

Configuration de l'interface de base

Ce chapitre comprend la configuration de l'interface de base, y compris les paramètres Ethernet et la configuration de la trame étendue.

Remarque Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Si vous n'êtes pas déjà dans l'espace d'exécution système, dans le volet Configuration > Device List (Liste des périphériques), double-cliquez sur **System (système)** sous l'adresse IP du périphérique actif.

Remarque Pour Firepower 2100 en mode plateforme et Châssis Firepower 4100/9300 , vous devez configurer les paramètres de l'interface de base dans le système d'exploitation FXOS. Consultez le guide de configuration ou de démarrage de votre châssis pour en savoir plus.

- À propos de la configuration de l'interface de base, à la page 1
- Lignes directrices pour la configuration de l'interface de base, à la page 4
- Paramètres par défaut pour la configuration de l'interface de base, à la page 4
- Activer l'interface physique et configurer les paramètres Ethernet, à la page 5
- Activez la prise en charge des bâtis grand format (ASA virtuel et ISA 3000), à la page 8
- Gérer le module réseau pour Cisco Secure Firewall 3100, à la page 9
- Exemples d'interfaces de base, à la page 13
- Historique de la configuration de l'interface de base, à la page 14

À propos de la configuration de l'interface de base

Cette section décrit les fonctionnalités de l'interface et les interfaces spéciales.

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.

Interface de gestion

L'interface de gestion, selon votre modèle, est une interface distincte réservée au trafic de gestion.

Présentation de l'interface de gestion

Vous pouvez gérer l'ASA en vous connectant à :

- Toute interface de trafic entrant
- Une interface *logement*/*port* de gestion dédiée (si disponible pour votre modèle)

Vous devrez peut-être configurer l'accès de gestion à l'interface en fonction de l'Accès de gestion.

L'interface de *logement*/*port* de gestion

Le tableau suivant présente les interfaces de gestion par modèle.

Tableau 1 : Interfaces de gestion par modèle

Modèle	Management 0/0	Management 0/1	Management 1/0	Management 1/1	Configurable pour le trafic de transit	Sous-interfaces autorisées
Firepower 1000	—	—	—	**Oui**	**Oui**	**Oui**
Firepower de la série 2100	—	—	—	**Oui**	— **Remarque :** techniquement, vous pouvez activer le trafic de transit; toutefois, le débit de cette interface n'est pas suffisant pour les opérations de données.	**Oui**
Secure Firewall 3100	—	—	—	**Oui**	**Oui**	**Oui**

Modèle	Management 0/0	Management 0/1	Management 1/0	Management 1/1	Configurable pour le trafic de transit	Sous-interfaces autorisées
Firepower 4100/9300	S. O. L'ID d'interface dépend de l'interface physique de type gestion que vous avez attribuée au périphérique logique ASA	—	—	—	—	**Oui**
ISA 3000	—	—	—	**Oui**	—	—
ASAv	**Oui**	—	—	—	**Oui**	—

Utiliser n'importe quelle interface pour le trafic de gestion uniquement

Vous pouvez utiliser n'importe quelle interface comme interface de gestion uniquement en la configurant pour le trafic de gestion, y compris une interface EtherChannel.

Interface de gestion pour le mode transparent

En mode de pare-feu transparent, en plus du nombre maximum d'interfaces de trafic autorisé, vous pouvez également utiliser l'interface de gestion (l'interface physique ou une sous-interface (si prise en charge par votre modèle)) en tant qu'interface de gestion distincte uniquement.

Vous ne pouvez pas utiliser d'autres types d'interfaces comme interfaces de gestion.

Pour le Châssis Firepower 4100/9300 , l'ID de l'interface de gestion dépend de l'interface de type gestion que vous avez attribuée au périphérique logique ASA.

Remarque L'interface de gestion ne fait pas partie d'un groupe de ponts normal. Notez que pour des raisons opérationnelles, elle fait partie d'un groupe de ponts non configurable.

Trafic de gestion uniquement

L'interface de gestion traite uniquement le trafic entrant et sortant et ne peut pas transmettre de trafic de transit. Dans tous les cas, comme les groupes de ponts ne peuvent pas communiquer avec d'autres groupes de ponts, il serait impossible à l'interface de gestion d'acheminer vers un groupe de ponts, ou inversement, même si elle prenait en charge le trafic.

