Configurar capturas de pacotes ASA com CLI e ASDM

Contents

Introduction

Este documento descreve como configurar o firewall Cisco ASA para capturar os pacotes desejados com o ASDM ou a CLI.

Prerequisites

Requirements

Este procedimento pressupõe que o ASA esteja totalmente operacional e configurado para permitir que o Cisco ASDM ou a CLI façam alterações de configuração.

Componentes Utilizados

Este documento não está restrito a versões específicas de hardware ou software.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Produtos Relacionados

Essa configuração também é usada com estes produtos da Cisco:

- Cisco ASA versões 9.1(5) e posteriores
- Cisco ASDM Versão 7.2.1

Informações de Apoio

Este documento descreve como configurar o **Cisco Adaptive Security Appliance (ASA) Next-Generation Firewall** para capturar os pacotes desejados com o comando **Cisco Adaptive Security Device Manager (ASDM)** ou **Command Line Interface (CLI) (ASDM).**

O processo de captura de pacotes é útil para solucionar problemas de conectividade ou monitorar atividades suspeitas. Além disso, é possível criar várias capturas para analisar diferentes tipos de tráfego em várias interfaces.

Configurar

Esta seção fornece informações usadas para configurar os recursos de captura de pacotes descritos neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Configurações

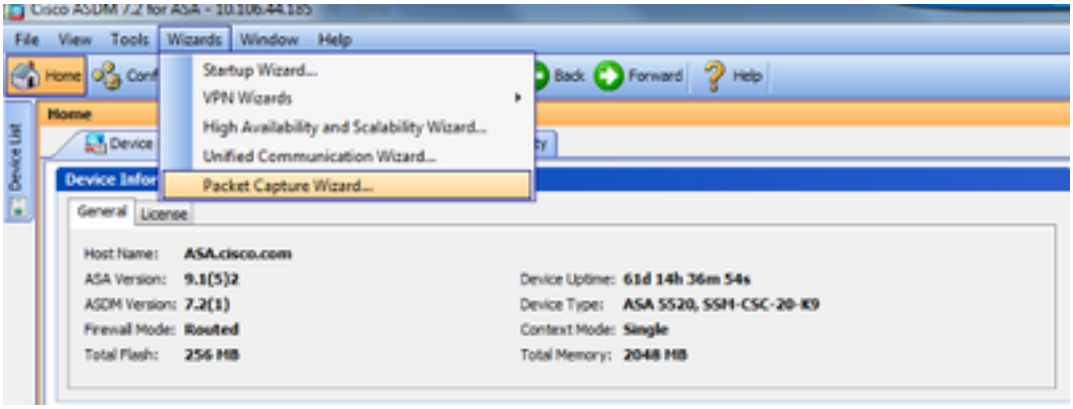
Os esquemas de endereço IP usados nesta configuração não são legalmente roteáveis na Internet. São endereços RFC 1918 usados em um ambiente de laboratório.

Configurar a Captura de Pacotes com o ASDM

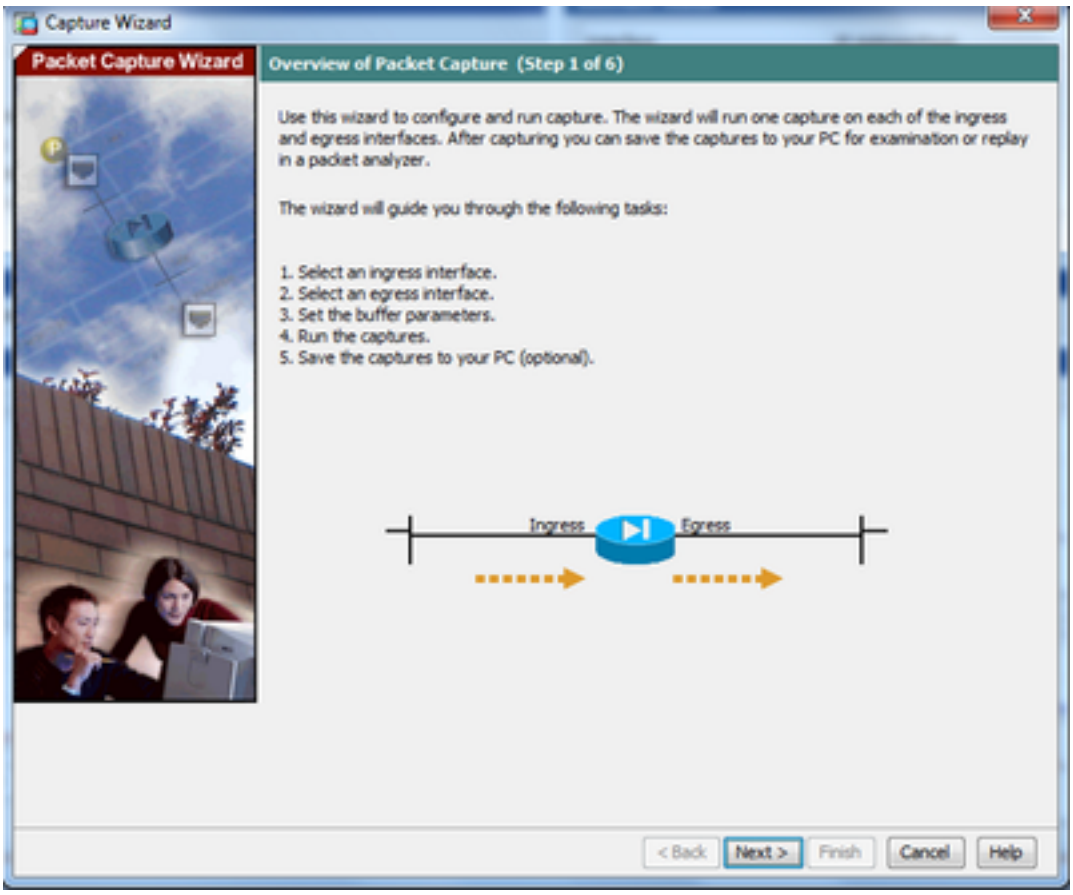
Esta configuração de exemplo é usada para capturar os pacotes que são transmitidos durante um ping do Usuário1 (rede interna) para o Roteador1 (rede externa).

