CHAPTER 24

FWSM 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手順について説明します。内容は次のとおりです。

- 設定のテスト（p.24-2）
- FWSM のリロード（p.24-7）
- パスワード復旧の実行（p.24-8）
- その他のトラブルシューティング ツール（p.24-10）
- 一般的な問題（p.24-11）

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 コンテキストについて、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 を実行する方法、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 を実行する方法を示しています。

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.24-6）の手順に従ってください。

ここでは、次の内容について説明します。

- ICMP デバッグ メッセージおよびシステム メッセージのイネーブル化（p.24-2）
- FWSM のインターフェイスへの ping の実行（p.24-3）
- FWSM 経由の ping の実行（p.24-5）
- テスト設定のディセーブル化（p.24-6）

ICMP デバッグ メッセージおよびシステム メッセージのイネーブル化

デバッグ メッセージおよびシステム メッセージは、ping が失敗した原因を判別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 のメッセージは表示されません。デバッグ メッセージおよびシステム 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 パケット情報が表示されるように設定します。

```
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 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、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、使用する Telnet または SSH セッションにシステム メッセージが送信されるように設定します。

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

ステップ 4　次のコマンドを入力して、システム 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 に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
```

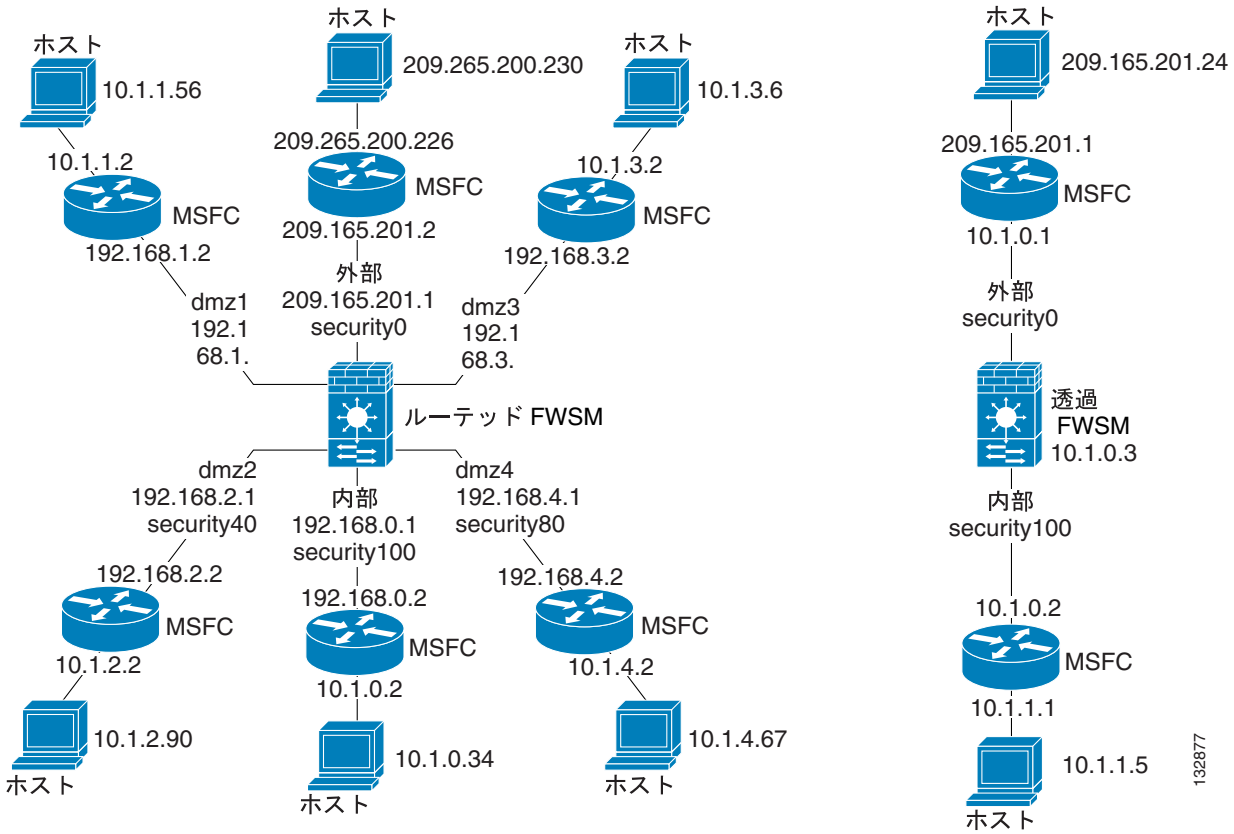
この例には、ICMP パケット長（32 バイト）、ICMP パケット ID（1）、および ICMP シーケンス番号が示されています（ICMP シーケンス番号は 0 から開始され、要求が送信されるごとに増分されます）。