Tableau d'adresses MAC partagées et connexions de commutateurs

En mode de pare-feu transparent, l'interface de gestion met à jour le tableau d'adresses MAC de l'ASA de la même manière qu'une interface de données; par conséquent, vous ne devez pas connecter à la fois une interface de gestion et une interface de données au même commutateur, sauf si vous configurez l'un des ports de commutation en tant que port routé (par défaut, les commutateurs Catalyst partagent une adresse MAC pour

tous les ports de commutation VLAN). Sinon, si le trafic arrive sur l'interface de gestion à partir du commutateur physiquement connecté, l'ASA met à jour le tableau d'adresses MAC pour utiliser l'interface de *gestion* pour accéder au commutateur, au lieu de l'interface de données. Cette action entraîne une interruption temporaire du trafic; pour des raisons de sécurité, l'ASA ne mettra pas à jour le tableau d'adresses MAC pour les paquets du commutateur vers l'interface de données pendant au moins 30 secondes.

Mode contexte multiple

En mode de contexte multiple, vous ne pouvez partager aucune interface, y compris l'interface de gestion, entre les contextes. Pour assurer la gestion par contexte sur les modèles pris en charge, vous pouvez créer des sous-interfaces de l'interface de gestion et attribuer une sous-interface de gestion à chaque contexte. Certains modèles n'autorisent pas les sous-interfaces sur l'interface de gestion. Par conséquent, la gestion par contexte pour ces modèles nécessite que vous vous connectiez à une interface de données. Pour le Châssis Firepower 4100/9300 , l'interface de gestion et ses sous-interfaces ne sont pas reconnues comme des interfaces de gestion spécialement autorisées dans les contextes; vous devez traiter une sous-interface de gestion comme une interface de données dans ce cas et l'ajouter à une BVI.

Lignes directrices pour la configuration de l'interface de base

Mode de pare-feu transparent

Pour le contexte multiple, en mode transparent, chaque contexte doit utiliser des interfaces différentes; vous ne pouvez pas partager une interface entre contextes.

Basculement

Vous ne pouvez pas partager une interface de basculement ou d'état avec une interface de données.

Directives supplémentaires

- Certains services liés à la gestion ne sont pas disponibles jusqu'à ce qu'une interface de non-gestion soit activée et que l'ASA atteigne l'état « Système prêt ». L'ASA génère le message de journal système suivant lorsqu'il est à l'état « Système prêt » :

```
%ASA-6-199002: Startup completed.  Beginning operation.
```

Paramètres par défaut pour la configuration de l'interface de base

Cette section répertorie les paramètres par défaut des interfaces si vous n'avez pas de configuration d'usine par défaut.

État par défaut des interfaces

L'état par défaut d'une interface dépend du type d'interface et du mode de contexte.

En mode de contexte multiple, toutes les interfaces allouées sont activées par défaut, quel que soit l'état de l'interface dans l'espace d'exécution du système. Cependant, pour que le trafic passe par l'interface, celle-ci

doit également être activée dans l'espace d'exécution du système. Si vous désactivez une interface dans l'espace d'exécution du système, cette interface est désactivée dans tous les contextes qui la partagent.

En mode unique ou dans l'espace d'exécution du système, les interfaces ont les états par défaut suivants :

- Interfaces physiques : désactivées.
- Sous-interfaces VLAN : activées. Cependant, pour que le trafic passe par la sous-interface, l'interface physique doit également être activée.
- Interfaces VXLAN VNI : activées.
- 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 (autres modèles) : désactivées.

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

Vitesse par défaut et duplex

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

Type de connecteur par défaut

Certains modèles comprennent deux types de connecteurs : le RJ-45 en cuivre et le SFP à fibre optique. RJ-45 est le type par défaut. Vous pouvez configurer l'ASA pour utiliser les connecteurs SFP à fibre optique.

Adresses MAC par défaut

Par défaut, l'interface physique utilise l'adresse MAC rémanente, et toutes les sous-interfaces d'une interface physique utilisent la même adresse MAC rémanente.