Conclua estas etapas para configurar o recurso de captura de pacotes no ASA com o ASDM:

1. Navegue até **Wizards > Packet Capture Wizard** para iniciar a configuração de captura de pacotes, conforme mostrado:



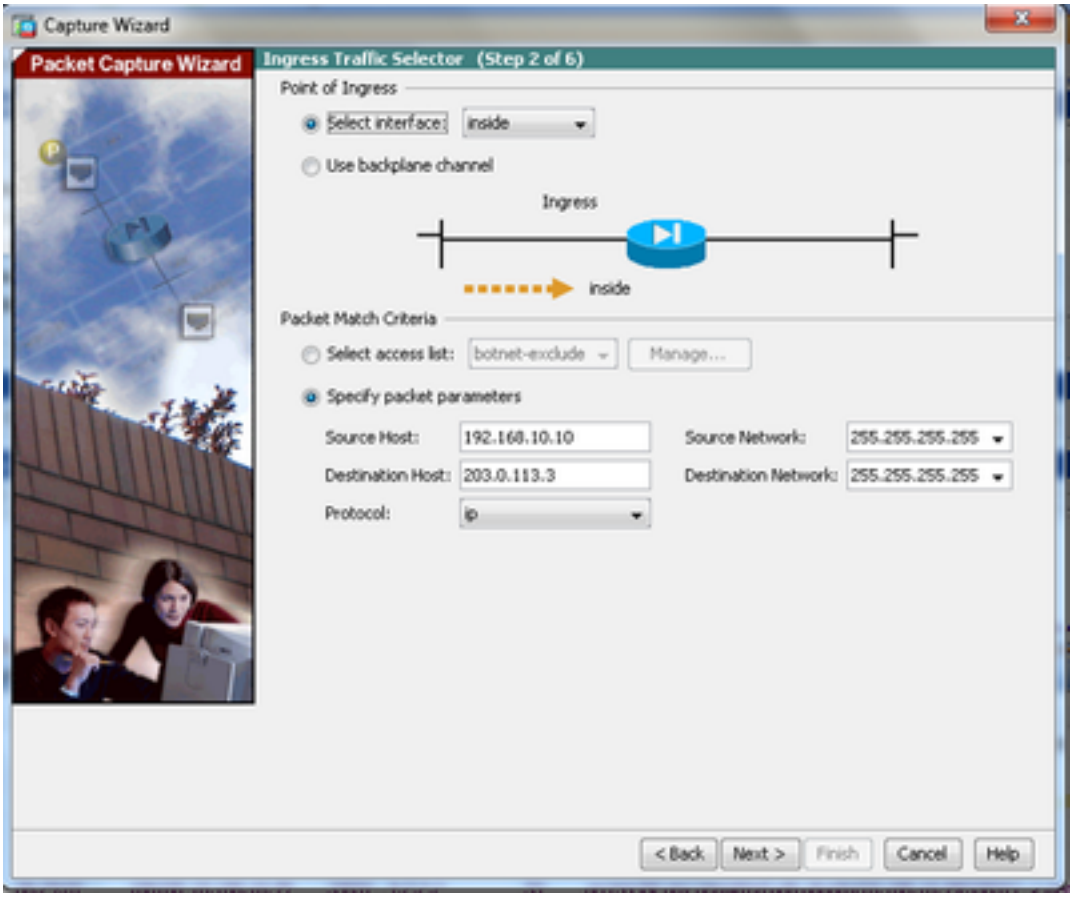
2. O **Capture Wizard** abre. Clique em **Next**.



3.0 Na nova janela, forneça os parâmetros que são usados para capturar o tráfego de entrada.

3.1 Selecionar **inside** para **Ingress Interface** e fornecem os endereços IP origem e destino dos pacotes a serem capturados, juntamente com sua máscara de sub-rede, no respectivo espaço fornecido.

