



Présentation de l'interface

L'appareil défense contre les menaces comprend des interfaces de données que vous pouvez configurer dans différents modes, ainsi qu'une interface de gestion et de dépistage.

- [Interface de gestion/dépistage, à la page 1](#)
- [Types et modes d'interface, à la page 2](#)
- [Zones de sécurité et groupes d'interfaces, à la page 4](#)
- [Fonctionnalité Auto-MDI/MDIX, à la page 5](#)
- [Paramètres par défaut des interfaces, à la page 6](#)
- [Créer des objets de zone de sécurité et de groupe d'interface, à la page 6](#)
- [Activer l'interface physique et configurer des paramètres Ethernet, à la page 7](#)
- [Configurer les interfaces EtherChannel, à la page 10](#)
- [Synchroniser les modifications apportées à l'interface avec le Centre de gestion, à la page 18](#)
- [Gérer le module de réseau pour Cisco Secure Firewall, à la page 21](#)
- [Historique des interfaces, à la page 37](#)

Interface de gestion/dépistage

, l'interface de gestion physique était partagée entre l'interface virtuelle de dépistage et l'interface virtuelle de gestion.

Interface de gestion

L'interface de gestion est distincte des autres interfaces sur le périphérique. Elle est utilisée pour configurer et enregistrer le périphérique sur le centre de gestion. Il utilise sa propre adresse IP et le routage statique. Vous pouvez configurer ses paramètres dans l'interface de ligne de commande à l'aide de la commande **configure network**. Si vous modifiez l'adresse IP au niveau de l'interface de ligne de commande après l'avoir ajoutée à centre de gestion, vous pouvez faire correspondre l'adresse IP dans Cisco Secure Firewall Management Center dans la zone **de gestion > périphériques > gestion des > périphériques**.

Vous pouvez également gérer le périphérique défense contre les menaces à l'aide d'une interface de données au lieu de l'interface de gestion.

Interface de diagnostic

L'interface logique de dépistage peut être configurée avec le reste des interfaces de données sur l'écran **Périphériques > Gestion de périphériques > Interfaces**. L'utilisation de l'interface de dépistage est facultative (consultez les déploiements en modes routé et transparent pour les scénarios). L'interface de diagnostic autorise uniquement le trafic de gestion et n'autorise pas le trafic de transit. Il ne prend pas en charge SSH; vous pouvez accéder à SSH avec les interfaces de données ou l'interface de gestion uniquement. L'interface de dépistage est utile pour la surveillance SNMP ou syslog.



Remarque Bien que les interfaces de dépistage et de gestion partagent un port physique, vous devez affecter des adresses IP différentes à chaque interface du même réseau.

Types et modes d'interface

Vous pouvez déployer des interfaces défense contre les menaces de deux manières : le mode de pare-feu normal et le mode IPS uniquement. Vous pouvez inclure des interfaces de pare-feu et des interfaces IPS uniquement sur le même périphérique.

Mode de pare-feu normal

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

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

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

Mode IPS seulement

Les interfaces en mode IPS uniquement contournent de nombreuses vérifications de pare-feu et ne prennent en charge que la politique de sécurité IPS. Vous pourriez souhaiter mettre en œuvre des interfaces IPS uniquement si vous avez un pare-feu distinct qui protège ces interfaces et que vous ne souhaitez pas le surdébit des fonctions du pare-feu.



Remarque Le mode de pare-feu affecte uniquement les interfaces de pare-feu standard, et non les interfaces IPS uniquement, comme les ensembles en ligne ou les interfaces passives. Les interfaces IPS uniquement peuvent être utilisées dans les deux modes de pare-feu.

Les interfaces IPS uniquement peuvent être déployées en tant que types suivants :

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

En mode TAP, le FTD est déployé en ligne, mais le flux du trafic réseau n'est pas perturbé. Au lieu de cela, FTD effectue une copie de chaque paquet afin de pouvoir analyser les paquets. Notez que les règles de ces types génèrent des incidents d'intrusion lorsqu'elles sont déclenchées, et la vue du tableau des incidents d'intrusion indique que les paquets de déclenchement auraient été abandonnés dans un déploiement en ligne. Il y a des avantages à utiliser le mode TAP avec les FTD déployés en ligne. Par exemple, vous pouvez configurer le câblage entre le FTD et le réseau comme si le FTD était en ligne et analyser les types d'incidents d'intrusion que le FTD génère. En fonction des résultats, vous pouvez modifier votre politique de prévention des intrusions et ajouter les règles d'abandon qui protègent le mieux votre réseau sans nuire à son efficacité. Lorsque vous êtes prêt à déployer le FTD en ligne, vous pouvez désactiver le mode TAP et commencer à abandonner le trafic suspect sans avoir à reconfigurer le câblage entre le FTD et le réseau.



Remarque Le mode TAP peut avoir un impact *considérable* sur les performances de FTD, selon le trafic.



Remarque Les ensembles en ligne vous sont peut-être familiers sous la forme « ensembles en ligne transparents », mais le type d'interface en ligne n'est pas lié au mode de pare-feu transparent ou aux interfaces de type pare-feu.

- Passive or ERSPAN Passive (passif ou ERSPAN 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. Les interfaces ERSPAN (Encapsulating Remote Switched Port Analyzer) vous permettent de surveiller le trafic à partir de ports sources répartis sur plusieurs commutateurs et utilisent GRE pour encapsuler le trafic. Les interfaces ERSPAN ne sont autorisées que lorsque FTD est en mode de pare-feu routé.



Remarque L'utilisation d'interfaces SR-IOV en tant qu'interfaces passives sur NGFWv n'est pas prise en charge sur certaines cartes réseau Intel (comme les Intel X710 ou 82599) utilisant les pilotes SR-IOV en raison d'une restriction de mode promiscuité. Dans ce cas, utilisez une carte réseau qui prend en charge cette fonctionnalité. Consultez la section [Produits Ethernet Intel](#) pour plus d'informations sur les cartes réseau Intel.

Zones de sécurité et groupes d'interfaces

Chaque interface doit être affectée à une *zone de sécurité* ou à un *groupe d'interfaces*. Vous appliquez ensuite votre politique de sécurité sur la base de zones ou de groupes. Par exemple, vous pouvez affecter l'interface interne, ou un ou plusieurs périphériques, à la zone interne; et l'interface externe à la zone externe. Vous pouvez ensuite configurer votre politique de contrôle d'accès de manière à permettre au trafic de passer de la zone interne à la zone externe pour chaque appareil utilisant les mêmes zones.

Pour afficher les interfaces qui appartiennent à chaque objet, sélectionnez **Objects (Objets) > Object Management (Gestion des objets)** et cliquez sur **Interface**. Cette page répertorie les zones de sécurité et les groupes d'interfaces configurés sur vos périphériques gérés. Vous pouvez développer chaque objet d'interface pour afficher le type d'interface dans chaque objet d'interface.



Remarque Les politiques qui s'appliquent à **n'importe quelle** zone (politiques globales) s'appliquent aux interfaces dans les zones ainsi qu'à toutes les interfaces qui ne sont pas affectées à une zone.



Remarque L'interface de dépistage ou de gestion n'appartient à aucune zone ou à aucun groupe d'interfaces.

Zones de sécurité par rapport aux groupes d'interface

Il existe deux types d'objets d'interface :

- Zones de sécurité - Une interface ne peut appartenir qu'à une seule zone de sécurité.
- Groupes d'interfaces : une interface peut appartenir à plusieurs groupes d'interfaces.

Vous pouvez utiliser des groupes d'interfaces dans les politiques NAT, les politiques de préfiltre et les politiques de QoS, ainsi que les fonctionnalités qui vous permettent de préciser directement le nom de l'interface, comme les serveurs Syslog ou DNS.

Certaines politiques ne prennent en charge que les zones de sécurité, tandis que d'autres prennent en charge les zones et les groupes. À moins que vous n'ayez besoin des fonctionnalités fournies par un groupe d'interface, vous devez utiliser par défaut les zones de sécurité, car les zones de sécurité sont prises en charge pour toutes les fonctionnalités.

Vous ne pouvez pas changer une zone de sécurité existante en groupe d'interface et inversement; vous devez plutôt créer un nouvel objet d'interface.

**Remarque**

Bien que les zones de tunnel ne soient pas des objets d'interface, vous pouvez les utiliser à la place de zones de sécurité dans certaines configurations; voir [Zones de tunnel et préfiltrage](#).

Types d'objets d'interface

Consultez les types d'objets d'interface suivants :

- Passive : pour les interfaces passives ou ERSPAN uniquement IPS.
- En ligne : pour les interfaces d'ensemble en ligne IPS uniquement.
- Commutée : pour les interfaces de groupe de ponts de pare-feu standard.
- Routée : pour les interfaces routées de pare-feu standard.
- ASA : (zones de sécurité uniquement) pour les interfaces de périphérique ASA FirePOWER existantes.

Toutes les interfaces d'un objet d'interface doivent être du même type. Après avoir créé un objet d'interface, vous ne pouvez pas modifier le type d'interfaces qu'il contient.

Noms d'interface

Notez que l'interface (ou le nom de zone) en elle-même ne fournit aucun comportement par défaut en ce qui concerne la politique de sécurité. Nous vous recommandons d'utiliser des noms qui parlent d'eux-mêmes pour éviter des erreurs de configuration futures. Un nom adéquat signifie un segment logique ou une spécification de trafic, par exemple :

- Noms des interfaces internes : InsideV110, InsideV160, InsideV195
- Noms des interfaces DMZ : DMZV11, DMZV12, DMZV-TEST
- Noms des interfaces externes : Outside-ASN78, Outside-ASN91

Objets de l'interface et emplacement de multidétention

Dans un déploiement multidomaine, vous pouvez créer des objets d'interface à n'importe quel niveau. Un objet d'interface créé dans un domaine ancêtre peut contenir des interfaces qui résident sur des périphériques dans différents domaines. Dans cette situation, les utilisateurs de sous-domaine qui consultent la configuration de l'objet d'interface ancêtre dans le gestionnaire d'objets ne peuvent voir que les interfaces de leur domaine.

