PIX/ASA 7.2(1) 이상:인터페이스 내 통신

목차

소개

이 문서는 소프트웨어 릴리스 7.2(1) 이상에서 작동하는 ASA(Adaptive Security Appliance) 또는 PIX에서 인터페이스 내 통신을 활성화할 때 발생하는 일반적인 문제를 해결하는 데 도움이 됩니다.소프트웨어 릴리스 7.2(1)에는 동일한 인터페이스에서 암호화되지 않은 텍스트 데이터를 송수신하는 기능이 포함되어 있습니다.이 기능을 **활성화하려면 same-security-traffic permit intra-interface** 명령을 입력합니다.이 문서에서는 네트워크 관리자가 이 기능을 활성화했거나 향후에 사용할 계획을 가지고 있다고 가정합니다.CLI(Command Line Interface)를 사용하여 컨피그레이션 및 트러블슈팅을 제공합니다.

참고: 이 문서에서는 ASA가 도착하고 나가는 일반(암호화되지 않은) 데이터에 초점을 맞춥니다.암호화된 데이터는 논의되지 않습니다.

IPsec 컨피그레이션을 위해 ASA/PIX에서 인터페이스 내 통신을 활성화하려면 Stick 컨피그레이션 예제의 PIX/ASA 및 VPN Client for Public Internet VPN을 참조하십시오.

ASA에서 SSL 컨피그레이션을 위해 인터페이스 내 통신을 활성화하려면 ASA 7.2(2)를 참조하십시오.Stick Configuration 예제의 공용 인터넷 VPN용 SSL VPN 클라이언트(SVC).

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 액세스 목록
- 라우팅
- AIP-SSM(Advanced Inspection and Prevention-Security Services Module) IPS(Intrusion Prevention System) - 이 모듈에 대한 정보는 모듈이 설치 및 작동하는 경우에만 필요합니다.
- IPS 소프트웨어 릴리스 5.x - AIP-SSM을 사용하지 않는 경우 IPS 소프트웨어에 대한 지식이 필요하지 않습니다.

사용되는 구성 요소

- ASA 5510 7.2(1) 이상
- IPS 소프트웨어 5.1.1을 작동하는 AIP-SSM-10

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

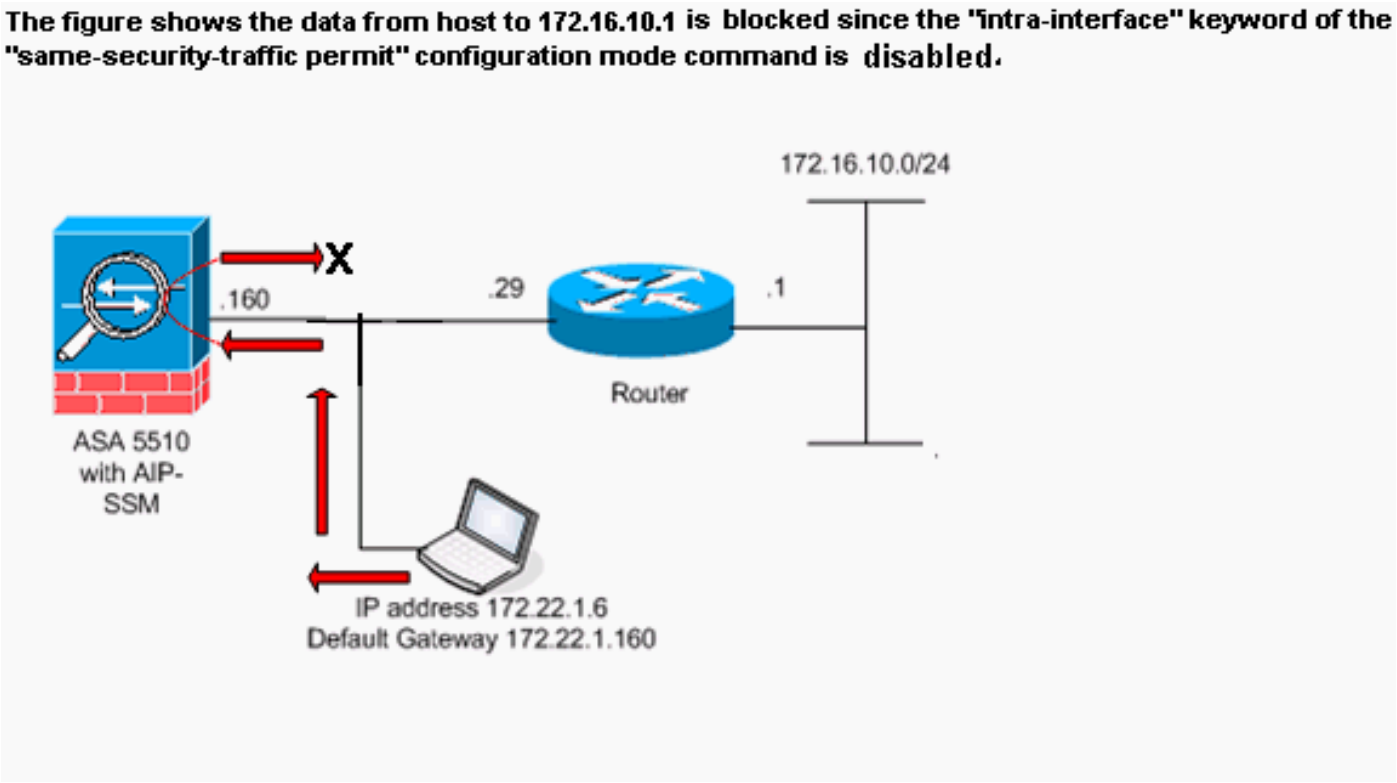
관련 제품

이 컨피그레이션은 버전 7.2(1) 이상을 실행하는 Cisco 500 Series PIX에서도 사용할 수 있습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

배경 정보



참고: 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다.이는 실

습 환경에서 사용된 RFC 1918 주소입니다.

다음 표에서는 ASA 시작 컨피그레이션을 보여 줍니다.

