

CLIおよびASDMによるASAパケットキャプチャの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[関連製品](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[ASDMによるパケットキャプチャの設定](#)

[CLIによるパケットキャプチャの設定](#)

[ASA上で使用可能なキャプチャタイプ](#)

[デフォルト](#)

[キャプチャされたパケットの表示](#)

[ASA](#)

[オフライン分析のためのASAからのダウンロード](#)

[キャプチャのクリア](#)

[キャプチャの停止](#)

[確認](#)

[トラブルシューティング](#)

はじめに

このドキュメントでは、ASDMまたはCLIを使用して目的のパケットをキャプチャするようにCisco ASA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

この手順では、ASAが完全に動作していて、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ています。

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ました。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。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

関連製品

この設定は、次のシスコ製品にも使用されます。

- 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

このドキュメントでは、Cisco Adaptive Security Device Manager (ASDM) またはコマンドラインインターフェイス (CLI) (ASDM) を使用して目的の packets をキャプチャするために、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 (NGFW) を設定する方法について説明します。

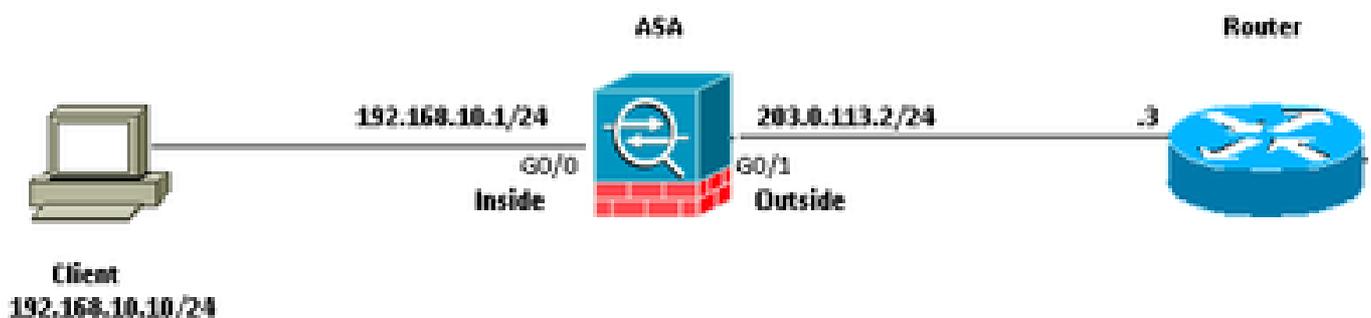
パケットキャプチャプロセスは、接続の問題のトラブルシューティングや疑わしいアクティビティの監視に役立ちます。また、複数のキャプチャを作成して、複数のインターフェイス上の異なるタイプのトラフィックを分析することもできます。

設定

このセクションでは、このドキュメントで説明するパケットキャプチャ機能の設定に使用する情報を提供します。

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 セットアップを使用します。



コンフィギュレーション

この設定で使用している IP アドレス スキームは、インターネット上で正式にルーティング可能

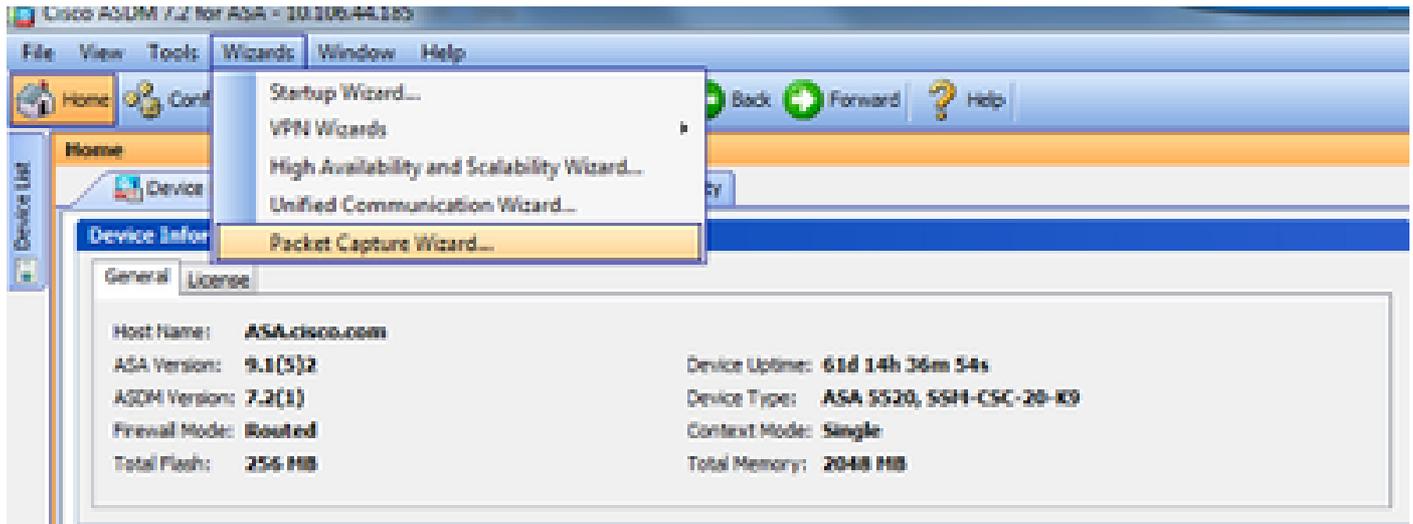
なものではありません。これらは RFC 1918 アドレスであり、ラボ環境で使用されるものです。

