FWSM の基本設定例

目次

概要

このドキュメントでは、Cisco 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータのいずれかにインストールしたファイアウォール サービス モジュール（FWSM）の基本設定方法について説明しています。 この基本設定には、IP アドレスの設定、デフォルト ルーティング、スタティック NAT とダイナミック NAT、必要なトラフィックの許可や不要なトラフィックのブロックを行うための ACL（アクセス コントロール リスト）文、内部ネットワークでのインターネット トラフィックを検査するための Websense のようなアプリケーション サーバ、およびインターネット ユーザ用の Webserver などがあります。

注: FWSM ハイ アベイラビリティ（HA）シナリオでは、ライセンス キーがモジュール間で同一である場合に限り、フェールオーバーの同期が成功します。 そのため、ライセンスの異なる FWSM 間ではフェールオーバーは機能しません。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- バージョン 3.1 以降のソフトウェアが稼働するファイアウォール サービス モジュール
- 次の必須コンポーネントを搭載した Catalyst 6500 シリーズ スイッチスーパーバイザ Cisco IOS、または Catalyst オペレーティング システム（OS）として知られる、Cisco IOS® スーパーバイザ エンジン。 サポートされるスーパーバイザ エンジンとソフトウェア リリースについては、表を参照してください。Cisco IOS ソフトウェア搭載のマルチレイヤ スイッチ フィーチャ カード（MSFC）2。 サポートされる Cisco IOS ソフトウェア リリースについては、表を参照してください。

1 FWSM では、スーパーバイザ 1 や 1A はサポートされていません。

2 スーパーバイザで Catalyst OS を使用する場合、MSFC ではこれらのサポート対象 Cisco IOS ソフトウェア リリースを使用できます。 スーパーバイザで Cisco IOS ソフトウェアを使用する場合、MSFC でも同じリリースを使用します。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

関連製品

この設定は、次の必須コンポーネントを搭載した Cisco 7600 シリーズ ルータでも使用できます。

- Cisco IOS ソフトウェアを搭載したスーパーバイザ エンジン。 サポートされるスーパーバイザ エンジンと Cisco IOS ソフトウェア リリースについては、表を参照してください。
- Cisco IOS ソフトウェアが搭載された MSFC 2。 サポートされる Cisco IOS ソフトウェア リリースについては、表を参照してください。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

FWSM は、Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータにインストールする、高性能で省スペースのステートフルなファイアウォール モジュールです。

ファイアウォールにより、内部ネットワークが外部ネットワークのユーザによる不正アクセスから保護されます。 ファイアウォールでは、さらに、人事部のネットワークをユーザのネットワークから隔離する場合など、内部ネットワーク間の保護を行うこともできます。 Web または FTP サーバーなどのネットワーク リソースを外部ユーザが使用できるようにする必要がある場合、非

武装地帯（DMZ）と呼ばれるファイアウォール背後の隔離されたネットワークに、これらのリソースを配置できます。 ファイアウォールにより DMZ への制限付きアクセスが許可されますが、DMZ に置かれているのはパブリック サーバだけなので、攻撃により影響を受けるのはこれらのパブリック サーバのみで、その他の内部ネットワークへの影響はありません。 また、内部ユーザがインターネットなどの外部ネットワークにアクセスする場合には、特定の外部アドレスのみを許可したり、認証や許可を要求したり、あるいは外部 URL フィルタリング サーバと協調して、アクセスを制御できます。

FWSM では、仮想化ファイアウォール、透過（レイヤ 2）ファイアウォール、またはルーティングされた（レイヤ 3）ファイアウォールに類似した複数のセキュリティ コンテキスト、および数百種類のインターフェイスなど、多種多様な拡張機能を用意しています。

ファイアウォールに接続されたネットワークについての説明では、外部ネットワークとはファイアウォールの前面にあるもの、内部ネットワークとはファイアウォールの背後で保護されているもの、DMZ とはファイアウォールの背後にありながら、外部ユーザには制限付きでアクセスが許可されているものを表します。 FWSM では、さまざまなセキュリティ ポリシーで数多くのインターフェイスを設定できます。この中には多くの内部インターフェイスや DMZ に加え、必要に応じてさらに多くの外部インターフェイスが含まれます。そのため、これらの用語は、一般的な意味での使用に限定されます。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

