Configuration avancée de l'interface

Ce chapitre décrit comment configurer les adresses MAC pour les interfaces, définir l'unité de transfert maximale (MTU), définir la taille de segment maximum TCP (TCP MSS) et autoriser une communication de même niveau de sécurité. La définition de la bonne MTU et de la taille de segment maximum TCP est essentielle pour garantir les meilleures performances du réseau.

À propos des configurations avancées de l'interface

Cette section décrit les paramètres d'interface avancés.

À propos des adresses MAC

Vous pouvez affecter manuellement des adresses MAC pour remplacer la valeur par défaut. Pour le mode de contexte multiple, vous pouvez générer automatiquement des adresses MAC uniques (pour toutes les interfaces affectées à un contexte) et un mode de contexte unique (pour les sous-interfaces)..

Remarque Vous pourriez souhaiter affecter des adresses MAC uniques aux sous-interfaces définies sur ASA, car elles utilisent la même adresse MAC gravée de l'interface parente. Par exemple, votre fournisseur de services peut effectuer un contrôle d'accès en fonction de l'adresse MAC. En outre, étant donné que les adresses locales de liaison IPv6 sont générées sur la base de l'adresse MAC, l'attribution d'adresses MAC uniques aux sous-interfaces permet d'obtenir des adresses locales de liaison IPv6 uniques, ce qui peut éviter la perturbation du trafic dans certaines instances du périphérique ASA.

Adresses MAC par défaut

Les attributions d'adresses MAC par défaut dépendent du type d'interface.

- Interfaces physiques : l'interface physique utilise l'adresse MAC gravée.

- Interfaces VLAN (Firepower 1010) —Mode de pare-feu routé : toutes les interfaces VLAN partagent une adresse MAC. Assurez-vous que tous les commutateurs connectés peuvent prendre en charge ce scénario. Si les commutateurs connectés nécessitent des adresses MAC uniques, vous pouvez attribuer manuellement des adresses MAC. Consultez Configurer manuellement l'adresse MAC, à la page 5

  Mode pare-feu transparent : chaque interface VLAN a une adresse MAC unique. Vous pouvez remplacer les adresses MAC générées si vous le souhaitez en attribuant manuellement des adresses MAC. Consultez Configurer manuellement l'adresse MAC, à la page 5.

- EtherChannels (modèles Firepower) : pour un EtherChannel, toutes les interfaces qui font partie du groupe de canaux partagent la même adresse MAC. Cette fonction rend l'EtherChannel transparent pour les applications et les utilisateurs du réseau, car ils ne voient qu'une seule connexion logique; ils n'ont aucune connaissance des liens individuels. L'interface du canal de port utilise une adresse MAC unique provenant d'un pool; L'appartenance à l'interface n'affecte pas l'adresse MAC.

- EtherChannels (modèles ASA) : l'interface du canal de port utilise l'adresse MAC d'interface de groupe de canaux du plus petit numéro comme adresse MAC du canal de port. Vous pouvez aussi configurer une adresse MAC pour l'interface du canal de port. Nous vous recommandons de configurer une adresse MAC unique au cas où l'appartenance à l'interface du canal de groupe changerait. Si vous supprimez l'interface qui fournissait l'adresse MAC du canal de port, l'adresse MAC du canal de port passe à l'interface ayant le numéro le plus bas, ce qui perturbe le trafic.

- Sous-interfaces : toutes les sous-interfaces d'une interface physique utilisent la même adresse MAC gravée. Vous pourriez souhaiter affecter des adresses MAC uniques aux sous-interfaces. Par exemple, votre fournisseur de services peut effectuer un contrôle d'accès en fonction de l'adresse MAC. En outre, étant donné que les adresses locales de lien IPv6 sont générées en fonction de l'adresse MAC, l'affectation d'adresses MAC uniques aux sous-interfaces permet d'établir des adresses locales de lien IPv6 uniques, ce qui peut éviter des perturbations de trafic dans certaines instances sur ASA.

Adresses MAC automatiques

En mode de contexte multiple, la génération automatique affecte des adresses MAC uniques à toutes les interfaces affectées à un contexte.

