Interfaces

Les rubriques suivantes expliquent comment configurer les interfaces sur votre appareil Cisco Firepower Threat Defense.

À propos des interfaces FTD

FTD comprend des interfaces de données ainsi qu'une interface Management (gestion)/Diagnostic.

Lorsque vous connectez un câble à un point de connexion d'interface (physiquement ou virtuellement), vous devez configurer l'interface. Au minimum, vous devez nommer l'interface et l'activer pour qu'elle puisse faire passer le trafic. Si l'interface est membre d'un groupe de ponts, il suffit de nommer l'interface. Pour les non-membres du groupe de ponts, vous devez également attribuer une adresse IP à l'interface. Si vous avez l'intention de créer des sous-interfaces VLAN plutôt qu'une interface physique unique sur un port donné, vous devez généralement configurer les adresses IP sur la sous-interface, et non sur l'interface physique. Les sous-interfaces VLAN permettent de diviser une interface physique en plusieurs interfaces logiques étiquetées avec différents ID de VLAN, ce qui est utile lorsque vous vous connectez à un port de jonction sur un commutateur. Vous ne configurez pas d'adresses IP sur les interfaces passives.

La page **Interfaces** comprend des sous-pages pour les types d'interfaces : **Interfaces** (pour les interfaces physiques), **Bridge Groups (Groupes de ponts)**, **Virtual Tunnel Interfaces (Interfaces de tunnel virtuel)**, **EtherChannels** et **VLAN** (pour le Firepower 1010). Notez que les EtherChannels Firepower 4100/9300 sont répertoriés sur la page **Interfaces** et non sur la page **EtherChannel**, car vous ne pouvez modifier les paramètres

EtherChannel que dans FXOS, et non dans le FDM. Chaque page affiche les interfaces disponibles : leurs noms, adresses, modes et états. Vous pouvez modifier l'état d'une interface, activé ou désactivé, directement dans la liste des interfaces. La liste affiche les caractéristiques de l'interface en fonction de votre configuration. Utilisez la flèche d'ouverture/fermeture sur une interface de groupe de ponts, EtherChannel ou VLAN pour afficher les interfaces membres, qui apparaissent également d'elles-mêmes dans la liste appropriée. Vous pouvez également afficher les sous-interfaces pour les interfaces parentes prises en charge. Pour en savoir plus sur le mappage de ces interfaces aux interfaces virtuelles et aux adaptateurs réseau, consultez Comment les adaptateurs réseau et les interfaces VMware correspondent aux interfaces physiques FTD.

Les rubriques suivantes expliquent les limites de la configuration des interfaces au moyen de FDM ainsi que d'autres concepts de gestion des interfaces.

Modes d'interface

Vous pouvez configurer l'un des modes suivants pour chaque interface :

Acheminé

Chaque interface routée de couche 3 nécessite une adresse IP sur un sous-réseau unique. Vous attachez généralement ces interfaces à des commutateurs, à un port d'un autre routeur ou à une passerelle de fournisseur de services Internet/de réseau étendu (WAN).

Passif

Les interfaces passives surveillent le trafic circulant sur un réseau à l'aide d'un commutateur SPAN ou d'un port miroir. Le port SPAN ou miroir permet de copier le trafic d'autres ports du commutateur. Cette fonction assure la visibilité du système dans le réseau sans être dans le flux du trafic réseau. Lorsqu'il est configuré dans un déploiement passif, le système ne peut pas prendre certaines mesures telles que le blocage ou la mise en forme du trafic. Les interfaces passives reçoivent tout le trafic sans condition et aucun trafic reçu sur ces interfaces n'est retransmis.

Ports de commutation (Firepower 1010)

Les ports de commutation redirigent le trafic au niveau de la couche 2 en utilisant la fonction de commutation matérielle. 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 Cisco Firepower Threat Defense. 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. Vous ne pouvez pas configurer l'interface de gestion comme port de commutation.

Membre du groupe du pont

Un groupe de ponts est un groupe d'interfaces que le périphérique Cisco Firepower Threat Defense relie par des ponts au lieu de routes. Toutes les interfaces se trouvent sur le même réseau. Le groupe de ponts est représenté par une interface virtuelle de pont (BVI) qui a une adresse IP sur le réseau de pont.

Vous pouvez acheminer entre les interfaces routées et les BVI, si vous nommez le BVI. Dans ce cas, le BVI agit comme passerelle entre les interfaces membres et les interfaces routées. Si vous ne nommez pas le BVI, le trafic sur les interfaces de membre du groupe de ponts ne peut pas quitter le groupe de ponts. Normalement, vous devez nommer l'interface afin de pouvoir acheminer les interfaces membres vers Internet.

L'une des utilisations d'un groupe de ponts en mode routé consiste à utiliser des interfaces supplémentaires sur le périphérique Cisco Firepower Threat Defense plutôt qu'un commutateur externe. Vous pouvez associer des points terminaux directement aux interfaces des membres du groupe de ponts. Vous pouvez également connecter des commutateurs pour ajouter d'autres points terminaux au même réseau que la BVI.

Interface de gestion/dépistage

Le port physique étiqueté Management (gestion) (ou pour FTDv, l'interface virtuelle de management 0/0 (gestion 0/0)) est en fait associé à deux interfaces distinctes.

- Interface virtuelle de gestion : cette adresse IP est utilisée pour la communication du système. Il s'agit de l'adresse utilisée par le système pour les licences Smart et pour récupérer les mises à niveau de la base de données. Vous pouvez ouvrir des sessions de gestion (FDM et interface de ligne de commande). Vous devez configurer une adresse de gestion, qui est définie sur **System Settings (paramètres système)** > **Management Interface (interface de gestion)**.
- Interface virtuelle de diagnostic : vous pouvez utiliser cette interface pour envoyer des messages syslog à un serveur syslog externe. La configuration d'une adresse IP pour l'interface de diagnostic est facultative. La principale raison de configurer l'interface est de l'utiliser pour les messages syslog. Cette interface apparaît et peut être configurée sur la page **Device (appareil)** > **Interfaces**. L'interface de diagnostic autorise uniquement le trafic de gestion et n'autorise pas le trafic de transit.

(Périphériques matériels.) Une façon de configurer la gestion et le diagnostic consiste à ne pas câbler le port physique à un réseau. À la place, configurez uniquement l'adresse IP de gestion et configurez-la pour utiliser les interfaces de données comme passerelle pour obtenir les mises à jour à partir d'Internet. Ensuite, ouvrez les interfaces internes au trafic HTTPS/SSH (par défaut, HTTPS est activé) et ouvrez le FDM à l'aide de l'adresse IP interne (voir Configuration de la liste d'accès de gestion).

Pour le FTDv, la configuration recommandée consiste à associer Management 0/0 (gestion 0/0) au même réseau que l'interface interne et à utiliser l'interface interne comme passerelle. Ne configurez pas d'adresse distincte pour le diagnostic.

Recommandations pour la configuration d'un réseau de gestion distinct

(Périphériques matériels.) Si vous souhaitez utiliser un réseau de gestion distinct, câblez l'interface de gestion physique à un commutateur ou à un routeur.

Pour FTDv, associez Management0/0 à un réseau distinct de celui des interfaces de données. Si vous utilisez toujours les adresses IP par défaut, vous devrez modifier l'adresse IP de gestion ou l'adresse IP de l'interface interne, car elles se trouvent sur le même sous-réseau.

Ensuite, configurez les éléments suivants :

- Sélectionnez **Device (Périphérique)** > **System Settings (Paramètres système)** > **Management Interface (Interface de gestion)** et configurez des adresses IPv4 ou IPv6 (ou les deux) sur le réseau connecté. Si vous le souhaitez, vous pouvez configurer un serveur DHCP pour fournir des adresses IPv4 à d'autres points terminaux du réseau. S'il y a un routeur avec une voie de routage vers l'Internet sur le réseau de gestion, utilisez-le comme passerelle. Sinon, utilisez les interfaces de données comme passerelle.
- Configurez une adresse pour l'interface de diagnostic (sur **Device (Périphérique)** > **Interfaces**) uniquement si vous avez l'intention d'envoyer des messages syslog vers un serveur syslog via cette interface. Sinon, ne configurez pas d'adresse pour le diagnostic; elle n'est pas nécessaire. Toute adresse IP que vous configurez doit se trouver sur le même sous-réseau que l'adresse IP de gestion et ne peut pas se trouver dans l'ensemble de serveurs DHCP. Par exemple, si vous utilisez 192.168.45.45 comme adresse de gestion et 192.168.45.46-192.168.45.254 comme ensemble DHCP, vous pouvez configurer le diagnostic en utilisant n'importe quelle adresse comprise entre 192.168.45.1 et 192.168.45.44.

Zones de sécurité

Chaque interface peut être affectée à une seule zone de sécurité. Vous appliquez votre politique de sécurité en fonction des zones. Par exemple, vous pouvez affecter l'interface interne à la zone interne; et l'interface externe avec la zone externe. Ensuite, vous pouvez configurer votre politique de contrôle d'accès pour permettre au trafic d'être acheminé de l'intérieur vers l'extérieur, mais pas de l'extérieur vers l'intérieur, par exemple.

Chaque zone a un mode qui est directement lié au mode d'interface. Vous pouvez ajouter des interfaces au même mode de zone de sécurité uniquement.

Pour les groupes de ponts, vous ajoutez des interfaces membres aux zones, vous ne pouvez pas ajouter l'interface virtuelle de pont (BVI).

Vous n'incluez pas l'interface Management (gestion)/Diagnostic dans une zone. Les zones s'appliquent uniquement aux interfaces de données.

Vous pouvez créer des zones de sécurité sur la page **Objects** (Objets).

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, vous configurez l'adresse globale sur l'interface virtuelle de pont (BVI), et non sur chaque interface membre. Vous ne pouvez spécifier aucune des adresses suivantes comme adresse globale.
  - Adresses IPv6 réservées en interne : fd00::/56 (from=fd00:: to= fd00:0000:0000:00ff:ffff:ffff:ffff:ffff)
  - Une adresse non spécifiée, telle que ::/128
  - L'adresse de bouclage, ::1/128
  - adresses multidiffusion, ff00::/8
  - adresses locales du lien, fe80::/10
- 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 d'adresse ou pour les fonctions de découverte de réseau telles que la résolution d'adresse et la découverte de voisin. Dans un groupe de ponts, l'activation d'IPv6 sur l'interface BVI configure automatiquement les adresses locales de lien pour chaque interface de membre du groupe de ponts. Chaque interface doit avoir sa propre adresse, car l'adresse locale de lien n'est disponible que sur un segment et est liée à l'adresse MAC de l'interface.

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. Si vous ne configurez pas d'adresse globale, vous devez configurer l'adresse locale de lien. La configuration peut s'effectuer automatiquement ou manuellement.

Fonctionnalité Auto-MDI/MDIX

Pour les interfaces RJ-45, 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. Pour Gigabit Ethernet, lorsque la vitesse et le mode duplex sont définis à 1000 et plein, l'interface négocie toujours automatiquement; par conséquent, Auto-MDI/MDIX est toujours activé et vous ne pouvez pas le désactiver.

Lignes directrices et limites des interfaces

Les rubriques suivantes traitent de certaines des limites des interfaces.

Limites de la configuration de l'interface

Lorsque vous utilisez le FDM pour configurer le périphérique, il existe plusieurs limites à la configuration de l'interface. Si vous avez besoin de l'une des fonctions suivantes, vous devez utiliser le FMC pour configurer l'appareil.

- Le mode de pare-feu routé uniquement est pris en charge. Vous ne pouvez pas configurer des interfaces transparentes en mode pare-feu.
- Vous pouvez configurer des interfaces passives, mais pas les interfaces ERSPAN.
- Vous ne pouvez pas configurer les interfaces en ligne (dans un ensemble intégré) ou le mode tap en ligne pour le traitement IPS uniquement. Les interfaces en mode IPS uniquement contournent de nombreuses vérifications de pare-feu et ne prennent en charge que la politique de sécurité IPS. En comparaison, 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 mode pare-feu en fonction de votre politique de sécurité.
- Vous ne pouvez pas configurer interfaces redondantes.
- Vous pouvez configurer les canaux EtherChannels dans FDM pour les modèles suivants : Firepower 1000, Firepower 2100, Secure Firewall 3100, ISA 3000. Le Firepower 4100/9300 prend en charge EtherChannels, mais vous devez effectuer toute la configuration matérielle des EtherChannels dans FXOS sur le châssis. Firepower 4100/9300Les EtherChannels apparaissent dans la page **Interfaces** FDMà côté des interfaces physiques simples.
- Vous ne pouvez ajouter qu'un seul groupe de ponts.
- FTD prend en charge IPv4 PPPoE sur les interfaces de distribution uniquement. PPPoE n'est pas pris en charge sur les unités à haute disponibilité.

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
FTDv	50
ISA 3000	100

Configurer une interface physique

Au minimum, vous devez activer une interface physique pour l'utiliser. Vous devez également le nommer et configurer l'adressage IP. Vous ne configureriez pas l'adressage IP si vous avez l'intention de créer des sous-interfaces VLAN, si vous configurez une interface en mode passif ou si vous avez l'intention d'ajouter l'interface à un groupe de ponts. Firepower 4100/9300 Les EtherChannels sont affichés dans les pages FDM **d'interfaces** à côté des interfaces physiques simples, et cette procédure s'applique également à ces EtherChannels. Vous devez effectuer toute la configuration matérielle des canaux EtherChannels de Firepower 4100/9300dans FXOS sur le châssis.

Remarque Pour configurer les interfaces physiques comme ports de commutateur Firepower 1010, consultez Configurer les interfaces VLAN et les ports de commutation (Firepower 1010), à la page 26.

Pour configurer les interfaces physiques comme interfaces passives, consultez Configurer l'interface physique en mode passif, à la page 46.

Vous pouvez désactiver une interface pour empêcher temporairement la transmission sur le réseau connecté. Vous n'avez pas besoin de supprimer la configuration de l'interface.

Procédure

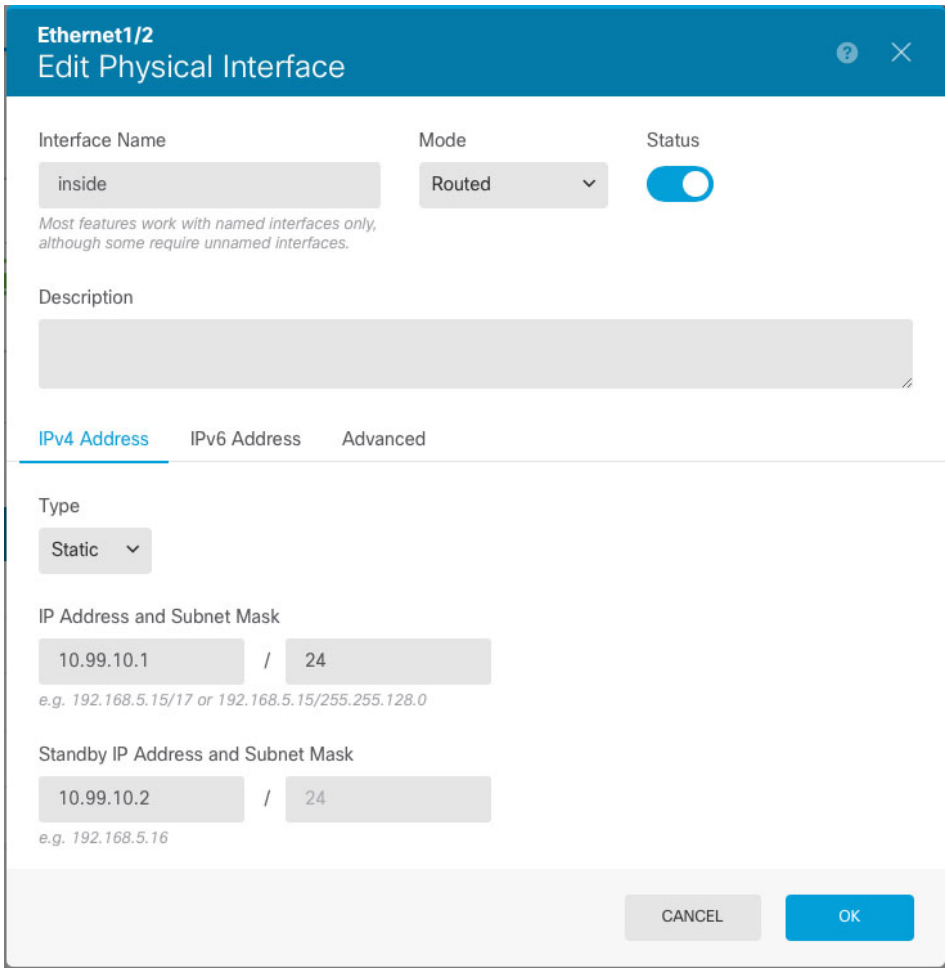
Étape 1 Cliquez sur **Device** (dispositif), puis sur le lien dans le résumé des **Interfaces**.

La page **Interfaces** est sélectionnée par défaut. La liste des interfaces affiche les interfaces physiques : leurs noms, adresses et états.

Étape 2 Cliquez sur l'icône de modification ( ) pour l'interface physique que vous souhaitez modifier.

Vous ne pouvez pas modifier une interface que vous utilisez comme lien de basculement ou de basculement avec état dans une configuration à haute disponibilité.

Étape 3 Définissez les paramètres suivants :



a) Définissez le nom de l'interface (**Interface Name**).

Définissez le nom de l'interface en utilisant au maximum 48 caractères. Les caractères alphabétiques doivent être en minuscules. Par exemple, **inside** (interne) or **outside** (externe). Sans nom, le reste de la configuration de l'interface est ignoré. Sauf si vous configurez des sous-interfaces, l'interface doit avoir un nom. **Remarque :** Ne configurez pas le nom d'une interface que vous souhaitez ajouter à un canal EtherChannel.

Remarque
Si vous modifiez le nom, la modification se répercute automatiquement partout où vous avez utilisé l'ancien nom, y compris les zones de sécurité, les objets du serveur syslog et les définitions du serveur DHCP. Cependant, vous ne pouvez pas supprimer le nom avant de supprimer toutes les configurations qui utilisent le nom, car vous ne pouvez généralement pas utiliser une interface sans nom pour une politique ou un paramètre.

b) Choisissez le **Mode**.

- **Routed** (routage) : Les interfaces en mode routage 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, ainsi que vos politiques de pare-feu. Il s'agit du mode d'interface normal.
- **Passive** (passif) : Les interfaces passives surveillent le trafic circulant sur un réseau à l'aide d'un commutateur SPAN ou d'un port miroir. Le port SPAN ou miroir permet de copier le trafic d'autres ports du commutateur. Cette fonction assure la visibilité du système dans le réseau sans être dans le flux du trafic réseau. Lorsqu'il est configuré dans un déploiement passif, le système ne peut pas prendre certaines mesures telles que le blocage ou la mise en forme du trafic. Les interfaces passives reçoivent tout le trafic sans condition et aucun trafic reçu sur ces interfaces n'est retransmis. Si vous sélectionnez ce mode, ne suivez pas le reste de cette procédure. Au lieu de cela, consultez Configurer l'interface physique en mode passif, à la page 46. Notez que vous ne pouvez pas configurer d'adresses IP sur les interfaces passives.
- **Switch Port** (port de commutation) : (Firepower 1010) Les ports de commutation permettent la commutation matérielle entre les ports du même réseau VLAN. Le trafic commuté n'est pas soumis à la politique de sécurité. Si vous sélectionnez ce mode, ne suivez pas le reste de cette procédure. Au lieu de cela, consultez Configurer les interfaces VLAN et les ports de commutation (Firepower 1010), à la page 26.

Si vous ajoutez ultérieurement cette interface à un groupe de ponts, le mode passera automatiquement à **BridgeGroupMember** (membre du groupe de ponts). Notez que vous ne pouvez pas configurer d'adresses IP sur les interfaces des membres de groupes de ponts.

c) Définissez le curseur **Status** (état) selon sur le paramètre activé ( ).

Pour les interfaces sur un Firepower 4100/9300 périphérique, vous devez également activer l'interface dans FXOS.

Si vous avez l'intention de configurer des sous-interfaces pour cette interface physique, vous avez probablement terminé. Cliquez sur **Save** (enregistrer) puis poursuivez avec Configurer les sous-interfaces VLAN et la jonction 802.1Q, à la page 38. Sinon, continuez.

Remarque
Même lors de la configuration des sous-interfaces, il est valable de nommer l'interface et de fournir les adresses IP. Ce n'est pas la configuration habituelle, mais si vous savez que c'est ce dont vous avez besoin, vous pouvez l'établir.

d) (Facultatif) Définissez la **Description**.

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

Étape 4 Cliquez sur l'onglet **IPv4 Address** (adresse IPv4) et configurez l'adresse IPv4.

Sélectionnez l'une des options suivantes dans le champ **Type** :

- **DHCP** : Sélectionnez cette option si l'adresse doit être obtenue du serveur DHCP sur le réseau. Vous ne pouvez pas utiliser cette option si vous configurez la haute disponibilité. Modifiez les options suivantes si nécessaire :
  - **Route Metric** (mesure de routage) : Si vous obtenez la voie de routage par défaut du serveur DHCP, il s'agit de la distance administrative par rapport à la route apprise (entre 1 et 255). La valeur par défaut est 1.
  - **Obtain Default Route** (obtenir la voie de routage par défaut) : Cette option permet d'obtenir la voie de routage par défaut à partir du serveur DHCP. Vous devez normalement sélectionner cette option, qui est la valeur par défaut.

- **Static** (statique) : Sélectionnez cette option si vous souhaitez affecter une adresse qui ne doit pas être modifiée. Saisissez l'adresse IP de l'interface et le masque de sous-réseau pour le réseau connecté à l'interface. Par exemple, si vous connectez le réseau 10.100.10.0/24, vous pouvez entrer 10.100.10.1/24. Assurez-vous que l'adresse n'est pas déjà utilisée sur le réseau.

