Ensembles en ligne et interfaces passives

Vous pouvez configurer des interfaces passives uniquement IPS, des interfaces ERSPAN passives et des ensembles en ligne. 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.

À propos des interfaces IPS

Cette section décrit les interfaces IPS.

Types d'interface IPS

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.

À propos de Hardware Bypass pour les ensembles en ligne

Pour certains modules d'interface sur les modèles pris en charge (voir Exigences et conditions préalables pour les ensembles en ligne, à la page 4), vous pouvez activer la fonction Hardware Bypass. Hardware Bypass garantit que le trafic continue de circuler entre une paire d'interfaces en ligne pendant une panne de courant.

Cette fonctionnalité peut servir à maintenir la connectivité du réseau en cas de défaillance matérielle ou logicielle.

Déclencheurs Hardware Bypass

Hardware Bypass peut être déclenchée dans les scénarios suivants :

- Plantage de Défense contre les menaces
- Redémarrage de Défense contre les menaces
- Redémarrage du module de sécurité
- Plantage du châssis
- Redémarrage du châssis
- Déclenchement manuel
- Perte d'alimentation du châssis
- Perte d'alimentation du module de sécurité

Remarque Le contournement matériel est destiné aux scénarios de défaillance imprévue et imprévue et n'est pas automatiquement déclenché lors des mises à niveau logicielles planifiées. Le contournement matériel ne s'active qu'à la fin d'un processus de mise à niveau planifiée, au redémarrage de l'application défense contre les menaces .

Commutation pour le contournement matériel

Lors du passage du fonctionnement normal au contournement matériel ou du fonctionnement du contournement matériel au fonctionnement normal, le trafic peut être interrompu pendant plusieurs secondes. Un certain nombre de facteurs peuvent influer sur la durée de l'interruption. par exemple, négociation automatique de port cuivre; le comportement du partenaire de liaison optique, par exemple sa gestion des défaillances de liaison et la synchronisation de l'antirebond; la convergence du protocole Spanning Tree; la convergence des protocoles de routage dynamique; et ainsi de suite. Pendant ce temps, il se peut que vous rencontriez des pertes de connexions.

Vous pourriez également rencontrer des interruptions de connexions en raison d'erreurs d'identification d'application lors de l'analyse des connexions à mi-chemin après le retour à la normale.

Snort Fail Open ou Hardware Bypass

Pour les ensembles en ligne autres que ceux en mode TAP, vous pouvez utiliser l'option Snort sur échec d'ouverture pour abandonner le trafic ou permettre au trafic de passer sans inspection lorsque le processus Snort est occupé ou en panne. Snort Fail Open est pris en charge sur tous les ensembles en ligne, à l'exception de ceux en mode TAP, et pas seulement sur les interfaces qui prennent en charge Hardware Bypass.

La fonctionnalité Hardware Bypass permet au trafic de circuler pendant une défaillance matérielle, y compris une panne de courant complète, et certaines défaillances logicielles limitées. Une défaillance logicielle qui déclenche Snort Fail Open ne déclenche pas de Hardware Bypass.

État Hardware Bypass

Si le système est alimenté, le voyant DEL de contournement indique l'état Hardware Bypass. Reportez-vous au guide d'installation du matériel du châssis Firepower pour obtenir une description des voyants DEL.

Exigences et conditions préalables pour les ensembles en ligne

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Prise en charge Hardware Bypass

défense contre les menaces prend en charge Hardware Bypass pour les paires d'interfaces sur des modules de réseau spécifiques sur les modèles suivants :

- Firepower 2130 et 2140
- Secure Firewall 3100
- Firepower 4100
- Firepower 9300

Remarque ISA 3000 a une implémentation distincte pour le contournement matériel, que vous pouvez activer à l'aide de FlexConfig uniquement (voir Politiques FlexConfig). N'utilisez pas ce chapitre pour configurer le contournement matériel d'ISA 3000.

Remarque Vous pouvez utiliser les interfaces Hardware Bypass comme des interfaces standard sans que la fonctionnalité Hardware Bypass ne soit activée.

