Exemple de configuration de base de FWSM

Table des matières

[Introduction](#)
[Conditions préalables](#)
[Exigences](#)
[Composants utilisés](#)
[Produits connexes](#)
[Conventions](#)
[Informations générales](#)
[Configurer](#)
[Diagramme du réseau](#)
[Configurations](#)
[Vérifier](#)
[Dépannage](#)
[Problème : Impossible de transmettre le trafic VLAN de FWSM au capteur IPS 4270](#)
[Solution](#)
[Problème de paquets hors ordre dans FWSM](#)
[Solution](#)
[Problème : Impossible de faire passer des paquets routés de manière asymétrique à travers le pare-feu](#)
[Solution](#)
[Prise en charge de Netflow dans FWSM](#)
[Solution](#)
[Informations connexes](#)

Introduction

Ce document décrit comment configurer la configuration de base du module de services de pare-feu (FWSM) installé dans les commutateurs de la gamme Cisco 6500 ou les routeurs de la gamme Cisco 7600. Cela inclut la configuration de l'adresse IP, le routage par défaut, la traduction d'adresses réseau statique et dynamique, les instructions des listes de contrôle d'accès (ACL) afin d'autoriser le trafic souhaité ou de bloquer le trafic indésirable, les serveurs d'applications comme Websense pour l'inspection du trafic Internet à partir du réseau interne, et le serveur Web pour les utilisateurs Internet.

Remarque : dans un scénario de haute disponibilité FWSM, le basculement ne peut se synchroniser que lorsque les clés de licence sont exactement les mêmes entre les modules. Par conséquent, le basculement ne peut pas fonctionner entre les FWSM avec des licences différentes.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à 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 les versions 3.1 et ultérieures du logiciel
- Commutateurs de la gamme Catalyst 6500, avec les composants requis comme indiqué :

    a. Supervisor Engine avec le logiciel Cisco IOS®, connu sous le nom de superviseur Cisco IOS ou de système d'exploitation Catalyst. Reportez-vous au Tableau pour connaître les versions du moteur de supervision et des logiciels pris en charge.

    b. Carte MSFC (Multilayer Switch Feature Card) 2 avec logiciel Cisco IOS. Reportez-vous au Tableau pour connaître les versions du logiciel Cisco IOS prises en charge.

	Moteurs de supervision[1]
Modification de la version du logiciel Cisco IOS	
Logiciel Cisco IOS version 12.2(18)SXF et ultérieure	720, 32
Logiciel Cisco IOS version 12.2(18)SXF2 et ultérieure	2, 720, 32
Modularité du logiciel Cisco IOS	
Logiciel Cisco IOS Version 12.2(18)SXF4	720, 32
Catalyst OS[2]	
8.5(3) et postérieures	2, 720, 32

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

[2]Lorsque vous utilisez Catalyst OS sur le superviseur, vous pouvez utiliser l'une de ces versions du logiciel Cisco IOS prises en charge sur la carte MSFC. Lorsque vous utilisez le logiciel Cisco IOS sur le superviseur, vous utilisez la même version sur le MSFC.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Produits connexes

Cette configuration peut également être utilisée pour les routeurs de la gamme Cisco 7600, avec les composants requis, comme indiqué :

- Supervisor Engine avec le logiciel Cisco IOS. Reportez-vous au Tableau pour connaître les versions du moteur de supervision et du logiciel Cisco IOS prises en charge.
- MSFC 2 avec le logiciel Cisco IOS. Reportez-vous au Tableau pour connaître les versions du logiciel Cisco IOS prises en charge.

Conventions

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

Informations générales

Le module FWSM est un module de pare-feu dynamique hautes performances, peu encombrant, qui s'installe dans les commutateurs de la gamme Catalyst 6500 et les routeurs de la gamme Cisco 7600.

