CLI 및 ASDM으로 ASA 패킷 캡처 구성

목차

소개

이 문서에서는 ASDM 또는 CLI를 사용하여 원하는 패킷을 캡처하도록 Cisco ASA 방화벽을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 절차에서는 ASA가 완전히 작동하며 Cisco ASDM 또는 CLI에서 컨피그레이션을 변경할 수 있도록 구성되었다고 가정합니다.

사용되는 구성 요소

이 문서는 특정 하드웨어 또는 소프트웨어 버전으로 제한되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

관련 제품

이 구성은 다음 Cisco 제품에도 사용됩니다.

- Cisco ASA 버전 9.1(5) 이상
- Cisco ASDM 버전 7.2.1

배경 정보

이 문서에서는 **Cisco Adaptive Security Appliance (ASA) Next-Generation Firewall** 원하는 패킷을 캡처하려면 **Cisco Adaptive Security Device Manager (ASDM)** 또는 **Command Line Interface (CLI) (ASDM).**

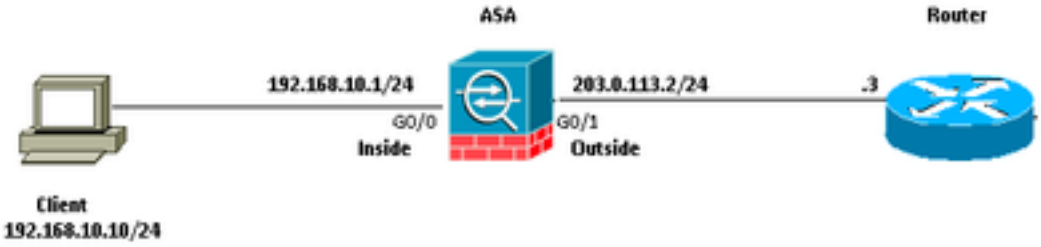
패킷 캡처 프로세스는 연결 문제를 해결하거나 의심스러운 활동을 모니터링하는 데 유용합니다. 또한 여러 인터페이스에서 서로 다른 유형의 트래픽을 분석하기 위해 여러 캡처를 생성할 수 있습니다.

구성

이 섹션에서는 이 문서에서 설명하는 패킷 캡처 기능을 구성하는 데 사용되는 정보를 제공합니다.

네트워크 다이어그램

이 문서에서는 이 네트워크 설정을 사용합니다.



설정

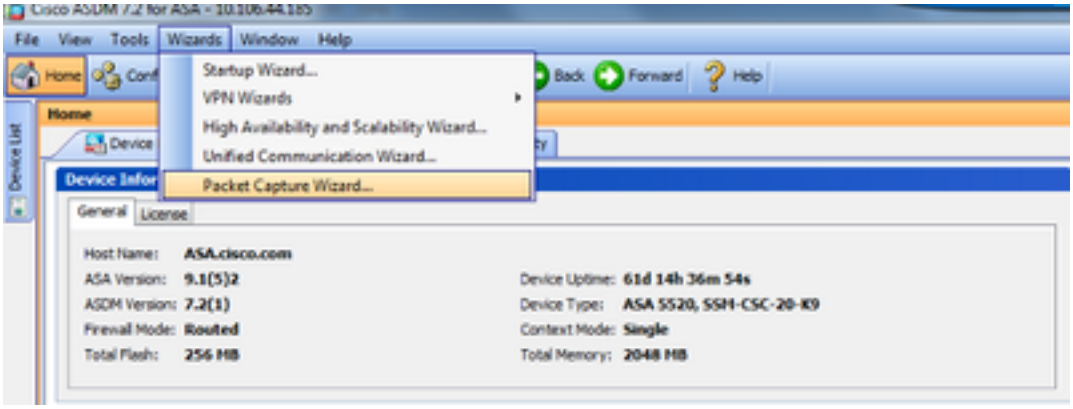
이 구성에 사용된 IP 주소 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다. 랩 환경에서 사용되는 RFC 1918 주소입니다.

ASDM으로 패킷 캡처 구성

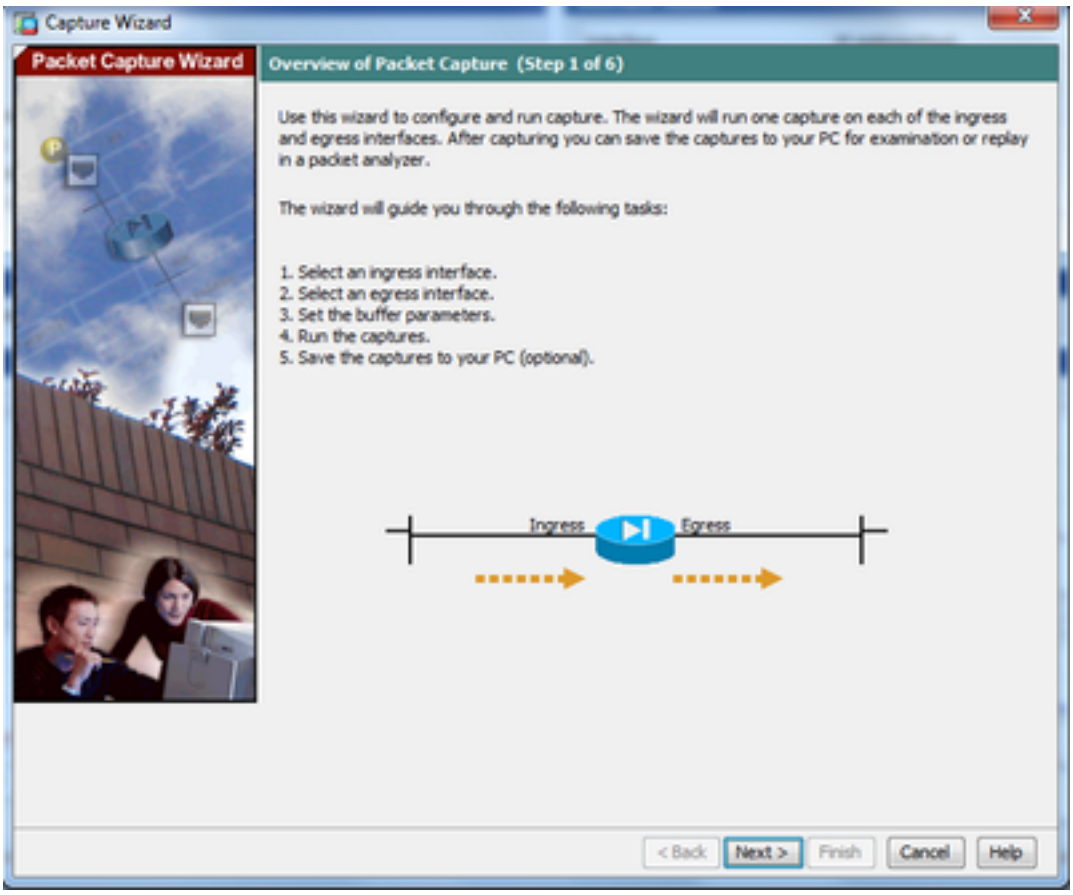
이 예제 컨피그레이션은에서 User1(내부 네트워크)에서 Router1(외부 네트워크)로 ping하는 동안 전송되는 패킷을 캡처하는 데 사용됩니다.

