Exemple de configuration de base de FWSM

Contenu

Introduction

Ce document décrit comment configurer la configuration de base du Module de services de Pare-feu (FWSM) a installé dans les Commutateurs ou le Routeurs de la gamme Cisco 7600 de gamme Cisco 6500. Ceci inclut la configuration de l'adresse IP, du NATing de routage, statique et dynamique par défaut, des déclarations de Listes de contrôle d'accès (ACL) afin de permettre le trafic désiré ou bloquer le trafic non désiré, des serveurs d'applications comme Websense pour l'inspection du trafic sur Internet du réseau intérieur, et le web server pour les internautes.

Remarque: Dans un scénario facilement disponible FWSM (ha), le Basculement peut seulement avec succès sync quand les clés de licence sont exactement identiques entre les modules. Par conséquent, le Basculement ne peut pas fonctionner entre le FWSMs avec différents permis.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Module de services de Pare-feu qui exécute la version de logiciel 3.1 et plus tard
- Commutateurs de gamme Catalyst 6500, avec requis les composants comme affiché :Engine de superviseur avec le logiciel de Cisco IOS®, qui est connu comme Cisco IOS de superviseur, ou le système d'exploitation de Catalyst (SYSTÈME D'EXPLOITATION). Voir le tableau pour l'engine et les versions logicielles prises en charge de superviseur.Carte de commutation multicouche (MSFC) 2 avec le logiciel de Cisco IOS. Voir le tableau pour les versions logicielles prises en charge de Cisco IOS.

[1]Le FWSM ne prend en charge pas le superviseur 1 ou 1A.

[2]When que vous utilisez le SYSTÈME D'EXPLOITATION de Catalyst sur le superviseur, vous peut utiliser l'un de ces versions logicielles prises en charge de Cisco IOS sur le MSFC. Quand vous utilisez le logiciel de Cisco IOS sur le superviseur, vous utilisez la même release sur le MSFC.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Produits connexes

Cette configuration peut également être utilisée pour le Routeurs de la gamme Cisco 7600, avec requis les composants comme affichée :

- Engine de superviseur avec le logiciel de Cisco IOS. Voir le tableau pour l'engine de superviseur et les versions logicielles prises en charge de Cisco IOS.
- MSFC2 avec le logiciel de Cisco IOS. Voir le tableau pour les versions logicielles prises en charge de Cisco IOS.

Conventions

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

Informations générales

Le FWSM est un à rendement élevé, économie de l'espace, le module de pare-feu dynamique qui installe dans les Commutateurs de gamme Catalyst 6500 et le Routeurs de la gamme Cisco 7600.

Les Pare-feu protègent les réseaux intérieurs contre l'accès non autorisé par des utilisateurs sur un réseau extérieur. Le Pare-feu peut également protéger les réseaux intérieurs entre eux, par exemple, quand vous gardez un réseau de ressources humaines séparé d'un réseau utilisateur. Si vous avez des ressources de réseau qui doivent être à la disposition d'un utilisateur externe, tel

qu'un Web ou un ftp server, vous pouvez placer ces ressources sur un réseau indépendant derrière le Pare-feu, appelé une zone démilitarisée (DMZ). Le Pare-feu permet l'accès limité au DMZ, mais parce que le DMZ inclut seulement les serveurs publics, une attaque là affecte seulement les serveurs et n'affecte pas l'autre des réseaux d'intérieur. Vous pouvez également contrôler quand accès utilisateur intérieur en dehors des réseaux, par exemple, l'accès à Internet, si vous permettez seulement certaines adresses, exigent l'authentification ou l'autorisation, ou coordonnent avec un serveur externe de Filtrage URL.

Le FWSM inclut beaucoup de fonctionnalité avancée, telle que les plusieurs contextes de sécurité qui sont semblables aux Pare-feu virtualisés, transparents (Pare-feu de couche 2) ou conduit (exécution de Pare-feu de couche 3), centaines d'interfaces, et beaucoup plus de caractéristiques.

