テストとトラブルシューティング

この章では、Cisco ASA のトラブルシューティング方法および基本接続のテスト方法について説明します。

- イネーブル パスワードと Telnet パスワードの回復 （1 ページ）
- Packet Capture Wizard を使用したキャプチャの設定と実行 （7 ページ）
- ASAv の vCPU 使用量 （13 ページ）
- 設定のテスト （15 ページ）
- パフォーマンスとシステム リソースのモニタリング （24 ページ）
- 接続のモニタリング （27 ページ）
- テストおよびトラブルシューティングの履歴 （27 ページ）

イネーブル パスワードと Telnet パスワードの回復

イネーブル パスワードまたは Telnet パスワードを忘れた場合は、それらを回復できます。手順は、デバイス タイプによって異なります。CLI を使用してタスクを実行する必要があります。

ASA のパスワードの回復

ASA のパスワードを回復するには、次の手順を実行します。

手順

ステップ 1 ASA のコンソール ポートに接続します。

ステップ 2 ASA の電源を切ってから、再び電源をオンにします。

ステップ 3 スタートアップ後、ROMMON モードに入るようにプロンプトが表示されたら、**Escape** キーを押します。

ステップ 4 コンフィギュレーション レジスタ値をアップデートするには、次のコマンドを入力します。

```
rommon #1> confreg 0x41
```

```
Update Config Register (0x41) in NVRAM...
```

ステップ 5 スタートアップ コンフィギュレーションを無視するように ASA を設定するには、次のコマンドを入力します。

```
rommon #1> confreg
```

ASA によって現在のコンフィギュレーションのレジスタ値が表示され、それを変更するかどうかが尋ねられます。

```
Current Configuration Register: 0x00000041
Configuration Summary:
  boot default image from Flash
  ignore system configuration

Do you wish to change this configuration? y/n [n]: y
```

ステップ 6 後で回復できるように、現在のコンフィギュレーションのレジスタ値を記録します。

ステップ 7 値を変更する場合は、プロンプトに対して **Y** を入力します。

ASA によって、新しい値の入力を求めるプロンプトが表示されます。

ステップ 8 「disable system configuration?」の値を除き、すべての設定についてデフォルト値を受け入れます。

ステップ 9 プロンプトに対して、**Y** を入力します。

ステップ 10 次のコマンドを入力して、ASA をリロードします。

```
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.

Loading disk0:/asa800-226-k8.bin... Booting...Loading...
```

ASA は、スタートアップ コンフィギュレーションの代わりにデフォルト コンフィギュレーションをロードします。

ステップ 11 次のコマンドを入力して、特権 EXEC モードにアクセスします。

```
ciscoasa# enable
```

ステップ 12 パスワードの入力を求められたら、**Enter** キーを押します。

パスワードは空白です。

ステップ 13 次のコマンドを入力して、スタートアップ コンフィギュレーションをロードします。

```
ciscoasa# copy startup-config running-config
```

ステップ 14 次のコマンドを入力して、グローバル コンフィギュレーション モードにアクセスします。

```
ciscoasa# configure terminal
```

ステップ 15 次のコマンドを入力して、デフォルト コンフィギュレーションで必要に応じてパスワードを変更します。

```
ciscoasa(config)# password password
ciscoasa(config)# enable password password
ciscoasa(config)# username name password password
```

ステップ 16 次のコマンドを入力して、デフォルト コンフィギュレーションをロードします。

```
ciscoasa(config)# no config-register
```

デフォルト コンフィギュレーションのレジスタ値は 0x1 です。コンフィギュレーション レジスタの詳細については、コマンド リファレンスを参照してください。

ステップ 17 次のコマンドを入力して、新しいパスワードをスタートアップ コンフィギュレーションに保存します。

```
ciscoasa(config)# copy running-config startup-config
```

ASA 5506-X、ASA 5508-X、ASA 5516-X でのパスワードの回復

ASA 5506-X、ASA 5508-X、ASA 5516-X のパスワードの回復には、次の手順を実行します。

手順

ステップ 1 ASA のコンソール ポートに接続します。

ステップ 2 ASA の電源を切ってから、再び電源をオンにします。

ステップ 3 スタートアップ後、ROMMON モードに入るようにプロンプトが表示されたら、**Escape** キーを押します。

ステップ 4 コンフィギュレーション レジスタ値をアップデートするには、次のコマンドを入力します。

```
rommon #1> confreg 0x41

You must reset or power cycle for new config to take effect
```

ASA で現在のコンフィギュレーション レジスタ値と構成オプションのリストが表示されます。後で回復できるように、現在のコンフィギュレーションのレジスタ値を記録します。

```
Configuration Register: 0x00000041

Configuration Summary
 [ 0 ] password recovery
 [ 1 ] display break prompt
 [ 2 ] ignore system configuration
 [ 3 ] auto-boot image in disks
 [ 4 ] console baud: 9600
 boot: ...... auto-boot index 1 image in disks
```

ステップ 5 次のコマンドを入力して、ASA をリロードします。

```
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.

Loading disk0:/asa932-226-k8.bin... Booting...Loading...
```

ASAは、スタートアップ コンフィギュレーションの代わりにデフォルト コンフィギュレーションをロードします。

ステップ 6 次のコマンドを入力して、特権 EXEC モードにアクセスします。

```
ciscoasa# enable
```

ステップ 7 パスワードの入力を求められたら、**Enter** キーを押します。

パスワードは空白です。

ステップ 8 次のコマンドを入力して、スタートアップ コンフィギュレーションをロードします。

```
ciscoasa# copy startup-config running-config
```

ステップ 9 次のコマンドを入力して、グローバル コンフィギュレーション モードにアクセスします。

```
ciscoasa# configure terminal
```

ステップ 10 次のコマンドを入力して、デフォルト コンフィギュレーションで必要に応じてパスワードを変更します。

```
ciscoasa(config)# password password
ciscoasa(config)# enable password password
ciscoasa(config)# username name password password
```

ステップ 11 次のコマンドを入力して、デフォルト コンフィギュレーションをロードします。

```
ciscoasa(config)# no config-register
```

デフォルト コンフィギュレーションのレジスタ値は 0x1 です。コンフィギュレーション レジスタの詳細については、コマンド リファレンスを参照してください。

ステップ 12 次のコマンドを入力して、新しいパスワードをスタートアップ コンフィギュレーションに保存します。

```
ciscoasa(config)# copy running-config startup-config
```

ASAv でのパスワードまたはイメージの回復

ASAv のパスワードまたはイメージを回復するには、次の手順を実行します。

手順

ステップ 1 実行コンフィギュレーションを ASAv のバックアップ ファイルにコピーします。

copy running-config *filename*

例：

```
ciscoasa# copy running-config backup.cfg
```

ステップ 2 ASAv を再始動します。

reload

ステップ 3 [GNU GRUB] メニューから、下矢印を押し、**コンフィギュレーションをロードしない**オプションで <**filename**> を選択し、Enter キーを押します。ファイル名は、ASAv のデフォルトのブートイメージのファイル名です。デフォルトのブートイメージは、**fallback** コマンドによって自動的にブートされることはありません。その後、選択したブート イメージをロードします。

```
GNU GRUB version 2.0(12)4
bootflash:/asa100123-20-smp-k8.bin
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

例：

