



## Interfaces de pare-feu standard

Ce chapitre traite de la configuration normale de l'interface de pare-feu défense contre les menaces, y compris les EtherChannels, les sous-interfaces VLAN, les adresses IP, etc.



**Remarque** Pour la configuration initiale de l'interface sur Firepower 4100/9300, consultez [Interfaces de configuration](#).

- [Exigences et conditions préalables pour les interfaces de pare-feu standard, à la page 1](#)
- [Configurer les ports de commutation de Firepower 1010, à la page 2](#)
- [Configurer les interfaces de bouclage, à la page 12](#)
- [Configurer les sous-interfaces VLAN et la jonction 802.1Q, à la page 18](#)
- [Configurer les interfaces VXLAN, à la page 22](#)
- [Configurer les interfaces en mode routage et en mode transparent, à la page 36](#)
- [Configurer les paramètres avancés de l'interface, à la page 60](#)
- [Historique des interfaces de pare-feu standard pour Cisco Secure Firewall Threat Defense, à la page 71](#)

## Exigences et conditions préalables pour les interfaces de pare-feu standard

### Prise en charge des modèles

Défense contre les menaces

### Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

# Configurer les ports de commutation de Firepower 1010

Vous pouvez configurer chaque interface Firepower 1010 pour qu'elle fonctionne comme une interface pare-feu normale ou comme un port de commutateur matériel de couche 2. Ce chapitre comprend les tâches de démarrage de la configuration de votre port de commutation, notamment l'activation ou la désactivation du mode de commutation, la création d'interfaces VLAN et l'affectation des ports de commutation aux réseaux VLAN. Cette section décrit également comment personnaliser l'alimentation par Ethernet (PoE) sur les interfaces prises en charge.

## À propos des ports de commutation Firepower 1010

Cette section décrit les ports de commutation du périphérique Firepower 1010.

## Comprendre les ports et les interfaces de Firepower 1010

### Ports et interfaces

Pour chaque interface physique Firepower 1010, vous pouvez définir son fonctionnement comme interface de pare-feu ou comme port de commutation. Consultez les renseignements suivants sur les interfaces physiques et les types de port, ainsi que sur les interfaces VLAN logiques auxquelles vous affectez des ports de commutation :

- **Interface de pare-feu physique** : En mode routé, ces interfaces transmettent le trafic entre les réseaux de la couche 3 en utilisant la politique de sécurité configurée pour appliquer les services de pare-feu et VPN. En mode transparent, ces interfaces sont des membres de groupes de ponts qui acheminent le trafic entre les interfaces du même réseau au niveau de la couche 2, en utilisant la politique de sécurité configurée pour appliquer les services de pare-feu. En mode routé, vous pouvez également utiliser le routage et le pont intégrés avec certaines interfaces comme membres du groupe de ponts et d'autres comme interfaces de couche 3. Par défaut, l'interface Ethernet 1/1 est configurée comme interface de pare-feu. Vous pouvez également configurer ces interfaces pour qu'elles soient IPS uniquement (ensembles en ligne et interfaces passives).
- **Port de commutation physique** : les ports de commutation transfèrent le trafic à la couche 2 en utilisant la fonction de commutation dans le matériel. Les ports de commutation sur le même VLAN peuvent communiquer entre eux grâce à la commutation matérielle, et le trafic n'est pas soumis à la politique de sécurité défense contre les menaces. Les ports d'accès acceptent uniquement le trafic non balisé et vous pouvez les affecter à un seul VLAN. Les ports de ligne principale acceptent le trafic non balisé et peuvent appartenir à plus d'un VLAN. Par défaut, les ports Ethernet 1/2 à 1/8 sont configurés comme ports de commutation d'accès sur le VLAN 1. Vous ne pouvez pas configurer l'interface Diagnostic comme port de commutation.
- **Logical VLAN interface (interface VLAN logique)** : Ces interfaces fonctionnent de la même façon que les interfaces de pare-feu physiques, à la différence que vous ne pouvez pas créer des sous-interfaces, des , des interfaces IPS seulement (ensembles en ligne et interfaces passives) ou des interfaces EtherChannel. Lorsqu'un port de commutation doit communiquer avec un autre réseau, le périphérique défense contre les menaces applique la politique de sécurité à l'interface VLAN et achemine le routage vers une autre interface VLAN logique ou une interface de pare-feu. Vous pouvez même utiliser le routage et le pont intégrés avec des interfaces VLAN comme membres du groupe de ponts. Le trafic entre les ports de commutation sur le même VLAN n'est pas soumis à la politique de sécurité, mais le trafic entre les VLAN d'un groupe de ponts est soumis à la politique de sécurité défense contre les

menaces. Vous pouvez donc choisir de superposer les groupes de ponts et les ports de commutation pour appliquer la politique de sécurité entre certains segments.

### Alimentation par Ethernet

Ethernet 1/7 et Ethernet 1/8 prennent en charge Power over Ethernet + (PoE +).

## Fonctionnalité Auto-MDI/MDIX

Pour toutes les interfaces Firepower 1010, le paramètre de négociation automatique par défaut inclut également la fonction Auto-MDI/MDIX. La fonction Auto-MDI/MDIX élimine le besoin de câblage croisé en effectuant un croisé interne lorsqu'un câble droit est détecté pendant la phase de négociation automatique. La vitesse ou le duplex doivent être réglés pour qu'ils soient négociés automatiquement afin d'activer Auto-MDI/MDIX pour l'interface. Si vous définissez explicitement la vitesse et le duplex à une valeur fixe, désactivant ainsi la négociation automatique pour les deux paramètres, Auto-MDI/MDIX est également désactivé. Lorsque la vitesse et le mode duplex sont définis à 1000 et que la vitesse maximale est atteinte, l'interface négocie toujours automatiquement; par conséquent, Auto-MDI/MDIX est toujours activé et vous ne pouvez pas le désactiver.

## Lignes directrices et limites pour les ports de commutation de Firepower 1010

### High Availability (haute disponibilité) et mise en grappe

- Aucune prise en charge de grappe.
- Vous ne devez pas utiliser la fonctionnalité de port de commutateur lors de l'utilisation de High Availability (haute disponibilité). Étant donné que les ports de commutation fonctionnent dans le matériel, ils continuent de faire circuler le trafic sur les unités actives *et* en veille. High Availability (haute disponibilité) est conçu pour empêcher le trafic de passer par l'unité en veille, mais cette fonctionnalité ne s'étend pas aux ports de commutation. Dans une configuration réseau High Availability (haute disponibilité) normale, les ports de commutateur actifs sur les deux unités mèneront à des boucles réseau. Nous vous suggérons d'utiliser des commutateurs externes pour toute capacité de commutation. Notez que les interfaces VLAN peuvent être surveillées par basculement, contrairement aux ports de commutation. Théoriquement, vous pouvez mettre un port de commutation unique sur un réseau VLAN et utiliser High Availability (haute disponibilité) avec succès, mais une configuration plus simple consiste à utiliser des interfaces physiques de pare-feu à la place.
- Vous ne pouvez utiliser qu'une interface de pare-feu comme lien de basculement.

### Interfaces logiques VLAN

- Vous pouvez créer jusqu'à 60 interfaces VLAN.
- Si vous utilisez également des sous-interfaces VLAN sur une interface de pare-feu, vous ne pouvez pas utiliser le même ID VLAN que pour une interface VLAN logique.
- Adresses MAC
  - Routed firewall mode (mode de pare-feu de routage) : Toutes les interfaces VLAN partagent une adresse MAC. Assurez-vous que tous les commutateurs connectés peuvent prendre en charge ce scénario. Si les commutateurs connectés nécessitent des adresses MAC uniques, vous pouvez attribuer manuellement des adresses MAC. Consultez [Configurer l'adresse MAC](#), à la page 66

- Mode pare-feu transparent : Chaque interface VLAN a une adresse MAC unique. Vous pouvez remplacer les adresses MAC générées si vous le souhaitez en attribuant manuellement des adresses MAC. Consultez [Configurer l'adresse MAC](#), à la page 66.

### Groupes de ponts

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

### Fonctionnalités non prises en charge de l'interface VLAN et du port de commutation

Les interfaces VLAN et les ports de commutation ne prennent pas en charge :

- Routage dynamique
- Routage multidiffusion
- Routage multiples chemins à coûts égaux (ECMP)
- Ensembles en ligne ou interfaces passives
- EtherChannels
- Basculement et lien d'état
- Balise du groupe de sécurité (SGT)

### Autres directives et limites

- Vous pouvez configurer un maximum de 60 interfaces nommées sur la Firepower 1010.
- Vous ne pouvez pas configurer l'interface Diagnostic comme port de commutation.

### Paramètres d'usine

- Ethernet 1/1 est une interface de pare-feu.
- Ethernet 1/2 à Ethernet 1/8 sont des ports de commutation affectés au VLAN 1.
- Vitesse et duplex par défaut: par défaut, la vitesse et le duplex sont configurés pour la négociation automatique.

## Configurer les ports de commutation et l'alimentation par Ethernet (PoE)

Pour configurer les ports de commutation et la PoE, procédez comme suit :

### Activer ou désactiver le mode Port de commutation

Vous pouvez définir chaque interface indépendamment comme interface de pare-feu ou comme port de commutation. Par défaut, Ethernet 1/1 est une interface de pare-feu et les autres interfaces Ethernet sont configurées comme des ports de commutation.

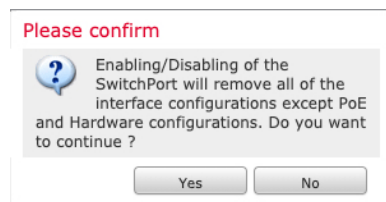
### Procédure

---

**Étape 1** Sélectionnez **Devices (périphériques) > Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

**Étape 2** Définissez le mode du port de commutation en faisant glisser le curseur dans la colonne **SwitchPort** pour qu'il s'affiche sous la forme **Curseur activé** (🔘) ou **Curseur désactivé** (🔘).

Par défaut, les ports de commutation sont définis sur le mode d'accès dans le VLAN 1. Vous devez ajouter manuellement une interface logique VLAN 1 (ou quel que soit le VLAN que vous définissez pour ces ports de commutation) pour que le trafic soit acheminé et qu'il participe à la politique de sécurité FTD (voir [Configurer une interface VLAN, à la page 5](#)). Vous ne pouvez pas définir l'interface de gestion sur le mode du port de commutation. Lorsque vous modifiez le mode du port du commutateur, toute la configuration non prise en charge est supprimée :



## Configurer une interface VLAN

Cette section décrit comment configurer les interfaces VLAN à utiliser avec les ports de commutation associés. Par défaut, les ports de commutation sont affectés au VLAN1; cependant, vous devez ajouter manuellement l'interface logique VLAN1 (ou le VLAN que vous définissez pour ces ports de commutation) pour que le trafic soit acheminé et participe à la politique de sécurité défense contre les menaces .

### Procédure

---

**Étape 1** Sélectionnez **Devices (périphériques) > Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

**Étape 2** Cliquez sur **Add Interfaces (ajouter des interfaces) > VLAN Interface (interface VLAN)**.

**Étape 3** Dans **Général**, définissez les paramètres propres au VLAN suivants :

### Add VLAN Interface ?

General
IPv4
IPv6
Advanced

Name:

Enabled

Description:

Mode:

Security Zone:

MTU:  
  
(64 - 9198)

Priority:  
 (0 - 65535)

VLAN ID \*:  
  
(1 - 4070)

Disable Forwarding on Interface Vlan:

Associated Interface	Port Mode
No records to display	

Si vous modifiez une interface VLAN existante, le tableau **des interfaces associées** affiche les ports de commutation sur ce VLAN.

- a) Définissez l' **ID de VLAN**, entre 1 et 4070, en excluant les ID de 3968 à 4047, qui sont réservés à un usage interne.

Vous ne pouvez pas modifier le numéro VLAN après avoir enregistré l'interface; le numéro VLAN est à la fois la balise VLAN utilisée et l'ID d'interface dans votre configuration.

- b) (Facultatif) Choisissez un ID de VLAN pour **Désactiver le transfert sur le VLAN de l'interface** pour désactiver le transfert vers un autre VLAN.

Par exemple, vous avez un VLAN affecté à l'extérieur pour l'accès Internet, un VLAN affecté à un réseau interne d'entreprise et un troisième VLAN affecté à votre réseau domestique. Le réseau domestique n'a pas besoin d'accéder au réseau de l'entreprise, vous pouvez donc désactiver le transfert sur le VLAN domestique; le réseau professionnel peut accéder au réseau domestique, mais le réseau domestique ne peut pas accéder au réseau d'entreprise.

**Étape 4** Pour terminer la configuration de l'interface, consultez l'une des procédures suivantes :

- [Configurer les interfaces en mode routé, à la page 39](#)
- [Configurer les paramètres généraux de l'interface de membre du groupe de ponts, à la page 44](#)

**Étape 5** Cliquez sur **OK**.

**Étape 6** Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer) > Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

---

## Configurer les ports de commutation comme ports d'accès

Pour affecter un port de commutation à un seul VLAN, configurez-le comme port d'accès. Les ports d'accès acceptent uniquement le trafic non balisé. Par défaut, Ethernet 1/2 à Ethernet 1/8 sont des ports de commutation affectés au VLAN 1.



---

**Remarque** L'appareil Firepower 1010 ne prend pas en charge le protocole Spanning Tree pour la détection de boucle dans le réseau. Par conséquent, vous devez vous assurer qu'une connexion avec le défense contre les menaces ne finit pas dans une boucle de réseau.

---

### Procédure

---

**Étape 1** Sélectionnez **Devices (périphériques) > Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

**Étape 2** Cliquez sur **Edit** (✎) pour l'interface que vous souhaitez modifier.

Illustration 1 : Modifier l'interface physique

Edit Physical Interface  
 General Hardware Configuration  
 Interface ID:  
 Ethernet1/2  
 Enabled  
 Description:  
  
 Port Mode:  
 Access  
 VLAN ID:  
 1  
 (1 - 4070)  
 Protected:

**Étape 3** Activez l'interface en cochant la case **Enabled** (activé).

**Étape 4** (Facultatif) Ajoutez une description dans le champ **Description**.

La description peut contenir jusqu'à 200 caractères sur une seule ligne (sans retour chariot).

**Étape 5** Définissez le **Mode de port** sur **Access**.

**Étape 6** Dans le champ **VLAN ID**, définissez le réseau VLAN pour ce port de commutation entre 1 et 4070.

L'ID VLAN par défaut est 1.

**Étape 7** (Facultatif) Cochez la case **Protected** (protégé) pour définir ce port de commutation comme protégé, afin de pouvoir l'empêcher de communiquer avec d'autres ports de commutation protégés sur le même VLAN.

Vous pourriez souhaiter empêcher les ports de commutation de communiquer entre eux dans les cas suivants : les périphériques sur ces ports de commutation sont principalement accessibles à partir d'autres VLAN; vous n'avez pas besoin d'autoriser l'accès intra-VLAN; et vous souhaitez isoler les périphériques les uns des autres en cas d'infection ou de toute autre faille de sécurité. Par exemple, si vous avez une DMZ qui héberge trois serveurs Web, vous pouvez isoler les serveurs Web les uns des autres si vous activez **Protected** sur chaque port de commutateur. Les réseaux interne et externe peuvent tous deux communiquer avec les trois serveurs Web, et inversement, mais les serveurs Web ne peuvent pas communiquer entre eux.

**Étape 8** (Facultatif) Définissez le mode duplex et la vitesse en cliquant sur **Hardware Configuration** (configuration matérielle).



Illustration 2 : Configurations du matériel

Edit Physical Interface

General Hardware Configuration

Speed

Duplex:  
full

Speed:  
1gbps

Auto-negotiation:

Cochez la case **Auto-negotiation** (Négociation automatique) (par défaut) pour détecter automatiquement la vitesse et le mode duplex. Si vous la décochez, vous pouvez définir la vitesse et le mode duplex manuellement :

- **Duplex** : choisissez entre **Full** ou **Half**.
- **Vitesse** : choisissez **10 Mbit/s** , **100 Mbit/s** ou **1 Gbit/s** .

**Étape 9**

Cliquez sur **OK**.

**Étape 10**

Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer)** > **Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

## Configurer les ports de commutation comme ports de ligne principale

Cette procédure décrit comment créer un port de liaison qui peut acheminer plusieurs VLAN à l'aide du balisage 802.1Q. Les ports de ligne principale acceptent le trafic non balisé et balisé. Le trafic sur les VLAN autorisés passe par le port de liaison sans changement.

Lorsque la ligne principale reçoit un trafic non balisé, elle le balise à l'ID de VLAN natif afin que l'ASA puisse transférer le trafic vers les ports de commutation appropriés ou l'acheminer vers une autre interface de pare-feu. Lorsque l'ASA envoie le trafic d'ID de VLAN natif hors du port de liaison, il supprime la balise VLAN. Assurez-vous de définir le même VLAN natif sur le port de liaison de l'autre commutateur afin que le trafic non balisé soit balisé vers le même VLAN.

### Procédure

**Étape 1**

Sélectionnez **Devices (périphériques)** > **Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

**Étape 2**

Cliquez sur **Edit** (✎) pour l'interface que vous souhaitez modifier.

Illustration 3 : Définir le mode du port de ligne principale

Edit Physical Interface

General Hardware Configuration

Interface ID:  
Ethernet1/2

Enabled

Description:

Port Mode:  
Trunk

Native VLAN ID:  
1  
(1 - 4070)

Allowed VLAN IDs:  
100,200,300  
(1 - 4070)

Protected:

**Étape 3** Activez l'interface en cochant la case **Enabled** (activé).

**Étape 4** (Facultatif) Ajoutez une description dans le champ **Description**.

La description peut contenir jusqu'à 200 caractères sur une seule ligne (sans retour chariot).

**Étape 5** Définissez le **mode du port** sur **Trunk** (Ligne principale).

**Étape 6** Dans le champ **Native VLAN ID**, définissez le VLAN natif pour ce port de commutation, entre 1 et 4070.

L'ID VLAN natif par défaut est 1.

Chaque port ne peut avoir qu'un seul VLAN natif, mais chaque port peut avoir le même VLAN natif ou un différent.

**Étape 7** Dans le champ **Allowed VLAN IDs** (ID de VLAN autorisés), saisissez les VLAN pour ce port de ligne principale entre 1 et 4070.

Vous pouvez identifier jusqu'à 20 identifiants de l'une des manières suivantes :

- Nombre unique (n)
- Plage A (n à x)
- Chiffres et plages séparés par des virgules, par exemple :

5,7-10,13,45-100

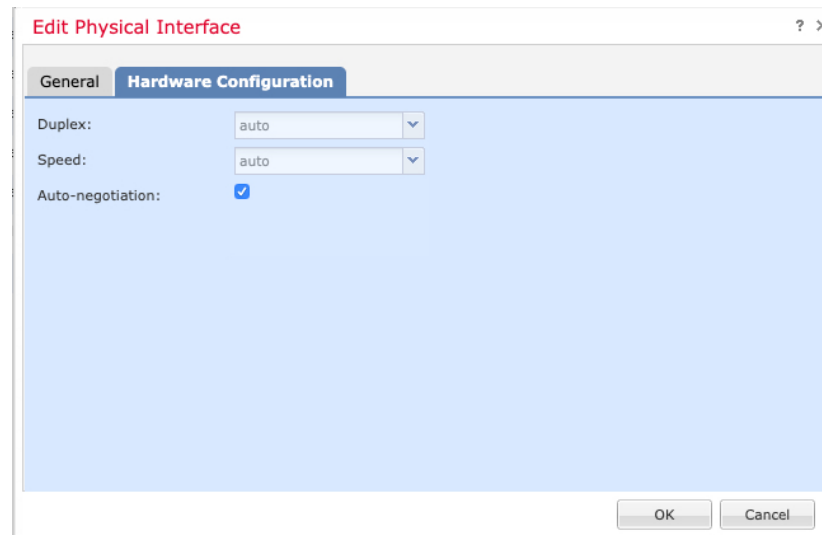
Vous pouvez utiliser des espaces au lieu de virgules.

Si vous incluez le VLAN natif dans ce champ, il est ignoré; Le port de liaison supprime toujours le balisage VLAN lors de l'envoi de trafic VLAN natif hors du port. De plus, il ne recevra pas le trafic qui a toujours un balisage VLAN natif.

**Étape 8** (Facultatif) Cochez la case **Protected** (protégé) pour définir ce port de commutation comme protégé, afin de pouvoir l'empêcher de communiquer avec d'autres ports de commutation protégés sur le même VLAN.

Vous pourriez souhaiter empêcher les ports de commutation de communiquer entre eux dans les cas suivants : les périphériques sur ces ports de commutation sont principalement accessibles à partir d'autres VLAN; vous n'avez pas besoin d'autoriser l'accès intra-VLAN; et vous souhaitez isoler les périphériques les uns des autres en cas d'infection ou de toute autre faille de sécurité. Par exemple, si vous avez une DMZ qui héberge trois serveurs Web, vous pouvez isoler les serveurs Web les uns des autres si vous activez **Protected** sur chaque port de commutateur. Les réseaux interne et externe peuvent tous deux communiquer avec les trois serveurs Web, et inversement, mais les serveurs Web ne peuvent pas communiquer entre eux.

**Étape 9** (Facultatif) Définissez le mode duplex et la vitesse en cliquant sur **Hardware Configuration** (configuration matérielle).



Cochez la case **Auto-negotiation** (Négociation automatique) (par défaut) pour détecter automatiquement la vitesse et le mode duplex. Si vous la décochez, vous pouvez définir la vitesse et le mode duplex manuellement :

- **Duplex** : choisissez entre **Full** ou **Half**.
- **Vitesse** : choisissez **10 Mbit/s** , **100 Mbit/s** ou **1 Gbit/s** .

**Étape 10** Cliquez sur **OK**.

**Étape 11** Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer) > Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

## Configurer Power Over Ethernet (alimentation électrique par câble Ethernet)

Ethernet 1/7 et Ethernet 1/8 prennent en charge Power over Ethernet (PoE) pour les périphériques tels que les téléphones IP ou les points d'accès sans fil. Le Firepower 1010 prend en charge IEEE 802.3af (PoE) et 802.3at (PoE+). PoE+ utilise le protocole LLDP (Link Layer Discovery Protocol) pour négocier le niveau de puissance. PoE+ peut fournir jusqu'à 30 W à un périphérique alimenté. L'alimentation n'est fournie qu'en cas de besoin.