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動作していて実行中であり、FWSM と接続先ルータのルーティングが正しく実行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。FWSM のインターフェイスに ping を実行する手順は、次のとおりです。

ステップ 1　シングルモード FWSM、または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 に対して ping を実行す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.24-5）の手順で使用します。次に例を示します。

図 24-1　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

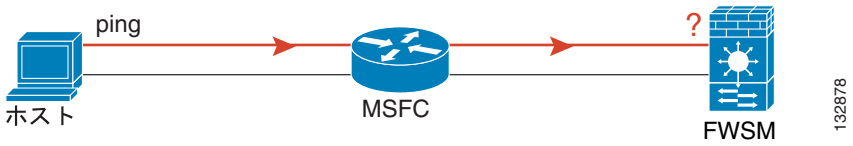


ステップ 2　*直接接続されたルータ*から FWSM の各インターフェイスに ping を実行します。透過モードの場合は、管理 IP アドレスに ping を送信します。

このテストによって、FWSM のインターフェイスがアクティブで、VLAN が正しく設定されているかどうかを確認します。

ping に失敗した場合、FWSM のインターフェイスがアクティブでないか、インターフェイスの設定が不正であるか、または FWSM とルータ間のスイッチがダウンしている可能性があります（図 24-2 を参照）。失敗した場合、パケットが到達しないので、FWSM 上にデバッグ メッセージまたはシステム メッセージは表示されません。

図 24-2　FWSM インターフェイスへの ping の失敗

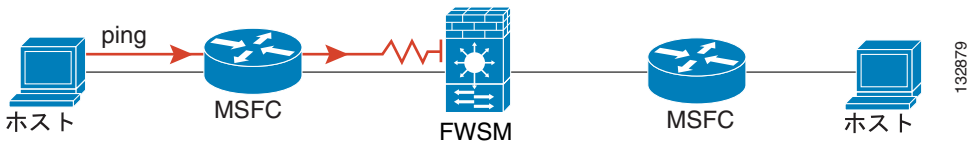


ping が FWSM に到達し、FWSM から応答が返されると、次のようなデバッグ メッセージが表示されます。

```
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 24-3 を参照）。

図 24-3　IP アドレスの重複による ping の失敗



ステップ 3　リモート ホストから FWSM の各インターフェイスに ping を実行します。透過モードの場合は、管理 IP アドレスに ping を送信します。

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、FWSM に、中継ルータを経由したホストまでのルートが正しく設定されていない可能性があります（図 24-4 を参照）。この場合、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 メッセージ 110001 によりルーティング障害が発生していることが示されます。

図 24-4　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 を使用しない透過モードの場合には、このテストによって FWSM が正しく動作していることを確認します。透過モードで 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 を実行する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、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、ホストがセキュリティの低いインターフェイスにアクセスする場合、すべてのトラフィックが許可されます。ただし、セキュリティの高いインターフェイスにアクセスするには、前述のアクセス 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
```

各送信元インターフェイスについて、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-map ICMP-POLICY global
```

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

ステップ 4　送信元インターフェイス上のホストまたはルータから、他のインターフェイス上の他のホストまたはルータに ping を実行します。

確認するインターフェイスの各ペアについて、この手順を繰り返します。

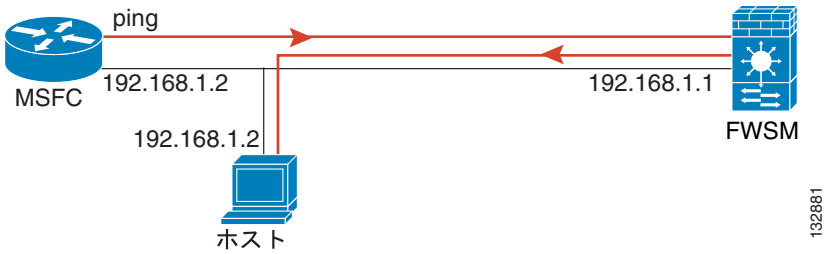
ping に成功すると、ルーテッド モードのアドレス変換を確認するシステム メッセージ（305009 または 305011）、および ICMP 接続が確立されたことを示すメッセージ（302020）が表示されます。**show xlate** コマンドまたは **show conns** コマンドを入力して、この情報を表示することもできます。

透過モードで ping に失敗した場合は、Cisco TAC に連絡してください。

ルーテッド モードで ping に失敗した場合、NAT が正しく設定されていない可能性があります（図 24-5 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、NAT 変換に失敗したことを示すシステム 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、スタティック変換が設定されていないと（NAT 制御に必要）、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 のメッセージは表示されません。

図 24-5　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、または 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用の設定をディセーブルにします。設定をそのまま有効にしておくと、重大なセキュリティ リスクが生じることがあります。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。

テスト設定をディセ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、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** コマンドを削除します。