```
GNU GRUB version 2.0(12)4
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

ステップ 4 実行コンフィギュレーションにバックアップ コンフィギュレーション ファイルをコピーします。

copy *filename* **running-config**

例：

```
ciscoasa (config)# copy backup.cfg running-config
```

ステップ 5 パスワードのリセット。

enable password *password*

例：

```
ciscoasa(config)# enable password cisco123
```

ステップ 6 新しい設定を保存します。

write memory

例：

```
ciscoasa(config)# write memory
```

パスワード回復のディセーブル化

（注） ASAv 上でパスワード回復をディセーブルにすることはできません。

権限のないユーザがパスワード回復メカニズムを使用して ASA を危険にさらすことがないように、パスワード回復をディセーブルにするには、次の手順を実行します。

始める前に

ASA で、**no service password-recovery** コマンドを使用すると ROMMON モードに入って、コンフィギュレーションの変更を防ぐことができます。ROMMON モードに入ると、ASA では、すべてのフラッシュ ファイル システムの消去を求めるプロンプトが表示されます。最初に消去を実行しないと、ROMMON モードを開始できません。フラッシュ ファイル システムを消去しない場合、ASA はリロードされます。パスワード回復は ROMMON モードの使用と既存のコンフィギュレーションの保持に依存しているので、この消去によって、パスワードの回復ができなくなります。ただし、パスワードを回復できなくすることで、不正なユーザがコンフィギュレーションを表示したり、別のパスワードを挿入したりすることがなくなります。この場合、システムを動作可能な状態に回復するには、新しいイメージとバックアップ コンフィギュレーション ファイル（入手できる場合）をロードします。

service password-recovery コマンドは、コンフィギュレーション ファイルに通知用としてのみ表示されます。CLI プロンプトに対してコマンドを入力すると、設定は NVRAM に保存されます。設定を変更する唯一の方法は、CLI プロンプトでコマンドを入力することです。このコマンドの異なるバージョンで新規コンフィギュレーションをロードしても、設定は変更されません。（パスワード回復の準備段階で）スタートアップ時にスタートアップ コンフィギュレー

ションを無視するようASAが設定されている場合にパスワード回復をディセーブルにすると、通常どおりスタートアップ コンフィギュレーションをロードするように ASA の設定が変更されます。フェールオーバーを使用し、スタートアップコンフィギュレーションを無視するようにスタンバイ装置が設定されている場合は、**no service password- recovery** コマンドでスタンバイ装置に複製したときに、コンフィギュレーション レジスタに同じ変更が加えられます。

手順

パスワード回復をディセーブルにします。

no service password-recovery

例：

```
ciscoasa (config)# no service password-recovery
```

Packet Capture Wizard を使用したキャプチャの設定と実行

Packet Capture Wizard を使用して、エラーのトラブルシューティングを行う場合のキャプチャを設定および実行できます。キャプチャでは ACL を使用して、キャプチャされるトラフィックのタイプを、送信元と宛先のアドレスとポート、および1つ以上のインターフェイスで制限できます。このウィザードは、入出力インターフェイスのそれぞれでキャプチャを1回実行します。キャプチャしたパケットは、PC に保存してパケット アナライザで分析できます。

（注） このツールは、クライアントレス SSL VPN キャプチャをサポートしていません。

キャプチャを設定および実行するには、次の手順を実行します。

手順

ステップ 1 **[Wizards]** > **[Packet Capture Wizard]** の順に選択します。

[Overview of Packet Capture] 画面には、ウィザードを完了するまでに行うタスクの一覧が表示されます。これらのタスクには、以下が含まれます。

- 入力インターフェイスの選択。
- 出力インターフェイスの選択。
- バッファ パラメータの設定。

- キャプチャの実行。
- （オプション）キャプチャ データの PC への保存。

ステップ 2 [Next] をクリックします。

クラスタ環境では、[Cluster Option] 画面が表示されます。ステップ 3 に進みます。

非クラスタ環境では、[Ingress Traffic Selector] 画面が表示されます。ステップ 4 に進みます。

ステップ 3 [Cluster Option] 画面で、キャプチャの実行対象として [This device only] または [The whole cluster] のいずれかのオプションを選択します。[Next] をクリックして [Ingress Selector] 画面を表示します。

ステップ 4 インターフェイスでパケットをキャプチャするには、[Select Interface] オプション ボタンをクリックします。

ステップ 5 ASA CX データプレーン上でパケットをキャプチャするには、[Use backplane channel] オプション ボタンをクリックします。

ステップ 6 [Packet Match Criteria] 領域で、次のいずれかを実行します。

- パケットの照合に使用する ACL を指定するには、[Specify access-list] オプション ボタンをクリックし、[Select ACL] ドロップダウン リストから ACL を選択します。以前設定した ACL を現在のドロップダウン リストに追加するには、[Manage] をクリックして [ACL Manager] ペインを表示します。ACL を選択して [OK] をクリックします。
- [**Specify Packet Parameters**] オプション ボタンをクリックして、パケット パラメータを指定します。

ステップ 7 以降の手順については、入力トラフィック セレクタ （10 ページ）を参照してください。

ステップ 8 [Next] をクリックして、[Egress Traffic Selector] 画面を表示します。

ステップ 9 インターフェイスでパケットをキャプチャするには、[Select Interface] オプション ボタンをクリックします。

（注） [Egress Traffic Selector] のフィールドの詳細については出力トラフィック セレクタ （11 ページ）を参照してください。

[Egress Traffic Selector] のフィールドの詳細については出力トラフィック セレクタ （11 ページ）を参照してください。

ステップ 10 [Next] をクリックして [Buffers & Captures] 画面を表示します。続行するには、「バッファ」(34-8 ページ）を参照してください。

ステップ 11 最新のキャプチャを 10 秒ごとに自動的に取得するように、[Capture Parameters] 領域で [Get capture every 10 seconds] チェックボックスをオンにします。デフォルトでは、このキャプチャは循環バッファを使用します。

ステップ 12 [Buffer Parameters] 領域で、バッファ サイズとパケット サイズを指定します。バッファ サイズは、キャプチャがパケットを保存するために使用可能なメモリの最大容量です。パケット サイズは、キャプチャが保持できる最長のパケットです。できる限り多くの情報をキャプチャするため、最長パケット サイズを使用することを推奨します。

a) パケット サイズを入力します。有効なサイズ範囲は 14 ～ 1522 バイトです。
b) バッファ サイズを入力します。有効なサイズ範囲は 1534 ～ 33554432 バイトです。
c) キャプチャされたパケットを保存するには、[Use circular buffer] チェックボックスをオンにします。

