ASA/PIX/FWSM：使用 CLI 和 ASDM 进行数据包捕获的配置示例

内容

前言

本文档说明如何使用自适应安全设备管理器 (ASDM) 或 CLI 配置 Cisco 5500 系列自适应安全设备 (ASA) 以捕获所需的数据包。ASDM 通过一个直观且易于使用的基于 Web 的管理界面提供一流的安全管理和监控。

前提条件

需求

本文档假设 ASA 处于完全运行状态，并配置为允许 Cisco ASDM 或 CLI 进行配置更改。

注意： 请参阅允许对 ASDM 进行 HTTPS 访问或 PIX/ASA 7.x：内部和外部接口上的 SSH 配置示例以允许通过 ASDM 或Secure Shell (SSH) 远程对设备进行配置。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco 自适应安全设备软件版本 7.x 及更高版本
- 自适应安全设备管理器版本 6.x 及更高版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

相关产品

此配置也可用于以下 Cisco 产品：

- Cisco PIX 安全设备版本 6.2 (1) 及更高版本
- 防火墙服务模块 (FWSM) 版本 2.2 (1) 及更高版本

注意： 在 FWSM 上只能使用 CLI 配置数据包捕获，因为此功能在 ASDM 中不受支持（ASDM 中不支持捕获命令）。有关详细信息，请参阅忽略的和仅限查看的命令。

惯例

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

在排除连接问题或监视可疑活动时，捕获数据包非常有用。您可以创建多个捕获。要针对数据包嗅探和网络故障隔离启用数据包捕获功能，请在特权 EXEC 模式下使用 capture 命令。要禁用数据包捕获功能，请使用此命令的 no 形式。要查看数据包捕获，请使用 show capture name 命令。要将捕获保存到文件，请使用 copy capture 命令。

在 ASA/PIX 中，请使用 https://security appliance-ip-address/admin/capture/capture_name[/pcap] 命令在 Web 浏览器中查看数据包捕获信息。如果指定 pcap 可选关键字，则会将一个 libpcap 格式的文件下载到 Web 浏览器中，并可使用 Web 浏览器保存该文件。如果将缓冲区内容以 ASCII 格式复制到 TFTP 服务器中，则只能看到报头，而看不到数据包的详细信息和十六进制转储。要查看详细信息和十六进制转储，需要将缓冲区转换为 PCAP 格式并使用 TCPDUMP 或 Ethereal 读取它。

在 3.1(7) 和 3.2(2) 以前的 FWSM 版本中，请使用 https://fwsm-ip-address/capture/capture_name[/pcap] 命令在 Web 浏览器中查看数据包捕获信息。

在 3.1(7) 和 3.2(2) 以后的 FWSM 版本中，请使用 https://fwsm-ip-address/capture/context_name/capture_name[/pcap] 命令在 Web 浏览器中查看数据包捕获信息。

