Configuración de capturas de paquetes ASA con CLI y ASDM

Contenido

Introducción

Este documento describe cómo configurar el firewall Cisco ASA para capturar los paquetes deseados con el ASDM o la CLI.

Prerequisites

Requirements

Este procedimiento supone que ASA está completamente operativo y está configurado para permitir que el Cisco ASDM o la CLI realicen cambios en la configuración.

Componentes Utilizados

Este documento no se limita a versiones específicas de hardware o 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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Productos Relacionados

Esta configuración también se utiliza con estos productos de Cisco:

- Cisco ASA versiones 9.1(5) y posteriores
- Cisco ASDM versión 7.2.1

Antecedentes

Este documento describe cómo configurar el **Cisco Adaptive Security Appliance (ASA) Next-Generation Firewall** para capturar los paquetes deseados con el **Cisco Adaptive Security Device Manager (ASDM)** o el **Command Line Interface (CLI) (ASDM).**

El proceso de captura de paquetes es útil para resolver problemas de conectividad o monitorear actividades sospechosas. Además, es posible crear capturas múltiples para analizar diferentes tipos de tráfico en interfaces múltiples.

Configurar

Esta sección proporciona información utilizada para configurar las funciones de captura de paquetes que se describen en este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Configuraciones

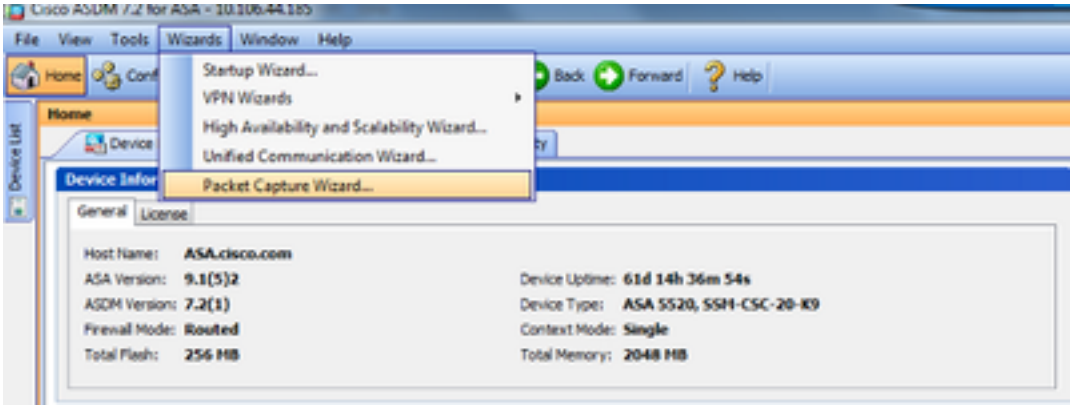
Los esquemas de dirección IP usados en esta configuración no son legalmente enrutables en Internet. Son direcciones RFC 1918 que se usan en un entorno de laboratorio.

Configuración de la captura de paquetes con el ASDM

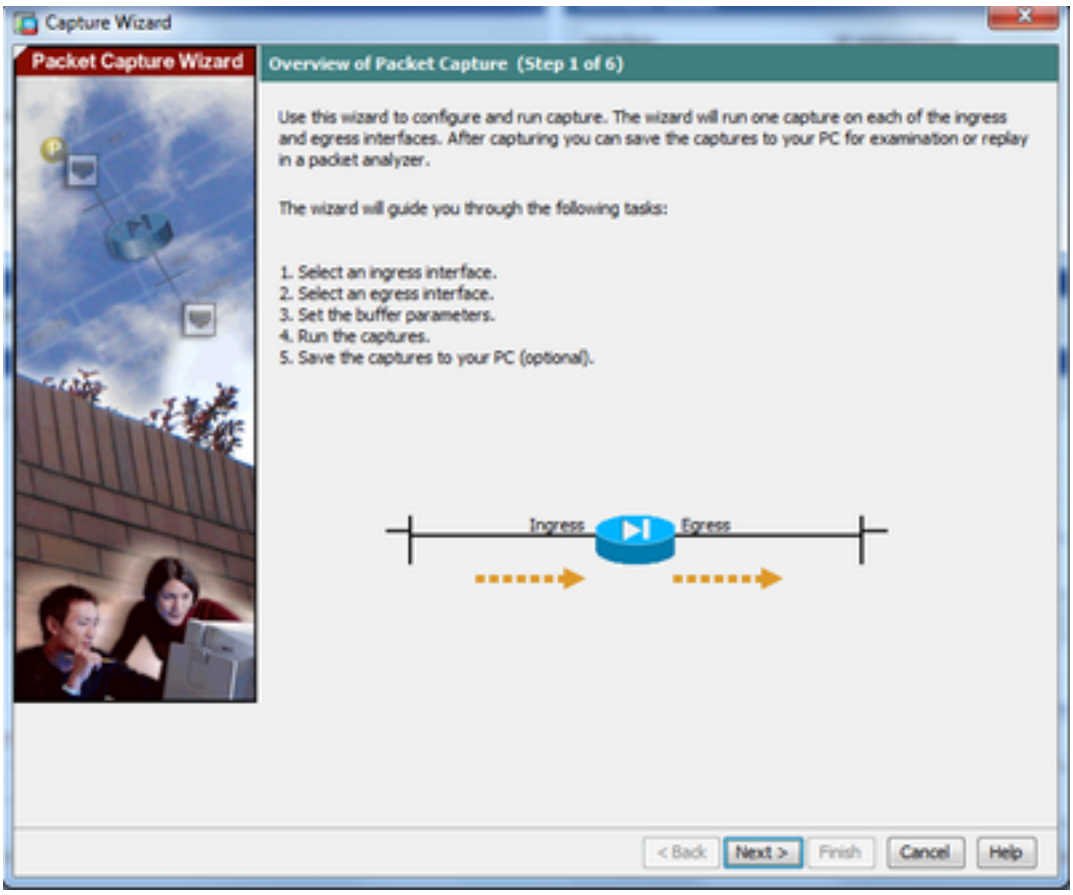
Este ejemplo de configuración se utiliza en para capturar los paquetes que se transmiten durante un ping de User1 (red interna) al Router1 (red externa).

