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 présente un exemple de configuration pour certaines fonctions de sécurité de couche 2, telles que la sécurité des ports, l'espionnage DHCP, l'inspection dynamique du protocole ARP (protocole de résolution d'adresse) et la protection des sources IP, qui peuvent être mises en œuvre sur les commutateurs à configuration fixes de couche 3 de la gamme Cisco Catalyst.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les renseignements contenus dans ce document reposent sur le commutateur de la gamme

Cisco Catalyst 3750 doté de la version 12.2(25)SEC2.

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 ce qui suit :

- Commutateurs Cisco Catalyst, série 3550
- Commutateurs Cisco Catalyst, série 3560
- Commutateurs Cisco Catalyst, série 3560-E
- Commutateurs Cisco Catalyst, série 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

Comme pour les routeurs, les commutateurs de couche 2 et 3 ont leurs propres exigences relativement à la sécurité du réseau. Les commutateurs sont vulnérables à de nombreuses attaques de couche 3, comme c'est le cas pour les routeurs. Toutefois, les commutateurs, et la couche 2 du modèle de référence OSI en général, s'exposent à des attaques de réseau de différentes manières. Ceux-ci incluent :

- **Débordement de la table CAM (mémoire adressable par le contenu)**La taille des tables CAM est limitée. Si suffisamment d'entrées sont saisies dans la table CAM avant l'expiration des autres entrées, alors la table CAM se remplit de sorte qu'aucune nouvelle entrée ne peut être acceptée. Généralement, une intrusion réseau inonde le commutateur avec de nombreuses adresses MAC (Media Access Control) sources non valides jusqu'à ce que la table CAM soit pleine. Dans un tel cas, le commutateur inonde tous les ports ayant un trafic entrant, parce qu'il ne parvient pas à trouver le numéro de port d'une adresse MAC précise dans la table CAM. Le commutateur agit essentiellement comme un concentrateur. Si l'intrusion ne maintient pas l'inondation des adresses MAC sources non valides, le commutateur finit par faire expirer les anciennes entrées d'adresses MAC de la table CAM et se met à agir de nouveau comme un commutateur. Le débordement de la table CAM n'inonde que le trafic sur le réseau VLAN. L'intrus ne voit donc que le trafic sur le réseau VLAN auquel il est connecté.L'attaque de débordement de la table CAM peut être atténuée en configurant la sécurité des ports sur le commutateur. Cette option fournit soit la spécification des adresses MAC sur un port de commutation précis, soit la spécification du nombre d'adresses MAC pouvant être détectées par un port de commutateur. Lorsqu'une adresse MAC non valide est détectée sur le port, le commutateur peut soit bloquer l'adresse MAC fautive, soit fermer le port. La spécification des adresses MAC sur les ports de commutation est une solution bien trop difficile à gérer pour un environnement de production. La limite du nombre d'adresses MAC sur un port de commutateur est gérable. La mise en œuvre de la sécurité des ports

dynamiques au niveau du commutateur est une solution plus évolutive sur le plan administratif. Afin de mettre en œuvre la sécurité de port dynamique, indiquez le nombre maximal d'adresses MAC qui seront enregistrées.