例如，可使用 Web 浏览器在以下位置查看名为 captest 的捕获的捕获内容，具体位置取决于如下所示的防火墙模式和版本：

版本 3.1(7) 和 3.2(2) 以前：

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

版本 3.1(7) 或 3.2(2) 以后并且在单上下文模式下：

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

版本 3.1(7) 或 3.2(2) 以后并且在多上下文模式下：

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

注意： 启用 WebVPN 捕获会影响安全设备的性能。请确保在生成您进行故障排除所需的捕获文件后禁用捕获。

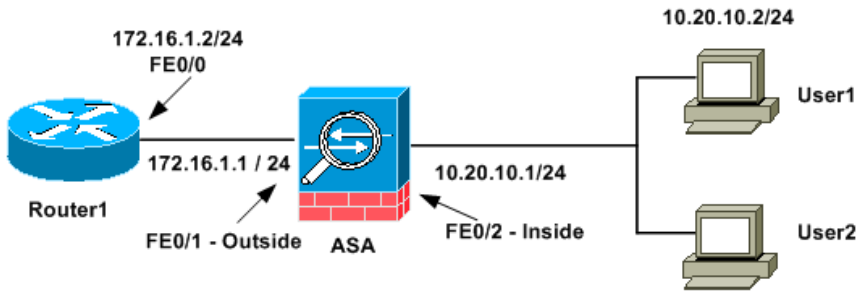
配置

此部分中将显示用于配置本文档中所述的数据包捕获功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：

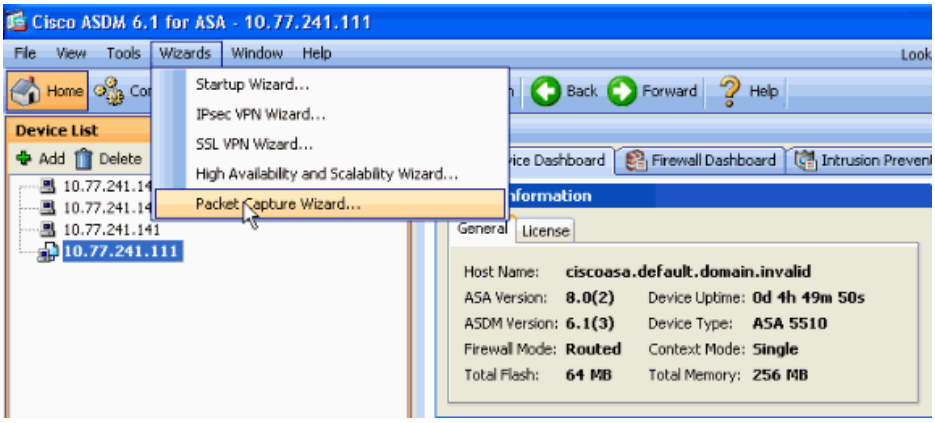


注意： 此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

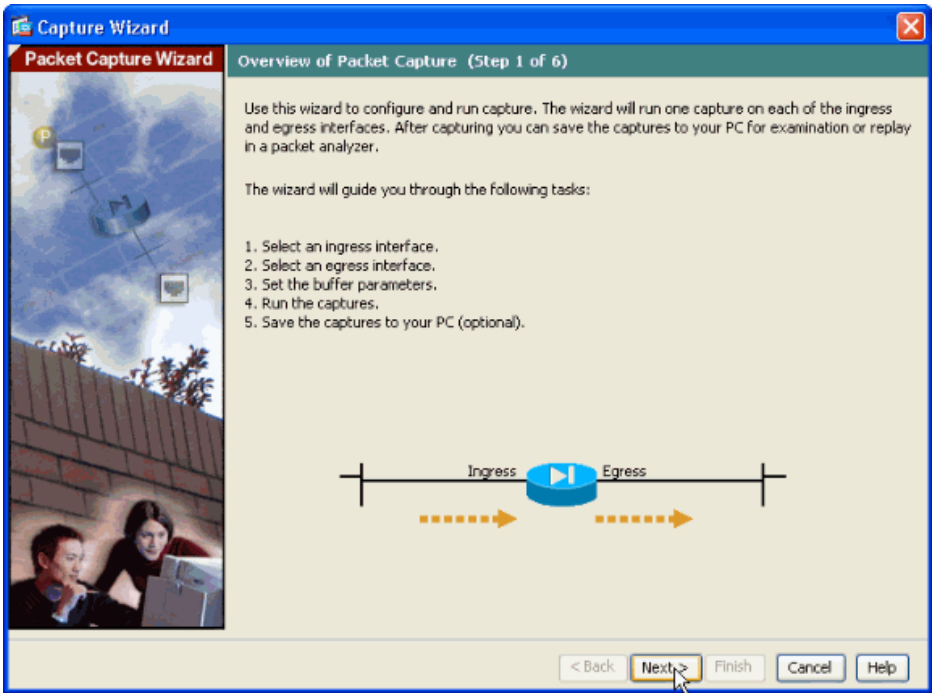
使用 ASDM 配置数据包捕获

要在 ASA 中配置数据包捕获功能，请完成以下步骤：例如，此处执行的配置是要捕获那些在执行从 User1（内部网络）到 Router1（外部网络）的 ping 操作期间传输的数据包：

