CHAPTER 59

接続のトラブルシューティングおよびリソース

この章では、ASA のトラブルシューティングの方法について説明します。次の項目を取り上げます。

コンフィギュレーションのテスト

この項では、シングル モード ASA または各セキュリティ コンテキストの接続性のテスト方法、ASA インターフェイスを ping する方法、およびあるインターフェイスにあるホストが他のインターフェイスのホストに ping できるようにする方法について説明します。

ping メッセージおよびデバッグ メッセージはトラブルシューティング時に限りイネーブルにしてください。ASA のテストが終了したら、「テスト コンフィギュレーションのディセーブル化」（P.59-6）の手順に従ってください。

この項では、次のトピックについて取り上げます。

ICMP デバッグ メッセージと Syslog メッセージのイネーブル化

デバッグ メッセージと syslog メッセージは、ping が成功しない理由をトラブルシューティングするのに役立ちます。ASA では、ASA インターフェイスへの ping に対する ICMP デバッグ メッセージだけが表示されます。ASA を経由する他のホストへの ping に対する ICMP デバッグ メッセージは表示されません。

デバッグ メッセージと syslog メッセージをイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	**debug icmp trace** **例：** `hostname(config)# debug icmp trace`	ASA インターフェイスへの ping の ICMP パケット情報を表示します。
ステップ 2	**logging monitor debug** **例：** `hostname(config)# logging monitor debug`	Telnet セッションまたは SSH セッションに送信する syslog メッセージを設定します。 **（注）** あるいは、**logging buffer debug** コマンドを使用してログ メッセージをバッファに送信してから、**show logging** コマンドを使用してそれらを表示することもできます。
ステップ 3	**terminal monitor** **例：** `hostname(config)# terminal monitor`	Telnet セッションまたは SSH セッションに syslog メッセージを送信します。
ステップ 4	**logging on** **例：** `hostname(config)# logging on`	syslog メッセージの生成をイネーブルにします。

