CLI および ASDM を使用した ASA パケット キャプチャの設定例

目次

概要

このドキュメントでは、Cisco Adaptive Security Device Manager（ASDM）と CLI のどちらかを使用して、必要なパケットをキャプチャするように Cisco 適応型セキュリティ アプライアンス（ASA）次世代ファイアウォールを設定する方法について説明します。

前提条件

要件

このドキュメントでは、ASA が正常に稼働しており、Cisco ASDM または CLI で設定を変更できるように設定されていることを前提とします。

使用するコンポーネント

このドキュメントは、特定のハードウェアまたはソフトウェア バージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

関連製品

この設定は、次のシスコ製品にも使用できます。

- Cisco ASA バージョン 9.1(5) 以降
- Cisco ASDM バージョン 7.2.1

背景説明

パケット キャプチャ プロセスは、接続の問題をトラブルシューティングしたり、異常なアクティビティをモニタしたりするときに役に立ちます。 加えて、複数のキャプチャを作成して、複数のインターフェイス上のさまざまなタイプのトラフィックを分析することができます。

設定

ここでは、このドキュメントで説明するパケット キャプチャ機能を設定するために使用可能な情報を提供します。

> **注:** このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

設定

> **注:** この設定で使用される IP アドレッシング方式は、インターネット上で正式にルーティング可能なものではありません。 これらは RFC 1918 アドレスであり、ラボ環境で使用されるものです。

ASDM によるパケット キャプチャの設定

注: この設定例は、**User1**(内部ネットワーク）から **Router1**（外部ネットワーク）への ping 中に送信されるパケットをキャプチャするために使用されます。

ASDM を使用して ASA 上のパケット キャプチャ機能を設定するには、次の手順を実行します。

1. 次のように、[Wizards] > [Packet Capture Wizard] の順に選択して、パケット キャプチャ設定を開始します。

2. キャプチャ ウィザードが表示されます。 [Next] をクリックします。

3. 新しいウィンドウで、**入力トラフィック**をキャプチャするために使用するパラメータを指定します。 [Ingress Interface] の [inside] を選択して、キャプチャするパケットの送信元 IP アドレスと宛先 IP アドレス、およびサブネット マスクを、指定されたそれぞれの場所に入力します。 また、次のように、ASA によってキャプチャされるパケット タイプを選択します（ここで選択するパケット タイプは IP です）。

   [Next] をクリックします。

4. [Egress Interface] の [outside] を選択して、キャプチャするパケットの送信元 IP アドレスと宛先 IP アドレス、およびサブネット マスクを、指定されたそれぞれの場所に入力します。 ネットワーク アドレス変換（NAT）がファイアウォール上で実施される場合は、このことも考慮してください。

   [Next] をクリックします。

5. 指定されたそれぞれの場所に、適切な [Packet Size] と [Buffer Size] を入力します。このデータはキャプチャを実行するために必要です。 また、循環バッファ オプションを使用する場合は、[Use circular buffer] チェックボックスをオンにします。 循環バッファは決していっぱいになりません。 バッファが最大サイズに到達すると、古いデータが破棄され、キャプチャが継続されます。 この例では、循環バッファが使用されないため、チェックボックスはオンになりません。

   [Next] をクリックします。

6. このウィンドウには、必要なパケットがキャプチャされるように ASA 上で設定する必要があ**るアクセス リスト**と、キャプチャするパケットのタイプが表示されます（この例では IP パケットがキャプチャされます）。 [Next] をクリックします。

7. 図のように、[Start] をクリックしてパケット キャプチャを開始します。

8. パケット キャプチャが開始されたら、内部ネットワークから外部ネットワークに ping を実行して、発信元 IP アドレスと宛先 IP アドレスの間を流れるパケットが ASA キャプチャ バッファでキャプチャされるようにします。

9. ASA キャプチャ バッファでキャプチャされたパケットを表示するには、[Get Capture Buffer] をクリックします。

10. **入力トラフィック**と**出力トラフィック**の両方に関してキャプチャされたパケットがこのウィンドウに表示されます。 キャプチャ情報を保存するには、[Save captures] をクリックします。

