

ASA/PIX/FWSM: Packet Capturing using CLI and ASDM Configuration Example

Document ID: 110117

Introduction

Prerequisites

- Requirements
- Components Used
- Related Products
- Conventions

Background Information

Configure

- Network Diagram
- Configure Packet Capture using ASDM
- Step-By-Step Procedure to Configure Packet Capture in ASA/PIX using CLI
- Viewing the Captured Packets on ASA

Related Information

Introduction

This document describes how to configure the Cisco 5500 Series Adaptive Security Appliance (ASA) to capture the desired packets using the Adaptive Security Device Manager (ASDM) or CLI. The ASDM delivers world-class security management and monitoring through an intuitive, easy-to-use Web-based management interface.

Prerequisites

Requirements

This document assumes that the ASA is fully operational and configured to allow the Cisco ASDM or CLI to make configuration changes.

Note: Refer to [Allowing HTTPS Access for ASDM or PIX/ASA 7.x: SSH on the Inside and Outside Interface Configuration Example](#) to allow the device to be remotely configured by the ASDM or Secure Shell (SSH).

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Adaptive Security Appliance Software Version 7.x and later
- Adaptive Security Device Manager Version 6.x and later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Related Products

This configuration can also be used with these Cisco products:

- Cisco PIX Security Appliance Version 6.2(1) and later
- Firewall Services Module (FWSM) Version 2.2(1) and later

Note: Packet Capture can be configured on FWSM only using CLI as this feature is not supported in ASDM (the Capture command is not supported in ASDM). Refer to the **Ignored and View-Only Commands** section for more information.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

Capturing packets is useful when you troubleshoot connectivity problems or monitor suspicious activity. You can create multiple captures. In order to enable packet capture capabilities for packet sniffing and network fault isolation, use the **capture** command in privileged EXEC mode. In order to disable packet capture capabilities, use the **no form** of this command. In order to view the packet capture, use the **show capture** name command. In order to save the capture to a file, use the **copy capture** command.

In ASA/PIX use the **https://security appliance-ip-address/admin/capture/capture_name[/pcap]** command to see the packet capture information with a web browser. If you specify the **pcap** optional keyword, then a **libpcap-format** file is downloaded to the web browser and can be saved using the web browser. If you copy the buffer contents to a TFTP server in ASCII format, you will see only the headers, not the details and hexadecimal dump of the packets. In order to see the details and hexadecimal dump, you need to transfer the buffer in PCAP format and read it with **TCPDUMP** or **Ethereal**.

In FWSM versions before 3.1(7) and 3.2(2), use the **https://fwsm-ip-address/capture/capture_name[/pcap]** command to see the packet capture information with a web browser.

In FWSM versions after 3.1(7) and 3.2(2), use the **https://fwsm-ip-address/capture/context_name/capture_name[/pcap]** command to see the packet capture information with a web browser.

For example, the capture contents for a capture named `captest` can be viewed using a web browser at the following location, depending on firewall mode and version as shown here:

Before version 3.1(7) and 3.2(2):

```
https://fwsm-ip-address/capture/captest
```

After version 3.1(7) or 3.2(2) and in single context mode:

```
https://fwsm-ip-address/capture/single_vf/captest
```

After version 3.1(7) or 3.2(2) and in multiple context mode:

```
https://fwsm-ip-address/capture/context_name/captest
```

Note: Enabling WebVPN capture affects the performance of the security appliance. Make sure to disable the

capture after you generate the capture files that you need for troubleshooting.

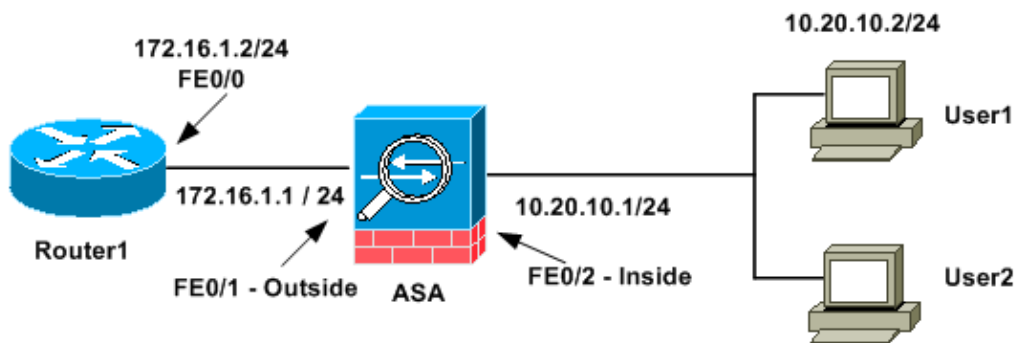
Configure

In this section, you are presented with the information to configure the packet capture feature described in this document.

Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:

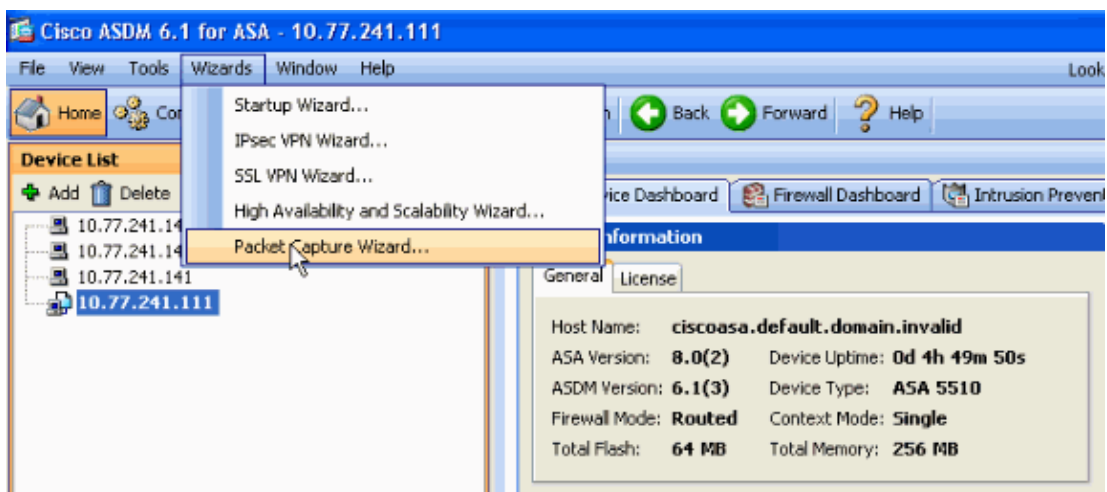


Note: The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 addresses which were used in a lab environment.