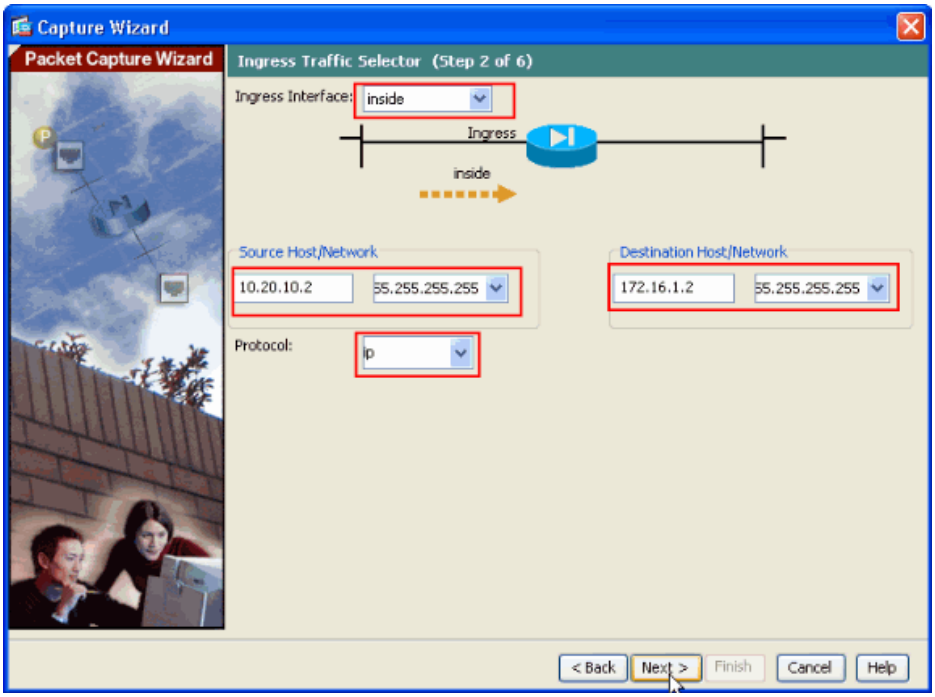
1. 选择 Wizards > Packet Capture Wizard 以开始数据包捕获配置，如下所示：



2. 将打开捕获向导。如下所示，单击 Next：

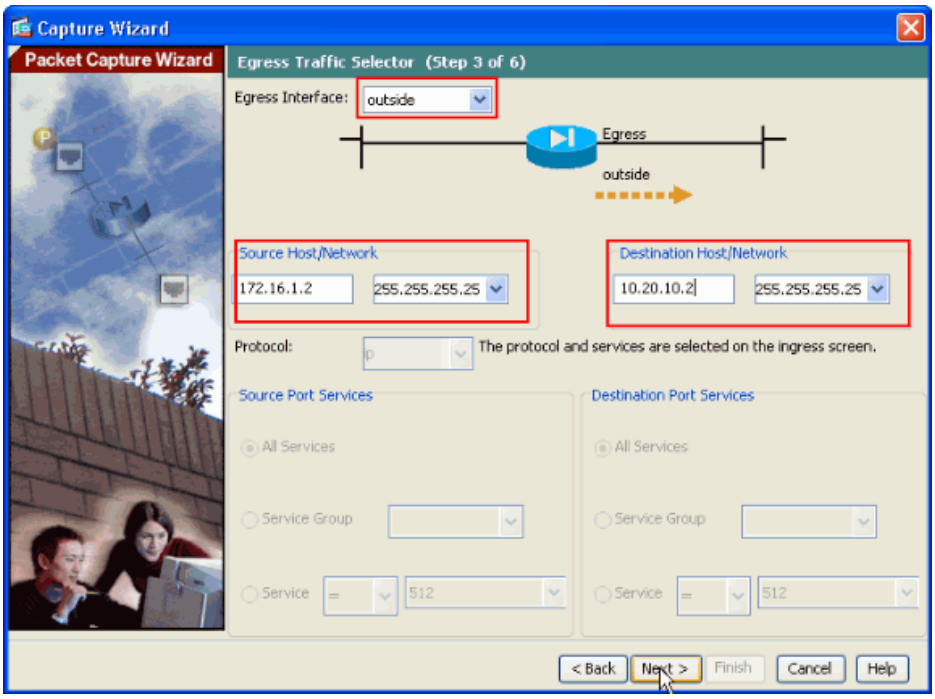


3. 在新窗口中，提供用于捕获输入数据流的参数。选择 Ingress interface 作为 Inside，并提供要捕获的数据包的源和目标 IP 地址，并在所提供的相应空白处提供其子网掩码。此外，选择要由 ASA 捕获的数据包类型（IP 是此处选择的数据包类型），如下显示：