ASDM을 사용하여 ASA에서 패킷 캡처 기능을 구성하려면 다음 단계를 완료합니다.

1. 다음으로 이동 **Wizards > Packet Capture Wizard** 표시된 대로 패킷 캡처 컨피그레이션을 시작하려면



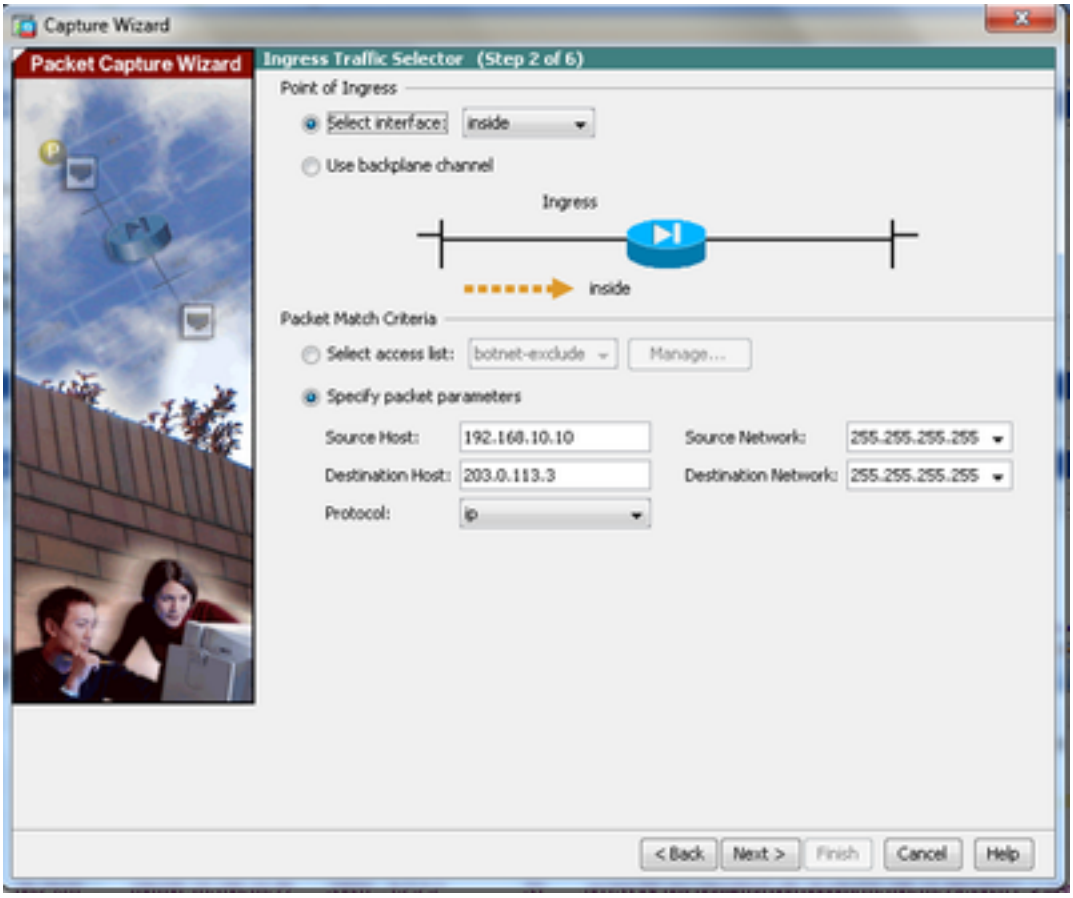
2. **Capture Wizard** 를 엽니다. 클릭 **Next.**



3.0 새 창에서 인그레스 트래픽 캡처에 사용되는 매개변수를 제공합니다.

3.1 선택 **inside** 의 **Ingress Interface** 및 제공되는 각 공간에 캡처할 패킷의 소스 및 목적지 IP 주소와 서브넷 마스크를 제공합니다.

