CHAPTER 2

ASA サービス モジュール を使用するためのスイッチの設定

この章では、Catalyst 6500 シリーズ スイッチを ASASM と使用するために設定する方法について説明します。この章で説明する作業を行う前に、スイッチに付属のマニュアルに従って、スイッチ ポートへの VLAN 割り当てをはじめ、スイッチの基本的なプロパティを設定してください。

この章は、次の項で構成されています。

スイッチに関する情報

Catalyst 6500 シリーズ スイッチに ASASM をインストールできます。スイッチにはスイッチ（スーパーバイザ エンジン）とルータ（MSFC）が組み込まれています。ASASM とスイッチは、単一の 20 GB インターフェイスで接続されています。

スイッチのスーパーバイザ エンジンと統合型の MSFC ルータの両方で Cisco IOS ソフトウェアがサポートされています。

（注） Catalyst オペレーティング システム ソフトウェアはサポートされていません。

ASASM は独自の OS で動作します。

（注） ASASM はその独自のオペレーティング システムを実行するので、Cisco IOS ソフトウェアをアップグレードしても ASASM の動作には影響しません。

ASASM および Cisco IOS バージョンのハードウェアとソフトウェアの互換性マトリクスを表示するには、次の URL にある『*Cisco ASA 5500 Series Hardware and Software Compatibility*』を参照してください。

http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

一部の ASASM の機能は Cisco IOS 機能と連携します。次の機能は、Cisco IOS ソフトウェアを必要とします。

- 仮想スイッチング システム（VSS）：ASASM 設定は必要ありません。
- 自動ステート：スーパーバイザは、指定 VLAN の最後のインターフェイスがダウンしたとき、ASASM に通知します。これは、フェールオーバー スイッチが必要かどうかの決定を支援します。
- フェールオーバー スイッチのスーパーバイザ MAC アドレス テーブルのエントリのクリア：ASASM 設定は必要ありません。
- バージョン互換性：スーパーバイザ/ASASM バージョン互換性マトリクス チェックが失敗した場合、ASASM は自動的に電源がオフになります。

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

VLAN の注意事項および制限事項

- VLAN ID 2 ～ 1000 および 1025 ～ 4094 を使用します。
- ルーテッド ポートと WAN ポートは内部 VLAN を使用するため、1020 ～ 1100 の範囲に含まれる番号は、すでに使用されている可能性があります。
- 予約済みの 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 ASASM 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（複数可）をスイッチ ポートに割り当てないでください。ただし、シャーシ間でフェールオーバーを使用する場合は、シャーシ間を結ぶトランク ポートに VLAN を組み込む必要があります。
- ASASM に VLAN を割り当てる前に、スイッチに VLAN を追加しなかった場合、VLAN はスーパーバイザ エンジンのデータベースに保管され、スイッチに追加された時点で ASASM に送信されます。
- VLAN がスイッチに割り当てられる前に、ASASM コンフィギュレーションに VLAN を設定できます。スイッチが VLAN を ASASM に送信すると、ASASM コンフィギュレーションでシャットダウンするかどうかにかかわらず、VLAN は ASASM 上で、デフォルトで管理上アップ状態になることに注意してください。この場合、再度シャットダウンする必要があります。

SPAN リフレクタのガイドライン

Cisco IOS ソフトウェア Version 12.2SXJ1 以前では、スイッチ内の ASASM ごとに SPAN リフレクタ機能がイネーブルになっています。この機能により、ASASM から送られてきたマルチキャスト トラフィック（および中央の書き換えエンジンを必要とする他のトラフィック）をスイッチングできます。SPAN リフレクタ機能は SPAN セッションを 1 つ使用します。この機能をディセーブルにするには、次のコマンドを入力します。

```
Router(config)# no monitor session servicemodule
```

モジュールの搭載確認

スイッチが ASASM を認識し、オンラインに移行させたことを確認するには、次のコマンドを入力します。

手順の詳細

コマンド	目的
show module [**switch** {**1** |**2**}] [*mod-num* | **all**]	モジュール情報を表示します。VSS 内のスイッチの場合、**switch** キーワードを入力します。
例： `Router# show module 1`	[Status] 列で、ASASM に対して [Ok] が表示されることを確認します。