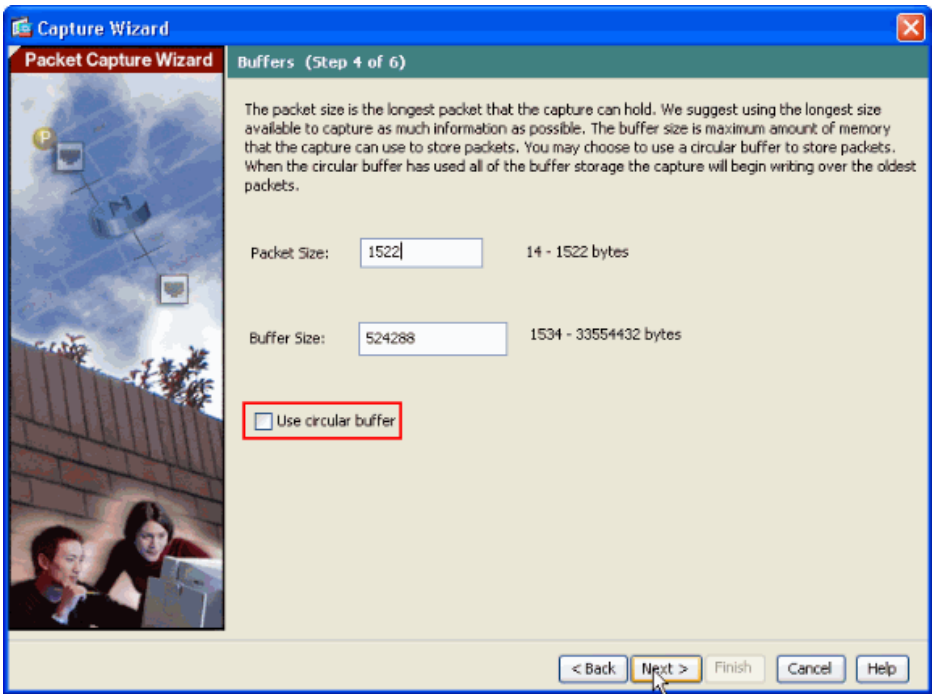
单击 Next。

4. 选择 Egress interface 作为 Outside，然后提供源和目标 IP 地址，并在所提供的相应空白处提供其子网掩码，如下所示：



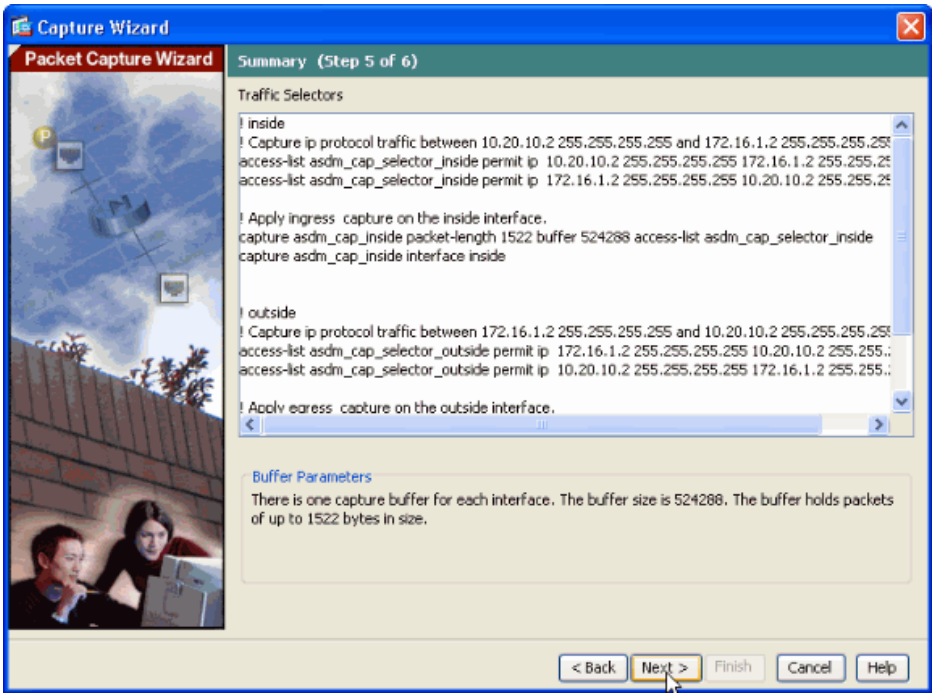
单击 Next。

5. 在所提供的相应空白处提供数据包大小和捕获缓冲区大小，因为这些数据是进行捕获所必需的。此外，如果要使用循环缓冲区选项，请记住选中 Use circular buffer 复选框。在本示例中，未使用循环缓冲区，因此未选中该复选框。