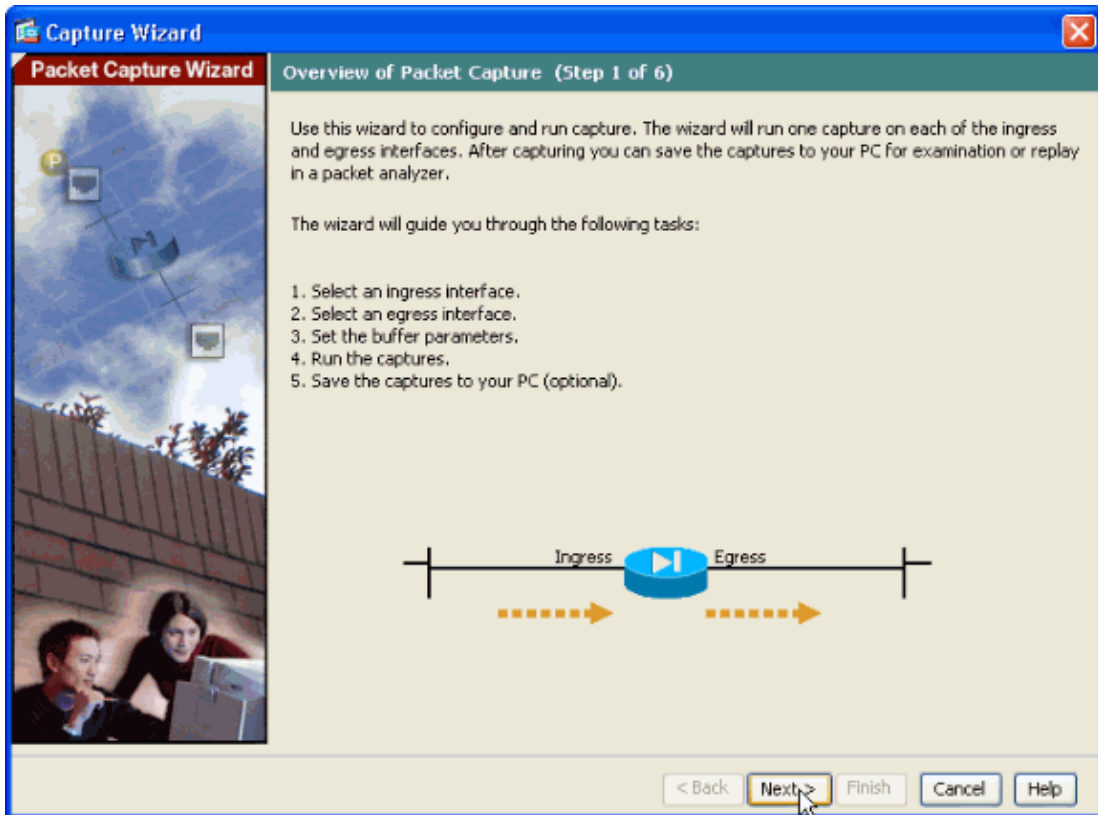
Configure Packet Capture using ASDM

Complete these steps in order to configure the Packet Capturing feature in ASA. For example, the configuration done here is to capture the packets transmitted during a ping from User1 (Inside network) to Router1 (Outside network):

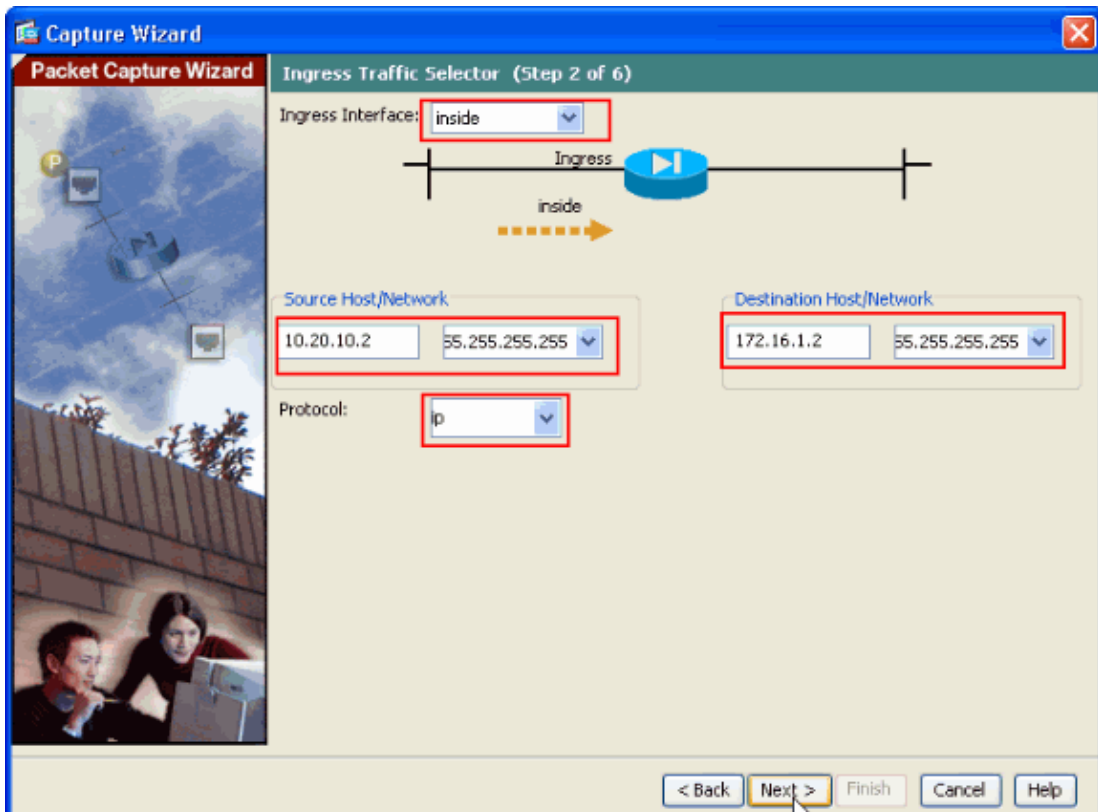
1. Choose **Wizards > Packet Capture Wizard** in order to start the packet capture configuration, as shown:



2. The capture wizard opens. Click **Next** as shown here:

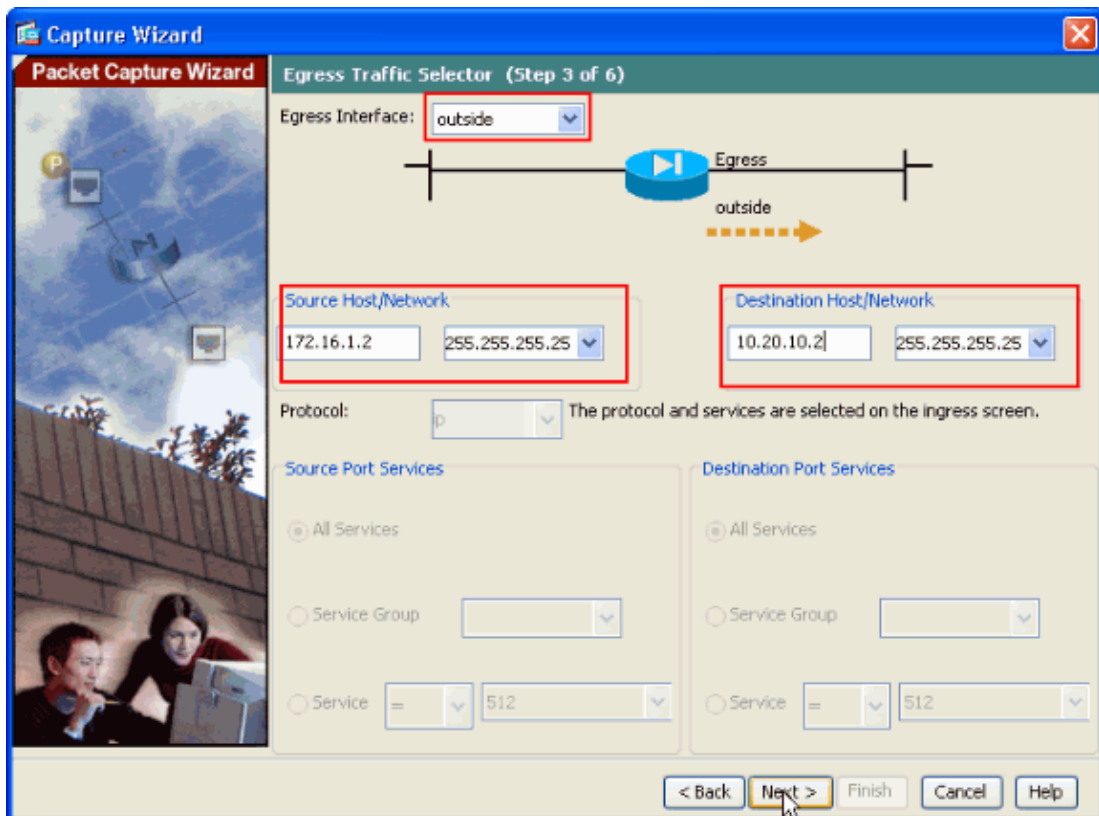


3. In the new window provide the parameters to capture the **INGRESS** traffic. Choose the **Ingress interface** as **Inside** and provide the source and the destination IP address of the packets to be captured with their subnetmask in the respective space provided. Also, choose the packet type to be captured by ASA (IP is the packet type chosen here), as shown:



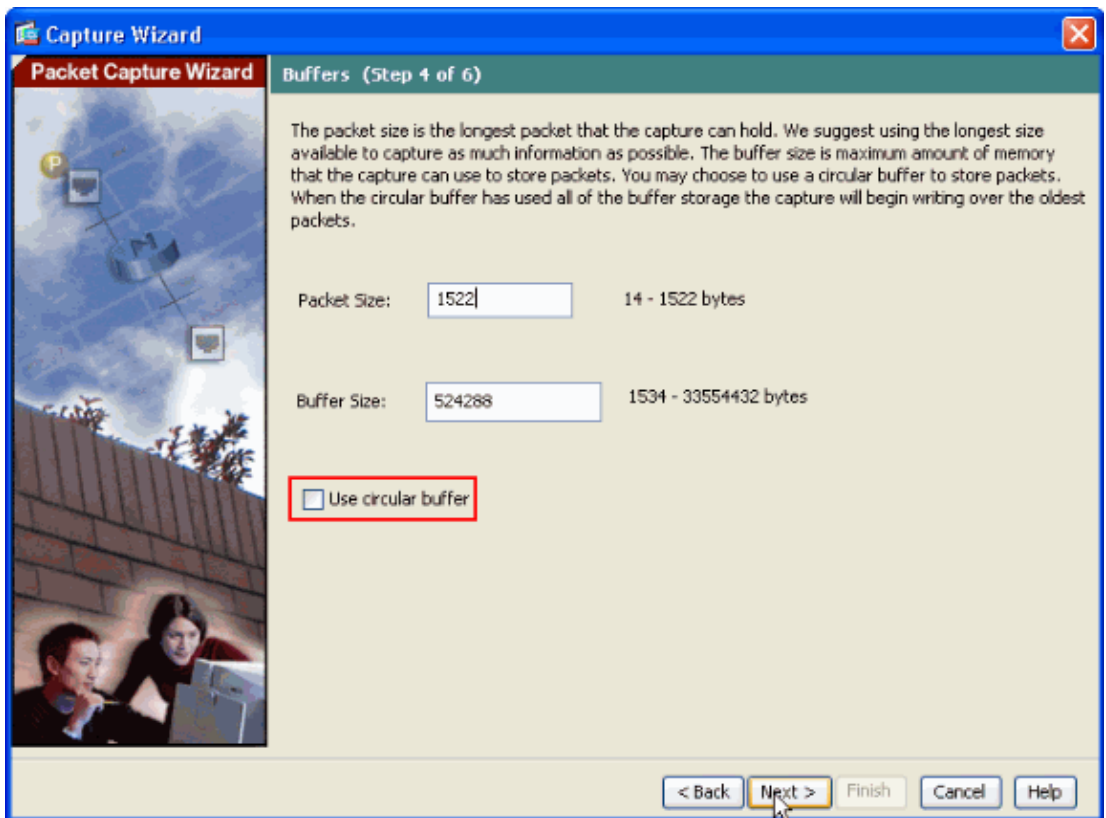
Click **Next**.