（注） この設定を選択すると、すべてのバッファ ストレージが使用されている場合、キャプチャは最も古いパケットへの上書きを始めます。

ステップ 13 [Next] をクリックして、入力したクラスタ内の全装置のクラスタ オプション（クラスタを使用している場合）、トラフィック セレクタ、バッファ パラメータを表示する [Summary] 画面を表示します。続行するには、「サマリー」(34-8 ページ）を参照してください。

ステップ 14 [Next] をクリックして [Run Captures] 画面を表示し、次に [Start] をクリックしてパケットのキャプチャを開始します。[Stop] をクリックしてキャプチャを終了します。以降の手順については、キャプチャの実行 （12ページ）を参照してください。クラスタリングを使用している場合は、ステップ 14 に進みます。

ステップ 15 残りのバッファ スペースを確認するには、[Get Capture Buffer] をクリックします。現在のパケットの内容を削除して、バッファに別のパケットをキャプチャするスペースを確保するには、[Clear Buffer on Device] をクリックします。

ステップ 16 クラスタ環境では、[Run Captures] 画面で、次の手順の 1 つ以上を実行します。

- [Get Cluster Capture Summary] をクリックすると、クラスタ内の全装置のパケット キャプチャ情報のサマリーに続いて、各装置のパケット キャプチャ情報が表示されます。
- [Get Capture Buffer] をクリックすると、クラスタの各装置にどの程度バッファ スペースが残っているかが表示されます。[Capture Buffer from Device] ダイアログ ボックスが表示されます。
- [Clear Capture Buffer] をクリックすると、クラスタ内の特定の装置またはすべての装置の現在のコンテンツを削除し、さらにパケットをキャプチャするためのバッファ容量を確保します。

ステップ 17 [Save captures] をクリックして、[Save Capture] ダイアログボックスを表示します。入力キャプチャ、出力キャプチャ、またはその両方を保存するオプションを選択できます。続行するには、「キャプチャの保存」(34-9 ページ）を参照してください。

ステップ 18 [Save Ingress Capture] をクリックして、[Save capture file] ダイアログボックスを表示します。PC 上の保存場所を指定して、[Save] をクリックします。

ステップ 19 [Launch Network Sniffer Application] をクリックして、**[Tools]** > **[Preferences]** で指定したパケット分析アプリケーションを起動し、入力キャプチャを分析します。

ステップ 20 [Save Egress Capture] をクリックして、[Save capture file] ダイアログボックスを表示します。PC 上の保存場所を指定して、[Save] をクリックします。

ステップ 21 [Launch Network Sniffer Application] をクリックして、**[Tools]** > **[Preferences]** で指定したパケット分析アプリケーションを起動し、出力キャプチャを分析します。

ステップ 22 [Close] をクリックし、次に [Finish] をクリックしてウィザードを終了します。

パケット キャプチャのガイドライン

コンテキスト モード

- コンテキスト内のクラスタ制御リンクでキャプチャを設定できます。この場合、そのクラスタ制御リンクで送信されるコンテキストに関連付けられているパケットだけがキャプチャされます。
- 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）キャプチャを削除した場合は、別のコンテキストで事前に設定したキャプチャがあっても、アクティブになるキャプチャはありません。キャプチャをアクティブにするには、キャプチャを削除して追加し直す必要があります。
- 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 上の他のコンテキストへのトラフィックも含まれます。したがって、ある VLAN のコンテキスト A でのキャプチャをイネーブルにしたときに、その VLAN がコンテキスト B でも使用される場合は、コンテキスト A とコンテキスト B の両方の入力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。

その他のガイドライン

- ASA が不正な形式の TCP ヘッダーを持つパケットを受信し、ASP が *invalid-tcp-hdr-length* であるというドロップ理由でそのパケットをドロップする場合、そのパケットを受信したインターフェイス上の **show capture** コマンド出力は、そのパケットを表示しません。
- IP トラフィックだけをキャプチャできます。ARP などの非 IP パケットはキャプチャできません。
- インライン SGT タグ付きパケットの場合、キャプチャされたパケットに含まれている追加 CMD ヘッダーを、PCAP ビューアが認識しないことがあります。
- パケットキャプチャには、システムを変更する、またはインスペクションのために接続に挿入されるパケット、NAT、TCP の正規化、パケットの内容を調整するその他の機能が含まれます。

入力トラフィック セレクタ

パケットキャプチャの入力インターフェイス、送信元と宛先のホストまたはネットワーク、およびプロトコルを設定するには、次の手順を実行します。

手順

ステップ 1 ドロップダウン リストから入力インターフェイス名を選択します。

ステップ 2 入力送信元ホストおよびネットワークを入力します。ASA CX データプレーン上でパケットをキャプチャするには、[Use backplane channel] オプション ボタンをクリックします。

ステップ 3 入力宛先ホストおよびネットワークを入力します。

ステップ 4 キャプチャするプロトコル タイプを指定します。指定できるプロトコルは、ah、eigrp、esp、gre、icmp、icmp6、igmp、igrp、ip、ipinip、nos、ospf、pcp、pim、snp、tcp、または udp です。

a) ICMP にのみ ICMP タイプを入力します。指定できるタイプは、all、alternate address、conversion-error、echo、echo-reply、information-reply、information-request、mask-reply、mask-request、mobile-redirect、parameter-problem、redirect、router-advertisement、router-solicitation、source-quench、time-exceeded、timestamp-reply、timestamp-request、traceroute、または unreachable です。

b) TCP および UDP プロトコルだけの送信元および宛先ポートのサービスを指定します。指定できるオプションは次のとおりです。

- すべてのサービスを含めるには、[All Services] を選択します。
- サービス グループを含めるには、[Service Groups] を選択します。

  特定のサービスを含めるには、aol、bgp、chargen、cifx、citrix-ica、ctiqbe、daytime、discard、domain、echo、exec、finger、ftp、ftp-data、gopher、h323、hostname、http、https、ident、imap4、irc、kerberos、klogin、kshell、ldap、ldaps、login、lotusnotes、lpd、netbios-ssn、nntp、pcanywhere-data、pim-auto-rp、pop2、pop3、pptp、rsh、rtsp、sip、smtp、sqlnet、ssh、sunrpc、tacacs、talk、telnet、uucp、または whois のいずれかを指定します。

ステップ 5 Cisco TrustSec サービスのパケット キャプチャをイネーブルにするには、[Security Group Tagging] 領域の [SGT number] チェックボックスをオンにして、セキュリティ グループ タグ番号を入力します。有効なセキュリティ グループ タグ番号は 2 ～ 65519 です。

