使用CLI和ASDM配置ASA数据包捕获

目录

简介

本文档介绍如何配置Cisco ASA防火墙以使用ASDM或CLI捕获所需数据包。

先决条件

要求

此过程假定ASA完全可操作，并且已进行配置以允许Cisco ASDM或CLI进行配置更改。

使用的组件

本文档不限于特定硬件或软件版本。

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

相关产品

以下思科产品也使用此配置：

- Cisco ASA 9.1(5)及更高版本
- Cisco ASDM 7.2.1 版

背景信息

本文档介绍如何配置 **Cisco Adaptive Security Appliance (ASA) Next-Generation Firewall** 以便使用 **Cisco Adaptive Security Device Manager (ASDM)** 或 **Command Line Interface (CLI) (ASDM).**

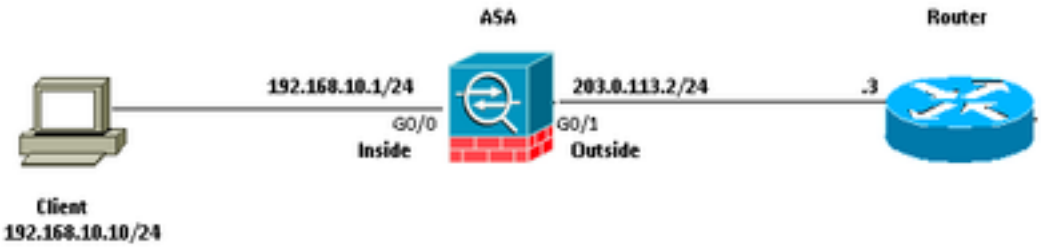
数据包捕获过程对于排除连接问题或监控可疑活动非常有用。此外，还可以创建多个捕获，以便分析多个接口上不同类型的流量。

配置

本节提供用于配置本文档中描述的数据包捕获功能的信息。

网络图

本文档使用以下网络设置：



配置

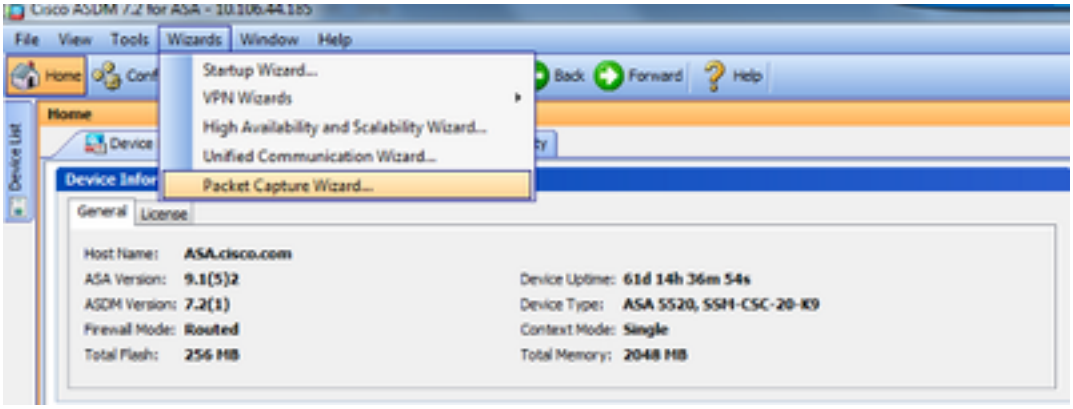
此配置中使用的 IP 编址方案在 Internet 上不能合法路由。它们是在实验室环境中使用的RFC 1918地址。

使用ASDM配置数据包捕获

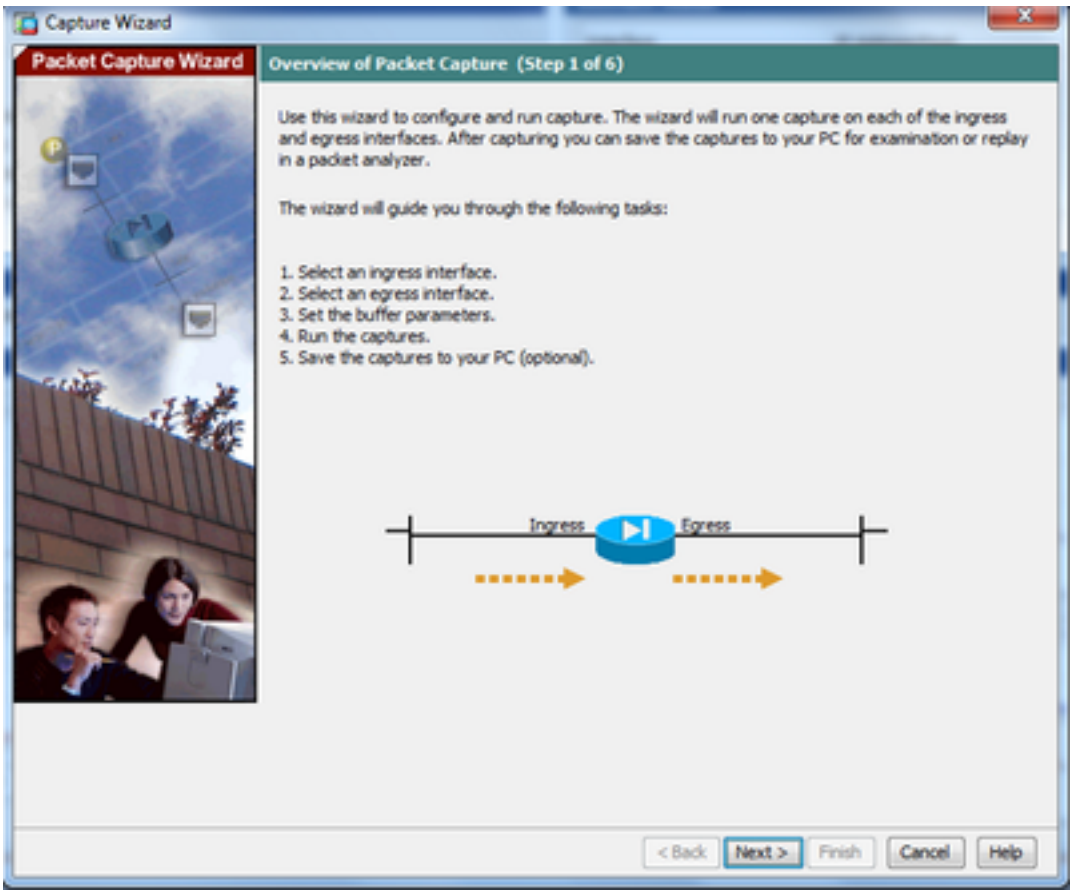
此示例配置用于捕获在从User1（内部网络）到Router1（外部网络）的ping操作期间传输的数据包。

