Périphériques logiques sur le Firepower 4100/9300

Firepower 4100/9300 est une plateforme de sécurité flexible sur laquelle vous pouvez installer un ou plusieurs *périphériques logiques*. Avant de pouvoir ajouter défense contre les menaces au centre de gestion, vous devez configurer les interfaces de châssis, ajouter un périphérique logique et affecter des interfaces au périphérique sur le châssis Firepower 4100/9300 à l'aide de la commande Cisco Secure Firewall chassis manager ou de la CLI FXOS. Ce chapitre décrit la configuration de l'interface de base et comment ajouter un périphérique logique autonome ou à haute disponibilité à l'aide de Cisco Secure Firewall chassis manager. 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, les sous-interfaces VLAN pour les instances de conteneurs 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 gestionnaire de châssis. Cette interface apparaît en haut de l'onglet **Interfaces** en tant que **MGMT**, et vous ne pouvez activer ou désactiver cette interface que dans l'onglet **Interfaces**. 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.

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

Types d'interface

Les interfaces physiques, les sous-interfaces VLAN pour les instances de conteneur 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 (Défense contre les menaces-utilisant-centre de gestion seulement). Chaque instance de conteneur peut communiquer sur le fond de panier avec toutes les autres instances qui partagent cette interface. Les interfaces partagées peuvent avoir une incidence sur le nombre d'instances de conteneur que vous pouvez déployer. Les interfaces partagées ne sont pas prises en charge pour les interfaces de membre de groupe de ponts (en mode transparent ou en mode routage), les ensembles en ligne, les interfaces passives, les grappes, ou les liens de basculement.
- 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 Défense contre les menaces-using- (en usage)centre de gestion. Pour utiliser cette interface, vous devez configurer son adresse IP et d'autres paramètres au niveau de l'interface de ligne de commande Défense contre les menaces. Par exemple, vous pouvez séparer le trafic de gestion des événements (comme les événements Web). Reportez-vous au guide de configuration du centre de gestion pour obtenir plus de renseignements. Les interfaces d'événements peuvent être partagées par un ou plusieurs dispositifs logiques pour accéder à des hôtes externes. Les dispositifs logiques ne peuvent pas communiquer sur cette interface avec d'autres

dispositifs logiques qui partagent l'interface. Si vous configurez ultérieurement une interface de données pour la gestion, vous ne pouvez pas utiliser une interface d'événement distincte.

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. Pour la mise en grappe multi-instances, vous ne pouvez pas partager une interface de type grappe sur plusieurs appareils. Vous pouvez ajouter des sous-interfaces VLAN à la grappe EtherChannel pour fournir des liaisons de commande de grappe distinctes par grappe. Si vous ajoutez des sous-interfaces à une interface Cluster, vous ne pouvez pas utiliser cette interface pour une grappe native. Le gestionnaire d'appareil et CDO ne prend pas en charge le regroupement (clustering).

Remarque Ce chapitre traite uniquement des sous-interfaces du VLAN *FXOS*. Vous pouvez créer séparément des sous-interfaces dans l'application défense contre les menaces . Consultez Interfaces FXOS par rapport aux interfaces d'application, à la page 4 pour obtenir de plus amples renseignements.

Reportez-vous à la table suivante pour la prise en charge des types d'interface pour les demandes défense contre les menaces 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
Défense contre les menaces	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, les sous-interfaces VLAN pour les instances de conteneur 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.

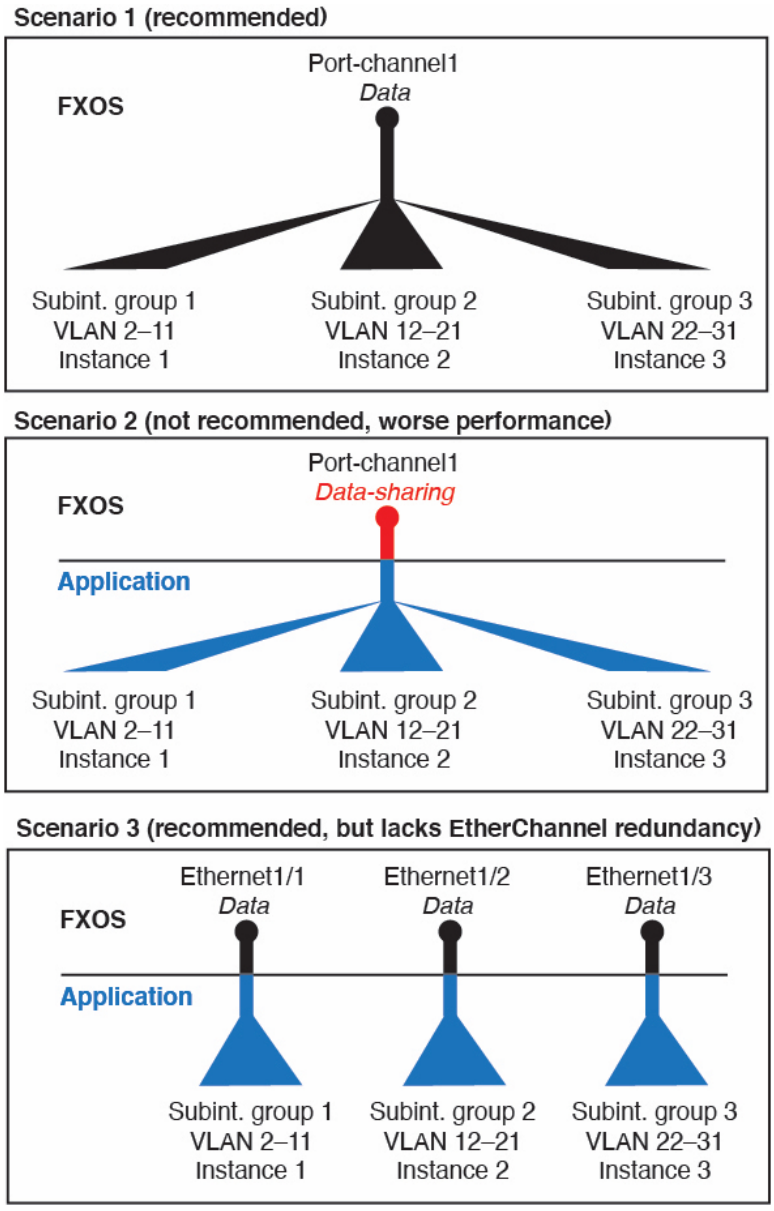
Les sections suivantes décrivent l'interaction entre FXOS et l'application pour les interfaces.

Sous-interfaces VLAN

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

Pour les instances de conteneur en mode autonome uniquement, vous pouvez *également* créer des sous-interfaces VLAN dans FXOS. Les grappes à plusieurs instances ne prennent pas en charge les sous-interfaces dans FXOS, sauf sur l'interface de type grappe. Les sous-interfaces définies par l'application ne sont pas soumises à la limite FXOS. Le choix du système d'exploitation pour la création des sous-interfaces dépend de votre déploiement réseau et de vos préférences personnelles. Par exemple, pour partager une sous-interface, vous devez créer la sous-interface dans FXOS. Un autre scénario qui favorise les sous-interfaces FXOS consiste à allouer des groupes de sous-interfaces distincts sur une seule interface à plusieurs instances. Par exemple, vous souhaitez utiliser le canal de port 1 avec le VLAN 2 à 11 sur l'instance A, le VLAN 12 à 21 sur l'instance B et le VLAN 22 à 31 sur l'instance C. Si vous créez ces sous-interfaces dans l'application, vous devrez partager l'interface parente dans FXOS, ce qui n'est peut-être pas souhaitable. Consultez l'illustration suivante qui présente les trois façons de réaliser ce scénario :

Illustration 1 : VLAN dans FXOS par rapport à l'application pour les instances de conteneur



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.

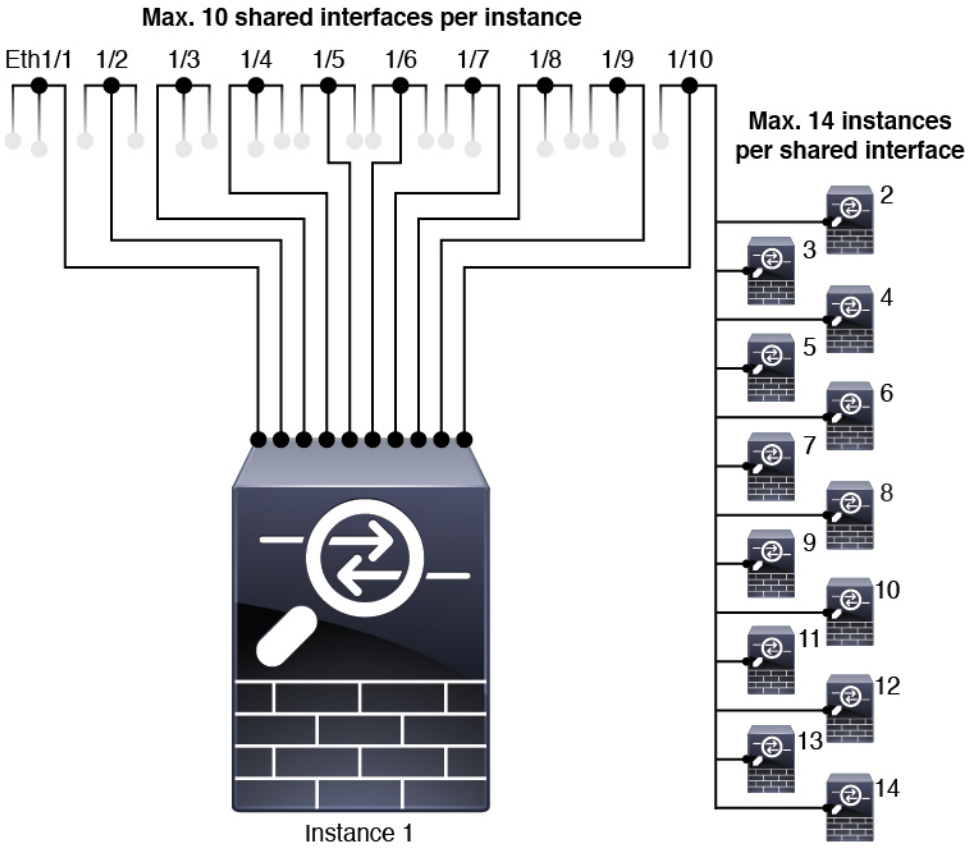
L'état par défaut d'une interface dans l'application dépend du type d'interface. Par exemple, l'interface physique ou EtherChannel est désactivée par défaut dans l'application, mais une sous-interface est activée par défaut.

Évolutivité de l'interface partagée

Les instances peuvent partager des interfaces de type partage de données. Cette fonctionnalité vous permet d'économiser l'utilisation de l'interface physique et de prendre en charge des déploiements réseau flexibles. Lorsque vous partagez une interface, le châssis utilise des adresses MAC uniques pour transférer le trafic vers la bonne instance. Cependant, les interfaces partagées peuvent faire grossir la table de transfert en raison de la nécessité d'une topologie de maillage complet dans le châssis (chaque instance doit pouvoir communiquer avec toutes les autres instances qui partagent la même interface). Par conséquent, il y a des limites au nombre d'interfaces que vous pouvez partager.

En plus du tableau de transfert, le châssis gère un tableau de groupes VLAN pour le transfert de la sous-interface VLAN. Vous pouvez créer jusqu'à 500 sous-interfaces VLAN.

Consultez les limites suivantes pour l'attribution d'interface partagée :



Bonnes pratiques en matière d'interface partagée

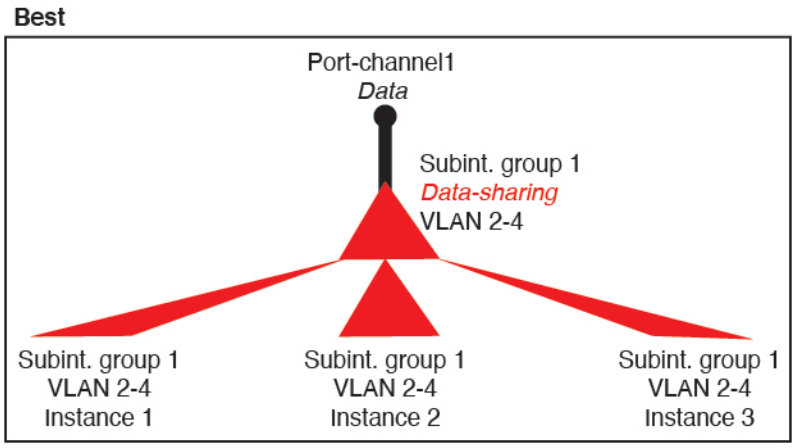
Pour une évolutivité optimale de la table de transfert, partagez le moins d'interfaces possible. Au lieu de cela, vous pouvez créer jusqu'à 500 sous-interfaces VLAN sur une ou plusieurs interfaces physiques, puis diviser les VLAN entre les instances de conteneur.

Lorsque vous partagez des interfaces, suivez ces pratiques dans l'ordre de la plus évolutive vers la moins évolutive :

1. Idéal : Partagez les sous-interfaces sous un parent unique et utilisez le même ensemble de sous-interfaces avec le même groupe d'instances.

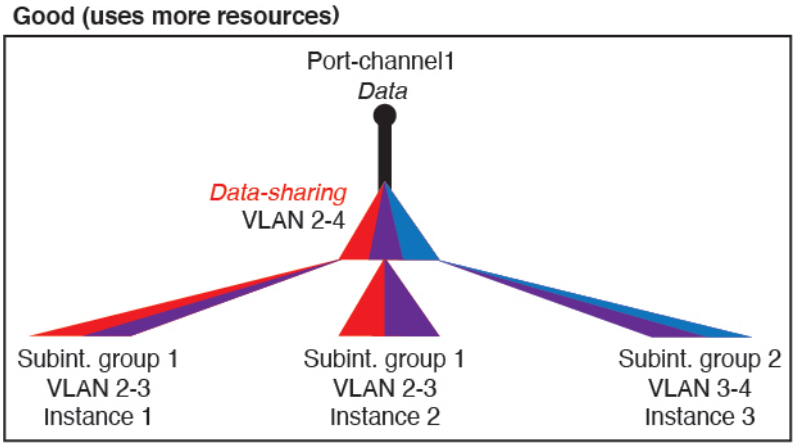
Par exemple, créez un grand EtherChannel pour regrouper toutes vos interfaces de même type, puis partagez les sous-interfaces de cet EtherChannel : Port-Channel1.2, 3 et 4 au lieu de Port-Channel2, Port-Channel3 et Port-Channel4 . Lorsque vous partagez des sous-interfaces d'un parent unique, la table de groupes VLAN offre une meilleure évolutivité de la table de transfert que lors du partage d'interfaces ou de sous-interfaces physiques/EtherChannel entre parents.

Illustration 2 : Excellent : groupe de sous-interface partagé sur un parent unique



Si vous ne partagez pas le même ensemble de sous-interfaces avec un groupe d'instances, votre configuration peut entraîner une utilisation plus importante des ressources (plus de groupes VLAN). Par exemple, partagez les canaux de ports 1.2, 3 et 4 avec les instances 1, 2 et 3 (un groupe VLAN) au lieu de partager les canaux de ports 1.2 et 3 avec les instances 1 et 2, lors du partage du canal de ports 1.3. et 4 avec l'instance 3 (deux groupes VLAN).

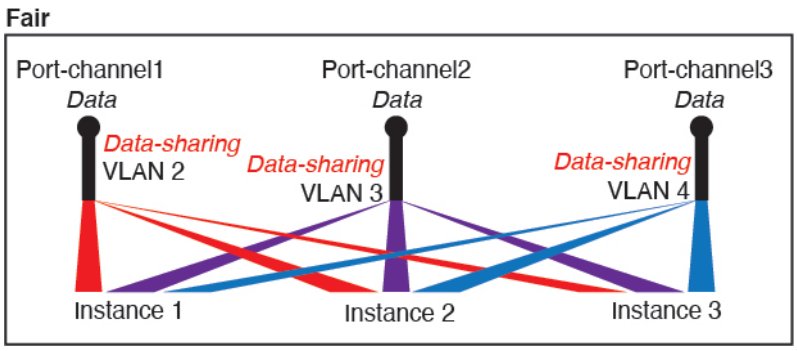
Illustration 3 : Bon : partage de plusieurs groupes de sous-interfaces sur un parent



2. Passable : partagez les sous-interfaces entre les parents.

   Par exemple, partagez Port-Channel1.2, Port-Channel2.3 et Port-Channel3.4 au lieu de Port-Channel2, Port-Channel4 et Port-Channel4. Bien que cette utilisation ne soit pas aussi efficace que le partage uniquement des sous-interfaces sur un même parent, elle profite tout de même des groupes VLAN.

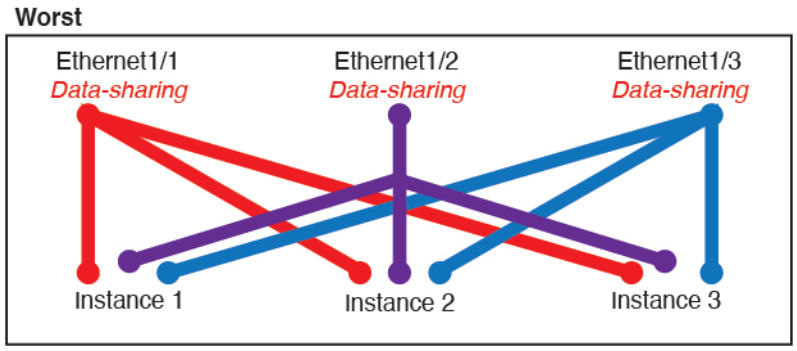
Illustration 4 : Passable : sous-interfaces partagées sur des parents distincts



3. Pire : partagez des interfaces parentes individuelles (physique ou EtherChannel).

   Cette méthode utilise le plus grand nombre d'entrées de tableau de transfert.