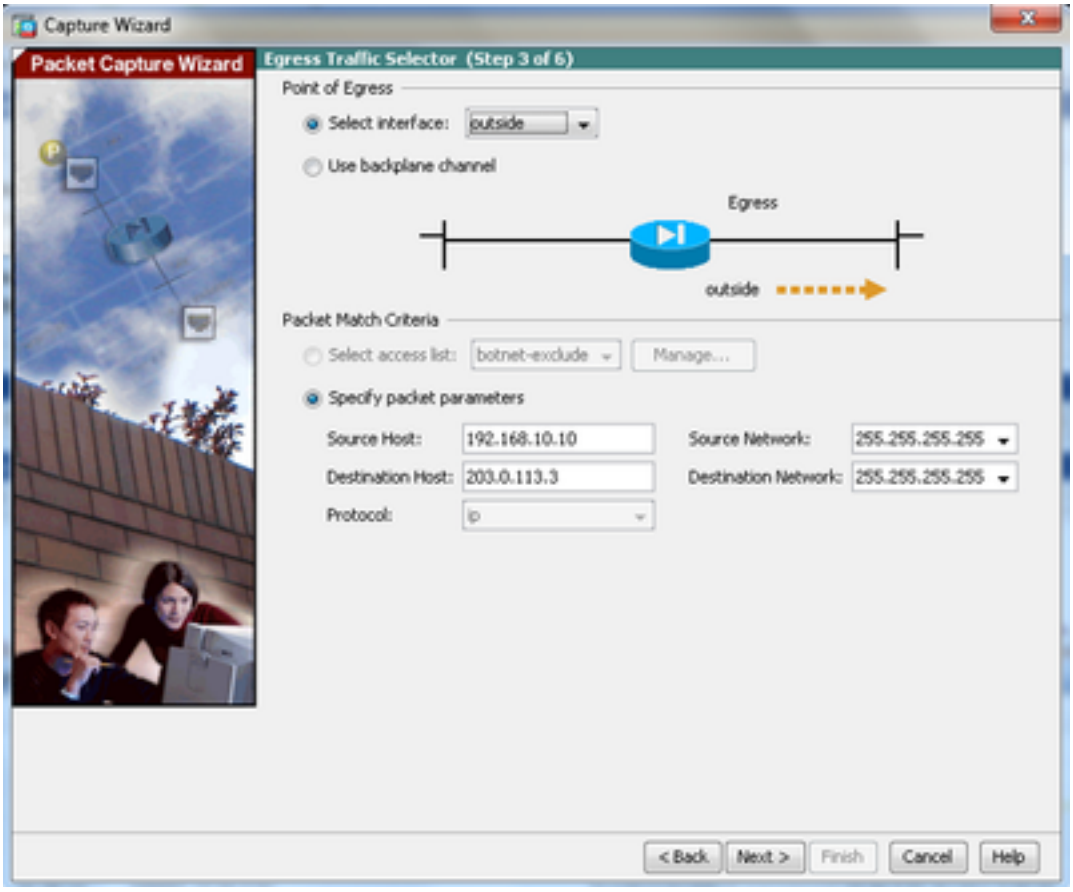
3.2 Escolha o tipo de pacote a ser capturado pelo ASA (IP é o tipo de pacote escolhido aqui), conforme mostrado:



3.3 Clique em **Next**.

4.1 Selecionar **outside** para **Egress Interface** e forneça os endereços IP origem e destino, juntamente com sua máscara de sub-rede, nos respectivos espaços fornecidos.

If Network Address Translation (NAT) é executado no Firewall, leve isso em consideração também.



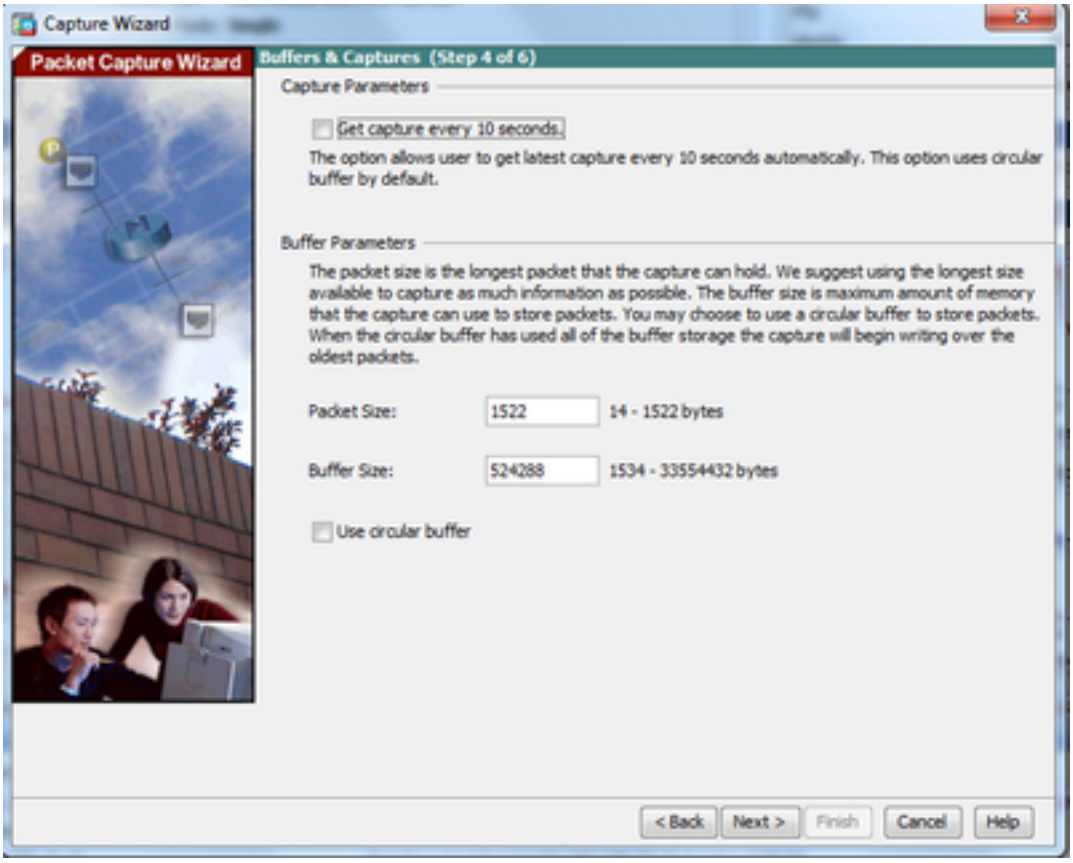
4.2 Clique em **Next**.

5.1 Insira as informações **Packet Size** e o **Buffer Size** no respectivo espaço fornecido. Esses dados são necessários para que a captura ocorra.

5.2 Verifique a **Use circular buffer** para usar a opção de buffer circular. Os buffers circulares nunca são preenchidos.

Àmedida que o buffer atinge seu tamanho máximo, os dados mais antigos são descartados e a captura continua.