Si vous désactivez le port de commutation ou que vous configurez le port comme interface de pare-feu, vous désactivez l'alimentation du périphérique .

La PoE est activée par défaut sur Ethernet 1/7 et Ethernet 1/8. Cette procédure décrit comment activer et désactiver la PoE et comment définir les paramètres facultatifs.

### Procédure

**Étape 1** Sélectionnez **Devices (périphériques) > Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

**Étape 2** Cliquez sur **Edit** (✎) pour Ethernet 1/7 ou 1/8.

**Étape 3** Cliquez sur **PoE**.

*Illustration 4 : Alimentation sur Ethernet (PoE)*

The screenshot shows the 'Edit Physical Interface' configuration page. The 'PoE' tab is selected. The 'Enable PoE' checkbox is checked. The 'Auto Negotiate Consumption Wattage' checkbox is also checked. The 'Consumption Wattage' field is empty, with a range of (4000 - 30000)mW indicated.

**Étape 4** Cochez la case **Enable PoE** (activer l'alimentation PoE).

Le mode PoE est activé par défaut.

**Étape 5** (Facultatif) Décochez la case **Auto Negotiate Consumption Wattage** (négociation automatique de la consommation en Watts) et saisissez la **consommation en Watts** si vous connaissez la puissance exacte en Watts dont vous avez besoin.

Par défaut, PoE fournit automatiquement du courant au périphérique alimenté en utilisant une puissance appropriée pour la classe du périphérique alimenté. L'appareil Firepower 1010 utilise LLDP pour négocier davantage la puissance en Watts. Si vous connaissez la puissance en Watts et souhaitez désactiver la négociation LLDP, saisissez une valeur comprise entre 4 000 et 30 000 milliwatts.

**Étape 6** Cliquez sur **OK**.

**Étape 7** Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer) > Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

## Configurer les interfaces de bouclage

Cette section explique comment configurer les interfaces de boucle avec retour.

## À propos des interfaces de boucle avec retour

Une interface de boucle avec retour est une interface logicielle uniquement qui émule une interface physique. Cette interface est accessible sur IPv4 et IPv6 par l'intermédiaire de plusieurs interfaces physiques. L'interface de boucle avec retour permet de résoudre les échecs de chemin. elle est accessible à partir de n'importe quelle interface physique. Par conséquent, si l'une d'elles tombe en panne, vous pouvez accéder à l'interface de boucle avec retour à partir d'une autre.

Les interfaces de boucle avec retour peuvent être utilisées pour :

- Tunnels VTI statiques et dynamiques

La défense contre les menaces peut distribuer l'adresse de boucle avec retour à l'aide de protocoles de routage dynamique, ou vous pouvez configurer une voie de routage statique sur le périphérique homologue pour atteindre l'adresse IP de boucle avec retour par l'une des interfaces physiques de défense contre les menaces. Vous ne pouvez pas configurer une voie de routage statique sur défense contre les menaces qui spécifie l'interface de boucle avec retour.

### Sujets connexes

[Directives et limites pour les interfaces de boucle avec retour](#), à la page 13

[Configurer une interface de boucle avec retour](#), à la page 13

## Directives et limites pour les interfaces de boucle avec retour

### Mode pare-feu

- Pris en charge en mode routé uniquement.

### High Availability (haute disponibilité) et mise en grappe

- Aucune prise en charge de mise en grappe.

### Directives et limites additionnelles

- La répartition aléatoire des séquences TCP est toujours désactivée pour le trafic de l'interface physique à l'interface de boucle avec retour.

## Configurer une interface de boucle avec retour

Pour ajouter une interface de boucle avec retour pour un périphérique :

### Procédure

- 
- Étape 1** Sélectionnez **Devices (périphériques) > Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.
- Étape 2** Dans la liste déroulante **Add Interfaces** (ajouter des interfaces), choisissez **Loopback Interface** (interface de boucle avec retour).
- Étape 3** Dans l'onglet **General** (Général), configurez les paramètres suivants :

- a) **Name** (Nom) : saisissez un nom pour l'interface de boucle avec retour.
- b) **Enabled** (Activé) : cochez la case pour activer l'interface de boucle avec retour.
- c) **Loopback ID** (ID de boucle avec retour) : Saisissez l'ID de boucle avec retour entre 1 et 1024.
- d) **Description** : saisissez une description pour l'interface de boucle avec retour.

**Étape 4**

Configurer les paramètres de l'interface en mode routé. Consultez [Configurer les interfaces en mode routé](#), à la page 39.

## Limite de débit du trafic vers l'interface de boucle avec retour

**Avant de commencer**

Vous devez limiter le trafic vers l'adresse IP de l'interface de boucle avec retour pour éviter une charge excessive sur le système. Vous pouvez ajouter une règle de limite de connexion à la politique de service globale.

**Procédure****Étape 1**

Créez une liste d'accès étendue identifiant le trafic vers les adresses IP de l'interface de boucle avec retour.

- a) Choisissez **Objets > Gestion des objets** et choisissez **Listes de contrôle d'accès > Étendu** dans la table des matières.
- b) Cliquez sur **Ajouter une liste d'accès étendue** pour créer une nouvelle ACL.
- c) Dans la boîte de dialogue **New Extended Access List Object** (nouvel objet de liste d'accès étendu), saisissez un nom pour la liste d'accès (aucune espace autorisé), puis cliquez sur **Add** (ajouter) pour créer une nouvelle entrée.

**Illustration 5 : Nommez l'ACL et ajoutez l'entrée**

New Extended Access List Object

Name  
rate-limiting

Entries (0)

Add

- d) Configurez les adresses de source (n'importe quelle) et de destination (adresses IP de boucle avec retour) sous l'onglet **Network** (réseau).

Illustration 6 : Réseau source et de destination

**Remarque** Conservez l'action par défaut sur **Autoriser** (correspondance) et les autres paramètres tels quels.

- Source : Sélectionnez **any** dans la liste des **réseaux disponibles**, puis cliquez sur **Add to Source** (Ajouter à la source). Vous pouvez également restreindre cette liste d'accès en spécifiant les adresses IP source plutôt que **any**.
- Destination : Saisissez une adresse dans la zone d'édition sous la liste des **réseaux de destination** et cliquez sur **Add** (Ajouter). Répétez l'opération pour chaque interface de boucle avec retour.

- e) Cliquez sur **Add** pour ajouter l'entrée à la liste de contrôle d'accès.
- f) Cliquez sur **Save** (Enregistrer) pour enregistrer la liste de contrôle d'accès.

**Illustration 7 : Enregistrer la liste de contrôle d'accès**

Edit Extended Access List Object

Name  
rate-limiting

Entries (1)

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT	
1	Allow	any	Any	10.1.1.1 10.2.1.1	Any	Any	Any	Any	

Allow Overrides

Cancel Save

**Étape 2**

Choisissez **Politiques > Contrôle d'accès > Contrôle d'accès** et cliquez sur **Edit** (✎) pour la politique de contrôle d'accès attribuée à votre périphérique.

**Étape 3**

Cliquez sur **Advanced Settings** (paramètres avancés) à partir de la flèche de la liste déroulante **More** (Plus) à la fin de la ligne de flux de paquets.

**Illustration 8 : Paramètres avancés**

in-out ✎

Packets → Prefilter Rules → Decryption → Security Intelligence → Identity → Access Control → More

Type to search

Name	Action	Zones	Networks	Source
Mandatory (1 - 1)				

Advanced Settings  
HTTP Responses  
Inheritance Settings  
Logging

**Étape 4**

Cliquez sur **Edit** (✎) dans le groupe de politiques du service **Threat Defense**.

**Illustration 9 : Politique du service Threat Defense**

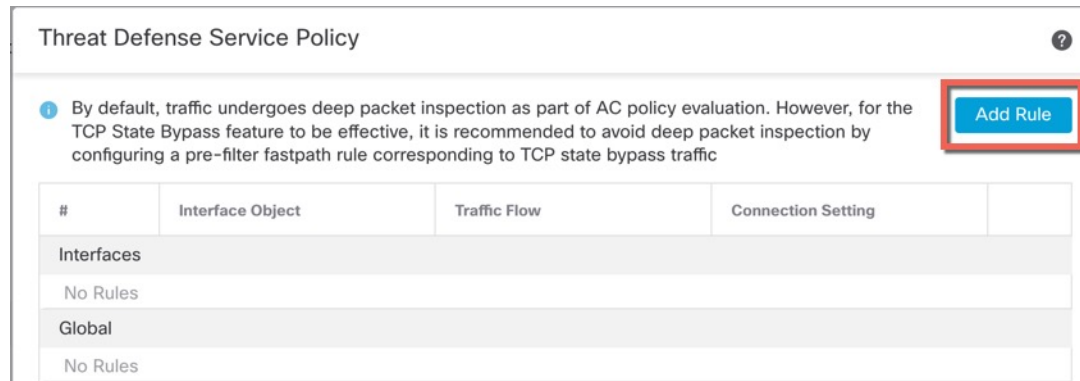
Threat Defense Service Policy

Threat Defense Service Rule(s) 0

**Étape 5**

Cliquez sur **Add Rule** (Ajouter une règle) pour créer une nouvelle règle.



**Illustration 10 : Ajouter une règle**

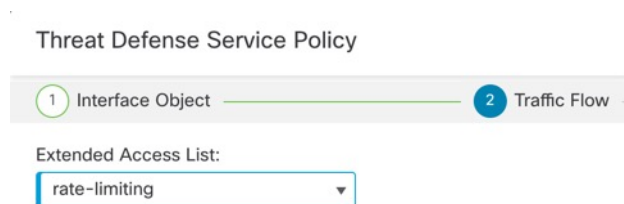
L'assistant de règle de politique de service s'ouvre pour vous guider dans le processus de configuration de la règle.

**Étape 6**

À l'étape **Interface Object** (objet d'interface), cliquez sur **Global** pour créer une règle globale, qui s'applique à toutes les interfaces, puis cliquez sur **Next**(suivant).

**Illustration 11 : Politique mondiale****Étape 7**

À l'étape du **flux de trafic**, sélectionnez l'objet de liste d'accès étendu que vous avez créé dans [Étape 1](#), à la [page 14](#), puis cliquez sur **Next** (suivant).

**Illustration 12 : Choisissez Liste d'accès étendue****Étape 8**

À l'étape **Connection Settings** (paramètres de connexion), définissez les limites de **connexions**.

Illustration 13 : Définir les limites de connexion

Threat Defense Service Policy

1 Interface Object — 2 Traffic Flow — 3 Connection Setting

Enable TCP State Bypass  Randomize TCP Sequence Number  Enable Decrement TTL

Connections:	Maximum TCP & UDP 24	Maximum Embryonic 12
Connections Per Client:	Maximum TCP & UDP 0	Maximum Embryonic 0

Définissez le nombre **maximal de connexions TCP et UDP** sur le nombre attendu de connexions pour l'interface de boucle avec retour et le **nombre maximal de connexions amorcées** à un nombre inférieur. Par exemple, vous pouvez lui régler la valeur 5/2, 10/5 ou 1024/512, selon le nombre de sessions d'interface de boucle avec retour attendues dont vous avez besoin.

La définition de la limite de connexions amorcées active l'interception de TCP, qui protège le système contre une attaque DoS perpétrée en inondant une interface de paquets SYN de TCP.

**Étape 9**

Cliquez sur le bouton « **Finish** » (terminer) pour enregistrer vos modifications.

**Étape 10**

Cliquez sur **OK**.

**Étape 11**

Cliquez sur **Save** (Enregistrer) dans la fenêtre **Advanced Settings** (paramètres avancés).

**Étape 12**

Vous devez déployer les modifications sur les périphériques concernés.

## Configurer les sous-interfaces VLAN et la jonction 802.1Q

Les sous-interfaces VLAN vous permettent de diviser une interface physique en plusieurs interfaces logiques qui sont étiquetées avec différents ID de VLAN. Une interface avec une ou plusieurs sous-interfaces VLAN est automatiquement configurée comme une ligne principale 802.1Q. Comme les réseaux VLAN vous permettent de conserver le trafic séparé sur une interface physique donnée, vous pouvez augmenter le nombre d'interfaces disponibles pour votre réseau sans ajouter d'interfaces physiques ou de périphériques supplémentaires.

## Lignes directrices et limites pour les sous-interfaces VLAN

### Prise en charge des modèles

- Firepower 1010 : Les sous-interfaces VLAN ne sont pas prises en charge sur les ports de commutation ou les interfaces VLAN.

### Haute disponibilité et mise en grappe

Vous ne pouvez pas utiliser de sous-interface pour le lien de basculement ou d'état ou pour la liaison de commande de grappe. Le mode multi-instance constitue une exception : vous pouvez utiliser une sous-interface définie par le *châssis* pour ces liaisons.

### Directives supplémentaires

- Prévention des paquets non balisés sur l'interface physique : Si vous utilisez des sous-interfaces, vous ne souhaitez généralement pas que l'interface physique achemine le trafic, car l'interface physique peut transmettre des paquets non balisés. Cette propriété est également vraie pour l'interface physique active dans une paire d'interfaces redondantes et pour les liaisons EtherChannel. Étant donné que l'interface physique doit être activée pour que la sous-interface achemine le trafic, assurez-vous que l'interface physique ne transmet pas le trafic en ne nommant pas l'interface. Si vous voulez laisser l'interface physique, redondante ou EtherChannel passer des paquets non balisés, vous pouvez configurer le nom comme d'habitude.
- Vous ne pouvez pas configurer de sous-interface sur l'interface de gestion.
- Toutes les sous-interfaces de la même interface parente doivent soit être des membres de groupes de ponts, soit des interfaces routées; vous ne pouvez pas combiner les deux types.
- défense contre les menaces ne prend pas en charge le protocole DTP (Dynamic Trunking Protocol), vous devez donc configurer le port de commutation connectée pour qu'il assure la liaison sans condition.
- Vous pourriez souhaiter affecter des adresses MAC uniques aux sous-interfaces définies sur défense contre les menaces, car elles utilisent la même adresse MAC gravée de l'interface parente. Par exemple, votre fournisseur de services peut effectuer un contrôle d'accès en fonction de l'adresse MAC. En outre, étant donné que les adresses locales de lien IPv6 sont générées en fonction de l'adresse MAC, l'affectation d'adresses MAC uniques aux sous-interfaces permet d'établir des adresses locales de lien IPv6 uniques, ce qui peut éviter des perturbations de trafic dans certaines instances sur défense contre les menaces.

## Nombre maximal de sous-interfaces VLAN par modèle de périphérique

Le modèle de périphérique limite le nombre maximal de sous-interfaces VLAN que vous pouvez configurer. Notez que vous pouvez configurer des sous-interfaces sur les interfaces de données uniquement, vous ne pouvez pas les configurer sur l'interface de gestion.

Le tableau suivant explique les limites pour chaque modèle de périphérique.

Modèle	Sous-interfaces VLAN maximales
Firepower 1010	60
Firepower 1120	512
Firepower 1140, 1150	1024
Firepower de la série 2100	1024
Secure Firewall 3100	1024
Firepower 4100	1024
Firepower 9300	1024

Modèle	Sous-interfaces VLAN maximales
Défense contre les menaces virtuelles	50
ISA 3000	100

## Ajouter une sous-interface

Ajouter une ou plusieurs sous-interfaces à une interface physique, redondante ou de canal de port.

Pour Firepower 4100/9300, vous pouvez configurer les sous-interfaces dans FXOS à utiliser avec les instances de conteneur; voir [Ajouter une sous-interface VLAN pour les instances de conteneur](#). Ces sous-interfaces apparaissent dans la liste des interfaces centre de gestion. Vous pouvez également ajouter des sous-interfaces dans centre de gestion, mais uniquement sur les interfaces parentes qui n'ont pas encore de sous-interfaces définies dans FXOS.



**Remarque** L'interface physique parente transmet des paquets non étiquetés. Vous ne souhaitez peut-être pas transmettre de paquets non étiquetés, alors assurez-vous de ne pas inclure l'interface parente dans votre politique de sécurité.

### Procédure

- Étape 1** Sélectionnez **Devices (périphériques) > Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.
- Étape 2** Activer l'interface parente en fonction de [Activer l'interface physique et configurer des paramètres Ethernet](#).
- Étape 3** Cliquez sur **Add Interfaces (ajoutez des interfaces) > VLAN Interface (interfaces VLAN)**.
- Étape 4** Sous **General** (Général), définissez les paramètres suivants :

Illustration 14 : Ajouter une sous-interface

**Add Sub Interface** ?

General IPv4 IPv6 Path Monitoring Advanced

Name:

Enabled  
 Management Only

Description:

Security Zone:

MTU:  
  
(64 - 9198)

Priority:  
  
(0 - 65535)

Propagate Security Group Tag:

Interface \*:

Enabled

Sub-Interface ID \*:  
  
(1 - 4294967295)

VLAN ID:  
  
(1 - 4094)

Cancel OK

- Interface** : choisissez l'interface physique, redondante ou de canal de port à laquelle vous souhaitez ajouter la sous-interface.
- Sub-Interface ID** (ID de sous-interface) : saisissez l'ID de la sous-interface sous la forme d'un nombre entier compris entre 1 et 4294967295. Le nombre de sous-interfaces autorisés dépend de votre plateforme. Vous ne pouvez pas modifier l'ID après l'avoir défini.
- VLAN ID**(ID du VLAN) : saisissez l'ID du VLAN entre 1 et 4094 qui sera utilisé pour étiqueter les paquets sur cette sous-interface.  
 Cet ID de VLAN doit être unique.

**Étape 5**Cliquez sur **OK**.**Étape 6**Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer) > Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

**Étape 7** Configurez les paramètres d'interface en mode routé ou transparent. Reportez-vous aux sections [Configurer les interfaces en mode routé](#), à la page 39 ou [Configurer les interfaces de groupe de ponts](#), à la page 44.

---

## Configurer les interfaces VXLAN

Ce chapitre explique comment configurer des interfaces Virtual eXtensible LAN (VXLAN). Les interfaces VXLAN agissent comme des réseaux virtuels de couche 2 sur des réseaux physiques de couche 3 pour étendre les réseaux de couche 2.

### À propos des interfaces VXLAN

Le réseau VXLAN fournit les mêmes services de réseau Ethernet de couche 2 que le réseau VLAN, mais avec une extensibilité et une flexibilité accrues. Par rapport au VLAN, le VXLAN offre les avantages suivants :

- Emplacement flexible des segments multidétenteurs dans le centre de données.
- Évolutivité accrue pour traiter un plus grand nombre de segments de couche 2 : jusqu'à 16 millions de segments VXLAN.

Cette section décrit le fonctionnement de VXLAN. Pour en savoir plus sur VXLAN, consultez RFC 7348. Pour des informations détaillées sur Geneve, consultez RFC 8926.

### Encapsulation

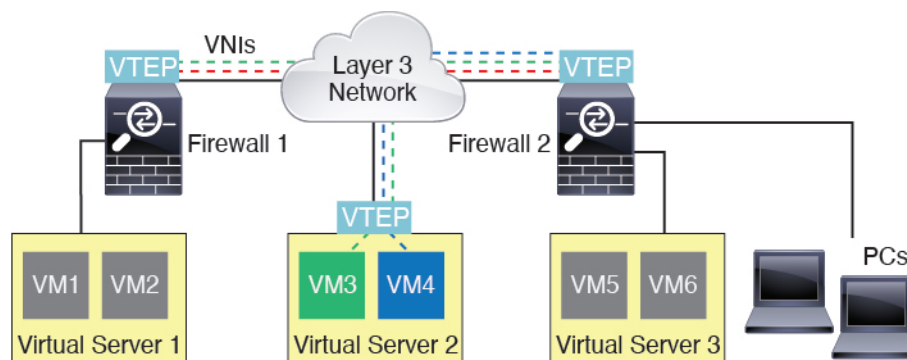
défense contre les menaces prend en charge deux types d'encapsulation VXLAN :

- VXLAN (tous les modèles) : VXLAN utilise l'encapsulation MAC Address-in-User Datagram Protocol (MAC-in-UDP). Un en-tête VXLAN est ajouté à la trame de couche 2 d'origine, qui est ensuite placée dans un paquet UDP-IP.
- Geneve (défense contre les menaces virtuelles uniquement) : Geneve a un en-tête interne flexible qui ne se limite pas à l'adresse MAC. L'encapsulation Geneve est requise pour un routage transparent des paquets entre un équilibreur de charge de passerelle Amazon Web Services (AWS) et les périphériques, et pour l'envoi d'informations supplémentaires.

### Point terminal du tunnel VXLAN

Les périphériques de point terminal de tunnel VXLAN (VTEP) effectuent l'encapsulation et la désencapsulation VXLAN. Chaque VTEP a deux types d'interface : une ou plusieurs interfaces virtuelles appelées interfaces VNI (VXLAN Network Identifier) auxquelles vous appliquez votre politique de sécurité, et une interface normale appelée l'interface source VTEP qui canalise les interfaces VNI entre les VTEP. L'interface source du VTEP est connectée au réseau IP de transport pour la communication de VTEP à VTEP.

La figure suivante montre deux défense contre les menaces et le serveur virtuel 2 agissant comme des VTEP dans un réseau de couche 3 et étendant les réseaux VNI 1, 2 et 3 entre les sites. Les défense contre les menaces agissent comme des ponts ou des passerelles entre les réseaux VXLAN et les non-VXLAN.



Le réseau IP sous-jacent entre les VTEP est indépendant de la superposition VXLAN. Les paquets encapsulés sont acheminés en fonction de l'en-tête d'adresse IP externe, qui a le VTEP de départ comme adresse IP source et le VTEP de fin comme adresse IP de destination. Pour l'encapsulation VXLAN : l'adresse IP de destination peut être un groupe de multidiffusion lorsque le VTEP distant est inconnu. À Geneve, la défense contre les menaces ne prend en charge que les homologues statiques. Le port de destination de VXLAN est le port UDP 4789 par défaut (configurable par l'utilisateur). Le port de destination pour Geneve est le 6081.