Les modules de réseau Hardware Bypass pris en charge pour ces modèles comprennent :

- Firepower 2130 et 2140
  - Module de réseau simple largeur Firepower SX FTW 6 ports 1G (FPR2K-NM-6X1SX-F)
  - Module de réseau simple largeur Firepower de 6 ports 10G SR FTW (FPR2K-NM-6X10SR-F)
  - Module de réseau simple largeur Firepower 10G LR FTW 6 ports (FPR2K-NM-6X10LR-F)
- Série Secure Firewall 3100 :
  - Module de réseau de basculement vers le fil à 6 ports SFP de 1G, SX (multimode) (FPR3K-XNM-6X1SXF)

- Module de réseau de basculement vers le fil de 6 ports 10G SFP, SR (multimode) (FPR3K-XNM-6X10SRF)
- Module de réseau de défaillance au fil de 6 ports 10G SFP, LR (mode unique) (FPR3K-XNM-6X10LRF)
- Module de réseau de basculement vers le fil de 6 ports 25G SFP, SR (multimode) (FPR3K-XNM-X25SRF)
- Module de réseau de basculement vers le fil, 6 ports 25G, LR (mode unique) (FPR3K-XNM-6X25LRF)
- Module de réseau de basculement vers le fil, 8 ports 1G, RJ45 (cuivre) (FPR3K-XNM-8X1GF)

- Firepower 4100
  - Module de réseau simple largeur Firepower SX FTW 6 ports 1G (FPR4K-NM-6X1SX-F)
  - Module de réseau simple largeur Firepower de 6 ports 10G SR FTW (FPR4K-NM-6X10SR-F)
  - Module de réseau simple largeur Firepower 10G LR FTW 6 ports (FPR4K-NM-6X10LR-F)
  - Module de réseau simple largeur Firepower de 2 ports 40G SR FTW (FPR4K-NM-2X40G-F)
  - Module de réseau simple largeur Firepower de 8 ports 1-G Firepower cuivre (FPR-NM-8X1G-F).
- Firepower 9300 :
  - Module de réseau simple largeur Firepower de 6 ports 10G SR FTW (FPR9K-NM-6X10SR-F)
  - Module de réseau simple largeur Firepower 10G LR FTW 6 ports (FPR9K-NM-6X10LR-F)
  - Module de réseau simple largeur Firepower de 2 ports 40G SR FTW (FPR9K-NM-2X40G-F)

Hardware Bypass ne peut utiliser que les paires de ports suivantes :

- 1 et 2
- 3 et 4
- 5 et 6
- 7 et 8

Directives pour les ensembles en ligne et les interfaces passives

Mode pare-feu

- Les interfaces ERSPAN ne sont autorisées que lorsque le périphérique est en mode de pare-feu routé.

Mise en grappes

- La propagation de l'état du lien pour un ensemble en ligne n'est pas prise en charge avec la mise en grappe.

Mode multi-instance

- Les interfaces partagées à plusieurs instances ne sont pas prises en charge. Vous devez utiliser une interface non partagée.
- Les sous-interfaces à instances multiples définies par le châssis ne sont pas prises en charge. Vous devez utiliser une interface physique ou un EtherChannel.

Directives générales

- Les ensembles en ligne et les interfaces passives prennent en charge les interfaces physiques et les EtherChannels uniquement et ne peuvent pas utiliser les VLAN ou d'autres interfaces virtuelles, y compris les sous-interfaces multi-instances définies par le châssis.
- Les paquets écho de la détection de transfert bidirectionnel (BFD) ne sont pas autorisés par le biais de défense contre les menaces lors de l'utilisation d'ensembles en ligne. S'il y a deux voisins de chaque côté de défense contre les menaces exécutant BFD, alors défense contre les menaces abandonnera les paquets écho BFD, car ils ont la même adresse IP de source et de destination et semblent faire partie d'une attaque LAND.
- Pour les ensembles en ligne et les interfaces passives, le défense contre les menaces prend en charge jusqu'à deux en-têtes 802.1Q dans un paquet (également appelé prise en charge Q-in-Q), à l'exception des périphériques Firepower 4100/9300, qui ne prennent en charge qu'un seul en-tête 802.1Q. **Remarque :** Les interfaces de type pare-feu ne prennent pas en charge Q-in-Q et ne prennent en charge qu'un seul en-tête 802.1Q.