例

次に、外部ホスト（209.165.201.2）から ASA 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
```

この出力では、ICMP パケット長（32 バイト）、ICMP パケット識別子（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、要求が送信されるたびに増分されます）が示されています。

ASA のインターフェイスへの ping の実行

ASA インターフェイスが起動して動作しているかどうか、および ASA と接続ルータが正しく動作しているかどうかをテストするには、ASA インターフェイスを ping します。

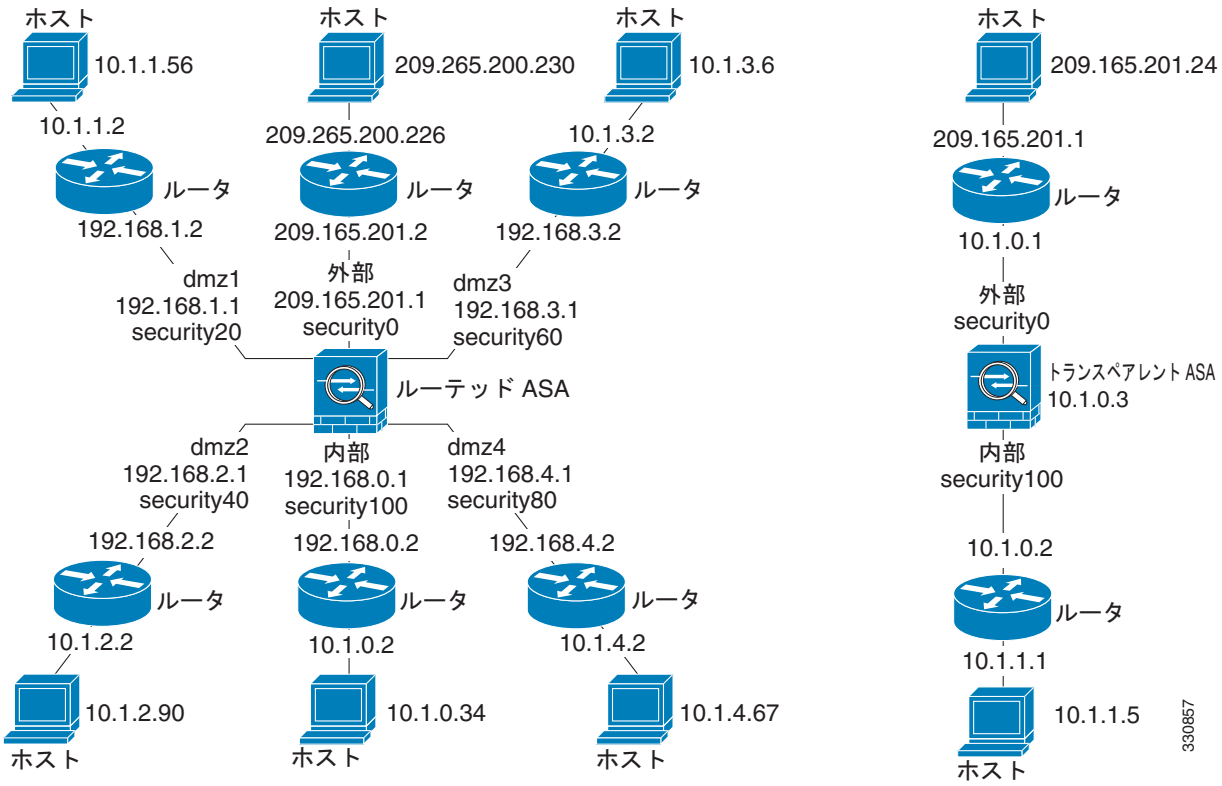
ASA インターフェイスを ping するには、次の手順を実行します。

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 アドレスを示すシングル モードの ASA またはセキュリティ コンテキストの図を作成します。

（注）　この手順では IP アドレスを使用しますが、**ping** コマンドでは、DNS 名および **name** コマンドを使用してローカル IP アドレスに割り当てられた名前もサポートされます。

図には、直接接続されたすべてのルータ、および ASA を ping するルータの反対側にあるホストも含める必要があります。この情報はこの手順と「トラフィックの ASA の通過」（P.59-5）の手順で使用します。（図 59-1 を参照）。

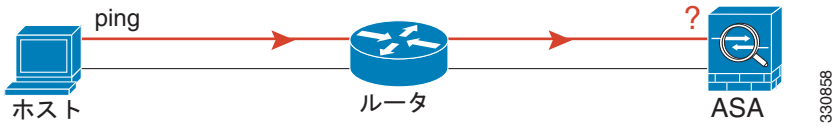
図 59-1　インターフェイス、ルータ、およびホストを含むネットワーク図



ステップ 2　直接接続されたルータから各 ASA 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。このテストは、ASA 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。

ASA インターフェイスがアクティブではない場合、インターフェイス コンフィギュレーションが正しくない場合、または ASA とルータの間でスイッチがダウンしている場合、ping は失敗する可能性があります（図 59-2 を参照）。この場合は、パケットが ASA に到達しないので、デバッグ メッセージや syslog メッセージは表示されません。

図 59-2　ASA のインターフェイスへの ping の失敗

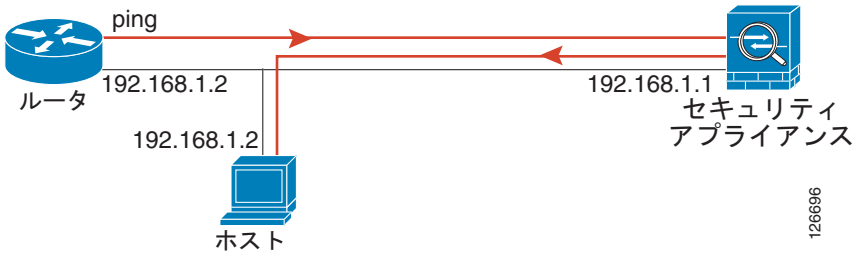


ping が ASA に到達し、応答があると、次のようなデバッグ メッセージが表示されます。