要使用ASDM在ASA上配置数据包捕获功能，请完成以下步骤：

1.导航至 **Wizards > Packet Capture Wizard** 要启动数据包捕获配置，如下所示：



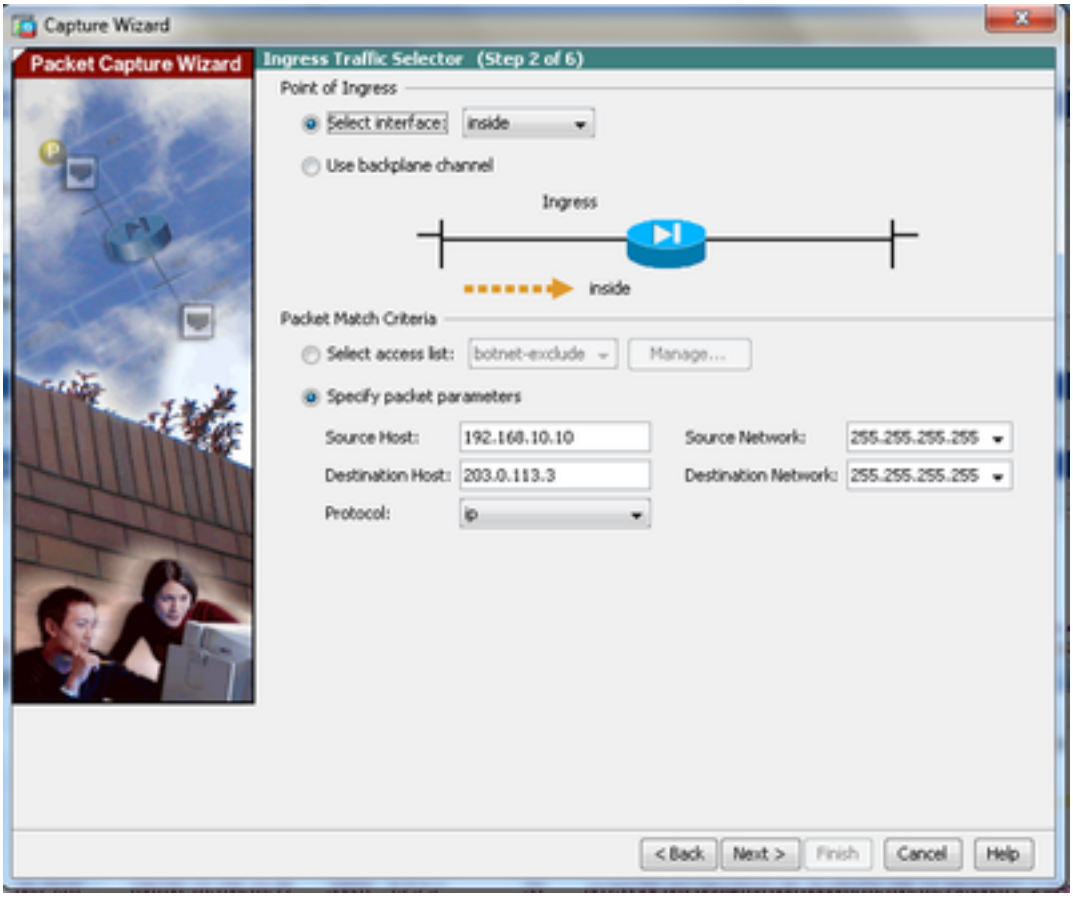
2. **Capture Wizard** 打开。点击 **Next**.



3.0在新窗口中，提供用于捕获入口流量的参数。

3.1选择 **inside** 对于 **Ingress Interface** 并提供要捕获的数据包的源IP地址和目的IP地址及其子网掩码（在相应的空白处）。

