CHAPTER 86

トラブルシューティング

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。

デバッグ メッセージの表示

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の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 セッションの間に限り **debug** コマンドを使用してください。さらに、**debug** コマンドはネットワーク トラフィックとユーザが少ないときに使用することをお勧めします。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方法は、*コマンド リファレンス*の **debug** コマンドを参照してください。

パケットの取得

パケットのキャプチャは、接続の問題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ときに役立つ可能性があります。パケット キャプチャ機能を使用する場合は、Cisco TAC に連絡することをお勧めします。

パケットをキャプチャするには、次のコマンドを入力します。

コマンド	目的
cluster exec] **capture** *capture_name* [**type** {**asp-drop all** [*drop-code*] | tls-proxy | **raw-data** | **lacp** | **isakmp** [**ikev1** | **ikev2**] | **decrypted** | **webvpn user** *webvpn-user* [**url** *url*]}] [**capture**] [**access-list** *access_list_name*] [**buffer** *buf_size*] [**ethernet-type** *type*] [**interface** *interface_name*] [**reinject-hide**] [**packet-length** *bytes*] [**circular-buffer**] [**trace** *trace_count*] [**real-time**] [**trace**] [**match** *prot* {**host** *source-ip* | *source-ip mask* | **any**}{**host** *destination-ip* | *destination-ip mask* | **any**} [*operator* **port**] **例：** hostname# **capture captest interface inside**	パケット スニッフィングおよびネットワーク障害の切り分けのためにパケット キャプチャ機能をイネーブルにします。 **access-list** *access_list_name* キーワード引数ペアを指定すると、アクセス リストに一致するトラフィックがキャプチャされます。マルチ コンテキスト モードでは、1 つのコンテキスト内でのみこのコマンドを使用できます。**any** キーワードは、単一の IP アドレスおよびマスクの代わりに任意の IP アドレスであることを指定します。**all** キーワードを指定すると、ASA によってドロップされたパケットがすべてキャプチャされます。**asp-drop** [*drop-code*] キーワード引数ペアを指定すると、高速セキュリティ パスによってドロップされたパケットがキャプチャされます。*drop-code* は、高速セキュリティ パスでドロップされるトラフィックのタイプを指定します。ドロップ コードのリストについては、**show asp drop frame** コマンドを参照してください。*drop-code* 引数を入力しないと、ドロップされるパケットすべてがキャプチャされます。このキーワードは、**packet-length**、**circular-buffer**、および **buffer** の各キーワードとともに入力できますが、**interface** キーワードや **ethernet-type** キーワードとともに入力することはできません。クラスタでは、ドロップされた、ユニット間の転送データ パケットもキャプチャされます。マルチ コンテキスト モードでは、このオプションがシステム コンテキストで発行されると、すべてのドロップされたデータ パケットがキャプチャされます。このオプションがユーザ コンテキストで発行されたときは、ドロップされたデータ パケットのうち、そのユーザ コンテキストに属するインターフェイスから入ったものだけがキャプチャされます。**buffer** *buf_size* キーワード引数ペアでは、パケットの格納に使用するバッファのサイズをバイト単位で定義します。このバイト バッファがいっぱいになると、パケット キャプチャは停止します。クラスタ内で使用されるときは、これはユニットあたりのサイズです（全ユニットの合計ではありません）。*capture_name* 引数では、パケット キャプチャの名前を指定します。複数のタイプのトラフィックをキャプチャするには、複数の **capture** ステートメントで同じ名前を使用します。**show capture** コマンドを使用してキャプチャのコンフィギュレーションを表示すると、すべてのオプションが 1 行にまとめられます。 **circular-buffer** キーワードを指定すると、バッファがいっぱいになったときに、バッファが先頭から順に上書きされます。**cluster exec** キーワードは、クラスタリング展開においてのみラッパー CLI プレフィックスとして使用され、**capture** コマンドおよび **show capture** コマンドとともに使用できます。このキーワードを使用すると、**capture** コマンドをあるユニットで発行して、そのコマンドを他のすべてのユニットで同時に実行することができます。**decrypted** キーワードを指定すると、復号化された TCP データを L2 ～ L4 ヘッダーでカプセル化してから、キャプチャ エンジンによってキャプチャすることができます。**ethernet-type** *type* キーワード引数ペアでは、キャプチャするイーサネット タイプを選択します。サポートされるイーサネット タイプには、8021Q、ARP、IP、IP6、IPX、LACP、PPPOED、PPPOES、RARP および VLAN などがあります。802.1Q タイプと VLAN タイプでは例外が発生します。802.1Q タグは自動的にスキップされ、照合には内部イーサネット タイプが使用されます。**host** *ip* キーワード引数ペアでは、パケットの送信先となるホストの単一の IP アドレスを指定します。**interface** *interface_name* キーワード引数ペアでは、パケット キャプチャを使用するインターフェイスの名前を設定します。キャプチャするすべてのパケットのインターフェイスを設定する必要があります。複数の **capture** コマンドで同じ名前を使用して、複数のインターフェイスを設定できます。ASA のデータプレーン上のパケットをキャプチャするには、**interface** キーワードを使用し、インターフェイス名として「asa_dataplane」を指定します。インターフェイス名として「cluster」を指定すると、クラスタ制御リンク インターフェイスのトラフィックをキャプチャできます。インターフェイス名「cluster」と「asa_dataplane」は固定であり、変更はできません。キャプチャのタイプとして **lacp** が設定されている場合は、インターフェイス名は物理名です。**isakmp** キーワードを指定すると、ISAKMP トラフィックがキャプチャされます。これは、マルチ コンテキスト モードでは使用できません。

