Configurazione delle acquisizioni di pacchetti ASA con CLI e ASDM

Sommario

Introduzione

Questo documento descrive come configurare il firewall Cisco ASA per acquisire i pacchetti desiderati con ASDM o CLI.

Prerequisiti

Requisiti

Questa procedura presuppone che l'ASA sia completamente operativa e configurata in modo da consentire a Cisco ASDM o CLI di apportare modifiche alla configurazione.

Componenti usati

Il documento può essere consultato per tutte le versioni hardware o software.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Questa configurazione viene utilizzata anche con i seguenti prodotti Cisco:

- Cisco ASA versione 9.1(5) e successive
- Cisco ASDM versione 7.2.1

Premesse

In questo documento viene descritto come configurare **Cisco Adaptive Security Appliance (ASA) Next-Generation Firewall** per acquisire i pacchetti desiderati con **Cisco Adaptive Security Device Manager (ASDM)** o **Command Line Interface (CLI) (ASDM)**.

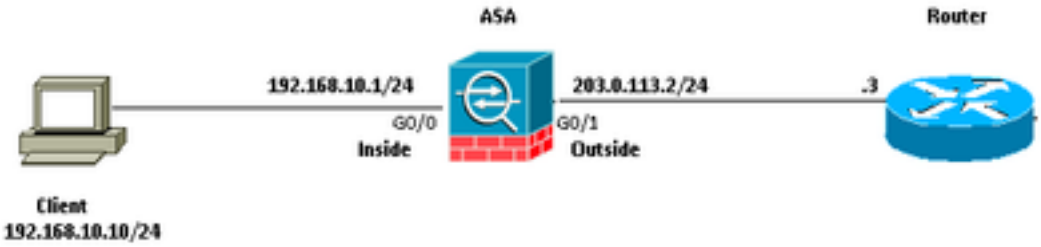
Il processo di acquisizione dei pacchetti è utile per risolvere i problemi di connettività o monitorare le attività sospette. Inoltre, è possibile creare più acquisizioni per analizzare diversi tipi di traffico su più interfacce.

Configurazione

In questa sezione vengono fornite le informazioni necessarie per configurare le funzionalità di acquisizione dei pacchetti descritte più avanti nel documento.

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazioni

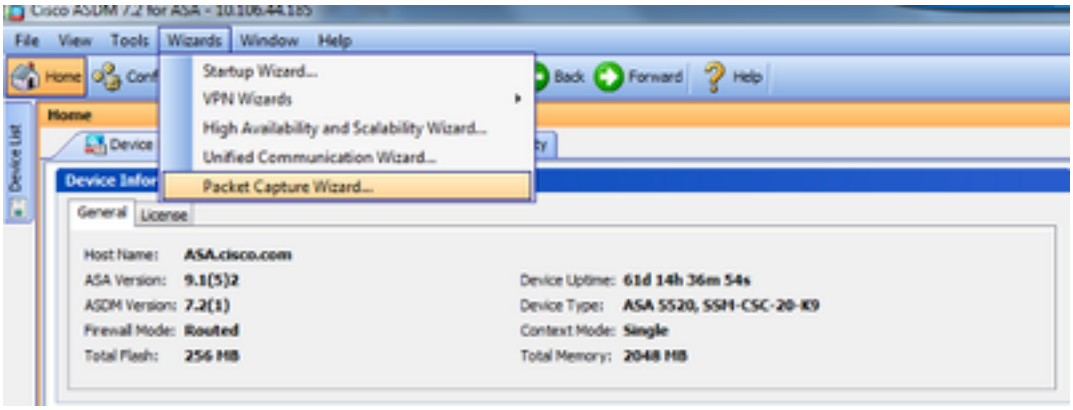
Gli schemi di indirizzi IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

Configurazione dell'acquisizione dei pacchetti con ASDM

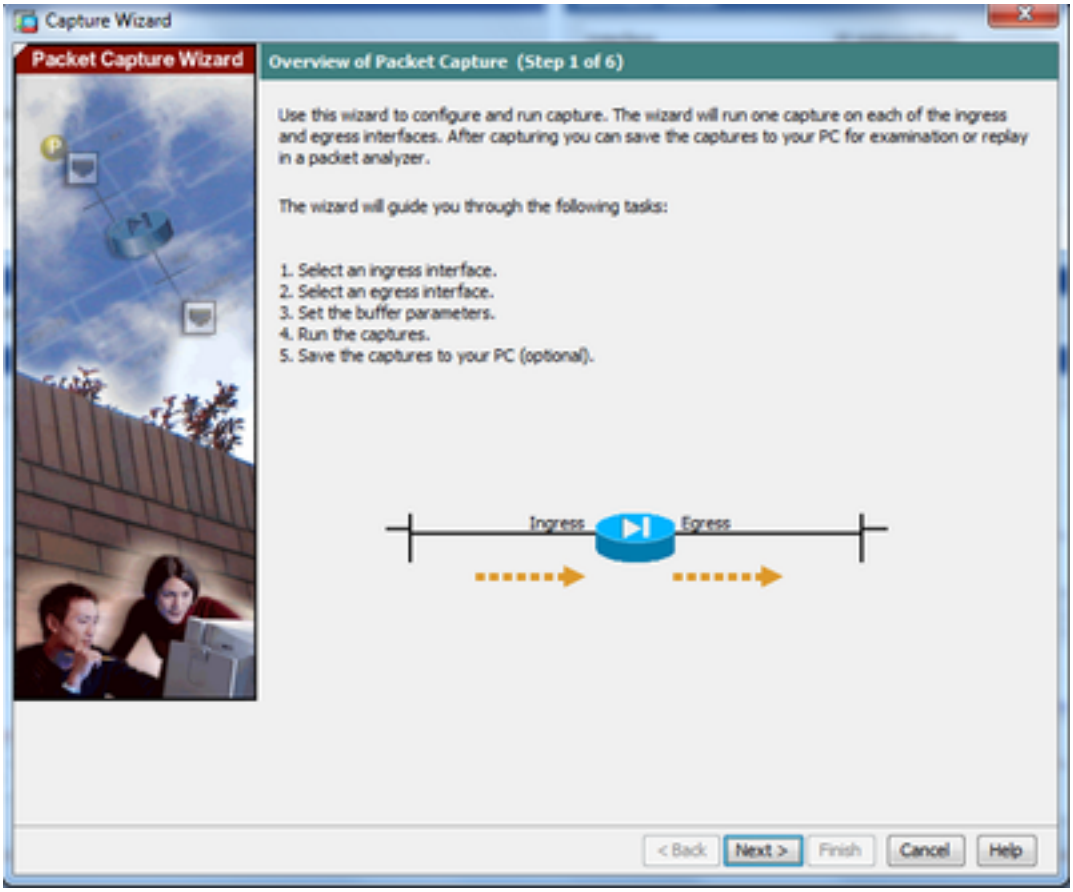
Questa configurazione di esempio viene usata per acquisire i pacchetti trasmessi durante il ping tra l'utente 1 (all'interno della rete) e il router 1 (all'esterno della rete).