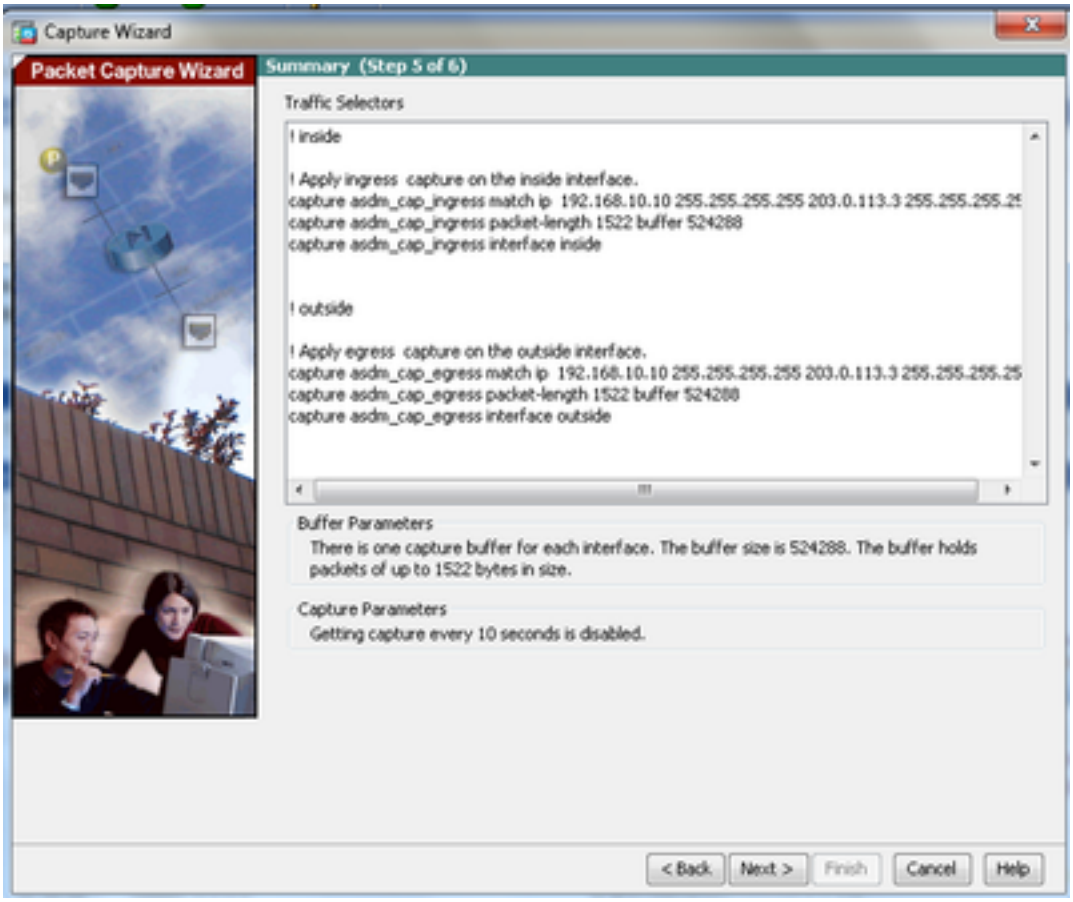
Neste exemplo, o buffer circular não é usado, portanto a caixa de seleção não é marcada.



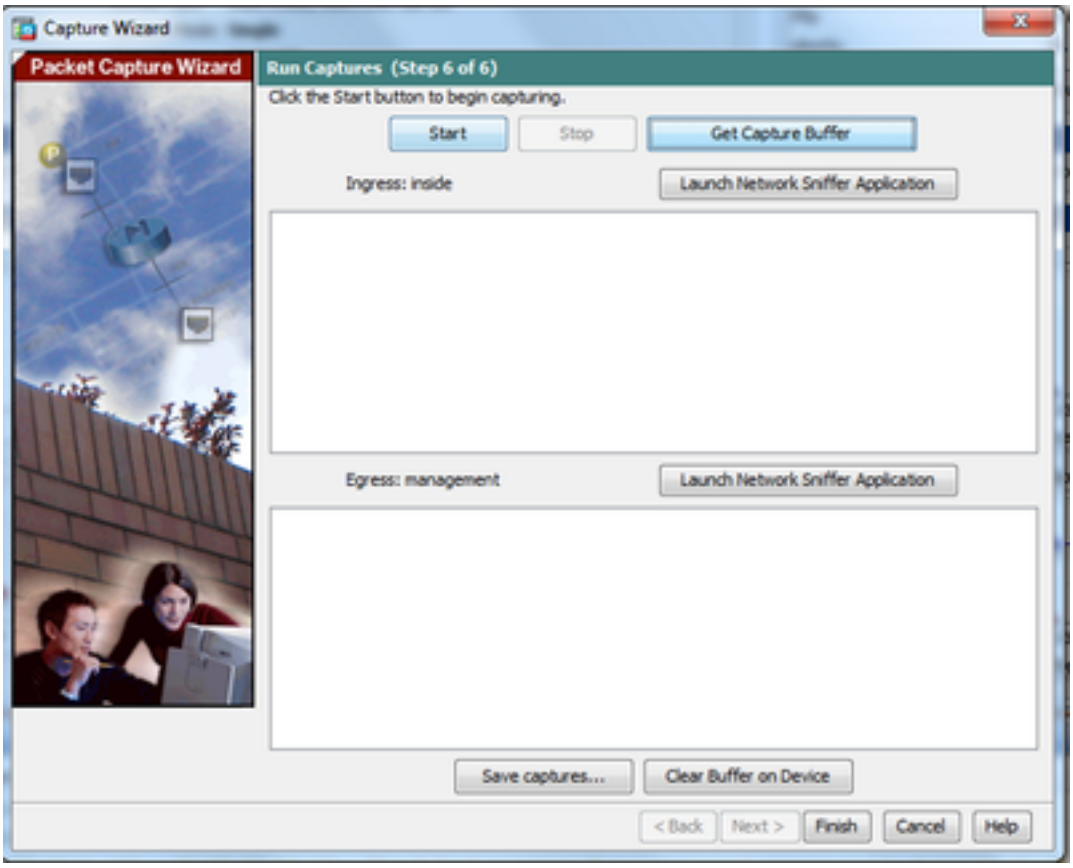
5.3 Clique em **Next**.