Complete estos pasos para configurar la función de captura de paquetes en el ASA con el ASDM:

1. Acceda a **Wizards > Packet Capture Wizard** para iniciar la configuración de captura de paquetes, como se muestra:



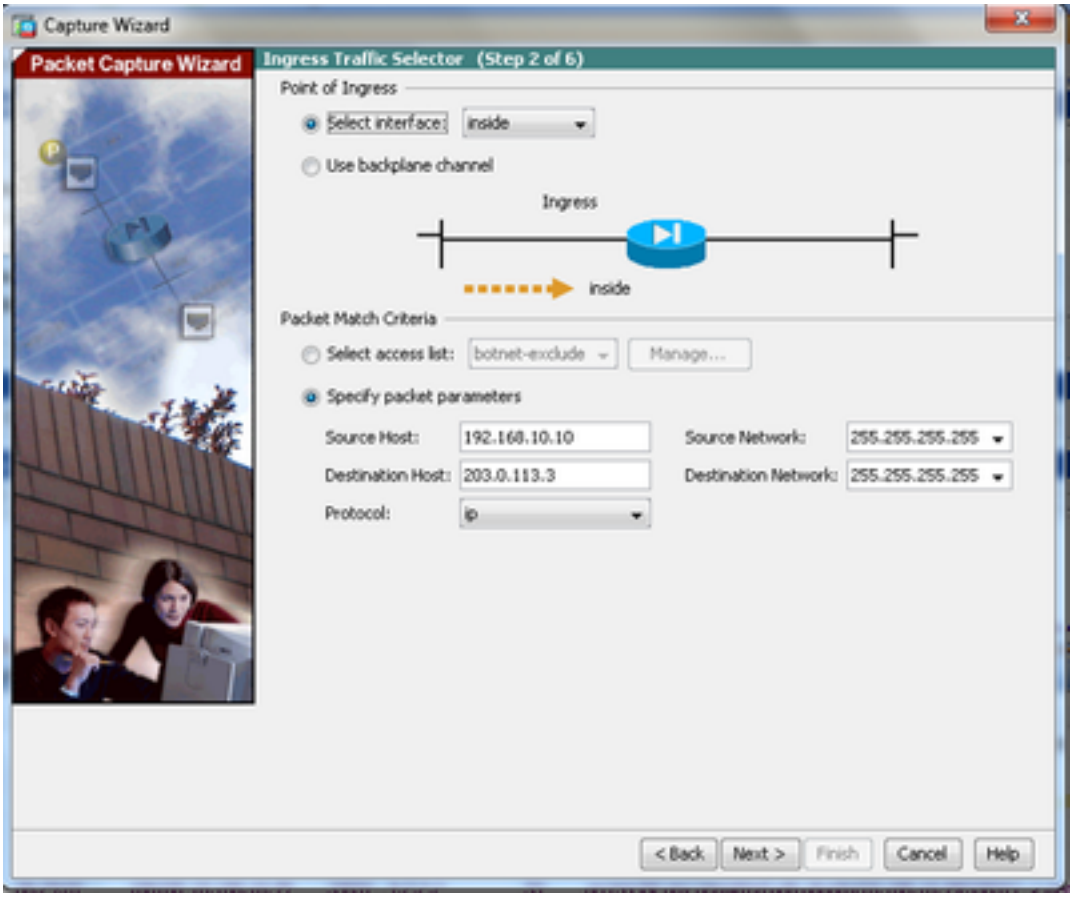
2. El **Capture Wizard** se abre. Haga clic **Next**.



3.0 En la nueva ventana, proporcione los parámetros que se utilizan en para capturar el tráfico de ingreso.

3.1 Selección **inside** para el **Ingress Interface** y proporcionar las direcciones IP de origen y destino de los paquetes que se van a capturar, junto con su máscara de subred, en el espacio respectivo proporcionado.

