Konfigurieren von ASA-Paketerfassungen mit CLI und ASDM

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die Cisco ASA-Firewall so konfigurieren, dass die gewünschten Pakete mit dem ASDM oder der CLI erfasst werden.

Voraussetzungen

Anforderungen

Bei diesem Verfahren wird davon ausgegangen, dass die ASA voll funktionsfähig ist und konfiguriert wurde, damit der Cisco ASDM oder die CLI Konfigurationsänderungen vornehmen können.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Hardware- oder Softwareversionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer

gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Verwandte Produkte

Diese Konfiguration kommt auch bei folgenden Cisco Produkten zum Einsatz:

- Cisco ASA Version 9.1(5) und höher
- Cisco ASDM Version 7.2.1

Hintergrundinformationen

In diesem Dokument wird die Konfiguration des **Cisco Adaptive Security Appliance (ASA) Next-Generation Firewall** um die gewünschten Pakete entweder mit dem **Cisco Adaptive Security Device Manager (ASDM)** oder **Command Line Interface (CLI) (ASDM)**.

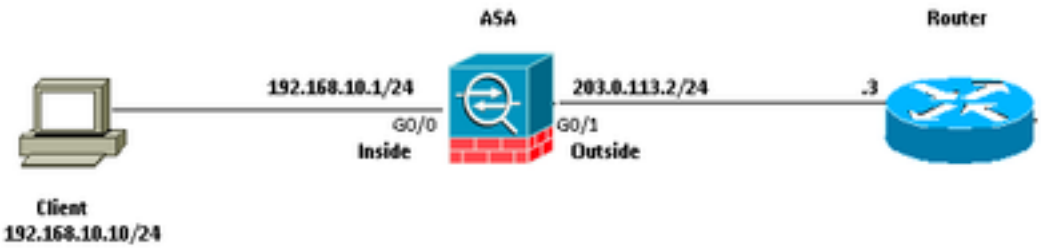
Der Paketerfassungsprozess ist nützlich, um Verbindungsprobleme zu beheben oder verdächtige Aktivitäten zu überwachen. Darüber hinaus ist es möglich, mehrere Erfassungen zu erstellen, um verschiedene Arten von Datenverkehr an mehreren Schnittstellen zu analysieren.

Konfigurieren

Dieser Abschnitt enthält Informationen zur Konfiguration der in diesem Dokument beschriebenen Paketerfassungsfunktionen.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

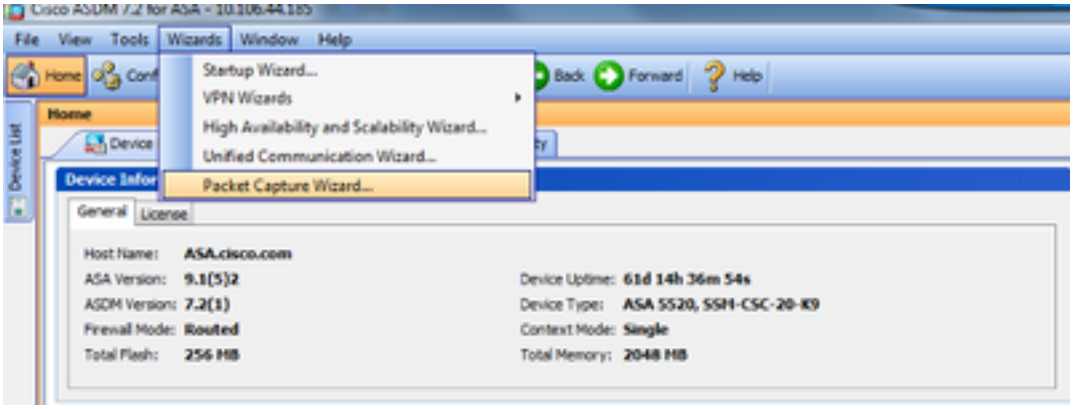
Die in dieser Konfiguration verwendeten IP-Adressschemata können nicht legal im Internet geroutet werden. Es handelt sich um RFC 1918-Adressen, die in Laborumgebungen verwendet werden.

Konfigurieren der Paketerfassung mit dem ASDM

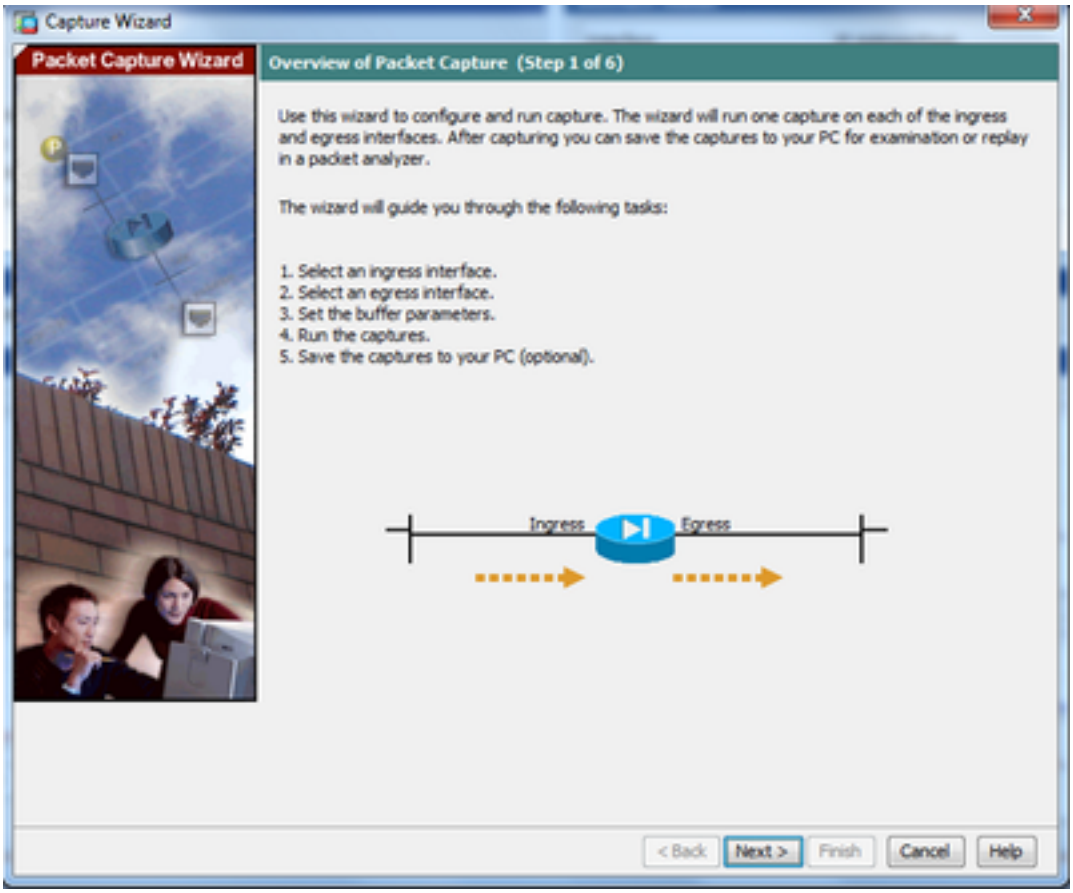
Diese Beispielkonfiguration wird in verwendet, um die Pakete zu erfassen, die während eines Pings von User1 (innerhalb des Netzwerks) an Router1 (außerhalb des Netzwerks) übertragen werden.