- **Usurpation d'adresses MAC (Media Access Control)**Les attaques par usurpation d'adresses MAC se font par l'utilisation d'une adresse MAC connue d'un hôte distant pour que le commutateur cible transfère au pirate du réseau les trames destinées à cet hôte distant. Lorsqu'une seule trame est envoyée au moyen de l'adresse Ethernet source de l'autre hôte, le pirate du réseau remplace l'entrée de la table CAM de sorte que le commutateur lui envoie les paquets destinés à l'hôte. Tant que l'hôte achemine du trafic, il n'en reçoit aucun. Lorsque l'hôte achemine du trafic, l'entrée de la table CAM est réécrite une fois de plus afin de revenir au port d'origine.Utilisez la fonction de sécurité des ports pour limiter les attaques d'usurpation d'adresses MAC. La sécurité des ports permet de préciser l'adresse MAC du système connecté à un port en particulier. Il est ainsi possible d'indiquer également une mesure à prendre en cas de violation de la sécurité du port.
- **Usurpation du protocole ARP (protocole de résolution d'adresse)**Le protocole ARP est utilisé pour faire correspondre les adresses IP avec les adresses MAC dans un segment de réseau local où résident les hôtes d'un même sous-réseau. Normalement, un hôte envoie une demande ARP en diffusion pour trouver l'adresse MAC d'un autre hôte avec une adresse IP particulière, et une réponse ARP est reçue de l'hôte dont l'adresse correspond à la demande. L'hôte demandeur met alors en cache la réponse ARP reçue. Dans le protocole ARP, il existe une autre configuration pour permettre aux hôtes de produire des réponses ARP indésirables. Les réponses ARP indésirables sont appelées Gratuitous ARP (GARP). Un pirate peut utiliser GARP de manière malveillante pour usurper l'identité liée à une adresse IP sur un segment de réseau local. Cette méthode sert généralement à usurper l'identité entre deux hôtes ou tout le trafic en provenance et à destination d'une passerelle par défaut lors d'une attaque de l'homme du milieu.Lorsqu'une réponse ARP est élaborée, un pirate de réseau peut faire apparaître son système comme l'hôte de destination recherché par l'expéditeur. La réponse ARP fait alors en sorte que l'expéditeur stocke l'adresse MAC du système du pirate de réseau dans la mémoire cache du protocole ARP. Le commutateur stocke également cette adresse MAC dans sa table CAM. C'est ainsi que le pirate du réseau a pu insérer l'adresse MAC de son système dans la table CAM du commutateur et dans le cache du protocole ARP de l'expéditeur. Le pirate du réseau peut alors intercepter les trames destinées à l'hôte qu'il usurpe.Les minuteurs de mise en attente dans le menu de configuration de l'interface peuvent être utilisés pour atténuer les attaques par usurpation du protocole ART en définissant la durée pendant laquelle une entrée demeure dans le cache ARP. Cependant, les minuteurs de mise en attente ne suffisent pas. La modification de l'heure d'expiration du cache ARP sur tous les systèmes d'extrémité est nécessaire, ainsi que les entrées statiques ARP. Une autre solution pouvant servir à atténuer diverses exploitations du réseau liées au protocole ARP est l'utilisation de l'espionnage DHCP et de l'inspection dynamique du protocole ARP. Ces fonctions de Catalyst viennent valider les paquets ARP dans un réseau et permettent l'interception, la journalisation et le rejet des paquets ARP dont les adresses MAC et IP ne sont pas valides.L'espionnage DHCP filtre les messages DHCP sécurisés afin de garantir la sécurité. Ces messages sont ensuite utilisés pour créer et maintenir une table de liaison d'espionnage DHCP. L'espionnage DHCP considère comme non sécurisés les messages DHCP qui proviennent de tout port axé sur l'utilisateur qui n'est pas un port de serveur DHCP. Du point de vue de l'espionnage DHCP, ces ports non sécurisés axés sur l'utilisateur ne doivent pas envoyer de réponses de type serveur DHCP, comme DHCPOFFER, DHCPACK ou DHCPNAK. La table de liaison d'espionnage DHCP contient l'adresse MAC, l'adresse IP,

la durée de bail, le type de liaison, le numéro du VLAN et les renseignements sur l'interface qui correspondent aux interfaces locales non sécurisées d'un commutateur. La table de liaison d'espionnage DHCP ne contient pas d'informations sur les hôtes interconnectés ayant une interface sécurisée. Une interface non sécurisée est une interface qui est configurée pour recevoir des messages de l'extérieur du réseau ou du pare-feu. Une interface sécurisée est une interface qui est configurée pour recevoir uniquement des messages provenant du réseau. La table de liaison d'espionnage DHCP peut contenir des liaisons dynamiques et statiques entre des adresses MAC et des adresses IP.L'inspection dynamique d'ARP détermine la validité d'un paquet ARP en fonction des liaisons valides entre l'adresse MAC et l'adresse IP, stockées dans une base de données d'espionnage DHCP. En outre, l'inspection dynamique d'ARP peut valider les paquets ARP selon les listes de contrôle d'accès configurables par l'utilisateur. L'inspection des paquets ARP pour les hôtes qui utilisent des adresses IP configurées de manière statique est alors possible. L'inspection dynamique d'ARP permet l'utilisation de listes de contrôle d'accès au VLAN et par port (PACL) afin de limiter les paquets ARP pour des adresses IP précises à des adresses MAC précises.