コマンド（続き）	目的（続き）
	ISAKMP サブシステムは、上位層プロトコルにアクセスできません。このキャプチャは、PCAP パーサーを満足させるために物理、IP、および UDP の各レイヤを 1 つにまとめた疑似キャプチャです。このピア アドレスは、SA 交換から取得され、IP レイヤに保存されます。IKEv1 または IKEv2 のプロトコル情報のみをキャプチャするには **ikev1** または **ikev2** キーワードを使用します。**lacp** キーワードを指定すると、LACP トラフィックがキャプチャされます。設定されている場合は、インターフェイス名は物理インターフェイス名です。**trace**、**match**、**access-list** の各キーワードは、**lacp** キーワードとともに使用することはできません。 *mask* 引数では、IP アドレスのサブネット マスクを指定します。ネットワーク マスクを指定する場合に使用する方式は、Cisco IOS ソフトウェア **access-list** コマンドの方式と異なります。ASA では、ネットワーク マスク（たとえば、Class C マスクの 255.255.255.0）が使用されます。Cisco IOS マスクでは、ワイルドカード ビット（たとえば、0.0.0.255）が使用されます。**match** *prot* キーワード引数ペアでは、5 タプルが一致するパケットをフィルタリングしてキャプチャすることを指定します。1 行に最大 3 回このキーワードを使用できます。*operator* 引数では、送信元または宛先で使用されるポート番号の条件を指定します。使用できる演算子は、次のとおりです。 • **lt**：より小さい • **gt**：より大きい • **eq**：等しい **packet-length** *bytes* キーワード引数ペアでは、各パケットのうち最大何バイトをキャプチャ バッファに格納するかを設定します。（任意）プロトコルを **tcp** または **udp** に設定する場合は、**port** キーワードで TCP または UDP ポートの番号（整数）または名前を指定します。**raw-data** キーワードを指定すると、1 つまたは複数のインターフェイスの受信および送信パケットがキャプチャされます。この設定は、デフォルトです。**real-time** キーワードを指定すると、キャプチャしたパケットがリアルタイムで連続して表示されます。リアルタイムのパケット キャプチャを終了するには、**Ctrl+C** を押します。キャプチャを完全に削除するには、このコマンドの **no** 形式を使用します。このオプションは、**raw-data** キャプチャおよび **asp-drop** キャプチャにだけ適用されます。このオプションは、**cluster exec capture** コマンドを使用するときはサポートされません。**reinject-hide** キーワードを指定すると、再注入されたパケットはキャプチャされません。これは、クラスタリング環境だけで適用されます。**tls-proxy** キーワードを指定すると、1 つ以上のインターフェイスで TLS プロキシからの復号化された発信および着信データがキャプチャされます。**trace** *trace_count* キーワード引数ペアでは、パケット トレース情報をキャプチャする場合に、キャプチャするパケット数を指定します。このオプションをアクセス リストとともに使用すると、トレース パケットがデータ パスに挿入されるので、パケットが想定どおりに処理されているかどうかを判別できます。**type** キーワードでは、キャプチャするデータのタイプを指定します。**url** *url* キーワード引数ペアでは、データ キャプチャの対象とする URL プレフィックスを指定します。サーバへの HTTP トラフィックをキャプチャするには、URL の形式として http://*server*/*path* を使用します。サーバへの HTTPS トラフィックをキャプチャするには、https://*server*/*path* を使用します。**user** *webvpn-user* キーワード引数ペアでは、WebVPN キャプチャのためのユーザ名を指定します。**webvpn** キーワードを指定すると、特定の WebVPN 接続の WebVPN データがキャプチャされます。