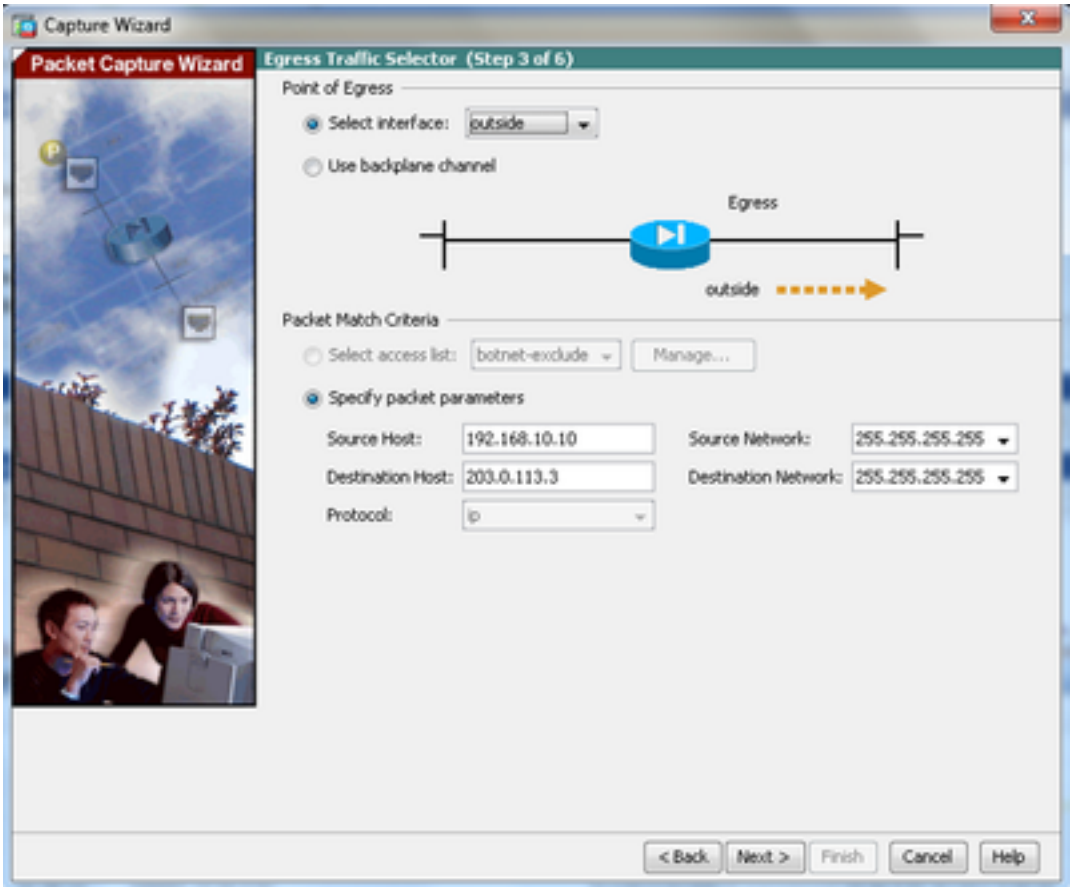
3.2选择要由ASA捕获的数据包类型（IP是此处选择的数据包类型），如下所示：



3.3单击 **Next.**

4.1选择 **outside** 对于 **Egress Interface** 并在提供的相应空白处提供源IP地址和目的IP地址及其子网掩码。

If Network Address Translation (NAT) 在防火墙上执行，也考虑这一点。