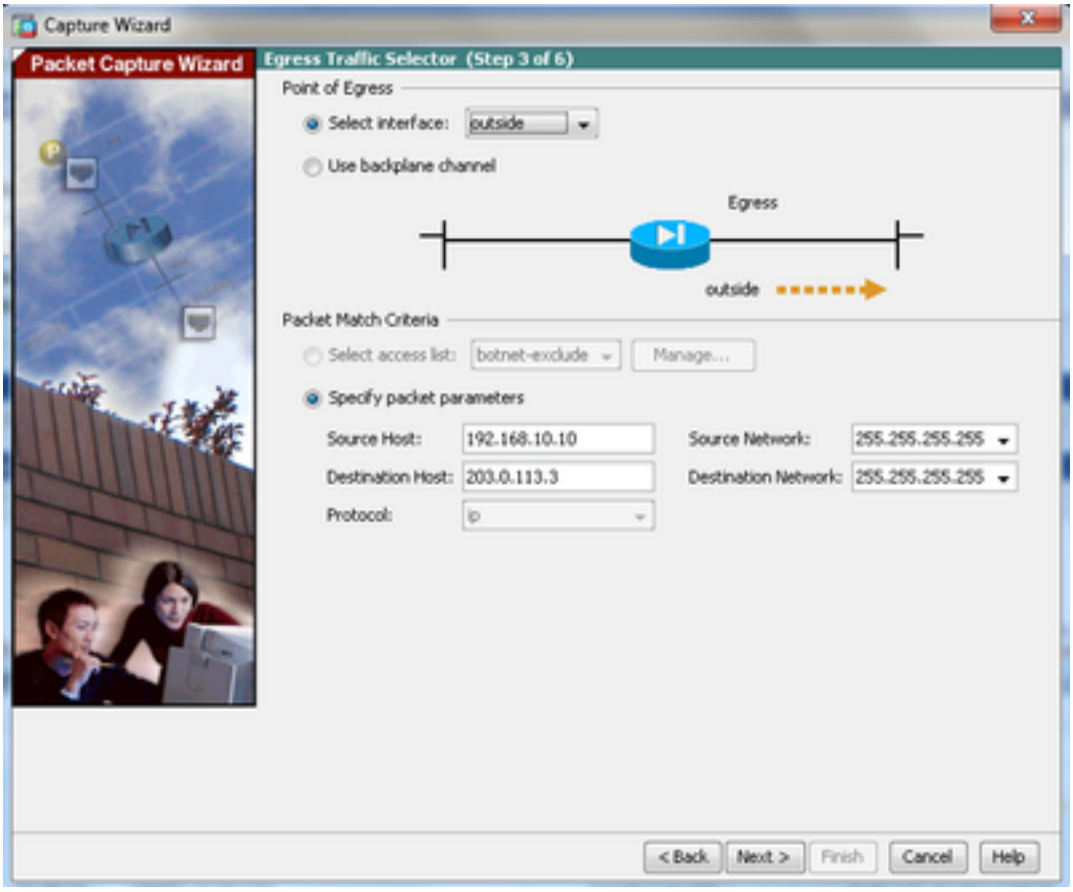
3.2 Elija el tipo de paquete que será capturado por el ASA (IP es el tipo de paquete elegido aquí), como se muestra:



3.3 Clic **Next.**

4.1 Selección **outside** para el **Egress Interface** y proporcionar las direcciones IP de origen y destino, junto con su máscara de subred, en los espacios respectivos proporcionados.

If Network Address Translation (NAT) se lleva a cabo en el firewall, tenga esto en cuenta también.



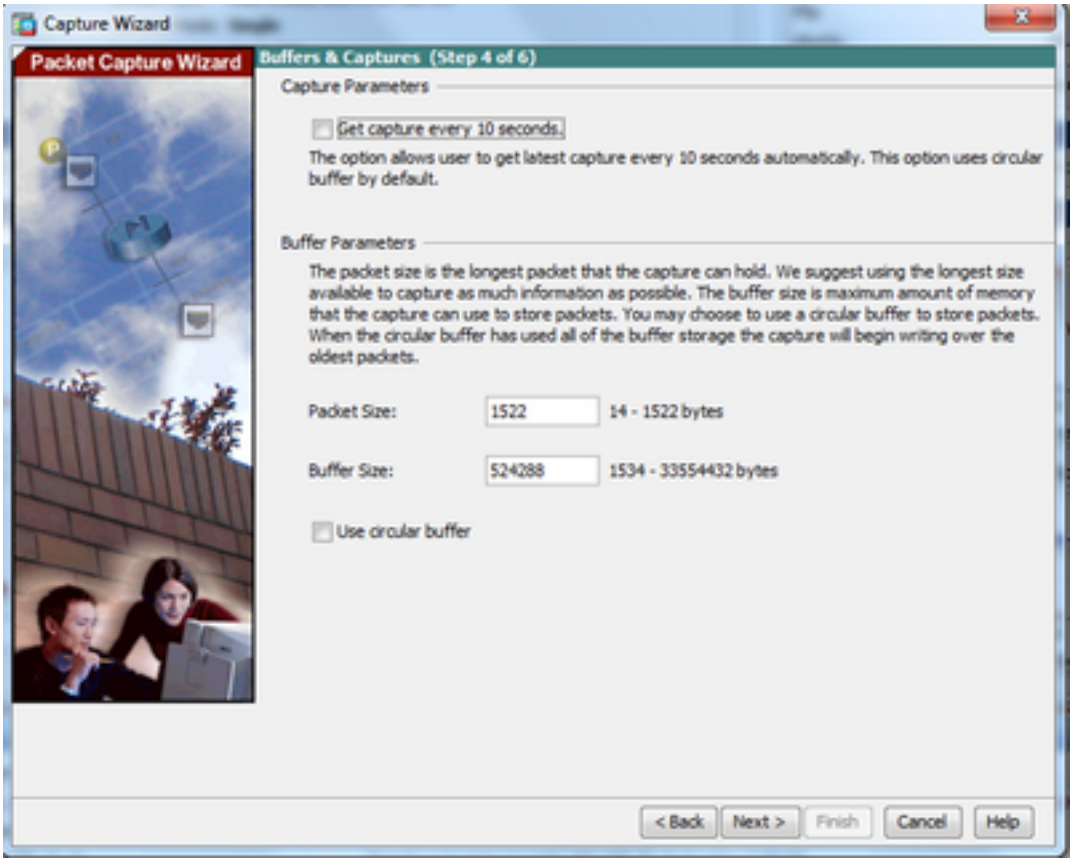
4.2 Haga clic en **Next**.

5.1 Introduzca la **Packet Size** y el **Buffer Size** en el espacio respectivo proporcionado. Estos datos son necesarios para que tenga lugar la captura.

5.2 Compruebe la **Use circular buffer** para utilizar la opción búfer circular. Las memorias intermedias circulares nunca se llenan.

A medida que el búfer alcanza su tamaño máximo, se descartan los datos más antiguos y continúa la captura.