例

次に、**show module** コマンドの出力例を示します。

```
Router# show module
Mod Ports Card Type                                Model              Serial No.
--- ----- ---------------------------------------- ------------------ -----------
 2    3  ASA Service Module                       WS-SVC-ASA-SM1     SAD143502E8
 4    3  ASA Service Module                       WS-SVC-ASA-SM1     SAD135101Z9
 5    5  Supervisor Engine 720 10GE (Active)      VS-S720-10G        SAL12426KB1
 6   16  CEF720 16 port 10GE                      WS-X6716-10GE      SAL1442WZD1

Mod MAC addresses                       Hw     Fw           Sw           Status
--- ----------------------------------- ------ ------------ ------------ -------
 2  0022.bdd4.016f to 0022.bdd4.017e   0.201 12.2(2010080 12.2(2010121 Ok
 4  0022.bdd3.f64e to 0022.bdd3.f655   0.109 12.2(2010080 12.2(2010121 PwrDown
 5  0019.e8bb.7b0c to 0019.e8bb.7b13   2.0   8.5(2)       12.2(2010121 Ok
 6  f866.f220.5760 to f866.f220.576f   1.0   12.2(18r)S1  12.2(2010121 Ok

Mod  Sub-Module                  Model              Serial       Hw     Status
---- --------------------------- ------------------ ------------ ------- -------
2/0 ASA Application Processor   SVC-APP-PROC-1     SAD1436015D  0.202  Other
4/0 ASA Application Processor   SVC-APP-INT-1      SAD141002AK  0.106  PwrDown
 5  Policy Feature Card 3       VS-F6K-PFC3C       SAL12437BM2  1.0    Ok
 5  MSFC3 Daughterboard         VS-F6K-MSFC3       SAL12426DE3  1.0    Ok
 6  Distributed Forwarding Card WS-F6700-DFC3C     SAL1443XRDC  1.4    Ok

Base PID:
Mod  Model            Serial No.
---- -----------      ----------
 2 WS-SVC-APP-HW-1    SAD143502E8
 4 TRIFECTA           SAD135101Z9

Mod  Online Diag Status
---- -------------------
 2  Pass
2/0 Not Applicable
 4  Not Applicable
4/0 Not Applicable
 5  Pass
 6  Pass
```

ASA サービス モジュールへの VLAN の割り当て

ここでは、ASASM に VLAN を割り当てる方法について説明します。ASASM には、外部物理インターフェイスが組み込まれていません。代わりに、VLAN インターフェイスが使用されます。ASASM への VLAN の割り当ては、スイッチ ポートへの VLAN の割り当てと同様です。ASASM には、スイッチ ファブリック モジュール（SFM）（搭載されている場合）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。

前提条件

VLAN をスイッチに追加してスイッチ ポートに割り当てる方法については、スイッチのマニュアルを参照してください。

ガイドライン

- ASASM ごとに最大 16 個のファイアウォール VLAN グループを割り当てることができます。（Cisco IOS ソフトウェアで 16 より多くの VLAN グループを作成できますが、ASASM ごとに 16 個だけを割り当てることができます）。たとえば、すべての VLAN を 1 つのグループに割り当てられます。または内部グループと外部グループを作成できます。またはカスタマーごとにグループを 1 つずつ作成できます。
- グループごとの VLAN の数に制限はありませんが、ASASM は VLAN を ASASM システム制限までしか使用できません（詳細については、ASASM ライセンス マニュアルを参照してください）。
- 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。
- 複数の .ASASM に単一のファイアウォール グループを割り当てることはできます。たとえば、複数の ASASM に割り当てる VLAN は、それぞれの ASASM に一意の VLAN とは別のグループに配置できます。
- 「VLAN の注意事項および制限事項」（P.2-2）を参照してください。

手順の詳細

	コマンド	目的
ステップ 1	**firewall vlan-group** *firewall_group vlan_range* **例：** `Router(config)# firewall vlan-group 50 55-57`	VLAN をファイアウォール グループに割り当てます。 *firewall_group* 引数には、整数値を指定します。*vlan_range* 引数には、次のいずれかの形式で 1 つまたは複数の VLAN（2 ～ 1000 および 1025 ～ 4094）を指定できます。 • 単一の番号（*n*） • 範囲（*n-x*） 次の例のように、番号または範囲をカンマで区切ります。 **5,7-10,13,45-100**
ステップ 2	**firewall** [**switch** {**1** |**2**}] **module** *slot* **vlan-group** *firewall_group* **例：** `Router(config)# firewall module 5 vlan-group 50,52`	ASASM にファイアウォール グループを割り当てます。 VSS 内のスイッチの場合、**switch** 引数を入力します。 ASASM がインストールされているスロットを表示するには、**show module** コマンドを入力します。 *firewall_group* 引数は、次のいずれか形式で 1 つ以上のグループ番号を指定します。 • 単一の番号（*n*） • 範囲（*n-x*） 次の例のように、番号または範囲をカンマで区切ります。 **5,7-10**

