Interfaces en mode routage et en mode transparent

Ce chapitre comprend des tâches pour terminer la configuration de l'interface pour tous les modèles en mode de pare-feu routé ou transparent.

Remarque Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Saisissez la commande **changeto context** *name* pour remplacer le contexte que vous souhaitez configurer.

À propos des interfaces en mode routage et en mode transparent

L'ASA prend en charge deux types d'interfaces : routées et pontées.

Chaque interface routée de couche 3 nécessite une adresse IP sur un sous-réseau unique.

Les interfaces pontées appartiennent à un groupe de ponts et toutes les interfaces se trouvent sur le même réseau. Le groupe de ponts est représenté par une interface virtuelle de pont (BVI) qui a une adresse IP sur le réseau de ponts. Le mode routé prend en charge les interfaces routées et pontées, et vous pouvez effectuer le routage entre des interfaces routées et des BVI. Le mode de pare-feu transparent ne prend en charge que les interfaces de groupe de ponts et BVI.

Niveaux de sécurité

Chaque interface doit avoir un niveau de sécurité de 0 (le plus bas) à 100 (le plus élevé), y compris les interfaces membres d'un groupe de ponts. Par exemple, vous devez affecter votre réseau le plus sécurisé, comme le réseau d'hôte interne, au niveau 100. Le réseau externe connecté à Internet peut quant à lui être attribué au

niveau 0. D'autres réseaux, tels que les DMZ, peuvent être entre les deux. Vous pouvez attribuer des interfaces au même niveau de sécurité.

L'attribution d'un niveau de sécurité à une BVI dépend du mode de pare-feu. En mode transparent, l'interface BVI n'a pas de niveau de sécurité, car elle ne participe pas au routage entre les interfaces. En mode routé, les interfaces BVI ont un niveau de sécurité si vous choisissez d'effectuer le routage entre les BVI et d'autres interfaces. Pour le mode routé, le niveau de sécurité d'une interface membre d'un groupe de ponts s'applique uniquement à la communication au sein du groupe de ponts. De même, le niveau de sécurité BVI s'applique uniquement à la communication inter-BVI/interface de couche 3.

Le niveau contrôle le comportement suivant :

- Accès au réseau : par défaut, il existe une autorisation implicite d'une interface de sécurité supérieure vers une interface de sécurité inférieure (sortante). Les hôtes de l'interface de sécurité supérieure peuvent accéder à n'importe quel hôte sur une interface de sécurité inférieure. Vous pouvez limiter l'accès en appliquant une ACL à l'interface.

  Si vous activez la communication pour des interfaces de même sécurité, il existe une autorisation implicite pour que les interfaces accèdent à d'autres interfaces sur le même niveau de sécurité ou un niveau de sécurité inférieur.

- Moteurs d'inspection : certains moteurs d'inspection d'applications dépendent du niveau de sécurité. Pour les interfaces de même sécurité, les moteurs d'inspection s'appliquent au trafic dans l'une ou l'autre direction.
  - Plateforme d'inspection NetBIOS : s'applique uniquement aux connexions sortantes.
  - Plateforme d'inspection SQL*Net : si une connexion de contrôle pour le port SQL*Net (anciennement OraServ) existe entre une paire d'hôtes, seule une connexion de données entrante est autorisée par l'ASA.

Double pile IP (IPv4 et IPv6)

L'ASA prend en charge les adresses IPv6 et IPv4 sur une interface. Assurez-vous de configurer une voie de routage par défaut pour IPv4 et IPv6.

Masque de sous-réseau 31 bits

Pour les interfaces routées, vous pouvez configurer une adresse IP sur un sous-réseau de 31 bits pour les connexions point à point. Le sous-réseau de 31 bits comprend seulement 2 adresses; normalement, la première et la dernière adresse du sous-réseau sont réservées pour le réseau et la diffusion, donc un sous-réseau à deux adresses n'est pas utilisable. Toutefois, si vous avez une connexion point à point et n'avez pas besoin d'adresses de réseau ou de diffusion, un sous-réseau de 31 bits est un moyen utile de conserver les adresses dans IPv4. Par exemple, le lien de basculement entre 2 ASA ne nécessite que 2 adresses; les paquets transmis par une extrémité de la liaison sont toujours reçus par l'autre extrémité, et la diffusion n'est pas nécessaire. Vous pouvez également avoir une station de gestion directement connectée exécutant SNMP ou Syslog.

Sous-réseau 31 bits et mise en grappe

Vous pouvez utiliser un masque de sous-réseau de 31 bits de grappe en mode de mise en grappe étendue, à l'exclusion de l'interface de gestion et de la liaison de commande de grappe.

Vous ne pouvez pas utiliser un masque de sous-réseau de 31 bits en mode de mise en grappe individuelle sur une interface.

Sous-réseau 31 bits et basculement

Pour le basculement, lorsque vous utilisez un sous-réseau de 31 bits pour l'adresse IP d'interface ASA, vous ne pouvez pas configurer d'adresse IP de secours pour l'interface, car il n'y a pas assez d'adresses. Normalement, une interface de basculement doit avoir une adresse IP de secours pour que l'unité active puisse effectuer des tests d'interface pour s'assurer de l'intégrité de l'interface de secours. Sans adresse IP de secours, ASA ne peut effectuer aucun test de réseau. seul l'état du lien peut être suivi.

Pour le basculement et le lien à état séparé facultatif, qui sont des connexions point à point, vous pouvez également utiliser un sous-réseau de 31 bits.

Gestion et sous-réseau 31 bits

Si vous avez une station de gestion directement connectée, vous pouvez utiliser une connexion point à point pour SSH ou HTTP sur ASA, ou pour SNMP ou Syslog sur le poste de gestion.

Fonctionnalités 31 bits non prises en charge

Les fonctionnalités suivantes ne prennent pas en charge le sous-réseau de 31 bits :

- Interfaces BVI pour les groupes de ponts : le groupe de ponts nécessite au moins 3 adresses d'hôte : les BVI et deux hôtes connectés à deux interfaces membres du groupe de ponts. vous devez utiliser un sous-réseau /29 ou moins.
- Routage multidiffusion

Directives et limites pour les interfaces en mode routé et en mode transparent

Mode contextuel

- En mode de contexte multiple, vous pouvez seulement configurer les interfaces de contexte que vous avez déjà affectées au contexte dans la configuration système en fonction de Configurer plusieurs contextes.
- PPPoE n'est pas pris en charge en mode de contexte multiple.
- Pour le mode à contextes multiples en mode transparent, chaque contexte doit utiliser des interfaces différentes; vous ne pouvez pas partager une interface entre contextes.
- Pour le mode à contexte multiple en mode transparent, chaque contexte utilise généralement un sous-réseau différent. Vous pouvez utiliser des sous-réseaux qui se chevauchent, mais la topologie de votre réseau nécessite une configuration de routeur et de NAT pour que cela soit possible du point de vue du routage.
- Les options de délégation de préfixe et de DHCPv6 ne sont pas prises en charge avec le mode de contexte multiple.
- En mode de pare-feu routé, les interfaces de groupes de ponts ne sont pas prises en charge dans le mode de contexte multiple.

Failover (basculement), mise en grappe

- Ne configurez pas les liens de basculement selon les procédures de ce chapitre. Consultez le chapitre Failover (basculement) pour plus de renseignements.
- Pour les interfaces de grappe, consultez le chapitre sur la mise en grappe pour connaître les exigences.
- Lorsque vous utilisez Failover (basculement), vous devez définir l'adresse IP et l'adresse de secours pour les interfaces de données manuellement. DHCP et PPPoE ne sont pas pris en charge.

IPv6

- IPv6 est pris en charge sur toutes les interfaces.
- Vous ne pouvez que configurer les adresses IPv6 manuellement en mode transparent.
- L'ASA ne prend pas en charge les adresses anycast IPv6.
- Les options de délégation de préfixe et de DHCPv6 ne sont pas prises en charge avec le mode à contexte multiple, le mode transparent, la mise en grappe ou Failover (basculement).

Directives sur les modèles

- Pour l’ASAv50, les groupes de ponts ne sont pas pris en charge en mode transparent ou routé.
- Pour les périphériques Firepower 2100, les groupes de ponts ne sont pas pris en charge en mode routé.

Directives relatives au mode transparent et au groupe de ponts

- Vous pouvez créer jusqu’à 250 groupes de ponts, avec interfaces par groupe de ponts.
- Chaque réseau connecté directement doit se trouver sur le même sous-réseau.
- L'ASA ne prend pas en charge le trafic sur les réseaux secondaires; seul le trafic sur le même réseau que l’adresse IP BVI est pris en charge.
- Une adresse IP pour les BVI est requise pour chaque groupe de ponts pour le trafic de gestion vers le périphérique et en provenance du périphérique, ainsi que pour le trafic de données qui doit passer par ASA. Pour le trafic IPv4, spécifiez une adresse IPv4. Pour le trafic IPv6, spécifiez une adresse IPv6.
- Vous ne pouvez configurer les adresses IPv6 que manuellement.
- L’adresse IP BVI doit se trouver sur le même sous-réseau que le réseau connecté. Vous ne pouvez pas définir le sous-réseau comme sous-réseau d’hôte (255.255.255.255).
- Les interfaces de gestion ne sont pas prises en charge en tant que membres de groupes de ponts.
- Pour l’ASAv50 sur VMware avec des interfaces ixgbevf pontées, le mode transparent n’est pas pris en charge et les groupes de ponts ne sont pas pris en charge en mode routé.
- Pour Série Firepower 2100, les groupes de ponts ne sont pas pris en charge en mode routé.
- Dans le cas du Firepower 1010, il n'est pas possible de mélanger des interfaces VLAN logiques et des interfaces de pare-feu physiques au sein du même groupe de ponts.
- En mode transparent, vous devez utiliser au moins un groupe de ponts; les interfaces de données doivent appartenir à un groupe de ponts.

- En mode transparent, ne spécifiez pas l'adresse IP des BVI comme passerelle par défaut pour les périphériques connectés; Les périphériques doivent spécifier le routeur de l'autre côté de la ASA comme passerelle par défaut.
- En mode transparent, la voie de routage *par défaut*, qui est requise pour fournir un chemin de retour au trafic de gestion, n'est appliquée qu'au trafic de gestion provenant d'un réseau de groupe de ponts. En effet, la voie de routage par défaut spécifie une interface dans le groupe de ponts ainsi que l'adresse IP du routeur sur le réseau du groupe de ponts, et vous ne pouvez définir qu'une seule voie de routage par défaut. Si votre trafic de gestion provient de plus d'un réseau de groupes de ponts, vous devez spécifier une voie de routage statique régulière qui identifie le réseau à partir duquel vous attendez le trafic de gestion.
- Le protocole PPPoE n'est pas pris en charge sur l'interface Management (gestion).
- En mode routé, pour le routage entre les groupes de ponts et les autres interfaces routées, vous devez nommer les BVI.
- En mode routé, les interfaces EtherChannel définies par ASA et VNI ne sont pas prises en charge en tant que membres de groupes de ponts. Les EtherChannels sur Firepower 4100/9300 peuvent être des membres de groupes de ponts.
- Les paquets écho de la détection de transfert bidirectionnel (BFD) ne sont pas autorisés par le biais de ASA lors de l'utilisation de membres de groupe de ponts. S'il y a deux voisins de chaque côté de l'ASA exécutant BFD, alors l'ASA abandonnera les paquets écho BFD, car ils ont la même adresse IP de source et de destination et semblent faire partie d'une attaque LAND.