Gehen Sie wie folgt vor, um die Paketerfassungsfunktion auf der ASA mit dem ASDM zu konfigurieren:

1. Navigieren Sie zu **Wizards > Packet Capture Wizard** um die Konfiguration der Paketerfassung zu starten, wie dargestellt:



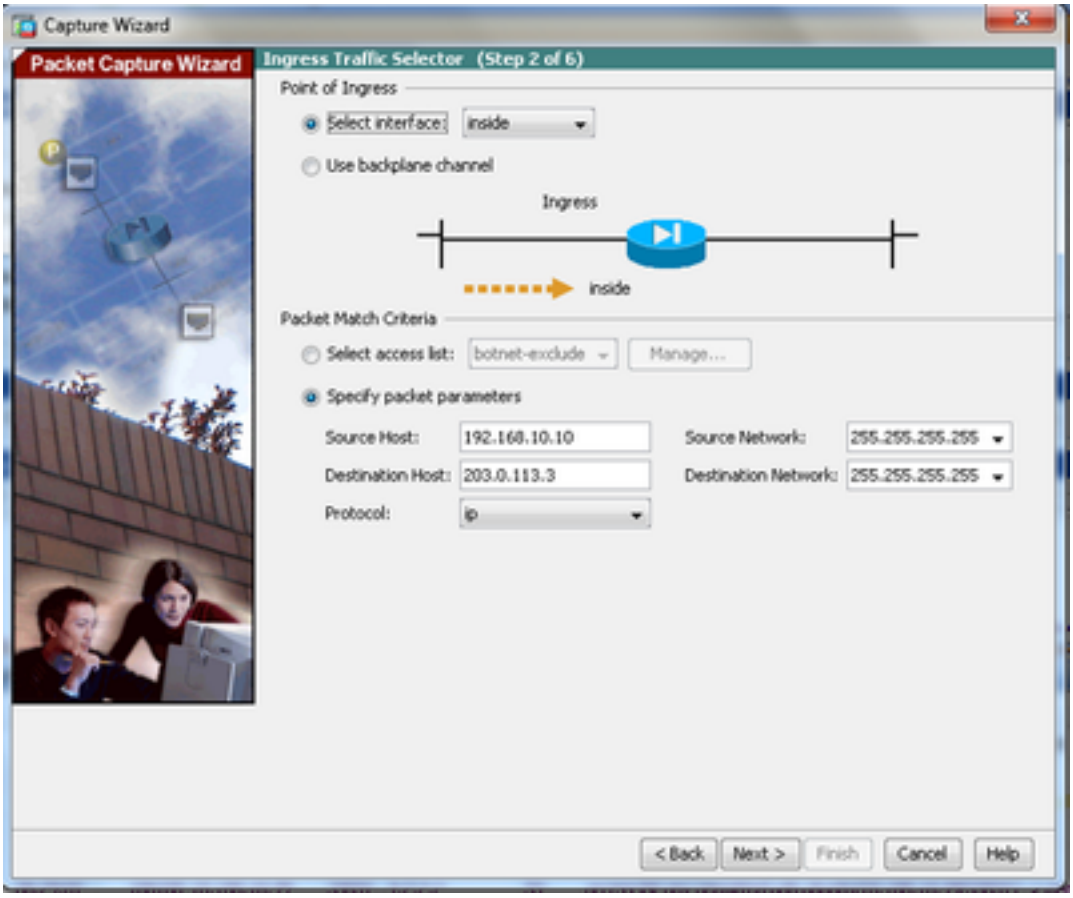
2. Die **Capture Wizard** öffnet. Klicken Sie auf **Next**.



3.0 Geben Sie im neuen Fenster die Parameter an, die zur Erfassung des eingehenden Datenverkehrs verwendet werden.

3.1 Auswahl **inside** für die **Ingress Interface** und geben die Quell- und Ziel-IP-Adressen der zu erfassenden Pakete zusammen mit ihrer Subnetzmaske in dem jeweiligen dafür vorgesehenen Raum an.

