Périphériques logiques pour le Firepower 4100/9300

Firepower 4100/9300 est une plateforme de sécurité flexible sur laquelle vous pouvez installer un ou plusieurs *périphériques logiques*. Ce chapitre décrit la configuration de l'interface de base et comment ajouter un périphérique logique autonome ou à haute accessibilité à l'aide de Firewall Chassis Manager. Pour ajouter un périphérique logique en grappe, consultez Grappe ASA pour le Firepower 4100/9300. Pour utiliser l'interface de ligne de commande de FXOS, consultez le guide de configuration de l'interface de ligne de commande FXOS. Pour des procédures FXOS et un dépannage plus avancés, consultez le guide de configuration FXOS.

À propos des interfaces

Le Châssis Firepower 4100/9300 prend en charge les interfaces physiques et les interfaces EtherChannel (canal de port). Les interfaces EtherChannel peuvent comprendre jusqu'à 16 interfaces membres du même type.

Interface de gestion de châssis

L'interface de gestionnaire de châssis est utilisée pour la gestion du châssis FXOS par SSH ou Firewall Chassis Manager. Cette interface est distincte de l'interface de type gestion (mgmt) que vous affectez aux périphériques logiques pour la gestion des applications.

Pour configurer les paramètres de cette interface, vous devez les configurer à partir de l'interface de ligne de commande. Pour afficher des informations sur cette interface dans l'interface de ligne de commande FXOS, connectez-vous à la gestion locale et affichez le port de gestion :

Firepower # **connect local-mgmt**

Firepower(local-mgmt) # **show mgmt-port**

Notez que l'interface de gestion du châssis reste active même si le câble physique ou le module SFP est débranché ou que la commande **mgmt-port shut** est exécutée ou si le périphérique logique est hors-ligne.

Remarque L'interface de gestion de châssis ne prend pas en charge les trames étendues.

Types d'interface

Les interfaces physiques et les interfaces EtherChannel (canal de port) peuvent être de l'un des types suivants :

- Données : à utiliser pour les données normales. Les interfaces de données ne peuvent pas être mises en commun entre les périphériques logiques, et les périphériques logiques ne peuvent pas communiquer avec d'autres périphériques logiques par le fond de panier Pour le trafic sur les interfaces de données, tout le trafic doit quitter le châssis sur une interface et revenir sur une autre interface pour atteindre un autre périphérique logique.
- Data-sharing (partage de données) : à utiliser pour les données normales. Pris en charge uniquement avec les instances de conteneur, ces interfaces de données peuvent être partagées par un ou plusieurs dispositifs logiques/Instances de conteneur (Firewall Threat Defense-utilisant-Firewall Management Center seulement).
- Gestion : permet de gérer les instances d'application. Ces interfaces peuvent être partagées par un ou plusieurs périphériques logiques pour accéder à des hôtes externes; les périphériques logiques ne peuvent pas communiquer sur cette interface avec d'autres périphériques logiques qui partagent l'interface. Vous ne pouvez affecter qu'une seule interface de gestion par périphérique logique. En fonction de votre application et de votre gestionnaire, vous pouvez ultérieurement activer la gestion à partir d'une interface de données; mais vous devez attribuer une interface de gestion au dispositif logique même si vous n'avez pas l'intention de l'utiliser après avoir activé la gestion des données.Pour en savoir plus sur l'interface de gestion de châssis distincte, consultez Interface de gestion de châssis, à la page 1.

Remarque La modification de l'interface de gestion entraînera le redémarrage du périphérique logique. Par exemple, une gestion des modifications de e1/1 à e1/2 entraînera le redémarrage du périphérique logique pour appliquer la nouvelle gestion.

- Créer un événement— Sert d'interface de gestion secondaire pour les périphériques Firewall Threat Defense-using- (en usage)Firewall Management Center.

Remarque Une interface Ethernet virtuelle est attribuée lors de l'installation de chaque instance applicative. Si l'application n'utilise pas d'interface événementielle, l'interface virtuelle sera dans un état "admin down".

```
Firepower # show interface Vethernet775
Firepower # Vethernet775 is down (Administratively down)
Bound Interface is Ethernet1/10
Port description is server 1/1, VNIC ext-mgmt-nic5
```

- Cluster (grappe) : à utiliser comme liaison de commande de grappe pour un périphérique logique en grappe. Par défaut, la liaison de commande de grappe est automatiquement créée sur le canal de port 48. Le type de grappe est uniquement pris en charge sur les interfaces EtherChannel.

Reportez-vous à la table suivante pour la prise en charge des types d'interface pour les demandes Firewall Threat Defense et ASA dans les déploiements autonomes et en grappe.