Pendant la discussion des réseaux connectés à un Pare-feu, le réseau extérieur est devant le Pare-feu, le réseau intérieur est protégé et derrière le Pare-feu, et un DMZ, alors que derrière le Pare-feu, permet l'accès limité aux utilisateurs externes. Puisque le FWSM vous permet de configurer beaucoup d'interfaces avec des stratégies de sécurité diverses, qui inclut beaucoup d'interfaces internes, beaucoup DMZs, et même beaucoup d'interfaces extérieures si désiré, ces termes sont utilisés dans un sens général seulement.

Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Remarque: Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisées dans un environnement de laboratoire.

Configurations

Ce document utilise les configurations suivantes :

- Configuration de commutateur de gamme Catalyst 6500
- Configuration FWSM

Configuration de commutateur de gamme Catalyst 6500

1. Vous pouvez installer le FWSM dans les Commutateurs de gamme Catalyst 6500 ou le Routeurs de la gamme Cisco 7600. La configuration des deux gamme est identique et la gamme désigné génériquement dans ce document sous le nom du **commutateur**.**Remarque:** Vous devez configurer le commutateur convenablement avant que vous configuriez FWSM.

2. **Assignez les VLAN au Module de services de Pare-feu** — Cette section décrit comment assigner des VLAN au FWSM. Le FWSM n'inclut aucune interface physique externe. Au lieu de cela, il utilise des interfaces VLAN. Assigner des VLAN au FWSM est semblable à la façon dont vous assignez un VLAN à un port de commutateur ; le FWSM inclut une interface interne au module de matrice de commutateur, si présent, ou le bus partagé.**Remarque:** Référez-vous à la section configurante VLAN du guide de configuration du logiciel de Commutateurs de Catalyst 6500 pour plus d'informations sur la façon créer des VLAN et les assigner aux ports de commutateur.**Instructions VLAN :**Vous pouvez utiliser des VLAN privés avec le FWSM. Assignez le VLAN primaire au FWSM ; le FWSM traite automatiquement le trafic de VLAN secondaire.Vous ne pouvez pas utiliser des VLAN réservés.Vous ne pouvez pas utiliser le VLAN 1.Si vous utilisez le Basculement FWSM dans le même châssis de commutateur, n'assignez pas le VLAN que vous avez réservé pour des transmissions de Basculement et d'avec état à un port de commutateur. Mais, si vous utilisez le Basculement entre le châssis, vous devez inclure les VLAN dans le port de joncteur réseau entre le châssis.Si vous n'ajoutez pas les VLAN au commutateur avant que vous les assigniez au FWSM, les VLAN sont enregistrés dans la base de données d'engine de superviseur et sont envoyés au FWSM dès qu'ils seront ajoutés au commutateur.Assignez les VLAN au FWSM avant que vous les assigniez au MSFC.Des VLAN qui ne remplissent pas cette condition sont jetés de la plage des VLAN que vous tentez d'assigner sur le FWSM.**Assignez les VLAN au FWSM en logiciel de Cisco IOS :**Dans le Cisco IOS logiciel, créez jusqu'à 16 groupes VLAN de Pare-feu, et puis affectez les groupes au FWSM. Par exemple, vous pouvez assigner tous les VLAN à un groupe, ou vous pouvez créer un groupe interne et un groupe extérieur, ou vous pouvez créer un groupe pour chaque client. Chaque groupe peut contenir des VLAN illimités.Vous ne pouvez pas assigner le même VLAN à de plusieurs groupes de Pare-feu ; cependant, vous pouvez affecter de plusieurs groupes de Pare-feu à un FWSM et vous pouvez affecter un seul groupe de Pare-feu à plusieurs FWSMs. Les VLAN que vous voulez assigner à plusieurs FWSMs, par exemple, peuvent résider dans un groupe distinct des VLAN qui sont seuls à chaque FWSM.Terminez-vous les étapes afin d'assigner des VLAN au FWSM :`Router(config)#`**`firewall vlan-group firewall_group vlan_range`** `Le vlan_range` peut être un ou plusieurs VLAN, par exemple, 2 à 1000 et à partir de 1025 à 4094, identifié comme numéro unique (n) comme 5, 10, 15 ou plage (n-x) comme 5-10, 10-20.**Remarque:** Les ports et les ports WAN conduits consomment des VLAN internes, ainsi il est possible que les VLAN dans la plage 1020-1100 puissent déjà être en service.**Exemple :**
`firewall vlan-group 1 10,15,20,25` Terminez-vous les étapes afin d'affecter les groupes de Pare-feu au FWSM.`Router(config)#`**`firewall module module_number vlan-group firewall_group`** `Le firewall_group` est un ou plusieurs nombres de groupe comme numéro unique (n) comme 5 ou plage comme 5-10.**Exemple :**
`firewall module 1 vlan-group 1` **Assignez les VLAN au FWSM en logiciel de système d'exploitation de Catalyst** — en logiciel Catalyst OS, vous assignez une liste de VLAN au FWSM. Vous pouvez assigner le même VLAN à plusieurs FWSMs si désiré. La liste peut contenir des VLAN illimités.Terminez-vous les étapes afin d'assigner des VLAN au FWSM.`Console> (enable)`**`set vlan vlan_list firewall-vlan mod_num`** `Le vlan_list` peut être un ou plusieurs VLAN, par exemple, 2 à 1000 et à partir de 1025 à 4094, identifié comme numéro unique (n) comme 5, 10, 15 ou plage (n-x) comme 5-10, 10-20.
3. **Ajoutez les interfaces virtuelles commutées au MSFC** — Un VLAN défini sur le MSFC s'appelle une interface virtuelle commutée. Si vous assignez le VLAN utilisé pour le SVI au FWSM, alors les artères MSFC entre le FWSM et autre posent 3 VLAN.Pour des raisons de