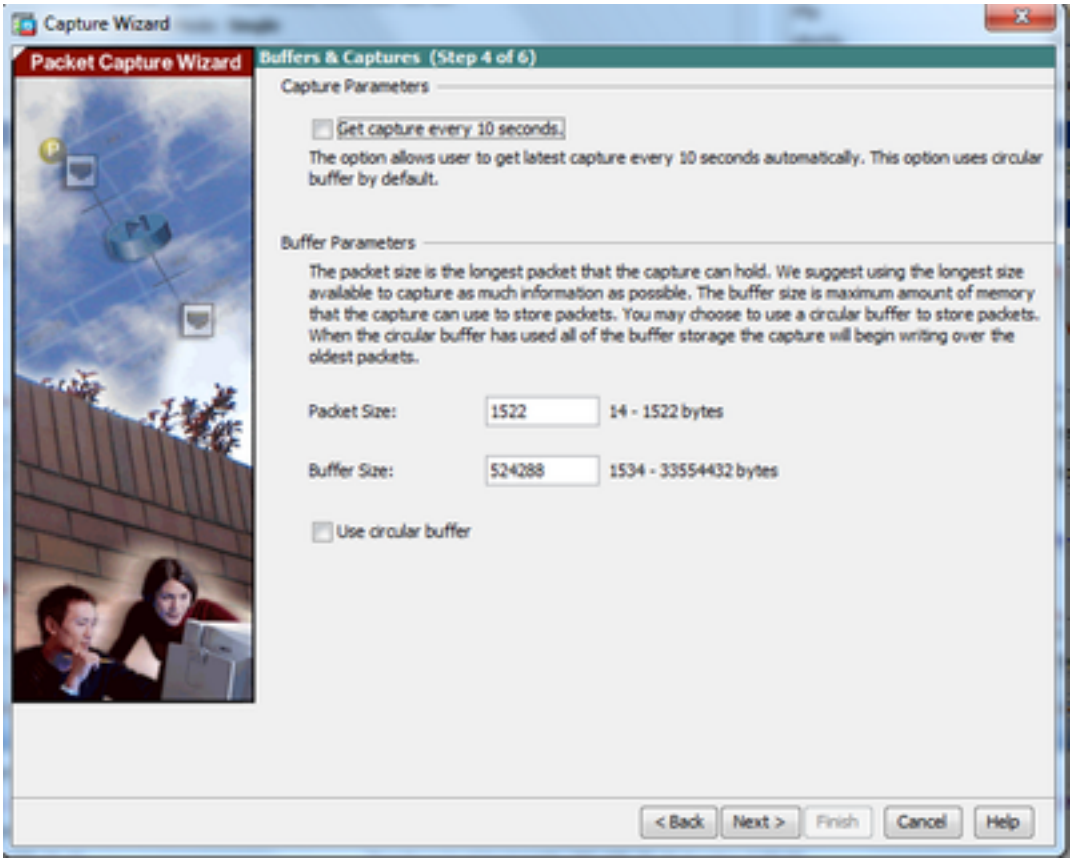
4.2单击 **Next.**

5.1输入适当的 **Packet Size** 和 **Buffer Size** 在相应的空间中。进行捕获需要此数据。

5.2查看 **Use circular buffer** 框以使用循环缓冲区选项。循环缓冲区永远不会满。