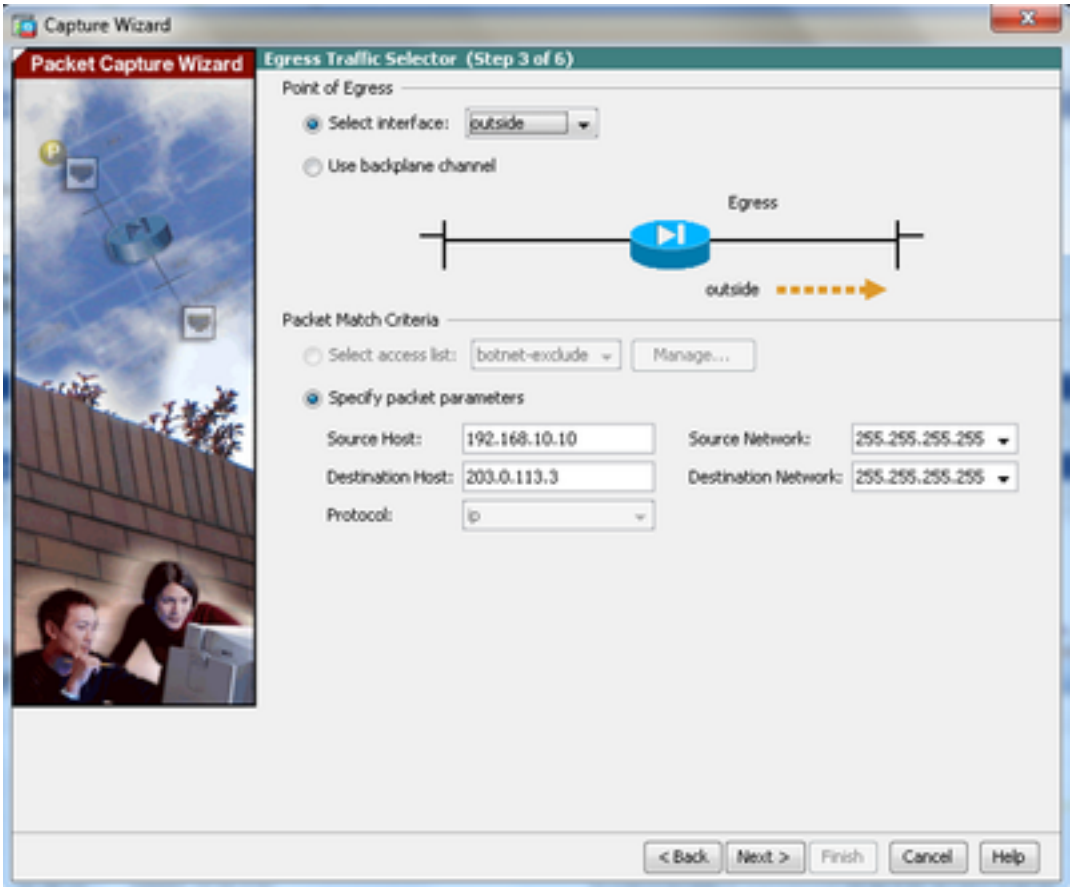
3.2 다음과 같이 ASA에서 캡처할 패킷 유형을 선택합니다(IP는 여기에서 선택한 패킷 유형).



3.3 클릭 **Next.**

4.1 선택 **outside** 의 **Egress Interface** 제공된 각 공간에 소스 및 목적지 IP 주소와 서브넷 마스크를 제공합니다.

If Network Address Translation (NAT) 방화벽에서 수행됩니다. 이 점도 고려하십시오.



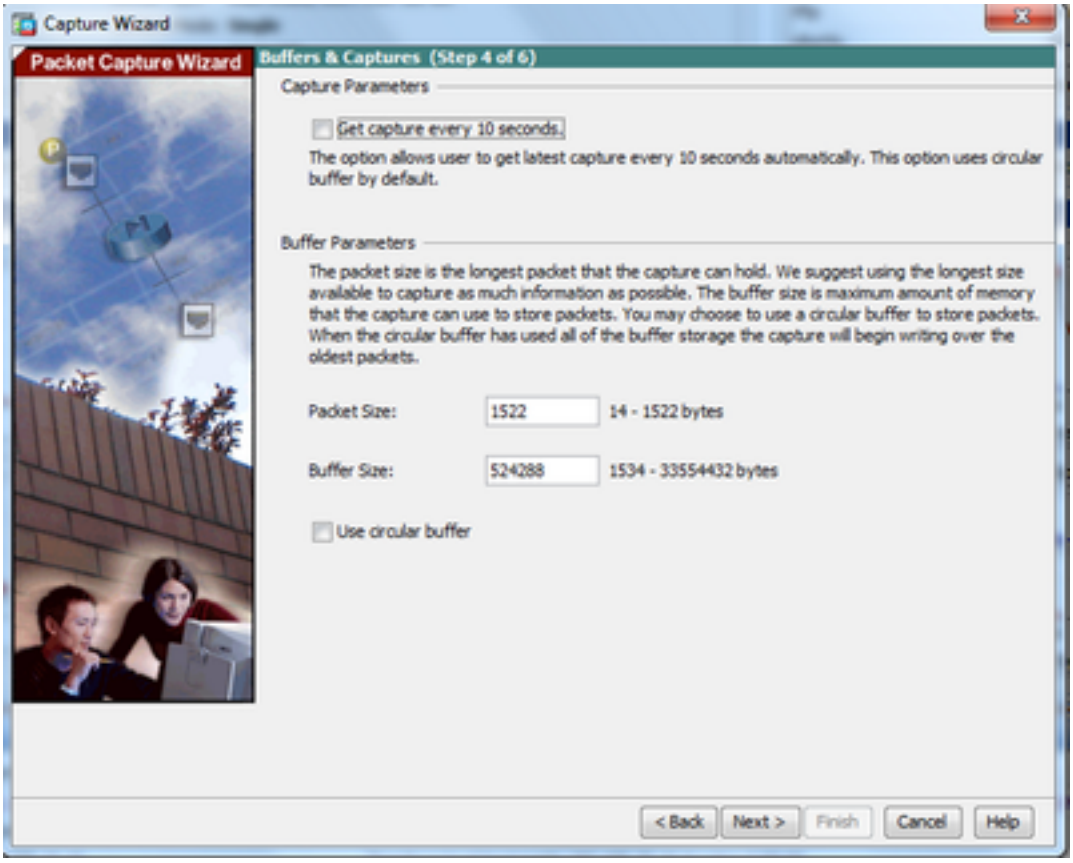
4.2 클릭 **Next**.

5.1 적절한 값을 입력합니다 **Packet Size** 및 **Buffer Size** 제공할 수 있습니다 이 데이터는 캡처가 발생하는 데 필요합니다.