## Interface de la source VTEP

L'interface source de VTEP est une interface normale (physique, EtherChannel ou même VLAN) à laquelle vous prévoyez d'associer toutes les interfaces VNI. Vous pouvez configurer une interface source de VTEP par défense contre les menaces virtuelles. Comme vous ne pouvez configurer qu'une seule interface source de VTEP, vous ne pouvez pas configurer les deux interfaces VXLAN et Geneve sur le même périphérique. Il y a une exception pour la mise en grappe de défense contre les menaces virtuelles sur AWS ou Azure, où vous pouvez avoir deux interfaces sources VTEP : une interface VXLAN est utilisée pour la liaison de commande de grappe, et une interface Geneve (AWS) ou VXLAN (Azure) peut être utilisée pour l'équilibreur de charge de la passerelle.

L'interface source du VTEP peut être entièrement dédiée au trafic VXLAN, bien qu'elle ne se limite pas à cet usage. Si vous le souhaitez, vous pouvez utiliser l'interface pour le trafic normal et appliquer une politique de sécurité à l'interface pour ce trafic. Pour le trafic VXLAN, cependant, toute la politique de sécurité doit être appliquée aux interfaces VNI. L'interface VTEP sert uniquement de port physique.

En mode de pare-feu transparent, l'interface source de VTEP ne fait pas partie d'un BVI, et vous configurez une adresse IP pour elle, similaire à la façon dont l'interface de gestion est traitée.

## Interface VNIs

Les interfaces VNI sont similaires aux interfaces VLAN : ce sont des interfaces virtuelles qui séparent le trafic réseau sur une interface physique donnée en utilisant le balisage. Vous appliquez votre politique de sécurité directement à chaque interface VNI.

Vous ne pouvez ajouter qu'une seule interface VTEP et toutes les interfaces VNI sont associées à la même interface VTEP. Il existe une exception pour la mise en grappe de défense contre les menaces virtuelles sur AWS ou Azure. Pour la mise en grappe d'AWS, vous pouvez avoir deux interfaces source VTEP : une interface VXLAN est utilisée pour la liaison de commande de grappe et une interface Geneve peut être utilisée pour AWS Gateway Load Balancer. Pour la mise en grappe Azure, vous pouvez avoir deux interfaces source VTEP : une interface VXLAN est utilisée pour la liaison de commande de grappe et une deuxième interface VXLAN peut être utilisée pour l'équilibreur de charge de passerelle Azure.

## Traitements de paquet VXLAN

### VXLAN

Le trafic entrant et sortant de l'interface source du VTEP est soumis au traitement VXLAN, en particulier à l'encapsulation ou à la désencapsulation.

Le traitement d'encapsulation comprend les tâches suivantes :

- L'interface source du VTEP encapsule la trame MAC interne avec l'en-tête VXLAN.
- Le champ de la somme de contrôle UDP est mis à zéro.
- L'adresse IP de la source de trame externe est définie sur l'adresse IP de l'interface VTEP.
- L'adresse IP de destination de la trame externe est déterminée par une recherche IP distante du VTEP.

Désencapsulation; le défense contre les menaces désencapsule un paquet VXLAN uniquement dans les cas suivants :

- Il s'agit d'un paquet UDP dont le port de destination est 4789 (cette valeur peut être configurée par l'utilisateur).
- L'interface d'entrée est l'interface source du VTEP.
- L'adresse IP de l'interface d'entrée est la même que l'adresse IP de destination.
- Le format des paquets VXLAN est conforme à la norme.

### Geneve

Le trafic entrant et sortant de l'interface source du VTEP est soumis au traitement de Geneve, en particulier à l'encapsulation ou à la désencapsulation.

Le traitement d'encapsulation comprend les tâches suivantes :

- L'interface source du VTEP encapsule la trame MAC interne avec l'en-tête Geneve.
- Le champ de la somme de contrôle UDP est mis à zéro.
- L'adresse IP de la source de trame externe est définie sur l'adresse IP de l'interface VTEP.
- L'adresse IP de destination de la trame externe est définie sur l'adresse IP homologue que vous avez configurée.

désencapsulation; l'ASA désencapsule un paquet Geneve uniquement dans les cas suivants :

- Il s'agit d'un paquet UDP dont le port de destination est 6081 (cette valeur peut être configurée par l'utilisateur).
- L'interface d'entrée est l'interface source du VTEP.
- L'adresse IP de l'interface d'entrée est la même que l'adresse IP de destination.
- Le format des paquets Geneve est conforme à la norme.



## VTEP homologues

Lorsque le défense contre les menaces envoie un paquet à un périphérique derrière un VTEP homologue, le défense contre les menaces a besoin de deux informations importantes :

- L'adresse MAC de destination du périphérique distant
- L'adresse IP de destination du VTEP homologue

le défense contre les menaces gère un mappage des adresses MAC de destination sur les adresses IP du VTEP distant pour les interfaces VNI.

### Homologue VXLAN

le défense contre les menaces peut trouver cette information de deux manières :

- Une adresse IP VTEP homologue unique peut être configurée de manière statique sur le défense contre les menaces .  
: le défense contre les menaces envoie ensuite une diffusion ARP encapsulée dans VXLAN au VTEP pour connaître l'adresse MAC du nœud d'extrémité.
- Un groupe d'adresses IP VTEP homologues peut être configurée de manière statique sur défense contre les menaces .  
: le défense contre les menaces envoie ensuite une diffusion ARP encapsulée dans VXLAN au VTEP pour connaître les adresses MAC du nœud d'extrémité.
- Un groupe de multidiffusion peut être configuré sur chaque interface VNI (ou sur le VTEP dans son ensemble).  
: le défense contre les menaces envoie un paquet de diffusion ARP encapsulé dans VXLAN dans un paquet IP de multidiffusion par l'intermédiaire de l'interface source de VTEP. La réponse à cette requête ARP permet au défense contre les menaces d'apprendre à la fois l'adresse IP du VTEP distant ainsi que l'adresse MAC de destination du nœud d'extrémité distant.

Cette option n'est pas prise en charge par Geneve.

### Homologue Geneve

Le défense contre les menaces virtuelles ne prend en charge que les homologues définis de manière statique. Vous pouvez définir l'adresse IP homologue défense contre les menaces virtuelles sur l'équilibreur de charge de passerelle AWS. Comme défense contre les menaces virtuelles n'initie jamais le trafic vers l'équilibreur de charge de passerelle, vous n'avez pas besoin de préciser l'adresse IP de l'équilibreur de charge de passerelle sur défense contre les menaces virtuelles; il connaît l'adresse IP homologue lorsqu'il reçoit le trafic de Geneve. Les groupes de multidiffusion ne sont pas pris en charge avec Geneve.

## Scénarios VXLAN

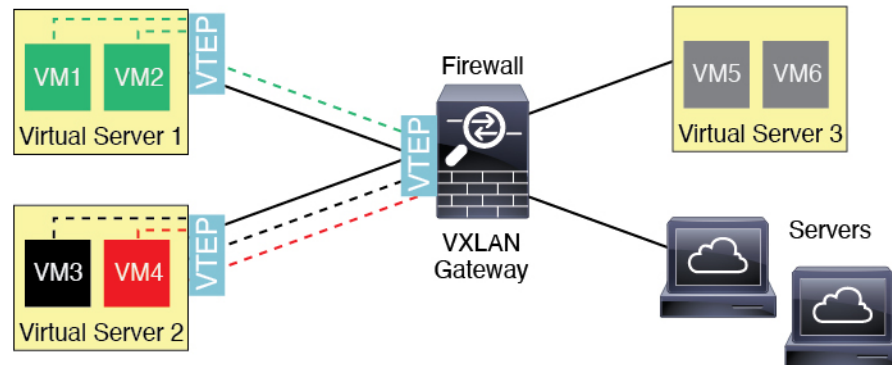
Cette section décrit les scénarios d'utilisation de la mise en œuvre de VXLAN sur défense contre les menaces .

### Présentation du pont ou de la passerelle VXLAN

Chaque VTEP défense contre les menaces agit comme un pont ou une passerelle entre les nœuds terminaux comme les machines virtuelles, les serveurs et les PC et le réseau de superposition VXLAN. Pour les trames

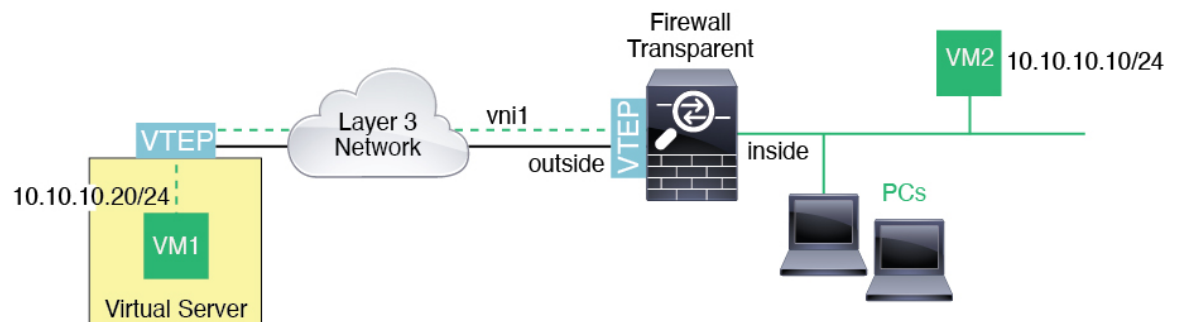
entrantes reçues avec encapsulation VXLAN sur l'interface source de VTEP, défense contre les menaces supprime l'en-tête VXLAN et le transfère vers une interface physique connectée à un réseau non VXLAN en fonction de l'adresse MAC de destination de la trame Ethernet interne.

Le défense contre les menaces traite toujours les paquets VXLAN; il ne se contente pas de transférer des paquets VXLAN inchangés entre deux autres VTEP.



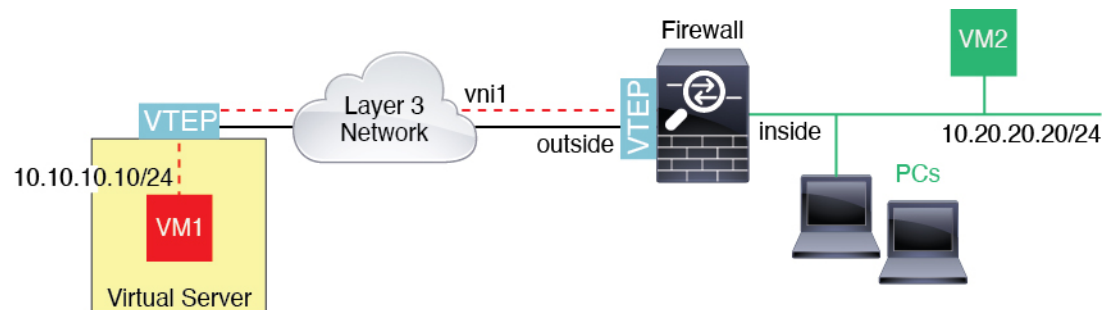
### Pont VXLAN

Lorsque vous utilisez un groupe de ponts (mode de pare-feu transparent ou mode de routage facultatif), défense contre les menaces peut servir de pont VXLAN entre un segment VXLAN (distant) et un segment local, où les deux se trouvent dans le même réseau. Dans ce cas, un membre du groupe de ponts est une interface standard tandis que l'autre membre est une interface VNI.



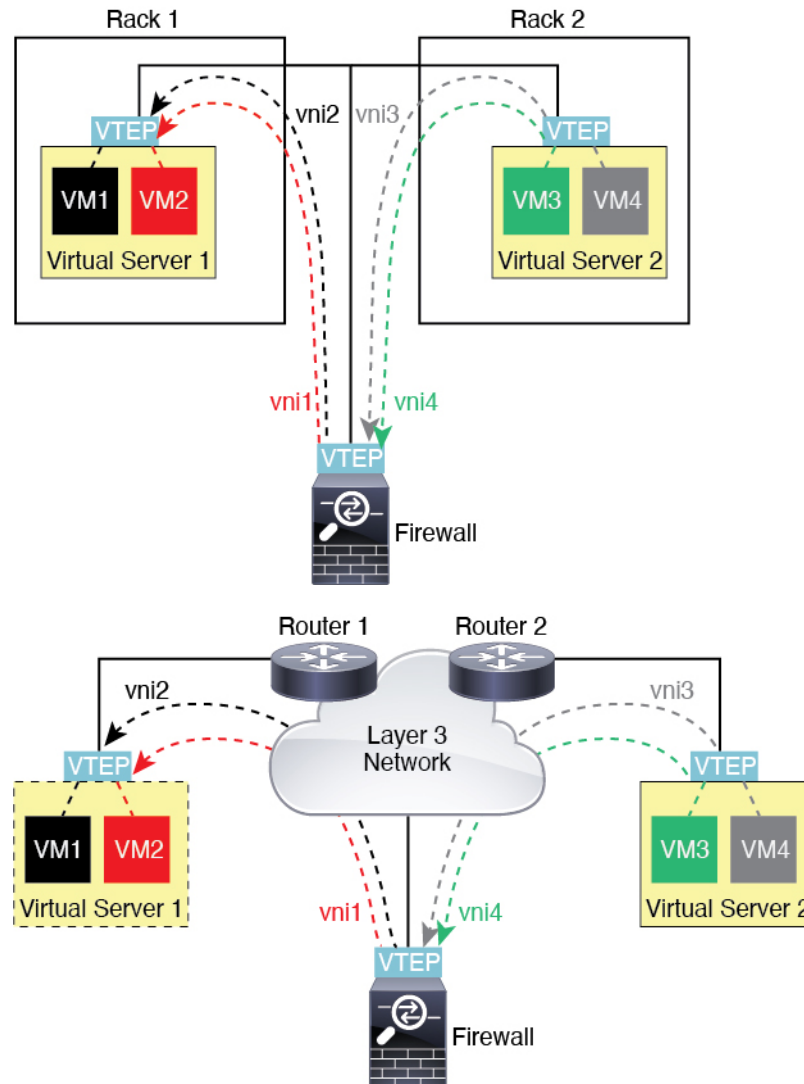
### Passerelle VXLAN (mode routé)

Le défense contre les menaces peut servir de routeur entre les domaines VXLAN et non-VXLAN, connectant des périphériques sur différents réseaux.



## Routeur entre domaines VXLAN

Avec un domaine de couche 2 étendu par VXLAN, une machine virtuelle peut pointer vers un défense contre les menaces comme passerelle lorsque défense contre les menaces ne se trouve pas sur le même rack, ou même lorsque défense contre les menaces est éloigné sur le réseau de couche 3.



Consultez les remarques suivantes à propos de ce scénario :

1. Pour les paquets de la VM3 à la VM1, l'adresse MAC de destination est l'adresse MAC défense contre les menaces, car défense contre les menaces est la passerelle par défaut.
2. L'interface source de VTEP sur le serveur virtuel 2 reçoit les paquets de VM3, puis encapsule les paquets avec la balise VXLAN de VNI 3 et les envoie à défense contre les menaces.
3. Lorsque le défense contre les menaces reçoit les paquets, il désencapsule les paquets pour obtenir les trames internes.

- Le défense contre les menaces utilise les cadres internes pour la recherche de routage, puis trouve que la destination est sur VNI 2. S'il n'a pas encore de mappage pour VM1, défense contre les menaces envoie une diffusion ARP encapsulée sur l'adresse IP du groupe de multidiffusion sur VNI 2.



**Remarque** Le défense contre les menaces doit utiliser la découverte d'homologues VTEP dynamique, car il a plusieurs homologues VTEP dans ce scénario.

- défense contre les menaces encapsule de nouveau les paquets avec la balise VXLAN pour VNI 2 et envoie les paquets au serveur virtuel 1. Avant l'encapsulation, défense contre les menaces modifie l'adresse MAC de destination de la trame interne pour qu'elle corresponde à l'adresse MAC de VM1 (l'ARP encapsulé en multidiffusion peut être nécessaire pour que défense contre les menaces apprenne l'adresse MAC de VM1).
- Lorsque le serveur virtuel 1 reçoit les paquets VXLAN, il désencapsule les paquets et achemine les trames internes à la VM1.

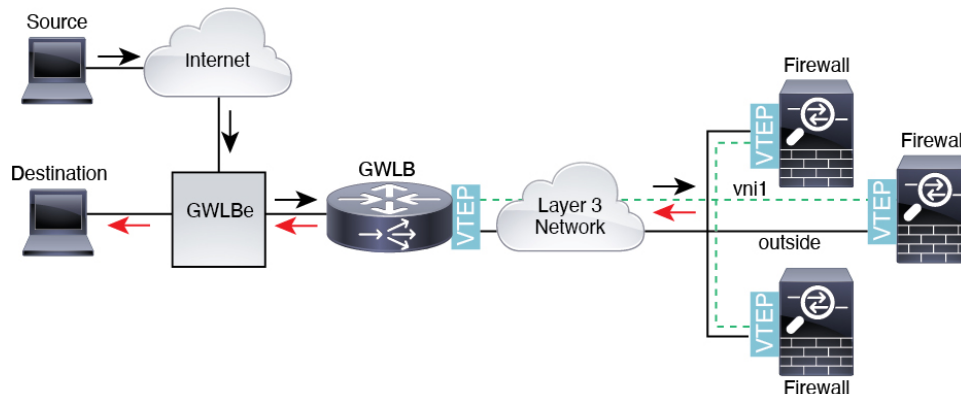
### Scénario de serveur mandataire à un seul groupe



**Remarque** Ce scénario est le seul actuellement pris en charge pour les interfaces de Geneve.

L'équilibreur de charge de passerelle AWS combine une passerelle de réseau transparente et un équilibreur de charge qui répartit le trafic et fait évoluer les périphériques virtuels à la demande. Le défense contre les menaces virtuelles prend en charge le plan de contrôle centralisé de l'équilibreur de charge de passerelle avec un plan de données distribué (point terminal de l'équilibreur de charge de passerelle). La figure suivante montre le trafic acheminé vers l'équilibreur de charge de passerelle à partir du point terminal de l'équilibreur de charge de passerelle. L'équilibreur de charge de passerelle équilibre le trafic entre plusieurs défense contre les menaces virtuelles, qui inspectent le trafic avant de l'abandonner ou de le renvoyer à l'équilibreur de charge de passerelle (trafic à demi-tour). L'équilibreur de charge de passerelle renvoie ensuite le trafic au point terminal de l'équilibreur de charge de passerelle et à la destination.

**Illustration 15 : Serveur mandataire à un seul volet Geneve**



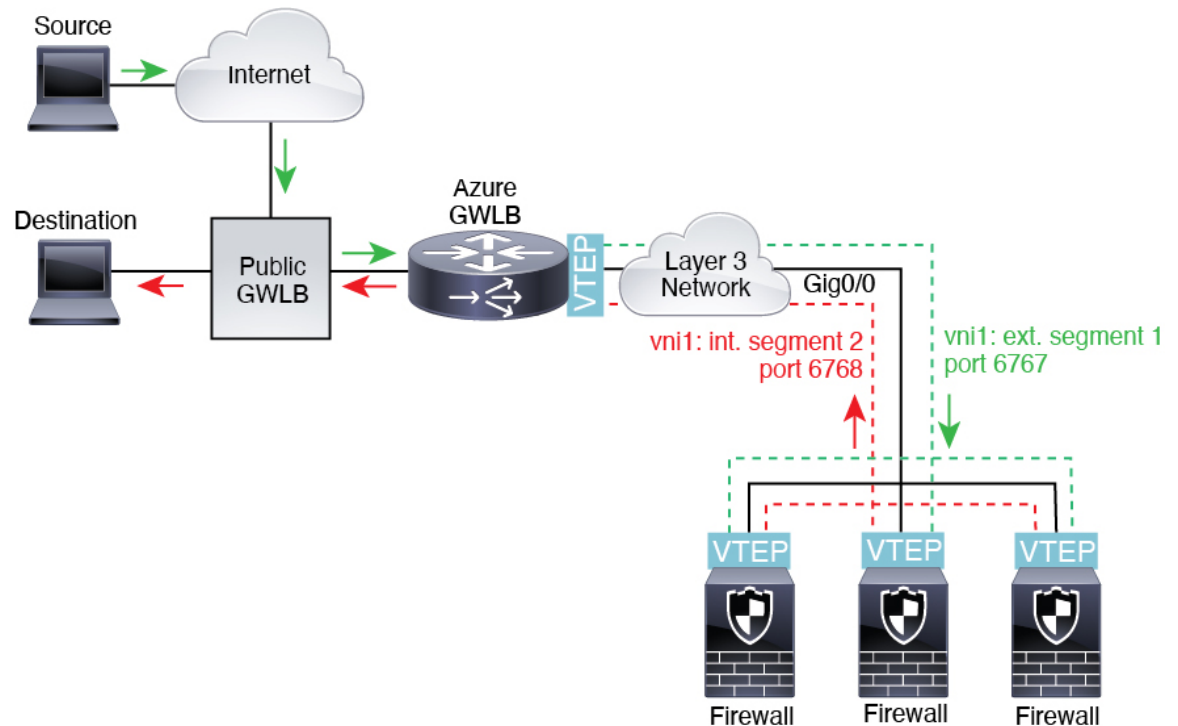
### Équilibreur de charge de passerelle Azure et serveur mandataire jumelé

Dans une chaîne de service Azure, les défense contre les menaces virtuelles agissent comme une passerelle transparente qui peut intercepter les paquets entre Internet et le service client. Le défense contre les menaces

virtuelles définit une interface externe et une interface interne sur une seule carte réseau en utilisant les segments VXLAN dans un serveur mandataire apparié.

La figure suivante montre le trafic transféré vers l'équilibreur de charge de passerelle Azure à partir de l'équilibreur de charge de passerelle publique sur le segment VXLAN externe. L'équilibreur de charge de passerelle équilibre le trafic entre plusieurs défense contre les menaces virtuelles, qui inspectent le trafic avant de l'abandonner ou de le renvoyer à l'équilibreur de charge de passerelle sur le segment VXLAN interne. L'équilibreur de charge de passerelle Azure renvoie ensuite le trafic vers l'équilibreur de charge de passerelle publique et vers la destination.

**Illustration 16 : Équilibreur de charge de passerelle Azure avec mandataire jumelé**



## Exigences et conditions préalables pour les interfaces VXLAN

### Exigences du modèle

- L'encapsulation VXLAN est prise en charge sur tous les modèles.
- L'encapsulation Geneve est prise en charge pour les modèles suivants :
  - Défense contre les menaces virtuelles dans Amazon Web Services (AWS)
- Le réseau VXLAN en *mode proxy jumelé* est pris en charge pour les modèles suivants :
  - Défense contre les menaces virtuelles dans Azure
- Firepower 1010 : Les sous-interfaces ne sont pas prises en charge sur les ports de commutation ou les interfaces VLAN.

