Inspection ARP et table des adresses MAC

Ce chapitre décrit comment personnaliser la table des adresses MAC et configurer l'inspection ARP pour les groupes de ponts.

- À propos de l'inspection ARP et de la table des adresses MAC, à la page 1
- Paramètres d'usine, à la page 2
- Lignes directrices pour l'inspection ARP et la table d'adresses MAC, à la page 3
- Configurer l'inspection ARP et les autres paramètres ARP, à la page 3
- Personnaliser la table des adresses MAC pour les groupes de ponts, à la page 5
- Supervision de l'inspection ARP et de la table des adresses MAC, à la page 7
- Historique de l'inspection ARP et de la table des adresses MAC, à la page 8

À propos de l'inspection ARP et de la table des adresses MAC

Pour les interfaces d'un groupe de ponts, l'inspection ARP empêche une attaque « man-in-the-middle ». Vous pouvez également personnaliser d'autres paramètres ARP. Vous pouvez personnaliser le tableau d'adresses MAC pour les groupes de ponts, y compris en ajoutant une entrée ARP statique pour éviter l'usurpation d'adresse MAC.

Inspection ARP pour le trafic de groupe de ponts

Par défaut, tous les paquets ARP sont autorisés entre les membres du groupe de ponts. Vous pouvez contrôler le flux de paquets ARP en activant l'inspection ARP.

L'inspection ARP empêche les utilisateurs malveillants d'usurper l'identité d'autres hôtes ou routeurs (connue sous le nom d'usurpation d'identité ARP). L'usurpation d'identité ARP peut permettre une attaque de l'intercepteur. Par exemple, un hôte envoie une requête ARP au routeur de passerelle; le routeur de passerelle répond par l'adresse MAC du routeur de passerelle. Cependant, l'agresseur envoie une autre réponse ARP à l'hôte avec l'adresse MAC de l'agresseur au lieu de l'adresse MAC du routeur. L'agresseur peut désormais intercepter tout le trafic de l'hôte avant de le transférer au routeur.

L'inspection ARP garantit qu'un agresseur ne peut pas envoyer une réponse ARP avec l'adresse MAC de l'agresseur, tant que la bonne adresse MAC et l'adresse IP associée figurent dans le tableau ARP statique.

Lorsque vous activez l'inspection ARP, ASA compare l'adresse MAC, l'adresse IP et l'interface source de tous les paquets ARP aux entrées statiques du tableau ARP, et effectue les actions suivantes :

- Si l’adresse IP, l’adresse MAC et l’interface source correspondent à une entrée ARP, le paquet est transmis.
- En cas de non-concordance entre l’adresse MAC, l’adresse IP ou l’interface, ASA abandonne le paquet.
- Si le paquet ARP ne correspond à aucune entrée dans le tableau ARP statique, vous pouvez définir ASA pour transférer le paquet hors de toutes les interfaces (flood) (submersion), ou pour abandonner le paquet.

Remarque L’interface dédiée Management (gestion) ne submerge jamais de paquets, même si ce paramètre est réglé à flood.

Tableau d'adresses MAC

Lorsque vous utilisez des groupes de ponts, l’ASA apprend et construit un tableau d’adresses MAC de la même manière qu’un pont ou un commutateur normal : lorsqu’un périphérique envoie un paquet par l’intermédiaire du groupe de ponts, l’ASA ajoute l’adresse MAC à son tableau. Le tableau associe l’adresse MAC à l’interface source de sorte que l’ASA sache envoyer tous les paquets adressés au périphérique par la bonne interface. Comme le trafic entre les membres du groupe de ponts est soumis à la politique de sécurité ASA, si l’adresse MAC de destination d’un paquet ne figure pas dans le tableau, l’ASA ne submerge pas le paquet d’origine sur toutes les interfaces comme un pont normal le fait. Au lieu de cela, il génère les paquets suivants pour les périphériques connectés directement ou pour les périphériques distants :

- Paquets pour les périphériques connectés directement : l’ASA génère une requête ARP pour l’adresse IP de destination, afin de pouvoir apprendre quelle interface reçoit la réponse ARP.
- Paquets pour les périphériques distants : l’ASA génère un message ping vers l’adresse IP de destination afin de pouvoir apprendre quelle interface reçoit la réponse ping.