当缓冲区达到最大容量时，旧数据将被丢弃，捕获将继续。

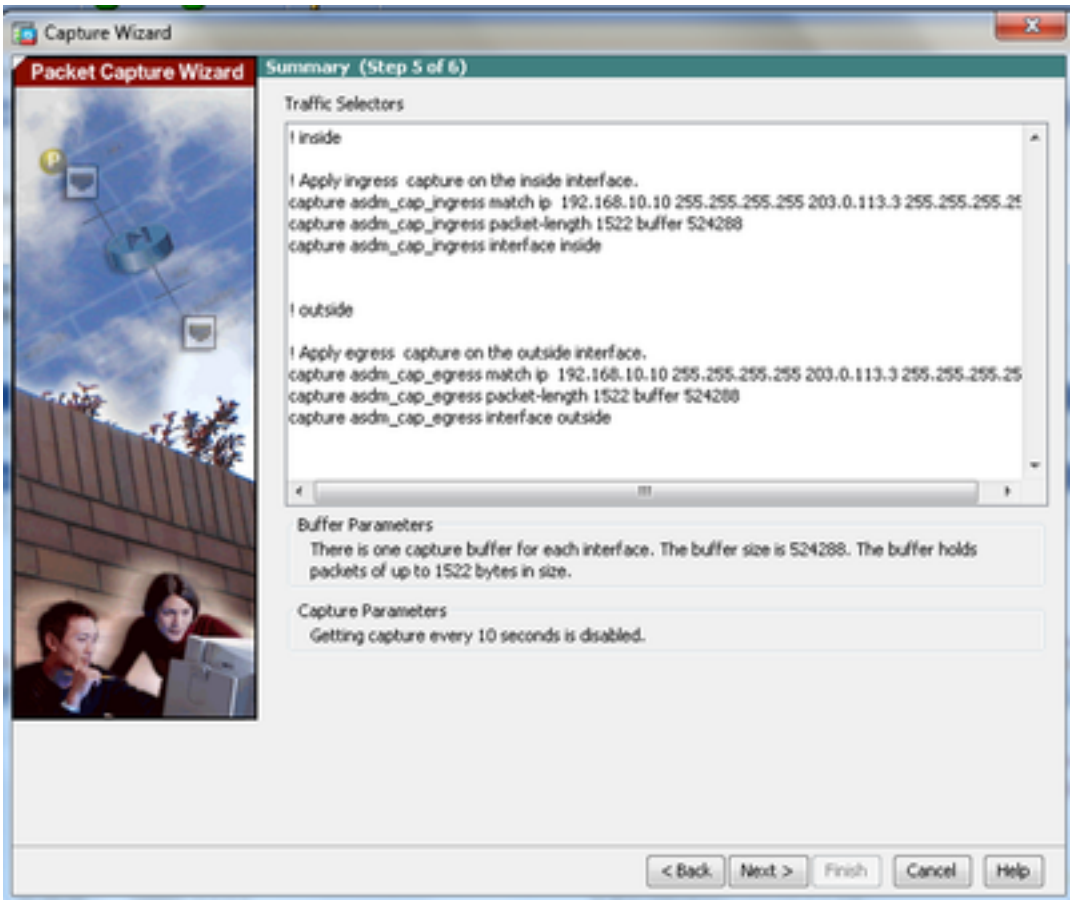
在本示例中，未使用循环缓冲区，因此未选中该复选框。



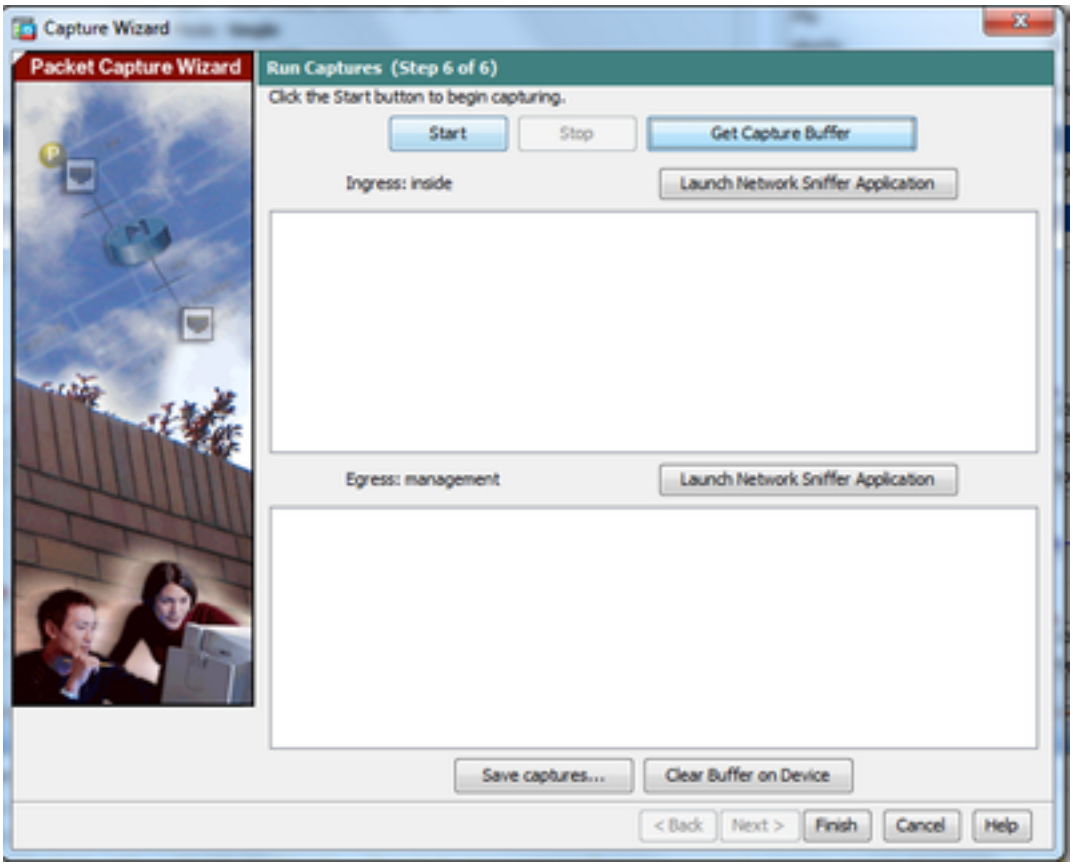
5.3单击 **Next.**

6.0此窗口显示 **Access-lists** 必须在ASA上配置（以便捕获所需的数据包）和要捕获的数据包类型（本示例中捕获IP数据包）。