  Si vous avez configuré la haute disponibilité et que vous surveillez cette interface pour la haute disponibilité, configurez également une adresse IP de veille sur le même sous-réseau. L'adresse en veille est utilisée par cette interface sur le périphérique de secours. 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.

  Remarque
  Si un serveur DHCP est configuré pour l'interface, la configuration s'affiche. Vous pouvez modifier ou supprimer l'ensemble d'adresses DHCP. Si vous modifiez l'adresse IP de l'interface pour un sous-réseau différent, vous devez soit supprimer le serveur DHCP, soit configurer un ensemble d'adresses sur le nouveau sous-réseau, avant de pouvoir enregistrer les modifications de l'interface. Consultez Configuration du serveur DHCP.

- **PPPoE** : Sélectionnez cette option si l'adresse doit être obtenue à l'aide du protocole PPPoE (Point-to-point Protocol over Ethernet). PPPoE peut être nécessaire si l'interface est connectée à un modem DSL, un modem câble ou une autre connexion à votre fournisseur de services Internet et que votre fournisseur de services Internet utilise PPPoE pour fournir votre adresse IP. Vous ne pouvez pas utiliser cette option si vous configurez la haute disponibilité. Définissez les paramètres suivants :
  - **Group Name** (nom du groupe) : Spécifiez le nom du groupe de votre choix pour représenter cette connexion.
  - **PPPoE Username** (nom d'utilisateur PPPoE) : Spécifiez le nom d'utilisateur fourni par votre fournisseur de services Internet.
  - **PPPoE Password** : 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.

- **PPPoE Learned Route Metric** (mesure de la voie de routage apprise 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.
- **Obtain Default Route from PPPoE** (obtenir la voie de routage par défaut à partir de PPPoE) : Cochez cette case pour activer l'obtention de la voie de routage par défaut à partir du serveur PPPoE.
- **IP Address Type (type d'adresse IP)** : Choisissez **Dynamic (dynamique)** pour obtenir l'adresse IP du serveur PPPoE. Vous pouvez également choisir **Static** (statique) si vous avez reçu une adresse IP statique du fournisseur de services Internet.

Étape 5 (Facultatif) Cliquez sur l'onglet **IPv6 Address** (adresse IPv6) et configurez l'adresse IPv6.

- **State** (état) : Pour activer le traitement IPv6 et configurer automatiquement l'adresse de liaison locale lorsque vous ne configurez pas l'adresse globale, sélectionnez **Enabled** (activé). L'adresse locale de liaison est générée en fonction des adresses MAC d'interface (format EUI-64 *modifié*).

  Remarque
  La désactivation de l'adresse IPv6 ne désactive pas le traitement IPv6 sur une interface configurée avec une adresse IPv6 explicite ou activée pour la configuration automatique.

- **Address Auto Configuration** (configuration automatique de l'adresse) : Sélectionnez cette option pour configurer l'adresse automatiquement. La configuration automatique sans état IPv6 générera une adresse IPv6 globale uniquement si le lien sur lequel le périphérique réside a un routeur configuré pour fournir des services IPv6, y compris la publicité d'un préfixe global IPv6 à utiliser sur le lien. Si les services de routage IPv6 ne sont pas disponibles sur le lien, vous obtiendrez uniquement une adresse IPv6 lien-local, à laquelle vous ne pourrez pas accéder en dehors du lien réseau immédiat de l'appareil. L'adresse locale de liaison est basée sur l'ID d'interface EUI-64 modifié.

  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 dispositif FTD envoie des messages de publicité de routeur dans ce cas. Sélectionnez **Suppress RA** (supprimer RA) pour supprimer les messages et se conformer au RFC.

- **Static Address/Prefix** (adresse statique/préfixe) : Si vous n'utilisez pas la configuration automatique sans état, saisissez l'adresse IPv6 globale statique complète et le préfixe de réseau. Par exemple : 2001:0DB8::BA98:0:3210/48. Pour en savoir plus sur l'adressage IPv6, consultez Adresse IPv6, à la page 4.

  Si vous souhaitez utiliser l'adresse comme lien local uniquement, sélectionnez l'option **Link - Local** (lien local). Les adresses locales de liaison ne sont pas accessibles en dehors du réseau local. Vous ne pouvez pas configurer une adresse lien-local sur une interface de groupe de ponts.

  Remarque
  Une adresse de lien local doit commencer par FE8, FE9, FEA ou FEB, par exemple fe80::20d:88ff:feee:6a82. 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.

- **Standby IP Address** (adresse IP en veille) : Si vous configurez la haute disponibilité et que vous surveillez cette interface pour la haute disponibilité, configurez également une adresse IPv6 de veille sur le même sous-réseau. L'adresse en veille est utilisée par cette interface sur le périphérique de secours. 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.

- **Suppress RA** : Cette option permet de supprimer les publicités de routeur. FTD peut participer à des publicités de routeur afin que les dispositifs voisins puissent apprendre de façon dynamique une adresse de routeur par défaut. Par défaut, des messages de publicité de routeur (ICMPv6 type 134) sont envoyés périodiquement à chaque interface configurée IPv6.

  Des publicités de routeur sont également envoyées en réponse à des 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 supprimer ces messages sur toute interface dont vous ne souhaitez pas que le dispositif FTD fournisse le préfixe IPv6 (par exemple, l'interface externe).

Étape 6 (Facultatif) Configurer les options avancées, à la page 49.

Les paramètres avancés comprennent des paramètres par défaut appropriés pour la plupart des réseaux. Modifiez-les uniquement lors de la résolution des problèmes de réseau.

Étape 7 Cliquez sur **OK**.

Prochaine étape

- Ajoutez les interfaces aux zones de sécurité appropriées. Consultez Configuration des zones de sécurité.
- Enregistrez un nom de domaine complet (FQDN) auprès de votre fournisseur de service DNS dynamique et configurez DDNS pour que le serveur DNS soit mis à jour avec les adresses d'interface pour IPv4 et IPv6. Consultez Configuration du DNS dynamique.

Configurer des groupes de ponts

Un groupe de ponts est une interface virtuelle qui regroupe une ou plusieurs interfaces. La principale raison du regroupement d'interfaces est de créer un groupe d'interfaces commutées. Ainsi, vous pouvez connecter des postes de travail ou d'autres périphériques d'extrémité directement aux interfaces incluses dans le groupe de ponts. Vous n'avez pas besoin de les connecter par l'intermédiaire d'un commutateur physique distinct, bien que vous puissiez également connecter un commutateur à un membre d'un groupe de ponts.

Les membres du groupe n'ont pas d'adresses IP. Au lieu de cela, toutes les interfaces membres partagent l'adresse IP de l'interface virtuelle de pont (BVI). Si vous activez IPv6 sur les BVI, des adresses de lien local uniques sont automatiquement attribuées aux interfaces membres.

Vous activez et désactivez les interfaces membres individuellement. Ainsi, vous pouvez désactiver toutes les interfaces inutilisées sans avoir à les supprimer du groupe de ponts. Le groupe de ponts lui-même est toujours activé.

Vous configurez généralement un serveur DHCP sur l'interface de groupe de ponts (BVI), qui fournit des adresses IP pour tous les points terminaux connectés par l'intermédiaire des interfaces membres. Cependant, vous pouvez configurer des adresses statiques sur les points terminaux connectés aux interfaces membres si vous le souhaitez. Tous les points terminaux du groupe de ponts doivent avoir des adresses IP sur le même sous-réseau que l'adresse IP du groupe de ponts.

Lignes directrices et limites relatives à la licence

- Vous ne pouvez ajouter qu'un seul groupe de ponts.
- Les EtherChannels définis par FDM ne sont pas pris en charge en tant que membres du groupe de ponts. Les EtherChannels sur le Firepower 4100/9300 peuvent être des membres de groupes de ponts.
- Vous ne pouvez pas configurer de groupes de ponts sur Série Firepower 2100 ou les périphériques FTDv.
- 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.
- L'ISA 3000 est préconfiguré avec le groupe de ponts BVI1 (non nommé, ce qui signifie qu'il ne participe pas au routage). BVI1 comprend toutes les interfaces de données : GigabitEthernet1/1 (outside1), GigabitEthernet1/2 (inside1), GigabitEthernet1/3 (outside2) et GigabitEthernet1/4 (inside2). Vous devez définir l'adresse IP de BVI1 pour qu'elle corresponde à votre réseau.

Avant de commencer

Configurez les interfaces qui seront membres du groupe de ponts. Plus précisément, chaque interface membre doit satisfaire aux exigences suivantes :

- L'interface doit avoir un nom.
- Aucune adresse IPv4 ou IPv6 ne peut être définie pour l'interface, qu'elle soit statique ou desservie par DHCP. Si vous devez supprimer l'adresse d'une interface que vous utilisez actuellement, vous devrez peut-être supprimer d'autres configurations pour l'interface, telles que les routes statiques, le serveur DHCP ou les règles NAT, qui dépendent du fait que l'interface possède une adresse.
- Vous devez retirer l'interface de sa zone de sécurité (si elle se trouve dans une zone) et supprimer toutes les règles NAT associées à cette interface avant de pouvoir l'ajouter à un groupe de ponts.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), cliquez sur le lien dans le résumé des **Interfaces**, puis cliquez sur **Bridge Groups** (Groupes de ponts).

La liste des groupes de ponts affiche les groupes de ponts existants. Cliquez sur la flèche d'ouverture/fermeture pour afficher les interfaces membres pour chaque groupe de ponts. Les interfaces membres s'affichent également séparément dans les pages **Interfaces** ou **VLAN**.

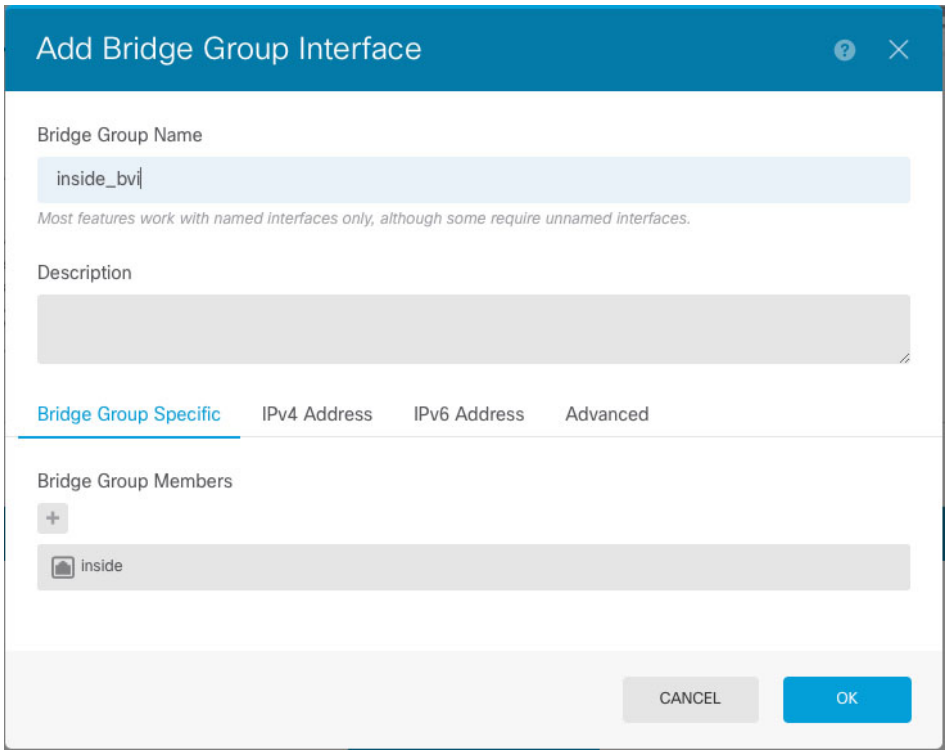
Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur l'icône de modification ( ) pour le BVI1 groupe de ponts.
- Cliquez sur **Create Bridge Grou**p (Créer un groupe de ponts) ou sur l'icône plus ( ) pour créer un nouveau groupe.

  Remarque
  Vous ne pouvez avoir qu'un seul groupe de ponts. Si vous avez déjà défini un groupe de ponts, vous devez modifier ce groupe au lieu d'essayer d'en créer un nouveau. Si vous devez créer un nouveau groupe de ponts, vous devez d'abord supprimer le groupe de ponts existant.

- Cliquez sur l'icône de suppression ( ) du groupe de ponts si vous n'en avez plus besoin. Lorsque vous supprimez un groupe de ponts, ses membres deviennent des interfaces routées standard, et toutes les règles de NAT ou l'appartenance à une zone de sécurité sont conservées. Vous pouvez modifier les interfaces pour leur attribuer des adresses IP. Si vous souhaitez les ajouter à un nouveau groupe de ponts, vous devez d'abord supprimer les règles de NAT et retirer l'interface de sa zone de sécurité.

Étape 3 Configurez les éléments suivants :



a) (Facultatif) Définissez le nom de l'interface (**Interface Name**).

Définissez le nom du groupe de ponts, en utilisant au maximum 48 caractères. Les caractères alphabétiques doivent être en minuscules. Par exemple, **inside** (interne) or **outside** (externe). Définissez le nom si vous souhaitez que ce BVI participe au routage entre lui et d'autres interfaces nommées.

Remarque
Si vous modifiez le nom, la modification se répercute automatiquement partout où vous avez utilisé l'ancien nom, y compris les zones de sécurité, les objets du serveur syslog et les définitions du serveur DHCP. Cependant, vous ne pouvez pas supprimer le nom avant de supprimer toutes les configurations qui utilisent le nom, car vous ne pouvez généralement pas utiliser une interface sans nom pour une politique ou un paramètre.

b) (Facultatif) Définissez la **Description**.

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

c) Modifiez la liste des **membres du groupe de ponts**.

Vous pouvez ajouter jusqu'à 64 interfaces ou sous-interfaces à un seul groupe de ponts.

- Ajouter une interface : cliquez sur l'icône plus (+), cliquez sur une ou plusieurs interfaces, puis cliquez sur **OK**.
- Supprimer une interface : passez le curseur sur une interface et cliquez sur le **x** sur le côté droit.

Étape 4 Cliquez sur l'onglet **IPv4 Address** (adresse IPv4) et configurez l'adresse IPv4.

Sélectionnez l'une des options suivantes dans le champ **Type** :

- **Static** (statique) : Sélectionnez cette option si vous souhaitez affecter une adresse qui ne doit pas être modifiée. Saisissez l'adresse IP du groupe de ponts et le masque de sous-réseau. Tous les points d'extrémité connectés seront sur ce réseau. Assurez-vous que l'adresse n'est pas déjà utilisée sur le réseau.

  Si vous avez configuré la haute disponibilité et que vous surveillez cette interface pour la haute disponibilité, configurez également une adresse IP de veille sur le même sous-réseau. L'adresse en veille est utilisée par cette interface sur le périphérique de secours. 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.

  Remarque
  Si un serveur DHCP est configuré pour l'interface, la configuration s'affiche. Vous pouvez modifier ou supprimer l'ensemble d'adresses DHCP. Si vous modifiez l'adresse IP de l'interface pour un sous-réseau différent, vous devez soit supprimer le serveur DHCP, soit configurer un ensemble d'adresses sur le nouveau sous-réseau, avant de pouvoir enregistrer les modifications de l'interface. Consultez Configuration du serveur DHCP.

- **Dynamic** (Dynamique) (DHCP) : sélectionnez cette option si l'adresse doit être obtenue du serveur DHCP sur le réseau. Ce n'est pas l'option habituelle pour les groupes de ponts, mais vous pouvez la configurer au besoin. Vous ne pouvez pas utiliser cette option si vous configurez la haute disponibilité. Modifiez les options suivantes si nécessaire :
  - **Route Metric** (mesure de routage) : Si vous obtenez la voie de routage par défaut du serveur DHCP, il s'agit de la distance administrative par rapport à la route apprise (entre 1 et 255). La valeur par défaut est 1.
  - **Obtain Default Route** (obtenir la voie de routage par défaut) : Cette option permet d'obtenir la voie de routage par défaut à partir du serveur DHCP. Vous devez normalement sélectionner cette option, qui est la valeur par défaut.

Étape 5 (Facultatif) Cliquez sur l'onglet **IPv6 Address** (adresse IPv6) et configurez l'adresse IPv6.

- **State** (état) : Pour activer le traitement IPv6 et configurer automatiquement l'adresse de liaison locale lorsque vous ne configurez pas l'adresse globale, sélectionnez **Enabled** (activé). L'adresse locale de liaison est générée en fonction des adresses MAC d'interface (format EUI-64 *modifié*).

  Remarque
  La désactivation de l'adresse IPv6 ne désactive pas le traitement IPv6 sur une interface configurée avec une adresse IPv6 explicite ou activée pour la configuration automatique.

- **Static Address/Prefix** (adresse statique/préfixe) : Si vous n'utilisez pas la configuration automatique sans état, saisissez l'adresse IPv6 globale statique complète et le préfixe de réseau. Par exemple : 2001:0DB8::BA98:0:3210/48. Pour en savoir plus sur l'adressage IPv6, consultez Adresse IPv6, à la page 4.

Si vous souhaitez utiliser l'adresse comme lien local uniquement, sélectionnez l'option **Link - Local** (lien local). Les adresses locales de liaison ne sont pas accessibles en dehors du réseau local. Vous ne pouvez pas configurer une adresse lien-local sur une interface de groupe de ponts.

Remarque
Une adresse de lien local doit commencer par FE8, FE9, FEA ou FEB, par exemple fe80::20d:88ff:feee:6a82. 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.

- **Standby IP Address** (adresse IP en veille) : Si vous configurez la haute disponibilité et que vous surveillez cette interface pour la haute disponibilité, configurez également une adresse IPv6 de veille sur le même sous-réseau. L'adresse en veille est utilisée par cette interface sur le périphérique de secours. 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.
- **Suppress RA** : Cette option permet de supprimer les publicités de routeur. appareil FTD peut participer à des publicités de routeur afin que les dispositifs voisins puissent apprendre de façon dynamique une adresse de routeur par défaut. Par défaut, des messages de publicité de routeur (ICMPv6 type 134) sont envoyés périodiquement à chaque interface configurée IPv6.

  Des publicités de routeur sont également envoyées en réponse à des 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 supprimer ces messages sur toute interface dont vous ne souhaitez pas que le dispositif FTD fournisse le préfixe IPv6 (par exemple, l'interface externe).

Étape 6 (Facultatif) Configurer les options avancées, à la page 49.

Vous configurez la plupart des options avancées sur les interfaces *membres* de groupe de ponts, mais certaines sont disponibles pour l'interface de groupe de ponts.

Les paramètres avancés comprennent des paramètres par défaut appropriés pour la plupart des réseaux. Modifiez-les uniquement lors de la résolution des problèmes de réseau.

Étape 7 Cliquez sur **OK**.

Prochaine étape

- Assurez-vous que toutes les interfaces membres que vous avez l'intention d'utiliser sont activées.
- Configurez un serveur DHCP pour le groupe de ponts. Consultez Configuration du serveur DHCP.
- Ajoutez les interfaces aux zones de sécurité appropriées. Consultez Configuration des zones de sécurité.
- Vérifiez que les politiques, telles que l'identité, la NAT et l'accès, fournissent les services requis pour le groupe de ponts et les interfaces de membre.

Configurer les EtherChannels

Cette section décrit les EtherChannels et comment les configurer.

Remarque Vous pouvez ajouter des EtherChannels dans le champ FDM aux modèles suivants :

- Firepower 1000
- Firepower de la série 2100
- Secure Firewall 3100
- ISA 3000

Le Firepower 4100/9300 prend en charge EtherChannels, mais vous devez effectuer toute la configuration matérielle des EtherChannels dans FXOS sur le châssis. Les EtherChannels Firepower 4100/9300 s'affichent dans la page Interfaces FDM à côté des interfaces physiques simples. Vous ne pouvez pas non plus configurer les EtherChannels dans le FDM sur d'autres modèles, comme le FTDv.

À propos des EtherChannels

Une EtherChannel 802.3ad est une interface logique (appelée interface de canal de port) composée d'un ensemble de liaisons Ethernet individuelles (un groupe de canaux), ce qui vous permet d'augmenter la bande passante pour un seul réseau. Une interface de canal de port est utilisée de la même manière qu'une interface physique lorsque vous configurez les fonctionnalités liées à l'interface.

Vous pouvez configurer jusqu'à 48 EtherChannels, selon le nombre d'interfaces prises en charge par votre modèle.

Interfaces des groupes de canaux

Chaque groupe de canaux peut avoir jusqu'à 8 interfaces actives.

Toutes les interfaces du groupe de canaux doivent être du même type et de la même vitesse. La première interface ajoutée au groupe de canaux détermine le type et la vitesse à respecter.

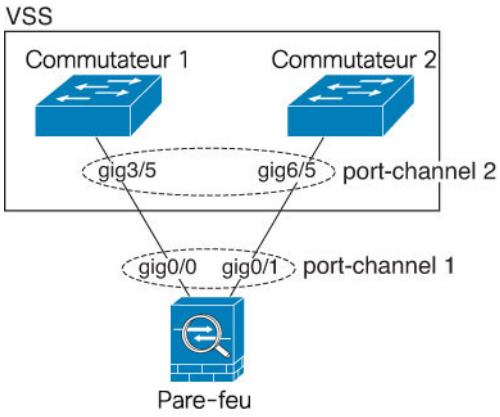
L'EtherChannel agrège le trafic sur toutes les interfaces actives disponibles dans le canal. L'interface est sélectionnée à l'aide d'un algorithme de hachage exclusif, en fonction des adresses MAC source ou de destination, des adresses IP, des numéros de ports TCP et UDP et des numéros de VLAN.