ASDM によるパケット キャプチャの設定

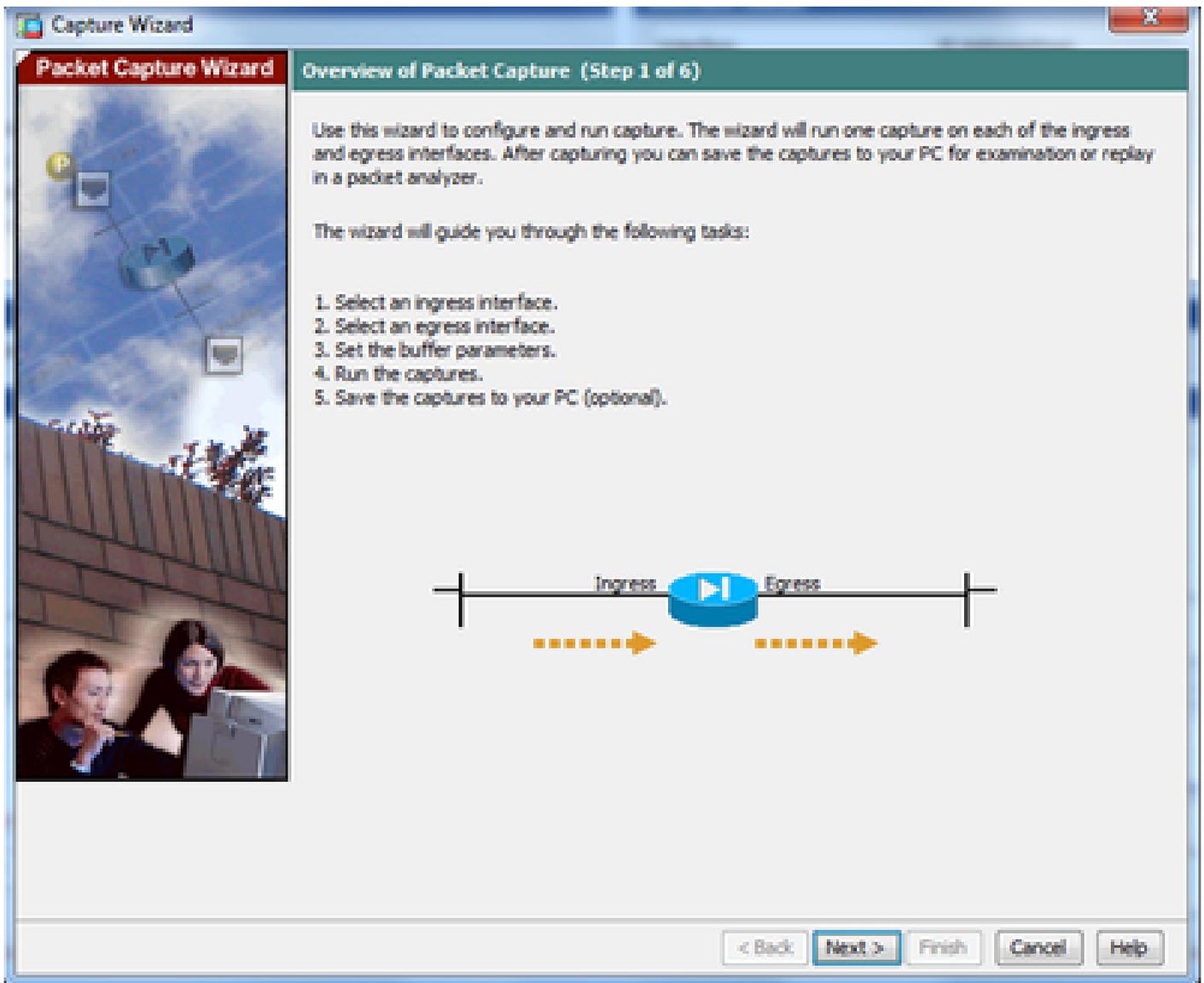
この設定例はで使用され、User1 (内部ネットワーク) から Router1 (外部ネットワーク) への ping 中に送信されるパケットをキャプチャします。

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の順に移動し、パケットキャプチャの設定を開始します。



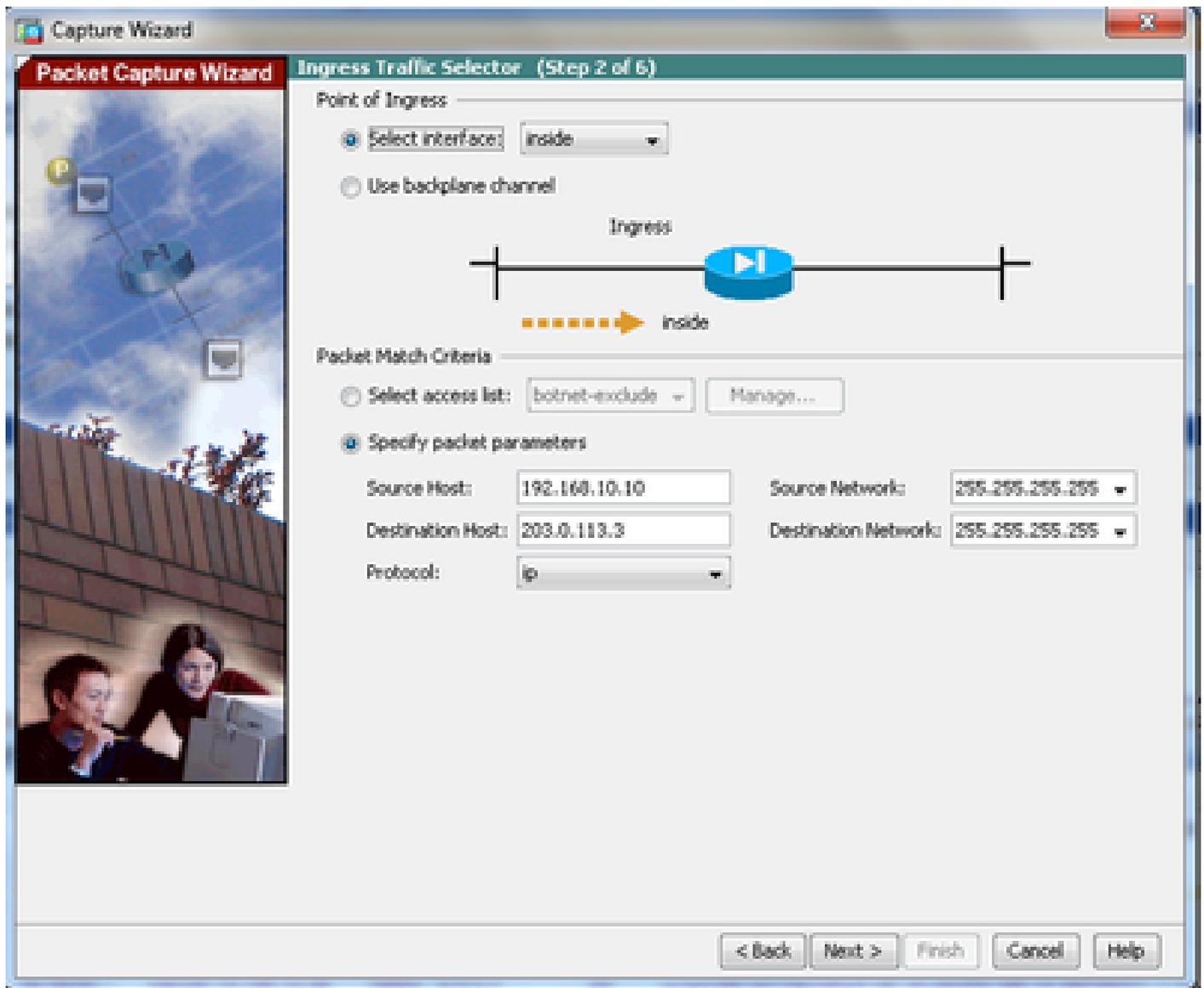
2. キャプチャウィザードが開きます。[Next] をクリックします。



3.0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。

3.1 入力インターフェイスとしてinsideを選択し、キャプチャされるパケットの送信元と宛先のIPアドレスを、サブネットマスクとともに、指定されたそれぞれの場所に入力します。