ASA

```
ciscoasa#show running-config
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
!--- The IP addressing assigned to interfaces. interface
Ethernet0/0 nameif inside security-level 100 ip address
10.1.1.2 255.255.255.0 ! interface Ethernet0/1 nameif
outside security-level 0 ip address 172.22.1.160
255.255.255.0 ! interface Ethernet0/2 shutdown no nameif
no security-level no ip address ! interface
Management0/0 shutdown no nameif no security-level no ip
address ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode
passive !--- Notice that there are no access-lists.
pager lines 24 logging enable logging buffered debugging
mtu inside 1500 mtu outside 1500 no asdm history enable
arp timeout 14400 !--- There are no network address
translation (NAT) rules. !--- The static routes are
added for test purposes. route inside 10.2.2.0
255.255.255.0 10.1.1.100 1 route outside 172.16.10.0
255.255.255.0 172.22.1.29 1 timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225
1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip
0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00 timeout uauth 0:05:00 absolute no
snmp-server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart telnet timeout 5 ssh timeout 5 console timeout
0 ! class-map inspection_default match default-
inspection-traffic ! ! policy-map type inspect dns
preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323 h225
inspect h323 ras inspect netbios inspect rsh inspect
rtsp inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global prompt hostname context
Cryptochecksum:
```

문제 해결

이 섹션에서는 인터페이스 내 통신과 관련된 여러 컨피그레이션 시나리오, 관련 syslog 메시지 및 패킷 추적기 출력을 설명합니다.

인터페이스 내 통신이 활성화되지 않음

ASA 구성에서 호스트 172.22.1.6은 호스트 172.16.10.1에 ping을 시도합니다. 호스트 172.22.1.6은

ICMP 에코 요청 패킷을 기본 게이트웨이(ASA)에 전송합니다. ASA에서 인터페이스 내 통신이 활성화되지 않았습니다.ASA는 에코 요청 패킷을 삭제합니다.테스트 ping이 실패합니다.ASA는 문제를 해결하는 데 사용됩니다.

다음 예에서는 syslog 메시지 및 패킷 추적기의 출력을 보여 줍니다.

- 버퍼에 로깅된 syslog 메시지입니다.

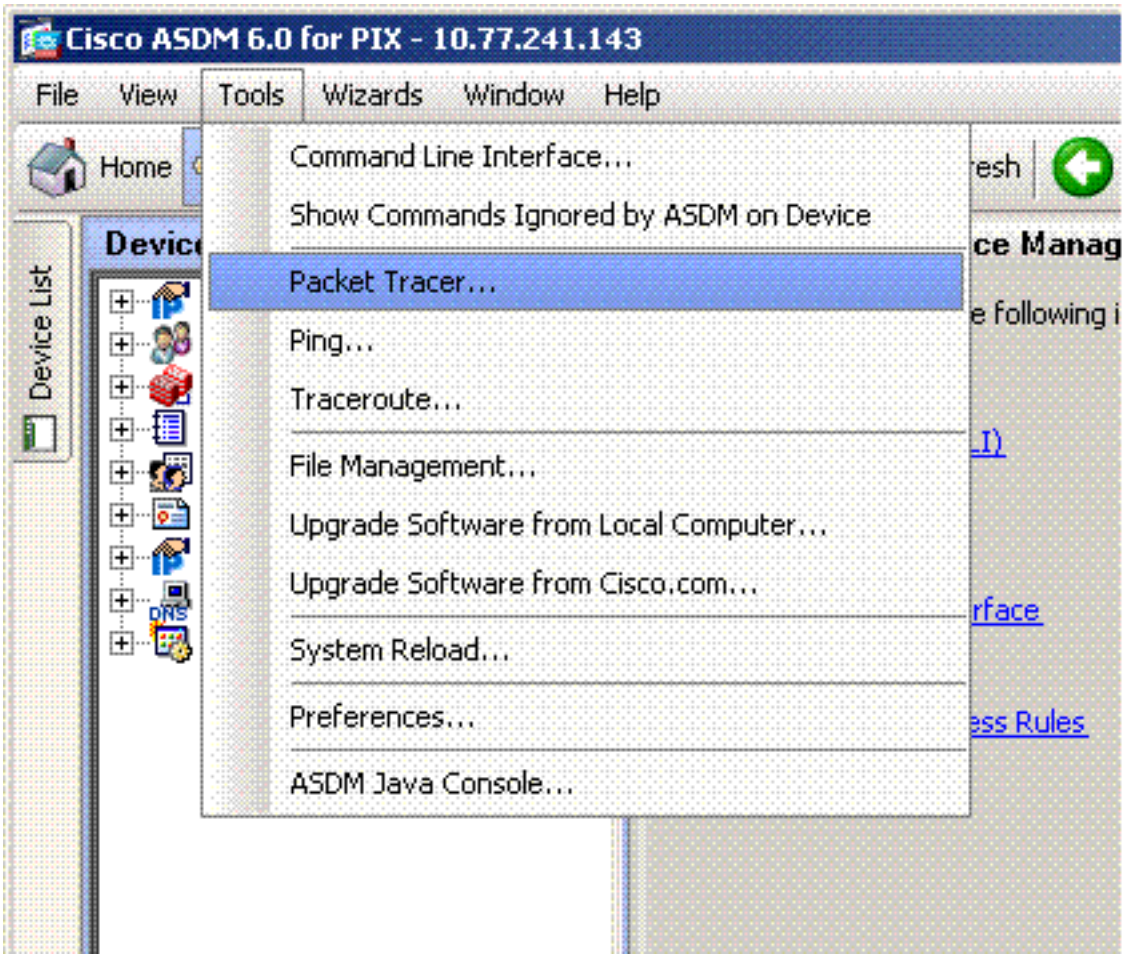
```
ciscoasa(config)#show logging
!--- Output is suppressed. %ASA-3-106014: Deny inbound icmp src outside:172.22.1.6 dst
outside:172.16.10.1 (type 8, code 0)
```

- 패킷 추적기 출력입니다.

