surveillance DHCP, la protection de source IP est activée sur les ports non approuvés de la couche 2. Tout le trafic IP est au commencement bloqué, excepté des paquets DHCP capturés par le procédé de surveillance DHCP. Une fois qu'un client reçoit une adresse IP valide du serveur DHCP, un PACL est appliqué au port. Ceci limite le trafic IP de client à ces adresses IP de source configurées dans l'attache. Tout autre trafic IP avec une adresse source autre que les adresses dans l'attache est filtré.

Configurez

Dans cette section, vous êtes présenté avec les informations pour configurer les fonctionnalités de sécurité de Sécurité de port, de surveillance DHCP, d'inspection dynamique d'ARP et de protection de source IP.

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

Les configurations du commutateur de Catalyst 3750 contiennent ces derniers :

- Sécurité de port
- Surveillance DHCP
- Inspection dynamique d'ARP
- Protection de la source IP

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

- PC 1 et PC 3 sont des clients connectés au commutateur.
- PC 2 est un serveur DHCP connecté au commutateur.
- Tous les ports du commutateur sont dans le même VLAN (VLAN 1).
- Le serveur DHCP est configuré pour assigner des adresses IP aux clients basés sur leurs adresses MAC.

Sécurité de port

Vous pouvez employer la caractéristique de Sécurité de port pour limiter et identifier des adresses MAC des stations permises pour accéder au port. Ceci limite l'entrée à une interface. Quand vous assignez des adresses MAC sécurisées à un port sécurisé, le port n'expédie pas des paquets avec des adresses sources en dehors du groupe d'adresses définies. Si vous limitez le nombre d'adresses MAC sécurisées à une et assignez une adresse MAC sécurisée simple, le poste de travail relié à ce port est assuré la bande passante complète du port. Si un port est configuré pendant qu'un port sécurisé et le nombre maximal d'adresses MAC sécurisées est atteint, quand l'adresse MAC d'une station qui tente d'accéder au port est différente des adresses MAC sécurisées identifiées l'unes des, une violation de sécurité se produit. En outre, si une station avec une adresse MAC sécurisée configurée ou apprise sur des tentatives d'un port sécurisé d'accéder à un autre port sécurisé, une violation est signalée. Par défaut, le port s'est arrêté quand le nombre maximal d'adresses MAC sécurisées est dépassé.

Remarque: Quand un commutateur de Catalyst 3750 joint une pile, le nouveau commutateur reçoit les adresses sécurisées configurées. Toutes les adresses sécurisées dynamiques sont téléchargées par le nouveau membre de pile des autres membres de pile.

Référez-vous aux instructions de configuration pour les instructions sur la façon dont configurer la Sécurité de port.

Ici, la caractéristique de Sécurité de port est affichée configurée sur le FastEthernet 1/0/2 interface. Par défaut, le nombre maximal d'adresses MAC sécurisées pour l'interface est une.

Vous pouvez émettre la **commande d'interface de show port-security** afin de vérifier l'état de Sécurité de port pour une interface.