5.2 **Use circular buffer** 상자 - 순환 버퍼 옵션을 사용합니다. 순환 버퍼가 가득 차지 않습니다.

버퍼가 최대 크기에 도달하면 이전 데이터가 폐기되고 캡처가 계속됩니다.

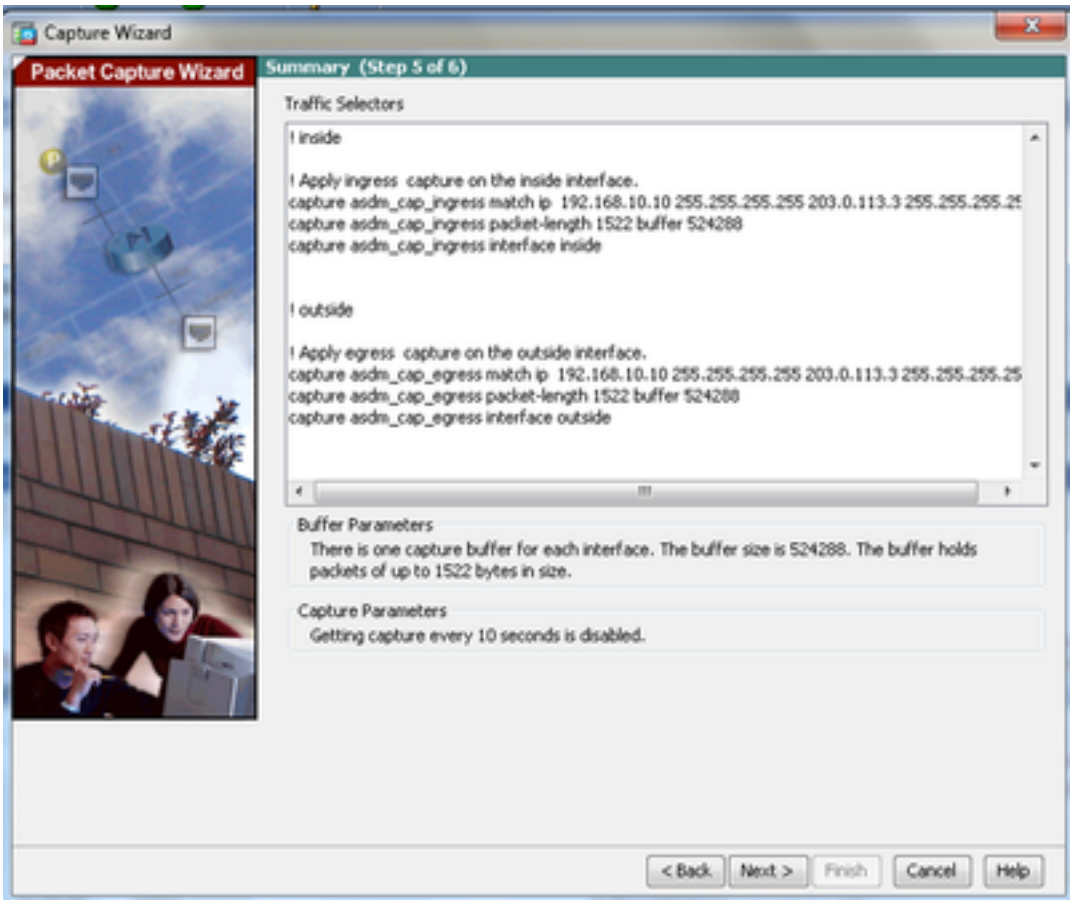
이 예에서는 순환 버퍼가 사용되지 않으므로 확인란이 선택되지 않습니다.