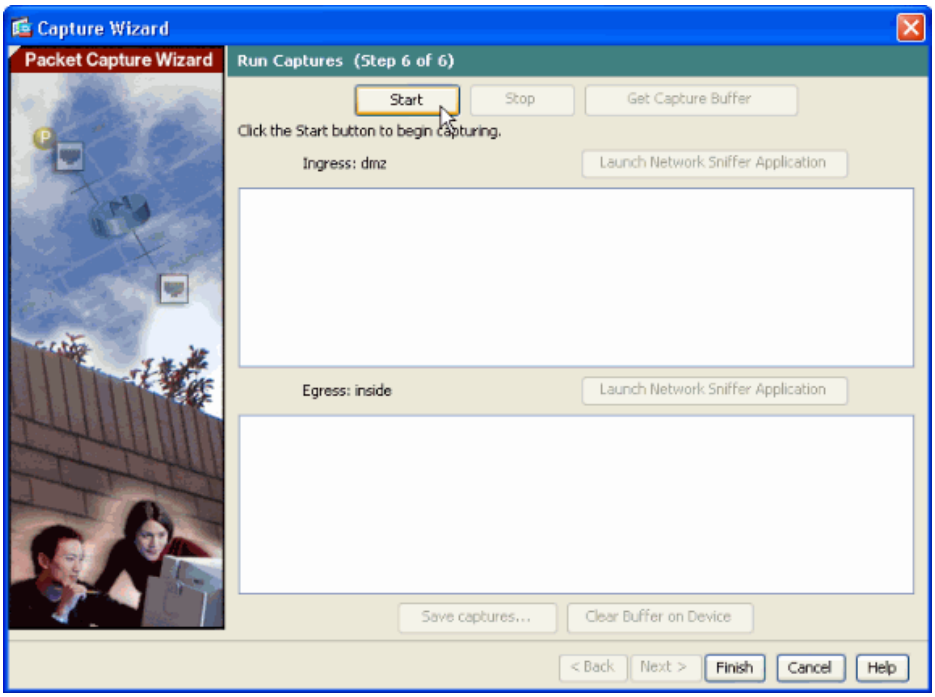


单击 Next。

6. 此窗口显示要在 ASA 上配置以使 ASA 捕获所需数据包的访问列表，并显示数据包的类型（在本示例中将捕获 IP 数据包）。单击 Next。

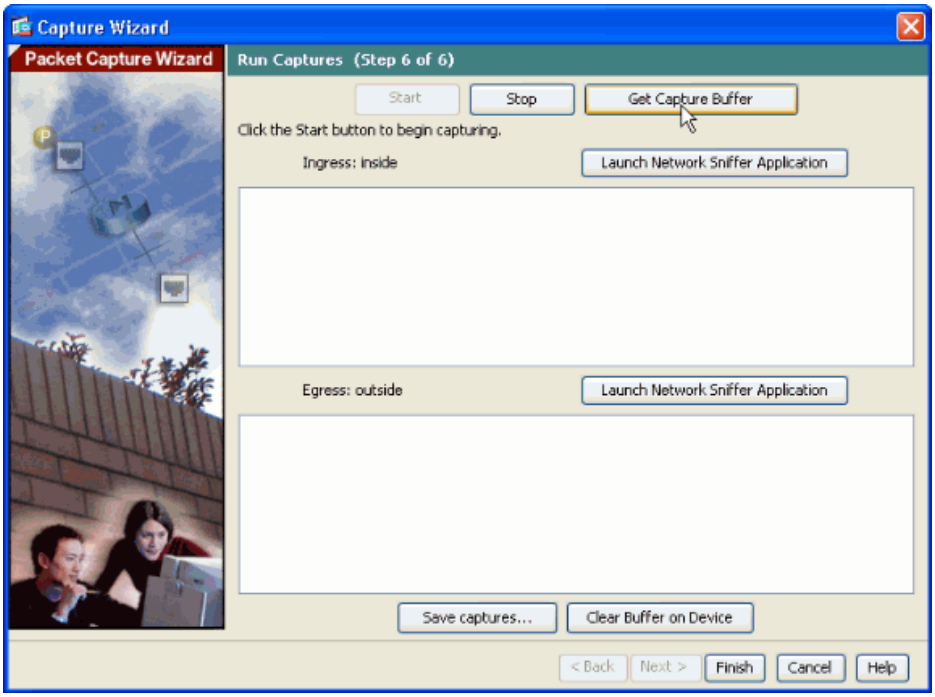


7. 如下所示，单击 Start 开始数据包捕获：