Niveau de sécurité par défaut

Le niveau de sécurité par défaut est 0. Si vous nommez une interface « intérieur » et que vous ne définissez pas explicitement le niveau de sécurité, l'ASA le définit à 100.

Remarque Si vous modifiez le niveau de sécurité d'une interface et que vous ne souhaitez pas attendre que les connexions existantes expirent avant d'utiliser les nouveaux renseignements sur la sécurité, vous pouvez effacer les connexions à l'aide de la commande **clear conn**.

Directives et exigences supplémentaires

- Le ASA ne prend en charge qu'un seul en-tête 802.1Q par paquet et ne prend pas en charge plusieurs en-têtes (appelé prise en charge Q-in-Q).
- Des problèmes d'interface, tels que de fréquents changements d'état haut/bas, peuvent empêcher la minuterie de connexion flottante de s'appliquer correctement aux connexions passant par l'interface. Si vous avez des problèmes avec l'état d'une interface, pensez à effacer toutes les connexions une fois que l'état est stabilisé afin de supprimer les connexions non valides.

Configurer les interfaces en mode routé

Pour configurer les interfaces en mode routé, procédez comme suit.

Configurer les paramètres généraux de l'interface en mode routé

Cette procédure décrit comment définir le nom, le niveau de sécurité, l'adresse IPv4 et d'autres options.

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
```

L'ID d'interface peut être :

- **canal de port**
- *physical*– Par exemple, **ethernet**, **gigabitethernet**, **10 gigabitethernet**, **gestion**. Reportez-vous au guide d'installation du matériel correspondant à votre modèle pour connaître les noms d'interface.
- *physical***.***subinterface*– Par exemple, **gigabitEthernet0/0.100**.
- **vni**
- **vlan**
- **loop back** (bouclage)
- *mapped_name*—Pour le mode de contexte multiple.

Remarque
Pour le Firepower 1010, vous ne pouvez pas configurer de ports de commutation en tant qu'interfaces en mode routé.

Étape 2 Nommez l'interface :

nameif *name*

Exemple :

```
ciscoasa(config-if)# nameif inside
```

Le *nom* est une chaîne de texte de 48 caractères maximum et n'est pas sensible à la casse. Vous pouvez modifier le nom en saisissant à nouveau cette commande avec une nouvelle valeur. Ne saisissez pas la forme **no** (non), car cette commande entraîne la suppression de toutes les commandes qui font référence à ce nom.

Étape 3 Définissez l'adresse IP à l'aide de l'une des méthodes suivantes.

Pour le basculement et la mise en grappe, ainsi que pour les interfaces de boucle avec retour, vous devez définir l'adresse IP manuellement; les protocoles DHCP et PPPoE ne sont pas pris en charge.

- Définissez l'adresse IP manuellement :

  ip address *ip_address* [*mask*] [**standby** *ip_address*]

  Exemple :

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
  ```

  L'argument *ip_address* en veille est utilisé pour le basculement. Si vous ne définissez pas l'adresse IP de veille, l'unité active ne peut pas surveiller l'interface de secours en utilisant des tests réseau; elle ne peut que suivre l'état du lien.

  Les arguments *ip_address* et *mask* définissent l'adresse IP de l'interface et le filtre d'adresse locale. Pour les connexions point à point, vous pouvez spécifier un filtre d'adresse locale de 31 bits (255.255.255.254). Dans ce cas, aucune adresse IP n'est réservée pour les adresses de réseau ou de diffusion. Vous ne pouvez pas définir l'adresse IP de secours dans ce cas.

  Exemple :

  ```
  ciscoasa(config-if)# ip address 10.1.1.0 255.255.255.254
  ```

- Obtenez une adresse IP à partir d'un serveur DHCP :

  ip address dhcp [**setroute**]

  Exemple :

  ```
  ciscoasa(config-if)# ip address dhcp
  ```

  Le mot clé **setroute** permet à l'ASA d'utiliser la route par défaut fournie par le serveur DHCP.

  Saisissez à nouveau cette commande pour réinitialiser le bail locatif DHCP et demander un nouveau bail locatif.

  Remarque
  Si vous n'activez pas l'interface à l'aide de la commande **no shutdown** avant de saisir la commande **ip address dhcp**, certaines demandes DHCP pourraient ne pas être envoyées.

- Obtenez une adresse IP à partir d'un serveur PPPoE :

  ip address pppoe [**setroute**]

  Exemple :

  ```
  ciscoasa(config-if)# ip address pppoe setroute
  ```

  Vous pouvez également activer PPPoE en saisissant manuellement l'adresse IP :

  ip address *ip_address mask* **pppoe**

  Exemple :

```
ciscoasa(config-if)# ip address 10.1.1.78 255.255.255.0 pppoe
```

L'option **setroute** définit les routes par défaut lorsque le client PPPoE n'a pas encore établi de connexion. Lorsque vous utilisez l'option **setroute**, vous ne pouvez pas avoir de route définie de manière statique dans la configuration.

Remarque
Si le protocole PPPoE est activé sur deux interfaces (comme une interface principale et une interface de secours) et que vous ne configurez pas la prise en charge du double FAI, l'ASA ne pourra envoyer le trafic que par la première interface pour acquérir une adresse IP.

Étape 4 Définissez le niveau de sécurité :

security-level *number*

Exemple :

```
ciscoasa(config-if)# security-level 50
```

Le paramètre *number* est un entier compris entre 0 (le plus bas) et 100 (le plus élevé).

Remarque
Pour les interfaces de boucle avec retour, vous ne définissez pas de niveau de sécurité, car l'interface n'est prise en charge que pour le trafic vers/depuis le périphérique.

Étape 5 (Facultatif) Définissez une interface en mode gestion uniquement afin qu'elle ne transmette pas de trafic :

management-only

Par défaut, les interfaces de gestion sont configurées en tant que gestion uniquement.

Remarque
Pour les interfaces de boucle avec retour, vous ne définissez pas le mode de gestion, car l'interface n'est prise en charge que pour le trafic vers/depuis le périphérique.

Exemples

L'exemple suivant configure les paramètres pour le VLAN 101 :

```
ciscoasa(config)# interface vlan 101
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
```

L'exemple suivant configure les paramètres en mode de contexte multiple pour la configuration de contexte. L'ID d'interface est un nom mappé.

```
ciscoasa/contextA(config)# interface int1
ciscoasa/contextA(config-if)# nameif outside
ciscoasa/contextA(config-if)# security-level 100
```

```
ciscoasa/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
```

Sujets connexes

Configuration de l'adressage IPv6, à la page 16
Activer l'interface physique et configurer les paramètres Ethernet
Configurer le protocole PPPoE, à la page 9

Configurer le protocole PPPoE

Si l'interface est connectée à une liaison ADSL, à un modem câble ou à une autre connexion à votre FAI et que ce dernier utilise PPPoE pour vous fournir votre adresse IP, configurez les paramètres suivants.

Procédure

Étape 1 Définissez le nom du groupe de réseaux privés virtuels à accès commuté (Virtual Private Dialup Network ou VPDN) de votre choix pour représenter cette connexion :

vpdn group *group_name* **request dialout pppoe**

Exemple :

```
ciscoasa(config)# vpdn group pppoe-sbc request dialout pppoe
```

Étape 2 Si votre FAI requiert une authentification, sélectionnez un protocole d'authentification :

vpdn group *group_name* **ppp authentication** {**chap** | **mschap** | **pap**}

Exemple :

```
ciscoasa(config)# vpdn group pppoe-sbc ppp authentication chap
```

Saisissez le mot clé approprié pour le type d'authentification utilisé par votre FAI.

Lors de l'utilisation de CHAP ou de MS-CHAP, le nom d'utilisateur peut être appelé nom du système distant, tandis que le mot de passe peut être appelé secret CHAP.

Étape 3 Associez le nom d'utilisateur attribué par votre FAI au groupe VPDN :

vpdn group *group_name* **localname** *username*

Exemple :

```
ciscoasa(config)# vpdn group pppoe-sbc localname johncrichton
```

Étape 4 Créez une paire de nom d'utilisateur et de mot de passe pour la connexion PPPoE :

vpdn username *username* **password** *password* [**store-local**]

Exemple :

```
ciscoasa(config)# vpdn username johncrichton password moya
```

L'option **store-local** stocke le nom d'utilisateur et le mot de passe dans un emplacement spécial de la NVRAM sur l'ASA. Si un Auto Update Server envoie une commande **clear config** à l'ASA et que la connexion est interrompue, l'ASA peut lire le nom d'utilisateur et le mot de passe de NVRAM et s'authentifier de nouveau auprès du concentrateur d'accès.

Configurer les interfaces de groupe de ponts

Un groupe de ponts est un groupe d'interfaces que ASA relie par des ponts au lieu de routes. Les groupes de ponts sont pris en charge à la fois en mode transparent et en mode pare-feu routé. Pour en savoir plus sur les groupes de ponts, consultez À propos des groupes de ponts.

Pour configurer des groupes de ponts et les interfaces associées, procédez comme suit.

Configurer la BVI (Bridge Virtual Interface)

Chaque groupe de ponts nécessite un BVI pour lequel vous configurez une adresse IP. L'ASA utilise cette adresse IP comme adresse source pour les paquets provenant du groupe de ponts. L'adresse IP BVI doit se trouver sur le même sous-réseau que le réseau connecté. Pour le trafic IPv4, l'adresse IP BVI est requise pour laisser passer le trafic. Pour le trafic IPv6, vous devez, au minimum, configurer les adresses de lien locales pour laisser passer le trafic, mais une adresse de gestion globale est recommandée pour les fonctionnalités complètes, y compris la gestion à distance et d'autres opérations de gestion.

Pour le mode routé, si vous fournissez un nom pour les BVI, alors les BVI participent au routage. Sans nom, le groupe de ponts reste isolé comme en mode transparent de pare-feu.

Certains modèles incluent un groupe de ponts et une BVI dans la configuration par défaut. Vous pouvez créer des groupes de ponts et des BVI supplémentaires et réaffecter des interfaces membres entre les groupes.

Remarque Pour une interface de gestion distincte en mode transparent (pour les modèles pris en charge), un groupe de ponts non configurables (ID 301) est automatiquement ajouté à votre configuration. Ce groupe de ponts n'est pas inclus dans la limite de groupes de ponts.

Procédure

Étape 1 Créez une BVI :

interface bvi *bridge_group_number*

Exemple :

```
ciscoasa(config)# interface bvi 2
```

Le *bridge_group_number* est un nombre entier compris entre 1 et 250. Vous attribuerez ultérieurement des interfaces physiques à ce numéro de groupe de ponts.

Étape 2 (Mode transparent) Spécifiez l'adresse IP de la BVI :

ip address *ip_address* [*mask*] [**standby** *ip_address*]

Exemple :

```
ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
```

N'affectez pas d'adresse hôte (/32 ou 255.255.255.255) au BVI. De plus, n'utilisez pas d'autres sous-réseaux contenant moins de 3 adresses d'hôte (une pour le routeur en amont, le routeur en aval et la BVI), comme un sous-réseau /30 (255.255.255.252). L'ASA abandonne tous les paquets ARP en provenance ou à destination de la première et de la dernière adresse d'un sous-réseau. Par conséquent, si vous utilisez un sous-réseau /30 et que vous affectez une adresse réservée de ce sous-réseau au routeur en amont, l'ASA abandonne la demande ARP du routeur en aval au routeur en amont.