Illustration 5 : Pire : interfaces parentes partagées



Exemples d'utilisation de l'interface partagée

Consultez les tableaux suivants pour voir des exemples de partage et d'évolutivité d'interface. Les scénarios ci-dessous supposent l'utilisation d'une interface physique/EtherChannel pour la gestion partagée sur toutes les instances, et d'une autre interface physique ou EtherChannel avec des sous-interfaces dédiées pour une utilisation avec la haute disponibilité.

- Tableau 2 : Interfaces et instances physiques/EtherChannel sur un Firepower 9300 avec trois SM-44, à la page 10
- Tableau 3 : Sous-interfaces sur le parent unique et les instances sur un Firepower 9300 avec trois SM-44, à la page 12
- Tableau 4 : Interfaces et instances physiques/EtherChannel sur un Firepower 9300 avec un SM-44, à la page 13
- Tableau 5 : Sous-interfaces sur le parent unique et instances sur un Firepower 9300 avec un SM-44, à la page 15

Firepower 9300 avec trois SM-44

Le tableau suivant s'applique à trois modules de sécurité SM-44 sur un périphérique 9300 utilisant uniquement des interfaces physiques ou des EtherChannels. Sans sous-interfaces, le nombre maximal d'interfaces est limité. De plus, le partage de plusieurs interfaces physiques utilise plus de ressources de la table de transfert que le partage de plusieurs sous-interfaces.

Chaque module SM-44 peut prendre en charge jusqu'à 14 instances. Les instances sont réparties entre les modules selon les besoins pour rester dans les limites.

Tableau 2 : Interfaces et instances physiques/EtherChannel sur un Firepower 9300 avec trois SM-44

Interfaces dédiées	Interfaces partagées	Nombre d'instances	% tableau de transfert utilisé
32 : • 8 • 8 • 8 • 8	**0**	**4 :** • Instance 1 • Instance 2 • Instance 3 • Instance 4	16 %
30 : • 15 • 15	**0**	**2 :** • Instance 1 • Instance 2	14 %
14 : • 14 (1 de chaque)	**1**	**14 :** • Instance 1 à Instance 14	46 %
33 : • 11 (1 de chaque) • 11 (1 de chaque) • 11 (1 de chaque)	**3 :** • 1 • 1 • 1	**33 :** • Instance 1 à Instance 11 • Instance 12 à Instance 22 • Instance 23 à Instance 33	98 %
33 : • *11 (1 de chaque)* • *11 (1 de chaque)* • *12 (1 de chaque)*	***3 :*** • *1* • *1* • *1*	***34 :*** • *Instance 1 à Instance 11* • *Instance 12 à Instance 22* • *Instance 23 à Instance 34*	*102 %* NON AUTORISÉ

Interfaces dédiées	Interfaces partagées	Nombre d'instances	% tableau de transfert utilisé
30 : • 30 (1 de chaque)	**1**	**6 :** • Instance 1 à Instance 6	25 %
30 : • 10 (5 de chaque) • 10 (5 de chaque) • 10 (5 de chaque)	**3 :** • 1 • 1 • 1	**6 :** • Instance 1 à Instance 2 • Instance 2 : Instance 4 • Instance 5 : Instance 6	23 %
30 : • 30 (6 de chaque)	**2**	**5 :** • Instance 1 à Instance 5	28 %
30 : • 12 (6 de chaque) • 18 (6 de chaque)	**4 :** • 2 • 2	**5 :** • Instance 1 à Instance 2 • Instance 2 : Instance 5	26 %
24 : • 6 • 6 • 6 • 6	**7**	**4 :** • Instance 1 • Instance 2 • Instance 3 • Instance 4	44 %
24 : • 12 (6 de chaque) • 12 (6 de chaque)	**14 :** • 7 • 7	**4 :** • Instance 1 à Instance 2 • Instance 2 : Instance 4	41 %

Le tableau suivant s'applique à trois modules de sécurité SM-44 sur un 9300 qui utilise des sous-interfaces sur une interface physique parente unique. Par exemple, créez un grand EtherChannel pour regrouper toutes vos interfaces de même type, puis partagez les sous-interfaces de cet EtherChannel. Le partage de plusieurs interfaces physiques utilise plus de ressources de la table de transfert que le partage de plusieurs sous-interfaces.

Chaque module SM-44 peut prendre en charge jusqu'à 14 instances. Les instances sont réparties entre les modules selon les besoins pour rester dans les limites.

Tableau 3 : Sous-interfaces sur le parent unique et les instances sur un Firepower 9300 avec trois SM-44

Sous-interfaces dédiées	Sous-interfaces partagées	Nombre d'instances	% tableau de transfert utilisé
168 : • 168 (4 de chaque)	**0**	**42 :** • Instance 1 à Instance 42	33 %
224 : • 224 (16 de chaque)	**0**	**14 :** • Instance 1 à Instance 14	27 %
14 : • 14 (1 de chaque)	**1**	**14 :** • Instance 1 à Instance 14	46 %
33 : • 11 (1 de chaque) • 11 (1 de chaque) • 11 (1 de chaque)	**3 :** • 1 • 1 • 1	**33 :** • Instance 1 à Instance 11 • Instance 12 à Instance 22 • Instance 23 à Instance 33	98 %
70 : • 70 (5 de chaque)	**1**	**14 :** • Instance 1 à Instance 14	46 %
165 : • 55 (5 de chaque) • 55 (5 de chaque) • 55 (5 de chaque)	**3 :** • 1 • 1 • 1	**33 :** • Instance 1 à Instance 11 • Instance 12 à Instance 22 • Instance 23 à Instance 33	98 %
70 : • 70 (5 de chaque)	**2**	**14 :** • Instance 1 à Instance 14	46 %

Sous-interfaces dédiées	Sous-interfaces partagées	Nombre d'instances	% tableau de transfert utilisé
165 : • 55 (5 de chaque) • 55 (5 de chaque) • 55 (5 de chaque)	**6 :** • 2 • 2 • 2	**33 :** • Instance 1 à Instance 11 • Instance 12 à Instance 22 • Instance 23 à Instance 33	98 %
70 : • 70 (5 de chaque)	**10**	**14 :** • Instance 1 à Instance 14	46 %
165 : • *55 (5 de chaque)* • *55 (5 de chaque)* • *55 (5 de chaque)*	***30 :*** • *10* • *10* • *10*	***33 :*** • *Instance 1 à Instance 11* • *Instance 12 à Instance 22* • *Instance 23 à Instance 33*	*102 %* NON AUTORISÉ

Firepower 9300 avec un SM-44

Le tableau suivant s'applique au périphérique Firepower 9300 avec un SM-44 et utilise uniquement des interfaces physiques ou des EtherChannels. Sans sous-interfaces, le nombre maximal d'interfaces est limité. De plus, le partage de plusieurs interfaces physiques utilise plus de ressources de la table de transfert que le partage de plusieurs sous-interfaces.

L'appareil Firepower 9300 avec un SM-44 peut prendre en charge jusqu'à 14 instances.

Tableau 4 : Interfaces et instances physiques/EtherChannel sur un Firepower 9300 avec un SM-44

Interfaces dédiées	Interfaces partagées	Nombre d'instances	% tableau de transfert utilisé
32 : • 8 • 8 • 8 • 8	**0**	**4 :** • Instance 1 • Instance 2 • Instance 3 • Instance 4	16 %

Interfaces dédiées	Interfaces partagées	Nombre d'instances	% tableau de transfert utilisé
30 : • 15 • 15	**0**	**2 :** • Instance 1 • Instance 2	14 %
14 : • 14 (1 de chaque)	**1**	**14 :** • Instance 1 à Instance 14	46 %
14 : • 7 (1 de chaque) • 7 (1 de chaque)	**2 :** • **1** • **1**	**14 :** • Instance 1 à Instance 7 • Instance 8 à Instance 14	37 %
32 : • 8 • 8 • 8 • 8	**1**	**4 :** • Instance 1 • Instance 2 • Instance 3 • Instance 4	21 %
32 : • 16 (8 de chaque) • 16 (8 de chaque)	**2**	**4 :** • Instance 1 à Instance 2 • Instance 3 : Instance 4	20 %
32 : • 8 • 8 • 8 • 8	**2**	**4 :** • Instance 1 • Instance 2 • Instance 3 • Instance 4	25 %
32 : • 16 (8 de chaque) • 16 (8 de chaque)	**4 :** • 2 • 2	**4 :** • Instance 1 à Instance 2 • Instance 3 : Instance 4	24 %

Interfaces dédiées	Interfaces partagées	Nombre d'instances	% tableau de transfert utilisé
24 : • 8 • 8 • 8	**8**	**3 :** • Instance 1 • Instance 2 • Instance 3	37 %
10 : • 10 (2 de chaque)	**10**	**5 :** • Instance 1 à Instance 5	69 %
10 : • 6 (2 de chaque) • 4 (2 de chaque)	**20 :** • 10 • 10	**5 :** • Instance 1 à Instance 3 • Instance 4, instance 5	59 %
14 : • *12 (2 de chaque)*	***10***	***7 :*** • *Instance 1 à Instance 7*	*109 %* NON AUTORISÉ

Le tableau suivant s'applique au périphérique Firepower 9300 avec un sous-interface SM-44 using sur une interface physique parente unique. Par exemple, créez un grand EtherChannel pour regrouper toutes vos interfaces de même type, puis partagez les sous-interfaces de cet EtherChannel. Le partage de plusieurs interfaces physiques utilise plus de ressources de la table de transfert que le partage de plusieurs sous-interfaces.

L'appareil Firepower 9300 avec un SM-44 peut prendre en charge jusqu'à 14 instances.

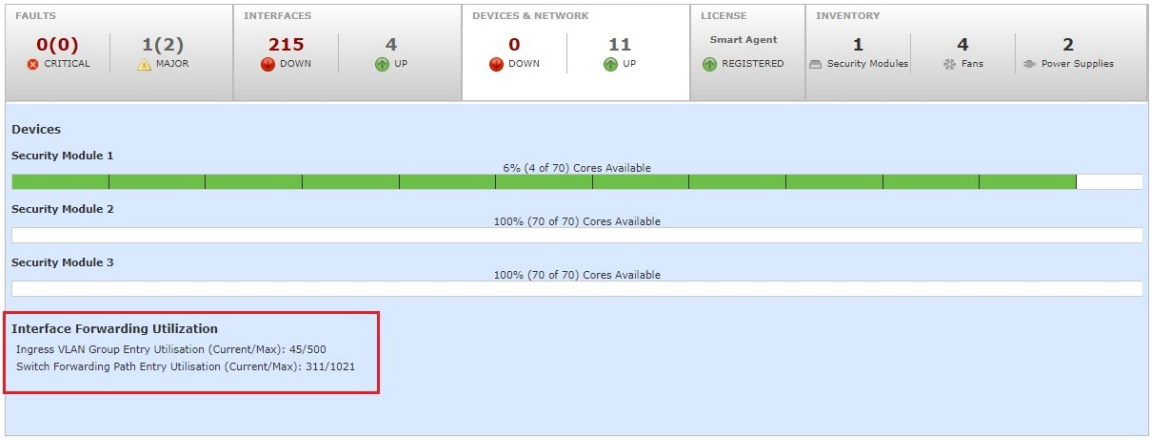
Tableau 5 : Sous-interfaces sur le parent unique et instances sur un Firepower 9300 avec un SM-44

Sous-interfaces dédiées	Sous-interfaces partagées	Nombre d'instances	% tableau de transfert utilisé
112 : • 112 (8 de chaque)	**0**	**14 :** • Instance 1 à Instance 14	17 %
224 : • 224 (16 de chaque)	**0**	**14 :** • Instance 1 à Instance 14	17 %
14 : • 14 (1 de chaque)	**1**	**14 :** • Instance 1 à Instance 14	46 %

Sous-interfaces dédiées	Sous-interfaces partagées	Nombre d'instances	% tableau de transfert utilisé
14 : • 7 (1 de chaque) • 7 (1 de chaque)	**2 :** • 1 • 1	**14 :** • Instance 1 à Instance 7 • Instance 8 à Instance 14	37 %
112 : • 112 (8 de chaque)	**1**	**14 :** • Instance 1 à Instance 14	46 %
112 : • 56 (8 de chaque) • 56 (8 de chaque)	**2 :** • 1 • 1	**14 :** • Instance 1 à Instance 7 • Instance 8 à Instance 14	37 %
112 : • 112 (8 de chaque)	**2**	**14 :** • Instance 1 à Instance 14	46 %
112 : • 56 (8 de chaque) • 56 (8 de chaque)	**4 :** • 2 • 2	**14 :** • Instance 1 à Instance 7 • Instance 8 à Instance 14	37 %
140 : • 140 (10 de chaque)	**10**	**14 :** • Instance 1 à Instance 14	46 %
140 : • 70 (10 de chaque) • 70 (10 de chaque)	**20 :** • 10 • 10	**14 :** • Instance 1 à Instance 7 • Instance 8 à Instance 14	37 %

Affichage des ressources de l'interface partagée

Pour afficher le tableau de transfert et l'utilisation de groupes VLAN, consultez la **Devices and Network** > **Interface Forwarding Utilization** (Périphériques et réseaux > utilisation de l'interface de transfert d'instances),. Par exemple :



Propagation de l'état du lien d'ensemble en ligne pour Défense contre les menaces

Un ensemble en ligne agit comme une bulle sur le câble et lie deux interfaces ensemble pour s'insérer dans un réseau existant. Cette fonction permet d'installer le système dans n'importe quel environnement réseau sans la configuration de périphériques réseau adjacents. Les interfaces passives reçoivent tout le trafic sans condition et aucun trafic reçu sur ces interfaces n'est retransmis.

Lorsque vous configurez un ensemble en ligne dans l'application Défense contre les menaces et activez la propagation de l'état de la liaison, Défense contre les menaces envoie l'appartenance à l'ensemble en ligne au châssis FXOS. La propagation de l'état de la liaison signifie que le châssis met automatiquement hors service la deuxième interface de la paire d'interfaces en ligne lorsque l'une des interfaces d'un ensemble en ligne tombe en panne. Lorsque l'interface en panne est relancée, la deuxième interface est automatiquement relancée. En d'autres termes, si l'état de liaison d'une interface change, le châssis détecte le changement et met à jour l'état de liaison de l'autre interface pour qu'il corresponde au changement. Vous observerez que les périphériques nécessitent jusqu'à 4 secondes pour propager les changements d'état de liaison. La propagation de l'état de liaison est particulièrement utile dans les environnements de réseau résilients où les routeurs sont configurés pour rediriger automatiquement le trafic autour des périphériques réseau en état de défaillance.

Remarque Ne pas activer Hardware Bypass et Propager l'état du lien pour le même ensemble en ligne.

À propos des périphériques logiques

Un périphérique logique vous permet d'exécuter une instance d'application (ASA ou Défense contre les menaces) 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 Défense contre les menaces) 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. gestionnaire d'appareil ne prend pas en charge la mise en grappe.

Instances d'application du périphérique logique : instance de conteneur et instance native

Les instances d'application du périphérique logique s'exécutent dans les types de déploiement suivants :

- Instance native : une instance native utilise toutes les ressources (CPU, RAM et espace disque) du module/moteur de sécurité, de sorte que vous ne pouvez installer qu'une seule instance native.
- Instance de conteneur : une instance de conteneur utilise un sous-ensemble de ressources du module/moteur de sécurité, de sorte que vous pouvez installer plusieurs instances de conteneur. La capacité multi-instances n'est prise en charge que pour les Défense contre les menaces utilisant centre de gestion; il n'est pas pris en charge par l'ASA ou les Défense contre les menaces utilisant gestionnaire d'appareil.

Remarque La capacité multi-instance est similaire au mode à contexte multiple ASA, bien que son implémentation soit différente. Le mode contexte multiple partitionne une seule instance d'application, tandis que la capacité multi-instance permet des instances de conteneur indépendantes. Les instances de conteneur permettent la séparation des ressources matérielles, la gestion distincte de la configuration, des rechargements distincts, des mises à jour logicielles distinctes et la prise en charge complète de la fonctionnalité Défense contre les menaces. Le mode contexte multiple, en raison des ressources partagées, prend en charge plus de contextes sur une plateforme donnée. Le mode contexte multiple n'est pas disponible sur Défense contre les menaces.

Pour le Firepower 9300, vous pouvez utiliser une instance native sur certains modules et des instances de conteneurs sur le(s) autre(s) module(s).

Interfaces d'instances de conteneur

Pour fournir une utilisation flexible de l'interface physique pour les instances de conteneur, vous pouvez créer des sous-interfaces VLAN dans FXOS et également partager des interfaces (VLAN ou physiques) entre plusieurs instances. Les instances natives ne peuvent pas utiliser de sous-interfaces VLAN ou d'interfaces partagées. Une grappe de plusieurs instances ne peut pas utiliser de sous-interfaces VLAN ou d'interfaces partagées. Une exception est faite pour la liaison de commande de grappe, qui peut utiliser une sous-interface de la grappe EtherChannel. Consultez Évolutivité de l'interface partagée, à la page 7 et Ajouter une sous-interface VLAN pour les instances de conteneur, à la page 42.

Remarque Ce chapitre traite uniquement des sous-interfaces du VLAN *FXOS*. Vous pouvez créer séparément des sous-interfaces dans l'application défense contre les menaces . Consultez Interfaces FXOS par rapport aux interfaces d'application, à la page 4 pour obtenir de plus amples renseignements.