À moins d'une restriction par leur rôle, les utilisateurs de sous-domaine peuvent afficher **et** modifier les objets d'interface créés dans les domaines ascendants. Les utilisateurs de sous-domaine peuvent ajouter et supprimer des interfaces à partir de ces objets d'interface. Ils ne peuvent pas, cependant, supprimer ou renommer les objets d'interface. Vous ne pouvez ni afficher ni modifier les objets d'interface créés dans des domaines descendants.

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.

Paramètres par défaut des interfaces

Cette section répertorie les paramètres par défaut pour les interfaces.

État par défaut des interfaces

L'état par défaut d'une interface dépend du type d'interface.

- Interfaces physiques : désactivées. L'exception est l'interface de gestion qui est activée pour la configuration initiale.
- Interfaces redondantes : activées. Cependant, pour que le trafic passe par l'interface redondante, les interfaces physiques membres doivent également être activées.
- Sous-interfaces VLAN : activées. Cependant, pour que le trafic passe par la sous-interface, l'interface physique doit également être activée.
- Interfaces de canal de port EtherChannel (ISA 3000) : activées. Cependant, pour que le trafic passe par l'EtherChannel, les interfaces physiques des groupes de canaux doivent également être activées.
- Interfaces de canal de port EtherChannel (modèles Firepower et Secure Firewall) : désactivées.



Remarque

Dans le cas du Firepower 4100/9300, vous pouvez activer et désactiver administrativement les interfaces dans le châssis et dans le centre de gestion. Pour qu'une interface soit opérationnelle, elle doit être activée dans les deux systèmes d'exploitation. Étant donné que l'état de l'interface est contrôlé indépendamment, il se peut que vous ayez une incompatibilité entre le châssis et centre de gestion.

Vitesse par défaut et duplex

Par défaut, la vitesse et les interfaces duplex pour les interfaces en cuivre (RJ-45) sont à négociation automatique.

Par défaut, la vitesse et les interfaces duplex pour la fibre optique (SFP) sont définies à la vitesse maximale, avec la négociation automatique activée.

Pour Secure Firewall, la vitesse est réglée pour détecter la vitesse du module SFP installé.

Créer des objets de zone de sécurité et de groupe d'interface

Ajoutez les zones de sécurité et les groupes d'interfaces auxquels vous pouvez affecter des interfaces de périphérique.



Astuces Vous pouvez créer des objets d'interface vides et y ajouter des interfaces ultérieurement. Pour ajouter une interface, celle-ci doit avoir un nom. Vous pouvez également créer des zones de sécurité (mais pas de groupes d'interfaces) lors de la configuration des interfaces.

Avant de commencer

Comprenez les exigences et les restrictions d'utilisation de chaque type d'objet d'interface. Consultez [Zones de sécurité et groupes d'interfaces](#), à la page 4.

Procédure

- Étape 1** Choisissez **Objects (objets) > Object Management (gestion des objets)**.
Vous pouvez également sélectionner **Objets > Autres objets FTD** pour créer des objets.
- Étape 2** Sélectionnez **Interface** dans la liste des types d'objets.
- Étape 3** Cliquez sur **Ajouter > Zone de sécurité** ou **Ajouter > Groupe d'interfaces**.
- Étape 4** Saisissez un **Nom**.
- Étape 5** Choisissez un **Type d'interface**.
- Étape 6** (Facultatif) Dans la liste déroulante **Device > Interfaces** (interfaces de périphériques), choisissez un périphérique qui contient des interfaces que vous souhaitez ajouter.
Vous n'avez pas besoin d'affecter des interfaces sur cet écran; vous pouvez plutôt affecter des interfaces à la zone ou au groupe lorsque vous configurez l'interface.
- Étape 7** Cliquez sur **Save** (enregistrer).

Prochaine étape

- Si une politique active fait référence à votre objet, déployer les changements de configuration.

Activer l'interface physique et configurer des paramètres Ethernet

Cette section décrit comment :

- Activez l'interface physique. Par défaut, les interfaces physiques sont désactivées (à l'exception de l'interface Diagnostic).
- Définissez une vitesse et un mode duplex spécifiques. Par défaut, la vitesse et le mode duplex sont réglés à Auto.

Cette procédure ne couvre qu'un petit sous-ensemble des paramètres de l'interface. S'abstenir de définir d'autres paramètres à ce stade. Par exemple, vous ne pouvez pas nommer une interface que vous souhaitez utiliser dans une interface EtherChannel.



Remarque Pour le Firepower 4100/9300, vous configurez les paramètres de base de l'interface dans FXOS. Consultez [Configurer une interface physique](#) pour obtenir de plus amples renseignements.



Remarque Pour les ports de commutation Firepower 1010, consultez [Configurer les ports de commutation de Firepower 1010](#).

Avant de commencer

Si vous avez modifié les interfaces physiques sur le périphérique après l'avoir ajouté au centre de gestion, vous devez actualiser la liste des interfaces en cliquant sur **Sync Interfaces from Device** (Synchroniser les interfaces à partir du périphérique) en haut à gauche de **Interfaces**. Pour Cisco Secure Firewall, qui prend en charge l'échange à chaud, consultez [Gérer le module de réseau pour Cisco Secure Firewall, à la page 21](#) avant de modifier les interfaces sur un périphérique.

Procédure

-
- Étape 1** Sélectionnez **Devices (périphériques) > Device Management** (gestion des appareils) et cliquez sur **Edit** () pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.
- Étape 2** Cliquez sur **Edit** () pour l'interface que vous souhaitez modifier.
- Étape 3** Activez l'interface en cochant la case **Enabled** (activé).
- Étape 4** (Facultatif) Ajoutez une description dans le champ **Description**.
La description peut contenir jusqu'à 200 caractères sur une seule ligne (sans retour chariot).
- Étape 5** (Facultatif) Synchroniser les interfaces à partir du périphérique **Hardware Configuration > Speed** (Configuration matérielle > Vitesse).
- **Duplex** : choisissez entre **Full** ou **Half**. Les interfaces SFP prennent uniquement en charge les conditions de duplex **full (complètes)**.
 - **Speed** : choisissez une vitesse (variable selon le modèle). (Secure Firewall 3100 uniquement) choisissez **Detect SFP** pour détecter la vitesse du module SFP installé et utiliser la vitesse appropriée. Le mode duplex est toujours Full (complet) et la négociation automatique est toujours activée. Cette option est utile si vous modifiez ultérieurement le module de réseau pour un modèle différent et que vous souhaitez que la vitesse se mette à niveau automatiquement.
 - **Négociation automatique** : définissez l'interface pour négocier le débit, l'état de la liaison et le contrôle de flux.
 - **Mode de correction d'erreur de transfert** : (cisco Secure Firewall 3100uniquement) Pour les interfaces de 25 Gbit/s et plus, activez la correction d'erreur de transfert (FEC). Pour une interface membre d'EtherChannel, vous devez configurer la correction d'erreur directe avant de l'ajouter à l'EtherChannel. Le paramètre choisi lorsque vous utilisez **Auto** dépend du type d'émetteur-récepteur et selon si l'interface est fixe (intégrée) ou sur un module de réseau.

Tableau 1 : FEC par défaut pour le réglage automatique

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

Étape 6

(Facultatif) (Firepower 1100/2100, Secure Firewall 3100) Activez le protocole LLDP (Link Layer Discovery Protocol) en cliquant sur **Hardware Configuration (Configuration matérielle) > Network Connectivity (Connectivité réseau)**.

- **Enable LLDP Receive** (activer la réception LLDP) : permet au pare-feu de recevoir des paquets LLDP de ses homologues.
- **Enable LLDP Transmit** (activer la transmission LLDP) : permet au pare-feu d'envoyer des paquets LLDP à ses homologues.

Étape 7

(Facultatif) (Secure Firewall) Activez l'activation des trames de pause (XOFF) pour le contrôle de flux en cliquant sur **Hardware Configuration > Network Connectivity** (Configuration matérielle > Connectivité réseau) puis en cochant **Flow Control Send** (envoi du contrôle de flux) .

Le contrôle de flux permet aux ports Ethernet connectés de contrôler les débits de trafic en cas de congestion en permettant aux nœuds encombrés de suspendre les opérations de liaison à l'autre extrémité. Si le port de défense contre les menaces est congestionné (épuisement des ressources en file d'attente sur le commutateur interne) et ne peut plus recevoir de trafic, il en informe l'autre port en envoyant une trame de pause pour interrompre l'envoi jusqu'à ce que la condition soit réglée. À la réception d'une trame de pause, le périphérique expéditeur arrête d'envoyer des paquets de données, ce qui empêche toute perte de paquets de données pendant la période de congestion.

Remarque La défense contre les menaces prend en charge la transmission de trames de pause afin que l'homologue distant puisse contrôler le débit du trafic.

Cependant, la réception de trames de pause n'est pas prise en charge.

Le commutateur interne dispose d'un ensemble global de 8 000 tampons de 250 octets chacun et le commutateur alloue des tampons de manière dynamique à chaque port. Une trame de pause est envoyée à chaque interface pour laquelle le contrôle de flux est activé lorsque l'utilisation de la mémoire tampon dépasse la borne supérieure globale (2 Mo (8 000 tampons)); et une trame de pause est envoyée par une interface particulière lorsque sa mémoire tampon dépasse le seuil supérieur du port (0,3125 Mo (1 250 tampons)). Après l'envoi d'une pause, une trame XON peut être envoyée lorsque l'utilisation de la mémoire tampon est réduite sous le seuil des faibles niveaux (1,25 Mo dans l'ensemble (5 000 tampons ; 0,25 Mo par port (1 000 tampons)). Le partenaire de liaison peut reprendre le trafic après avoir reçu une trame XON.

Seules les trames de contrôle de flux définies dans la norme 802.3x sont prises en charge. Le contrôle de flux basé sur la priorité n'est pas pris en charge.

Étape 8

Dans la liste déroulante **Mode**, choisissez :

- **Aucun** : choisissez ce paramètre pour les interfaces de pare-feu et les ensembles en ligne standard. Le mode passera automatiquement à Routé, Commutateur ou En ligne en fonction de la configuration ultérieure.
- **Passif** : choisissez ce paramètre pour les interfaces passives IPS uniquement.
- **Ersipan** : choisissez ce paramètre pour les interfaces ERSPAN passives uniquement IPS.