Per configurare la funzione di acquisizione dei pacchetti sull'appliance ASA con ASDM, completare la procedura seguente:

1. Passare a **Wizards > Packet Capture Wizard** per avviare la configurazione di acquisizione dei pacchetti, come mostrato:



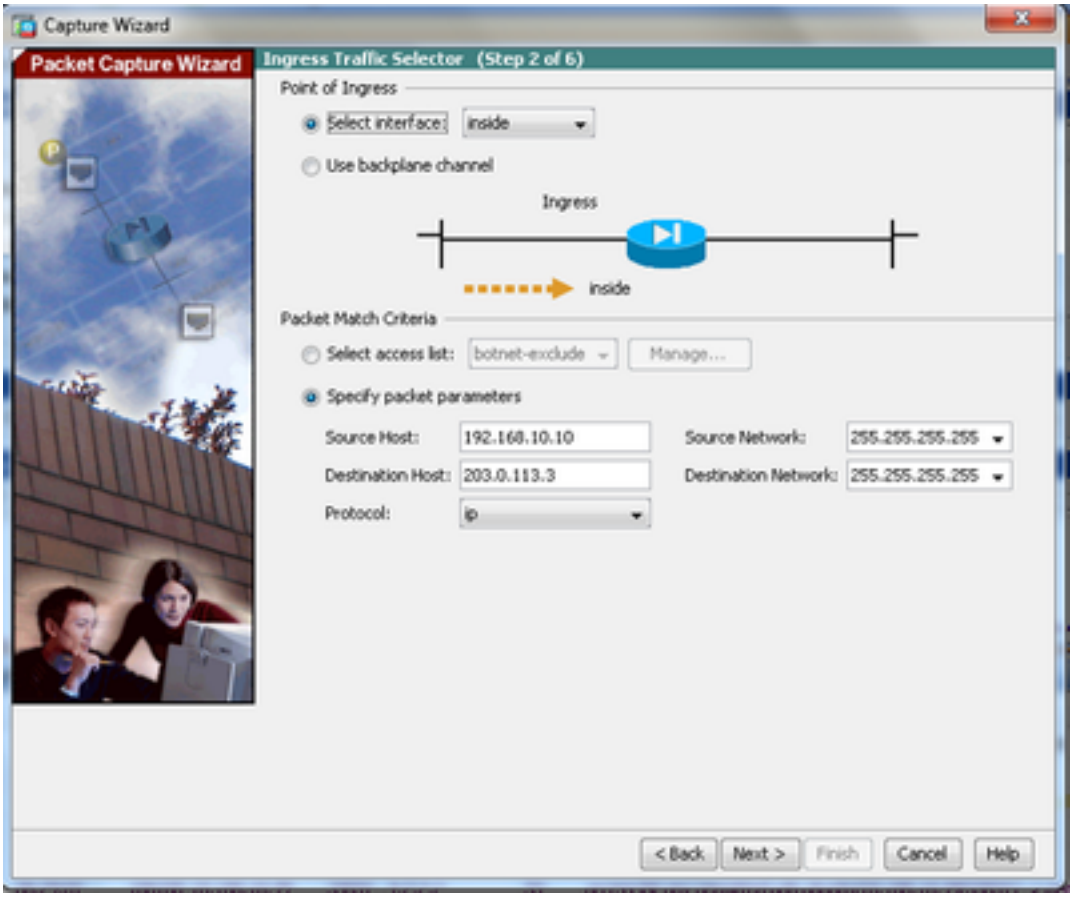
2. Il **Capture Wizard** si apre. Clic **Next**.



3.0 Nella nuova finestra, fornire i parametri utilizzati in per acquisire il traffico in entrata.

3.1 Seleziona **inside** per **Ingress Interface** e fornire gli indirizzi IP di origine e di destinazione dei pacchetti da acquisire, insieme alla relativa subnet mask, nello spazio disponibile.