## Directives pour les interfaces VXLAN

### Mode pare-feu

- Les interfaces Geneve ne sont prises en charge qu'en mode de pare-feu routé.
- Les interfaces VXLAN mandataires jumelées ne sont prises en charge qu'en mode de pare-feu routé.

### IPv6

- L'interface VNI prend en charge le trafic IPv4 et IPv6.
- L'adresse IP de l'interface source VTEP prend uniquement en charge IPv4.

### Mise en grappes

- La mise en grappe ne prend pas en charge VXLAN en mode d'interface individuelle, sauf pour la liaison de commande de grappe (défense contre les menaces virtuelles seulement). Seul le mode EtherChannel étendu prend en charge VXLAN.

Une exception est faite pour AWS, qui peut utiliser une interface Geneve supplémentaire à utiliser avec GWLB et pour Azure, qui peut utiliser une interface VXLAN jumelée mandataire à utiliser avec GWLB.

### Routage

- Seul le routage statique ou le routage basé sur des politiques est pris en charge sur l'interface VNI; Les protocoles de routage dynamique ne sont pas pris en charge.

### MTU

- Encapsulation VXLAN : si la MTU de l'interface source est inférieure à 1 554 octets, défense contre les menaces augmente automatiquement la MTU à 1 554 octets. Dans ce cas, le datagramme Ethernet entier est encapsulé, de sorte que le nouveau paquet est plus volumineux et nécessite une MTU plus grande. Si la MTU utilisée par d'autres périphériques est supérieure, vous devez définir la MTU de l'interface source comme étant la MTU du réseau + 54 octets. Pour défense contre les menaces virtuelles, cette MTU nécessite un redémarrage pour activer la réservation de trame étendue.
- Encapsulation Geneve : Si la MTU de l'interface source est inférieure à 1 806 octets, défense contre les menaces fait automatiquement passer la MTU à 1 806 octets. Dans ce cas, le datagramme Ethernet entier est encapsulé, de sorte que le nouveau paquet est plus volumineux et nécessite une MTU plus grande. Si la MTU utilisée par d'autres périphériques est supérieure, vous devez définir la MTU de l'interface source comme étant la MTU du réseau + 306 octets. Cette MTU nécessite un redémarrage pour activer la réservation de trame étendue.

## Configurer les interfaces VXLAN ou Geneve

Vous pouvez configurer les interfaces VXLAN ou Geneve.

### Configurer les interfaces VXLAN

Pour configurer les interfaces VXLAN, procédez comme suit.



**Remarque** Vous pouvez configurer VXLAN ou Geneve (défense contre les menaces virtuelles uniquement). Pour les interfaces Geneve, consultez [Configurer les interfaces Geneve, à la page 33](#).





**Remarque** Pour Azure GWLB, l'interface VXLAN est configurée lorsque vous déployez la machine virtuelle à l'aide du modèle ARM. Vous pouvez utiliser cette section pour modifier votre configuration.

1. [Configurer l'interface source VTEP, à la page 31](#).
2. [Configurer l'interface VNI, à la page 32](#).
3. (Azure GWLB) [Autoriser les vérifications de l'intégrité de l'équilibreur de charge de la passerelle, à la page 35](#).

## Configurer l'interface source VTEP

Vous pouvez configurer une interface source de VTEP par périphérique défense contre les menaces. Le VTEP est défini comme un point terminal de virtualisation du réseau (NVE). VXLAN est le type d'encapsulation par défaut. Une exception est faite pour la mise en grappe sur défense contre les menaces virtuelles dans Azure, où vous pouvez utiliser une interface source VTEP pour la liaison de commande de grappe et une autre pour l'interface de données connectée à Azure GWLB.

### Procédure

- 
- Étape 1** Si vous souhaitez spécifier un groupe de VTEP homologues, ajoutez un objet réseau avec les adresses IP homologues. Consultez [Création d'objets réseau](#).
- Étape 2** Choisissez **Devices (périphériques) > Device Management (gestion des périphériques)**.
- Étape 3** Cliquez sur **Edit (Modifier)** () à côté du périphérique sur lequel vous souhaitez configurer VXLAN.
- Étape 4** (Facultatif) Indiquez que l'interface source est NVE uniquement.
- Ce paramètre est facultatif pour le mode routé, où il restreint le trafic vers VXLAN et le trafic de gestion commune uniquement sur cette interface. Ce paramètre est automatiquement activé pour le mode de pare-feu transparent.
- a) Cliquez sur **Interfaces**.
  - b) Cliquez sur **Edit (Modifier)** () pour l'interface source de VTEP.
  - c) Dans la page **General (Général)**, cochez la case **NVE Only (NVE uniquement)**.
- Étape 5** Cliquez sur **VTEP** s'il ne s'affiche pas déjà.
- Étape 6** Cochez la case **Enable NVE (Activer NVE)**.
- Étape 7** Cliquez sur **Add VTEP (Ajouter VTEP)**.
- Étape 8** Pour le **type d'encapsulation**, choisissez **VxLAN**.
- Pour AWS, vous pouvez choisir entre **VxLAN** et **Geneve**. **VxLAN** est choisi automatiquement sur les autres plateformes.
- Étape 9** Saisissez la valeur du **port d'encapsulation** dans la plage spécifiée.

La valeur par défaut est 4789.

**Étape 10** Sélectionnez l'**Interface de la source VTEP**

Sélectionnez dans la liste des interfaces physiques disponibles sur le périphérique. Si la MTU de l'interface source est inférieure à 1 554 octets, centre de gestion augmente automatiquement la MTU à 1 554 octets.

**Étape 11** Sélectionnez l'**adresse du voisin**. Les options disponibles sont les suivantes :

- **Aucune** : aucune adresse de voisin n'est spécifiée.
- **VTEP homologue** : spécifiez une adresse VTP homologue.
- **Groupe d'homologues** : spécifiez un objet réseau avec les adresses IP homologues.
- **Multidiffusion par défaut** : spécifiez un groupe de multidiffusion par défaut pour toutes les interfaces VNI associées. Si vous ne configurez pas le groupe de multidiffusion par interface VNI, ce groupe est utilisé. Si vous configurez un groupe au niveau de l'interface VNI, ce groupe remplace ce paramètre.

**Étape 12** Cliquez sur **OK**.

**Étape 13** Cliquez sur **Save** (enregistrer).

**Étape 14** Configurer les paramètres d'interface routée. Voir [Configurer les interfaces en mode routage](#).

## Configurer l'interface VNI

Ajoutez une interface VNI, associez-la à l'interface source VTEP et configurez les paramètres de l'interface de base.

Pour défense contre les menaces virtuelles dans Azure, vous pouvez configurer une interface VXLAN standard ou une interface VXLAN en mode proxy jumelé à utiliser avec la GWLB Azure. Le mode proxy jumelé est le seul mode avec mise en grappe pris en charge.

### Procédure

**Étape 1** Choisissez **Devices (périphériques) > Device Management (gestion des périphériques)**.

**Étape 2** Cliquez sur **Edit (Modifier)** (✎) à côté du périphérique sur lequel vous souhaitez configurer VXLAN.

**Étape 3** Cliquez sur **Interfaces**.

**Étape 4** Cliquez sur **Add Interfaces** (Ajouter des interfaces), puis sélectionnez **VNI Interface** (interface VNI).

**Étape 5** Saisissez le **Name** (nom) et la **Description** de l'interface.

**Étape 6** Dans la liste déroulante **Security Zone** (zone de sécurité), choisissez une zone de sécurité ou ajoutez-en une en cliquant sur **New** (nouveau).

**Étape 7** Saisissez une valeur pour le champ **Priority** (Priorité) dans la plage spécifiée. Par défaut, 0 est sélectionné.

**Étape 8** Saisissez une valeur pour l' **ID VNI** comprise entre 1 et 10000.

Cet ID est uniquement un identifiant d'interface interne.

**Étape 9** (Serveur mandataire VXLAN jumelé pour Azure GWLB) Activez le mode de mandataire jumelé et définissez les paramètres requis.

- a) Cochez la case **mandataire jumelé**.
- b) Réglez le **port interne** entre 1024 et 65535.



- c) Définissez l'**ID de segment interne** entre 1 et 1677 275.
- d) Réglez le **port externe** entre 1024 et 65535.
- e) Définissez l'**ID de segment externe** entre 1 et 1677 275.

**Étape 10** (VXLAN normal) Saisissez une valeur pour l'**ID de segment VNI** comprise entre 1 et 1677 275.  
L'ID de segment est utilisé pour le balisage VXLAN.

**Étape 11** Saisissez l'**adresse IP du groupe multidiffusion**.

Si vous ne définissez pas le groupe de multidiffusion pour l'interface VNI, le groupe par défaut de la configuration de l'interface source VTEP est utilisé, s'il est disponible. Si vous définissez manuellement une adresse IP homologue VTEP pour l'interface source de VTEP, vous ne pouvez pas spécifier de groupe de multidiffusion pour l'interface VNI.

**Étape 12** Cochez **NVE mappé à l'interface VTEP**.

Cette option associe cette interface à l'interface source VTEP.

**Étape 13** Cliquez sur **OK**.

**Étape 14** Pour enregistrer la configuration de l'interface, cliquez sur **Save** (Enregistrer).

**Étape 15** Configurez les paramètres de l'interface routée ou transparente. Consultez [Configurer les interfaces en mode routage et en mode transparent, à la page 36](#).

## Configurer les interfaces Geneve

Pour configurer les interfaces de Geneve pour défense contre les menaces virtuelles, procédez comme suit.



**Remarque** Vous pouvez configurer VXLAN ou Geneve. Pour les interfaces VXLAN, consultez [Configurer les interfaces VXLAN, à la page 30](#).

1. [Configurer l'interface source VTEP, à la page 33](#).
2. [Configurer l'interface VNI, à la page 34](#).
3. [Autoriser les vérifications de l'intégrité de l'équilibreur de charge de la passerelle, à la page 35](#).

### Configurer l'interface source VTEP

Vous pouvez configurer une interface source de VTEP par périphérique défense contre les menaces virtuelles. Le VTEP est défini comme un terminal de virtualisation de réseau (NVE).

#### Procédure

**Étape 1** Choisissez **Devices (périphériques) > Device Management (gestion des périphériques)**.

**Étape 2** Cliquez sur **Edit** (Modifier) (✎) à côté du périphérique sur lequel vous souhaitez configurer Geneve.

**Étape 3** Cliquez sur **VTEP**.

**Étape 4** Cochez la case **Enable NVE** (Activer NVE).

- Étape 5** Cliquez sur **Add VTEP** (Ajouter VTEP).
- Étape 6** Pour le type d'encapsulation **Encapsulation Type**, choisissez **Geneve**.
- Étape 7** Saisissez la valeur du **port d'encapsulation** dans la plage spécifiée.  
Nous vous déconseillons de modifier le port Geneve; AWS nécessite un port 6081.
- Étape 8** Sélectionnez l'**Interface de la source VTEP**  
Vous pouvez effectuer une sélection dans la liste des interfaces physiques disponibles sur le périphérique. Si la MTU de l'interface source est inférieure à 1 806 octets, le centre de gestion augmente automatiquement la MTU à 1 806 octets.
- Étape 9** Cliquez sur **OK**.
- Étape 10** Cliquez sur **Save** (enregistrer).
- Étape 11** Configurer les paramètres d'interface routée. Voir [Configurer les interfaces en mode routage](#).
- 

## Configurer l'interface VNI

Ajoutez une interface VNI, associez-la à l'interface source VTEP et configurez les paramètres de l'interface de base.

### Procédure

---

- Étape 1** Choisissez **Devices (périphériques) > Device Management (gestion des périphériques)**.
- Étape 2** Cliquez sur **Edit** (Modifier) (✎) à côté du périphérique sur lequel vous souhaitez configurer Geneve.
- Étape 3** Cliquez sur **Interfaces**.
- Étape 4** Cliquez sur **Add Interfaces** (Ajouter des interfaces), puis sélectionnez **VNI Interface** (interface VNI).
- Étape 5** Saisissez le **Name** (nom) et la **Description** de l'interface.
- Étape 6** Saisissez une valeur pour l' **ID VNI** comprise entre 1 et 10000.  
Cet ID est uniquement un identifiant d'interface interne.
- Étape 7** Cochez la case **Enable Proxy** (activer le serveur mandataire).  
Cette option active le serveur mandataire à une seule branche et permet au trafic de quitter l'interface dans laquelle il est entré (trafic en demi-tour). Si vous modifiez l'interface ultérieurement, vous ne pourrez pas désactiver le serveur mandataire à une seule branche. Pour ce faire, vous devez supprimer l'interface existante et créer une nouvelle interface VNI.  
Cette option est uniquement disponible pour un VTEP Geneve.
- Étape 8** Sélectionnez **NVE Mapped to VTEP Interface** (NVE mappé à l'interface VTEP).  
Cette option associe cette interface à l'interface source VTEP.
- Étape 9** Cliquez sur **OK**.
- Étape 10** Pour enregistrer la configuration de l'interface, cliquez sur **Save** (Enregistrer).
- Étape 11** Configurer les paramètres d'interface routée. Voir [Configurer les interfaces en mode routage](#).
-

# Autoriser les vérifications de l'intégrité de l'équilibreur de charge de la passerelle

AWS ou Azure GWLB nécessite des périphériques pour répondre correctement à une vérification de l'intégrité. La GWLB enverra uniquement le trafic vers des périphériques considérés comme intègres. Vous devez configurer défense contre les menaces virtuelles pour répondre à une vérification de l'intégrité SSH, HTTP ou HTTPS.

Configurez l'une des méthodes suivantes.

## Procédure

### Étape 1

Configurez SSH. Consulter [Configure Secure Shell](#) (Configurer le protocole Secure Shell)

Autorisez le protocole SSH à partir de l'adresse IP GWLB. La GWLB tentera d'établir une connexion à défense contre les menaces virtuelles, et l'invite de connexion de défense contre les menaces virtuelles est considérée comme une preuve de l'intégrité. Une tentative de connexion SSH expirera après 1 minute. Vous devrez configurer un intervalle de vérification de l'intégrité plus long sur la GWLB pour tenir compte de ce délai.

### Étape 2

Configurez la redirection HTTP(S) à l'aide de la NAT d'interface statique avec traduction de port.

Vous pouvez configurer défense contre les menaces virtuelles pour rediriger les vérifications de l'intégrité vers un serveur HTTP(S) de métadonnées. Pour les vérifications de l'intégrité HTTP(S), le serveur HTTP(S) doit répondre à la GWLB avec un code d'état compris entre 200 et 399. Étant donné que la défense contre les menaces virtuelles a des limites sur le nombre de connexions de gestion simultanées, vous pouvez choisir de téléverser le contrôle de l'intégrité sur un serveur externe.

La NAT d'interface statique avec traduction de port vous permet de rediriger une connexion vers un port (comme le port 80) vers une adresse IP différente. Par exemple, traduisez un paquet HTTP de la GWLB avec la destination de l'interface externe défense contre les menaces virtuelles de sorte qu'il semble provenir de l'interface externe défense contre les menaces virtuelles avec la destination du serveur HTTP. Le défense contre les menaces virtuelles transfère ensuite le paquet vers l'adresse de destination mappée. Le serveur HTTP répond à l'interface externe défense contre les menaces virtuelles, puis défense contre les menaces virtuelles renvoie la réponse à la GWLB. Vous avez besoin d'une règle d'accès qui autorise le trafic de la GWLB vers le serveur HTTP.

- a) Autorisez le trafic HTTP(S) sur l'interface externe à partir du réseau avec préparatifs de l'outil GWLB dans une règle d'accès. Consultez [Règles de contrôle d'accès](#).
- b) Pour HTTP(S), traduire l'adresse IP source GWLB en adresse IP de l'interface externe défense contre les menaces virtuelles ; Traduire ensuite la destination de l'adresse IP de l'interface externe en adresse IP du serveur HTTP(S). Consultez [Configurer la NAT manuelle statique](#).

# Configurer les interfaces en mode routage et en mode transparent

Cette section comprend des tâches pour effectuer la configuration normale de l'interface pour tous les modèles en mode de pare-feu routé ou transparent.

## À propos des interfaces en mode routage et en mode transparent

Les interfaces en mode pare-feu soumettent le trafic aux fonctions de pare-feu telles que la maintenance des flux, le suivi des états de flux aux niveaux IP et TCP, la défragmentation IP et la normalisation TCP. Vous pouvez également configurer des fonctions IPS pour ce trafic en fonction de votre politique de sécurité.

Les types d'interfaces de pare-feu que vous pouvez configurer dépendent du mode de pare-feu défini pour le périphérique : mode routé ou transparent. Consultez [Mode pare-feu transparent ou routé](#) pour obtenir de plus amples renseignements.

- Interfaces en mode routé (mode pare-feu routé uniquement) : chaque interface entre laquelle vous souhaitez établir un routage se trouve sur un sous-réseau différent.
- Interfaces de groupe de ponts (mode routé et pare-feu transparent) : vous pouvez regrouper plusieurs interfaces sur un réseau, et le périphérique Firepower Threat Defense utilise des techniques de pont pour acheminer le trafic entre les interfaces. Chaque groupe de ponts comprend une interface virtuelle de pont (BVI) à laquelle vous attribuez une adresse IP sur le réseau. en mode routé, le périphérique Firepower Threat Defense achemine entre les BVI et les interfaces de routage normales. En mode transparent, chaque groupe de ponts est distinct et ne peut pas communiquer avec les autres.

## Double pile IP (IPv4 et IPv6)

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

## Masque de sous-réseau 31 bits

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

## Sous-réseau 31 bits et mise en grappe

Vous pouvez utiliser un masque de sous-réseau de 31 bits pour les interfaces, à l'exclusion de l'interface de gestion et de la liaison de commande de grappe.

## Sous-réseau 31 bits et basculement

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

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

## Gestion et sous-réseau 31 bits

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

## Fonctionnalités 31 bits non prises en charge

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

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

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

## High Availability (haute disponibilité), mise en grappe et multi-instance

- Ne configurez pas les liens de basculement selon les procédures de ce chapitre. Consultez le chapitre High Availability (haute disponibilité) pour plus de renseignements.
- Pour les interfaces de grappe, consultez le chapitre sur la mise en grappe pour connaître les exigences.
- En mode multi-instance, les interfaces partagées ne sont pas prises en charge pour les interfaces des membres des groupes de ponts (en mode transparent ou en mode routé).
- Lorsque vous utilisez High Availability (haute disponibilité), vous devez définir l'adresse IP et l'adresse de secours pour les interfaces de données manuellement. DHCP et PPPoE ne sont pas pris en charge. Définissez les adresses IP de secours dans l'onglet **Devices (Périphériques) > Device Management (Gestion des périphériques) > High Availability (Haute disponibilité)** dans la zone **Monitored interfaces** (interfaces surveillées). Consultez le chapitre High Availability (haute disponibilité) pour plus d'informations.

## IPv6

- IPv6 est pris en charge sur toutes les interfaces.
- Vous ne pouvez que configurer les adresses IPv6 manuellement en mode transparent.
- L'appareil de défense contre les menaces ne prend pas en charge les adresses anycast IPv6.

- Les options de délégation de préfixe et de DHCPv6 ne sont pas prises en charge avec le mode à mode transparent, la mise en grappe ou High Availability (haute disponibilité).

### Directives sur les modèles

- Pour défense contre les menaces virtuelles sur VMware avec interfaces ixgbevf pontées, les groupes de ponts ne sont pas pris en charge.
- Pour les périphériques Firepower 2100, les groupes de ponts ne sont pas pris en charge en mode routé.

### Directives relatives au mode transparent et au groupe de ponts

- Vous pouvez créer jusqu'à 250 groupes de ponts, avec interfaces par groupe de ponts.
- Chaque réseau connecté directement doit se trouver sur le même sous-réseau.
- L'appareil de défense contre les menaces ne prend pas en charge le trafic sur les réseaux secondaires; seul le trafic sur le même réseau que l'adresse IP BVI est pris en charge.
- Une adresse IP pour les BVI est requise pour chaque groupe de ponts pour le trafic de gestion vers le périphérique et en provenance du périphérique, ainsi que pour le trafic de données qui doit passer par appareil de défense contre les menaces. Pour le trafic IPv4, spécifiez une adresse IPv4. Pour le trafic IPv6, spécifiez une adresse IPv6.
- Vous ne pouvez configurer les adresses IPv6 que manuellement.
- L'adresse IP BVI doit se trouver sur le même sous-réseau que le réseau connecté. Vous ne pouvez pas définir le sous-réseau comme sous-réseau d'hôte (255.255.255.255).
- Les interfaces de gestion ne sont pas prises en charge en tant que membres de groupes de ponts.
- En mode multi-instance, les interfaces partagées ne sont pas prises en charge pour les interfaces des membres des groupes de ponts (en mode transparent ou en mode routé).
- Pour défense contre les menaces virtuelles sur VMware avec interfaces ixgbevf pontées, le mode transparent n'est pas pris en charge et les groupes de ponts ne sont pas pris en charge en mode routé.
- Pour Série Firepower 2100, les groupes de ponts ne sont pas pris en charge en mode routé.
- Dans le cas du Firepower 1010, il n'est pas possible de mélanger des interfaces VLAN logiques et des interfaces de pare-feu physiques au sein du même groupe de ponts.
- Pour Firepower 4100/9300, les interfaces de partage de données ne sont pas prises en charge en tant que membres de groupes de ponts.
- En mode transparent, vous devez utiliser au moins un groupe de ponts; les interfaces de données doivent appartenir à un groupe de ponts.
- En mode transparent, ne spécifiez pas l'adresse IP des BVI comme passerelle par défaut pour les périphériques connectés; Les périphériques doivent spécifier le routeur de l'autre côté de la défense contre les menaces comme passerelle par défaut.
- En mode transparent, la voie de routage *par défaut*, qui est requise pour fournir un chemin de retour au trafic de gestion, n'est appliquée qu'au trafic de gestion provenant d'un réseau de groupe de ponts. En effet, la voie de routage par défaut spécifie une interface dans le groupe de ponts ainsi que l'adresse IP du routeur sur le réseau du groupe de ponts, et vous ne pouvez définir qu'une seule voie de routage par

défaut. Si votre trafic de gestion provient de plus d'un réseau de groupes de ponts, vous devez spécifier une voie de routage statique régulière qui identifie le réseau à partir duquel vous attendez le trafic de gestion.