Étape 9

Dans le champ **Priority** (Priorité), saisissez un nombre compris entre 0 et 65 535.

Cette valeur est utilisée dans la configuration de routage basée sur les politiques. La priorité est utilisée pour déterminer la façon dont vous souhaitez répartir le trafic sur plusieurs interfaces de sortie.

Étape 10

Cliquez sur **OK**.

Étape 11

Cliquez sur **Save** (enregistrer).

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

Étape 12

Poursuivez la configuration des interfaces.

- [Interfaces de pare-feu standard](#)
- [Ensembles en ligne et interfaces passives](#)

Configurer les interfaces EtherChannel

Cette section explique comment configurer les interfaces EtherChannel.

**Remarque**

Pour Firepower 4100/9300, vous configurez les EtherChannels dans FXOS. Consultez la [Ajouter un canal EtherChannel \(canal de port\)](#) pour de plus amples renseignements.

À propos des EtherChannels

La présente section décrit les canaux EtherChannels.

About 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, sauf pour ASA, les l'ISA 3000, qui prend en charge 16 interfaces actives. Pour les commutateurs qui prennent en charge seulement 8 interfaces actives, vous pouvez affecter jusqu'à 16 interfaces à un groupe de canaux : alors que seules 8 interfaces peuvent être actives, les interfaces restantes peuvent servir de liaisons de secours en cas de défaillance de l'interface.

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.

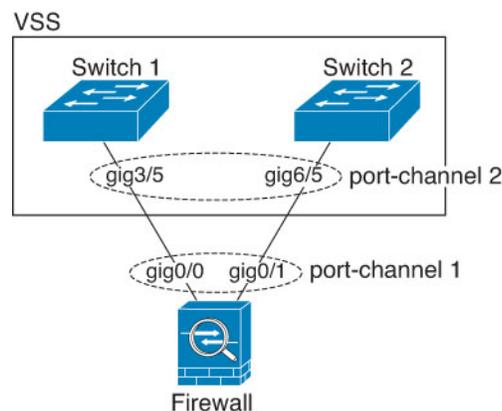
L'EtherChannel agrège le trafic sur toutes les interfaces actives disponibles dans le canal. L'interface est sélectionnée à l'aide d'un algorithme de hachage exclusif, en fonction des adresses MAC source ou de destination, des adresses IP, des numéros de ports TCP et UDP et des numéros de VLAN.

Connexion à un EtherChannel sur un autre périphérique

Le périphérique auquel vous connectez l'EtherChannel défense contre les menaces 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 défense contre les menaces 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

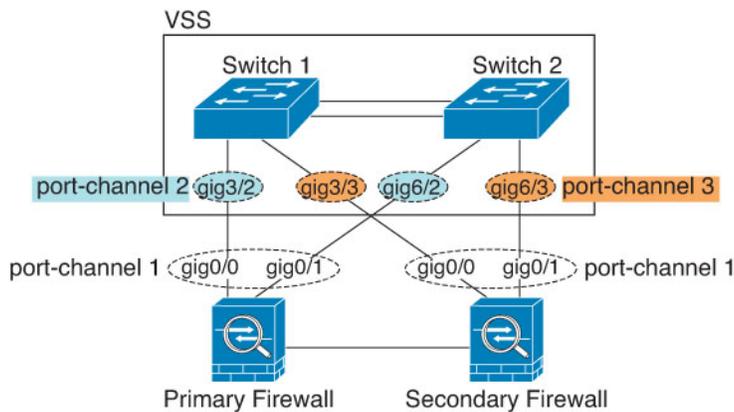


Remarque

Si le périphérique défense contre les menaces est en mode de pare-feu transparent et que vous placez le périphérique défense contre les menaces 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 défense contre les menaces 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 défense contre les menaces dans un déploiement de basculement actif/en veille, vous devez créer des EtherChannels distincts sur les commutateurs du VSS/vPC, un pour chaque périphérique défense contre les menaces. Sur chaque périphérique défense contre les menaces, 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 défense contre les menaces (dans ce cas, l'EtherChannel ne sera pas établi en raison des ID de système défense contre les menaces distincts), un seul EtherChannel ne serait pas souhaitable, car vous ne pouvez pas souhaiter que le trafic soit envoyé au périphérique défense contre les menaces.

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.
- **Passive** : reçoit les mises à jour du protocole LACP. Un EtherChannel passif ne peut établir une connectivité qu'avec un EtherChannel actif. Non pris en charge sur les modèles matériel.
- **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 défense contre les menaces 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

En mode routé, les EtherChannels définis par l'Centre de gestion 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 (pour une interface EtherChannel, le nombre d'interfaces membres autorisées à échouer peut être configuré).

- 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 ne pouvez pas ajouter d'EtherChannels dans le centre de gestion pour le Firepower 4100/9300 ou le défense contre les menaces virtuelles. Le Firepower 4100/9300 prend en charge EtherChannels, mais vous devez effectuer toute la configuration matérielle des EtherChannels dans FXOS sur le châssis.
- 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, sauf pour ASA, les l'ISA 3000, qui prend en charge 16 interfaces actives. Pour les commutateurs qui prennent en charge seulement 8 interfaces actives, vous pouvez affecter jusqu'à 16 interfaces à un groupe de canaux : alors que seules 8 interfaces peuvent être actives, les interfaces restantes peuvent servir de liaisons de secours en cas de défaillance de l'interface.
- 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 Cisco Secure Firewall, qui prend en charge différentes capacités d'interface à condition que la vitesse soit réglée pour détecter SFP; dans ce cas, la vitesse la plus basse est utilisée.
- Le périphérique auquel vous connectez l'EtherChannel défense contre les menaces doit également prendre en charge l'EtherChannel 802.3ad.
- Le périphérique défense contre les menaces 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 défense contre les menaces abandonnera les LACPDU balisées. Assurez-vous de désactiver le balisage VLAN natif sur le commutateur voisin.
- Les périphériques ne prennent pas en charge le débit LACP rapide, sauf les, les et l'ISA 3000; 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.
- Dans les versions du logiciel Cisco IOS antérieures à la 15.1(1)S2, défense contre les menaces 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 défense contre les menaces 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 défense contre les menaces fait référence à l'interface logique EtherChannel plutôt qu'aux interfaces physiques membres.

Configurer un EtherChannel

Cette section décrit comment créer une interface de canal de port EtherChannel, affecter des interfaces à l'EtherChannel et personnaliser l'EtherChannel.

Directives

- Vous pouvez configurer jusqu'à 48 EtherChannels, selon le nombre d'interfaces de votre modèle.
- Chaque groupe de canaux peut avoir jusqu'à 8 interfaces actives, sauf pour ISA 3000, qui prend en charge 16 interfaces actives. Pour les commutateurs qui prennent en charge uniquement 8 interfaces actives, vous pouvez affecter jusqu'à 16 interfaces à un groupe de canaux : alors que seules 8 interfaces peuvent être actives, les interfaces restantes peuvent servir de liaisons de secours en cas de défaillance de l'interface.
- 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 Cisco Secure Firewall , qui prend en charge différentes capacités d'interface à condition que la vitesse soit réglée pour détecter SFP; dans ce cas , la vitesse la plus basse est utilisée.



Remarque

Pour Firepower 4100/9300, vous configurez les EtherChannels dans FXOS. Consultez [Ajouter un canal EtherChannel \(canal de port\)](#) pour obtenir de plus amples renseignements.

Avant de commencer

- Vous ne pouvez pas ajouter d'interface physique au groupe de canaux si vous lui avez configuré un nom. Vous devez d'abord supprimer le nom.



Remarque

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

Procédure

Étape 1

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

- Étape 2** Activer les interfaces membres en fonction de [Activer l'interface physique et configurer des paramètres Ethernet, à la page 7](#).
- Étape 3** Cliquez **Add Interfaces (ajoutez des interfaces) > Ether Channel Interface (interfaces EtherChannel)**.
- Étape 4** Sous l'onglet **General (General)**, définissez l' **Ether Channel ID (ID EtherChannel)** sur un nombre compris entre 1 et 48 (1 et 8 pour Firepower 1010).

Illustration 3 : Ajouter une interface Ethernet

The screenshot shows the 'Add Ether Channel Interface' dialog box with the following configuration:

- Name:** dmz
- Enabled
- Management Only
- Description:** (empty field)
- Mode:** None
- Security Zone:** dmz_zone
- MTU:** 1500 (range: 64 - 9198)
- Priority:** 0 (range: 0 - 65535)
- Propagate Security Group Tag:
- Ether Channel ID *:** 1

Buttons: Cancel, OK

- Étape 5** Dans la zone **Available Interfaces Pairs** (paires d'interfaces disponibles), cliquez sur une paire, puis sur **Add** (ajouter) pour la déplacer vers la zone **Selected Interface Pair** (paire d'interfaces choisies). Répétez l'opération pour toutes les interfaces que vous souhaitez rendre membres.
- Vérifiez que toutes les interfaces sont du même type et ont la même capacité de vitesse.

Illustration 4 : Interfaces disponibles

Ether Channel ID *:
1
(1-8)

Available Interfaces ↻

Search

Ethernet1/1 Add

Selected Interfaces

NVE Only:

Cancel OK

Étape 6

(Facultatif) Cliquez sur l'onglet **Advanced** (Avancé) pour personnaliser l'EtherChannel. Définissez les paramètres suivants dans le sous-onglet **Information** :

Illustration 5 : Advanced (niveau avancé)

Add Ether Channel Interface ?