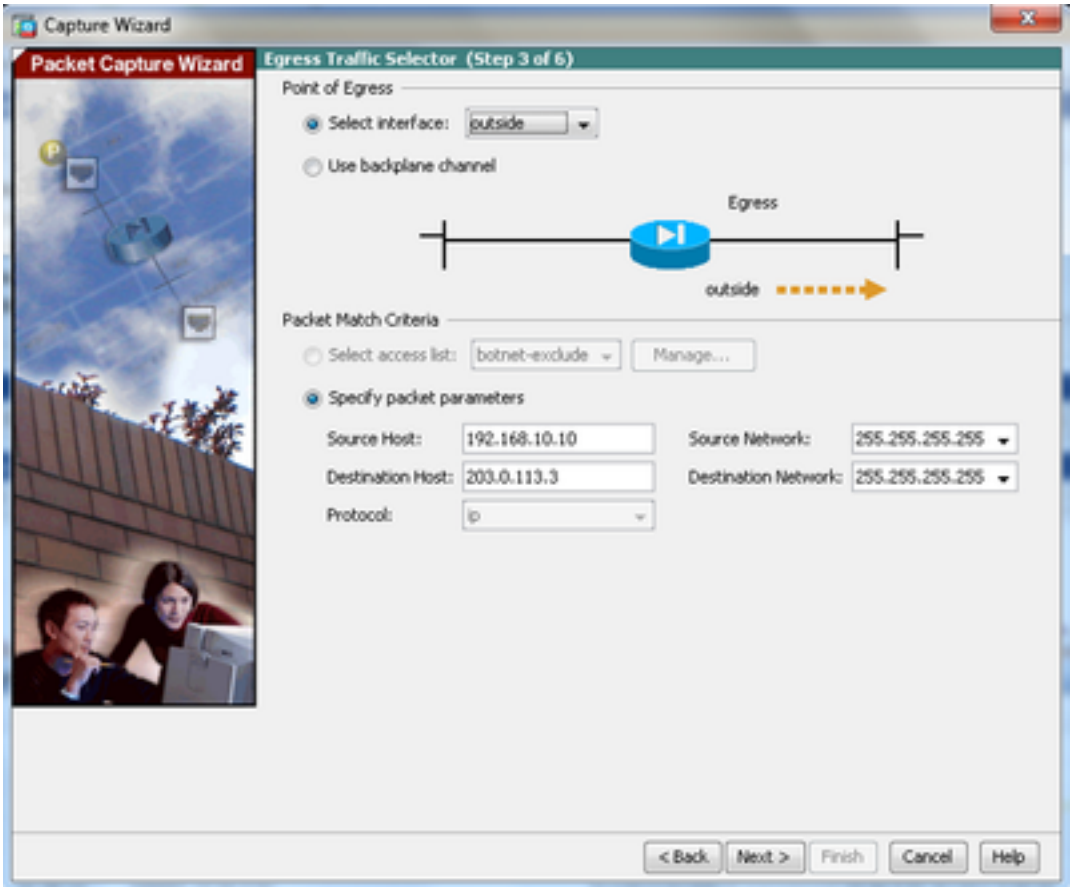
3.2 Scegliere il tipo di pacchetto da acquisire dall'ASA (IP è il tipo di pacchetto scelto qui), come mostrato:



3.3 Fare clic su **Next**.

4.1 Selezione **outside** per **Egress Interface** e fornire gli indirizzi IP di origine e di destinazione, insieme alla relativa subnet mask, negli spazi appositi.

If Network Address Translation (NAT) viene eseguito sul firewall, tenerne conto.



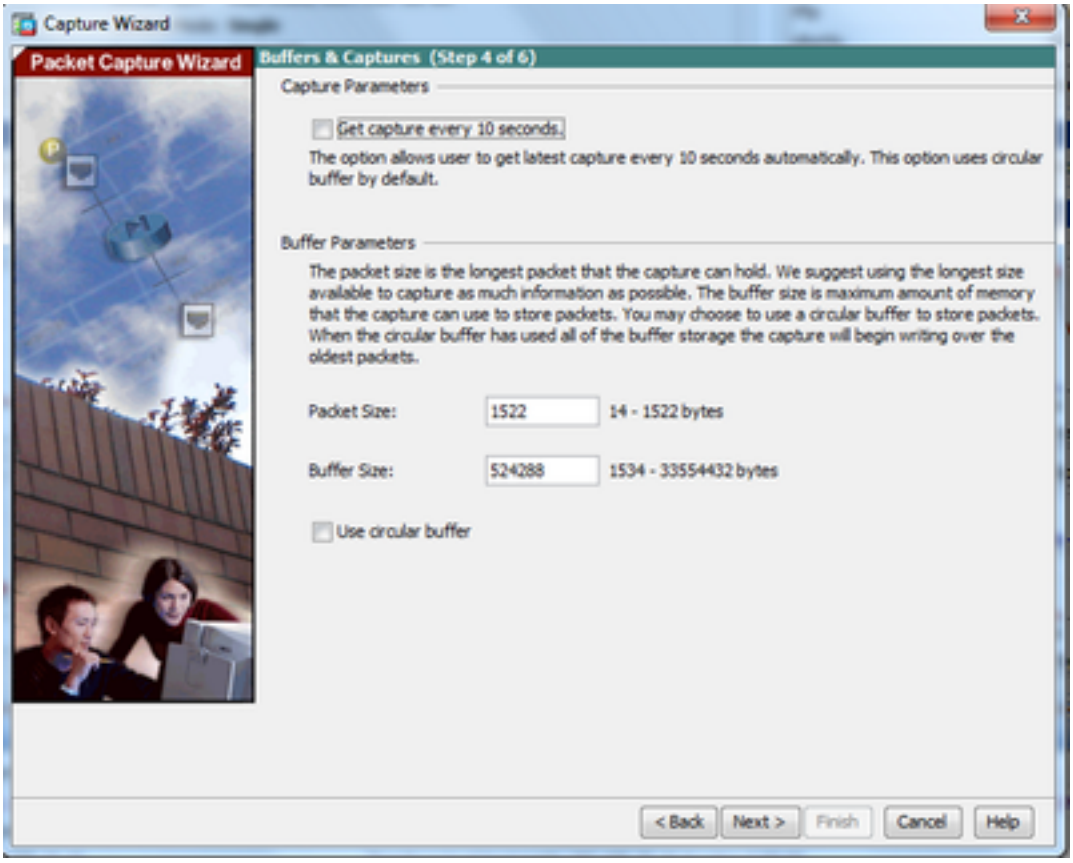
4.2 Fare clic su **Next**.

5.1 Inserire il **Packet Size** e **Buffer Size** nello spazio corrispondente. Questi dati sono necessari per l'acquisizione.

