CHAPTER 26

ファイアウォール サービス モジュールのトラブルシューティング

この章では、FWSM のトラブルシューティングの方法について説明します。また、この章は、次の項で構成されています。

設定のテスト

ここでは、シングルモードの FWSM または各セキュリティ コンテキストに対して接続テストを行う手順について説明します。FWSM のインターフェイスに ping を実行する手順、および 1 つのインターフェイス上のホストから他のインターフェイス上のホストに ping を実行する手順を示します。

トラブルシューティングでは、ping およびデバッグに関するメッセージだけをイネーブルにすることを推奨します。FWSM のテストが終了したら、「テスト設定のディセーブル化」（P.26-5）の手順に従ってください。

この項では、次の内容について説明します。

ICMP デバッグ メッセージとシステム ログ メッセージのイネーブル化

デバッグ メッセージとシステム ログ メッセージは、ping に失敗した原因を特定する場合に役立ちます。FWSM には、FWSM のインターフェイスへの ping に関する ICMP デバッグ メッセージだけが表示されます。FWSM 経由で他のホストに宛てた ping に関するメッセージは表示されません。デバッグ メッセージとシステム ログ メッセージをイネーブルにする手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、FWSM のインターフェイスへの ping に関する ICMP パケット情報を表示します。

```
hostname(config)# debug icmp trace
```

ステップ 2　次のコマンドを入力して、Telnet または SSH セッションにシステム ログ メッセージが送信されるように設定します。

```
hostname(config)# logging monitor debug
```

または、**logging buffer debug** コマンドを使用してメッセージをバッファに送信し、そのあとで **show logging** コマンドを使用して表示することもできます。

ステップ 3　次のコマンドを入力して、Telnet または SSH セッションにシステム ログ メッセージを送信します。

```
hostname(config)# terminal monitor
```

ステップ 4　次のコマンドを入力して、システム ログ メッセージをイネーブルにします。

```
hostname(config)# logging enable
```

次に、外部ホスト（209.165.201.2）から FWSM の外部インターフェイス（209.165.201.1）への ping が成功した例を示します。

```
hostname(config)# debug icmp trace
Inbound ICMP echo reply (len 32 id 1 seq 256) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 512) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 512) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 768) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 768) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 1024) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 1024) 209.165.201.1 > 209.165.201.2
```

この例には、ICMP パケット長（32 バイト）、ICMP パケット ID（1）、および ICMP シーケンス番号（ICMP シーケンス番号は 0 から始まり、要求が送信されるごとに増分されます）が示されています。