6.0 Essa janela mostra o **Access-lists** que devem ser configurados no ASA (para que os pacotes desejados sejam capturados) e o tipo de pacotes a serem capturados (os pacotes IP são capturados neste exemplo).

6.1 Clique em **Next**.

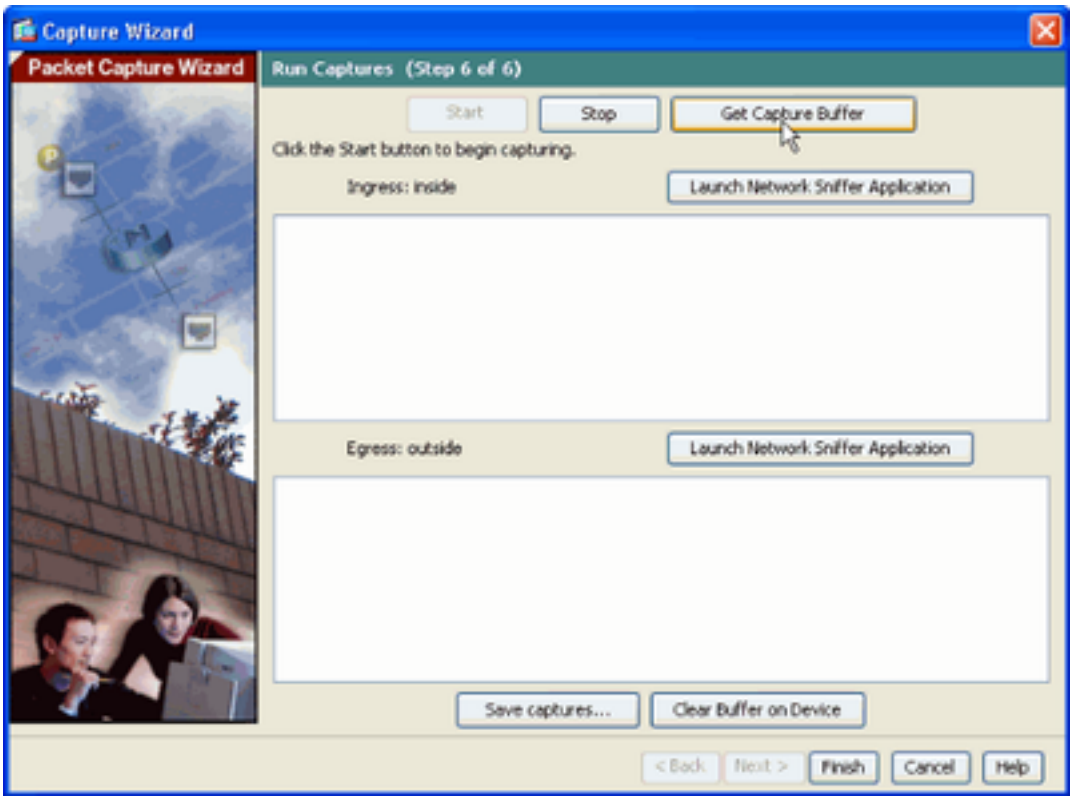


7. Clique em **Start** para iniciar a captura de pacotes, como mostrado:



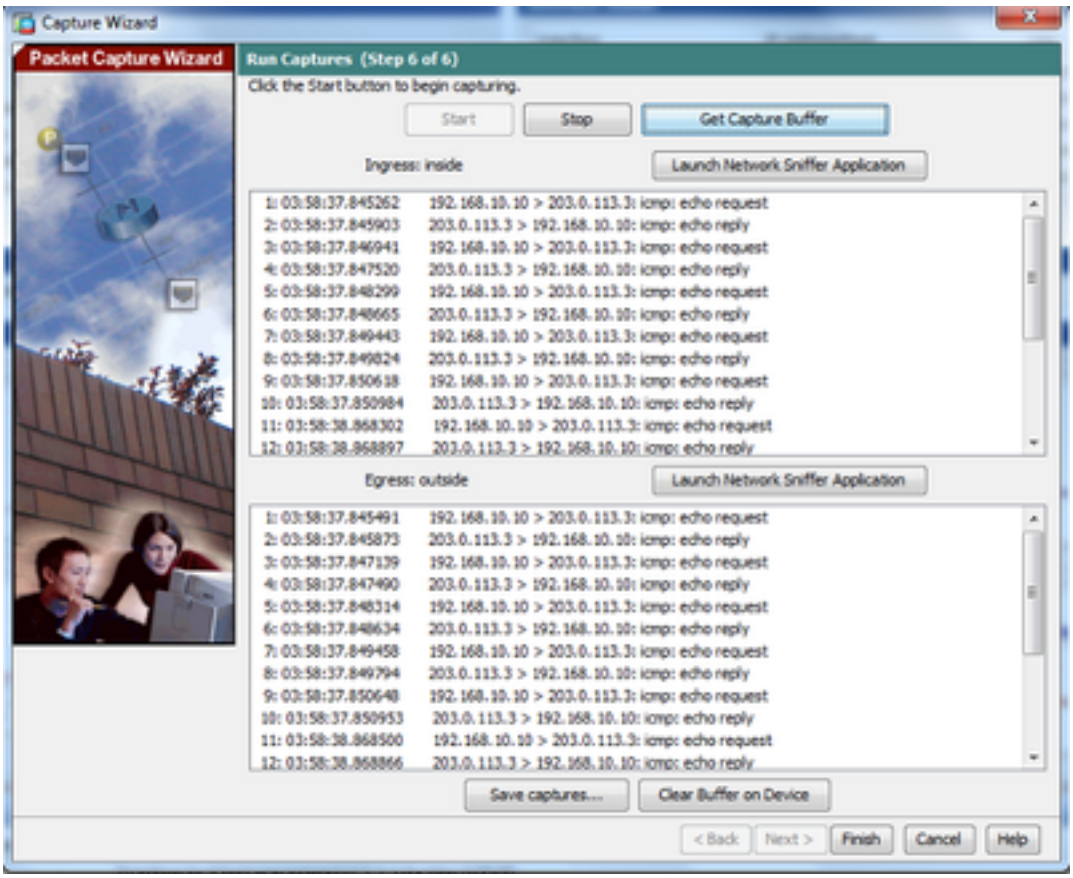
Quando a captura de pacotes for iniciada, tente fazer ping na rede externa a partir da rede interna para que os pacotes que fluem entre os endereços IP origem e destino sejam capturados pelo buffer de captura ASA.