5.2 Controllare il **Use circular buffer** per utilizzare l'opzione buffer circolare. I buffer circolari non si riempiono mai.

Quando il buffer raggiunge le dimensioni massime, i dati meno recenti vengono eliminati e l'acquisizione continua.

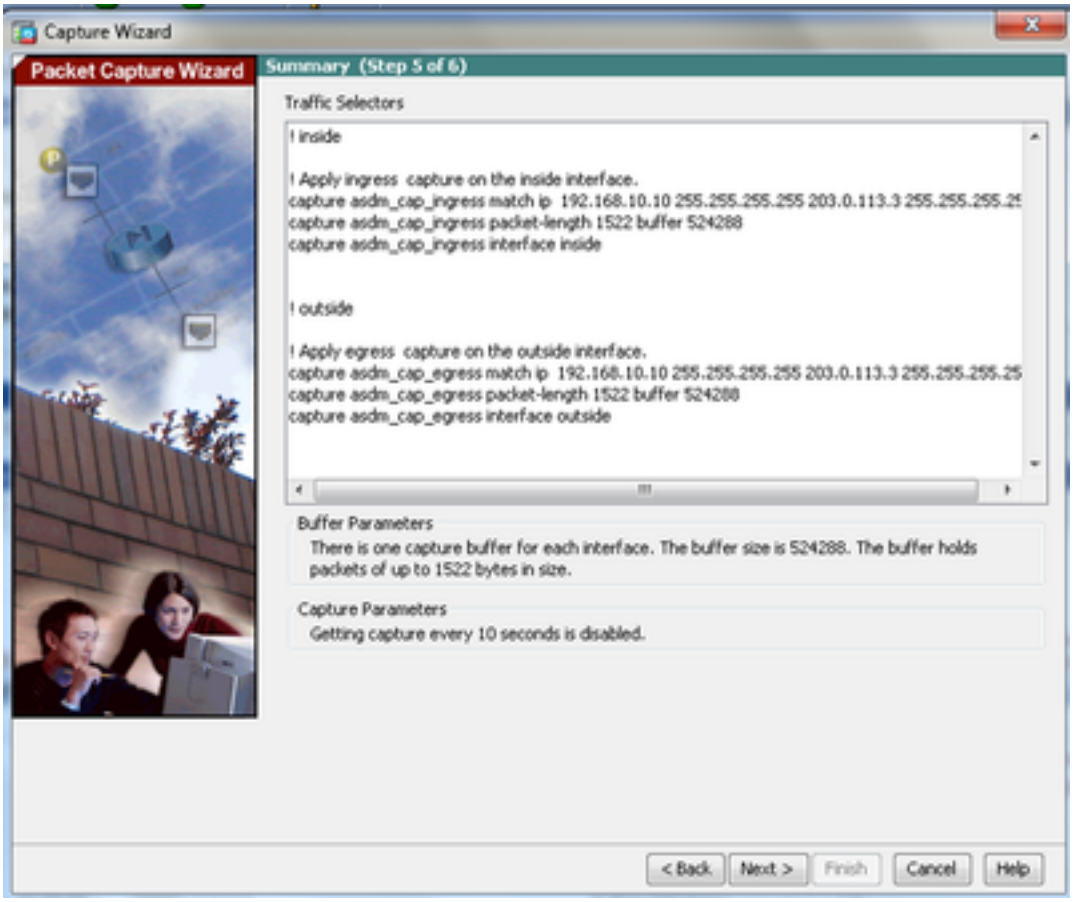
In questo esempio, il buffer circolare non viene utilizzato, quindi la casella di controllo non è selezionata.



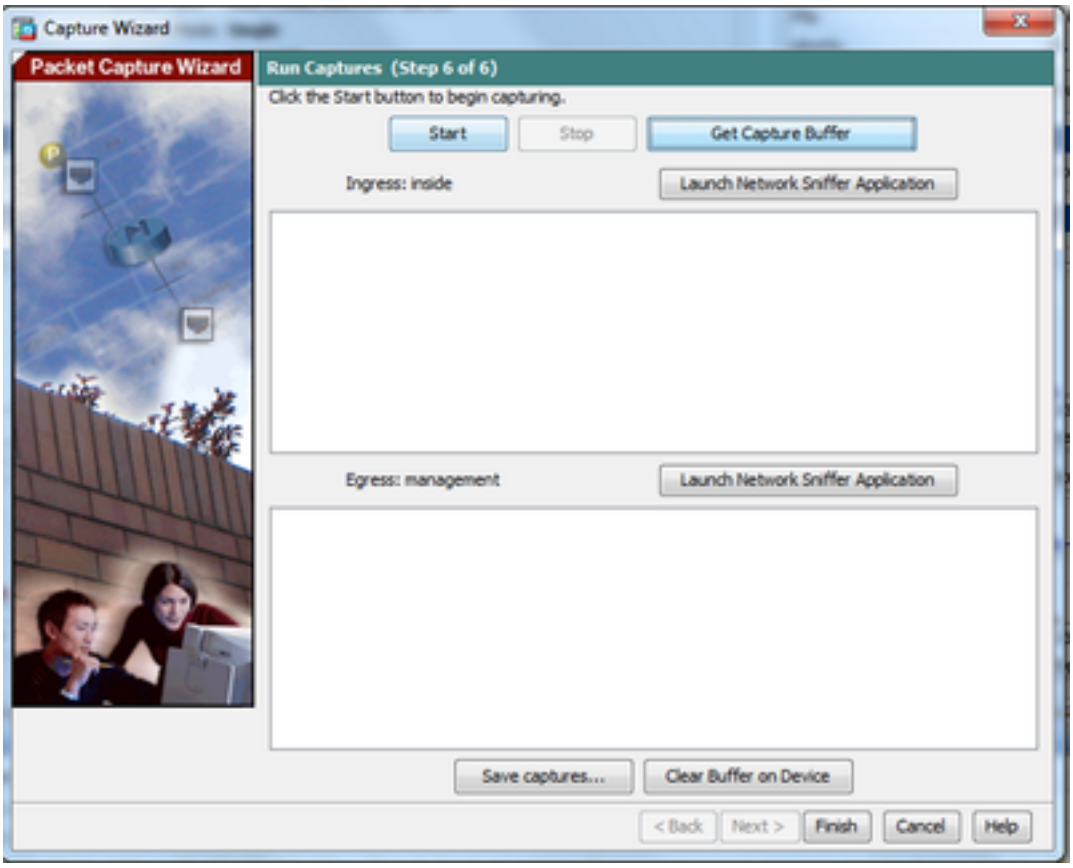
5.3 Fare clic su **Next**.