Connexion à un EtherChannel sur un autre périphérique

Le périphérique auquel vous connectez l'EtherChannel FTD doit également prendre en charge l'EtherChannel 802.3ad; par exemple, vous pouvez vous connecter au commutateur Catalyst 6500 ou à Cisco Nexus 7000.

Lorsque le commutateur fait partie d'un système de commutation virtuelle (VSS) ou d'un canal de port virtuel (vPC), vous pouvez connecter des interfaces FTD dans le même EtherChannel pour séparer les commutateurs dans le VSS/vPC. Les interfaces des commutateurs sont membres de la même interface de canal de port EtherChannel, car les commutateurs distincts se comportent comme un seul commutateur.

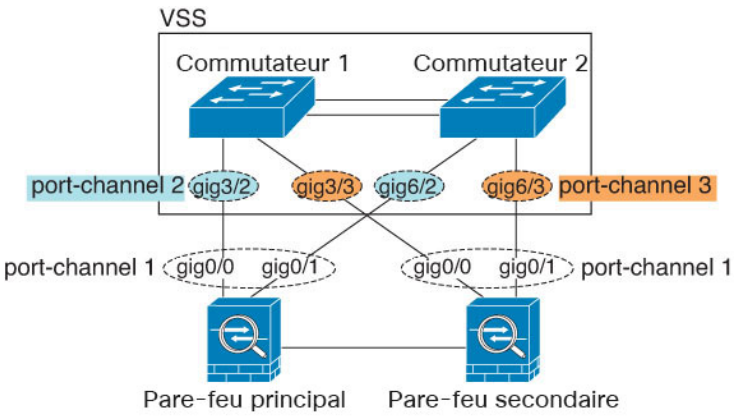
Illustration 1 : Connexion à un VSS/vPC



Remarque Si le périphérique FTD est en mode de pare-feu transparent et que vous placez le périphérique FTD entre deux ensembles de commutateurs VSS/vPC, veillez à désactiver la détection unidirectionnelle de liaison (UDLD) sur tous les ports de commutateur connectés au périphérique FTD avec un EtherChannel. Si vous activez UDLD, un port de commutation peut recevoir des paquets UDLD provenant des deux commutateurs de l'autre paire VSS/vPC. Le commutateur de réception place l'interface de réception à l'état inactif avec la raison « UDLD Neighbor mismatch » (Mauvaise correspondance des voisins UDLD).

Si vous utilisez le périphérique FTD dans un déploiement de basculement actif/en veille, vous devez créer des EtherChannels distincts sur les commutateurs du VSS/vPC, un pour chaque périphérique FTD. Sur chaque périphérique FTD, un seul EtherChannel se connecte aux deux commutateurs. Même si vous pouviez regrouper toutes les interfaces de commutateur dans un seul EtherChannel qui vous connecte aux deux périphériques FTD (dans ce cas, l'EtherChannel ne sera pas établi en raison des ID de système FTD distincts), un seul EtherChannel ne serait pas souhaitable, car vous ne pouvez pas souhaitez que le trafic soit envoyé au périphérique FTD.

Illustration 2 : Basculement actif/en veille et VSS/vPC



Protocole LACP (Link Aggregation Control Protocol)

Le protocole LACP (Link Aggregation Control Protocol) agrège les interfaces en échangeant les LACPDU (Link Aggregation Control Protocol Data Unit) entre deux périphériques réseau.

Vous pouvez configurer chaque interface physique d'un EtherChannel pour qu'elle soit :

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

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

Équilibrage de la charge

Le périphérique FTD distribue les paquets aux interfaces de l'EtherChannel en hachant l'adresse IP de source et de destination du paquet (ce critère est configurable). Le hachage obtenu est divisé par le nombre de liens actifs dans une opération modulo, le reste déterminant l'interface propriétaire du flux. Tous les paquets avec un résultat *hash_value* **mod** *active_links* de 0 sont dirigés vers la première interface de l'EtherChannel, les paquets avec un résultat de 1 vont à la deuxième interface, les paquets de résultat de 2 à la troisième interface, etc. Par exemple, si vous avez 15 liens actifs, l'opération modulo fournit des valeurs de 0 à 14. Pour six liens actifs, les valeurs sont comprises entre 0 et 5, et ainsi de suite.

Si une interface active tombe en panne et n'est pas remplacée par une interface de secours, le trafic est rééquilibrage entre les liaisons restantes. La défaillance est masquée à la fois par le Spanning Tree au niveau de la couche 2 et la table de routage au niveau de la couche 3, de sorte que le basculement est transparent pour les autres périphériques du réseau.

Adresse MAC de l'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.

Matériel Firepower et Cisco Secure Firewall

L'interface du canal de port utilise l'adresse MAC de l'interface interne Internal-Data 0/1. Vous pouvez également configurer manuellement une adresse MAC pour l'interface du canal de port. Toutes les interfaces EtherChannel d'un châssis utilisent la même adresse MAC. Sachez donc que si vous utilisez l'interrogation SNMP, par exemple, plusieurs interfaces auront la même adresse MAC.

Remarque Les interfaces membres utilisent l'adresse MAC Internal-Data 0/1 uniquement après un redémarrage. Avant de redémarrer, l'interface membre utilise sa propre adresse MAC. Si vous ajoutez une nouvelle interface membre après un redémarrage, vous devrez effectuer un autre redémarrage pour mettre à jour son adresse MAC.

Directives pour les EtherChannels

Groupe de ponts

les EtherChannels définis par l'FDM ne sont pas pris en charge en tant que membres du groupe de ponts. Les EtherChannels sur Firepower 4100/9300 peuvent être des membres de groupes de ponts.

High Availability (haute disponibilité)

- Lorsque vous utilisez une interface EtherChannel comme lien High Availability (haute disponibilité), elle doit être préconfigurée sur les deux unités de la paire High Availability (haute disponibilité); vous ne pouvez pas le configurer sur l'unité principale et vous attendre à ce qu'il soit dupliquée sur l'unité secondaire, car *le lien High Availability (haute disponibilité) lui-même est requis pour la duplication*.
- Si vous utilisez une interface EtherChannel , aucune configuration particulière n'est requise; la configuration peut être répliquée normalement à partir de l'unité principale. Pour Châssis Firepower 4100/9300 , toutes les interfaces, y compris l'EtherChannels, doivent être préconfigurées sur les deux unités.
- Vous pouvez surveiller l'EtherChannel pour High Availability (haute disponibilité). Lorsqu'une interface membre active bascule vers une interface de secours, cette activité ne fait pas apparaître l'EtherChannel comme défaillant lors de la surveillance au niveau du périphérique High Availability (haute disponibilité). Ce n'est que lorsque toutes les interfaces physiques tombent en panne que l'EtherChannel semble défaillante.
- Si vous utilisez une interface EtherChannel pour un High Availability (haute disponibilité) ou une liaison d'état, pour éviter les paquets dans le désordre, une seule interface de l'EtherChannel est utilisée. Si cette interface échoue, l'interface suivante de l'EtherChannel est utilisée. Vous ne pouvez pas modifier la configuration de l'EtherChannel lorsqu'elle est utilisée en tant que lien High Availability (haute disponibilité). Pour modifier la configuration, vous devez désactiver temporairement High Availability (haute disponibilité), ce qui empêche High Availability (haute disponibilité) de se produire pendant la durée.

Prise en charge des modèles

- Vous pouvez ajouter des EtherChannels dans le champ FDM aux modèles suivants :
  - Firepower 1000
  - Firepower de la série 2100
  - Cisco Secure Firewall 3100
  - ISA 3000

  Le Firepower 4100/9300 prend en charge EtherChannels, mais vous devez effectuer toute la configuration matérielle des EtherChannels dans FXOS sur le châssis. Les EtherChannels Firepower 4100/9300 s'affichent dans la page Interfaces FDM à côté des interfaces physiques simples. Vous ne pouvez pas non plus configurer les EtherChannels de FDM sur d'autres modèles, comme la gamme ASA 5500-X.
- Vous ne pouvez pas utiliser les ports de commutation ni les interfaces VLAN de Firepower 1010 dans les EtherChannels.

Directives générales EtherChannel

- Vous pouvez configurer jusqu'à 48 EtherChannels, selon le nombre d'interfaces disponibles sur votre modèle.
- Chaque groupe de canaux peut avoir jusqu'à 8 interfaces actives.
- Toutes les interfaces du groupe de canaux doivent être du même type de médias et de la même capacité de vitesse. Le type de support peut être RJ-45 ou SFP. Des SFP de différents types (cuivre et fibre optique) peuvent être mélangés. Vous ne pouvez pas combiner les capacités d'interface (par exemple, les interfaces 1 Go et 10 Go) en réglant la vitesse pour qu'elle soit inférieure sur l'interface de plus grande capacité, sauf pour le Secure Firewall 3100, qui prend en charge différentes capacités d'interface à condition que la vitesse soit réglée sur Detect SFP (Détecter SFP) ; dans ce cas, la vitesse la plus basse est utilisée.
- Le périphérique auquel vous connectez l'EtherChannel FTD doit également prendre en charge l'EtherChannel 802.3ad.
- Le périphérique FTD ne prend pas en charge les unités LACPDU marquées VLAN. Si vous activez le balisage VLAN natif sur le commutateur voisin à l'aide de la commande Cisco IOS **vlan dot1Q tag native**, le périphérique FTD abandonnera les LACPDU balisées. Assurez-vous de désactiver le balisage VLAN natif sur le commutateur voisin.
- Les modèles de périphériques suivants ne prennent pas en charge le débit LACP rapide ; le protocole LACP utilise toujours le débit normal. Ce paramètre n'est pas configurable. Notez que le Firepower 4100/9300, qui configure les EtherChannels dans FXOS, a le débit LACP rapide par défaut; sur ces plateformes, le débit peut être configuré.
  - Firepower 1000
  - Firepower de la série 2100
  - Cisco Secure Firewall 3100
- Dans les versions du logiciel Cisco IOS antérieures à la 15.1(1)S2, FTD ne prenait pas en charge la connexion d'un EtherChannel à une pile de commutateurs. Avec les paramètres par défaut du commutateur, si l'EtherChannel FTD est connecté en pile croisée, et si le commutateur principal est mis hors tension, l'EtherChannel connecté au commutateur restant ne sera pas mis en service. Pour améliorer la compatibilité, définissez la commande **stack-mac persistent timer** sur une valeur suffisamment grande pour prendre en compte le temps de rechargement; par exemple, 8 minutes ou 0 pour indéfini. Vous pouvez également effectuer une mise à niveau vers une version plus stable du logiciel du commutateur, comme par exemple 15.1(1)S2.
- Toute la configuration FTD fait référence à l'interface logique EtherChannel plutôt qu'aux interfaces physiques membres.

Ajouter un canal EtherChannel

Ajoutez un EtherChannel et affectez-y des interfaces membres.

Remarque Vous pouvez ajouter des EtherChannels dans le champ FDM aux modèles suivants :

- Firepower 1000
- Firepower de la série 2100
- Secure Firewall 3100
- ISA 3000

Le Firepower 4100/9300 prend en charge EtherChannels, mais vous devez effectuer toute la configuration matérielle des EtherChannels dans FXOS sur le châssis. Les EtherChannels Firepower 4100/9300 s'affichent dans la page Interfaces FDM à côté des interfaces physiques simples. Vous ne pouvez pas non plus configurer les EtherChannels dans le FDM sur d'autres modèles, comme la gamme ASA 5500-X.

Avant de commencer

- Toutes les interfaces du groupe de canaux doivent être du même type de médias et de la même capacité de vitesse. Le type de support peut être RJ-45 ou SFP. Des SFP de différents types (cuivre et fibre optique) peuvent être mélangés. Vous ne pouvez pas combiner les capacités d'interface (par exemple, les interfaces 1 Go et 10 Go) en réglant la vitesse pour qu'elle soit inférieure sur l'interface de plus grande capacité, sauf pour le Secure Firewall 3100, qui prend en charge différentes capacités d'interface à condition que la vitesse soit réglée sur Detect SFP (Détecter SFP) ; dans ce cas, la vitesse la plus basse est utilisée.
- Les interfaces membres ne peuvent pas être nommées.

Mise en garde Si vous utilisez une interface déjà présente dans votre configuration, la suppression du nom effacera toute configuration faisant référence à l'interface.

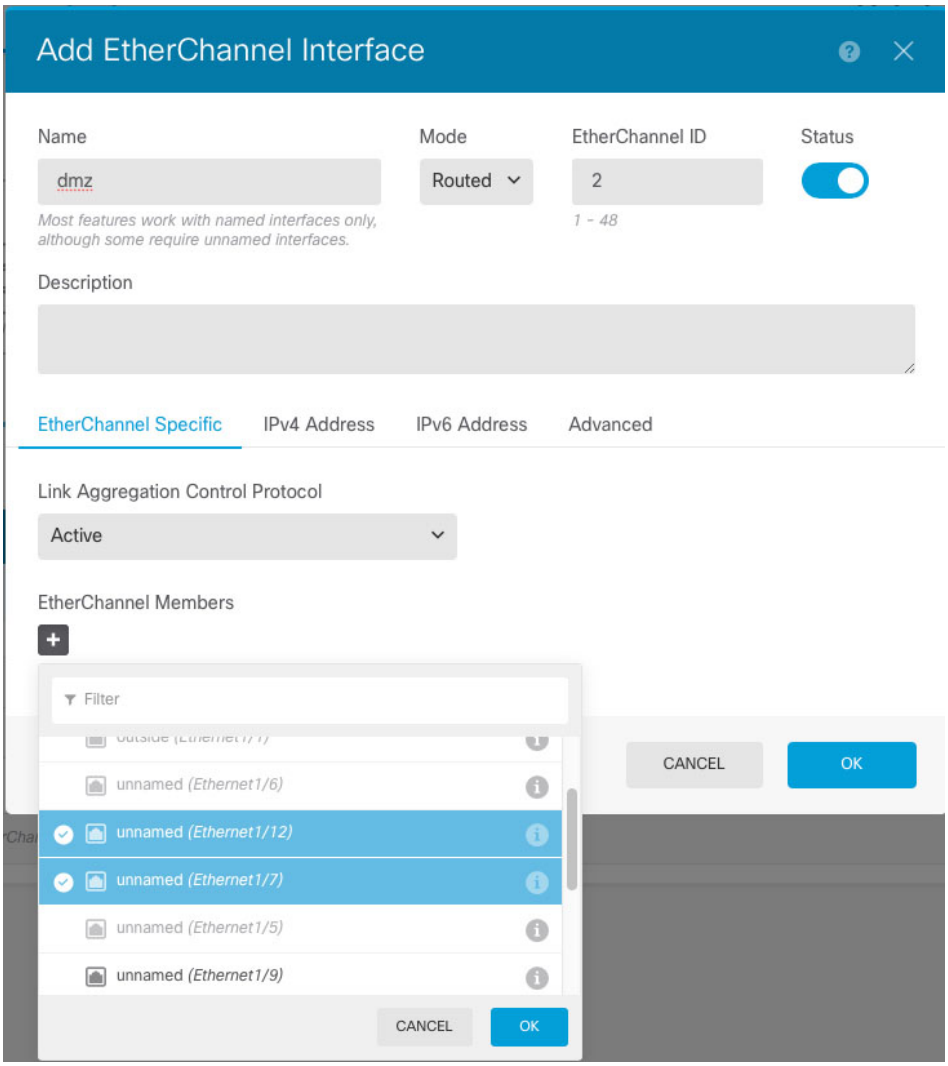
Procédure

Étape 1 Cliquez sur **Device** (périphérique), cliquez sur le lien dans le résumé **Interfaces**, puis cliquez sur **EtherChannels**.

La liste EtherChannels affiche les EtherChannels existants, leurs noms, adresses et états. Cliquez sur la flèche d'ouverture/fermeture pour afficher les interfaces membres pour chaque EtherChannel. Les interfaces membres s'affichent également séparément sur la page **Interfaces**.

Étape 2 Cliquez sur **Create EtherChannel (Créer un EtherChannel)** (s'il n'y a pas d'EtherChannel actuel) ou sur l'icône plus ( ), puis **EtherChannel** pour créer un nouvel EtherChannel.

Étape 3 Configurez les éléments suivants :



a) Définissez le nom de l'interface (**Interface Name**).

Définissez le nom de l'EtherChannel, jusqu'à 48 caractères. Les caractères alphabétiques doivent être en minuscules. Par exemple, **inside** (interne) or **outside** (externe).

Remarque
Si vous modifiez le nom, la modification se répercute automatiquement partout où vous avez utilisé l'ancien nom, y compris les zones de sécurité, les objets du serveur syslog et les définitions du serveur DHCP. Cependant, vous ne pouvez pas supprimer le nom avant de supprimer toutes les configurations qui utilisent le nom, car vous ne pouvez généralement pas utiliser une interface sans nom pour une politique ou un paramètre.

b) Définissez le **Mode**.

- **Routed** (routage) : Les interfaces en mode routage 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, ainsi que vos politiques de pare-feu. Utilisez ce mode si vous avez l'intention de faire passer le trafic par l'interface. Il s'agit du mode d'interface normal.

- **Passive** (passif) : Les interfaces passives surveillent le trafic circulant sur un réseau à l'aide d'un commutateur SPAN ou d'un port miroir. Le port SPAN ou miroir permet de copier le trafic d'autres ports du commutateur. Cette fonction assure la visibilité du système dans le réseau sans être dans le flux du trafic réseau. Lorsqu'il est configuré dans un déploiement passif, le système ne peut pas prendre certaines mesures telles que le blocage ou la mise en forme du trafic. Les interfaces passives reçoivent tout le trafic sans condition et aucun trafic reçu sur ces interfaces n'est retransmis. Si vous sélectionnez ce mode, ne suivez pas le reste de cette procédure. Au lieu de cela, consultez Configurer l'interface physique en mode passif, à la page 46.

c) Définissez l'**ID EtherChannel** sur un nombre compris entre 1 et 48 (1 et 8 pour le Firepower 1010).

d) Définissez le curseur **Status** (état) selon sur le paramètre activé ( ).

e) (Facultatif) Définissez la **Description**.

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

f) Choisissez le **mode EtherChannel**.

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

g) Ajoutez **les membres de l'EtherChannel**.

Vous pouvez ajouter jusqu'à 8 interfaces (sans nom) à l'EtherChannel.

- Ajouter une interface : cliquez sur l'icône plus ( ), cliquez sur une ou plusieurs interfaces, puis cliquez sur **OK**.
- Supprimer une interface : passez le curseur sur une interface et cliquez sur le **x** dans le côté droit.

Étape 4 Cliquez sur l'onglet **IPv4 Address** (adresse IPv4) et configurez l'adresse IPv4.

Sélectionnez l'une des options suivantes dans le champ **Type** :

- **DHCP** : Sélectionnez cette option si l'adresse doit être obtenue du serveur DHCP sur le réseau. Vous ne pouvez pas utiliser cette option si vous configurez la haute disponibilité. Modifiez les options suivantes si nécessaire :
  - **Route Metric** (mesure de routage) : Si vous obtenez la voie de routage par défaut du serveur DHCP, il s'agit de la distance administrative par rapport à la route apprise (entre 1 et 255). La valeur par défaut est 1.
  - **Obtain Default Route** (obtenir la voie de routage par défaut) : Cette option permet d'obtenir la voie de routage par défaut à partir du serveur DHCP. Vous devez normalement sélectionner cette option, qui est la valeur par défaut.
- **Static** (statique) : Sélectionnez cette option si vous souhaitez affecter une adresse qui ne doit pas être modifiée. Saisissez l'adresse IP de l'interface et le masque de sous-réseau pour le réseau connecté à l'interface. Par exemple, si vous connectez le réseau 10.100.10.0/24, vous pouvez entrer 10.100.10.1/24. Assurez-vous que l'adresse n'est pas déjà utilisée sur le réseau.

Si vous avez configuré la haute disponibilité et que vous surveillez cette interface pour la haute disponibilité, configurez également une adresse IP de veille sur le même sous-réseau. L'adresse en veille est utilisée par cette interface sur le périphérique de secours. 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.

Remarque
Si un serveur DHCP est configuré pour l'interface, la configuration s'affiche. Vous pouvez modifier ou supprimer l'ensemble d'adresses DHCP. Si vous modifiez l'adresse IP de l'interface pour un sous-réseau différent, vous devez soit supprimer le serveur DHCP, soit configurer un ensemble d'adresses sur le nouveau sous-réseau, avant de pouvoir enregistrer les modifications de l'interface. Consultez Configuration du serveur DHCP.

- **PPPoE** : Sélectionnez cette option si l'adresse doit être obtenue à l'aide du protocole PPPoE (Point-to-point Protocol over Ethernet). PPPoE peut être nécessaire si l'interface est connectée à un modem DSL, un modem câble ou une autre connexion à votre fournisseur de services Internet et que votre fournisseur de services Internet utilise PPPoE pour fournir votre adresse IP. Vous ne pouvez pas utiliser cette option si vous configurez la haute disponibilité. Définissez les paramètres suivants :
  - **Group Name** (nom du groupe) : Spécifiez le nom du groupe de votre choix pour représenter cette connexion.
  - **PPPoE Username** (nom d'utilisateur PPPoE) : Spécifiez le nom d'utilisateur fourni par votre fournisseur de services Internet.
  - **PPPoE Password** : 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.
  - **PPPoE Learned Route Metric** (mesure de la voie de routage apprise 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.
  - **Obtain Default Route from PPPoE** (obtenir la voie de routage par défaut à partir de PPPoE) : Cochez cette case pour activer l'obtention de la voie de routage par défaut à partir du serveur PPPoE.
  - **IP Address Type (type d'adresse IP)** : Choisissez **Dynamic (dynamique)** pour obtenir l'adresse IP du serveur PPPoE. Vous pouvez également choisir **Static** (statique) si vous avez reçu une adresse IP statique du fournisseur de services Internet.