例

次に、3 つのファイアウォール VLAN グループ（各 ASASM 用のグループおよび両方の ASASM に割り当てられた VLAN を含むグループ）を作成する例を示します。

```
Router(config)# firewall vlan-group 50 55-57
Router(config)# firewall vlan-group 51 70-85
Router(config)# firewall vlan-group 52 100
Router(config)# firewall module 5 vlan-group 50,52
Router(config)# firewall module 8 vlan-group 51,52
```

直接接続されたルータとしての MSFC の使用

ルータに直接接続されたルータとして（たとえば、ASASM outside インターフェイスに接続されているデフォルト ゲートウェイとして）MSFC を使用する場合は、スイッチ仮想インターフェイス（SVI）として MSFC に ASASM VLAN インターフェイスを追加します。

この項は、次の内容で構成されています。

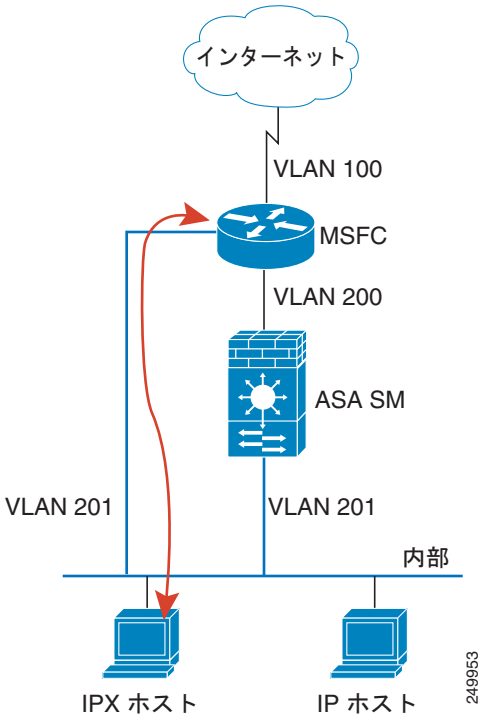
SVI に関する情報

セキュリティ上の理由から、デフォルトでは、MSFC と ASASM の間の 1 つの SVI を設定できます。複数の SVI をイネーブルにできますが、誤ってネットワークの設定をしないよう注意してください。

たとえば、複数の SVI を設定した場合、MSFC に内部 VLAN と外部 VLAN の両方が割り当てられていることによって、トラフィックが偶発的に ASASM をバイパスする可能性があります。

ネットワーク シナリオの中には、ASASM をバイパスする必要があるものもあります。図 2-1 に、IP ホストと同じイーサネット セグメント上にある IPX ホストを示します。ルーテッド ファイアウォール モードの ASASM は IP トラフィックしか処理せず、IPX などの他のプロトコル トラフィックを廃棄するため（トランスペアレント ファイアウォール モードでは IP 以外のトラフィックの通過が任意に許可されます）、IPX トラフィックで ASASM をバイパスする必要があります。この場合は、必ず VLAN 201 を通過できるのが IPX トラフィックに限定されるアクセス リストを使用して MSFC を設定してください。

図 2-1　IPX 対応の複数の SVI



トランスペアレント ファイアウォールがマルチ コンテキスト モードの場合は、複数の SVI を使用する必要があります。コンテキストごとに、対応する外部インターフェイス上に固有の VLAN が必要なためです。ルーテッド モードの場合でも複数の SVI を使用できるので、外部インターフェイス用に 1 つの VLAN を共有する必要はありません。