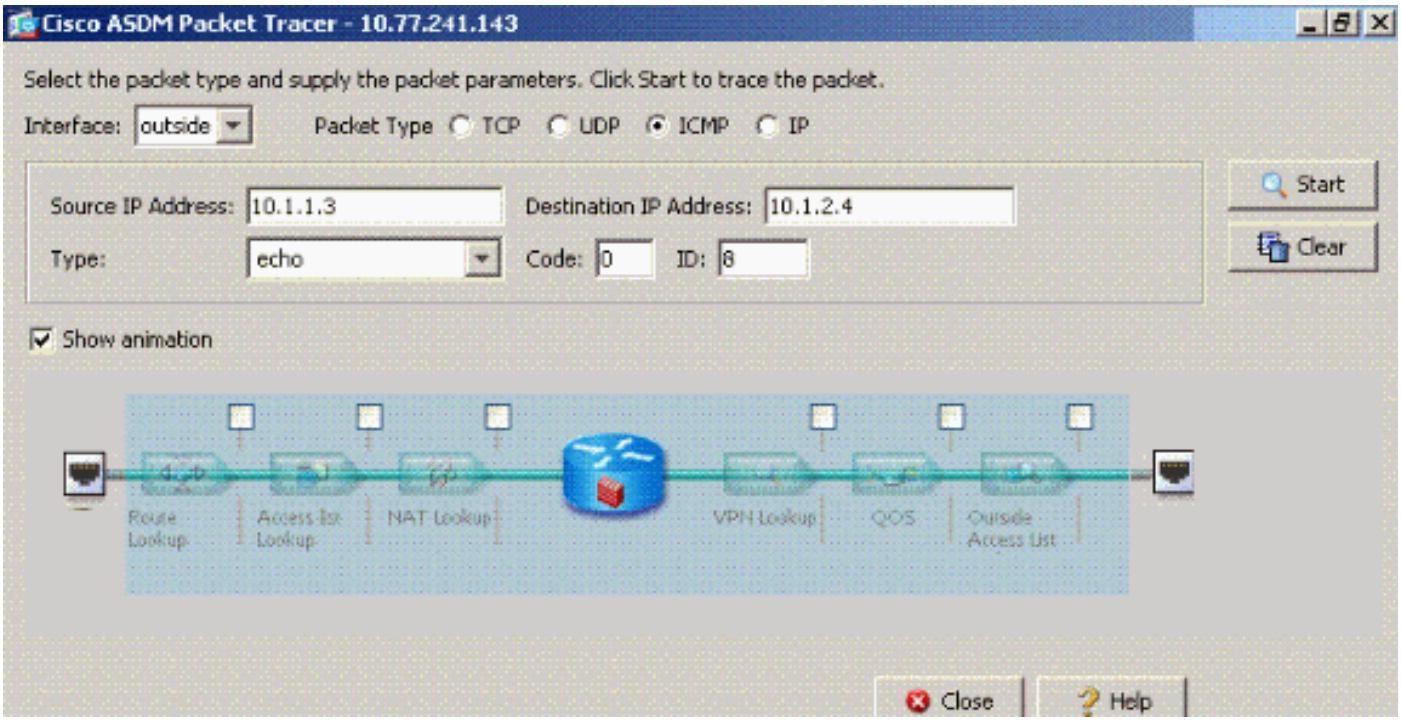
```
ciscoasa(config)#packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1 detailed
Phase: 1
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found no matching flow, creating a new flow

Phase: 2
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in   172.16.10.0     255.255.255.0   outside

Phase: 3
Type: ACCESS-LIST
Subtype:
Result: DROP

Config:
Implicit Rule

!--- Implicit rule refers to configuration rules not configured !--- by the user. By
default, intra-interface communication is not permitted. !--- In this example, the user has
not enabled intra-interface communications !--- and therefore the traffic is implicitly
denied. Additional Information: Forward Flow based lookup yields rule: in id=0x3bd8480,
priority=111, domain=permit, deny=true hits=0, user_data=0x0, cs_id=0x0, flags=0x4000,
protocol=0 src ip=0.0.0.0, mask=0.0.0.0, port=0 dst ip=0.0.0.0, mask=0.0.0.0, port=0 Result:
input-interface: outside input-status: up input-line-status: up output-interface: outside
output-status: up output-line-status: up Action: drop Drop-reason: (acl-drop) Flow is denied
by configured rule
```

다음 그림에는 ASDM의 CLI 명령과 동일한 명령이 나와 있습니다.

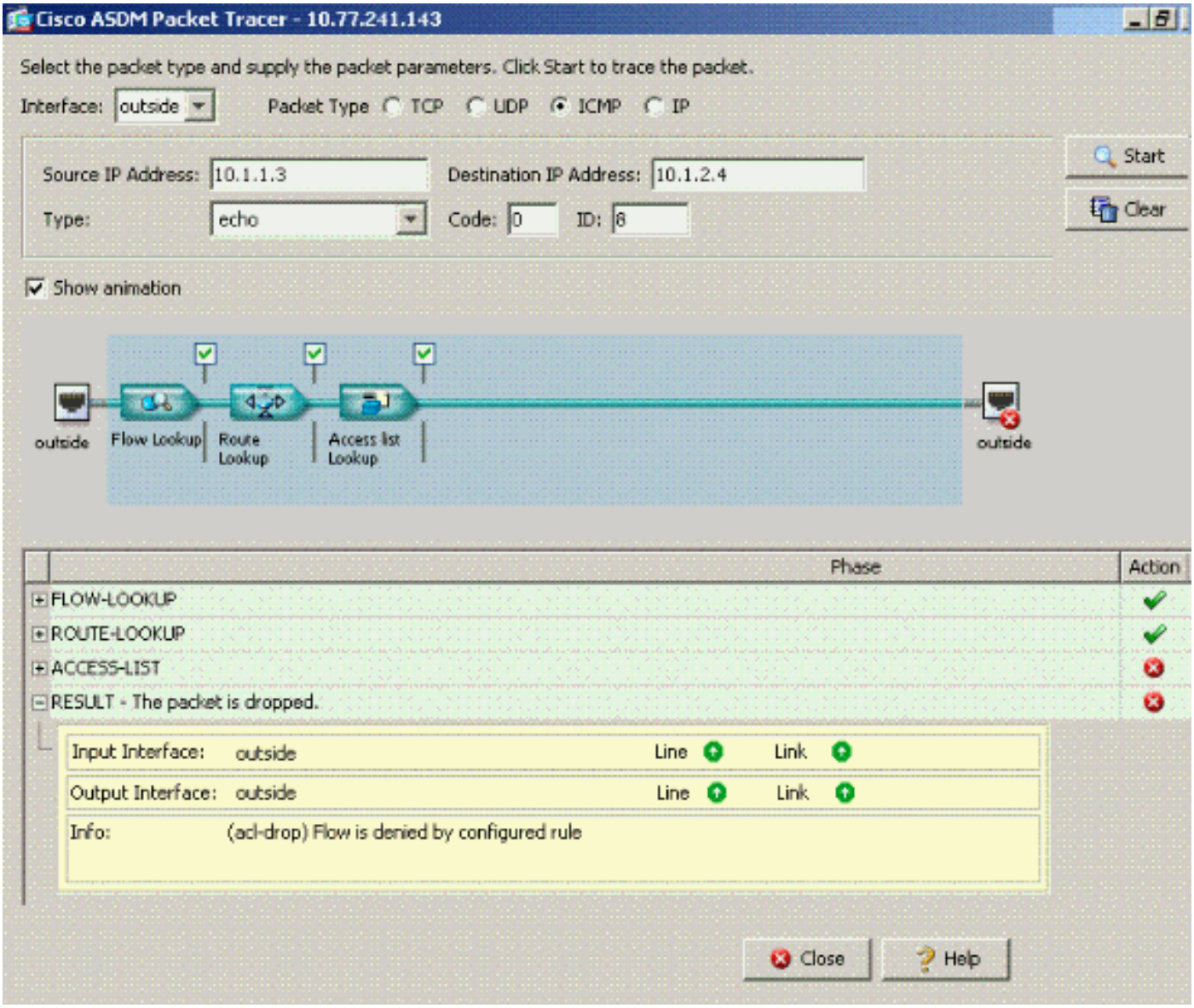
1단계:



2단계:



same-security-traffic을 사용하는 packet-tracer 출력**은 intra-interface 명령을 사용할 수 없도록** 설정합니다.



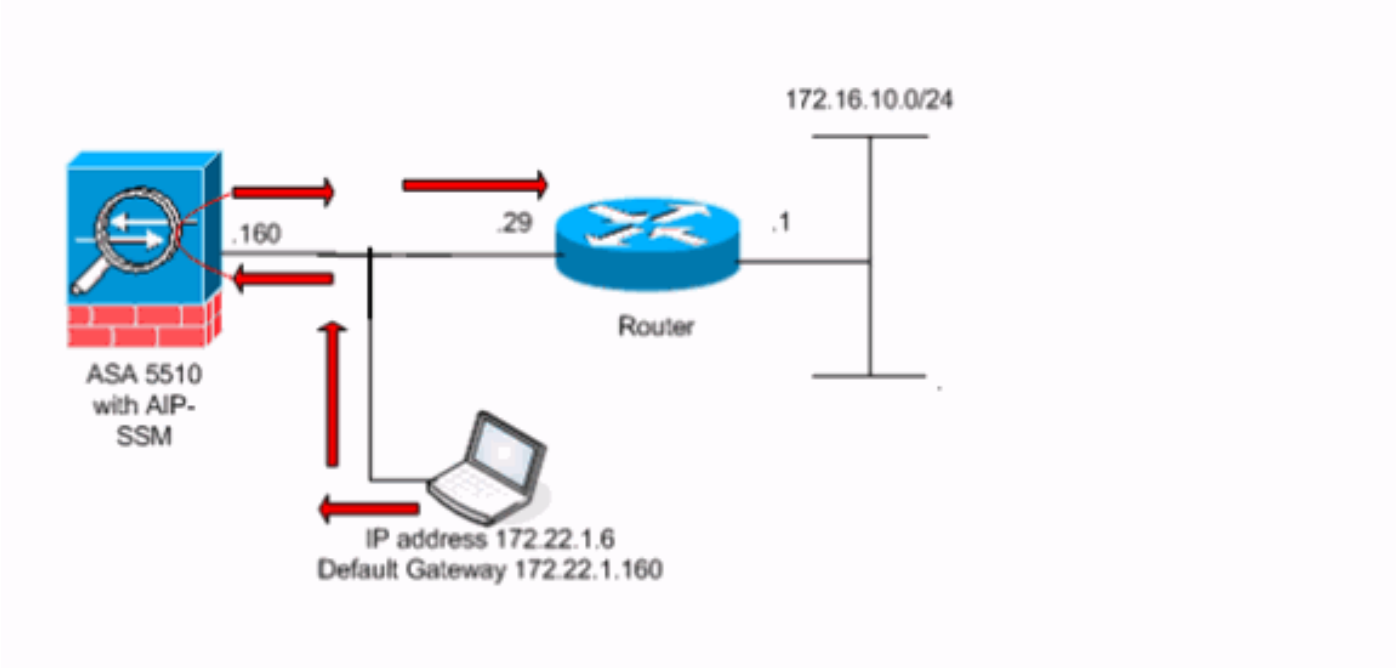
packet-tracer 출력 . . . 은 기본 컨피그레이션 설정이 트래픽을 차단하고 있음을 나타냅니다.관리자는 실행 중인 컨피그레이션을 확인하여 인터페이스 내 통신이 활성화되었는지 확인해야 합니다.이 경우 ASA 컨피그레이션에서는 인터페이스 내 통신을 활성화해야 합니다(**동일한 보안 트래픽**에서 **인터페이스 내**를 허용함).

```
ciscoasa#show running-config
!--- Output is suppressed. interface Ethernet5 shutdown no nameif no security-level no ip
address ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode passive same-security-traffic permit intra-
interface

!--- When intra-interface communications are enabled, the line !--- highlighted in bold font
appears in the configuration. The configuration line !--- appears after the interface
configuration and before !--- any access-list configurations. access-list... access-list...
```

인터페이스 내 통신 사용

이제 인터페이스 내 통신이 활성화됩니다.**same-security-traffic permit intra-interface** 명령이 이전 컨피그레이션에 추가됩니다.호스트 172.22.1.6은 호스트 172.16.10.1에 ping을 시도합니다. 호스트 172.22.1.6은 ICMP 에코 요청 패킷을 기본 게이트웨이(ASA)에 전송합니다. 호스트 172.22.1.6은 172.16.10.1의 성공적인 응답을 기록합니다. ASA는 ICMP 트래픽을 성공적으로 전달합니다.

The figure shows the data from host to 172.16.10.1 is allowed since the "intra-interface" keyword of the "same-security-traffic permit" configuration mode command is enabled.



다음 예에서는 ASA syslog 메시지 및 packet-tracer 출력을 보여 줍니다.

- 다음은 버퍼에 로깅된 syslog 메시지입니다.