FWSM のインターフェイスへの ping の実行

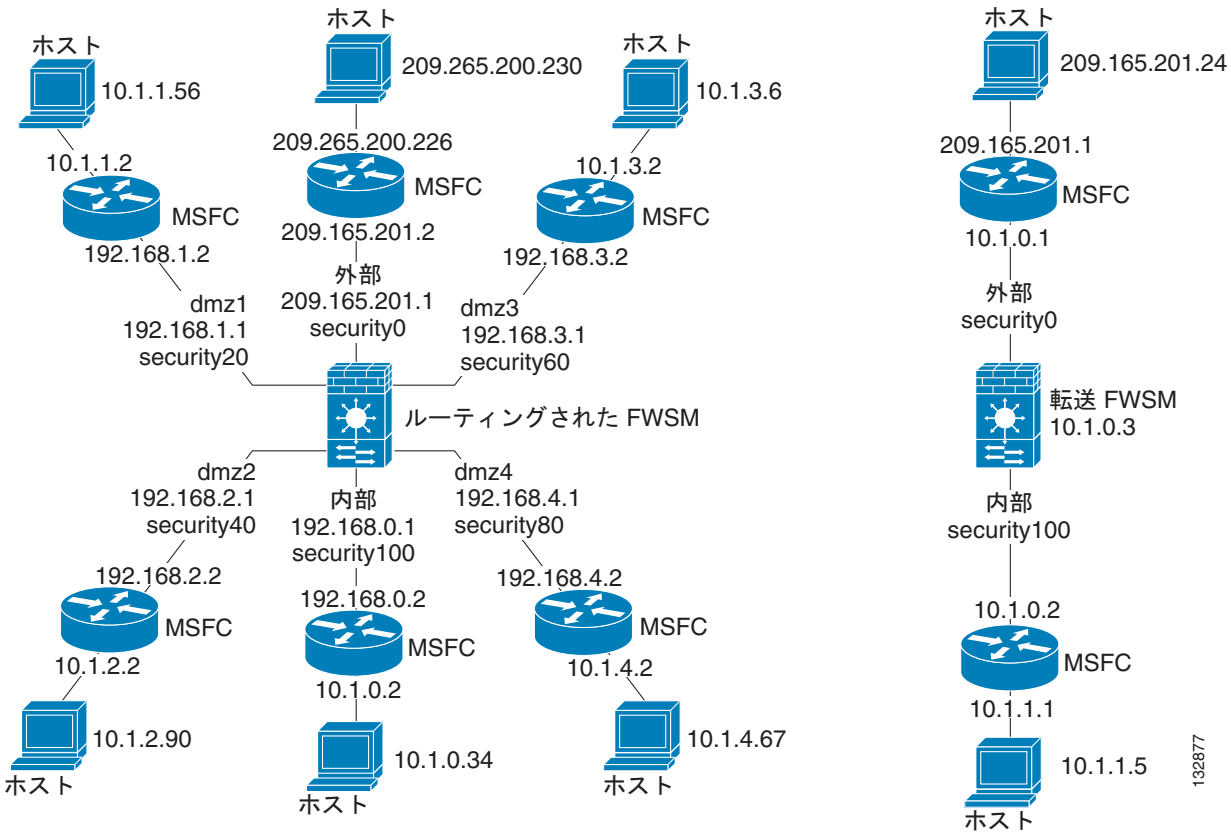
FWSM のインターフェイスが稼動中であり、FWSM と接続先ルータが正しくルーティングされているかどうかをテストするには、FWSM のインターフェイスに ping を実行します。

（注）　最も隣接するインターフェイスのみ ping できます。遠方のインターフェイスの ping はサポートされていません。

FWSM インターフェイスを ping するには、次の手順を実行します。

ステップ 1　インターフェイス名、セキュリティ レベル、および IP アドレスを明記したシングルモードの FWSM またはセキュリティ コンテキストの接続図を作成します。この接続図には、直接接続されたルータ、および FWSM への ping の実行元となるルータの反対側のホストも明記する必要があります。この情報は、ここで説明する手順、および「FWSM 経由の ping の実行」（P.26-4）の手順で使用します。次に例を示します。

図 26-1　インターフェイス、ルータ、およびホストを明記したネットワーク接続図

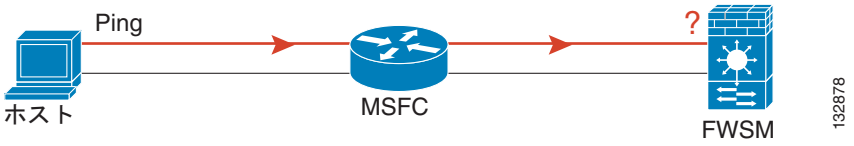


ステップ 2　*直接接続されたルータ*から FWSM の各インターフェイスに ping を実行します。トランスペアレント モードでは、管理 IP アドレスを ping します。

このテストは、FWSM インターフェイスがアクティブであること、およびインターフェイス コンフィギュレーションが正しいことを確認します。

ping に失敗した場合は、FWSM のインターフェイスがアクティブでないか、インターフェイスが正しく設定されていないか、または FWSM とルータ間のスイッチが停止している可能性があります（図 26-2 を参照）。この場合は、パケットが到達しないため、FWSM 上にデバッグ メッセージもシステム ログ メッセージも表示されません。

図 26-2　FWSM のインターフェイスへの ping の失敗

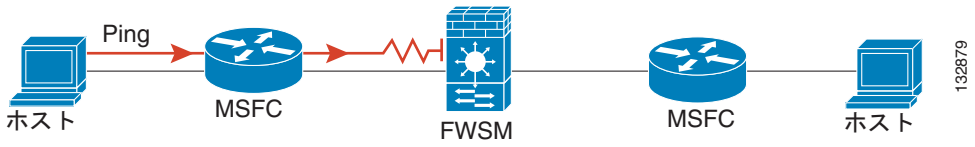


ping が FWSM に到達し、FWSM から応答が返されると、次のようなデバッグ メッセージが表示されます。

```
ICMP echo reply (len 32 id 1 seq 256) 209.165.201.1 > 209.165.201.2
ICMP echo request (len 32 id 1 seq 512) 209.165.201.2 > 209.165.201.1
```