6.1单击 **Next.**

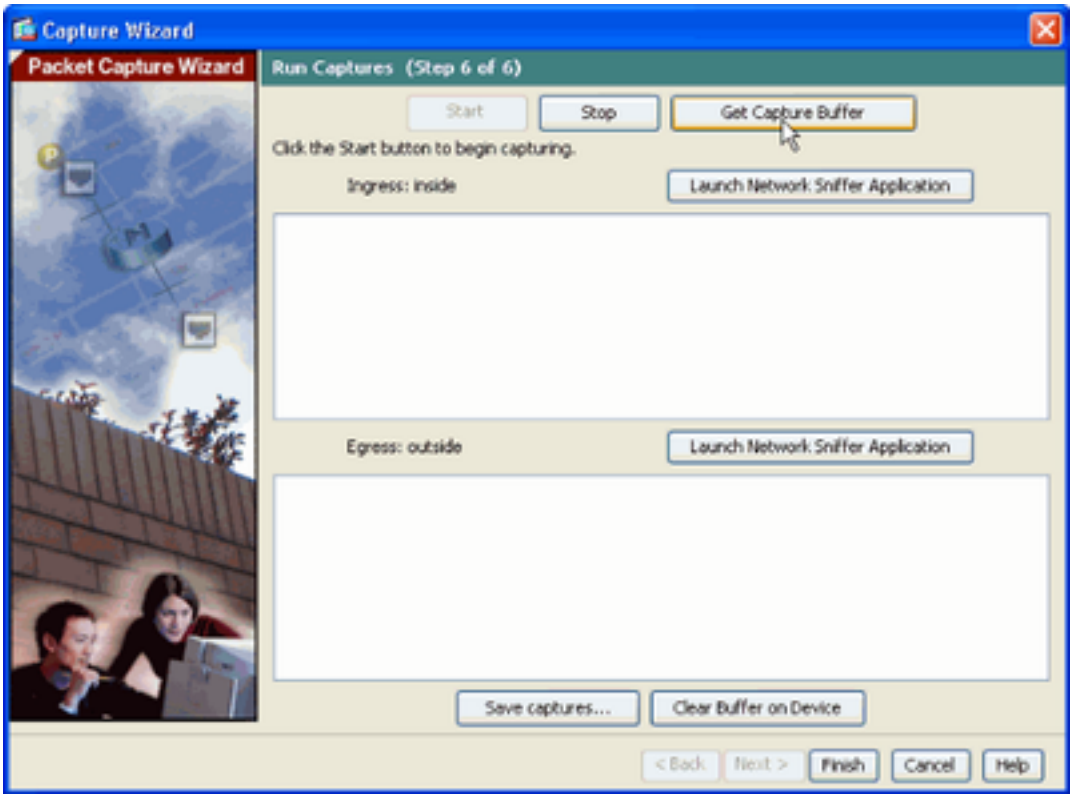


7.单击 **Start** 为了开始数据包捕获，如下所示：



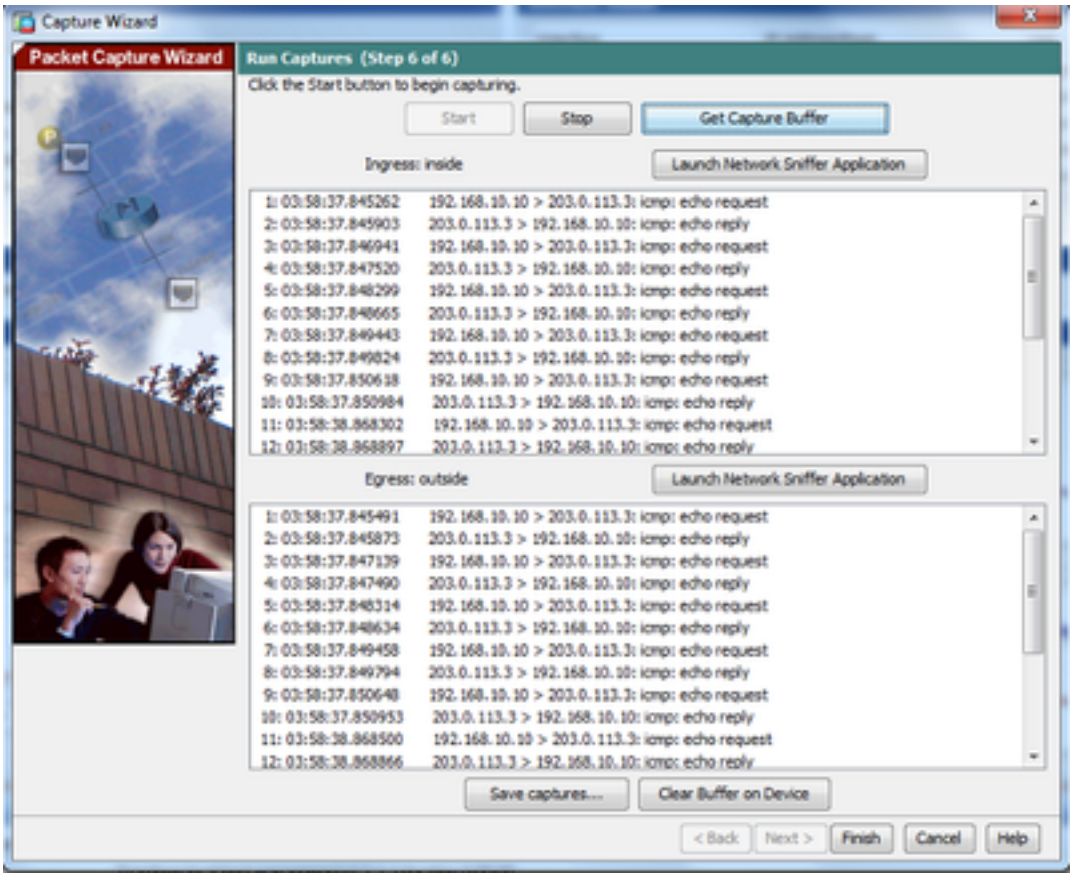
数据包捕获开始后，尝试从内部网络ping外部网络，以便源和目标IP地址之间流的数据包由ASA捕获缓冲区捕获。