Classement des paquets par le châssis

Chaque paquet qui entre dans le châssis doit être classé, de sorte que ce dernier puisse déterminer à quelle instance envoyer un paquet.

- Interfaces uniques : si une seule instance est associée à l'interface d'entrée, le châssis classe le paquet dans cette instance. Pour les interfaces membres de groupes de ponts (en mode transparent ou en mode routé), les ensembles en ligne ou les interfaces passives, cette méthode est utilisée en permanence pour classer les paquets.
- Adresses MAC uniques : le châssis génère automatiquement des adresses MAC uniques pour toutes les interfaces, y compris les interfaces partagées. Si plusieurs instances partagent une interface, le classificateur utilise des adresses MAC uniques attribuées à l'interface dans chaque instance. Un routeur en amont ne peut pas acheminer directement vers une instance sans adresse MAC unique. Vous pouvez également définir les adresses MAC manuellement lorsque vous configurez chaque interface dans l'application.

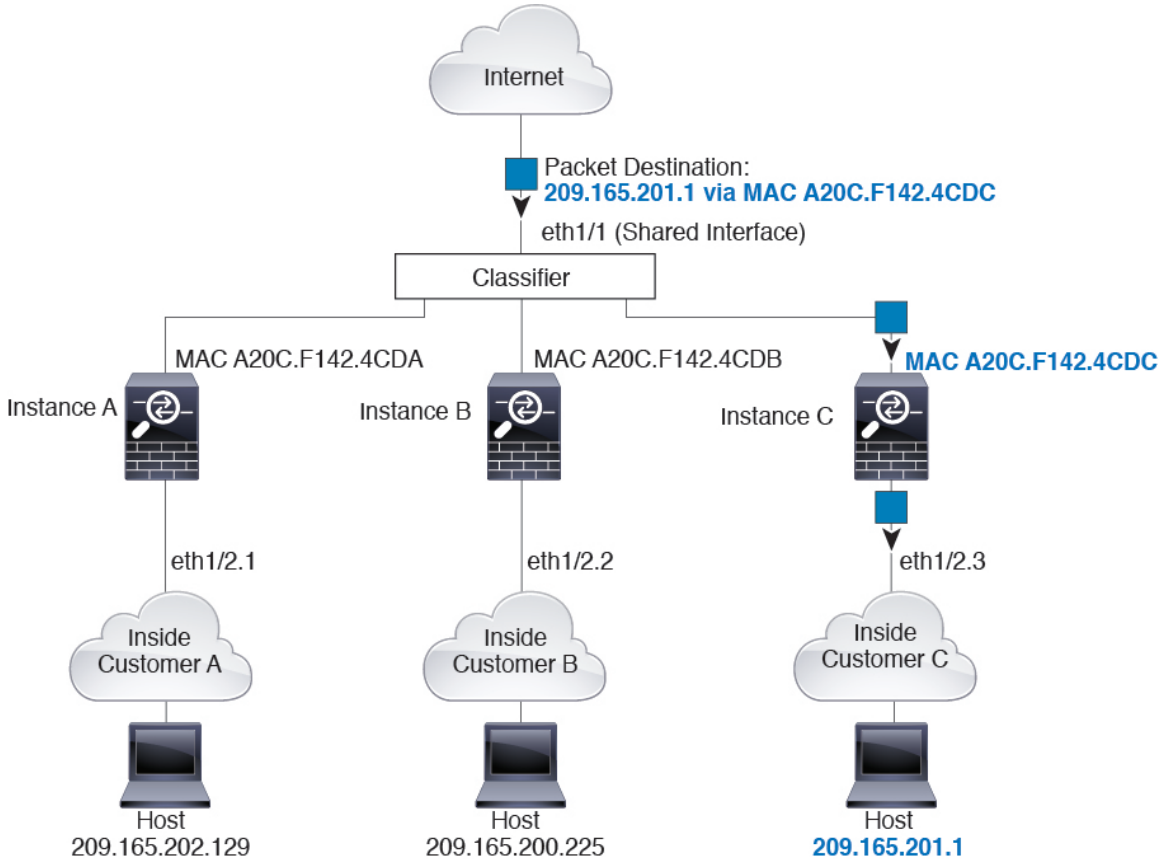
Remarque Si l'adresse MAC de destination est une adresse MAC de multidiffusion ou de diffusion, le paquet est dupliqué et remis à chaque instance.

Exemples de classement

Classification des paquets avec une interface partagée à l'aide d'adresses MAC

La figure suivante montre plusieurs instances partageant une interface externe. Le classificateur affecte le paquet à l'instance C, car l'instance C comprend l'adresse MAC à laquelle le routeur envoie le paquet.

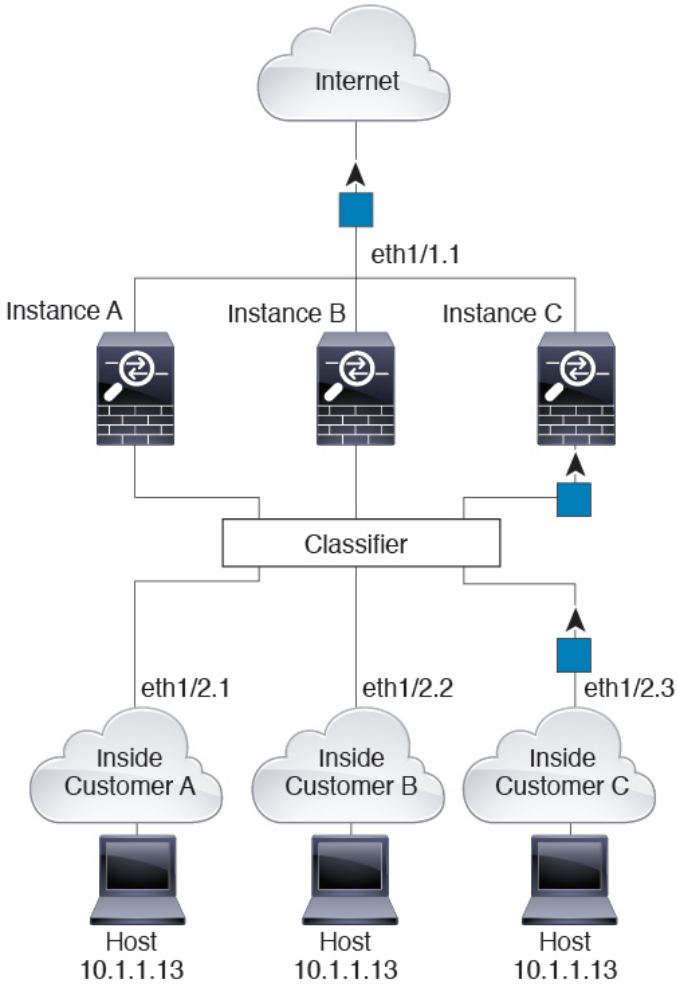
Illustration 6 : Classification des paquets avec une interface partagée à l'aide d'adresses MAC



Trafic entrant des réseaux internes

Notez que tout nouveau trafic entrant doit être classé, même en provenance des réseaux internes. La figure suivante montre un hôte sur le réseau interne de l'instance C qui accède à Internet. Le classificateur affecte le paquet à l'instance C, car l'interface d'entrée est Ethernet 1/2,3, qui est affectée à l'instance C.

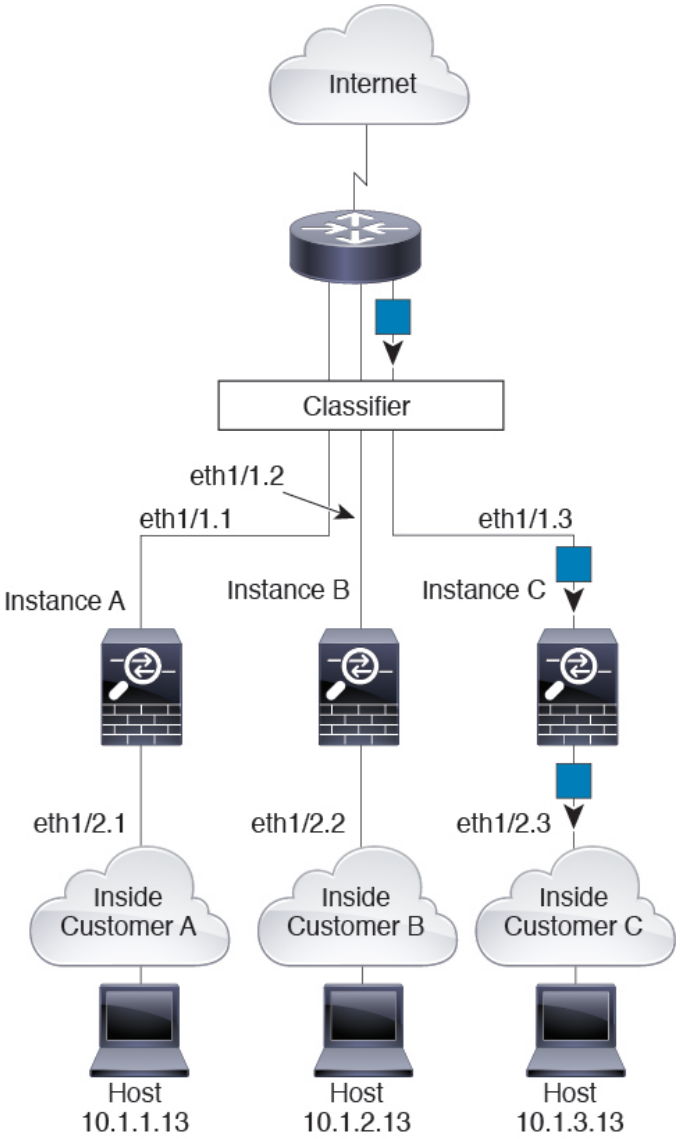
Illustration 7 : Trafic entrant des réseaux internes



Instances de pare-feu transparent

Pour les pare-feu transparents, vous devez utiliser des interfaces uniques. La figure suivante montre un paquet destiné à un hôte de l'instance C à partir d'Internet. Le classificateur affecte le paquet à l'instance C, car l'interface d'entrée est Ethernet 1/2,3, qui est affectée à l'instance C.

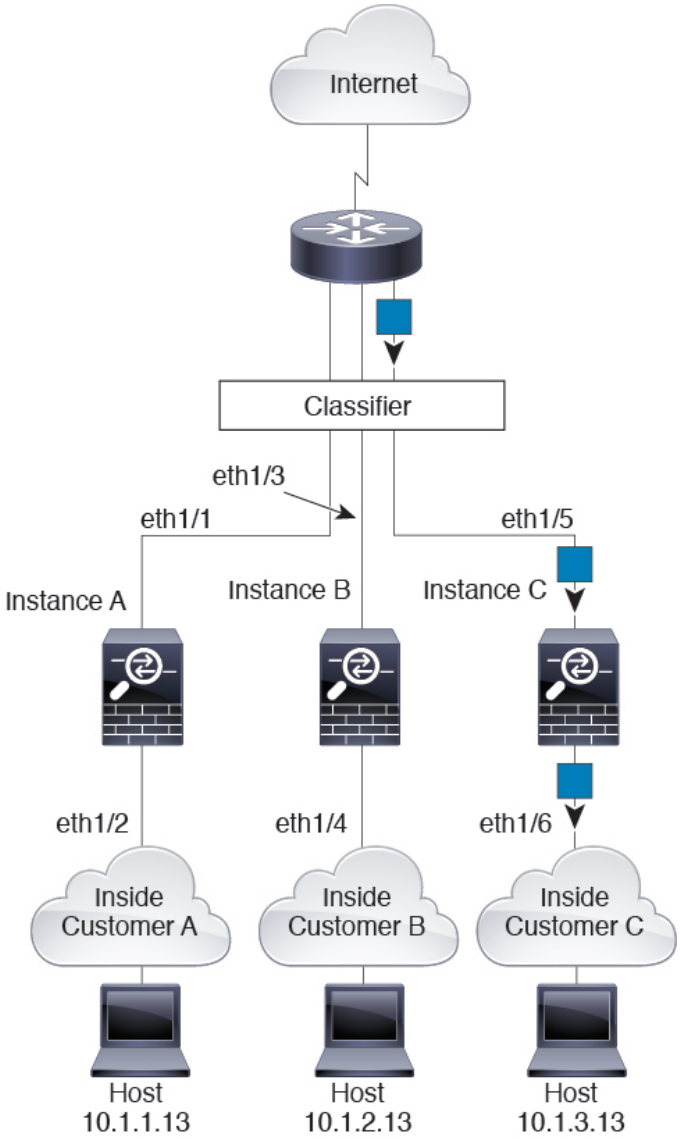
Illustration 8 : Instances de pare-feu transparent



Ensembles en ligne

Pour les ensembles en ligne, vous devez utiliser des interfaces uniques et il doit s'agir d'interfaces physiques ou d'EtherChannels. La figure suivante montre un paquet destiné à un hôte de l'instance C à partir d'Internet. Le classificateur affecte le paquet à l'instance C, car l'interface d'entrée est Ethernet 1/5, qui est affectée à l'instance C.

Illustration 9 : Ensembles en ligne

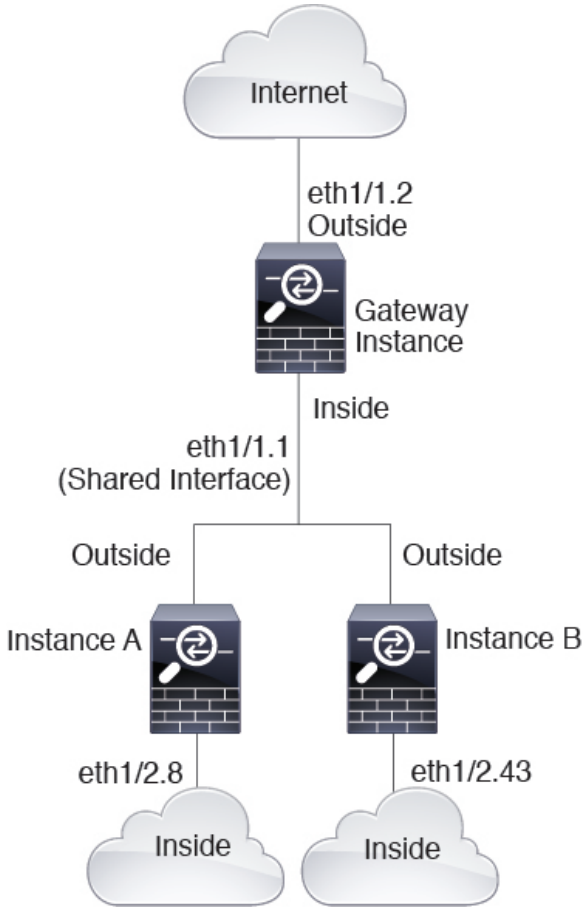


Instances de conteneur en chaîne

Le fait de placer une instance directement devant une autre instance s'appelle *des instances en chaîne*; l'interface externe d'une instance est la même que l'interface interne d'une autre instance. Vous pourriez souhaiter mettre des instances en chaîne si vous souhaitez simplifier la configuration de certaines instances en configurant des paramètres partagés dans l'instance supérieure.

La figure suivante montre une instance de passerelle avec deux instances derrière la passerelle.

Illustration 10 : Instances en chaîne



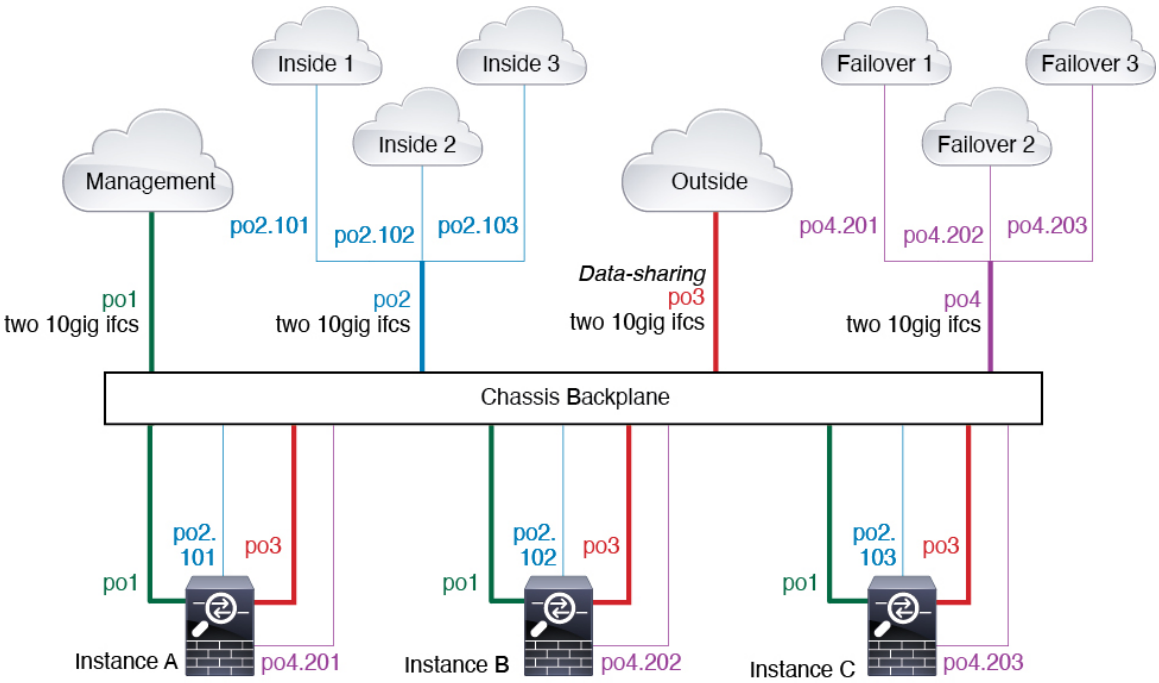
Remarque N'utilisez pas des instances en chaîne (en utilisant une interface partagée) avec la haute disponibilité. Après un basculement et le rapprochement de l'unité de secours, les adresses MAC peuvent se chevaucher temporairement et provoquer une panne. Vous devez plutôt utiliser des interfaces uniques pour l'instance de passerelle et une instance interne en utilisant un commutateur externe pour faire passer le trafic entre les instances.