出力トラフィック セレクタ

パケットキャプチャでの出力インターフェイス、送信元と宛先のホストとネットワーク、および送信元と宛先ポートのサービスを設定するには、次の手順を実行します。

手順

ステップ 1 インターフェイスでパケットをキャプチャするには、[Select Interface] オプション ボタンをクリックします。ASA CX データプレーン上でパケットをキャプチャするには、[Use backplane channel] オプション ボタンをクリックします。

ステップ 2 ドロップダウン リストから出力インターフェイス名を選択します。

ステップ 3 出力送信元ホストおよびネットワークを入力します。

ステップ 4 出力宛先ホストおよびネットワークを入力します。

入力設定時に選択したプロトコル タイプがすでにリストされています。

Buffers

パケット キャプチャのパケット サイズ、バッファ サイズ、および循環バッファを使用するかどうかを設定するには、次の手順を実行します。

手順

ステップ 1 キャプチャが保持できる最長のパケットを入力します。できるだけ多くの情報をキャプチャするために、指定可能な最長サイズを使用してください。

ステップ 2 パケットを保存するためにキャプチャが使用できるメモリの最大容量を入力します。

ステップ 3 パケットの保存には循環バッファを使用します。循環バッファのバッファ ストレージがすべて使い尽くされると、キャプチャは最も古いパケットから上書きを始めます。

概要

[Summary] 画面には、クラスタ オプション（クラスタリングを使用している場合）、トラフィック セレクタ、前のウィザード画面で選択したパケット キャプチャのためのバッファ パラメータが表示されます。

キャプチャの実行

キャプチャ セッションの開始および停止、キャプチャ バッファの表示、ネットワーク アナライザ アプリケーションの起動、パケット キャプチャの保存、およびバッファのクリアを行うには、次の手順を実行します。

手順

ステップ 1 [Start] をクリックして、選択したインターフェイス上でパケット キャプチャ セッションを開始します。

ステップ 2 [Stop] をクリックして、選択したインターフェイス上のパケット キャプチャ セッションを停止します。

ステップ 3 [Get Capture Buffer] をクリックして、インターフェイス上でキャプチャされたパケットのスナップショットを取得します。

ステップ 4 [Ingress] をクリックして、入力インターフェイスのキャプチャ バッファを表示します。

ステップ 5 [Egress] をクリックして、出力インターフェイスのキャプチャ バッファを表示します。

ステップ 6 [Clear Buffer on Device] をクリックして、デバイス上のバッファを消去します。

ステップ 7 [Launch Network Sniffer Application] をクリックして、**[Tools]** > **[Preferences]** で指定した、入力キャプチャまたは出力キャプチャを分析するためのパケット分析アプリケーションを起動します。

ステップ 8 [Save Captures] をクリックして、入力キャプチャおよび出力キャプチャを ASCII または PCAP 形式で保存します。

キャプチャの保存

パケットをさらに分析するために、入力および出力パケット キャプチャを ASCII または PCAP ファイル形式で保存するには、次の手順を実行します。

手順

ステップ 1 キャプチャ バッファを ASCII 形式で保存するには、[ASCII] をクリックします。

ステップ 2 キャプチャ バッファを PCAP 形式で保存するには、[PCAP] をクリックします。

ステップ 3 入力パケット キャプチャを保存するファイルを指定するには、[Save ingress capture] をクリックします。

ステップ 4 出力パケット キャプチャを保存するファイルを指定するには、[Save egress capture] をクリックします。

ASAv の vCPU 使用量

ASAv の vCPU 使用率では、データ パス、制御ポイント、および外部プロセスで使用されている vCPU の量を表示します。

vSphere で報告される vCPU の使用率には、この ASAv の使用率に加えて、次のものが含まれます。

- ASAv アイドル時間
- ASAv VM に使用された %SYS オーバーヘッド
- vSwitch、vNIC および pNIC の間を移動するパケットのオーバーヘッド。このオーバーヘッドは非常に大きくなる場合があります。

CPU 使用率の例

報告された vCPU の使用率が大幅に異なる例を次に示します。

- ASAv のレポート：40%
- DP：35%
- 外部プロセス：5%
- vSphere のレポート：95%
- ASA（ASAv レポートとして）：40%
- ASA アイドル ポーリング：10%
- オーバーヘッド：45%

オーバーヘッドは、ハイパーバイザ機能の実行、および vSwitch を使用した NIC と vNIC の間のパケット転送に使用されています。

ASAv のためのオーバーヘッドとして、ESXi サーバが追加のコンピューティング リソースを使用する場合があるため、使用率は 100% を超えることがあります。

VMware の CPU 使用率のレポート

vSphere で [VM Performance] タブをクリックし、[Advanced] をクリックすると [Chart Options] ドロップダウンリストが表示されます。ここには VM の各ステート（%USER、%IDLE、%SYS など）の vCPU 使用率が表示されます。この情報は、VMware の観点から CPU リソースが使用されている場所を理解するのに役立ちます。

ESXi サーバのシェル（ホストへの接続に SSH を使用してシェルにアクセスします）では、esxtop を使用できます。Esxtop は Linux の **top** コマンドに似た操作性と外観を持ち、次の内容を含む vSphere のパフォーマンスに関する VM のステート情報を提供します。

- vCPU、メモリ、ネットワーク使用率の詳細
- 各 VM のステートごとの vCPU 使用率
- メモリ（実行中に「M」と入力）とネットワーク（実行中に「N」と入力）に加えて、統計情報と RX ドロップ数

ASAv のグラフと vCenter のグラフ

ASAv と vCenter の間で CPU 使用率の数字に違いがあります。

- vCenter のグラフの数値は常に ASAv の数値よりも大きくなります。
- vCenter ではこの値は「%CPU usage」と呼ばれ、ASAv ではこの値は「%CPU utilization」と呼ばれます。

用語「%CPU utilization」と「%CPU usage」は別のものを意味しています。

- CPU utilization は、物理 CPU の統計情報を提供します。

- CPU usage は CPU のハイパースレッディングに基づいた論理 CPU の統計情報を提供します。しかし、1 つの vCPU のみが使用されるため、ハイパースレッディングは動作しません。

vCenter は CPU % usage を次のように計算します。

アクティブに使用された仮想 CPU の量。使用可能な CPU の合計に対する割合として指定されます。

この計算は、ホストから見た CPU 使用率であり、ゲスト オペレーティング システムから見た CPU 使用率ではありません。また、これは仮想マシンで使用可能なすべての仮想 CPU の平均 CPU 使用率になります。

たとえば、1 個の仮想 CPU を搭載した 1 つの仮想マシンが、4 個の物理 CPU を搭載した 1 台のホストで実行されており、その CPU 使用率が 100% の場合、仮想マシンは、1 個の物理 CPU をすべて使用しています。仮想 CPU の使用率は、「MHz 単位の使用率 / 仮想 CPU の数 x コア周波数」として計算されます。

使用率を MHz で比較すると、vCenter と ASAv の両方の数値は一致します。vCenter グラフから、MHz % CPU 使用率は 60/(2499 x 1 vCPU) = 2.4 と求められます。