ping 応答がルータに返らない場合、スイッチ ループが発生しているか、または IP アドレスが重複している可能性があります（図 26-3 を参照）。

図 26-3　IP アドレッシングの問題による ping の失敗



ステップ 3　リモート ホストから各 FWSM インターフェイスを ping します。トランスペアレント モードでは、管理 IP アドレスを ping します。

このテストでは、直接接続されたルータがホストと FWSM 間のパケットをルーティングできること、および FWSM からホストに返されるパケットが正しくルーティングされていることを確認します。

ping に失敗した場合は、中継ルータを経由したホストまでのルートが FWSM に正しく設定されていない可能性があります（図 26-4 を参照）。この場合は、ping に成功したことを示すデバッグ メッセージが表示されますが、システム ログ メッセージ 110001 でルーティング障害が発生していることが示されます。

図 26-4　FWSM のルート未設定による ping の失敗

FWSM 経由の ping の実行

FWSM のインターフェイスへの ping に成功したら、FWSM 経由でトラフィックを正しく転送できるかどうかを確認する必要があります。ルーテッド モードでは、このテストによって、NAT が設定されている場合に正しく実行されるかどうかを確認できます。NAT を使用しないトランスペアレント モードの場合は、FWSM が正しく動作していることをこのテストで確認します。トランスペアレント モードで ping に失敗した場合は、Cisco TAC に連絡してください。

異なるインターフェイス上のホスト間で ping するには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、任意の送信元ホストからの ICMP を許可するアクセス リストを追加します。

```
hostname(config)# access-list ICMPACL extended permit icmp any any
```

デフォルトでは、ホストが低セキュリティ インターフェイスにアクセスすると、すべてのトラフィックが通過を許可されます。ただし、高セキュリティ インターフェイスにアクセスするには、先行するアクセス リストが必要です。

ステップ 2　次のコマンドを入力して、各送信元インターフェイスにアクセス リストを割り当てます。

```
hostname(config)# access-group ICMPACL in interface interface_name
```

各発信元インターフェイスに対してこのコマンドを繰り返します。

ステップ 3　次のコマンドを入力して、ICMP 応答が送信元ホストに戻されるように、ICMP インスペクション エンジンをイネーブルにします。

```
hostname(config)# class-map ICMP-CLASS
hostname(config-cmap)# match access-list ICMPACL
hostname(config-cmap)# policy-map ICMP-POLICY
```

```
hostname(config-pmap)# class ICMP-CLASS
hostname(config-pmap-c)# inspect icmp
hostname(config-pmap-c)# service-policy ICMP-POLICY global
```

または、FWSM 経由で ICMP トラフィックを返すことを許可するために、ICMPACL アクセス リストを宛先インターフェイスに適用することもできます。

ステップ 4　ホストまたはルータから発信元インターフェイスを介して別のインターフェイス上の別のホストまたはルータに ping します。

確認が必要なすべてのインターフェイス ペアに対して、このステップを繰り返します。

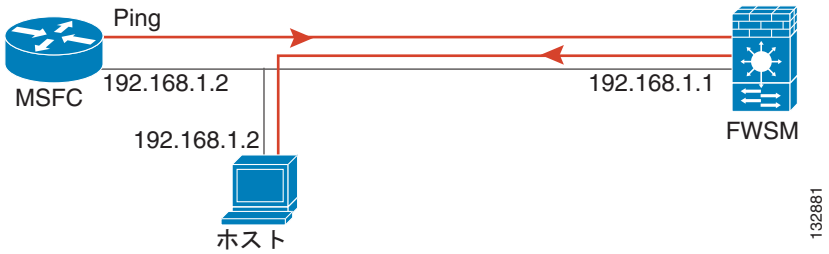
ping に成功すると、ルーテッド モードのアドレス変換を確認するシステム ログ メッセージ（305009 または 305011）と ICMP 接続が確立されたことを示すメッセージ（302020）が表示されます。**show xlate** コマンドと **show conns** コマンドを入力して、この情報を表示することもできます。