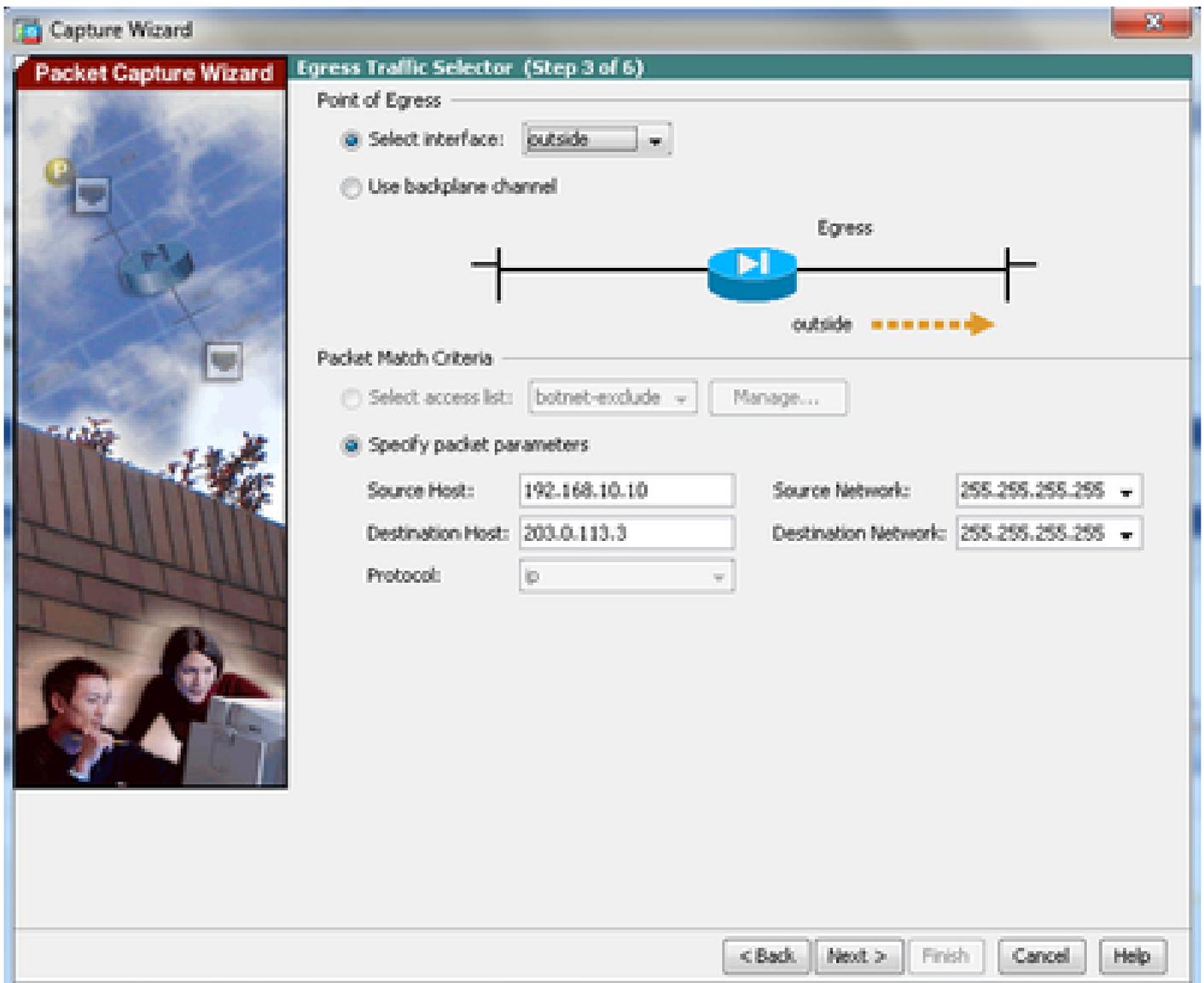
3.2次に示すように、ASAによってキャプチャされるパケットタイプを選択します（ここで選択されるパケットタイプはIP）。