6.0 In questa finestra viene visualizzata la **Access-lists** che devono essere configurati sull'appliance ASA (in modo che vengano acquisiti i pacchetti desiderati) e il tipo di pacchetti da acquisire (in questo esempio, i pacchetti IP vengono acquisiti).

6.1 Fare clic su **Next**.

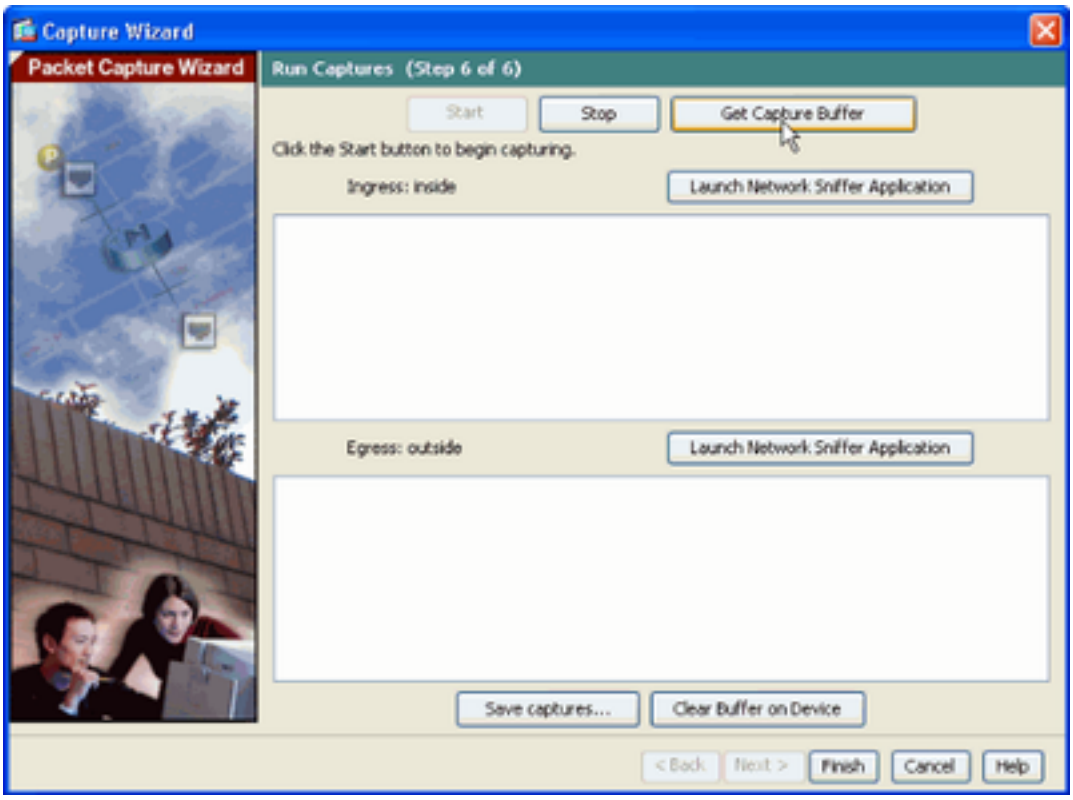


7. Fare clic su **Start** per avviare l'acquisizione del pacchetto, come mostrato:



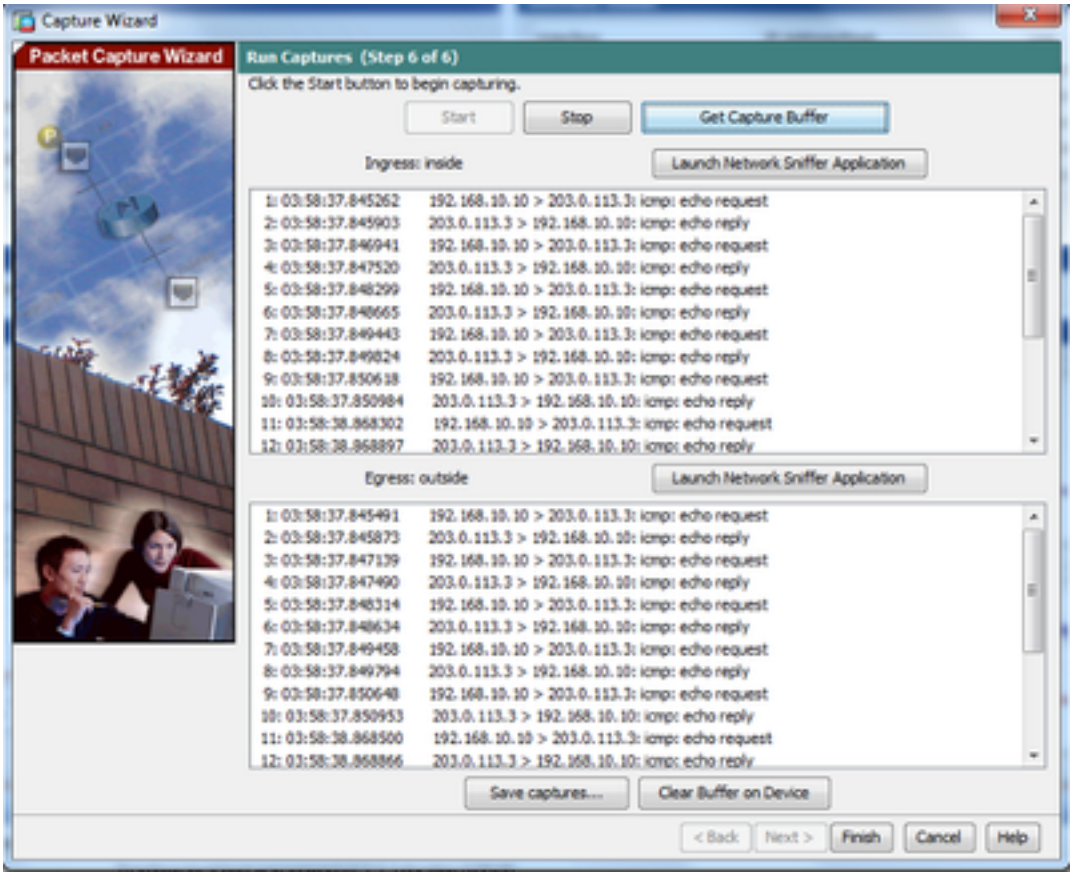
All'avvio dell'acquisizione dei pacchetti, provare a eseguire il ping della rete esterna dalla rete interna in modo che i pacchetti che passano tra gli indirizzi IP di origine e di destinazione vengano acquisiti dal buffer di acquisizione ASA.