sécurité, par défaut, seulement un SVI peut exister entre le MSFC et le FWSM. Par exemple, si vous misconfigure le système avec le multiple SVI, vous pouvez accidentellement permettre au trafic pour passer autour du FWSM si vous assignez les les deux les VLAN intérieurs et extérieurs au MSFC.Terminez-vous les étapes afin de configurer le SVI`Router(config)#` **`interface vlan vlan_number`** `Router(config-if)#` **`ip address address mask`**
Exemple :
`interface vlan 20 ip address 192.168.1.1 255.255.255.0`

Configuration de commutateur de gamme Catalyst 6500

`!--- Output Suppressed` `firewall vlan-group 1 10,15,20,25`
`firewall module 1 vlan-group 1 interface vlan 20 ip`
`address 192.168.1.1 255.255.255.0` `!--- Output Suppressed`

Remarque: Session dedans au FWSM du commutateur avec la commande appropriée pour votre système d'exploitation de commutateur :

- Logiciel Cisco IOS :**`Router#session slot <number> processor 1`**
- Logiciel Catalyst OS :`Console> (enable)` **`session module_number`**

(Facultatif) partageant des VLAN avec d'autres modules de service — si le commutateur a d'autres modules de service, par exemple, engine de contrôle d'application (ACE), il est possible que vous deviez partager quelques VLAN avec ces modules de service. Référez-vous à la conception de module de service avec ACE et au FWSM pour plus d'informations sur la façon optimiser la configuration FWSM quand vous travaillez avec de tels autres modules.