3.3 Nextをクリックします。

4.1 出カインターフェイスとしてoutsideを選択し、表示されるそれぞれの場所に、送信元と宛先のIPアドレスとサブネットマスクを入力します。

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。



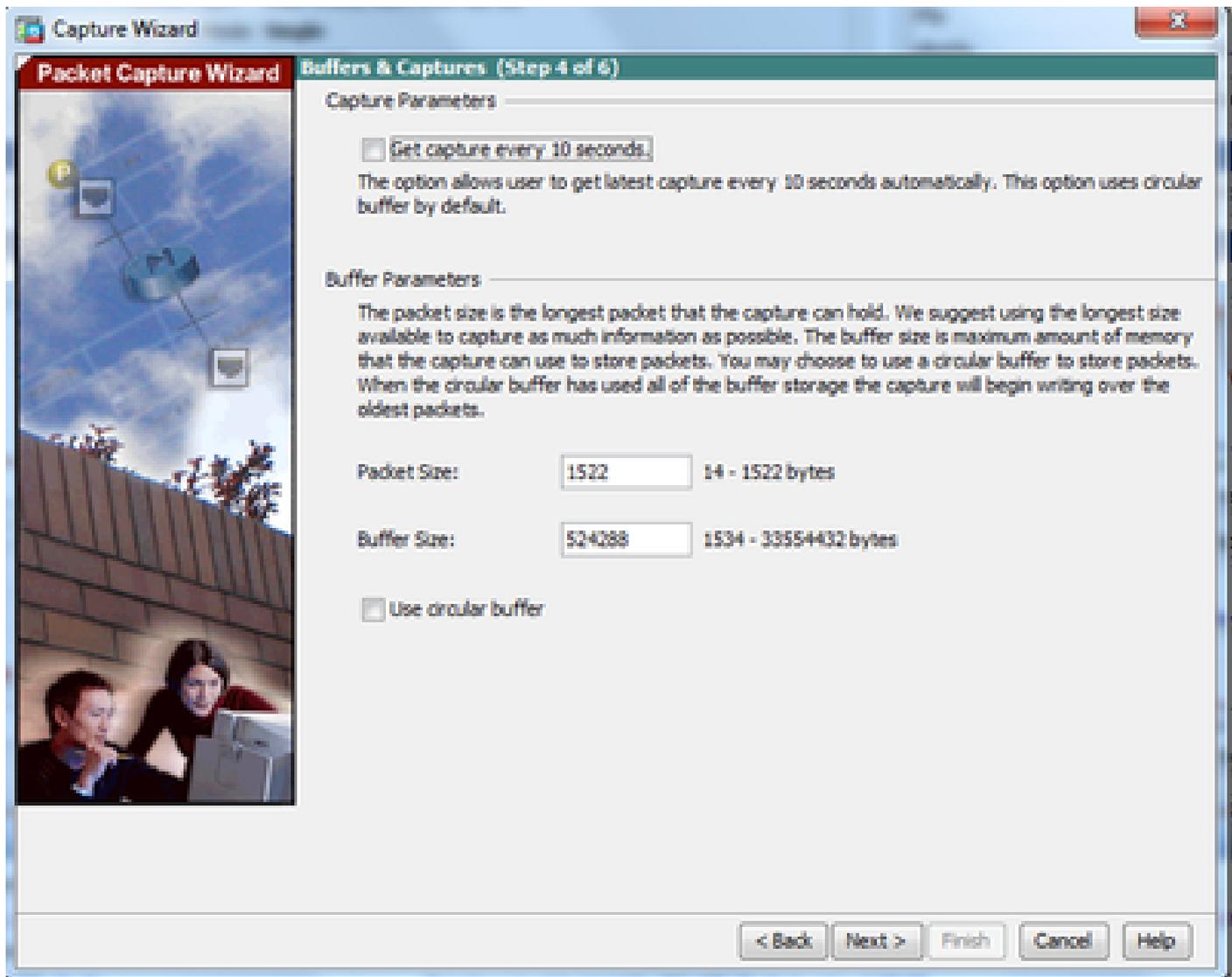
4.2 Nextをクリックします。

5.1表示されたそれぞれの領域に適切なパケットサイズとバッファサイズを入力します。このデータは、キャプチャを実行するために必要です。

5.2 circular bufferオプションを使用するには、Use circular bufferボックスにチェックマークを入れます。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。

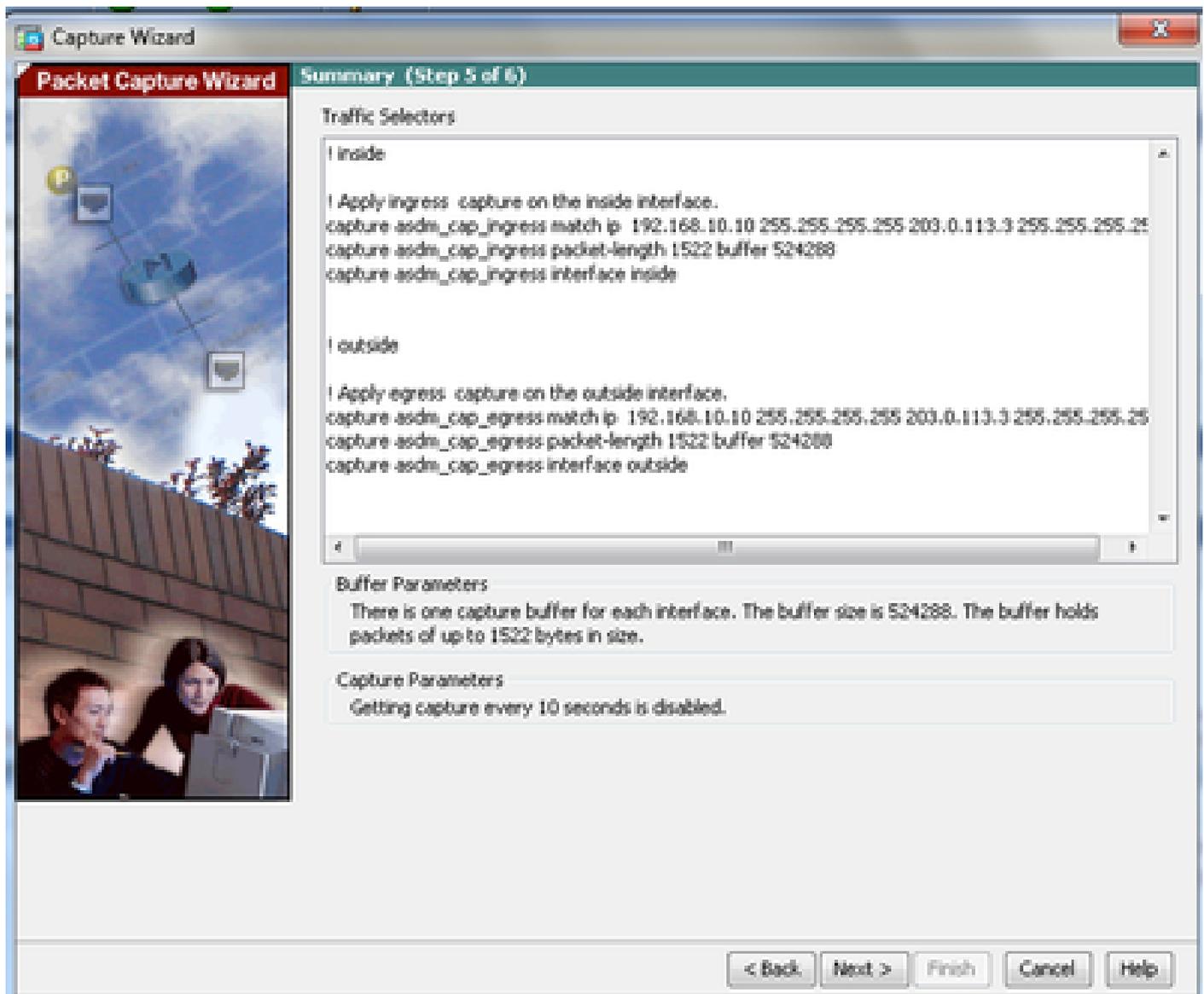
この例では、循環バッファが使用されないため、チェックボックスはオンになりません。