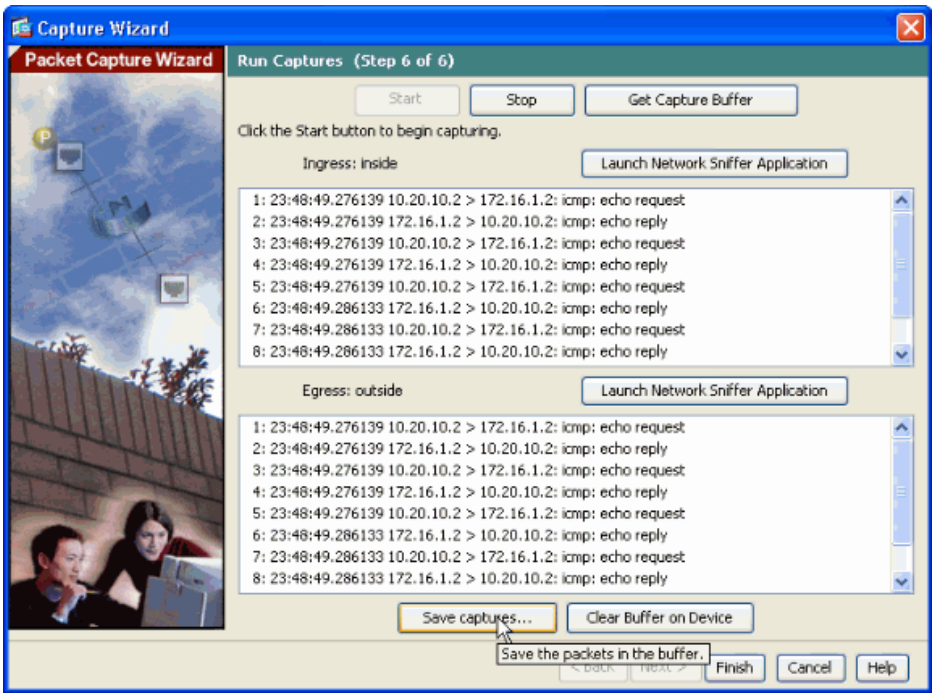


8. 由于数据包捕获已经开始，请尝试从内部网络 ping 外部网络，以便在源和目标之间流动的数据包被 ASA 捕获缓冲区捕获。

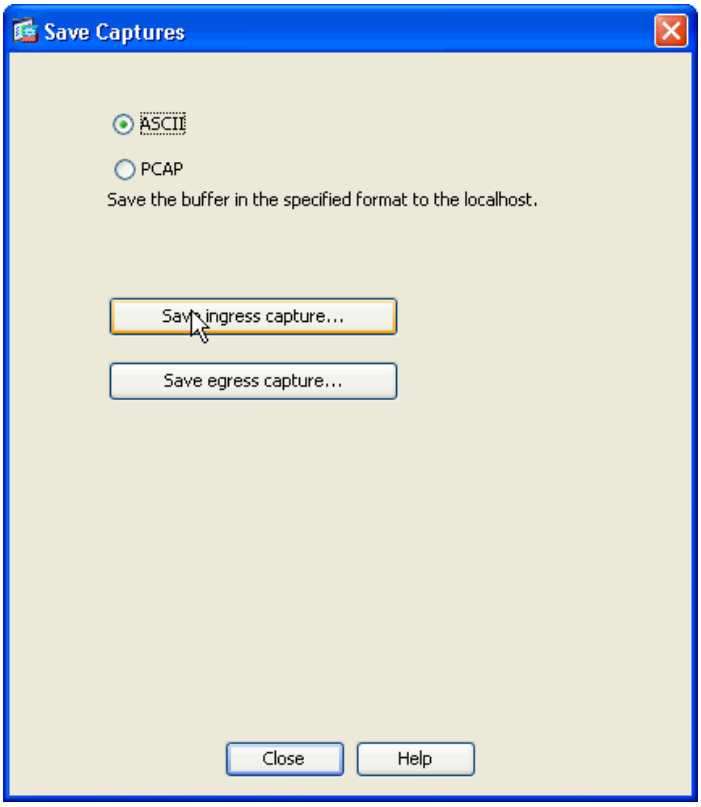
9. 单击 Get Capture Buffer 以查看由 ASA 捕获缓冲区捕获的数据包。



