Module de services de pare-feu (FWSM) - Forum aux questions

Contenu

Introduction

Ce document contient une foire aux questions au sujet du module de services pare-feu de la gamme Catalyst 6500 (FWSM).

Remarque: Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Caractéristiques prises en charge

Q. Quelle est la version minimum de code que j'ai besoin d'exécuter pour prendre en charge mon FWSM, mon module système de détection des intrusions 2 (IDSM2) et mon module de services VPN (VPNSM) ?

A. La version appropriée du code dépend du type de module de supervision dans votre châssis 6500 ou 7600, ainsi que du type de logiciel que vous exécutez (CatOS [hybride] ou Cisco IOS [natif]). Reportez-vous à ce tableau pour les versions de code spécifiques pour votre module et votre carte de commutation multicouche (MSFC).

	Sup1 (avec MSFC)		Sup2 (avec MSFC)		Sup720	
Module	Cisco IOS	Cat OS	Cisco IOS	Cat OS	Cisco IOS	Cat OS
FWSM	12.1(13)E	7.5(1)	12.1(13)E	7.5(1)	12.2(14)SX1	8.2(1)
IDSM 2	Non pris en charge	7.6(1)	12.1(19)E	7.6(1)	12.2(14)SX1	8.2(1)

VPN SM	Non pris en charge	Non pris en charge	12.2(14)SY	Non pris en charge	12.2(17a)SX10	Non pris en charge *

* Des plans existent pour introduire la prise en charge.

Remarque: Reportez-vous à Comparaison des systèmes d'exploitation Cisco Catalyst et Cisco IOS pour le commutateur de la gamme Cisco Catalyst 6500 pour obtenir des informations sur les différences entre CatOS (hybride) et Cisco IOS (natif).

Q. Puis-je exécuter le FWSM, le module système de détection des intrusions 2 (IDSM2) et le module de services VPN (VPNSM) dans le même châssis ?

A. Oui, vous pouvez exécuter ces modules dans le même châssis si le commutateur exécute le logiciel Cisco IOS intégré avec au minimum le logiciel Cisco IOS Version 12.2(14)SY (Sup2) ou 12.2(17a)SX10 (Sup720). Actuellement, il n'y a aucune version de CatOS qui peut prendre en charge ces modules de service dans le mêmes châssis 6500 ou 7600.

Q. Quelles sont mes options de configuration et de gestion pour le FWSM ?

A. Les options de configuration et d'administration incluent notamment les suivantes.

Option	Version	Description
Management Center for Firewalls	Versions 1.1.1 et ultérieures*	Interface Web permettant de configurer et gérer plusieurs pare-feu. **Remarque:** La prise en charge des groupes de service dans le regroupement d'objet est limitée. Les groupes de service sont correctement analysés, mais aplatis immédiatement. Ceci affecte les commandes avec les mots clés **icmp-type**, **protocol** et **service**. Cette limitation s'applique aux versions 1.3 et antérieures.
Monitoring Center for Security	Versions 1.2 et ultérieures*	Interface Web permettant de contrôler les dispositifs de sécurité Cisco. Le logiciel centralise la gestion Syslog de plusieurs dispositifs de sécurité Cisco avec des options de rapport et d'alerte flexibles.
Monitoring Center for Performance	Versions 2.0 et ultérieures*	Interface Web permettant de contrôler et de dépanner l'intégrité et les performances des services qui contribuent à la sécurité du réseau. Le protocole SNMP (Simple Network Management Protocol) est le protocole sous-jacent utilisé.
PDM	Version	Interface Web permettant de configurer,

	2.1	gérer et contrôler un pare-feu simple. PIX Device Manager (PDM) doit être installé localement sur le pare-feu PIX.
Telnet	S/O	Telnet fournit un accès distant par le biais de l'interface de ligne de commande (CLI) à un pare-feu. **Remarque:** Afin de permettre l'accès Telnet à l'interface à niveau de sécurité le plus bas (généralement connue sous le nom d'interface externe), vous devez configurer IPsec pour la gestion.
Secure Shell (SSH)	S/O	SSH fournit un accès CLI distant sécurisé à un pare-feu.
SNMP	S/O	SNMP fournit une méthode de contrôle du FWSM. **Remarque:** SNMP est en lecture seule sur le FWSM.
Syslog	S/O	Syslog fournit une méthode de contrôle du FWSM.

* Ce logiciel fait partie du lot CiscoWorks VPN/Security Management Solution (VMS). Ce logiciel fournit une approche intégrée pour gérer des périphériques de sécurité Cisco par l'intermédiaire d'une interface basée sur le navigateur pour les réseaux d'entreprise.