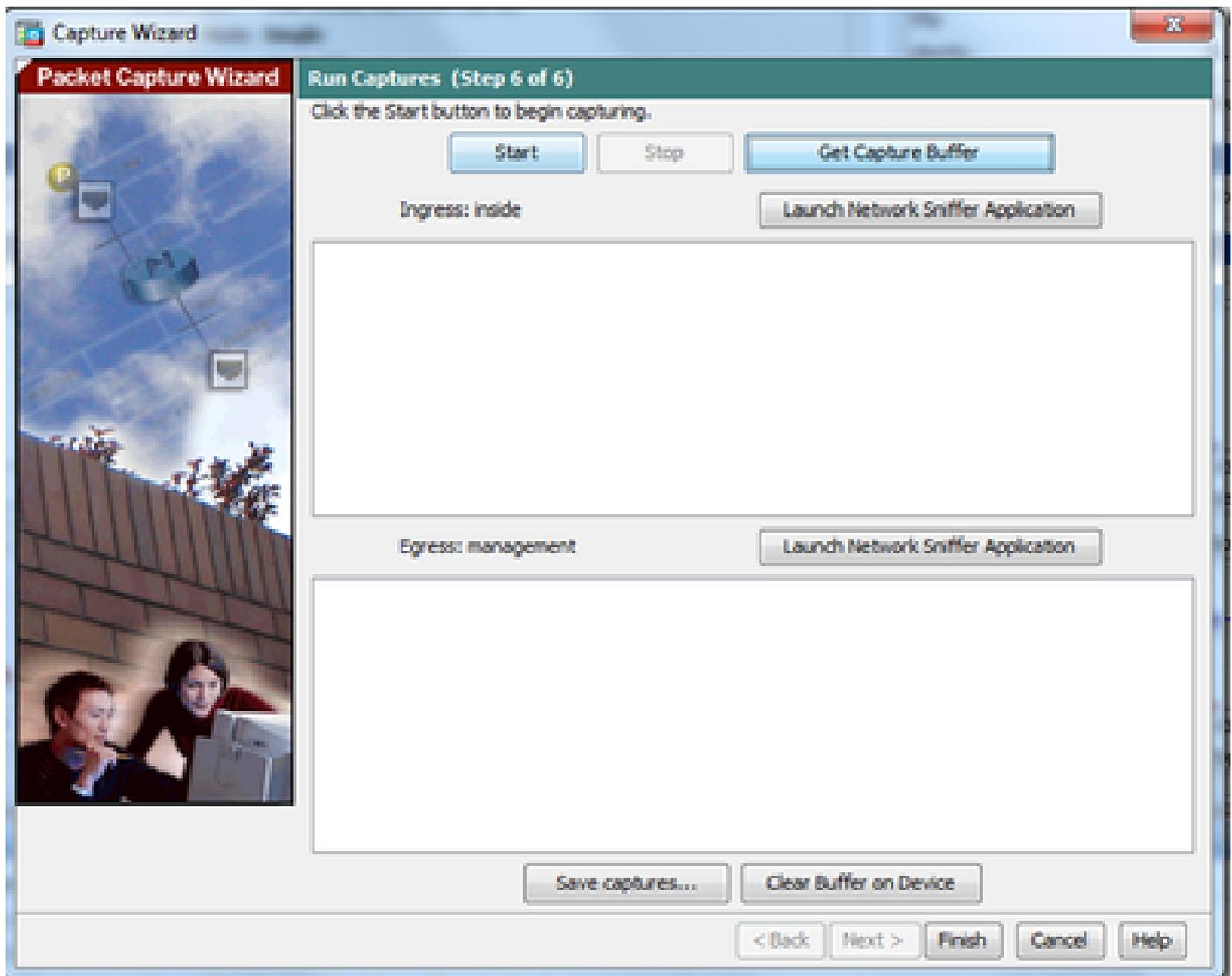
5.3 Nextをクリックします。

6.0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(この例ではIPパケットがキャプチャされます)が表示されます。