- **DHCP Starvation**Une attaque DHCP Starvation consiste en la diffusion de requêtes DHCP avec des adresses MAC usurpées. Si suffisamment de requêtes sont envoyées, le pirate du réseau peut alors épuiser l'espace d'adresse disponible pour les serveurs DHCP pendant un certain temps. Le pirate peut alors configurer un serveur DHCP malveillant sur son système et répondre aux nouvelles requêtes DHCP des clients sur le réseau. Avec l'installation d'un serveur DHCP malveillant sur le réseau, un pirate peut fournir aux clients des adresses et d'autres renseignements sur le réseau. Comme les réponses DHCP comprennent généralement des renseignements sur la passerelle par défaut et le serveur DNS, le pirate peut utiliser son propre système comme passerelle par défaut et serveur DNS. Il s'agit alors d'une attaque de l'homme du milieu. Cependant, il n'est pas nécessaire d'épuiser les adresses DHCP pour introduire un serveur DHCP malveillant.Des fonctions supplémentaires de la gamme de commutateurs Catalyst, comme l'espionnage DHCP, peuvent être utilisées comme protection contre une attaque DHCP Starvation. L'espionnage DHCP est une fonction de sécurité qui filtre les messages DHCP non sécurisés, tout en créant et en gérant une table de liaison d'espionnage DHCP. La table de liaison contient des renseignements comme l'adresse MAC, l'adresse IP, la durée du bail, le type de liaison, le numéro du réseau VLAN et les renseignements de l'interface qui correspondent aux interfaces locales non sécurisées d'un commutateur. Les messages non sécurisés sont ceux qui proviennent de l'extérieur du réseau ou du pare-feu. Les interfaces de commutateur non sécurisées sont celles qui sont configurées pour recevoir ces messages, qui proviennent de l'extérieur du réseau ou du pare-feu.D'autres fonctions du commutateur Catalyst, comme la protection des sources IP, peuvent fournir une protection supplémentaire contre les attaques DHCP Starvation et l'usurpation d'adresses IP, notamment. Comme pour l'espionnage DHCP, la protection de la source IP est activée sur les ports de couche 2 qui ne sont pas sécurisés. Tout le trafic IP est en premier lieu bloqué, à l'exception des paquets DHCP saisis par le processus d'espionnage DHCP. Lorsqu'un client reçoit du serveur DHCP une adresse IP valide, un PACL est alors appliqué au port. Ainsi est limité le trafic IP du client vers les adresses IP source configurées dans la liaison. Tout autre trafic IP ayant une adresse source différente des adresses de liaison est filtré.

Configuration

Dans cette section figurent les renseignements qui permettent de configurer les fonctions de sécurité des ports, d'espionnage DHCP, d'inspection ARP dynamique et de protection des sources IP.

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

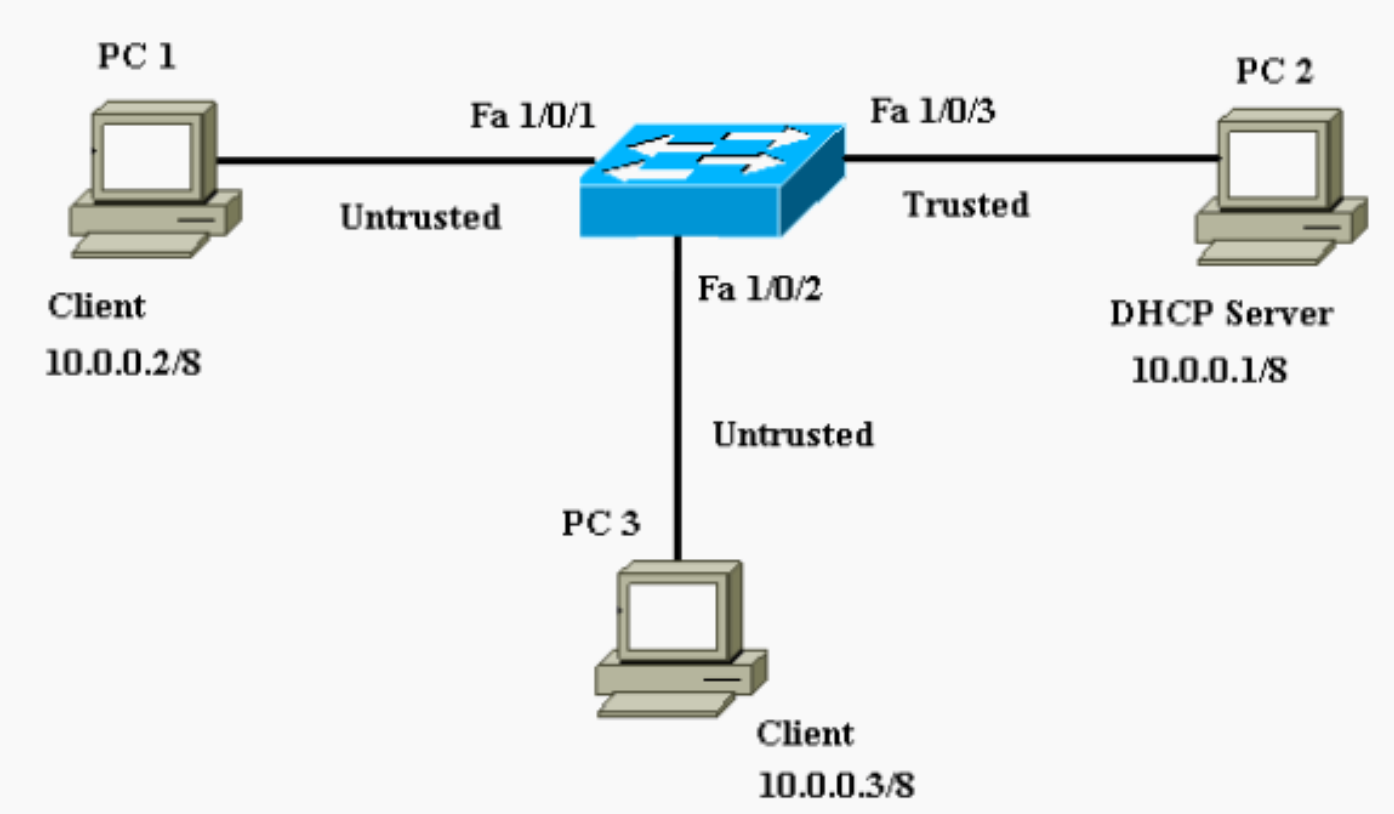
Voici ce que comprennent les configurations du commutateur Catalyst 3750 :