Sécurité de port
Cat3750#**show port-security interface fastEthernet 1/0/2** Port Security : Disabled Port Status : Secure-down Violation Mode : Shutdown Aging Time : 0 mins Aging Type : Absolute SecureStatic Address Aging : Disabled Maximum MAC Addresses : 1 Total MAC Addresses : 0 Configured MAC Addresses : 0 Sticky MAC Addresses : 0 Last Source Address:Vlan : 0000.0000.0000:0 Security Violation Count : 0 *!--- Default port security configuration on the switch.* Cat3750#**conf t** Enter configuration commands, one per line. End with CNTL/Z. Cat3750(config)#**interface fastEthernet 1/0/2** Cat3750(config-if)#**switchport port-security** Command rejected: FastEthernet1/0/2 is a dynamic port. *!--- Port security can only be configured on static access ports or trunk ports.* Cat3750(config-if)#**switchport mode access** *!--- Sets the interface switchport mode as access.* Cat3750(config-if)#**switchport port-security** *!--- Enables port security on the interface.* Cat3750(config-if)#**switchport port-security mac-address 0011.858D.9AF9** *!--- Sets the secure MAC address for the interface.* Cat3750(config-if)#**switchport port-security violation shutdown** *!--- Sets the violation mode to shutdown. This is the default mode.* Cat3750# *!--- Connected a different PC (PC 4) to the FastEthernet 1/0/2 port !--- to verify the port security feature.* 00:22:51: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa1/0/2, putting Fa1/0/2 in err-disable state 00:22:51: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0011.8565.4B75 on port FastEthernet1/0/2. 00:22:52: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0/2, changed state to down 00:22:53: %LINK-3-UPDOWN: Interface FastEthernet1/0/2, changed state to down *!--- Interface shuts down when a security violation is detected.* Cat3750#**show interfaces fastEthernet 1/0/2** FastEthernet1/0/2 is down, line protocol is down (err-disabled) *!--- Output Suppressed. !--- The port is shown error-disabled. This verifies the configuration. !--- **Note**: When a secure port is in the error-disabled state, !--- you can bring it out of this state by entering !--- the **errdisable recovery cause psecure-violation** global configuration command, !--- or you can manually re-enable it by entering the !--- **shutdown** and **no shutdown** interface configuration commands.* Cat3750#**show port-security interface fastEthernet 1/0/2** Port Security : Enabled Port Status : Secure-shutdown Violation Mode : Shutdown Aging Time : 0 mins Aging Type : Absolute SecureStatic Address Aging : Disabled Maximum MAC Addresses : 1 Total MAC Addresses : 1 Configured MAC Addresses : 1 Sticky MAC Addresses : 0 Last Source Address:Vlan : 0011.8565.4B75:1 Security Violation Count : 1

Remarque: Les mêmes adresses MAC ne devraient pas être configurées que l'adresse MAC sécurisée et statique sur différents ports d'un commutateur.

Quand un téléphone IP est connecté à un commutateur par le switchport configuré pour la Voix VLAN, le téléphone envoie les paquets non-marqués de CDP et les paquets étiquetés de CDP de

Voix. Ainsi l'adresse MAC du téléphone IP est apprise sur le PVID et le VVID. Si le numéro approprié d'adresses sécurisées ne sont pas configurés, vous pouvez recevoir un message d'erreur semblable à ce message :

```
%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred,
caused by MAC address 001b.77ee.eeee on port GigabitEthernet1/0/18.
PSECURE: Assert failure: psecure_sb->info.num_addrs <= psecure_sb->max_addrs:
```

Vous devez placer les adresses sécurisées de maximum autorisé sur le port à deux (pour le téléphone IP) plus le nombre maximal d'adresses sécurisées permises sur l'accès VLAN afin de résoudre ce problème.

Référez-vous à configurer le pour en savoir plus de Sécurité de port.

Surveillance DHCP

La surveillance DHCP agit comme un Pare-feu entre les hôtes non approuvés et les serveurs DHCP. Vous employez la surveillance DHCP pour différencier entre les interfaces non approuvées connectées à l'utilisateur final et les interfaces de confiance connectées à un serveur DHCP ou à un commutateur différent. Quand un commutateur reçoit un paquet sur une interface non approuvée et l'interface appartient à un VLAN qui a la surveillance DHCP activée, le commutateur compare l'adresse MAC source et l'adresse de matériel de DHCP Client. Si les adresses s'assortissent (le par défaut), le commutateur en avant le paquet. Si les adresses ne s'assortissent pas, le commutateur relâche le paquet. Le commutateur relâche un paquet DHCP quand une de ces situations se produit :