- Le protocole PPPoE n'est pas pris en charge sur l'interface Diagnostic.
- Le mode transparent n'est pas pris en charge sur les instances virtuelles de défense contre les menaces déployées sur Amazon Web Services, Microsoft Azure, Google Cloud Platform et Oracle Cloud Infrastructure.
- En mode routé, pour le routage entre les groupes de ponts et les autres interfaces routées, vous devez nommer les BVI.
- En mode routé, les interfaces EtherChannel définies par défense contre les menaces ne sont pas prises en charge en tant que membres de groupes de ponts. Les EtherChannels sur Firepower 4100/9300 peuvent être des membres de groupes de ponts.
- Les paquets écho de la détection de transfert bidirectionnel (BFD) ne sont pas autorisés par le biais de défense contre les menaces lors de l'utilisation de membres de groupe de ponts. S'il y a deux voisins de chaque côté de défense contre les menaces exécutant BFD, alors défense contre les menaces abandonnera les paquets écho BFD, car ils ont la même adresse IP de source et de destination et semblent faire partie d'une attaque LAND.

#### Directives et exigences supplémentaires

- La défense contre les menaces ne prend en charge qu'un seul en-tête 802.1Q par paquet et ne prend pas en charge plusieurs en-têtes (appelé prise en charge Q-in-Q) pour les interfaces de pare-feu. **Remarque** : pour les ensembles en ligne et les interfaces passives, le FTD prend en charge Q-in-Q jusqu'à deux en-têtes 802.1Q dans un paquet, à l'exception de Firepower 4100/9300, qui ne prend en charge qu'un seul en-tête 802.1Q.

## Configurer les interfaces en mode routé

Cette procédure décrit comment définir le nom, la zone de sécurité et l'adresse IPv4.



**Remarque** Tous les champs ne sont pas pris en charge pour tous les types d'interface.

#### Avant de commencer

- **Firepower 4100/9300**
  1. [Configurer une interface physique](#)
  2. (Facultatif) Configurez les interfaces spéciales.
    - [Ajouter un canal EtherChannel \(canal de port\)](#)
    - [Ajouter une sous-interface VLAN pour les instances de conteneur](#) dans FXOS
    - [Configurer une interface de boucle avec retour](#), à la page 13
    - [Ajouter une sous-interface](#), à la page 20 dans centre de gestion

- [Configurer les interfaces VXLAN, à la page 30](#)
- (Facultatif) **Tous les autres modèles :**
  - [Configurer un EtherChannel](#)
  - [Configurer une interface de boucle avec retour, à la page 13](#)
  - [Ajouter une sous-interface, à la page 20](#)
  - [Configurer les interfaces VXLAN, à la page 30](#)
  - Défense contre les menaces virtuelles Sur AWS : [Configurer les interfaces Geneve, à la page 33](#)
  - Firepower 1010 : [Configurer une interface VLAN, à la page 5](#)

## Procédure

---

- Étape 1** Sélectionnez **Devices (périphériques) > Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.
- Étape 2** Cliquez sur **Edit** (✎) pour l'interface que vous souhaitez modifier.
- Étape 3** Dans le champ **Nom**, saisissez un nom renfermant au maximum 48 caractères.
- Vous ne pouvez pas commencer le nom par l'expression « cluster » (grappe). Elle est réservée à un usage interne.
- Étape 4** Activez l'interface en cochant la case **Enabled** (activé).
- Étape 5** (Facultatif) Réglez cette interface sur **Gestion uniquement** pour limiter le trafic au trafic de gestion. le trafic traversant la boîte n'est pas autorisé.
- Étape 6** (Facultatif) Ajoutez une description dans le champ **Description**.
- La description peut contenir jusqu'à 200 caractères sur une seule ligne (sans retour chariot).
- Étape 7** Dans la liste déroulante **Mode**, choisissez **None** (aucun).
- Le mode des interfaces de pare-feu standard est défini sur Aucun. Les autres modes sont destinés aux types d'interface IPS uniquement.
- Étape 8** Dans la liste déroulante **Security Zone** (zone de sécurité), choisissez une zone de sécurité ou ajoutez-en une en cliquant sur **New** (nouveau).
- L'interface routée est une interface de type routé et ne peut appartenir qu'aux zones de type routé.
- Étape 9** Consultez [Configurer la MTU, à la page 65](#) pour obtenir des renseignements sur la **MTU**.
- Étape 10** Dans le champ **Priority** (Priorité), saisissez un nombre compris entre 0 et 65 535.
- Cette valeur est utilisée dans la configuration de routage basée sur les politiques. La priorité est utilisée pour déterminer comment vous souhaitez acheminer le trafic sur plusieurs interfaces de sortie. Pour en savoir plus, consultez [Configurer la politique de routage basée sur les politiques](#).
- Étape 11** Cliquez sur l'onglet **IPv4**. Pour définir l'adresse IP, utilisez l'une des options suivantes dans la liste déroulante **IP Type** (Type d'adresse IP).



Les interfaces à haute disponibilité, de mise en grappe et de boucle avec retour prennent uniquement en charge la configuration d'adresses IP statiques; DHCP et PPPoE ne sont pas pris en charge.

- **Utiliser une adresse IP statique** saisissez l'adresse IP et le masque de sous-réseau. Pour les connexions point à point, vous pouvez spécifier un masque de sous-réseau de 31 bits (255.255.255.254 ou /31). Dans ce cas, aucune adresse IP n'est réservée pour les adresses de réseau ou de diffusion. Vous ne pouvez pas définir l'adresse IP de secours dans ce cas. Pour la haute disponibilité, vous pouvez uniquement utiliser une adresse IP statique. Définissez l'adresse IP de secours sous l'onglet **Devices > Device Management > High Availability** dans la zone **Monitored Interfaces**. :: s Si vous ne définissez pas l'adresse IP de veille, l'unité active ne peut pas surveiller l'interface de secours en utilisant des tests réseau; elle ne peut que suivre l'état du lien.
- **Utiliser DHCP** : configurez les paramètres facultatifs suivants :
  - **Obtain Default Route Using DHCP** (obtenir la voie de routage par défaut en utilisant DHCP) : Obtenir la voie de routage par défaut à partir du serveur DHCP.
  - **DHCP route metric** (mesure de la voie de routage DHCP) : Attribue une distance administrative à la voie de routage apprise (entre 1 et 255). La distance administrative par défaut pour les routes apprises est de 1.
- **Utiliser PPPoE** : si l'interface est connectée à une liaison ADSL, à un modem câble ou à une autre connexion à votre FAI et que ce dernier utilise PPPoE pour vous fournir votre adresse IP, configurez les paramètres suivants :

- **Nom du groupe VPDN** : spécifiez le nom du groupe de votre choix pour représenter cette connexion.
- **Nom d'utilisateur PPPoE** : spécifiez le nom d'utilisateur fourni par votre fournisseur de services Internet.
- **Mot de passe PPPoE** : spécifiez le mot de passe fourni par votre fournisseur de services Internet.
- **PPP Authentication** (authentification PPP) : Choisissez **PAP**, **CHAP** ou **MSCHAP**.

Le PAP transmet un nom d'utilisateur et un mot de passe en clair lors de l'authentification et n'est pas sécurisé. Avec le protocole CHAP, le client renvoie le [défi plus mot de passe] chiffré, avec un nom d'utilisateur en texte clair en réponse au défi du serveur. Le protocole CHAP est plus sécurisé que le protocole PAP, mais il ne chiffre pas les données. MSCHAP est similaire à CHAP, mais est plus sécurisé, car le serveur stocke et compare uniquement les mots de passe chiffrés plutôt que les mots de passe en clair comme dans CHAP. MSCHAP génère également une clé pour le chiffrement des données par MPPE.

- **Mesure de la voie de routage PPPoE** : attribue une distance administrative à la voie de routage apprise. Cette valeur peut être comprise entre 1 et 255. Par défaut, la distance administrative pour les routes apprises est de 1.
- **Activer les paramètres de routage** : pour configurer manuellement l'adresse IP PPPoE, cochez cette case, puis saisissez l'**adresse IP**.

Si vous cochez la case **Enable Route Settings** (activer les paramètres de routage) et laissez le champ **IP Address** (adresse IP) vide, la commande **ip address pppoe setroute** est appliquée, comme l'illustre cet exemple :

```
interface GigabitEthernet0/2
nameif inside2_pppoe
cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
```

```

security-level 0
pppoe client vpdn group test
pppoe client route distance 10
ip address pppoe setroute

```

- **Store Username and Password in Flash**(enregistrer le nom d'utilisateur et le mot de passe dans la mémoire flash) : enregistre le nom d'utilisateur et le mot de passe dans la mémoire flash.

Le périphérique défense contre les menaces stocke le nom d'utilisateur et le mot de passe dans un emplacement spécial de la NVRAM.

- Étape 12** (Facultatif) Consultez [Configuration de l'adressage IPv6, à la page 48](#) pour configurer l'adressage IPv6 sur l'onglet **IPv6**.
- Étape 13** (Facultatif) Voir [Configurer l'adresse MAC, à la page 66](#) pour configurer manuellement l'adresse MAC sous l'onglet **Advanced** (Avancé).
- Étape 14** (Facultatif) Synchroniser les interfaces à partir du périphérique **Hardware Configuration > Speed** (Configuration matérielle > Vitesse).

- **Duplex** : choisissez entre **Full** ou **Half**. Les interfaces SFP prennent uniquement en charge les conditions de duplex **full (complètes)**.
- **Speed** : choisissez une vitesse (variable selon le modèle). (Secure Firewall 3100 uniquement) choisissez **Detect SFP** pour détecter la vitesse du module SFP installé et utiliser la vitesse appropriée. Le mode duplex est toujours Full (complet) et la négociation automatique est toujours activée. Cette option est utile si vous modifiez ultérieurement le module de réseau pour un modèle différent et que vous souhaitez que la vitesse se mette à niveau automatiquement.
- **Négociation automatique** : définissez l'interface pour négocier le débit, l'état de la liaison et le contrôle de flux.
- **Mode de correction d'erreur de transfert** : (cisco Secure Firewall 3100uniquement) Pour les interfaces de 25 Gbit/s et plus, activez la correction d'erreur de transfert (FEC). Pour une interface membre d'EtherChannel, vous devez configurer la correction d'erreur directe avant de l'ajouter à l'EtherChannel. Le paramètre choisi lorsque vous utilisez **Auto** dépend du type d'émetteur-récepteur et selon si l'interface est fixe (intégrée) ou sur un module de réseau.

**Tableau 1 : FEC par défaut pour le réglage automatique**

Type d'émetteur/récepteur	FEC par défaut du port fixe (Ethernet 1/9 à 1/16)	FEC par défaut du module de réseau
25G-SR	Article 108 RS-FEC	Article 108 RS-FEC
25G-LR	Article 108 RS-FEC	Article 108 RS-FEC
10/25G-CSR	Article 108 RS-FEC	Article 74 FC-FEC
25G-AOCxM	Article 74 FC-FEC	Article 74 FC-FEC
25G-CU2.5/3M	Négociation automatique	Négociation automatique
25G-CU4/5M	Négociation automatique	Négociation automatique

**Étape 15**

(Facultatif) Activez l'accès du gestionnaire centre de gestion sur une interface de données dans la page d'accès **d'accès du gestionnaire**.

Vous pouvez activer l'accès du gestionnaire à partir d'une interface de données lors de la configuration initiale de défense contre les menaces . Si vous souhaitez activer ou désactiver l'accès du gestionnaire après avoir ajouté défense contre les menaces à centre de gestion, consultez :

- Activer l'accès du gestionnaire : [Modifier l'interface d'accès du gestionnaire de Management à Data \(données\)](#)

**Remarque** Vous ne pouvez pas activer l'accès du gestionnaire à moins de lancer la migration de l'interface du gestionnaire de l'interface de gestion vers une interface de données. Après avoir lancé la migration, vous pouvez activer l'accès du gestionnaire dans la page **Manager Access** et enregistrer la configuration avec succès.

- Désactiver l'accès du gestionnaire : [Modifier l'interface d'accès du gestionnaire de données à gestion](#)

Si vous souhaitez remplacer l'interface d'accès du gestionnaire d'une interface de données à une autre interface de données, vous devez désactiver l'accès du gestionnaire sur l'interface de données d'origine, mais ne désactivez pas encore l'interface elle-même; l'interface de données d'origine doit être utilisée pour effectuer le déploiement. Si vous souhaitez utiliser la même adresse IP sur la nouvelle interface d'accès du gestionnaire, vous pouvez supprimer ou modifier la configuration IP sur l'interface d'origine. cette modification ne devrait pas affecter le déploiement. Si vous utilisez une adresse IP différente pour la nouvelle interface, modifiez également l'adresse IP du périphérique indiquée dans centre de gestion; voir [Mettez à jour le nom d'hôte ou l'adresse IP dans Centre de gestion](#). Assurez-vous de également mettre à jour la configuration associée pour utiliser la nouvelle interface, comme les routes statiques et les paramètres DDNS et DNS.

L'accès du gestionnaire à partir d'une interface de données présente les limites suivantes :

- Vous ne pouvez activer l'accès du gestionnaire sur une seule interface physique de données. Vous ne pouvez pas utiliser une sous-interface ou EtherChannel. Vous pouvez également utiliser les centre de gestion pour activer l'accès du gestionnaire sur une interface secondaire unique à des fins de redondance.
- Cette interface ne peut pas être une interface de gestion uniquement.
- Mode de pare-feu routé uniquement, en utilisant une interface routée.
- PPPoE n'est pas pris en charge. Si votre FAI exige PPPoE, vous devrez placer un routeur avec support PPPoE entre le défense contre les menaces et le modem WAN.
- L'interface doit être dans le VRF global seulement.
- SSH n'est pas activé par défaut pour les interfaces de données, vous devrez donc activer SSH ultérieurement à l'aide de l'option centre de gestion. Comme la passerelle de l'interface de gestion sera transformée en interfaces de données, vous ne pouvez pas non plus autoriser SSH vers l'interface de gestion à partir d'un réseau distant, sauf si vous ajoutez une route statique pour l'interface de gestion à l'aide de la commande **configure network static-routes**. Pour défense contre les menaces virtuelles sur Amazon Web Services, un port de console n'est pas disponible, vous devez donc maintenir votre accès SSH à l'interface de gestion : ajoutez une route statique pour la Gestion avant de poursuivre votre configuration. Sinon, assurez-vous de terminer toute la configuration de l'interface de ligne de commande (y compris la commande **configure manager add**) avant de configurer l'interface de données pour l'accès du gestionnaire et d'être déconnecté.
- La mise en grappe n'est pas prise en charge. Dans ce cas, vous devez utiliser l'interface de gestion.
-

Illustration 17 : Accès du gestionnaire

- Cochez la case **Enable management on this interface for the manager** (activer la gestion sur cette interface du gestionnaire) sur cette interface pour que le utilise cette interface de données pour la gestion au lieu de l'interface de gestion dédiée.
- (Facultatif) Dans la zone **Allowed Management Networks** (réseaux de gestion autorisés), ajoutez les réseaux pour lesquels vous souhaitez autoriser l'accès des gestionnaires. Par défaut, tous les réseaux sont autorisés.

**Étape 16**Cliquez sur **OK**.**Étape 17**Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer) > Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

## Configurer les interfaces de groupe de ponts

Un groupe de ponts est un groupe d'interfaces que l'appareil Cisco Secure Firewall Threat Defense relie par des ponts au lieu de routes. Les groupes de ponts sont pris en charge à la fois en mode transparent et en mode pare-feu routé. Pour en savoir plus sur les groupes de ponts, consultez [À propos des groupes de ponts](#).

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

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

Cette procédure décrit comment définir le nom et la zone de sécurité pour chaque interface de membre de groupe de ponts. Un même groupe de ponts peut inclure différents types d'interfaces : des interfaces physiques, des sous-interfaces VLAN, des interfaces VLAN Firepower 1010, des EtherChannels et des interfaces redondantes. Le protocole PPPoE n'est pas pris en charge sur l'interface de gestion. En mode routé, les

EtherChannels ne sont pas pris en charge. Pour le Firepower 4100/9300, les interfaces de type partage de données ne sont pas prises en charge.

### Avant de commencer

- **Firepower 4100/9300**

1. [Configurer une interface physique](#)
2. (Facultatif) Configurez les interfaces spéciales.
  - [Ajouter un canal EtherChannel \(canal de port\)](#)
  - [Ajouter une sous-interface VLAN pour les instances de conteneur](#) dans FXOS
  - [Ajouter une sous-interface, à la page 20](#) dans centre de gestion

- (Facultatif) **Tous les autres modèles :**

- [Configurer un EtherChannel](#)
- [Ajouter une sous-interface, à la page 20](#)
- Firepower 1010 : [Configurer une interface VLAN, à la page 5](#)

### Procédure

- 
- Étape 1** Sélectionnez **Devices (périphériques) > Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.
- Étape 2** Cliquez sur **Edit** (✎) pour l'interface que vous souhaitez modifier.
- Étape 3** Dans le champ **Nom**, saisissez un nom renfermant au maximum 48 caractères.  
Vous ne pouvez pas commencer le nom par l'expression « cluster » (grappe). Elle est réservée à un usage interne.
- Étape 4** Activez l'interface en cochant la case **Enabled** (activé).
- Étape 5** (Facultatif) Réglez cette interface sur **Gestion uniquement** pour limiter le trafic au trafic de gestion. le trafic traversant la boîte n'est pas autorisé.
- Étape 6** (Facultatif) Ajoutez une description dans le champ **Description**.  
La description peut contenir jusqu'à 200 caractères sur une seule ligne (sans retour chariot).
- Étape 7** Dans la liste déroulante **Mode**, choisissez **None** (aucun).  
Le mode des interfaces de pare-feu standard est défini sur Aucun. Les autres modes sont destinés aux types d'interface IPS uniquement. Après avoir affecté cette interface à un groupe de ponts, le mode commuté sera **Commuté**.
- Étape 8** Dans la liste déroulante **Security Zone** (zone de sécurité), choisissez une zone de sécurité ou ajoutez-en une en cliquant sur **New** (nouveau).  
L'interface membre du groupe de ponts est de type commuté et ne peut appartenir qu'à des zones de type commuté. Ne configurez aucun paramètre d'adresse IP pour cette interface. Vous définirez l'adresse IP pour

le BVI (Bridge Virtual Interface) uniquement. Notez que les BVI n'appartiennent pas à une zone et que vous ne pouvez pas appliquer des politiques de contrôle d'accès aux BVI.

**Étape 9**

Consultez [Configurer la MTU, à la page 65](#) pour obtenir des renseignements sur la MTU.

**Étape 10**

(Facultatif) Synchroniser les interfaces à partir du périphérique **Hardware Configuration > Speed** (Configuration matérielle > Vitesse).

- **Duplex** : choisissez entre **Full** ou **Half**. Les interfaces SFP prennent uniquement en charge les conditions de duplex **full (complètes)**.
- **Speed** : choisissez une vitesse (variable selon le modèle). (Secure Firewall 3100 uniquement) choisissez **Detect SFP** pour détecter la vitesse du module SFP installé et utiliser la vitesse appropriée. Le mode duplex est toujours Full (complet) et la négociation automatique est toujours activée. Cette option est utile si vous modifiez ultérieurement le module de réseau pour un modèle différent et que vous souhaitez que la vitesse se mette à niveau automatiquement.
- **Négociation automatique** : définissez l'interface pour négocier le débit, l'état de la liaison et le contrôle de flux.
- **Mode de correction d'erreur de transfert** : (cisco Secure Firewall 3100 uniquement) Pour les interfaces de 25 Gbit/s et plus, activez la correction d'erreur de transfert (FEC). Pour une interface membre d'EtherChannel, vous devez configurer la correction d'erreur directe avant de l'ajouter à l'EtherChannel. Le paramètre choisi lorsque vous utilisez **Auto** dépend du type d'émetteur-récepteur et selon si l'interface est fixe (intégrée) ou sur un module de réseau.

**Tableau 2 : FEC par défaut pour le réglage automatique**

Type d'émetteur/récepteur	FEC par défaut du port fixe (Ethernet 1/9 à 1/16)	FEC par défaut du module de réseau
25G-SR	Article 108 RS-FEC	Article 108 RS-FEC
25G-LR	Article 108 RS-FEC	Article 108 RS-FEC
10/25G-CSR	Article 108 RS-FEC	Article 74 FC-FEC
25G-AOCxM	Article 74 FC-FEC	Article 74 FC-FEC
25G-CU2.5/3M	Négociation automatique	Négociation automatique
25G-CU4/5M	Négociation automatique	Négociation automatique

**Étape 11**

(Facultatif) Consultez [Configuration de l'adressage IPv6, à la page 48](#) pour configurer l'adressage IPv6 sur l'onglet **IPv6**.

**Étape 12**

(Facultatif) Voir [Configurer l'adresse MAC, à la page 66](#) pour configurer manuellement l'adresse MAC sous l'onglet **Advanced** (Avancé).

**Étape 13**

Cliquez sur **OK**.

**Étape 14**

Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer) > Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

## Configurer la BVI (Bridge Virtual Interface)

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

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



**Remarque** Pour une interface Diagnostic distincte, un groupe de ponts non configurables (ID 301) est automatiquement ajouté à votre configuration. Ce groupe de ponts n'est pas inclus dans la limite de groupes de ponts.

### Avant de commencer

Vous ne pouvez pas ajouter les BVI à une zone de sécurité; par conséquent, vous ne pouvez pas appliquer de politiques de contrôle d'accès aux BVI. Vous devez appliquer votre politique aux interfaces des membres des groupes de ponts en fonction de leurs zones.

### Procédure

- Étape 1** Sélectionnez **Devices (périphériques) > Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces. La page **Interfaces** est sélectionnée par défaut.
- Étape 2** Choisissez **Add Interfaces (Ajouter des interfaces) > Bridge Group Interface (interface de groupe de ponts)**.
- Étape 3** (Mode routé) Dans le champ **Nom**, saisissez un nom renfermant au maximum 48 caractères.  
Vous devez nommer le BVI si vous souhaitez acheminer le trafic extérieur aux membres du groupe de pont, par exemple vers l'interface externe ou vers les membres d'autres groupes de pont. Le nom n'est pas sensible à la casse.
- Étape 4** Dans le champ **Bridge Group ID** (ID de groupe de ponts), saisissez un ID de groupe de ponts compris entre 1 et 250.
- Étape 5** Dans le champ **Description**, saisissez une description pour le groupe de ponts.
- Étape 6** Dans l'onglet **Interfaces**, cliquez sur une interface, puis sur **Ajouter** pour la déplacer dans la zone **Interfaces sélectionnées**. Répétez l'opération pour toutes les interfaces dont vous souhaitez faire des membres du groupe de pont.
- Étape 7** (mode transparent) Cliquez sur l'onglet **IPv4**. Dans le champ **IP Address** (Adresse IP), saisissez l'adresse IP et le masque de sous-réseau.