General IPv4 IPv6 Hardware Configuration Path Monitoring **Advanced**

Information

LACP Mode: Active

Active Mac Address:

Standby Mac Address:

- (ISA 3000 uniquement) **Équilibrage de la charge** : sélectionnez les critères utilisés pour équilibrer la charge des paquets sur les interfaces de canal de groupe. Par défaut, le périphérique défend contre les menaces équilibre la charge de paquets sur les interfaces en fonction de l'adresse IP de source et de destination du paquet. Si vous souhaitez modifier les propriétés selon lesquelles le paquet est classé, choisissez un ensemble de critères différent. Par exemple, si votre trafic est fortement orienté vers les mêmes adresses IP de source et de destination, l'affectation du trafic aux interfaces de l'EtherChannel ne sera pas équilibrée. Le passage à un algorithme différent peut entraîner une répartition plus uniforme du trafic. Pour plus d'informations sur l'équilibrage de la charge, consultez [Équilibrage de la charge, à la page 12](#).
- **Mode LACP** : Choisissez Actif, Passif ou Activé. Nous vous recommandons d'utiliser le mode actif (par défaut).
- (ISA 3000 uniquement) **Active Physique Interface : Plage** : Dans la liste déroulante de gauche, choisissez le nombre minimal d'interfaces actives requises pour que l'EtherChannel soit actif, entre 1 et 16. La valeur par défaut est 1. Dans la liste déroulante de droite, choisissez le nombre maximal d'interfaces

actives autorisées dans l'EtherChannel entre 1 et 16. Par défaut, c'est 16. Si votre commutateur ne prend pas en charge 16 interfaces actives, veillez à régler cette commande à 8 ou moins.

- **Active Mac Address** (adresse MAC active) : définissez une adresse MAC manuelle, si vous le souhaitez. La `mac_address` est au format H.H.H., où H est une valeur hexadécimale de 16 bits. Par exemple, l'adresse MAC 00-0C-F1-42-4C-DE est saisie comme suit : 00C.F142.4CDE.

Étape 7 Cliquez sur l'onglet **Hardware Configuration** (configuration matérielle) et définissez les conditions de duplex et la vitesse pour toutes les interfaces membres.

Étape 8 Cliquez sur **OK**.

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

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

Étape 10 (Facultatif) Ajouter une sous-interface VLAN Consultez [Ajouter une sous-interface](#).

Étape 11 Configurez les paramètres d'interface en mode routé ou transparent. Reportez-vous aux sections [Configurer les interfaces en mode routé](#) ou [Configurer les interfaces de groupe de ponts](#).

Synchroniser les modifications apportées à l'interface avec le Centre de gestion

Les modifications apportées à la configuration de l'interface sur le périphérique peuvent désynchroniser le centre de gestion et le périphérique. Le centre de gestion peut détecter les modifications apportées à l'interface par l'une des méthodes suivantes :

- Événement envoyé à partir du périphérique
- Synchroniser lorsque vous déployez à partir de centre de gestion

Si le centre de gestion détecte des modifications d'interface lors de la tentative de déploiement, le déploiement échouera. Vous devez d'abord accepter les modifications apportées à l'interface.

- Synchronisation manuelle

Il existe deux types de modifications d'interface effectuées en dehors de centre de gestion qui doivent être synchronisées :

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

Lorsque le centre de gestion détecte des changements, la page **Interface** affiche l'état (supprimé, modifié ou ajouté) à gauche de chaque interface.

- Modifications de l'interface d'accès Centre de gestion : Si vous configurez une interface de données pour gérer le en utilisant la commande **configure network management-data-interface**, vous devez effectuer manuellement les modifications de configuration correspondantes dans le puis valider les modifications. Ces modifications d'interface ne peuvent pas être apportées automatiquement.

Cette procédure décrit comment synchroniser manuellement les modifications apportées aux périphériques, le cas échéant, et comment accuser réception des modifications détectées. Si les modifications de périphérique sont temporaires, vous ne devez pas les enregistrer dans centre de gestion; vous devez attendre que le périphérique soit stable, puis synchroniser.

Avant de commencer

Procédure

- Étape 1** Sélectionnez **Devices (périphériques) > Device Management** (gestion des appareils) et cliquez sur **Edit** (✎) pour votre appareil défense contre les menaces . La page **Interfaces** est sélectionnée par défaut.
- Étape 2** Si nécessaire, cliquez sur **Sync Device** (synchroniser le périphérique) dans le coin supérieur gauche de **Interfaces**.
- Étape 3** Une fois les modifications détectées, passez aux étapes suivantes.

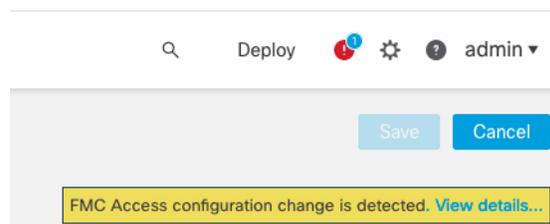
Ajout ou suppression d'interfaces physiques

- Vous verrez une bannière rouge sur les **interfaces** pour indiquer que la configuration de l'interface a été modifiée. Cliquez sur le lien **Cliquez pour en savoir plus** pour afficher les modifications apportées à l'interface.
- Cliquez sur **Validate Changes** (valider les modifications) pour vous assurer que votre politique fonctionnera toujours avec les modifications apportées à l'interface.
S'il y a des erreurs, vous devez modifier votre politique et réexécuter la validation.
- Cliquez sur **Save** (enregistrer).

Vous pouvez maintenant aller à **Deploy (déployer) > Deployment (déploiement)** afin de déployer la politique sur les appareils attribués.

L'interface d'accès FMC est modifiée.

- Vous verrez une bannière jaune dans le coin supérieur droit de la page **Périphérique** indiquant que la configuration de l'accès centre de gestion a été modifiée. Cliquez sur le lien **View Details** (Afficher les détails) pour afficher les modifications apportées à l'interface.



La boîte de dialogue **FMC Access - Configuration Details** (Détails de la configuration de l'accès à FMC) s'affiche.

- b) Prenez note de toutes les configurations en surbrillance, en particulier de celles surlignées en rouge. Vous devez faire correspondre toutes les valeurs de défense contre les menaces en les configurant manuellement sur centre de gestion.

Par exemple, les surlignages blancs ci-dessous indiquent une configuration qui existe sur le défense contre les menaces, mais pas encore sur le centre de gestion.

FMC Access - Configuration Details ? x

FMC Access configuration on device have been updated outside of FMC. Review the differences and update FMC values accordingly.

Configuration CLI Output Connection Status

Last updated: 2020-06-23 at 23:36:16 UTC [Refresh]

	Configuration on FMC	Configuration on Device
Host Name		
Method Name		
DDNS - Update Methods		
Method Type		
Web URL		
Web Update Type		
▼ 4. GigabitEthernet1/1		
Interface Configuration		
FMC Access Enabled	Disabled	Enabled
FMC Access - Allowed Networks		any
Interface Name		outside
IPv4/IPv6 Address		10.89.5.29 255.255.255.192
Static Route Configuration		
IPv4 Gateway		10.89.5.1
IPv6 Gateway		

Legend: Above configurations will be ■ added, ■ modified or ■ disassociated from FMC Access interface on next deploy to FTD.

Acknowledge Close

L'exemple suivant montre cette page après la configuration de l'interface dans centre de gestion; les paramètres de l'interface correspondent et la surbrillance rouge a été supprimée.

FMC Access - Configuration Details

FMC Access configuration on device have been updated outside of FMC. Review the differences and update FMC values accordingly.

Configuration | CLI Output | Connection Status

Last updated: 2020-06-23 at 23:36:16 UTC [Refresh]

	Configuration on FMC	Configuration on Device
DDNS - Update Methods		
Host Name		
Method Name		
Method Type		
Web URL		
Web Update Type		
▼ 4. GigabitEthernet1/1		
Interface Configuration		
FMC Access Enabled	Enabled	Enabled
FMC Access - Allowed Networks	any	any
Interface Name	outside	outside
IPv4/IPv6 Address	10.89.5.29 255.255.255.192	10.89.5.29 255.255.255.192
Static Route Configuration		
IPv4 Gateway		10.89.5.1
IPv6 Gateway		

Legend: Above configurations will be ■ added, ■ modified or ■ disassociated from FMC Access interface on next deploy to FTD.

Acknowledge Close

- c) Cliquez sur **Acknowledge** (Reconnaître).

Nous vous recommandons de ne pas cliquer sur **Reconnaître** avant d'avoir terminé la configuration centre de gestion et d'être prêt à procéder au déploiement. Cliquez sur **Reconnaître** pour supprimer le blocage lors du déploiement. Lors du prochain déploiement, la configuration centre de gestion remplacera tous les paramètres en conflit restants sur défense contre les menaces. Il est de votre responsabilité de corriger manuellement la configuration centre de gestion avant de procéder au redéploiement.

- d) Vous pouvez maintenant aller à **Deploy (déployer) > Deployment (déploiement)** afin de déployer la politique sur les appareils attribués.

Gérer le module de réseau pour Cisco Secure Firewall

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

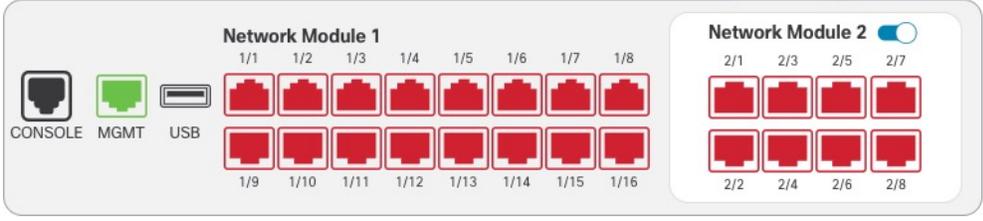
Pour afficher les détails de l'interface physique du périphérique et gérer le module de réseau, ouvrez la page **Chassis Operations** (fonctionnement du châssis). Dans la liste déroulante **Devices (Périphériques) > Device Management (Gestion des périphériques)**, cliquez sur **Manage** (Gestion) dans la colonne **Chassis** (châssis). Pour la mise en grappe ou la haute disponibilité, cette option est uniquement disponible pour le nœud de contrôle ou l'unité active. La page **Chassis Operations** (Fonctionnement du châssis) s'ouvre pour le périphérique.

Illustration 6 : Fonctionnement du châssis

172.16.0.51 (Chassis Operations)
Network module and interface breakout details for device.