複数の SVI の設定

SVI を MSFC を追加するには、次の手順を実行します。

手順の詳細

	コマンド	目的
ステップ 1	（任意） **firewall multiple-vlan-interfaces** **例：** `Router(config)# firewall multiple-vlan-interfaces`	ASASM に 1 つまたは複数の SVI を追加できます。
ステップ 2	**interface vlan** *vlan_number* **例：** `Router(config)# interface vlan 55`	MSFC に VLAN インターフェイスを追加します。
ステップ 3	**ip address** *address mask* **例：** `Router(config-if)# ip address 10.1.1.1 255.255.255.0`	MSFC でこのインターフェイスの IP アドレスを設定します。
ステップ 4	**no shutdown** **例：** `Router(config-if)# no shutdown`	インターフェイスをイネーブルにします。

例

次に、複数の SVI を使用する一般的な設定例を示します。

```
Router(config)# firewall vlan-group 50 55-57
Router(config)# firewall vlan-group 51 70-85
Router(config)# firewall module 8 vlan-group 50-51
Router(config)# firewall multiple-vlan-interfaces
Router(config)# interface vlan 55
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# interface vlan 56
Router(config-if)# ip address 10.1.2.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# end
Router#
```

ASA フェールオーバーのスイッチの設定

この項は、次の内容で構成されています。

セカンダリ ASA サービス モジュール への VLAN の割り当て

両方の装置が同じように内部ネットワークと外部ネットワークにアクセスできる必要があるため、スイッチ上の両方の ASASM に同じ VLAN を割り当てる必要があります。「セカンダリ ASA サービス モジュール への VLAN の割り当て」（P.2-8）を参照してください。

プライマリ スイッチとセカンダリ スイッチ間のトランクの追加

スイッチ間フェールオーバーを使用している場合、2 つのスイッチ間に 802.1Q VLAN トランクを設定してフェールオーバーとステート リンクを処理する必要があります。CoS 値が 5（ハイ プライオリティ）のフェールオーバー VLAN パケットがこれらのポートでハイ プライオリティとして処理されるように、トランクで QoS をイネーブルにしておく必要があります。

EtherChannel とトランクの設定については、スイッチのマニュアルを参照してください。

トランスペアレント ファイアウォール モードとの両立

トランスペアレント モードでフェールオーバーを使用した場合にループが発生しないように、ブリッジ プロトコル データ ユニット（BPDU）の転送をサポートするスイッチ ソフトウェアを使用してください。ASASM がトランスペアレント モードの場合、スイッチでグローバルに LoopGuard をイネーブルにしないでください。LoopGuard は、スイッチと ASASM 間の内部 EtherChannel に自動的に適用されます。そのため、フェールオーバーおよびフェールバック後、EtherChannel がエラー ディセーブル ステートになるため、LoopGuard によりセカンダリ装置が切断されます。

高速リンク障害検出のための自動ステート メッセージングのイネーブル化

スーパーバイザ エンジンから ASASM に、ASASM VLAN に関連付けられている物理インターフェイスのステータスに関する自動ステート メッセージが送信されます。たとえば、VLAN に関連付けられたすべての物理インターフェイスが停止すると、VLAN が停止したことを示す自動ステート メッセージが ASASM に届きます。この情報に基づいて ASASM は VLAN が停止していると判断できます。この場合は、いずれの側でリンク障害が発生したかを判別するのに必要となるインターフェイス モニタリング テストが回避されます。自動ステート メッセージングにより、ASASM がリンク障害を検出するのに要する時間が大幅に短縮されます（自動ステートがサポートされていない場合の最長 45 秒に対し、数ミリ秒に短縮されます）。

次の場合に、スイッチのスーパーバイザから ASASM に自動ステート メッセージが送信されます。

- VLAN に属している最後のインターフェイスが停止した。
- VLAN に属している最初のインターフェイスが動作を開始した。

手順の詳細

コマンド	目的
firewall autostate **例：** `Router(config)# firewall autostate`	Cisco IOS ソフトウェアで自動ステート メッセージングをイネーブルにします。デフォルトでは、自動ステート メッセージングはディセーブルになっています。

ASA サービス モジュール のリセット

ここでは、ASASM をリセットする方法について説明します。CLI または外部 Telnet セッションから ASASM にアクセスできない場合は、ASASM のリセットが必要となります。リセットすると、完了までに数分間かかることがあります。

手順の詳細

コマンド	目的
hw-module [**switch** {**1** |**2**}] **module** *slot* **reset** **例：** `Router# hw-module module 9 reset`	ASASM をリセットします。 VSS 内のスイッチの場合、**switch** 引数を入力します。 *slot* 引数は、モジュールがインストールされているスロット番号を示します。ASASM がインストールされているスロットを表示するには、**show module** コマンドを入力します。 **（注）** 現在ログイン済みの ASASM をリセットするには、**reload** コマンドまたは **reboot** コマンドを入力します。