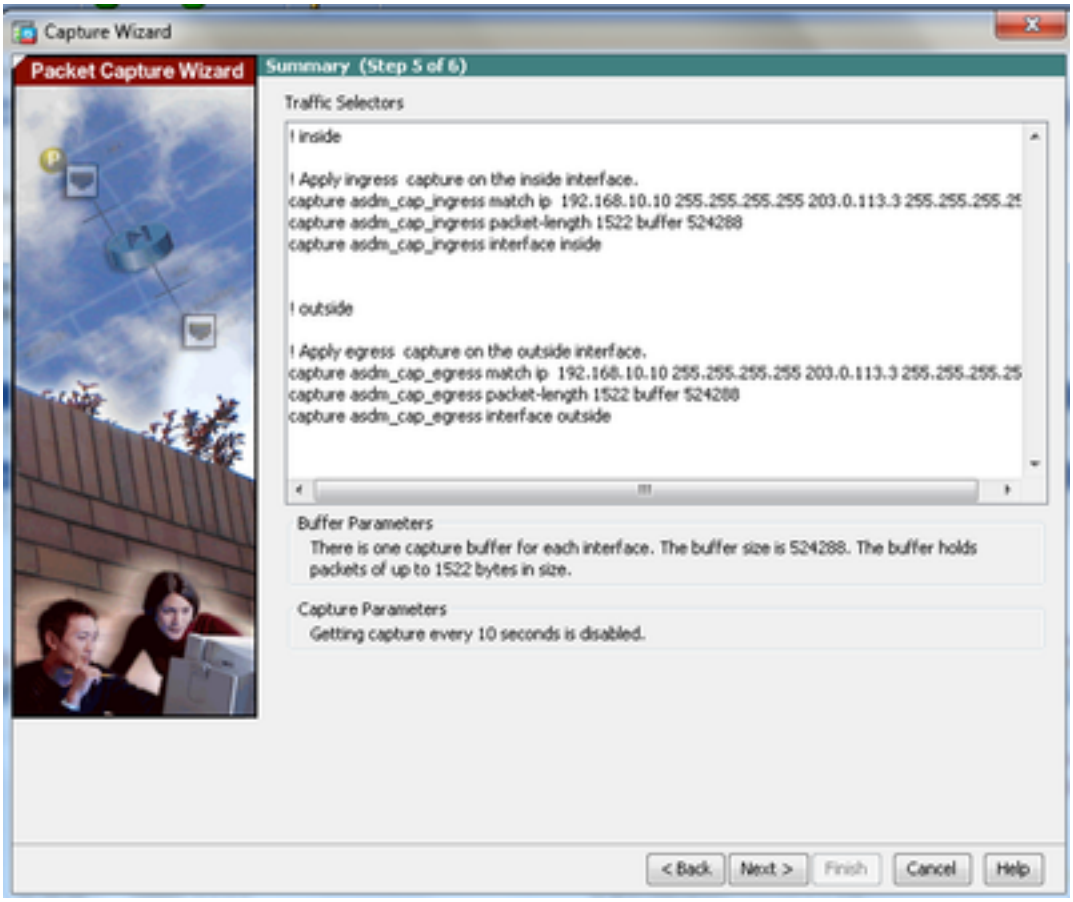
En este ejemplo, no se utiliza búfer circular, por lo que la casilla de verificación no está activada.



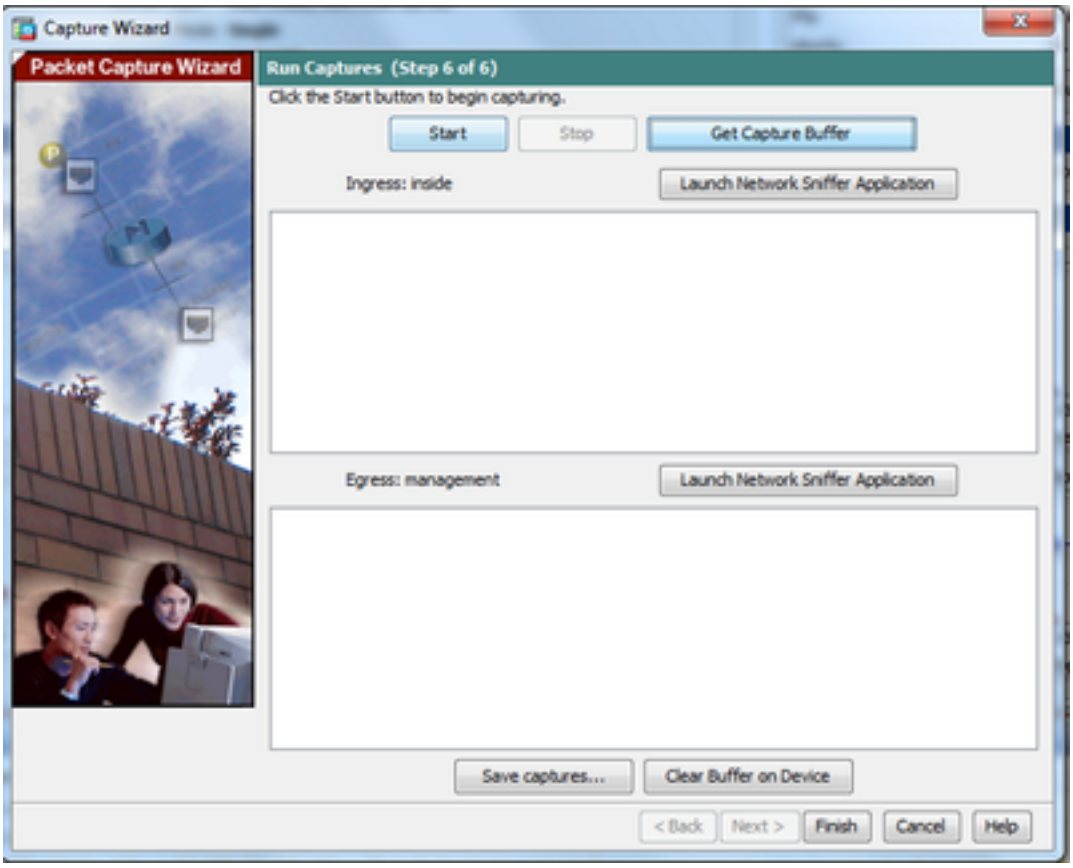
5.3 Clic **Next**.