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

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

- Les PC 1 et 3 sont des clients connectés au commutateur.
- Le PC 2 est un serveur DHCP connecté au commutateur.
- Tous les ports du commutateur font partie du même VLAN (VLAN 1).
- Le serveur DHCP est configuré pour attribuer aux clients des adresses IP en fonction de leurs adresses MAC.



Sécurité de port

Vous pouvez utiliser la fonction de sécurité du port pour limiter et cibler les adresses MAC des stations qui sont autorisées à accéder au port. L'entrée à une interface est ainsi restreinte. Lorsque vous affectez des adresses MAC sécurisées à un port sécurisé, le port ne transfère pas les paquets avec des adresses sources à l'extérieur du groupe d'adresses définies. Si vous limitez

le nombre d'adresses MAC sécurisées pour n'en affecter qu'une seule, l'ordinateur connecté au port bénéficie de la totalité de la bande passante du port. Dans l'éventualité où un port est configuré comme port sécurisé et où le nombre maximal d'adresses MAC sécurisées est atteint, si l'adresse MAC d'une station tentant d'accéder au port diffère d'une des adresses MAC sécurisées identifiées, alors une violation de sécurité survient. De plus, si une station ayant une adresse MAC sécurisée configurée ou enregistrée sur un port sécurisé tente d'accéder à un autre port sécurisé, une violation est signalée. Par défaut, le port s'éteint si le nombre maximal d'adresses MAC sécurisées est dépassé.

Remarque : Lorsqu'un commutateur Catalyst 3750 rejoint une pile, le nouveau commutateur reçoit les adresses sécurisées configurées. Toutes les adresses sécurisées dynamiques sont téléchargées par le nouveau membre de la pile à partir des autres membres.

Consultez les Directives de configuration pour savoir comment configurer la sécurité des ports.

Ici, la fonction de sécurité du port est configurée sur l'interface FastEthernet 1/0/2. Par défaut, le maximum fixé pour l'interface est une seule adresse MAC sécurisée. Vous pouvez lancer la **commande show port-security interface pour vérifier l'état de la sécurité du 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 doivent pas être configurées en tant qu'adresses MAC sécurisées et statiques sur différents ports d'un commutateur.

Lorsqu'un téléphone IP est connecté à un commutateur par le port de commutation configuré pour le VLAN vocal, le téléphone envoie des paquets CDP non balisés et des paquets CDP vocaux balisés. Ainsi, l'adresse MAC du téléphone IP est enregistrée sur le PVID et le VVID. Si le nombre approprié d'adresses sécurisées n'est pas configuré, vous pouvez obtenir 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 fixer à deux le nombre maximal d'adresses sécurisées autorisées sur le port (pour le téléphone IP), en plus du nombre maximal d'adresses sécurisées autorisées sur le réseau d'accès VLAN pour résoudre ce problème.