Si vous attribuez manuellement une adresse MAC et activez la génération automatique, l'adresse MAC attribuée manuellement est utilisée. Si vous supprimez ultérieurement l'adresse MAC manuelle, l'adresse générée automatiquement est utilisée, si elle est activée.

Dans les rares cas où l'adresse MAC générée entre en conflit avec une autre adresse MAC privée de votre réseau, vous pouvez définir manuellement l'adresse MAC pour l'interface.

Comme les adresses générées automatiquement (lors de l'utilisation d'un préfixe) commencent par A2, vous ne pouvez pas commencer les adresses MAC manuelles par A2 si vous souhaitez également utiliser la génération automatique.

Le châssis génère l'adresse MAC en utilisant le format suivant :

A2*xx.yyzz.zzzz*

Où *xx.yy* est un préfixe défini par l'utilisateur ou un préfixe généré automatiquement en fonction des deux derniers octets de l'adresse MAC de l'interface, et *zz.zzzz* est un compteur interne généré par l'ASA. Pour l'adresse MAC de secours, l'adresse est identique, sauf que le compteur interne est augmenté de 1.

Pour donner un exemple d'utilisation du préfixe, si vous définissez le préfixe 77, l'ASA convertit 77 en valeur hexadécimale 004D (*yyxx*). Lorsqu'il est utilisé dans l'adresse MAC, le préfixe est inversé (*xxyy*) pour correspondre à la forme native de l'ASA :

A2**4D.00***zz.zzzz*

Pour un préfixe 1009 (03F1), l'adresse MAC est :

A2**F1.03***zz.zzzz*

Remarque Le format d'adresse MAC sans préfixe est une version existante. Consultez la commande **mac-address auto** dans la référence de commandes pour plus d'informations sur le format existant.

À propos de la MTU

La MTU spécifie la taille maximale de la *charge utile* de trame que l'ASA peut transmettre sur une interface Ethernet donnée. La valeur MTU correspond à la taille de la trame *sans* en-tête Ethernet, sans balisage VLAN ou autre surdébit. Par exemple, lorsque vous définissez la MTU sur 1500, la taille de trame attendue est de 1518 octets, en-têtes compris, ou de 1522 lorsque vous utilisez le VLAN. Ne définissez pas la valeur MTU plus élevée pour prendre en charge ces en-têtes.

Pour VXLAN ou Geneve, le datagramme Ethernet entier est encapsulé, de sorte que le nouveau paquet IP est plus volumineux et nécessite une MTU plus grande : vous devez définir la MTU de l'interface source VTEP ASA sur la MTU du réseau + 54 octets (pour VXLAN) ou + 306 octets (Genève).

Chemin de découverte de MTU

L'ASA prend en charge la découverte de chemin MTU (comme défini dans la RFC 1191), qui permet à tous les périphériques d'un chemin réseau entre deux hôtes de coordonner la MTU afin qu'ils puissent normaliser sur la MTU la plus basse du chemin.

MTU par défaut

Par défaut, la MTU sur ASA est de 1500 octets. Cette valeur n'inclut pas les 18 à 22octets pour l'en-tête Ethernet, le balisage VLAN ou d'autres surdébits.

Lorsque vous activez VXLAN sur l'interface source VTEP, si la MTU est inférieure à 1 554 octets, l'ASA l'augmente automatiquement à 1 554 octets. Dans ce cas, le datagramme Ethernet entier est encapsulé, de sorte que le nouveau paquet est plus volumineux et nécessite une MTU plus grande. En général, vous devez définir la MTU de l'interface source de l'ASA comme étant la MTU du réseau + 54 octets.

MTU et fragmentation.

Pour IPv4, si un paquet IP sortant dépasse la MTU spécifiée, il est fragmenté en au moins deux trames. Les fragments sont réassemblés à la destination (et parfois aux sauts intermédiaires), et la fragmentation peut dégrader les performances. Pour IPv6, la fragmentation des paquets n'est généralement pas autorisée. Par conséquent, vos paquets IP doivent respecter la taille de la MTU pour éviter la fragmentation.