例

次に、**hw-module module reset** コマンドの出力例を示します。

```
Router# hw-module 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 ...
```

ASA サービス モジュール のモニタリング

ASA をモニタするには、次のいずれかのコマンドを入力します。

コマンド	目的
show firewall module [*mod-num*] **state**	ASA の状態を確認します。
show firewall module [*mod-num*] **traffic**	トラフィックが ASA を通過していることを確認します。
show firewall module [*mod-num*] **version**	ASA ソフトウェアのバージョンを示します。
show firewall multiple-vlan-interfaces	複数の VLAN インターフェイスのステータスを示します (イネーブルまたはディセーブル)。
show firewall vlan-group	設定されているすべての VLAN グループを表示します。
show interface vlan	設定されている VLAN インターフェイスに関するステータスおよび情報を表示します。

例

次に、**show firewall module** [*mod-num*] **state** コマンドの出力例を示します。

```
Router> show firewall module 11 state
Firewall module 11:
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: 3,6,7,20-24,40,59,85,87-89,99-115,150,188-191,200,250,
     501-505,913,972
Pruning VLANs Enabled: 2-1001
Vlans allowed on trunk:
Vlans allowed and active in management domain:
Vlans in spanning tree forwarding state and not pruned:
```

次に、**show firewall module** [*mod-num*] **traffic** コマンドの出力例を示します。

```
Router> show firewall module 11 traffic
Firewall module 11:

Specified interface is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 0014.1cd5.bef6 (bia 0014.1cd5.bef6)
  MTU 1500 bytes, BW 6000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Full-duplex, 1000Mb/s, media type is unknown
  input flow-control is on, output flow-control is on
  Members in this channel: Gi11/1 Gi11/2 Gi11/3 Gi11/4 Gi11/5 Gi11/6
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queuing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 10000 bits/sec, 17 packets/sec
     8709 packets input, 845553 bytes, 0 no buffer
     Received 745 broadcasts, 0 runts, 0 giants, 0 throttles
```

```
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     18652077 packets output, 1480488712 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

次に、**show firewall multiple-vlan-interfaces** コマンドの出力例を示します。

```
Router# show firewall multiple-vlan-interfaces
Multiple firewall vlan interfaces feature is enabled
```

次に、**show firewall module state** コマンドの出力例を示します。

```
Router# show firewall module
Module Vlan-groups
  5    50,52
  8    51,52
```

次に、**show firewall module** [*mod-num*] **version** コマンドの出力例を示します。

```
Router# show firewall module 2 version
ASA Service Module 2:

Sw Version: 100.7(8)19
```

次に、**show firewall vlan-group** コマンドの出力例を示します。

```
Router# show firewall vlan-group
Group vlans
----- ------
   50 55-57
   51 70-85
   52 100
```

次に、**show interface vlan** コマンドの出力例を示します。

```
Router# show interface vlan 55
Vlan55 is up, line protocol is up
  Hardware is EtherSVI, address is 0008.20de.45ca (bia 0008.20de.45ca)
  Internet address is 10.1.1.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type:ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:08, output hang never
  Last clearing of "show interface" counters never
  Input queue:0/75/0/0 (size/max/drops/flushes); Total output drops:0
  Queueing strategy:fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  L2 Switched:ucast:196 pkt, 13328 bytes - mcast:4 pkt, 256 bytes
  L3 in Switched:ucast:0 pkt, 0 bytes - mcast:0 pkt, 0 bytes mcast
  L3 out Switched:ucast:0 pkt, 0 bytes
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     4 packets output, 256 bytes, 0 underruns
     0 output errors, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

ASA サービス モジュール を使用するためのスイッチの機能履歴

表 2-1 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。

表 2-1　ASASM を使用するためのスイッチの機能履歴

機能名	プラットフォーム リリース	機能情報
Cisco Catalyst 6500 スイッチでの ASA サービス モジュール のサポート	8.5(1)	ASASM は、Catalyst 6500 シリーズ スイッチ用の高性能セキュリティ モジュールです。本章の手順に従って設定します。 **firewall transparent, mac address auto, firewall autostate** （IOS）、**interface vlan** コマンドを導入または変更しました。