Déploiement multi-instance typique

L'exemple suivant comprend trois instances de conteneur dans le mode de pare-feu routé. Elles comprennent les interfaces suivantes :

- Management : toutes les instances utilisent l'interface Port-Channel1 (type de gestion). Cet EtherChannel comprend deux interfaces Ethernet 10 Gigabits. Dans chaque application, l'interface utilise une adresse IP unique sur le même réseau de gestion.
- Inside (à l'intérieur) : chaque instance utilise une sous-interface sur le Port-Channel2 (type de données). Cet EtherChannel comprend deux interfaces Ethernet 10 Gigabits. Chaque sous-interface se trouve sur un réseau distinct.

- Outside (à l'extérieur) : toutes les instances utilisent l'interface Port-Channel3 (type de partage de données). Cet EtherChannel comprend deux interfaces Ethernet 10 Gigabits. Dans chaque application, l'interface utilise une adresse IP unique sur le même réseau externe.
- Failover (asculement) : chaque instance utilise une sous-interface sur le Port-Channel4 (type de données).b Cet EtherChannel comprend deux interfaces Ethernet 10 Gigabits. Chaque sous-interface se trouve sur un réseau distinct.



Adresses MAC automatiques pour les interfaces d'instance de conteneur

Le châssis génère automatiquement les adresses MAC pour les interfaces d'instance et garantit qu'une interface partagée dans chaque instance utilise une adresse MAC unique.

Si vous attribuez manuellement une adresse MAC à une interface partagée dans l'instance, l'adresse MAC attribuée manuellement est utilisée. Si vous supprimez ultérieurement l'adresse MAC manuelle, l'adresse générée automatiquement est utilisée. Dans les rares cas où l'adresse MAC générée entre en conflit avec une autre adresse MAC privée de votre réseau, nous vous suggérons de définir manuellement l'adresse MAC pour l'interface dans l'instance.

Étant donné que les adresses générées automatiquement commencent par A2, vous ne devez pas commencer les adresses MAC manuelles par A2 en raison du risque de chevauchement d'adresses.

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

A2*xx.yyzz.zzzz*

Où *xx.yy* est un préfixe défini par l'utilisateur ou un préfixe défini par le système, et *zz.zzzz* est un compteur interne généré par le châssis. Le préfixe défini par le système correspond aux 2 octets inférieurs de la première adresse MAC dans l'ensemble d'adresses MAC gravées qui est programmée dans la mémoire IDPROM. Utilisez **connect fxos**, puis **show module** pour afficher l'ensemble des adresses MAC. Par exemple, si la plage d'adresses MAC affichée pour le module 1 va de b0aa.772f.f0b0 à b0aa.772f.f0bf, le préfixe du système sera f0b0.

Le préfixe défini par l'utilisateur est un entier qui est converti en hexadécimal. Pour donner un exemple de la façon dont le préfixe défini par l'utilisateur est utilisé, si vous définissez un préfixe de 77, le châssis convertit 77 dans la valeur hexadécimale 004D (*yyxx*). Lorsqu'il est utilisé dans l'adresse MAC, le préfixe est inversé (*xxyy*) pour correspondre à la forme native du châssis :

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

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

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

Gestion des ressources d'instance de conteneur

Pour spécifier l'utilisation des ressources par instance de conteneur, créez un ou plusieurs profils de ressource dans FXOS. Lorsque vous déployez l'instance d'application ou de périphérique logique, vous spécifiez le profil de ressource que vous souhaitez utiliser. Le profil de ressource définit le nombre de cœurs de CPU; la mémoire RAM est allouée de façon dynamique en fonction du nombre de cœurs et l'espace disque est défini sur 40 Go par instance. Pour afficher les ressources disponibles par modèle, consultez Exigences et prérequis pour les instances de conteneur, à la page 29. Pour ajouter un profil de ressource, consultez Permet d'ajouter un profil de ressource pour les instances de conteneur, à la page 43.

Facteur d'échelle de rendement pour la capacité multi-instance

Le débit maximal (connexions, sessions VPN et sessions mandataires TLS) pour une plateforme est calculé pour l'utilisation de la mémoire et du processeur par une instance native (et cette valeur est affichée dans **show resource usage**). Si vous utilisez plusieurs instances, vous devez calculer le débit en fonction du pourcentage de cœurs de CPU que vous affectez à l'instance. Par exemple, si vous utilisez une instance de conteneur avec 50 % des cœurs, vous devez d'abord calculer 50 % du débit. De plus, le débit disponible pour une instance de conteneur peut être inférieur à celui d'une instance native.

Pour obtenir des instructions détaillées sur le calcul du débit des instances, consultez https://www.cisco.com/c/en/us/products/collateral/security/firewalls/white-paper-c11-744750.html.

Instances de conteneur et haute disponibilité

Vous pouvez utiliser la haute disponibilité en utilisant une instance de conteneur sur deux châssis distincts; par exemple, si vous avez deux châssis de 10 instances chacun, vous pouvez créer 10 paires à haute disponibilité. Notez que la haute disponibilité n'est pas configurée dans FXOS; configurez chaque paire à haute disponibilité dans le gestionnaire d'applications.

Pour connaître le détail des exigences, reportez-vous aux sections Exigences et prérequis pour la haute disponibilité, à la page 30 et Ajouter une paire à haute disponibilité, à la page 58.

Instances de conteneur et mise en grappe

Vous pouvez créer une grappe d'instances de conteneur en utilisant une instance de conteneur par module ou moteur de sécurité.

Licences pour les instances de conteneur

Toutes les licences sont utilisées par moteur de sécurité/châssis (pour le périphérique Firepower 4100) ou par module de sécurité (pour le périphérique Firepower 9300), et non par instance de conteneur. Consultez les renseignements suivants :

- Essentielle les licences sont attribuées automatiquement : une par security module/engine.
- Les licences de fonctionnalités sont attribuées manuellement à chaque instance; mais vous n'utilisez qu'une seule licence par fonctionnalité et par security module/engine. Par exemple, pour le périphérique Firepower 9300 avec 3 modules de sécurité, vous avez besoin d'une seule licence Filtrage d'URL par module, pour un total de 3 licences, quel que soit le nombre d'instances utilisées.

Par exemple :

Tableau 6 : Exemple d'utilisation de licences pour des instances de conteneur sur un appareil Firepower 9300

Firepower 9300	Instance	Licences
Modules de sécurité 1	Instance 1	Essentielle, Filtrage d'URL, Défense contre les programmes malveillants
	Instance 2	Essentielle, Filtrage d'URL
	Instance 3	Essentielle, Filtrage d'URL
Modules de sécurité 2	Instance 4	Essentielle, IPS
	Instance 5	Essentielle, Filtrage d'URL, Défense contre les programmes malveillants, IPS
Modules de sécurité 3	Instance 6	Essentielle, Défense contre les programmes malveillants, IPS
	Instance 7	Essentielle, IPS

Tableau 7 : Nombre total de licences

Essentielle	Filtrage d'URL	Défense contre les programmes malveillants	IPS
3	2	3	2

Exigences et conditions préalables des périphériques logiques

Consultez les sections suivantes pour connaître les exigences et les prérequis.

Exigences et conditions préalables pour les combinaisons matérielles et logicielles de l'

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 :

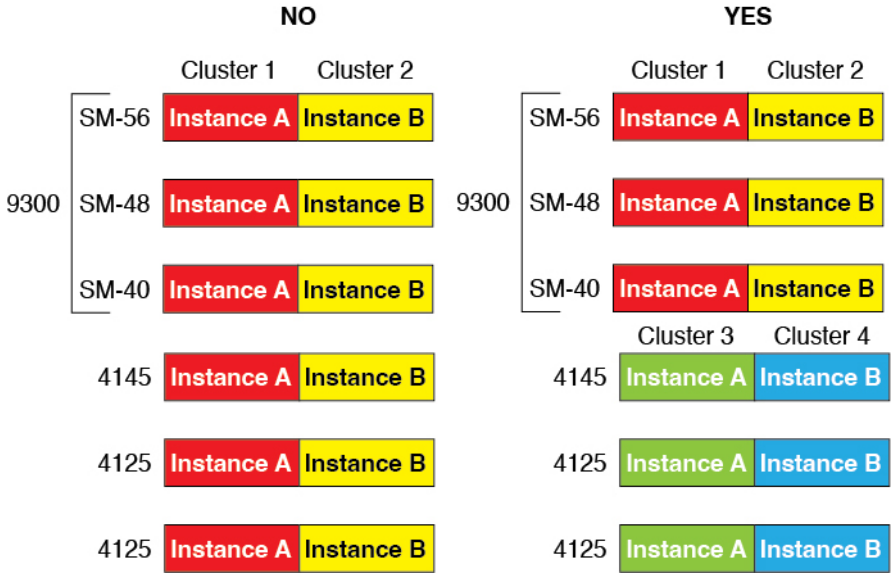
- Security Module Types (types de modules de sécurité) : Vous pouvez installer des modules de différents types dans le périphérique Firepower 9300. Par exemple, vous pouvez installer le SM-48 comme module 1, le SM-40 comme module 2 et le SM-56 comme module 3.
- Mise en grappe des instances natives : 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.
- Mise en grappe d'instances de conteneur : vous pouvez créer une grappe en utilisant des instances sur différents types de modèles. Par exemple, vous pouvez créer une grappe en utilisant une instance sur une Firepower 9300 SM-56, SM-48 et SM-40. Vous *ne pouvez pas* combiner le Firepower 9300 et le Firepower 4100 dans la même grappe.

- 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 défense contre les menaces :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 défense contre les menaces sur le module 3.
- Versions ASA ou défense contre les menaces : 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 défense contre les menaces 6.3 sur le module 1, défense contre les menaces 6.4 sur le module 2 et défense contre les menaces 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 native des instances : tous les châssis de la grappe doivent être du même modèle.
- Mise en grappe d'instances de conteneur : vous pouvez créer une grappe en utilisant des instances sur différents types de modèles. Par exemple, vous pouvez créer une grappe en utilisant une instance sur un Firepower 4145 et une sur un 4125. Vous *ne pouvez pas* combiner le Firepower 9300 et le Firepower 4100 dans la même grappe.



- Haute disponibilité : la haute disponibilité est uniquement prise en charge entre les modèles du même type.
- Types d'application ASA et défense contre les menaces : Firepower 4100 ne peut exécuter qu'un seul type d'application.
- Les versions des instances de conteneur défense contre les menaces : vous pouvez exécuter différentes versions de Défense contre les menaces en tant qu'instances de conteneur distinctes sur le même module.

Exigences et prérequis pour les instances de conteneur

Pour en savoir plus sur les exigences de haute disponibilité ou de mise en grappe avec des instances multiples, consultez Exigences et prérequis pour la haute disponibilité, à la page 30 et Exigences et conditions préalables à la mise en grappe, à la page 31.

Types d'applications prises en charge

- Le défense contre les menaces utilise centre de gestion

Nombre maximal d'instances et de ressources de conteneur par modèle

Pour chaque instance de conteneur, vous pouvez spécifier le nombre de cœurs de CPU à affecter à l'instance. La RAM est allouée de façon dynamique en fonction du nombre de cœurs et l'espace disque est défini pour 40 Go par instance.

Tableau 8 : Nombre maximal d'instances et de ressources de conteneur par modèle

Modèle	Nombre maximal d'instances de conteneur	Cœurs de CPU disponibles	RAM disponible	Espace disque disponible
Firepower 4112	3	22	78 Go	308 Go
Firepower 4115	7	46	162 Go	308 Go
Firepower 4125	10	62	162 Go	644 Go
Firepower 4140	7	70	222 Go	311.8 Go
Firepower 4145	14	86	344 Go	608 Go
Module de sécurité Firepower 9300 SM-40	13	78	334 Go	1359 Go
Module de sécurité Firepower 9300 SM-48	15	94	334 Go	1341 Go
Module de sécurité Firepower 9300 SM-56	18	110	334 Go	1314 Go

Centre de gestion Exigences

Pour toutes les instances sur un châssis Firepower 4100 ou un module Firepower 9300, vous devez utiliser le même centre de gestion en raison de la mise en œuvre de la licence.

Exigences et prérequis pour la haute disponibilité

- Les deux unités d'une configuration de basculement à haute disponibilité doivent :
  - Être sur un châssis séparé; la haute disponibilité 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 disponibilité.
  - 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 disponibilité.
- La haute disponibilité 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 disponibilité entre les modules SM-56, entre les modules SM-48 et entre les modules SM-40.

- Pour les instances de conteneur, chaque unité doit utiliser les mêmes attributs de profil de ressource.
- Pour les instances de conteneurs : N'utilisez pas des instances en chaîne (en utilisant une interface partagée) avec la haute disponibilité. Après un basculement et le rapprochement de l'unité de secours, les adresses MAC peuvent se chevaucher temporairement et provoquer une panne. Vous devez plutôt utiliser des interfaces uniques pour l'instance de passerelle et une instance interne en utilisant un commutateur externe pour faire passer le trafic entre les instances.
- Pour les autres exigences du système en matière de haute disponibilité, consultez Configuration système requise pour High Availability (haute disponibilité).

Exigences et conditions préalables à la mise en grappe

Prise en charge des modèles de grappe

Défense contre les menaces prend en charge la mise en grappe sur les modèles suivants :

- Firepower 9300 – Vous pouvez inclure jusqu'à 16 nœuds dans la grappe. Par exemple, vous pouvez utilisermodule dans 16 châssis, ou modules dans 8 châssis, ou toute combinaison offrant un maximum de 16 modules. Prend en charge la mise en grappe avec plusieurs châssis et la mise en grappe isolée pour les modules de sécurité dans un châssis.
- Firepower 4100 : pris en charge pour un maximum de 16à nœuds grâce à la mise en grappe avec plusieurs châssis.

Rôles utilisateur

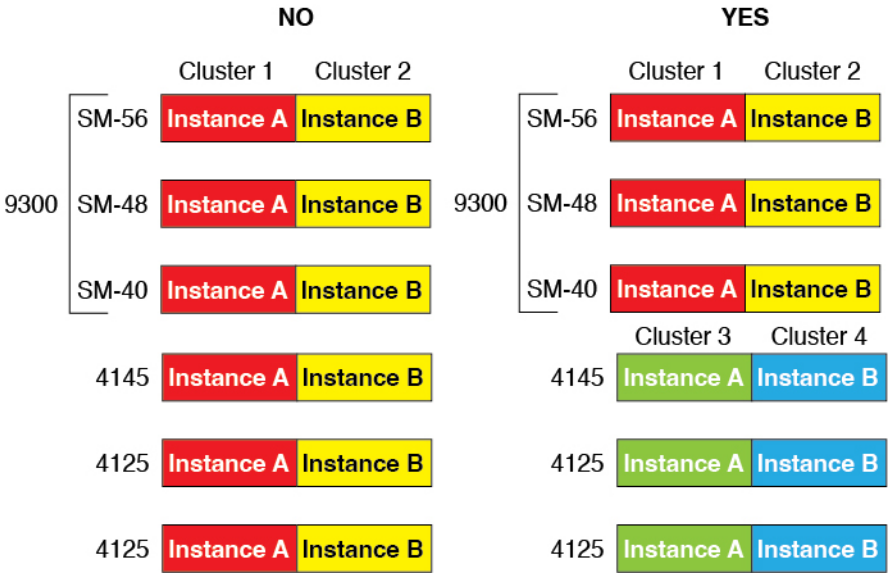
- Admin
- Administrateur d'accès
- Administrateur de réseau

Exigences matérielles et logicielles en matière de mise en grappe

Tous les châssis d'une grappe :

- Mise en grappe native des instances : pour Firepower 4100 : tous les châssis doivent être du même modèle. Pour le périphérique Firepower 9300 : tous les modules de sécurité doivent être du même type. Par exemple, si vous utilisez la mise en grappe, tous les modules du périphérique Firepower 9300 doivent être des SM-40. 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.
- Mise en grappe d'instances de conteneur : nous vous recommandons d'utiliser le même module de sécurité ou modèle de châssis pour chaque instance de grappe. Cependant, vous pouvez combiner des instances de conteneur sur différents types de modules de sécurité Firepower 9300 ou modèles Firepower 4100 dans la même grappe, au besoin. Vous ne pouvez pas combiner des instances Firepower 9300 et 4100 dans la même grappe. Par exemple, vous pouvez créer une grappe en utilisant une instance sur une

Firepower 9300 SM-56, SM-48 et SM-40. Vous pouvez aussi créer une grappe sur un Firepower 4145 et un 4125.