Configuration FWSM

1. **Configurez les interfaces pour FWSM** — Avant que vous puissiez permettre le trafic par le FWSM, vous devez configurer un nom d'interface et une adresse IP. Vous devriez également changer le niveau de Sécurité du par défaut, qui est 0. Si vous nommez une interface `à l'intérieur`, et vous ne placez pas le niveau de Sécurité explicitement, alors le FWSM place le niveau de Sécurité à 100.**Remarque:** Chaque interface doit avoir un niveau de Sécurité de 0 (le plus bas) à 100 (le plus élevé). Par exemple, vous devriez assigner votre la plupart de réseau sécurisé, tel que le réseau d'hôte interne, au niveau 100, alors que le réseau connecté extérieur à l'Internet peut être le niveau 0. D'autres réseaux, tels que DMZs, peuvent être dans l'intervalle.Vous pouvez ajouter n'importe quel ID DE VLAN à la configuration, mais seulement les VLAN, par exemple, 10, 15, 20 et 25, qui sont assignés au FWSM par le commutateur peuvent passer le trafic. Employez la **commande show vlan** afin de visualiser tous les VLAN assignés au FWSM.
   `interface vlan 20 nameif outside security-level 0 ip address 192.168.1.2 255.255.255.0`
   `interface vlan 10 nameif inside security-level 100 ip address 10.1.1.1 255.255.255.0`
   `interface vlan 15 nameif dmz1 security-level 60 ip address 192.168.2.1 255.255.255.224`
   `interface vlan 25 nameif dmz2 security-level 50 ip address 192.168.3.1 255.255.255.224`
   Conseil : Dans la commande de *<name> de* **nameif**, le *nom* est une chaîne de texte jusqu'à 48 caractères et ne distingue pas les majuscules et minuscules. Vous pouvez changer le nom si vous ressaisissez cette commande avec une nouvelle valeur. N'entrez pas dans le forme no, parce que cette commande entraîne toutes les commandes qui se rapportent à ce nom à supprimer.
2. **Configurez le default route :**
   `route outside 0.0.0.0 0.0.0.0 192.168.1.1` Un default route identifie l'adresse IP de

passerelle (192.168.1.1) auquel FWSM envoie tous les paquets IP pour lesquels il n'a pas une artère instruite ou statique. Un default route est simplement une artère statique avec 0.0.0.0/0 comme adresse IP de destination. Les artères qui identifient une destination spécifique ont la priorité au-dessus du default route.

3. **NAT dynamique** traduit un groupe de vraies adresses (10.1.1.0/24) à un groupe d'adresses tracées (192.168.1.20-192.168.1.50) qui sont routable sur le réseau de destination. Le groupe tracé peut inclure moins d'adresses que le vrai groupe. Quand un hôte que vous voulez se traduire accède au réseau de destination, le FWSM lui assigne une adresse IP du groupe tracé. La traduction est ajoutée seulement quand le vrai hôte initie la connexion. La traduction est en place seulement pour la durée de la connexion, et un utilisateur donné n'empêche pas d'entrer la même adresse IP après les temps de traduction.
nat (inside) 1 10.1.1.0 255.255.255.0 global (outside) 1 192.168.1.20-192.168.1.50 netmask 255.255.255.0 access-list Internet extended deny ip any 192.168.2.0 255.255.255.0 access-list Internet extended permit ip any any access-group Internet in interface inside Vous devez créer un ACL afin de refuser le trafic du réseau intérieur 10.1.1.0/24 pour entrer dans le réseau DMZ1 (192.168.2.0) et pour permettre les autres genres de trafic à l'Internet par l'application de l'*Internet d'*ACL à l'interface interne en tant que vers l'intérieur direction pour le trafic entrant.
4. **NAT statique** crée une traduction fixe de vraie adresse aux adresses tracées. Avec NAT dynamique et PAT, chaque hôte utilise une adresse ou un port différente pour chaque traduction ultérieure. Puisque l'adresse tracée est identique pour chaque connexion consécutive avec NAT statique, et une règle de conversion persistante existe, NAT statique permet à des hôtes sur le réseau de destination pour initier le trafic à un hôte traduit, s'il y a une liste d'accès qui le permet.La principale différence entre NAT dynamique et une plage d'adresses pour NAT statique est que NAT statique permet à un serveur distant pour initier une connexion à un hôte traduit, s'il y a une liste d'accès qui le permet, alors que NAT dynamique ne fait pas. Vous avez besoin également d'un nombre équivalent d'adresses tracées en tant que vraies adresses avec NAT statique.
static (dmz1,outside) 192.168.1.6 192.168.2.2 netmask 255.255.255.255 static (dmz2,outside) 192.168.1.10 192.168.3.2 netmask 255.255.255.255 access-list outside extended permit tcp any host 192.168.1.10 eq http access-list outside extended permit tcp host 192.168.1.30 host 192.168.1.6 eq pcanywhere-data access-list outside extended permit udp host 192.168.1.30 host 192.168.1.6 eq pcanywhere-status access-list inbound extended permit udp any host 216.70.55.69 range 8766 30000 access-group outside in interface outside Ce sont les deux déclarations NAT statiques affichées. Le premier est censé pour traduire le vrai IP 192.168.2.2 sur l'interface interne à l'IP tracé 192.168.1.6 sur le sous-réseau extérieur à condition que l'ACL permette au trafic de la source 192.168.1.30 à l'IP tracé 192.168.1.6 afin d'accéder au serveur de Websense dans le réseau DMZ1. De même, la deuxième déclaration NAT statique a signifié pour traduire le vrai IP 192.168.3.2 sur l'interface interne à l'IP tracé 192.168.1.10 sur le sous-réseau extérieur à condition que l'ACL permettent au trafic de l'Internet à l'IP tracé 192.168.1.10 afin d'accéder au web server dans le réseau DMZ2 et avoir le numéro de port d'UDP de l'ordre de 8766 à 30000.
5. L'ordre d'URL-**serveur** indique le serveur qui exécute l'application de Filtrage URL de Websense. La limite est 16 serveurs URL en mode de contexte unique et quatre serveurs URL dans la multimode, mais vous pouvez utiliser seulement une application, N2H2 ou Websense, à la fois. Supplémentaire, si vous changez votre configuration sur les dispositifs de sécurité, ceci ne met pas à jour la configuration sur le serveur d'applications. Ceci doit être fait séparément, dans l'accord aux instructions de constructeur.L'ordre d'URL-**serveur** doit être configuré avant que vous émettiez la commande de **filtre** pour HTTPS et FTP. Si