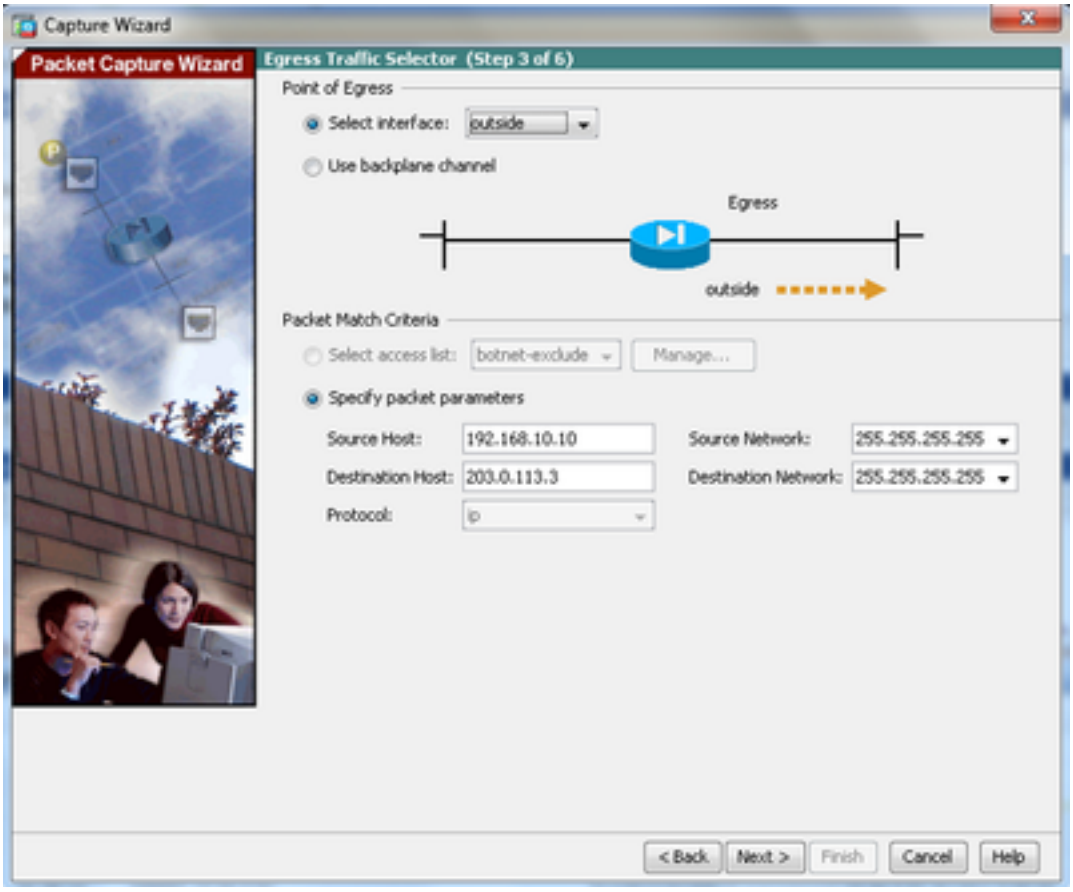
3.2 Wählen Sie den von der ASA zu erfassenden Pakettyp aus (IP ist der hier ausgewählte Pakettyp), wie dargestellt:



3.3 Klicken Sie auf **Next**.

4.1 Auswahl **outside** für die **Egress Interface** und geben die Quell- und Ziel-IP-Adressen zusammen mit ihrer Subnetzmaske in den jeweiligen vorgesehenen Bereichen an.

If Network Address Translation (NAT) auf der Firewall ausgeführt wird, berücksichtigen Sie dies ebenfalls.



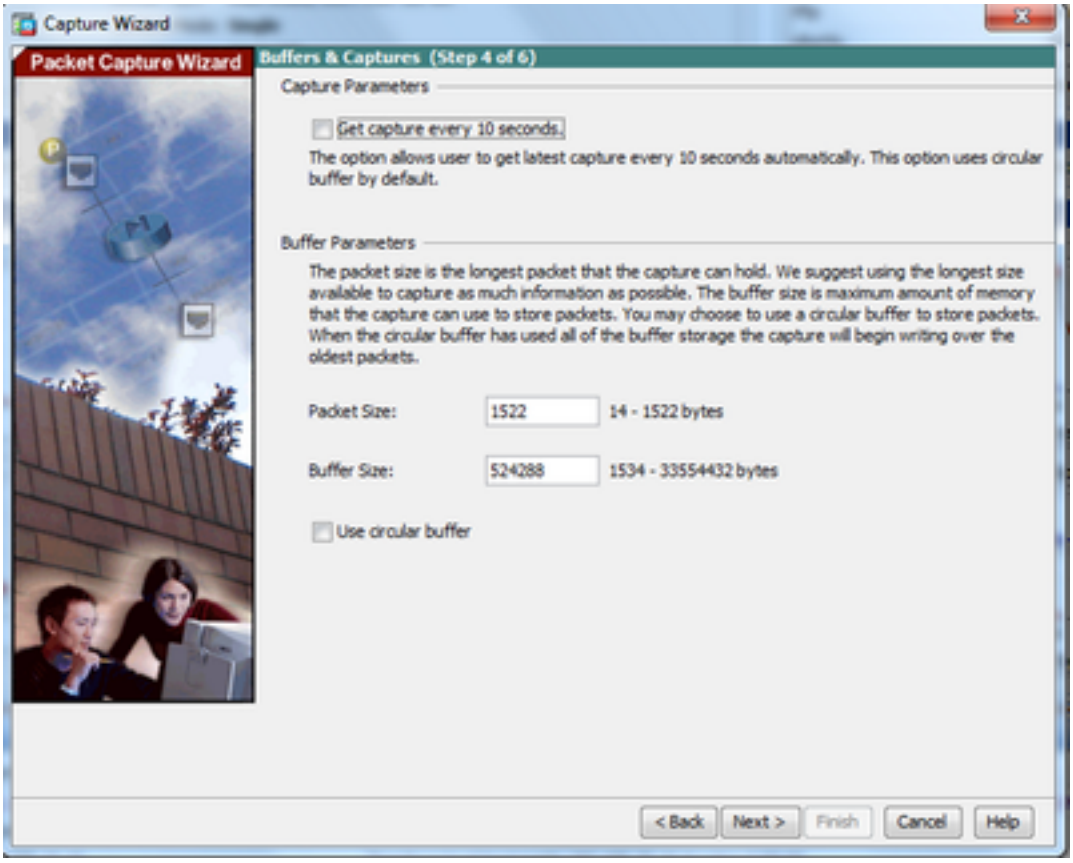
4.2 Klicken Sie auf **Next**.

5.1 Geben Sie die entsprechenden **Packet Size** und **Buffer Size** in dem jeweiligen vorgesehenen Raum. Diese Daten sind für die Erfassung erforderlich.