トランスペアレント モードの ping が失敗した場合は、Cisco TAC にお問い合わせください。

ルーテッド モードでは、NAT が正しく設定されていないために ping が失敗することがあります（図 26-5 を参照）。この状況は、NAT 制御をイネーブルにしている場合によく発生します。この場合は、NAT 変換に失敗したことを示すシステム ログ メッセージ（305005 または 305006）が表示されます。外部ホストから内部ホストに ping を実行した場合に、スタティック変換（NAT 制御に必要）が設定されていないと、メッセージ 106010：deny inbound icmp が表示されます。

（注）　FWSM には、FWSM のインターフェイスへの ping に関する ICMP デバッグ メッセージだけが表示されます。FWSM 経由で他のホストに宛てた ping に関するメッセージは表示されません。

図 26-5　FWSM のアドレス変換の問題による ping の失敗



テスト設定のディセーブル化

テストが完了したら、FWSM 宛ての ICMP と FWSM 経由の ICMP を許可し、デバッグ メッセージを出力するテスト設定をディセーブルにします。このコンフィギュレーションをそのままにしておくと、深刻なセキュリティ リスクが生じる可能性があります。また、デバッグ メッセージを生成すると、FWSM のパフォーマンスが遅くなります。

テスト コンフィギュレーションをディセーブルにするには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、ICMP デバッグ メッセージをディセーブルにします。

```
hostname(config)# no debug icmp trace
```

ステップ 2　必要に応じて、次のコマンドを入力して、ロギングをディセーブルにします。

```
hostname(config)# no logging on
```

ステップ 3　次のコマンドを入力して、ICMPACL アクセス リストを削除し、関連する **access-group** コマンドも削除します。

```
hostname(config)# no access-list ICMPACL
```

ステップ 4　（任意）ICMP インスペクション エンジンをディセーブルにする場合には、次のコマンドを入力します。

```
hostname(config)# no service-policy ICMP-POLICY
```

FWSM のリロード

マルチモードでは、システム実行スペースからしかリロードできません。FWSM をリロードするには、次のコマンドを入力します。

```
hostname# reload
```

パスワード復旧の実行

ここでは、パスワードを忘れた場合または AAA 設定が原因でロックアウトされた場合の回復手順について説明します。

- 「アプリケーション パーティションのパスワードおよび AAA 設定の消去」（P.26-6）
- 「メンテナンス パーティション パスワードのリセット」（P.26-7）

アプリケーション パーティションのパスワードおよび AAA 設定の消去

パスワードを忘れた場合、または AAA（認証、許可、アカウンティング）設定によってロックアウトされた場合には、パスワードおよび AAA コンフィギュレーションの一部をデフォルト値にリセットできます。この手順を実行するには、メンテナンス パーティションにログインする必要があります。

ステップ 1　スイッチのプロンプトで次のコマンドを入力して、アプリケーション ブート パーティションを設定します。

```
Router# set boot device cf:n [mod_num]
```

モジュール用のデフォルトのブート パーティションは cf:4 です。メンテナンス パーティションは cf:1 です。この手順の後半で、パスワードの消去対象とするブート パーティションを指定します。

ステップ 2　次のコマンドを入力して、FWSM をメンテナンス パーティションで起動します。

```
Router# hw-module module mod_num reset cf:1
```

ステップ 3　次のコマンドを入力して、FWSM とのセッションを確立します。

```
Router# session slot mod_num processor 1
```

ステップ 4　次のコマンドを入力して、メンテナンス パーティションにルートとしてログインします。

```
Login: root
```

ステップ 5　プロンプトにパスワードを入力します。

```
Password: password
```

デフォルトのパスワードは「cisco」です。

ステップ 6　ログインおよびイネーブル パスワードを消去するには、**aaa authentication console** および **aaa authorization command** コマンドを消去し、パスワードを消去するブート パーティションを指定して、次のコマンドを入力します。

シングル コンテキスト モード*限定*：

```
root@localhost# clear passwd cf:{4 | 5}
```

マルチ コンテキスト モード*限定*：

```
root@localhost# clear admin-context cf:{4 | 5}
```

FWSM はデフォルトで **cf:4** から起動します。ブート パーティションの表示方法の詳細については、ステップ 1 を参照してください。

ステップ 7　次のように、画面のプロンプトに従って入力します。

```
Do you wish to erase the passwords? [yn] y
The following lines will be removed from the configuration:
        enable password 8Ry2YjIyt7RRXU24 encrypted
        passwd 2KFQnbNIdI.2KYOU encrypted
Do you want to remove the commands listed above from the configuration?
[yn] y
Passwords and aaa commands have been erased.
```