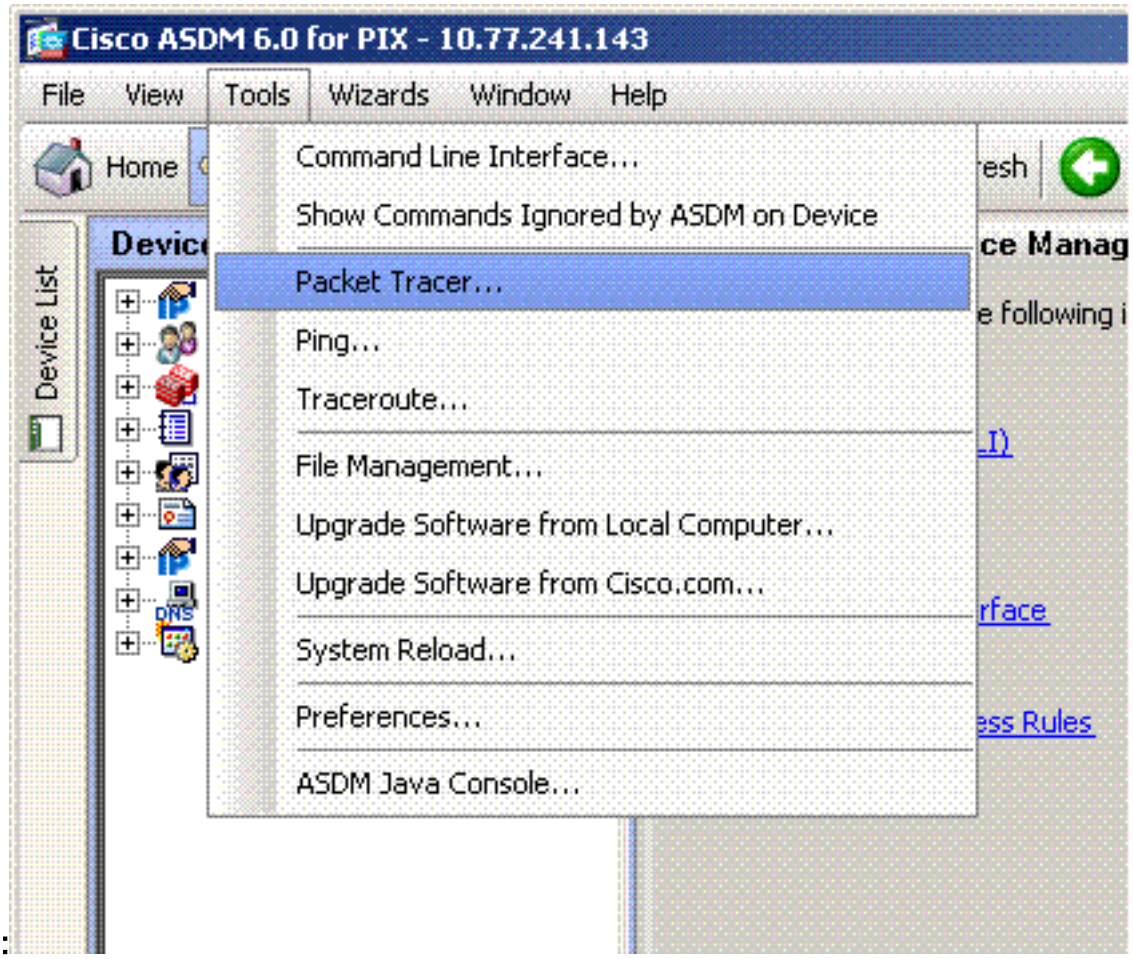
```
ciscoasa#show logging
!--- Output is suppressed. %PIX-7-609001: Built local-host outside:172.22.1.6 %PIX-7-609001:
Built local-host outside:172.16.10.1 %PIX-6-302020: Built ICMP connection for faddr
172.22.1.6/64560 gaddr 172.16.10.1/0 laddr 172.16.10.1/0 %PIX-6-302021: Teardown ICMP
connection for faddr 172.22.1.6/64560 gaddr 172.16.10.1/0 laddr 172.16.10.1/0 %PIX-7-609002:
Teardown local-host outside:172.22.1.6 duration 0:00:04 %PIX-7-609002: Teardown local-host
outside:172.16.10.1 duration 0:00:04
```

- 패킷 추적기 출력입니다.

```
ciscoasa(config)#packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1

Phase: 1
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found no matching flow, creating a new flow

Phase: 2
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in   172.16.10.0     255.255.255.0   outside

Phase: 3
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:

Phase: 4      (
```