5.2 Überprüfen Sie die **Use circular buffer** um die Option "Ringpuffer" zu verwenden. Kreisförmige Puffer füllen sich nie.

Wenn der Puffer seine maximale Größe erreicht, werden ältere Daten verworfen und die Erfassung wird fortgesetzt.

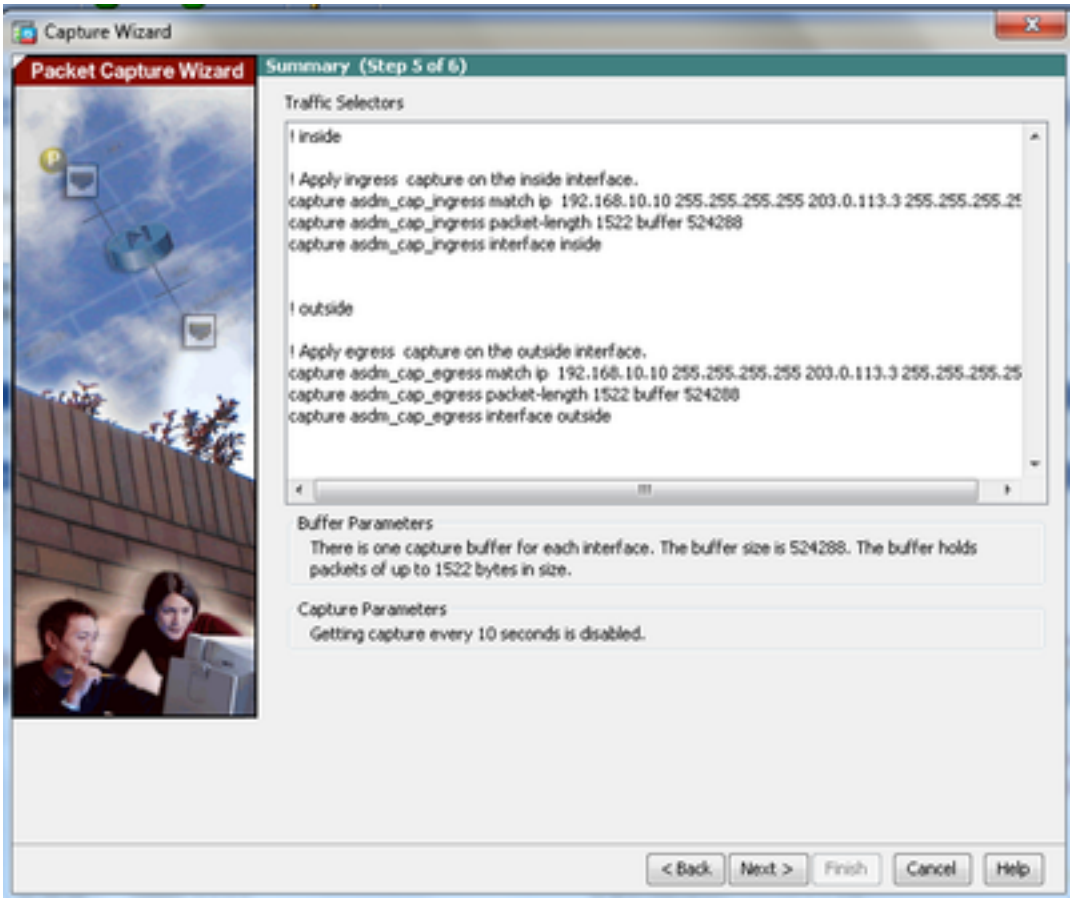
In diesem Beispiel wird kein zirkulärer Puffer verwendet, daher ist das Kontrollkästchen nicht aktiviert.



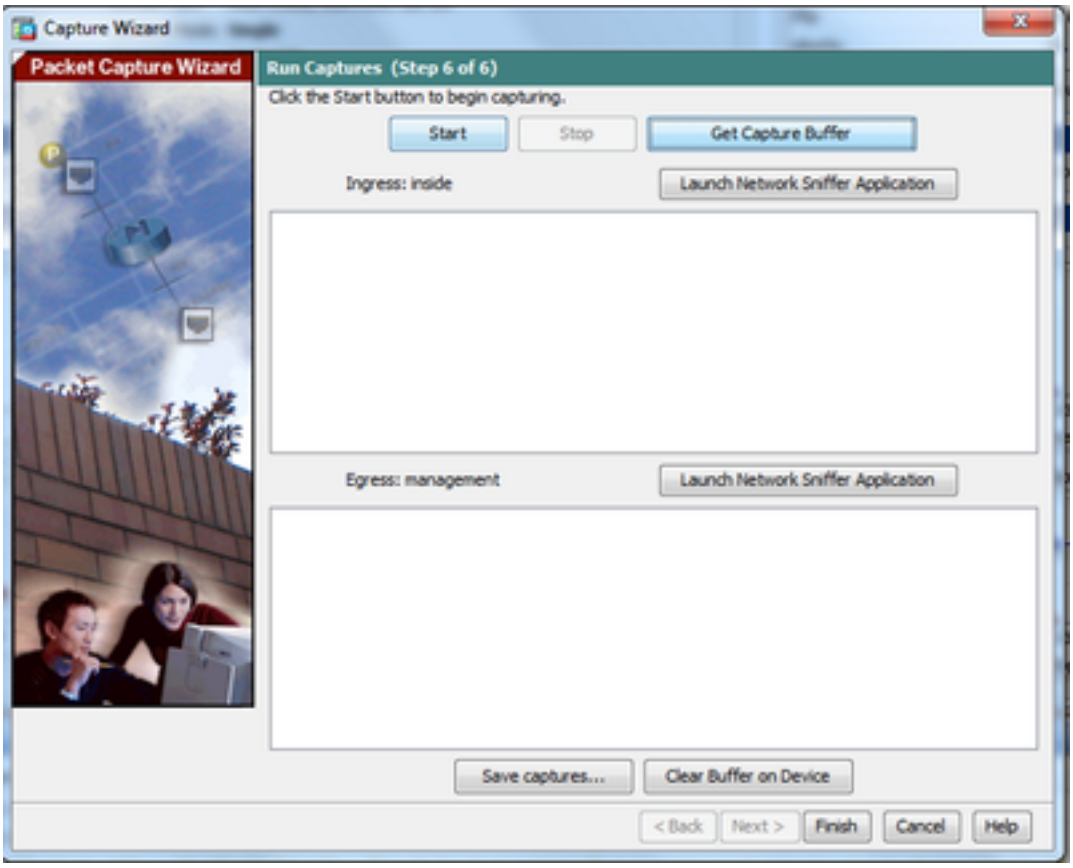
5.3 Klicken Sie auf **Next**.