設定のテスト

ここでは、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上のホストから他のインターフェイス上のホストに ping できるようにする方法について説明します。

基本接続のテスト：アドレス向けの ping の実行

ping は、特定のアドレスが使用可能で、応答するかどうかを確認するための単純なコマンドです。次のトピックでは、このコマンドの詳細とそれを使って実行可能なテストについて説明します。

ping で実行可能なテスト

デバイスを ping すると、そのデバイスにパケットが送信され、デバイスが応答を返します。このプロセスを使用して、ネットワーク デバイスは、相互に検出、識別、およびテストすることができます。

ping を使用して、次のテストを実行できます。

- 2 つのインターフェイスのループバック テスト：同じ ASA で一方のインターフェイスからもう一方のインターフェイスに ping を外部ループバック テストとして起動すると、双方のインターフェイスの基本的な「アップ」ステータスおよび動作を検証できます。
- ASA の ping：別の ASA のインターフェイスを ping し、そのインターフェイスがアップしていて応答することを確認できます。

- ASA 経由の ping：ASA の反対側のデバイスを ping することによって、中間 ASA 経由で ping することができます。パケットは、それぞれの方向に移動するときに、2 つの中間 ASA のインターフェイスを通過します。このアクションは、中間ユニットのインターフェイス、動作、および応答時間の基本テストになります。
- ネットワーク デバイスの疑わしい動作をテストするための ping：ASA インターフェイスから、正常に機能していないと思われるネットワーク デバイスに ping することができます。インターフェイスが正しく設定されているにもかかわらずエコーが受信されない場合は、デバイスに問題があると考えられます。
- 中間通信をテストするための ping：ASA インターフェイスから、正常に機能することがわかっているネットワークデバイスにpingすることができます。エコーを受信した場合、中間にあるデバイスがすべて正常に動作し、物理的に正しく接続されていることが確認されたことになります。

ICMP ping と TCP ping の選択

ASA には、ICMP エコー要求パケットを送信して、エコー応答パケットを受信する従来の ping が付属しています。これは、標準ツールで、すべての仲介ネットワークデバイスでICMP トラフィックが許可される場合にうまく機能します。ICMP ping を使用して、IPv4/IPv6 アドレスまたはホスト名を ping することができます。

ただし、ICMP を禁止しているネットワークもあります。ご使用のネットワークがこれに該当する場合は、代わりに、TCP ping を使用してネットワーク接続をテストできます。TCP ping では、ping から TCP SYN パケットが送信され、応答で SYN-ACK が受信された段階でその ping が成功したと見なされます。また、TCP ping では、IPv4 アドレスまたはホスト名は ping できますが、IPv6 アドレスは ping できません。

正常な ICMP または TCP ping とは、使用されているアドレスが有効で特定のタイプのトラフィックに応答することを意味しているにすぎません。これは基本接続が機能していることを意味します。デバイス上で動作する他のポリシーで、特定のタイプのトラフィックがデバイスを通過できないようにすることができます。

ICMP の有効化

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。セキュリティの低いインターフェイスから高いインターフェイスに 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。

ASA インターフェイスを ping する場合は、そのインターフェイスに適用された ICMP ルールによって、エコー要求パケットとエコー応答パケットが許可される必要があります。ICMP ルールは省略可能です。このルールを設定しなかった場合は、インターフェイスへのすべてのICMP トラフィックが許可されます。

この手順では、ASA インターフェイスの ICMP ping をイネーブルにするため、または、ASA 経由の ping 用に構成する必要のある ICMP コンフィギュレーションのすべてについて説明します。

手順

ステップ 1 ICMP ルールでエコー要求/エコー応答が許可されることを確認します。

ICMP ルールは、省略可能で、インターフェイスに直接送信される ICMP パケットに適用されます。ICMP ルールを適用しなかった場合は、すべての ICMP アクセスが許可されます。この場合は、アクションが不要です。

ただし、ICMP ルールを実装する場合は、エコー要求メッセージとエコー応答メッセージのアドレスを許可するルールが各インターフェイスに含まれていることを確認します。[Configuration] > [Device Management] > [Management Access] > [ICMP] ペインで ICMP ルールを設定します。

ステップ 2 アクセス ルールで ICMP が許可されることを確認します。

ASA 経由でホストを ping する場合は、アクセス ルールで ICMP トラフィックの送受信が許可される必要があります。アクセス ルールは、少なくとも、エコー要求/エコー応答 ICMP パケットを許可する必要があります。これらのルールはグローバル ルールとして追加することができます。

アクセス ルールを使用しない場合は、必要な他のタイプのトラフィックも許可する必要があります。これは、インターフェイスにアクセス ルールを適用すると、暗黙の deny が追加されるため、他のすべてのトラフィックが破棄されるためです。

[Configuration] > [Firewall] > [Access Rules] ペインでアクセス ルールを設定します。単にテスト目的でルールを追加する場合は、テストの終了後にそのルールを削除できます。

ステップ 3 ICMP インスペクションをイネーブルにします。

インターフェイスの ping とは対照的に、ASA 経由で ping する場合は、ICMP インスペクションが必要です。インスペクションを使用すれば、リターン トラフィック（つまり、エコー応答パケット）を ping を開始したホストに返すことができるうえ、パケットあたり 1 つの応答の存在が保証されるため、特定のタイプの攻撃を防止することができます。

ICMP インスペクションは、デフォルトのグローバル インスペクション ポリシーでイネーブルにできます。

a) **[Configuration] > [Firewall] > [Service Policy Rules]** の順に選択します。
b) **inspection_default** グローバル ルールを編集します。
c) [Rule Actions] > [Protocol Inspection] タブで、ICMP を選択します。
d) [OK] をクリックし、さらに [Apply] をクリックします。

ホストの ping

デバイスを ping するには、[Tools] > [Ping] を選択して、ping する宛先の IP アドレスまたはホスト名を入力し、[Ping] をクリックするだけです。TCP ping の場合は、[TCP] を選択して、宛先ポートも含めます。通常は、実行する必要のあるテストの範囲にします。

成功した ping の出力例：

```
Sending 5, 100-byte ICMP Echos to out-pc, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

ping が失敗した場合は、失敗した試行が ? で示され、成功率が 100% 未満になります（すべて失敗した場合は 0% になります）。

```
Sending 5, 100-byte ICMP Echos to 10.132.80.101, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

ただし、ping の一部の側面を制御するパラメータを追加することもできます。以下に基本オプションを示します。

- ICMP ping：宛先ホストに接続するインターフェイスを選択できます。インターフェイスを選択しなかった場合は、ルーティングテーブルを使用して、適切なインターフェイスが決定されます。IPv4/IPv6 アドレスまたはホスト名を ping することができます。
- TCP ping：ping する宛先の TCP ポートを選択する必要もあります。たとえば、HTTP ポートを ping するには **www.example.com 80** とします。IPv4 アドレスまたはホスト名を ping することはできますが、IPv6 アドレスを ping することはできません。

  ping を送信する送信元アドレスおよびポートを指定するオプションもあります。この場合は、任意で、送信元から ping が送信されるインターフェイスを選択します（インターフェイスを選択しなかった場合は、ルーティング テーブルが使用されます）。