Le mot clé **standby** et l'adresse sont utilisés pour le basculement.

Étape 3 (Mode routé) Définissez l'adresse IP à l'aide de l'une des méthodes suivantes.

Pour le basculement et la mise en grappe, vous devez définir l'adresse IP manuellement; le protocole DHCP n'est pas pris en charge.

- Définissez l'adresse IP manuellement :

  ip address *ip_address* [*mask*] [**standby** *ip_address*]

  Exemple :

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
  ```

  L'argument *ip_address* en veille est utilisé pour le basculement.

  Les arguments *ip_address* et *mask* définissent l'adresse IP de l'interface et le filtre d'adresse locale.

- Obtenez une adresse IP à partir d'un serveur DHCP :

  ip address dhcp [**setroute**]

  Exemple :

  ```
  ciscoasa(config-if)# ip address dhcp
  ```

  Le mot clé **setroute** permet à l'ASA d'utiliser la route par défaut fournie par le serveur DHCP.

  Saisissez à nouveau cette commande pour réinitialiser le bail locatif DHCP et demander un nouveau bail locatif.

  Si vous n'activez pas l'interface à l'aide de la commande no shutdown avant de saisir la commande **ip address dhcp**, certaines demandes DHCP pourraient ne pas être envoyées.

Étape 4 (Mode routé) Nommez l'interface :

nameif *name*

Exemple :

```
ciscoasa(config-if)# nameif inside
```

Vous devez nommer le BVI si vous souhaitez acheminer le trafic extérieur aux membres du groupe de pont, par exemple vers l'interface externe ou vers les membres d'autres groupes de pont. Le *nom* est une chaîne de texte de 48 caractères maximum et n'est pas sensible à la casse. Vous pouvez modifier le nom en saisissant à nouveau cette commande avec une nouvelle valeur. Ne saisissez pas la forme **no** (non), car cette commande entraîne la suppression de toutes les commandes qui font référence à ce nom.

Étape 5 (Mode routé) Définissez le niveau de sécurité :

security-level *number*

Exemple :

```
ciscoasa(config-if)# security-level 50
```

Le paramètre *number* est un entier compris entre 0 (le plus bas) et 100 (le plus élevé).

Exemple

L'exemple suivant définit l'adresse BVI 2 et l'adresse de veille :

```
ciscoasa(config)# interface bvi 2
ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
```

Configurer les paramètres généraux de l'interface de membre du groupe de ponts

Cette procédure décrit comment définir le nom, le niveau de sécurité et le groupe de ponts pour chaque interface membre du groupe de ponts.

Avant de commencer

- Un même groupe de ponts peut inclure différents types d'interfaces : des interfaces physiques, des sous-interfaces VLAN, des interfaces VNI et des EtherChannels. Le protocole PPPoE n'est pas pris en charge sur l'interface de gestion. En mode routé, les EtherChannels et les VNI ne sont pas pris en charge.
- 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 le mode transparent, n'utilisez pas cette procédure pour les interfaces de gestion; consultez Configurer une interface de gestion pour le mode transparent, à la page 14 pour configurer l'interface de gestion.

Procédure

Étape 1 Entrez le mode de configuration d'interface :

interface *id*

Exemple :

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

L'ID d'interface peut être :

- **canal de port**
- *physical*– Par exemple, **ethernet**, **gigabitethernet**, **10 gigabitethernet**. Les interfaces de gestion ne sont pas prises en charge. Reportez-vous au guide d'installation du matériel correspondant à votre modèle pour connaître les noms d'interface.
- *Physical_or_port-canal***.***subinterface*– Par exemple, **gigabitethernet0/0.100** ou **port-channel1.100**.
- **vni**
- **vlan**
- *mapped_name*—Pour le mode de contexte multiple.

Remarque
Pour Firepower 1010, vous ne pouvez pas configurer de ports de commutation en tant que membres d'un groupe de ponts.

Vous ne pouvez pas mélanger des interfaces VLAN logiques et des interfaces de routeur physiques dans le même groupe de ponts.

Remarque
En mode routé, les interfaces **port-channel** et **vni** ne sont pas prises en charge en tant que membres de groupes de ponts.

Étape 2 Affectez l'interface à un groupe de ponts :

bridge-group *number*

Exemple :

```
ciscoasa(config-if)# bridge-group 1
```

Le *nombre* est un entier compris entre 1 et 250 et doit correspondre au numéro d'interface BVI. Vous pouvez attribuer jusqu'à 64 interfaces à un groupe de ponts. Vous ne pouvez pas attribuer la même interface à plusieurs groupes de ponts.

Étape 3 Nommez l'interface :

nameif *name*

Exemple :

```
ciscoasa(config-if)# nameif inside1
```

Le *nom* est une chaîne de texte de 48 caractères maximum et n'est pas sensible à la casse. Vous pouvez modifier le nom en saisissant à nouveau cette commande avec une nouvelle valeur. Ne saisissez pas la forme **no** (non), car cette commande entraîne la suppression de toutes les commandes qui font référence à ce nom.

Étape 4 Définissez le niveau de sécurité :

security-level *number*

Exemple :

```
ciscoasa(config-if)# security-level 50
```

Le paramètre *number* est un entier compris entre 0 (le plus bas) et 100 (le plus élevé).

Sujets connexes

Configurer , la et le TCP MSS

Configurer une interface de gestion pour le mode transparent

En mode de pare-feu transparent, toutes les interfaces doivent appartenir à un groupe de ponts. La seule exception est l'interface de gestion (l'interface physique, une sous-interface (si prise en charge pour votre modèle) ou une interface EtherChannel composée d'interfaces de gestion (si vous avez plusieurs interfaces de gestion)) que vous pouvez configurer en tant qu'interface de gestion distincte; pour le Châssis Firepower 4100/9300 , l'ID de l'interface de gestion dépend de l'interface de type gestion que vous avez attribuée au périphérique logique ASA. Vous ne pouvez pas utiliser d'autres types d'interfaces comme interfaces de gestion. Vous pouvez configurer une interface de gestion en mode unique ou par contexte. Pour obtenir plus de renseignements, consultez Interface de gestion pour le mode transparent.

L'interface de gestion traite uniquement le trafic entrant et sortant et ne peut pas transmettre de trafic de transit.

Avant de commencer

- N'attribuez pas cette interface à un groupe de ponts; un groupe de ponts non configurable (ID 301) est automatiquement ajouté à votre configuration. Ce groupe de ponts n'est pas inclus dans la limite de groupes de ponts.
- Pour le Châssis Firepower 4100/9300 , l'ID de l'interface de gestion dépend de l'interface de type gestion que vous avez attribuée au périphérique logique ASA.
- En mode de contexte multiple, vous ne pouvez partager aucune interface, y compris l'interface de gestion, entre les contextes. Vous devez vous connecter à une interface de données.
- 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, saisissez la commande **changeto context** *name*.

Procédure

Étape 1 Entrez le mode de configuration d'interface :

interface {{**port-channel** *number* | **management** *slot*/*port* | *mgmt-type_interface_id* }[**.** *subinterface*] | *mapped_name*}

Exemple :

```
ciscoasa(config)# interface management 0/0.1
```

L'argument **port-channel** *number* est l'ID de l'interface EtherChannel, tel que **port-channel 1**. L'interface EtherChannel ne doit avoir que des interfaces membres de gestion.

En mode de contexte multiple, saisissez le *mapped_name* s'il a été attribué à l'aide de la commande **allocate-interface**.

Pour le Châssis Firepower 4100/9300 , spécifiez l'ID d'interface pour l'interface de type de gestion (individuelle ou EtherChannel) que vous avez attribuée au périphérique logique ASA.

Étape 2 Nommez l'interface :

nameif *name*

Exemple :

```
ciscoasa(config-if)# nameif management
```

Le *nom* est une chaîne de texte de 48 caractères maximum et n'est pas sensible à la casse. Vous pouvez modifier le nom en saisissant à nouveau cette commande avec une nouvelle valeur. Ne saisissez pas la forme **no** (non), car cette commande entraîne la suppression de toutes les commandes qui font référence à ce nom.

Étape 3 Définissez l'adresse IP à l'aide de l'une des méthodes suivantes.

- Définissez l'adresse IP manuellement :

  Pour une utilisation avec le basculement, vous devez définir manuellement l'adresse IP et l'adresse en veille; le protocole DHCP n'est pas pris en charge.

  Les arguments *ip_address* et *mask* définissent l'adresse IP de l'interface et le filtre d'adresse locale.

  L'argument *ip_address* en veille est utilisé pour le basculement.

  ip address *ip_address* [*mask*] [**standby** *ip_address*]

  Exemple :

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
  ```

- Obtenez une adresse IP à partir d'un serveur DHCP :

  ip address dhcp [**setroute**]

  Exemple :

```
ciscoasa(config-if)# ip address dhcp
```

Le mot clé **setroute** permet à l'ASA d'utiliser la route par défaut fournie par le serveur DHCP.

Saisissez à nouveau cette commande pour réinitialiser le bail locatif DHCP et demander un nouveau bail locatif.

Si vous n'activez pas l'interface à l'aide de la commande no shutdown avant de saisir la commande **ip address dhcp**, certaines demandes DHCP pourraient ne pas être envoyées.

Étape 4 Définissez le niveau de sécurité :

security-level *number*

Exemple :

```
ciscoasa(config-if)# security-level 100
```

Le paramètre *number* est un entier compris entre 0 (le plus bas) et 100 (le plus élevé).

Configuration de l'adressage IPv6

Cette section décrit comment configurer l'adressage IPv6.

À propos d'IPv6

Cette section comprend des informations sur IPv6.

Adresse IPv6

Vous pouvez configurer deux types d'adresses de monodiffusion pour IPv6 :

- Adresse globale (global) : l'adresse globale est une adresse publique que vous pouvez utiliser sur le réseau public. Pour un groupe de ponts, cette adresse doit être configurée pour les BVI, et non par interface membre. Vous pouvez également configurer une adresse IPv6 globale pour l'interface de gestion en mode transparent.
- Adresse locale du lien (link-local) : l'adresse locale du lien est une adresse privée que vous ne pouvez utiliser que sur le réseau directement connecté. Les routeurs ne transfèrent pas les paquets en utilisant des adresses locales du lien; ils sont uniquement destinés à la communication sur un segment de réseau physique donné. Ils peuvent être utilisés pour la configuration des adresses ou pour les fonctions de découverte du voisin telles que la résolution d'adresses. Dans un groupe de ponts, seules les interfaces membres ont des adresses de lien locales; les BVI n'ont pas d'adresse locale de lien.

Au minimum, vous devez configurer une adresse locale de lien pour que IPv6 fonctionne. Si vous configurez une adresse globale, une adresse locale de lien est automatiquement configurée sur l'interface, vous n'avez donc pas besoin de configurer spécifiquement une adresse locale de lien. Pour les interfaces membres des groupes de ponts, lorsque vous configurez l'adresse globale sur les BVI, ASA génère automatiquement des adresses link-local pour les interfaces membres. Si vous ne configurez pas d'adresse globale, vous devez configurer l'adresse locale de lien. La configuration peut s'effectuer automatiquement ou manuellement.