8.单击 **Get Capture Buffer** 查看ASA捕获缓冲区捕获的数据包。



此窗口中显示入口和出口流量的捕获数据包。

9.单击 **Save captures** 保存捕获信息。

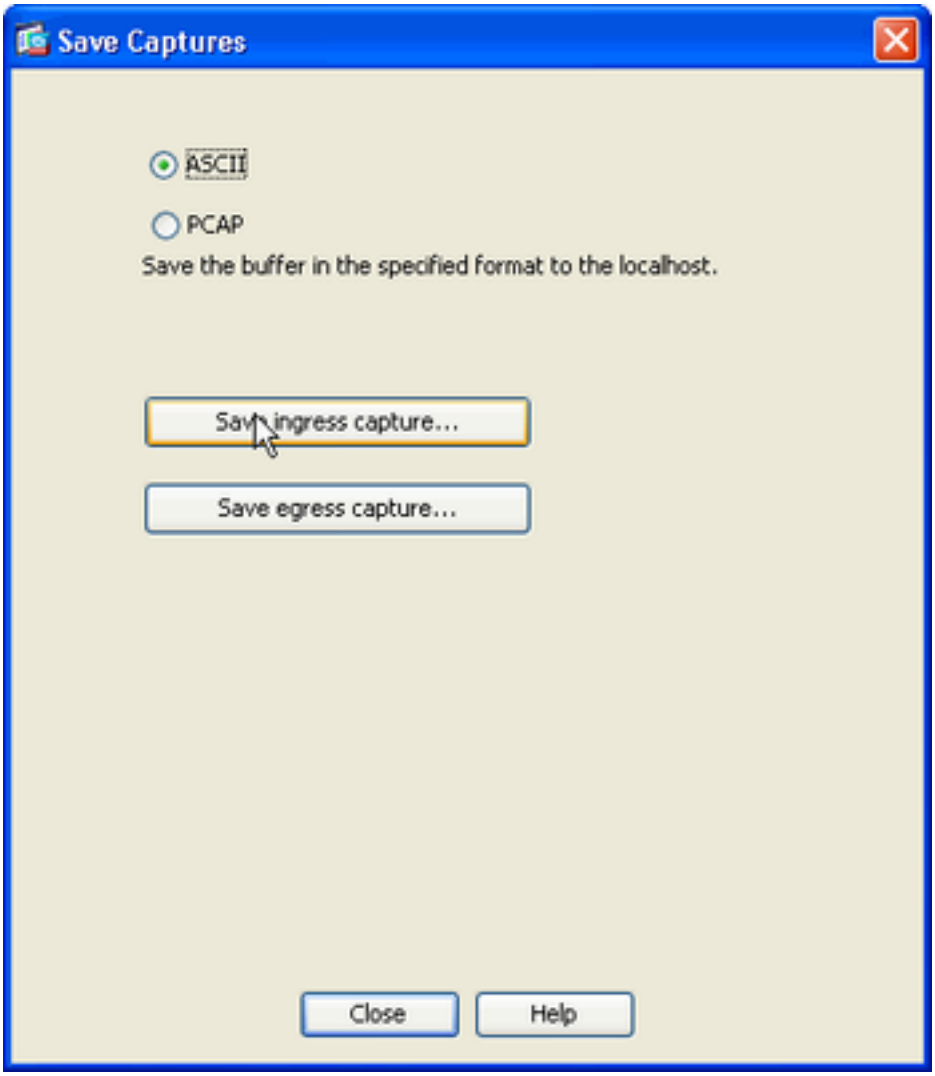


10.1来自 **Save captures** 窗口中，选择保存捕获缓冲区所需的格式。

10.2这是ASCII或PCAP。单击格式名称旁边的单选按钮。

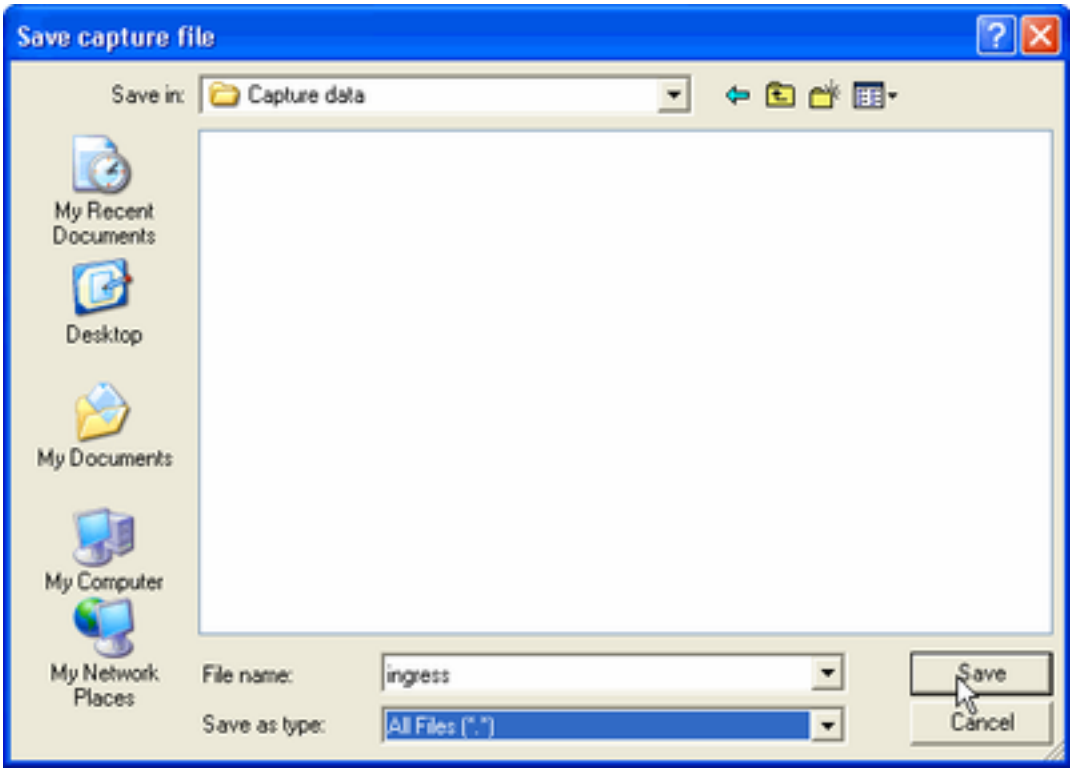
10.3然后，单击 **Save ingress capture** 或 **Save egress capture** 根据需要。