Q. Qu'est-ce qu'un SVI ? Est-ce que je peux configurer plusieurs SVI ?

A. SVI est l'acronyme de Switched Virtual Interface (interface virtuelle commutée). Elle représente une interface logique de couche 3 sur un commutateur. Pour les versions de CatOS antérieures à 7.6(1) et les versions du logiciel Cisco IOS antérieures à 12.2(14)SY, seul un SVI est autorisé en tant qu'élément des VLAN pare-feu. En d'autres termes, seule une interface de couche 3 peut être configurée entre le FWSM et la carte de commutation multicouche (MSFC). Une tentative de configuration de plusieurs SVI produit un message d'erreur au niveau de l'interface de ligne de commande (CLI).

Pour les versions 7.6(1) et ultérieures de CatOS et les versions 12.2(14)SY et ultérieures du logiciel Cisco IOS, le FWSM prend en charge plusieurs SVI. Par défaut, seul un SVI est pris en charge. Utilisez l'une de ces commandes pour activer la prise en charge de plusieurs SVI sur votre commutateur.

- Pour CatOS, saisissez set firewall multiple-vlan-interfaces enable.Pour Cisco IOS, saisissez firewall multiple-vlan-interfaces.

Si vous configurez votre commutateur pour les VLAN FWSM et recevez un message d'erreur qui indique que vous avez plusieurs SVI, inspectez votre commutateur et/ou configuration MSFC pour vous assurer qu'une seule interface de couche 3 (ou interface VLAN) existe en tant qu'élément des VLAN pare-feu.

Remarque: Utilisez uniquement un SVI. Ceci vous permet d'éviter une configuration compliquée qui implique le routage de stratégie.

Q. FWSM prend-il en charge SNMPv3 ?

A. Non.

Q. Combien de VLAN le FWSM prend-il en charge ?

A. FWSM version 1.1 prend en charge 100 VLAN et FWSM version 2.1 prend en charge 250 VLAN.

Q. Le FWSM prend-il en charge la commande access-list compiled ?

A. Puisque le FWSM compile automatiquement les listes d'accès dans le matériel après 10 secondes d'inactivité au niveau de la CLI, les listes d'accès turbo sont inutiles. FWSM version 2.1 offre également la possibilité de décider quand les listes d'accès sont compilées.

Q. Le FWSM prend-il en charge la commande auto-cost reference-bandwidth Open Shortest Path First (OSPF) IOS ?

A. Non. Le FWSM n'a pas conscience des ports physiques qui lui sont connectés. Le coût OSPF doit être configuré manuellement pour chaque interface avec la commande ospf cost.

Q. Est-ce que je peux exécuter le protocole Open Shortest Path First (OSPF) dans une topologie où deux interfaces différentes du FWSM se connectent au même réseau ?

A. Oui. Cette fonctionnalité est prise en charge dans les versions 2.1 et ultérieures.

Q. Quels protocoles de routage sont pris en charge par le FWSM ?

A. Open Shortest Path First (OSPF) et le protocole d'informations de routage (RIP) sont les protocoles de routage pris en charge. Pour plus d'informations sur FWSM, reportez-vous à la documentation disponible à la page Module de services pare-feu de la gamme Cisco Catalyst 6500.

Q. Est-ce que Multicast (Internet Group Management Protocol [IGMP] v2 et routage multicast d'extrémité) est pris en charge sur le FWSM ?

A. Oui. Cette fonctionnalité est prise en charge dans FWSM versions 2.1 et ultérieures. Si vous exécutez la version 1.1, vous pouvez utiliser la transmission tunnel par encapsulation de routage générique (GRE) comme solution de contournement.

Q. Le FWSM prend-il en charge le filtrage URL ?

A. Oui. Websense est pris en charge dans les versions 1.1 et ultérieures, avec en plus la prise en charge de N2H2 dans la version 2.1.

Q. Pourquoi est-ce que des paquets fragmentés sont déposés par le FWSM ?

A. Par défaut, les paquets fragmentés ne peuvent pas traverser le FWSM. Vous pouvez utiliser la commande fragment pour configurer cette fonctionnalité. Ce comportement diffère de celui du

pare-feu PIX. Les protocoles communs qui utilisent les paquets fragmentés sont Open Shortest Path First (OSPF) et le système de fichiers en réseau (NFS).

Q. Est-ce que je peux terminer des connexions VPN sur mon FWSM ?

A. La fonctionnalité VPN n'est pas prise en charge sur le FWSM. La terminaison des connexions VPN est la responsabilité du commutateur et/ou du module de services VPN. La licence 3DES est fournie à des fins de gestion uniquement, comme la connexion à une interface à niveau de sécurité faible via Telnet, Secure Shell (SSH) et Secure HTTP (HTTPS).

Q. Est-ce que le protocole AAA (Authentication, Authorization, and Accounting) pour RADIUS ou TACACS+ est pris en charge sur le FWSM ?

A. AAA est pris en charge pour la gestion et le trafic FWSM passant par le FWSM. Reportez-vous à la documentation du module de services pare-feu pour des détails supplémentaires.