Le paquet d'origine est abandonné.

Pour le mode routé, vous pouvez éventuellement activer la submersion des paquets non IP sur toutes les interfaces.

Paramètres d'usine

- Si vous activez l’inspection ARP, le paramètre par défaut est d’inonder les paquets non correspondants.
- La valeur du délai d’expiration par défaut pour les entrées du tableau d’adresses MAC dynamiques est de 5 minutes.
- Par défaut, chaque interface apprend automatiquement les adresses MAC du trafic d’entrée et ASA ajoute les entrées correspondantes au tableau d’adresses MAC.

Remarque Cisco Secure Firewall ASA génère un paquet de réinitialisation pour réinitialiser une connexion qui est refusée par un moteur d'inspection dynamique. Ici, l'adresse MAC de destination du paquet n'est pas déterminée en fonction de la recherche de la table ARP, mais est plutôt tirée directement des paquets (connexions) qui sont refusés.

Lignes directrices pour l'inspection ARP et la table d'adresses MAC

- L'inspection ARP n'est possible que pour les groupes de ponts.
- La configuration de la table des adresses MAC n'est possible que pour les groupes de ponts.

Configurer l'inspection ARP et les autres paramètres ARP

Pour les groupes de ponts, vous pouvez activer l'inspection ARP. Vous pouvez également configurer d'autres paramètres ARP pour les groupes de ponts et pour les interfaces en mode routé.

Procédure

Étape 1 Ajoutez des entrées ARP statiques en fonction de Ajouter une entrée ARP statique et personnaliser d'autres paramètres ARP, à la page 3. L'inspection ARP compare les paquets ARP avec les entrées ARP statiques dans le tableau ARP. Par conséquent, des entrées ARP statiques sont nécessaires pour cette fonctionnalité. Vous pouvez également configurer d'autres paramètres ARP.

Étape 2 Activez l'inspection ARP conformément à Activer l'inspection ARP, à la page 5.

Ajouter une entrée ARP statique et personnaliser d'autres paramètres ARP

Par défaut, pour les groupes de ponts, tous les paquets ARP sont autorisés entre les interfaces membres des groupes de ponts. Vous pouvez contrôler le flux de paquets ARP en activant l'inspection ARP. L'inspection ARP compare les paquets ARP avec les entrées ARP *statiques* dans le tableau ARP.

Pour les interfaces routées, vous pouvez saisir des entrées ARP statiques, mais normalement, les entrées dynamiques sont suffisantes. Pour les interfaces routées, la table ARP est utilisée pour acheminer des paquets aux hôtes connectés directement. Bien que les expéditeurs identifient la destination d'un paquet par une adresse IP, la livraison réelle du paquet sur Ethernet dépend de l'adresse MAC Ethernet. Lorsqu'un routeur ou un hôte souhaite acheminer un paquet sur un réseau directement connecté, il envoie une requête ARP demandant l'adresse MAC associée à l'adresse IP, puis achemine le paquet à l'adresse MAC en fonction de la réponse ARP. L'hôte ou le routeur conserve une table ARP pour ne pas avoir à envoyer des demandes ARP pour chaque paquet à livrer. La table ARP est mise à jour dynamiquement chaque fois que des réponses ARP sont

envoyées sur le réseau et, si une entrée n'est pas utilisée pendant un certain temps, elle expire. Si une entrée est incorrecte (par exemple, l'adresse MAC change pour une adresse IP donnée), l'entrée doit expirer avant de pouvoir être mise à jour avec les nouvelles informations.

En mode transparent, l'ASA utilise uniquement les entrées ARP dynamiques de la table ARP pour le trafic entrant et sortant de l'ASA, tel que le trafic de gestion.

Vous pouvez également définir le délai d'expiration d'ARP et d'autres comportements d'ARP.