Remarque Si vous souhaitez configurer uniquement les adresses link-local, consultez la commande **ipv6 Enable** (pour la configuration automatique) ou **ipv6 address link-local** (pour la configuration manuelle) dans la référence de commandes.

ID d'interface EUI-64 modifiées

RFC 3513 : IPv6 (Internet Protocol Version 6) exige que la partie identifiant d'interface de toutes les adresses IPv6 de monodiffusion, à l'exception de celles qui commencent par la valeur binaire 000, ait une longueur de 64 bits et soit bâtie au format EUI-64 modifié. L'ASA peut appliquer cette exigence pour les hôtes associés au lien local.

Lorsque cette fonctionnalité est activée sur une interface, les adresses source des paquets IPv6 reçus sur cette interface sont comparées aux adresses MAC sources pour s'assurer que les identifiants d'interface utilisent le format EUI-64 modifié. Si les paquets IPv6 n'utilisent pas le format EUI-64 modifié comme identifiant d'interface, les paquets sont abandonnés et le message de journal système suivant est généré :

```
325003: EUI-64 source address check failed.
```

La vérification du format de l'adresse n'est effectuée que lors de la création d'un flux. Les paquets d'un flux existant ne sont pas vérifiés. De plus, la vérification de l'adresse ne peut être effectuée que pour les hôtes du lien local.

Configurer le client de délégation de préfixe IPv6

Le ASA peut servir de client de délégation de préfixe DHPCv6 de sorte que l'interface client, par exemple l'interface externe connectée à un modem câble, puisse recevoir un ou plusieurs préfixes IPv6 que le ASA peut ensuite utiliser en sous-réseau et attribuer à ses interfaces internes.

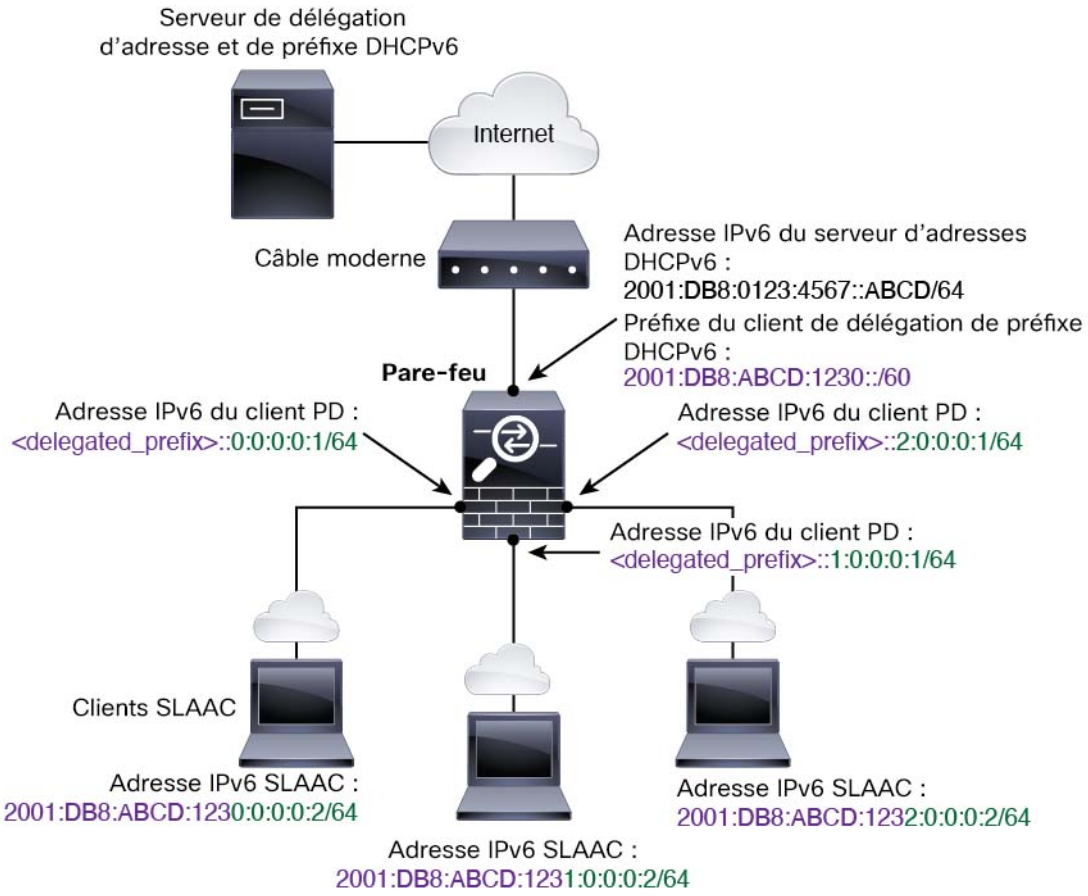
À propos de la délégation de préfixe IPv6

Le ASA peut servir de client de délégation de préfixe DHPCv6 de sorte que l'interface client, par exemple l'interface externe connectée à un modem câble, puisse recevoir un ou plusieurs préfixes IPv6 que le ASA peut ensuite utiliser en sous-réseau et attribuer à ses interfaces internes. Les hôtes connectés aux interfaces internes peuvent ensuite utiliser la configuration automatique sans état (SLAAC) pour obtenir des adresses IPv6 globales. Notez que les interfaces ASA internes n'agissent pas à leur tour comme des serveurs de délégation de préfixe; Le ASA ne peut fournir des adresses IP globales qu'aux clients SLAAC. Par exemple, si un routeur est connecté à l'ASA, il peut agir en tant que client SLAAC pour obtenir son adresse IP. Mais si vous souhaitez utiliser un sous-réseau du préfixe délégué pour les réseaux derrière le routeur, vous devez configurer manuellement ces adresses sur les interfaces internes du routeur.

L'ASA comprend un serveur DHCPv6 léger, de sorte que l'ASA peut fournir des informations telles que le serveur DNS et le nom de domaine aux clients SLAAC lorsqu'ils envoient des paquets de demande d'information (IR) à l'ASA. L'ASA accepte uniquement les paquets IR et n'affecte pas d'adresse aux clients. Vous configurerez le client pour générer sa propre adresse IPv6 en activant la configuration automatique IPv6 sur le client. L'activation de la configuration automatique sans état sur un client configure les adresses IPv6 en fonction des préfixes reçus dans les messages de publicité de routeur; en d'autres termes, en fonction du préfixe que ASA a reçu à l'aide de la délégation de préfixe.

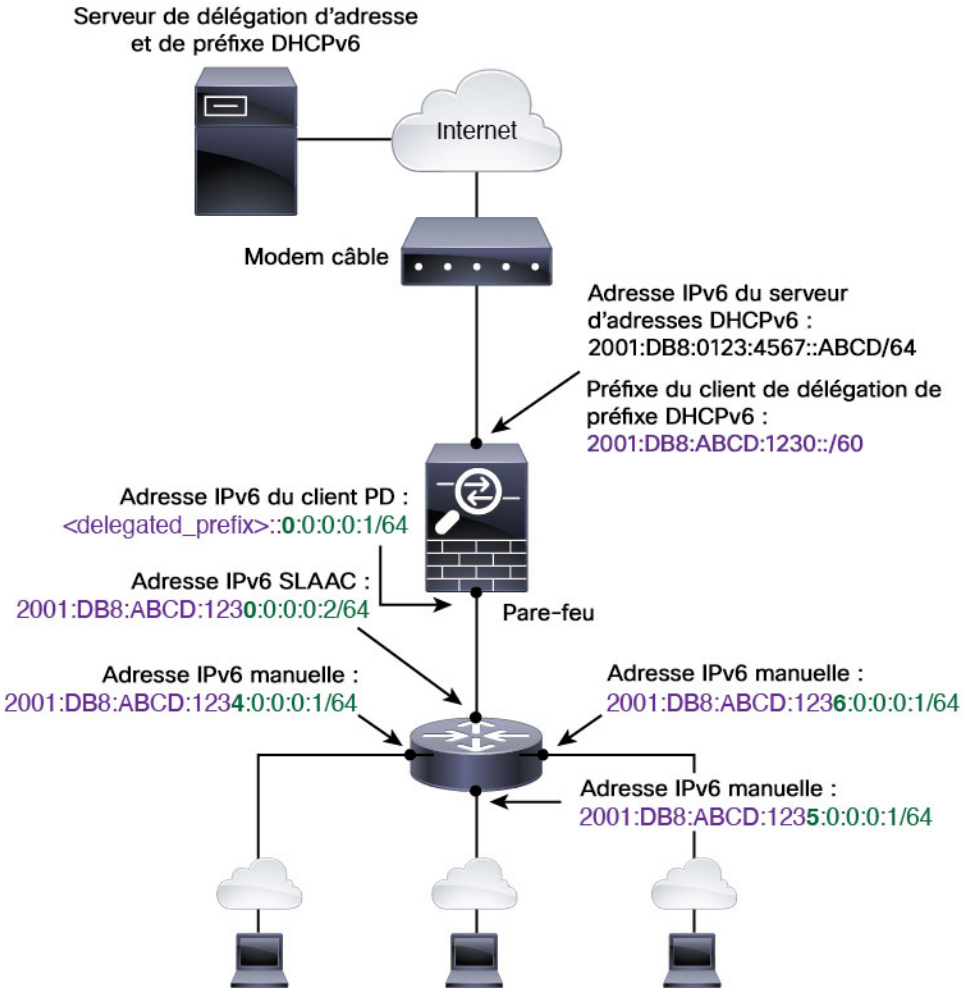
Exemple de délégation de préfixe IPv6 /de sous-réseau 64

L'exemple suivant montre que ASA reçoit une adresse IP sur l'interface externe en utilisant l'adresse DHCPv6. Il obtient également un préfixe délégué à l'aide du client de délégation de préfixe DHCPv6. Le ASA subdivise le préfixe délégué en réseaux /64 et attribue des adresses IPv6 globales à ses interfaces internes de manière dynamique en utilisant le préfixe délégué plus un sous-réseau configuré manuellement (::0, ::1 ou ::2) et une adresse IPv6 (0:0:0:1) par interface. Les clients SLAAC connectés à ces interfaces internes obtiennent des adresses IPv6 sur chaque sous-réseau /64.



Exemple de délégation de préfixe IPv6 /de sous-réseau 62

L'exemple suivant montre la sous-réseaux ASA du préfixe en 4 sous-réseaux /62 : 2001:DB8:ABCD:123**0**:/62, 2001:DB8:ABCD:123**4**:/62, 2001:DB8:ABCD:123**8**::/62 et 2001:DB8:ABCD:123 **C**::/62. ASA utilise l'un des 4 sous-réseaux /64 disponibles sur 2001:DB8:ABCD:1230::/62 pour son réseau interne (::0). Vous pouvez ensuite utiliser manuellement des sous-réseaux /62 supplémentaires pour les routeurs en aval. Le routeur illustré utilise 3 des 4 sous-réseaux /64 disponibles sur 2001:DB8:ABCD:1234::/62 pour ses interfaces internes (::4,::5 et::6). Dans ce cas, les interfaces de routeur internes ne peuvent pas obtenir dynamiquement le préfixe délégué. Vous devez donc afficher le préfixe délégué sur ASA, puis utiliser ce préfixe pour la configuration de votre routeur. Habituellement, les fournisseurs de services Internet délèguent le même préfixe à un client donné à l'expiration du bail, mais si ASA reçoit un nouveau préfixe, vous devrez modifier la configuration du routeur pour utiliser le nouveau préfixe. L'identifiant unique (DUID) de DHCP est persistant pendant les redémarrages.