Tableau 1 : Prise en charge des types d'interface

Application		Données	Données : sous-interface	Partage de données	Partage de données : sous-interface	Gestion	Créer des événements	Grappe (EtherChannel uniquement)	Grappe : sous-interface
Firewall Threat Defense	Instance native autonome	**Oui**	—	—	—	**Oui**	**Oui**	—	—
	Instance de conteneur autonome	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	**Oui**	—	—
	Instance native de grappe	**Oui** (EtherChannel uniquement pour la grappe inter-châssis)	—	—	—	**Oui**	**Oui**	**Oui**	—
	Instance de conteneur de grappe	**Oui** (EtherChannel uniquement pour la grappe inter-châssis)	—	—	—	**Oui**	**Oui**	**Oui**	**Oui**
ASA	Instance native autonome	**Oui**	—	—	—	**Oui**	—	**Oui**	—
	Instance native de grappe	**Oui** (EtherChannel uniquement pour la grappe inter-châssis)	—	—	—	**Oui**	—	**Oui**	—

Interfaces FXOS par rapport aux interfaces d'application

Le Firepower 4100/9300 gère les paramètres Ethernet de base des interfaces physiques et les interfaces EtherChannel (canal de port). Dans l'application, vous configurez les paramètres de niveau supérieur. Par

exemple, vous pouvez uniquement créer des EtherChannels dans FXOS; mais vous pouvez attribuer une adresse IP à l'EtherChannel dans l'application.

Les sections suivantes décrivent l'interaction entre FXOS et l'application pour les interfaces.

Sous-interfaces VLAN

Pour tous les périphériques logiques, vous pouvez créer des sous-interfaces VLAN dans l'application.

États indépendants de l'interface dans le châssis et dans l'application

Vous pouvez activer et désactiver administrativement les interfaces dans le châssis et dans l'application. Pour qu'une interface soit opérationnelle, elle doit être activée dans les deux systèmes d'exploitation. Étant donné que l'état de l'interface est contrôlé indépendamment, il se peut que vous ayez une incompatibilité entre le châssis et l'application.

À propos des périphériques logiques

Un périphérique logique vous permet d'exécuter une instance d'application (ASA ou Firewall Threat Defense) ainsi qu'une application de décochage facultative (Radware DefensePro) pour former une chaîne de services.

Lorsque vous ajoutez un périphérique logique, vous définissez également le type et la version de l'instance d'application, vous affectez des interfaces et vous configurez les paramètres de démarrage qui sont transmis à la configuration de l'application.

Remarque Pour Firepower 9300, vous pouvez installer différents types d'applications (ASA et Firewall Threat Defense) sur des modules distincts du châssis. Vous pouvez également exécuter différentes versions d'un type d'instance d'application sur des modules distincts.

Périphériques logiques autonomes et en grappe

Vous pouvez ajouter les types d'unités logiques suivants :

- Autonome : un périphérique logique autonome fonctionne comme une unité autonome ou comme une unité dans une paire à haute disponibilité.
- Grappe : un appareil logique en grappe vous permet de regrouper plusieurs unités ensemble, offrant toute la commodité d'un seul appareil (gestion, intégration dans un réseau) tout en obtenant le débit accru et la redondance de plusieurs périphériques. Les périphériques à modules multiples, comme le périphérique Firepower 9300, prennent en charge la mise en grappe à l'intérieur des châssis. Pour le périphérique Firepower 9300, les trois modules doivent faire partie de la grappe, à la fois pour les instances natives et de conteneur.

Exigences et conditions préalables pour les combinaisons matérielles et logicielles

Le Firepower 4100/9300 prend en charge plusieurs modèles, modules de sécurité, types d'applications, et de haute disponibilité et d'évolutivité. Consultez les exigences suivantes pour connaître les combinaisons autorisées.

Exigences du périphérique Firepower 9300

L'appareil Firepower 9300 comprend 3 logements pour module de sécurité et plusieurs types de modules de sécurité. Consultez les exigences suivantes :

- Security Module Types (types de modules de sécurité) : Vous pouvez installer des modules de différents types dans le périphérique Firepower 9300. Par exemple, vous pouvez installer le SM-48 comme module 1, le SM-40 comme module 2 et le SM-56 comme module 3.
- Instances natives et de conteneur : lorsque vous installez une instance de conteneur sur un module de sécurité, ce module ne peut prendre en charge que d'autres instances de conteneur. Une instance native utilise toutes les ressources d'un module, vous ne pouvez donc installer qu'une seule instance native sur un module. Vous pouvez utiliser des instances natives sur certains modules et des instances de conteneur sur les autres modules. Par exemple, vous pouvez installer une instance native sur le module 1 et le module 2, mais des instances de conteneur sur le module 3.
- Mise en grappe : tous les modules de sécurité de la grappe, qu'elle soit intra-châssis ou inter-châssis, doivent être du même type. Vous pouvez avoir différentes quantités de modules de sécurité installés dans chaque châssis, bien que tous les modules présents dans le châssis doivent appartenir à la grappe, y compris les logements vides. Par exemple, vous pouvez installer 2 SM-40 dans le châssis 1 et 3 SM-40 dans le châssis 2. Vous ne pouvez pas utiliser la mise en grappe si vous installez 1 SM-48 et 2 SM-40 dans le même châssis.
- High Availability (haute disponibilité) : la haute disponibilité est prise en charge uniquement entre les modules de même type sur le périphérique Firepower 9300. Cependant, les deux châssis peuvent comprendre des modules mixtes. Par exemple, chaque châssis a un SM-40, SM-48 et SM-56. Vous pouvez créer des paires à haute disponibilité entre les modules SM-40, entre les modules SM-48 et entre les modules SM-56.
- Types d'applications ASA et Firewall Threat Defense :Vous pouvez installer différents types d'applications sur des modules distincts dans le châssis. Par exemple, vous pouvez installer ASA sur le module 1 et le module 2, et Firewall Threat Defense sur le module 3.
- Versions ASA ou Firewall Threat Defense : vous pouvez exécuter différentes versions d'un type d'instance d'application sur des modules distincts ou en tant qu'instances de conteneur distinctes sur le même module. Par exemple, vous pouvez installer Firewall Threat Defense 6.3 sur le module 1, Firewall Threat Defense 6.4 sur le module 2 et Firewall Threat Defense 6.5 sur le module 3.