```
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 応答がルータに戻されない場合は、スイッチ ループまたは冗長 IP アドレスが存在する可能性があります（図 59-3 を参照）。

図 59-3　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 ASA 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。このテストは、直接接続されたルータがホストと ASA の間でパケットをルーティングできるかどうか、および ASA がパケットを正確にルーティングしてホストに戻せるかどうかを確認します。

中間ルータを通ってホストに戻るルートが ASA にない場合、ping は失敗する可能性があります（図 59-4 を参照）。この場合は、デバッグ メッセージは ping が成功したことを示しますが、ルーティングの失敗を示す syslog メッセージ 110001 が表示されます。

図 59-4　ASA に戻りルートがないことによる ping の失敗

トラフィックの ASA の通過

ASA インターフェイスを正常に ping した後で、トラフィックが ASA を正常に通過できることを確認します。デフォルトでは、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 ping を実行できます。リターン トラフィックを通過させるように ICMP インスペクションをイネーブルにすることだけが必要です。高位から低位に ping するには、トラフィックを許可する ACL を適用する必要があります。NAT を使用する場合は、このテストを行うと NAT が正しく動作していることがわかります。

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 が成功すると、ルーテッド モードのアドレス変換（305009 または 305011）と ICMP 接続が確立されたこと（302020）を確認する syslog メッセージが表示されます。**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。

NAT が正しく設定されていないことが原因で、ping に失敗することもあります。この場合、NAT が失敗したことを示す syslog メッセージが表示されます（305005 または 305006）。外部ホストから内部ホストに ping し、スタティック変換がない場合は、次の syslog メッセージが表示されます。

```
%ASA-3-106010: deny inbound icmp.
```

（注） ASA によって ICMP デバッグ メッセージが表示されるのは、ASA インターフェイスへの ping に対してのみであり、ASA 経由の他のホストへの ping に対しては表示されません。

図 59-5　ASA のアドレス変換の問題による ping の失敗

手順の詳細

	コマンド	目的
ステップ 1	`policy-map global_policy`	デフォルト グローバル ポリシーを編集し、ポリシー マップ コンフィギュレーション モードを開始します。
ステップ 2	`class inspection_default`	デフォルトのクラス マップを編集します。これには、標準のプロトコルとポートのアプリケーション トラフィックが一致します。ICMP の場合は、このクラスには、すべての ICMP トラフィックが一致します。
ステップ 3	`inspect icmp`	ICMP インスペクション エンジンをイネーブルにします。ICMP 応答が発信元ホストに戻されるようになります。

ステップ 4	（任意、低セキュリティ インターフェイスの場合） **access-list ICMPACL extended permit icmp any any**	発信元ホストから ICMP トラフィックを許可するアクセス リストを追加します。
ステップ 5	**access-group ICMPACL in interface outside**	アクセス リストを外部インターフェイスに割り当てます。「outside」を実際のインターフェイス名で置き換えます（これとは異なる場合）。高位から低位への ICMP トラフィックを許可するインターフェイスごとに、このコマンドを繰り返します。 **（注）** セキュリティが最低ではないインターフェイスにこの ACL を適用すると、ICMP トラフィックだけが許可されます。つまり、高位から低位への暗黙的な許可が削除されます。たとえば、DMZ インターフェイス（レベル 50）から内部インターフェイス（レベル 100）に ping できるようにするには、この ACL を適用する必要があります。ただし、この時点では、DMZ から外部（レベル 0）へのトラフィックは ICMP トラフィックのみに制限されます。適用前は、暗黙的な許可によってすべてのトラフィックが許可されていました。ping のテストの後は、必ずこの ACL をインターフェイスから削除してください。特に、暗黙的な許可を復元したいインターフェイスです（**no access-list ICMPACL**）。