Activer le client de délégation de préfixe IPv6

Activez le client de délégation de préfixe DHCPv6 sur une ou plusieurs interfaces. L'ASA obtient un ou plusieurs préfixes IPv6 qu'elle peut subdiviser en sous-réseaux et attribuer à des réseaux internes. En règle générale, l'interface sur laquelle vous activez la délégation de préfixe client obtient son adresse IP à l'aide de l'adresse client DHCPv6; Seules les autres interfaces ASA utilisent des adresses dérivées du préfixe délégué.

Avant de commencer

- Cette fonction n'est prise en charge qu'en mode pare-feu routé.
- Cette fonctionnalité n'est pas prise en charge en mode contexte multiple.
- Cette fonctionnalité n'est pas prise en charge lors de la mise en grappe.
- Vous ne pouvez pas configurer cette fonction sur une interface de gestion uniquement.
- Lorsque vous utilisez la délégation de préfixe, vous devez définir l'intervalle d'annonce du routeur de découverte des voisins IPv6 de l'ASA de manière à ce qu'il soit bien inférieur à la durée de vie souhaitée du préfixe attribué par le serveur DHCPv6, afin d'éviter toute interruption du trafic IPv6. Par exemple, si le serveur DHCPv6 définit la durée de vie préférée de délégation de préfixe à 300 secondes, vous devez

définir l'intervalle d'annonce de routeur de l'ASA à 150 secondes. Pour définir la durée de vie préférée, utilisez la commande **show ipv6 general-prefix**. Pour définir l'intervalle d'annonce de routeur de l'ASA, consultez Configurer la découverte des voisins IPv6, à la page 24; la valeur par défaut est de 200 secondes.

Procédure

Étape 1 Passez en mode de configuration d'interface pour l'interface connectée au réseau du serveur DHCPv6 :

interface *ID*

Exemple :

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

Étape 2 Activez le client DHCPv6 Prefix Delegation et nommez le(s) préfixe(s) obtenu(s) sur cette interface :

ipv6 dhcp client pd *name*

Exemple :

```
ciscoasa(config-if)# ipv6 dhcp client pd Outside-Prefix
```

Le *nom* peut comporter jusqu'à 200 caractères.

Étape 3 Fournissez un ou plusieurs conseils sur le préfixe délégué que vous souhaitez recevoir :

ipv6 dhcp client pd hint *ipv6_prefix/prefix_length*

Exemple :

```
ciscoasa(config-if)# ipv6 dhcp client pd hint 2001:DB8:ABCD:1230::/60
```

En règle générale, vous souhaitez demander une longueur de préfixe particulière, telle que ::/60, ou si vous avez déjà reçu un préfixe particulier et que vous souhaitez vous assurer de le recevoir à nouveau à l'expiration du bail, vous pouvez saisir le préfixe complet comme conseil. Si vous saisissez plusieurs conseils (préfixes ou longueurs différents), il appartient au serveur DHCP de choisir de respecter le conseil ou non.

Étape 4 Consultez Configuration d'une adresse globale IPv6, à la page 21 pour affecter un sous-réseau du préfixe comme adresse IP globale pour une interface ASA.

Étape 5 (Facultatif) Consultez Configurer le serveur sans état DHCPv6 pour fournir le nom de domaine et les paramètres de serveur aux clients SLAAC.

Étape 6 (Facultatif) Consultez Configurer les paramètres réseau IPv6 pour annoncer le ou les préfixes avec BGP.

Exemple

Dans l'exemple suivant, le client d'adresse DHCPv6 et le client de délégation de préfixe sont configurés sur GigabitEthernet 0/0, puis attribuent les adresses avec le préfixe sur les GigabitEthernet 0/1 et 0/2 :

```
interface gigabitethernet 0/0
  ipv6 address dhcp default
  ipv6 dhcp client pd Outside-Prefix
  ipv6 dhcp client pd hint ::/60
interface gigabitethernet 0/1
  ipv6 address Outside-Prefix ::1:0:0:0:1/64
interface gigabitethernet 0/2
  ipv6 address Outside-Prefix ::2:0:0:0:1/64
```

Configuration d'une adresse globale IPv6

Pour configurer une adresse IPv6 globale pour une interface en mode routé et pour le BVI en mode transparent ou routé, procédez comme suit.

Les options de délégation de préfixe et de DHCPv6 ne sont pas prises en charge avec le mode de contexte multiple.

Remarque La configuration de l'adresse globale configure automatiquement l'adresse de lien local, de sorte que vous n'avez pas besoin de la configurer séparément. Pour les groupes de ponts, la configuration de l'adresse globale sur les BVI configure automatiquement les adresses de lien locales sur toutes les interfaces membres.

Pour les sous-interfaces, nous vous recommandons de définir également l'adresse MAC manuellement, car elles utilisent la même adresse MAC gravée de l'interface parente. 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 l'ASA. Consultez Configurer manuellement l'adresse MAC.

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
```

En mode transparent ou pour un groupe de ponts en mode routé, spécifiez le BVI :

Exemple :

```
ciscoasa(config)# interface bvi 1
```

En mode transparent, en plus des BVI, vous pouvez également spécifier une interface de gestion :

Exemple :

```
ciscoasa(config)# interface management 1/1
```

Étape 2 (interface routée) Définissez l'adresse IP à l'aide de l'une des méthodes suivantes.

Pour le basculement et la mise en grappe, ainsi que pour les interfaces de boucle avec retour, vous devez définir l'adresse IP manuellement. Pour la mise en grappe, la configuration manuelle de l'adresse Link-Local n'est pas prise en charge.

- Activez l'autoconfiguration d'adresse sans état (SLAAC) sur l'interface :

  ipv6 address autoconfig [**default trust** {**dhcp** | **ignore**}]

  L'activation de la SLAAC sur l'interface configure les adresses IPv6 en fonction des préfixes reçus dans les messages d'annonce de routeur. Une adresse Link-Local, basée sur l'ID d'interface EUI-64 modifiée, est automatiquement générée pour l'interface lorsque la SLAAC est activée.

  Remarque
  Bien que la RFC 4862 spécifie que les hôtes configurés pour une SLAAC n'envoient pas de messages d'annonce de routeur, l'ASA envoie ces messages dans ce cas. Consultez la commande **ipv6 nd suppress-ra** pour supprimer les messages.

  Si vous souhaitez installer une voie de routage par défaut, spécifiez **default trust dhcp** ou **ignore**. **dhcp** précise que l'ASA utilise uniquement une voie de routage par défaut des annonces de routeur qui proviennent d'une source de confiance (c'est-à-dire du même serveur qui a fourni l'adresse IPv6). **ignore** spécifie que les annonces de routeur peuvent provenir d'un autre réseau, ce qui peut être une méthode plus risquée.

- Obtenez une adresse à l'aide de DHCPv6 :

  ipv6 address dhcp [**default**]

  Exemple :

  ```
  ciscoasa(config-if)# ipv6 address dhcp default
  ```

  Le mot clé **default** obtient une voie de routage par défaut à partir des publicités de routeur.

- Attribuez manuellement une adresse globale à l'interface :

  ipv6 address *ipv6_address*/*prefix-length* [**standby** *ipv6_address*]

  Exemple :

  ```
  ciscoasa(config-if)# ipv6 address 2001:0DB8:BA98::3210/64 standby 2001:0DB8:BA98::3211
  ```

  Lorsque vous attribuez une adresse globale, l'adresse locale du lien est automatiquement créée pour l'interface.

  standby (veille/secours) spécifie l'adresse d'interface utilisée par l'unité secondaire ou le groupe de basculement dans une paire de basculement.

- Attribuez une adresse globale à l'interface en combinant le préfixe spécifié avec un ID d'interface généré à partir de l'adresse MAC d'interface au moyen du format EUI-64 modifié :

  ipv6 address *ipv6-prefix*/*prefix-length* **eui-64**

  Exemple :

  ```
  ciscoasa(config-if)# ipv6 address 2001:0DB8:BA98::/64 eui-64
  ```

  Lorsque vous attribuez une adresse globale, l'adresse locale du lien est automatiquement créée pour l'interface.

  Vous n'avez pas besoin de préciser l'adresse de secours; l'ID d'interface sera généré automatiquement.

- Utilisez un préfixe délégué :

  ipv6 address *prefix_name ipv6_address*/*prefix_length*

  Exemple :

  ```
  ciscoasa(config-if)# ipv6 address Outside-Prefix ::1:0:0:0:1/64
  ```

  Cette fonctionnalité exige que l'ASA ait activé la délégation de préfixe DHCPv6 *sur une interface différente*. Consultez Activer le client de délégation de préfixe IPv6, à la page 19. En règle générale, le préfixe délégué est /60 ou moins, de sorte que vous pouvez créer un sous-réseau à plusieurs réseaux /64. /64 est la longueur de sous-réseau prise en charge si vous souhaitez prendre en charge SLAAC pour les clients connectés. Vous devez spécifier une adresse qui complète le sous-réseau /60, par exemple ::1:0:0:0:1. Saisissez : avant l'adresse si le préfixe est inférieur à 60. Par exemple, si le préfixe délégué est 2001:DB8:1234:5670::60, l'adresse IP globale attribuée à cette interface est 2001:DB8:1234:5671::1/64. Le préfixe annoncé dans les annonces des routeurs est 2001:DB8:1234:5671::/64. Dans cet exemple, si le préfixe est inférieur à 60, les bits restants du préfixe seront des 0, comme l'indique le préfixe::. Par exemple, si le préfixe est 2001:DB8:1234::/48, l'adresse IPv6 sera 2001:DB8:1234::1:0:0:0:1/64.

Étape 3 (interface BVI) Attribuez manuellement une adresse globale aux BVI. Pour une interface de gestion en mode transparent, utilisez également cette méthode.

ipv6 address *ipv6_address*/*prefix-length* [**standby** *ipv6_address*]

Exemple :

```
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
```

Lorsque vous attribuez une adresse globale, l'adresse locale du lien est automatiquement créée pour l'interface.

standby (veille/secours) spécifie l'adresse d'interface utilisée par l'unité secondaire ou le groupe de basculement dans une paire de basculement.

Étape 4 (Facultatif) Appliquer l'utilisation d'identifiants d'interface au format EUI-64 modifié dans les adresses IPv6 sur un lien local :

ipv6 enforce-eui64 *if_name*

Exemple :

```
ciscoasa(config)# ipv6 enforce-eui64 inside
```

L'argument *if_name* est le nom de l'interface, comme spécifié par la commande **nameif**, sur laquelle vous activez l'application du format d'adresse.

Configurer la découverte des voisins IPv6

Le processus de découverte des voisins IPv6 utilise des messages ICMPv6 et des adresses de multidiffusion de nœud sollicité pour déterminer l'adresse de couche de liaison d'un voisin sur le même réseau (lien local), vérifier la lisibilité d'un voisin et suivre les routeurs voisins.

Les nœuds (hôtes) utilisent la découverte des voisins pour déterminer les adresses de couche de liaison des voisins connus pour résider sur les liens attachés et pour purger rapidement les valeurs en cache qui deviennent non valides. Les hôtes ont également recours à la découverte des voisins pour trouver les routeurs voisins qui sont prêts à transférer des paquets en leur nom. En outre, les nœuds utilisent le protocole pour garder activement une trace des voisins accessibles et de ceux qui ne le sont pas, et pour détecter les adresses de couche de liaison modifiées. Lorsqu'un routeur ou le chemin d'accès à un routeur tombe en panne, un hôte recherche activement des solutions de remplacement qui fonctionnent.

Procédure

Étape 1 Précisez l'interface IPv6 que vous souhaitez configurer.

interface *name* (Nom d'interface)

Exemple :

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)#
```

Étape 2 Précisez le nombre de tentatives de détection d'adresses en double (DAD).

ipv6 nd dad attempts *value*

Les valeurs valides pour l'argument *value* sont comprises entre 0 et 600. La valeur 0 désactive le traitement de la DAD sur l'interface spécifiée. La valeur par défaut est de 1 message par seconde.