Exigences du périphérique Firepower 4100

L'appareil Firepower 4100 est offert en plusieurs modèles. Consultez les exigences suivantes :

- Instances natives et de conteneur : lorsque vous installez une instance de conteneur sur une Firepower 4100, cet appareil ne peut prendre en charge que d'autres instances de conteneur. Une instance native

utilise toutes les ressources d'un périphérique, vous ne pouvez donc installer qu'une seule instance native sur le périphérique.

- Mise en grappe : tous les châssis de la grappe doivent être du même modèle.
- Haute disponibilité : la haute disponibilité est uniquement prise en charge entre les modèles du même type.
- Types d'application ASA et Firewall Threat Defense : Firepower 4100 ne peut exécuter qu'un seul type d'application.

Lignes directrices et limites relatives aux périphériques logiques

Consultez les sections suivantes pour connaître les instructions et les limites.

Lignes directrices et limites des interfaces

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.
- EtherChannels : Pour un EtherChannel, toutes les interfaces 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.

Lignes directrices et limites générales

Mode pare-feu

Vous pouvez définir le mode de pare-feu routé ou transparent dans la configuration de démarrage des Firewall Threat Defense et ASA.

Haute disponibilité

- Configurez la haute disponibilité dans la configuration de l'application.
- Vous pouvez utiliser n'importe quelle interface de données comme liens de basculement et d'état.Les interfaces de partage de données ne sont pas prises en charge.

Mode contexte

- Activez le mode de contexte multiple dans l'ASA après le déploiement.

Exigences et prérequis pour la haute accessibilité

- Les deux unités d'une configuration de basculement à haute accessibilité doivent :
  - Être sur un châssis séparé; la haute accessibilité intra-châssis pour le Firepower 9300 n'est pas prise en charge.
  - être du même modèle.
  - Avoir les mêmes interfaces que celles des périphériques logiques à haute accessibilité.
  - Avoir le même nombre et les mêmes types d'interfaces. Toutes les interfaces doivent être préconfigurées de manière identique dans FXOS avant que vous activiez la haute accessibilité.
- La haute accessibilité est uniquement prise en charge entre les modules de même type sur le Firepower 9300; toutefois, les deux châssis peuvent inclure des modules mixtes. Par exemple, chaque châssis a un SM-56, SM-48 et SM-40. Vous pouvez créer des paires à haute accessibilité entre les modules SM-56, entre les modules SM-48 et entre les modules SM-40.
- Pour les autres exigences du système en matière de haute accessibilité, consultez Configuration système requise pour Failover (basculement).

Interfaces de configuration

Par défaut, les interfaces physiques sont désactivées. Vous pouvez activer les interfaces, ajouter des canaux EtherChannels, et modifier les propriétés de l'interface et .

Remarque Si vous supprimez une interface dans FXOS (p. ex., si vous supprimez un module de réseau, supprimez un canal EtherChannel ou réaffectez une interface à un canal EtherChannel), la configuration ASA conserve les commandes d'origine afin que vous puissiez effectuer les ajustements nécessaires; retirer une interface de la configuration peut avoir des effets considérables. Vous pouvez supprimer manuellement l'ancienne configuration d'interface dans le système d'exploitation ASA.

Configurer une interface physique

Vous pouvez physiquement activer et désactiver les interfaces, ainsi que définir la vitesse d'interface et le mode duplex. Pour utiliser une interface, elle doit être physiquement activée dans FXOS et logiquement activée dans l'application.

Remarque

- Dans le cas de QSFPH40G-CUxM, la négociation automatique est toujours activée par défaut et vous ne pouvez pas la désactiver.
- Si vous remplacez un module SFP sur un port par un module SFP différent, la vitesse, les conditions de duplex et la négociation automatique de l'interface ne sont pas mises à jour automatiquement. Vous devez reconfigurer manuellement l'interface.

Avant de commencer

- Les interfaces qui sont déjà membres d'un EtherChannel ne peuvent pas être modifiées individuellement. Assurez-vous de configurer les paramètres avant de les ajouter au canal EtherChannel.

Procédure

Étape 1 Entrez le mode d'interface.

scope eth-uplink

scope fabric a

Étape 2 Activez l'interface.

enter interface *identifiant_de_l_interface*

enable

Exemple :

```
Firepower /eth-uplink/fabric # enter interface Ethernet1/8
Firepower /eth-uplink/fabric/interface # enable
```

Remarque
Les interfaces qui sont déjà membres d'un canal de port ne peuvent pas être modifiées individuellement. Si vous utilisez la commande **enter interface** ou **scope interface** sur une interface membre d'un canal de port, vous recevrez un message d'erreur indiquant que l'objet n'existe pas. Vous devez modifier les interfaces à l'aide de la commande **enter interface** avant de les ajouter à un canal de port.