Activer l'interface physique et configurer les paramètres Ethernet

Cette section décrit comment :

- Activer l'interface physique
- Définir une vitesse et un duplex (si disponible)
- Activer les trames de pause pour le contrôle de flux
- Configuration de la correction d'erreurs sans voie de retour

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. Les options d'interface exactes varient selon votre modèle et votre type d'interface.

Remarque Pour le Firepower 4100/9300, vous configurez les paramètres de base de l'interface dans FXOS.

Remarque Pour les ports de commutation / 1010/ , consultez Configuration de base de l'interface pour les ports de commutation du Firepower 1010.

Avant de commencer

Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Si vous n'êtes pas déjà en mode de configuration système, dans le volet **Configuration** > **Device List (Liste des périphériques)**, double-cliquez sur **System** (Système) sous l'adresse IP du périphérique actif.

Procédure

Étape 1 Selon votre mode de contexte :

- Pour le mode unique, choisissez le volet **Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces**.
- Pour le mode multiple dans l'espace d'exécution du système, choisissez le volet **Configuration > Context Management (Gestion des contextes) > Interfaces** .

Par défaut, toutes les interfaces physiques sont répertoriées.

Étape 2 Cliquez sur une interface physique que vous souhaitez configurer, puis cliquez sur **Edit** (Modifier).

La boîte de dialogue **Edit Interface** (Modifier l'interface) s'affiche.

Remarque En mode unique, cette procédure ne couvre qu'un sous-ensemble des paramètres de la boîte de dialogue **Edit Interface** (Modifier l'interface). Notez qu'en mode de contexte multiple, avant de terminer la configuration de l'interface, vous devez attribuer des interfaces aux contextes.

Étape 3 Pour activer l'interface, cochez la case **Enable Interface** (Activer l'interface).

Étape 4 Pour ajouter une description, saisissez du texte dans le champ Description.

La description peut contenir jusqu'à 240 caractères sur une seule ligne (sans retour chariot). Dans le cas d'une liaison de basculement ou d'état, la description fixe est « LAN Failover Interface », « STATE Failover Interface » ou « LAN/STATE Failover Interface » par exemple. Vous ne pouvez pas modifier cette description. La description fixe remplace toute description que vous saisissez ici si vous faites de cette interface une liaison de basculement ou un lien d'état.

Étape 5 Pour activer les trames de pause (XOFF) pour le contrôle de flux, cochez la case **Flow-Control** (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 ASA 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 L'ASA 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 6 (Facultatif) Pour définir le type de support, les conditions de duplex, la vitesse et activer les trames de pause pour le contrôle de flux, cliquez sur **Configure Hardware Properties** (Configurer les propriétés matérielles).

a) Pour définir les conditions de **duplex**, choisissez **Full** (Intégral), **Half** (Semi-duplex) ou **Auto** (Automatique), selon le type d'interface dans la liste déroulante.



Remarque Les interfaces SFP prennent uniquement en charge les conditions de duplex intégral.

b) Pour définir la **vitesse**, choisissez une valeur dans la liste déroulante (varie selon le modèle).

Pour les interfaces SFP Firepower 1000 et 2100, le paramètre **Negotiate** définit la vitesse à 1 000 Mbit/s et active la négociation de liaison pour les paramètres de contrôle de flux et les renseignements sur les défaillances à distance. Pour les interfaces de 10 Gbit/s, cette option définit la vitesse à 1 000 Mbit/s. L'option **Nonegotiate** (Aucune négociation) désactive la négociation de liaison.Pour d'autres options de négociation automatique de modèle, consultez la case **Auto-negotiate** (Négociation automatique) de l'onglet **Advanced** (Avancé), qui vous permet d'activer ou de désactiver la négociation automatique sur toute interface de 1 000 Mbit/s et plus.

Choisissez **Detect SFP** (Détecter SFP) pour détecter la vitesse du module SFP installé et utiliser la vitesse appropriée. Le duplex est toujours réglé sur intégral, la négociation automatique est activée et la FEC est réglée sur Auto Pour les émetteurs-récepteurs à double vitesse, la vitesse inférieure est utilisée. 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. Certains commutateurs et émetteurs-récepteurs

ne prennent pas en charge la négociation automatique, en particulier pour les interfaces à vitesse plus élevée. Dans ce cas, réglez l'interface ASA à une vitesse manuelle et désactivez également **Auto-negotiate** (Négociation automatique) afin que la liaison puisse s'établir.

c) Pour définir le **FEC Mode** (Mode de correction d'erreurs sans voie de retour) pour les interfaces de 25 Gbit/s et plus, choisissez une valeur dans la liste déroulante.