Étape 5 (Facultatif) Cliquez sur l'onglet **IPv6 Address** (adresse IPv6) et configurez l'adresse IPv6.

- **State** (état) : Pour activer le traitement IPv6 et configurer automatiquement l'adresse de liaison locale lorsque vous ne configurez pas l'adresse globale, sélectionnez **Enabled** (activé). L'adresse locale de liaison est générée en fonction des adresses MAC d'interface (format EUI-64 *modifié*).

Remarque

La désactivation de l'adresse IPv6 ne désactive pas le traitement IPv6 sur une interface configurée avec une adresse IPv6 explicite ou activée pour la configuration automatique.

- **Address Auto Configuration** (configuration automatique de l'adresse) : Sélectionnez cette option pour configurer l'adresse automatiquement. La configuration automatique sans état IPv6 générera une adresse IPv6 globale uniquement si le lien sur lequel le périphérique réside a un routeur configuré pour fournir des services IPv6, y compris la publicité d'un préfixe global IPv6 à utiliser sur le lien. Si les services de routage IPv6 ne sont pas disponibles sur le lien, vous obtiendrez uniquement une adresse IPv6 lien-local, à laquelle vous ne pourrez pas accéder en dehors du lien réseau immédiat de l'appareil. L'adresse locale de liaison est basée sur l'ID d'interface EUI-64 modifié.

  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 dispositif FTD envoie des messages de publicité de routeur dans ce cas. Sélectionnez **Suppress RA** (supprimer RA) pour supprimer les messages et se conformer au RFC.

- **Static Address/Prefix** (adresse statique/préfixe) : Si vous n'utilisez pas la configuration automatique sans état, saisissez l'adresse IPv6 globale statique complète et le préfixe de réseau. Par exemple : 2001:0DB8::BA98:0:3210/48. Pour en savoir plus sur l'adressage IPv6, consultez Adresse IPv6, à la page 4.

  Si vous souhaitez utiliser l'adresse comme lien local uniquement, sélectionnez l'option **Link - Local** (lien local). Les adresses locales de liaison ne sont pas accessibles en dehors du réseau local. Vous ne pouvez pas configurer une adresse lien-local sur une interface de groupe de ponts.

  Remarque
  Une adresse de lien local doit commencer par FE8, FE9, FEA ou FEB, par exemple fe80::20d:88ff:feee:6a82. 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.

- **Standby IP Address** (adresse IP en veille) : Si vous configurez la haute disponibilité et que vous surveillez cette interface pour la haute disponibilité, configurez également une adresse IPv6 de veille sur le même sous-réseau. L'adresse en veille est utilisée par cette interface sur le périphérique de secours. 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.

- **Suppress RA** : Cette option permet de supprimer les publicités de routeur. FTD peut participer à des publicités de routeur afin que les dispositifs voisins puissent apprendre de façon dynamique une adresse de routeur par défaut. Par défaut, des messages de publicité de routeur (ICMPv6 type 134) sont envoyés périodiquement à chaque interface configurée IPv6.

  Des publicités de routeur sont également envoyées en réponse à des 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 supprimer ces messages sur toute interface dont vous ne souhaitez pas que le dispositif FTD fournisse le préfixe IPv6 (par exemple, l'interface externe).

Étape 6 Définissez la vitesse des interfaces membres en cliquant sur **Advanced (Avancé)**, et définissez la vitesse.

Vous pouvez également configurer d'autres options avancées. Consultez Configurer les options avancées, à la page 49

Étape 7 Cliquez sur **OK**.

Prochaine étape

- Ajoutez les EtherChannels aux zones de sécurité appropriées. Consultez Configuration des zones de sécurité.

Configurer les interfaces VLAN et les ports de commutation (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. Cette section 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.

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 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).
- 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 FTD. 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 Management (gestion) 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 interfacesIPS seulement (ensembles en ligne et interfaces passives) ou des interfaces EtherChannel. Lorsqu'un port de commutation doit communiquer avec un autre réseau, le périphérique FTD 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 FTD. 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 +).

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

High Availability (haute disponibilité)

- 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
  - 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 les options avancées, à la page 49

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)
- interfaces passives
- EtherChannels
- Basculement et lien d'état

Autres lignes directrices et limites

- Vous pouvez configurer un maximum de 60 interfaces nommées sur la Firepower 1010.
- Vous ne pouvez pas configurer l'interface Management (gestion) 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 une interface VLAN

Cette section décrit comment configurer les interfaces VLAN à utiliser avec les ports de commutation associés. Vous devez d'abord configurer une interface VLAN pour chaque VLAN que vous souhaitez affecter à un port de commutation.

Remarque Si vous souhaitez uniquement activer la commutation entre les ports de commutation d'un VLAN donné et ne pas effectuer de routage entre ce VLAN et d'autres VLAN ou interfaces de pare-feu, laissez le champ Nom d'interface VLAN vide. Dans ce cas, vous n'avez pas non plus besoin de configurer d'adresse IP ; toute configuration IP est ignorée.

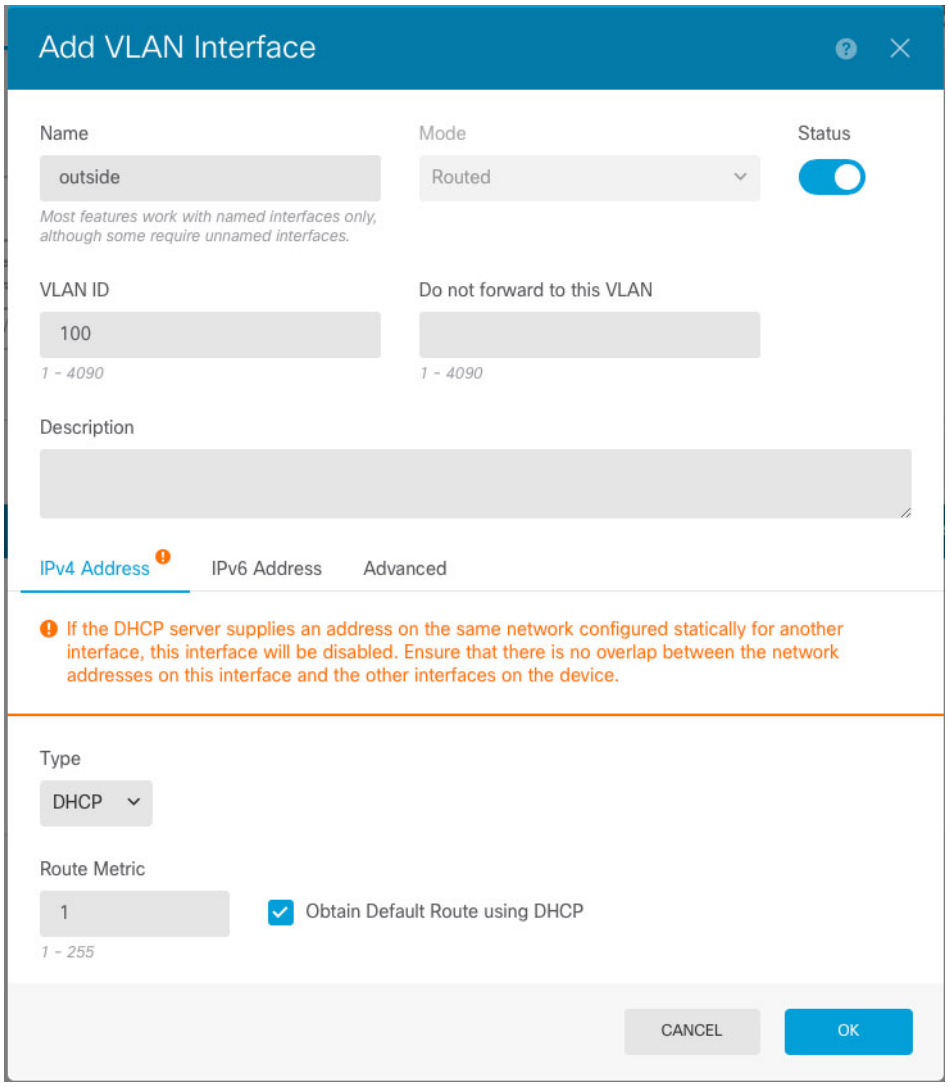
Procédure

Étape 1 Cliquez sur **Device** (Périphérique), cliquez sur le lien dans le résumé des **Interfaces**, puis cliquez sur **VLANs** (VLAN).

La liste des VLAN affiche les interfaces VLAN existantes. Cliquez sur la flèche d'ouverture/fermeture pour afficher les ports de commutation associés à chaque VLAN. Les ports de commutation sont également affichés séparément dans la page **Interfaces**.

Étape 2 Cliquez sur **Create VLAN Interface** (Créer une interface VLAN) (s'il n'y a aucun VLAN actuel) ou sur l'icône plus (+) pour créer une nouvelle interface VLAN.

Étape 3 Configurez les éléments suivants :



a) Définissez le nom de l'interface (**Interface Name**).

Définissez le nom du VLAN en utilisant au maximum 48 caractères. Les caractères alphabétiques doivent être en minuscules. Par exemple, **inside** (interne) or **outside** (externe).

Si vous ne souhaitez pas effectuer le routage entre le VLAN et d'autres VLAN ou interfaces de pare-feu, laissez le champ Nom d'interface VLAN vide.

Remarque
Si vous modifiez le nom, la modification se répercute automatiquement partout où vous avez utilisé l'ancien nom, y compris les zones de sécurité, les objets du serveur syslog et les définitions du serveur DHCP. Cependant, vous ne pouvez pas supprimer le nom avant de supprimer toutes les configurations qui utilisent le nom, car vous ne pouvez généralement pas utiliser une interface sans nom pour une politique ou un paramètre.

b) Laissez le **Mode** défini sur **Routed** (Routé).

Si vous ajoutez ultérieurement cette interface à un groupe de ponts, le mode passera automatiquement à **BridgeGroupMember** (membre du groupe de ponts). Notez que vous ne pouvez pas configurer d'adresses IP sur les interfaces des membres de groupes de ponts.

c) Définissez le curseur **Status** (état) selon sur le paramètre activé ( ).

d) Définissez l'**ID VLAN** entre 1 et 4070.

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.

e) (Facultatif) Dans le champ **Do not forward to this VLAN** (Ne pas transférer vers ce VLAN), saisissez un ID de VLAN vers lequel cette interface VLAN ne peut pas initier de trafic.

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 utiliser l'option Block Traffic From this Interface to (Bloquer le trafic depuis cette interface vers) sur le VLAN domestique ; le réseau professionnel peut accéder au réseau domestique, mais le réseau domestique ne peut pas accéder au réseau d'entreprise.

f) (Facultatif) Définissez la **Description**.

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

Étape 4 Cliquez sur l'onglet **IPv4 Address** (adresse IPv4) et configurez l'adresse IPv4.

Sélectionnez l'une des options suivantes dans le champ **Type** :

- **DHCP** : Sélectionnez cette option si l'adresse doit être obtenue du serveur DHCP sur le réseau. Vous ne pouvez pas utiliser cette option si vous configurez la haute disponibilité. Modifiez les options suivantes si nécessaire :
  - **Route Metric** (mesure de routage) : Si vous obtenez la voie de routage par défaut du serveur DHCP, il s'agit de la distance administrative par rapport à la route apprise (entre 1 et 255). La valeur par défaut est 1.
  - **Obtain Default Route** (obtenir la voie de routage par défaut) : Cette option permet d'obtenir la voie de routage par défaut à partir du serveur DHCP. Vous devez normalement sélectionner cette option, qui est la valeur par défaut.
- **Static** (statique) : Sélectionnez cette option si vous souhaitez affecter une adresse qui ne doit pas être modifiée. Saisissez l'adresse IP de l'interface et le masque de sous-réseau pour le réseau connecté à l'interface. Par exemple, si vous connectez le réseau 10.100.10.0/24, vous pouvez entrer 10.100.10.1/24. Assurez-vous que l'adresse n'est pas déjà utilisée sur le réseau.

  Si vous avez configuré la haute disponibilité et que vous surveillez cette interface pour la haute disponibilité, configurez également une adresse IP de veille sur le même sous-réseau. L'adresse en veille est utilisée par cette interface sur le périphérique de secours. 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.

  Remarque
  Si un serveur DHCP est configuré pour l'interface, la configuration s'affiche. Vous pouvez modifier ou supprimer l'ensemble d'adresses DHCP. Si vous modifiez l'adresse IP de l'interface pour un sous-réseau différent, vous devez soit supprimer le serveur DHCP, soit configurer un ensemble d'adresses sur le nouveau sous-réseau, avant de pouvoir enregistrer les modifications de l'interface. Consultez Configuration du serveur DHCP.

- **PPPoE** : Sélectionnez cette option si l'adresse doit être obtenue à l'aide du protocole PPPoE (Point-to-point Protocol over Ethernet). PPPoE peut être nécessaire si l'interface est connectée à un modem DSL, un modem câble ou une autre connexion à votre fournisseur de services Internet et que votre fournisseur de services Internet utilise PPPoE pour fournir votre adresse IP. Vous ne pouvez pas utiliser cette option si vous configurez la haute disponibilité. Définissez les paramètres suivants :
  - **Group Name** (nom du groupe) : Spécifiez le nom du groupe de votre choix pour représenter cette connexion.
  - **PPPoE Username** (nom d'utilisateur PPPoE) : Spécifiez le nom d'utilisateur fourni par votre fournisseur de services Internet.
  - **PPPoE Password** : 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.
  - **PPPoE Learned Route Metric** (mesure de la voie de routage apprise 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.
  - **Obtain Default Route from PPPoE** (obtenir la voie de routage par défaut à partir de PPPoE) : Cochez cette case pour activer l'obtention de la voie de routage par défaut à partir du serveur PPPoE.
  - **IP Address Type (type d'adresse IP)** : Choisissez **Dynamic (dynamique)** pour obtenir l'adresse IP du serveur PPPoE. Vous pouvez également choisir **Static** (statique) si vous avez reçu une adresse IP statique du fournisseur de services Internet.

Étape 5 (Facultatif) Cliquez sur l'onglet **IPv6 Address** (adresse IPv6) et configurez l'adresse IPv6.

- **State** (état) : Pour activer le traitement IPv6 et configurer automatiquement l'adresse de liaison locale lorsque vous ne configurez pas l'adresse globale, sélectionnez **Enabled** (activé). L'adresse locale de liaison est générée en fonction des adresses MAC d'interface (format EUI-64 *modifié*).

  Remarque
  La désactivation de l'adresse IPv6 ne désactive pas le traitement IPv6 sur une interface configurée avec une adresse IPv6 explicite ou activée pour la configuration automatique.

- **Address Auto Configuration** (configuration automatique de l'adresse) : Sélectionnez cette option pour configurer l'adresse automatiquement. La configuration automatique sans état IPv6 générera une adresse IPv6 globale uniquement si le lien sur lequel le périphérique réside a un routeur configuré pour fournir des services IPv6, y compris la publicité d'un préfixe global IPv6 à utiliser sur le lien. Si les services de routage IPv6 ne sont pas disponibles sur le lien, vous obtiendrez uniquement une adresse IPv6 lien-local, à laquelle vous ne pourrez pas accéder en dehors du lien réseau immédiat de l'appareil. L'adresse locale de liaison est basée sur l'ID d'interface EUI-64 modifié.

  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 dispositif FTD envoie des messages de publicité de routeur

dans ce cas. Sélectionnez **Suppress RA** (supprimer RA) pour supprimer les messages et se conformer au RFC.

- **Static Address/Prefix** (adresse statique/préfixe) : Si vous n'utilisez pas la configuration automatique sans état, saisissez l'adresse IPv6 globale statique complète et le préfixe de réseau. Par exemple : 2001:0DB8::BA98:0:3210/48. Pour en savoir plus sur l'adressage IPv6, consultez Adresse IPv6, à la page 4.

  Si vous souhaitez utiliser l'adresse comme lien local uniquement, sélectionnez l'option **Link - Local** (lien local). Les adresses locales de liaison ne sont pas accessibles en dehors du réseau local. Vous ne pouvez pas configurer une adresse lien-local sur une interface de groupe de ponts.

  Remarque
  Une adresse de lien local doit commencer par FE8, FE9, FEA ou FEB, par exemple fe80::20d:88ff:feee:6a82. 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.

- **Standby IP Address** (adresse IP en veille) : Si vous configurez la haute disponibilité et que vous surveillez cette interface pour la haute disponibilité, configurez également une adresse IPv6 de veille sur le même sous-réseau. L'adresse en veille est utilisée par cette interface sur le périphérique de secours. 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.

- **Suppress RA** : Cette option permet de supprimer les publicités de routeur. FTD peut participer à des publicités de routeur afin que les dispositifs voisins puissent apprendre de façon dynamique une adresse de routeur par défaut. Par défaut, des messages de publicité de routeur (ICMPv6 type 134) sont envoyés périodiquement à chaque interface configurée IPv6.

  Des publicités de routeur sont également envoyées en réponse à des 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 supprimer ces messages sur toute interface dont vous ne souhaitez pas que le dispositif FTD fournisse le préfixe IPv6 (par exemple, l'interface externe).

Étape 6 (Facultatif) Configurer les options avancées, à la page 49.

Les paramètres avancés comprennent des paramètres par défaut appropriés pour la plupart des réseaux. Modifiez-les uniquement lors de la résolution des problèmes de réseau.

Étape 7 Cliquez sur **OK**.

Prochaine étape

- Ajoutez les VLAN aux zones de sécurité appropriées. Consultez Configuration des zones de sécurité.

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. Par défaut, Ethernet 1/2 à Ethernet 1/8 sont des ports de commutation activés et 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 périphérique FTD ne finit pas dans une boucle de réseau.

Avant de commencer

Ajoutez une interface VLAN pour l'ID du VLAN auquel vous souhaitez affecter le port d'accès. Les ports d'accès acceptent uniquement le trafic non balisé. Consultez Configurer une interface VLAN, à la page 28.

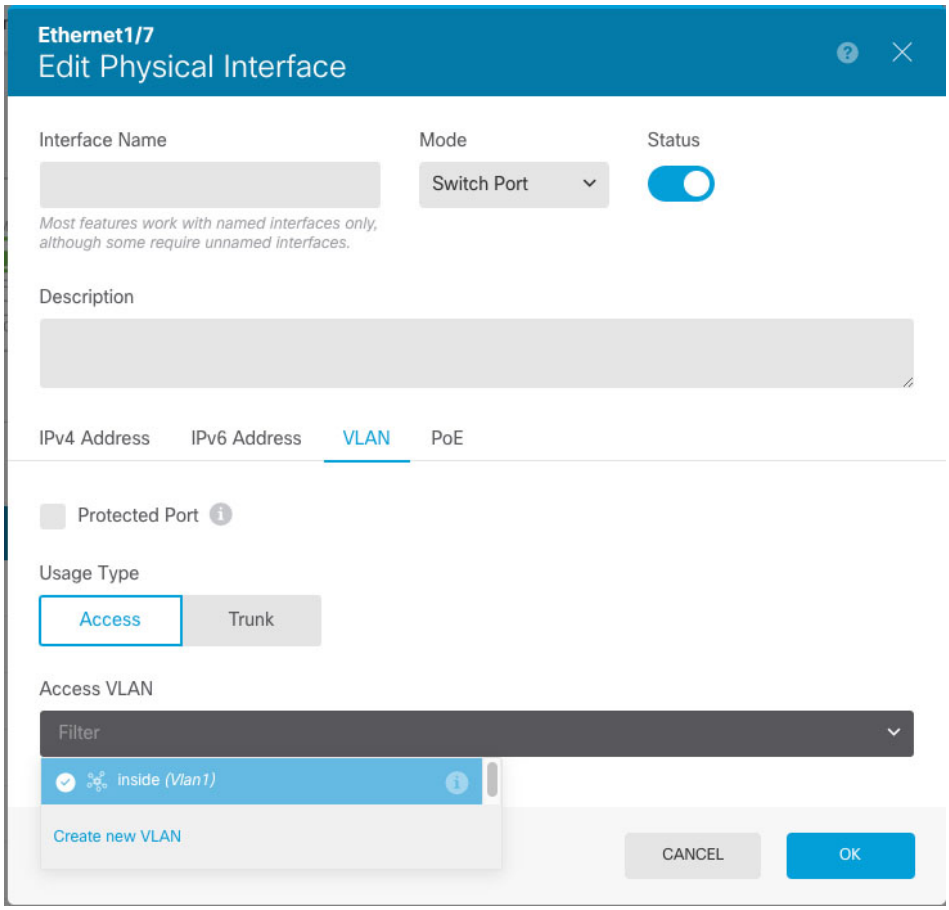
Procédure

Étape 1 Cliquez sur **Device** (dispositif), puis sur le lien dans le résumé des **Interfaces**.

La page **Interfaces** est sélectionnée par défaut. La liste des interfaces affiche les interfaces physiques : leurs noms, adresses et états.

Étape 2 Cliquez sur l'icône de modification ( ) pour l'interface physique que vous souhaitez modifier.

Étape 3 Définissez les paramètres suivants :



a) Ne définissez pas **Interface Name** (Nom d'interface) pour les ports de commutation ; seule l'interface VLAN associée est une interface nommée.

b) Définissez **Mode** sur **Switch Por**t (Port de commutation).

c) Définissez le curseur **Status** (état) selon sur le paramètre activé ( ).

d) (Facultatif) Définissez la **Description**.

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

Étape 4 Cliquez sur **VLAN** pour définir les éléments suivants :

a) (Facultatif) Cochez la case **Protected Port** (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 l'option Protected (Protégé) sur chaque port de commutation. 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.

b) Pour **Usage Type** (Type d'utilisation, cliquez sur **Access** (Accès).

c) Pour **Access VLAN** (VLAN d'accès), cliquez sur la flèche vers le bas pour choisir l'une des interfaces VLAN existantes.