Étape 3 (Facultatif) Définir le délai anti-rebond.

set debounce-time 5000 {Enter a value between 0-15000 milli-seconds}

Exemple :

```
Firepower /eth-uplink/fabric/interface # set debounce-time 5000
```

Exemple :

Remarque
La configuration du délai antirebond n'est pas prise en charge sur les interfaces 1G.

Étape 4 (Facultatif) Définissez le type d'interface.

set port-type {**data** | **mgmt** | **cluster**}

Exemple :

```
Firepower /eth-uplink/fabric/interface # set port-type mgmt
```

Le mot clé **data** est le type par défaut. Ne choisissez pas le mot clé **cluster**; par défaut, la liaison de commande de grappe est automatiquement créée sur le canal de port 48.

Étape 5 Activez ou désactivez la négociation automatique, si elle est prise en charge pour votre interface.

set auto-negotiation {**on** | **off**}

Exemple :

```
Firepower /eth-uplink/fabric/interface* # set auto-negotiation off
```

Étape 6 Définissez la vitesse de l'interface.

set admin-speed {**1gbps** | **10gbps** | **40gbps** | **100gbps**}

Exemple :

```
Firepower /eth-uplink/fabric/interface* # set admin-speed 1gbps
```

Étape 7 Définissez le mode duplex de l'interface.

set admin-duplex {**fullduplex** | **halfduplex**}

Exemple :

```
Firepower /eth-uplink/fabric/interface* # set admin-duplex halfduplex
```

Étape 8 Si vous avez modifié la politique de contrôle de flux par défaut, elle est déjà appliquée aux interfaces. Si vous avez créé une nouvelle politique, appliquez-la à l'interface.

set flow-control-policy *name*

Exemple :

```
Firepower /eth-uplink/fabric/interface* # set flow-control-policy flow1
```

Étape 9 Enregistrez la configuration.

commit-buffer

Exemple :

```
Firepower /eth-uplink/fabric/interface* # commit-buffer
Firepower /eth-uplink/fabric/interface #
```

Ajouter un canal EtherChannel (canal de port)

Un EtherChannel (également appelé canal de port) peut inclure jusqu'à 16 interfaces membres de même type de support et de capacité, et doit être réglé à la même vitesse et au même duplex. Le type de support peut être RJ-45 ou SFP. Des SFP de différents types (cuivre et fibre optique) peuvent être mélangés. Vous ne pouvez pas combiner les capacités d'interface (par exemple, interfaces de 1 Go et de 10 Go) en réduisant la vitesse sur l'interface de plus grande capacité. Le protocole LACP (Link Aggregation Control Protocol) agrège les interfaces en échangeant les LACPDU (Link Aggregation Control Protocol Data Unit) entre deux périphériques réseau.

Vous pouvez configurer chaque interface physique de données dans un EtherChannel pour qu'elle soit :

- Actif : envoie et reçoit les mises à jour du protocole LACP. Un EtherChannel actif peut établir une connectivité avec un EtherChannel actif ou passif. Vous devez utiliser le mode actif, sauf si vous devez réduire au minimum le trafic LACP.
- Activé : l'EtherChannel est toujours activé et le protocole LACP n'est pas utilisé. Un EtherChannel « activé » ne peut établir une connexion qu'avec un autre EtherChannel « activé ».

Remarque Cela peut prendre jusqu'à trois minutes à un EtherChannel de revenir à l'état opérationnel si vous faites passer son mode de On (Activé) à Actif ou de Actif à Activé.

Les interfaces sans données ne prennent en charge que le mode actif.

Le protocole LACP coordonne l'ajout et la suppression automatiques des liens vers l'EtherChannel sans l'intervention de l'utilisateur. Il gère également les erreurs de configuration et vérifie que les deux extrémités des interfaces membres sont connectées au groupe de canaux approprié. Le mode « Activé» ne peut pas utiliser les interfaces en veille dans le groupe de canaux lorsqu'une interface tombe en panne et que la connectivité et les configurations ne sont pas vérifiées.

Lorsque Châssis Firepower 4100/9300 crée un EtherChannel, l'EtherChannel reste dans un état **Suspendu** pour le mode LACP actif ou à l'arrêt pour le mode LACP **activé** jusqu'à ce que vous l'affectiez à un périphérique logique, même si le lien physique est actif. L'EtherChannel sortira de l'état **Suspendu** dans les situations suivantes :

- L'EtherChannel est ajouté en tant qu'interface de données ou de gestion pour un périphérique logique autonome
- L'EtherChannel est ajouté en tant qu'interface de gestion ou liaison de commande de grappe pour un périphérique logique qui fait partie d'une grappe
- L'EtherChannel est ajouté en tant qu'interface de données pour un périphérique logique qui fait partie d'une grappe et au moins une unité a rejoint la grappe

Notez que l'EtherChannel ne s'affiche pas tant que vous ne l'avez pas affecté à un périphérique logique. Si l'EtherChannel est retiré de l'unité logique ou si l'unité logique est supprimée, il repasse à l'état **Suspendu** ou **Inactif**.