注: この設定で使用している IP アドレス スキームは、インターネット上で正式にルーティング可能なものではありません。 これらはラボ環境で使用された RFC 1918 でのアドレスです。

設定

このドキュメントでは、次の設定を使用します。

- Catalyst 6500 シリーズ スイッチの設定
- FWSM 設定

Catalyst 6500 シリーズ スイッチの設定

1. FWSM は、Catalyst 6500 シリーズ スイッチや Cisco 7600 シリーズ ルータにインストールできます。 両シリーズでの設定は同じで、このドキュメント内では両シリーズを**スイッチ**と総称しています。**注:** FWSM を設定する前に、スイッチを適切に設定する必要があります。
2. **VLAN をファイアウォール サービス モジュールに割り当てる**：このセクションは VLAN を FWSM に割り当てる方法について説明しています。 FWSM には、外部物理インターフェイ

スは搭載されていません。 代わりに、VLAN インターフェイスが使用されます。 FWSM への VLAN の割り当ては、スイッチ ポートへの VLAN の割り当て方法と同様です。 FWSM には、スイッチ ファブリック モジュール（存在する場合）または共有バスへの内部インターフェイスが組み込まれています。**注:** VLAN を作成し、スイッチ ポートに割り当てる方法の詳細については、『Catalyst 6500 シリーズ スイッチ ソフトウェア コンフィギュレーション ガイド』の「VLAN の設定」の項を参照してください。**VLAN ガイドライン**：FWSM では、プライベート VLAN を使用できます。 プライマリ VLAN を FWSM に割り当てます。 FWSM はセカンダリ VLAN トラフィックを自動的に処理します。予約された VLAN は使用できません。VLAN 1 は使用できません。同一スイッチ シャーシ内で FWSM フェールオーバーを使用する場合は、フェールオーバーおよびステートフル通信のために確保してある VLAN をスイッチ ポートに割り当てないでください。 ただし、シャーシ間のフェールオーバーを使用する場合、シャーシの間のトランク ポートに VLAN を含める必要があります。 FWSM に割り当てる前に VLAN をスイッチに追加しないと、VLAN はスーパーバイザ エンジン データベースに格納され、VLAN をスイッチに追加するとすぐに FWSM に送信されます。VLAN は、MSFC に割り当てる前に FWSM に割り当ててください。この条件を満たしていない VLAN は、FWSM での割り当てを試行する対象の VLAN の範囲からは削除されます。**Cisco IOS ソフトウェアで VLAN を FWSM に割り当てる。**Cisco IOS ソフトウェアで、最大 16 のファイアウォール VLAN グループを作成し、グループを FWSM に割り当てます。 たとえば、すべての VLAN を 1 つのグループに割り当てることも、内部グループと外部グループを作成することも、カスタマーごとに 1 つのグループを作成することもできます。 それぞれのグループには、VLAN を無制限に含めることができます。同じ VLAN を複数のファイアウォール グループに関連付けることはできません。 ただし、複数のファイアウォール グループを 1 つの FWSM に割り当てたり、1 つのファイアウォール グループを複数の FWSM に割り当てたりすることはできます。 たとえば、複数の FWSM に割り当てたい VLAN を、各 FWSM に対して一意な VLAN とは別のグループに含めることができます。 VLAN を FWSM に割り当てるには、次の手順を実行します。`Router(config)#`**`firewall vlan-group firewall_group vlan_range`** vlan_range には、2 ～ 1000 や 1025 ～ 4094 などの複数の VLAN を設定でき、5、10、15 のような単一の数字（n）または 5-10、10-20 のような範囲（n-x）のいずれかで指定します。**注:** ルーティングされたポートと WAN ポートでは内部 VLAN が使用されます。そのため、1020 ～ 1100 の範囲の VLAN はすでに使用されている可能性があります。**例：**

`firewall vlan-group 1 10,15,20,25` ファイアウォール グループを FWSM に割り当てるには、次の手順を実行します。`Router(config)#`**`firewall module module_number vlan-group firewall_group`** firewall_group には、1 つ以上のグループ番号を設定でき、5 のような単一の数字（n）または 5-10 のような範囲のいずれかで指定します。**例：**