Pour une interface membre d'EtherChannel, vous devez configurer la correction d'erreur directe avant de l'ajouter à l'EtherChannel. Si vous supprimez l'interface de l'EtherChannel, après le redémarrage, vous devrez peut-être reconfigurer la FEC pour l'interface.

Certains commutateurs ne prennent pas en charge le mode automatique pour la FEC, en particulier pour les interfaces de plus grande taille. Assurez-vous de désactiver la FEC ou de configurer manuellement le paramètre, en fonction de la prise en charge du commutateur.

Le paramètre choisi lorsque vous utilisez **auto** dépend du type d'émetteur-récepteur et selon si l'interface est fixe (intégrée) ou sur un module de réseau.

Tableau 2 : FEC par défaut pour le réglage automatique

Type d'émetteur/récepteur	FEC par défaut du port fixe	FEC par défaut du module de réseau
25G-SR	cl108-rs	cl108-rs
25G-LR	cl108-rs	cl108-rs
10/25G-CSR	cl108-rs	cl74-fc
25G-AOC*x*M	cl74-fc	cl74-fc
25G-CU2.5/3M	Négociation automatique	Négociation automatique
25G-CU4/5M	Négociation automatique	Négociation automatique

d) Cliquez sur **OK** pour accepter les modifications apportées aux **Hardware Properties** (Propriétés matérielles).

Étape 7 Cliquez sur **OK** pour accepter les modifications apportées à l'**Interface**.

Activez la prise en charge des bâtis grand format (ASA virtuel et ISA 3000)

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 activer la prise en charge des trames étendues pour toutes les interfaces en augmentant la quantité de mémoire nécessaire pour traiter les trames Ethernet. L'attribution de plus de mémoire aux trames étendues peut limiter l'utilisation maximale d'autres fonctionnalités, telles que les listes de contrôle d'accès. Remarque : la MTU ASA définit la taille de la charge utile sans inclure la couche 2 (14 octets) et l'en-tête VLAN (4 octets), donc la MTU maximale peut s'élever à 9198, selon votre modèle.

Cette procédure s'applique uniquementà l'ISA 3000, et à l'ASA virtuel. D'autres modèles prennent en charge les bâtis grand format par défaut.

Les bâtis grand format ne sont pas pris en charge sur les ASAv5 et ASAv10 avec moins de 8 Go de RAM.

Avant de commencer

- En mode contexte multiple, définissez cette option dans l'espace d'exécution du système.
- Les modifications de ce paramètre nécessitent que vous rechargiez l'ASA.
- Assurez-vous de définir la MTU pour chaque interface devant transmettre des trames étendues à une valeur supérieure à la valeur par défaut 1500; par exemple, définissez la valeur sur 9198. En mode contexte multiple, définissez la MTU dans chaque contexte.
- Veillez à régler le TCP MSS, soit pour le désactiver pour le trafic non-IPsec, soit pour l'augmenter en fonction de la MTU.

Procédure

Selon votre mode de contexte :

- Mode multiple : Pour activer la prise en charge des trames étendues, sélectionnez **Configuration > Context Management (gestion de contexte) > Interfaces**, puis cliquez **Enable jumbo frame support**.
- Mode simple : Le réglage de la MTU à plus de 1500 octets active automatiquement les trames étendues. Pour activer ou désactiver manuellement ce paramètre, sélectionnez **Configuration > Device Setup (configuration du périphérique) > Interface Settings (paramètres de l'interface) > Interfaces**, puis cliquez dans la case à cocher **Enable jumbo frame support**.

Gérer le module 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.

Configurer les ports d'éclatement

Vous pouvez configurer des ports d'éclatement plus petits pour chaque interface de 40 Gbit/s ou plus. Cette procédure vous indique comment diviser et regrouper les ports. Les ports d'éclatement peuvent être utilisés comme n'importe quel autre port Ethernet physique, y compris lorsqu'ils sont ajoutés aux EtherChannels. Par exemple, vous pouvez répartir quatre ports de 10 Gbit/s à partir d'une interface de 40 Gbit/s. La taille exacte et le nombre de ports dépendent de votre modèle.