クラスタリング環境でのパケット キャプチャ

クラスタ全体のトラブルシューティングをサポートするには、**cluster exec capture** コマンドを使用してマスター ユニット上でのクラスタ固有トラフィックのキャプチャをイネーブルにします。これで、クラスタ内のすべてのスレーブ ユニットでも自動的にイネーブルになります。**cluster exec** キーワードは新しいキーワードであり、**capture** コマンドの前に置くとクラスタ全体のキャプチャがイネーブルになります。

「cluster」というインターフェイス名はクラスタ制御リンクのデフォルト名であり、変更できません。インターフェイス名として「cluster」を指定すると、クラスタ制御リンク インターフェイス上のトラフィックがキャプチャされます。クラスタ制御リンク上のパケットには、コントロール プレーン パケットとデータ プレーン パケットの 2 種類があり、どちらも、転送されたデータ トラフィックとクラスタ LU メッセージが含まれています。IP アドレス ヘッダーの TTL フィールドは、この 2 種類のパケットを区別できるように符号化されます。転送されたデータ パケットがキャプチャされるときは、デバッグのためにクラスタリング トレーラもキャプチャ ファイルに出力されます。

マルチ コンテキスト モードでは、クラスタ インターフェイスはシステム コンテキストに属していますが、ユーザはそのインターフェイスを認識できるので、クラスタ リンクでのキャプチャをユーザ コンテキストで設定できます。システム コンテキストでは、コントロール プレーンとデータ プレーンの両方のパケットが使用できます。データ プレーンでは LU パケットがキャプチャされ、データ パケットのうち、システム コンテキストだけに属するものが転送されます。ユーザ コンテキストでは、コントロール プレーン パケットは認識されません。指定のユーザ コンテキストに属する転送されたデータ パケットと、LU パケットだけがキャプチャされます。セキュリティのために、各コンテキストが認識するのは、そのコンテキストに属するパケットだけとなっています。

注意事項と制限事項

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。

制限の大部分は、ASA のアーキテクチャが本質的に分散型であることと、ASA で使用されるハードウェア アクセラレータによるものです。

- 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。
- マルチ コンテキスト モードでのクラスタ制御リンク キャプチャの場合は、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たパケットだけがキャプチャされます。
- マルチ コンテキスト モードでは、**copy capture** コマンドはシステム スペースでのみ使用できます。構文は次のようになります。

  copy /pcap capture:*Context-name*/*in-cap* **tftp**

  in-cap は、コンテキスト *context-name* で設定されたキャプチャです。
- **cluster exec capture realtime** コマンドはサポートされません。次のエラー メッセージが表示されます。

  ```
  Error: Real-time capture can not be run in cluster exec mode.
  ```

- 共有 VLAN には、次のガイドラインが適用されます。
  - 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。
- 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 リストの設定が終われば、キャプチャを定義し、キャプチャを設定するインターフェイスとともに、このアクセス リストをキャプチャに関連付ける必要があります。

クラスタ全体のキャプチャを実行した後で、同じクラスタ全体のキャプチャ ファイルを TFTP サーバにコピーするには、マスター ユニットで次のコマンドを入力します。

```
hostname (cfg-cluster)# cluster exec copy /pcap capture: cap_name
tftp://location/path/filename.pcap
```

複数の PCAP ファイル（各ユニットから 1 つずつ）が TFTP サーバにコピーされます。宛先のキャプチャ ファイル名には自動的にユニット名が付加され、filename_A.pcap、filename_B.pcap などとなります。この例では、A と B がクラスタ ユニット名です。ファイル名の末尾にユニット名を追加すると、別の宛先名が生成されます。