DAD garantit l'unicité des nouvelles adresses IPv6 de monodiffusion avant qu'elles ne soient attribuées et veille à ce que les adresses IPv6 en double soient détectées dans le réseau selon les liaisons. Le ASA utilise les messages de sollicitation des voisins pour effectuer le DAD.

Lorsqu'une adresse en double est identifiée, l'état de l'adresse est défini à DUPLICATE, l'adresse n'est pas utilisée et le message d'erreur suivant est généré :

```
325002: Duplicate address ipv6_address/MAC_address on interface
```

Si l'adresse en double est l'adresse link-local de l'interface, le traitement des paquets IPv6 est désactivé sur l'interface. Si l'adresse en double est une adresse globale, l'adresse n'est pas utilisée.

Exemple :

```
ciscoasa(config-if)# ipv6 nd dad attempts 20
```

Étape 3 Définissez l'intervalle entre les retransmissions de sollicitation d'un voisin IPv6.

ipv6 nd ns-interval *value*

Les valeurs de l'argument *value* sont comprises entre 1000 et 3600000 millisecondes.

Les messages de sollicitation des voisins (ICMPv6 de type 135) sont envoyés sur la liaison locale par les nœuds qui tentent de découvrir les adresses de couche de liaison d'autres nœuds sur la liaison locale. Après avoir reçu un message de sollicitation de voisin, le nœud de destination répond en envoyant un message d'annonce de voisin (ICPMv6 type 136) sur la liaison locale.

Une fois que le nœud source a reçu l'annonce de voisin, le nœud source et le nœud de destination peuvent communiquer. Les messages de sollicitation de voisin sont également utilisés pour vérifier l'accessibilité d'un voisin après avoir identifié l'adresse de couche de liaison d'un voisin. Lorsqu'un nœud souhaite vérifier l'accessibilité d'un voisin, l'adresse de destination dans un message de sollicitation de voisin est l'adresse de monodiffusion du voisin.

Des messages d'annonce de voisin sont également envoyés en cas de changement dans l'adresse de couche de liaison d'un nœud sur une liaison locale.

Exemple :

```
ciscoasa(config-if)# ipv6 nd ns-interval 9000
```

Étape 4 Définissez la durée pendant laquelle un nœud IPv6 distant est accessible.

ipv6 nd reachable-time *value*

Les valeurs de l'argument *value* sont comprises entre 0 et 3600000 millisecondes. Lorsque 0 est utilisé pour la valeur, la durée accessible est envoyée comme indéterminée. Il appartient aux périphériques de réception de définir et de suivre la durée accessible.

La durée d'accessibilité du voisin permet de détecter les voisins non disponibles. Des durées configurées plus courtes permettent de détecter plus rapidement les voisins non disponibles, mais des durées plus courtes consomment plus de bande passante réseau IPv6 et de ressources de traitement dans tous les périphériques réseau IPv6. Des durées configurées très courtes ne sont pas recommandées pour le fonctionnement normal d'un IPv6.

Exemple :

```
ciscoasa config-if)# ipv6 nd reachable-time 1700000
```

Étape 5 Définissez l'intervalle entre les transmissions des annonces du routeur IPv6.

ipv6 nd ra-interval [**msec**] *value*

Le mot clé **msec** indique que la valeur fournie est en millisecondes. Si ce mot clé n'est pas présent, la valeur fournie est en secondes. Les valeurs valides pour l'argument *value* sont comprises entre 3 et 1 800 secondes ou entre 500 et 1 800 000 millisecondes si le mot clé **msec** est fourni. La valeur par défaut est de 200 secondes.

La valeur d'intervalle est incluse dans toutes les annonces de routeur IPv6 qui sont envoyées à partir de cette interface.

L'intervalle entre les transmissions doit être inférieur ou égal à la durée de vie des annonces du routeur IPv6 si l'ASA est configuré comme routeur par défaut.

Pour empêcher la synchronisation avec d'autres nœuds IPv6, l'ASA ajuste de manière aléatoire la valeur que vous avez définie (gigue).

Exemple :

```
ciscoasa(config-if)# ipv6 nd ra-interval 201
```

Étape 6 Spécifiez la durée pendant laquelle les nœuds de la liaison locale doivent considérer l'ASA comme routeur par défaut sur la liaison.

ipv6 nd ra-lifetime [**msec**] *value*

Le mot clé facultatif **msec** indique que la valeur fournie est en millisecondes. Sinon, la valeur est en secondes. Les valeurs de l'argument *value* sont comprises entre 0 et 9 000 secondes. Si la valeur 0 est saisie, l'ASA ne doit pas être considéré comme un routeur par défaut sur l'interface sélectionnée.

La valeur de vie du routeur est incluse dans toutes les annonces de routeur IPv6 envoyées hors de l'interface. La valeur indique l'utilité de l'ASA en tant que routeur par défaut sur cette interface.

Exemple :

```
ciscoasa(config-if)# ipv6 nd ra-lifetime 2000
```

Étape 7 Supprimer les annonces du routeur.

ipv6 nd suppress-ra

Les messages d'annonce de routeur (ICMPv6 Type 134) sont automatiquement envoyés en réponse aux messages de sollicitation de routeur (ICMPv6 Type 133). Les messages de sollicitation de routeur sont envoyés par les hôtes au démarrage du système, ce qui permet à l'hôte de se configurer automatiquement sans avoir à attendre le prochain message de publicité de routeur planifié.

Vous pouvez souhaiter désactiver ces messages sur toute interface pour laquelle vous ne souhaitez pas que l'ASA fournisse le préfixe IPv6 (par exemple, l'interface extérieure).

Cette commande fait que l'ASA s'affiche comme un voisin IPv6 standard sur la liaison et non comme un routeur IPv6.

Étape 8 Ajoutez un indicateur aux annonces de routeur IPv6 pour informer les clients d'autoconfiguration d'adresse sans état (SLAAC) IPv6 d'utiliser DHCPv6 pour obtenir une adresse IPv6, en plus de l'adresse SLAAC dérivée.

ipv6 nd managed-config-flag

Cette option définit l'indicateur de configuration d'adresse gérée dans le paquet d'annonce du routeur IPv6.

Étape 9 Ajoutez un indicateur aux annonces de routeur IPv6 pour informer les clients SLAAC IPv6 d'utiliser DHCPv6 pour obtenir l'adresse du serveur DNS ou d'autres renseignements.

ipv6 nd other-config-flag

Cette option définit l'indicateur Another Address Config (Configuration d'une autre adresse) dans le paquet d'annonce du routeur IPv6.

Étape 10 Configurez quels préfixes IPv6 sont inclus dans les annonces de routeur IPv6 :

ipv6 nd prefix {*ipv6_prefix*/*prefix_length* | **default**} [*valid_lifetime preferred_lifetime* | **at** *valid_date preferred_date*] [**no-advertise**] [**no-autoconfig**] [ ] [**off-link**]

L'annonce de préfixe peut être utilisée par les périphériques voisins pour configurer automatiquement leurs adresses d'interface. SLAAC utilise les préfixes IPv6 fournis dans les messages d'annonce des routeurs pour créer l'adresse de monodiffusion globale à partir de l'adresse Link-Local.

Par défaut, les préfixes configurés comme adresses sur une interface à l'aide de la commande **d'adresse ipv6** sont annoncés dans les annonces de routeur. Si vous configurez des préfixes pour publication à l'aide de la commande **ipv6 nd prefix**, seuls ces préfixes sont annoncés.

Pour que SLAAC fonctionne correctement, la longueur du préfixe annoncée dans les messages d'annonce du routeur doit toujours être de 64 bits.

- **default** : pour indiquer que le préfixe par défaut est utilisé.
- *valid_lifetime preferred_lifetime* : spécifie la durée pendant laquelle le préfixe IPv6 spécifié est annoncé comme valide et préféré. Une adresse n'a aucune restriction pendant sa durée de vie préférée. À l'expiration de la durée de vie préférée, l'adresse passe à l'état obsolète. Lorsqu'une adresse est dans un état obsolète, son utilisation est déconseillée, mais pas formellement interdite. Après l'expiration de la durée de vie valide, l'adresse devient non valide et ne peut pas être utilisée. La durée de vie valide doit être supérieure ou égale à la durée de vie préférée. Les valeurs sont comprises entre 0 et 4294967295 secondes. La valeur maximale représente l'éternité, et peut également être spécifiée à l'aide du mot clé **infinite**. La valeur par défaut de la durée de vie valide est de 2 592 000 (30 jours). La durée de vie par défaut préférée est 604 800 (7 jours).
- **at** *valid_date preferred_date* : indique une date et une heure spécifiques à laquelle le préfixe expire. Spécifiez la date au format *mois_jour hh*:*mm*. Par exemple, saisissez **déc 1 13:00**.
- **no-advertise** : pour désactiver l'annonce du préfixe. Pour le préfixe **default**, ce paramètre s'applique uniquement aux préfixes sur la liaison. Les préfixes hors liaison seront toujours annoncés, sauf si vous spécifiez **no-advertise** pour un préfixe hors liaison précis.
- **no-autoconfig** : spécifie que le préfixe ne peut pas être utilisé pour SLAAC IPv6.
- **off-link** : pour configurer le préfixe spécifié comme hors liaison. Le préfixe sera annoncé avec le bit L en effacement. Le préfixe ne sera pas inséré dans la table de routage en tant que préfixe connecté.

  Lorsque onlink est activé (par défaut), le préfixe spécifié est affecté au lien. Les nœuds envoyant du trafic vers de telles adresses qui contiennent le préfixe spécifié considèrent la destination comme accessible localement sur le lien.

Exemple :

```
ciscoasa(config-if)# ipv6 nd prefix 2001:DB8::/32 1000 900
```

Étape 11 Configurez une entrée statique dans le cache de découverte des voisins IPv6.

ipv6 neighbor *ipv6_address if_name mac_address*

Les directives et limites suivantes s'appliquent à la configuration d'un voisin IPv6 statique :

- La commande **ipv6 neighbor** est similaire à la commande **arp**. Si une entrée pour l'adresse IPv6 précisée existe déjà dans le cache de découverte des voisins (apprise par le processus de découverte des voisins IPv6), elle est automatiquement convertie en entrée statique. Ces entrées sont stockées dans la configuration lorsque la commande copy est utilisée pour stocker la configuration.