メンテナンス パーティション パスワードのリセット

メンテナンス パーティションのパスワードを忘れた場合は、デフォルト値にリセットできます。この場合は、アプリケーション パーティションにログインしている必要があります。マルチモードでは、システム実行スペースからだけパスワードをリセットできます。

メンテナンス パスワードをリセットするには、次のコマンドを入力します。

```
hostname# clear mp-passwd
```

パスワードをリセットしたあと、デフォルト値を使用して FWSM にログインできます。

FWSM にログインしたら、**reload** または **reboot** コマンドを入力して再起動します。

メンテナンス パーティションから起動するように FWSM を設定し直すには、**hw-module module** *mod_num* **reset cf:1** コマンドを入力します。

詳細については、「デフォルト ブート パーティションの設定」（P.2-13）および「FWSM のリセットまたは特定のパーティションからの起動」（P.2-13）を参照してください。

その他のトラブルシューティング ツール

FWSM には、Cisco TAC から支援を受ける際に役立つ他のトラブルシューティング ツールが用意されています。

- 「デバッグ メッセージの表示」（P.26-8）
- 「パケットのキャプチャ」（P.26-8）

- 「クラッシュ ダンプの表示」（P.26-10）

デバッグ メッセージの表示

デバッグ出力には、CPU プロセスで高いプライオリティが与えられるため、システムが使用不能になる可能性があります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、または Cisco TAC とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。このような時間帯を選んでデバッグを実行すると、debug コマンドの処理の負担によってシステム利用が影響を受ける可能性が少なくなります。デバッグ メッセージをイネーブルにする場合は、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の **debug** コマンドの説明を参照してください。

パケットのキャプチャ

パケットの取得は、接続障害のトラブルシューティングや不審なアクティビティのモニタを行う場合に便利です。ここでは、次の内容について説明します。

- 「キャプチャの概要」（P.26-8）
- 「キャプチャの制限事項」（P.26-8）
- 「パケット キャプチャの設定」（P.26-9）

キャプチャの概要

FWSM は、それ自体を通過する IP トラフィックをすべてトラッキングできます。また、FWSM へのすべての管理トラフィック（SSH トラフィックや Telnet トラフィックなど）を含む、FWSM 宛ての IP トラフィックをすべてキャプチャすることもできます。

FWSM のアーキテクチャは、パケット処理のための異なる 3 セットのプロセッサで構成されています。このアーキテクチャに起因して、キャプチャ機能の性能に一定の制限が加わります。通常、FWSM のパケット フォワーディング機能の大部分は、2 つのフロントエンド ネットワーク プロセッサで処理されます。アプリケーション インスペクションが必要な場合にかぎり、パケットはコントロール プレーンの汎用プロセッサに送信されます（詳細については、「ステートフル インスペクションの概要」（P.1-8）を参照してください）。パケットがセッション管理パス ネットワーク プロセッサに送信されるのは、高速パス プロセッサで処理されないセッションがある場合だけです。

FWSM によって転送またはドロップされるすべてのパケットがこの 2 つのフロントエンド ネットワーク プロセッサを通るため、パケット キャプチャ機能はこれらのネットワーク プロセッサに実装されています。したがって、該当するトラフィック インターフェイス用の適切なキャプチャが設定されていれば、FWSM を通過するすべてのパケットをこれらのフロントエンド プロセッサでキャプチャできます。入力側では、FWSM インターフェイスに到着した時点でパケットがキャプチャされ、出力側では、ネットワークに送信される直前でパケットがキャプチャされます。

キャプチャの制限事項

次に、キャプチャ機能の制限の一部を示します。ほとんどの制限事項は、FWSM アーキテクチャの分散特性と、FWSM で使用されているハードウェア アクセラレータによるものです。

- 1 つのインターフェイスに複数のキャプチャを設定することはできません。ただし、キャプチャ アクセス リストに ACE を複数設定して柔軟なコンフィギュレーションにすることはできます。