Vous pouvez ajouter une nouvelle interface VLAN en cliquant sur **Create new VLAN** (Créer un nouveau VLAN). Consultez Configurer une interface VLAN, à la page 28

Étape 5 Cliquez sur **OK**.

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.

Avant de commencer

Ajoutez une interface VLAN pour chaque ID de VLAN auquel vous souhaitez affecter le port de ligne principale. Consultez Configurer une interface VLAN, à la page 28.

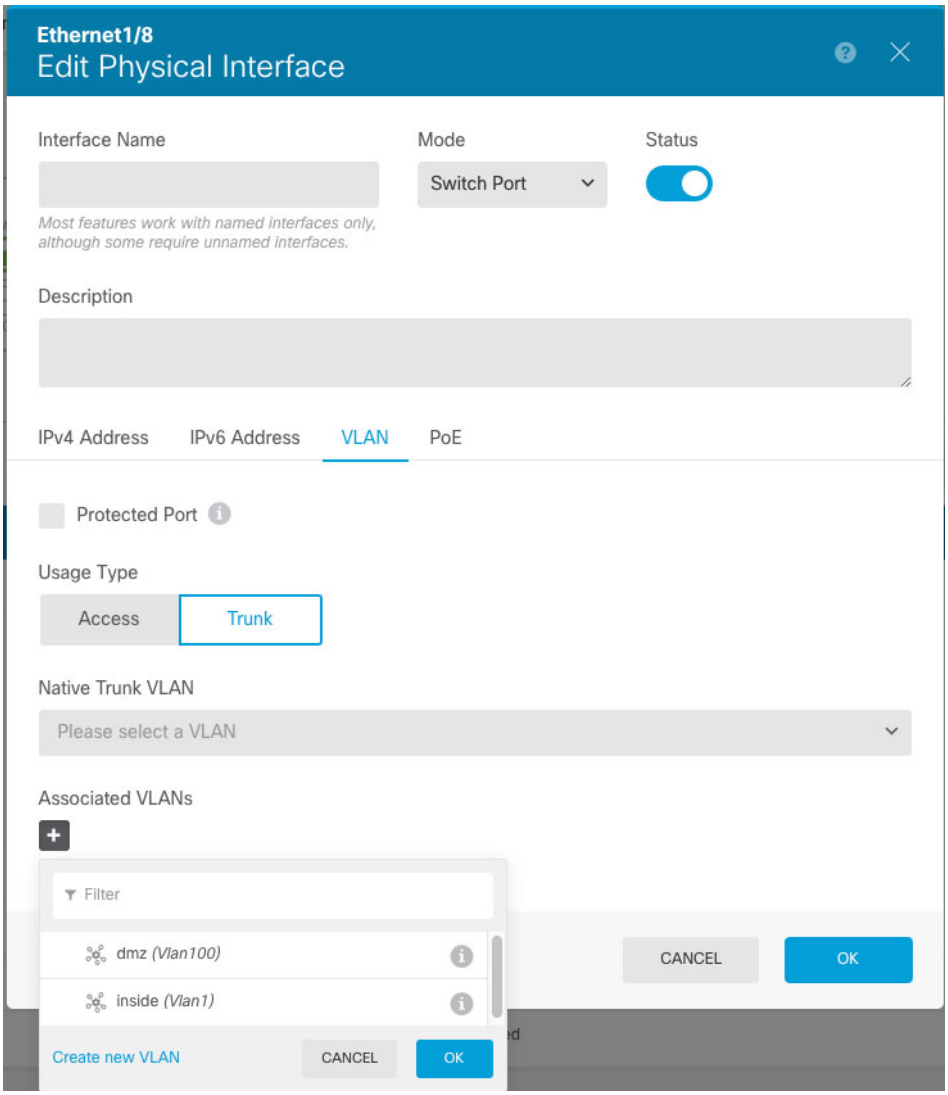
Procédure

Étape 1 Cliquez sur **Device** (dispositif), puis sur le lien dans le résumé des **Interfaces**.

La page **Interfaces** est sélectionnée par défaut. La liste des interfaces affiche les interfaces physiques : leurs noms, adresses et états.

Étape 2 Cliquez sur l'icône de modification () pour l'interface physique que vous souhaitez modifier.

Étape 3 Définissez les paramètres suivants :



a) Ne définissez pas **Interface Name** (Nom d'interface) pour les ports de commutation ; seule l'interface VLAN associée est une interface nommée.

b) Définissez le champ **Mode** sur **Switch Por**t (Port de commutation).

c) Définissez le curseur **Status** (état) selon sur le paramètre activé ( ).

d) (Facultatif) Définissez la **Description**.

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

Étape 4 Cliquez sur **VLAN** pour définir les éléments suivants :

a) (Facultatif) Cochez la case **Protected Port** (Port protégé) pour définir ce port de commutation comme protégé, afin de 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 appliquez cette option à 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.

b) Pour **Usage Type** (Type d'utilisation, cliquez sur **Trunk**.

c) (Facultatif) Pour **Native Trunk VLAN** (VLAN de tronc natif), cliquez sur la flèche vers le bas pour choisir l'une des interfaces VLAN existantes pour le VLAN natif.

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.

Vous pouvez ajouter une nouvelle interface VLAN en cliquant sur **Create new VLAN** (Créer un nouveau VLAN). Consultez Configurer une interface VLAN, à la page 28.

d) Pour **Associated VLANs** (VLAN associés), cliquez sur l'icône plus ( ) pour sélectionner une ou plusieurs interfaces VLAN existantes.

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.

Vous pouvez ajouter une nouvelle interface VLAN en cliquant sur **Create new VLAN** (Créer un nouveau VLAN). Consultez Configurer une interface VLAN, à la page 28

Étape 5 Cliquez sur **OK**.

Configurer Power Over Ethernet (alimentation électrique par câble Ethernet)

Ethernet1/7 et Ethernet1/8 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 l'interface, vous désactivez l'alimentation du périphérique.

Le PoE est activé par défaut sur Ethernet1/7 et Ethernet1/8. Cette procédure décrit comment activer et désactiver la PoE et comment définir les paramètres facultatifs.

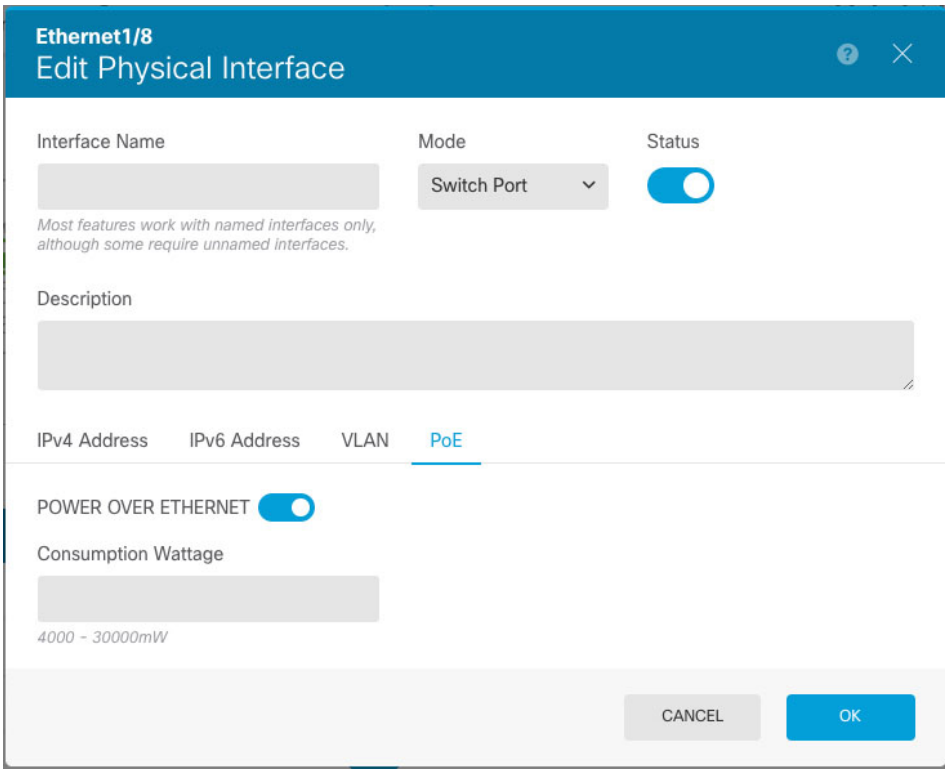
Procédure

Étape 1 Cliquez sur **Device** (dispositif), puis sur le lien dans le résumé des **Interfaces**.

La page **Interfaces** est sélectionnée par défaut. La liste des interfaces affiche les interfaces physiques : leurs noms, adresses et états.

Étape 2 Cliquez sur l'icône de modification ( ) pour Ethernet1/7 ou 1/8.

Étape 3 Cliquez sur **PoE**, et définissez les éléments suivants :



a) Pour activer **Power over Ethernet** (alimentation électrique par Ethernet), cliquez sur le curseur ( ) afin de l'activer.

   Le mode PoE est activé par défaut.

b) (Facultatif) Saisissez la **consommation en watts** si vous connaissez la puissance exacte 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 4 Cliquez sur **OK**.

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 garder 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.

Créez des sous-interfaces si vous connectez l'interface physique à un port de ligne principale sur un commutateur. Créez une sous-interface pour chaque réseau VLAN pouvant apparaître sur le port de ligne principale du commutateur. Si vous connectez l'interface physique à un port d'accès sur le commutateur, il est inutile de créer une sous-interface.

Lignes directrices et limites relatives à la licence

- 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. 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 souhaitez laisser l'interface physique passer des paquets non étiquetés, vous pouvez nommer l'interface comme d'habitude.
- Firepower 1010 : Les sous-interfaces ne sont pas prises en charge sur les ports de commutation ou les interfaces VLAN.
- Vous ne pouvez pas configurer d'adresses IP sur les interfaces de membre de groupe de passerelle, mais vous pouvez modifier les paramètres avancés au besoin.
- 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.
- FTD ne prend pas en charge le protocole DTP (Dynamic Trunking Protocol), vous devez donc configurer le port du commutateur connecté pour qu'il puisse établir une liaison sans condition.
- Vous pouvez vouloir attribuer des adresses MAC uniques aux sous-interfaces définies sur le périphérique Cisco Firepower Threat Defense, car elles utilisent la même adresse MAC gravée de l'interface parent. 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 Cisco Firepower Threat Defense.

Procédure

Étape 1 Cliquez sur **Device** (dispositif), puis sur le lien dans le résumé des **Interfaces**.

La page **Interfaces** est sélectionnée par défaut. Pour ajouter une sous-interface à un canal EtherChannel, cliquez sur **EtherChannel**. La liste des interfaces affiche les interfaces physiques : leurs noms, adresses et états.

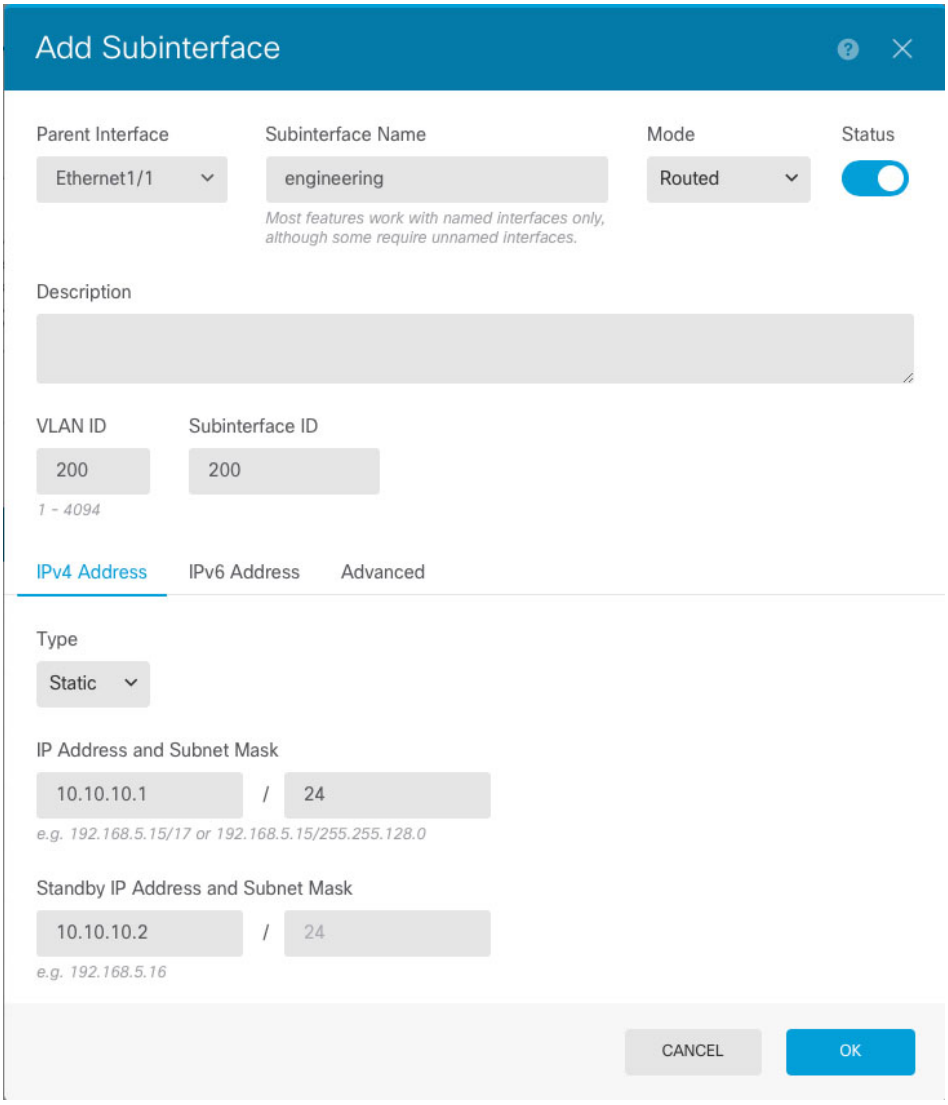
Étape 2 Effectuez l'une des opérations suivantes :

- Dans la page des **Interfaces**, cliquez sur l'icône plus ( ) pour créer une nouvelle sous-interface.
- Sur la page **EtherChannel**, cliquez sur l'icône de flèche vers le haut et vers le bas ( ), puis sélectionnez **Subinterface** (sous-interface).
- Cliquez sur l'icône de modification ( ) pour la sous-interface que vous souhaitez modifier.

Si vous n'avez plus besoin d'une sous-interface, cliquez sur l'icône de suppression ( ) pour la supprimer.

Étape 3 Définissez le curseur **Status** (état) selon sur le paramètre activé ( ).

Étape 4 Configurez l'interface parente en précisant son nom et en indiquant une description :



a) Choisissez l'interface parente **Parent Interface**.

L'interface parente est l'interface physique à laquelle vous souhaitez ajouter la sous-interface. Vous ne pouvez pas modifier l'interface parente après avoir créé la sous-interface.

b) Définissez le nom de la sous-interface (**Subinterface Name**) en utilisant au maximum 48 caractères.

Les caractères alphabétiques doivent être en minuscules. Par exemple, **inside** (interne) or **outside** (externe). Sans nom, le reste de la configuration de l'interface est ignoré.

Remarque
Si vous modifiez le nom, la modification se répercute automatiquement partout où vous avez utilisé l'ancien nom, y compris les zones de sécurité, les objets du serveur syslog et les définitions du serveur DHCP. Cependant, vous ne pouvez pas supprimer le nom avant de supprimer toutes les configurations qui utilisent le nom, car vous ne pouvez généralement pas utiliser une interface sans nom pour une politique ou un paramètre.

c) Réglez le **Mode** sur **Routed** (routé).

Si vous ajoutez ultérieurement cette interface à un groupe de ponts, le mode passera automatiquement à **BridgeGroupMember** (membre du groupe de ponts). Notez que vous ne pouvez pas configurer d'adresses IP sur les interfaces des membres de groupes de ponts.

d) (Facultatif) Définissez la **description**.

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

e) Définissez le numéro VLAN (**VLAN ID**).

Entrez le numéro du VLAN entre 1 et 4094 qui sera utilisé pour baliser les paquets sur cette sous-interface.

f) Définissez l'ID de sous-interface (**Subinterface ID**).

Entrez l'ID de la sous-interface comme un nombre entier entre 1 et 4294967295. Cet ID est ajouté à l'ID de l'interface; par exemple Ethernet 1/1.100. Vous pouvez faire correspondre le numéro VLAN pour plus de commodité, mais ce n'est pas obligatoire. Vous ne pouvez pas modifier l'ID après avoir créé la sous-interface.

Étape 5 Cliquez sur l'onglet **IPv4 Address** (adresse IPv4) et configurez l'adresse IPv4.

Sélectionnez l'une des options suivantes dans le champ **Type** :

- **DHCP** : Sélectionnez cette option si l'adresse doit être obtenue du serveur DHCP sur le réseau. Vous ne pouvez pas utiliser cette option si vous configurez la haute disponibilité. Modifiez les options suivantes si nécessaire :
  - **Route Metric** (mesure de routage) : Si vous obtenez la voie de routage par défaut du serveur DHCP, il s'agit de la distance administrative par rapport à la route apprise (entre 1 et 255). La valeur par défaut est 1.
  - **Obtain Default Route** (obtenir la voie de routage par défaut) : Cette option permet d'obtenir la voie de routage par défaut à partir du serveur DHCP. Vous devez normalement sélectionner cette option, qui est la valeur par défaut.
- **Static** (statique) : Sélectionnez cette option si vous souhaitez affecter une adresse qui ne doit pas être modifiée. Saisissez l'adresse IP de l'interface et le masque de sous-réseau pour le réseau connecté à l'interface. Par exemple, si vous connectez le réseau 10.100.10.0/24, vous pouvez entrer 10.100.10.1/24. Assurez-vous que l'adresse n'est pas déjà utilisée sur le réseau.

  Si vous avez configuré la haute disponibilité et que vous surveillez cette interface pour la haute disponibilité, configurez également une adresse IP de veille sur le même sous-réseau. L'adresse en veille est utilisée par cette interface sur le périphérique de secours. 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.

  Remarque
  Si un serveur DHCP est configuré pour l'interface, la configuration s'affiche. Vous pouvez modifier ou supprimer l'ensemble d'adresses DHCP. Si vous modifiez l'adresse IP de l'interface pour un sous-réseau différent, vous devez soit supprimer le serveur DHCP, soit configurer un ensemble d'adresses sur le nouveau sous-réseau, avant de pouvoir enregistrer les modifications de l'interface. Consultez Configuration du serveur DHCP.
- **PPPoE** : Sélectionnez cette option si l'adresse doit être obtenue à l'aide du protocole PPPoE (Point-to-point Protocol over Ethernet). PPPoE peut être nécessaire si l'interface est connectée à un modem DSL, un

modem câble ou une autre connexion à votre fournisseur de services Internet et que votre fournisseur de services Internet utilise PPPoE pour fournir votre adresse IP. Vous ne pouvez pas utiliser cette option si vous configurez la haute disponibilité. Définissez les paramètres suivants :

- **Group Name** (nom du groupe) : Spécifiez le nom du groupe de votre choix pour représenter cette connexion.
- **PPPoE Username** (nom d'utilisateur PPPoE) : Spécifiez le nom d'utilisateur fourni par votre fournisseur de services Internet.
- **PPPoE Password** : 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.
- **PPPoE Learned Route Metric** (mesure de la voie de routage apprise 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.
- **Obtain Default Route from PPPoE** (obtenir la voie de routage par défaut à partir de PPPoE) : Cochez cette case pour activer l'obtention de la voie de routage par défaut à partir du serveur PPPoE.
- **IP Address Type (type d'adresse IP)** : Choisissez **Dynamic (dynamique)** pour obtenir l'adresse IP du serveur PPPoE. Vous pouvez également choisir **Static** (statique) si vous avez reçu une adresse IP statique du fournisseur de services Internet.

Étape 6 (Facultatif) Cliquez sur l'onglet **IPv6 Address** (adresse IPv6) et configurez l'adresse IPv6.

- **State** (état) : Pour activer le traitement IPv6 et configurer automatiquement l'adresse de liaison locale lorsque vous ne configurez pas l'adresse globale, sélectionnez **Enabled** (activé). L'adresse locale de liaison est générée en fonction des adresses MAC d'interface (format EUI-64 *modifié*).

  Remarque
  La désactivation de l'adresse IPv6 ne désactive pas le traitement IPv6 sur une interface configurée avec une adresse IPv6 explicite ou activée pour la configuration automatique.

- **Address Auto Configuration** (configuration automatique de l'adresse) : Sélectionnez cette option pour configurer l'adresse automatiquement. La configuration automatique sans état IPv6 générera une adresse IPv6 globale uniquement si le lien sur lequel le périphérique réside a un routeur configuré pour fournir des services IPv6, y compris la publicité d'un préfixe global IPv6 à utiliser sur le lien. Si les services de routage IPv6 ne sont pas disponibles sur le lien, vous obtiendrez uniquement une adresse IPv6 lien-local, à laquelle vous ne pourrez pas accéder en dehors du lien réseau immédiat de l'appareil. L'adresse locale de liaison est basée sur l'ID d'interface EUI-64 modifié.

  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 dispositif FTD envoie des messages de publicité de routeur dans ce cas. Sélectionnez **Suppress RA** (supprimer RA) pour supprimer les messages et se conformer au RFC.

- **Static Address/Prefix** (adresse statique/préfixe) : Si vous n'utilisez pas la configuration automatique sans état, saisissez l'adresse IPv6 globale statique complète et le préfixe de réseau. Par exemple : 2001:0DB8::BA98:0:3210/48. Pour en savoir plus sur l'adressage IPv6, consultez Adresse IPv6, à la page 4.