  最後に、ping を繰り返す回数（デフォルトは 5 回）または各試行のタイムアウト（デフォルトは 2 秒）を指定できます。

ASA 接続の体系的なテスト

ASA 接続のさらに体系的なテストを実行する場合は、次の一般的な手順を使用できます。

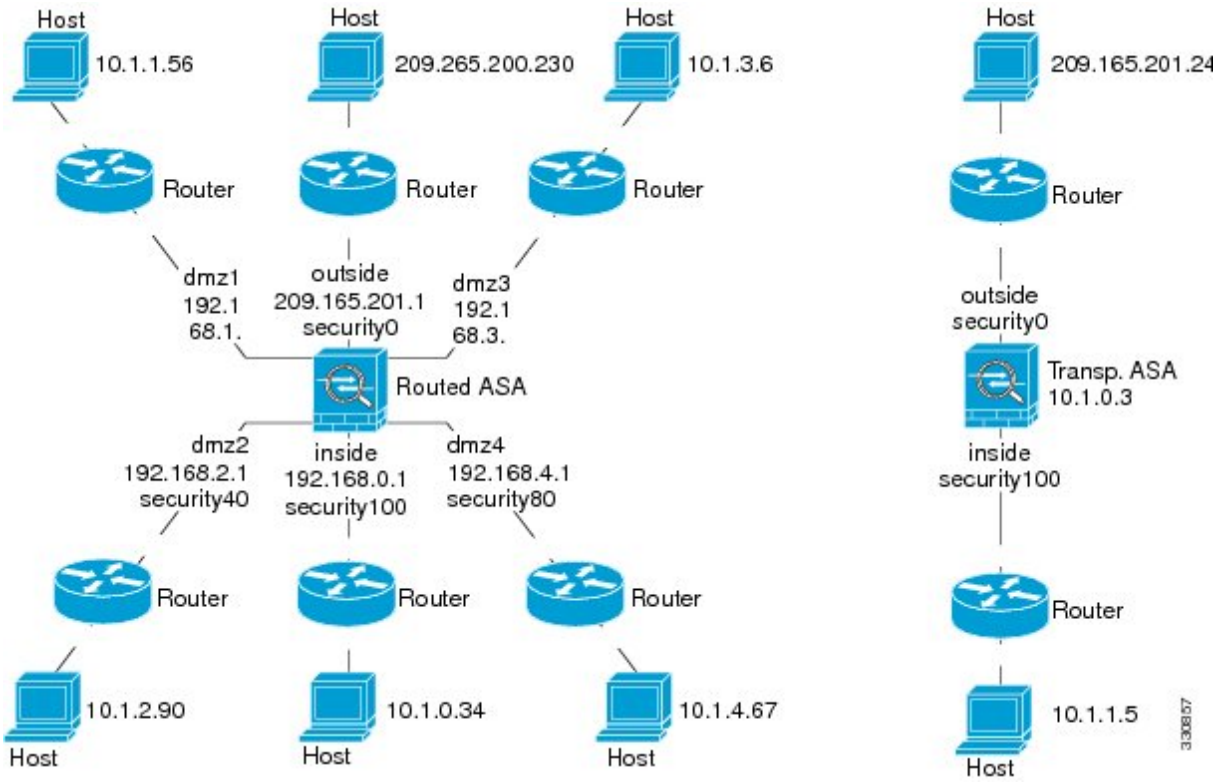
始める前に

手順で説明した syslog メッセージを確認する場合は、ロギングをイネーブルにします（**logging enable** コマンドまたは ASDM の [Configuration] > [Device Management] > [Logging] > [Logging Setup]）。

手順

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。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。

図 *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、BVI IP アドレスを ping します。このテストでは、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（次の図を参照）。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 *2*：*ASA* インターフェイスでの *ping* の失敗

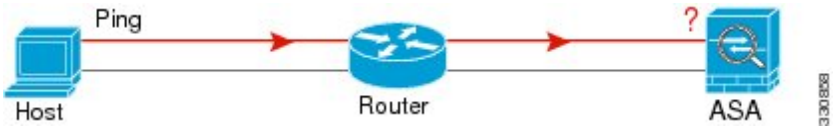
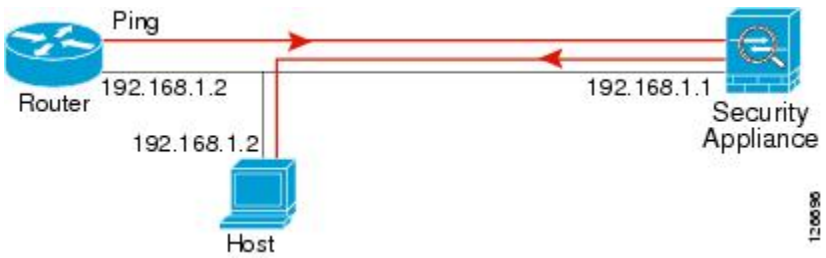


図 *3 : IP* アドレッシングの問題による *ping* の失敗



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（次の図を参照）。

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、BVI 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 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（次の図を参照）。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 *4 : ASA* の戻りルート未設定による *ping* の失敗

ステップ 4 ASA インターフェイスから既知のネットワーク デバイスへの ping は正しく機能しています。

- ping を受信しない場合は、送信ハードウェアまたはインターフェイスのコンフィギュレーションに問題がある可能性があります。
- ASA のインターフェイスが正しく設定されているにもかかわらず、「既知の正常な」デバイスからエコー応答を受信しない場合は、インターフェイスハードウェアの受信機能に問題があると考えられます。「既知の正常な」受信機能を持つ別のインターフェイスで、同じ「既知の正常な」デバイスに対して ping を送信してエコーを受信できる場合、最初のインターフェイスのハードウェアの受信機能に問題があると確認されたことになります。

ステップ 5 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。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。

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）。ping

が外部ホストから内部ホストへ送信され、スタティック変換が存在しない場合は、メッセージ 106010 が表示されます。

図 5 : ASA のアドレス変換の問題による ping の失敗

ホストまでのルートの追跡

IP アドレスへのトラフィックの送信で問題が発生している場合は、ホストまでのルートを追跡することによってネットワーク パスに問題がないかどうかを確認できます。

手順

ステップ 1 トレース ルート上の ASA の表示 （21 ページ）。

ステップ 2 パケット ルートの決定 （22 ページ）を使用して無効にすることができます。

トレース ルート上の ASA の表示

デフォルトで、ASA はトレース ルート上にホップとして表示されません。これを表示するには、ASA を通過するパケットの存続可能時間を減らして、ICMP 到達不能メッセージのレート制限を増やす必要があります。