Si une interface est déjà utilisée dans votre configuration, vous devrez supprimer manuellement toute configuration liée aux interfaces qui ne seront plus présentes.

Avant de commencer

- Vous devez utiliser un câble épanoui pris en charge. Consultez le guide d'installation du matériel pour plus d'informations.
- Pour la mise en grappe ou le basculement, assurez-vous que la liaison de basculement n'utilise pas l'interface parent (pour la séparation) ou l'interface enfant (pour la jonction); vous ne pouvez pas apporter de modifications à l'interface si elle est utilisée pour la liaison de grappe/basculement.

Procédure

Étape 1 Séparez les ports à partir d'une ou plusieurs interfaces de 40 Go ou plus en sélectionnant **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **EPM**, et en saisissant un ou plusieurs **Port Numbers** (Numéros de port) que vous souhaitez diviser, séparés par des virgules (sans espace).

Le logement est toujours **2**.

Par exemple, pour séparer les interfaces Ethernet2/1 et Ethernet 2/2, vous devez spécifier **1,2** dans le champ **Port Number** (Numéro de port). Les interfaces enfants résultantes seront identifiées comme Ethernet2/1/1, Ethernet2/1/2, Ethernet2/1/3, Ethernet2/1/4, Ethernet2/2/1, Ethernet2/2/2, Ethernet2/2/3 et Ethernet2/2/4.

Pour la mise en grappe ou le basculement, effectuez cette étape sur le nœud de contrôle/l'unité active; les modifications d'interface sont répliquées sur les autres nœuds.

Étape 2 Joignez les ports d'éclatement pour restaurer l'interface en sélectionnant **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **EPM**, et en supprimant un ou plusieurs **Port Numbers** (Numéros de port).

Pour la mise en grappe ou le basculement, effectuez cette étape sur le nœud de contrôle/l'unité active; l'état du module est répliqué sur les autres nœuds.

Vous devez joindre tous les ports enfants d'une interface donnée.

Étape 3 Cliquez sur **Apply** (Appliquer).

La configuration est appliquée au pare-feu.

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 rechargement. Pour la mise en grappe ou le basculement, aucun temps d'arrêt n'est pris en charge. Veuillez donc vous assurer d'effectuer cette procédure pendant une fenêtre de maintenance.

Procédure

Étape 1 Installez le module de réseau en suivant le guide d'installation du matériel. Vous pouvez installer le module de réseau lorsque le pare-feu est sous tension.

Pour la mise en grappe ou le basculement, installez le module de réseau sur tous les nœuds.

Étape 2 Rechargez le pare-feu; consultez **Tools (Outils) > System Reload (Rechargement du système)**.

Pour la mise en grappe ou le basculement, rechargez tous les nœuds. Étant donné que les nœuds dotés de modules de réseau différents ne peuvent pas rejoindre la paire de grappe/basculement, vous devez recharger tous les nœuds avec le nouveau module avant qu'ils puissent reformer la paire de grappe/basculement.

Étape 3 Activez le module de réseau en choisissant **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **EPM** et en décochant **Disable Netmod** (Désactiver Netmod).

Pour la mise en grappe ou le basculement, effectuez cette étape sur le nœud de contrôle/l'unité active; l'état du module est répliqué sur les autres nœuds.

Étape 4 Cliquez sur **Apply** (Appliquer).

La configuration est appliquée au 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 recharger. 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.

Pour la mise en grappe ou le basculement, vous ne pouvez pas désactiver un module de réseau si la liaison de commande de grappe ou de basculement se trouve sur le module.

Procédure

Étape 1 Pour la mise en grappe ou le basculement, 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 (voir Modifier le nœud de contrôle); puis désactivez la mise en grappe sur le nœud. Reportez-vous aux sections Devenir un nœud inactif ou Désactiver un nœud de données du nœud de contrôle.

  Si la liaison de commande de grappe se trouve sur le module de réseau, vous devez quitter la grappe. Consultez Quitter la grappe. La désactivation du module de réseau avec une liaison de commande de grappe active n'est pas autorisée.