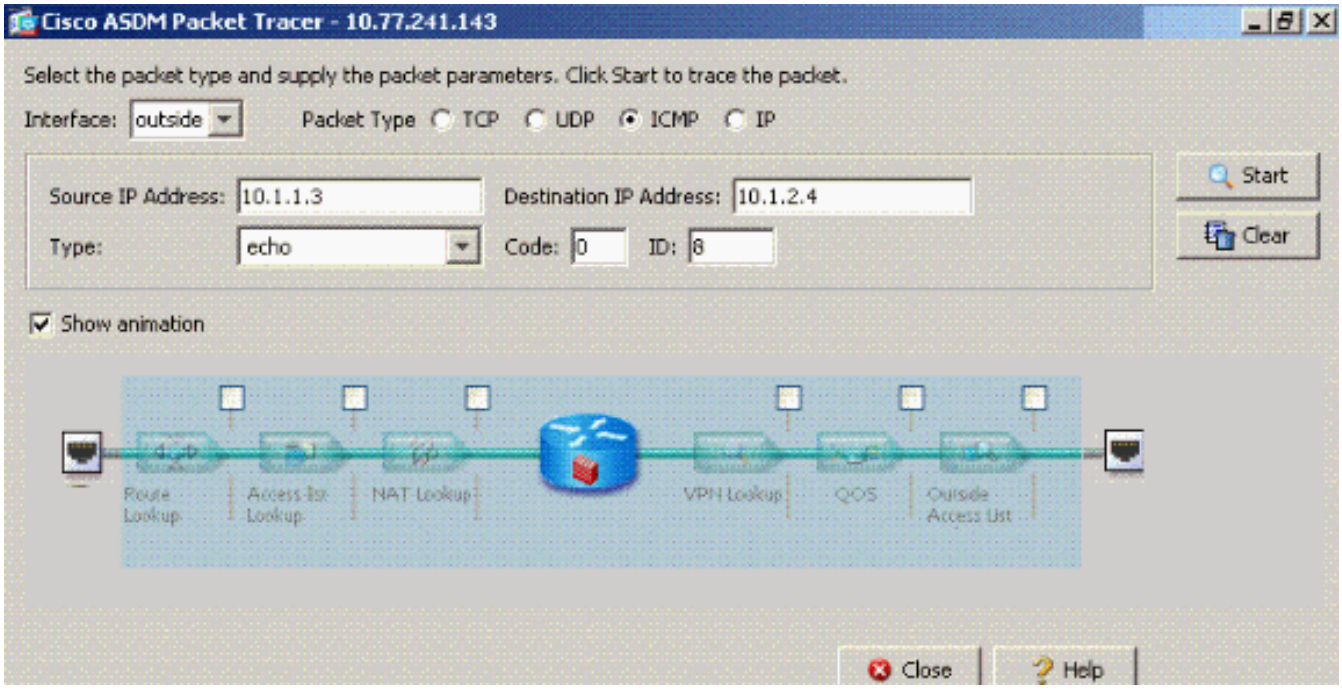
```
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 23, packet dispatched to next module

Phase: 7
Type: ROUTE-LOOKUP
Subtype: output and adjacency
Result: ALLOW
Config:
Additional Information:
found next-hop 172.22.1.29 using egress ifc outside
adjacency Active
next-hop mac address 0030.a377.f854 hits 0

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

다음 그림에는 ASDM의 CLI 명령과 동일한 명령이 나와 있습니다.**1단계**



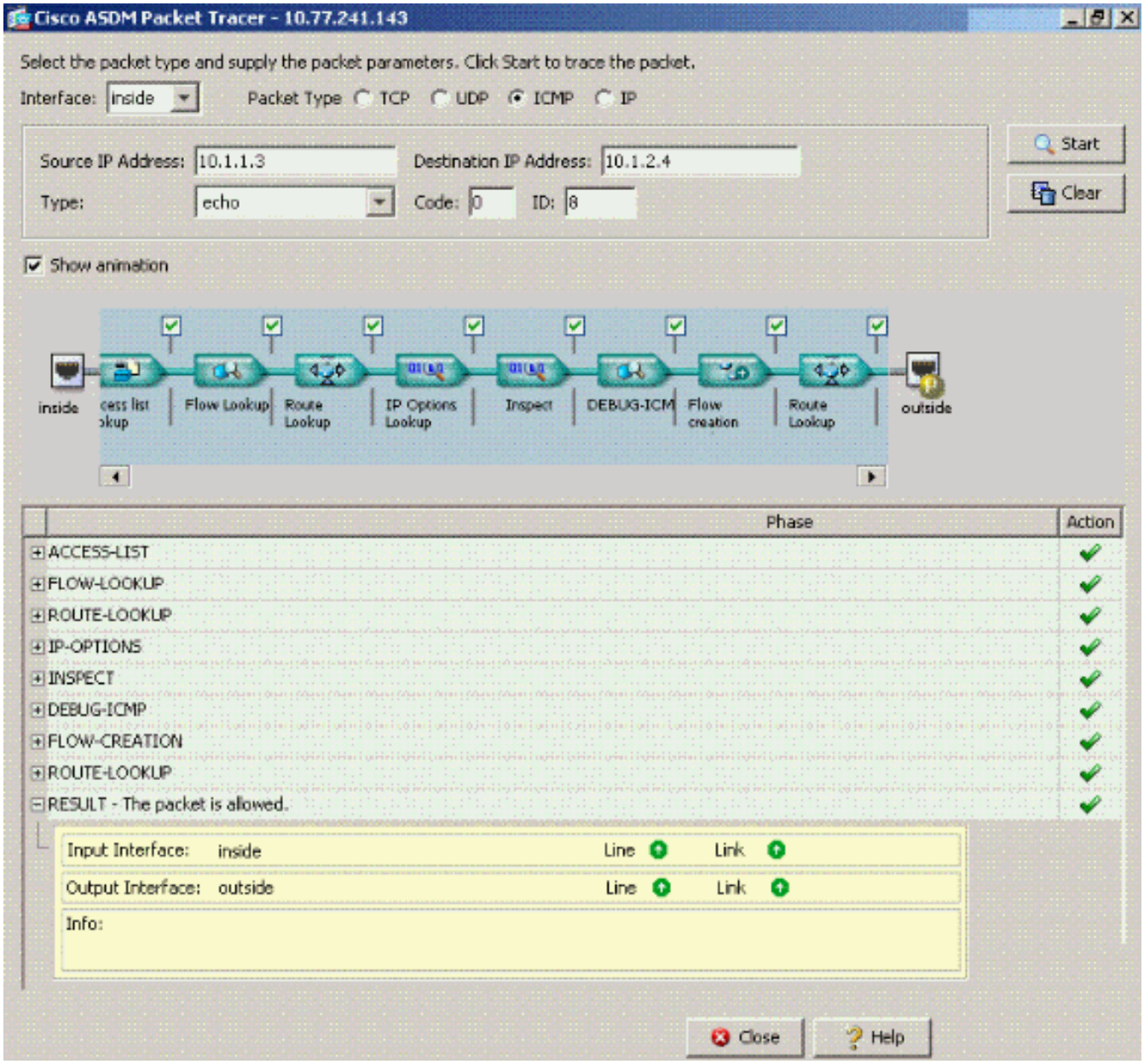
: **2단계**

:



same-security-traffic을 사용하는 packet-tracer 출력은 **intra-interface** 명령을 활성화합니다

.



참고: 외부 인터페이스에 액세스 목록이 적용되지 않습니다.샘플 컨피그레이션에서는 외부 인터페이스에 보안 레벨 0이 할당됩니다. 기본적으로 방화벽은 보안 수준이 낮은 인터페이스에서 보안 수준이 높은 인터페이스로의 트래픽을 허용하지 않습니다.그러면 관리자가 액세스 목록의 권한 없이 인터페이스 내 트래픽이 외부(낮은 보안) 인터페이스에서 허용되지 않는다고 생각할 수 있습니다.그러나 인터페이스에 access-list가 적용되지 않은 경우에도 동일한 인터페이스 트래픽이 자유롭게 전달됩니다.

인트라 인터페이스 활성화 및 검사를 위해 AIP-SSM에 전달된 트래픽

인터페이스 내 트래픽은 검사를 위해 AIP-SSM에 전달될 수 있습니다.이 섹션에서는 관리자가 AIP-SSM에 트래픽을 전달하도록 ASA를 구성했으며 관리자가 IPS 5.x 소프트웨어를 구성하는 방법을 알고 있다고 가정합니다.

이 시점에서 ASA 컨피그레이션에는 이전 샘플 컨피그레이션이 포함되며, 인터페이스 내 통신이 활성화되며 모든(any) 트래픽이 AIP-SSM으로 전달됩니다.IPS 서명 2004는 에코 요청 트래픽을 삭제하도록 수정되었습니다.호스트 172.22.1.6은 호스트 172.16.10.1에 ping을 시도합니다. 호스트 172.22.1.6은 ICMP 에코 요청 패킷을 기본 게이트웨이(ASA)에 전송합니다. ASA는 검사를 위해 에코 요청 패킷을 AIP-SSM에 전달합니다.AIP-SSM은 IPS 컨피그레이션에 따라 데이터 패킷을 삭제합니다.

다음 예에서는 ASA syslog 메시지 및 packet-tracer 출력을 보여 줍니다.

- 버퍼에 로깅된 syslog 메시지입니다.