Interfaces

Refresh Sync Modules



Network Module 1

1/1 1/2 1/3 1/4 1/5 1/6 1/7 1/8
1/9 1/10 1/11 1/12 1/13 1/14 1/15 1/16

Network Module 2

2/1 2/3 2/5 2/7
2/2 2/4 2/6 2/8

CONSOLE MGMT USB

Physical Interfaces

This view lists only the physical interfaces to perform chassis related advanced operations. To view complete list of physical and logical interfaces, navigate to [Interface page in device details](#)

Interface Name	Duplex	Auto Negotiation	Admin FEC	Admin Speed	Media Type
Ethernet1/1	FULL	No	AUTO	1gbps	rj45
Ethernet1/2	FULL	No	AUTO	1gbps	rj45
Ethernet1/3	FULL	No	AUTO	1gbps	rj45
Ethernet1/4	FULL	No	AUTO	1gbps	rj45

Cliquez sur **Refresh** (Actualiser) pour actualiser l'état de l'interface. Cliquez sur **Sync Modules** (synchroniser les modules) si vous avez apporté une modification matérielle sur le périphérique que vous devez détecter.

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

Configurer les ports d'éclatement

Vous pouvez configurer des ports d'épanouissement de 10 Go pour chaque interface de 40 Go ou plus. Cette procédure vous explique comment rompre et rejoindre les ports. Les ports d'épanouissement peuvent être utilisés comme n'importe quel autre port Ethernet physique, y compris lorsqu'ils sont ajoutés aux EtherChannels.

Les changements sont immédiats; vous n'avez pas besoin de déployer sur le périphérique. Après la rupture ou la jonction, vous ne pouvez pas restaurer l'état précédent de l'interface.

Avant de commencer

- Vous devez utiliser un câble épanoui pris en charge. Consultez le guide d'installation du matériel pour plus d'informations.
- L'interface ne peut pas être utilisée pour les éléments suivants avant la rupture ou la jonction :
 - lien de basculement

- Liaison de commande de la grappe
 - Ajouter une sous-interface
 - Membre de l'interface EtherChannel
 - Membre BVI
 - Interface d'accès du gestionnaire
- La rupture ou la jonction et l'interface utilisée directement dans votre politique de sécurité peuvent avoir une incidence sur la configuration. cependant, l'action n'est pas bloquée.

Procédure

Étape 1

Dans la liste déroulante **Devices (Périphériques) > Device Management (Gestion des périphériques)**, cliquez sur **Manage** (Gestion) dans la colonne **Chassis** (châssis). Pour la mise en grappe ou la haute disponibilité, cette option est uniquement disponible pour le nœud de contrôle/l'unité active; les modifications du module de réseau sont répliquées sur tous les nœuds.

Illustration 7 : Gérer le châssis

<input type="checkbox"/>	Name	Model	Version	Chassis
<input type="checkbox"/>	▼ Ungrouped (2)			
<input type="checkbox"/>	172.16.0.51 Snort 3 172.16.0.51 - Transparent	Firewall 3120 Threat Defense	7.1.0	Manage

La page **Chassis Operations** (opérations de châssis) s'ouvre pour le périphérique. Cette page affiche les détails de l'interface physique du périphérique.

Étape 2

Séparer les ports de 10 Go d'une interface de 40 Go ou plus.

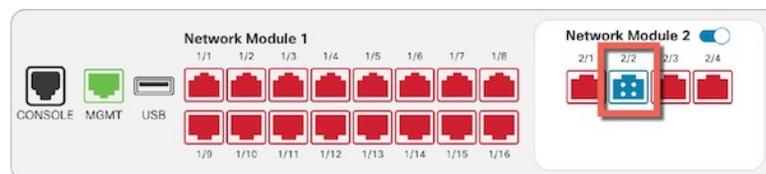
- a) cliquez sur **Rupture** (↔) à droite de l'interface.

Dans la boîte de dialogue de confirmation, cliquez sur **Yes** (Oui). Si l'interface est en cours d'utilisation, vous verrez un message d'erreur. Vous devez résoudre tous les scénarios d'utilisation avant de pouvoir réessayer la division.

Par exemple, pour diviser l'interface Ethernet2/1 40 Go, les interfaces enfants résultantes seront identifiées comme Ethernet2/1/1, Ethernet2/1/2, Ethernet2/1/3 et Ethernet2/1/4.

Sur le graphique des interfaces, un port rompu a l'aspect suivant :

Illustration 8 : Ports d'éclatement



- b) Cliquez sur le lien dans le message en haut de l'écran pour accéder à la page **Interfaces** et enregistrer les modifications à l'interface.

Illustration 9 : Aller à la page de l'interface

▲ This device has configuration changes that were performed directly on the device. Visit [Interface page in device details](#)

- c) En haut de la page **Interfaces**, cliquez sur **Cliquez pour en savoir plus**. La boîte de dialogue **Interface Changes** (modifications de l'interface) s'ouvre.

Illustration 10 : Afficher les modifications de l'interface

Interface configuration has changed on device. [Click to know more.](#)

Illustration 11 : Modifications des interfaces

Interface	Type	Change Description
Ethernet2/2	Physical	Interface is disassociated
Ethernet2/2/1	Physical	Interface is associated
Ethernet2/2/2	Physical	Interface is associated
Ethernet2/2/3	Physical	Interface is associated

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

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

Le remplacement de l'interface parente utilisée dans votre politique de sécurité peut avoir une incidence sur la configuration. Les interfaces peuvent être référencées directement à de nombreux endroits dans la configuration, notamment les règles d'accès, NAT, SSL, les règles d'identité, le VPN, le serveur DHCP, etc. La suppression d'une interface supprimera toute configuration associée à cette interface. Les politiques qui font référence aux zones de sécurité ne sont pas touchées.

- e) Cliquez sur **Close** (Fermer) pour revenir à la page **Interfaces**.
 f) Cliquez sur **Save** (Enregistrer) pour enregistrer les modifications apportées à l'interface du pare-feu.
 g) Si vous deviez modifier une configuration, allez à **Deploy > Deployment** (déployer le déploiement), puis déployez la politique.

Vous n'avez pas besoin d'effectuer le déploiement uniquement pour enregistrer les modifications apportées au port d'éclatement.

Étape 3 Rejoindre les ports d'éclatement.

Vous devez joindre tous les ports enfants de l'interface.

- a) Cliquez sur **Rejoindre** (↪) à droite de l'interface.

Dans la boîte de dialogue de confirmation, cliquez sur **Yes** (Oui). Si des ports enfants sont utilisés, vous verrez un message d'erreur. Vous devez résoudre tous les scénarios d'utilisation avant de pouvoir réessayer la jonction.

- b) Cliquez sur le lien dans le message en haut de l'écran pour accéder à la page **Interfaces** et enregistrer les modifications à l'interface.

Illustration 12 : Aller à la page de l'interface

▲ This device has configuration changes that were performed directly on the device. Visit [Interface page in device details](#)

- c) En haut de la page **Interfaces**, cliquez sur **Cliquez pour en savoir plus**. La boîte de dialogue **Interface Changes** (modifications de l'interface) s'ouvre.

Illustration 13 : Afficher les modifications de l'interface

Interface configuration has changed on device. [Click to know more.](#)

Illustration 14 : Modifications des interfaces

Interface	Type	Change Description
Ethernet2/2	Physical	Interface is disassociated
Ethernet2/2/1	Physical	Interface is associated
Ethernet2/2/2	Physical	Interface is associated
Ethernet2/2/3	Physical	Interface is associated

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

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

Le remplacement des interfaces enfants utilisées dans votre politique de sécurité peut avoir une incidence sur la configuration. Les interfaces peuvent être référencées directement à de nombreux endroits dans la configuration, notamment les règles d'accès, NAT, SSL, les règles d'identité, le VPN, le serveur DHCP, etc. La suppression d'une interface supprimera toute configuration associée à cette interface. Les politiques qui font référence aux zones de sécurité ne sont pas touchées.

- e) Cliquez sur **Close** (Fermer) pour revenir à la page **Interfaces**.
- f) Cliquez sur **Save** (Enregistrer) pour enregistrer les modifications apportées à l'interface du pare-feu.
- g) Si vous deviez modifier une configuration, allez à **Deploy > Deployment** (déployer le déploiement), puis déployez la politique.

Vous n'avez pas besoin d'effectuer le déploiement uniquement pour enregistrer les modifications apportées au port d'éclatement.

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

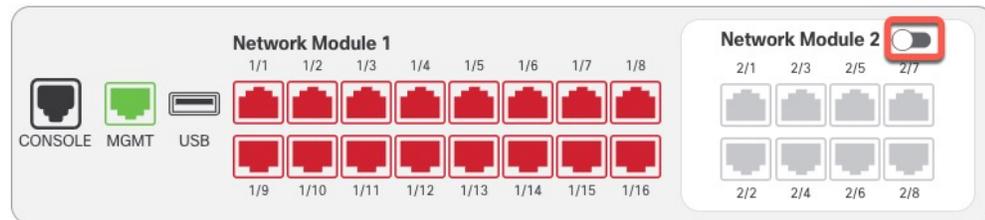
- Étape 1** Installez le module de réseau en suivant le guide d'installation du matériel.
Pour la mise en grappe ou la haute disponibilité, installez le module de réseau sur tous les nœuds.
- Étape 2** Redémarrez le pare-feu; voir [Arrêter ou redémarrer le périphérique](#).
Pour la mise en grappe ou la haute disponibilité, redémarrez d'abord les nœuds de données/l'unité de secours et attendez qu'ils se réactivent. Vous pouvez ensuite changer de nœud de contrôle ou d'unité active (voir [Modifier l'homologue actif dans la paire à haute disponibilité Défense contre les menaces](#)) et redémarrer l'ancien nœud de contrôle ou l'unité active.
- Étape 3** Dans la liste déroulante **Devices (Périphériques) > Device Management (Gestion des périphériques)**, cliquez sur **Manage** (Gestion) dans la colonne **Chassis** (châssis). Pour la mise en grappe ou la haute disponibilité, cette option est uniquement disponible pour le nœud de contrôle/l'unité active; les modifications du module de réseau sont répliquées sur tous les nœuds.