Pour en savoir plus sur la configuration de la sécurité des ports, consultez le document à cet effet.

Surveillance DHCP

L'espionnage DHCP agit comme un pare-feu entre les serveurs DHCP et les hôtes non sécurisés. Vous utilisez l'espionnage DHCP pour différencier les interfaces non sécurisées connectées à l'utilisateur final des interfaces sécurisées connectées au serveur DHCP ou à un autre

commutateur. Lorsqu'un commutateur reçoit un paquet sur une interface non sécurisée et que l'interface appartient à un VLAN sur lequel l'espionnage DHCP est activée, le commutateur compare l'adresse MAC source et l'adresse matérielle du client DHCP. Si les adresses correspondent (par défaut), le commutateur transfère le paquet. Si les adresses ne correspondent pas, le commutateur abandonne le paquet. Le commutateur abandonne un paquet DHCP lorsqu'une des situations suivantes se produit :

- Un paquet provenant d'un serveur DHCP, comme un paquet DHCPOFFER, DHCPACK, DHCPNAK ou DHCPLEASEQUERY, provient de l'extérieur du réseau ou du pare-feu.
- Un paquet est reçu sur une interface non sécurisée, et l'adresse MAC source ainsi que l'adresse matérielle du client DHCP ne correspondent pas.
- Le commutateur reçoit un message de diffusion DHCPRELEASE ou DHCPDECLINE qui comprend une adresse MAC dans la base de données de liaison de l'espionnage DHCP, mais les renseignements de l'interface dans la base de données de liaison ne correspondent pas à l'interface sur laquelle le message a été reçu.
- Un agent de relais DHCP transfère un paquet DHCP, qui comprend une adresse IP d'agent de relais différente de 0.0.0.0, ou l'agent de relais transfère à un port non sécurisé un paquet contenant des renseignements sur l'option 82.

Consultez les directives de configuration de l'espionnage DHCP pour savoir comment configurer l'espionnage DHCP.

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

Remarque : Dans une pile de commutateurs avec des commutateurs Catalyst 3750, la surveillance DHCP est gérée sur le maître de pile. Lorsqu'un nouveau commutateur se joint à la pile, le commutateur reçoit la configuration de l'espionnage DHCP du maître de la pile. Lorsqu'un membre quitte la pile, toutes les liaisons de l'espionnage DHCP associées au commutateur expirent.

Remarque : Afin de s'assurer que la durée du bail dans la base de données est exacte, Cisco vous recommande d'activer et de configurer NTP. Si NTP est configuré, le commutateur écrit les modifications de liaison dans le fichier de liaison seulement lorsque l'horloge système du commutateur est synchronisée avec NTP.

Les serveurs DHCP malveillants peuvent être maîtrisés grâce aux fonctions d'espionnage DHCP. La commande **ip dhcp snooping est émise afin d'activer DHCP globalement sur le commutateur.** Lorsqu'ils sont configurés avec l'espionnage DHCP, les ports du réseau VLAN ne sont pas sécurisés pour les réponses DHCP. Ici, seule l'interface FastEthernet 1/0/3 connectée au serveur DHCP est configurée comme sécurisée.