Procédure

Étape 1 Entrez le mode d'interface.

scope eth-uplink

scope fabric a

Étape 2 Créez le canal de port :

create port-channel *id*

enable

Étape 3 Affectez des interfaces membres :

create member-port *interface_id*

Vous pouvez ajouter jusqu'à 16 interfaces du même type et de la même vitesse. Les interfaces membres doivent être réglées à la même vitesse et au même duplex et doivent correspondre à la vitesse et au duplex que vous avez configurés pour ce canal de port. Le type de support peut être RJ-45 ou SFP. Des SFP de différents types (cuivre et fibre optique) peuvent être mélangés. Vous ne pouvez pas combiner les capacités d'interface (par exemple, interfaces de 1 Go et de 10 Go) en réduisant la vitesse sur l'interface de plus grande capacité.

Exemple :

```
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
```

Étape 4 (Facultatif) Définissez le type d'interface.

set port-type {**data** | **mgmt** | **cluster**}

Exemple :

```
Firepower /eth-uplink/fabric/port-channel # set port-type data
```

Le mot clé **data** est le type par défaut. Ne choisissez pas le mot clé **cluster**, sauf si vous souhaitez utiliser ce canal de port comme liaison de commande de grappe au lieu de la valeur par défaut.

Étape 5 Définissez la vitesse d'interface requise pour les membres du canal de port.

set speed {**10mbps** | **100mbps** | **1gbps** | **10gbps** | **40gbps** | **100gbps**}

Si vous ajoutez une interface membre qui n'a pas la vitesse spécifiée, elle ne pourra pas rejoindre le canal de port. La valeur par défaut est **10gbps**.

Exemple :

```
Firepower /eth-uplink/fabric/port-channel* # set speed 1gbps
```

Étape 6 (Facultatif) Définissez le duplex requis pour les membres du canal de port.

set duplex {**fullduplex** | **halfduplex**}

Si vous ajoutez une interface membre configurée avec le duplex précisé, elle ne rejoindra pas le canal de port. La valeur par défaut est **fullduplex**.

Exemple :

```
Firepower /eth-uplink/fabric/port-channel* # set duplex fullduplex
```

Étape 7 Activez ou désactivez la négociation automatique, si elle est prise en charge pour votre interface.

set auto-negotiation {**on** | **off**}

Exemple :

```
Firepower /eth-uplink/fabric/interface* # set auto-negotiation off
```

Étape 8 Définissez le mode du canal de port LACP pour les interfaces de données.

Pour les interfaces sans données, le mode est toujours actif.

set port-channel-mode {**active** | **on**}

Exemple :

```
Firepower /eth-uplink/fabric/port-channel* # set port-channel-mode on
```

Étape 9 Si vous avez modifié la politique de contrôle de flux par défaut, elle est déjà appliquée aux interfaces. Si vous avez créé une nouvelle politique, appliquez-la à l'interface.

set flow-control-policy *name*

Exemple :

```
Firepower /eth-uplink/fabric/interface* # set flow-control-policy flow1
```

Étape 10 Validez la configuration :

commit-buffer

Configurer les périphériques logiques

Ajoutez un périphérique logique autonome ou une paire à haute disponibilité sur le Châssis Firepower 4100/9300 .

Pour la mise en grappe, consultez #unique_219.

Ajouter un ASA autonome

Les périphériques logiques autonomes fonctionnent seuls ou dans une paire haute disponibilité. Sur Firepower 9300 avec plusieurs modules de sécurité, vous pouvez déployer une grappe ou des appareils autonomes. La grappe doit utiliser tous les modules. Par conséquent, vous ne pouvez pas combiner une grappe à deux modules et un seul périphérique autonome.

Vous pouvez déployer un ASA routé ou transparent en mode pare-feu à partir de Châssis Firepower 4100/9300 .

Pour le mode à contextes multiples, vous devez d'abord déployer le périphérique logique, puis activer le mode à contextes multiples dans l'application ASA.

Avant de commencer

- Téléchargez l'image de l'application que vous souhaitez utiliser pour le périphérique logique à partir de Cisco.com), puis téléchargez cette image sur Châssis Firepower 4100/9300 .

Remarque Pour Firepower 9300, vous pouvez installer différents types d'applications (ASA et Firewall Threat Defense) sur des modules distincts du châssis. Vous pouvez également exécuter différentes versions d'un type d'instance d'application sur des modules distincts.

- Configurez une interface de gestion à utiliser avec le périphérique logique. L'interface de gestion est requise. Notez que cette interface de gestion n'est pas la même que le port de gestion de châssis qui est utilisé uniquement pour la gestion de châssis (dans FXOS, vous pouvez la voir s'afficher comme MGMT, management0 ou autres noms semblables)
- Recueillez les informations suivantes :
  - l'ID d'interface pour ce périphérique
  - l'adresse IP et le masque de réseau de l'interface de gestion
  - Adresse IP de la passerelle

Procédure

Étape 1 Entrez le mode de services de sécurité.

scope ssa

Exemple :

```
Firepower# scope ssa
Firepower /ssa #
```

Étape 2 Définissez la version de l'image de l'instance de l'application.

a) Affichez les images disponibles. Notez le numéro de version que vous souhaitez utiliser.

show app

Exemple :

```
Firepower /ssa # show app
    Name       Version         Author     Supported Deploy Types CSP Type    Is Default
 App
    ---------- --------------- ---------- ---------------------- -----------
--------------
    asa        9.9.1           cisco      Native                 Application No
    asa        9.10.1          cisco      Native                 Application Yes
    ftd        6.2.3           cisco      Native                 Application Yes
```

b) Définissez la portée au niveau du module de sécurité/logement du moteur.

scope slot *slot_id*

L'id *slot_id* est toujours 3 pour la Firepower 4100 et 1, 2 ou 3 pour la Firepower 9300.