`firewall module 1 vlan-group 1` **Catalyst オペレーティング システム ソフトウェアで FWSM に VLAN を割り当てる**：Catalyst OS ソフトウェアで、VLAN のリストを FWSM に割り当てます。 必要に応じて、同じ VLAN を複数の FWSM に割り当てることができます。 リストには、VLAN を無制限に含めることができます。VLAN を FWSM に割り当てるには、次の手順を実行します。`Console> (enable)`**`set vlan vlan_list firewall-vlan mod_num`** vlan_list には、2 ～ 1000 や 1025 ～ 4094 などの複数の VLAN を設定でき、5、10、15 のような単一の数字（n）または 5-10、10-20 のような範囲（n-x）のいずれかで指定します。

3. **スイッチ仮想インターフェイスを MSFC に追加する**：MSFC 上で定義された VLAN はスイッチ仮想インターフェイスと呼ばれます。 SVI に使用される VLAN を FWSM に割り当てると、MSFC では FWSM とその他のレイヤ 3 VLAN の間のルーティングが行われます。セキュリティ上の理由から、デフォルトでは、MSFC と FWSM の間に配置できる SVI は 1 つだけです。 たとえば、複数の SVI を配置して誤ったシステム設定を行うと、内部 VLAN と外部 VLAN の両方を MSFC に割り当てた場合に、トラフィックが FWSM を誤って通過してし

まう可能性があります。SVI を設定するには、次の手順を実行します。

```
Router(config)#interface vlan vlan_number Router(config-if)#ip address address mask 例：
interface vlan 20 ip address 192.168.1.1 255.255.255.0
```

Catalyst 6500 シリーズ スイッチの設定
!--- 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*

注: 使用しているスイッチのオペレーティング システムに適したコマンドを使用して、スイッチから FWSM へのセッションを確立してください。

- Cisco IOS ソフトウェア：`Router#session slot <number> processor 1`
- Catalyst OS ソフトウェア：`Console> (enable) session module_number`

((オプション) VLAN を他のサービス モジュールと共有する：スイッチにたとえば Application Control Engine (ACE) のような他のサービス モジュールがある場合、一部の VLAN とこれらのサービス モジュールとの共有が必要な場合があります。 このような他のモジュールを使用する場合に FWSM 設定を最適化する方法の詳細は、ACE および FWSM でのサービス モジュール設計を参照してください。

FWSM 設定

1. **FWSM のインターフェイスを設定する**：FWSM からのトラフィックを許可するには、インターフェイス名と IP アドレスを設定する必要があります。 また、セキュリティ レベルをデフォルトの 0 から変更する必要があります。 インターフェイスの名前を inside とし、明示的にセキュリティ レベルを設定しない場合、FWSM はセキュリティ レベルを 100 に設定します。**注:** 各インターフェイスのセキュリティ レベルは、0 (最低) から 100 (最高) にする必要があります。 たとえば、ホスト ネットワーク内部のような最もセキュアなネットワークにはレベル 100 を割り当てる必要がありますが、インターネットに接続する外部ネットワークはレベル 0 でもかまいません。 DMZ など、その他のネットワークにはその中間を設定できます。任意の VLAN ID を設定に追加できますが、トラフィックを渡すことができるのは、スイッチによって FWSM に割り当てられた 10、15、20、25 などの VLAN のみです。 FWSM に割り当てられたすべての VLAN を参照するには、**show vlan** コマンドを使用します。

   ```
   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 ヒント：
   ```

   nameif <name> コマンドで、*name* は 48 文字までのテキスト文字列で、大文字と小文字は区別されません。 新しい値でこのコマンドを再入力する場合、名前を変更できます。no 形式は入力しないでください。このコマンドを使用すると、その名前を参照するすべてのコマンドが削除されてしまいます。
2. **デフォルト ルートを設定します。**

   route outside 0.0.0.0 0.0.0.0 192.168.1.1 デフォルト ルートは、学習されたルートやスタティック ルートのないすべての IP パケットを FWSM が送信するゲートウェイ IP アドレス (192.168.1.1) を示しています。 デフォルト ルートは、宛先 IP アドレスが 0.0.0.0/0 のスタティック ルートです。 特定の宛先が指定されたルートは、デフォルト ルートよりも優先されます。
3. **ダイナミック NAT** は、実アドレス (10.1.1.0/24) のグループを、宛先ネットワークでルー

ティング可能な、マッピングされたアドレスのプール（192.168.1.20 ~ 192.168.1.50）に変換します。 マッピングされたプールに含めることができるアドレスの数は、リアル グループと比べて少なくなります。 変換するホストが宛先ネットワークにアクセスすると、マッピングされたプールから IP アドレスが FWSM によって割り当てられます。 変換は、リアル ホストが接続を開始しなければ追加されません。 変換が有効なのは接続期間中のみであり、変換のタイムアウト後に所定のユーザが同じ IP アドレスを維持し続けることはありません。