4. Choose the **Egress interface** as **Outside** and provide the source and the destination IP address with their subnetmask in the respective spaces provided as shown:



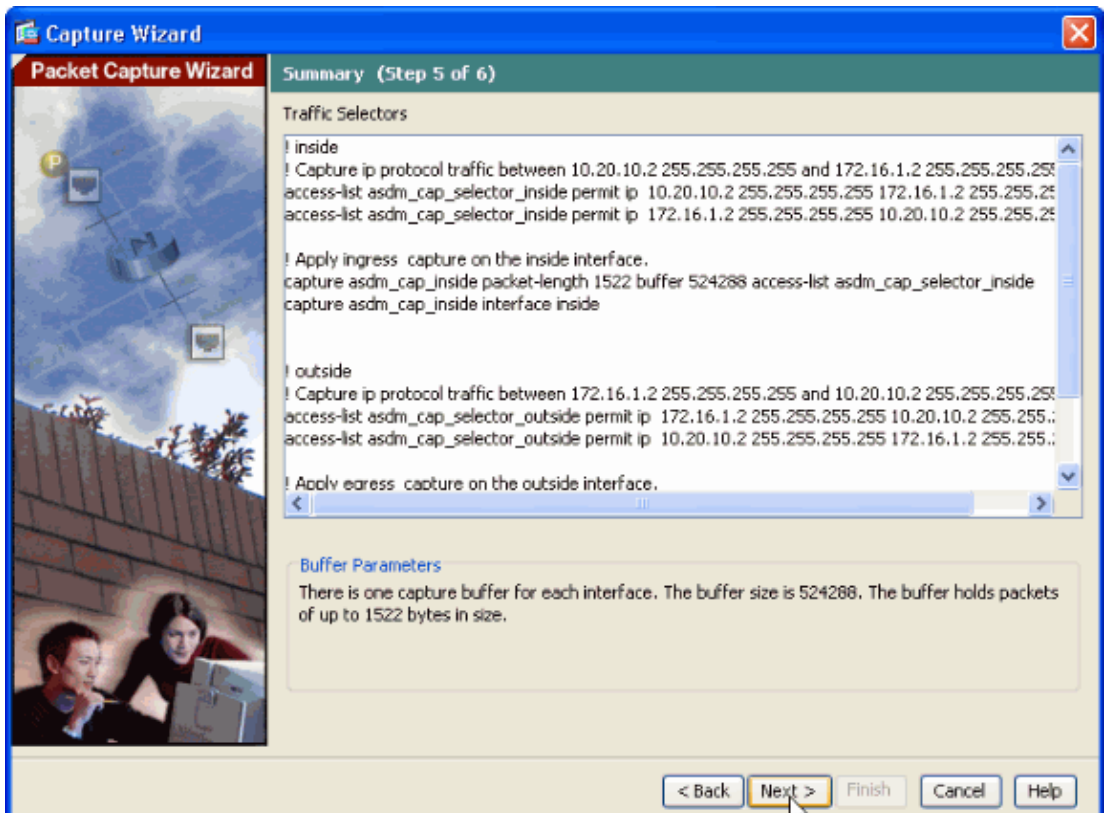
Click **Next**.

5. Provide the **Packet size** and the **Capture buffer size** in the respective space provided as these data are required for the capture to take place. Also, remember to check the **Use circular buffer** check box if you want to use the circular buffer option. In this example, circular buffer is not used so the check box is not checked.