8. Fare clic su **Get Capture Buffer** per visualizzare i pacchetti acquisiti dal buffer di acquisizione ASA.



I pacchetti acquisiti vengono mostrati in questa finestra sia per il traffico in entrata che per il traffico in uscita.

9. Fare clic su **Save captures** per salvare le informazioni di acquisizione.

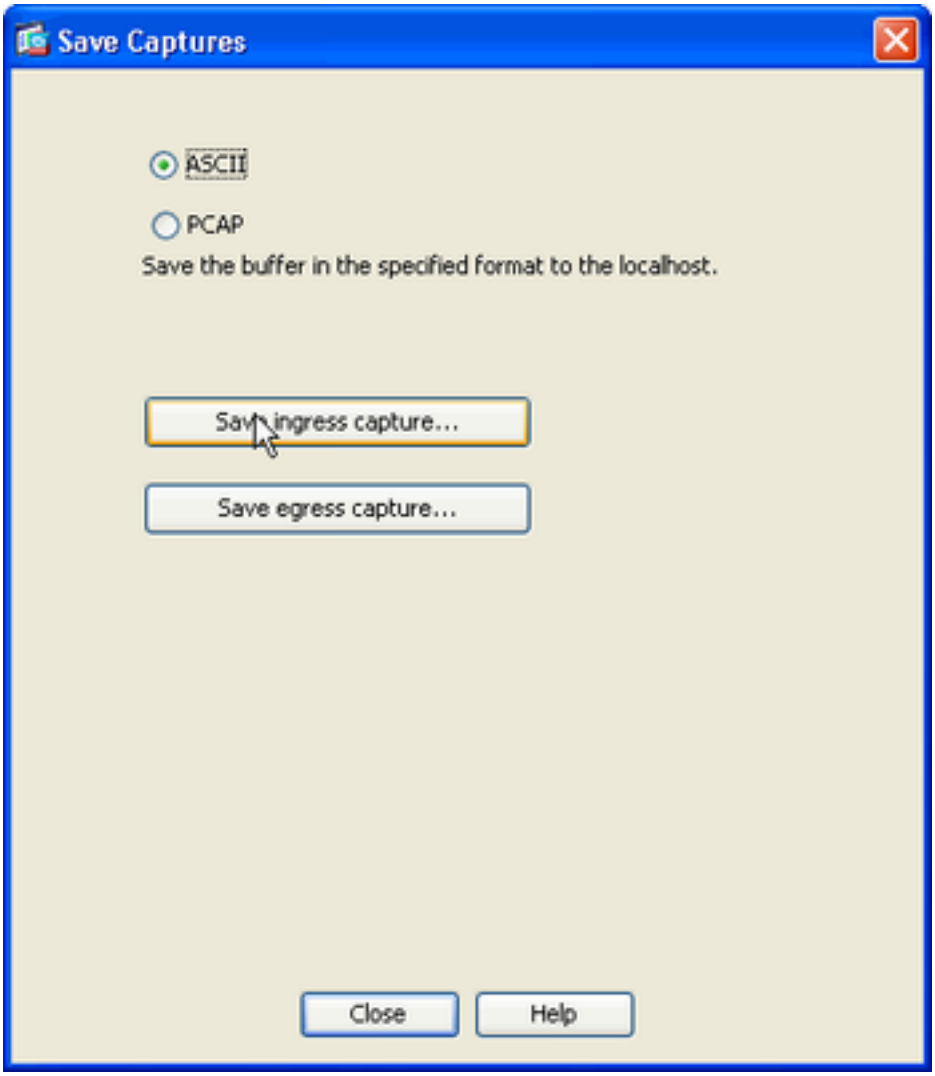


10.1 Dalla **Save captures** scegliere il formato richiesto in cui salvare il buffer di acquisizione.

10.2 **ASCII** o **PCAP**. Fare clic sul pulsante di opzione accanto ai nomi dei formati.