Le FWSM offre une fonctionnalité semblable à celle du pare-feu PIX, à l'exception de listes d'accès téléchargeables et des VPN. En gardant cela à l'esprit, vous pouvez utiliser ces documents du pare-feu PIX comme guides pour la configuration de FWSM.

- Comment assurer l'authentification et l'activation sur le pare-feu Cisco Secure PIX Firewall (versions 5.2 à 6.2)
- Authentification, autorisation et traçabilité des utilisateurs par le biais du logiciel PIX version 5.2 et ultérieure

Q. Comment est-ce que j'exécute une récupération de mot de passe pour le FWSM ?

A. Reportez-vous à ces documents pour des informations sur la récupération de mot de passe.

- Pour la version 1.1(1), reportez-vous à la Note de configuration de FWSM 1.1(1) suivante : Modification et récupération de mots de passe.
- Pour les versions 1.1(2) et 1.1(3), reportez-vous à la Note de configuration de FWSM 1.1(2) suivante : Modification et récupération de mots de passe.

Q. FWSM prend-il en charge les trames jumbo ?

A. Oui, FWSM peut prendre en charge les trames jumbo.

Q. Comment le FWSM répond-il quand il reçoit un paquet avec son adresse source comme adresse de réalimentation ?

A. Il traite le paquet en tant que non valide et relâche le paquet. Par défaut, FWSM relâche les paquets avec une adresse source incorrecte telle qu'une adresse de réalimentation, a annoncé l'adresse et le host address de destination. Un message de log suivant les indications de cet exemple est généré.

```
%FWSM-2-106016: Deny IP spoof from (IP_address) to
 IP_address on interface interface_name.
```

Q. PVLAN est-il pris en charge sur FWSM ?

A. La prise en charge de PVLAN commence à la version 3.1 du logiciel. Si vous exécutez une version du logiciel antérieure à 3.1, la seule solution de contournement possible est de connecter le port proche du PVLAN à l'aide du câble croisé à un port d'accès normal, puis de protéger le VLAN de ce port d'accès par pare-feu.

Q. Le nombre de lignes de liste d'accès est-il pris en charge dans FWSM ?

A. Cette fonctionnalité est uniquement prise en charge dans les versions 3.1 et ultérieures du logiciel.

Q. Pouvez-vous limiter le nombre de connexions qu'un utilisateur peut avoir sur le FWSM ?

A. Oui, vous pouvez limiter les connexions à l'aide du cadre de stratégie modulaire. Complétez ces étapes afin de limiter le nombre de connexions :

1. Créez une carte de classe afin de faire correspondre le trafic.
2. Placez la carte de classe sur une carte de stratégie et utilisez la limitation de connexion dans la carte de stratégie.
3. Appliquez la carte de stratégie à l'aide de la stratégie de service.

Reportez-vous à Configuration des limites et des délais d'attente de connexion pour plus d'informations et des étapes détaillées.

Q. Y a-t-il des limitations dans l'implémentation du multicast dans FWSM ?

A. Oui. FWSM ne prend pas en charge le sous-réseau 232.x.x.x comme nom de groupe, car il a déjà été réservé pour le module de services de sécurité (SSM).

Q. Est-ce que la diffusion dirigée est autorisée par le biais de FWSM ?

A. Non. À la différence d'un routeur, le FWSM ne permet pas la diffusion dirigée par le biais de ses interfaces. Une solution de contournement plus semblable est d'employer la fonctionnalité intégrée de relais DHCP pour transférer les diffusions d'une interface à l'autre.

Q. Le moteur d'inspection HTTP peut-il détecter le trafic non-HTTP ou le trafic non-standard dans une session HTTP ?

A. Oui. Le pare-feu d'application avec inspection HTTP avancée peut détecter et contrôler ce trafic. Reportez-vous à Aperçu du moteur d'inspection d'application pour plus d'informations.

Q. Les fonctionnalités de normalisation dans ASA et FWSM sont-elles compatibles ?

A. Dans FWSM, la normalisation TCP s'applique uniquement au trafic qui concerne le complexe TCP. Le trafic normal de plan de données (chemin rapide) n'est pas affecté. Ceci diffère de l'ASA dans le sens où tout le trafic ASA est soumis au normalisateur.

Sur le FWSM, si le normalisateur est désactivé, le module revient à un comportement 2.3. Mais, si vous désactivez **control-point tcp-normalizer**, ceci empêche les contrôles stricts de TCP, tels que la détection des segments hors séquence et la surveillance des options TCP, sur les paquets TCP reçus sur le plan de contrôle pour l'inspection de couche 7 dans le FWSM. Ainsi, il est recommandé de ne pas le désactiver. FWSM ne permet pas le réglage des paramètres tcp-map par défaut.