6.0 Dieses Fenster zeigt **Access-lists** die auf der ASA konfiguriert werden müssen (damit die gewünschten Pakete erfasst werden) und welche Art von Paketen erfasst werden sollen (IP-Pakete werden in diesem Beispiel erfasst).

6.1 Klicken Sie auf **Next**.

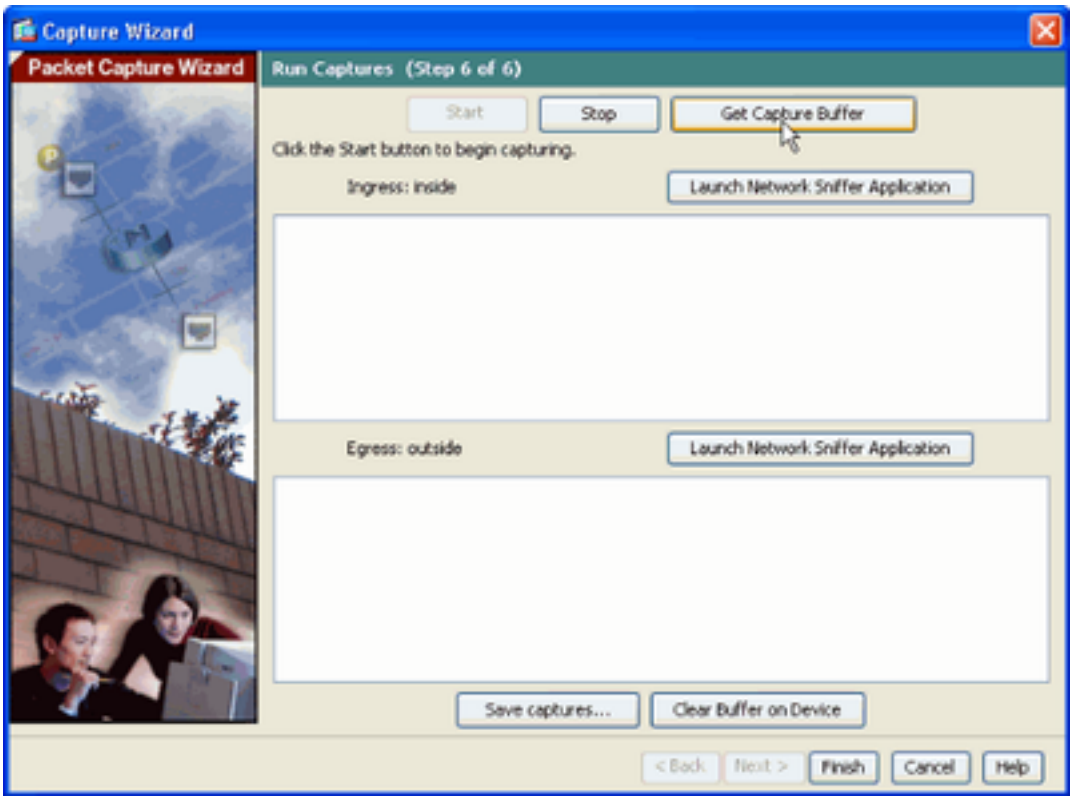


7. Klicken Sie **Start** um die Paketerfassung zu starten, wie dargestellt:



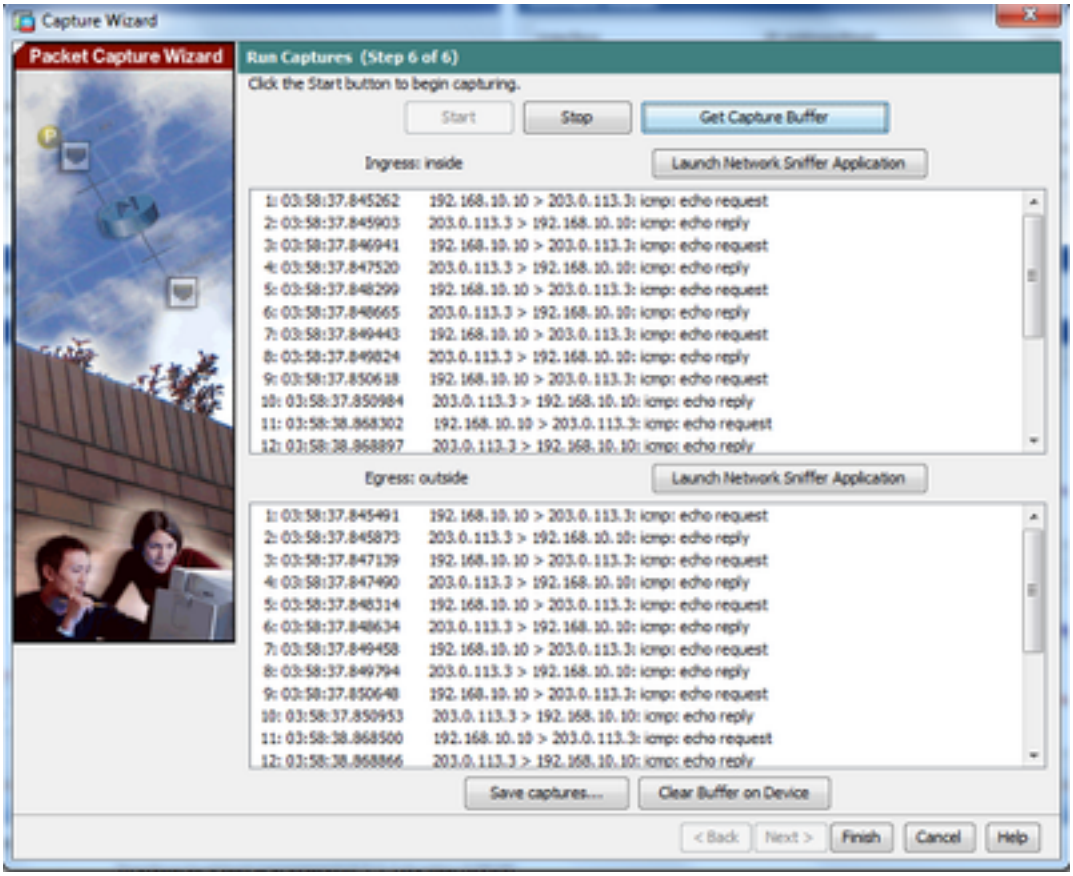
Versuchen Sie beim Start der Paketerfassung, einen Ping an das externe Netzwerk im internen Netzwerk zu senden, damit die Pakete, die zwischen der Quell- und der Ziel-IP-Adresse übertragen werden, vom ASA-Erfassungspuffer erfasst werden.