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.
```

Consultez la section sur la configuration des fonctions DHCP pour en savoir plus.

Inspection dynamique d'ARP

L'inspection dynamique d'ARP est une fonction de sécurité qui valide les paquets ARP dans un réseau. Il intercepte, enregistre et rejette les paquets ARP ayant des liaisons d'adresses IP à MAC non valides. Cette fonction protège le réseau contre certaines attaques de l'homme du milieu.

L'inspection dynamique d'ARP garantit que seules les requêtes et les réponses d'ARP valides sont relayées. Le commutateur effectue les activités suivantes :

- Il intercepte toutes les requêtes et les réponses ARP sur les ports non sécurisés.
- Il vérifie que chaque paquet intercepté a une liaison d'adresse IP à MAC valide avant de mettre à jour le cache ARP local ou de transférer le paquet vers la destination appropriée.
- Il abandonne les paquets ARP non valides.

L'inspection dynamique d'ARP détermine la validité d'un paquet ARP en fonction des liaisons d'adresses IP à MAC valides stockées dans une base de données sécurisée, la base de données de liaison d'espionnage DHCP. Cette base de données est créée par l'espionnage DHCP si ce dernier est activé sur les réseaux VLAN et le commutateur. Si le paquet ARP entre sur une interface sécurisée, le commutateur le transfère sans vérification. Sur les interfaces non sécurisées, le commutateur transmet le paquet uniquement s'il est valide.

Dans les environnements autres que DHCP, l'inspection dynamique d'ARP peut valider les paquets ARP par rapport aux ACL d'ARP configurées par l'utilisateur pour les hôtes ayant des

adresses IP configurées de manière statique. Vous pouvez exécuter la commande de configuration globale **arp access-list pour définir une liste de contrôle d'accès ARP.** Les listes de contrôle d'accès ARP ont priorité sur les entrées de la base de données de liaison de l'espionnage DHCP. Le commutateur utilise les listes de contrôle d'accès seulement si vous exécutez la commande de configuration globale **ip arp inspection filter vlan afin de configurer les listes de contrôle d'accès.** 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.

Consultez les Directives de configuration d'inspection dynamique d'ARP pour savoir comment configurer l'inspection dynamique d'ARP.

La commande de configuration globale **ip arp inspection vlan est exécutée pour permettre l'inspection dynamique d'ARP par VLAN.** Ici, seule l'interface FastEthernet 1/0/3 qui est connectée au serveur DHCP est configurée comme sécurisée avec la commande **ip arp inspection trust.** L'espionnage DHCP doit être activé pour autoriser les paquets ARP auxquels des adresses IP ont été affectées de façon dynamique. Consultez la section sur l'espionnage DHCP dans le présent document pour en savoir plus sur le sujet.

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#
```

Consultez la section sur la configuration de l'inspection dynamique d'ARP pour en savoir plus sur le sujet.

Protection de la source IP

La protection de source IP est une fonction de sécurité qui filtre le trafic en fonction de la base de données des liaisons de l'espionnage DHCP et des liaisons de source IP configurées manuellement afin de restreindre le trafic IP sur les interfaces de couche 2 non routées. Vous pouvez utiliser la protection de source IP pour éviter les attaques de trafic causées lorsque l'hôte

tente d'utiliser l'adresse IP de son voisin. La protection de source IP empêche l'usurpation d'adresse IP/MAC.

Vous pouvez activer la protection de source IP lorsque l'espionnage DHCP est activée sur une interface non sécurisée. Une fois que la protection de source IP est activée sur une interface, le commutateur bloque tout le trafic IP reçu sur l'interface, hormis les paquets DHCP autorisés par l'espionnage DHCP. L'ACL du port est alors appliquée à l'interface. L'ACL du port autorise seulement le trafic IP ayant une adresse IP source dans la table de liaison de la source IP et refuse tout autre trafic.

La table de liaison de la source IP comporte des liaisons qui sont enregistrées par l'espionnage DHCP ou qui sont configurées manuellement (liaisons de source IP statiques). Une entrée figurant dans cette table comporte une adresse IP, son adresse MAC associée ainsi que son numéro de VLAN correspondant. Le commutateur utilise la table de liaison de source IP uniquement lorsque la protection de source IP est activée.

Vous pouvez configurer la protection de la source IP avec le filtrage des adresses IP sources ou avec le filtrage des adresses IP et MAC sources. Lorsque la protection de source IP est activée avec cette option, le trafic IP est alors filtré selon l'adresse IP source. Le commutateur transfère le trafic IP lorsque l'adresse IP source correspond à une entrée qui figure dans la base de données des liaisons d'espionnage DHCP ou à une liaison figurant dans la table de liaisons de source IP. Lorsque la protection de source IP est activée grâce à cette option, le trafic IP est alors filtré selon les adresses IP et MAC sources. Le commutateur transfère le trafic seulement lorsque les adresses IP et MAC sources correspondent à une entrée figurant dans la table de liaisons de source IP.

Remarque : la protection de la source IP est prise en charge uniquement sur les ports de couche 2, qui incluent les ports d'accès et d'agrégation.

Consultez les Directives de configuration de la protection de source IP pour savoir comment configurer la protection de source IP.

Ici, la protection de source IP avec le filtrage de source IP est configurée sur l'interface FastEthernet 1/0/1 avec la commande **ip verify source.** Lorsque la protection de source IP avec filtrage de source IP est activée sur un VLAN, l'espionnage DHCP doit être activé sur le VLAN d'accès auquel l'interface appartient. Exécutez la commande **show ip verify source pour vérifier la configuration de la 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#
```

Pour en savoir plus sur la protection de source IP, consultez la section à cet effet.

Vérification

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

Dépannage

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