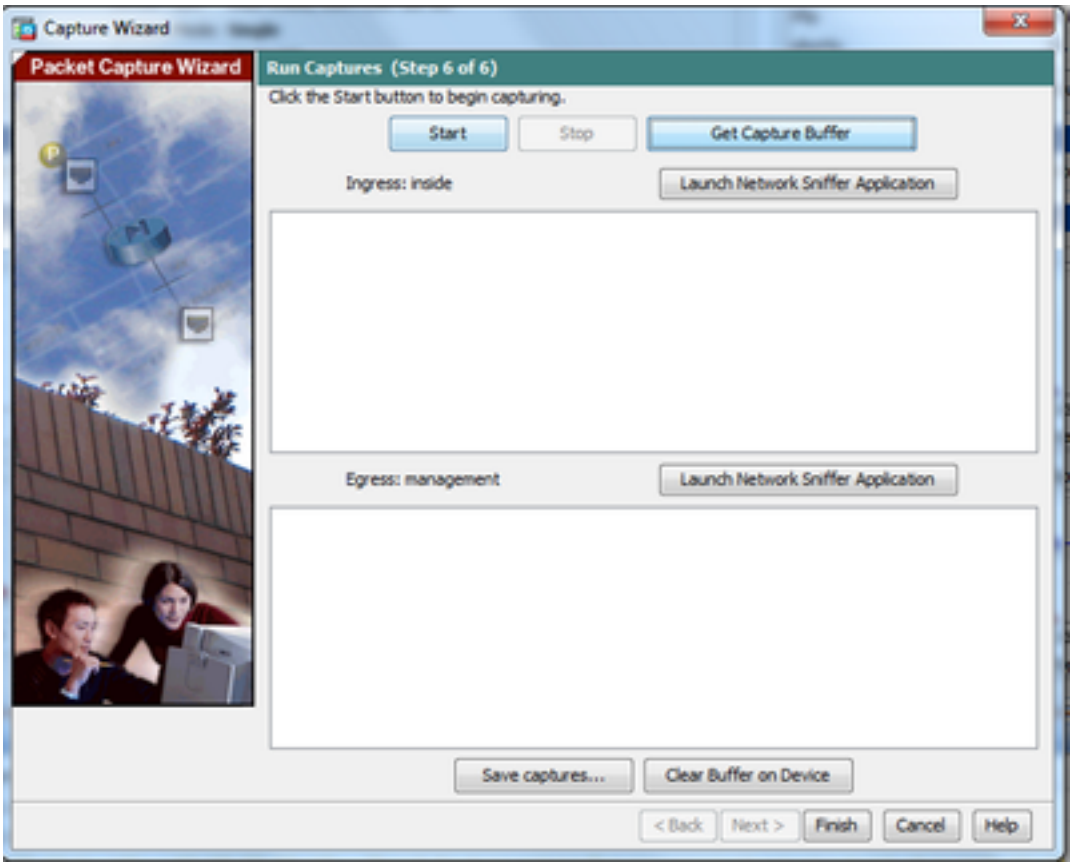
5.3 클릭 **Next.**

6.0 이 창에는 **Access-lists** ASA에서 구성해야 하는 패킷(원하는 패킷이 캡처되도록) 및 캡처할 패킷의 유형(이 예에서는 IP 패킷이 캡처됨)입니다.

6.1 클릭 **Next.**

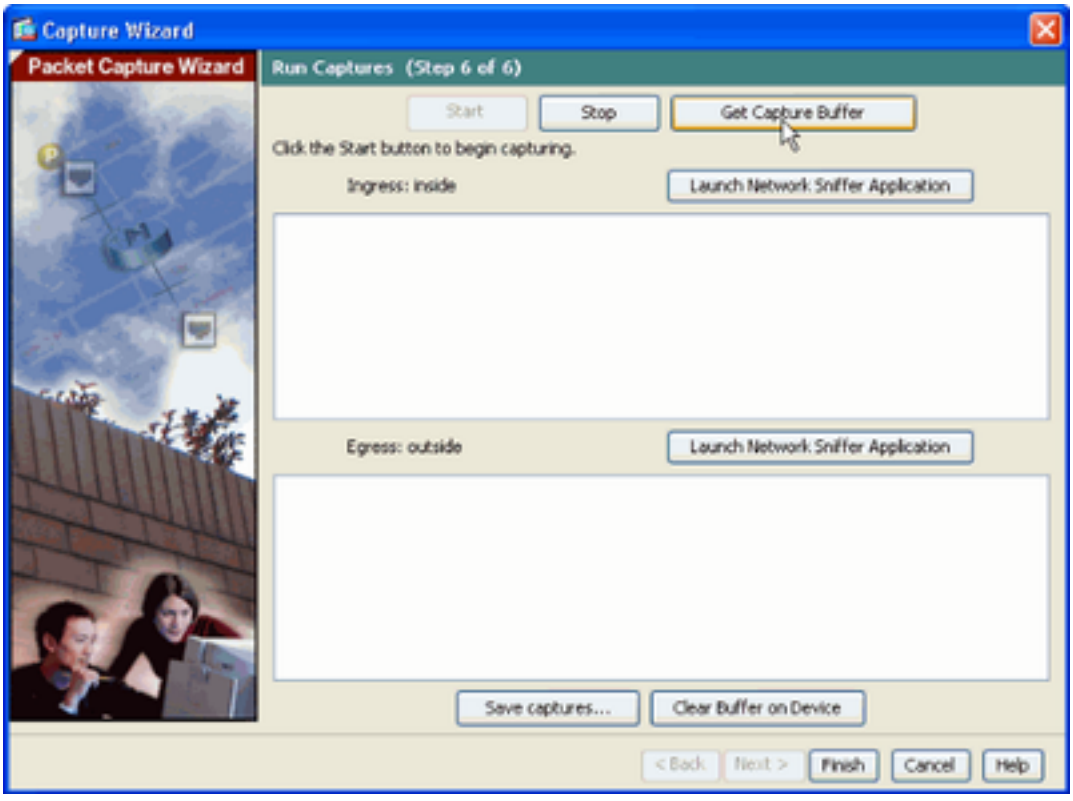


7. 클릭 **Start** 패킷 캡처를 시작하려면 다음과 같이 하십시오.



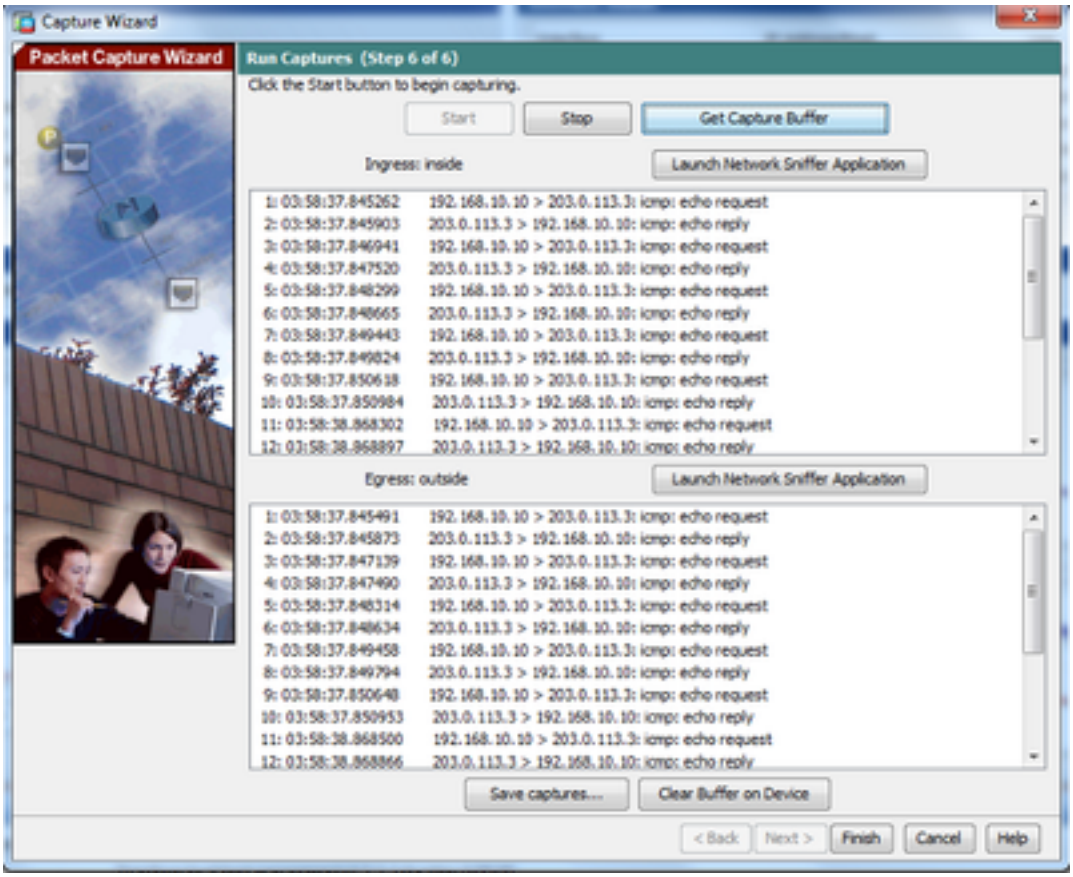
패킷 캡처가 시작되면 소스 및 목적지 IP 주소 간에 흐르는 패킷이 ASA 캡처 버퍼에 캡처되도록 내부 네트워크에서 외부 네트워크에 ping을 시도합니다.