Procédure

Étape 1 Ajoutez une entrée ARP statique :

arp *interface_name ip_address mac_address* [**alias**]

Exemple :

```
ciscoasa(config)# arp outside 10.1.1.1 0009.7cbe.2100
```

Cet exemple autorise les réponses ARP du routeur à l'adresse 10.1.1.1 avec l'adresse MAC 0009.7cbe.2100 sur l'interface externe.

Précisez **alias** dans le mode routé pour activer le serveur mandataire ARP pour ce mappage. Si l'ASA reçoit une requête ARP pour l'adresse IP spécifiée, il répond par l'adresse MAC de l'ASA. Ce mot clé est utile si certains de vos périphériques n'effectuent pas d'ARP, par exemple. En mode transparent de pare-feu, ce mot clé est ignoré; l'ASA n'exécute pas le protocole ARP par mandataire.

Étape 2 Définissez le délai d'expiration ARP pour les entrées ARP dynamiques :

arp timeout *secondes*

Exemple :

```
ciscoasa(config)# arp timeout 5000
```

Ce champ définit le délai avant que l'ASA recrée la table ARP, entre 60 et 4294967 secondes. La valeur par défaut est de 14400 secondes. La reconstitution de la table ARP met automatiquement à jour les nouvelles informations sur l'hôte et supprime les anciennes. Vous pourriez souhaiter réduire le délai d'expiration, car les informations sur l'hôte changent fréquemment.

Étape 3 Autorisez les sous-réseaux non connectés :

arp permit-nonconnected

Le cache ARP de l'ASA contient uniquement les entrées des sous-réseaux connectés directement par défaut. Vous pouvez activer le cache ARP pour inclure également les sous-réseaux non connectés directement. Nous vous déconseillons d'activer cette fonctionnalité, sauf si vous connaissez les risques de sécurité. Cette fonctionnalité pourrait faciliter les attaques par déni de service contre l'ASA; un utilisateur, sur n'importe quelle interface, pourrait envoyer de nombreuses réponses ARP et sur téléverser la table ARP de l'ASA de fausses entrées.

Vous souhaiterez peut-être utiliser cette fonctionnalité si vous utilisez :

- Sous-réseaux secondaires.

- Serveur mandataire ARP sur les routes adjacentes pour le transfert du trafic.

Étape 4 Définissez la limite de débit ARP pour contrôler le nombre de paquets ARP par seconde :

arp rate-limit *secondes*

Exemple :

```
ciscoasa(config)# arp rate-limit 1000
```

Saisissez une valeur entre 10 et 32 768. La valeur par défaut dépend de votre modèle d'ASA. Vous pouvez personnaliser cette valeur pour empêcher une attaque de tempête ARP.

Activer l'inspection ARP

Cette section décrit comment activer l'inspection ARP pour les groupes de ponts.

Procédure

Activez l'inspection ARP :

arp-inspection *interface_name* **enable** [**flood** | **no-flood**]

Exemple :

```
ciscoasa(config)# arp-inspection outside enable no-flood
```

Le mot clé **flood** transfère les paquets ARP non correspondants sur toutes les interfaces et **no-flood** abandonne les paquets non correspondants.

Le paramètre par défaut est d'inonder les paquets non correspondants. Pour restreindre le protocole ARP par l'ASA aux entrées statiques uniquement, définissez cette commande sur **no-flood**.

Personnaliser la table des adresses MAC pour les groupes de ponts

Cette section décrit comment vous pouvez personnaliser le tableau d'adresses MAC pour les groupes de ponts.

Ajouter une adresse MAC statique pour les groupes de ponts

Normalement, les adresses MAC sont ajoutées au tableau d'adresses MAC de manière dynamique au fur et à mesure que le trafic en provenance d'une adresse MAC particulière entre dans une interface. Vous pouvez ajouter des adresses MAC statiques au tableau d'adresses MAC. L'ajout d'entrées statiques offre l'avantage de prévenir l'usurpation d'adresse MAC. Si un client avec la même adresse MAC qu'une entrée statique tente

d'envoyer le trafic vers une interface qui ne correspond pas à l'entrée statique, l'ASA abandonne le trafic et génère un message système. Lorsque vous ajoutez une entrée ARP statique (voir Ajouter une entrée ARP statique et personnaliser d'autres paramètres ARP, à la page 3), une entrée d'adresse MAC statique est automatiquement ajoutée au tableau d'adresses MAC.