- IP トラフィックだけをキャプチャできます。ARP など IP 以外のパケットは、キャプチャ機能でキャプチャできません。
- パケット キャプチャ機能は、TCP パケット順序の再設定またはその他の同様なパフォーマンス トラブルシューティングには使用しないでください。FWSM アーキテクチャにより、キャプチャ ACL をマッチングするパケットの順序が、中継で保存されない場合があります。また、ネットワーク プロセッサ完了装置は、キャプチャされる通過トラフィックの順序を保存できません。そのため、キャプチャ自体をイネーブルにすると、通過トラフィックでパフォーマンス問題が発生する可能性があります。
- 共有 VLAN の場合：
  - VLAN ごとに設定できるキャプチャは 1 つだけです。共有 VLAN の複数のコンテキストでキャプチャを設定した場合は、最後に設定したキャプチャだけが使用されます。

    最後に設定した（アクティブな）キャプチャを削除すると、他のコンテキストにキャプチャが設定されている場合でも、アクティブなキャプチャが存在しなくなります。キャプチャをアクティブにするには、削除したキャプチャをもう一度追加する必要があります。
  - キャプチャを指定したインターフェイス（キャプチャ アクセス リストと一致するインターフェイス）に着信するすべてのトラフィックがキャプチャされます。これには、共有 VLAN の他のコンテキストへのトラフィックが含まれます。

    したがって、コンテキスト B でも使用されている VLAN 上のコンテキスト A でキャプチャをイネーブルにすると、コンテキスト A とコンテキスト B の両方の入トラフィックがキャプチャされます。

    出力トラフィックの場合は、アクティブ キャプチャのあるコンテキストのトラフィックだけがキャプチャされます。唯一の例外は、ICMP 検査をイネーブルにしない（したがって、ICMP トラフィックのセッションが高速パスにない）場合です。この場合は、共有 VLAN のすべてのコンテキストで入力と出力の ICMP トラフィックがキャプチャされます。

パケット キャプチャの設定

キャプチャを設定する場合、通常は、キャプチャする必要のあるトラフィックを照合するアクセス リストを設定します。トラフィック パターンを照合するアクセス リストを設定したら、キャプチャを定義し、このアクセス リストをキャプチャと、キャプチャの設定対象となるインターフェイスに関連付ける必要があります。キャプチャは、アクセス リストおよびインターフェイスと、IPv4 トラフィックをキャプチャするためのキャプチャを関連付けた場合に限り機能することに注意してください。IPv6 トラフィックの場合、アクセス リストは不要です。

IPv4 トラフィック用のパケット キャプチャを設定する手順は、次のとおりです。

ステップ 1　「拡張アクセス リストの追加」（P.13-6）に従って、キャプチャする必要のあるトラフィックを照合する拡張アクセス リストを設定します。

次に、すべてのトラフィックを識別するアクセス リストの例を示します。

```
hostname(config)# access-list capture extended permit ip any any
```

ステップ 2　キャプチャを設定するには、次のコマンドを入力します。

```
hostname(config)# capture name access-list acl_name interface interface_name
```

デフォルトでは、キャプチャを設定すると、サイズが 512 KB のリニア キャプチャ バッファが作成されます。オプションで循環バッファを設定できます。デフォルトでは、68 バイトのパケットだけがバッファ内にキャプチャされます。オプションでこの値を変更できます。これらのオプションとその他のオプションについては、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の **capture** コマンドの説明を参照してください。

次に、ステップ 1 で設定した（外部インターフェイスに適用される）キャプチャ アクセス リストを使用して、ip-capture というキャプチャを作成するコマンドの例を示します。

```
hostname(config)# capture ip-capture access-list capture interface outside
```

ステップ 3　キャプチャを表示するには、次のコマンドを入力します。

```
hostname(config)# show capture name
```

copy capture コマンドを使用してキャプチャをコピーすることもできます。詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』を参照してください。

ステップ 4　バッファを保持してキャプチャを終了するには、次のコマンドを入力します。

```
hostname(config)# no capture name access-list acl_name interface interface_name
```

ステップ 5　バッファを削除してキャプチャを終了するには、次のコマンドを入力します。

```
hostname(config)# no capture name
```

クラッシュ ダンプの表示

FWSM がクラッシュした場合に、クラッシュ ダンプ情報を表示できます。クラッシュ ダンプの内容を調べる必要がある場合は、Cisco TAC に連絡することをお勧めします。『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の **show crashdump** コマンドを参照してください。