11. [Save Captures] ウィンドウで、キャプチャ バッファの保存形式を選択します。 これは、[ASCII] と [PCAP] のどちらかです。 形式名の横にあるオプション ボタンをクリックします。 次に、必要に応じて、[Save ingress capture] または [Save egress capture] をクリックします。 PCAP ファイルは Wireshark などのキャプチャ アナライザで開くことができ、これが推奨されている方法です。

12. [Save capture file] ウィンドウで、キャプチャ ファイルを保存するファイル名と場所を指定します。 [Save] をクリックします。

13. **[Finish] をクリックします。**

パケット キャプチャの手順は、これで終わりです。

CLI によるパケット キャプチャの設定

CLI を使用して ASA 上のパケット キャプチャ機能を設定するには、次の手順を実行します。

1. ネットワーク図に示すように、正しい IP アドレスとセキュリティ レベルで内部インターフェイスと外部インターフェイスを設定します。

2. パケット キャプチャ プロセスを開始するには、特権 EXEC モードで capture コマンドを使用します。 この設定例では、**capin** という名前のキャプチャが定義されます。 それを**内部インターフェイス**にバインドし、対象のトラフィックと一致するパケットのみがキャプチャされるように **match** キーワードを指定します。

```
ASA# capture capin interface inside match ip 192.168.10.10 255.255.255.255
203.0.113.3 255.255.255.255
```

3. 同様に、**capout** という名前のキャプチャを定義します。 それを**外部インターフェイス**にバインドし、対象のトラフィックと一致するパケットのみがキャプチャされるように **match** キーワードを指定します。

```
ASA# capture capout interface outside match ip 192.168.10.10 255.255.255.255
203.0.113.3 255.255.255.255
```

これで、ASA がインターフェイス間のトラフィック フローのキャプチャを開始します。 どの時点でも、キャプチャを停止するには、no capture コマンドに続けてキャプチャ名を入力します。

次に例を示します。

```
no capture capin interface inside
no capture capout interface outside
```

ASA 上で使用可能なキャプチャ タイプ

ここでは、ASA 上で使用可能なさまざまなタイプのキャプチャについて説明します。

- **asa_dataplane** ：ASA とバックプレーンを使用するモジュール（ASA CX や IPS モジュールなど）の間を通過する ASA バックプレーン上でパケットをキャプチャします。

```
ASA# cap asa_dataplace interface asa_dataplane
ASA# show capture
capture asa_dataplace type raw-data interface asa_dataplane [Capturing - 0 bytes]
```

- **asp-drop** *drop-code* ：高速セキュリティ パスで破棄されるパケットをキャプチャします。 *drop-code* は、高速セキュリティ パスで破棄されるトラフィックのタイプを指定します。

```
ASA# capture asp-drop type asp-drop acl-drop
ASA# show cap
ASA# show capture asp-drop

2 packets captured

1: 04:12:10.428093 192.168.10.10.34327 > 10.94.0.51.15868: S
2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
Flow is denied by configured rule
2: 04:12:12.427330 192.168.10.10.34327 > 10.94.0.51.15868: S
2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
Flow is denied by configured rule
2 packets shown

ASA# show capture asp-drop

2 packets captured

1: 04:12:10.428093 192.168.10.10.34327 > 10.94.0.51.15868: S
2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
```

```
Flow is denied by configured rule
2: 04:12:12.427330 192.168.10.10.34327 > 10.94.0.51.15868: S
2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
Flow is denied by configured rule
2 packets shown
```

- **ethernet-type** *type* ：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。

  この例では、**ARP トラフィック**のキャプチャ方法を示します。

```
ASA# cap arp ethernet-type ?

exec mode commands/options:
 802.1Q
 <0-65535>  Ethernet type
 arp
 ip
 ip6
 ipx
 pppoed
 pppoes
 rarp
 vlan

cap arp ethernet-type arp interface inside


ASA# show cap arp

22 packets captured

1: 05:32:52.119485 arp who-has 10.10.3.13 tell 10.10.3.12
 2: 05:32:52.481862       arp who-has 192.168.10.123 tell 192.168.100.100
3: 05:32:52.481878 arp who-has 192.168.10.50 tell 192.168.100.10
4: 05:32:53.409723 arp who-has 10.106.44.135 tell 10.106.44.244
5: 05:32:53.772085 arp who-has 10.106.44.108 tell 10.106.44.248
6: 05:32:54.782429 arp who-has 10.106.44.135 tell 10.106.44.244
7: 05:32:54.784695 arp who-has 10.106.44.1 tell 11.11.11.112:
```