手順

ステップ 1 サービス ポリシーを使用して TTL を減らします。

a) [Configuration] > [Firewall] > [Service Policy Rules] の順に選択します。

b) ルールを追加または編集します。たとえば、TTL を減らすためのオプションを追加可能なルールがすでに存在する場合は、新しいルールを作成する必要はありません。

c) ルールをグローバルまたはインターフェイスに適用し、トラフィック照合を指定する [Rule Actions] ページまでウィザードを進めます。たとえば、グローバル match any ルールを作成できます。

d) [Rule Actions] ページで、[Connection Settings] タブをクリックして、[Decrement time to live for a connection] を選択します。

e) [OK] または [Finish] をクリックしてから、[Apply] をクリックします。

ステップ 2 ICMP 到達不能レート制限を増やします。

a) [Configuration] > [Device Management] > [Management Access] > [ICMP] を選択します。
b) ページの下部にある [IPv4 ICMP Unreachable Message Limits] > [Rate Limit] の値を増やします。たとえば、50 に増やします。
c) [Apply] をクリックします。

パケット ルートの決定

traceroute を使用すれば、パケットが宛先に到着するまでのルートを特定できます。traceroute は、無効なポート上の宛先に UDP パケットまたは ICMPv6 エコーを送信することで機能します。ポートが有効でないため、宛先への途中にあるルータは ICMP または ICMPv6 Time Exceeded Message で応答し、そのエラーを ASA に報告します。

traceroute は送信された各プローブの結果を表示します。出力の各行が 1 つの TTL 値に対応します（昇順）。次の表に、出力記号の説明を示します。

出力記号	説明
*	タイムアウトの期間内にプローブへの応答を受信しませんでした。
U	宛先へのルートが存在しません。
nn msec	各ノードに対する、指定した数のプローブのラウンドトリップ時間（ミリ秒）。
!N.	ICMP ネットワークに到達できません。ICMPv6 では、アドレスは対象外です。
!H	ICMP ホストに到達できません。
!P	ICMP に到達できません。ICMPv6 では、ポートが到達不能です。
!A	ICMP が設定によって禁止されています。
?	ICMP の原因不明のエラーが発生しました。

手順

ステップ 1 **Tools** > **Traceroute** の順に選択します。

ステップ 2 ルートを追跡する宛先ホスト名または IP アドレスを入力します。ホスト名を使用するように DNS サーバを設定します。

ステップ 3 （オプション）トレースの特性を設定します。デフォルトがほとんどのケースに適合します。

- [Timeout]：タイムアウトするまで応答を待機する時間。デフォルトは 3 秒です。

- [Port]：使用する UDP ポート。デフォルトは 33434 です。
- [Probe]：各 TTL レベルで送信するプローブの数。デフォルトは 3 です。
- [TTL]：プローブの最小および最大存続可能時間。デフォルトの最小値は 1 ですが、この値を増やして、既知のホップの表示を抑制することができます。デフォルトの最大値は30です。トレースルートは、パケットが宛先に到達するか、または最大値に達すると終了します。
- [Specify source interface or IP address]：トレースの送信元として使用するインターフェイス。インターフェイスは、名前または IP アドレスで指定できます。IPv6 では、送信元インターフェイスを指定できません。送信元 IP アドレスだけを指定できます。IPv6 アドレスは、ASA インターフェイスで IPv6 を有効にしている場合にのみ有効です。トランスペアレント モードでは、管理アドレスを使用する必要があります。
- [Reverse Resolve]：DNS 名前解決が設定されている場合に検出されたホップの名前を出力に表示するかどうか。IP アドレスのみを表示するオプションを選択解除します。
- [Use ICMP]：UDP プローブ パケットの代わりに ICMP プローブ パケットを送信するかどうか。

ステップ 4 [Trace Route] をクリックしてトレースルートを開始します。

[Traceroute Output] 領域に、トレースルートの結果についての詳細なメッセージが表示されます。

パケット トレーサを使用したポリシー設定のテスト

送信元と宛先のアドレスおよびプロトコルの特性に基づいてパケットをモデル化することによってポリシー設定をテストできます。トレースは、ポリシー参照を実行してアクセスルールや NAT などをテストし、パケットを許可するか、拒否するかを確認します。

このようにパケットをテストすることによって、ポリシーの結果を確認し、必要に応じて、許可または拒否するトラフィックのタイプが処理されるかどうかをテストできます。設定の確認に加えて、トレーサを使用して許可すべきパケットが拒否されるなどの予期せぬ動作をデバッグできます。

手順

ステップ 1 **[Tools]** > **[Packet Tracer]** の順に選択します。

ステップ 2 パケット トレースの送信元**インターフェイス**を選択します。

ステップ 3 パケットトレースの**パケットタイプ**を指定します。指定できるプロトコルタイプは、ICMP、IP、TCP、UDP、および SCTP です。

ステップ 4 （オプション）。セキュリティ グループ タグの値がレイヤ 2 CMD ヘッダーに埋め込まれたパケットを追跡する（Trustsec）場合は、[SGT number] をオンにして、セキュリティ グループ タグの番号（0 ～ 65533）を入力します。

ステップ 5 （トランスペアレント モード）パケット トレーサが（後でサブインターフェイスにリダイレクトされる）親インターフェイスに入るようにするには、[VLAN ID] をオンにして、1 ～ 4096 の範囲の ID を入力します。VLAN ID は、入力インターフェイスがサブインターフェイスでない場合にのみ使用できます。

ステップ 6 （トランスペアレント モード）**宛先 MAC アドレス**を指定します。

ステップ 7 パケットの送信元と宛先を指定します。

Cisco TrustSec を使用する場合は、IPv4 または IPv6 アドレス、完全修飾ドメイン名（FQDN）、またはセキュリティ グループの名前あるいはタグを指定できます。送信元アドレスに対して、Domain\username 形式でユーザ名を指定することもできます。

ステップ 8 プロトコルの特性を指定します。

- [ICMP]：ICMP タイプ、ICMP コード（0 ～ 255）、およびオプションで ICMP 識別子を入力します。
- [TCP/UDP/SCTP]：送信元および宛先のポート番号を入力します。
- [Raw IP]：プロトコル番号(0 ～ 255）を入力します。

ステップ 9 [Start] をクリックして、パケットをトレースします。

[Information Display Area] に、パケット トレースの結果に関する詳細情報が表示されます。

パフォーマンスとシステム リソースのモニタリング

さまざまなシステム リソースをモニタすることによって、パフォーマンス上の問題またはその他の潜在的な問題を特定することができます。

パフォーマンスのモニタリング

ASA のパフォーマンス情報をグラフ形式または表形式で表示できます。

手順

ステップ 1 **[Monitoring]** ＞ **[Properties]** ＞ **[Connection Graphs]** ＞ **[Perfmon]** の順に選択します。