8. Klicken Sie auf **Get Capture Buffer** um die vom ASA-Erfassungspuffer erfassten Pakete anzuzeigen.



In diesem Fenster werden die erfassten Pakete für den Eingangs- und Ausgangsverkehr angezeigt.

9. Klicken Sie auf **Save captures** , um die Erfassungsinformationen zu speichern.

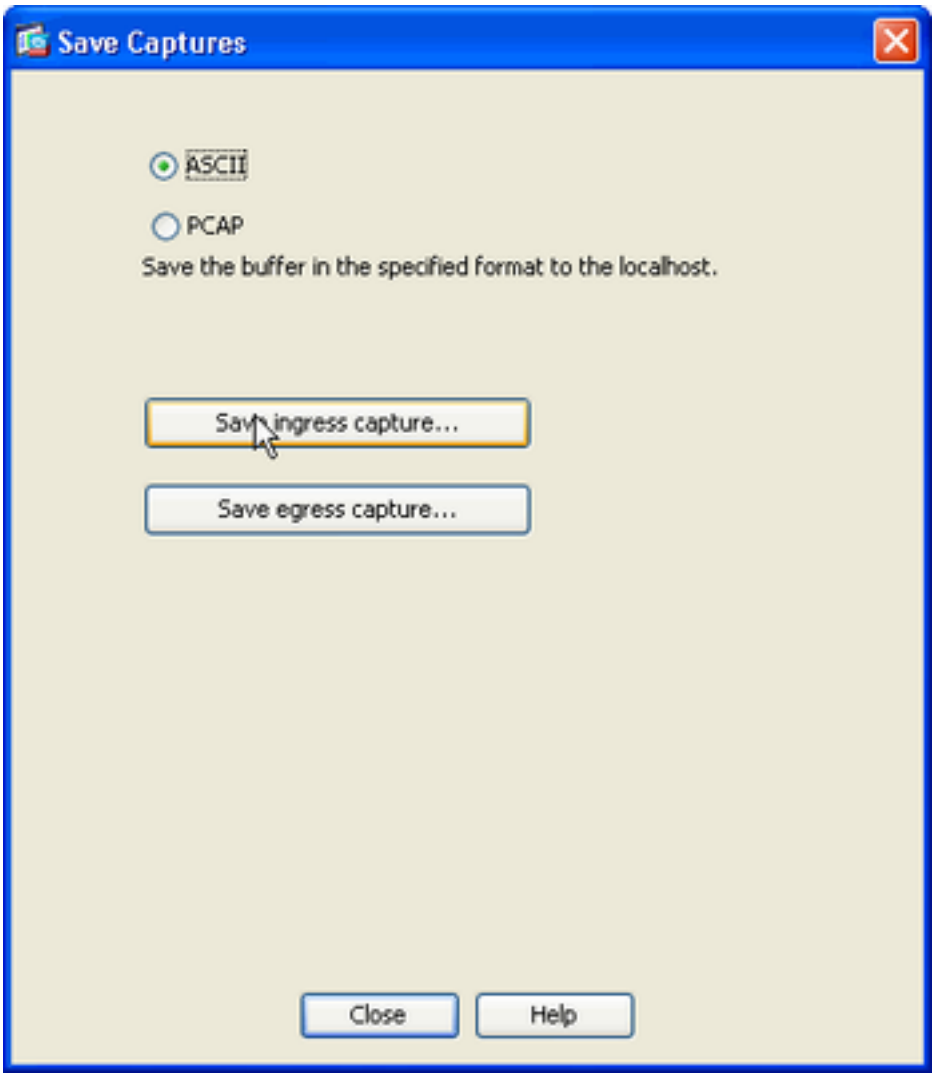


10.1 Aus dem **Save captures** das gewünschte Format auswählen, in dem der Capture-Puffer gespeichert werden soll.

10.2 Dies ist entweder **ASCII** oder **PCAP**. Klicken Sie auf das Optionsfeld neben den Formatnamen.

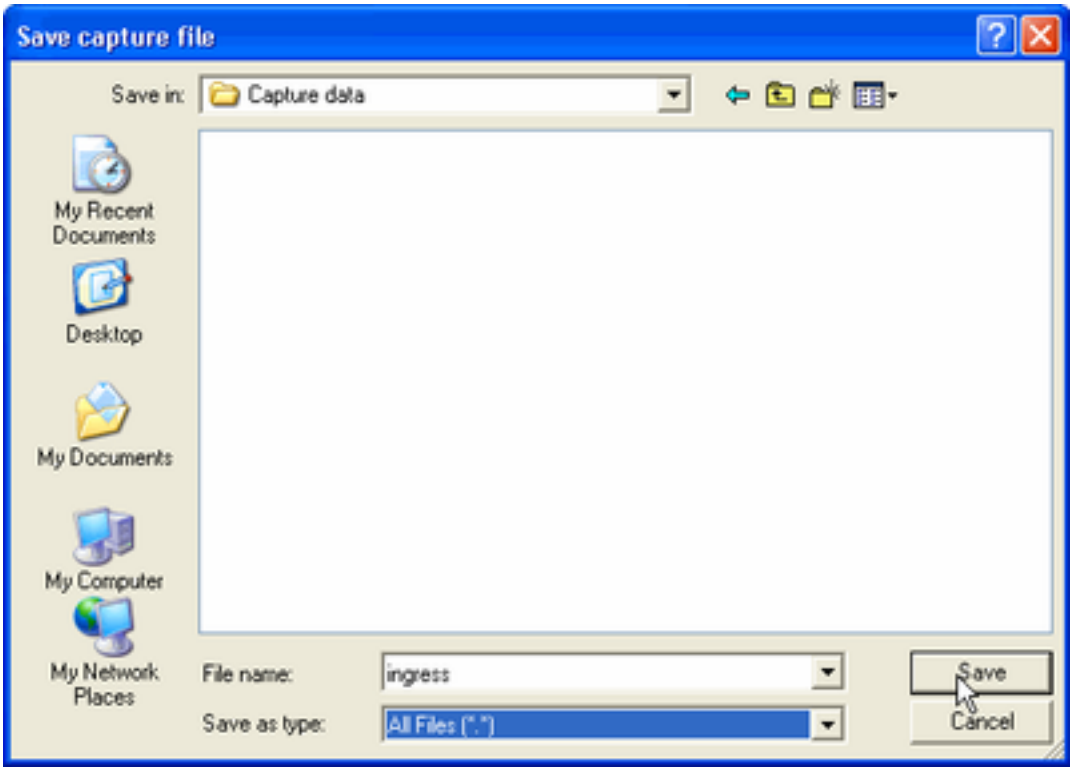
10.3 Klicken Sie anschließend auf **Save ingress capture** Oder **Save egress capture** je nach Bedarf.