6.0 Esta ventana muestra el **Access-lists** que se deben configurar en el ASA (para que se capturen los paquetes deseados) y el tipo de paquetes que se van a capturar (los paquetes IP se capturan en este ejemplo).

6.1 Clic **Next**.

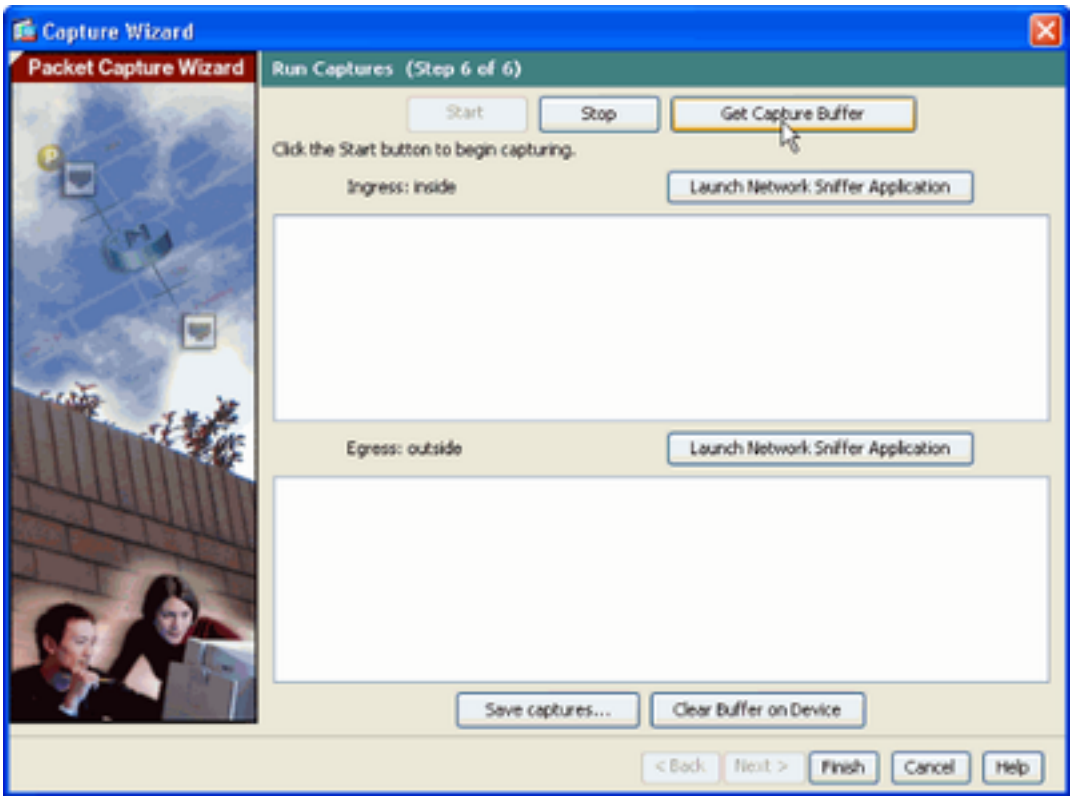


7. Haga clic en **Start** para iniciar la captura de paquetes, como se muestra:



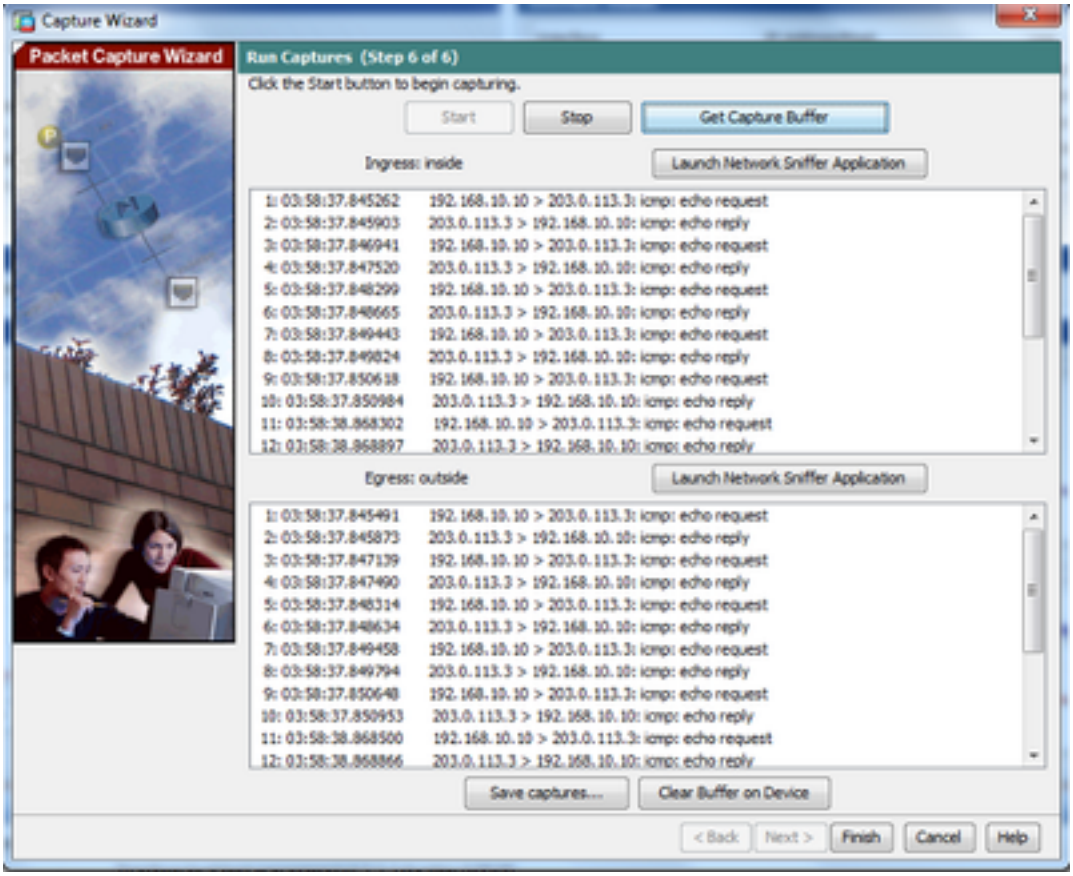
A medida que se inicia la captura de paquetes, intente hacer ping a la red externa desde la red interna para que los paquetes que fluyen entre las direcciones IP de origen y destino sean capturados por el búfer de captura de ASA.