```
ciscoasa(config)#show logging
!--- Output is suppressed. %ASA-4-420002: IPS requested to drop ICMP packet from
outside:172.22.1.6/2048 to outside:172.16.10.1/0 !--- ASA syslog message records the IPS
request !--- to drop the ICMP traffic.
```

- 패킷 추적기 출력입니다.

```
ciscoasa#packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1

Phase: 1
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found no matching flow, creating a new flow

Phase: 2
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in   172.16.10.0     255.255.255.0   outside

Phase: 3
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:

Phase: 4
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: IDS
Subtype:
Result: ALLOW

Config:
class-map traffic_for_ips match any policy-map global_policy class traffic_for_ips ips
inline fail-open service-policy global_policy global

!--- The packet-tracer recognizes that traffic is to be sent to the AIP-SSM. !--- The
packet-tracer does not have knowledge of how the !--- IPS software handles the traffic.
Additional Information: Phase: 7 Type: FLOW-CREATION Subtype: Result: ALLOW Config:
Additional Information: New flow created with id 15, packet dispatched to next module
Result: input-interface: outside input-status: up input-line-status: up output-interface:
outside output-status: up output-line-status: up Action: allow
```

```
!--- From the packet-tracer perspective the traffic is permitted. !--- The packet-tracer
does not interact with the IPS configuration. !--- The packet-tracer indicates traffic is
allowed even though the IPS !--- might prevent inspected traffic from passing.
```

관리자는 문제를 조사할 때 최대한 많은 문제 해결 도구를 사용해야 한다는 점에 유의해야 합니다 .이 예에서는 서로 다른 두 가지 문제 해결 도구를 사용하여 그림을 그리는 방법을 보여 줍니다.두 가지 툴을 함께 사용하면 완벽한 이야기를 얻을 수 있습니다.ASA 컨피그레이션 정책은 트래픽을 허용하지만 IPS 컨피그레이션은 허용하지 않습니다.

인터페이스에 적용된 인터페이스 내 활성화 및 액세스 목록

이 섹션에서는 이 문서의 원래 샘플 컨피그레이션, 인터페이스 내 통신이 활성화되고 테스트된 인터페이스에 적용되는 액세스 목록을 사용합니다.이러한 행이 구성에 추가됩니다.액세스 목록은 프로덕션 방화벽에서 구성할 수 있는 항목을 간단하게 나타낸 것입니다.

```
ciscoasa(config)#access-list outside_acl permit tcp any host 172.22.1.147 eq 80
ciscoasa(config)#access-group outside_acl in interface outside
!--- Production firewalls also have NAT rules configured. !--- This lab tests intra-interface
communications. !--- NAT rules are not required.
```

호스트 172.22.1.6은 호스트 172.16.10.1에 ping을 시도합니다. 호스트 172.22.1.6은 ICMP 에코 요청 패킷을 기본 게이트웨이(ASA)에 전송합니다. ASA는 access-list 규칙에 따라 에코 요청 패킷을 삭제합니다.호스트 172.22.1.6 테스트 ping에 실패합니다.

다음 예에서는 ASA syslog 메시지 및 packet-tracer 출력을 보여 줍니다.

- 버퍼에 로깅된 syslog 메시지입니다.

```
ciscoasa(config)#show logging
!--- Output is suppressed. %ASA-4-106023: Deny icmp src outside:172.22.1.6 dst
outside:172.16.10.1 (type 8, code 0) by access-group "outside_acl" [0xc36b9c78, 0x0]
```

- 패킷 추적기 출력입니다.

```
ciscoasa(config)#packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1 detailed

Phase: 1
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found no matching flow, creating a new flow

Phase: 2
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in   172.16.10.0     255.255.255.0   outside

Phase: 3
Type: ACCESS-LIST
Subtype:
Result: DROP

Config:
Implicit Rule

!--- The implicit deny all at the end of an access-list prevents !--- intra-interface
traffic from passing. Additional Information: Forward Flow based lookup yields rule: in
```