ステップ 2 [Graph Window Title] にグラフ ウィンドウのタイトルを入力することも、既存のタイトルを選択することもできます。

ステップ 3 [Available Graphs] リストから最大 4 つのエントリを選択してから、[Add] をクリックしてそれらのエントリを [Selected Graphs] リストに移動します。使用可能なオプションは次のとおりです。

- [AAA Perfmon]：認証、許可、およびアカウンティング要求に関する秒単位の要求数。
- [Inspection Perfmon]：HTTP、FTP、および TCP インスペクションに関する秒単位のパケット数。
- [Web Perfmon]：URL アクセス要求と URL サーバ要求に関する秒単位の要求数。
- [Connections Perfmon]：すべての接続、UDP 接続、TCP 接続、および TCP 代行受信に関する秒単位の接続数。
- [Xlate Perfmon]：秒単位の NAT xlate。

ステップ 4 [Show Graphs] をクリックします。

グラフ ビューとテーブル ビューの間でそれぞれの表示を切り替えることができます。また、データの更新頻度を変更したり、データをエクスポートまたは印刷したりすることもできます。

メモリ ブロックのモニタリング

空きメモリ ブロックと使用中のメモリ ブロックをグラフ形式または表形式で表示できます。

手順

ステップ 1 **[Monitoring]** > **[Properties]** > **[System Resources Graphs]** > **[Blocks]** の順に選択します。

ステップ 2 [Graph Window Title] にグラフ ウィンドウのタイトルを入力することも、既存のタイトルを選択することもできます。

ステップ 3 [Available Graphs] リストからエントリを選択してから、[Add] をクリックしてそれらのエントリを [Selected Graphs] リストに移動します。使用可能なオプションは次のとおりです。

- [Blocks Used]：ASA で使用中のメモリ ブロックを表示します。
- [Blocks Free]：ASA の空きメモリ ブロックを表示します。

ステップ 4 [Show Graphs] をクリックします。

グラフ ビューとテーブル ビューの間でそれぞれの表示を切り替えることができます。また、データの更新頻度を変更したり、データをエクスポートまたは印刷したりすることもできます。

CPU のモニタリング

CPU 使用率を表示できます。

手順

ステップ 1 **[Monitoring]** > **[Properties]** > **[System Resources Graphs]** > **[CPU]** の順に選択します。

ステップ 2 [Graph Window Title] にグラフ ウィンドウのタイトルを入力することも、既存のタイトルを選択することもできます。

ステップ 3 [Selected Graphs] リストに [CPU Utilization] を追加します。

ステップ 4 [Show Graphs] をクリックします。

グラフ ビューとテーブル ビューの間で表示を切り替えることができます。また、データの更新頻度を変更したり、データをエクスポートまたは印刷したりすることもできます。

メモリのモニタリング

メモリ使用量情報をグラフ形式または表形式で表示できます。

手順

ステップ 1 **[Monitoring]** > **[Properties]** > **[System Resources Graphs]** > **[Memory]** の順に選択します。

ステップ 2 [Graph Window Title] にグラフ ウィンドウのタイトルを入力することも、既存のタイトルを選択することもできます。

ステップ 3 [Available Graphs] リストからエントリを選択してから、[Add] をクリックしてそれらのエントリを [Selected Graphs] リストに移動します。使用可能なオプションは次のとおりです。

- [Free Memory]：ASA の空きメモリを表示します。
- [Used Memory]：ASA の使用中のメモリを表示します。

ステップ 4 [Show Graphs] をクリックします。

グラフ ビューとテーブル ビューの間でそれぞれの表示を切り替えることができます。また、データの更新頻度を変更したり、データをエクスポートまたは印刷したりすることもできます。

プロセス単位の 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。ASDM では、30 秒おきに更新されます。

プロセス単位の CPU 使用率を表示するには、**[Monitoring]** > **[Properties]** > **[Per-Process CPU Usage]** の順に選択します。

自動更新を停止して、情報を手動で更新し、ファイルに保存することができます。[Configure CPU Usage Colors] をクリックして、使用率に基づいて背景色と前景色を選択することによって、使用率の高いプロセスのスキャンを実行しやすくすることもできます。

接続のモニタリング

現在の接続を表形式で表示するには、ASDM メイン ウィンドウで、[Monitoring] > [Properties] > [Connections] の順に選択します。各接続に関する情報には、プロトコル、送信元アドレスと宛先アドレスの特性、最後のパケットが送信または受信されてからのアイドル時間、および接続中のトラフィック量が含まれます。

テストおよびトラブルシューティングの履歴

機能名	プラットフォーム リリース	説明
traceroutenの IPv6 サポート	9.7(1)	**traceroute** コマンドが変更され、IPv6 アドレスも受け入れられるようになりました。 次の画面が変更されました。**[Tools]** > **[Traceroute]**
ブリッジグループ メンバーインターフェイス用のパケット トレーサのサポート	9.7(1)	ブリッジグループ メンバーインターフェイスにパケット トレーサを使用できるようになりました。 パケット トレーサの画面に [VLAN ID] および [Destination MAC Address] フィールドが追加されました。**[Tools]** > **[Packet Tracer]**

機能名	プラットフォーム リリース	説明
手動によるパケット キャプチャの開始と停止	9.7(1)	キャプチャを手動で停止および開始できるようになりました。 追加/変更された画面：**[Wizards]** > **[Packet Capture Wizard]** > **[Run Captures]** 追加/変更されたオプション：[Start] ボタン、[Stop] ボタン

機能名	プラットフォーム リリース	説明
強化されたパケット トレーサおよびパケット キャプチャ機能	9.9(1)	

機能名	プラットフォーム リリース	説明
		パケット トレーサは次の機能で強化されました。 • パケットがクラスタ ユニット間を通過するときにパケットを追跡します。 • シミュレートされたパケットが ASA から出られるようにします。 • シミュレートされたパケットのセキュリティ チェックをバイパスします。 • シミュレートされたパケットを IPsec/SSL で復号化されたパケットとして扱います。 パケット キャプチャは次の機能で強化されました。 • パケットを復号化した後にキャプチャします。 • トレースをキャプチャし、永続リストに保持します。 新規または変更された画面： **[Tools] > [Packet Tracer]** 次のオプションをサポートする [Cluster Capture] フィールドを追加しました：[decrypted]、[persist]、[bypass-checks]、[transmit] [All Sessions] ドロップダウン リストの下の [Filter By] ビューに 2 つの新しいオプションを追加しました：[Origin] および [Origin-ID] **[Monitoring] > [VPN] > [VPN**

機能名	プラットフォーム リリース	説明
		Statistics] > **[Packet Tracer and Capture]** [Packet Capture Wizard] 画面に [ICMP Capture] フィールドを追加しました：**[Wizards]** > **[Packet Capture Wizard]** ICMP キャプチャをサポートする 2 つのオプション、**include-decrypted** および **persist** を追加しました。