- Un paquet d'un serveur DHCP, tel qu'un DHCPOFFER, paquet DHCPACK, DHCPNAK, ou DHCPLEASEQUERY, est reçu de l'extérieur du réseau ou du Pare-feu.
- Un paquet est reçu sur une interface non approuvée, et l'adresse MAC source et l'adresse de matériel de DHCP Client ne s'assortissent pas.
- Le commutateur reçoit un message de diffusion DHCPRELEASE ou DHCPDECLINE qui a une adresse MAC dans la surveillance DHCP liant la base de données, mais les informations d'interface dans la base de données obligatoire n'apparient pas l'interface sur laquelle le message a été reçu.
- Un agent de relais DHCP en avant un paquet DHCP, qui inclut une adresse IP de relais-agent qui n'est pas 0.0.0.0, ou l'agent de relais en avant un paquet qui inclut les informations option-82 à un port non approuvé.

Référez-vous aux instructions de configuration de surveillance DHCP pour les instructions sur la façon dont configurer la surveillance DHCP.

Remarque: Pour que la surveillance DHCP fonctionne correctement, tous les serveurs DHCP doivent être connectés au commutateur par les interfaces de confiance.

Remarque: Dans une pile de commutateurs avec des Commutateurs de Catalyst 3750, la surveillance DHCP est gérée sur le maître de pile. Quand un nouveau commutateur joint la pile, le commutateur reçoit la configuration de surveillance DHCP du maître de pile. Quand un membre laisse la pile, toutes les attaches de surveillance DHCP ont associé avec l'âge de commutateur.

Remarque: Afin de s'assurer que la durée de bail dans la base de données est précise, Cisco recommande que vous activiez et configuriez le NTP. Si le NTP est configuré, le commutateur écrit des modifications d'obligatoire au fichier obligatoire seulement quand l'horloge système de commutateur est synchronisée avec le NTP.

Des serveurs DHCP escrocs peuvent être atténués par des caractéristiques de surveillance DHCP. La commande d'**ip dhcp snooping** est émise afin d'activer le DHCP globalement sur le commutateur. Une fois configurés avec la surveillance DHCP, tous les ports dans le VLAN sont non approuvés pour des réponses DHCP. Ici, seulement l'interface FastEthernet 1/0/3 connectée au serveur DHCP est configurée comme fait confiance.

Surveillance DHCP

```
Cat3750#conf t Enter configuration commands, one per
line. End with CNTL/Z. Cat3750(config)#ip dhcp snooping
!--- Enables DHCP snooping on the switch.
Cat3750(config)#ip dhcp snooping vlan 1 !--- DHCP
snooping is not active until DHCP snooping is enabled on
a VLAN. Cat3750(config)#no ip dhcp snooping information
option !--- Disable the insertion and removal of the
option-82 field, if the !--- DHCP clients and the DHCP
server reside on the same IP network or subnet.
Cat3750(config)#interface fastEthernet 1/0/3
Cat3750(config-if)#ip dhcp snooping trust !---
Configures the interface connected to the DHCP server as
trusted. Cat3750#show ip dhcp snooping Switch DHCP
snooping is enabled DHCP snooping is configured on
following VLANs: 1 Insertion of option 82 is disabled
Option 82 on untrusted port is not allowed Verification
of hwaddr field is enabled Interface Trusted Rate limit
(pps) ------------------------ ------- ----------------
FastEthernet1/0/3 yes unlimited !--- Displays the DHCP
snooping configuration for the switch. Cat3750#show ip
dhcp snooping binding MacAddress IpAddress Lease(sec)
Type VLAN Interface ------------------ --------------- -
--------- ------------- ---- --------------------
00:11:85:A5:7B:F5 10.0.0.2 86391 dhcp-snooping 1
FastEtheret1/0/1 00:11:85:8D:9A:F9 10.0.0.3 86313 dhcp-
snooping 1 FastEtheret1/0/2 Total number of bindings: 2
!--- Displays the DHCP snooping binding entries for the
switch. Cat3750# !--- DHCP server(s) connected to the
untrusted port will not be able !--- to assign IP
addresses to the clients.
```

Référez-vous à configurer le pour en savoir plus de caractéristiques DHCP.