可以使用捕获分析器打开PCAP文件，例如 **Wireshark**，并且它是首选方法。

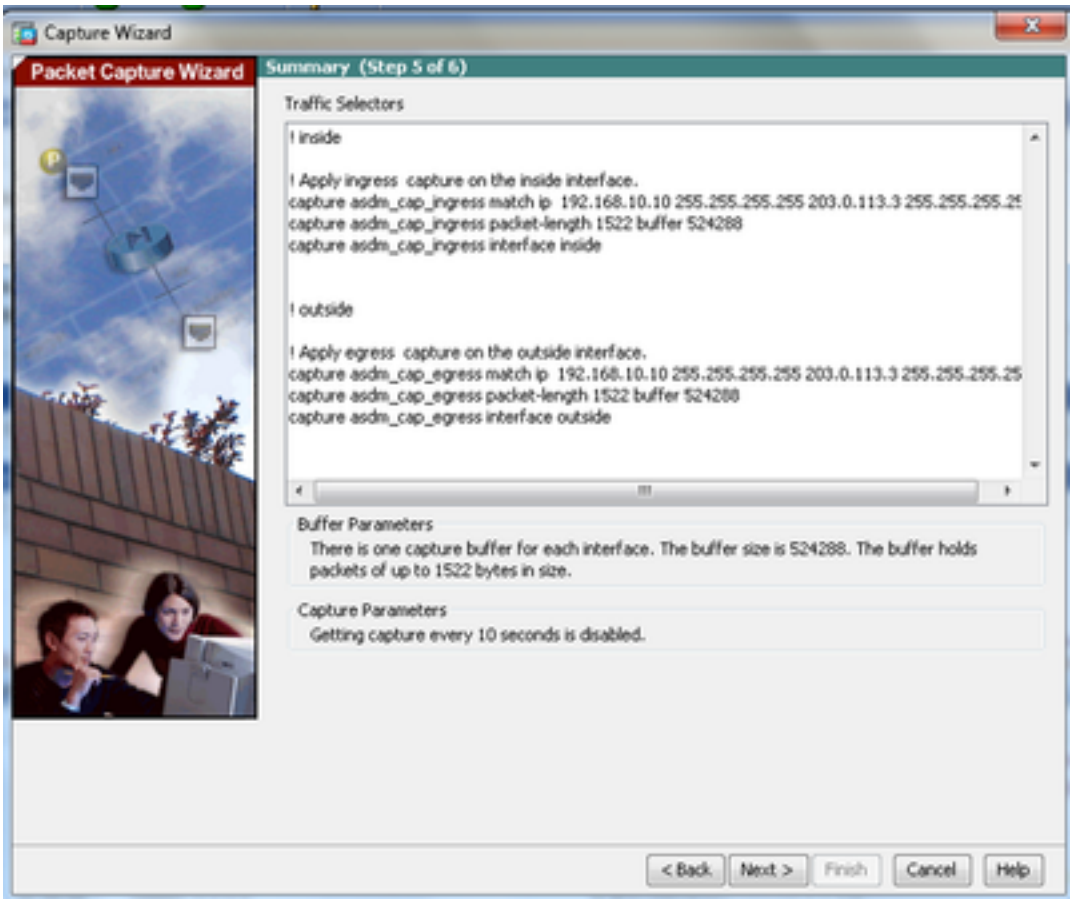


11.1来自 **Save capture file** 窗口中，提供文件名和保存捕获文件的位置。

11.2单击 **Save**.



12.单击 **Finish**.



这样就完成了GUI数据包捕获过程。

使用CLI配置数据包捕获

要使用CLI在ASA上配置数据包捕获功能，请完成以下步骤：

1. 按照网络图所示使用正确的IP地址和安全级别配置内部和外部接口。

2. 在特权EXEC模式下使用capture命令启动数据包捕获过程。在此配置示例中，将定义名为 **capin 的捕获。**将其绑定到**inside**接口，并使用**match**关键字指定仅捕获与所需流量匹配的数据包：

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

3. 同样地，定义名为 **capout 的捕获。**将其绑定到**outside**接口，并使用**match**关键字指定仅捕获与所需流量匹配的数据包：

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

ASA现在开始捕获接口之间的流量。要随时停止捕获，请输入no capture命令，后跟捕获名称。

示例如下：

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

ASA上的可用捕获类型

本节介绍ASA上可用的不同类型的捕获。

- **asa_dataplane** — 捕获在ASA背板上通过ASA与使用背板的模块（例如ASA CX或IPS模块）之间的数据包。

```
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 — 捕获加速安全路径丢弃的数据包。drop-code指定加速安全路径丢弃的流量类型。

```
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 — 选择要捕获的以太网类型。支持的以太网类型包括8021Q、ARP、IP、IP6、LACP、PPPOED、PPPOES、RARP和VLAN。

本示例展示如何捕获ARP流量：

```
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** — 实时连续显示捕获的数据包。要终止实时数据包捕获，请按Ctrl-C。要永久删除捕获，请使用此命令的no形式。
- 当您使用 **cluster exec capture** 命令。

```
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** — 以类似于ASA Packet Tracer功能的方式跟踪捕获的数据包。

```
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
```

注意：在ASA 9.10+上，any关键字仅捕获具有ipv4地址的数据包。any6关键字可捕获所有ipv6寻址流量。

这些是可使用数据包捕获配置的高级设置。

请查看命令参考指南，了解如何设置它们。

- **ikev1/ikev2** — 仅捕获Internet密钥交换版本1(IKEv1)或IKEv2协议信息。
- **isakmp** — 捕获VPN连接的Internet安全关联和密钥管理协议(ISAKMP)流量。ISAKMP子系统无权访问上层协议。捕获是伪捕获，将物理、IP和UDP层结合在一起以满足PCAP解析器的要求。对等体地址从SA交换获得并存储在IP层中。
- **lacp** — 捕获链路汇聚控制协议(LACP)流量。如果已配置，则接口名称是物理接口名称。当您使用Etherchannel识别LACP的当前行为时，这非常有用。
- **tls-proxy** — 从一个或多个接口上的传输层安全(TLS)代理捕获已解密的入站和出站数据。
- **webvpn** — 捕获特定WebVPN连接的WebVPN数据。

警告：启用WebVPN捕获时，它会影响安全设备的性能。确保在生成故障排除所需的捕获文件后禁用捕获。

默认设置

以下是ASA系统默认值：

- 默认类型为raw-data。
- 默认缓冲区大小为512 KB。
- 默认以太网类型为IP数据包。
- 默认数据包长度为1,518字节。

查看捕获的数据包

在ASA上

要查看捕获的数据包，请输入show capture命令，后跟捕获名称。本节提供捕获缓冲区内容的show命令输出。此 **show capture capin** 命令显示名为的捕获缓冲区的内容 **capin**:

```
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
```

此 **show capture capout** 命令显示名为的捕获缓冲区的内容 **capout**:

```
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
```

从ASA下载以进行离线分析

下载数据包捕获以供离线分析有以下几种方法：

1. 导航至 https://<ip_of_asa>/admin/capture/<capture_name>/pcap在任何浏览器上。

   提示：如果您不考虑 **pcap** 关键字，则仅等效于 **show capture** 提供了命令输出。

1. 输入copy capture命令和您的首选文件传输协议以下载捕获：

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

提示：对数据包捕获的使用问题进行故障排除时，Cisco建议您下载捕获以进行离线分析。

清除捕获

要清除捕获缓冲区，请输入 **clear capture** 指令：

```
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
```

输入 **clear capture /all** 命令清除所有捕获的缓冲区：

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

停止捕获

在ASA上停止捕获的唯一方法是使用以下命令完全禁用捕获：

```
no capture <capture-name>
```

验证

当前没有可用于此配置的验证过程。

故障排除

当前没有可用于此配置的特定故障排除信息。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。