Directives Hardware Bypass

- Les ports Hardware Bypass ne sont pris en charge que pour les ensembles en ligne.
- Les ports Hardware Bypass ne peuvent pas faire partie d'un EtherChannel.
- Hardware Bypass n'est pas pris en charge en mode haute disponibilité.
- Les ports Hardware Bypass sont pris en charge avec la mise en grappe à l'intérieur du châssis sur le périphérique Firepower 9300. Les ports sont placés en mode Hardware Bypass lorsque la dernière unité du châssis tombe en panne. La mise en grappe inter-châssis n'est pas prise en charge, car elle ne prend en charge que les EtherChannels étendus; Les ports Hardware Bypass ne peuvent pas faire partie d'un EtherChannel.
- Si tous les modules d'un groupe à l'intérieur du châssis du périphérique Firepower 9300 tombent en panne, Hardware Bypass est déclenché sur l'unité finale et le trafic continue de passer. Lorsque les unités sont réactivées, Hardware Bypass revient en mode veille. Cependant, lorsque vous utilisez des règles qui correspondent au trafic d'application, ces connexions peuvent être abandonnées et doivent être rétablies. Les connexions sont abandonnées, car les informations d'état ne sont pas conservées sur l'unité de grappe et l'unité ne peut pas identifier le trafic comme appartenant à une application autorisée. Pour éviter une baisse du trafic, utilisez une règle basée sur le port plutôt qu'une règle basée sur l'application, si votre déploiement est approprié.

- Vous pouvez utiliser les interfaces Hardware Bypass comme des interfaces standard sans que la fonctionnalité Hardware Bypass ne soit activée.
- Ne pas activer Hardware Bypass et Propager l'état du lien pour le même ensemble en ligne.

Fonctionnalités de pare-feu non prises en charge sur les interfaces IPS

- Serveur DHCP
- Relais DHCP
- Client DHCP
- Interception TCP
- Routage
- NAT
- VPN
- Inspection des applications
- Qualité de service
- NetFlow
- VXLAN

Configurer une interface passive

Cette section décrit comment :

- Activez l'interface. Par défaut, les interfaces sont désactivées.
- Définissez le mode d'interface sur Passif ou ERSPAN. Pour les interfaces ERSPAN, vous devez définir les paramètres ERSPAN et l'adresse IP.
- Modifier la MTU Par défaut, la MTU est définie sur 1500 octets. Pour plus d'informations sur la MTU, consultez À propos de la MTU.
- Définissez une vitesse et un duplex (si disponible). Par défaut, la vitesse et le mode duplex sont réglés à Auto.

Remarque Pour Cisco Secure Firewall Threat Defense sur le châssis FXOS, vous configurez les paramètres de base de l'interface sur Firepower 4100/9300. Consultez Configurer une interface physique pour de plus amples renseignements.

Avant de commencer

- Si vous utilisez des EtherChannels, ajoutez-les en fonction de Configurer un EtherChannel.

Procédure

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

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

Étape 3 Dans la liste déroulante **Mode**, choisissez **Passif** ou **Erspan**.

Étape 4 Activez l'interface en cochant la case **Enabled** (activé).

Étape 5 Dans le champ **Nom**, saisissez un nom renfermant au maximum 48 caractères.

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

Étape 7 (Facultatif) Ajoutez une description dans le champ **Description**.

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

Étape 8 (Facultatif) Dans **General**(généralité), définissez la **MTU** entre 64 et 9198 octets; pour Cisco Secure Firewall Threat Defense Virtual et Cisco Secure Firewall Threat Defense sur le châssis FXOS, le maximum est de 9000 octets.

Par défaut, c'est de 1500 octets.

Étape 9 Pour les interfaces ERSPAN, définissez les paramètres suivants :

- **Id de flux** : Configurez l'ID utilisé par les sessions de source et de destination pour identifier le trafic ERSPAN, entre 1 et 1023. Cet ID doit également être entré dans la configuration de la session de destination ERSPAN.
- **Adresse IP source** : Configurez l'adresse IP utilisée comme source du trafic ERSPAN.

Étape 10 Pour les interfaces ERSPAN, définissez l'adresse IPv4 et le masque **IPv4**.