tous les serveurs URL sont retirés de la liste de serveur, alors toutes les commandes de filtre liées au Filtrage URL sont également retirées.Une fois que vous indiquez le serveur, activez le service de Filtrage URL avec la commande **URL de filtre**.

`url-server (dmz1) vendor websense host 192.168.2.2 timeout 30 protocol TCP version 1 connections 5` La commande **URL de filtre** permet la prévention de l'accès des utilisateurs sortants du World Wide Web URLS que vous indiquez avec l'application de filtrage de Websense.

`filter url http 10.1.1.0 255.255.255.0 0 0`

Configuration FWSM

```
!--- Output Suppressed interface vlan 20 nameif outside
security-level 0 ip address 192.168.1.2 255.255.255.0
interface vlan 10 nameif inside security-level 100 ip
address 10.1.1.1 255.255.255.0 interface vlan 15 nameif
dmz1 security-level 60 ip address 192.168.2.1
255.255.255.224 interface vlan 25 nameif dmz2 security-
level 50 ip address 192.168.3.1 255.255.255.224 passwd
fl0wer enable password treeh0u$e route outside 0 0
192.168.1.1 1 url-server (dmz1) vendor websense host
192.168.2.2 timeout 30 protocol TCP version 1
connections 5 url-cache dst 128 filter url http 10.1.1.0
255.255.255.0 0 0 !--- When inside users access an HTTP
server, FWSM consults with a !--- Websense server in
order to determine if the traffic is allowed. nat
(inside) 1 10.1.1.0 255.255.255.0 global (outside) 1
192.168.1.20-192.168.1.50 netmask 255.255.255.0 !---
Dynamic NAT for inside users that access the Internet
static (dmz1,outside) 192.168.1.6 192.168.2.2 netmask
255.255.255.255 !--- A host on the subnet 192.168.1.0/24
requires access to the Websense !--- server for
management that use pcAnywhere, so the Websense server
!--- uses a static translation for its private address.
static (dmz2,outside) 192.168.1.10 192.168.3.2 netmask
255.255.255.255 !--- A host on the Internet requires
access to the Webserver, so the Webserver !--- uses a
static translation for its private address. access-list
Internet extended deny ip any 192.168.2.0 255.255.255.0
access-list Internet extended permit ip any any access-
group Internet in interface inside !--- Allows all
inside hosts to access the outside for any IP traffic,
!--- but denies them access to the dmz1 access-list
outside extended permit tcp any host 192.168.1.10 eq
http !--- Allows the traffic from the internet with the
destination IP address !--- 192.168.1.10 and destination
port 80 access-list outside extended permit tcp host
192.168.1.30 host 192.168.1.6 eq pcanywhere-data access-
list outside extended permit udp host 192.168.1.30 host
192.168.1.6 eq pcanywhere-status !--- Allows the
management host 192.168.1.30 to use !--- pcAnywhere on
the Websense server access-list inbound extended permit
udp any host 216.70.55.69 range 8766 30000 !--- Allows
udp port number in the range of 8766 to 30000. access-
group outside in interface outside access-list WEBSENSE
extended permit tcp host 192.168.2.2 any eq http access-
group WEBSENSE in interface dmz1 !--- The Websense
server needs to access the Websense !--- updater server
on the outside. !--- Output Suppressed
```