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

routeur en amont, le périphérique défend contre les menaces et abandonne la requête ARP du routeur en aval au routeur en amont.

Pour la haute disponibilité, définissez l'adresse IP de secours sous l'onglet **Devices > Device Management > High Availability** (Périphériques > Gestion des périphériques > Haute disponibilité) dans la zone des **interfaces surveillées**. Si vous ne définissez pas l'adresse IP de veille, l'unité active ne peut pas surveiller l'interface de secours en utilisant des tests réseau; elle ne peut que suivre l'état du lien.

### Étape 8

(Mode routé) Cliquez sur l'onglet **IPv4**. Pour définir l'adresse IP, utilisez l'une des options suivantes dans la liste déroulante **IP Type** (Type d'adresse IP).

Les interfaces à haute disponibilité et de mise en grappe prennent uniquement en charge la configuration d'adresses IP statiques; DHCP n'est pas pris en charge.

- **Utiliser une adresse IP statique** saisissez l'adresse IP et le masque de sous-réseau. Pour la haute disponibilité, vous pouvez uniquement utiliser une adresse IP statique. Définissez l'adresse IP de secours sous l'onglet **Devices > Device Management > High Availability** dans la zone **Monitored Interfaces**. Si vous ne définissez pas l'adresse IP de veille, l'unité active ne peut pas surveiller l'interface de secours en utilisant des tests réseau; elle ne peut que suivre l'état du lien.
- **Utiliser DHCP** : configurez les paramètres facultatifs suivants :
  - **Obtain Default Route Using DHCP** (obtenir la voie de routage par défaut en utilisant DHCP) : Obtenir la voie de routage par défaut à partir du serveur DHCP.
  - **DHCP route metric** (mesure de la voie de routage DHCP) : Attribue une distance administrative à la voie de routage apprise (entre 1 et 255). La distance administrative par défaut pour les routes apprises est de 1.

### Étape 9

(Facultatif) Consultez [Configuration de l'adressage IPv6, à la page 48](#) pour configurer l'adressage IPv6.

### Étape 10

(Facultatif) Consultez [Ajouter une entrée ARP statique, à la page 67](#) et [Ajouter une adresse MAC statique et désactiver l'apprentissage MAC pour un groupe de ponts, à la page 68](#) (pour le mode transparent uniquement) pour configurer les paramètres **ARP** et **MAC**.

### Étape 11

Cliquez sur **OK**.

### Étape 12

Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer) > Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

## Configuration de l'adressage IPv6

Cette section décrit comment configurer l'adressage IPv6 en mode routé et transparent.

### À propos d'IPv6

Cette section comprend des informations sur IPv6.

#### Adresse IPv6

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



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

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

## ID d'interface EUI-64 modifiées

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

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

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

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

## Configurer le client de délégation de préfixe IPv6

Le défense contre les menaces peut servir de client de délégation de préfixe DHCPv6 de sorte que l'interface client, par exemple l'interface externe connectée à un modem câble, puisse recevoir un ou plusieurs préfixes IPv6 que le défense contre les menaces peut ensuite utiliser en sous-réseau et attribuer à ses interfaces internes.

### À propos de la délégation de préfixe IPv6

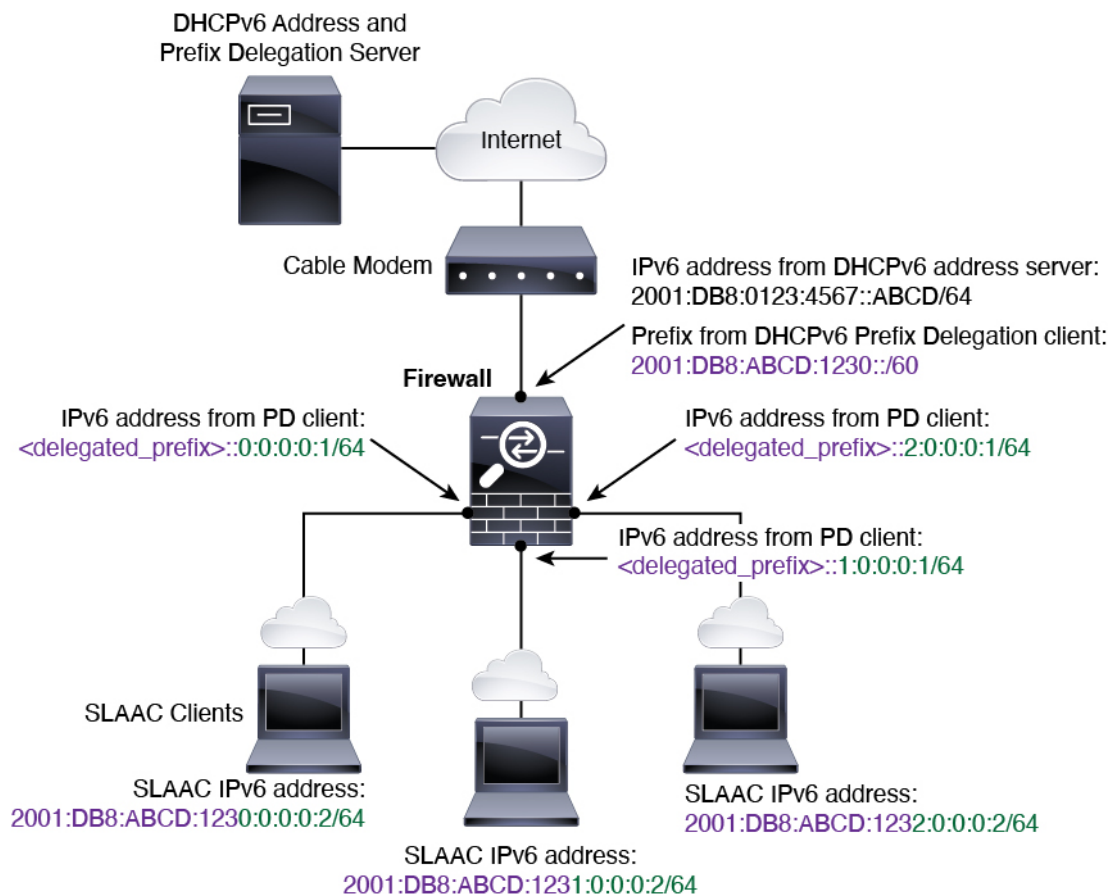
Le défense contre les menaces peut servir de client de délégation de préfixe DHCPv6 de sorte que l'interface client, par exemple l'interface externe connectée à un modem câble, puisse recevoir un ou plusieurs préfixes IPv6 que le défense contre les menaces peut ensuite utiliser en sous-réseau et attribuer à ses interfaces internes. Les hôtes connectés aux interfaces internes peuvent ensuite utiliser la configuration automatique sans état (SLAAC) pour obtenir des adresses IPv6 globales. Notez que les interfaces défense contre les menaces internes n'agissent pas à leur tour comme des serveurs de délégation de préfixe; Le défense contre les menaces ne peut fournir des adresses IP globales qu'aux clients SLAAC. Par exemple, si un routeur est connecté à défense

contre les menaces, il peut agir en tant que client SLAAC pour obtenir son adresse IP. Mais si vous souhaitez utiliser un sous-réseau du préfixe délégué pour les réseaux derrière le routeur, vous devez configurer manuellement ces adresses sur les interfaces internes du routeur.

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

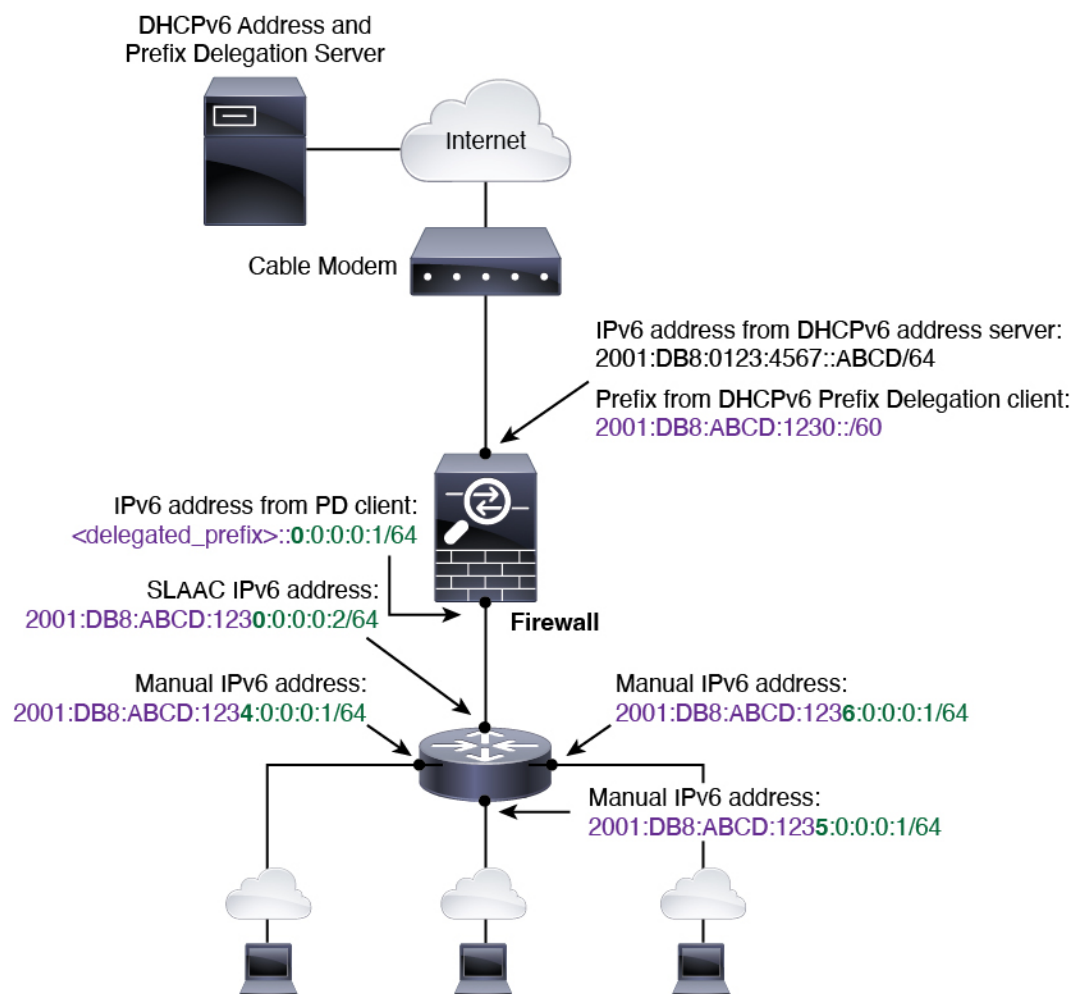
#### Exemple de délégation de préfixe IPv6 /de sous-réseau 64

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



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

L'exemple suivant montre la sous-réseaux défense contre les menaces du préfixe en 4 sous-réseaux /62 : 2001:DB8:ABCD:1230:/62, 2001:DB8:ABCD:1234:/62, 2001:DB8:ABCD:1238::/62 et 2001:DB8:ABCD:123C::/62. défense contre les menaces utilise l'un des 4 sous-réseaux /64 disponibles sur 2001:DB8:ABCD:1230::/62 pour son réseau interne (::0). Vous pouvez ensuite utiliser manuellement des sous-réseaux /62 supplémentaires pour les routeurs en aval. Le routeur illustré utilise 3 des 4 sous-réseaux /64 disponibles sur 2001:DB8:ABCD:1234::/62 pour ses interfaces internes (::4,::5 et::6). Dans ce cas, les interfaces de routeur internes ne peuvent pas obtenir dynamiquement le préfixe délégué. Vous devez donc afficher le préfixe délégué sur défense contre les menaces, puis utiliser ce préfixe pour la configuration de votre routeur. Habituellement, les fournisseurs de services Internet délèguent le même préfixe à un client donné à l'expiration du bail, mais si défense contre les menaces reçoit un nouveau préfixe, vous devrez modifier la configuration du routeur pour utiliser le nouveau préfixe. L'identifiant unique (DUID) de DHCP est persistant pendant les redémarrages.



### Activer le client de délégation de préfixe IPv6

Activer le client de délégation de préfixe DHCPv6 sur une ou plusieurs interfaces. Le défense contre les menaces obtient un ou plusieurs préfixes IPv6 qu'il peut utiliser en sous-réseau et affecter aux réseaux internes. En règle générale, l'interface sur laquelle vous activez la délégation de préfixe client obtient son adresse IP à

l'aide de l'adresse client DHCPv6; Seules les autres interfaces défense contre les menaces utilisent des adresses dérivées du préfixe délégué.

Cette fonctionnalité n'est prise en charge qu'en mode routé. Cette fonctionnalité n'est pas prise en charge lors de la mise en grappe ou pour la haute disponibilité.

### Avant de commencer

Lorsque vous utilisez la délégation de préfixe, vous devez définir l'intervalle d'annonce du routeur de découverte du voisin IPv6 défense contre les menaces comme très inférieur à la durée de vie préférée du préfixe attribué par le serveur DHCPv6 pour éviter toute interruption de trafic IPv6. Par exemple, si le serveur DHCPv6 définit la durée de vie préférée de délégation de préfixe à 300 secondes, vous devez définir l'intervalle d'accès distant (RA) défense contre les menaces à 150 secondes. Pour définir la durée de vie préférée, utilisez la commande **show ipv6 general-prefix**. Pour définir l'intervalle d'accès distant défense contre les menaces, consultez [Configurer la découverte des voisins IPv6, à la page 57](#); la valeur par défaut est de 200 secondes.

### Procédure

- Étape 1** Sélectionnez **Devices (périphériques) > Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces. La page **Interfaces** est sélectionnée par défaut.
- Étape 2** Cliquez sur **Edit** (✎) pour l'interface que vous souhaitez modifier.
- Étape 3** Cliquez sur la page **IPv6**, puis sur **DHCP**.
- Étape 4** Cliquez sur **Client PD Prefix Name** (Nom du préfixe DP du client) et saisissez un nom pour ce préfixe.

*Illustration 18 : Activer le client de délégation de préfixe*

Client PD Prefix Name

Outside-Prefix

Client PD Hint Prefixes

Add

2001:DB8:ABCD:1230::/60

Le nom peut comporter jusqu'à 200 caractères.

- Étape 5** (Facultatif) Saisissez le préfixe et la longueur du préfixe dans le champ **Client PD Hint Prefixes** (Préfixes de conseils DP du client) pour fournir un ou plusieurs conseils au serveur DHCP à propos de la délégation de préfixe que vous souhaitez recevoir, puis cliquez sur **Add** (Ajouter).

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

- Étape 6** Cliquez sur **OK**.
- Étape 7** Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer) > Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

## Configuration d'une adresse globale IPv6

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



### Remarque

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

En ce qui concerne les sous-interfaces définies sur défense contre les menaces, nous vous recommandons de définir également l'adresse MAC manuellement, car elles utilisent la même adresse MAC gravée que l'interface parente. En outre, étant donné que les adresses locales de lien IPv6 sont générées en fonction de l'adresse MAC, l'affectation d'adresses MAC uniques aux sous-interfaces permet d'établir des adresses locales de lien IPv6 uniques, ce qui peut éviter des perturbations de trafic dans certaines instances sur défense contre les menaces. Consultez [Configurer l'adresse MAC, à la page 66](#).

### Avant de commencer

En ce qui concerne la découverte de voisins IPv6 pour les groupes de ponts, vous devez autoriser explicitement les paquets de sollicitation de voisin (ICMPv6 type 135) et de publicité de voisin (ICMPv6 type 136) par le biais des interfaces membres du groupe de ponts défense contre les menaces en utilisant une règle d'accès bidirectionnel.

### Procédure

- Étape 1** Sélectionnez **Devices (périphériques) > Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces. La page **Interfaces** est sélectionnée par défaut.
- Étape 2** Cliquez sur **Edit** (✎) pour l'interface que vous souhaitez modifier.
- Étape 3** Cliquez sur la page **IPv6**.  
Pour le mode routé, la page **Basic** (de base) est sélectionnée par défaut. En mode transparent, la page d'**adresses** est sélectionnée par défaut.
- Étape 4** (Facultatif) Dans la page de **base**, cochez **Enable IPv6** (Activer IPv6).  
Utilisez cette option si vous souhaitez configurer uniquement les adresses de lien locales. Sinon, la configuration d'une adresse IPv6 a activé le traitement IPv6 automatiquement.
- Étape 5** Configurez l'adresse IPv6 globale en utilisant l'une des méthodes suivantes.  
Les interfaces de boucle avec retour ne prennent en charge que la configuration manuelle.
  - ( Interface routée) Autoconfiguration sans état : cochez la case **Autoconfiguration**.  
L'activation de la configuration automatique sans état sur l'interface configure les adresses IPv6 en fonction des préfixes reçus dans les messages d'annonce de routeur. Une adresse de lien local, basée sur

L'ID d'interface EUI-64 modifiée, est automatiquement générée pour l'interface lorsque la configuration automatique sans état est activée.

Bien que la RFC 4862 spécifie que les hôtes configurés pour une autoconfiguration sans état n'envoient pas de messages de publicité de routeur, le périphérique défense contre les menaces envoie des messages de publicité de routeur dans ce cas. Décochez la case **IPv6 > Paramètres > Activer l'accès à distance** pour supprimer les messages.

- Configuration manuelle : pour configurer manuellement une adresse IPv6 globale :

1. Cliquez sur la page **Address** (adresses), puis sur (+) **Add Address** (ajouter une adresse).

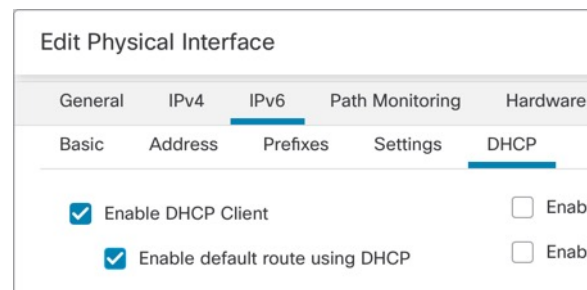
La boîte de dialogue **Add Address** (ajouter une adresse) s'affiche.

2. Dans le champ **Address** (adresse), saisissez une adresse IPv6 globale complète, y compris l'ID de l'interface, ou saisissez le préfixe IPv6 ainsi que la longueur du préfixe IPv6. (mode routé) Si vous saisissez uniquement le préfixe, assurez-vous de cocher la case **Enforce EUI 64** (Appliquer EUI 64) pour générer l'ID d'interface en utilisant le format EUI-64 modifié. Par exemple, 2001:0DB8::BA98:0:3210/48 (adresse complète) ou 2001:0DB8::/48 (préfixe, avec EUI 64 cochée).

Pour la haute disponibilité (si vous n'avez pas défini **Enforce EUI 64**), définissez l'adresse IP de secours sur la page **Devices > Device Management > High Availability** dans la zone **Monitored Interfaces**. Si vous ne définissez pas l'adresse IP de veille, l'unité active ne peut pas surveiller l'interface de secours en utilisant des tests réseau; elle ne peut que suivre l'état du lien.

- (interface routé) Obtain an address using DHCPv6 (obtenir une adresse avec DHCPv6) : pour utiliser DHCPv6 :

**Illustration 19 : Activer le client DHCPv6**



1. Cliquez sur la page **DHCP**.
2. Cochez la case **Enable DHCP Client** (activer le client DHCP).
3. (Facultatif) Cochez la case **Enable default route using DHCP** (Activer l'itinéraire par défaut en utilisant DHCP) pour obtenir un itinéraire par défaut à partir des annonces du routeur.

- (Interface routée) Utiliser un préfixe délégué - Pour attribuer une adresse IPv6 à l'aide d'un préfixe délégué :

Cette fonctionnalité nécessite défense contre les menaces pour que le client de délégation de préfixe DHCPv6 soit activé *sur une interface différente*. Consultez [Activer le client de délégation de préfixe IPv6, à la page 51](#).

1. Cliquez sur la page **DHCP**.

2. Cliquez sur **Ajouter (+)**.

*Illustration 20 : Utiliser un préfixe délégué*

Edit Physical Interface

General IPv4 IPv6 Path Monitoring Hardware Configuration Manager Access Adva

Basic Address Prefixes Settings DHCP

+ Add

Prefix Name	Prefix Length
No records to display	

3. Saisissez le **nom de préfixe** que vous avez spécifié pour le client de délégation de préfixe (voir [Activer le client de délégation de préfixe IPv6, à la page 51](#)) sur une autre interface.

*Illustration 21 : Précisez le nom et l'adresse du préfixe*

Prefixes ?

Prefix Name:

Prefix Length:


Cancel OK

4. Saisissez la **longueur du préfixe** de l'adresse IP.

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

5. Cliquez sur **OK**.

Illustration 22 : Tableau de délégation de préfixe

Prefix Name	Prefix Length	
Outside-Prefix	::1:0:0:1/64	

+ Add

- Vous pouvez également activer le serveur sans état DHCPv6 sur cette interface (voir [Activer le serveur sans état DHCPv6](#)). Ce faisant, nous vous recommandons de cocher également l'option **Enable DHCP for non-address config** (Activer DHCP pour les configurations sans adresse).

### Étape 6

Pour les interfaces routées, vous pouvez éventuellement définir les valeurs suivantes dans la page de **base** :

- Pour appliquer l'utilisation des identifiants d'interface au format EUI-64 modifié dans les adresses IPv6 sur un lien local, cochez la case **Enforce EUI-64**.
- Pour définir manuellement l'adresse du lien local, saisissez une adresse dans le champ **Link-Local address** (adresse du lien-local).