- **real-time**：キャプチャされたパケットをリアルタイムで連続表示します。 リアルタイム パケット キャプチャを終了するには、**Ctrl + C** キーを押します。 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、**cluster exec capture** コマンドを使用するときはサポートされません。

```
ASA# cap capin interface inside real-time

Warning: using this option with a slow console connection may
result in an excessive amount of non-displayed packets
due to performance limitations.

Use ctrl-c to terminate real-time capture
```

- **Trace**：ASA パケット トレーサ機能と同様に、キャプチャされたパケットを追跡します。

```
ASA#cap in interface Webserver trace match tcp any any eq 80

// Initiate Traffic

1: 07:11:54.670299 192.168.10.10.49498 > 198.51.100.88.80: S
2322784363:2322784363(0) win 8192
```

```
<mss 1460,nop,wscale 2,nop,nop,sackOK>

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 0.0.0.0 0.0.0.0 outside

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group any in interface inside
access-list any extended permit ip any4 any4 log
Additional Information:

Phase: 5
Type: NAT
Subtype:
Result: ALLOW
Config:
object network obj-10.0.0.0
nat (inside,outside) dynamic interface
Additional Information:
Dynamic translate 192.168.10.10/49498 to 203.0.113.2/49498

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type:
Subtype:
Result: ALLOW
```

```
Config:
Additional Information:

Phase: 9
Type: ESTABLISHED
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 10
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 12
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 13
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 41134, packet dispatched to next module

Phase: 14
Type: ROUTE-LOOKUP
Subtype: output and adjacency
Result: ALLOW
Config:
Additional Information:
found next-hop 203.0.113.1 using egress ifc outside
adjacency Active
next-hop mac address 0007.7d54.1300 hits 3170

Result:
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

- **ikev1/ikev2**：インターネット キー エクスチェンジ バージョン 1（IKEv1）または IKEv2 プロトコル情報のみをキャプチャします。

- **isakmp**：VPN 接続に関する Internet Security Association and Key Management Protocol（ISAKMP）トラフィックをキャプチャします。 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 の各層を 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。

- **lacp**：Link Aggregation Control Protocol（LACP）トラフィックをキャプチャします。 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。 これは、LACP の現在の動作を特定するために Etherchannel を使用している場合に役に立つ可能性があります。

- **tls-proxy**：1 つ以上のインターフェイス上で Transport Layer Security（TLS）プロキシからの復号化された着信データと発信データをキャプチャします。

- **webvpn**：特定の WebVPN 接続に関する WebVPN データをキャプチャします。
  注意： WebVPN キャプチャをイネーブルにすると、セキュリティ アプライアンスのパフォーマンスに影響します。 トラブルシューティングに必要なキャプチャ ファイルを生成したら、必ず、キャプチャを無効にしてください。

デフォルト

ASA システムのデフォルト値を以下に示します。

- デフォルトの*タイプ*は **ローデータ** です。
- デフォルトの*バッファ サイズ*は **512 KB** です。
- デフォルトの*イーサネット タイプ*は **IP パケット**です。
- デフォルトの*パケット長*は **1,518 バイト**です。

キャプチャされたパケットの表示

ASA 上で次を実行します。

キャプチャされたパケットを表示するには、show capture コマンドに続けてキャプチャ名を入力します。 ここでは、キャプチャ バッファの内容の **show コマンドの出力**を示します。 **show capture capin** コマンドは、**capin** という名前のキャプチャ バッファの内容を表示します。