Les pare-feu protègent les réseaux internes contre les accès non autorisés par les utilisateurs sur un réseau externe. Le pare-feu peut également protéger les réseaux internes les uns des autres, par exemple, lorsque vous séparez un réseau de ressources humaines d'un réseau d'utilisateurs. Si vous disposez de ressources réseau devant être disponibles pour un utilisateur externe, tel qu'un serveur Web ou FTP, vous pouvez placer ces ressources sur un réseau distinct derrière le pare-feu, appelé zone démilitarisée (DMZ). Le pare-feu autorise un accès limité à la DMZ, mais comme celle-ci inclut uniquement les serveurs publics, une attaque n'affecte que les serveurs et n'affecte pas les autres réseaux internes. Vous pouvez également contrôler le moment où les utilisateurs internes accèdent à des réseaux externes, par exemple l'accès à Internet, si vous autorisez uniquement certaines adresses à sortir, si vous exigez une authentification ou une autorisation, ou si vous vous coordonnez avec un serveur de filtrage d'URL externe.

Le FWSM inclut de nombreuses fonctionnalités avancées, telles que plusieurs contextes de sécurité similaires aux pare-feu virtualisés, le fonctionnement transparent (couche 2) ou routé (couche 3) du pare-feu, des centaines d'interfaces et bien d'autres fonctionnalités.

Lors de la discussion sur les réseaux connectés à un pare-feu, le réseau externe se trouve devant le pare-feu, le réseau interne est protégé et derrière le pare-feu, et une DMZ, tandis que derrière le pare-feu, permet un accès limité aux utilisateurs externes. Étant donné que le FWSM vous permet de configurer de nombreuses interfaces avec des stratégies de sécurité variées, qui incluent de nombreuses interfaces internes, de nombreuses DMZ et même de nombreuses interfaces externes si vous le souhaitez, ces termes sont utilisés dans un sens général uniquement.

Configurer

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

document.

Remarque : Utilisez l’outil de recherche de commandes (clients enregistrés seulement) pour en savoir plus sur les commandes employées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Remarque : les schémas d'adressage 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 des commutateurs de la gamme Catalyst 6500
- Configuration FWSM

Configuration des commutateurs de la gamme Catalyst 6500

1. Vous pouvez installer le module FWSM dans les commutateurs de la gamme Catalyst 6500 ou dans les routeurs de la gamme Cisco 7600. La configuration des deux séries est identique et les séries sont désignées de manière générique dans ce document sous le nom de commutateur.

   Remarque : vous devez configurer le commutateur correctement avant de configurer FWSM.

2. Assign VLAN to the Firewall Services Module : cette section décrit comment attribuer des VLAN au FWSM. Le FWSM n'inclut aucune interface physique externe. Au lieu de cela, il utilise des interfaces VLAN. L'attribution de VLAN au FWSM est similaire à l'attribution d'un VLAN à un port de commutateur ; le FWSM inclut une interface interne vers le module de matrice de commutation, le cas échéant, ou vers le bus partagé.

   Remarque : référez-vous à la section Configuration des VLAN du Guide de configuration du logiciel des commutateurs Catalyst 6500 pour plus d'informations sur la façon de créer des VLAN et de l'attribuer aux ports de commutateur.

   a. Directives VLAN :

      a. Vous pouvez utiliser des VLAN privés avec le FWSM. Attribuez le VLAN principal au FWSM ; Le FWSM gère automatiquement le trafic VLAN secondaire.

      b. Vous ne pouvez pas utiliser de VLAN réservés.

      c. Vous ne pouvez pas utiliser le VLAN 1.

d. Si vous utilisez le basculement FWSM dans le même châssis de commutateur, n'attribuez pas le ou les VLAN que vous avez réservés pour le basculement et les communications avec état à un port de commutateur. Cependant, si vous utilisez le basculement entre les châssis, vous devez inclure les VLAN dans le port trunk entre les châssis.

e. Si vous n'ajoutez pas les VLAN au commutateur avant de les affecter au FWSM, les VLAN sont stockés dans la base de données du moteur de supervision et sont envoyés au FWSM dès qu'ils sont ajoutés au commutateur.

f. Attribuez des VLAN au FWSM avant de les attribuer au MSFC.