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 ユーザは次のような ACL を作成する必要があります。まず、内部ネットワーク 10.1.1.0/24 から DMZ1 ネットワーク（192.168.2.0）へのトラフィックは拒否し、逆に、内向きの着信トラフィックである内部インターフェイスに ACL *Internet* を適用して、インターネットへのその他のトラフィックは許可するような ACL です。

4. **スタティック NAT** では、実アドレスからマッピング アドレスへの固定変換が作成されます。ダイナミック NAT および PAT では、各ホストは変換するたびに異なるアドレスまたはポートを使用します。 マップ アドレスは同じであり、永続的な変換規則が存在するため、スタティック NAT では、それを許可するアクセス リストがあれば、宛先ネットワーク上のホストで変換済みホストへのトラフィックを開始できます。ダイナミック NAT と、スタティック NAT 用のアドレス範囲の主な違いは、スタティック NAT では有効なアクセス リストがあればリモート ホストが変換済みホストへの接続を開始できるのに対し、ダイナミック NAT ではこれができないことです。 また、スタティック NAT では、リアル アドレスと同じ数のマップ アドレスが必要です。

   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 これらは、2 種類のスタティック NAT 文です。 1 つ目の文は、内部インターフェイス上のリアル IP 192.168.2.2 を、外部サブネット上のマッピングされた IP 192.168.1.6 に変換するという意味で、DMZ1 ネットワーク上の Websense サーバにアクセスするために、ACL ではマッピングされた IP 192.168.1.6 へのソース 192.168.1.30 からのトラフィックが許可されています。 同様に 2 つ目のスタティック NAT 文は、内部インターフェイス上の実 IP 192.168.3.2 を、外部サブネット上のマッピングされた IP 192.168.1.10 に変換することを意味し、ACL では、DMZ2 ネットワーク上の Web サーバにアクセスするために、インターネットからマッピングされた IP 192.168.1.10 へのトラフィックが許可され、8766 から 30000 までの範囲の udp ポート番号が設定されています。

5. **url-server** コマンドでは、Websense URL フィルタリング アプリケーションを実行するサーバを指定します。 シングル コンテキスト モードでは URL サーバは 16 まで、マルチ モードでは 4 までという制限がありますが、一度に使用できるアプリケーションは N2H2 または Websense のいずれか 1 つです。 さらに、セキュリティ アプライアンスで設定を変更しても、アプリケーション サーバの設定はアップデートされません。 アプリケーション サーバの更新は、ベンダーの指示に従って個別に行う必要があります。HTTPS および FTP に対して **filter** コマンドを発行する前に、**url-server** コマンドを設定する必要があります。 すべての URL サーバをサーバ リストから削除すると、URL フィルタリングに関連するすべてのフィルタ コマンドも削除されます。サーバを指定してから、**filter url** コマンドを使用して URL フィルタリング サービスを有効にします。

   url-server (dmz1) vendor websense host 192.168.2.2 timeout 30 protocol TCP version 1 connections 5 filter url コマンドを使用すると、Websense フィルタリング アプリケーション

で指定した World Wide Web URL からの発信ユーザのアクセスを防御できます。

```
filter url http 10.1.1.0 255.255.255.0 0 0
```

FWSM 設定

```
!--- 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
```

確認

このセクションでは、設定が正常に機能していることを確認します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

1. オペレーティング システムに応じたモジュール情報を参照することにより、スイッチが FWSM に確認応答し、FWSM をオンラインにしたことを確認してください。Cisco IOS ソフトウエア：`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` Catalyst OS ソフトウエア：`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`**注:** show module コマンドでは、FWSM に対して 6 つのポートが表示されます。 これらは、EtherChannel としてグループ化された内部ポートです。
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. 現在のブート パーティションを参照するには、次のようにオペレーティング システムに対するコマンドを入力します。Cisco IOS ソフトウエア：`Router#show boot device [mod_num]` **例**：`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 ]`:Catalyst OS ソフトウエア：`Console> (enable) show boot device mod_num` **例**：`Console> (enable) show boot device 6 Device BOOT variable = cf:5`