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Employez l'OIT afin d'afficher une analyse de la sortie de la commande show.

1. Visualisez les informations sur le module dans l'accord à votre du système d'exploitation afin de vérifier que le commutateur reconnaît le FWSM et l'a apporté en ligne :Logiciel Cisco IOS :`Router#show module Mod Ports Card Type Model Serial No. --- ----- -------------------- ---------- ---------- ----------- 1 2 Catalyst 6000 supervisor 2 (Active) WS-X6K-SUP2-2GE SAD0444099Y 2 48 48 port 10/100 mb RJ-45 ethernet WS-X6248-RJ-45 SAD03475619 3 2 Intrusion Detection System WS-X6381-IDS SAD04250KV5 4 6 Firewall Module WS-SVC-FWM-1 SAD062302U4` Logiciel Catalyst OS :`Console>**show module [mod-num]** The following is sample output from the show module command: Console> show module Mod Slot Ports Module-Type Model Sub Status --- ---- ----- ------------------------ ------------------ --- ------ 1 1 2 1000BaseX Supervisor WS-X6K-SUP1A-2GE yes ok 15 1 1 Multilayer Switch Feature WS-F6K-MSFC no ok 4 4 2 Intrusion Detection Syste WS-X6381-IDS no ok **5 5 6 Firewall Module WS-SVC-FWM-1 no ok** 6 6 8 1000BaseX Ethernet WS-X6408-GBIC no ok`**Remarque:** La commande de **show module** affiche six ports pour le FWSM. Ce sont des ports internes qui sont groupés ensemble comme EtherChannel.
2. `Router#**show firewall vlan-group** Group vlans ----- ------ 1 10,15,20 51 70-85 52 100`
3. `Router#**show firewall module** Module Vlan-groups 5 1,51 8 1,52`
4. Sélectionnez la commande pour votre du système d'exploitation afin de visualiser la partition de boot en cours :Logiciel Cisco IOS :`Router#show boot device [mod num]` **Exemple :**`Router#**show boot device** [mod:1 ]: [mod:2 ]: [mod:3 ]: [mod:4 ]: cf:4 [mod:5 ]: cf:4 [mod:6 ]: [mod:7 ]: cf:4 [mod:8 ]: [mod:9 ]:`Logiciel Catalyst OS :`Console> (enable) **show boot device mod_num`** **Exemple :**`Console> (enable) **show boot device 6** Device BOOT variable = cf:5`