6.1 Nextをクリックします。

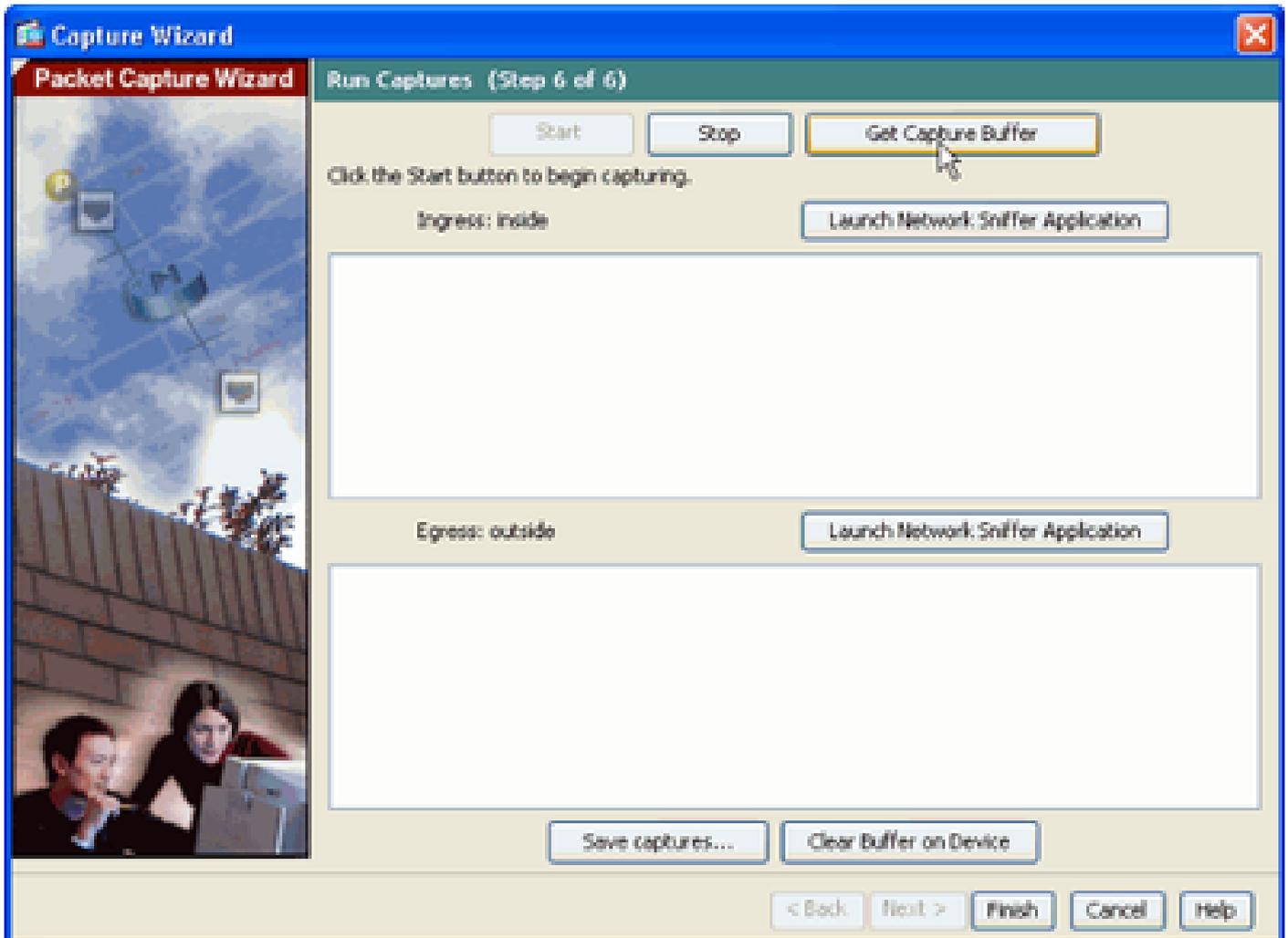


7. 次に示すように、パケットキャプチャを開始するには、Startをクリックします。



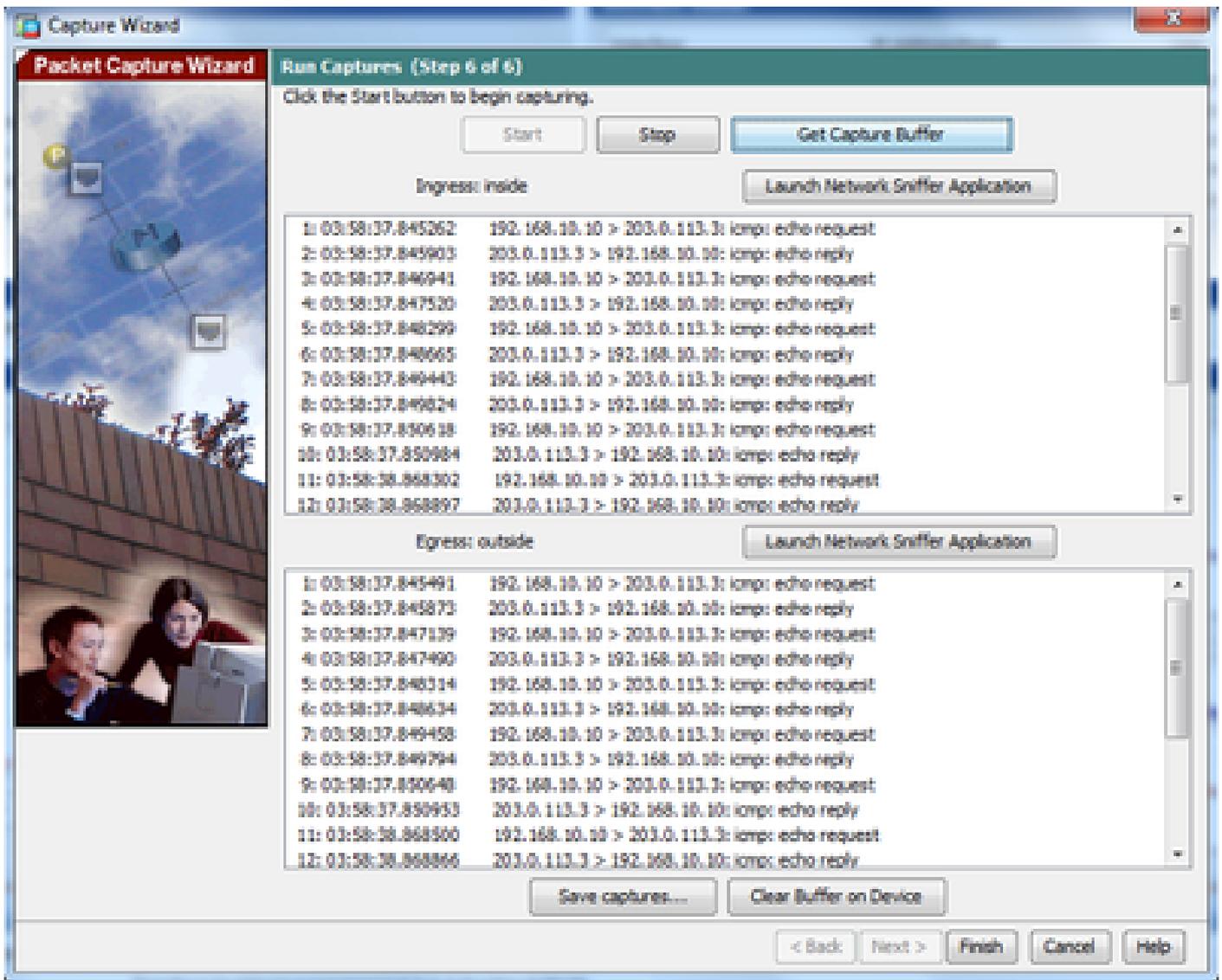
パケットキャプチャが開始されたら、内部ネットワークから外部ネットワークにpingを実行して、送信元と宛先のIPアドレス間を流れるパケットがASAキャプチャバッファによってキャプチャされるようにします。