```
ASA# show cap capin

8 packets captured

1: 03:24:35.526812 192.168.10.10 > 203.0.113.3: icmp: echo request
2: 03:24:35.527224 203.0.113.3 > 192.168.10.10: icmp: echo reply
3: 03:24:35.528247 192.168.10.10 > 203.0.113.3: icmp: echo request
4: 03:24:35.528582 203.0.113.3 > 192.168.10.10: icmp: echo reply
5: 03:24:35.529345 192.168.10.10 > 203.0.113.3: icmp: echo request
6: 03:24:35.529681 203.0.113.3 > 192.168.10.10: icmp: echo reply
7: 03:24:57.440162 192.168.10.10 > 203.0.113.3: icmp: echo request
8: 03:24:57.440757 203.0.113.3 > 192.168.10.10: icmp: echo reply
```

show capture capout コマンドは、**capout** という名前のキャプチャ バッファの内容を表示します。

```
ASA# show cap capout

8 packets captured

1: 03:24:35.526843 192.168.10.10 > 203.0.113.3: icmp: echo request
2: 03:24:35.527179 203.0.113.3 > 192.168.10.10: icmp: echo reply
```

```
3: 03:24:35.528262 192.168.10.10 > 203.0.113.3: icmp: echo request
4: 03:24:35.528567 203.0.113.3 > 192.168.10.10: icmp: echo reply
5: 03:24:35.529361 192.168.10.10 > 203.0.113.3: icmp: echo request
6: 03:24:35.529666 203.0.113.3 > 192.168.10.10: icmp: echo reply
7: 03:24:47.014098 203.0.113.3 > 203.0.113.2: icmp: echo request
8: 03:24:47.014510 203.0.113.2 > 203.0.113.3: icmp: echo reply
```

オフライン分析のための ASA からのダウンロード

オフラインで分析するためにパケット キャプチャをダウンロードする方法がいくつかあります。

1. 任意のブラウザで、https://<ip_of_asa>/admin/capture/<capture_name>/pcap にアクセスします。
   ヒント： pcap キーワードを省略した場合は、**show capture <cap_name>** コマンドの出力と同様の出力しか得られません。
2. キャプチャをダウンロードするには、**copy capture** コマンドと必要なファイル転送プロトコルを入力します。

```
ASA# show cap capout

8 packets captured

1: 03:24:35.526843 192.168.10.10 > 203.0.113.3: icmp: echo request
2: 03:24:35.527179 203.0.113.3 > 192.168.10.10: icmp: echo reply
3: 03:24:35.528262 192.168.10.10 > 203.0.113.3: icmp: echo request
4: 03:24:35.528567 203.0.113.3 > 192.168.10.10: icmp: echo reply
5: 03:24:35.529361 192.168.10.10 > 203.0.113.3: icmp: echo request
6: 03:24:35.529666 203.0.113.3 > 192.168.10.10: icmp: echo reply
7: 03:24:47.014098 203.0.113.3 > 203.0.113.2: icmp: echo request
8: 03:24:47.014510 203.0.113.2 > 203.0.113.3: icmp: echo reply
```

ヒント： パケット キャプチャの使用に伴う問題をトラブルシューティングする場合は、オフライン分析のためにキャプチャをダウンロードすることをお勧めします。

キャプチャのクリア

キャプチャ バッファをクリアするには、**clear capture <capture-name>** コマンドを入力します。

```
ASA# show capture
capture capin type raw-data interface inside [Capturing - 8190 bytes]
match icmp any any
capture capout type raw-data interface outside [Capturing - 11440 bytes]
match icmp any any

ASA# clear cap capin
ASA# clear cap capout

ASA# show capture
capture capin type raw-data interface inside [Capturing - 0 bytes]
match icmp any any
capture capout type raw-data interface outside [Capturing - 0 bytes]
match icmp any any
```

すべてのキャプチャのバッファをクリアするには、**clear capture /all** コマンドを入力します。

```
ASA# clear capture /all
```

キャプチャの停止

ASA 上でキャプチャを停止する唯一の方法は、次のコマンドを使用して完全に無効にする方法です。

no capture <capture-name>
Cisco Bug ID CSCuv74549 が導入された結果、キャプチャを完全に無効にせずに停止して、トラフィックのキャプチャが開始されるタイミングを制御できるようになりました。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。