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

1. **デフォルトのブート パーティションの設定**：デフォルトで FWSM は **cf:4** アプリケーション パーティションから起動します。 ただし、**cf:5** アプリケーション パーティションからのブート、または **cf:1** メンテナンス パーティションのブートを選択できます。 デフォルト ブート パーティションを変更するには、オペレーティング システムに対するコマンドを入力します。Cisco IOS ソフトウエア：`Router(config)#boot device module mod_num cf:n` ここで、n は 1（メンテナンス）、4（アプリケーション）、または 5（アプリケーション）です。Catalyst OS ソフトウエア：`Console> (enable) set boot device cf:n mod_num` ここで、n は 1（メンテナンス）、4（アプリケーション）、または 5（アプリケーション）です。
2. **Cisco IOS ソフトウエアでの FWSM のリセット**：FWSM をリセットするには、次のようにコマンドを入力します。`Router#hw-module module mod_num reset [cf:n] [mem-test-full]` **cf: n** 引数はパーティションを示し、1（メンテナンス）、4（アプリケーション）、または 5（アプリケーション）のいずれかになります。 パーティションを指定しないと、デフォルト パーティションが使用されます。通常は **cf:4** です。**mem-test-full** オプションを使用すると、フル メモリ テストが実行され、約 6 分で完了します。**例**：`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 ...` **Catalyst OS ソフトウエア**の場合：`Console> (enable) reset mod_num [cf:n]` **cf: n** はパーティションを示し、1（メンテナンス）、4（アプリケーション）、または 5（アプリケーション）のいずれかになります。 パーティションを指定しないと、デフォルト パーティションが使用されます。通常は **cf:4** です。

注: FWSM では、設定はスイッチから取得されるため、NTP を設定することはできません。

問題： FWSM からの VLAN トラフィックを IPS Sensor 4270 に転送できない

FWSM から IPS センサーにはトラフィックを転送できません。

解決策

強制的に IPS を経由してトラフィックを転送するには、補助 VLAN を作成して現在の VLAN の 1 つを事実上 2 つに分割し、その後 2 つをブリッジします。 理解をより明確にするために、ここで VLAN 401 および 501 の例を示します。

- メインの **VLAN 401** 上でトラフィックをスキャンする場合は、別の vlan **VLAN 501**（補助 VLAN）を作成します。 次に、401 内のホストが現在デフォルト ゲートウェイとして使用する VLAN インターフェイス 401 を無効にします。
- 次に、VLAN 401 インターフェイス上で無効にしたものと*同じ*アドレスで VLAN 501 インターフェイスを有効にします。
- VLAN 401 内に IPS インターフェイスの一方を置き、もう一方を VLAN 501 内に置きます。

ユーザが実施する必要があるのは、VLAN 401 のデフォルト ゲートウェイを VLAN 501 に移動することだけです。 VLAN が複数存在する場合は、各 VLAN に対して同様の変更を行う必要があります。 VLAN は基本的に LAN セグメントと同様であることに注意してください。 ホストが使用するものと異なる有線ネットワーク上にデフォルトのゲートウェイを置くことができます。

FWSM でのパケット順序不正の問題

FWSM 内のパケット順序不正の問題をどのように解決できますか。

解決策

FWSM 内のパケット順序不正の問題を解決するには、グローバル コンフィギュレーション モードで sysopt np completion-unit コマンドを発行します。 このコマンドは、FWSM バージョン 3.2(5) で導入され、パケットが受信したのと同じ順序で転送されることが保証されます。

問題： 非対称にルーティングされたパケットがファイアウォールを通過できない

非対称にルーティングされたパケットはファイアウォールを通過させることができません。

解決策

非対称にルーティングされたパケットがファイアウォールを通過できるようにするには、クラス コンフィギュレーション モードで set connection advanced-options tcp-state-bypass コマンドを発行します。 このコマンドは、FWSM バージョン 3.2(1) で導入されました。

FWSM の NetFlow サポート

FWSM は NetFlow をサポートしますか。

解決策

NetFlow は、FWSM ではサポートされていません。

関連情報

- Cisco Catalyst 6500 シリーズ ファイアウォール サービス モジュールに関するサポート ページ
- Cisco Catalyst 6500 シリーズ スイッチに関するサポート ページ (英語)
- Cisco 7600
- FWSM による TCP インターセプトと SYN クッキーの説明
- テクニカルサポートとドキュメント - Cisco Systems