Les VLAN qui ne remplissent pas cette condition sont ignorés de la plage de VLAN que vous essayez d'attribuer sur le FWSM.

b. Attribuez des VLAN au FWSM dans le logiciel Cisco IOS :

Dans le logiciel Cisco IOS, créez jusqu'à 16 groupes VLAN de pare-feu, puis attribuez les groupes au FWSM. Par exemple, vous pouvez attribuer tous les VLAN à un groupe, ou vous pouvez créer un groupe interne et un groupe externe, ou vous pouvez créer un groupe pour chaque client. Chaque groupe peut contenir un nombre illimité de VLAN.

Vous ne pouvez pas attribuer le même VLAN à plusieurs groupes de pare-feu ; cependant, vous pouvez attribuer plusieurs groupes de pare-feu à un FWSM et vous pouvez attribuer un seul groupe de pare-feu à plusieurs FWSM. Les VLAN que vous souhaitez attribuer à plusieurs FWSM, par exemple, peuvent résider dans un groupe distinct des VLAN qui sont uniques à chaque FWSM.

a. Complétez les étapes afin d'attribuer des VLAN au FWSM :

<#root>

```
Router(config)#
```

firewall vlan-group firewall_group vlan_range

La `plage_vlan` peut être un ou plusieurs VLAN, par exemple, 2 à 1000 et de 1025 à 4094, identifiés comme un nombre unique (n) comme 5, 10, 15 ou une plage (n-x) comme 5-10, 10-20.

Remarque : les ports routés et les ports WAN consomment des VLAN internes. Il est donc possible que des VLAN compris entre 1020 et 1100 soient déjà utilisés.

Exemple :

<#root>

```
firewall vlan-group 1 10,15,20,25
```

b. Complétez les étapes afin d'attribuer les groupes de pare-feu au FWSM.

<#root>

```
Router(config)#
```

firewall module module_number vlan-group firewall_group

Le `firewall_group` est un ou plusieurs numéros de groupe sous la forme d'un numéro unique (n) comme 5 ou d'une plage comme 5-10.

Exemple :

<#root>

firewall module 1 vlan-group 1

c. Attribution de VLAN au FWSM dans le logiciel du système d'exploitation Catalyst : dans le logiciel du système d'exploitation Catalyst, vous attribuez une liste de VLAN au FWSM. Vous pouvez attribuer le même VLAN à plusieurs FWSM si vous le souhaitez. La liste peut contenir un nombre illimité de VLAN.

Complétez les étapes afin d'attribuer des VLAN au FWSM.

<#root>

```
Console> (enable)
```

set vlan vlan_list firewall-vlan mod_num

La `vlan_list` peut être un ou plusieurs VLAN, par exemple, 2 à 1000 et de 1025 à 4094, identifiés comme un nombre unique (n) comme 5, 10, 15 ou une plage (n-x) comme 5-10, 10-20.

3. Ajouter des interfaces virtuelles commutées à la carte MSFC : un VLAN défini sur la carte MSFC est appelé interface virtuelle commutée. Si vous attribuez le VLAN utilisé pour l'interface SVI au FWSM, les routes MSFC entre le FWSM et les autres VLAN de couche 3.

Pour des raisons de sécurité, par défaut, une seule interface SVI peut exister entre le MSFC et le FWSM. Par exemple, si vous avez mal configuré le système avec plusieurs interfaces SVI, vous pouvez accidentellement autoriser le trafic à circuler autour du FWSM si vous

attribuez les VLAN internes et externes au MSFC.