Étape 11 (Facultatif) Définissez le mode duplex et la vitesse en cliquant sur **Hardware Configuration** (configuration matérielle).

Les fonctionnalités exactes de vitesse et de duplex dépendent de votre matériel.

- **Duplex** : Choisissez entre **Full**, **Half** ou **Auto**. Auto est la valeur par défaut.
- **Speed** : Choisissez entre **10**, **100**, **1000** ou **Auto**. Auto est la valeur par défaut.

Étape 12 Cliquez sur **OK**.

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

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

Configurer un ensemble en ligne

Cette section active et nomme deux interfaces physiques ou EtherChannels que vous pouvez ajouter à un ensemble intégré. Vous pouvez également activer Hardware Bypass pour les paires d'interfaces prises en charge.

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

Avant de commencer

- Si vous utilisez des EtherChannels, ajoutez-les en fonction de Configurer un EtherChannel.
- Nous recommandons de définir STP PortFast pour les commutateurs compatibles STP qui se connectent aux défense contre les menaces interfaces de la paire en ligne. Ce paramètre est particulièrement utile pour les Hardware Bypass configurations et peut réduire les temps de contournement.

Procédure

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

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

Étape 3 Dans la liste déroulante **Mode**, choisissez **None** (aucun).

Après avoir ajouté cette interface à un ensemble en ligne, ce champ indique « Inline » pour le mode.

Étape 4 Activez l'interface en cochant la case **Enabled** (activé).

Étape 5 Dans le champ **Nom**, saisissez un nom renfermant au maximum 48 caractères.

Ne définissez pas encore la zone de sécurité; vous devez le définir après avoir créé l'ensemble en ligne (plus tard au cours de cette procédure).

Étape 6 (Facultatif) Ajoutez une description dans le champ **Description**.

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

Étape 7 (Facultatif) Définissez le mode duplex et la vitesse en cliquant sur **Hardware Configuration** (configuration matérielle).

Les fonctionnalités exactes de vitesse et de duplex dépendent de votre matériel.

- **Duplex** : Choisissez entre **Full**, **Half** ou **Auto**. Auto est la valeur par défaut.
- **Speed** : Choisissez entre **10**, **100**, **1000** ou **Auto**. Auto est la valeur par défaut.

Étape 8 Cliquez sur **OK**.

Ne définissez aucun autre paramètre pour cette interface.

Étape 9 Cliquez sur **Edit** ( ) pour la deuxième interface que vous souhaitez ajouter à l'ensemble en ligne.

Étape 10 Configurez les paramètres comme vous l'avez fait pour la première interface.

Étape 11 Cliquez sur **Inline Sets** (ensembles en ligne).

Étape 12 Cliquez sur **Add Inline Set** (ajouter un ensemble en ligne).
La boîte de dialogue **Add Inline Set**, l'option **General** est sélectionnés.

Étape 13 Dans le champ **Nom**, entrez un nom pour l'ensemble.

Étape 14 (Facultatif) Modifiez la **MTU** pour activer les trames étendues.

Pour les ensembles en ligne, le paramètre MTU n'est pas utilisé. Cependant, le paramètre de trame jumbo *est* pertinent pour les ensembles en ligne; les trames étendues permettent aux interfaces en ligne de recevoir des paquets allant jusqu'à 9 000 octets. Pour activer les trames étendues, vous devez définir la MTU de *toute* interface sur le périphérique au-dessus de 1 500 octets.

Étape 15 Configurez Hardware Bypass.

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

a) Pour le mode **Bypass** (contournement), choisissez l'une des options suivantes :

- **Disabled** (désactivé) : Désactivez Hardware Bypass pour les interfaces sur lesquelles Hardware Bypass est pris en charge ou utilisez les interfaces où Hardware Bypass n'est pas pris en charge.
- **Standby** (veille) : Réglez Hardware Bypass en mode veille sur les interfaces prises en charge. Seules les paires d'interfaces Hardware Bypass sont affichées. En mode veille, les interfaces conservent leur fonctionnement normal jusqu'à ce qu'il y ait un événement déclencheur.
- **Bypass-Force** (contournement par la force) : Force manuellement la paire d'interfaces à passer en mode de contournement. La rubrique **Inline Sets** indique **Yes** (oui) pour toutes les paires d'interfaces en mode Bypass-Force.

b) 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).