Une adresse de lien local doit commencer par FE8, FE9, FEA ou FEB, par exemple fe80::20d:88ff:feee:6a82. Si vous ne souhaitez pas configurer d'adresse globale et que vous avez seulement besoin de configurer une adresse link-local, vous avez la possibilité de définir manuellement cette dernière. Notez que nous vous recommandons d'attribuer automatiquement l'adresse de lien local en fonction du format EUI-64 modifié. Par exemple, si d'autres appareils imposent l'utilisation du format EUI-64 modifié, une adresse de lien local attribuée manuellement peut entraîner la perte de paquets.

### Étape 7

Pour les interfaces routées, vous pouvez éventuellement définir les valeurs suivantes dans la page **DHCP** :

- Cochez la case **Enable DHCP for IPv6 non-address configuration** (activer DHCP pour la configuration sans adresse IPv6) pour définir l'indicateur de configuration d'adresse gérée dans le paquet de publication de routeur IPv6.

Cet indicateur dans le paquet de publication du routeur signale aux clients d'autoconfiguration IPv6 qu'ils doivent utiliser DHCPv6 pour obtenir des adresses, en plus de l'adresse d'autoconfiguration sans état dérivée.

- Cochez la case **Enable DHCP for IPv6 non-address configuration** (activer DHCP pour la configuration sans adresse IPv6) pour définir l'indicateur de configuration d'autre adresse dans le paquet de publication de routeur IPv6.

Cet indicateur dans le paquet de publication du routeur signale aux clients d'autoconfiguration IPv6 qu'ils doivent utiliser DHCPv6 pour obtenir des informations supplémentaires de DHCPv6, telles que l'adresse du serveur DNS. Utilisez cette option lorsque vous utilisez le serveur sans état DHCPv6 avec la délégation de préfixe DHCPv6.

### Étape 8

Pour les interfaces routées, consultez [Configurer la découverte des voisins IPv6](#), à la page 57 pour configurer les paramètres dans les pages **Préfixes** et **Paramètres**. Pour les interfaces BVI, consultez les paramètres en suivants sur la page **Paramètres** :

- Tentatives DAD** : nombre maximum de tentatives DAD, entre 1 et 600. Définissez la valeur sur 0 pour désactiver le traitement de la détection d'adresses en double (DAD). Ce paramètre configure le nombre



de messages consécutifs de sollicitation de voisin qui sont envoyés sur une interface pendant que la DAD est effectuée sur les adresses IPv6. La valeur par défaut est 1 tentative.

- **Intervalle NS** : l'intervalle entre les retransmissions de sollicitation des voisins IPv6 sur une interface, entre 1 000 et 3600 000 ms. La valeur par défaut est 1000 ms.
- **Temps d'accessibilité** : Il s'agit de la durée pendant laquelle un nœud IPv6 distant est considéré comme accessible après qu'un événement de confirmation d'accessibilité se soit produit, entre 0 et 3600 000 ms. La valeur par défaut est 0 ms. Lorsque 0 est utilisé pour la valeur, la durée accessible est envoyée comme indéterminée. Il appartient aux périphériques de réception de définir et de suivre la durée accessible. La durée d'accessibilité du voisin permet de détecter les voisins non disponibles. Des durées configurées plus courtes permettent de détecter plus rapidement les voisins non disponibles, mais des durées plus courtes consomment plus de bande passante réseau IPv6 et de ressources de traitement dans tous les périphériques réseau IPv6. Des durées configurées très courtes ne sont pas recommandées pour le fonctionnement normal d'un IPv6.

**Étape 9** Cliquez sur **OK**.

**Étape 10** Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer) > Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

---

## Configurer la découverte des voisins IPv6

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

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

### Avant de commencer

Pris en charge en mode routé uniquement. Pour les paramètres de voisins IPv6 pris en charge en mode transparent, consultez [Configuration d'une adresse globale IPv6, à la page 53](#).

### Procédure

---

**Étape 1** Sélectionnez **Devices (périphériques) > Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.

**Étape 2** Cliquez sur **Edit** (✎) pour l'interface que vous souhaitez modifier.

**Étape 3** Cliquez sur **IPv6**, puis sur **Prefixes** (préfixes).

**Étape 4**

(Facultatif) Procédez comme suit pour configurer les préfixes IPv6 à inclure dans les annonces de routeur IPv6 :

- a) Cliquez sur (+) **Add Prefix** (Ajouter un préfixe).
- b) Dans le champ **Address** (adresse), saisissez l'adresse IPv6 avec la longueur du préfixe ou cochez la case **par défaut** pour utiliser le préfixe par défaut.
- c) (Facultatif) Décochez la case **Advertisement** (Publicité) pour indiquer que le préfixe IPv6 n'est pas annoncé.
- d) Cochez la case **Off Link** (désactiver le lien) pour indiquer que le préfixe spécifié est affecté au lien. Les nœuds envoyant du trafic vers des adresses qui contiennent le préfixe spécifié considèrent la destination comme accessible localement sur le lien. Ce préfixe ne doit pas être utilisé pour la détermination sur la liaison.
- e) Pour utiliser le préfixe précisé pour la configuration automatique, cochez la case **Autoconfiguration**.
- f) Pour la **durée de vie du préfixe**, cliquez sur la **durée** ou la **date d'expiration**.

- **Duration** (Durée) : saisissez une **durée de vie préférée** pour le préfixe en secondes. Ce paramètre correspond à la durée pendant laquelle le préfixe IPv6 spécifié est annoncé comme valide. La valeur maximale représente l'éternité. Les valeurs valides sont comprises entre 0 et 4294967295. La valeur par défaut de la durée de vie valide est de 2 592 000 (30 jours). Saisissez une **durée de vie valide** pour le préfixe en secondes. Ce paramètre correspond à la durée pendant laquelle le préfixe IPv6 spécifié est annoncé comme préféré. La valeur maximale représente l'éternité. Les valeurs valides sont comprises entre 0 et 4294967295. Le paramètre par défaut est 604 800 (sept jours). Vous pouvez également cocher la case **Infinite** pour définir une durée illimitée.

- **Expiration Date** (Date d'expiration) : choisissez une date et une heure **Valides et préférées**.

- g) Cliquez sur **OK**.

**Étape 5**

Cliquez sur **Settings** (Paramètres).

**Étape 6**

(Facultatif) Définissez le nombre maximal de **tentatives DAD**, entre 1 et 600. La valeur par défaut est 1 tentative. Définissez la valeur sur 0 pour désactiver le traitement de la détection d'adresses en double (DAD).

Ce paramètre configure le nombre de messages consécutifs de sollicitation de voisin qui sont envoyés sur une interface pendant que la DAD est effectuée sur des adresses IPv6.

Pendant le processus d'autoconfiguration sans état, la DAD (Détection des doublons d'adresse) vérifie le caractère unique des nouvelles adresses IPv6 monodiffusion avant que les adresses ne soient affectées aux interfaces.

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

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

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

**Étape 7**

(Facultatif) Configurez l'intervalle entre les retransmissions de sollicitation de voisin IPv6 dans le champ **Intervalle NS**, entre 1 000 et 3 600 000 ms.

La valeur par défaut est 1000 ms.

Les messages de sollicitation des voisins (ICMPv6 de type 135) sont envoyés sur la liaison locale par les nœuds qui tentent de découvrir les adresses de couche de liaison d'autres nœuds sur la liaison locale. Après

avoir reçu un message de sollicitation de voisin, le nœud de destination répond en envoyant un message d'annonce de voisin (ICPMv6 type 136) sur la liaison locale.

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

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

### Étape 8

(Facultatif) Configurez la durée pendant laquelle un nœud IPv6 distant est considéré comme accessible après qu'un événement de confirmation d'accessibilité se soit produit dans le champ **Reachable Time** (Temps d'accessibilité), entre 0 et 360 000 ms.

La valeur par défaut est 0 ms. Lorsque 0 est utilisé pour la valeur, la durée accessible est envoyée comme indéterminée. Il appartient aux périphériques de réception de définir et de suivre la durée accessible.

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

### Étape 9

(Facultatif) Pour supprimer les transmissions d'annonces de routeur, décochez la case **Enable RA** (activer les annonces de serveur). Si vous activez les transmissions d'annonces de routeur, vous pouvez définir leur durée de vie et l'intervalle.

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

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

- **RA Lifetime** : configurez la valeur de vie du routeur dans les annonces du routeur IPv6, entre 0 et 9 000 secondes.

La valeur par défaut est de 1800 secondes.

- **RA Interval** : configurez l'intervalle entre les transmissions des annonces du routeur IPv6, entre 3 et 1 800 secondes.

La valeur par défaut est de 200 secondes.

### Étape 10

Cliquez sur **OK**.

### Étape 11

Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer) > Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

# Configurer les paramètres avancés de l'interface

Cette section décrit comment configurer les adresses MAC pour les interfaces normales de pare-feu, comment définir l'unité de transmission maximale (MTU) et comment définir d'autres paramètres avancés.

## À propos des configurations avancées de l'interface

Cette section décrit les paramètres d'interface avancés.

## À propos des adresses MAC

Vous pouvez affecter manuellement des adresses MAC pour remplacer la valeur par défaut. Pour les instances de conteneur, le châssis FXOS génère automatiquement des adresses MAC uniques pour toutes les interfaces.



### Remarque

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



### Remarque

Pour les instances de conteneur, même si vous ne partagez pas une sous-interface, si vous configurez manuellement les adresses MAC, vérifiez que vous utilisez des adresses MAC uniques pour toutes les sous-interfaces de la même interface parente afin d'assurer une classification correcte.

## 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.
- Routed firewall mode (mode de pare-feu de routage) : toutes les interfaces VLAN partagent une adresse MAC. Assurez-vous que tous les commutateurs connectés peuvent prendre en charge ce scénario. Si les commutateurs connectés nécessitent des adresses MAC uniques, vous pouvez attribuer manuellement des adresses MAC. Consultez la section [Configurer l'adresse MAC, à la page 66](#).

Mode pare-feu transparent : chaque interface VLAN a une adresse MAC unique. Vous pouvez remplacer les adresses MAC générées si vous le souhaitez en attribuant manuellement des adresses MAC. Consultez [Configurer l'adresse MAC, à la page 66](#).

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

- EtherChannels (modèles ASA) : l'interface du canal de port utilise l'adresse MAC d'interface de groupe de canaux du plus petit numéro comme adresse MAC du canal de port. Vous pouvez aussi configurer une adresse MAC pour l'interface du canal de port. Nous vous recommandons de configurer une adresse MAC unique au cas où l'appartenance à l'interface du canal de groupe changerait. Si vous supprimez l'interface qui fournissait l'adresse MAC du canal de port, l'adresse MAC du canal de port passe à l'interface ayant le numéro le plus bas, ce qui perturbe le trafic.
- Sous-interfaces (définies par défense contre les menaces) : toutes les sous-interfaces d'une interface physique utilisent la même adresse MAC gravée. Vous pourriez souhaiter affecter des adresses MAC uniques aux sous-interfaces. Par exemple, votre fournisseur de services peut effectuer un contrôle d'accès en fonction de l'adresse MAC. En outre, étant donné que les adresses locales de lien IPv6 sont générées en fonction de l'adresse MAC, l'affectation d'adresses MAC uniques aux sous-interfaces permet d'établir des adresses locales de lien IPv6 uniques, ce qui peut éviter des perturbations de trafic dans certaines instances sur défense contre les menaces.

#### 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 propos de la MTU

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

Pour Geneve, le datagramme Ethernet entier est encapsulé, de sorte que le nouveau paquet IP est plus volumineux et nécessite une MTU plus grande : vous devez définir la MTU de l'interface source VTEP ASA comme étant la MTU du réseau + 306 octets.

### Chemin de découverte de MTU

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

### MTU par défaut

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

### MTU et fragmentation.

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

Pour les paquets TCP, les points terminaux utilisent généralement leur MTU pour déterminer la taille maximale du segment TCP (MTU – 40, par exemple). Si des en-têtes TCP supplémentaires sont ajoutés en cours de

route, par exemple pour les tunnels VPN de site à site, le MSS TCP devra peut-être être ajusté par l'entité de tunnellation. Consultez [À propos de TCP MSS, à la page 62](#).

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




---

**Remarque** L'appareil de défense contre les menaces peut recevoir des trames plus grandes que la MTU configurée tant qu'il y a de l'espace en mémoire.

---

## MTU et trames grand format

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

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

## À propos de TCP MSS

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

Vous pouvez définir le MSS TCP sur l'appareil de défense contre les menaces pour le trafic de transit à l'aide de l'objet Sysopt\_Basic dans FlexConfig; voir [#unique\\_433](#); par défaut, le MSS TCP maximal est défini sur 1380 octets. Ce paramètre est utile lorsque l'appareil de défense contre les menaces doit augmenter la taille du paquet pour l'encapsulation VPN IPsec. Cependant, pour les points terminaux non IPsec, vous devez désactiver le MSS TCP maximal sur l'appareil de défense contre les menaces .

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

Vous pouvez également configurer le MSS TCP minimal; si un hôte ou un serveur demande un très petit MSS TCP, l'appareil de défense contre les menaces peut augmenter la valeur. Par défaut, le MSS TCP minimal n'est pas activé.

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

## TCP MSS par défaut

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

## Paramètre MSS TCP maximal suggéré

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

Si vous modifiez la valeur MTU, utilisez IPv6 ou n'utilisez pas l'appareil de défense contre les menaces comme point terminal VPN IPsec, vous devez modifier le paramètre TCP MSS à l'aide de l'objet Sysopt\_Basic dans FlexConfig.



---

**Remarque** Même si vous définissez explicitement un MSS, si un composant comme le déchiffrement TLS/SSL ou la découverte de serveur nécessite un MSS particulier, il définit ce MSS en fonction de la MTU de l'interface et ignore votre paramètre MSS.

---

Consultez les consignes suivantes :

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

## Inspection ARP pour le trafic de groupe de ponts

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

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

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

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

- Si l'adresse IP, l'adresse MAC et l'interface source correspondent à une entrée ARP, le paquet est transmis.

- En cas de non-concordance entre l'adresse MAC, l'adresse IP ou l'interface, appareil de défense contre les menaces abandonne le paquet.
- Si le paquet ARP ne correspond à aucune entrée dans le tableau ARP statique, vous pouvez définir appareil de défense contre les menaces pour transférer le paquet hors de toutes les interfaces (flood) (submersion), ou pour abandonner le paquet.




---

**Remarque** L'interface dédiée Diagnostic ne submerge jamais de paquets, même si ce paramètre est réglé à flood.

---

## Tableau d'adresses MAC

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

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

Le paquet d'origine est abandonné.

## Paramètres d'usine

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




---

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

---



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

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

## Configurer la MTU

Personnaliser la MTU sur l'interface, par exemple, pour autoriser les trames étendues.

Pour les l'ISA 3000 et le défense contre les menaces virtuelles : la modification de la MTU au-delà de 1500 octets active automatiquement la réservation de trame étendue. Vous devez redémarrer le système avant de pouvoir utiliser des trames étendues. Pour le défense contre les menaces virtuelles qui prend en charge la mise en grappe, vous pouvez activer la réservation de trame étendue dans la configuration Day0 afin que, dans ce cas, vous n'ayez pas besoin de redémarrer. Après le redémarrage, vous ne pouvez pas désactiver la réservation de trame étendue. Une exception existe pour le défense contre les menaces virtuelles, où vous pouvez désactiver la réservation de trame étendue dans la configuration Day0, si elle est prise en charge. Si vous utilisez une interface dans un ensemble en ligne, le paramètre MTU n'est pas utilisé. Cependant, le paramètre de trame étendue *est* pertinent pour les ensembles en ligne; les trames étendues permettent aux interfaces en ligne de recevoir des paquets allant jusqu'à 9 000 octets. Pour activer la réservation des trames étendues, vous devez définir la MTU de *toute* interface au-dessus de 1 500 octets.

Les trames étendues sont activées par défaut sur les autres plateformes.



### Mise en garde

La modification de la valeur MTU la plus élevée sur le périphérique pour une interface de données redémarre le processus Snort lorsque vous déployez des changements de configuration, interrompant temporairement l'inspection du trafic. L'inspection est interrompue sur toutes les interfaces de données, pas seulement sur l'interface que vous avez modifiée. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend du modèle de l'appareil géré et du type d'interface. Cette mise en garde ne s'applique pas à l'interface de dépistage ni aux interfaces de gestion uniquement. Consultez [Comportement du trafic au redémarrage de Snort](#) pour obtenir de plus amples renseignements.

### Procédure

- Étape 1** Sélectionnez **Devices (périphériques) > Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.
- Étape 2** Cliquez sur **Edit** (✎) pour l'interface que vous souhaitez modifier.
- Étape 3** Sous l'onglet **General** (Général), définissez la **MTU**. Le minimum et le maximum dépendent de votre plateforme.  
Par défaut, c'est de 1500 octets.
- Étape 4** Cliquez sur **OK**.
- Étape 5** Cliquez sur **Save** (enregistrer).
- Vous pouvez maintenant aller à **Deploy (déployer) > Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

- Étape 6** Pour les ISA 3000 et défense contre les menaces virtuelles, si vous définissez l'unité de transfert maximale MTU au-dessus de 1500 octets, redémarrez le système pour activer la réservation de trame étendue. Consultez [Arrêter ou redémarrer le périphérique](#).

## Configurer l'adresse MAC

Vous devrez peut-être attribuer manuellement une adresse MAC. Vous pouvez également définir les adresses MAC actives et de veille sous l'onglet **Devices (périphériques) > Device Management (gestion des périphériques) > High Availability (haute disponibilité)**. Si vous définissez l'adresse MAC d'une interface sur les deux écrans, les adresses de l'onglet **Interfaces > Advanced (avancées)** ont préséance.



**Remarque** Pour les instances de conteneur, même si vous ne partagez pas une sous-interface, si vous configurez manuellement les adresses MAC, vérifiez que vous utilisez des adresses MAC uniques pour toutes les sous-interfaces de la même interface parente afin d'assurer une classification correcte.

### Procédure

- Étape 1** Sélectionnez **Devices (périphériques) > Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces. La page **Interfaces** est sélectionnée par défaut.
- Étape 2** Cliquez sur **Edit** (✎) pour l'interface que vous souhaitez modifier.
- Étape 3** Cliquez sur l'onglet **Advanced (Avancé)**.  
L'onglet **Information** est sélectionné.
- Étape 4** Définissez les adresses MAC active et en veille.
- Dans le champ **Active MAC Address**, entrez une adresse MAC au format H.H.H., où H est une valeur hexadécimale de 16 bits.  
  
Par exemple, l'adresse MAC 00-0C-F1-42-4C-DE serait saisie comme suit : 000C.F142.4CDE. L'adresse MAC ne doit pas avoir le bit de multidiffusion activé; autrement dit, le deuxième chiffre hexadécimal à partir de la gauche ne peut pas être un nombre impair.
  - Dans le champ **Standby MAC Address** (adresse MAC en veille), entrez une adresse MAC à utiliser avec la haute disponibilité.  
  
Si l'unité active bascule et que l'unité en veille devient active, la nouvelle unité active commence à utiliser les adresses MAC actives pour minimiser les perturbations du réseau, tandis que l'ancienne unité active utilise l'adresse en veille.
- Étape 5** Cliquez sur **OK**.
- Étape 6** Cliquez sur **Save** (enregistrer).
- Vous pouvez maintenant aller à **Deploy (déployer) > Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

## Ajouter une entrée ARP statique

Par défaut, tous les paquets ARP sont autorisés entre les membres du groupe de ponts. Vous pouvez contrôler le flux de paquets ARP en activant l'inspection ARP (voir [Inspection ARP](#)). L'inspection ARP compare les paquets ARP avec les entrées ARP *statiques* dans le tableau ARP.

Pour les interfaces routées, vous pouvez saisir des entrées ARP statiques, mais normalement, les entrées dynamiques sont suffisantes. Pour les interfaces routées, la table ARP est utilisée pour acheminer des paquets aux hôtes connectés directement. Bien que les expéditeurs identifient la destination d'un paquet par une adresse IP, la livraison réelle du paquet sur Ethernet dépend de l'adresse MAC Ethernet. Lorsqu'un routeur ou un hôte souhaite acheminer un paquet sur un réseau directement connecté, il envoie une requête ARP demandant l'adresse MAC associée à l'adresse IP, puis achemine le paquet à l'adresse MAC en fonction de la réponse ARP. L'hôte ou le routeur conserve une table ARP pour ne pas avoir à envoyer des demandes ARP pour chaque paquet à livrer. La table ARP est mise à jour dynamiquement chaque fois que des réponses ARP sont envoyées sur le réseau et, si une entrée n'est pas utilisée pendant un certain temps, elle expire. Si une entrée est incorrecte (par exemple, l'adresse MAC change pour une adresse IP donnée), l'entrée doit expirer avant de pouvoir être mise à jour avec les nouvelles informations.

Pour le mode transparent, la défense contre les menaces utilise uniquement les entrées ARP dynamiques dans le tableau ARP pour le trafic à destination et en provenance du périphérique défense contre les menaces, comme le trafic de gestion.

### Avant de commencer

Cet écran est uniquement disponible pour les interfaces nommées.

### Procédure

- 
- Étape 1** Sélectionnez **Devices (périphériques) > Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces. La page **Interfaces** est sélectionnée par défaut.
- Étape 2** Cliquez sur **Edit** (✎) pour l'interface que vous souhaitez modifier.
- Étape 3** Cliquez sur l'onglet **Advanced** (Avancé), puis sur l'onglet **ARP** (appelé **ARP et MAC** pour le mode transparent).
- Étape 4** Cliquez sur (+) **Add ARP config** (ajouter une configuration ARP). La boîte de dialogue **Add ARP Config** (Ajouter une configuration ARP) apparaît.
- Étape 5** Dans le champ **IP Address** (Adresse IP), saisissez l'adresse IP de l'hôte.
- Étape 6** Dans le champ **MAC Address** (adresse MAC), saisissez l'adresse MAC de l'hôte; par exemple, 00e0.1e4e.3d8b.
- Étape 7** Pour effectuer un ARP par mandataire pour cette adresse, cochez la case **Enable Alias** (activer l'alias).  
Si le périphérique défense contre les menaces reçoit une demande ARP pour l'adresse IP précisée, il répond avec l'adresse MAC précisée.
- Étape 8** Cliquez sur **OK**, puis cliquez à nouveau sur **OK** pour quitter les paramètres avancés.
- Étape 9** Cliquez sur **Save** (enregistrer).  
Vous pouvez maintenant aller à **Deploy (déployer) > Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.
-

## Ajouter une adresse MAC statique et désactiver l'apprentissage MAC pour un groupe de ponts

Normalement, les adresses MAC sont ajoutées au tableau d'adresses MAC de manière dynamique au fur et à mesure que le trafic en provenance d'une adresse MAC particulière entre dans une interface. Vous pouvez désactiver l'apprentissage des adresses MAC; cependant, à moins que vous ajoutiez statiquement des adresses MAC au tableau, aucun trafic ne peut passer par le périphérique de défense contre les menaces. Vous pouvez également ajouter des adresses MAC statiques au tableau d'adresses MAC. L'ajout d'entrées statiques offre l'avantage de prévenir l'usurpation d'adresse MAC. Si un client avec la même adresse MAC qu'une entrée statique tente d'envoyer le trafic vers une interface qui ne correspond pas à l'entrée statique, le périphérique de défense contre les menaces abandonne le trafic et génère un message système. Lorsque vous ajoutez une entrée ARP statique (voir [Ajouter une entrée ARP statique](#), à la page 67), une entrée d'adresse MAC statique est automatiquement ajoutée au tableau d'adresses MAC.