Q. Devons-nous activer/désactiver le normalisateur TCP ?

A. En raison de l'incapacité de passer certaines informations spécifiques à la connexion de NP au plan de contrôle, il est possible que le normalisateur TCP ne fonctionne pas correctement tout le temps dans le FWSM. Par ailleurs , les tcp-maps uniques associés aux connexions ne peuvent pas être identifiés. Ainsi, le FWSM se fonde sur le tcp-map par défaut qui ne fonctionne probablement pas correctement pour toutes les connexions. En raison de ces limitations, il est nécessaire d'activer/désactiver le normalisateur TCP dans le plan de contrôle pour le trafic passant par le pare-feu. FWSM ne permet pas le réglage des paramètres tcp-map par défaut.

Q. Quel est le nombre maximal d'entrées mfib qu'un FWSM peut prendre en charge ?

A. Le nombre maximal d'entrées est de 5 000.

Q. Comment capturer les paquets dans FWSM ?

A. Les paquets peuvent être capturés dans FWSM. L'utilisation du CLI pour capturer des paquets n'est pas prise en charge dans ASDM et la commande **capture** n'est pas prise en charge dans ASDM. Reportez-vous à Commandes ignorées et réservées à l'affichage pour plus d'informations. Reportez-vous à Capture de paquets pour plus d'informations sur la configuration de la capture de paquet dans FWSM. Reportez-vous à ASA/PIX/FWSM : Exemple de configuration de capture de paquet à l'aide de la CLI et d'ASDM pour plus d'informations sur un exemple de configuration de capture de paquet.

Q. Quelle est la version d'ASDM prise en charge par FWSM ?

A. Reportez-vous à Compatibilité des versions de FWSM et d'ASDM pour plus d'informations sur la compatibilité des versions de FWSM et d'ASDM.

Autorisation

Q. J'ai une licence pour un FWSM qui fonctionne en mode contexte multiple. Est-ce que je peux obtenir une licence pour un FWSM de rechange en cas de défaillance matérielle ?

A. Vous pouvez obtenir une licence pour un FWSM de rechange. Cependant, vous devez commander la licence du FWSM de rechange au même titre qu'une licence normale. En cas d'une défaillance matérielle, contactez l'assistance technique de Cisco pour vérifier la panne et obtenir une licence pour le FWSM de rechange. Reportez-vous à Logiciel du module pare-feu Cisco version 2.2(1) pour des informations sur la licence.

Q. FWSM prend-il en charge plusieurs interfaces partagées ?

A. FWSM ne prend pas en charge plusieurs interfaces partagées, mais vous pouvez au lieu de cela avoir un VLAN à travers plusieurs contextes. Reportez-vous à Partage des ressources et des interfaces entre les contextes pour plus d'informations.

Questions VLAN

Q. Comment est-ce que je place des VLAN supplémentaires derrière le FWSM ?

A. Utilisez la commande **nameif** si vous voulez ajouter VLAN 200 à la configuration. Le niveau de sécurité doit être compris entre 0 et 100. La syntaxe de commande complète est **nameif vlan200 <nom interface> <niveau sécurité>**.

Q. Combien de VLAN est-ce que je peux placer derrière le FWSM à l'aide du mode routé à contexte simple ?

A. Vous pouvez placer 1000 VLAN derrière le FWSM à l'aide du mode routé à contexte simple.

Questions de ping

Q. Pourquoi est-ce que je ne peux pas exécuter une commande ping sur mon FWSM sur une interface directement connectée ?

A. Par défaut, chaque interface refuse le protocole ICMP (Internet Control Message Protocol). Utilisez la commande **icmp** pour autoriser ce trafic à l'interface. Ce comportement diffère de celui du PIX.

Remarque: Quand ICMP à l'interface est refusé par la commande **icmp**, vous voyez toujours l'adresse MAC correcte dans la table Protocole de résolution d'adresse (ARP). Si vous ne voyez pas l'adresse MAC, reportez-vous à la question suivante.

Q. Je ne peux pas exécuter une commande ping sur mon FWSM sur une interface directement connectée, et je ne vois pas d'entrée Protocole de résolution d'adresse (ARP) pour l'interface. J'exécute le logiciel CatOS (ou hybride) sur mon commutateur. Que dois-je faire ?

A. Le fait de configurer les interfaces dans la configuration FWSM (avec la commande nameif) ou sur la carte de commutation multicouche (MSFC) [avec la commande interface vlan] avant qu'elles ne soient configurées sur le commutateur (sur le module supervisor dans CatOS) peut faire apparaître les interfaces comme ne répondant pas du tout, sans entrée ARP ni réponse Internet Control Message Protocol (ICMP).

Si vous avez configuré une interface sur le FWSM ou le MSFC qui appartient aux VLAN pare-feu avant de configurer le commutateur, supprimez l'entrée FWSM ou MSFC, rechargez le module, puis rajoutez l'entrée.

Q. Pourquoi est-ce que je ne peux pas exécuter une commande ping ou faire

passer du trafic par le biais du FWSM ?