- **Basculement** : assurez-vous que l'unité sur laquelle vous souhaitez effectuer l'échange à chaud est le nœud de secours. Consultez Forcer le basculement.

  Si la liaison de basculement se trouve sur le module de réseau, vous devez désactiver le basculement. Consultez Désactiver le basculement. La désactivation du module de réseau avec une liaison de basculement actif n'est pas autorisée.

Étape 2 Désactivez le module de réseau en choisissant **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **EPM** et en cochant **Disable Netmod** (Désactiver Netmod).

Étape 3 Cliquez sur **Apply** (Appliquer).

La configuration est appliquée au pare-feu.

Étape 4 Remplacez le module de réseau en suivant le guide d'installation du matériel. Vous pouvez remplacer le module de réseau lorsque le pare-feu est sous tension.

Étape 5 Activez le module de réseau en choisissant **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **EPM** et en décochant **Disable Netmod** (Désactiver Netmod).

Étape 6 Cliquez sur **Apply** (Appliquer).

La configuration est appliquée au pare-feu.

Étape 7 Pour la mise en grappe ou le basculement, procédez comme suit :

- Mise en grappe : **rajoutez** le nœud à la grappe. Consultez Rejoindre la grappe ou Ajouter un nouveau nœud de données à partir du nœud de contrôle.
- **Basculement** : si vous avez désactivé le basculement, veuillez le reconfigurer.

Remplacer le module de réseau par un module de type différent

Si vous remplacez un module de réseau par un autre type, un rechargement 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. Pour la mise en grappe ou le basculement, aucun temps d'arrêt n'est pris en charge. Veuillez donc vous assurer d'effectuer cette procédure pendant une fenêtre de maintenance.

Procédure

Étape 1 Désactivez le module de réseau en choisissant **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **EPM** et en cochant **Disable Netmod** (Désactiver Netmod).

Pour la mise en grappe ou le basculement, effectuez cette étape sur le nœud de contrôle/l'unité active; l'état du module est répliqué sur les autres nœuds.

Étape 2 Cliquez sur **Apply** (Appliquer).

La configuration est appliquée au pare-feu. N'enregistrez pas la configuration; lors du rechargement, le module sera activé à l'aide de la configuration enregistrée.

Étape 3 Remplacez le module de réseau en suivant le guide d'installation du matériel. Vous pouvez remplacer le module de réseau lorsque le pare-feu est sous tension.

Pour la mise en grappe ou le basculement, installez le module de réseau sur tous les nœuds.

Étape 4 Rechargez le pare-feu; consultez **Tools (Outils) > System Reload (Rechargement du système)**.

Pour la mise en grappe ou le basculement, rechargez tous les nœuds. Étant donné que les nœuds dotés de modules de réseau différents ne peuvent pas rejoindre la paire de grappe/basculement, vous devez recharger tous les nœuds avec le nouveau module avant qu'ils puissent reformer la paire de grappe/basculement.

Étape 5 Si vous avez enregistré la configuration avant le rechargement, vous devrez réactiver le module.

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 rechargement. Pour la mise en grappe ou le basculement, aucun temps d'arrêt n'est pris en charge. Veuillez donc vous assurer d'effectuer cette procédure pendant une fenêtre de maintenance.

Avant de commencer

Pour la mise en grappe ou le basculement, assurez-vous que la liaison de basculement ne se trouve pas sur le module de réseau; dans ce cas, vous ne pouvez pas retirer le module.

Procédure

Étape 1 Désactivez le module de réseau en choisissant **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **EPM** et en cochant **Disable Netmod** (Désactiver Netmod).

Pour la mise en grappe ou le basculement, effectuez cette étape sur le nœud de contrôle/l'unité active; l'état du module est répliqué sur les autres nœuds.

Étape 2 Cliquez sur **Apply** (Appliquer), puis sur **Save** (Enregistrer).

La configuration est enregistrée sur le pare-feu.

Étape 3 Retirez le module de réseau en suivant le guide d'installation du matériel. Vous pouvez retirer le module de réseau lorsque le pare-feu est sous tension.

Pour la mise en grappe ou le basculement, retirez le module de réseau sur tous les nœuds.