Pour les paquets TCP, les points terminaux utilisent généralement leur MTU pour déterminer la taille maximale du segment TCP (MTU – 40, par exemple). Si des en-têtes TCP supplémentaires sont ajoutés en cours de route, par exemple pour les tunnels VPN de site à site, le MSS TCP devra peut-être être ajusté par l'entité de tunnellisation. Consultez À propos de TCP MSS, à la page 4.

Pour UDP ou ICMP, l'application doit prendre en compte la MTU pour éviter la fragmentation.

Remarque L'ASA peut recevoir des trames plus grandes que la MTU configurée tant qu'il y a de l'espace en mémoire.

MTU et trames grand format

Une MTU plus grande vous permet d'envoyer des paquets plus volumineux. Des paquets plus volumineux pourraient être plus efficaces pour votre réseau. Consultez les consignes suivantes :

- Correspondance des MTU sur le chemin de trafic : nous vous recommandons de définir la MTU sur toutes les interfaces ASA et les autres interfaces de périphériques le long du chemin de trafic. La correspondance des MTU empêche les périphériques intermédiaires de fragmenter les paquets.
- Prise en charge des trames étendues : vous pouvez définir la MTU à 9 000 octets ou plus lorsque vous activez les trames étendues. Le maximum dépend du modèle.

À propos de TCP MSS

La taille maximale de segment (MSS) TCP est la taille de la charge utile TCP *avant* l'ajout des en-têtes TCP et IP. Les paquets UDP ne sont pas concernés. Le client et le serveur échangent des valeurs TCP MSS lors de la prise de contact tridirectionnelle lors de l'établissement de la connexion.

Vous pouvez définir le MSS TCP sur l'ASA pour le trafic de transit; par défaut, le MSS TCP maximal est défini sur 1380 octets. Ce paramètre est utile lorsque ASA doit augmenter la taille du paquet pour l'encapsulation VPN IPsec. Cependant, pour les points terminaux non IPsec, vous devez désactiver le MSS TCP maximal sur ASA.

Si vous définissez un MSS TCP maximal, si l'une ou l'autre des extrémités d'une connexion demande un MSS TCP supérieur à la valeur définie sur l'ASA, alors l'ASA remplace le MSS TCP dans le paquet de demande par l'ASA maximum. Si l'hôte ou le serveur ne demande pas de message MSS du protocole TCP, ASA assume la valeur par défaut de la RFC 793 de 536 octets (IPv4) ou de 1 220 octets (IPv6), mais ne modifie pas le paquet. Par exemple, vous laissez la MTU par défaut à 1500 octets. Un hôte demande un MSS de 1500 moins la longueur de l'en-tête TCP et IP, ce qui définit le MSS à 1460. Si le MSS TCP maximal de l'ASA est de 1 380 (par défaut), l'ASA modifie la valeur du MSS dans le paquet de demande TCP à 1380. Le serveur envoie ensuite des paquets avec une charge utile de 1380 octets. L'ASA peut alors ajouter jusqu'à 120 octets d'en-tête au paquet tout en conservant la taille de MTU de 1500.

Vous pouvez également configurer le MSS TCP minimal; si un hôte ou un serveur demande un très petit MSS TCP, ASA peut augmenter la valeur. Par défaut, le MSS TCP minimal n'est pas activé.

Pour le trafic vers la boîte, y compris pour les connexions SSL VPN, ce paramètre ne s'applique pas. L'ASA utilise la MTU pour calculer le TCP MSS : MTU – 40 (IPv4) ou MTU – 60 (IPv6).

TCP MSS par défaut

Par défaut, le MSS TCP maximal sur l'ASA est de 1380 octets. Cette valeur par défaut convient aux connexions VPN IPsec IPv4 où la valeur des en-têtes peut atteindre 120 octets; Cette valeur correspond à la MTU par défaut de 1500 octets.

Paramètre MSS TCP maximal suggéré

Le MSS TCP par défaut suppose que l'ASA agit comme un point terminal de VPN IPsec IPv4 et a une MTU de 1500. Lorsque l'ASA agit comme un point terminal de VPN IPsec IPv4, il doit gérer jusqu'à 120 octets pour les en-têtes TCP et IP.