Illustration 15 : Gérer le châssis

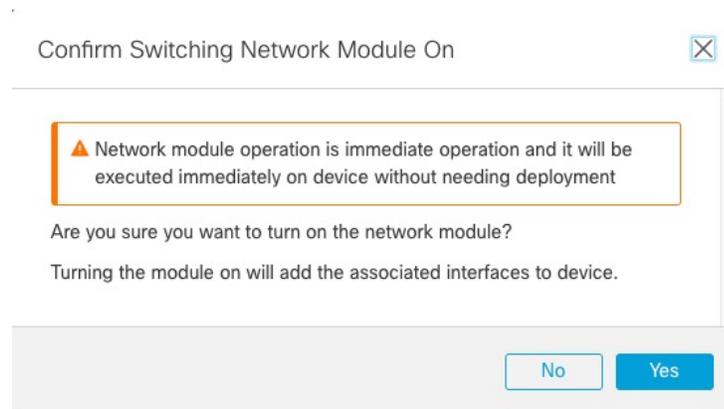
<input type="checkbox"/>	Name	Model	Version	Chassis
<input type="checkbox"/>	Ungrouted (2)			
<input type="checkbox"/>	172.16.0.51 Snort 3 172.16.0.51 - Transparent	Firewall 3120 Threat Defense	7.1.0	Manage

La page **Chassis Operations** (Fonctionnement du châssis) s'ouvre pour le périphérique. Cette page affiche les détails de l'interface physique du périphérique.

- Étape 4** Cliquez sur **Sync Modules** (synchroniser les modules) pour mettre à jour la page avec les nouveaux détails du module de réseau.
- Étape 5** Sur le graphique des interfaces, cliquez sur le curseur () pour activer le module de réseau.

Illustration 16 : Activez le module de réseau**Étape 6**

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

Illustration 17 : Confirmer l'activation**Étape 7**

Un message s'affiche en haut de l'écran. Cliquez sur le lien pour accéder à la page **Interfaces** et enregistrer les modifications apportées à l'interface.

Illustration 18 : Aller à la page de l'interface**Étape 8**

(Facultatif) En haut de la page **Interfaces**, un message indique que la configuration de l'interface a été modifiée. Vous pouvez cliquer sur **Cliquez pour en savoir plus** pour ouvrir la boîte de dialogue **Interface Changes** (Modifications d'interface) et afficher les modifications.

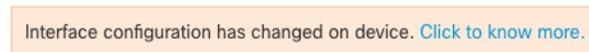
Illustration 19 : Afficher les modifications de l'interface

Illustration 20 : Modifications des interfaces

Interface Changes

The following interface changes have been detected. Click "Validate Changes" to know if there is any impact on current configuration.

Interface	Type	Change Description
Ethernet2/1	Physical	Interface is associated
Ethernet2/2	Physical	Interface is associated
Ethernet2/5	Physical	Interface is associated
Ethernet2/6	Physical	Interface is associated
Ethernet2/7	Physical	Interface is associated
Ethernet2/8	Physical	Interface is associated

Close Validate Changes

Cliquez sur **Close** (Fermer) pour revenir à la page **Interfaces**. (Comme vous ajoutez un nouveau module, il ne devrait y avoir aucune incidence sur la configuration; vous n'avez donc pas besoin de cliquer sur **Validate Changes** (Valider les modifications).)

Étape 9 Cliquez sur **Save** (Enregistrer) pour enregistrer les modifications apportées à l'interface du pare-feu.

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.

Dans le cas de la mise en grappe ou de la haute disponibilité, vous ne pouvez effectuer des opérations de châssis que sur le nœud de contrôle ou l'unité active. Vous ne pouvez pas désactiver un module de réseau si la liaison de commande de grappe ou de basculement se trouve sur le module.

Avant de commencer

Procédure

Étape 1 Pour la mise en grappe ou la haute disponibilité, procédez comme suit :

- **Mise en grappe** : assurez-vous que l'unité sur laquelle vous souhaitez effectuer l'échange à chaud est un nœud de données; puis cassez le nœud pour qu'il ne fasse plus partie de la grappe.

Vous rajouterez le nœud à la grappe après avoir effectué l'échange à chaud. Sinon, vous pouvez effectuer toutes les opérations sur le nœud de contrôle, et les modifications du module de réseau seront synchronisées avec tous les nœuds de données. Cependant, vous perdrez l'utilisation de ces interfaces sur tous les nœuds pendant l'échange à chaud.

- **Haute disponibilité** : pour éviter le basculement lorsque vous désactivez le module de réseau :

- Si le lien de basculement se trouve sur le module de réseau, vous devez interrompre la haute disponibilité. Consultez [Rompre une paire à haute disponibilité](#). La désactivation du module de réseau avec un lien de basculement actif n'est pas autorisée.
- Désactivez la surveillance des interfaces pour les interfaces du module de réseau. Consultez [Configurer les adresses IP de secours et la surveillance de l'interface](#).

Étape 2

Dans la liste déroulante **Devices (Périphériques) > Device Management (Gestion des périphériques)**, cliquez sur **Manage** (Gestion) dans la colonne **Chassis** (châssis). Pour la mise en grappe ou la haute disponibilité, cette option est uniquement disponible pour le nœud de contrôle/l'unité active; les modifications du module de réseau sont répliquées sur tous les nœuds.

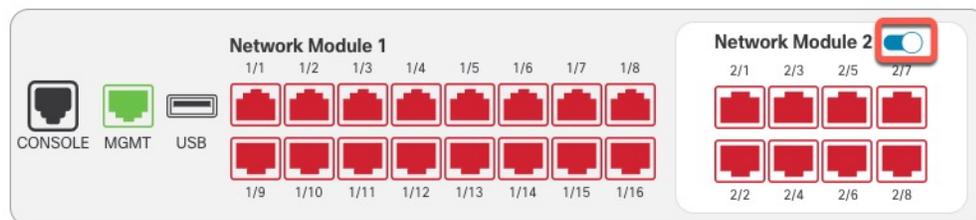
Illustration 21 : Gérer le châssis

<input type="checkbox"/>	Name	Model	Version	Chassis
<input type="checkbox"/>	▼ Ungrouped (2)			
<input type="checkbox"/>	172.16.0.51 Snort 3 172.16.0.51 - Transparent	Firewall 3120 Threat Defense	7.1.0	Manage

La page **Chassis Operations** (Fonctionnement du châssis) s'ouvre pour le périphérique. Cette page affiche les détails de l'interface physique du périphérique.

Étape 3

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

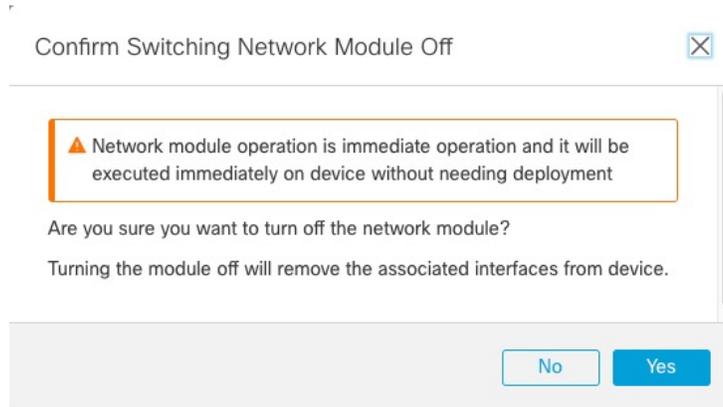
Illustration 22 : Désactiver le module de réseau

N'enregistrez aucune modification dans la page **Interfaces**. Puisque vous remplacez le module de réseau, vous ne voulez perturber aucune configuration existante.

Étape 4

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

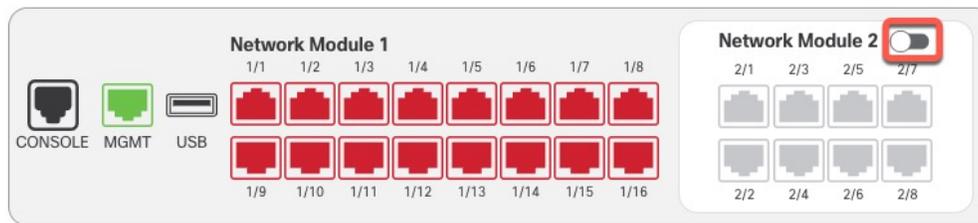
Illustration 23 : Confirmer la désactivation



Étape 5 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.

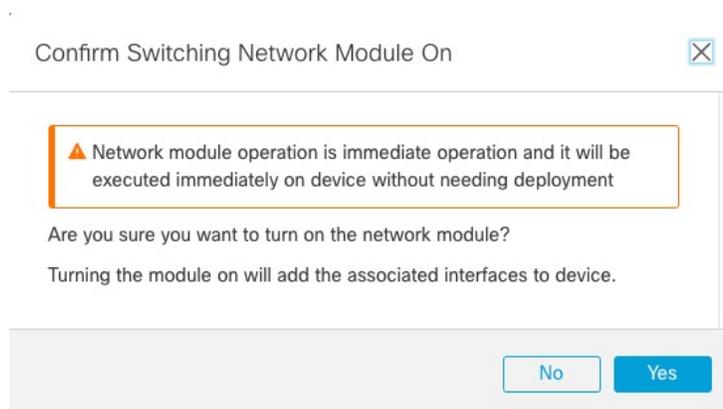
Étape 6 Dans centre de gestion, activez le nouveau module en cliquant sur le curseur ().

Illustration 24 : Activez le module de réseau



Étape 7 Vous êtes invité à confirmer que vous souhaitez activer le module de réseau. Cliquez sur **Yes** (Oui).

Illustration 25 : Confirmer l'activation



Étape 8 Pour la mise en grappe ou la haute disponibilité, procédez comme suit :

- Mise en grappe : **rajoutez** le nœud à la grappe.
- Haute disponibilité :

- Si vous avez rompu la haute disponibilité, modifiez le mode haute disponibilité. Consultez [Ajouter une paire à haute disponibilité](#).
- Réactivez la surveillance d'interface pour les interfaces sur le module de réseau. Consultez [Configurer les adresses IP de secours et la surveillance de l'interface](#).

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.

Dans le cas de la mise en grappe ou de la haute disponibilité, vous ne pouvez effectuer des opérations de châssis que sur le nœud de contrôle ou l'unité active.