8. Get Capture Bufferをクリックして、ASAキャプチャバッファによってキャプチャされたパケットを表示します。



入カトラフィックと出カ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。

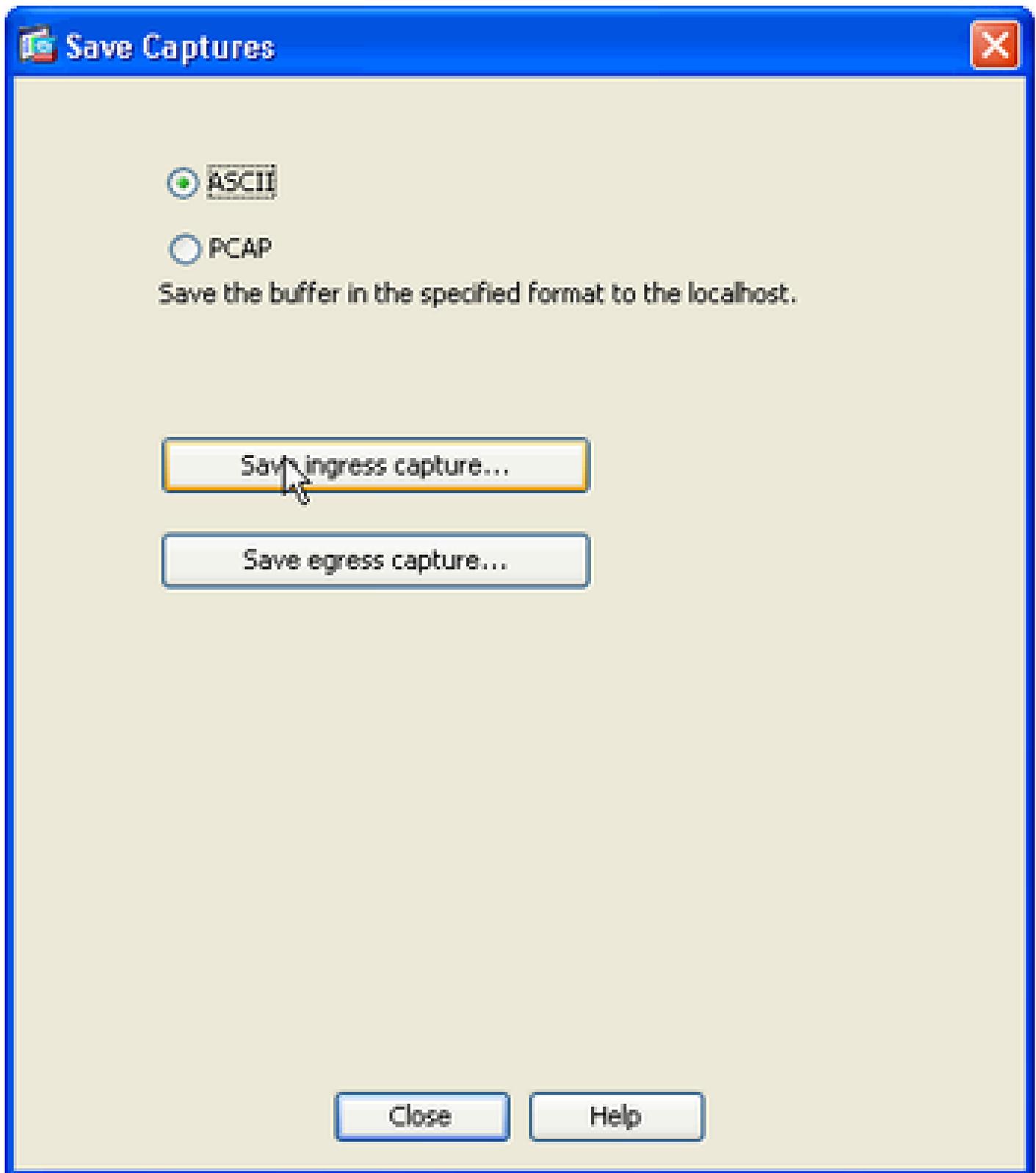
9. Save capturesをクリックして、キャプチャ情報を保存します。



10.1 Save capturesウィンドウで、キャプチャバッファの保存に必要な形式を選択します。これは、[ASCII]と[PCAP]のどちらかです。

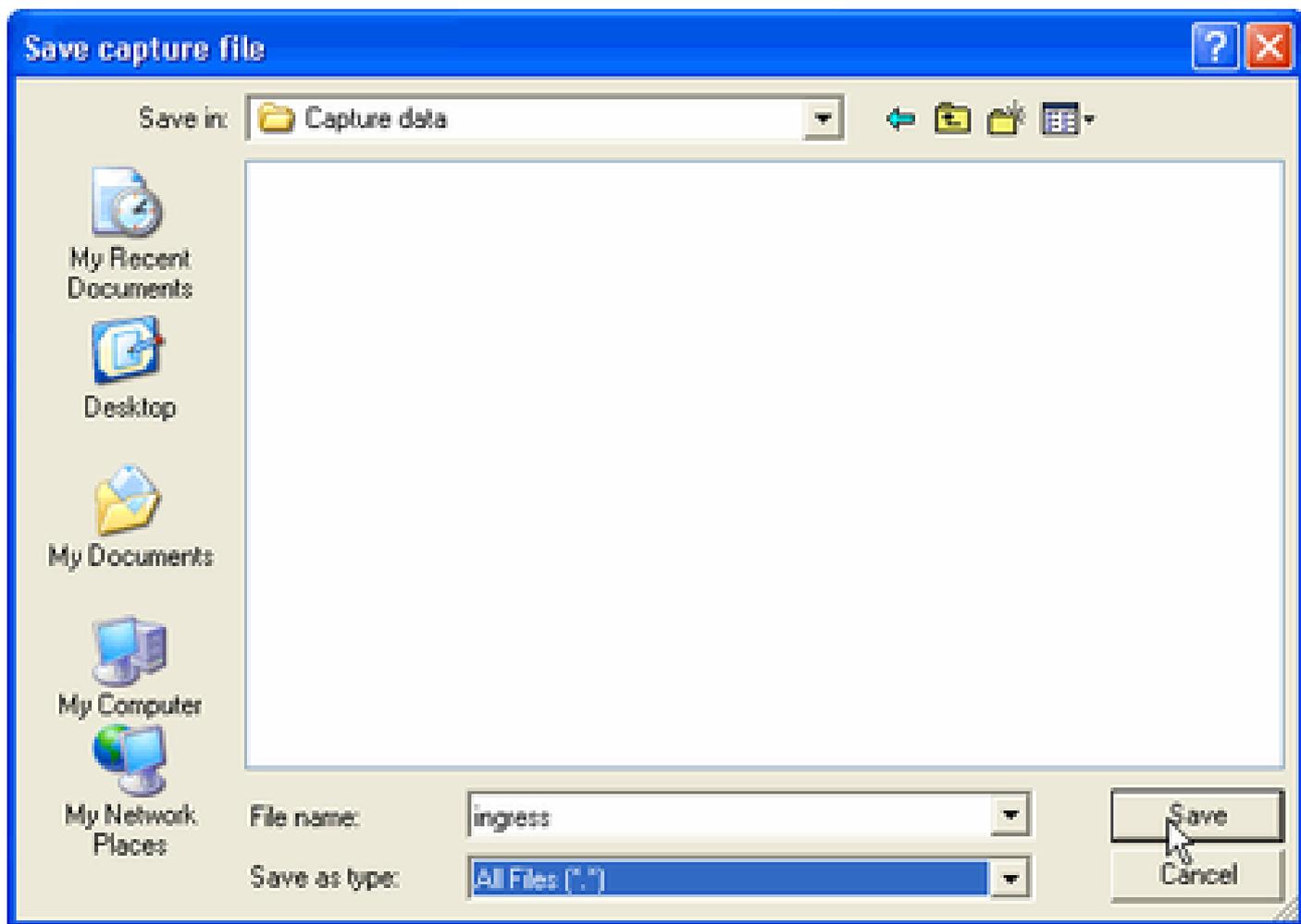
10.2形式名の横にあるオプションボタンをクリックします。

10.3必要に応じて、Save ingress captureまたはSave egress captureをクリックします。この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、推奨される方法です。