指定したインターフェイスでのクラスタ全体のキャプチャをイネーブルにするには、例に示したコマンドそれぞれの前に **cluster exec** キーワードを追加します。これらの **capture** コマンドは、マスター ユニットからスレーブ ユニットへの複製だけが可能です。ただし、指定したインターフェイスでのローカル ユニットのキャプチャを、これらの **capture** コマンドを使用して設定することは可能です。

例

次の例では、クラスタ全体の LACP キャプチャを作成する方法を示します。

```
hostname (config)# cluster exec capture lacp type lacp interface gigabitEthernet0/0
```

次の例では、クラスタリング リンクでの制御パス パケットのキャプチャを作成する方法を示します。

```
hostname (config)# capture cp interface cluster match udp any eq 49495 any
hostname (config)# capture cp interface cluster match udp any any eq 49495
```

次の例では、クラスタリング リンクでのデータ パス パケットのキャプチャを作成する方法を示します。

```
hostname (config)# access-list cc1 extended permit udp any any eq 4193
hostname (config)# access-list cc1 extended permit udp any eq 4193 any
hostname (config)# capture dp interface cluster access-list ccl
```

次の例では、クラスタを通過するデータ パス トラフィックをキャプチャする方法を示します。

```
hostname (config)# capture abc interface inside match tcp host 1.1.1.1 host 2.2.2.2 eq www
hostname (config)# capture abc interface inside match udp host 1.1.1.1 any
hostname (config)# capture abc interface inside access-list xxx
```

次の例では、指定した実際の発信元から実際の宛先へのフローに対する論理更新メッセージをキャプチャし、指定した実際の発信元から実際の宛先へ CCL を介して転送されるパケットをキャプチャする方法を示します。

```
hostname (config)# access-list dp permit ip real_src real_dst
```

次の例では、特定タイプのデータ プレーン メッセージ（たとえば ICMP エコー要求/応答）のうち、ある ASA から別の ASA に転送されたものを、メッセージ タイプに応じた **match** キーワードまたはアクセス リストを使用してキャプチャする方法を示します。

```
hostname (config)# capture capture_name interface cluster access-list match icmp any any
```

次の例では、クラスタ制御リンク上でアクセス リスト 103 を使用してキャプチャを作成する方法を示します。

```
hostname (config)# access-list 103 permit ip A B
hostname (config)# capture example1 interface cluster access-list 103
```

前の例で、A と B が CCL インターフェイスの IP アドレスである場合は、この 2 つのユニット間で送信されるパケットだけがキャプチャされます。

A および B が、デバイスを通過するトラフィックの IP アドレスである場合は、次のことが当てはまります。

- 転送されたパケットは、通常どおりにキャプチャされます。ただし、送信元および宛先の IP アドレスがアクセス リストに一致することが条件です。
- データ パス ロジック更新メッセージがキャプチャされるのは、そのメッセージが A と B の間のフローに対するものであるか、特定のアクセス リスト（たとえば、access-list 103）に対するものである場合です。埋め込まれたフローの 5 タプルが一致するものがキャプチャされます。
- UDP パケットの送信元と宛先のアドレスは CCL のアドレスですが、このパケットがフローを更新するためのものであり、そのフローにアドレス A および B が関連付けられている場合は、このパケットもキャプチャされます。つまり、パケットに埋め込まれているアドレス A および B が一致している限り、そのパケットもキャプチャされます。

クラスタリングの詳細については、第 7 章「ASA のクラスタの設定」を参照してください。

クラッシュ ダンプの表示

ASA 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 に連絡することを推奨します。*コマンド リファレンス*の **show crashdump** コマンドを参照してください。

コア ダンプの表示

コア ダンプは、プログラムが異常終了（クラッシュ）した場合の実行中のプログラムのスナップショットです。コア ダンプは、エラーを診断またはデバッグするため、および障害を後からオフサイトで分析できるよう、クラッシュを保存するために使用されます。Cisco TAC では、ユーザがコア ダンプ機能をイネーブルにして、ASA でのアプリケーションまたはシステムのクラッシュをトラブルシューティングする必要がある場合があります。*コマンド リファレンス*の **coredump** コマンドを参照してください。