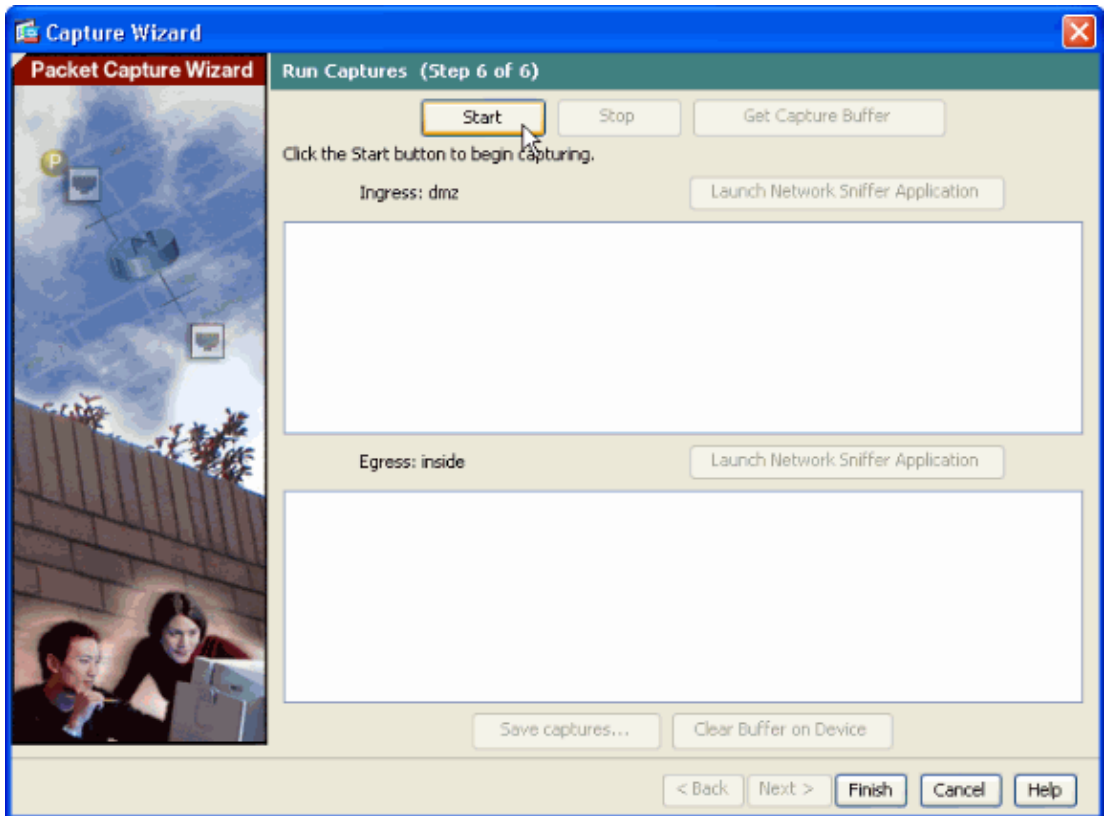


Click **Next**.

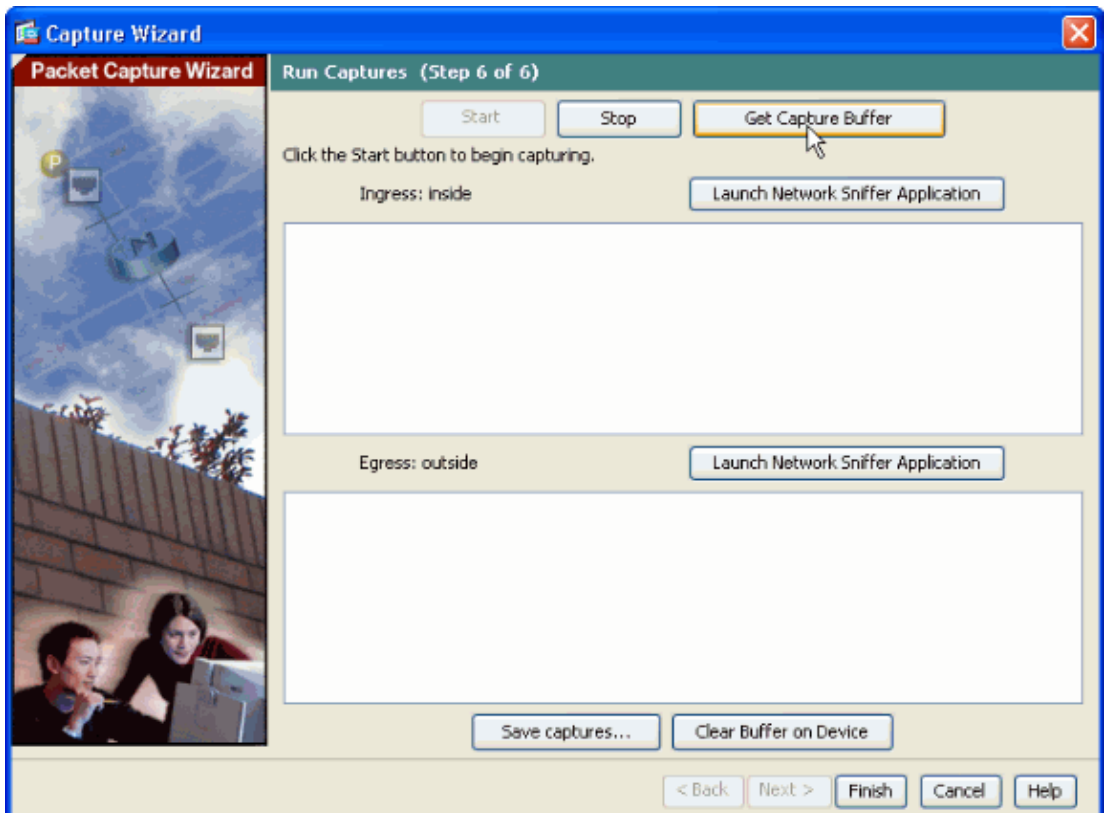
- This window shows the **Access-lists** to be configured on the ASA for the the ASA to capture the desired packets and shows the type of packet (IP packets are captured in this example). Click **Next**.