Inspection dynamique d'ARP

L'inspection dynamique d'ARP est une fonctionnalité de sécurité qui valide des paquets d'ARP dans un réseau. Il intercepte, se connecte, et jette des paquets d'ARP avec les liaisons d'adresse non valides d'IP-à-MAC. Cette capacité protège le réseau contre certaines attaques homme-dans-le-moyennes.

L'inspection dynamique d'ARP s'assure que seulement des demandes valides et les réponses d'ARP sont transmises par relais. Le commutateur exerce ces activités :

- Intercepte toutes les demandes et réponses d'ARP sur les ports non approuvés
- Vérifie que chacun de ces paquets interceptés a une liaison d'adresse valide d'IP-à-MAC avant qu'il mette à jour le cache local d'ARP ou avant qu'il en avant le paquet à la destination appropriée
- Relâche les paquets non valides d'ARP

L'inspection dynamique d'ARP détermine la validité d'un paquet d'ARP basé sur les liaisons

d'adresse valides d'IP-à-MAC enregistrées dans une base de données de confiance, la surveillance DHCP liant la base de données. Cette base de données est établie par surveillance DHCP si la surveillance DHCP est activée sur les VLAN et sur le commutateur. Si le paquet d'ARP est reçu sur une interface de confiance, le commutateur en avant le paquet sans tous contrôles. Sur les interfaces non approuvées, le commutateur en avant le paquet seulement s'il est valide.

Dans les environnements non-DHCP, l'inspection dynamique d'ARP peut valider des paquets d'ARP contre l'ARP utilisateur-configuré ACLs pour des hôtes avec les adresses IP statiquement configurées. Vous pouvez émettre la commande de configuration globale d'**arp access-list** afin de définir un ACL d'ARP. L'ARP ACLs ont la priorité au-dessus des entrées dans la surveillance DHCP liant la base de données. Le commutateur utilise ACLs seulement si vous émettez la commande de configuration globale d'**ip arp inspection filter vlan** afin de configurer l'ACLs. Le commutateur compare d'abord les paquets ARP aux ACL ARP configurées par l'utilisateur. Si l'ACL ARP refuse le paquet ARP, le commutateur refuse également le paquet même si une liaison valide existe dans la base de données remplie par la surveillance DHCP.

Référez-vous aux instructions de configuration d'inspection dynamique d'ARP pour les instructions sur la façon dont configurer l'inspection dynamique d'ARP.

La commande de configuration globale d'**ip arp inspection vlan** est émise afin d'activer l'inspection dynamique d'ARP sur une base par-VLAN. Ici, seulement l'interface FastEthernet 1/0/3 connectée au serveur DHCP est configurée comme fait confiance avec la commande d'**ip arp inspection trust**. La surveillance DHCP doit être activée afin de permettre les paquets d'ARP qui ont dynamiquement assigné des adresses IP. Voyez la section de surveillance DHCP de ce document pour les informations de configuration de surveillance DHCP.

Inspection dynamique d'ARP

```
Cat3750#conf t Enter configuration commands, one per
line. End with CNTL/Z. Cat3750(config)#ip arp inspection
vlan 1 !--- Enables dynamic ARP inspection on the VLAN.
Cat3750(config)#interface fastEthernet 1/0/3
Cat3750(config-if)#ip arp inspection trust !---
Configures the interface connected to the DHCP server as
trusted. Cat3750#show ip arp inspection vlan 1 Source
Mac Validation : Disabled Destination Mac Validation :
Disabled IP Address Validation : Disabled Vlan
Configuration Operation ACL Match Static ACL ---- ------
------- --------- --------- ---------- 1 Enabled Active
Vlan ACL Logging DHCP Logging ---- ----------- ---------
--- 1 Deny Deny !--- Verifies the dynamic ARP inspection
configuration. Cat3750#
```

Référez-vous à configurer le pour en savoir plus d'inspection dynamique d'ARP.