10. 此窗口中显示了所捕获的输入数据流和输出数据流的数据包。如下所示，单击 Save captures 以保存捕获信息：

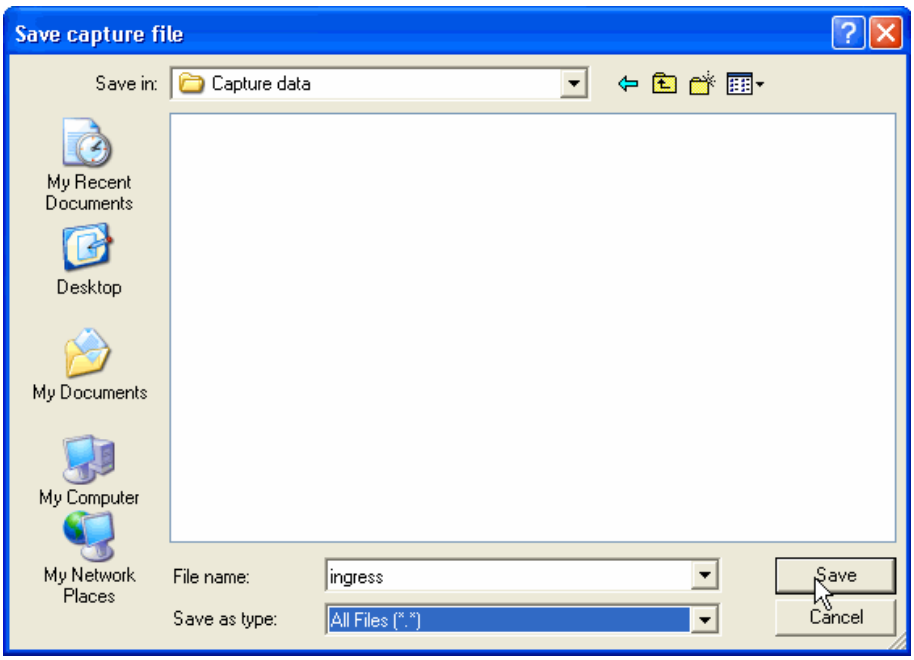


11. 在 Save Captures 窗口中，选择用来保存捕获缓冲区的所需格式。可以是 ASCII 或 PCAP。单击格式名称旁边的单选按钮。然后，根据需要单击 Save ingress capture 或 Save egress capture。