Exemple :

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot #
```

c) Créez l'instance d'application.

enter app-instance asa *device_name*

Device_name peut comporter entre 1 et 64 caractères. Vous utiliserez ce nom de périphérique lorsque vous créerez le périphérique logique pour cette instance.

Exemple :

```
Firepower /ssa/slot # enter app-instance asa ASA1
Firepower /ssa/slot/app-instance* #
```

d) Définissez la version de l'image ASA.

set startup-version *version*

Exemple :

```
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
```

e) Quittez pour passer en mode logement.

exit

Exemple :

```
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* #
```

f) Quittez le mode ssa.

exit

Exemple :

```
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

Exemple :

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance asa ASA1
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

Étape 3 Créez le périphérique logique.

enter logical-device *device_name* **asa** *slot_id* **standalone**

Utilisez le même *Device_name* que celui de l'instance d'application que vous avez ajoutée précédemment.

Exemple :

```
Firepower /ssa # enter logical-device ASA1 asa 1 standalone
Firepower /ssa/logical-device* #
```

Étape 4 Attribuez les interfaces de gestion et de données au périphérique logique. Répétez l'opération pour chaque interface.

create external-port-link *name interface_id* **asa**

set description *description*

exit

- *name* : le nom est utilisé par le superviseur Châssis Firepower 4100/9300 . il ne s'agit pas du nom d'interface utilisé dans la configuration de l'ASA.
- *description* : utilisez des guillemets (") autour des expressions avec des espaces.

L'interface de gestion n'est pas la même que le port de gestion du châssis. Vous activerez et configurerez ultérieurement ces interfaces dans l'ASA, y compris la définition des adresses IP.

Exemple :

```
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 asa
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 asa
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 asa
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
```

Étape 5 Configurez les renseignements de démarrage de gestion.

a) Créez l'objet de démarrage.

create mgmt-bootstrap asa

Exemple :

```
Firepower /ssa/logical-device* # create mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

b) Spécifiez le mode de pare-feu, routage ou transparent.

create bootstrap-key FIREWALL_MODE

set value {**routed** | **transparent**}

exit

En mode routage, l'appareil est considéré comme un saut de routeur dans le réseau. Chaque interface par laquelle vous souhaitez acheminer le trafic réseau se trouve sur un sous-réseau différent. Un pare-feu transparent, en revanche, est un pare-feu de couche 2 qui agit comme une « présence sur le réseau câblé » ou un « pare-feu furtif », et qui n'est pas considéré comme un saut de routeur vers les appareils connectés.

Le mode pare-feu est uniquement défini lors du déploiement initial. Si vous appliquez à nouveau les paramètres de démarrage, ce paramètre n'est pas utilisé.

Exemple :

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

c) Spécifiez le mot de passe d'administrateur et d'activation.

create bootstrap-key-secret PASSWORD

set value

Saisissez une valeur *mot de passe*

Confirmez la valeur : *mot de passe*

exit

Exemple :

L'utilisateur admin ASA et le mot de passe d'activation préconfigurés sont utiles pour la récupération du mot de passe. si vous avez un accès FXOS, vous pouvez réinitialiser le mot de passe de l'utilisateur admin en cas d'oubli.

Exemple :

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

d) Configurez les paramètres de l'interface de gestion IPv4.

create ipv4 *slot_id* **default**

set ip *ip_address* **mask** *network_mask*

set gateway *gateway_address*

exit

Exemple :

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.34 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

e) Configurez les paramètres de l'interface de gestion IPv6.

create ipv6 *slot_id* **default**

set ip *ip_address* **prefix-length** *prefix*

set gateway *gateway_address*

exit

Exemple :

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

f) Quittez le mode de démarrage de gestion.

exit

Exemple :

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

Étape 6 Enregistrez la configuration.

commit-buffer

Le châssis déploie le périphérique logique en téléchargeant la version de logiciel spécifiée et en envoyant les paramètres de l'interface de gestion et de configuration du démarrage à l'instance d'application. Vérifiez l'état du déploiement à l'aide de la commande **show app-instance**. L'instance d'application est en cours d'exécution et prête à être utilisée lorsque l'état **Admin State** est **Enabled** (Activé) et que l'état **Oper State** est **Online** (En ligne).

Exemple :

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State      Running Version Startup Version
 Deploy Type Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- ---------------- --------------- ---------------
 ----------- ------------ --------------- ------------
asa        asa1       2          Disabled    Not Installed                    9.12.1
    Native                   Not Applicable  None
ftd        ftd1       1          Enabled     Online           6.4.0.49        6.4.0.49
    Container   Default-Small Not Applicable  None
```

Étape 7 Consultez le guide de configuration ASA pour commencer à configurer votre politique de sécurité.

Exemple

```
Firepower# scope ssa
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance asa MyDevice1
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* # create logical-device MyDevice1 asa 1 standalone
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 asa
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 asa
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 asa
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value transparent
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: secretglassine
Confirm the value: secretglassine
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.31 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # commit-buffer
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key #
```

Ajouter une paire à haute disponibilité

La haute disponibilité Firewall Threat DefenseASA (également appelée basculement) est configurée dans l'application, pas dans FXOS. Toutefois, pour préparer votre châssis à la haute disponibilité, consultez les étapes suivantes.