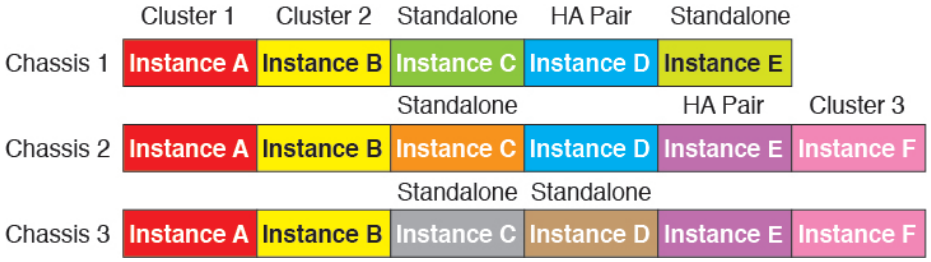
- Doit exécuter FXOS et le logiciel d'application identiques, sauf au moment d'une mise à niveau d'image. Des versions logicielles non concordantes peuvent entraîner une dégradation des performances. Assurez-vous donc de mettre à niveau tous les nœuds dans la même fenêtre de maintenance.
- Doit inclure la même configuration d'interface pour les interfaces que vous affectez à la grappe, comme la même interface de gestion, les mêmes EtherChannels, les interfaces actives, la vitesse et le duplex, etc. Vous pouvez utiliser différents types de modules de réseau sur le châssis tant que les capacités correspondent pour les mêmes ID d'interface et que les interfaces peuvent être groupées avec succès dans le même EtherChannel étendu. Notez que toutes les interfaces de données doivent être des EtherChannels dans des grappes à plusieurs châssis. Si vous modifiez les interfaces dans FXOS après avoir activé la mise en grappe (en ajoutant ou en supprimant des modules d'interface, ou en configurant EtherChannels, par exemple), vous effectuez les mêmes modifications sur chaque châssis, en commençant par les nœuds de données jusqu'au nœud de contrôle.
- Doit utiliser le même serveur NTP. Pour Défense contre les menaces, centre de gestion doit également utiliser le même serveur NTP. Ne réglez pas l'heure manuellement.

Exigences de la mise en grappe en plusieurs instances

- Pas de mise en grappe intra-module/moteur de sécurité : pour une grappe donnée, vous ne pouvez utiliser qu'une seule instance de conteneur par module de sécurité/moteur. Vous ne pouvez pas ajouter deux instances de conteneur à la même grappe si elles fonctionnent sur le même module.

- Combinez les grappes et les instances autonomes : toutes les instances de conteneur sur un module ou un moteur de sécurité n'ont pas besoin d'appartenir à une grappe. Vous pouvez utiliser certaines instances

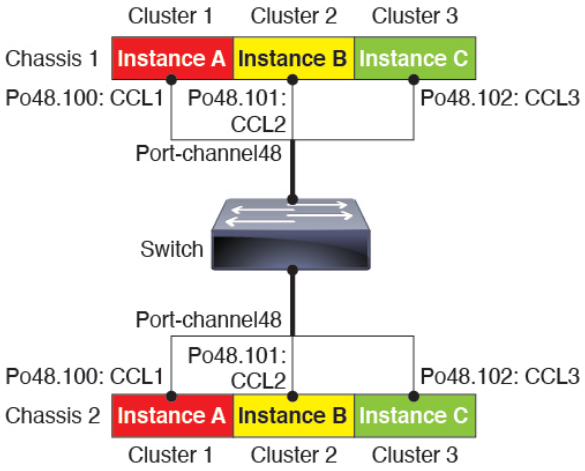
en tant que nœuds autonomes ou à haute disponibilité. Vous pouvez également créer plusieurs grappes en utilisant des instances distinctes sur le même module/moteur de sécurité.



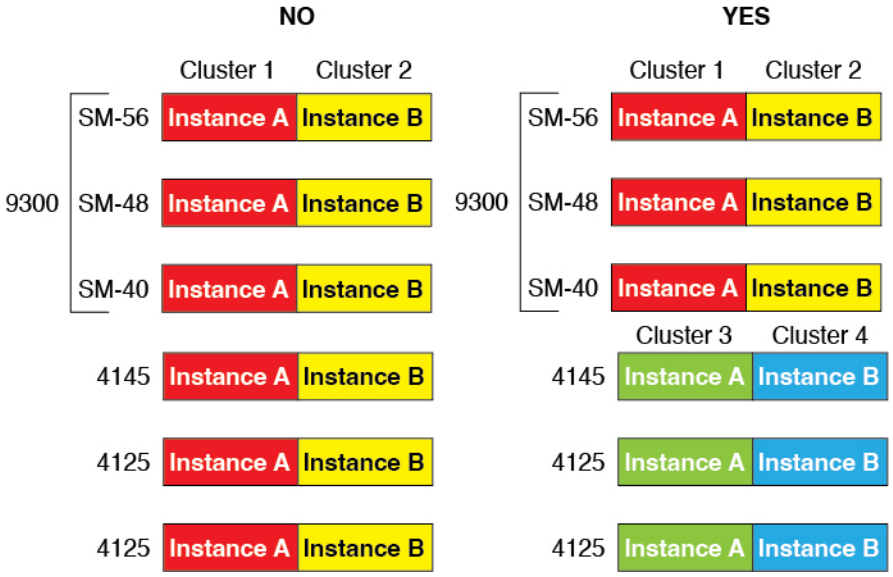
- Les 3 modules d'un appareil Firepower 9300 doivent appartenir à la grappe : Pour le périphérique Firepower 9300, une grappe nécessite une seule instance de conteneur sur les 3 modules. Vous ne pouvez pas créer une grappe à l'aide d'instances du module 1 et 2, puis utiliser une instance native sur le module 3, ou example.

- Faire correspondre les profils de ressources : Nous recommandons que chaque nœud de la grappe utilise les mêmes attributs de profils de ressources; cependant, des ressources non concordantes sont autorisées lors du remplacement des nœuds de la grappe par un profil de ressource différent ou lors de l'utilisation de différents modèles.

- Liaison de commande de grappe dédiée : pour les grappes à plusieurs châssis, chaque grappe a besoin d'une liaison de commande de grappe dédiée. Par exemple, chaque grappe peut utiliser une sous-interface distincte sur le même EtherChannel de type de grappe, ou utiliser des EtherChannel distincts.



- No Shared Interface (Aucune interface partagée) : les interfaces de type partagé ne sont pas prises en charge avec la mise en grappe. Cependant, les mêmes interfaces de gestion et d'événements peuvent être utilisées par plusieurs grappes.
- No subinterfaces (Pas de sous-interfaces) : une grappe de plusieurs instances ne peut pas utiliser les sous-interfaces VLAN définies par FXOS. Une exception est faite pour la liaison de commande de grappe, qui peut utiliser une sous-interface de la grappe EtherChannel.
- Combiner les modèles de châssis : nous vous recommandons d'utiliser le même module de sécurité ou modèle de châssis pour chaque instance de grappe. Cependant, vous pouvez combiner des instances de conteneur sur différents types de modules de sécurité Firepower 9300 ou modèles Firepower 4100 dans la même grappe, au besoin. Vous ne pouvez pas combiner des instances Firepower 9300 et 4100 dans la même grappe. Par exemple, vous pouvez créer une grappe en utilisant une instance sur une Firepower 9300 SM-56, SM-48 et SM-40. Vous pouvez aussi créer une grappe sur un Firepower 4145 et un 4125.



- Maximum de 6 nœuds : vous pouvez utiliser jusqu'à six instances de conteneur dans une grappe.

Exigences du commutateur

- Assurez-vous de terminer la configuration du commutateur et de connecter avec succès tous les canaux EtherChannels du châssis aux commutateurs avant de configurer la mise en grappe sur Châssis Firepower 4100/9300 .
- Pour les caractéristiques de commutateur prises en charge, consultez la Compatibilité Cisco FXOS.

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

Sous-interfaces VLAN

- Ce chapitre traite uniquement des sous-interfaces du VLAN *FXOS*. Vous pouvez créer séparément des sous-interfaces dans l'application défense contre les menaces . Consultez Interfaces FXOS par rapport aux interfaces d'application, à la page 4 pour obtenir de plus amples renseignements.
- Les sous-interfaces (et les interfaces parentes) ne peuvent être affectées qu'à des instances de conteneur.

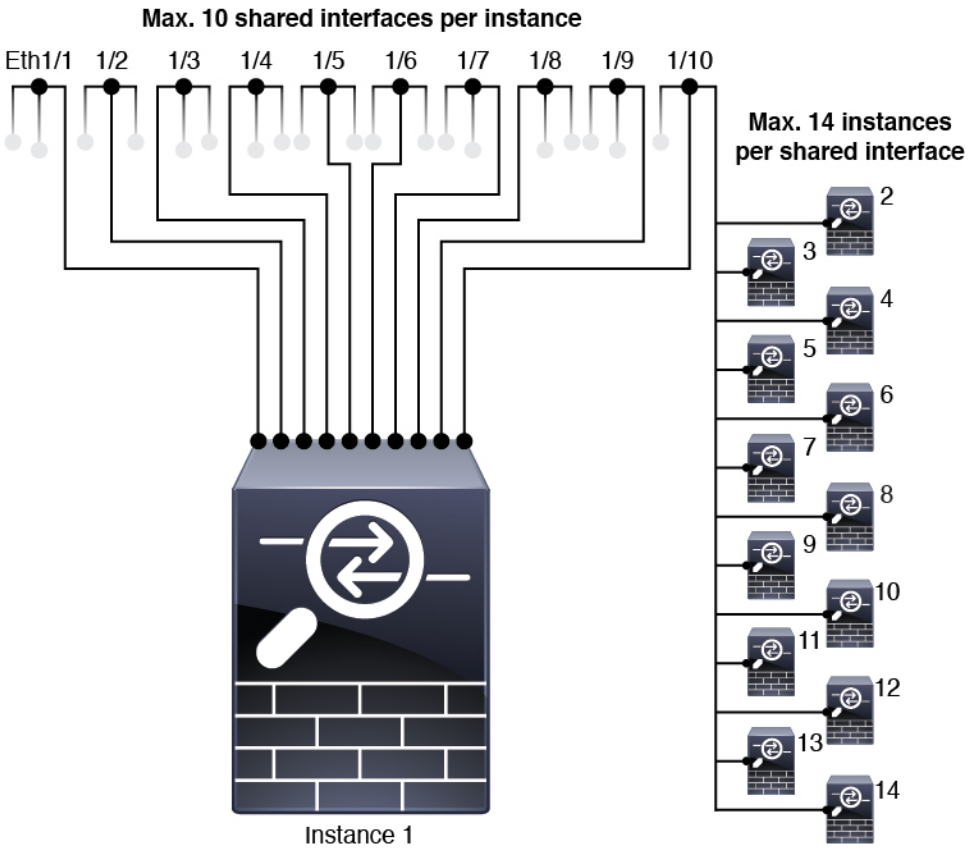
Remarque Si vous affectez une interface parente à une instance de conteneur, celle-ci ne transmet que le trafic non balisé (non VLAN). N'affectez pas d'interface parente, sauf si vous avez l'intention de transmettre du trafic non balisé. Pour les interfaces de type Grappe, l'interface parente ne peut pas être utilisée.

- Les sous-interfaces sont prises en charge sur les interfaces de type données ou partage de données, ainsi que les interfaces de type grappe. Si vous ajoutez des sous-interfaces à une interface de grappe, vous ne pouvez pas utiliser cette interface pour une grappe native.
- Pour la mise en grappe de plusieurs instances, les sous-interfaces FXOS ne sont pas prises en charge sur les interfaces de données. Cependant, les sous-interfaces sont prises en charge pour la liaison de commande de grappe, de sorte que vous pouvez utiliser un EtherChannel dédié ou une sous-interface d'EtherChannel pour la liaison de commande de grappe. Notez que les sous-interfaces définies par *l'application* sont prises en charge pour les interfaces de données.
- Vous pouvez créer jusqu'à 500 ID de VLAN.
- Consultez les limites suivantes dans l'application de périphérique logique; Gardez ces limites à l'esprit lorsque vous planifiez l'attribution de votre interface.
  - Vous ne pouvez pas utiliser des sous-interfaces pour un ensemble Défense contre les menaces en ligne ou comme interface passive.
  - Si vous utilisez une sous-interface pour la liaison de basculement, toutes les sous-interfaces de ce parent, et le parent lui-même, sont limités à une utilisation en tant que liaisons de basculement. Vous ne pouvez pas utiliser certaines sous-interfaces comme liaisons de basculement et d'autres comme interfaces de données normales.

Interfaces de partage de données

- Vous ne pouvez pas utiliser une interface de partage de données avec une instance native.
- Maximum de 14 instances par interface partagée. Par exemple, vous pouvez allouer Ethernet1/1 aux Instance1 à Instance14.

  Maximum de 10 interfaces partagées par instance. Par exemple, vous pouvez allouer Ethernet1/1.1 à Ethernet1/1.10 à l'Instance 1.



- Vous ne pouvez pas utiliser une interface de partage de données dans une grappe.
- Consultez les limites suivantes dans l'application de périphérique logique; Gardez ces limites à l'esprit lorsque vous planifiez l'attribution de votre interface.
  - Vous ne pouvez pas utiliser une interface de partage de données avec un périphérique en mode de pare-feu transparent.
  - Vous ne pouvez pas utiliser une interface de partage de données avec des ensembles de en ligne ou des interfaces passives Défense contre les menaces.
  - Vous ne pouvez pas utiliser une interface de partage de données pour la liaison de basculement.

Ensembles en ligne pour Défense contre les menaces

- Pris en charge pour les interfaces physiques (ports standard et ports d'éclatement) et les EtherChannels. Les sous-interfaces ne sont pas prises en charge.
- La propagation de l'état de liaison est prise en charge.
- Ne pas activer Hardware Bypass et Propager l'état du lien pour le même ensemble en ligne.

Contournement matériel

- Pris en charge pour Défense contre les menaces; vous pouvez les utiliser comme interfaces normales pour l'ASA.

- Défense contre les menaces ne prend en charge Hardware Bypass qu'avec les ensembles en ligne.
- Les interfaces compatibles Hardware Bypass ne peuvent pas être configurées pour les ports d'éclatement.
- Vous ne pouvez pas inclure des interfaces Hardware Bypass dans un EtherChannel et les utiliser pour Hardware Bypass; vous pouvez les utiliser comme des interfaces standard dans un EtherChannel.
- Hardware Bypass n'est pas pris en charge en mode haute disponibilité.
- Ne pas activer Hardware Bypass et Propager l'état du lien pour le même ensemble en ligne.

Adresses MAC par défaut

Pour les instances natives :

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.

Pour les instances de conteneurs :

- Les adresses MAC de toutes les interfaces proviennent d'un ensemble d'adresses MAC. Dans le cas des sous-interfaces, si vous décidez de configurer manuellement les adresses MAC, veillez à utiliser des adresses MAC uniques pour toutes les sous-interfaces sur la même interface parente afin de garantir une classification correcte. Consultez Adresses MAC automatiques pour les interfaces d'instance de conteneur, à la page 25.

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 Défense contre les menaces.

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 multi-instance

- La capacité multi-instance avec des instances de conteneur est uniquement disponible pour les Défense contre les menaces utilisant centre de gestion.
- Pour les instances de conteneur Défense contre les menaces, un seul centre de gestion doit gérer toutes les instances sur un security module/engine.

- Pour les instances de conteneur Défense contre les menaces, les fonctionnalités suivantes ne sont pas prises en charge :
  - décorateur de lien Radware DefensePro
  - Mode UCAPL/CC Centre de gestion
  - Décharge du flux vers le matériel

Interfaces de configuration

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

Activer ou désactiver une interface

Vous pouvez modifier l' **état d'administration** de chaque interface pour l'activer ou la désactiver. Par défaut, les interfaces physiques sont désactivées. Pour les sous-interfaces VLAN, l'état d'administration est hérité de l'interface parente.

Procédure

Étape 1 Choisissez **Interfaces** pour ouvrir la page des interfaces.

La page Interfaces présente une représentation visuelle des interfaces actuellement installées en haut de la page et fournit une liste des interfaces installées dans un tableau (voir ci-dessous).

Étape 2 Pour activer l'interface, cliquez sur le bouton désactivé **Curseur désactivé** ( ) pour qu'il devienne activé **Curseur activé** ( ).

Cliquez sur **Yes** (oui) pour confirmer la modification. L'interface correspondante dans la représentation visuelle passe du gris au vert.

Étape 3 Pour désactiver l'interface, cliquez sur le **Curseur activé** ( ) activé pour qu'elle devienne désactivée **Curseur désactivé** ( ).

Cliquez sur **Yes** (oui) pour confirmer la modification. L'interface correspondante dans la représentation visuelle passe du vert au gris.

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.

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 Choisissez **Interfaces** pour ouvrir la page des interfaces.

La page **All Interfaces** (toutes les interfaces) présente une représentation visuelle des interfaces actuellement installées en haut de la page et fournit une liste des interfaces installées dans un tableau (voir ci-dessous).

Étape 2 Cliquez sur **Edit** (modifier) dans la ligne de l'interface à modifier pour ouvrir la boîte de dialogue **Edit Interface** (modifier l'interface).

Étape 3 Activez l'interface en cochant la case **Enable** (activer). Désactivez l'interface en décochant la case **Enable** (activer).

Étape 4 Choisissez le **Type** d'interface :

Consultez Types d'interface, à la page 2 pour obtenir plus de détails sur l'utilisation de ce type d'interface.

- **Données**
- **Data-sharing (mise en commun des données)** : pour les instances de conteneur uniquement.
- **Gestion**
- **Firepower-eventing**— Pour Défense contre les menaces seulement.
- **Cluster (grappe)** : Ne choisissez pas le type **Cluster**; par défaut, la liaison de commande de grappe est automatiquement créée sur le port-canal 48.

Étape 5 (Facultatif) Choisissez la vitesse de l'interface dans la liste déroulante **Speed**.

Étape 6 (Facultatif) Si votre interface prend en charge la négociation automatique (**Auto Negotiation**), cliquez sur le bouton radio **Yes** (oui) ou **No** (non).

Étape 7 (Facultatif) Choisissez le duplex de l'interface dans la liste déroulante **Duplex**.

Étape 8 (Facultatif) Configurez explicitement le **Délai anti-rebond (ms)**. Saisissez une valeur comprise entre 0 et 15 000 milli-secondes.

Étape 9 Cliquez sur **OK**.