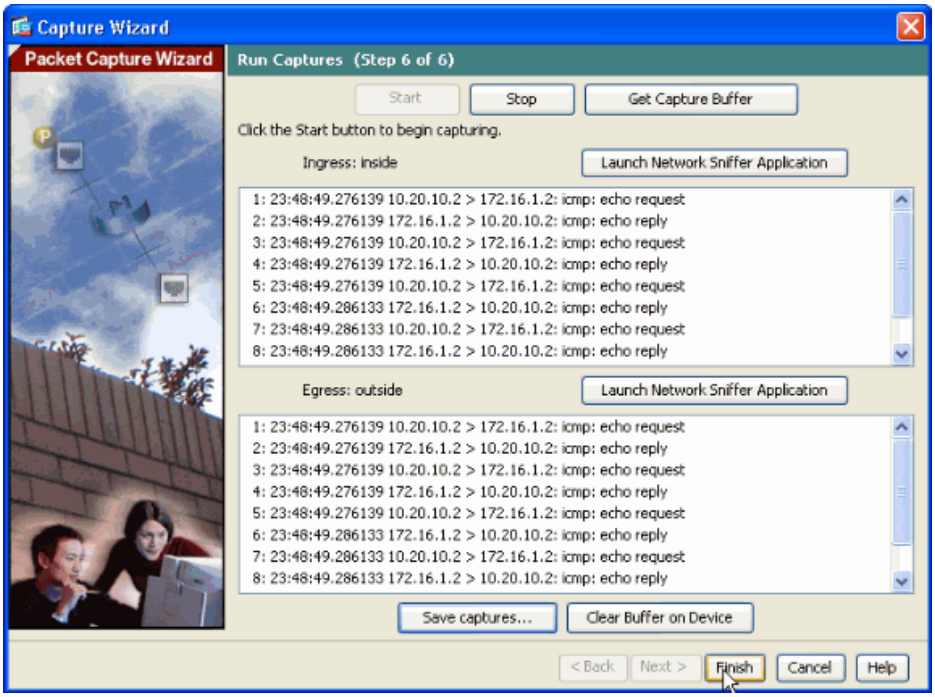


如果指定 pcap 格式，则可以使用 TCPDUMP 或 Ethereal 打开文件。ASCII 格式的捕获文件可以使用 Web 浏览器进行查看。

12. 如下所示，在 Save capture file 窗口中，提供捕获文件的文件名和要将捕获文件保存到的位置，然后单击 Save：



13. 单击 完成。



这便完成了数据包捕获过程。

使用 CLI 在 ASA/PIX 中配置数据包捕获的分步过程

要使用 CLI 在 ASA/PIX 中配置数据包捕获，请完成以下步骤：

1. 如网络图中所示，配置内部和外部接口，并配置 IP 地址和安全等级。
2. 配置访问列表 asdm_cap_selector_inside 和 asdm_cap_selector_outside 以捕获从内部网络传输到外部网络和从外部网络传输到内部网络的数据包。

```
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. 在特权 EXEC 模式下，使用 capture 命令启动数据包捕获进程。capture 命令应在访问列表已按 ASA 配置中所示进行了配置后再使用。在此配置示例中，将定义名为 capin 的捕获。将其绑定到内部接口，并指定只捕获与访问列表 asdm_cap_selector_inside 匹配的数据包，如下所示：

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

同样地，定义名为 capout 的捕获。将其绑定到外部接口，并指定只捕获与访问列表 asdm_cap_selector_outside 匹配的数据包，如下所示：

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

现在，ASA 将开始捕获接口之间的数据流。在任何时候要停止捕获，均可使用后跟捕获名称的 no capture 命令。

在 ASA 上查看捕获的数据包

在 ASA 设备上查看捕获的数据包
要查看捕获的数据包，请使用后跟捕获名称的 show capture 命令。以下是捕获缓冲区内容的 show 命令输出：show capture capin 命令显示名为 capin 的捕获缓冲区的内容。 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#
```

show capture capout 命令显示名为 capout 的捕获缓冲区的内容。

```
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#
```

相关信息

- Cisco PIX 500 系列安全设备命令参考
- 故障排除技术说明

文件创建日期: 2013 年 8 月 5 日

http://www.cisco.com/cisco/web/support/CN/109/1091/1091197_asa-capture-asdm-config.html