A. La traduction d'adresses de réseau (NAT) doit être configurée à l'aide de la commande nat 0 , nat/global ou static pour que le trafic passe par le biais du FWSM d'une interface à niveau de sécurité plus élevé (interface interne) à une interface à niveau de sécurité inférieur (interface externe).

Vous devez également utiliser la commande access-list pour implémenter des listes d'accès qui permettent au trafic de passer par le FWSM. Par défaut, les listes d'accès refusent tout le trafic sur toutes les interfaces (**deny ip any any**). Ce comportement diffère de la configuration par défaut du PIX, qui autorise le trafic d'un niveau de sécurité élevé à un niveau de sécurité inférieur et qui refuse le trafic d'un niveau de sécurité inférieur à un niveau de sécurité plus élevé. Configurez une liste d'accès avec **permit ip any any** et appliquez-la aux interfaces à niveau de sécurité élevé pour que le FWSM se comporte comme le PIX.

Q. Je peux exécuter une commande ping sur l'interface FWSM qui est directement connectée à mon réseau, mais je ne peux pas exécuter une commande ping sur d'autres interfaces. Est-ce normal ?

A. Oui. Il s'agit d'un mécanisme de sécurité intégré qui existe également sur le pare-feu PIX.

Questions de Basculement

Q. Est-ce que je peux configurer le basculement entre deux FWSM qui exécutent des versions différentes de code ?

A. Non. Le basculement requiert que les deux FWSM exécutent la même version du code. Un mécanisme dans la fonctionnalité de basculement vérifie la version d'homologue et empêche le basculement si les versions de code sont différentes. Pour cette raison, vous devez mettre à niveau les deux FWSM en même temps.

Q. Est-ce que je peux configurer le basculement entre deux FWSM dans différents châssis ?

A. Oui. Mais les FWSM doivent être connectés par la couche 2 sur toutes les interfaces. En d'autres termes, toutes les interfaces doivent pouvoir permuter des paquets de diffusion de couche 2 [Protocole de résolution d'adresse (ARP), et ainsi de suite] entre elles. Les paquets de protocole de basculement ne peuvent pas être routés au niveau de la couche 3.

Q. J'ai installé le basculement entre deux FWSM, mais ils ne sont pas synchronisés. Quel a pu être le problème ?

A. Assurez-vous que votre configuration répond aux exigences suivantes en matière de basculement.

- Les deux FWSM doivent exécuter la même version du code.
- Les deux FWSM doivent avoir le même nombre de VLAN.
- Une connexion de couche 2 doit exister entre tous les VLAN sur les FWSM. Si les FWSM

existent dans différents châssis avec une ligne réseau configurée entre eux, vérifiez que tous les VLAN existent et qu'ils sont autorisés sur la ligne réseau.

Q. Est-ce que je peux configurer le basculement pour trois unités FWSM ou plus qui sont réparties sur différents châssis de commutateur ?

A. **Non.** La configuration de basculement est uniquement prise en charge pour une paire de FWSM, par exemple 2 unités. Ces deux unités peuvent être dans un même commutateur ou dans deux commutateurs distincts. Si vous installez le FWSM secondaire dans le même commutateur que le FWSM primaire, vous êtes protégé des pannes au niveau du module. Afin de vous protéger des pannes au niveau du module et des pannes au niveau du commutateur, vous pouvez installer le FWSM secondaire dans un commutateur distinct. FWSM ne coordonne pas le basculement directement avec le commutateur, mais il fonctionne en harmonie avec l'opération de basculement de commutateur. Reportez-vous à Placement de module intra-châssis et inter-châssis pour plus d'informations.

Divers

Q. Le FWSM a une étiquette qui indique : « Ne retirez pas la carte lorsque la lumière d'état est verte ou lorsqu'une corruption de disque peut se produire. » Qu'est-ce que cela signifie ?

A. Vous ne pouvez retirer le module pare-feu qu'après avoir coupé l'alimentation à l'aide de l'une de ces méthodes. (Il n'y a aucune préférence pour une méthode particulière.)

- Utilisez l'interface de ligne de commande (CLI) du commutateur et émettez l'une de ces commandes.CatOS - **set module power down mod**Logiciel de Cisco IOS® - *aucun emplacement de* **module de power enable**
- Appuyez sur le bouton **shutdown** sur la lame.
- Arrêtez physiquement le châssis.

Vous pouvez retirer le module sans risque quand la lumière d'état n'est pas verte.

Q. J'ai utilisé la commande show module , et mon FWSM a un état faulty/other. Que dois-je faire ?

A. Reportez-vous à cette liste de contrôle pour dépanner un FWSM avec un état faulty/other.

- Assurez-vous que vous exécutez une version prise en charge du code sur votre commutateur.
- Assurez-vous que le FWSM peut coexister avec les autres lames situées dans le même châssis. Reportez-vous à Notes de version pour Catalyst 6500 et/ou Software Advisor (clients inscrits uniquement) pour plus d'informations.
- Si vous exécutez du code CatOS/hybride sur votre commutateur, réinitialisez la configuration pour l'emplacement occupé par le module FWSM. Pour cela, employez ces commandes.Saisissez **set module power down mod** pour mettre le FWSM hors tension.Saisissez **clear config mod** pour effacer la configuration du commutateur associé à cet emplacement et pour mettre le module sous tension.