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 ou de partage 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 Choisissez **Interfaces** pour ouvrir la page des interfaces.

La page **All Interfaces** (toutes les interfaces) présente une représentation visuelle des interfaces actuellement installées en haut de la page et fournit une liste des interfaces installées dans un tableau (voir ci-dessous).

Étape 2 Cliquez sur **Add Port Channel** (ajouter un canal de port) au-dessus du tableau des interfaces pour ouvrir la boîte de dialogue **Add Port Channel** (ajouter un canal de port).

Étape 3 Dans le champ **Port Channel ID**, entrez un numéro identifiant le canal de port. Les valeurs valides sont comprises entre 1 et 47.

Le canal de port 48 est réservé pour la liaison de commande de grappe lorsque vous déployez un périphérique logique en grappe. Si vous ne souhaitez pas utiliser le canal de port 48 pour la liaison de commande de grappe, vous pouvez le supprimer et configurer un EtherChannel de type grappe avec un ID différent.Vous pouvez ajouter plusieurs EtherChannels de type grappe et ajouter des sous-interfaces VLAN à utiliser avec la mise en grappe à instances multiples. Pour la mise en grappe intra-châssis, n'affectez aucune interface à la grappe EtherChannel.

Étape 4 Cochez la case **Enable** pour activer le canal de port. Cochez la case **Disable** pour désactiver le canal de port.

Étape 5 Choisissez le **Type** d'interface :

Consultez Types d'interface, à la page 2 pour obtenir plus de détails sur l'utilisation de ce type d'interface.

- **Données**
- **Data-sharing (mise en commun des données)** : pour les instances de conteneur uniquement.
- **Gestion**
- **Firepower-eventing**— Pour Défense contre les menaces seulement.
- **Cluster** (Grappe)

Étape 6 Définissez la **vitesse d'administration** requise pour les interfaces membres dans la liste déroulante.

Si vous ajoutez une interface membre qui n'a pas la vitesse spécifiée, elle ne pourra pas rejoindre le canal de port.

Étape 7 Pour les données ou les interfaces de partage de données, choisissez le **mode**du canal de port LACP , **Actif** ou **Activé**.

Pour les interfaces sans données ou qui ne partagent pas de données, le mode est toujours actif.

Étape 8 Définissez le **duplex d'administration** requis pour les interfaces membres, soit **le duplex intégral** ou **semi-duplex**.

Si vous ajoutez une interface membre configurée avec le duplex précisé, elle ne rejoindra pas le canal de port.

Étape 9 Pour ajouter une interface au canal de port, sélectionnez l'interface dans la liste des **interfaces disponibles** et cliquez sur **Add Interface** (ajouter une interface) pour déplacer l'interface vers la liste d'ID de membre.

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.

Astuces Vous pouvez ajouter plusieurs interfaces en même temps. Pour sélectionner plusieurs interfaces, cliquez sur les interfaces souhaitées tout en maintenant la touche **Ctrl** enfoncée. Pour sélectionner une plage d'interfaces, sélectionnez la première interface de la plage, puis, tout en maintenant la touche **Maj** (Shift) enfoncée, cliquez pour sélectionner la dernière interface de la plage.

Étape 10 Pour supprimer une interface du canal de port, cliquez sur le bouton **Supprimer** à droite de l'interface dans la liste des ID de membre.

Étape 11 Cliquez sur **OK**.

Ajouter une sous-interface VLAN pour les instances de conteneur

Vous pouvez ajouter entre 250 et 500 sous-interfaces VLAN au châssis, selon votre déploiement réseau. Vous pouvez ajouter jusqu'à 500 sous-interfaces à votre châssis.

Pour la mise en grappe à instances multiples, vous ne pouvez ajouter des sous-interfaces qu'à l'interface de type grappe; les sous-interfaces des interfaces de données ne sont pas prises en charge.

Les ID de VLAN par interface doivent être uniques et, dans une instance de conteneur, les ID de VLAN doivent être uniques pour toutes les interfaces attribuées. Vous pouvez réutiliser les ID de VLAN sur des interfaces *distinctes*, à condition qu'ils soient affectés à différentes instances de conteneur. Cependant, chaque sous-interface compte toujours dans la limite, même si elle utilise le même ID.

Ce chapitre traite uniquement des sous-interfaces du VLAN *FXOS*. Vous pouvez créer séparément des sous-interfaces dans l'application défense contre les menaces . Pour plus d'informations sur le moment d'utilisation des sous-interfaces FXOS par rapport aux sous-interfaces d'application, consultez Interfaces FXOS par rapport aux interfaces d'application, à la page 4.

Procédure

Étape 1 Choisissez **Interfaces** pour ouvrir l'onglet **Toutes les interfaces**.

La page **All Interfaces** (toutes les interfaces) présente une représentation visuelle des interfaces actuellement installées en haut de la page et fournit une liste des interfaces installées dans un tableau (voir ci-dessous).

Étape 2 Cliquez sur **Add New** > **Subinterface** (Ajouter une nouvelle sous-interface) pour ouvrir la boîte de dialogue Add **Subinterface (ajouter** une sous-interface).

Étape 3 Choisissez le **Type** d'interface :

Consultez Types d'interface, à la page 2 pour obtenir plus de détails sur l'utilisation de ce type d'interface.

- **Données**
- **Partage de données**
- **Grappe** : si vous ajoutez des sous-interfaces à une interface de grappe, vous ne pouvez pas utiliser cette interface pour une grappe native.

Pour les données et les interfaces de partage de données : le type est indépendant du type d'interface parent; vous pouvez avoir un parent de partage de données et une sous-interface de données, par exemple.

Étape 4 Choisissez **l'interface** parente dans la liste déroulante.

Vous ne pouvez pas ajouter une sous-interface à une interface physique qui est actuellement allouée à une unité logique. Si d'autres sous-interfaces du parent sont allouées, vous pouvez ajouter une nouvelle sous-interface tant que l'interface parente elle-même n'est pas allouée.

Étape 5 Entrez **l'ID de la sous-interface** comme un nombre entier entre 1 et 4294967295.

Cet ID sera ajouté à l'ID de l'interface parente sous le nom *interface_id.subinterface_id*. Par exemple, si vous ajoutez une sous-interface à Ethernet1/1 avec l'ID 100, l'ID de la sous-interface sera : Ethernet1/1.100. Cet ID est différent de l'ID VLAN, bien que vous puissiez définir ces ID pour des raisons de commodité.

Étape 6 Définissez l'**ID VLAN** entre 1 et 4095.

Étape 7 Cliquez sur **OK**.

Développez l'interface parente pour afficher toutes les sous-interfaces qu'elle contient.

Configurer les périphériques logiques

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

Permet d'ajouter un profil de ressource pour les instances de conteneur

Pour spécifier l'utilisation des ressources par instance de conteneur, créez un ou plusieurs profils de ressource. Lorsque vous déployez l'instance d'application ou de périphérique logique, vous spécifiez le profil de ressource que vous souhaitez utiliser. Le profil de ressource définit le nombre de cœurs de CPU; la mémoire RAM est allouée de façon dynamique en fonction du nombre de cœurs et l'espace disque est défini sur 40 Go par instance.

- Le nombre minimum de cœurs est de 6.

Remarque Les instances avec un plus petit nombre de cœurs peuvent connaître une utilisation du processeur relativement plus élevée que celles avec un plus grand nombre de cœurs. Les instances avec un plus petit nombre de cœurs sont plus sensibles aux changements de charge de trafic. Si vous rencontrez des pertes de trafic, essayez d'assigner plus de cœurs.

- Vous pouvez affecter un nombre pair de cœurs (6, 8, 10, 12, 14, etc.) jusqu'au nombre maximal.
- Le nombre maximal de cœurs disponibles dépend du module de sécurité ou du modèle de châssis (voir Exigences et prérequis pour les instances de conteneur, à la page 29).

Le châssis comprend un profil de ressource par défaut appelé « Default-Small », qui comprend le nombre minimal de cœurs. Vous pouvez modifier la définition de ce profil et même le supprimer s'il n'est pas utilisé. Notez que ce profil est créé lors du rechargement du châssis et qu'aucun autre profil n'existe sur le système.

La modification du profil de ressource après son affectation entraîne une perturbation. Consultez les consignes suivantes :

- Vous ne pouvez pas modifier les paramètres du profil de ressource s'il est actuellement utilisé. Vous devez désactiver toutes les instances qui l'utilisent, puis modifier le profil de ressource et enfin réactiver l'instance.
- Si vous modifiez les paramètres du profil de ressources après avoir ajouté l'instance à la base de données, mettez ensuite à niveau l'inventaire de chaque unité sur la base de données de l'instanceDéfense contre les menaces sur le centre de gestion, puis mettez à niveau l'inventaire pour chaque unité sur la boîte de

dialogue de centre de gestion **Devices (appareils)** > **Device Management (gestion des appareils)** > **Device (appareil)** > **System (système)** > **Inventory (inventaire)**.

- Si vous affectez un profil différent à une instance, elle redémarre.
- Si vous affectez un profil différent aux instances d'une paire à haute disponibilité établie, ce qui nécessite que le profil soit le même sur les deux unités, vous devez :
  1. Rompre la haute disponibilité
  2. Attribuer le nouveau profil aux deux unités.
  3. Rétablir la haute disponibilité.
- Si vous affectez un profil différent aux instances d'une grappe établie, ce qui permet des profils non concordants, appliquez d'abord le nouveau profil sur les nœuds de données; après leur redémarrage, vous pouvez appliquer le nouveau profil au nœud de contrôle.

Procédure

Étape 1 Choisissez **Platform Settings (paramètres de la plateforme)** > **Resource Profiles (profils de ressource)**, puis cliquez sur **Add** pour ajouter.

La boîte de dialogue **Add Resource Profile** (ajouter un profil de ressource) apparaît.

Étape 2 Définissez les paramètres suivants.

- **Name** (nom) : indiquer le nom du profil (entre 1 et 64 caractères). Notez que vous ne pourrez plus modifier le nom de ce profil après l'avoir ajouté.
- **Description** : décrire profil (jusqu'à 510 caractères).
- **Number of Cores** (nombre de cœurs) : préciser un nombre pair de cœurs pour le profil, entre 6 et le maximum, selon votre châssis.

Étape 3 Cliquez sur **OK**.

Ajouter un appareil autonome Défense contre les menaces

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 utiliser des instances natives sur certains modules et des instances de conteneur sur les autres modules.

Avant de commencer

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

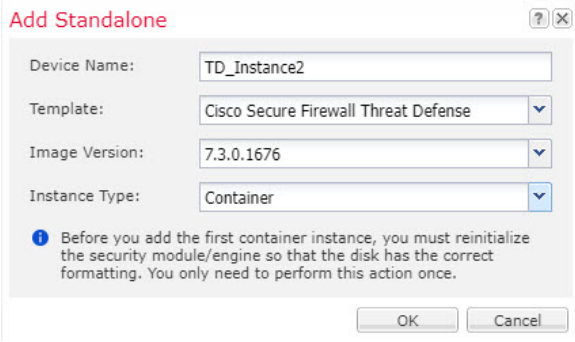
Remarque Pour Firepower 9300, vous pouvez installer différents types d'applications (ASA et défense contre les menaces) sur des modules distincts du châssis. Vous pouvez également exécuter différentes versions d'un type d'instance d'application sur des modules distincts.

- 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 (et qui apparaît en haut de l'onglet **Interfaces** comme **MGMT**).
- Vous pouvez activer ultérieurement la gestion à partir d'une interface de données; mais vous devez affecter une interface de gestion au périphérique logique même si vous n'avez pas l'intention de l'utiliser après avoir activé la gestion des données. Consultez la commande **configure network management-data-interface** dans la référence de commande FTD pour en savoir plus.
- Vous devez également configurer au moins une interface de données. Vous pouvez également créer une interface d'événement Firepower pour acheminer tout le trafic des événements (comme les événements Web). Consultez Types d'interface, à la page 2 pour obtenir de plus amples renseignements.
- Pour les instances de conteneur, si vous ne souhaitez pas utiliser le profil par défaut, ajoutez un profil de ressource en fonction de Permet d'ajouter un profil de ressource pour les instances de conteneur, à la page 43.
- Pour les instances de conteneur, avant de pouvoir installer une instance de conteneur pour la première fois, vous devez réinitialiser le security module/engine pour que le formatage du disque soit correct. Choisissez **Security Modules** (modules de sécurité) ou **Security Engine** (moteur de sécurité), puis cliquez sur l'icône **Reinitialize** (réinitialiser). Un périphérique logique existant sera supprimé, puis réinstallé en tant que nouveau périphérique, perdant toute configuration d'application locale. Si vous remplacez une instance native par des instances de conteneur, vous devrez supprimer l'instance native dans tous les cas. Vous ne pouvez pas migrer automatiquement une instance native vers une instance de conteneur.
- Recueillez les informations suivantes :
  - l'ID d'interface pour ce périphérique
  - l'adresse IP et le masque de réseau de l'interface de gestion
  - l'adresse IP de la passerelle
  - centre de gestion l'adresse IP et/ou l'ID NAT de votre choix
  - l'adresses IP du serveur DNS
  - Nom d'hôte et le nom de domaine Défense contre les menaces

Procédure

Étape 1 Choisissez **Logical Devices** (périphériques logiques).

Étape 2 Cliquez sur **Add** > **Standalone**, puis définissez les paramètres suivants :



a) Indiquez un nom de périphérique (**Device Name**).

Ce nom est utilisé par le superviseur du châssis pour configurer les paramètres de gestion et affecter des interfaces; ce n'est pas le nom de périphérique utilisé dans la configuration de l'application.

Remarque Vous ne pouvez pas modifier ce nom après avoir ajouté le périphérique logique.

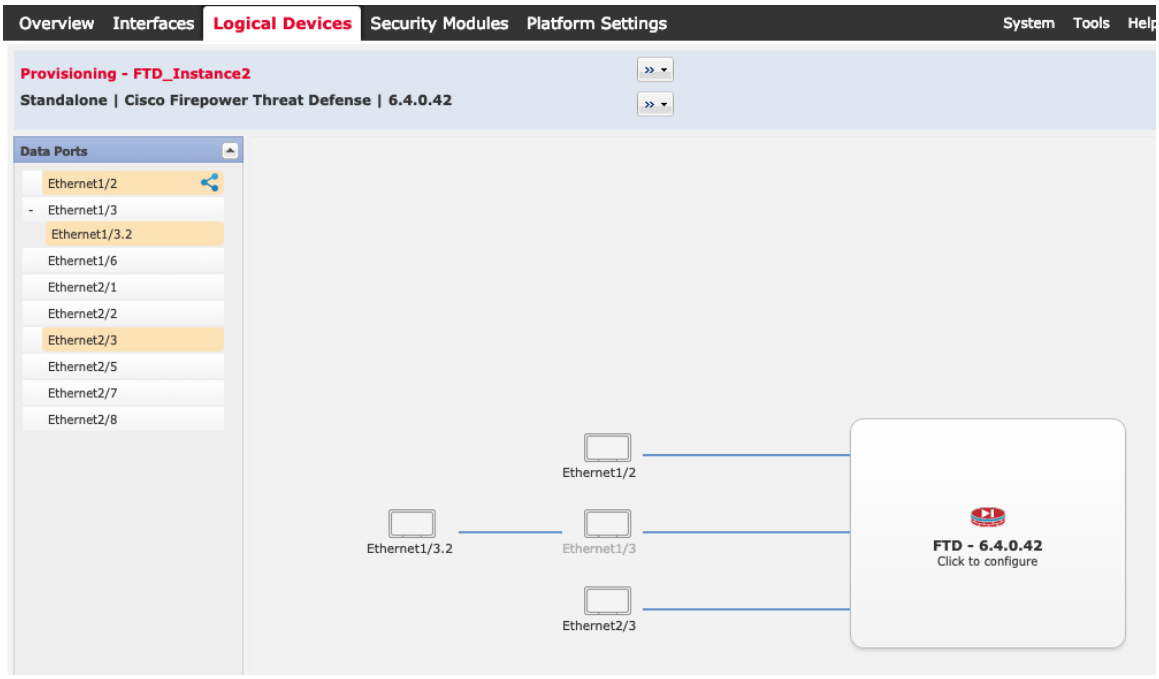
b) Pour le modèle (**Template**), choisissez **Cisco Firepower Threat Defense**.
c) Choisissez la version de l'image (**Image Version**).
d) Choisissez le type d'instance (**Instance Type**): instance de conteneur (**Container**) ou instance native (**Native**).

Une instance native utilise toutes les ressources (CPU, RAM et espace disque) de security module/engine. Vous ne pouvez donc installer qu'une seule instance native. Une instance de conteneur utilise un sous-ensemble de ressources de security module/engine. Vous pouvez donc installer plusieurs instances de conteneur.

e) Cliquez sur **OK**.

Vous voyez la fenêtre Provisioning - *device name* (provisionnement, nom du périphérique).

Étape 3 Développez la zone des ports de données (**Data Ports**), puis cliquez sur chaque interface que vous souhaitez affecter au périphérique.



Vous pouvez uniquement affecter des données et des **interfaces de partage de données** que vous avez précédemment activées dans la page Interfaces. Vous pourrez ensuite activer et configurer ces interfaces dans centre de gestion, y compris pour ce qui concerne la définition des adresses IP.