- Utilisez la commande **show ipv6 neighbor** pour afficher les entrées statiques dans le cache de découverte IPv6 neighbor.
- La commande **clear ipv6 neighbor** supprime toutes les entrées du cache de découverte IPv6 neighbor, à l'exception des entrées statiques. La commande **no ipv6 neighbor** supprime une entrée statique spécifiée de la mémoire cache de découverte du voisin; la commande ne supprime pas les entrées dynamiques (les entrées apprises du processus de découverte des voisins IPv6) du cache. La désactivation d'IPv6 sur une interface à l'aide de la commande **no ipv6 enable** supprime toutes les entrées du cache de découverte des voisins IPv6 configurées pour cette interface, à l'exception des entrées statiques (l'état de l'entrée passe à INCMP [Incomplete]).
- Les entrées statiques de la mémoire cache de découverte du voisin IPv6 ne sont pas modifiées par le processus de découverte du voisin.
- La commande **clear ipv6 neighbor** ne supprime pas les entrées statiques de la mémoire cache de découverte IPv6 neighbor; il efface uniquement les entrées dynamiques.
- Les journaux système ICMP générés sont provoqués par une actualisation régulière des entrées IPv6 neighbor. La minuterie par défaut de l'ASA pour l'entrée du voisin IPv6 est de 30 secondes, donc l'ASA génère des paquets de découverte et de réponse des voisins ICMPv6 toutes les 30 secondes. Si l'ASA est dotée d'interfaces LAN et d'état de basculement configurées avec des adresses IPv6, toutes les 30 secondes, des paquets de réponse et de découverte de voisin ICMPv6 seront générés par les deux ASA pour les adresses IPv6 configurées et celles liées au lien local. En outre, chaque paquet génère plusieurs syslogs (connexion ICMP et création ou démontage de l'hôte local), de sorte qu'il peut sembler que des syslogs ICMP sont générés en permanence. L'heure d'actualisation de l'entrée du voisin IPV6 peut être configurée sur l'interface de données normale, mais pas sur l'interface de basculement. Cependant, l'impact sur le CPU pour ce trafic de découverte de voisin ICMP est minime.

Exemple :

```
ciscoasa(config)# ipv6 neighbor 3001:1::45A inside 002.7D1A.9472
```

Supervision des interfaces en mode routé et en mode transparent

Vous pouvez superviser les statistiques d'interface, l'état, PPPoE

Remarque Pour les modèles Firepower et Secure Firewall, certaines statistiques ne sont pas affichées à l'aide des commandes ASA. Vous devez consulter des statistiques d'interface plus détaillées à l'aide des commandes FXOS.

- /eth-uplink/fabric# **show interface**
- /eth-uplink/fabric# **show port-channel**
- /eth-uplink/fabric/interface# **show stats**

Pour Firepower 2100 en mode plateforme, consultez aussi les commandes FXOS connect local-mgmt suivantes :

- (local-mgmt)# **show portmanager counters**
- (local-mgmt)# **show lacp**
- (local-mgmt)# **show portchannel**

Consultez le guide de dépannage FXOS pour plus d'informations.

Statistiques et informations sur l'interface

- **show interface**

  Affiche des statistiques sur l'interface.

- **show interface ip brief**

  Affiche les adresses IP et l'état de l'interface.

- **show bridge-group**

  Affiche les renseignements sur le groupe de ponts, comme les interfaces attribuées, les adresses MAC et les adresses IP.

Renseignements sur DHCP

- **show ipv6 dhcp interface** [*ifc_name* [**statistics**]]

  La commande **show ipv6 dhcp interface** affiche les renseignements DHCPv6 pour toutes les interfaces. Si l'interface est configurée pour la configuration du serveur sans état DHCPv6 (voir Configurer le serveur sans état DHCPv6), cette commande répertorie l'ensemble DHCPv6 utilisé par le serveur. Si l'interface a une configuration de client d'adresse DHCPv6 ou de client de délégation de préfixe, cette commande affiche l'état de chaque client et les valeurs reçues du serveur. Pour une interface en particulier, vous pouvez afficher les statistiques des messages pour le serveur ou le client DHCP. Les exemples suivants montrent les renseignements fournis par cette commande :

```
ciscoasa(config-if)# show ipv6 dhcp interface
GigabitEthernet1/1 is in server mode
  Using pool: Sample-Pool

GigabitEthernet1/2 is in client mode
  Prefix State is OPEN
```

```
  Renew will be sent in 00:03:46
  Address State is OPEN
  Renew for address will be sent in 00:03:47
  List of known servers:
    Reachable via address: fe80::20c:29ff:fe96:1bf4
    DUID: 000100011D9D1712005056A07E06
    Preference: 0
    Configuration parameters:
      IA PD: IA ID 0x00030001, T1 250, T2 400
        Prefix: 2005:abcd:ab03::/48
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      IA NA: IA ID 0x00030001, T1 250, T2 400
        Address: 2004:abcd:abcd:abcd:abcd:abcd:abcd:f2cb/128
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      DNS server: 2004:abcd:abcd:abcd::2
      DNS server: 2004:abcd:abcd:abcd::4
      Domain name: relay.com
      Domain name: server.com
      Information refresh time: 0
  Prefix name: Sample-PD

Management1/1 is in client mode
  Prefix State is IDLE
  Address State is OPEN
  Renew for address will be sent in 11:26:44
  List of known servers:
    Reachable via address: fe80::4e00:82ff:fe6f:f6f9
    DUID: 000300014C00826FF6F8
    Preference: 0
    Configuration parameters:
      IA NA: IA ID 0x000a0001, T1 43200, T2 69120
        Address: 2308:2308:210:1812:2504:1234:abcd:8e5a/128
                preferred lifetime INFINITY, valid lifetime INFINITY
      Information refresh time: 0


ciscoasa(config-if)# show ipv6 dhcp interface outside statistics

DHCPV6 Client PD statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0

DHCPV6 Client address statistics:

Protocol Exchange Statistics:
```

```
 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                1
 Number of Message Validation errors in received messages: 0
```

- **show ipv6 dhcp client** [**pd**] **statistics**

  La commande **show ipv6 dhcp client statistics** affiche les statistiques du client DHCPv6 et indique le résultat du nombre de messages envoyés et reçus. La commande **show ipv6 dhcp client pd statistics** affiche les statistiques du client de délégation de préfixes. Les exemples suivants montrent les renseignements fournis par cette commande :

```
ciscoasa(config)# show ipv6 dhcp client statistics

Protocol Exchange Statistics:
  Total number of Solicit messages sent:              4
  Total number of Advertise messages received:        4
  Total number of Request messages sent:              4
  Total number of Renew messages sent:                92
  Total number of Rebind messages sent:               0
  Total number of Reply messages received:            96
  Total number of Release messages sent:              6
  Total number of Reconfigure messages received:      0
  Total number of Information-request messages sent:  0

Error and Failure Statistics:
  Total number of Re-transmission messages sent:                  8
  Total number of Message Validation errors in received messages: 0


ciscoasa(config)# show ipv6 dhcp client pd statistics

Protocol Exchange Statistics:


 Total number of Solicit messages sent:              1
 Total number of Advertise messages received:        1
 Total number of Request messages sent:              1
 Total number of Renew messages sent:                92
 Total number of Rebind messages sent:               0
 Total number of Reply messages received:            93
 Total number of Release messages sent:              0
 Total number of Reconfigure messages received:      0
 Total number of Information-request messages sent:  0

Error and Failure Statistics:
```

```
 Total number of Re-transmission messages sent:                 1
 Total number of Message Validation errors in received messages: 0
```

- **show ipv6 dhcp ha statistics**

  La commande **show ipv6 dhcp ha statistics** affiche les statistiques de transaction entre les unités de basculement, y compris le nombre de fois où les renseignements DUID ont été synchronisés entre les unités. Les exemples suivants montrent les renseignements fournis par cette commande.

  Sur une unité active :

```
ciscoasa(config)# show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:             1
  DUID sync messages received:         0

DHCPv6 HA error statistics:
  Send errors:                         0
```

  Sur une unité de secours :

```
ciscoasa(config)# show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:             0
  DUID sync messages received:         1

DHCPv6 HA error statistics:
  Send errors:                         0
```

- **show ipv6 general-prefix**

  La commande **show ipv6 general-prefix** affiche tous les préfixes acquis par les clients de délégation de préfixe DHCPv6 et la distribution ASA de ce préfixe à d'autres processus (« Liste des consommateurs »). L'exemple suivant montre les renseignements fournis par cette commande :

```
ciscoasa(config)# show ipv6 general-prefix
IPv6 Prefix Sample-PD, acquired via DHCP PD
  2005:abcd:ab03::/48 Valid lifetime 524, preferred lifetime 424
   Consumer List               Usage count
    BGP network command        1
    inside (Address command)   1
```

PPPoE

- **show ip address** *interface_name* **pppoe**

  Affiche les renseignements de configuration actuels du client PPPoE.

- **debug pppoe** {**event** | **error** | **packet**}

  Active le débogage pour le client PPPoE.

- **show vpdn session** [**l2tp** | **pppoe**] [**id** *sess_id* | **packets** | **state** | **window**]

Affiche l'état des sessions PPPoE.

Les exemples suivants montrent les renseignements fournis par cette commande :

```
ciscoasa# show vpdn

Tunnel id 0, 1 active sessions
     time since change 65862 secs
     Remote Internet Address 10.0.0.1
    Local Internet Address 199.99.99.3
     6 packets sent, 6 received, 84 bytes sent, 0 received
Remote Internet Address is 10.0.0.1
     Session state is SESSION_UP
       Time since event change 65865 secs, interface outside
       PPP interface id is 1
       6 packets sent, 6 received, 84 bytes sent, 0 received
ciscoasa#
ciscoasa# show vpdn session
PPPoE Session Information (Total tunnels=1 sessions=1)
Remote Internet Address is 10.0.0.1
  Session state is SESSION_UP
    Time since event change 65887 secs, interface outside
    PPP interface id is 1
    6 packets sent, 6 received, 84 bytes sent, 0 received
ciscoasa#
ciscoasa# show vpdn tunnel
PPPoE Tunnel Information (Total tunnels=1 sessions=1)
Tunnel id 0, 1 active sessions
   time since change 65901 secs
   Remote Internet Address 10.0.0.1
   Local Internet Address 199.99.99.3
   6 packets sent, 6 received, 84 bytes sent, 0 received
ciscoasa#
```

Découverte de voisin IPv6

Pour superviser les paramètres de découverte de voisin IPv6, saisissez les commandes suivantes.

- **show ipv6 interface**

  Cette commande affiche l'état de convivialité des interfaces configurées pour IPv6, y compris le nom de l'interface, tel que « externe », et affiche les paramètres de l'interface spécifiée. Cependant, elle exclut le nom de la commande et affiche les paramètres de toutes les interfaces sur lesquelles IPv6 est activé. La sortie de la commande affiche les éléments suivants :

  - Le nom et l'état de l'interface.
  - Les adresses de monodiffusion Link-Local et globale.
  - Les groupes de multidiffusion auxquels appartient l'interface.
  - Les paramètres de redirection ICMP et de message d'erreur.
  - Les paramètres du protocole ndp (Neighbor Discovery Protocol)
  - L'heure réelle à laquelle la commande est définie sur 0.
  - L'heure d'accessibilité utilisée pour la découverte du voisin.