8. 클릭 **Get Capture Buffer** ASA 캡처 버퍼에서 캡처한 패킷을 보려면 다음을 수행합니다.



인그레스 및 이그레스 트래픽에 대해 캡처된 패킷이 이 창에 표시됩니다.

9. 클릭 **Save captures** 캡처 정보를 저장합니다.

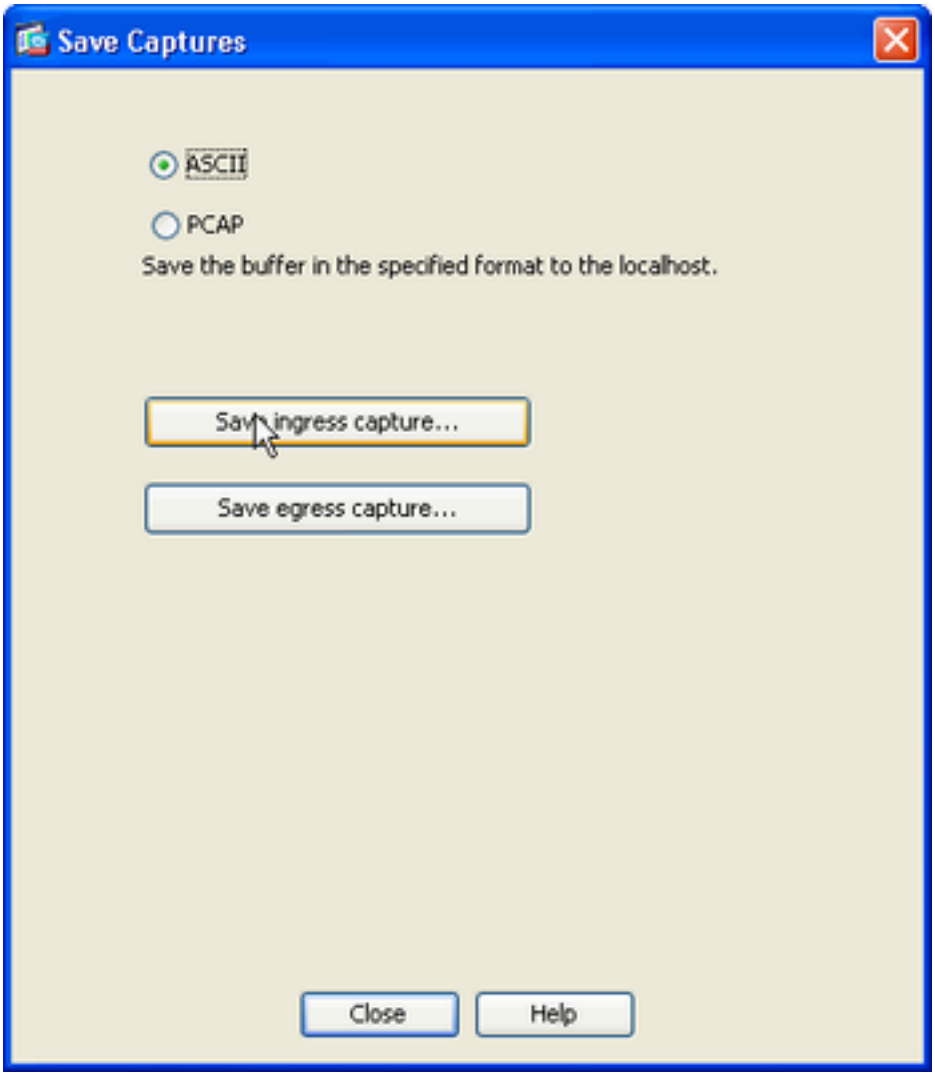


10.1 **Save captures** 창에서 캡처 버퍼를 저장할 필수 형식을 선택합니다.