Avant de commencer

Consultez la section Configuration système requise pour Failover (basculement).

Procédure

Étape 1 Attribuez les mêmes interfaces à chaque périphérique logique.

Étape 2 Attribuez une ou deux interfaces de données au basculement et à l'état des liens.

Ces interfaces échangent le trafic à haute disponibilité entre les deux châssis. Nous vous recommandons d'utiliser une interface de données de 10 Go pour un basculement et une liaison d'état combinés. Si vous avez des interfaces disponibles, vous pouvez utiliser des liaisons de basculement et d'état distincts; le lien d'état nécessite le plus de bande passante. Vous ne pouvez pas utiliser l'interface de type de gestion pour la liaison

de basculement ou d'état. Nous vous recommandons d'utiliser un commutateur entre les châssis, afin qu'aucun autre périphérique ne se trouve sur le même segment de réseau que les interfaces de basculement.

Étape 3 Activez la haute disponibilité sur les périphériques logiques. Consultez Basculement pour la haute disponibilité.

Étape 4 Si vous modifiez les interfaces après avoir activé la haute disponibilité, modifiez l'interface dans FXOS sur l'unité en veille, puis apportez les mêmes modifications à l'unité active.

Remarque
Dans le cas de l'ASA, si vous supprimez une interface dans FXOS (p. ex., si vous supprimez un module de réseau, supprimez un canal EtherChannel ou réaffectez une interface à un canal EtherChannel), la configuration ASA conserve les commandes d'origine afin que vous puissiez effectuer les ajustements nécessaires; retirer une interface de la configuration peut avoir des effets considérables. Vous pouvez supprimer manuellement l'ancienne configuration d'interface dans le système d'exploitation de l'ASA.

Modifier une interface sur un périphérique logique ASA

Vous pouvez allouer, annuler l'allocation ou remplacer une interface de gestion sur un périphérique logique ASA. ASDM détecte automatiquement les nouvelles interfaces.

L'ajout d'une nouvelle interface ou la suppression d'une interface inutilisée a une incidence minime sur la configuration de l'ASA. Cependant, si vous supprimez une interface allouée dans FXOS (par exemple, si vous supprimez un module de réseau, supprimez un EtherChannel ou réaffectez une interface allouée à un EtherChannel) et que l'interface est utilisée dans votre politique de sécurité, la suppression aura une incidence sur la configuration de l'ASA. Dans ce cas, la configuration de l'ASA conserve les commandes d'origine afin que vous puissiez apporter les ajustements nécessaires. Vous pouvez supprimer manuellement l'ancienne configuration d'interface dans le système d'exploitation de l'ASA.

Remarque Vous pouvez modifier les membres d'un EtherChannel alloué sans affecter le périphérique logique.

Avant de commencer

- Configurez vos interfaces et ajoutez tous les EtherChannels en fonction de Configurer une interface physique, à la page 7 et Ajouter un canal EtherChannel (canal de port), à la page 9.
- Si vous souhaitez ajouter une interface déjà allouée à un EtherChannel (par exemple, toutes les interfaces sont allouées par défaut à une grappe), vous devez d'abord désallouer l'interface du périphérique logique, puis ajouter l'interface à l'EtherChannel. Pour un nouvel EtherChannel, vous pouvez ensuite l'affecter au périphérique.
- Pour la mise en grappe ou le basculement, assurez-vous d'ajouter ou de supprimer l'interface sur toutes les unités. Nous vous recommandons d'effectuer les modifications d'interface d'abord sur l'unité de données ou de secours, puis sur l'unité de contrôle ou l'unité active. Les nouvelles interfaces sont ajoutées dans un état administrativement inactif, de sorte qu'elles n'affectent pas la supervision des interfaces.

Procédure

Étape 1 Entrez le mode de services de sécurité :

Firepower# **scope ssa**

Étape 2 Modifiez le périphérique logique :

Firepower /ssa # **scope logical-device** *device_name*

Étape 3 Annulez l'allocation d'une interface du périphérique logique :

Firepower /ssa/logical-device # **delete external-port-link** *name*

Saisissez la commande **show external-port-link** pour afficher les noms d'interface.

Pour une interface de gestion, supprimez l'interface actuelle, puis validez votre modification à l'aide de la commande **commit-buffer** avant d'ajouter la nouvelle interface de gestion.

Étape 4 Attribuez une nouvelle interface à l'unité logique :

Firepower /ssa/logical-device* # **create external-port-link** *name interface_id* **asa**

Étape 5 Validez la configuration :

commit-buffer

Validez la transaction dans la configuration système.

Se connecter à la console de l'application

Suivez la procédure ci-dessous pour vous connecter à la console de l'application.

Procédure

Étape 1 Connectez-vous à l'interface de ligne de commande du module à l'aide d'une connexion de console ou d'une connexion Telnet.

connect module *slot_number* {**console** | **telnet**}

Pour vous connecter au moteur de sécurité d'un périphérique qui ne prend pas en charge plusieurs modules de sécurité, utilisez toujours **1** comme *slot_number*.

Les avantages de l'utilisation d'une connexion Telnet sont que vous pouvez avoir plusieurs sessions sur le module en même temps et que la vitesse de connexion est plus rapide.