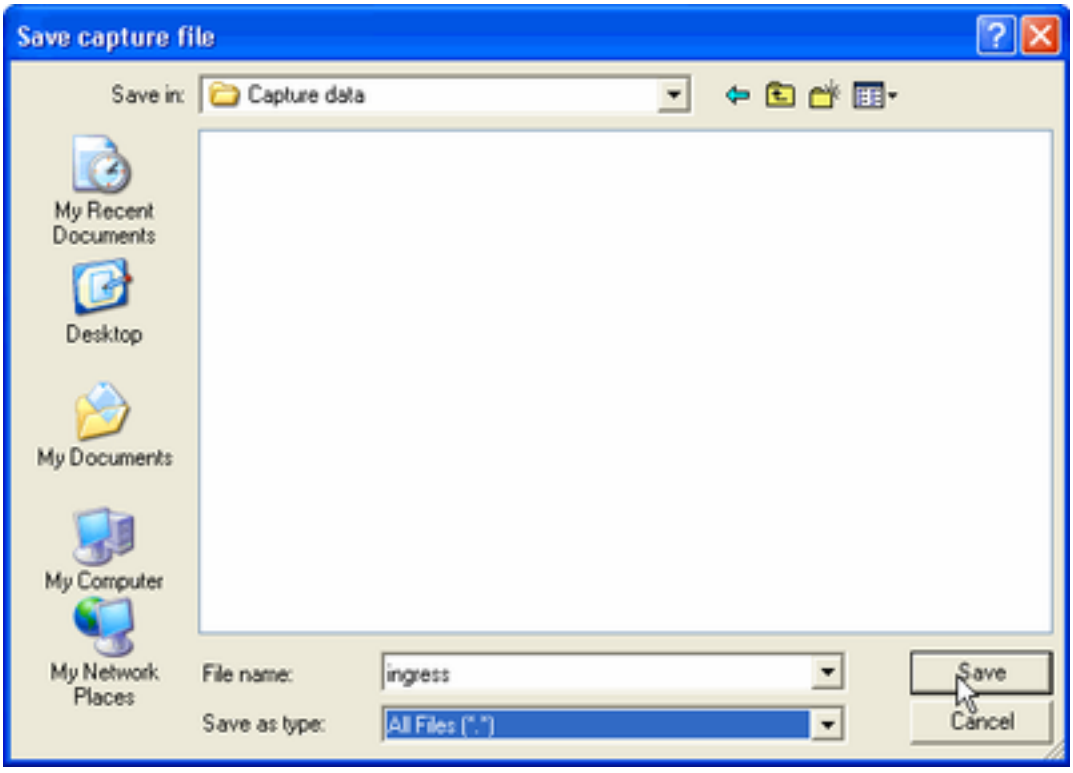
10.3 Fare quindi clic su **Save ingress capture** o **Save egress capture** come richiesto.

I file PCAP possono essere aperti con analizzatori di acquisizione, quali **Wireshark**ed è il metodo preferito.

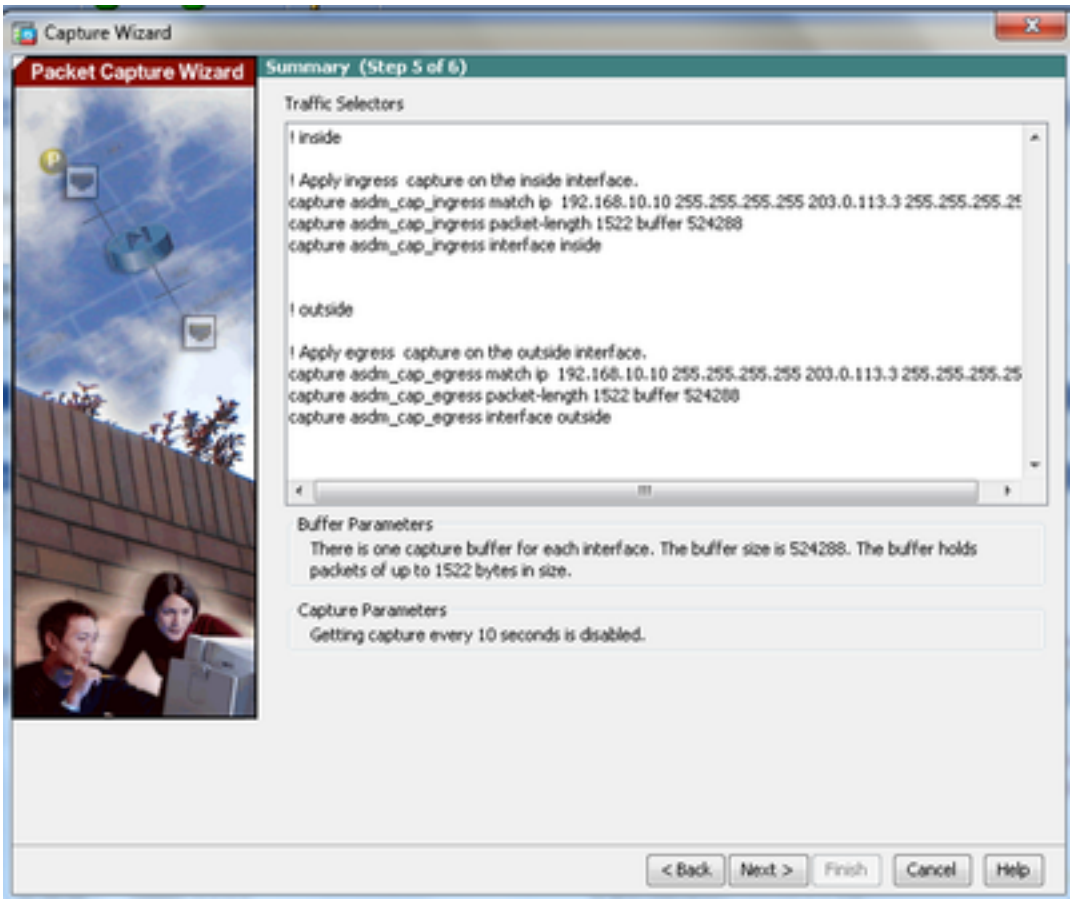


11.1 Dalla **Save capture file** fornire il nome del file e la posizione in cui salvare il file di acquisizione.

11.2 Fare clic su **Save**.



12. Fare clic su **Finish**.



La procedura di acquisizione dei pacchetti GUI è completata.