Pour ajouter une adresse MAC statique au tableau d'adresses MAC, procédez comme suit.

Procédure

Ajouter une adresse MAC statique

mac-address-table statique *interface_name mac_address*

Exemple :

```
ciscoasa(config)# mac-address-table static inside 0009.7cbe.2100
```

Le *nom d'interface* est l'interface source.

Définir le délai d'expiration de l'adresse MAC

La valeur du délai d'expiration par défaut pour les entrées du tableau d'adresses MAC dynamiques est de 5 minutes, mais vous pouvez modifier ce délai. Pour modifier le délai d'expiration, procédez comme suit.

Procédure

Définissez le délai d'expiration de l'entrée d'adresse MAC :

mac-address-table aging-time *timeout_value*

Exemple :

```
ciscoasa(config)# mac-address-table aging-time 10
```

La valeur *timeout_value* (en minutes) est comprise entre 5 et 720 (12 heures). La valeur par défaut est de 5 minutes.

Configurer l'apprentissage de l'adresse MAC

Par défaut, chaque interface apprend automatiquement les adresses MAC du trafic d'entrée et l'ASA ajoute les entrées correspondantes au tableau d'adresses MAC. Vous pouvez désactiver l'apprentissage des adresses MAC si vous le souhaitez; cependant, à moins que vous ajoutiez statiquement des adresses MAC au tableau, aucun trafic ne peut passer par l'ASA. En mode routé, vous pouvez activer la submersion des paquets non IP sur toutes les interfaces.

Pour configurer l'apprentissage des adresses MAC, procédez comme suit :

Procédure

Étape 1 Désactivez l'apprentissage des adresses MAC :

mac-learn *interface_name* **disable**

Exemple :

```
ciscoasa(config)# mac-learn inside disable
```

La forme **no** (non) de cette commande réactive l'apprentissage des adresses MAC.

La commande **clear configure mac-learn** réactive l'apprentissage des adresses MAC sur toutes les interfaces.

Étape 2 (Mode routé uniquement) Activez la submersion des paquets non IP.

mac-learn flood

Exemple :

```
ciscoasa(config)# mac-learn flood
```

Supervision de l'inspection ARP et de la table des adresses MAC

- **show arp-inspection**

  Supervise l'inspection ARP. Affiche les paramètres actuels pour l'inspection ARP sur toutes les interfaces.

- **show mac-address-table [*interface_name*]**

  Supervise le tableau d'adresses MAC. Vous pouvez afficher le tableau d'adresses MAC entier (y compris les entrées statiques et dynamiques pour les deux interfaces) ou vous pouvez afficher le tableau d'adresses MAC d'une interface.

  Voici un exemple de sortie de la commande **show mac-address-table** qui affiche le tableau entier :

```
ciscoasa# show mac-address-table
interface        mac address           type         Time Left
------------------------------------------------------------------------
outside     0009.7cbe.2100       static    -
inside     0010.7cbe.6101       static    -
inside     0009.7cbe.5101       dynamic    10
```

  Voici un exemple de sortie de la commande **show mac-address-table** qui affiche le tableau de l'interface interne :

```
ciscoasa# show mac-address-table inside
```

```
interface        mac address       type         Time Left
-----------------------------------------------------------------------
inside     0010.7cbe.6101       static    -
inside     0009.7cbe.5101       dynamic    10
```

Voici un exemple de sortie de la commande **show mac-address-table** qui affiche le nombre total d'entrées de groupe de ponts statiques et dynamiques :

```
ciscoasa# show mac-address-table count
Static     mac-address bridges (curr/max): 0/16384
Dynamic    mac-address bridges (curr/max): 0/16384
```