Exemple :

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
```

```
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

Étape 2 Connectez-vous à la console d'application.

connect asa *name*

Pour afficher les noms des instances, entrez la commande sans nom.

Exemple :

```
Firepower-module1> connect asa asa1
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

Étape 3 Quittez la console d'application pour accéder à l'interface de ligne de commande du module FXOS.

- ASA : Saisissez **Ctrl-a, d**

Étape 4 Revenez au niveau de superviseur du Interface de ligne de commande FXOS.

Quittez la console :

a) Entrez **~**

Vous quittez l'application Telnet.

b) Pour quitter l'application Telnet, entrez :

telnet>**quit**

Quittez la session Telnet :

a) Entrez **Ctrl-], .**

Exemple

Dans l'exemple suivant, une connexion est établie à un ASA sur le module de sécurité 1, puis retourne au niveau de superviseur du Interface de ligne de commande FXOS.

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect asa asa1
asa> ~
telnet> quit
```

```
Connection closed.
Firepower#
```

Historique des périphériques logiques

Fonctionnalités	Version	Détails
ASA pour le Firepower 4112	9.14(1)	Nous avons lancé le Firepower 4112. **Remarque** FXOS 2.8.1 est nécessaire.
Prise en charge du Firepower 9300 SM-56	9.12.2	Nous avons lancé le module de sécurité SM-56. **Remarque** FXOS 2.6.1.157 est nécessaire.
ASA pour les Firepower 4115, 4125 et 4145	9.12(1)	Nous avons lancé les Firepower 4115, 4125 et 4145. **Remarque** FXOS 2.6.1 est nécessaire.
Prise en charge des Firepower 9300 SM-40 et SM-48	9.12.1	Nous avons lancé les modules de sécurité SM-40 et SM-48. **Remarque** FXOS 2.6.1 est nécessaire.
Prise en charge d'ASA et de Firewall Threat Defense sur des modules distincts du même Firepower 9300	9.12.1	Vous pouvez maintenant déployer ASA et des périphériques logiques Firewall Threat Defense sur le même Firepower 9300. **Remarque** FXOS 2.6.1 est nécessaire.
Adresse IP personnalisable par liaison de commande de grappe pour le Firepower 4100/9300	9.10.1	Par défaut, la liaison de commande de grappe utilise le réseau 127.2.0.0/16. Vous pouvez maintenant définir le réseau lorsque vous déployez la grappe dans FXOS. Le châssis génère automatiquement l'adresse IP de l'interface de liaison de commande de grappe pour chaque unité en fonction de l'ID du châssis et de l'ID d'emplacement : 127.2.*chassis_id*.*slot_id*. Cependant, certains déploiements réseau ne permettent pas le passage du trafic 127.2.0.0/16. Par conséquent, vous pouvez maintenant définir un sous-réseau personnalisé /16 pour la liaison de commande de grappe dans FXOS, à l'exception des adresses de boucle avec retour (127.0.0.0/8) et de multidiffusion (224.0.0.0/4). **Remarque** FXOS 2.4.1 est nécessaire. Commandes FXOS nouvelles ou modifiées : **set cluster-control-link network**

Fonctionnalités	Version	Détails
Prise en charge des données EtherChannels en mode activé	9.10.1	Vous pouvez maintenant définir les données et les EtherChannels de partage de données en mode LACP actif ou en mode Activé. Les autres types d'EtherChannels ne prennent en charge que le mod actif. **Remarque** FXOS 2.4.1 est nécessaire. Commandes FXOS nouvelles ou modifiées : **set port-channel-mode**
Amélioration de la mise en grappe inter-sites pour l'ASA sur le Châssis Firepower 4100/9300	9.7(1)	Vous pouvez maintenant configurer l'ID de site pour chaque Châssis Firepower 4100/9300 lorsque vous déployez la grappe ASA. Auparavant, vous deviez configurer l'ID de site dans l'application ASA cette nouvelle fonctionnalité facilite le déploiement initial. Notez que vous ne pouvez plus définir l'I de site dans la configuration ASA. En outre, pour une meilleure compatibilité avec la mise en grapp inter-sites, nous vous recommandons de mettre à niveau vers ASA 9.7(1) et FXOS 2.1.1, ce qui compren plusieurs améliorations de la stabilité et des performances. Nous avons modifié la commande suivante : **site-id**
Prise en charge de Firepower 4100	9.6(1)	Avec FXOS 1.1.4, l'ASA prend en charge la mise en grappe inter-châssis sur le Firepower 4100. Nous n'avons pas modifié de commandes.
Mise en grappe inter-châssis pour 6 modules et mise en grappe inter-sites pour l'application ASA Firepower 9300	9.5(2.1)	Grâce à FXOS 1.1.3, vous pouvez désormais activer la mise en grappe inter-châssis et par extension inter-sites. Vous pouvez inclure jusqu'à 6 modules dans un maximum de 6 châssis. Nous n'avons pas modifié de commandes.
Mise en grappe d'ASA intra-châssis pour le Firepower 9300	9.4(1.150)	Vous pouvez mettre en grappe jusqu'à 3 modules de sécurité dans le châssis Firepower 9300. Tous le modules dans le châssis doivent appartenir à la grappe. Nous avons introduit les commandes suivantes : **cluster replication delay, debug service-module, management-only individual, show cluster chassis**

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.