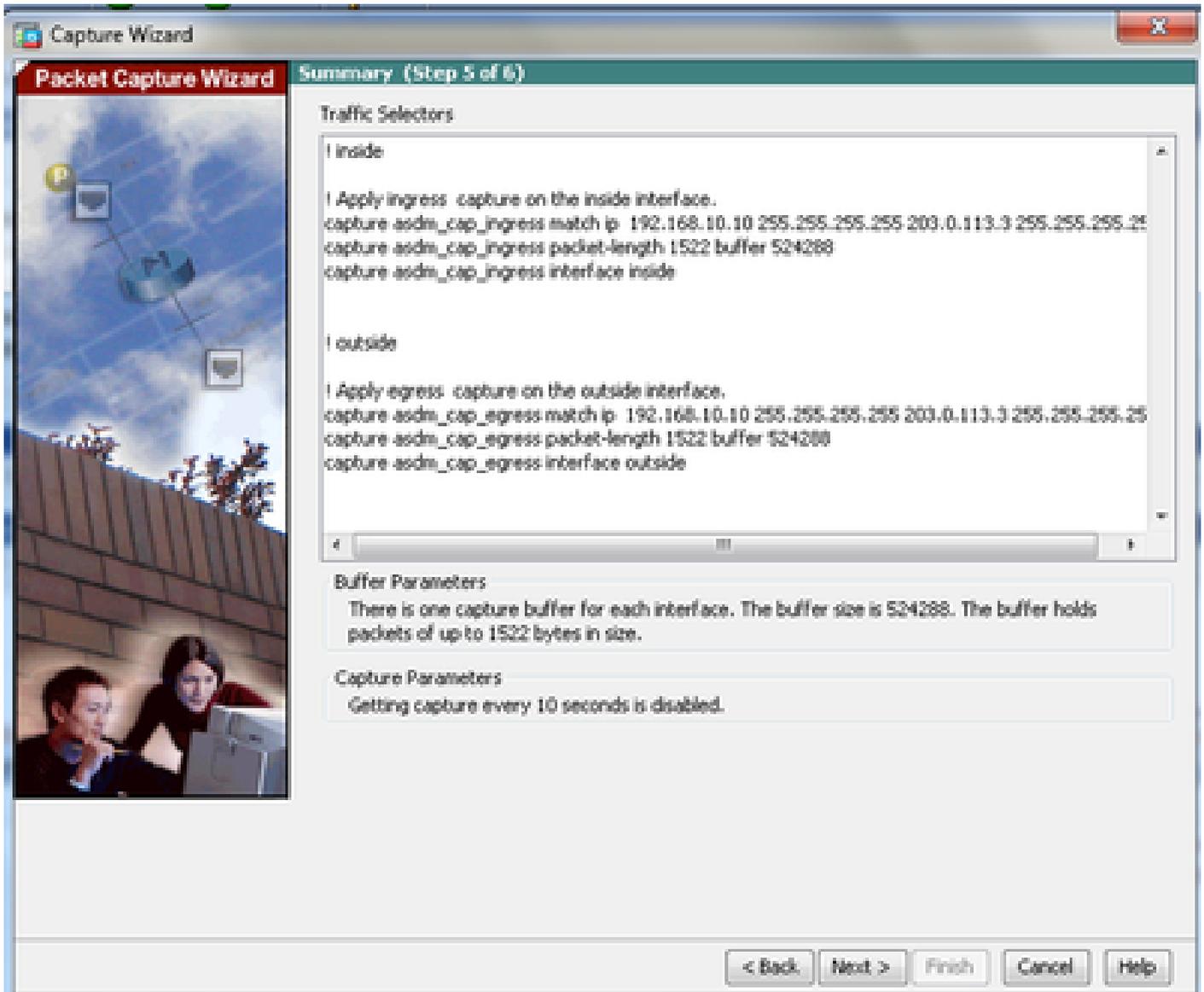


11.1 Save capture fileウィンドウで、ファイル名とキャプチャファイルを保存する場所を指定します。

11.2 Saveをクリックします。



12. Finishをクリックします。



これで、GUIのパケットキャプチャ手順は完了です。

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. ネットワークダイアグラムに示すように、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。

```
<#root>
```

```
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。

```
<#root>
```

```
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。

ランダム データの例は次のとおりです。

```
<#root>
```

```
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。

```
<#root>
```

```
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。

```
<#root>
```

```
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、LACP、PPPOED、PPPOES、RARP、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。

```
<#root>
```

```
ASA#
```

```
cap arp ethernet-type ?
```

```
exec mode commands/options:
 802.1Q
<0-65535> Ethernet type
arp
ip
ip6
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 xx.xx.xx.xxx:
```

- 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。

```
<#root>
```

```
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。

<#root>

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
```

 注:ASA 9.10+では、anyキーワードはipv4アドレスを持つパケットのみをキャプチャします。
。any6キーワードは、すべてのipv6アドレスのトラフィックをキャプチャします。

これらは、パケットキャプチャで設定できる高度な設定です。

設定方法については、コマンドリファレンスガイドを参照してください。

- 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、
Etherchannelを使用してLACPの現在の動作を特定する場合に便利です。
- 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キャプチャを有効にすると、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

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。

```
<#root>
```

```
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。

```
<#root>
```

```
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. 移動先

https://<ip_of_asa>/admin/capture/<capture_name>/pcap

あらゆるブラウザで利用できます

 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。

1. 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。

```
copy /pcap capture:<capture-name> tftp://<server-ip-address>
```

 ヒント: パケットキャプチャを使用して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。

```
<#root>
```

```
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。

```
<#root>
```

```
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>
```

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。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。