Tous les appariements possibles entre les interfaces nommées et activées avec le mode défini sur aucun (None) s'affichent dans cette zone.

Étape 16 (Facultatif) Cliquez sur **Advanced** (réglages avancés) pour définir les paramètres facultatifs suivants :

- **Tap Mode** : Activez le mode Tap en ligne.

  Notez que vous ne pouvez pas activer cette option et appliquer strictement le TCP sur le même ensemble en ligne.

  Remarque Si vous devez activer ou désactiver le mode Tap, vous devez le faire pendant une fenêtre de maintenance. Le changement de mode pendant que le périphérique transmet du trafic peut perturber le trafic.

  Remarque Le mode Tap a des répercussions *importantes* sur le défense contre les menaces le rendement, en fonction du trafic.

- **Propagate Link State** : Configurez la propagation de l'état du lien.

  La propagation de l'état de liaison entraîne automatiquement le retrait de la deuxième interface de la paire d'interfaces en ligne lorsque l'une des interfaces d'un ensemble en ligne ne fonctionne plus. Lorsque

l'interface en panne est relancée, la deuxième interface est automatiquement relancée. En d'autres termes, si l'état de liaison d'une interface change, l'appareil détecte le changement et met à jour l'état de liaison de l'autre interface pour les faire correspondre. Vous observerez que les périphériques nécessitent jusqu'à 4 secondes pour propager les changements d'état de liaison. La propagation de l'état de liaison est particulièrement utile dans les environnements de réseau résilients où les routeurs sont configurés pour rediriger automatiquement le trafic autour des périphériques réseau en état de défaillance.

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

N'activez pas la **propagation de l'état du lien** lors de l'utilisation de la mise en grappe.

- **Snort Fail Open**(admission même en cas de non-conformité de Snort) : Activez ou désactivez l'une des options **Busy** (occupé) et **Down** (arrêté) ou les deux si vous souhaitez que le trafic nouveau ou existant passe sans inspection (activé) ou soit abandonné (désactivé) lorsque le processus Snort est occupé ou arrêté.

  Par défaut, le trafic passe sans inspection lorsque le processus Snort est arrêté et est abandonné lorsque le processus est occupé.

  Lorsque le processus Snort est :

  - Busy (occupé) : il ne peut pas traiter le trafic assez rapidement, car les tampons de trafic sont saturés, ce qui indique que le trafic est supérieur aux capacités de l'appareil ou en raison d'autres problèmes de ressources logicielles.
  - Down (arrêté) : il redémarre car vous avez déployé une configuration qui nécessite le redémarrage. Consultez Configurations qui redémarrent le processus Snort lors de leur déploiement ou activation.

  Lorsque le processus Snort est arrêté et redémarre, il inspecte les *nouvelles* connexions. Pour éviter les faux positifs et les faux négatifs, il n'inspecte pas les connexions existantes sur les interfaces en ligne, routées ou transparentes, car les informations de la session initiale pourraient avoir été perdues pendant leur interruption.

  Remarque Lorsque Snort ne s'ouvre pas, les fonctionnalités qui dépendent du processus Snort ne fonctionnent pas. Celles-ci comprennent le contrôle des applications et l'inspection approfondie. Le système effectue uniquement un contrôle d'accès de base en utilisant des caractéristiques de transport et de couche réseau simples et faciles à déterminer.

  Remarque L'option **Strict TCP Enforcement** (Application stricte du protocole TCP) n'est pas prise en charge.

Étape 17 Cliquez sur **Interfaces**.

Étape 18 Cliquez sur **Edit** (✎) l'une des interfaces membres.

Étape 19 Dans la liste déroulante **Security Zone** (zone de sécurité), choisissez une zone de sécurité ou ajoutez-en une en cliquant sur **New** (nouveau).

Vous ne pouvez définir la zone qu'après avoir ajouté l'interface à l'ensemble en ligne; l'ajouter à un ensemble en ligne configure le mode en ligne et vous permet de choisir des zones de sécurité de type en ligne.

Étape 20 Cliquez sur **OK**.

Étape 21 Définissez la zone de sécurité pour la deuxième interface.

Étape 22 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.

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.