Historique de l'inspection ARP et de la table des adresses MAC

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Inspection ARP	7.0(1)	L'inspection ARP compare l'adresse MAC, l'adresse IP et l'interface source de tous les paquets ARP aux entrées statiques du tableau ARP. Cette fonctionnalité est disponible pour le mode de pare-feu transparent et pour les interfaces d'un groupe de ponts en mode transparent et en mode routé à partir de la version 9.7(1). Nous avons introduit les commandes suivantes : **arp**, **arp-inspection** et **show arp-inspection**.
Tableau d'adresses MAC	7.0(1)	Vous souhaiterez peut-être personnaliser le tableau des adresses MAC pour le mode transparent et pour les interfaces d'un groupe de ponts en mode transparent et en mode routé à partir de la version 9.7(1). Nous avons introduit les commandes suivantes : **mac-address-table static**, **mac-address-table aging-time**, **mac-learn disable** et **show mac-address-table**.

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Ajouts de cache ARP pour les sous-réseaux non connectés	8.4(5)/9.1(2)	Le cache ARP de l'ASA contient uniquement les entrées des sous-réseaux connectés directement par défaut. Vous pouvez désormais activer le cache ARP pour inclure également les sous-réseaux non connectés directement. Nous vous déconseillons d'activer cette fonctionnalité, sauf si vous connaissez les risques de sécurité. Cette fonctionnalité pourrait faciliter les attaques par déni de service contre l'ASA; un utilisateur, sur n'importe quelle interface, pourrait envoyer de nombreuses réponses ARP et sur téléverser la table ARP de l'ASA de fausses entrées. Vous souhaiterez peut-être utiliser cette fonctionnalité si vous utilisez : • Sous-réseaux secondaires. • Serveur mandataire ARP sur les routes adjacentes pour le transfert du trafic. Nous avons introduit la commande suivante : **arp permit-nonconnected**.
Limitation de débit ARP personnalisable	9.6(2)	Vous pouvez définir le nombre maximum de paquets ARP autorisés par seconde. La valeur par défaut dépend de votre modèle d'ASA. Vous pouvez personnaliser cette valeur pour empêcher une attaque de tempête ARP. Nous avons ajouté les commandes suivantes : **arp rate-limit, show arp rate-limit**

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Routage et pont intégrés	9.7(1)	Le routage et le pont intégrés permettent d'effectuer le routage entre un groupe de ponts et une interface routée. Un groupe de ponts est un groupe d'interfaces que l'ASA relie par des ponts au lieu de routes. L'ASA n'est pas un vrai pont, car l'ASA continue d'agir comme un pare-feu : le contrôle d'accès entre les interfaces est contrôlé et toutes les vérifications de pare-feu usuelles sont en place. Auparavant, vous ne pouviez configurer les groupes de ponts qu'en mode de pare-feu transparent, où vous ne pouvez pas effectuer d'acheminement entre les groupes de ponts. Cette fonctionnalité vous permet de configurer des groupes de ponts en mode de pare-feu routé et pour effectuer le routage entre des groupes de ponts et entre un groupe de ponts et une interface routée. Le groupe de ponts participe au routage en utilisant une interface virtuelle de pont (BVI) pour servir de passerelle au groupe de ponts. Le routage et le pont intégrés offrent une solution de rechange au commutateur de couche 2 externe si vous avez des interfaces supplémentaires sur l'ASA à affecter au groupe de ponts. En mode routé, les BVI peuvent être une interface nommée et participer séparément des interfaces membres à certaines fonctionnalités, telles que les règles d'accès et le serveur DHCP. Les fonctionnalités suivantes, prises en charge en mode transparent, ne sont pas prises en charge en mode routé : mode de contexte multiple, mise en grappe d'ASA. Les fonctionnalités suivantes ne sont pas prises en charge sur les BVI : le routage dynamique et le routage de multidiffusion. Nous avons modifié les commandes suivantes : **access-group, access-list ethertype, arp-inspection, dhcpd, mac-address-table static, mac-address-table aging-time, mac-learn, route, show arp-inspection, show bridge-group, show mac-address-table, show mac-learn**

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.