8. Clique em **Get Capture Buffer** para visualizar os pacotes capturados pelo buffer de captura do ASA.



Os pacotes capturados são mostrados nessa janela para o tráfego de entrada e saída.

9. Clique em **Save captures** para salvar as informações de captura.

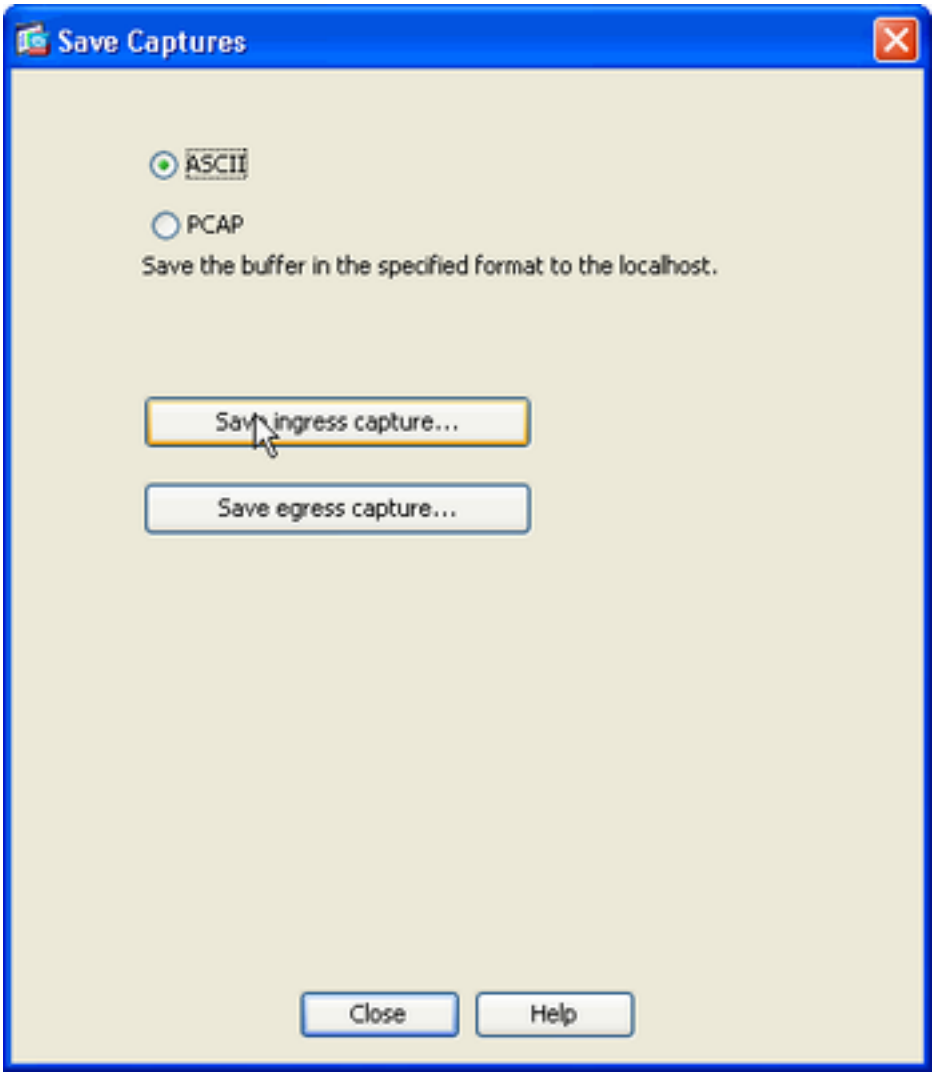


10.1 Na guia **Save captures** escolha o formato necessário no qual o buffer de captura deve ser salvo.

10.2 Este é **ASCII** ou **PCAP**. Clique no botão de opção ao lado dos nomes dos formatos.