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 [Rompre une paire à 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

Pour la mise en grappe ou la haute disponibilité, procédez comme suit :

- **Mise en grappe** : pour éviter les temps d'arrêt, vous pouvez casser chaque nœud un à la fois afin qu'il ne fasse plus partie de la grappe pendant que vous remplacez le module de réseau.

Vous rajouterez le nœud à la grappe après avoir effectué le remplacement.

- **Haute disponibilité** : pour éviter le basculement lorsque vous remplacez le module de réseau, désactivez la surveillance des interfaces pour les interfaces sur le module de réseau. Consultez [Configurer les adresses IP de secours et la surveillance de l'interface](#).

Étape 2

Dans la liste déroulante **Devices (Périphériques) > Device Management (Gestion des périphériques)**, cliquez sur **Manage** (Gestion) dans la colonne **Chassis** (châssis). Pour la mise en grappe ou la haute disponibilité, cette option est uniquement disponible pour le nœud de contrôle/l'unité active; les modifications du module de réseau sont répliquées sur tous les nœuds.

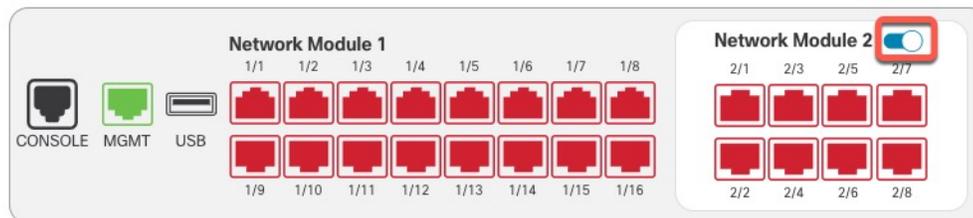
Illustration 26 : Gérer le châssis

<input type="checkbox"/>	Name	Model	Version	Chassis
<input type="checkbox"/>	Ungrouted (2)			
<input type="checkbox"/>	172.16.0.51 Short 3 172.16.0.51 - Transparent	Firewall 3120 Threat Defense	7.1.0	Manage

La page **Chassis Operations** (Fonctionnement du châssis) s'ouvre pour le périphérique. Cette page affiche les détails de l'interface physique du périphérique.

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

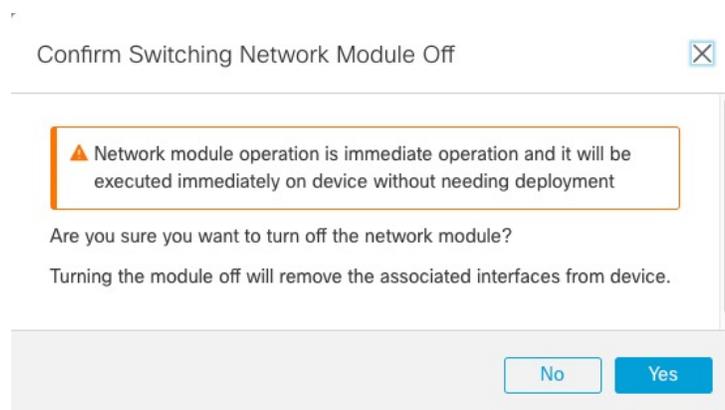
Illustration 27 : Désactiver le module de réseau



N'enregistrez aucune modification dans la page **Interfaces**. Puisque vous remplacez le module de réseau, vous ne voulez perturber aucune configuration existante.

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

Illustration 28 : Confirmer la désactivation



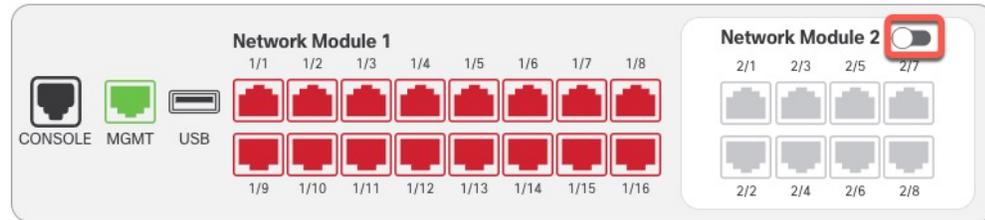
Étape 5 Sur le périphérique, retirez l'ancien module de réseau et remplacez-le par le nouveau module de réseau en suivant le guide d'installation du matériel.

Étape 6 Redémarrez le pare-feu; voir [Arrêter ou redémarrer le périphérique](#).

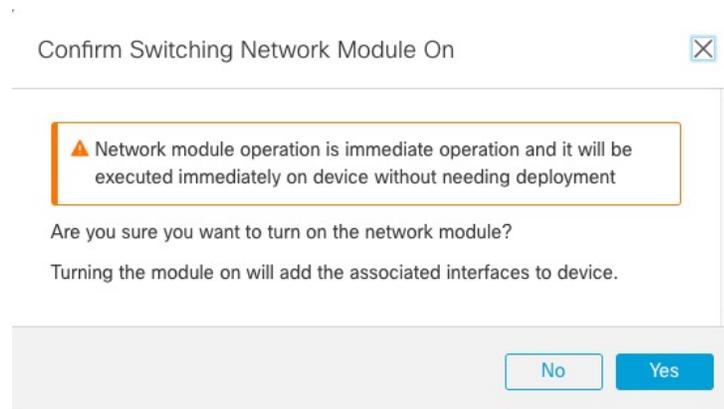
Pour la mise en grappe ou la haute disponibilité, redémarrez d'abord les nœuds de données/l'unité de secours et attendez qu'ils se réactivent. Vous pouvez ensuite changer de nœud de contrôle ou d'unité active (voir [Modifier l'homologue actif dans la paire à haute disponibilité Défense contre les menaces](#)) et redémarrer l'ancien nœud de contrôle ou l'unité active.

Étape 7 Dans centre de gestion, cliquez sur **Sync Modules** (synchroniser les modules) pour mettre à jour la page avec les nouveaux détails du module de réseau.

Étape 8 Activez le nouveau module en faisant glisser le curseur ()

Illustration 29 : Activez le module de réseau**Étape 9**

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

Illustration 30 : Confirmer l'activation**Étape 10**

Cliquez sur le lien dans le message en haut de l'écran pour accéder à la page **Interfaces** et enregistrer les modifications à l'interface.

Illustration 31 : Aller à la page de l'interface**Étape 11**

Si le module de réseau compte *moins* d'interfaces :

- a) En haut de la page **Interfaces**, cliquez sur **Cliquez pour en savoir plus**. La boîte de dialogue **Interface Changes** (modifications de l'interface) s'ouvre.

Illustration 32 : Afficher les modifications de l'interface

Illustration 33 : Modifications des interfaces

Interface Changes

The following interface changes have been detected. Click "Validate Changes" to know if there is any impact on current configuration.

Interface	Type	Change Description
Ethernet2/1	Physical	Interface is associated
Ethernet2/2	Physical	Interface is associated
Ethernet2/5	Physical	Interface is associated
Ethernet2/6	Physical	Interface is associated
Ethernet2/7	Physical	Interface is associated
Ethernet2/8	Physical	Interface is associated

Close Validate Changes

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

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

La suppression d'une interface utilisée dans votre politique de sécurité peut avoir une incidence sur la configuration. Les interfaces peuvent être référencées directement à de nombreux endroits dans la configuration, notamment les règles d'accès, NAT, SSL, les règles d'identité, le VPN, le serveur DHCP, etc. La suppression d'une interface supprimera toute configuration associée à cette interface. Les politiques qui font référence aux zones de sécurité ne sont pas touchées.

- c) Cliquez sur **Close** (Fermer) pour revenir à la page **Interfaces**.

Étape 12

Pour modifier la vitesse de l'interface, consultez [Activer l'interface physique et configurer des paramètres Ethernet](#), à la page 7.

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 13

Cliquez sur **Save** (Enregistrer) pour enregistrer les modifications apportées à l'interface du pare-feu.

Étape 14

Si vous deviez modifier une configuration, allez à **Deploy > Deployment** (déployer le déploiement), puis déployez la politique.

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

Étape 15

Pour la mise en grappe ou la haute disponibilité, procédez comme suit :

- Mise en grappe : **rajoutez** le nœud à la grappe.
- **Haute disponibilité** : réactiver la surveillance d'interface pour les interfaces sur le module de réseau. Consultez [Configurer les adresses IP de secours et la surveillance de l'interface](#).

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.

Dans le cas de la mise en grappe ou de la haute disponibilité, vous ne pouvez effectuer des opérations de châssis que sur le nœud de contrôle ou l'unité active.

Avant de commencer

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

Procédure

Étape 1

Dans la liste déroulante **Devices (Périphériques) > Device Management (Gestion des périphériques)**, cliquez sur **Manage (Gestion)** dans la colonne **Chassis (châssis)**. Pour la mise en grappe ou la haute disponibilité, cette option est uniquement disponible pour le nœud de contrôle/l'unité active; les modifications du module de réseau sont répliquées sur tous les nœuds.

Illustration 34 : Gérer le châssis

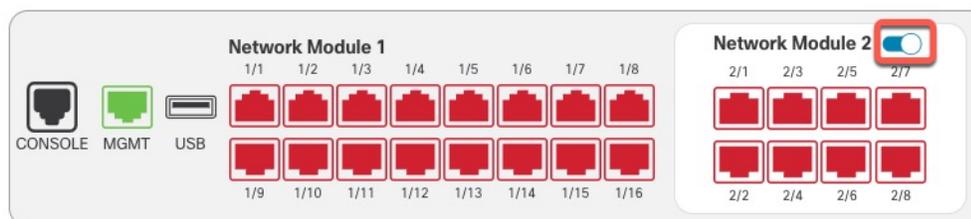
<input type="checkbox"/>	Name	Model	Version	Chassis
<input type="checkbox"/>	Ungrouped (2)			
<input type="checkbox"/>	172.16.0.51 Snort 3 172.16.0.51 - Transparent	Firewall 3120 Threat Defense	7.1.0	Manage

La page **Chassis Operations (Fonctionnement du châssis)** s'ouvre pour le périphérique. Cette page affiche les détails de l'interface physique du périphérique.