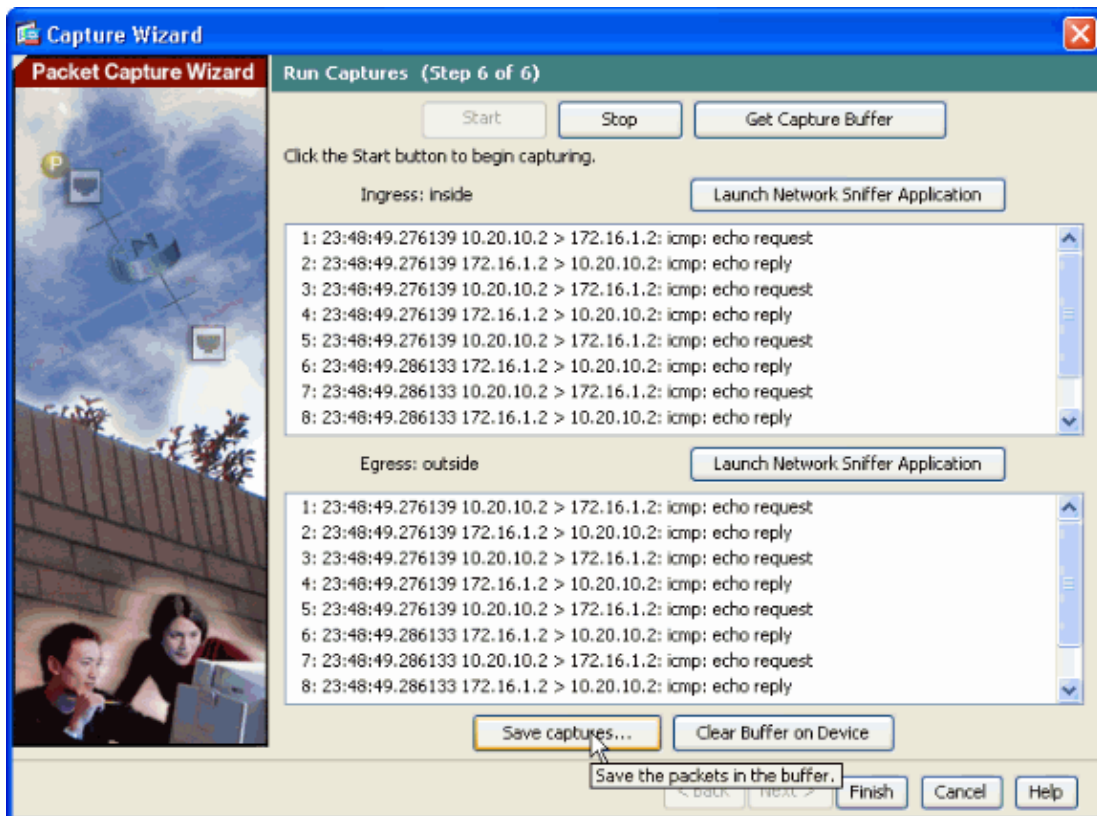
- Click **Start** to start the Packet capture as shown here:



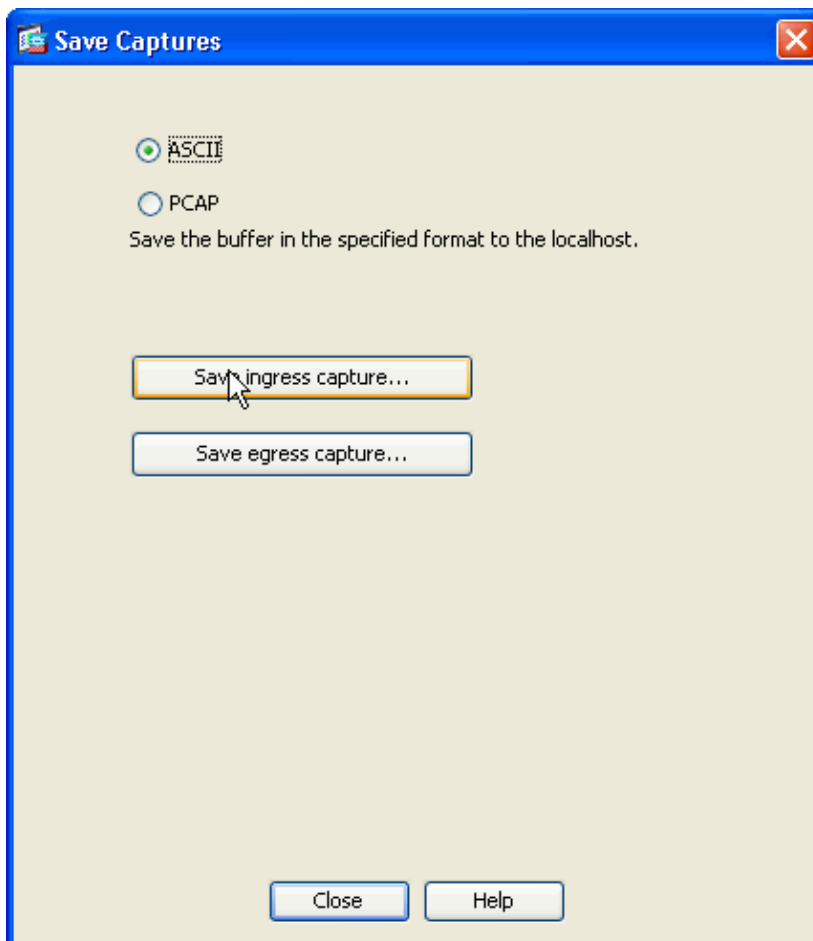
8. As the Packet capture has been started, try to ping the Outside network from the Inside network so that the packets flowing between the source and the destination are captured by the ASA Capture buffer.
9. Click **Get Capture Buffer** in order to view the packets captured by the ASA capture buffer.



10. The captured packets are shown in this window for both **Ingress** and **Egress** traffic. Click **Save captures** in order to save the capture information as shown:

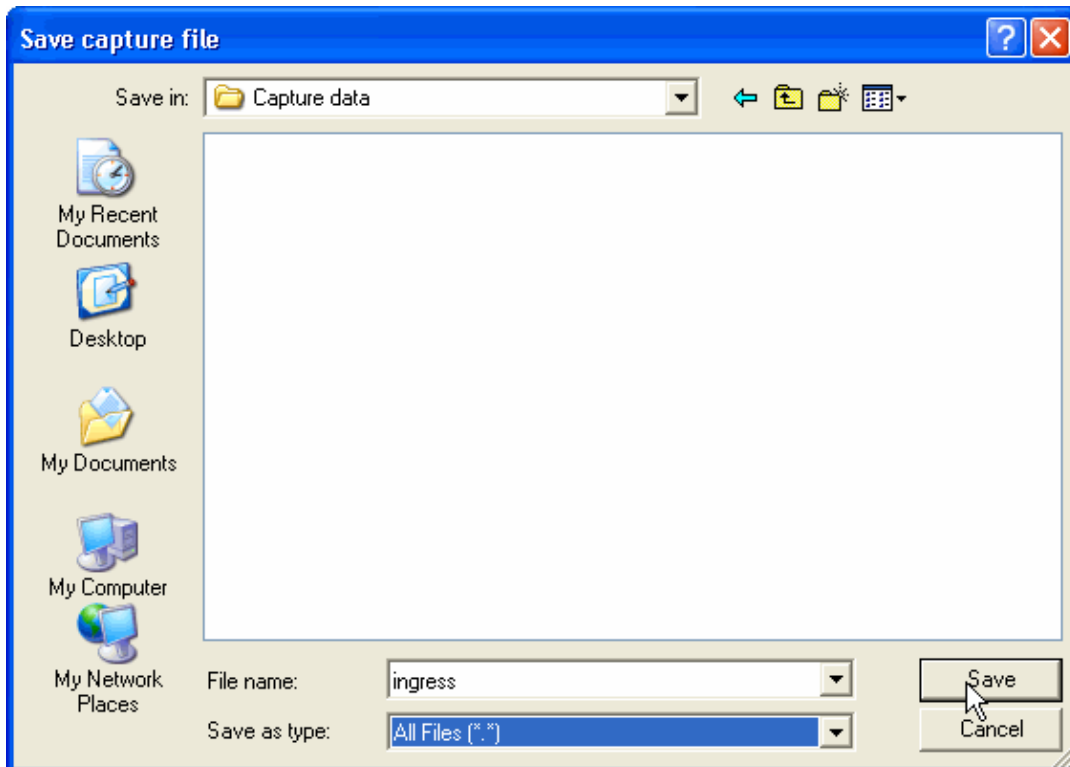


- In the Save Captures window choose the required format in which the capture buffer is to be saved. This is either **ASCII** or **PCAP**. Click the radio button next to the format names. Then, click **Save ingress capture** or **Save egress capture** as required.

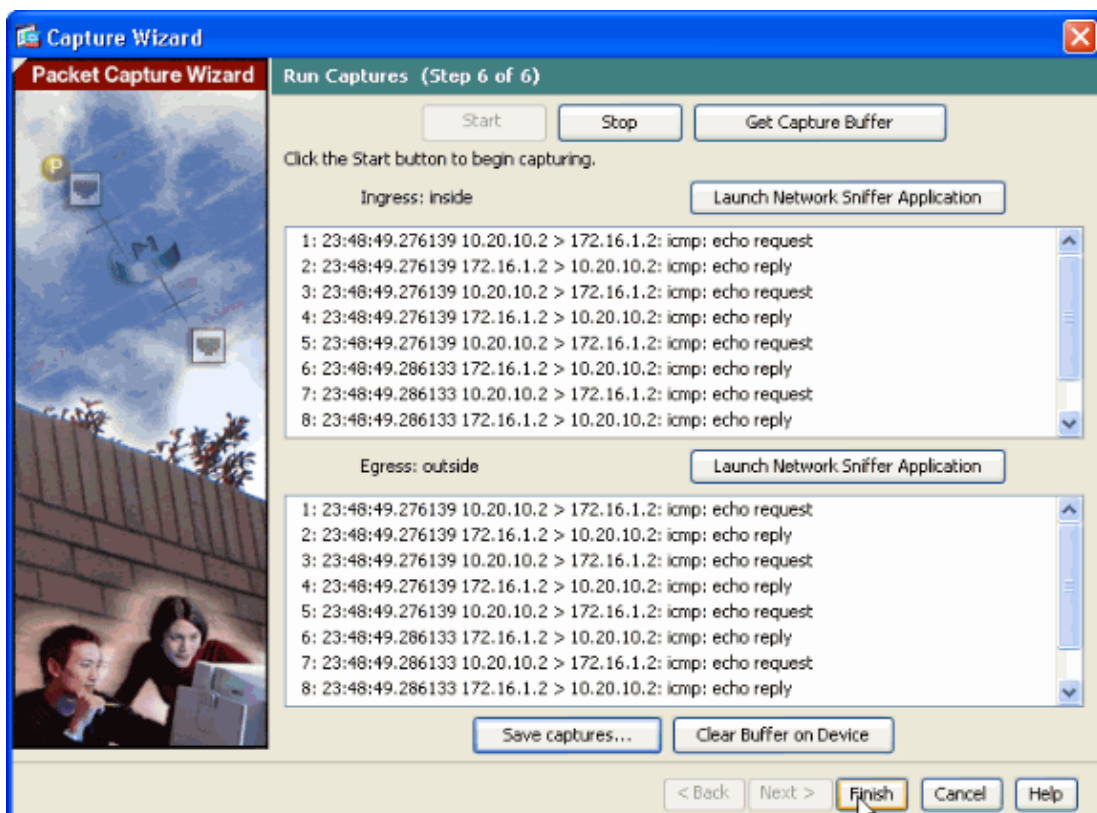


If you specify the **pcap** format, then you can open the file using **TCPDUMP** or **Ethereal**. The capture file in **ASCII** format can be viewed using the web browser.

12. In the Save capture file window provide the file name and the location where the capture file is to be saved, then click **Save** as shown:



13. Click **Finish**.



This completes the packet capture procedure.