Die PCAP-Dateien können mit Erfassungsanalysatoren wie **Wireshark**und ist die bevorzugte Methode.

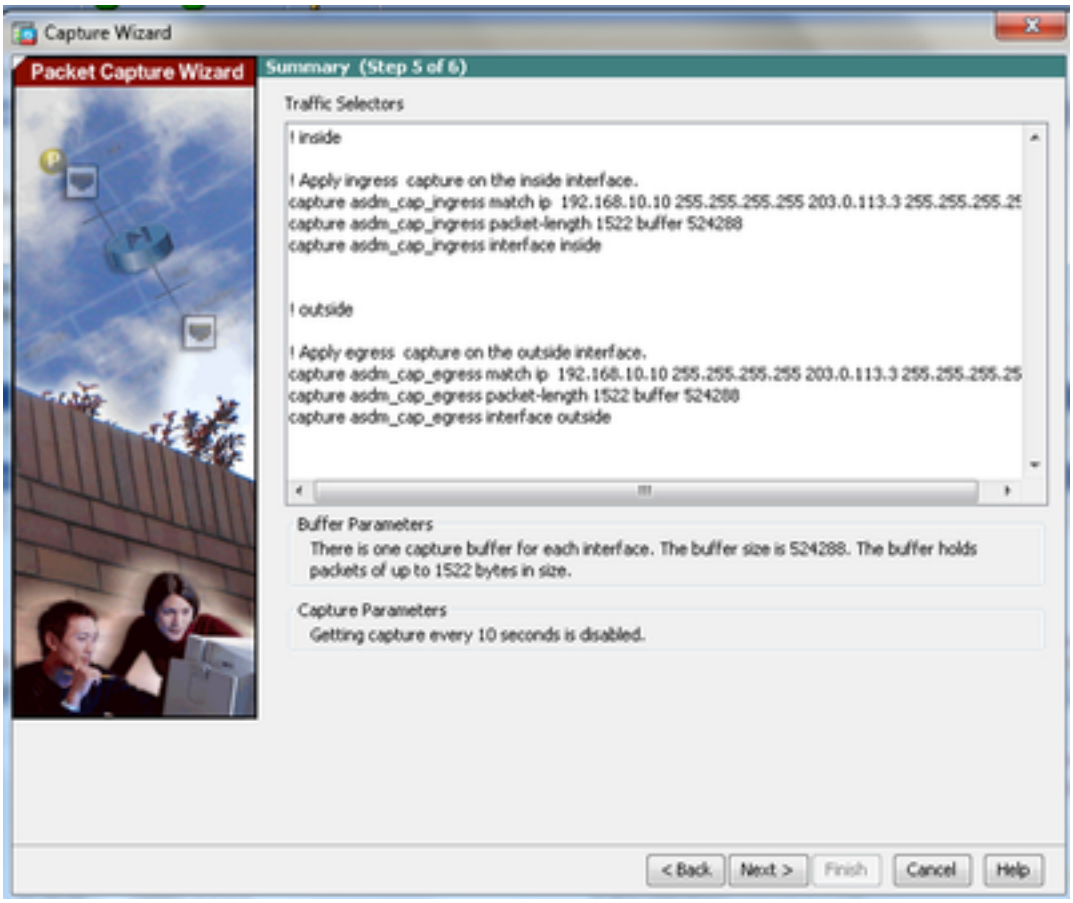


11.1 Aus dem **Save capture file** den Dateinamen und den Speicherort der Erfassungsdatei an.

11.2 Klicken Sie auf **Save**.



12. Klicken Sie auf **Finish**.



Damit ist die GUI-Paketerfassung abgeschlossen.

Konfigurieren der Paketerfassung mit der CLI

Gehen Sie wie folgt vor, um die Paketerfassungsfunktion auf der ASA mit der CLI zu konfigurieren:

1. Konfigurieren Sie die internen und externen Schnittstellen wie im Netzwerkdiagramm dargestellt mit den richtigen IP-Adressen und Sicherheitsstufen.