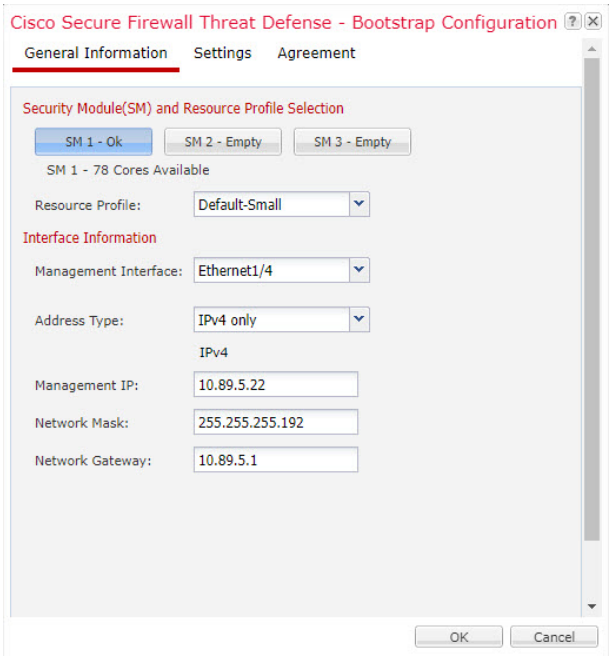
Vous pouvez affecter au maximum 10 interfaces de partage de données à une instance de conteneur. En outre, chaque interface de partage de données peut être affectée à tout au plus 14 instances de conteneur. Une interface de partage de données est indiquée par icône partage ( ).

Les ports compatibles Hardware Bypass sont représentés par l'icône suivante : . Pour certains modules d'interface, vous pouvez activer la fonction de contournement matériel pour les interfaces d'ensemble en ligne uniquement (consultez le guide de configuration de centre de gestion pour obtenir des renseignements). Le contournement matériel garantit que le trafic continue de circuler entre une paire d'interfaces en ligne pendant une panne de courant. Cette fonctionnalité peut servir à maintenir la connectivité du réseau en cas de défaillance matérielle ou logicielle. Si vous n'affectez pas les deux interfaces dans une paire de Hardware Bypass, un message d'avertissement s'affiche pour vous assurer que votre affectation est intentionnelle. Vous n'avez pas besoin d'utiliser la fonctionnalité Hardware Bypass, vous pouvez donc affecter des interfaces uniques si vous préférez.

Étape 4 Cliquez sur l'icône de périphérique au centre de l'écran.

Une boîte de dialogue s'affiche. Dans cette boîte, vous pouvez configurer les paramètres initiaux du démarrage. Ces paramètres sont destinés uniquement au déploiement initial ou à la reprise après sinistre. Pour un fonctionnement normal, vous pouvez ultérieurement modifier la plupart des valeurs dans la configuration de l'interface de ligne de commande de l'application.

Étape 5 Dans la page des informations générales (**General Information**), procédez comme suit :



a) (Pour Firepower 9300) Sous **Security Module Selection** (sélection du module de sécurité), cliquez sur le module de sécurité que vous souhaitez utiliser pour ce périphérique logique.

b) Pour une instance de conteneur, spécifiez le profil des ressources (**Resource Profile**).

Si vous affectez ultérieurement un profil de ressource différent, l'instance sera rechargée, ce qui peut prendre environ 5 minutes.

Remarque Si vous affectez ultérieurement un profil différent aux instances d'une paire à haute disponibilité établie, ce qui nécessite que le profil soit le même sur les deux unités, vous devez :

1. Rompre la haute disponibilité
2. Attribuer le nouveau profil aux deux unités.
3. Rétablir la haute disponibilité.

c) Choisissez l'interface de gestion (**Management Interface**).

Cette interface est utilisée pour gérer le périphérique logique. Cette interface est distincte du port de gestion du châssis.

d) Choisissez le type d'adresse de l'interface de gestion (**Address Type**) : **IPv4 only** (IPv4 seulement), **IPv6 only** (IPv6 seulement), ou **IPv4 and IPv6** (IPv4 et IPv6).

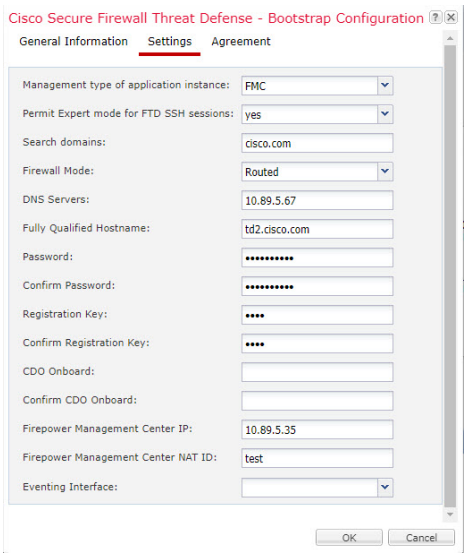
e) Configurez l'adresse IP de gestion (**Management IP**).

Définissez une adresse IP unique pour cette interface.

f) Saisissez un masque de réseau (**Network Mask**) ou une longueur de préfixe (**Prefix Length**).

g) Entrez une adresse **Network Gateway** (passerelle réseau).

Étape 6 Sous l'onglet **Settings** (paramètres), procédez comme suit :



a) Pour une instance native, dans la liste déroulante **Management type of application instance** (type de gestion de l'instance d'application), choisissez **FMC**.

   Les instances natives prennent également en charge le gestionnaire d'appareil comme gestionnaire. Après avoir déployé le périphérique logique, vous ne pouvez pas modifier le type de gestionnaire.

b) Entrez l'adresse IP du centre de gestion Firepower (**Firepower Management Center IP**) du centre de gestion gestionnaire.Si vous ne connaissez pas l'adresse IP de centre de gestion, laissez ce champ vide et saisissez une phrase d'accès dans le champ **ID NAT du Firepower Management Center**.

c) Pour une instance de conteneur, à la question sur l'autorisation du mode expert à partir de sessions SSD FTD (**Permit Expert mode from FTD SSH sessions**): répondez oui (**Yes**) ou non (**No**). Le mode expert fournit à Défense contre les menaces un accès à l'interpréteur de commandes (shell) pour un dépannage avancé.

   Si vous choisissez **Yes** (oui) pour cette option, les utilisateurs qui accèdent à l'instance de conteneur directement à partir d'une session SSH peuvent passer en mode expert. Si vous choisissez **No** (non), seuls les utilisateurs qui accèdent à l'instance de conteneur à partir de l'interface de ligne de commande de FXOS peuvent passer en mode expert. Nous vous recommandons de choisir **No** (non) pour augmenter l'isolement entre les instances.

   Utilisez le mode expert uniquement si une procédure documentée vous indique que c'est nécessaire ou si le Centre d'assistance technique (TAC) de Cisco vous demande de l'utiliser. Pour entrer dans ce mode, utilisez la commande **expert** dans l'interface de ligne de commande de Défense contre les menaces.

d) Entrez les domaines de recherche (**Search Domains**) sous forme de liste dont les éléments sont séparés par des virgules.

e) Choisissez le mode du pare-feu (**Firewall Mode**) : **Transparent** ou **Routed** (routage).

   En mode routage, l'Défense contre les menaces 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.

f) Entrez les serveurs DNS (**DNS Servers**) sous forme de liste dont les éléments sont séparés par des virgules.

Par exemple, Défense contre les menaces utilise DNS si vous spécifiez un nom d'hôte pour centre de gestion.

g) Entrez le nom complet du domaine (**Fully Qualified Hostname**) pour Défense contre les menaces.

h) Saisissez une clé d'enregistrement (**Registration Key**) à partager entre centre de gestion et l'appareil lors de l'enregistrement.

Vous pouvez choisir n'importe quelle chaîne de texte pour cette clé entre 1 et 37 caractères; vous entrez la même clé sur centre de gestion lorsque vous ajoutez Défense contre les menaces.

i) Saisissez un mot de passe (**Password**) pour l'utilisateur admin Défense contre les menaces pour l'accès à l'interface de ligne de commande.

j) Choisissez **l'interface d'événements** sur laquelle les événements doivent être envoyés. Si aucune interface d'événement n'est pas spécifiée, l'interface de gestion sera utilisée.

Cette interface doit être définie comme une interface pour événements Firepower.

k) Pour une instance de conteneur, définissez **Hardware Crypto** sur activé (**Enabled**) ou désactivé (**Disabled**).

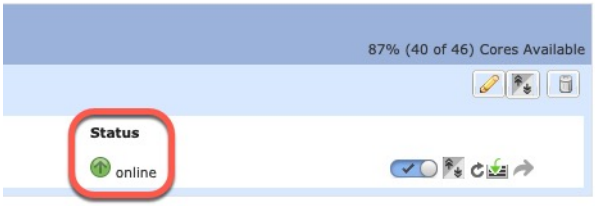
Ce paramètre active l'accélération cryptographique TLS dans le matériel et améliore les performances pour certains types de trafic. Cette fonction est activée par défaut. Vous pouvez activer l'accélération cryptographique TLS pour un maximum de 16 instances par module de sécurité. Cette fonctionnalité est toujours activée pour les instances natives. Pour afficher le pourcentage de ressources matérielles de chiffrement allouées à cette instance, entrez la commande **show hw-crypto**.

Étape 7 Sous l'onglet **Agreement** (accord), lisez et acceptez le contrat de licence d'utilisateur final.

Étape 8 Cliquez sur **OK** pour fermer la boîte de dialogue de configuration.

Étape 9 Cliquez sur **Save** (enregistrer).

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. Consultez l'état du nouveau périphérique logique dans la page **Logical Devices**. Lorsque le périphérique logique indique que son état (**Status**) est en ligne (**online**), vous pouvez commencer à configurer la politique de sécurité dans l'application.



Étape 10 Consultez le guide de configuration centre de gestion pour ajouter Défense contre les menaces en tant que périphérique géré et commencer à configurer votre politique de sécurité.

Ajouter un périphérique autonome Threat Defense pour Cisco Defense Orchestrator

Vous pouvez utiliser CDO avec les instances natives et de conteneur. Les périphériques logiques autonomes fonctionnent seuls ou dans une paire haute disponibilité.

Avant de commencer

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

Remarque Pour Firepower 9300, vous pouvez installer différents types d'applications (ASA et défense contre les menaces) 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 (et qui apparaît en haut de l'onglet **Interfaces** comme **MGMT**).
- Vous devez également configurer au moins une interface de données.
- Vous devez intégrer le périphérique FTD dans CDO.
- Recueillez les informations suivantes :
  - l'ID d'interface pour ce périphérique
  - l'adresse IP et le masque de réseau de l'interface de gestion
  - l'adresse IP de la passerelle
  - l'adresses IP du serveur DNS
  - Nom d'hôte et nom de domaine de Threat Defense
  - Chaîne intégrée de CDO
  - Nom d'hôte et le nom de domaine Défense contre les menaces

Procédure

Étape 1 Choisissez **Logical Devices** (périphériques logiques).

Étape 2 Click **Add (Ajouter)** > **Standalone (Autonome)**, et définissez les paramètres suivants :

a) Indiquez un nom de périphérique (**Device Name**).

Ce nom est utilisé par le superviseur du châssis pour configurer les paramètres de gestion et affecter des interfaces; ce n'est pas le nom de périphérique utilisé dans la configuration de l'application.

Remarque Vous ne pouvez pas modifier ce nom après avoir ajouté le périphérique logique.

b) Pour le modèle (**Template**), choisissez **Cisco Firepower Threat Defense**.
c) Choisissez la version de l'image (**Image Version**).
d) Choisissez le type d'instance (**Instance Type**): instance de conteneur (**Container**) ou instance native (**Native**).

   Une instance native utilise toutes les ressources (CPU, RAM et espace disque) de security module/engine. Vous ne pouvez donc installer qu'une seule instance native. Une instance de conteneur utilise un sous-ensemble de ressources de security module/engine. Vous pouvez donc installer plusieurs instances de conteneur.

e) Cliquez sur **OK**.

   Vous voyez la fenêtre Provisioning - *device name* (provisionnement, nom du périphérique).

Étape 3 Développez la zone des ports de données (**Data Ports**), puis cliquez sur chaque interface que vous souhaitez affecter au périphérique.

Vous pouvez uniquement affecter des données et des **interfaces de partage de données** que vous avez précédemment activées dans la page Interfaces. Vous pourrez ensuite activer et configurer ces interfaces dans centre de gestion, y compris pour ce qui concerne la définition des adresses IP.

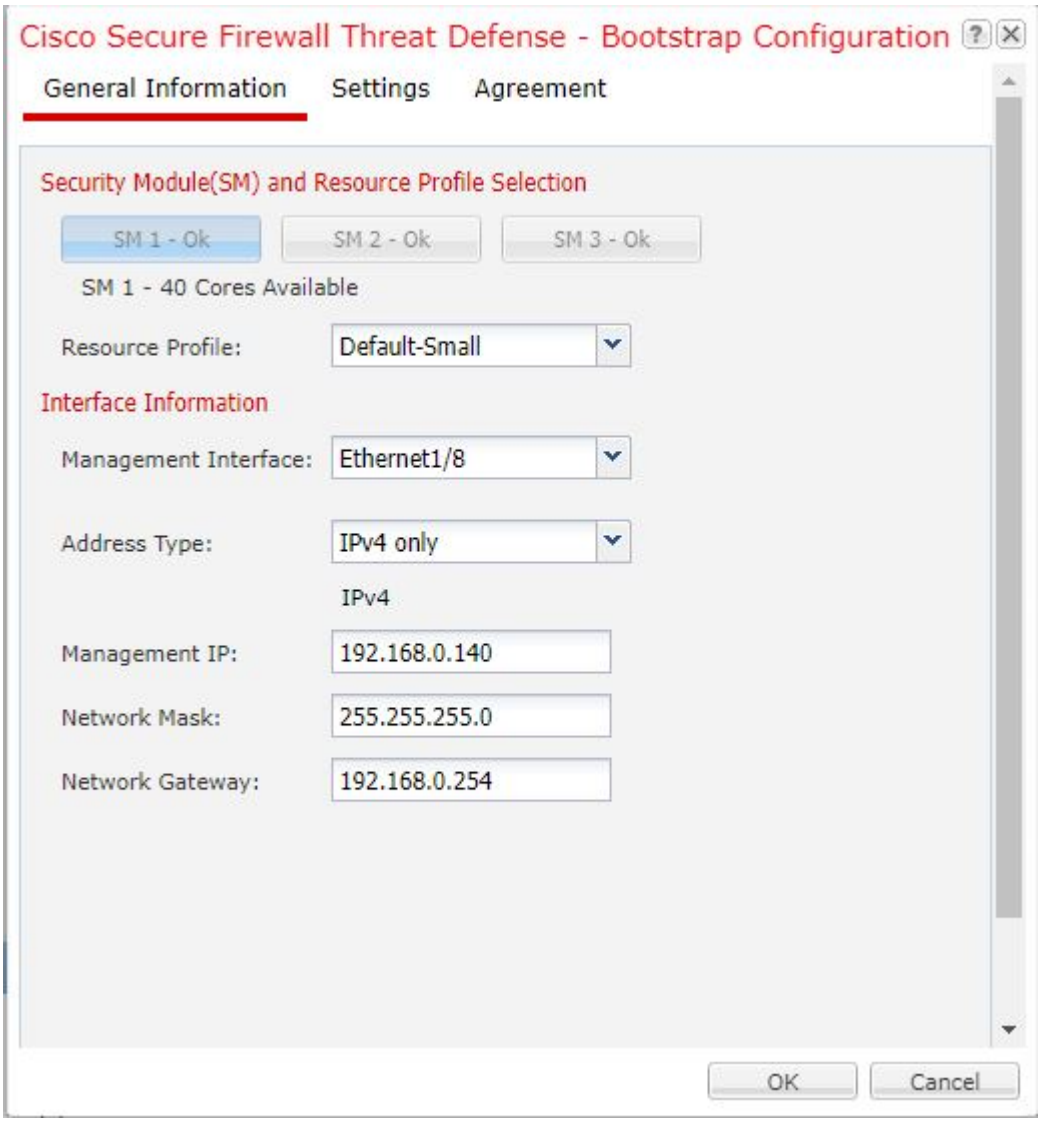
Vous pouvez affecter au maximum 10 interfaces de partage de données à une instance de conteneur. En outre, chaque interface de partage de données peut être affectée à tout au plus 14 instances de conteneur. Une interface de partage de données est indiquée par icône partage ( ).

Les ports compatibles Hardware Bypass sont représentés par l'icône suivante : . Pour certains modules d'interface, vous pouvez activer la fonction de contournement matériel pour les interfaces d'ensemble en ligne uniquement (consultez le guide de configuration de centre de gestion pour obtenir des renseignements). Le contournement matériel garantit que le trafic continue de circuler entre une paire d'interfaces en ligne pendant une panne de courant. Cette fonctionnalité peut servir à maintenir la connectivité du réseau en cas de défaillance matérielle ou logicielle. Si vous n'affectez pas les deux interfaces dans une paire de Hardware Bypass, un message d'avertissement s'affiche pour vous assurer que votre affectation est intentionnelle. Vous n'avez pas besoin d'utiliser la fonctionnalité Hardware Bypass, vous pouvez donc affecter des interfaces uniques si vous préférez.

Étape 4 Cliquez sur l'icône de périphérique au centre de l'écran.

Une boîte de dialogue s'affiche. Dans cette boîte, vous pouvez configurer les paramètres initiaux du démarrage. Ces paramètres sont destinés uniquement au déploiement initial ou à la reprise après sinistre. Pour un fonctionnement normal, vous pouvez ultérieurement modifier la plupart des valeurs dans la configuration de l'interface de ligne de commande de l'application.

Étape 5 Dans la page des informations générales (**General Information**), procédez comme suit :



a) (Pour Firepower 9300) Sous **Security Module Selection** (sélection du module de sécurité), cliquez sur le module de sécurité que vous souhaitez utiliser pour ce périphérique logique.

b) Pour une instance de conteneur, spécifiez le profil des ressources (**Resource Profile**).