  Si vous souhaitez utiliser l'adresse comme lien local uniquement, sélectionnez l'option **Link - Local** (lien local). Les adresses locales de liaison ne sont pas accessibles en dehors du réseau local. Vous ne pouvez pas configurer une adresse lien-local sur une interface de groupe de ponts.

  Remarque
  Une adresse de lien local doit commencer par FE8, FE9, FEA ou FEB, par exemple fe80::20d:88ff:feee:6a82. 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.

- **Standby IP Address** (adresse IP en veille) : Si vous configurez la haute disponibilité et que vous surveillez cette interface pour la haute disponibilité, configurez également une adresse IPv6 de veille sur le même sous-réseau. L'adresse en veille est utilisée par cette interface sur le périphérique de secours. 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.

- **Suppress RA** : Cette option permet de supprimer les publicités de routeur. FTD peut participer à des publicités de routeur afin que les dispositifs voisins puissent apprendre de façon dynamique une adresse de routeur par défaut. Par défaut, des messages de publicité de routeur (ICMPv6 type 134) sont envoyés périodiquement à chaque interface configurée IPv6.

  Des publicités de routeur sont également envoyées en réponse à des 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 supprimer ces messages sur toute interface dont vous ne souhaitez pas que le dispositif FTD fournisse le préfixe IPv6 (par exemple, l'interface externe).

Étape 7 (Facultatif) Configurer les options avancées, à la page 49.

Les paramètres avancés comprennent des paramètres par défaut appropriés pour la plupart des réseaux. Modifiez-les uniquement lors de la résolution des problèmes de réseau.

Étape 8 Cliquez sur **OK**.

Prochaine étape

- Ajoutez les sous-interfaces aux zones de sécurité appropriées. Consultez Configuration des zones de sécurité.
- Enregistrez un nom de domaine complet (FQDN) auprès de votre fournisseur de service DNS dynamique et configurez DDNS pour que le serveur DNS soit mis à jour avec les adresses d'interface pour IPv4 et IPv6. Consultez Configuration du DNS dynamique.

Configurer les interfaces passives

Les interfaces passives surveillent le trafic circulant sur un réseau à l'aide d'un commutateur SPAN ou d'un port miroir. Le port SPAN ou miroir permet de copier le trafic d'autres ports du commutateur. Cette fonction assure la visibilité du système dans le réseau sans être dans le flux du trafic réseau.

Lorsqu'il est configuré dans un déploiement passif, le système ne peut pas prendre certaines mesures telles que le blocage du trafic. Les interfaces passives reçoivent tout le trafic sans condition et aucun trafic reçu sur ces interfaces n'est retransmis.

Vous utilisez une interface passive pour surveiller le trafic sur le réseau afin de recueillir des informations sur le trafic. Par exemple, vous pouvez appliquer des politiques de prévention des intrusions pour identifier les types de menaces qui affectent le réseau ou pour voir les catégories d'URL pour les demandes Web des utilisateurs. Vous pouvez mettre en œuvre diverses politiques et règles de sécurité pour voir ce que ferait le système s'il était déployé activement, afin qu'il puisse abandonner le trafic en fonction de votre contrôle d'accès et d'autres règles.

Cependant, comme les interfaces passives ne peuvent pas avoir d'incidence sur le trafic, il existe de nombreuses limites de configuration. Ces interfaces laissent simplement le système surveiller le trafic : aucun paquet qui entre dans une interface passive ne quitte le périphérique.

Les rubriques suivantes expliquent plus en détail les interfaces passives et comment les configurer.

Interfaces passives

L'objectif principal des interfaces passives est de fournir un mode de démonstration simple. Vous pouvez configurer le commutateur pour surveiller un seul port source, puis utiliser un poste de travail pour envoyer le trafic de test surveillé par l'interface passive. Ainsi, vous pouvez voir comment le système Cisco Firepower Threat Defense évalue les connexions, identifie les menaces, etc. Une fois que vous êtes satisfait des performances du système, vous pouvez le déployer activement dans votre réseau et supprimer la configuration d'interface passive.

Cependant, vous pouvez également utiliser des interfaces passives dans un environnement de production pour fournir les services suivants :

- Déploiement d'IDS pur : si vous ne souhaitez pas utiliser le système comme pare-feu ou IPS (système de prévention des intrusions), vous pouvez le déployer de manière passive en tant que IDS (système de détection d'intrusion) . Dans cette méthode de déploiement, vous utiliseriez une règle de contrôle d'accès pour appliquer une politique de prévention des intrusions à tout le trafic. Le système surveillerait également plusieurs ports sources sur le commutateur. Ensuite, vous pourrez utiliser les tableaux de bord pour surveiller les menaces vues sur le réseau. Cependant, dans ce mode, le système ne peut rien faire pour empêcher ces menaces.
- Déploiement mixte : vous pouvez combiner des interfaces routées actives avec des interfaces passives sur le même système. Ainsi, vous pouvez déployer le périphérique Cisco Firepower Threat Defense en tant que pare-feu dans certains réseaux, tout en configurant une ou plusieurs interfaces passives pour surveiller le trafic dans d'autres réseaux.

Limites pour les interfaces passives

Toute interface physique que vous définissez comme interface en mode passif a les restrictions suivantes :

- Vous ne pouvez pas configurer de sous-interfaces sur l'interface passive.
- Vous ne pouvez pas ajouter une interface en mode passif à un groupe de pont.
- Vous ne pouvez pas configurer les adresses IPv4 ou IPv6 sur une interface passive.
- Vous ne pouvez pas sélectionner l'option Management Only (Gestion uniquement) pour une interface passive.
- Vous pouvez inclure l'interface dans une zone de sécurité en mode passif uniquement, vous ne pouvez pas l'inclure dans une zone de sécurité routée.
- Vous pouvez inclure des zones de sécurité passive dans les critères de source des règles de contrôle d'accès ou d'identité. Vous ne pouvez pas utiliser de zones passives dans les critères de destination. Vous ne pouvez pas combiner des zones de sécurité passives et routées dans une seule règle.
- Vous ne pouvez pas configurer de règles d'accès de gestion (HTTPS ou SSH) pour une interface passive.
- Vous ne pouvez pas utiliser une interface en mode passif dans les règles NAT.
- Vous ne pouvez pas configurer de routes statiques pour une interface passive. Vous ne pouvez pas non plus utiliser une interface passive dans la configuration d'un protocole de routage.
- Vous ne pouvez pas configurer un serveur DHCP sur une interface en mode passif. Vous ne pouvez pas non plus utiliser une interface passive pour obtenir des paramètres DHCP par le biais de la configuration automatique.
- Vous ne pouvez pas utiliser une interface passive dans une configuration de serveur syslog.
- Vous ne pouvez pas configurer de type de VPN sur une interface passive.

Configurer le commutateur pour une interface matérielle FTD passive

Une interface passive sur du matériel Cisco Firepower Threat Defense ne fonctionne que si vous configurez correctement le commutateur de réseau. La procédure suivante est basée sur un commutateur de la gamme Cisco Nexus 5000. Si vous avez un autre type de commutateur, les commandes pourraient différer.

L'idée de base consiste à configurer un port SPAN (Switched Port Analyzer) ou miroir, à connecter l'interface passive à ce port et à configurer une session de surveillance sur le commutateur pour envoyer des copies du trafic d'un ou de plusieurs ports sources au port SPAN ou miroir.

Procédure

Étape 1 Configurez un port du commutateur comme port de surveillance (SPAN ou miroir).

```
switch(config)# interface Ethernet1/48
switch(config-if)# switchport monitor
switch(config-if)#
```

Étape 2 Définissez une session de surveillance pour définir les ports à surveiller.

Assurez-vous de définir le port SPAN ou miroir comme port de destination. Dans l'exemple suivant, deux ports source sont surveillés.

```
switch(config)# monitor session 1
switch(config-monitor)# source interface ethernet 1/7
switch(config-monitor)# source interface ethernet 1/8
switch(config-monitor)# destination interface ethernet 1/48
switch(config-monitor)# no shut
```

Étape 3 (Facultatif) Vérifiez la configuration à l'aide de la commande **show monitor session**.

L'exemple suivant présente la sortie brève pour la session 1.

```
switch# show monitor session 1 brief
   session 1
---------------
type              : local
state             : up
source intf       :
    rx            : Eth1/7        Eth1/8
    tx            : Eth1/7        Eth1/8
    both          : Eth1/7        Eth1/8
source VSANs      :
destination ports : Eth1/48

Legend: f = forwarding enabled, l = learning enabled
```

Étape 4 Connectez physiquement le câble de l'interface passive Cisco Firepower Threat Defense au port de destination du commutateur.

Vous pouvez configurer l'interface en mode passif avant ou après la connexion physique. Consultez Configurer l'interface physique en mode passif, à la page 46.

Configurer le VLAN pour une interface passive FTDv

Une interface passive sur un périphérique FTDv ne fonctionne que si vous configurez correctement le réseau VLAN sur le réseau virtuel. Assurez-vous de procéder comme suit :

- Connectez l'interface FTDv à un réseau VLAN que vous avez configuré en mode promiscuité. Ensuite, configurez l'interface comme expliqué dans Configurer l'interface physique en mode passif, à la page 46. L'interface passive verra une copie de tout le trafic sur le VLAN en mode promiscuité.
- Sur le même réseau VLAN, connectez un ou plusieurs périphériques d'extrémité, tels que des systèmes Windows virtuels. Vous pouvez utiliser un seul périphérique s'il y a une connexion du VLAN à Internet. Sinon, vous avez besoin d'au moins deux appareils pour transmettre le trafic entre eux. Pour obtenir des données pour les catégories d'URL, vous devez avoir une connexion Internet.

Configurer l'interface physique en mode passif

Vous pouvez configurer une interface en mode passif. Lorsqu'elle agit de manière passive, l'interface surveille simplement le trafic provenant des ports source dans le cadre d'une session de surveillance configurée sur le commutateur lui-même (pour les périphériques matériels) ou sur le réseau VLAN en mode promiscuité (pour FTDv). Pour obtenir des informations détaillées sur ce que vous devez configurer dans le commutateur ou le réseau virtuel, consultez les rubriques suivantes :

- Configurer le commutateur pour une interface matérielle FTD passive, à la page 45
- Configurer le VLAN pour une interface passive FTDv, à la page 46

Utilisez le mode passif lorsque vous souhaitez analyser le trafic entrant par les ports de commutation surveillés sans impact sur le trafic. Pour un exemple de bout en bout d'utilisation du mode passif, consultez Comment surveiller passivement le trafic sur un réseau.

Procédure

Étape 1 Cliquez sur **Device** (périphérique), puis sur le lien dans le résumé des **interfaces**. Cliquez ensuite sur **Interfaces** ou **EtherChannels**.

Étape 2 Cliquez sur l'icône de modification ( ) pour l'interface physique ou le port EtherChannel que vous souhaitez modifier.

Choisissez une interface actuellement inutilisée. Si vous avez l'intention de convertir une interface en cours d'utilisation en interface passive, vous devez d'abord supprimer l'interface de toute zone de sécurité et supprimer toutes les autres configurations qui utilisent l'interface.

Étape 3 Définissez le curseur **Status** (état) selon sur le paramètre activé ( ).

Étape 4 Configurez les éléments suivants :

- **Interface Name** : le nom de l'interface (jusqu'à 48 caractères). Les caractères alphabétiques doivent être en minuscules. Par exemple, surveiller.
- **Mode** : Sélectionnez **Passive** (passif).
- (Facultatif) **Description** : La description peut contenir jusqu'à 200 caractères sur une seule ligne (sans retour chariot).

Remarque
Vous ne pouvez pas configurer les adresses IPv4 ou IPv6. Sous l'onglet des paramètres avancés, vous pouvez modifier uniquement les paramètres MTU, duplex et de vitesse.

Étape 5 Cliquez sur **OK**.

Prochaine étape

La création d'une interface passive n'est pas suffisante pour remplir les tableaux de bord avec les informations sur le trafic vu sur l'interface. Vous devez également procéder comme précisé ci-après. Le scénarios d'utilisation traitent de ces étapes. Consultez Comment surveiller passivement le trafic sur un réseau.

- Créez une zone de sécurité passive et ajoutez-y l'interface. Consultez Configuration des zones de sécurité.
- Créez des règles de contrôle d'accès qui utilisent la zone de sécurité passive comme zone source. En règle générale, vous devez appliquer des politiques d'intrusion dans ces règles pour mettre en œuvre la surveillance IDS (système de détection d'intrusion). Consultez Configuration de la politique de contrôle d'accès.

- Vous pouvez également créer des règles d'identité et de déchiffrement SSL pour la zone de sécurité passive et activer la politique de renseignement de sécurité.

Configurer les options d'interface avancées

Les options avancées comprennent la définition de l'unité de transfert maximale (MTU), des paramètres matériels, du mode gestion uniquement, de l'adresse MAC et d'autres paramètres.

À propos des adresses MAC

Vous pouvez configurer manuellement des adresses Media Access Control (MAC) afin de remplacer la valeur par défaut.

Pour une configuration de haute disponibilité, vous pouvez configurer, pour une interface, l'adresse MAC active et l'adresse MAC de secours. 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.

Adresses MAC par défaut

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

- Interfaces physiques : l'interface physique utilise l'adresse MAC gravée.
- (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 les options avancées, à la page 49.
- EtherChannels: 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.
- Sous-interfaces : toutes les sous-interfaces d'une interface physique utilisent la même adresse MAC gravée. Vous pourriez souhaiter affecter des adresses MAC uniques aux sous-interfaces. Par exemple, votre fournisseur de services peut effectuer un contrôle d'accès en fonction de l'adresse MAC. En outre, étant donné que les adresses locales de lien IPv6 sont générées en fonction de l'adresse MAC, l'affectation d'adresses MAC uniques aux sous-interfaces permet d'établir des adresses locales de lien IPv6 uniques, ce qui peut éviter des perturbations de trafic dans certaines instances sur FTD.

À propos de la MTU

La MTU spécifie la taille maximale de la *charge utile* de trame que l' appareil FTD 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.

Chemin de découverte de MTU

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

Remarque L' appareil FTD 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 FTD et les autres interfaces de périphériques le long du chemin de trafic. La correspondance des MTU empêche les périphériques intermédiaires de fragmenter les paquets.
- Une trame étendue est un paquet Ethernet supérieur au maximum standard de 1518 octets (y compris l'en-tête de couche 2 et l'en-tête VLAN) qui peut s'élever jusqu'à 9216 octets. Vous pouvez définir la MTU à 9 000 octets ou plus pour la prise en charge des trames étendues. Le maximum dépend du modèle.

Remarque L'augmentation de la MTU affecte plus de mémoire aux trames étendues, ce qui peut limiter l'utilisation maximale d'autres fonctions, telles que les règles d'accès. Si vous augmentez le MTU au-delà de 1500 sur des périphériques de la série ISA 3000, , vous devez redémarrer le périphérique. Si le périphérique est configuré pour la haute disponibilité, vous devez également redémarrer le périphérique en veille. Vous n'avez pas besoin de redémarrer les autres modèles, où la prise en charge des trames étendues est toujours activée.

Configurer les options avancées

Les options d'interface avancées ont des paramètres par défaut adaptés à la plupart des réseaux. Ne les configurez que si vous résolvez des problèmes de réseau ou si vous configurez la haute disponibilité.

La procédure suivante suppose que l'interface est déjà définie. Vous pouvez également modifier ces paramètres lors de la modification ou de la création de l'interface.

Restrictions

- Pour les groupes de ponts, vous configurez la plupart de ces options sur les interfaces membres. À l'exception des tentatives DAD et de l'option Enable for HA Monitoring (activer pour), ces options ne sont pas disponibles pour l'interface virtuelle de pont (BVI).
- Vous ne pouvez pas définir le MTU, les conditions de duplex ou la vitesse pour l'interface.
- Les options avancées ne sont pas disponibles pour les ports de commutateur Firepower 1010.
- Vous ne pouvez pas définir les conditions de duplex ou la vitesse pour les interfaces sur le Firepower 4100/9300. Définissez ces fonctionnalités pour l'interface avec FXOS.
- Pour les interfaces passives, vous pouvez définir uniquement la MTU, le duplex et la vitesse. Vous ne pouvez pas effectuer uniquement la gestion de l'interface.

Procédure

Étape 1 Cliquez sur **Device** (périphérique), cliquez sur le lien dans le résumé des **Interfaces**. Cliquez ensuite sur le type d'interfaces pour consulter la liste des interfaces.

Étape 2 Cliquez sur l'icône de modification ( ) pour l'interface que vous souhaitez modifier.

Étape 3 Cliquez sur **Advanced Options** (options avancées).

Étape 4 Sélectionnez **Enable for HA Monitoring** (activer pour la surveillance haute disponibilité) si vous souhaitez que l'intégrité de l'interface soit prise en compte lorsque le système décide de basculer vers l'unité homologue dans une configuration à haute disponibilité.

Cette option est ignorée si vous ne configurez pas la haute accessibilité. Elle est également ignorée si vous ne configurez pas de nom pour l'interface.

Étape 5 Pour assurez la gestion de l'interface de données uniquement, sélectionnez **Management Only** (gestion uniquement).

Une interface de gestion uniquement ne permet pas le trafic traversant, il est donc très peu utile de définir une interface de données pour la gestion uniquement. Vous ne pouvez pas modifier ce paramètre pour l'interface de gestion/diagnostic, qui se destine toujours à la gestion uniquement.

Étape 6 Modifiez la **MTU** (unité de transmission maximale) à la valeur souhaitée.

Par défaut, la MTU est de 1500 octets. Le minimum et le maximum dépendent de votre plateforme. Définissez une valeur élevée si vous voyez généralement des trames étendues sur votre réseau.

Remarque
Si vous augmentez le MTU au-delà de 1500 sur les périphériques suivants, vous devez redémarrer le périphérique : Périphériques de la série ISA 3000,FTDv. Si le périphérique est configuré pour la haute disponibilité, vous devez également redémarrer le périphérique en veille. Vous n'avez pas besoin de redémarrer les autres modèles, où la prise en charge des trames étendues est toujours activée.

Étape 7 (Interface physique uniquement.) Modifiez les paramètres de vitesse et de duplex.

Par défaut, l'interface négocie le meilleur duplex et la meilleure vitesse avec l'interface à l'autre extrémité du câble, mais vous pouvez forcer un duplex ou une vitesse spécifique si nécessaire. Les options répertoriées sont uniquement celles prises en charge par l'interface. Avant de définir ces options pour les interfaces sur un module de réseau, veuillez lire Limites de la configuration de l'interface, à la page 5.

- **Conditions de duplex**— Choisissez **Half (demi)** ou **Full (complet)**. Les interfaces SFP prennent uniquement en charge les conditions de duplex **full (complètes)**.
- **Speed**(vitesse) : les options exactes dépendent du modèle et du type d'interface. Choisissez une vitesse, **Auto**, **No Negotiate** ou **Detect SFP**. Pour les ports de fibre optique Firepower 1100 ou 2100, **No Negotiate** (Sans négociation) définit la vitesse à 1000 Mbit/s et désactive la négociation de liaison pour les paramètres de contrôle de flux et les informations sur les défaillances à distance. (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.
- (Secure Firewall uniquement) **Négociation automatique** : Selon le type d'interface, régler l'interface pour négocier l'état de la liaison pour les paramètres de contrôle de flux et les informations sur les défaillances à distance.
- **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 74FC-FEC	Article 108 RS-FEC
25G-LR	Article 74FC-FEC	Article 108 RS-FEC
10/25G-CSR	Article 74FC-FEC	Article 74 FC-FEC
25G-AOC*x*M	Article 74 FC-FEC	Article 74 FC-FEC
25G-CU2.5/3M	Négociation automatique	Négociation automatique
25G-CU4/5M	Négociation automatique	Négociation automatique

Étape 8 Modifiez les paramètres **IPv6 Configuration**.

- **Enable DHCP for IPv6 address configuration** (activer DHCP pour la configuration d'adresse IPv6) : Pour définir l'indicateur de configuration d'adresse gérée dans le paquet de publication de routeur IPv6. Cet indicateur 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.
- **Enable DHCP for IPv6 non-address configuration** (activer DHCP pour la configuration sans adresse IPv6) : Pour définir l'indicateur de configuration d'adresse autre dans le paquet de publication de routeur IPv6. Cet indicateur 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.
- **DAD Attempts** (tentatives de DAD) : La fréquence à laquelle l'interface effectue la détection d'adresses en double (DAD) est de 0 à 600. La valeur par défaut est 1. Pendant le processus d'autoconfiguration sans état, DAD vérifie le caractère unique des nouvelles adresses IPv6 monodiffusion avant que les adresses ne soient affectées aux interfaces. 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. L'interface utilise des messages de sollicitation de voisin pour effectuer la détection des adresses en double. Définissez la valeur sur 0 pour désactiver le traitement de la détection d'adresses en double (DAD).

Étape 9 (Facultatif, recommandé pour les sous-interfaces et les unités à haute accessibilité.) Configurez l'adresse MAC

Par défaut, le système utilise l'adresse MAC gravée dans la carte d'interface réseau (NIC) pour l'interface. Ainsi, toutes les sous-interfaces d'une interface utilisent la même adresse MAC. Vous pouvez donc créer des adresses uniques par sous-interface. Des adresses MAC actives/en attente configurées manuellement sont également recommandées si vous configurez la haute accessibilité. La définition des adresses MAC permet de maintenir la cohérence du réseau en cas de basculement.

- **MAC Address** : Le contrôle d'accès au support est au format H.H.H., où H est une valeur hexadécimale de 16 bits. Par exemple, vous devez entrer l'adresse MAC 00-0C-F1-42-4C-DE comme 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.
- **Standby MAC Address** (adresse MAC en veille) : 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 10 Cliquez sur **OK**.