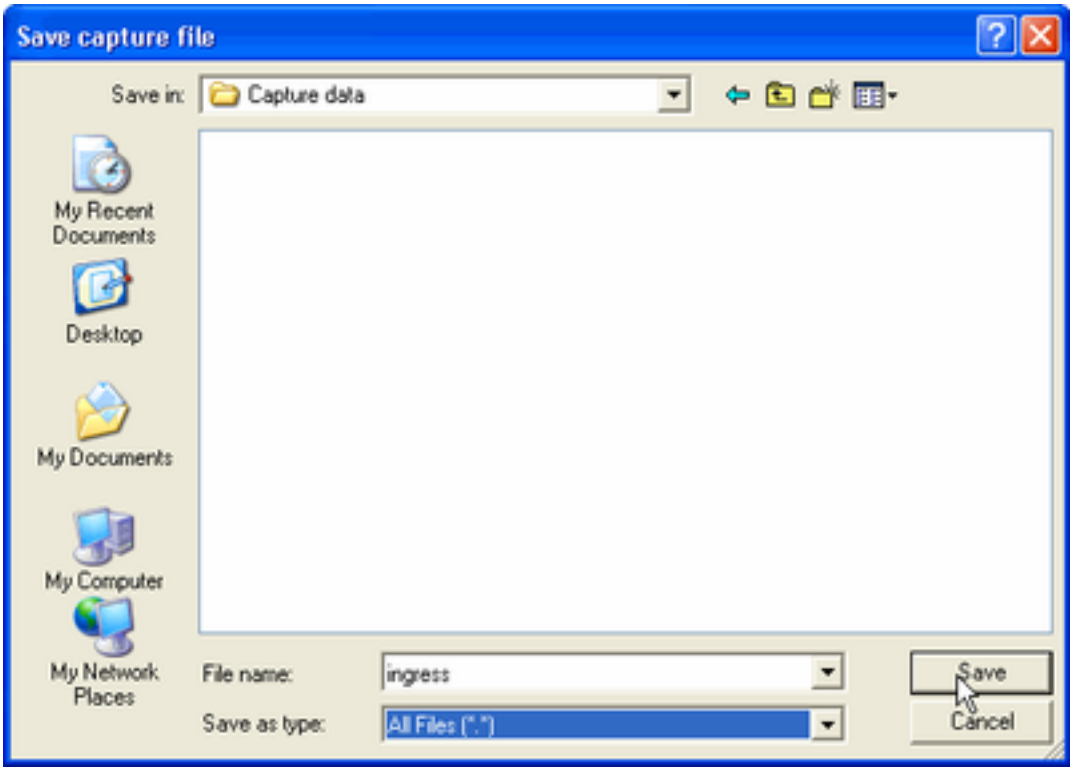
10.3 Em seguida, clique em **Save ingress capture** or **Save egress capture** conforme necessário.

Os arquivos PCAP podem ser abertos com analisadores de captura, como **Wireshark**e é o método preferido.

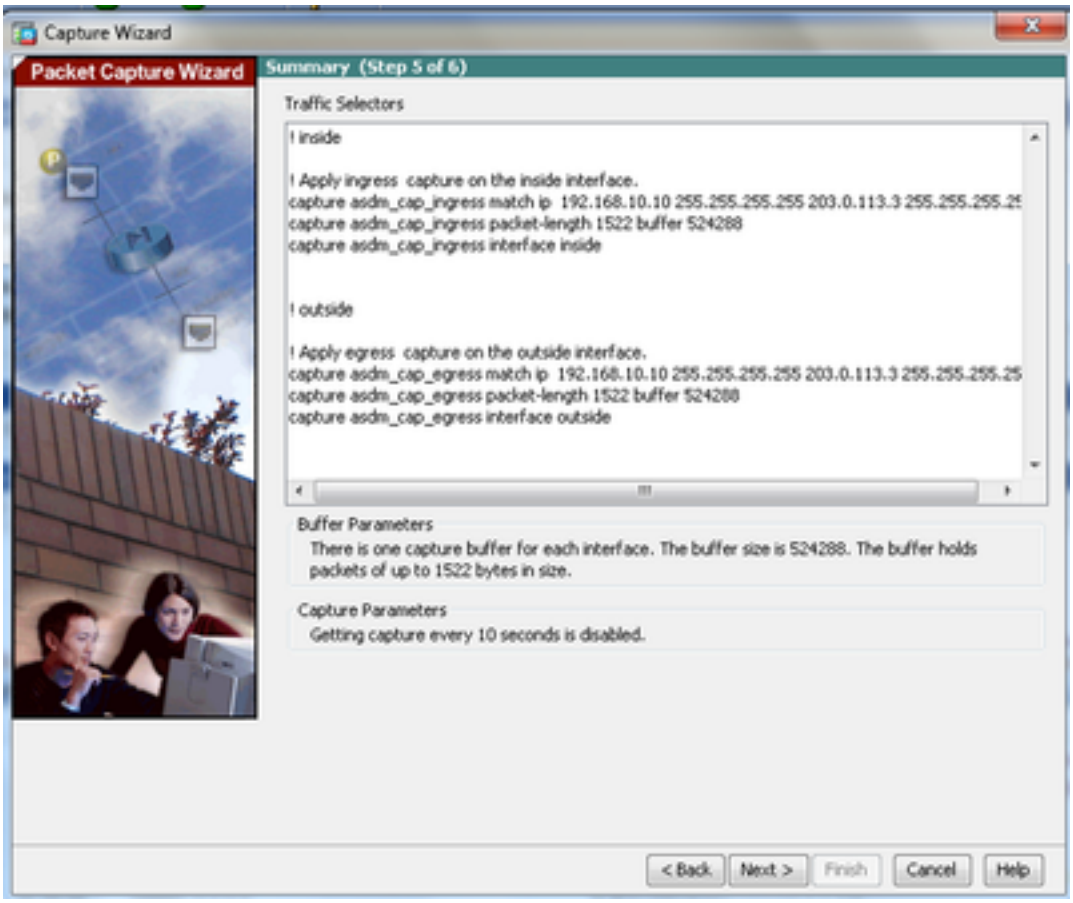


11.1 A partir da **Save capture file** forneça o nome do arquivo e o local em que o arquivo de captura deve ser salvo.

11.2 Clique em **Save**.



12. Clique em **Finish**.



Isso conclui o procedimento de captura de pacotes da GUI.