一般的な問題

この項では、FWSM の一般的な問題とそれらを解決する方法について説明します。

症状　スイッチの CLI から FWSM をリセットすると、システムが常にメンテナンス パーティションで起動される。

考えられる原因　デフォルトのブート パーティションが cf:1 に設定されています。

推奨処置　「デフォルト ブート パーティションの設定」（P.2-13）の説明に従って、デフォルトのブート パーティションを変更します。

症状　アプリケーション パーティションと同じパスワードでメンテナンス パーティションにログインできない。

考えられる原因　アプリケーション パーティションとメンテナンス パーティションのパスワード データベースが異なっています。

推奨処置　パーティションに対応するパスワードを使用します。詳細については、「パスワードの変更」（P.7-1）を参照してください。

症状　トラフィックが FWSM を通過しない。

考えられる原因　VLAN がスイッチ上に設定されていないか、FWSM に割り当てられていません。

推奨処置　VLAN を設定し、「ファイアウォール サービス モジュールへの VLAN の割り当て」（P.2-4）の説明に従って FWSM に VLAN を割り当てます。

症状　コンテキスト内で VLAN インターフェイスを設定できない。

考えられる原因　その VLAN はコンテキストに割り当てられていません。

推奨処置　「セキュリティ コンテキストの設定」（P.4-27）の説明に従って、コンテキストに VLAN を割り当てます。

症状　MSFC に複数の Switched Virtual Interface（SVI; スイッチ仮想インターフェイス）を追加できない。

考えられる原因　複数の SVI がイネーブルに設定されていません。

推奨処置　「MSFC へのスイッチ仮想インターフェイスの追加」（P.2-6）の説明に従って、複数の SVI をイネーブルにします。

症状　FWSM のインターフェイスに Telnet も SSH（セキュア シェル）も接続できない。

考えられる原因　FWSM への Telnet または SSH をイネーブルにしませんでした。

推奨処置　「Telnet アクセスの許可」（P.23-1）または「SSH アクセスの許可」（P.23-2）の説明に従って FWSM への Telnet 接続または SSH 接続をイネーブルにします。

症状　FWSM インターフェイスを ping できません。

考えられる原因　FWSM への ICMP がイネーブルに設定されていません。

推奨処置　「FWSM との ICMP 送受信の許可」（P.23-9）の説明に従って FWSM への ICMP をイネーブルにします。

症状　アクセス リストで許可されているにもかかわらず、FWSM 経由で ping を実行できない。

考えられる原因　ICMP インスペクション エンジンがイネーブルに設定されていないか、送信元インターフェイスおよび宛先インターフェイスの両方にアクセス リストが適用されていません。

推奨処置　ICMP はコネクションレス型プロトコルなので、FWSM はトラフィックが戻ることを自動的には許可しません。応答トラフィックを許可するには、送信元インターフェイスだけでなく宛先インターフェイスにもアクセス リストを適用するか、または ICMP インスペクション エンジンをイネーブルにして、ICMP 接続をステートフル接続として処理します。

症状　セキュリティの高いインターフェイスからセキュリティの低いインターフェイスへのトラフィックが FWSM を通過しない。

考えられる原因　セキュリティの高いインターフェイスに、トラフィックを許可するアクセス リストが適用されていません。PIX ファイアウォールとは異なり、FWSM はインターフェイス間のトラフィックの通過を自動的に許可しません。

推奨処置　送信元インターフェイスに、トラフィックを許可するアクセス リストを適用します。「拡張アクセス リストの追加」（P.13-6）を参照してください。

症状　同一セキュリティ レベルにある 2 つのインターフェイス間をトラフィックが通過しません。

考えられる原因　同じセキュリティ レベルのインターフェイス間のトラフィックを許可する機能が、イネーブルに設定されていません。

推奨処置　「同一セキュリティ レベルのインターフェイス間の通信の許可」（P.6-10）の説明に従って、この機能をイネーブルにします。

症状　FWSM でフェールオーバーが実行された場合でも、セカンダリ ユニットがトラフィックを転送しない。

考えられる原因　両方の装置に共通の VLAN が割り当てられていません。

推奨処置　スイッチ コンフィギュレーションで、両方の装置に共通の VLAN が割り当てられているかどうかを確認します。