2. Starten Sie den Paketerfassungsprozess mit dem Befehl capture im privilegierten EXEC-Modus. In diesem Konfigurationsbeispiel wird die Erfassung mit dem Namen **capin** definiert. Binden Sie es an die **interne** Schnittstelle, und geben Sie mit dem **match-**Schlüsselwort an, dass nur die Pakete erfasst werden, die dem gewünschten Datenverkehr entsprechen:

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

3. Entsprechend wird die Erfassung mit dem Namen **capout** definiert. Binden Sie es an die **externe** Schnittstelle, und geben Sie mit dem **match-**Schlüsselwort an, dass nur die Pakete erfasst werden, die dem gewünschten Datenverkehr entsprechen:

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

   Die ASA beginnt nun mit der Erfassung des Datenverkehrs zwischen den Schnittstellen. Um die Erfassung jederzeit zu beenden, geben Sie den Befehl no capture gefolgt vom Namen der Erfassung ein.

   Hier ein Beispiel:

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

Verfügbare Erfassungstypen auf der ASA

In diesem Abschnitt werden die verschiedenen Aufnahmetypen beschrieben, die auf der ASA zur Verfügung stehen.

- **asa_dataplane** - Erfasst Pakete auf der ASA-Backplane, die zwischen der ASA und einem Modul, das die Backplane nutzt, weitergeleitet werden, z. B. die ASA CX oder das IPS-Modul.

```
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 - Erfasst Pakete, die über den beschleunigten Sicherheitspfad verworfen werden. Der Drop-Code gibt den Typ des Datenverkehrs an, der über den beschleunigten Sicherheitspfad verworfen wird.

```
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 - Wählt einen Ethernet-Typ für die Erfassung aus. Zu den unterstützten Ethernet-Typen gehören 8021Q, ARP, IP, IP6, LACP, PPPOED, PPPOES, RARP und VLAN.

  Dieses Beispiel zeigt, wie ARP-Datenverkehr erfasst wird:

```
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** - Zeigt die erfassten Pakete kontinuierlich in Echtzeit an. Um eine Echtzeit-Paketerfassung zu beenden, drücken Sie Strg-C. Um die Erfassung dauerhaft zu entfernen, verwenden Sie die negative Form dieses Befehls.
- Diese Option wird nicht unterstützt, wenn Sie die **cluster exec capture** aus.

```
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** - Verfolgt die erfassten Pakete auf eine ähnliche Weise wie die ASA-Funktion zur Paketverfolgung.

```
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
```

Anmerkung: Auf ASA 9.10+ erfasst das Schlüsselwort any nur Pakete mit IPv4-Adressen. Das Schlüsselwort any6 erfasst den gesamten IPv6-adressierten Datenverkehr.

Dies sind erweiterte Einstellungen, die mit Packet Captures konfiguriert werden können.

Lesen Sie die Befehlsreferenz, wie Sie diese festlegen.

- **ikev1/ikev2** - Erfasst nur Protokollinformationen zu Internet Key Exchange Version 1 (IKEv1) oder IKEv2.

- **isakmp** - Erfasst Internet Security Association and Key Management Protocol (ISAKMP)-Datenverkehr für VPN-Verbindungen Das ISAKMP-Subsystem hat keinen Zugriff auf die Protokolle der oberen Schicht. Die Erfassung ist eine Pseudo-Erfassung, bei der die physischen, die IP- und die UDP-Schichten miteinander kombiniert werden, um einen PCAP-Parser zu befriedigen. Die Peer-Adressen werden vom SA-Austausch abgerufen und in der IP-Schicht gespeichert.

- **lacp** - Erfasst LACP-Datenverkehr (Link Aggregation Control Protocol). Bei entsprechender Konfiguration ist der Schnittstellenname der Name der physischen Schnittstelle. Dies ist nützlich, wenn Sie mit Etherchannels arbeiten, um das aktuelle Verhalten von LACP zu identifizieren.

- **tls-proxy** - Erfasst entschlüsselte ein- und ausgehende Daten vom TLS-Proxy (Transport Layer Security) auf einer oder mehreren Schnittstellen.

- **webvpn** - Erfasst WebVPN-Daten für eine bestimmte WebVPN-Verbindung.

  Vorsicht: Wenn Sie die WebVPN-Erfassung aktivieren, wirkt sich dies auf die Leistung der Sicherheits-Appliance aus. Stellen Sie sicher, dass Sie die Erfassung deaktivieren, nachdem Sie die für die Fehlerbehebung erforderlichen Erfassungsdateien erstellt haben.

Standardwerte

Dies sind die ASA-Standardwerte:

- Der Standardtyp ist raw-data.
- Die Standardpuffergröße beträgt 512 KB.
- Der standardmäßige Ethernet-Typ ist IP-Pakete.
- Die Standard-Paketlänge beträgt 1.518 Byte.

Erfasste Pakete anzeigen

Auf der ASA

Um die erfassten Pakete anzuzeigen, geben Sie den Befehl show capture gefolgt vom Namen der Erfassung ein. Dieser Abschnitt enthält die Ausgabe des Befehls **show** des Inhalts des Erfassungspuffers. Die Fehlermeldung **show capture capin** zeigt den Inhalt des Capture-Puffers mit dem Namen **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
```

Die Fehlermeldung **show capture capout** zeigt den Inhalt des Capture-Puffers mit dem Namen **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
```

ASA für Offline-Analysen herunterladen

Es gibt mehrere Möglichkeiten, die Paketerfassungen zur Analyse offline herunterzuladen:

1. Navigieren Sie zu https://<ip_of_asa>/admin/capture/<capture_name>/pcapin jedem Browser.

   Tipp: Wenn Sie das **pcap** -Schlüsselwort, dann nur das Äquivalent des **show capture** wird ausgegeben.

1. Geben Sie den Befehl copy capture und Ihr bevorzugtes Dateiübertragungsprotokoll ein, um die Aufzeichnung herunterzuladen:

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

   Tipp: Wenn Sie ein Problem mit der Verwendung von Paketerfassungen beheben, empfiehlt Cisco, die Erfassungen zur Offline-Analyse herunterzuladen.

Erfassung löschen

Um den Capture-Puffer zu löschen, geben Sie den **clear capture** command:

```
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
```

Geben Sie **clear capture /all** Befehl, um den Puffer für alle Aufnahmen zu löschen:

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

Erfassen stoppen

Die einzige Möglichkeit, eine Erfassung auf der ASA zu stoppen, besteht darin, sie mit dem folgenden Befehl vollständig zu deaktivieren:

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

Überprüfung

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.