Si vous modifiez la valeur MTU, utilisez IPv6 ou n'utilisez pas ASA comme point terminal VPN IPsec, vous devez modifier le paramètre TCP MSS.

Consultez les consignes suivantes :

- Normal Traffic (Trafic normal) : Désactivez la limite TCP MSS et acceptez la valeur établie entre les points terminaux de connexion. Étant donné que les points terminaux de connexion dérivent généralement le MSS TCP de la MTU, les paquets non IPsec correspondent généralement à ce MSS TCP.
- IPv4 IPsec endpoint traffic : Définissez le MSS TCP maximal sur la MTU - 120. Par exemple, si vous utilisez des trames étendues et que vous définissez la MTU à 9000, vous devez définir le MSS TCP sur 8880 pour profiter de la nouvelle MTU.
- IPv6 IPsec endpoint Traffic (Trafic de point terminal IPsec IPv6) : définissez le MSS TCP maximal sur la MTU - 140.

Communication inter-interface

Permettre à des interfaces de même niveau de sécurité de communiquer entre elles offre les avantages suivants :

- Vous pouvez configurer plus de 101 interfaces de communication.

  Si vous utilisez différents niveaux pour chaque interface et n'affectez aucune interface au même niveau de sécurité, vous ne pouvez configurer qu'une seule interface par niveau (de 0 à 100).

- Vous souhaitez que le trafic passe librement entre toutes les mêmes interfaces de sécurité sans ACL.

Si vous activez la même communication d'interface de sécurité, vous pouvez toujours configurer des interfaces à différents niveaux de sécurité, comme d'habitude.

Communication intra-interface (mode de pare-feu routé)

La communication intra-interface peut être utile pour le trafic VPN qui entre dans une interface, mais qui est ensuite acheminé vers la même interface. Dans ce cas, le trafic VPN peut être non chiffré ou rechiffré pour une autre connexion VPN. Par exemple, si vous avez un réseau VPN en étoile, où l'ASA est le concentrateur et les réseaux VPN distants sont des rayons, pour qu'un rayon communique avec un autre rayon, le trafic doit entrer dans l'ASA, puis ressortir vers l'autre rayon.

Remarque Tout le trafic autorisé par cette fonctionnalité reste soumis aux règles du pare-feu. Veillez à ne pas créer de situation de routage asymétrique qui pourrait empêcher le trafic de retour de traverser l'ASA.

Configurer manuellement l'adresse MAC

Si vous devez attribuer manuellement l'adresse MAC, vous pouvez le faire en suivant cette procédure.

Vous pourriez souhaiter affecter des adresses MAC uniques aux sous-interfaces définies sur ASA, car elles utilisent la même adresse MAC gravée de l'interface parente. Par exemple, votre fournisseur de services peut effectuer un contrôle d'accès en fonction de l'adresse MAC. En outre, étant donné que les adresses locales de lien IPv6 sont générées en fonction de l'adresse MAC, l'affectation d'adresses MAC uniques aux sous-interfaces permet d'établir des adresses locales de lien IPv6 uniques, ce qui peut éviter des perturbations de trafic dans certaines instances sur ASA.

Avant de commencer

Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, entrez la commande **changeto context** *name*.

Procédure

Étape 1 Entrez le mode de configuration d'interface :

interface *id*

Exemple :

```
ciscoasa(config)# interface gigabithethernet 0/0
```

Étape 2 Attribuez une adresse MAC privée à cette interface :

mac-address *mac_address* [**standby** *mac_address*]

Exemple :

```
ciscoasa(config-if)# mac-address 000C.F142.4CDE
```

La *mac_address* est au format H.H.H., où H est une valeur hexadécimale de 16 bits. Par exemple, l'adresse MAC 00-0C-F1-42-4C-DE est saisie comme suit : 000C.F142.4CDE. L'adresse MAC ne doit pas avoir le bit de multidiffusion activé; autrement dit, le deuxième chiffre hexadécimal à partir de la gauche ne peut pas être un nombre impair.