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

1. **Plaçant la partition de boot par défaut** — Par défaut, le FWSM démarre de la partition de l'application **cf:4**. Mais, vous pouvez choisir de démarrer de la partition de l'application **cf:5** ou dans la partition de la maintenance **cf:1**. Afin de changer la partition de boot par défaut, sélectionnez la commande pour votre système d'exploitation :Logiciel Cisco IOS :`Router(config)#boot device module mod_num cf:n` Là où n est 1 (maintenance), 4 (application), ou 5 (application).Logiciel Catalyst OS :`Console> (enable) **set boot device cf:n mod_num`** Là où n est 1 (maintenance), 4 (application), ou 5 (application).
2. **Remettant à l'état initial le FWSM en logiciel de Cisco IOS** — Afin de remettre à l'état initial le FWSM, sélectionnez la commande comme affichée :`Router#**hw-module module mod_num reset [cf:n] [mem-test-full]`** **Les Cf :** l'argument **n** est la partition, 1 (maintenance), 4 (application), ou 5 (application). Si vous ne spécifiez pas la partition, la partition par défaut est utilisée, qui est typiquement **cf:4**.**La mem-test-pleine** option exécute un plein test mémoire, qui prend approximativement six minutes.**Exemple :**`Router#**hw-mod module 9 reset** Proceed with reload of module? [confirm] y % reset issued for module 9 Router# 00:26:55:%SNMP-5-MODULETRAP:Module 9 [Down] Trap 00:26:55:SP:The PC in slot 8 is shutting down. Please wait ...` Pour le **logiciel Catalyst OS** :`Console> (enable) **reset mod_num [cf:n]`** Là où **Cf : n** est la partition, 1 (maintenance), 4 (application), ou 5 (application). Si vous ne spécifiez pas la partition, la partition par défaut est utilisée, qui est typiquement **cf:4**.

Remarque: Le NTP ne peut pas être configuré sur FWSM, parce qu'il prend ses configurations du

commutateur.

Problème : Incapable de passer le trafic VLAN de FWSM au capteur 4270 IPS

Vous ne pouvez pas passer le trafic de FWSM aux capteurs IPS.

Solution

Afin de forcer le trafic par l'IPS, l'astuce est de créer un VLAN auxiliaire afin d'efficacement diviser un de votre courant VLAN en deux et les jeter un pont sur alors ensemble. Vérifiez cet exemple avec VLAN 401 et 501 afin de clarifier :

- Si vous voulez balayer le trafic sur **VLAN** principal **401**, créez un autre VLAN **VLAN 501** (VLAN auxillary). Désactivez alors l'interface VLAN 401, qui les hôtes dans actuellement l'utilisation 401 en tant que leur passerelle par défaut.
- Prochaine interface de l'enable VLAN 501 avec la *même* adresse cette vous avez précédemment désactivé sur l'interface VLAN 401.
- Placez une des interfaces IPS dans VLAN 401 et l'autre dans VLAN 501.

Tout que vous devez faire est de déplacer la passerelle par défaut pour VLAN 401 sur VLAN 501. Vous devez faire les modifications semblables pour des VLAN si présent. Notez que les VLAN sont essentiellement comme des segments de RÉSEAU LOCAL. Vous pouvez avoir une passerelle par défaut sur une partie différente de fil que les hôtes qui l'utilisent.

Question de paquets en panne dans FWSM

Comment est-ce que je peux résoudre les paquets en panne émets dans FWSM ?

Solution

Émettez la commande de fin-unité du NP de sysopt en mode de configuration globale afin de résoudre le problème de paquet en panne dans FWSM. Cette commande a été introduite dans la version 3.2(5) FWSM et s'assure que des paquets sont expédiés dans la même commande qu'ils ont été reçus.

Problème : Incapable de passer asymétriquement des paquets routés par le Pare-feu

Vous ne pouvez pas passer asymétriquement des paquets routés par le Pare-feu.

Solution

Émettez la commande de TCP-état-contournement de connection advanced-options de positionnement dans le mode de configuration de classe afin de passer asymétriquement des paquets routés par le Pare-feu. Cette commande a été introduite dans la version 3.2(1) FWSM.

Support de NetFlow dans FWSM

FWSM prend en charge-il le NetFlow ?

Solution

Le NetFlow n'est pas pris en charge dans FWSM.

Informations connexes

- Page de support de Module de services pare-feu de la gamme Cisco Catalyst 6500
- Page de support de Commutateurs de la gamme Cisco Catalyst 6500
- Page de support de routeur de gamme Cisco 7600
- Interception TCP FWSM et Témoins de synchronisation expliqués
- Support et documentation techniques - Cisco Systems