Étape 4 Rechargez le pare-feu; consultez **Tools (Outils) > System Reload (Rechargement du système)**.

Pour la mise en grappe ou le basculement, rechargez tous les nœuds. Étant donné que les nœuds dotés de modules de réseau différents ne peuvent pas rejoindre la paire de grappe/basculement, vous devez recharger tous les nœuds sans le module avant qu'ils puissent reformer la paire de grappe/basculement.

Exemples d'interfaces de base

Consultez les exemples de configuration suivants.

Exemple de paramètres d'interface physique

L'exemple suivant configure les paramètres de l'interface physique en mode unique :

```
interface gigabitethernet 0/1
speed 1000
duplex full
no shutdown
```

Exemple de mode de contexte multiple

L'exemple suivant configure les paramètres d'interface en mode de contexte multiple pour la configuration système et attribue la sous-interface gigabitEthernet 0/1.1 à contexteA :

```
interface gigabitethernet 0/1
speed 1000
duplex full
no shutdown
interface gigabitethernet 0/1.1
vlan 101
context contextA
allocate-interface gigabitethernet 0/1.1
```

Historique de la configuration de l'interface de base

Tableau 3 : Historique des interfaces

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
La correction d'erreur par défaut (FEC) sur les ports fixes du Secure Firewall 3100 est passée de cl74-fc à cl108-rs pour les émetteurs-récepteurs SR, CSR et LR de 25 Go+.	9.18(3)/9.19(1)	Lorsque vous définissez le FEC sur Auto sur les ports fixes du Secure Firewall 3100, le type par défaut est désormais défini sur cl108-rs au lieu de cl74-fc pour les émetteurs-récepteurs SR, CSR et LR de 25 Go. Écrans nouveaux/modifiés : **Configuration (configuration)** > **Device Setup (configuration de l'appareil)** > **Interface Settings (paramètres de l'interface)** > **Interfaces** > **Edit Interface (éditer l'interface)** > **Configure Hardware Properties (configurer les propriétés du matériel)** > **FEC Mode (mode FEC)**
Mettre en pause les trames pour le contrôle de flux sur Cisco Secure Firewall 3100	9.18(1)	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. Écrans nouveaux ou modifiés : **Configuration** > **Device Settings (Paramètres de l'appareil)** > **Interfaces** > **General (Général)**
Ports d'éclatement pour Secure Firewall 3130 et 3140	9.18(1)	Vous pouvez maintenant configurer quatre ports d'éclatement de 10 Go pour chaque interface de 40 Go sur les Cisco Secure Firewall 3130 et 3140. Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **EPM**

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Prise en charge de l'échange à chaud du module de réseau pour Secure Firewall 3100	9.17(1)	Vous pouvez ajouter ou retirer le module de réseau sur le pare-feu Secure Firewall 3100 lorsque le pare-feu est sous tension. Pour remplacer un module par un autre module du même type, vous n'avez pas besoin de redémarrer. Après le démarrage initial, l'ajout d'un module, le retrait permanent d'un module ou le remplacement d'un module par un nouveau type nécessite un redémarrage. Écrans Nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **EPM**
Prise en charge de la correction d'erreurs sans voie de retour pour Cisco Secure Firewall 3100	9.17(1)	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. Écrans Nouveaux ou modifiés : **Configuration** > **Device Settings (Paramètres de l'appareil)** > **Interfaces** > **Edit Interface (Modifier l'interface)** > **Configure Hardware Properties (Configurer les propriétés du matériel)**
Prise en charge du réglage de la vitesse en fonction du SFP pour Secure Firewall 3100	9.17(1)	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. Écrans Nouveaux ou modifiés : **Configuration** > **Device Settings (Paramètres de l'appareil)** > **Interfaces** > **Edit Interface (Modifier l'interface)** > **Configure Hardware Properties (Configurer les propriétés du matériel)**
La négociation automatique de Secure Firewall 3100 peut être activée ou désactivée pour les interfaces de 1 Gigabit et les versions ultérieures.	9.17(1)	La négociation automatique de Secure Firewall 3100 peut être activée ou désactivée séparément de la vitesse pour les interfaces de 1 Gigabit et les versions ultérieures. Écrans Nouveaux ou modifiés : **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** > **Advanced (Avancé)**
La négociation automatique de la vitesse peut être désactivée sur les interfaces à fibre optique sur les périphériques Firepower 1100 et 2100.	9.14(1)	Vous pouvez maintenant configurer une interface à fibre optique Firepower 1100 ou 2100 pour désactiver la négociation automatique. Pour les interfaces de 10 Go, vous pouvez configurer la vitesse à 1 Go sans négociation automatique; vous ne pouvez pas désactiver la négociation automatique pour une interface dont la vitesse est réglée à 10 Go. Écrans nouveaux ou modifiés : **Configuration** > **Device Settings (Paramètres de l'appareil)** > **Interfaces** > **Edit Interface (Modifier l'interface)** > **Configure Hardware Properties (Configurer les propriétés du matériel)** > **Speed (Vitesse)**