```
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-map 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のみリロードできます。次のコマンドを入力して、FWSM をリロードします。

```
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.24-8）
- メンテナンス パーティション パスワードのリセット（p.24-9）

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、現在のアプリケーション ブート パーティションを確認します。

```
Router# show boot device [mod_num]
```

モジュールのブート パーティションが、cf:4 または cf:5 として出力されます。このあとの手順で、パスワードを消去するブート 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 とのセッションを開始します。

```
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 root 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　次のコマンドを入力して、ログイン パスワード、イネーブル パスワード、**aaa authentication console** コマンド、および **aaa authorization command** コマンドを消去します。

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

パスワードを消去するブート パーティションを指定します。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、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のみ、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
```

その他のトラブルシューティング ツール

FWSM には、Cisco TAC から支援を受けるときに役立つ、他のトラブルシューティング ツールが提供されています。

- デバッグ メッセージの表示（p.24-10）
- パケットのキャプチャ（p.24-10）
- クラッシュ ダンプの表示（p.24-10）

デバッグ メッセージの表示

デバッグ出力には、CPU 処理の中で高いプライオリティが割り当てられるため、システム性能が低下することがあります。このため、**debug** コマンドは、特別な問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッション中以外は使用しないでください。また、**debug** コマンドの実行は、使用中のユーザが少なく、ネットワーク トラフィックが少ないときに行うようにしてください。こうすることにより、デバッグ コマンドの処理のオーバーヘッドによって被る影響が少なくなります。デバッグ メッセージをイネーブルにするときは、『*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

接続に関する問題のトラブルシューティングを行ったり、不審な動作をモニタしたりする場合には、パケットのキャプチャが役立つことがあります。FWSM では、管理トラフィックおよびインスペクション エンジンを含め、汎用プロセッサを通過するトラフィックのパケット情報を追跡できます。（多くの転送トラフィックのように）ネットワーク プロセッサを通過するトラフィックを、FWSM でキャプチャすることはできません。パケット キャプチャ機能を使用する場合には、テクニカルサポートに連絡することを推奨します。『*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。

クラッシュ ダンプの表示

FWSM がクラッシュした場合には、クラッシュ ダンプ情報を表示できます。クラッシュ ダンプを解釈する際には、Cisco TAC に連絡することを推奨します。『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』の **show crashdump** コマンドの説明を参照してください。

一般的な問題

ここでは、FWSM の一般的な問題と、解決方法について説明します。

現象　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.2-14）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。

現象　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.7-2）を参照してください。

現象　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、「Firewall Services Module への VLAN 割り当て」（p.2-4）の説明に従って、FWSM に VLAN を割り当てます。

現象　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.4-20）の説明に従って、コンテキストに VLAN を割り当てます。

現象　MSFC に複数の Switched Virtual Interface（SVI）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 SVI の追加」（p.2-7）の説明に従って、複数の SVI をイネーブルにします。

現象　FWSM のインターフェイスに Telnet または SSH（セキュア シェル）で接続できない。

考えられる原因　FWSM への Telnet 接続または SSH 接続がイネーブルに設定されていません。

推奨処置　「Telnet アクセスの許可」（p.21-2）または「SSH アクセスの許可」（p.21-3）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。

現象　FWSM のインターフェイスに ping を実行できない。

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.21-12）の説明に従って、FWSM への ICMP をイネーブルにします。

現象　アクセス リストで許可されているのに、FWSM から 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 は戻りトラフィック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。

現象　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 セキュリティ アプライアンスと異なり、FWSM では、インターフェイス間のトラフィックは自動的には許可されません。

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.10-7）を参照してください。

現象　同じセキュリティ レベルの 2 つのインターフェイス間でトラフィックを転送できない。

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　「同じセキュリティ レベルのインターフェイス間の通信の許可」（p.6-8）の説明に従って、この機能をイネーブルにします。

現象　FWSM のフェールオーバーが実行されても、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。