8. Haga clic en **Get Capture Buffer** para ver los paquetes que son capturados por el buffer de captura ASA.



Los paquetes capturados se muestran en esta ventana para el tráfico de ingreso y egreso.

9. Haga clic en **Save captures** para guardar la información de captura.



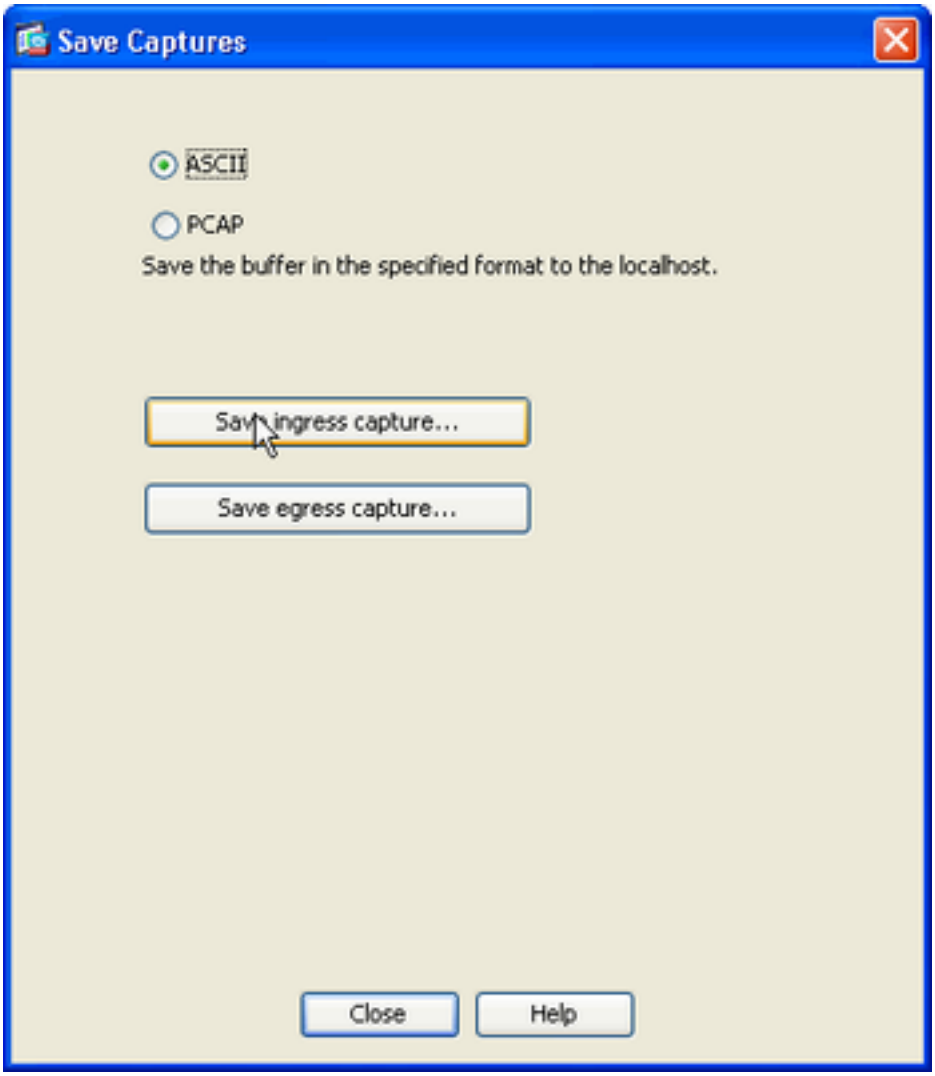
10.1 Desde el **Save captures** seleccione el formato necesario en el que se guardará el búfer de

captura.