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Prise en charge du trafic de transit sur l'interface de gestion Management 0/0 pour l'ASA virtuel	9.6(2)	Vous pouvez maintenant autoriser le trafic de transit sur l'interface de gestion Management 0/0 sur l'ASA virtuel. Auparavant, seul l'ASA virtuel sur Microsoft Azure prenait en charge le trafic de transit; maintenant, tous les ASA virtuel le prennent en charge. Vous pouvez éventuellement configurer cette interface pour qu'elle soit en gestion uniquement, mais elle n'est pas configurée par défaut.
Prise en charge des trames de pause pour le contrôle de flux sur les interfaces Gigabit Ethernet	8.2(5)/8.4(2)	Vous pouvez maintenant activer des trames de pause (XOFF) pour le contrôle de flux des interfaces Gigabit Ethernet sur tous les modèles ASA. Nous avons modifié les écrans suivants : (Mode unique) Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces > Add/Edit Interface (Ajouter/modifier une interface) > General (Général) (Mode multiple, système) Configuration > Interfaces > Add/Edit Interface (Ajouter/modifier une interface).
Prise en charge des trames de pause pour le contrôle de flux sur les interfaces ASA 5580 10 Gigabit Ethernet	8.2(2)	Vous pouvez maintenant activer des trames de pause (XOFF) pour le contrôle de flux. Cette fonctionnalité est également prise en charge sur l'ASA 5585-X. Nous avons modifié les écrans suivants : (Mode unique) Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces > Add/Edit Interface (Ajouter/modifier une interface) > General (Général) (Mode multiple, système) Configuration > Interfaces > Add/Edit Interface (Ajouter/modifier une interface).
Prise en charge des paquets étendus pour l'ASA 5580	8.1(1)	L'ASA 5580 prend en charge les bâtis grand format. Une trame étendue est un paquet Ethernet supérieur au maximum standard de 1 518 octets (y compris l'en-tête de couche 2 et FCS) qui peut s'élever jusqu'à 9 216 octets. Vous pouvez activer la prise en charge des trames étendues pour toutes les interfaces en augmentant la quantité de mémoire nécessaire pour traiter les trames Ethernet. L'attribution de plus de mémoire aux trames étendues peut limiter l'utilisation maximale d'autres fonctionnalités, telles que les listes de contrôle d'accès. Cette fonctionnalité est également prise en charge sur l'ASA 5585-X. Nous avons modifié l'écran suivant : Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces > Add/Edit Interface (Ajouter/modifier une interface) > Advanced (Avancé).

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Prise en charge de Gigabit Ethernet pour la licence Security Plus sur l'ASA 5510	7.2(3)	L'ASA 5510 prend désormais en charge GE (Gigabit Ethernet) pour les ports 0 et 1 avec la licence Security Plus. Si vous mettez à niveau la licence de base vers Security Plus, la capacité des ports Ethernet0/0 et Ethernet0/1 externes passe de FE (Fast Ethernet) (100 Mbps) à GE (1 000 Mbps). Les noms d'interface resteront Ethernet 0/0 et Ethernet 0/1.
Augmentation du nombre d'interfaces pour la licence de base sur l'ASA 5510	7.2(2)	Pour la licence de base sur l'ASA 5510, le nombre maximum d'interfaces est passé de 3 plus une interface de gestion à un nombre illimité d'interfaces.

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.

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.

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.

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.