テスト コンフィギュレーションのディセーブル化

テストの完了後、ICMP の ASA への送信および通過を許可し、デバッグ メッセージを表示するテスト コンフィギュレーション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 メッセージを表示すると、ASA のパフォーマンスが低下します。

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。

	コマンド	目的
ステップ 1	**no debug icmp trace**	ICMP デバッグ メッセージをディセーブルにします。
ステップ 2	**no logging on**	ロギングをディセーブルにします。
ステップ 3	**no access-list ICMPACL**	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。
ステップ 4	**policy-map global_policy** ** class inspection_default** ** no inspect icmp**	（任意）ICMP インスペクション エンジンをディセーブルにします。

トレースルートによるパケット ルーティングの決定

パケットのルートは、トレースルート機能を使用してトレースできます。この機能には、**traceroute** コマンドでアクセスできます。トレースルートは、無効なポート上の宛先に UDP パケットを送信することで機能します。ポートが有効ではないため、宛先までの間にあるルータから ICMP Time Exceeded メッセージが返され、ASA にエラーが報告されます。

パケット トレーサによるパケットの追跡

パケット トレーサ ツールは、パケット スニフィングとネットワーク障害箇所特定のためのパケット追跡を実現するとともに、パケットに関する詳細情報と ASA によるパケットの処理方法を示します。コンフィギュレーション コマンドがパケット ドロップの原因ではない場合は、パケット トレーサ ツールを実行すると、その原因に関する情報が読みやすい形式で表示されます。

また、パケットが正しく動作しているかどうかを確認するために、パケット トレーサ ツールを使用して、ASA を通過するパケットのライフスパンをトレースできます。このツールを使用して、次のことを行えます。

- ネットワーク内にドロップするすべてのパケットをデバッグする。
- コンフィギュレーションが意図したとおりに機能しているかを確認する。
- パケットに適用可能なすべてのルール、およびルールが追加される原因となった CLI コマンドを表示する。
- データ パス内でのパケット変化を時系列で表示する。
- データ パスにトレーサ パケットを挿入する。
- ユーザ アイデンティティおよび FQDN に基づいて IPv4 アドレスまたは IPv6 アドレスを検索する。

パケットを追跡するには、次のコマンドを入力します。

コマンド	目的
packet-tracer input [*ifc_name*] [**icmp** [*sip* | **user** *username* | **fqdn** *fqdn-string*] *type code ident* [*dip* | **fqdn** *fqdn-string*]] | [**tcp** [*sip* | **user** *username* | **fqdn** *fqdn-string*] *sport* [*dip* | **fqdn** *fqdn-string*] *dport*] | [**udp** [*sip* | **user** *username* | **fqdn** *fqdn-string*] *sport* [*dip* | **fqdn** *fqdn-string*] *dport*] | [**rawip** [*sip* | **user** *username* | **fqdn** *fqdn-string*] [*dip* | **fqdn** *fqdn-string*]] [**detailed**] [**xml**] **例：** `hostname# packet-tracer input inside tcp 10.2.25.3 www 209.165.202.158 aol detailed`	パケットに関する詳細情報と ASA によるパケットの処理方法を示します。詳細情報を出力し、内部ホスト 10.2.25.3 から外部ホスト 209.165.202.158 にパケット トレーシングをイネーブルにする例を示します。

プロセスごとの CPU 使用率のモニタリング

CPU で実行されているプロセスをモニタできます。特定のプロセスで使用される CPU の使用率に関する情報を取得できます。CPU 使用率の統計情報は降順で並べられ、使用率の最も高いプロセスが先頭に表示されます。また、プロセスごとの CPU に対する負荷に関する情報（記録時間の 5 秒前、1 分前、および 5 分前の情報）も含まれています。この情報は 5 秒おきに自動的に更新され、リアルタイムの統計情報が表示されます。

show process cpu-usage sorted コマンドを使用すると、設定済みコンテキストで消費されるプロセス関連の CPU 負荷の内訳がわかります。