Analyser les modifications d'interface et migrer une interface

Lorsque vous modifiez des interfaces sur le périphérique, le périphérique informe le FDM qu'une modification a eu lieu. Vous ne pourrez pas déployer votre configuration avant d'avoir effectué une analyse d'interface. Le FDM prend en charge la migration d'une interface de votre politique de sécurité vers une autre interface, donc la suppression d'une interface peut être presque transparente.

À propos de l'analyse et de la migration des interfaces

Analyse en cours :

Lorsque vous modifiez des interfaces sur le périphérique, le périphérique informe le FDM qu'une modification a eu lieu. Vous ne pourrez pas déployer votre configuration avant d'avoir effectué une analyse d'interface. Après une analyse, qui détecte toutes les interfaces ajoutées, supprimées ou restaurées, vous pouvez déployer votre configuration; cependant, les parties de la configuration qui font référence à des interfaces supprimées ne seront pas déployées.

Les modifications d'interfaces qui nécessitent une analyse comprennent l'ajout ou la suppression d'interfaces. Par exemple : changement de module réseau ; changement de l'interface allouée sur le châssis Firepower 4100/9300 ; changement d'interface sur le FTDv.

Les modifications suivantes ne bloquent pas le déploiement après une analyse :

- Appartenance à une zone de sécurité

- Appartenance à une interface EtherChannel
- Appartenance au port de commutation de l'interface VLAN Firepower 1010
- Appartenance à une interface de groupe de ponts, pour les politiques qui font référence aux BVI

Remarque Une modification de l'interface de sortie du serveur syslog ne bloquera pas le déploiement, bien que vous deviez corriger la configuration du serveur syslog, manuellement ou à l'aide de la fonction de remplacement d'interface.

Migration en cours

L'ajout d'une nouvelle interface ou la suppression d'une interface inutilisée a une incidence minime sur la configuration Cisco Firepower Threat Defense. Cependant, la suppression d'une interface utilisée dans votre politique de sécurité aura une incidence sur la configuration. Les interfaces peuvent être référencées directement à de nombreux endroits dans la configuration Cisco Firepower Threat Defense, notamment les zones de sécurité, la NAT, le VPN, le serveur DHCP, etc.

FDM prend en charge la migration d'une interface de votre politique de sécurité vers une autre interface, afin que la suppression d'une interface puisse être presque transparente.

Remarque La fonctionnalité de migration ne copie *pas* le nom, l'adresse IP et les autres paramètres de configuration d'une interface à une autre ; au lieu de cela, cette fonctionnalité modifie la politique de sécurité pour faire référence à la nouvelle interface plutôt qu'à l'ancienne interface. Vous devez configurer manuellement les nouveaux paramètres d'interface avant la migration.

Si vous devez supprimer une interface, nous vous recommandons d'ajouter la nouvelle interface et de migrer l'ancienne interface *avant* de la supprimer. Si vous ajoutez et supprimez des interfaces en même temps, le processus de migration fonctionnera toujours ; cependant, vous ne pouvez pas modifier *manuellement* les interfaces supprimées ni les politiques qui y font référence, de sorte qu'il peut être plus simple d'effectuer la migration par étapes.

Si vous remplacez une interface par une interface du même type (par exemple, vous devez effectuer une RMA sur un module réseau), vous pouvez procéder comme suit : 1. Retirez l'ancien module du châssis ; 2. Effectuez une analyse ; 3. Déployez les modifications sans rapport avec les interfaces supprimées ; 4. Remplacez le module ; 5. Effectuez une nouvelle analyse ; 6. Déployez votre configuration, y compris toutes les modifications liées aux interfaces. Vous n'avez pas besoin d'effectuer une migration si la nouvelle interface a le même identifiant d'interface et les mêmes caractéristiques que l'ancienne interface.

Lignes directrices et limites pour l'analyse et la migration d'interfaces

Migrations d'interface non prises en charge

- Interface physique vers BVI
- Interface passive vers l'interface de pare-feu
- Membres du groupe de pont
- Membres de l'interface EtherChannel

- Membres du contournement matériel ISA 3000
- Interfaces ou ports de commutation VLAN Firepower 1010
- Interface de diagnostic
- Basculement et liens d'état HA
- Migration d'interfaces de différents types, par exemple la migration d'une interface de groupe de ponts vers une fonctionnalité nécessitant une interface physique

Directives supplémentaires

- Si vous devez supprimer une interface, nous vous recommandons d'ajouter la nouvelle interface et de migrer l'ancienne interface *avant* de la supprimer.
- Pour FTDv, ajoutez et supprimez des interfaces uniquement à la fin de la liste des interfaces. Si vous ajoutez ou supprimez une interface ailleurs, l'hyperviseur renumérotera vos interfaces, de sorte que les ID d'interface dans votre configuration s'alignent sur les mauvaises interfaces.
- Si une analyse ou une migration se passe mal, restaurez les interfaces d'origine sur le châssis et réanalysez pour revenir à l'état d'origine.
- Pour les sauvegardes, veillez à créer une nouvelle sauvegarde avec les nouvelles interfaces. Une restauration avec l'ancienne configuration restaurera les informations d'interface d'origine, et vous devrez refaire l'analyse/le remplacement.
- Pour la haute disponibilité, apportez les mêmes modifications d'interface sur les deux unités avant d'effectuer l'analyse d'interface sur l'unité active. Il vous suffit d'effectuer l'analyse ou la migration sur l'unité active. Les modifications de configuration sont répliquées sur l'unité de secours.

Analyser et migrer les interfaces

Analyser les modifications d'interface dans FDM, et migrer les configurations d'interface à partir des interfaces supprimées. Si vous souhaitez uniquement migrer une configuration d'interface (et qu'aucune analyse n'est requise), ignorez les étapes de la procédure suivante relatives à l'analyse.

Remarque La fonctionnalité de migration ne copie *pas* le nom, l'adresse IP et les autres paramètres de configuration d'une interface à une autre ; au lieu de cela, cette fonctionnalité modifie la politique de sécurité pour faire référence à la nouvelle interface plutôt qu'à l'ancienne interface. Vous devez configurer manuellement les nouveaux paramètres d'interface avant la migration.

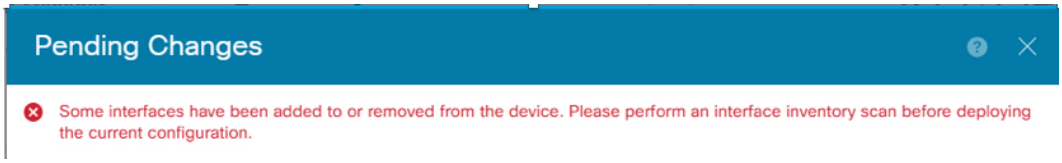
Procédure

Étape 1 Ajouter ou supprimer des interfaces sur le châssis.

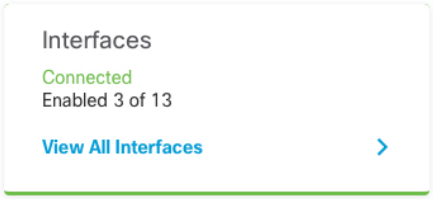
Si vous devez supprimer une interface, nous vous recommandons d'ajouter la nouvelle interface et d'effectuer un remplacement de l'ancienne interface *avant* de la supprimer.

Étape 2 Analyser les modifications d'interface.

Vous ne pourrez pas déployer votre configuration avant d'avoir effectué une analyse d'interface. Si vous essayez d'effectuer le déploiement avant une analyse, l'erreur suivante s'affiche :

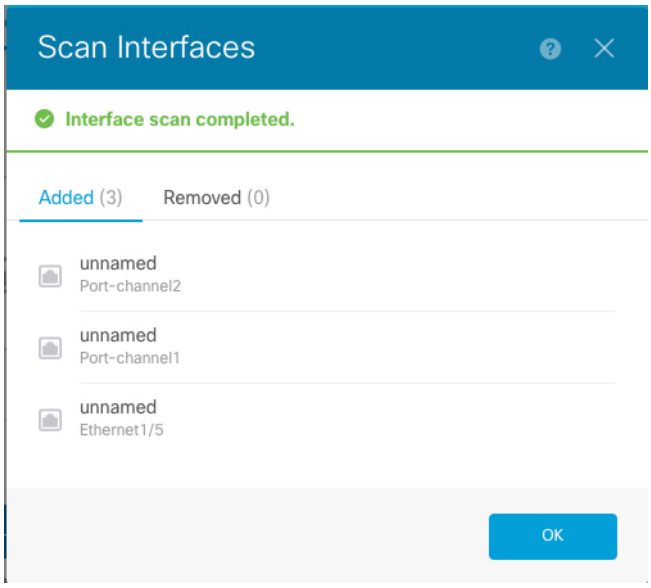


a) Cliquez sur **Device** (Périphériques), puis sur le lien **View All Interfaces** (Afficher toutes les interfaces) du résumé **Interfaces**.

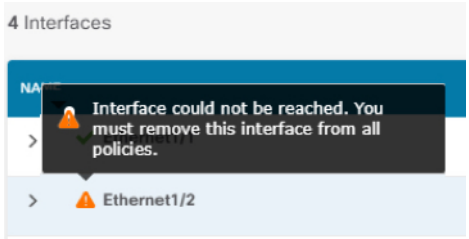


b) Cliquez sur l'icône Scan Interfaces (Analyser les interfaces) ( ).

c) Attendez que les interfaces effectuent l'analyse, puis cliquez sur **OK**.



Après l'analyse, les interfaces supprimées s'affichent sur la page Interfaces avec des symboles d'avertissement :



Étape 3 Pour migrer une interface existante vers une nouvelle interface :

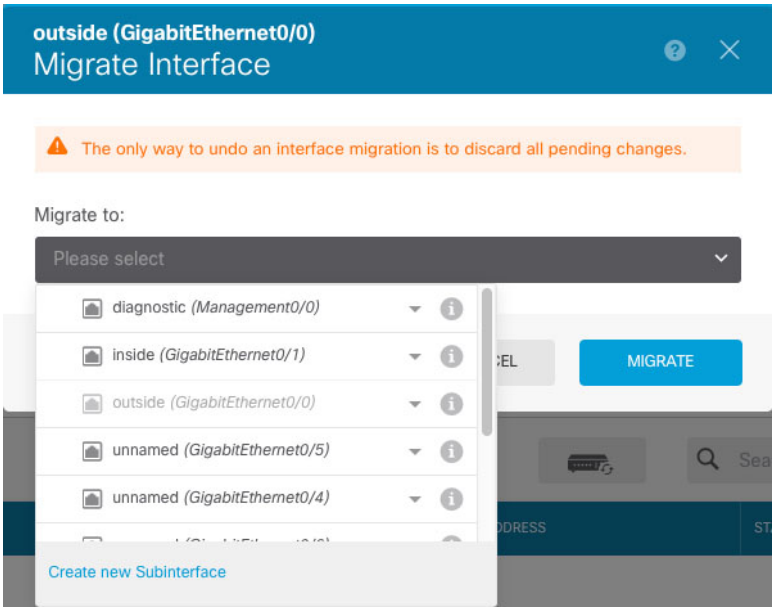
a) Configurez la nouvelle interface avec un nom, une adresse IP, etc.

Si vous souhaitez utiliser l'adresse IP existante et le nom d'une interface que vous souhaitez supprimer, vous devez reconfigurer l'ancienne interface avec un nom et une adresse IP fictifs afin de pouvoir utiliser ces paramètres sur la nouvelle interface.

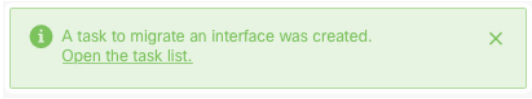
b) Cliquez sur l'icône Migrate (Migration) pour l'ancienne interface.

Ce processus remplace l'ancienne interface par la nouvelle interface dans tous les paramètres de configuration qui font référence à l'interface.

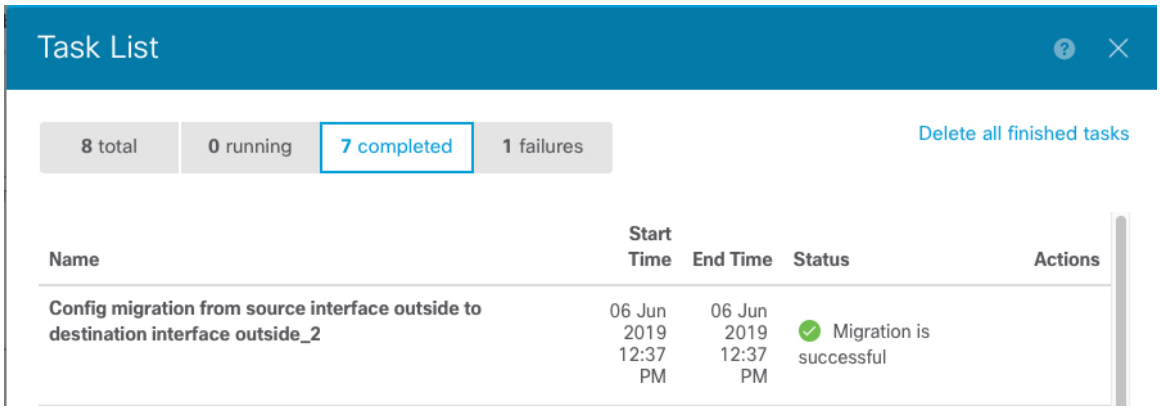
c) Choisissez la nouvelle interface dans la liste déroulante **Migrate to: (Migrer vers :)**.



d) Un message s'affiche sur la page **Interfaces**. Cliquez sur le lien dans le message.



e) Vérifiez la **liste des tâches** pour vous assurer que la migration a réussi.

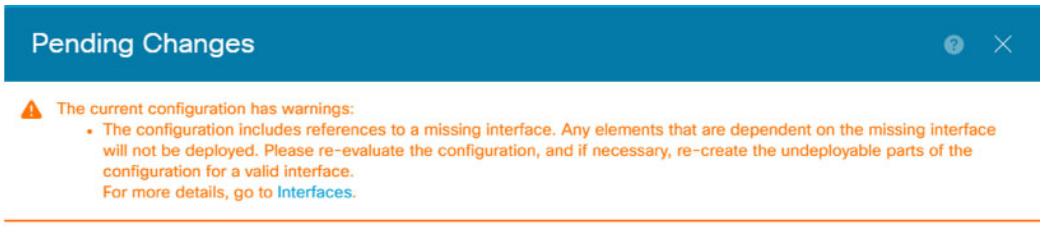


f) Si la migration échoue, vous pouvez en afficher les raisons dans API Explorer (Explorateur d'API).

Pour ouvrir l'API Explorer, cliquez sur le bouton des autres options (⋮) et choisissez **API Explorer** (Explorateur d'interface de protocole d'application). Choisissez **Interface** > **GET /jobs/interfacemigrations**, puis cliquez sur**Try it Out! (Essayez-le !)**.

Étape 4 Déployez votre configuration.

Les parties de la configuration qui font référence à des interfaces supprimées ne seront pas déployées, auquel cas vous verrez le message suivant :



Étape 5 Supprimez les anciennes interfaces du châssis, et effectuez une autre analyse.

Les interfaces supprimées qui ne sont plus utilisées dans votre politique seront supprimées de la page **Interfaces**.

Étape 6 Redéployez votre configuration pour supprimer les interfaces inutilisées de votre configuration.

Gérer le module de réseau pour Cisco Secure Firewall 3100

Si vous installez un module de réseau avant de mettre le pare-feu sous tension pour la première fois, aucune action n'est requise; le module de réseau est activé et prêt à l'emploi.

Si vous devez apporter des modifications à l'installation de votre module de réseau après le démarrage initial, consultez les procédures suivantes.

Ajouter un module de réseau

Pour ajouter un module de réseau à un pare-feu après le démarrage initial, procédez comme suit. L'ajout d'un nouveau module nécessite un redémarrage.

Procédure

Étape 1 Installez le module de réseau en suivant le guide d'installation du matériel.

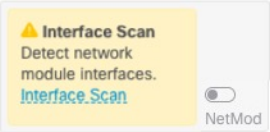
Pour la haute disponibilité, installez le module réseau sur les deux unités.

Étape 2 Redémarrez le pare-feu; voir Redémarrage ou arrêt du système. Pour la haute disponibilité, redémarrez l'unité en veille, puis effectuez le reste de cette procédure sur l'unité en veille.

Étape 3 Cliquez sur **Device** (Périphériques), puis sur le lien **View All Interfaces** (Afficher toutes les interfaces) du résume **Interfaces**.

Le graphique montre qu'une analyse d'interface est requise.

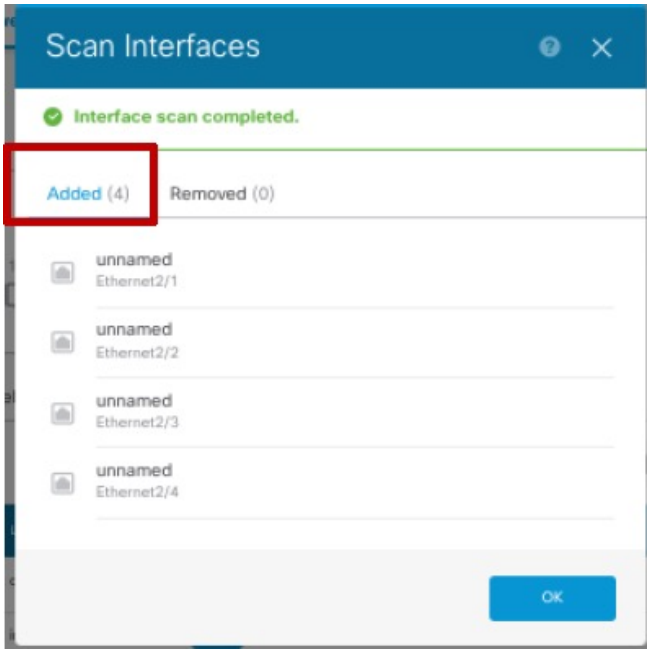
Illustration 3 : Analyse d'interface requise



Étape 4 Cliquez sur **Interface Scan** (analyse d'interface) pour mettre à jour la page avec les nouveaux détails du module de réseau.

Attendez que les interfaces effectuent l'analyse, puis cliquez sur **OK**.

Illustration 4 : Analyser les interfaces

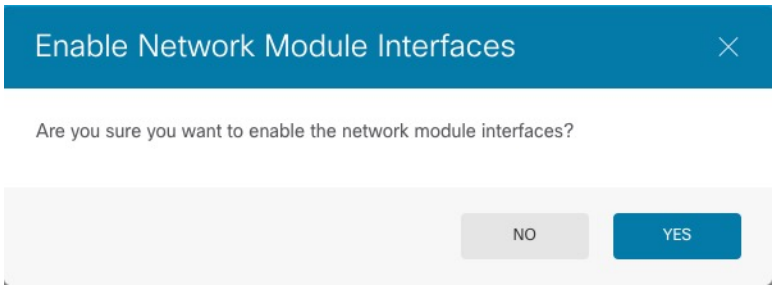


Étape 5 Sur le graphique des interfaces, cliquez sur le curseur ( ) pour activer le module de réseau.

Illustration 5 : Activer le module de réseau

Étape 6 Vous devez confirmer que vous souhaitez activer le module réseau. Cliquez sur **Yes** (Oui).

Illustration 6 : Confirmer l'activation



Étape 7 Pour la haute disponibilité, modifiez l'unité active (voir Commutation des homologues actifs et de secours (forcer le basculement)), puis effectuez les étapes ci-dessus pour la nouvelle unité de secours.

Échange à chaud du module de réseau

Vous pouvez échanger à chaud un module de réseau contre un nouveau module du même type sans avoir à redémarrer. Cependant, vous devez arrêter le module actuel pour le retirer en toute sécurité. Cette procédure décrit comment arrêter l'ancien module, installer un nouveau module et l'activer.

Avant de commencer

Pour la haute disponibilité, vous ne pouvez pas désactiver un module de réseau si le lien de basculement se trouve sur le module. Vous devrez interrompre la haute disponibilité (voir Rupture de la haute disponibilité). Après avoir permuté le module à chaud, vous pouvez reformer la haute disponibilité.

Procédure

Étape 1 Pour la haute disponibilité, assurez-vous que l'unité sur laquelle vous souhaitez effectuer le remplacement à chaud est le nœud de secours. Consultez Commutation des homologues actifs et de secours (forcer le basculement).

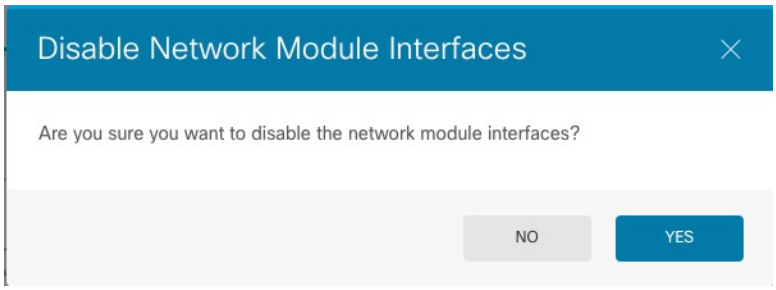
Étape 2 Cliquez sur **Device** (Périphérique), puis sur le lien **View All Interfaces** (Afficher toutes les interfaces) du résumé **Interfaces**.

Étape 3 Sur le graphique des interfaces, cliquez sur le curseur ( ) pour désactiver le module de réseau.

Illustration 7 : Désactiver le module de réseau

Étape 4 Vous êtes invité à confirmer que vous souhaitez désactiver le module de réseau. Cliquez sur **Yes** (Oui).