Si vous affectez ultérieurement un profil de ressource différent, l'instance sera rechargée, ce qui peut prendre environ 5 minutes.

Remarque Si vous affectez ultérieurement un profil différent aux instances d'une paire à haute disponibilité établie, ce qui nécessite que le profil soit le même sur les deux unités, vous devez :

1. Rompre la haute disponibilité
2. Attribuer le nouveau profil aux deux unités.
3. Rétablir la haute disponibilité.

c) Choisissez l'interface de gestion (**Management Interface**).

Cette interface est utilisée pour gérer le périphérique logique. Cette interface est distincte du port de gestion du châssis.

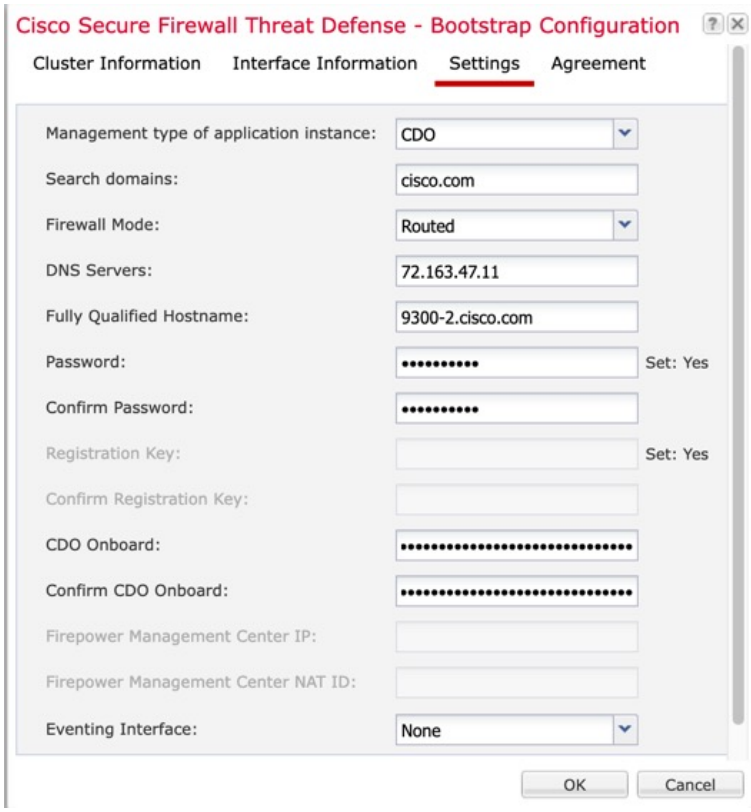
d) Choisissez le type d'adresse de l'interface de gestion (**Address Type**) : **IPv4 only** (IPv4 seulement), **IPv6 only** (IPv6 seulement), ou **IPv4 and IPv6** (IPv4 et IPv6).
e) Configurez l'adresse IP de gestion (**Management IP**).

Définissez une adresse IP unique pour cette interface.

f) Saisissez un masque de réseau (**Network Mask**) ou une longueur de préfixe (**Prefix Length**).
g) Entrez une adresse **Network Gateway** (passerelle réseau).

Étape 6 Sous l'onglet **Settings** (paramètres), procédez comme suit :

Illustration 11 : Paramètres



a) Dans la liste déroulante **Type de gestion de l'instance d'application**, choisissez **CDO**.
b) Entrez les domaines de recherche (**Search Domains**) sous forme de liste dont les éléments sont séparés par des virgules.
c) Choisissez le **mode de pare-feu** : **Transparent** ou **Routé**.
d) Entrez les serveurs DNS (**DNS Servers**) sous forme de liste dont les éléments sont séparés par des virgules.
e) Entrez le nom complet du domaine (**Fully Qualified Hostname**) pour Threat Defense.
f) Saisissez un mot de passe (**Password**) pour l'utilisateur admin Threat Defense pour l'accès à l'interface de ligne de commande.

g) Saisissez à nouveau le mot de passe dans le champ **Confirm Password** (confirmer le mot de passe) pour l'utilisateur administrateur de la défense contre les menaces pour l'accès à l'interface de ligne de commande

h) Saisissez la chaîne de commande **CDO Onboard** (Intégrer CDO) pour la défense contre les menaces.

CDO génère une chaîne de commande d'intégration une fois que vous avez intégré votre FTD. Copiez cette chaîne et placez-la dans le champ **CDO Onboard**.

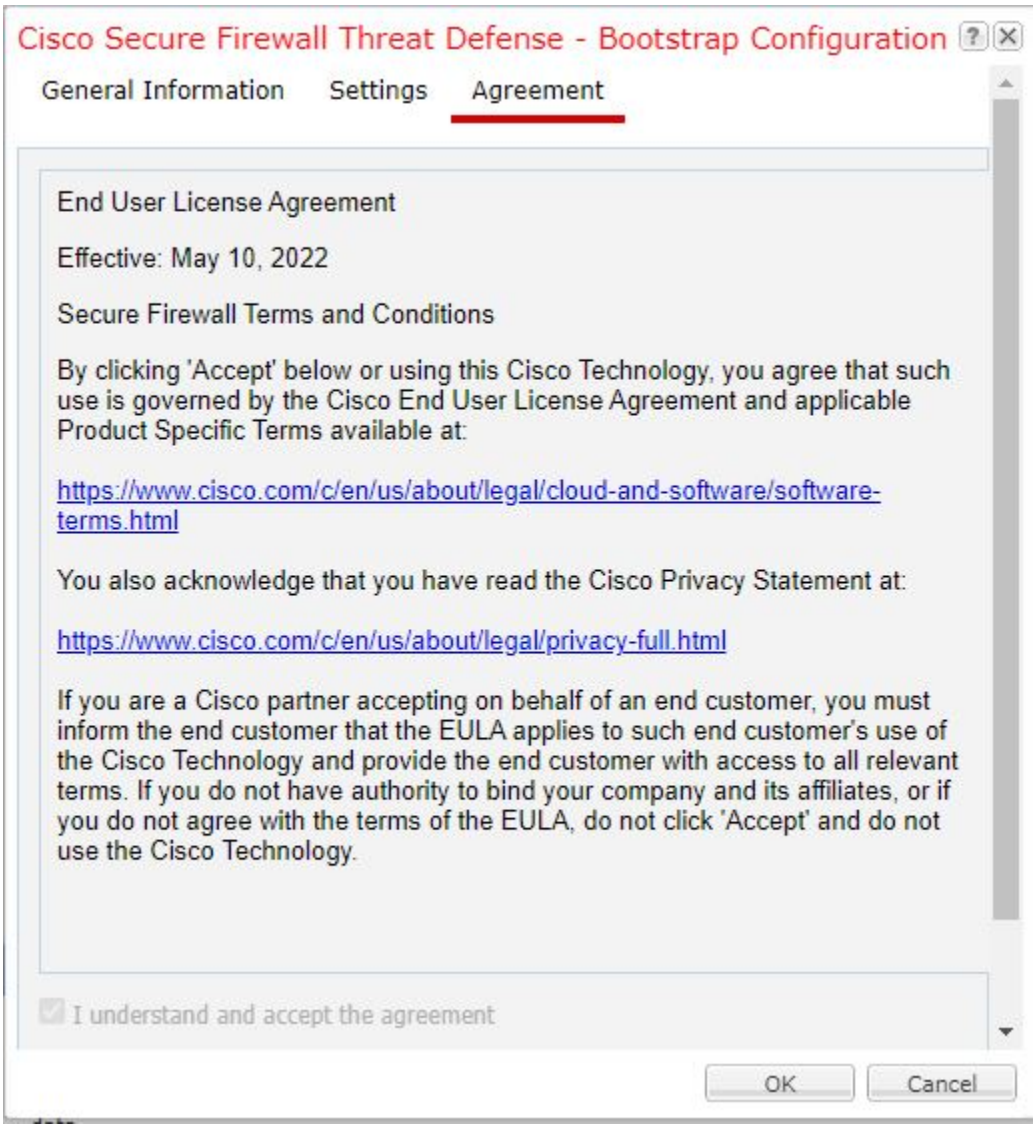
Par exemple :

```
configure manager add cisco-sapphire.app.staging.cdo.cisco.com
TuNDBm6peReVDbUkOpZCgtJ1GqWKbD30
o9B064UXEwmr3AYAEpuflf4qE2E3JKY5 cisco-sapphire.app.staging.cdo.cisco.com
```

i) Saisissez à nouveau la chaîne de commande dans **Confirm CDO Onboard** (Confirmer l'intégration de CDO).

j) Une interface d'événement **Eventing Interface** distincte n'est pas prise en charge pour CDO, donc ce paramètre sera ignoré.

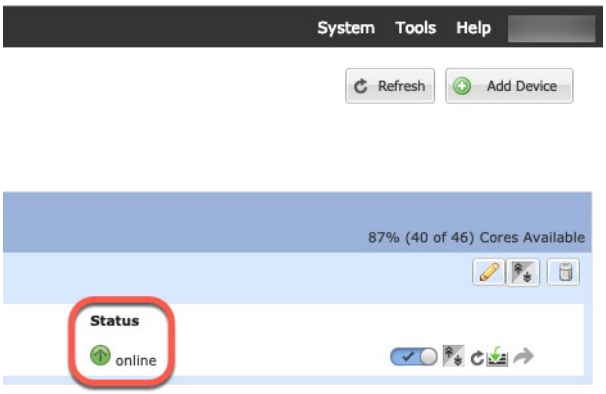
Étape 7 Sous l'onglet **Agreement** (accord), lisez et acceptez le contrat de licence d'utilisateur final.



Étape 8 Cliquez sur **OK** pour fermer la boîte de dialogue de configuration.

Étape 9 Cliquez sur **Save** (enregistrer).

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. Consultez l'état du nouveau périphérique logique dans la page **Logical Devices**. Lorsque le périphérique logique indique que son état (**Status**) est en ligne (**online**), vous pouvez commencer à configurer la politique de sécurité dans l'application.



Étape 10 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 activé (**Enabled**) et que l'état **Oper State** est **Online**.

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          7.3.0            7.3.0
  Container   Default-Small Not Applicable  None
```

Étape 11 Consultez le guide de configuration de CDO pour commencer à configurer votre politique de sécurité.

Ajouter une paire à haute disponibilité

La haute disponibilité Défense contre les menaces (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 Exigences et prérequis pour la haute disponibilité, à la page 30.

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.

Pour les instances de conteneur, les interfaces de partage de données ne sont pas prises en charge pour le liaison de basculement. Nous vous recommandons de créer des sous-interfaces sur une interface parente ou l'EtherChannel et d'affecter une sous-interface à chaque instance à utiliser comme liaison de basculement. Notez que vous devez utiliser toutes les sous-interfaces sur le même parent en tant que liaisons de basculement. Vous ne pouvez pas utiliser une sous-interface comme liaison de basculement, puis utiliser les autres sous-interfaces (ou l'interface parente) comme interfaces de données normales.

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

Modifier une interface sur un périphérique logique Défense contre les menaces

Vous pouvez allouer ou annuler l'allocation d'une interface ou remplacer une interface de gestion sur le périphérique logique Défense contre les menaces. Vous pouvez ensuite synchroniser la configuration de l'interface dans centre de gestiondans .

L'ajout d'une nouvelle interface ou la suppression d'une interface inutilisée a une incidence minime sur la configuration Défense contre les menaces. Cependant, la suppression d'une interface utilisée dans votre politique de sécurité aura une incidence sur la configuration. Les interfaces peuvent être référencées directement à de nombreux endroits dans la configuration Défense contre les menaces, notamment les règles d'accès, la NAT, le SSL, les règles d'identité, le VPN, le serveur DHCP, etc. Les politiques qui font référence aux zones de sécurité ne sont pas touchées. Vous pouvez également modifier les membres d'un EtherChannel alloué sans affecter le périphérique logique ou nécessiter de synchronisation sur centre de gestionsur .

suppression d'une interface supprimera toute configuration associée à cette interface.

Avant de commencer

- Configurez vos interfaces et ajoutez tous les EtherChannels en fonction de Configurer une interface physique, à la page 38 et Ajouter un canal EtherChannel (canal de port), à la page 39.
- 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.
- Si vous souhaitez remplacer l'interface de gestion ou d'événements par un EtherChannel de gestion, vous devez créer l'EtherChannel avec au moins une interface de membre de données non allouée, puis remplacer l'interface de gestion actuelle par l'EtherChannel. Une fois que le périphérique défense contre les menaces a redémarré (les modifications de l'interface de gestion entraînent un redémarrage) et que vous avez synchronisé la configuration dans centre de gestion, vous pouvez également ajouter l'interface de gestion (désormais non allouée) à l'EtherChannel.

- Pour la mise en grappe ou la haute disponibilité, assurez-vous d'ajouter ou de supprimer l'interface sur toutes les unités avant de synchroniser la configuration dans centre de gestiondans . 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. Notez que les nouvelles interfaces sont ajoutées dans un état administrativement inactif, de sorte qu'elles n'affectent pas la surveillance des interfaces.
- En mode multi-instance, pour modifier une sous-interface par une autre sous-interface avec la même balise VLAN, vous devez d'abord supprimer toute la configuration (y compris la configuration Nameif) de l'interface, puis annuler l'allocation de l'interface dans gestionnaire de châssis. Une fois non allouée, ajoutez la nouvelle interface, puis utilisez les interfaces de synchronisation de centre de gestion.

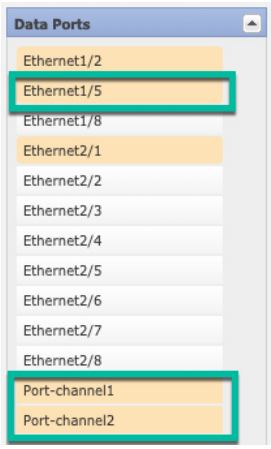
Procédure

Étape 1 Dans gestionnaire de châssis, sélectionner **Logical Devices (dispositifs logiques)**.

Étape 2 Cliquez sur l'icône **Edit** (modifier) en haut à droite pour modifier le périphérique logique.

Étape 3 Attribuez une nouvelle interface de données en la sélectionnant dans la zone **Data Ports** (Ports de données).

Ne supprimez aucune interface pour le moment.



Étape 4 Remplacer l'interface de gestion ou d'événement :

Pour ces types d'interfaces, le périphérique redémarre après que vous ayez enregistré vos modifications.

a) Cliquez sur l'icône de périphérique au centre de l'écran.
b) Sous l'onglet **General** ou **Cluster Information** (informations générales ou sur la grappe), choisissez la nouvelle **interface de gestion** dans la liste déroulante.
c) Sous l'onglet **Settings** (paramètres), choisissez la nouvelle **Eventing Interface** (interface d'événement) dans la liste déroulante.
d) Cliquez sur **OK**.

Si vous modifiez l'adresse IP de l'interface de gestion, vous devez également modifier l'adresse IP du périphérique dans centre de gestion : accédez à **Devices** > **Device Management** > **Device/Cluster** (Périphériques > Gestion des périphériques > Périphérique/Grappe). Dans la zone **Management** -gestion), définissez l'adresse IP pour qu'elle corresponde à l'adresse de configuration de démarrage.

Étape 5 Cliquez sur **Save** (enregistrer).

Étape 6 Synchronisez les interfaces dans centre de gestion.

a) Connectez-vous à centre de gestion.
b) Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des appareils) et cliquez sur **Modifier** ( ) pour votre appareil Défense contre les menaces. La page **Interfaces** est sélectionnée par défaut.
c) Cliquez sur le bouton **Sync Device** (synchroniser le périphérique) dans le coin supérieur gauche de la page **Interfaces**.
d) Une fois les modifications détectées, vous verrez une bannière rouge sur la page **Interfaces** indiquant que la configuration de l'interface a été modifiée. Cliquez sur le lien **Cliquez pour en savoir plus** pour afficher les modifications apportées à l'interface.
e) Si vous prévoyez de supprimer une interface, transférez manuellement toute configuration d'interface de l'ancienne interface à la nouvelle.

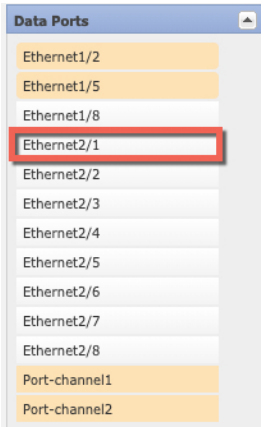
   Comme vous n'avez encore supprimé aucune interface, vous pouvez vous reporter à la configuration existante. Vous aurez davantage d'occasions de corriger la configuration après avoir supprimé l'ancienne interface et réexécuté la validation. La validation vous montrera tous les emplacements dans lesquels l'ancienne interface est toujours utilisée.

f) Cliquez sur **Validate Changes** (valider les modifications) pour vous assurer que votre politique fonctionnera toujours avec les modifications apportées à l'interface.

   S'il y a des erreurs, vous devez modifier votre politique et réexécuter la validation.

g) Cliquez sur **Save** (enregistrer).
h) Cliquez sur **Déployer** > **Déploiement**.
i) Sélectionnez les périphériques et cliquez sur **Deploy** pour déployer la politique sur les périphériques affectés. Les modifications ne sont actives que lorsque vous les déployez.

Étape 7 Dans gestionnaire de châssis, annulez l'allocation d'une interface de données en désélectionnant l'interface dans la zone **Ports de données**.



Étape 8 Cliquez sur **Save** (enregistrer).

Étape 9 Synchronisez de nouveau les interfaces dans centre de gestion dans .

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 ftd *name*

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

Exemple :

```
Firepower-module1> connect ftd ftd1
Connecting to ftd(ftd-native) console... enter exit to return to bootCLI
[...]
>
```

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

- Défense contre les menaces : Saisissez **exit**

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-], .**

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.