Configurazione dell'acquisizione dei pacchetti con la CLI

Completare questa procedura per configurare la funzione di acquisizione dei pacchetti sull'appliance ASA con la CLI:

1. Configurare le interfacce interne ed esterne come mostrato nel diagramma di rete con l'indirizzo IP e i livelli di sicurezza corretti.

2. Avviare il processo di acquisizione dei pacchetti con il comando capture in modalità di esecuzione privilegiata. In questo esempio di configurazione è definita l'acquisizione denominata **capin**. Associarlo all'interfaccia **interna** e specificare con la parola chiave **match** che verranno acquisiti solo i pacchetti che corrispondono al traffico a cui si è interessati:

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

3. Analogamente, viene definita la cattura denominata **capout**. Associarlo all'interfaccia **esterna** e specificare con la parola chiave **match** che verranno acquisiti solo i pacchetti che corrispondono al traffico a cui si è interessati:

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

   L'ASA inizia a catturare il flusso del traffico tra le interfacce. Per interrompere l'acquisizione in qualsiasi momento, immettere il comando no capture seguito dal nome dell'acquisizione.

   Di seguito è riportato un esempio:

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

Tipi di acquisizione disponibili sull'appliance ASA

In questa sezione vengono descritti i diversi tipi di clip disponibili sull'appliance ASA.

- **asa_dataplane** - Cattura i pacchetti sul backplane ASA che passano tra l'ASA e un modulo che utilizza il backplane, ad esempio il modulo ASA CX o 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: acquisisce i pacchetti scartati dal percorso di sicurezza accelerato. Il codice di rilascio specifica il tipo di traffico che viene scartato dal percorso di sicurezza accelerato.

```
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 - Seleziona un tipo Ethernet da acquisire. I tipi Ethernet supportati includono 8021Q, ARP, IP, IP6, LACP, PPPOED, PPPOES, RARP e VLAN.

  Nell'esempio viene mostrato come acquisire il traffico 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** - Visualizzazione continua in tempo reale dei pacchetti acquisiti. Per terminare un'acquisizione del pacchetto in tempo reale, premere Ctrl-C. Per rimuovere definitivamente l'acquisizione, usare la forma no di questo comando.
- Questa opzione non è supportata quando si utilizza **cluster exec capture**

```
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** - Traccia i pacchetti acquisiti in modo simile alla funzione ASA packet tracer.

```
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: Su ASA 9.10+, la parola chiave any acquisisce solo i pacchetti con indirizzi ipv4. La parola chiave any6 acquisisce tutto il traffico indirizzato ipv6.

Si tratta di impostazioni avanzate che è possibile configurare con Packet Capture.

Per informazioni su come impostarli, consultare la guida di riferimento dei comandi.

- **ikev1/ikev2** - Acquisisce solo le informazioni sul protocollo IKEv1 (Internet Key Exchange versione 1) o IKEv2.

- **isakmp** - Acquisisce il traffico ISAKMP (Internet Security Association and Key Management Protocol) per le connessioni VPN. Il sottosistema ISAKMP non ha accesso ai protocolli di livello superiore. L'acquisizione è una pseudo acquisizione, con i livelli fisici, IP e UDP combinati per soddisfare un parser PCAP. Gli indirizzi peer vengono ottenuti dallo scambio SA e vengono memorizzati nel livello IP.

- **lacp** - Acquisisce il traffico LACP (Link Aggregation Control Protocol). Se configurato, il nome dell'interfaccia è il nome dell'interfaccia fisica. Ciò è utile quando si lavora con Etherchannel per identificare il comportamento attuale di LACP.

- **tls-proxy** - Acquisisce dati decrittografati in entrata e in uscita dal proxy TLS (Transport Layer Security) su una o più interfacce.

- **webvpn** - Acquisisce i dati WebVPN per una connessione WebVPN specifica.

  Attenzione: L'abilitazione dell'acquisizione WebVPN influisce sulle prestazioni dell'appliance di sicurezza. Assicurarsi di disattivare l'acquisizione dopo aver generato i file di acquisizione necessari per la risoluzione dei problemi.

Valori predefiniti

Di seguito sono riportati i valori predefiniti del sistema ASA:

- Il tipo predefinito è dati non elaborati.
- La dimensione predefinita del buffer è 512 KB.
- Il tipo Ethernet predefinito è IP packets.
- La lunghezza predefinita del pacchetto è 1.518 byte.

Visualizza i pacchetti acquisiti

Sull'appliance ASA

Per visualizzare i pacchetti acquisiti, immettere il comando show capture seguito dal nome dell'acquisizione. Questa sezione fornisce gli output del comando **show** per il contenuto del buffer di acquisizione. OSPF (Open Shortest Path First) **show capture capin** mostra il contenuto del buffer di

acquisizione denominato **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
```

OSPF (Open Shortest Path First) **show capture capout** mostra il contenuto del buffer di acquisizione denominato **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
```

Scarica dall'appliance ASA per analisi offline

Èpossibile scaricare le clip dei pacchetti per l'analisi offline in un paio di modi:

1. Passa a https://<ip_of_asa>/admin/capture/<nome_acquisizione>/pcapin qualsiasi browser.

   Suggerimento: Se si esclude il **pcap** , quindi solo l'equivalente della **show capture** viene fornito l'output del comando.

1. Immettere il comando copy capture e il protocollo di trasferimento file preferito per scaricare l'acquisizione:

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

   Suggerimento: Quando si risolve un problema con l'uso delle acquisizioni dei pacchetti, Cisco consiglia di scaricare le acquisizioni per l'analisi offline.

Cancella un'acquisizione

Per cancellare il buffer di acquisizione, immettere il **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
```

Immettere il **clear capture /all** per cancellare il buffer per tutte le acquisizioni:

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

Interrompere un'acquisizione

L'unico modo per interrompere un'acquisizione sull'appliance ASA è disabilitarla completamente con questo comando:

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

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Non sono attualmente disponibili informazioni specifiche per la risoluzione dei problemi per questa configurazione.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).