10.2 Esto es **ASCII** o **PCAP**. Haga clic en el botón de opción situado junto a los nombres de formato.

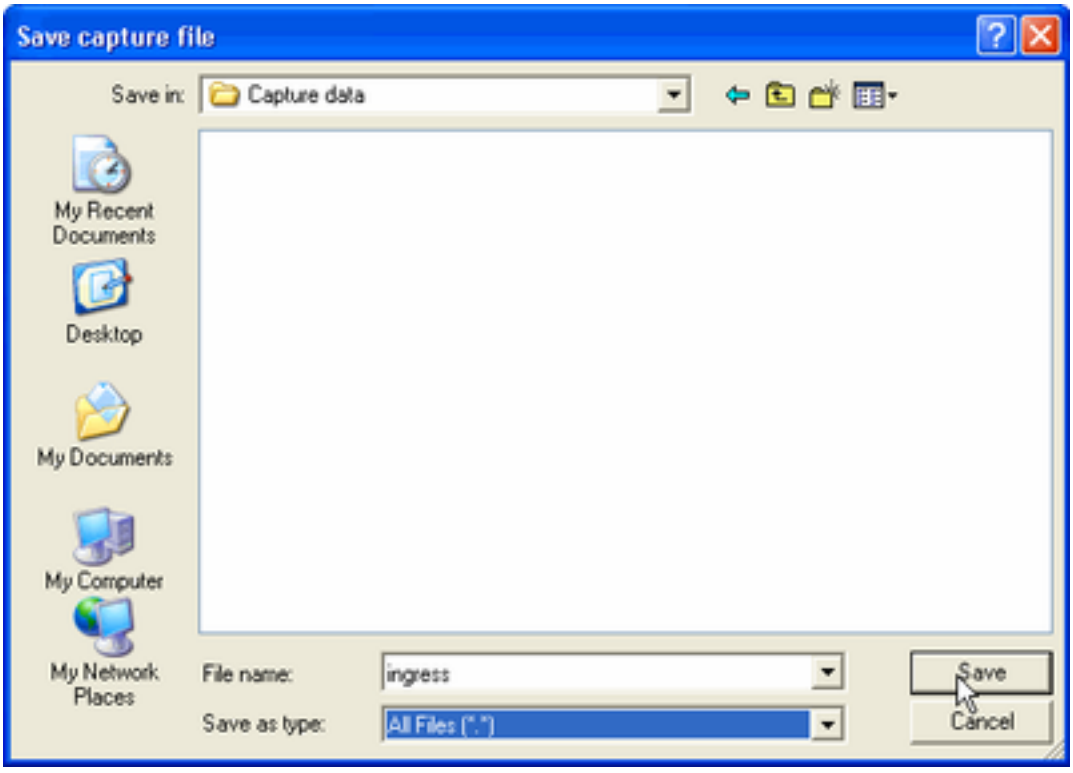
10.3 A continuación, haga clic en **Save ingress capture** or **Save egress capture** según sea necesario.

Los archivos PCAP se pueden abrir con analizadores de captura, como **Wireshark**y es el método preferido.

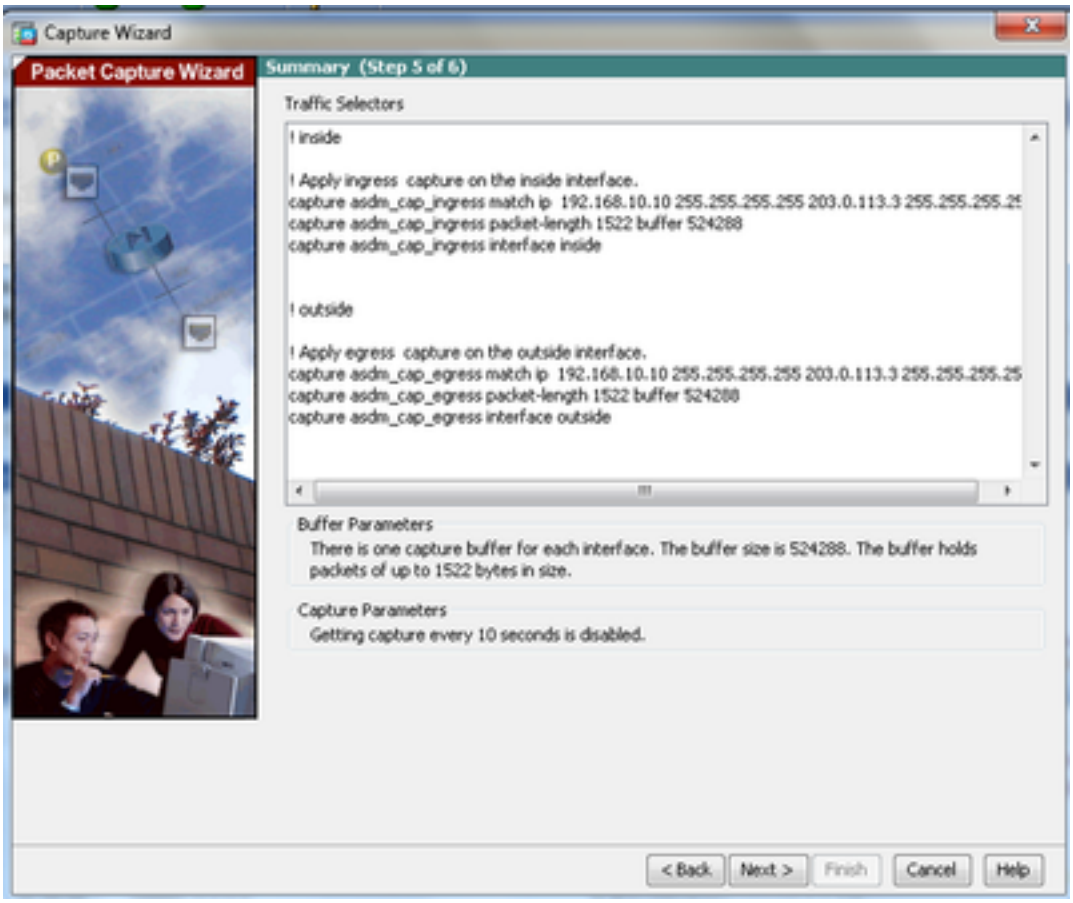


11.1 Desde el **Save capture file** , proporcione el nombre de archivo y la ubicación en la que se guardará el archivo de captura.