Reportez-vous à cette documentation pour plus d'informations.

- Liste de contrôle des défaillances matérielles pour les commutateurs des gammes Catalyst 4000, 5000 et 6000 exécutant CatOS
- Résolution des problèmes matériels et courants sur les commutateurs de la gamme Catalyst 6000 exécutant le logiciel Cisco IOS intégré (mode natif)

Si vous continuez de rencontrer des problèmes, contactez l'assistance technique de Cisco pour obtenir davantage d'informations de dépannage.

Q. Où puis-je trouver la documentation FWSM ?

A. Les notes de version pour le FWSM sont disponibles sous les Notes de version de la gamme Catalyst 6500. Pour plus d'informations, reportez-vous à la documentation disponible à la page Module de services pare-feu de la gamme Cisco Catalyst 6500.

Q. Où puis-je trouver des informations sur les messages d'erreur que je vois sur mon FWSM ?

A. Le Décodeur de message d'erreur (clients inscrits uniquement) fournit des détails sur de nombreux messages d'erreur FWSM. La documentation du produit sur les messages système contient également des informations utiles. Si vous avez besoin d'une assistance supplémentaire, contactez l'assistance technique de Cisco.

Q. Où puis-je trouver des informations sur les bogues existants pour mon FWSM ?

A. Des détails sur les bogues existants sont disponibles dans la boîte à outils de bogue (clients inscrits uniquement).

Q. Quelles sont les différences entre le pare-feu PIX et le module de services pare-feu ?

A. Le PIX et le FWSM sont basés sur du code semblable. Cependant, il y a deux différences fondamentales. Le PIX (offre assistance) fournit une fonctionnalité VPN et IDS. Le FWSM ne fournit pas de fonctionnalité VPN et ID, car ces fonctionnalités sont offertes dans d'autres cartes de ligne. Reportez-vous à la Fiche technique du module de services Intrusion Detection System (IDSM-2) de la gamme Catalyst 6500 pour plus d'informations sur le module de services Intrusion Detection System (IDSM-2) de la gamme Catalyst 6500. Reportez-vous à la Fiche technique produit du module de services VPN IPSec Catalyst 6500 pour plus d'informations sur le module de services VPN IPSec Catalyst 6500.

Reportez-vous à cette documentation pour connaître les différences mineures entre PIX et FWSM :

- Documentation technique sur PIX
- Notes de publication PIX
- **Références des commandes du pare-feu PIX**
- Documentation technique sur FWSM
- Notes de publication FWSM
- Références des commandes du pare-feu FWSM

Q. Je ne peux pas émettre des commandes access-group sur le FWSM par

interface. FWSM semble prendre seulement un groupe d'accès par interface.
Pourquoi ?

A. Lorsque vous émettez ces commandes dans FWSM, seule la dernière commande **access-group** apparaît :

```
access-group allow_icmp in interface outside
access-group allow_caltech in interface outside
```

Cela est dû au fait que FWSM autorise seulement une liste d'accès par interface par direction.

Q. Quelles sont les informations stockées dans les entrées xlate dans FWSM ?

A. Les entrées Xlate stockent ces informations :

1. **Interface source** — Il s'agit de l'interface que le paquet a reçu, par exemple, outside.
2. **Adresse IP source** — Il s'agit de l'adresse IP source du paquet.
3. **Adresse IP traduite** — S'il n'y a pas d'instructions NAT, l'adresse IP traduite et l'adresse IP source sont identiques.
4. **Interface de destination** — L'interface que le paquet quitte selon la recherche dans la table de routage de l'adresse IP de destination du paquet.

Q. Qu'est-ce que les valeurs et les statistiques dans show perfmon sur FWSM impliquent ?

A. Employez la commande **show perfmon** afin de capturer des informations sur les performances du FWSM.

```
FWSM#show perfmon FWSM#show console-output Context: my_context PERFMON STATS: Current Average
Xlates 0/s 0/s Connections 0/s 0/s TCP Conns 0/s 0/s UDP Conns 0/s 0/s URL Access 0/s 0/s URL
Server Req 0/s 0/s WebSns Req 0/s 0/s TCP Fixup 0/s 0/s TCP Intercept 0/s 0/s HTTP Fixup 0/s 0/s
FTP Fixup 0/s 0/s AAA Authen 0/s 0/s AAA Author 0/s 0/s AAA Account 0/s 0/s
```

La colonne Current montre les statistiques dans l'intervalle actuel, tandis que la dernière colonne Average montre la moyenne cumulative depuis le dernier effacement des statistiques. Ceci apparaît sous la forme /s, car il s'agit d'un débit et non d'une valeur absolue.