Étape 2

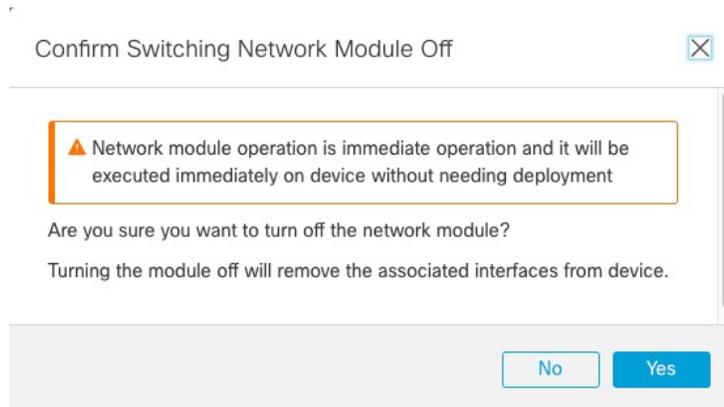
Sur le graphique des interfaces, cliquez sur le curseur  pour désactiver le module de réseau.

Illustration 35 : 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 36 : Confirmer la désactivation

Étape 4 Un message s'affiche en haut de l'écran. Cliquez sur le lien pour accéder à la page **Interfaces** et enregistrer les modifications apportées à l'interface.

Illustration 37 : Aller à la page de l'interface

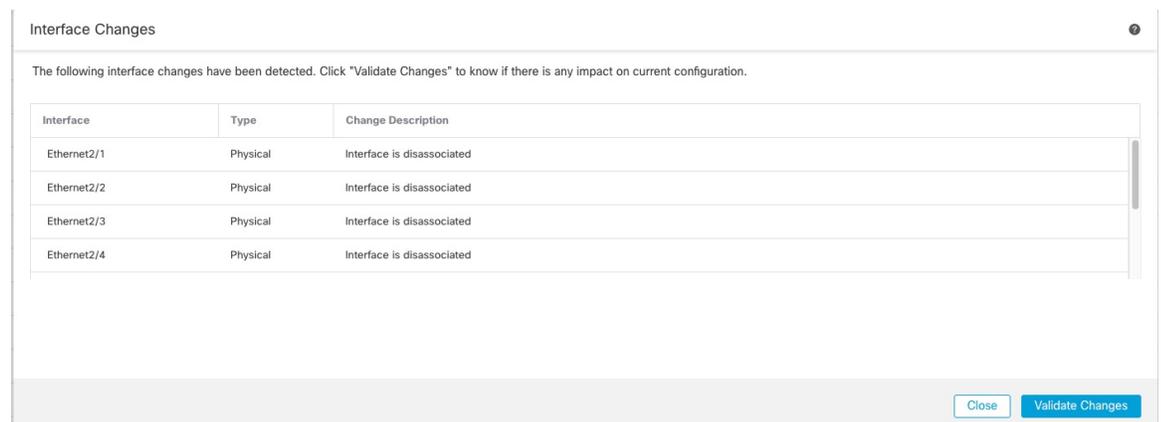
▲ This device has configuration changes that were performed directly on the device. Visit [Interface page in device details](#)

Étape 5 En haut de la page **Interfaces**, un message indique que la configuration de l'interface a été modifiée.

Illustration 38 : Afficher les modifications de l'interface

Interface configuration has changed on device. [Click to know more.](#)

a) Cliquez sur **pour en savoir plus** pour ouvrir la boîte de dialogue **Interface Changes** et afficher les modifications de l'interface.

Illustration 39 : Modifications des interfaces

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

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

La suppression d'une interface utilisée dans votre politique de sécurité peut avoir une incidence sur la configuration. Les interfaces peuvent être référencées directement à de nombreux endroits dans la configuration, notamment les règles d'accès, NAT, SSL, les règles d'identité, le VPN, le serveur DHCP, etc. La suppression d'une interface supprimera toute configuration associée à cette interface. Les politiques qui font référence aux zones de sécurité ne sont pas touchées.

c) Cliquez sur **Close** (Fermer) pour revenir à la page **Interfaces**.

Étape 6 Cliquez sur **Save** (Enregistrer) pour enregistrer les modifications apportées à l'interface du pare-feu.

Étape 7 Si vous deviez modifier une configuration, allez à **Deploy > Deployment** (déployer le déploiement), puis déployez la politique.

Étape 8 Redémarrez le pare-feu; voir [Arrêter ou redémarrer le périphérique](#).

Pour la mise en grappe ou la haute disponibilité, redémarrez d'abord les nœuds de données/l'unité de secours et attendez qu'ils se réactivent. Vous pouvez ensuite changer de nœud de contrôle ou d'unité active (voir [Modifier l'homologue actif dans la paire à haute disponibilité Défense contre les menaces](#)) et redémarrer l'ancien nœud de contrôle ou l'unité active.

Historique des interfaces

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Correction de transfert d'erreurs par défaut sur les ports fixes du pare-feu 3100 modifié pour l'article 108 de la RS-FEC au lieu de l'article 74 de la FC-FEC pour les émetteurs-récepteurs SR, CSR et LR de 25 Go et plus	N'importe lequel	7.2.4/7.3	Lorsque vous définissez la FEC sur Auto sur les ports fixes de Cisco Secure Firewall 3100, le type par défaut est désormais l'article 108 RS-FEC au lieu de l'article 74 FC-FEC pour les émetteurs-récepteurs SR, CSR et LR de 25 Go+. Plateformes prises en charge : Cisco Secure Firewall 3100
Prise en charge de LLDP pour Firepower 2100et Secure Firewall 3100	N'importe lequel	7.2	Vous pouvez activer le protocole LLDP (Link Layer Discovery Protocol) pour les interfaces Firepower 2100 et Secure Firewall 3100. Écrans Nouveaux ou modifiés : Périphériques > Gestion des périphériques > Interfaces > Configuration matérielle > Connectivité du réseau Commandes nouvelles ou modifiées : show lldp status, show lldp neighbors, show lldp statistics Plates-formes prises en charge : Firepower 2100 , Secure Firewall 3100

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Mettre en pause les trames pour le contrôle de flux sur Cisco Secure Firewall 3100	N'importe lequel	7.2	<p>S'il y a une rafale de trafic, des paquets abandonnés peuvent se produire si la rafale dépasse la capacité de mise en mémoire tampon de la mémoire tampon FIFO sur la carte réseau et les mémoires tampons des anneaux de réception. L'activation des trames de pause pour le contrôle de flux peut atténuer ce problème.</p> <p>Écrans nouveaux ou modifiés : Périphériques > Gestion des périphériques > Interfaces > Configuration matérielle > Connectivité du réseau</p> <p>Plateformes prises en charge : Cisco Secure Firewall 3100</p>
Prise en charge de la correction d'erreurs sans voie de retour pour Cisco Secure Firewall 3100	N'importe lequel	7.1	<p>Les interfaces de Cisco Secure Firewall 3100 25 Gbit/s prennent en charge la correction d'erreurs sans voie de retour (FEC). La FEC est activée par défaut et définie sur Auto.</p> <p>Écrans nouveaux ou modifiés : Périphériques > Gestion des périphériques > Interfaces > Modifier l'interface physique > Configuration du matériel</p>
Prise en charge du réglage de la vitesse en fonction du SFP pour Secure Firewall 3100	N'importe lequel	7.1	<p>Le pare-feu Secure Firewall 3100 prend en charge la détection de la vitesse pour les interfaces basées sur SFP installées. La détection de SFP est activée par défaut. 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.</p> <p>Écrans nouveaux ou modifiés : Périphériques > Gestion des périphériques > Interfaces > Modifier l'interface physique > Configuration du matériel</p>
Prise en charge de LLDP pour le périphérique Firepower 1100	N'importe lequel	7.1	<p>Vous pouvez activer le protocole LLDP (Link Layer Discovery Protocol) pour les interfaces Firepower 1100.</p> <p>Écrans nouveaux ou modifiés : Périphériques > Gestion des périphériques > Interfaces > Configuration du matériel > LLDP</p> <p>Commandes nouvelles ou modifiées : show lldp status, show lldp neighbors, show lldp statistics</p> <p>Plateformes prises en charge : Firepower 1100</p>
La négociation automatique de l'interface est maintenant définie indépendamment de la vitesse et du mode duplex, et la synchronisation de l'interface a été améliorée	N'importe lequel	7.1	<p>La négociation automatique de l'interface est désormais définie indépendamment de la vitesse et du mode duplex. En outre, lorsque vous synchronisez les interfaces dans centre de gestion, les modifications matérielles sont détectées plus efficacement.</p> <p>Écrans nouveaux ou modifiés : Périphériques > Gestion des périphériques > Interfaces > Configuration du matériel > Vitesse</p> <p>Plates-formes prises en charge : Firepower 1000/2100, Secure Firewall 3100</p>

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
<p>Les interfaces à fibre optique des séries Firepower 1100/2100 prennent désormais en charge la désactivation de la négociation automatique.</p>	<p>N'importe lequel</p>	<p>6.7</p>	<p>Vous pouvez maintenant configurer une interface à fibre optique des gammes Firepower 1100/2100 pour désactiver le contrôle de flux et la négociation de l'état de la liaison.</p> <p>Auparavant, lorsque vous définissiez la vitesse de l'interface à fibre optique (1 000 ou 10 000 Mbit/s) sur ces périphériques, le contrôle de flux et la négociation de l'état de la liaison étaient automatiquement activés. Vous ne pouvez pas le désactiver.</p> <p>Vous pouvez maintenant désélectionner la négociation automatique et régler la vitesse à 1000 pour désactiver le contrôle de flux et la négociation de l'état de la liaison. Vous ne pouvez pas désactiver la négociation à 10 000 Mbit/s.</p> <p>Écrans nouveaux ou modifiés : Périphériques > Gestion des périphériques > Interfaces > Configuration du matériel > Vitesse</p> <p>Plateformes prises en charge : Firepower 1100 et 2100</p>

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d'incohérence, la version anglaise du présent contenu prévaudra.