Configurar a captura de pacotes com o CLI

Conclua estes passos para configurar o recurso de captura de pacotes no ASA com a CLI:

1. Configure as interfaces interna e externa conforme ilustrado no diagrama de rede com o endereço IP e os níveis de segurança corretos.

2. Inicie o processo de captura de pacotes com o comando capture no modo EXEC privilegiado. Neste exemplo de configuração, a captura chamada **capin** é definida. Vincule-o à interface **interna** e especifique, com a palavra-chave **match**, que somente os pacotes correspondentes ao tráfego de interesse sejam capturados:

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

3. Da mesma forma, a captura chamada **capout** é definida. Vincule-o à interface **externa** e especifique, com a palavra-chave **match**, que somente os pacotes correspondentes ao tráfego de interesse sejam capturados:

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

   O ASA agora começa a capturar o fluxo de tráfego entre as interfaces. Para interromper a captura a qualquer momento, insira o comando no capture seguido do nome da captura.

   Aqui está um exemplo:

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

Tipos de captura disponíveis no ASA

Esta seção descreve os diferentes tipos de capturas disponíveis no ASA.

- **asa_dataplane** - Captura pacotes no painel traseiro do ASA que passam entre o ASA e um módulo que usa o painel traseiro, como o ASA CX ou o módulo IPS.

```
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 - Captura pacotes que são descartados pelo caminho de segurança acelerado. O código de queda especifica o tipo de tráfego que é descartado pelo caminho de segurança acelerado.

```
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 - Seleciona um tipo de Ethernet a ser capturado. Os tipos de Ethernet suportados incluem 8021Q, ARP, IP, IP6, LACP, PPPOED, PPPOES, RARP e VLAN.

  Este exemplo mostra como capturar o tráfego ARP:

```
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** Exibe os pacotes capturados continuamente em tempo real. Para encerrar uma captura de pacote em tempo real, pressione Ctrl-C. Para remover permanentemente a captura, use a forma no desse comando.
- Esta opção não é suportada quando você usa o comando **cluster exec capture** comando.

```
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** - Rastreia os pacotes capturados de maneira semelhante ao recurso de rastreador de pacotes ASA.

```
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
```

Note: No ASA 9.10+, a palavra-chave any captura apenas pacotes com endereços ipv4. A palavra-chave any6 captura todo o tráfego endereçado ipv6.

Essas são configurações avançadas que podem ser configuradas com Capturas de pacotes.

Leia o guia de referência de comandos para saber como defini-los.

- **ikev1/ikev2** - Captura somente informações de protocolo IKEv1 ou IKEv2.
- **isakmp** - Captura o tráfego ISAKMP (Internet Security Association and Key Management Protocol) para conexões VPN. O subsistema ISAKMP não tem acesso aos protocolos das camadas superiores. A captura é uma pseudo captura, com as camadas física, IP e UDP combinadas para satisfazer um analisador PCAP. Os endereços de peer são obtidos do intercâmbio SA e são armazenados na camada IP.
- **lacp** - Captura o tráfego do LACP (Link Aggregation Control Protocol). Se configurado, o nome da interface é o nome da interface física. Isso é útil quando você trabalha com Etherchannels para identificar o comportamento atual do LACP.
- **tls-proxy** - Captura dados de entrada e saída descriptografados do proxy TLS (Transport Layer Security) em uma ou mais interfaces.
- **webvpn** - Captura dados WebVPN para uma conexão WebVPN específica.

  Caution: Quando você habilita a captura WebVPN, ela afeta o desempenho do Security Appliance. Certifique-se de desabilitar a captura depois de gerar os arquivos de captura necessários para solucionar problemas.

Defaults

Estes são os valores padrão do sistema ASA:

- O tipo padrão é raw-data.
- O tamanho de buffer padrão é 512 KB.
- O tipo de Ethernet padrão são pacotes IP.
- O comprimento padrão do pacote é de 1.518 bytes.

Exibir os pacotes capturados

No ASA

Para visualizar os pacotes capturados, insira o comando show capture seguido do nome da captura. Esta seção fornece as saídas do comando **show** do conteúdo do buffer de captura. O

show capture capin mostra o conteúdo do buffer de captura chamado **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
```

O **show capture capout** mostra o conteúdo do buffer de captura chamado **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
```

Download do ASA para análise off-line

Há algumas maneiras de baixar as capturas de pacotes para análise off-line:

1. Navegue até https://<ip_of_asa>/admin/capture/<capture_name>/pcapem qualquer navegador.

   Tip: Se você deixar de fora o **pcap** palavra-chave, somente o equivalente do **show capture** é fornecida a saída do comando.

1. Insira o comando copy capture e o protocolo de transferência de arquivos preferencial para baixar a captura:

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

   Tip: Ao solucionar um problema com o uso de capturas de pacotes, a Cisco recomenda que você faça o download das capturas para análise off-line.

Limpar uma captura

Para limpar o buffer de captura, insira o comando **clear capture** comando:

```
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
```

Digite o **clear capture /all** para limpar o buffer de todas as capturas:

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

Parar uma captura

A única maneira de parar uma captura no ASA é desativá-la completamente com este comando:

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

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

No momento, não há informações específicas de solução de problemas disponíveis para essa configuração.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.