Les statistiques montrées dans la sortie de la commande sont mises à jour à un intervalle de 120 secondes par défaut. L'intervalle peut être modifié avec la commande **perfmon interval**.

```
FWSM#perfmon interval 20
```

Cela signifie que les statistiques signalées dans la colonne Current sont calculées toutes les 20 secondes. En outre, chaque fois que vous sélectionnez la commande **show perfmon**, les débits sont calculés avec les statistiques à ce moment-là.

Le FWSM n'inclut pas de port de console série, mais certains messages sont seulement affichés sur un port de console, notamment la sortie des commandes **show perfmon** et **perfmon**. Employez la commande **show output-console** pour afficher la mémoire tampon de console, qui inclut la sortie de la commande **show perfmon**.

Q. Les performances sur le FWSM sont-elles impactées avec la commande no monitor session servicemodule ?

A. La session span est requise sur le FWSM en raison d'une limitation matérielle d'un ASIC pour la réplication du trafic. FWSM a besoin d'un ASIC pour la réplication de paquet et la session de span passe les paquets au commutateur pour cela à l'aide de la session span. Le trafic affecté par cette commande est EtherChannel distribué, Multicast et GRE. Il est recommandé de configurer la session span et de ne pas la supprimer.

Si, pour une raison quelconque, vous devez la supprimer, assurez-vous que vous n'avez pas répliqué le trafic de nature, par exemple EtherChannel distribué, qui peut être affecté par la Notice de champ : FN - 61935 - Incompatibilité du module de services de la gamme Catalyst 6500 et de la gamme 7600 avec EtherChannel distribué la recirculation de paquet.

Q. Pouvez-vous augmenter la mémoire afin d'enregistrer plus de listes de contrôle d'accès (ACL) ?

A. La mémoire allouée pour les ACL dans FWSM est limitée. Reportez-vous à Caractéristiques - Limites des règles pour plus d'informations sur l'allocation des ressources FWSM.

Quand la mémoire allouée pour ACLs dans un contexte est dépassée, vous pouvez recevoir l'un de ces messages d'erreur :

- `ERREUR : Incapable d'ajouter, limite de config de liste d'accès atteinte`
- `ERREUR : Incapable d'ajouter des règles de stratégie`
- `Incapable d'ajouter un trou à la règle de stratégie`

Certaines listes d'accès utilisent plus de mémoire que d'autres. Cela dépend du type de liste d'accès, et la limite réelle que le système peut prendre en charge est inférieure au maximum. Le mappage entre les règles et l'allocation de mémoire ne correspond pas à un mappage un pour un. En fait, cela dépend de la règle et la façon dont elle est programmée dans le matériel.

Vous avez deux options pour l'optimisation de l'utilisation mémoire d'ACE :

- Récapitulez et simplifiez vos entrées ACE ; ceci peut être fait si vous suivez ces méthodes recommandées :Utilisez des adresses d'hôtes contiguës autant que possible. Rassemblez les instructions d'hôte dans les ACE/groupes d'objets en réseaux.Utilisez any au lieu de réseaux et des réseaux plutôt que des hôtes si possible.Essayez de simplifier les groupes d'objets. Ceci peut vous économiser des centaines d'ACE lorsque les ACL sont développées. Pr exemple, regroupez toutes les instructions de port individuelles dans une seule plage.
- Repartitionnez la mémoire allouée pour ACE sur chaque partition. Ceci requiert le redémarrage du module FWSM.Le FWSM partitionne la mémoire allouée au ACE en 12 partitions et alloue la mémoire correspondante à chacune d'elles. Ceci se fait automatiquement. Dans les versions 2.3(2) et ultérieures, vous pouvez utiliser le gestionnaire de ressources pour redistribuer la mémoire selon le nombre de contextes que vous avez.Émettez la commande **show context count** afin de vérifier combien de contextes vous avez. Vous pouvez alors vérifier ceci avec la configuration. Recherchez ensuite le nombre de partitions qui utilisent la commande **show resource acl-partition**. Si vous avez plus de partitions que votre contexte défini, vous pouvez alors accorder le nombre de partitions au nombre de contextes avec la commande **resource acl-partition nombre de partitions**.Vous devez enregistrer la configuration et redémarrer le FWSM après cela. La commande précédente vous donne plus de mémoire pour l'ACE ; cette quantité e mémoire peut être suffisante ou non selon l'ACE que vous ajoutez au contexte.**Attention :** Un inconvénient du remappage précédent est que si vous voulez ajouter un autre contexte, vous devez allouer de

nouveau le mappage de mémoire. Ceci va réduire la mémoire disponible pour chaque contexte et peut rompre les définitions actuelles d'ACE. La mémoire allouée au FWSM est une quantité finie qui est découpée selon une méthode prédéterminée ou par le biais de l'allocation manuelle de ressources, comme indiqué précédemment.