Suivez les étapes pour configurer l'interface SVI

<#root>

```
Router(config)#
interface vlan vlan_number
Router(config-if)#
ip address address mask
```

Exemple :

<#root>

```
interface vlan 20
ip address 192.168.1.1 255.255.255.0
```

Configuration des commutateurs de la 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 : Connectez-vous au FWSM à partir du commutateur avec la commande appropriée pour votre système d'exploitation de commutateur :

- Logiciel Cisco IOS :

<#root>

```
Router#
session slot
```

```
processor 1
```

- Logiciel Catalyst OS :

<#root>

```
Console> (enable)
session module_number
```

(Facultatif) Partage de VLAN avec d'autres modules de service : si le commutateur dispose d'autres modules de service, par exemple, Application Control Engine (ACE), il est possible que vous deviez partager certains VLAN avec ces modules de service. Référez-vous à Conception de module de service avec ACE et FWSM pour plus d'informations sur la façon d'optimiser la configuration FWSM quand vous travaillez avec de tels autres modules.

Configuration FWSM

1. Configurer les interfaces pour FWSM : avant d'autoriser le trafic via FWSM, vous devez configurer un nom d'interface et une adresse IP. Vous devez également modifier le niveau de sécurité par défaut, qui est 0. Si vous nommez une interface `interne`, et que vous ne définissez pas le niveau de sécurité explicitement, alors le FWSM définit le niveau de sécurité sur 100.

   Remarque : chaque interface doit avoir un niveau de sécurité compris entre 0 (le plus bas) et 100 (le plus élevé). Par exemple, vous devez affecter votre réseau le plus sécurisé, tel que le réseau hôte interne, au niveau 100, tandis que le réseau externe connecté à Internet peut être de niveau 0. D'autres réseaux, tels que les DMZ, peuvent se trouver entre les deux.

   Vous pouvez ajouter n'importe quel ID de VLAN à la configuration, mais seuls les VLAN, par exemple, 10, 15, 20 et 25, qui sont affectés au FWSM par le commutateur peuvent transmettre le trafic. Utilisez la commande show vlan afin d'afficher tous les VLAN attribués au FWSM.

<#root>

```
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 nameif <name>, le nom est une chaîne de texte de 48 caractères maximum et ne respecte pas la casse. Vous pouvez modifier le nom si vous entrez à nouveau cette commande avec une nouvelle valeur. N'entrez pas la forme no, car cette commande entraîne la suppression de toutes les commandes qui font référence à ce nom.

2. Configurez la route par défaut :

<#root>

```
route outside 0.0.0.0 0.0.0.0 192.168.1.1
```

Une route par défaut identifie l'adresse IP de passerelle (192.168.1.1) à laquelle FWSM envoie tous les paquets IP pour lesquels il n'a pas de route apprise ou statique. Une route par défaut est simplement une route statique avec 0.0.0.0/0 comme adresse IP de destination. Les routes qui identifient une destination spécifique sont prioritaires sur la route par défaut.

3. La fonction NAT dynamique traduit un groupe d’adresses réelles (10.1.1.0/24) en un pool d’adresses mappées (192.168.1.20-192.168.1.50) routables sur le réseau de destination. Le pool mappé peut inclure moins d'adresses que le groupe réel. Lorsqu'un hôte que vous voulez traduire accède au réseau de destination, le FWSM lui attribue une adresse IP du pool mappé. La traduction est ajoutée uniquement lorsque l'hôte réel initie la connexion. La traduction n'est en place que pendant la durée de la connexion et un utilisateur donné ne conserve pas la même adresse IP après l'expiration du délai de traduction.

<#root>

```
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 une liste de contrôle d'accès afin de refuser le trafic provenant du réseau interne 10.1.1.0/24 pour aller dans le réseau DMZ1 (192.168.2.0) et d'autoriser les autres types de trafic vers Internet via l'application de la liste de contrôle d'accès Internet vers l'interface interne comme direction entrante pour le trafic entrant.

4. La fonction NAT statique crée une traduction fixe des adresses réelles en adresses mappées.Avec la fonction NAT et PAT dynamiques, chaque hôte utilise une adresse ou un port différent pour chaque traduction suivante. Étant donné que l'adresse mappée est la même pour chaque connexion consécutive avec la NAT statique et qu'une règle de traduction persistante existe, la NAT statique permet aux hôtes du réseau de destination d'initier le trafic vers un hôte traduit, s'il existe une liste d'accès qui l'autorise.