10.2 ASCII 또**는** PCAP**입니다**. 형식 이름 옆의 라디오 버튼을 클릭합니다.

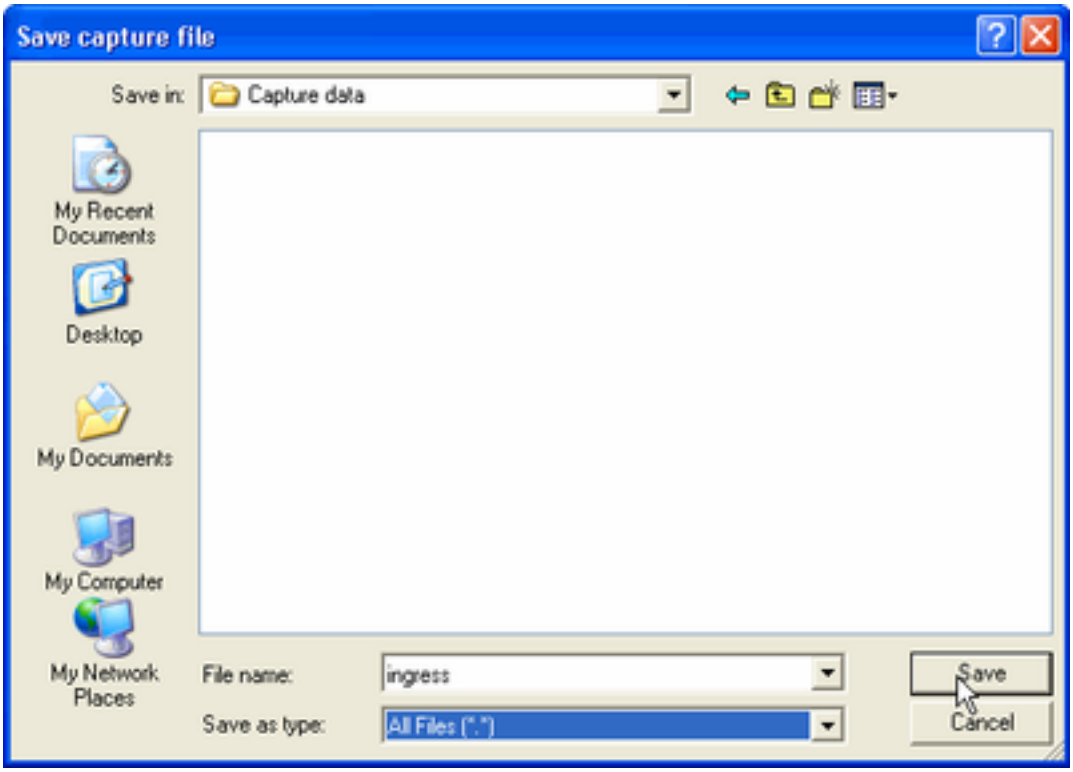
10.3 그런 다음 **Save ingress capture** 또는 **Save egress capture** 제공합니다.

PCAP 파일은 다음과 같은 캡처 분석기로 열 수 있습니다 **Wireshark** 및 이 방법이 기본 방법입니다.

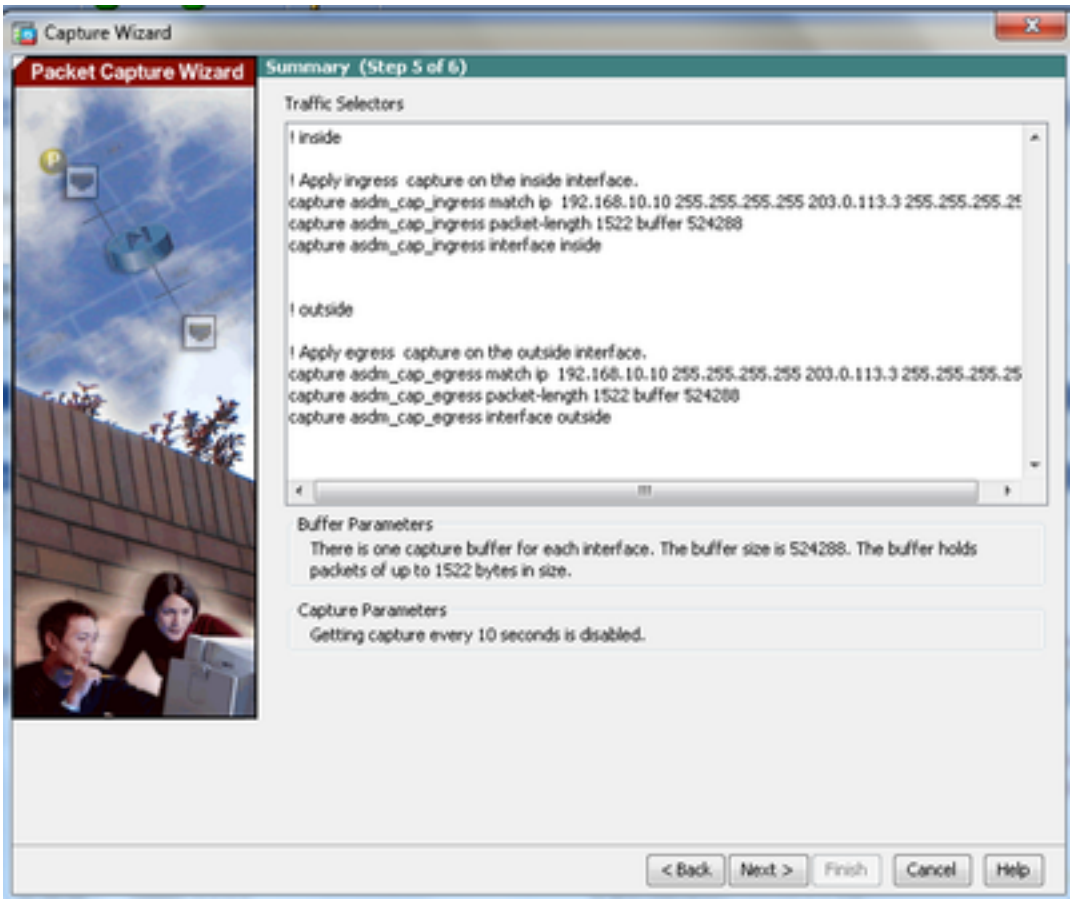


11.1 **Save capture file** 창에서 파일 이름과 캡처 파일을 저장할 위치를 제공합니다.

11.2 클릭 **Save**.



12. 클릭 **Finish.**



이렇게 하면 GUI 패킷 캡처 절차가 완료됩니다.

CLI로 패킷 캡처 구성

CLI를 사용하여 ASA에서 패킷 캡처 기능을 구성하려면 다음 단계를 완료하십시오.

1. 올바른 IP 주소 및 보안 수준으로 네트워크 다이어그램에 표시된 대로 내부 및 외부 인터페이스를 구성합니다.