Les deux premiers octets d'une adresse MAC manuelle ne peuvent pas être A2 si vous souhaitez également utiliser des adresses MAC générées automatiquement.

Pour une utilisation avec le basculement, définissez l'adresse MAC en veille (**standby**). Si l'unité active bascule et que l'unité en veille devient active, la nouvelle unité active commence à utiliser les adresses MAC actives pour minimiser les perturbations du réseau, tandis que l'ancienne unité active utilise l'adresse en veille.

Attribuer automatiquement des adresses MAC

Cette section décrit comment configurer la génération automatique des adresses MAC. Pour le mode de contexte multiple, cette fonctionnalité attribue des adresses MAC uniques à tous les types d'interfaces qui sont affectés à un contexte. Pour le mode de contexte unique, cette fonctionnalité attribue des adresses MAC uniques aux sous-interfaces VLAN.

Avant de commencer

- Lorsque vous configurez une commande **nameif** pour l'interface, la nouvelle adresse MAC est générée immédiatement. Si vous activez cette fonctionnalité après avoir configuré les interfaces, les adresses MAC sont générées pour toutes les interfaces immédiatement après leur activation. Si vous désactivez cette fonctionnalité, l'adresse MAC par défaut de chaque interface revient à l'adresse MAC. Par exemple, les sous-interfaces de GigabitEthernet 0/1 utilisent l'adresse MAC de GigabitEthernet 0/1.
- Dans les rares cas où l'adresse MAC générée entre en conflit avec une autre adresse MAC privée de votre réseau, vous pouvez définir manuellement l'adresse MAC pour l'interface.
- Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Pour passer du contexte à l'espace d'exécution du système, saisissez la commande **changeto system**.

Procédure

Attribuez automatiquement des adresses MAC privées à chaque interface :

mac-address auto [**prefix** *prefix*]

Si vous n'écrivez pas de préfixe, l'ASA génère automatiquement ce dernier en fonction des deux derniers octets de l'adresse MAC de l'interface.

Si vous saisissez manuellement un préfixe, le *préfixe* est une valeur décimale comprise entre 0 et 65 535. Ce préfixe est converti en nombre hexadécimal à quatre chiffres et utilisé dans l'adresse MAC.

Exemple :

```
ciscoasa(config)# mac-address auto prefix 19
```

Configurer , la et le TCP MSS

Avant de commencer

- Dans le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du contexte. Pour passer du système à une configuration de contexte, entrez la commande **changeto context** *name*.
- Pour augmenter la MTU au-dessus de 1500, activez les trames étendues selon Activez la prise en charge des bâtis grand format (ASA virtuel et ISA 3000).

Procédure

Étape 1 Définissez la MTU. Le minimum et le maximum dépendent de votre plateforme.

mtu *interface_name bytes*

Exemple :

```
ciscoasa(config-if)# mtu inside ?

configure mode commands/options:
  <64-9198>  MTU bytes
ciscoasa(config)# mtu inside 9000
```

Par défaut, la MTU est de 1500 octets.

Remarque
Lorsque vous définissez le MTU pour une interface ou de canal de port, l'ASA applique le paramètre à toutes les interfaces membres.

Pour certains modèles qui prennent en charge les bâtis grand format, si vous entrez une valeur supérieure à 1500 pour une interface, vous devez activer la prise en charge des bâtis grand format. Consultez Activez la prise en charge des bâtis grand format (ASA virtuel et ISA 3000).

Étape 2 Configurez la taille de segment TCP maximale en octets, entre 48 et tout nombre maximal :

sysopt connection tcpmss [**minimum**] *bytes*

Exemple :

```
ciscoasa(config)# sysopt connection tcpmss 8500
ciscoasa(config)# sysopt connection tcpmss minimum 1290
```

Par défaut, la MTU est de 1380 octets. Vous pouvez désactiver cette fonctionnalité en mettant les octets à **0**.

Pour le mot clé **minimum**, définit la taille de segment maximale pour qu'elle ne soit pas inférieure à *octets* (entre 48 et 65 535). La fonctionnalité minimale est désactivée par défaut (définie sur 0).