   La principale différence entre la NAT dynamique et une plage d'adresses pour la NAT statique est que la NAT statique permet à un hôte distant d'établir une connexion avec un hôte traduit, s'il existe une liste d'accès qui l'autorise, alors que la NAT dynamique ne l'autorise pas. Vous avez également besoin d'un nombre égal d'adresses mappées en tant qu'adresses réelles avec la NAT statique.

   <#root>

   ```
   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
   ```

   Il s'agit des deux instructions NAT statiques affichées. La première est destinée à traduire l'IP réelle 192.168.2.2 sur l'interface interne en l'IP mappée 192.168.1.6 sur le sous-réseau externe, à condition que la liste de contrôle d'accès autorise le trafic de la source 192.168.1.30 vers l'IP mappée 192.168.1.6 afin d'accéder au serveur Websense dans le réseau DMZ1. De même, la deuxième instruction NAT statique visait à traduire l'adresse IP réelle 192.168.3.2 sur l'interface interne en l'adresse IP mappée 192.168.1.10 sur le sous-réseau externe, à condition que la liste de contrôle d'accès autorise le trafic d'Internet vers l'adresse IP mappée 192.168.1.10 afin d'accéder au serveur Web dans le réseau DMZ2 et ait le numéro de port udp dans la plage de 8766 à 30000.

5. La commande url-server désigne le serveur qui exécute l'application de filtrage d'URL Websense. La limite est de 16 serveurs d'URL en mode de contexte unique et de quatre serveurs d'URL en mode multiple, mais vous ne pouvez utiliser qu'une seule application, N2H2 ou Websense, à la fois. En outre, si vous modifiez votre configuration sur l'appliance de sécurité, cela ne met pas à jour la configuration sur le serveur d'applications. Cette opération doit être effectuée séparément, conformément aux instructions du fournisseur.

   La commande url-server doit être configurée avant d'émettre la commande filter pour HTTPS et FTP. Si tous les serveurs d'URL sont supprimés de la liste des serveurs, toutes les

commandes de filtrage associées au filtrage d'URL sont également supprimées.

Une fois que vous avez désigné le serveur, activez le service de filtrage d'URL avec la commande filter url.

<#root>

url-server (dmz1) vendor websense host 192.168.2.2 timeout 30 protocol TCP version 1 connections 5

La commande filter url permet d'empêcher l'accès des utilisateurs sortants à partir des URL World Wide Web que vous désignez avec l'application de filtrage Websense.

<#root>

filter url http 10.1.1.0 255.255.255.0 0 0

Configuration

```
!--- 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 de

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 tha


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 trans


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



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 destina


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
```

Vérifier

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. Affichez les informations du module en fonction de votre système d'exploitation afin de vérifier que le commutateur accuse réception du FWSM et l'a mis en ligne :
    - Logiciel Cisco IOS :

<#root>

```
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 :

<#root>

```
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 show module affiche six ports pour le FWSM. Il s'agit de ports internes regroupés en tant qu'EtherChannel.

2.

<#root>

```
Router#

show firewall vlan-group

Group vlans
----- ------
   1 10,15,20
   51 70-85
   52 100
```

3.

<#root>

```
Router#

show firewall module

Module Vlan-groups
  5    1,51
  8    1,52
```

4. Entrez la commande correspondant à votre système d'exploitation afin d'afficher la partition de démarrage actuelle :

   - Logiciel Cisco IOS :

     <#root>

     ```
     Router#

     show boot device [mod_num]
     ```

     Exemple :

     <#root>

     ```
     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 :

     <#root>

     ```
     Console> (enable)

     show boot device mod_num
     ```

     Exemple :

```
<#root>

Console> (enable)

show boot device 6

Device BOOT variable = cf:5
```

Dépannage

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

1. Setting the Default Boot Partition : par défaut, le FWSM démarre à partir de la partition d'application cf:4. Mais, vous pouvez choisir de démarrer à partir de la partition cf:5 application ou dans la partition cf:1 maintenance. Afin de changer la partition de démarrage par défaut, entrez la commande pour votre système d'exploitation :

   - Logiciel Cisco IOS :

     ```
     <#root>

     Router(config)#

     boot device module mod_num cf:n
     ```

     Où n est 1 (maintenance), 4 (application) ou 5 (application).