De la version 4.0 en avant, FWSM a introduit une caractéristique appelée la « optimisation d'ACL » qui utilise efficacement les ressources en mémoire pour des rubriques de liste ACL de multiple enregistrant. Ceci traite un algorithme intégré qui agrège automatiquement les rubriques de liste ACL dans la mesure du possible sans manquer l'efficacité de n'importe quel un rubrique de liste ACL. Cet algorithme joint ensemble des sous-réseaux contigus visés dans différents rubriques de liste ACL dans une déclaration simple, et détecte des superpositions dans des plages de port. Cette caractéristique est activée à l'aide d'une commande et, après que l'optimisation soit exécutée, des aspects complets de configuration d'ACL différemment de la configuration (d'origine) précédente d'ACL. Cette configuration ordonnée d'ACL pourrait être retenue après vérification et l'optimisation pourrait être désactivée pour sauvegarder la surcharge de calcul CPU. Pour plus d'informations sur cette caractéristique, référez-vous à la section d'optimisation de groupe de liste d'accès qui décrit la fonctionnalité de l'optimisation d'ACL avec ses détails de configuration.

La version 4.0 a également introduit une autre caractéristique appelée « la capacité de liste d'accès d'Increasaed ». Avec cette configuration, les utilisateurs ont maintenant la capacité d'enregistrer 130,000 rubriques de liste ACL dans le mode de contexte unique et 150,000 entrées dans le mode de multicontext. Pour plus d'informations sur cette caractéristique, référez-vous à la section « de capacité accrue de liste d'accès » dans le bulletin de la version de logiciel 4.0 de Module de services de Pare-feu de Cisco.

Q. Pourquoi la commande capture appliquée au FWSM s'arrête et ne capture pas le trafic dès qu'une autre commande capture est appliquée sur l'interface ?

A. Quand vous configurez la capture « z » sur la même interface où la capture « x » est déjà appliquée, la capture « z » remplace alors la capture « x ». La capture active est la dernière attachée à l'interface particulière.

La seule exception est quand la liste d'accès sur la capture « x » se superpose à la liste d'accès de la capture « z ». Si c'est le cas, les deux captures continuent alors à capturer le trafic où les listes d'accès se superposent.

Q. Comment est-ce que je peux résoudre l'erreur de dépassement de délai NP-PCcmplx logger frame sur FWSM ?

A. Rechargez le module FWSM afin de résoudre cette erreur.

Q. Comment est-ce que je peux configurer FWSM pour employer l'Interception TCP pour défendre contre certains types d'inondations de synchronisation ?

A. Vous pouvez configurer FWSM pour employer l'Interception TCP pour défendre contre certains types d'inondations de synchronisation. Référez-vous à l'Interception TCP FWSM et au pour en savoir plus expliqué par Témoins de synchronisation.

Q. Y aurait-il des problèmes de performance pour traiter des paquets d'IPv6 ?

A. Oui. Vous pouvez voir des problèmes de performance en envoyant le trafic d'IPv6, comme paquet doit être traité par la CPU. En raison des différences en traitant le trafic d'ipv4 et le trafic d'IPv6 par la CPU, le traitement de paquets d'IPv6 entraînera certains problèmes de performance avec le FWSM.

Q. Comment est-ce que je peux empêcher le FWSM de répondre à un serveur éloigné avec sa propre adresse MAC ?

A. Vous devez désactiver la configuration de proxy ARP sur l'interface spécifiée avec cette commande :

```
"sysopt noproxyarp <interface>"
```

Pour plus d'informations sur la caractéristique de proxy ARP, référez-vous au guide de référence des commandes FWSM.

Q. Comment est-ce que je peux empêcher les appels par FWSM d'être lâché ?

A. Afin de résoudre ce problème, inspection de débronchement pour le h323 et H225 :

```
policy-map global_policy
class inspection_default
no inspect h323 h225
no inspect h323 ras
```

Q. Comment est-ce que je peux résoudre des problèmes de traduction NAT sur FWSM ?

A. Afin de résoudre ce problème, utilisez la commande de xlate-contournement. Par défaut, le FWSM crée des sessions NAT pour toutes les connexions même si vous n'utilisez pas NAT. Vous pouvez désactiver des sessions NAT pour le trafic non traduit, qui s'appelle le contournement de xlate, afin d'éviter la limite NAT maximum de session. La commande de xlate-**contournement** peut être configurée comme affichée :

```
hostname(config)#xlate-bypass
```

Référez-vous à configurer le contournement de Xlate pour plus d'informations sur comment à la configuration du xlate-contournement.

Informations connexes

- Exemple de configuration de base de FWSM
- Documentation du module de services pare-feu
- Page de support produit du module de services pare-feu
- Support et documentation techniques - Cisco Systems