Étape 3 Configurez le nombre maximal de segments TCP non traités.

sysopt connection tcp-max-unprocessed-seg *segments non traités*

Exemple :

```
ciscoasa(config)# sysopt connection tcp-max-unprocessed-seg 7
```

La valeur par défaut est 6. La valeur doit être comprise entre 6 et 24.

Exemples

Dans l’exemple suivant, les trames étendues sont activées, la MTU est augmentée sur toutes les interfaces et TCP MSS est désactivé pour le trafic en dehors de VPN (en définissant TCP MSS sur 0, ce qui signifie qu’il n’y a pas de limite) :

```
mtu inside 9198
mtu outside 9198
sysopt connection tcpmss 0
```

Dans l'exemple suivant, les trames étendues sont activées, la MTU est augmentée sur toutes les interfaces et TCP MSS est modifié pour le trafic VPN à 9078 (la MTU moins 120) :

```
mtu inside 9198
mtu outside 9198
sysopt connection tcpmss 9078
```

Autoriser la communication de niveau de sécurité identique

Par défaut, les interfaces de même niveau de sécurité ne peuvent pas communiquer entre elles, et les paquets ne peuvent pas entrer ni sortir de la même interface. Cette section décrit comment activer la communication inter-interfaces lorsque les interfaces se trouvent sur le même niveau de sécurité et comment activer la communication intra-interface.

Procédure

Étape 1 Activez les interfaces sur le même niveau de sécurité afin qu'elles puissent communiquer entre elles :

same-security-traffic permit inter-interface

Étape 2 Activez la communication entre les hôtes connectés à la même interface :

same-security-traffic permit intra-interface

Historique de la configuration avancée de l'interface

Tableau 1 : Historique de la configuration avancée de l'interface

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
La MTU maximale est maintenant de 9 198 octets.	9.1(6), 9.2(1)	La MTU maximale que l'ASA peut utiliser est de 9 198 octets (vérifiez la limite exacte de votre modèle à l'aide de l'interface de ligne de commande). Cette valeur n'inclut pas l'en-tête de couche 2. L'ASA vous a permis de définir une MTU maximale de 65 535 octets, ce qui était inexact et pourrait causer des problèmes. Si votre MTU a été définie à une valeur supérieure à 9 198, la MTU est automatiquement réduite lors de la mise à niveau. Dans certains cas, cette modification de la MTU peut entraîner une non-concordance de la MTU. Assurez-vous de configurer tout équipement de connexion pour utiliser la nouvelle valeur MTU. Nous avons modifié la commande suivante : **mtu**

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Augmentation de la taille de la MTU pour l'ASA sur le Châssis Firepower 4100/9300	9.6(2)	Vous pouvez définir la MTU maximale à 9 184 octets sur les périphériques Firepower 4100 et 9300; auparavant, le maximum était de 9 000 octets. Cette MTU est prise en charge par FXOS 2.0.1.68 et les versions ultérieures. Nous avons modifié la commande suivante : **mtu**
Génération d'adresses MAC uniques en mode de contexte unique	9.8(3), 9.8(4), 9.9(2)	Vous pouvez maintenant activer la génération d'adresses MAC uniques pour les sous-interfaces VLAN en mode de contexte unique. Normalement, les sous-interfaces partagent la même adresse MAC avec l'interface principale. Comme les adresses Link-Local IPv6 sont générées en fonction de l'adresse MAC, cette fonctionnalité permet d'utiliser des adresses Link-Local IPv6 uniques. Commande nouvelle ou modifiée : **mac-address auto**
La négociation automatique de Secure Firewall 3100 peut être activée ou désactivée pour les interfaces de 1 Gigabit et les versions ultérieures.	9.17(1)	La négociation automatique de Secure Firewall 3100 peut être activée ou désactivée pour les interfaces de 1 Gigabit et les versions ultérieures. Pour les autres modèles de ports SFP, l'option **no speed nonegotiate** définit la vitesse à 1 000 Mbit/s; la nouvelle commande signifie que vous pouvez définir la négociation automatique et la vitesse indépendamment. Commandes nouvelles ou modifiées : **negotiate-auto**

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.