Step-By-Step Procedure to Configure Packet Capture in ASA/PIX using CLI

Complete these steps in order to configure Packet capture in ASA/PIX using CLI:

1. Configure the Inside and Outside interfaces as shown in the network diagram with IP address and Security-levels.
2. Configure the access-lists **asdm_cap_selector_inside** and **asdm_cap_selector_outside** for capturing the packets that travel from the inside network to the outside network and outside network to inside network .

```
access-list asdm_cap_selector_inside extended permit ip host 10.20.10.2 host 172.16.1.2
access-list asdm_cap_selector_inside extended permit ip host 172.16.1.2 host 10.20.10.2
access-list asdm_cap_selector_outside extended permit ip host 172.16.1.2 host 10.20.10.2
access-list asdm_cap_selector_outside extended permit ip host 10.20.10.2 host 172.16.1.2
```

3. Start the packet capture process using the **capture** command in privileged EXEC mode. The **capture** command should be used after the access-lists have been configured as shown in the ASA configuration. In this configuration example, the capture named **capin** is defined. Bind it to the **inside** interface, and specify to only capture packets that match the access-list **asdm_cap_selector_inside** as shown here:

```
ASA#capture capin interface inside access-list asdm_cap_selector_inside
```

Similarly, the capture named **capout** is defined. Bind it to the **outside** interface, and specify to only capture packets that match the access-list **asdm_cap_selector_outside** as shown here:

```
ASA#capture capout interface outside access-list asdm_cap_selector_outside
```

The ASA will now start capturing the traffic flow between the interfaces. In order to stop the capture at anytime, use the **no capture** command followed by the capture name.

Viewing the Captured Packets on ASA

Viewing the Captured packets on the ASA Device

In order to view the captured packets, use the **show capture** command followed by the capture name. These are the **show** command outputs of the capture buffer contents:

The **show capture capin** command shows the contents of the capture buffer named **capin**.

```
ASA#show capture capin
20 packets captured
 1: 01:49:24.087474 10.20.10.2 > 172.16.1.2: icmp: echo request
 2: 01:49:24.087474 172.16.1.2 > 10.20.10.2: icmp: echo reply
 3: 01:49:24.087474 10.20.10.2 > 172.16.1.2: icmp: echo request
 4: 01:49:24.087474 172.16.1.2 > 10.20.10.2: icmp: echo reply
 5: 01:49:24.087474 10.20.10.2 > 172.16.1.2: icmp: echo request
 6: 01:49:24.087474 172.16.1.2 > 10.20.10.2: icmp: echo reply
 7: 01:49:24.087474 10.20.10.2 > 172.16.1.2: icmp: echo request
 8: 01:49:24.087474 172.16.1.2 > 10.20.10.2: icmp: echo reply
 9: 01:49:24.087474 10.20.10.2 > 172.16.1.2: icmp: echo request
10: 01:49:24.087474 172.16.1.2 > 10.20.10.2: icmp: echo reply
11: 01:49:26.247042 172.16.1.2 > 10.20.10.2: icmp: echo request
12: 01:49:26.247042 10.20.10.2 > 172.16.1.2: icmp: echo reply
13: 01:49:26.247042 172.16.1.2 > 10.20.10.2: icmp: echo request
```

```
14: 01:49:26.247042 10.20.10.2 > 172.16.1.2: icmp: echo reply
15: 01:49:26.257051 172.16.1.2 > 10.20.10.2: icmp: echo request
16: 01:49:26.257051 10.20.10.2 > 172.16.1.2: icmp: echo reply
17: 01:49:26.257051 172.16.1.2 > 10.20.10.2: icmp: echo request
18: 01:49:26.257051 10.20.10.2 > 172.16.1.2: icmp: echo reply
19: 01:49:26.257051 172.16.1.2 > 10.20.10.2: icmp: echo request
20: 01:49:26.257051 10.20.10.2 > 172.16.1.2: icmp: echo reply
```

20 packets shown

ASA#

The **show capture capout** command shows the contents of the capture buffer named **capout**.

ASA#**show capture capout**

20 packets captured

```
1: 01:49:24.087474 10.20.10.2 > 172.16.1.2: icmp: echo request
2: 01:49:24.087474 172.16.1.2 > 10.20.10.2: icmp: echo reply
3: 01:49:24.087474 10.20.10.2 > 172.16.1.2: icmp: echo request
4: 01:49:24.087474 172.16.1.2 > 10.20.10.2: icmp: echo reply
5: 01:49:24.087474 10.20.10.2 > 172.16.1.2: icmp: echo request
6: 01:49:24.087474 172.16.1.2 > 10.20.10.2: icmp: echo reply
7: 01:49:24.087474 10.20.10.2 > 172.16.1.2: icmp: echo request
8: 01:49:24.087474 172.16.1.2 > 10.20.10.2: icmp: echo reply
9: 01:49:24.087474 10.20.10.2 > 172.16.1.2: icmp: echo request
10: 01:49:24.087474 172.16.1.2 > 10.20.10.2: icmp: echo reply
11: 01:49:26.247042 172.16.1.2 > 10.20.10.2: icmp: echo request
12: 01:49:26.247042 10.20.10.2 > 172.16.1.2: icmp: echo reply
13: 01:49:26.247042 172.16.1.2 > 10.20.10.2: icmp: echo request
14: 01:49:26.247042 10.20.10.2 > 172.16.1.2: icmp: echo reply
15: 01:49:26.257051 172.16.1.2 > 10.20.10.2: icmp: echo request
16: 01:49:26.257051 10.20.10.2 > 172.16.1.2: icmp: echo reply
17: 01:49:26.257051 172.16.1.2 > 10.20.10.2: icmp: echo request
18: 01:49:26.257051 10.20.10.2 > 172.16.1.2: icmp: echo reply
19: 01:49:26.257051 172.16.1.2 > 10.20.10.2: icmp: echo request
20: 01:49:26.257051 10.20.10.2 > 172.16.1.2: icmp: echo reply
```

20 packets shown

ASA#

Related Information

- [Cisco ASA 5500 Series Adaptive Security Appliances Support Page](#)
- [Cisco ASA 5500 Series Adaptive Security Appliances Command References](#)
- [Cisco PIX 500 Series Security Appliances Support Page](#)
- [Cisco PIX 500 Series Security Appliances Command Reference](#)
- [Cisco Adaptive Security Device Manager](#)
- [Cisco Catalyst 6500 Series Firewall Services Module Support Page](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Mar 23, 2009

Document ID: 110117