2. 특권 EXEC 모드에서 capture 명령을 사용하여 패킷 캡처 프로세스를 시작합니다. 이 컨피그레이션 예에서는 capin이라는 캡처**가** 정의됩니다. **내부** 인터페이스에 **바인딩하고**, **match** 키워드로 관심 트래픽과 일치하는 패킷만 캡처하도록 지정합니다.

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

3. 마찬가지로 capout이라는 캡처**가** 정의됩니다. **외부** 인터페이스에 **바인딩하고**, **match** 키워드로 관심 트래픽과 일치하는 패킷만 캡처하도록 지정합니다.

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

이제 ASA가 인터페이스 간의 트래픽 흐름을 캡처하기 시작합니다. 언제든지 캡처를 중지하려

면 no capture 명령 다음에 캡처 이름을 입력합니다.

예를 들면 다음과 같습니다.

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

ASA에서 사용 가능한 캡처 유형

이 섹션에서는 ASA에서 사용할 수 있는 여러 유형의 캡처에 대해 설명합니다.

- **asa_dataplane** - ASA와 백플레인을 사용하는 모듈(예: ASA CX 또는 IPS 모듈) 사이를 통과하는 ASA 백플레인의 패킷을 캡처합니다.

```
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 - 가속화된 보안 경로에 의해 삭제된 패킷을 캡처합니다. drop-code는 가속화된 보안 경로에 의해 삭제되는 트래픽의 유형을 지정합니다.

```
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 - 캡처할 이더넷 유형을 선택합니다. 지원되는 이더넷 유형에는 8021Q, ARP, IP, IP6, LACP, PPPOED, PPPOES, RARP 및 VLAN이 있습니다.

다음 예에서는 ARP 트래픽을 캡처하는 방법을 보여 줍니다.

```
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** - 캡처된 패킷을 실시간으로 지속적으로 표시합니다. 실시간 패킷 캡처를 종료하려면 Ctrl-C를 누릅니다. 캡처를 영구적으로 제거하려면 이 명령의 no 형식을 사용합니다.
- 이 옵션은 **cluster exec capture** 명령을 실행합니다.

```
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** - ASA 패킷 추적기 기능과 유사한 방식으로 캡처된 패킷을 추적합니다.

```
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
```

참고: ASA 9.10+에서 any 키워드는 ipv4 주소의 패킷만 캡처합니다. any6 키워드는 모든 ipv6 주소 지정 트래픽을 캡처합니다.

패킷 캡처를 사용하여 구성할 수 있는 고급 설정입니다.

설정 방법에 대한 명령 참조 가이드를 참조하십시오.

- **ikev1/ikev2** - IKEv1(Internet Key Exchange Version 1) 또는 IKEv2 프로토콜 정보만 캡처합니다.
- **isakmp** - VPN 연결을 위해 ISAKMP(Internet Security Association and Key Management Protocol) 트래픽을 캡처합니다. ISAKMP 하위 시스템은 상위 계층 프로토콜에 액세스할 수 없습니다. 캡처는 의사 캡처이며 PCAP 파서를 만족시키기 위해 물리적, IP 및 UDP 레이어가 함께 결합됩니다. 피어 주소는 SA 교환에서 가져와 IP 레이어에 저장됩니다.
- **lacp** - LACP(Link Aggregation Control Protocol) 트래픽을 캡처합니다. 구성된 경우 인터페이스 이름은 물리적 인터페이스 이름입니다. 이는 LACP의 현재 동작을 식별하기 위해 Etherchannel로 작업할 때 유용합니다.

- **tls-proxy** - 하나 이상의 인터페이스에 있는 TLS(Transport Layer Security) 프록시에서 해독된 인바운드 및 아웃바운드 데이터를 캡처합니다.

- **webvpn** - 특정 WebVPN 연결에 대한 WebVPN 데이터를 캡처합니다.

  주의: WebVPN 캡처를 활성화하면 보안 어플라이언스의 성능에 영향을 줍니다. 문제 해결에 필요한 캡처 파일을 생성한 후 캡처를 비활성화해야 합니다.

기본값

다음은 ASA 시스템 기본값입니다.

- 기본 유형은 raw-data입니다.
- 기본 버퍼 크기는 512KB입니다.
- 기본 이더넷 유형은 IP 패킷입니다.
- 기본 packet-length는 1,518바이트입니다.

캡처된 패킷 보기

ASA에서

캡처된 패킷을 보려면 show capture 명령 다음에 캡처 이름을 입력합니다. 이 섹션에서는 캡처 버퍼 내용의 **show** 명령 출력을 제공합니다. 이 **show capture capin** 명령은 이름이 인 캡처 버퍼의 내용을 표시합니다 **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
```

이 **show capture capout** 명령은 이름이 인 캡처 버퍼의 내용을 표시합니다 **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
```

오프라인 분석을 위해 ASA에서 다운로드

분석용 패킷 캡처를 오프라인으로 다운로드하는 방법에는 두 가지가 있습니다.

1. 탐색 https://<ip_of_asa>/admin/capture/<capture_name>/pcap사용할 수 있습니다.

   팁: Cisco의 **pcap** 키워드를 사용하면 **show capture** 명령 출력이 제공됩니다.

1. 캡처를 다운로드하려면 copy capture 명령과 기본 파일 전송 프로토콜을 입력합니다.

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

   팁: 패킷 캡처 사용과 관련된 문제를 해결할 때 오프라인 분석을 위해 캡처를 다운로드하는 것이 좋습니다.

캡처 지우기

캡처 버퍼를 지우려면 **clear capture** 명령을 사용합니다:

```
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
```

다음을 입력합니다. **clear capture /all** 명령을 사용하여 모든 캡처에 대한 버퍼를 지웁니다.

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

캡처 중지

ASA에서 캡처를 중지하는 유일한 방법은 다음 명령을 사용하여 캡처를 완전히 비활성화하는 것입니다.

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

다음을 확인합니다.

현재 이 설정에 사용 가능한 확인 절차는 없습니다.

문제 해결

현재 이 구성에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.