Protection de la source IP

La protection de source IP est une fonctionnalité de sécurité que les filtres trafiquent basé sur la surveillance DHCP liant la base de données et sur les attaches manuellement configurées de source IP afin de limiter le trafic IP sur les interface de couche 2 non-conduits. Vous pouvez utiliser la protection de source IP pour empêcher des attaques du trafic entraînées quand des essais d'un hôte pour utiliser l'adresse IP de son voisin. La protection de source IP empêche la mystification IP/MAC.

Vous pouvez activer la protection de source IP quand la surveillance DHCP est activée sur une

interface non approuvée. Après que la protection de source IP soit activée sur une interface, le commutateur bloque tout le trafic IP reçu sur l'interface, excepté des paquets DHCP permis de surveillance DHCP. Un ACL de port est appliqué à l'interface. L'ACL de port permet seulement le trafic IP avec une adresse IP source dans la table d'ip source binding et refuse tout autre trafic.

La table d'ip source binding a les attaches qui sont apprises par surveillance DHCP ou sont manuellement configurées (les attaches statiques de source IP). Une entrée dans cette table a une adresse IP, son adresse MAC associée, et son nombre associé VLAN. Le commutateur utilise la table d'ip source binding seulement quand la protection de source IP est activée.

Vous pouvez configurer la protection de source IP avec l'adresse IP source filtrant, ou avec le source ip et le filtrage des adresses MAC. Quand la protection de source IP est activée avec cette option, le trafic IP est filtré a basé sur l'adresse IP source. De commutateur le trafic IP en avant quand l'adresse IP source apparie une entrée dans la surveillance DHCP liant la base de données ou une attache dans la table d'ip source binding. Quand la protection de source IP est activée avec cette option, le trafic IP est filtré a basé sur le source ip et les adresses MAC. Le commutateur trafiquent en avant seulement quand le source ip et les adresses MAC apparient une entrée dans la table d'ip source binding.

Remarque: La protection de source IP est prise en charge seulement sur des ports de la couche 2, qui inclut des ports d'accès et de joncteur réseau.

Référez-vous aux instructions de configuration de protection de source IP pour des instructions sur la façon dont configurer la protection de source IP.

Ici, la protection de source IP avec le filtrage de source ip est configurée sur le FastEthernet 1/0/1 interface avec la commande d'**ip verify source**. Quand la protection de source IP avec le filtrage de source ip est activée sur un VLAN, la surveillance DHCP doit être activée sur l'accès VLAN auquel l'interface appartient. Émettez la commande de **show ip verify source** afin de vérifier la configuration de protection de source IP sur le commutateur.

Protection de la source IP

```
Cat3750#conf t Enter configuration commands, one per
line. End with CNTL/Z. Cat3750(config)#ip dhcp snooping
Cat3750(config)#ip dhcp snooping vlan 1 !--- See the
DHCP Snooping section of this document for !--- DHCP
snooping configuration information.
Cat3750(config)#interface fastEthernet 1/0/1
Cat3750(config-if)#ip verify source !--- Enables IP
source guard with source IP filtering. Cat3750#show ip
verify source Interface Filter-type Filter-mode IP-
address Mac-address Vlan --------- ----------- ---------
-- --------------- ----------------- ----- Fa1/0/1 ip
active 10.0.0.2 1 !--- For VLAN 1, IP source guard with
IP address filtering is configured !--- on the interface
and a binding exists on the interface. Cat3750#
```

Référez-vous compréhension derrière le pour en savoir plus de protection de source IP.

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

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

Informations connexes

- Sécurisation des réseaux avec des VLAN privés et des listes de contrôle d'accès VLAN
- Support pour les produits LAN
- Prise en charge de la technologie de commutation LAN
- Support et documentation techniques - Cisco Systems