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。

- 「Packet Capture Wizard を使用したキャプチャの設定と実行」（P.47-1）

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、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にキャプチャされるトラフィックのタイプを制限できます。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。

ステップ 1 メイン ASDM アプリケーション ウィンドウで、[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 パラメータのセット。
- キャプチャの実行。
- （任意）PC へのキャプチャの保存。

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。

（注） クラスタリングの詳細については、第 10 章「ASA のクラスタの設定」を参照してください。

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 オプション] 画面で、[This device only] または [The whole cluster] のどちらかのオプションを選択して検出を実行し、[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検出するには、[Select Interface] オプション ボタンをクリックします。ASA データ プレーン上のパケットを検出するには、[Use backplane channel] オプション ボタンをクリックします。

ステップ 5　[Packet Match Criteria] 領域で、次のいずれかの操作を実行します。

- パケット一致で使用する 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。現在のドロップダウン リストに事前に設定されている ACL を追加するには、[Manage] をクリックして [ACL Manager] ペインを表示します。ACL を選択し、[OK] をクリックします。
- パケット パラメータを指定するには、[Specify Packet Parameters] オプション ボタンをクリックします。

ステップ 6　以降の手順については、「Ingress Traffic Selector」（P.47-3）を参照してください。

ステップ 7　[Next] をクリックして、[Egress Traffic Selector] 画面を表示します。以降の手順については、「Egress Traffic Selector」（P.47-4）を参照してください。

（注）　送信元ポートのサービス、宛先ポートのサービスおよび ICMP タイプは読み取り専用であり、[Ingress Traffic Selector] 画面での選択に基づきます。

ステップ 8　[Next] をクリックして [Buffers & Captures] 画面を表示します。以降の手順については、「Buffers」（P.47-4）を参照してください。

ステップ 9　[Capture Parameters] 領域で、10 秒ごとに最新のキャプチャを自動的に保持するには、[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 10　[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 11　[Next] をクリックして、クラスタ（クラスタを使用する場合）の全装置のクラスタ オプション、トラフィック セレクタ、入力したバッファ パラメータを表示する [Summary] 画面を表示します。以降の手順については、「サマリー」（P.47-5）を参照してください。

ステップ 12　[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」（P.47-5）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 13　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 14　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、クラスタの全装置のパケット検出情報のサマリーが表示されます。続いて、各装置のパケット検出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 Buffer on Device] をクリックして、クラスタのある装置またはすべての装置の現在のコンテンツを削除うし、より多くのパケットを検出するためのバッファの容量を確保します。

ステップ 15　[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。以降の手順については、「キャプチャの保存」（P.47-5）を参照してください。

ステップ 16　入力パケット キャプチャを保存するには、[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 上でのストレージの場所を指定し、[Save] をクリックします。

ステップ 17　[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 18　出力パケット キャプチャを保存するには、[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 上でのストレージの場所を指定し、[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、出力キャプチャを分析します。

ステップ 20　[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。

Ingress Traffic Selector

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。

ステップ 1　[Point of Ingress] 領域で、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。

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。

Egress Traffic Selector

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。

ステップ 1　インターフェイスでパケットを検出するには、[Select Interface] オプション ボタンをクリックします。ASA データ プレーン上のパケットを検出するには、[Use backplane channel] オプション ボタンをクリックします。

ステップ 2　[Point of Egress] 領域で、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。

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。

サマリー

[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検出のためのバッファ 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。

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

ステップ 2　選択したインターフェイスでパケット キャプチャ セッションを停止するには、[Stop] をクリックします。

ステップ 3　インターフェイス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するには、[Get Capture Buffer] をクリックします。

ステップ 4　入力インターフェイスでキャプチャ バッファを表示するには、[Ingress] をクリックします。

ステップ 5　出力インターフェイスでキャプチャ バッファを表示するには、[Egress] をクリックします。

ステップ 6　デバイスのバッファをクリアするには、[Clear Buffer on Device] をクリックします。

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

ステップ 8　入力キャプチャと出力キャプチャを ASCII または PCAP 形式で保存するには、[Save Captures] をクリックします。

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。

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。