   - Logiciel Catalyst OS :

     ```
     <#root>

     Console> (enable)

     set boot device cf:n mod_num
     ```

     Où n est 1 (maintenance), 4 (application) ou 5 (application).

2. Réinitialisation du FWSM dans le logiciel Cisco IOS : afin de réinitialiser le FWSM, entrez la commande comme indiqué :

   ```
   <#root>

   Router#

   hw-module module mod_num reset [cf:n] [mem-test-full]
   ```

L'argument cf : n est la partition, soit 1 (maintenance), 4 (application), ou 5 (application). Si vous ne spécifiez pas la partition, la partition par défaut est utilisée, qui est généralement cf:4.

L'option mem-test-full exécute un test de mémoire complète, qui prend environ six minutes.

Exemple :

<#root>

```
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 :

<#root>

```
Console> (enable)

reset mod_num [cf:n]
```

Où cf:n est la partition, soit 1 (maintenance), 4 (application), ou 5 (application). Si vous ne spécifiez pas la partition, la partition par défaut est utilisée, qui est généralement cf:4.

Remarque : NTP ne peut pas être configuré sur FWSM, car il prend ses paramètres du commutateur.

Problème : Impossible de transmettre le trafic VLAN de FWSM au capteur IPS 4270

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

Solution

Afin de forcer le trafic via l'IPS, l'astuce consiste à créer un VLAN auxiliaire afin de diviser efficacement l'un de vos VLAN actuels en deux, puis de les relier ensemble. Vérifiez cet exemple avec VLAN 401 et 501 afin de clarifier :

- Si vous voulez analyser le trafic sur le VLAN principal 401, créez un autre VLAN VLAN 501 (VLAN auxiliaire). Ensuite, désactivez l'interface VLAN 401, que les hôtes de la passerelle 401 utilisent actuellement comme passerelle par défaut.

- Activez ensuite l'interface VLAN 501 avec la même adresse que celle précédemment désactivée sur l'interface VLAN 401.
- Placez l'une des interfaces IPS dans le VLAN 401 et l'autre dans le VLAN 501.

Tout ce que vous avez à faire est de déplacer la passerelle par défaut pour VLAN 401 sur VLAN 501. Vous devez faire les modifications similaires pour les VLAN s'il y a lieu. Notez que les VLAN sont essentiellement semblables aux segments LAN. Vous pouvez avoir une passerelle par défaut sur un élément de câble différent de celui des hôtes qui l'utilisent.

Problème de paquets hors ordre dans FWSM

Comment puis-je résoudre le problème des paquets dans le désordre dans FWSM ?

Solution

Émettez la commande sysopt np complete-unit en mode de configuration globale afin de résoudre le problème de paquet hors commande dans FWSM. Cette commande a été introduite dans FWSM Version 3.2(5) et garantit que les paquets sont transférés vers l'extérieur dans le même ordre que celui dans lequel ils ont été reçus.

Problème : Impossible de faire passer des paquets routés de manière asymétrique à travers le pare-feu

Vous ne pouvez pas passer des paquets routés de manière asymétrique à travers le pare-feu.

Solution

Émettez la commande set connection advanced-options tcp-state-bypass en mode de configuration de classe afin de passer des paquets routés de façon asymétrique à travers le pare-feu. Cette commande a été introduite dans FWSM Version 3.2(1).

Prise en charge de Netflow dans FWSM

FWSM prend-il en charge Netflow ?

Solution

Netflow n'est pas pris en charge dans FWSM.

Informations connexes

- Page d'assistance du module de services de pare-feu Cisco Catalyst 6500
- Page d'assistance des commutateurs Cisco Catalyst 6500
- Page d'assistance des routeurs Cisco 7600
- Interception TCP FWSM et cookies SYN expliqués

- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.