Exemples d'interfaces en mode routé et en mode transparent

Exemple de mode transparent avec 2 groupes de ponts

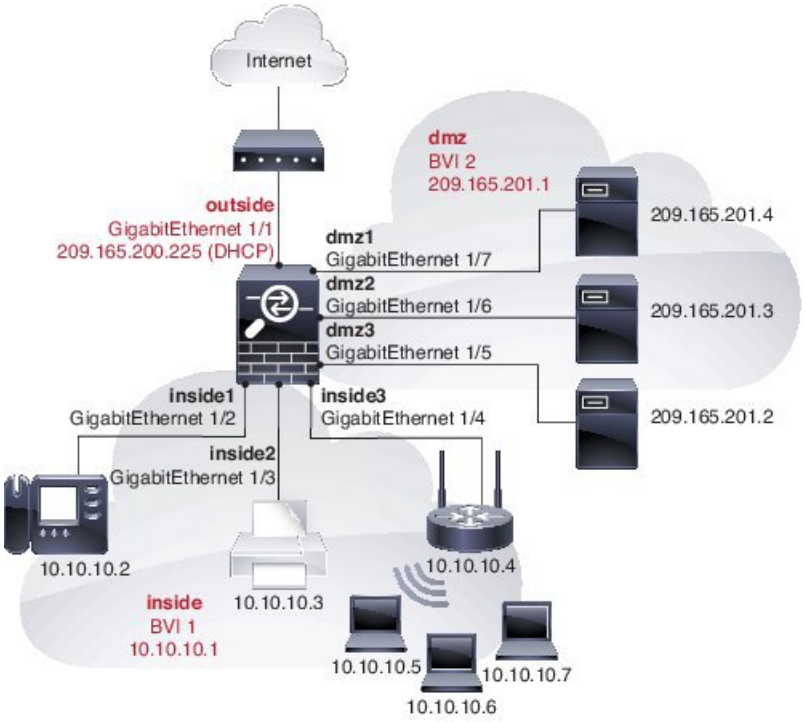
L'exemple suivant de mode transparent comprend deux groupes de ponts de trois interfaces chacun, plus une interface de gestion uniquement :

```
interface gigabitethernet 0/0
  nameif inside1
  security-level 100
  bridge-group 1
  no shutdown
interface gigabitethernet 0/1
  nameif outside1
  security-level 0
  bridge-group 1
  no shutdown
interface gigabitethernet 0/2
  nameif dmz1
  security-level 50
  bridge-group 1
  no shutdown
interface bvi 1
  ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2

interface gigabitethernet 1/0
  nameif inside2
  security-level 100
  bridge-group 2
  no shutdown
interface gigabitethernet 1/1
  nameif outside2
  security-level 0
  bridge-group 2
  no shutdown
interface gigabitethernet 1/2
  nameif dmz2
  security-level 50
  bridge-group 2
  no shutdown
interface bvi 2
  ip address 10.3.5.8 255.255.255.0 standby 10.3.5.9

interface management 0/0
  nameif mgmt
  security-level 100
  ip address 10.2.1.1 255.255.255.0 standby 10.2.1.2
  no shutdown
```

Exemple de segment LAN commuté avec 2 groupes de ponts

Dans l'exemple suivant, deux groupes de ponts de 3 interfaces et une interface routée standard pour l'extérieur sont configurés. Le groupe de ponts 1 est à l'intérieur et le groupe de ponts 2 est une zone DMZ avec des serveurs Web publics. Les interfaces membres du groupe de ponts peuvent communiquer librement au sein du groupe de ponts, car chaque membre se trouve au même niveau de sécurité et nous avons activé la même

communication de sécurité. Bien que le niveau de sécurité du membre interne soit de 100 et que celui du membre de la zone DMZ soit également de 100, ces niveaux de sécurité ne s'appliquent pas aux communications inter-BVI; seuls les niveaux de sécurité BVI affectent le trafic inter-BVI. Les niveaux de sécurité des BVI et de l'extérieur (100, 50 et 0) autorisent implicitement le trafic de l'intérieur vers la zone DMZ et de l'intérieur vers l'extérieur; ainsi que de la zone DMZ vers l'extérieur. Un critère d'accès est appliqué à l'extérieur pour autoriser le trafic vers les serveurs de la zone DMZ.




```
interface gigabitethernet 1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface gigabitethernet 1/2
  nameif inside1
  security-level 100
  bridge-group 1
  no shutdown
interface gigabitethernet 1/3
  nameif inside2
  security-level 100
  bridge-group 1
  no shutdown
interface gigabitethernet 1/4
  nameif inside3
  security-level 100
  bridge-group 1
  no shutdown
!
interface bvi 1
  nameif inside
  security-level 100
  ip address 10.10.10.1 255.255.255.0
```

```
!
interface gigabitethernet 1/5
  nameif dmz1
  security-level 100
  bridge-group 2
  no shutdown
interface gigabitethernet 1/6
  nameif dmz2
  security-level 100
  bridge-group 2
  no shutdown
interface gigabitethernet 1/7
  nameif dmz3
  security-level 100
  bridge-group 2
  no shutdown
!
interface bvi 2
  nameif dmz
  security-level 50
  ip address 209.165.201.1 255.255.255.224
!
same-security-traffic permit inter-interface
!
# Assigns IP addresses to inside hosts
dhcpd address 10.10.10.2-10.10.10.200 inside
dhcpd enable inside
!
# Applies interface PAT for inside traffic going outside
nat (inside1,outside) source dynamic any interface
nat (inside2,outside) source dynamic any interface
nat (inside3,outside) source dynamic any interface
!
# Allows outside traffic to each server for specific applications
object network server1
  host 209.165.201.2
object network server2
  host 209.165.201.3
object network server3
  host 209.165.201.4
!
# Defines mail services allowed on server3
object-group service MAIL
  service-object tcp destination eq pop3
  service-object tcp destination eq imap4
  service-object tcp destination eq smtp
!
# Allows access from outside to servers on the DMZ
access-list SERVERS extended permit tcp any object server1 eq www
access-list SERVERS extended permit tcp any object server2 eq ftp
access-list SERVERS extended permit tcp any object server3 object-group MAIL
access-group SERVERS in interface outside
```

Historique des interfaces en mode routé et en mode transparent

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Découverte de voisin IPv6	7.0(1)	Nous avons introduit cette fonctionnalité. Nous avons introduit les commandes suivantes : **ipv6 nd ns-interval**, **ipv6 nd ra-lifetime**, **ipv6 nd suppress-ra**, **ipv6 neighbor**, **ipv6 nd prefix**, **ipv6 nd dad-attempts**, **ipv6 nd reachable-time**, **ipv6 address**, **ipv6 enforce-eui64**.
Prise en charge d'IPv6 pour le mode transparent	8.2(1)	La prise en charge d'IPv6 a été introduite pour le mode de pare-feu transparent.
Groupes de ponts pour le mode transparent	v 8.4(1)	Si vous ne souhaitez pas le surdébit des contextes de sécurité ou si vous souhaitez optimiser votre utilisation des contextes de sécurité, vous pouvez regrouper les interfaces dans un groupe de ponts, puis configurer plusieurs groupes de ponts, un pour chaque réseau. Le trafic de groupe de ponts est isolé des autres groupes de ponts. Vous pouvez configurer jusqu'à huit groupes de ponts de quatre interfaces chacun en mode unique ou par contexte. Nous avons introduit les commandes suivantes : **interface bvi**, **show bridge-group**
Indicateurs de configuration d'adresse pour le relais DHCP IPv6	9.0(1)	Nous avons introduit les commandes suivantes : **ipv6 nd managed-config-flag**, **ipv6 nd other-config-flag**.
Nombre maximum de groupes de ponts en mode transparent augmenté à 250	9.3(1)	Le nombre maximum de groupes de ponts est passé de 8 à 250 groupes de ponts. Vous pouvez configurer jusqu'à 250 groupes de ponts en mode unique ou par contexte en mode multiple, avec 4 interfaces maximum par groupe de ponts. Nous avons modifié les commandes suivantes : **interface bvi**, **bridge-group**
Nombre maximum d'interfaces en mode transparent par groupe de ponts augmenté à 64	9.6(2)	Le nombre maximum d'interfaces par groupe de ponts est passé de 4 à 64. Nous n'avons pas modifié de commandes.

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
DHCP IPv6	9.6(2)	L'ASA prend désormais en charge les fonctionnalités suivantes pour l'adressage IPv6 : • Client d'adresse DHCPv6 : l'ASA obtient une adresse globale IPv6 et une route par défaut facultative du serveur DHCPv6. • Client de délégation de préfixe DHCPv6 : l'ASA obtient le ou les préfixes délégués d'un serveur DHCPv6. L'ASA peut ensuite utiliser ces préfixes pour configurer d'autres adresses d'interface ASA afin que les clients SLAAC (StateLess Address Auto Configuration) puissent configurer automatiquement les adresses IPv6 sur le même réseau. • Annonce de routeur BGP pour les préfixes délégués • Serveur sans état DHCPv6 : l'ASA fournit d'autres renseignements tels que le nom de domaine aux clients SLAAC lorsqu'ils envoient des paquets de demande d'information (IR) à l'ASA. L'ASA accepte uniquement les paquets IR et n'affecte pas d'adresses aux clients. Nous avons ajouté ou modifié les commandes suivantes : **clear ipv6 dhcp statistics, domain-name, dns-server, import, ipv6 address autoconfig, ipv6 address dhcp, ipv6 dhcp client pd, ipv6 dhcp client pd hint, ipv6 dhcp pool, ipv6 dhcp server, network, nis address, nis domain-name, nisp address, nisp domain-name, show bgp ipv6 unicast, show ipv6 dhcp, show ipv6 general-prefix, sip address, sip domain-name, sntp address**

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**
Masque de sous-réseau 31 bits	9.7(1)	Pour les interfaces routées, vous pouvez configurer une adresse IP sur un sous-réseau de 31 bits pour les connexions point à point. Le sous-réseau de 31 bits comprend seulement 2 adresses; normalement, la première et la dernière adresse du sous-réseau sont réservées pour le réseau et la diffusion, donc un sous-réseau à deux adresses n'est pas utilisable. Toutefois, si vous avez une connexion point à point et n'avez pas besoin d'adresses de réseau ou de diffusion, un sous-réseau de 31 bits est un moyen utile de conserver les adresses dans IPv4. Par exemple, la liaison de basculement entre 2 ASA ne nécessite que 2 adresses; les paquets transmis par une extrémité de la liaison sont toujours reçus par l'autre extrémité, et la diffusion n'est pas nécessaire. Vous pouvez également avoir une station de gestion directement connectée exécutant SNMP ou Syslog. Cette fonctionnalité n'est pas prise en charge pour les BVI pour les groupes de ponts ou avec le routage de multidiffusion. Nous avons modifié les commandes suivantes : **ip address, http, logging host, snmp-server, ssh**

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.