### Avant de commencer

Cet écran est uniquement disponible pour les BVI nommés en mode transparent.

### Procédure

- 
- Étape 1** Sélectionnez **Devices (périphériques) > Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil de défense contre les menaces. La page **Interfaces** est sélectionnée par défaut.
  - Étape 2** Cliquez sur **Edit** (✎) pour l'interface que vous souhaitez modifier.
  - Étape 3** Cliquez sur l'onglet **Advanced** (Avancé), puis sur l'onglet **ARP and MAC** (ARP et MAC).
  - Étape 4** (Facultatif) Désactivez l'apprentissage MAC en décochant la case **Enable MAC Learning** (activer l'apprentissage MAC).
  - Étape 5** Pour ajouter une adresse MAC statique, cliquez sur **Add MAC Config** Ajouter une configuration MAC). La boîte de dialogue **Add MAC Config** (Ajouter une configuration MAC) apparaît.
  - Étape 6** Dans le champ **MAC Address** (adresse MAC), saisissez l'adresse MAC de l'hôte; par exemple, 00e0.1e4e.3d8b. Cliquez sur **OK**.
  - Étape 7** Cliquez sur **OK** pour quitter les paramètres avancés.
  - Étape 8** Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer) > Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.

---

## Définir les paramètres de configuration de la sécurité

Cette section décrit comment empêcher l'usurpation d'adresse IP, autoriser le réassemblage des fragments complets et remplacer le paramètre de fragment par défaut défini au niveau du périphérique dans les **paramètres de la plateforme**.

### Anti-usurpation d'identité

Cette section vous permet d'activer le transfert de chemin inverse de monodiffusion sur une interface. Le RPF de monodiffusion protège contre l'usurpation d'adresse IP (un paquet utilise une adresse IP source incorrecte

pour masquer sa source réelle) en veillant à ce que tous les paquets aient une adresse IP source qui correspond à l'interface source correcte selon la table de routage.

Normalement, le périphérique défense contre les menaces n'examine que l'adresse de destination pour déterminer vers où transférer le paquet. Le RPF de monodiffusion demande au périphérique de vérifier également l'adresse source; C'est pourquoi on l'appelle Reverse Path Forwarding. Pour tout trafic que vous souhaitez autoriser via le périphérique défense contre les menaces, la table de routage du périphérique doit inclure une route de retour vers l'adresse source. Consultez RFC 2267 pour plus d'informations.

Pour le trafic externe, par exemple, le périphérique défense contre les menaces peut utiliser la voie de routage par défaut pour satisfaire à la protection RPF de monodiffusion. Si le trafic entre par une interface externe et que l'adresse source n'est pas connue de la table de routage, le périphérique utilise la voie de routage par défaut pour identifier correctement l'interface externe comme interface source.

Si le trafic entre dans l'interface externe à partir d'une adresse connue de la table de routage, mais associée à l'interface interne, le périphérique défense contre les menaces abandonne le paquet. De même, si le trafic entre dans l'interface interne à partir d'une adresse source inconnue, le périphérique abandonne le paquet, car la route correspondante (la route par défaut) indique l'interface externe.

Le RPF de monodiffusion est mis en œuvre comme suit :

- Les paquets ICMP n'ont pas de session, donc chaque paquet est vérifié.
- UDP et TCP ont des sessions, donc le paquet initial nécessite une recherche de route inversée. Les paquets suivants arrivant au cours de la session sont vérifiés à l'aide d'un état existant conservé dans le cadre de la session. Les paquets non initiaux sont vérifiés pour s'assurer qu'ils sont arrivés sur la même interface utilisée par le paquet initial.

### Fragment par paquet

Par défaut, le périphérique défense contre les menaces autorise jusqu'à 24 fragments par paquet IP et jusqu'à 200 fragments en attente d'être réassemblés. Vous devrez peut-être laisser les fragments entrer dans votre réseau si vous avez une application qui fragmente régulièrement les paquets, comme NFS sur UDP. Toutefois, si vous n'avez pas d'application qui fragmente le trafic, nous vous recommandons de ne pas autoriser les fragments par le biais du périphérique défense contre les menaces. Les paquets fragmentés sont souvent utilisés comme attaques DoS.

### Réassemblage des fragments

Le périphérique défense contre les menaces effectue les processus de réassemblage de fragments suivants :

- Les fragments IP sont collectés jusqu'à ce qu'un ensemble de fragments soit formé ou jusqu'à ce qu'un délai d'expiration se soit écoulé.
- Si un ensemble de fragments est formé, des vérifications d'intégrité sont effectuées sur l'ensemble. Ces vérifications comprennent l'absence de chevauchement, de débordement de fin et de débordement de chaîne.
- Les fragments IP qui se terminent au périphérique défense contre les menaces sont toujours entièrement réassemblés.
- Si **Réassemblage complet des fragments** est désactivé (par défaut), l'ensemble de fragments est transféré à la couche de transport pour traitement ultérieur.
- Si **Réassemblage complet des fragments** est activé, l'ensemble de fragments est d'abord fusionné en un seul paquet IP. Le paquet IP unique est ensuite acheminé à la couche de transport pour traitement ultérieur.

### Avant de commencer

Cet écran est uniquement disponible pour les interfaces nommées.

### Procédure

---

- Étape 1** Sélectionnez **Devices (périphériques) > Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.
- Étape 2** Cliquez sur **Edit** (✎) pour l'interface que vous souhaitez modifier.
- Étape 3** Cliquez sur l'onglet **Advanced** (Avancé), puis sur l'onglet **Security Configuration** (Configuration de sécurité).
- Étape 4** Pour activer le transfert de chemin inverse de monodiffusion, cochez la case **Enable Anti Spoofing** (activer la protection contre l'usurpation d'adresse).
- Étape 5** Pour activer le réassemblage des fragments complets, cochez la case **Allow Full Fragment Reassembly** (autoriser le réassemblage des fragments complets).
- Étape 6** Pour modifier le nombre de fragments autorisés par paquet, cochez la case **Override Default Fragment Settings** (remplacer le paramètre de fragment par défaut) et définissez les valeurs suivantes :
- **Size** (Taille) : définit le nombre maximal de paquets qui peuvent être dans la base de données de réassemblage IP en attente de réassemblage. Par défaut, c'est 200. Définissez cette valeur sur 1 pour désactiver les fragments.
  - **Chain** (Chaîne) : définit le nombre maximal de paquets en lesquels un paquet IP complet peut être fragmenté. La valeur par défaut est 24 paquets.
  - **Timeout**(délai d'expiration) : définit le nombre maximum de secondes d'attente pour l'arrivée d'un paquet fragmenté complet. La minuterie démarre après l'arrivée du premier fragment d'un paquet. Si tous les fragments du paquet n'arrivent pas avant le nombre de secondes spécifié, tous les fragments du paquet déjà reçus seront rejetés. La valeur par défaut est de 5 secondes.
- Étape 7** Cliquez sur **OK**.
- Étape 8** Cliquez sur **Save** (enregistrer).
- Vous pouvez maintenant aller à **Deploy (déployer) > Deployment (déploiement)** afin de déployer la politique sur les appareils attribués. Les modifications ne sont actives que lorsque vous les déployez.
-

# Historique des interfaces de pare-feu standard pour Cisco Secure Firewall Threat Defense

Fonctionnalités	Version	Défense contre les menaces Minimum	Détails
Prise en charge de l'interface de boucle avec retour pour VTI	7.3	N'importe lequel	<p>Vous ne pouvez pas sélectionner une interface de bouclage. L'interface de boucle avec retour permet de résoudre les échecs de chemin. Si une interface tombe en panne, vous pouvez accéder à toutes les interfaces grâce à l'adresse IP attribuée à l'interface de boucle avec retour. Pour VTI, en plus de définir une interface de boucle avec retour comme interface source, la prise en charge a également été ajoutée pour permettre d'hériter de l'adresse IP d'une interface de boucle avec retour au lieu d'une adresse IP configurée de manière statique.</p> <p>Écrans Nouveaux ou modifiés :</p> <p><b>Périphériques &gt; Gestion des périphériques &gt; Interfaces &gt; Ajouter des interfaces &gt; Ajouter une interface de boucle avec retour</b></p>

Fonctionnalités	Version	Défense contre les menaces Minimum	Détails
DHCP IPv6	7.3	N'importe lequel	<p>défense contre les menaces prend désormais en charge les fonctionnalités suivantes pour l'adressage IPv6 :</p> <ul style="list-style-type: none"> <li>• Client d'adresse DHCPv6 : Le défense contre les menaces obtient une adresse globale IPv6 et une voie de routage par défaut facultative du serveur DHCPv6.</li> <li>• Client de délégation de préfixe DHCPv6 : le défense contre les menaces obtient le ou les préfixes délégués d'un serveur DHCPv6. Les défense contre les menaces peuvent ensuite utiliser ces préfixes pour configurer d'autres adresses d'interface défense contre les menaces afin que les clients SLAAC (StateLess Address Auto Configuration) puissent configurer automatiquement les adresses IPv6 sur le même réseau.</li> <li>• Annonce de routeur BGP pour les préfixes délégués</li> <li>• Serveur sans état DHCPv6 : Le défense contre les menaces fournit d'autres informations telles que le nom de domaine aux clients SLAAC lorsqu'ils envoient des paquets de demande d'information (IR) à défense contre les menaces . Le défense contre les menaces accepte uniquement les paquets IR et n'affecte pas d'adresse aux clients.</li> </ul> <p>Écrans Nouveaux ou modifiés :</p> <ul style="list-style-type: none"> <li>• <b>Périphériques &gt; Gestion des périphériques &gt; Interfaces &gt; Ajouter/modifier des interfaces &gt; IPv6 &gt; DHCP</b></li> <li>• <b>Objects (Objets) &gt; Object Management (Gestion des objets) &gt; DHCP IPv6 Pool (Bassin IPv6 DHCP)</b></li> </ul> <p>Commandes nouvelles ou modifiées : <b>show bgp ipv6 unicast, show ipv6 dhcp, show ipv6 general-prefix</b></p>
Proxy jumelé VXLAN pour défense contre les menaces virtuelles pour l'équilibreur de charge de passerelle Azure	7.3	N'importe lequel	<p>Vous pouvez configurer une interface VXLAN en mode proxy jumelé pour défense contre les menaces virtuelles dans Azure en vue de l'utiliser avec l'équilibreur de charge de passerelle Azure (GWLb). Le défense contre les menaces virtuelles définit une interface externe et une interface interne sur une seule carte réseau en utilisant les segments VXLAN dans un serveur mandataire apparié.</p> <p>Écrans Nouveaux ou modifiés :</p> <ul style="list-style-type: none"> <li>• <b>Périphériques &gt; Gestion des périphériques &gt; périphérique &gt; interfaces &gt; Ajouter des interfaces &gt; interface VNI</b></li> </ul> <p>Plateformes prises en charge : Défense contre les menaces virtuelles dans Azure</p>



Fonctionnalités	Version	Défense contre les menaces Minimum	Détails
Prise en charge de VXLAN	7.2	N'importe lequel	<p>Prise en charge de l'encapsulation VXLAN a été ajoutée.</p> <p>Écrans Nouveaux ou modifiés :</p> <ul style="list-style-type: none"> <li>• <b>Devices (Périphériques) &gt; Device Management (Gestion des périphériques) &gt; Device (périphérique) &gt; VTEP</b></li> <li>• <b>Périphériques &gt; Gestion des périphériques &gt; périphérique &gt; interfaces &gt; Ajouter des interfaces &gt; interface VNI</b></li> <li>• <b>Périphériques &gt; Gestion des périphériques &gt; Périphérique Interfaces modifier l'interface physique &gt; Général</b></li> </ul> <p>Plateformes prises en charge : toutes.</p>
Prise en charge de Geneve pour Défense contre les menaces virtuelles	7.1	N'importe lequel	<p>La prise en charge de l'encapsulation de Geneve a été ajoutée pour défense contre les menaces virtuelles afin de prendre en charge le serveur mandataire à un seul volet pour l'équilibreur de charge de passerelle AWS Amazon Web Services. L'équilibreur de charge de passerelle AWS combine une passerelle de réseau transparente (avec un point d'entrée et de sortie unique pour tout le trafic) et un équilibreur de charge qui répartit le trafic et adapte défense contre les menaces virtuelles à la demande.</p> <p>Cette fonctionnalité nécessite Snort 3.</p> <p>Écrans Nouveaux ou modifiés :</p> <ul style="list-style-type: none"> <li>• <b>Devices (Périphériques) &gt; Device Management(Gestion des périphériques) &gt; Device (périphérique) &gt; VTEP</b></li> <li>• <b>Périphériques &gt; Gestion des périphériques &gt; périphérique &gt; interfaces &gt; Ajouter des interfaces &gt; interface VNI</b></li> <li>• <b>Périphériques &gt; Gestion des périphériques &gt; Périphérique Interfaces modifier l'interface physique &gt; Général</b></li> </ul> <p>Plateformes prises en charge : Défense contre les menaces virtuelles dans AWS</p>

Fonctionnalités	Version	Défense contre les menaces Minimum	Détails
Masque de sous-réseau 31 bits	7.0	N'importe lequel	<p>Pour les interfaces routées, vous pouvez configurer une adresse IP sur un sous-réseau de 31 bits pour les connexions point à point. Le sous-réseau de 31 bits comprend seulement 2 adresses; normalement, la première et la dernière adresse du sous-réseau sont réservées pour le réseau et la diffusion, donc un sous-réseau à deux adresses n'est pas utilisable. Toutefois, si vous avez une connexion point à point et n'avez pas besoin d'adresses de réseau ou de diffusion, un sous-réseau de 31 bits est un moyen utile de conserver les adresses dans IPv4. Par exemple, le lien de basculement entre 2 FTD ne nécessite que 2 adresses; les paquets transmis par une extrémité de la liaison sont toujours reçus par l'autre extrémité, et la diffusion n'est pas nécessaire. Vous pouvez également avoir une station de gestion directement connectée exécutant SNMP ou Syslog. Cette fonctionnalité n'est pas prise en charge pour les BVI pour les groupes de ponts ou avec le routage de multidiffusion.</p> <p>Écrans Nouveaux ou modifiés :</p> <p><b>Devices(Périphériques) &gt; Device Management (Gestion des périphériques) &gt; Interfaces(interfaces).</b></p>
Synchronisation entre l'état du lien opérationnel défense contre les menaces et l'état du lien physique pour les périphériques Firepower 4100/9300	6.7	N'importe lequel	<p>Les châssis Firepower 4100/9300 peuvent maintenant synchroniser l'état de la liaison opérationnelle défense contre les menaces avec l'état de la liaison physique pour les interfaces de données. Actuellement, les interfaces sont dans un état opérationnel tant que l'état de l'administrateur FXOS et que l'état du lien physique sont actifs. L'état administratif de l'interface de l'application défense contre les menaces n'est pas pris en compte. Sans synchronisation à partir de défense contre les menaces, les interfaces de données peuvent être physiquement opérationnelles avant que l'application défense contre les menaces ne soit complètement en ligne, par exemple, ou peuvent rester actives pendant un certain temps après que vous ayez lancé un arrêt défense contre les menaces. Pour les ensembles en ligne, cette incompatibilité d'état peut entraîner l'abandon de paquets, car les routeurs externes peuvent commencer à envoyer du trafic vers défense contre les menaces avant que défense contre les menaces ne puisse le gérer. Cette fonctionnalité est désactivée par défaut et peut être activée par périphérique logique dans FXOS.</p> <p><b>Remarque</b> Cette fonctionnalité n'est pas prise en charge pour la mise en grappe, les instances de conteneur ou les défense contre les menaces avec un décorateur Radware vDP. Elle n'est pas non plus prise en charge pour ASA.</p> <p>Écrans nouveaux ou modifiés du gestionnaire de châssis Firepower Chassis Manager : <b>Logical Devices &gt; Enable Link State</b> (Périphériques logiques &gt; Activer l'état des liens)</p> <p>Commandes FXOS nouvelles ou modifiées : <b>set link-state-sync enabled, show interface expand detail</b></p> <p>Plateformes prises en charge : Firepower 4100/9300</p>

Fonctionnalités	Version	Défense contre les menaces Minimum	Détails
Prise en charge du commutateur matériel Firepower 1010	6.5	N'importe lequel	<p>L'appareil Firepower 1010 prend en charge la définition de chaque interface Ethernet comme port de commutation ou interface de pare-feu.</p> <p>Écrans Nouveaux ou modifiés :</p> <ul style="list-style-type: none"> <li>• <b>Devices (Périphériques) &gt; Device Management (Gestion des périphériques) &gt; Interfaces(interfaces).</b></li> <li>• <b>Devices (Périphériques) &gt; Device Management (Gestion des périphériques) &gt; Interfaces &gt; Edit Physical Interface (Modifier les interfaces physiques)</b></li> <li>• <b>Périphériques &gt; Gestion des périphériques &gt; Interfaces &gt; Ajouter des interfaces VLAN</b></li> </ul>
Prise en charge du Firepower 1010 PoE+ sur Ethernet 1/7 et Ethernet 1/8	6.5	N'importe lequel	<p>L'appareil Firepower 1010 prend en charge Power over Ethernet+ (PoE+) sur Ethernet 1/7 et Ethernet 1/8 lorsqu'ils sont configurés comme ports de commutation.</p> <p>Écrans Nouveaux ou modifiés :</p> <p><b>Périphériques &gt; Gestion des périphériques &gt; Interfaces Modifier l'interface physique PoE</b></p>
Sous-interfaces VLAN à utiliser avec des instances de conteneur	6.3.0	N'importe lequel	<p>Pour fournir une utilisation flexible de l'interface physique, vous pouvez créer des sous-interfaces VLAN dans FXOS et également partager des interfaces entre plusieurs instances.</p> <p>Écrans Nouveaux ou modifiés de Cisco Secure Firewall Management Center :</p> <p><b>Icône Devices (Périphériques) &gt; &gt; Device Management (Gestion des périphériques) &gt; &gt; Edit (Modifier) Onglet &gt; Interfaces</b></p> <p>Écrans Nouveaux ou modifiés de Cisco Secure Firewall chassis manager :</p> <p><b>Interfaces &gt; Toutes les interfaces &gt; Ajouter une nouvelle menu déroulant &gt; Sous-interface</b></p> <p>Commandes FXOS nouvelles ou modifiées : <b>create subinterface, set vlan, show interface, show subinterface</b></p> <p>Plateformes prises en charge : Firepower 4100/9300</p>

Fonctionnalités	Version	Défense contre les menaces Minimum	Détails
Interfaces de partage de données pour les instances de conteneurs	6.3.0	N'importe lequel	<p>Pour fournir une utilisation de l'interface physique flexible, vous pouvez partager des interfaces entre plusieurs instances.</p> <p>Écrans Nouveaux ou modifiés de Cisco Secure Firewall chassis manager :</p> <p><b>Interfaces &gt; All Interfaces (Toutes les interfaces) &gt; Type</b></p> <p>Commandes FXOS nouvelles ou modifiées : <b>set port-type data-sharing, show interface</b></p> <p>Plateformes prises en charge : Firepower 4100/9300</p>
Routage et pont intégrés	6.2.0	N'importe lequel	<p>Le routage et le pont intégrés permettent d'effectuer le routage entre un groupe de ponts et une interface routée. Un groupe de ponts est un groupe d'interfaces que défense contre les menaces relie par des ponts au lieu de routes. Le défense contre les menaces n'est pas un vrai pont, car défense contre les menaces continue d'agir comme un pare-feu : le contrôle d'accès entre les interfaces est contrôlé et toutes les vérifications de pare-feu usuelles sont en place.</p> <p>Auparavant, vous ne pouviez configurer les groupes de ponts qu'en mode de pare-feu transparent, où vous ne pouvez pas effectuer d'acheminement entre les groupes de ponts. Cette fonctionnalité vous permet de configurer des groupes de ponts en mode de pare-feu routé et pour effectuer le routage entre des groupes de ponts et entre un groupe de ponts et une interface routée. Le groupe de ponts participe au routage en utilisant une interface virtuelle de pont (BVI) pour servir de passerelle au groupe de ponts. Le routage et le pont intégrés offrent une solution de rechange au commutateur de couche 2 externe si vous avez des interfaces supplémentaires sur défense contre les menaces à affecter au groupe de ponts. En mode routé, les BVI peuvent être une interface nommée et participer séparément des interfaces membres à certaines fonctionnalités, telles que les règles d'accès et le serveur DHCP.</p> <p>Les fonctionnalités suivantes, prises en charge en mode transparent, ne sont pas prises en charge en mode routé : la mise en grappe. Les fonctionnalités suivantes ne sont pas prises en charge sur les BVI : le routage dynamique et le routage de multidiffusion.</p> <p>Écrans Nouveaux ou modifiés :</p> <ul style="list-style-type: none"> <li>• <b>Devices (Périphériques) &gt; Device Management (Gestion des périphériques) &gt; Interfaces &gt; Edit Physical Interface (Modifier les interfaces physiques)</b></li> <li>• <b>Périphériques &gt; Gestion des périphériques &gt; Interfaces &gt; Ajouter des interfaces &gt; Interfaces de groupe de pont</b></li> </ul> <p>Plateformes prises en charge : toutes, à l'exception de Firepower 2100 et de défense contre les menaces virtuelles</p>

## 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.