11.2 Haga clic en **Save**.



12. Haga clic en **Finish**.



Esto completa el procedimiento de captura de paquetes GUI.

Configuración de la captura de paquetes con la CLI

Complete estos pasos para configurar la función de captura de paquetes en el ASA con la CLI:

1. Configure las interfaces internas y externas como se muestra en el diagrama de red con la dirección IP y los niveles de seguridad correctos.

2. Inicie el proceso de captura de paquetes con el comando capture en el modo EXEC privilegiado. En este ejemplo de configuración, se define la captura denominada **capin**. Enlazarlo a la interfaz **inside** y especificar con la palabra clave **match** que sólo se capturan los paquetes que coinciden con el tráfico de interés:

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

3. De manera similar, se define la captura denominada **capout**. Enlaza el paquete a la interfaz **externa** y especifica con la palabra clave **match** que sólo se capturan los paquetes que coinciden con el tráfico de interés:

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

   ASA ahora comienza a capturar el flujo de tráfico entre las interfaces. Para detener la captura en cualquier momento, ingrese el comando no capture seguido del nombre de la captura.

   Aquí tiene un ejemplo:

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

Tipos de capturas disponibles en ASA

Esta sección describe los diferentes tipos de capturas que están disponibles en ASA.

- **asa_dataplane** - Captura paquetes en la placa posterior ASA que pasan entre ASA y un módulo que utiliza la placa posterior, como ASA CX o el 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 los paquetes que son descartados por la trayectoria de seguridad acelerada. El código de acceso especifica el tipo de tráfico que descarta la ruta de seguridad acelerada.

```
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: selecciona el tipo de Ethernet que se desea capturar. Los tipos de Ethernet compatibles incluyen 8021Q, ARP, IP, IP6, LACP, PPPOED, PPPOES, RARP y VLAN.

  Este ejemplo muestra cómo capturar el tráfico 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** - Muestra los paquetes capturados continuamente en tiempo real. Para terminar una captura de paquetes en tiempo real, presione Ctrl-C. Para eliminar permanentemente la captura, utilice la forma no de este comando.
- Esta opción no se admite cuando se utiliza el **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** - Rastrea los paquetes capturados de una manera similar a la función de seguimiento de paquetes 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
```

> **Nota:** En ASA 9.10+, la palabra clave any solo captura paquetes con direcciones ipv4. La palabra clave any6 captura todo el tráfico con dirección ipv6.

Estos son ajustes avanzados que se pueden configurar con Capturas de paquetes.

Revise la guía de referencia de comandos sobre cómo configurarlos.

- **ikev1/ikev2** - Captura sólo información del protocolo de intercambio de claves de Internet versión 1 (IKEv1) o IKEv2.

- **isakmp** - Captura el tráfico de la Asociación de seguridad de Internet y del Protocolo de administración de claves (ISAKMP) para las conexiones VPN. El subsistema ISAKMP no tiene acceso a los protocolos de capa superior. La captura es una pseudo captura, con las capas físicas, IP y UDP combinadas para satisfacer un analizador PCAP. Las direcciones de peer se obtienen del intercambio SA y se almacenan en la capa IP.

- **lacp** - Captura el tráfico del protocolo de control de agregación de enlaces (LACP). Si se configura, el nombre de la interfaz es el nombre de la interfaz física. Esto es útil cuando se trabaja con Etherchannels para identificar el comportamiento actual de LACP.

- **tls-proxy** - Captura datos entrantes y salientes descifrados del proxy de seguridad de la capa de transporte (TLS) en una o más interfaces.

- **webvpn** - Captura los datos de WebVPN para una conexión WebVPN específica.

  > **Precaución:** Cuando habilita la captura WebVPN, afecta el rendimiento del dispositivo de seguridad. Asegúrese de inhabilitar la captura después de generar los archivos de captura que se necesitan para resolver problemas.

Valores predeterminados

Estos son los valores predeterminados del sistema ASA:

- El tipo predeterminado es raw-data.
- El tamaño predeterminado del búfer es de 512 KB.
- El tipo de Ethernet predeterminado es paquetes IP.
- La longitud de paquete predeterminada es de 1.518 bytes.

Ver los paquetes capturados

En ASA

Para ver los paquetes capturados, ingrese el comando show capture seguido del nombre de la captura. Esta sección proporciona los resultados del comando **show** del contenido del buffer de captura. **show capture capin** muestra el contenido del búfer de captura denominado **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
```

show capture capout muestra el contenido del búfer de captura denominado **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
```

Descarga desde ASA para análisis sin conexión

Hay un par de maneras de descargar las capturas de paquetes para su análisis sin conexión:

1. Vaya a https://<ip_of_asa>/admin/capture/<capture_name>/pcapen cualquier navegador.

   Consejo: Si deja fuera la **pcap** , sólo el equivalente de la palabra clave **show capture** se proporciona el resultado del comando.

1. Ingrese el comando copy capture y su protocolo de transferencia de archivos preferido para descargar la captura:

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

   Consejo: Cuando resuelva un problema con el uso de capturas de paquetes, Cisco recomienda que descargue las capturas para el análisis sin conexión.

Borrar una captura

Para borrar el buffer de captura, ingrese el **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
```

Escriba el **clear capture /all** para borrar el buffer para todas las capturas:

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

Detener una captura

La única manera de detener una captura en el ASA es desactivarla completamente con este comando:

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

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente no hay información de troubleshooting específica disponible para esta configuración.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).