Illustration 8 : Confirmer la désactivation



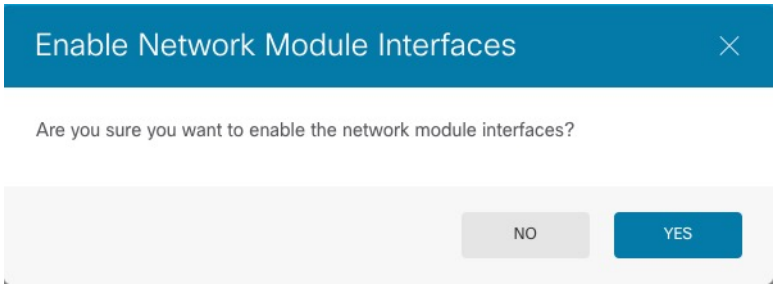
Étape 5 Installez le module de réseau en suivant le guide d'installation du matériel.

Étape 6 Sur le graphique des interfaces, cliquez sur le curseur ( ) pour activer le module de réseau.

Illustration 9 : Activer le module de réseau

Étape 7 Vous devez confirmer que vous souhaitez activer le module réseau. Cliquez sur **Yes** (Oui).

Illustration 10 : Confirmer l'activation



Remplacer le module de réseau par un module de type différent

Si vous remplacez un module de réseau par un autre type, un redémarrage est nécessaire. Si le nouveau module comporte moins d'interfaces que l'ancien module, vous devrez supprimer manuellement toute configuration liée aux interfaces qui ne seront plus présentes.

Avant de commencer

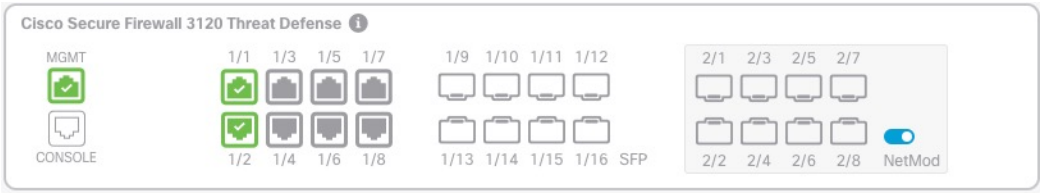
Pour la haute disponibilité, vous ne pouvez pas désactiver un module de réseau si le lien de basculement se trouve sur le module. Vous devrez désactiver la haute disponibilité (voir Rupture de la haute disponibilité), ce qui signifie qu'il y aura un temps d'arrêt au redémarrage de l'unité active. Une fois que les unités ont redémarré, vous pouvez rétablir la haute disponibilité.

Procédure

Étape 1 Cliquez sur **Device** (Périphériques), puis sur le lien **View All Interfaces** (Afficher toutes les interfaces) du résumé **Interfaces**. Pour la haute disponibilité, effectuez d'abord cette procédure sur l'unité de secours.

Étape 2 Sur le graphique des interfaces, cliquez sur le curseur ( ) pour désactiver le module de réseau.

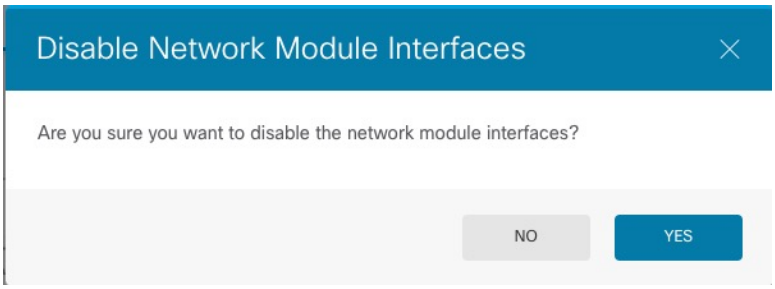
Illustration 11 : Désactiver le module de réseau



(Désactiver le module de réseau)

Étape 3 Vous êtes invité à confirmer que vous souhaitez désactiver le module de réseau. Cliquez sur **Yes** (Oui).

Illustration 12 : Confirmer la désactivation



Étape 4 Sur le périphérique, retirez l'ancien module de réseau et remplacez-le par le nouveau module de réseau en suivant le guide d'installation du matériel.

Étape 5 Redémarrez le pare-feu; voir Redémarrage ou arrêt du système.

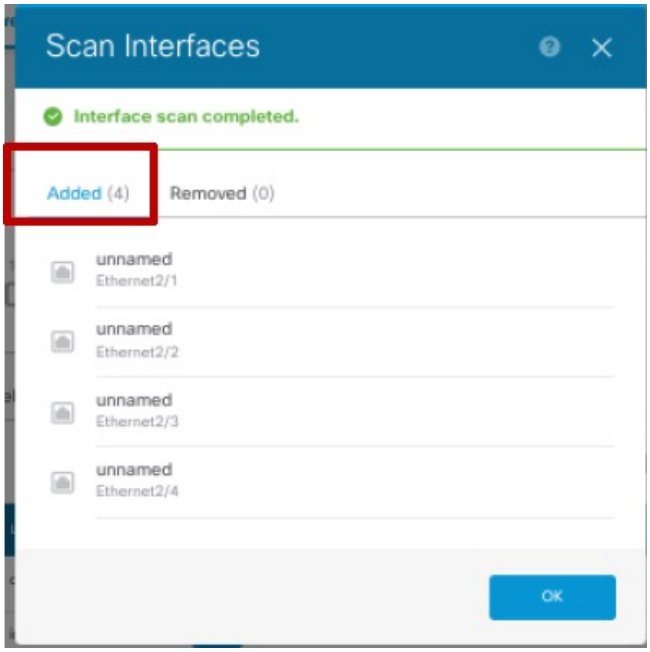
Étape 6 Dans la page **Interfaces**, le graphique indique qu'une analyse d'interface est requise. Cliquez sur **Interface Scan** (Analyse d'interface) pour mettre à jour la page avec les nouveaux détails du module de réseau.

Illustration 13 : Analyse d'interface requise

(Analyse d'interface requise)

Étape 7 Attendez que les interfaces effectuent l'analyse, puis cliquez sur **OK**.

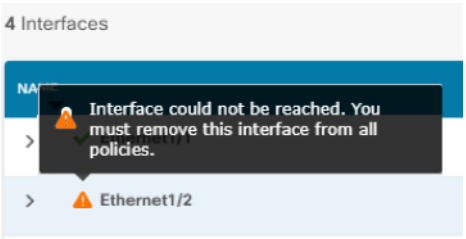
Illustration 14 : Analyser les interfaces



(Analyser les interfaces)

Après l'analyse, les interfaces supprimées s'affichent sur la page **Interfaces** avec des symboles d'avertissement :

Illustration 15 : Interfaces supprimées



Étape 8 Si le module de réseau comporte *moins* d'interfaces, vous devez supprimer toute configuration faisant directement référence aux interfaces supprimées.

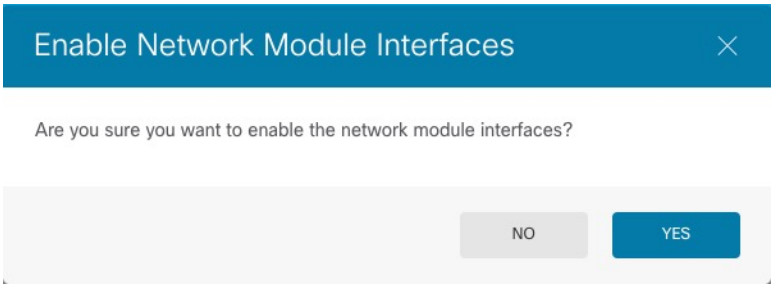
Les politiques qui font référence aux zones de sécurité ne sont pas touchées. Vous pouvez éventuellement migrer la configuration vers une autre interface. Consultez Analyser et migrer les interfaces, à la page 54.

Étape 9 Sur le graphique des interfaces, cliquez sur le curseur ( ) pour activer le module de réseau.

Illustration 16 : Activez le module de réseau

Étape 10 Vous devez confirmer que vous souhaitez activer le module réseau. Cliquez sur **Yes** (Oui).

Illustration 17 : Confirmer l'activation



Étape 11 Pour modifier la vitesse de l'interface, consultez Configurer les options avancées, à la page 49.

La vitesse par défaut est Detect SFP, qui détecte la vitesse correcte à partir du SFP installé. Vous devez seulement fixer la vitesse si vous la réglez manuellement à une valeur particulière et que vous avez maintenant besoin d'une nouvelle vitesse.

Étape 12 Si vous deviez modifier une configuration, cliquez sur l'icône **Déploiement**.

Vous n'avez pas besoin de procéder au déploiement juste pour enregistrer les modifications du module de réseau.

Étape 13 Pour la haute disponibilité, modifiez l'unité active (voir Commutation des homologues actifs et de secours (forcer le basculement)), puis effectuez les étapes ci-dessus pour la nouvelle unité de secours.

Retirer le module de réseau

Si vous souhaitez retirer définitivement le module de réseau, procédez comme suit. Le retrait d'un module de réseau nécessite un redémarrage.

Avant de commencer

Pour la haute disponibilité, assurez-vous que le lien de basculement ne se trouve pas sur le module de réseau.

Procédure

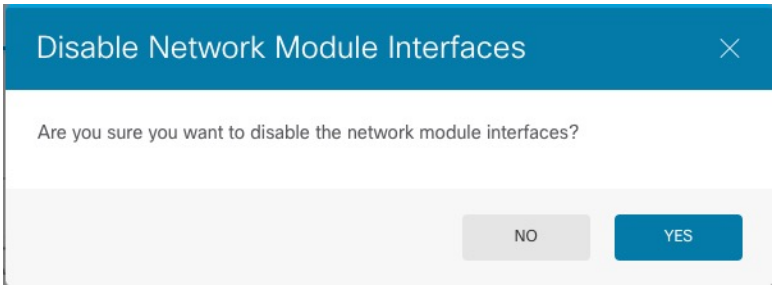
Étape 1 Cliquez sur **Device** (Périphérique), puis sur le lien **View All Interfaces** (Afficher toutes les interfaces) du résumé **Interfaces**. Pour la haute disponibilité, effectuez d'abord cette procédure sur l'unité de secours.

Étape 2 Sur le graphique des interfaces, cliquez sur le curseur ( ) pour désactiver le module de réseau.

Illustration 18 : Désactiver le module de réseau

Étape 3 Vous êtes invité à confirmer que vous souhaitez désactiver le module de réseau. Cliquez sur **Yes** (Oui).

Illustration 19 : Confirmer la désactivation



Étape 4 Sur le pare-feu, retirez le module de réseau.

Étape 5 Redémarrez le pare-feu; voir Redémarrage ou arrêt du système.

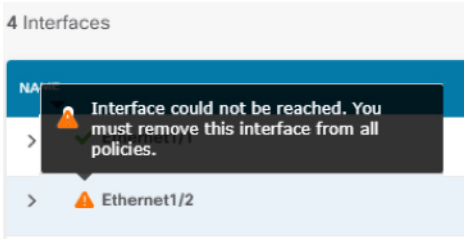
Étape 6 Dans la page **Interfaces**, le graphique indique qu'une analyse d'interface est requise. Cliquez sur **Interface Scan** (Analyse d'interface) pour mettre à jour la page avec les détails corrects du module réseau.

Illustration 20 : Analyse d'interface requise

Étape 7 Attendez que les interfaces effectuent l'analyse, puis cliquez sur **OK**.

Après l'analyse, les interfaces supprimées s'affichent sur la page **Interfaces** avec des symboles d'avertissement :

Illustration 21 : Interfaces supprimées



Étape 8 Vous devez supprimer toute configuration qui fait directement référence aux interfaces supprimées.

Les politiques qui font référence aux zones de sécurité ne sont pas touchées. Vous pouvez éventuellement migrer la configuration vers une autre interface. Consultez Analyser et migrer les interfaces, à la page 54.

Étape 9 Si vous deviez modifier une configuration, cliquez sur l'icône **Deployment** (Déploiement).

Vous n'avez pas besoin de procéder au déploiement juste pour enregistrer les modifications du module de réseau.

Étape 10 Pour la haute disponibilité, modifiez l'unité active (voir Commutation des homologues actifs et de secours (forcer le basculement)), puis effectuez les étapes ci-dessus pour la nouvelle unité de secours.

Configurer le contournement matériel automatique en cas de panne de courant (ISA 3000)

Le contournement matériel garantit que le trafic continue de circuler entre une paire d'interfaces en ligne pendant une panne de courant. Les paires d'interfaces prises en charge sont les interfaces en cuivre GigabitEthernet 1/1 et 1/2; et GigabitEthernet 1/3 et 1/4. Si vous avez un modèle Ethernet à fibre optique, seule la paire Ethernet en cuivre (GigabitEthernet 1/1 et 1/2) prend en charge le contournement matériel. Par défaut, le contournement matériel est activé pour les deux paires d'interfaces si elles sont prises en charge.

Lorsque le contournement matériel est actif, le trafic passe entre ces paires d'interfaces au niveau de la couche 1. Par défaut, l'interface FDM et la CLI FTD verront ces interfaces comme étant hors service. Aucune fonction de pare-feu n'est en place, assurez-vous donc de comprendre les risques de laisser le trafic passer par le périphérique.

Nous vous suggérons de désactiver l'aléatoire des numéros de séquence TCP (comme décrit dans cette procédure). Par défaut, l'ISA 3000 réécrit le numéro de séquence initial (ISN) des connexions TCP qui le traversent en nombre aléatoire. Lorsque le contournement matériel est activé, l'ISA 3000 ne se trouve plus dans le chemin de données et ne traduit pas les numéros de séquence. Le client destinataire reçoit un numéro de séquence inattendu et interrompt la connexion. La session TCP doit donc être rétablie. Même lorsque la répartition aléatoire des numéros de séquence TCP est désactivée, certaines connexions TCP devront être rétablies car la liaison a été temporairement interrompue pendant le basculement.

Dans la console de l'interface de ligne de commande ou dans une session SSH, utilisez la commande **show hardware-bypass** pour surveiller l'état opérationnel.

Avant de commencer

Pour que le contournement matériel fonctionne :

- Vous devez placer les paires d'interfaces dans le même groupe de ponts.
- Vous devez connecter les interfaces pour accéder aux ports du commutateur. Ne les connectez pas aux ports de ligne principale.

Procédure

Étape 1 Cliquez sur **Device** (Périphérique), puis sur le lien dans le résumé des Interfaces.

La section **Hardware Bypass** (Contournement matériel) en haut de la page, affiche la configuration actuelle des paires d'interfaces autorisées pour ce périphérique.

Cependant, vous devez vous assurer que les paires sont configurées dans le même groupe de ponts avant de pouvoir activer le contournement matériel.

Étape 2 Cliquez sur **Edit** (Modifier) pour configurer le contournement matériel.

La boîte de dialogue **Hardware Bypass Configuration** (Configuration du contournement matériel) s'affiche.

Étape 3 Pour configurer le comportement de contournement matériel automatique, choisissez, pour chaque paire d'interfaces, l'une des options suivantes dans la zone **Hardware Bypass during Power Down** (Contournement matériel pendant la mise hors tension).

- **Disable** (Désactiver) : désactive le contournement matériel. Le trafic ne passera pas par l'appareil en cas de panne de courant.
- **Enable** (Activer) : active le contournement matériel en cas de panne de courant. Le contournement matériel garantit que le trafic n'est pas interrompu en cas de panne de courant. Notez que le trafic contourné n'est pas inspecté et que les politiques de sécurité ne sont pas appliquées. Après le rétablissement de l'alimentation, le contournement matériel est automatiquement désactivé pour que le trafic puisse circuler normalement, avec inspection. Il peut y avoir une brève interruption du trafic lorsque le contournement matériel est désactivé.
- **Enable with Persistence** (Activer avec persistance) : active le contournement matériel en cas de panne de courant et le maintient activé après le rétablissement de l'alimentation. Une fois le courant rétabli, vous devez désactiver le contournement matériel à l'aide du curseur **Manual Hardware Bypass** (Contournement matériel manuel). Cette option vous permet de contrôler le moment de la brève interruption du trafic.

Étape 4 (Facultatif) Pour activer ou désactiver manuellement le contournement matériel, cliquez sur le curseur **Manual Hardware Bypass** (Contournement matériel manuel).

Par exemple, vous pourriez vouloir tester le système ou contourner temporairement le périphérique pour une raison quelconque. Notez que vous devez déployer la configuration pour modifier l'état du contournement matériel ; la simple modification des paramètres ne suffit pas.

Lorsque vous activez ou désactivez manuellement le contournement matériel, vous verrez les messages de journal système suivants, où *paire* est 1/1-1/2 ou 1/3-1/4.

- %FTD-6-803002 : aucune protection ne sera fournie par le système pour le trafic sur GigabitEthernet *pair*

- %FTD-6-803003 : l'utilisateur a désactivé le contournement manuel sur GigabitEthernet *pair*

Étape 5 Cliquez sur **OK**.

La modification n'est pas immédiate. Vous devez déployer la configuration.

Étape 6 (Facultatif) Créez l'objet FlexConfig et la politique nécessaires pour désactiver la aléatoireisation du numéro de séquence TCP.

a) Cliquez sur **View Configuration** (Afficher la configuration) dans **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)**.

b) Cliquez sur **FlexConfig** > **FlexConfig Objects (Objets FlexConfig)** dans la table des matières de configuration avancée.

c) Cliquez sur le bouton **+** pour créer un nouvel objet.

d) Saisissez un nom pour l'objet. Par exemple, **Disable_TCP_Randomization**.

e) Dans l'éditeur **Template** (Modèle), saisissez les commandes permettant de désactiver la randomisation du numéro de séquence TCP.

La commande est **set connection random-sequence-number disable**, mais vous devez la configurer pour une classe spécifique dans une carte de politique. De loin, l'approche la plus simple est de désactiver les numéros de séquence aléatoires globalement, ce qui nécessite les commandes suivantes :

```
policy-map global_policy
 class default_class
  set connection random-sequence-number disable
```

f) Dans l'éditeur **Negate Template** (Modèle d'annulation), saisissez les lignes nécessaires pour annuler cette configuration.

Par exemple, si vous désactivez la randomisation du numéro de séquence TCP globalement, le modèle d'annulation serait le suivant :

```
policy-map global_policy
 class default_class
  set connection random-sequence-number enable
```

g) Cliquez sur **OK** pour enregistrer l'objet.

Vous devez maintenant ajouter l'objet à FlexConfig Policy (politique FlexConfig). La création de l'objet n'est pas suffisante.

h) Cliquez sur **FlexConfig Policy** (Politique FlexConfig) dans la table des matières.

i) Cliquez sur **+** dans la liste des groupes.

j) Sélectionnez l'objet Disable_TCP_RandOMization et cliquez sur **OK**.

L'aperçu doit être mis à jour avec les commandes du modèle. Vérifiez que vous voyez les commandes attendues.

k) Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant déployer la politique.

Surveillance des interfaces

Vous pouvez afficher des renseignements de base sur les interfaces dans les zones suivantes :

- **Device** (Périphérique). Utilisez le graphique de port pour surveiller l'état actuel des interfaces. Passez le curseur sur un port pour voir ses adresses IP, l'appartenance à EtherChannel et les états d'activation et de liaison. Les adresses IP peuvent être attribuées statiquement ou obtenues à l'aide de DHCP.

  Les ports d'interface utilisent le code de couleur suivant :

  - Vert — l'interface est configurée, activée et la liaison est activée.
  - Gris — l'interface n'est pas activée.
  - Orange/rouge — l'interface est configurée et activée, mais la liaison est en panne. Si l'interface est câblée, il s'agit d'une condition d'erreur qui doit être corrigée. Si l'interface n'est pas câblée, il s'agit de l'état attendu.

- **Monitoring (Surveillance)** > **System (Système)**. Le tableau de bord **Throughput** (Débit) affiche des informations sur le trafic circulant dans le système. Vous pouvez afficher les informations sur toutes les interfaces ou sélectionner une interface spécifique à examiner.
- **Monitoring (Surveillance)** > **Zones**. Ce tableau de bord affiche les statistiques en fonction des zones de sécurité, qui sont composées d'interfaces. Vous pouvez explorer ces informations pour plus de détails.

Surveillance des interfaces dans l'interface de ligne de commande

Vous pouvez également ouvrir la console CLI ou vous connecter à l'interface de ligne de commande du périphérique et utiliser les commandes suivantes pour obtenir des informations plus détaillées sur le comportement et les statistiques liés à l'interface.

- **show interface** affiche les informations de configuration et d'état de l'interface. Cette commande comporte de nombreux mots-clés que vous pouvez utiliser pour obtenir les informations dont vous avez besoin. Utilisez ? en tant que mot-clé pour voir les options disponibles.
- **show ipv6 interface** affiche les informations de configuration IPv6 des interfaces.
- **show bridge-group** affiche les informations sur les interfaces virtuelles de pont (BVI), y compris les informations sur les membres et les adresses IP.
- **show conn** affiche les informations sur les connexions actuellement établies par les interfaces.
- **show traffic** affiche les statistiques sur le trafic circulant dans chaque interface.
- **show ipv6 traffic** affiche les statistiques sur le trafic IPv6 circulant dans le périphérique.
- **show dhcpd** affiche les statistiques et d'autres informations sur l'utilisation de DHCP sur les interfaces, en particulier sur les serveurs DHCP configurés sur les interfaces.
- **show switch vlan** affiche l'association VLAN-port de commutation.
- **show switch mac-address-table** affiche les entrées d'adresses MAC statiques et dynamiques.
- **show arp** affiche les entrées d'ARP dynamiques, statiques et de serveur mandataire.
- **show power inline** affiche l'état PoE.

- **show vpdn group** affiche les groupes PPPoE ainsi que les noms d'utilisateurs et l'authentification configurés.
- **show vpdn username** affiche les noms d'utilisateur et les mots de passe PPPoE.
- **show vpdn session pppoe state** affiche l'état de la session PPPoE.

Exemples d'interfaces

Le chapitre de scénarios d'utilisation comprend les exemples liés aux interfaces suivants :

- Comment configurer l'appareil en FDM
- Comment ajouter un sous-réseau
- Comment surveiller passivement le trafic sur un réseau

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.