```
id=0x264f010, priority=11, domain=permit, deny=true hits=0, user_data=0x5, cs_id=0x0,
flags=0x0, protocol=0 src ip=0.0.0.0, mask=0.0.0.0, port=0 dst ip=0.0.0.0, mask=0.0.0.0,
port=0 Result: input-interface: outside input-status: up input-line-status: up output-
interface: outside output-status: up output-line-status: up Action: drop Drop-reason: (acl-
drop) Flow is denied by configured rule
```

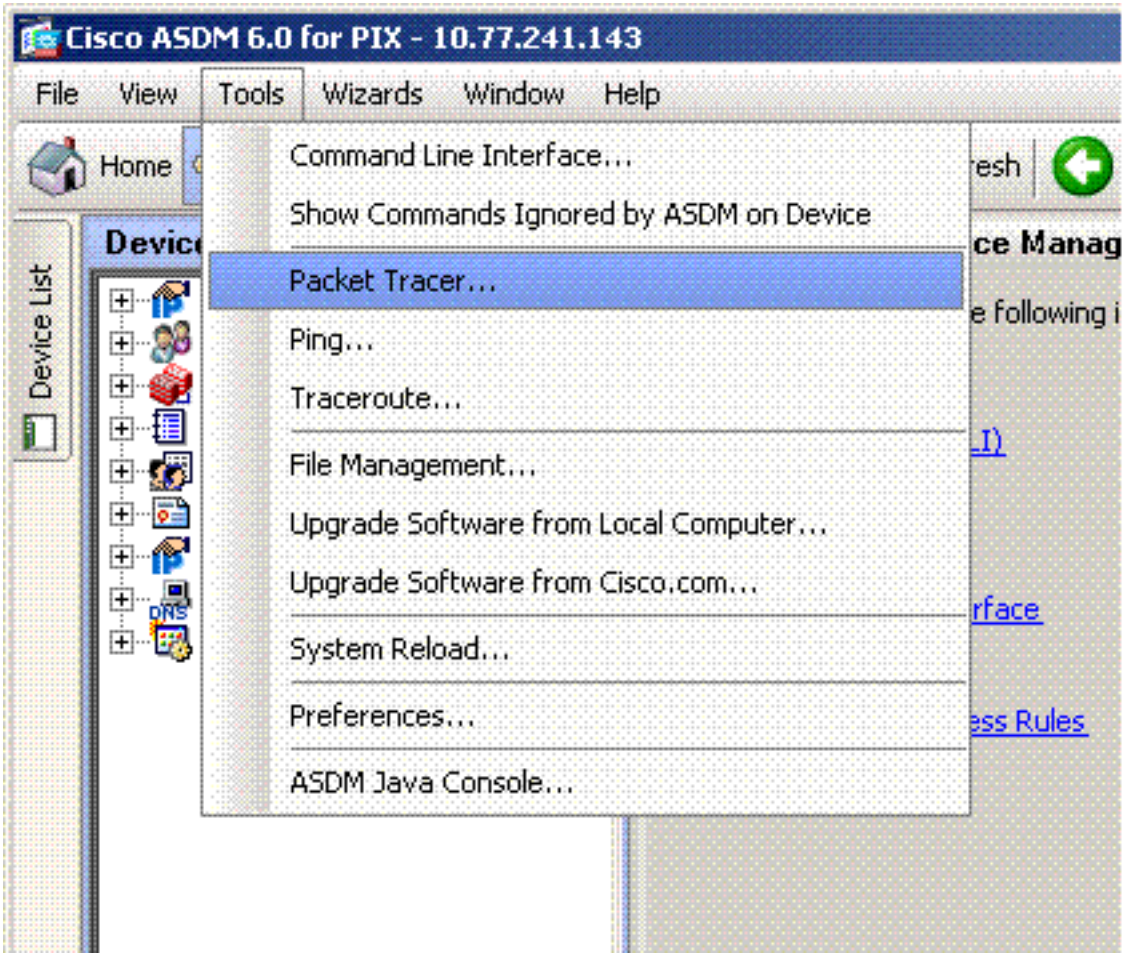
packet-tracer 명령에 대한 자세한 내용은 packet-tracer를 참조하십시오.

참고: 인터페이스에 적용된 액세스 목록에 deny 문이 포함되어 있으면 packet-tracer의 출력이 변경됩니다.예:

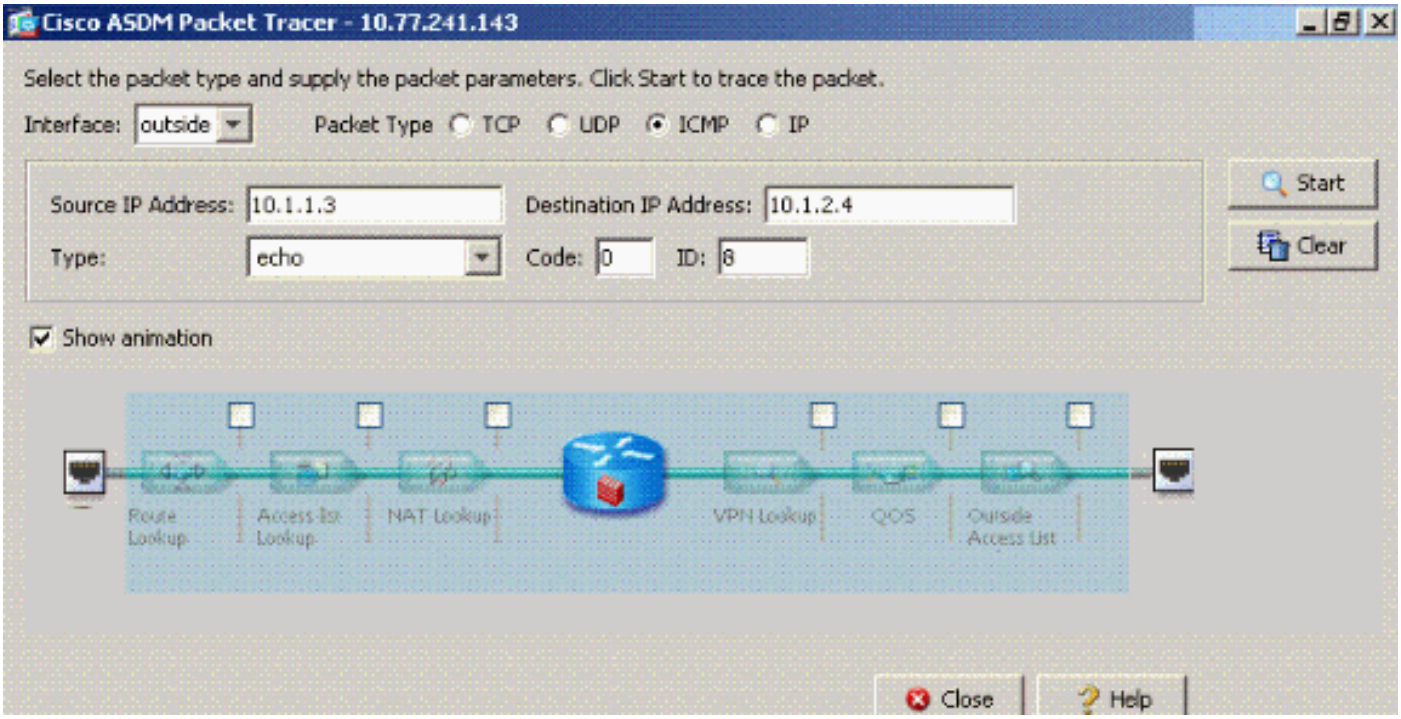
```
ciscoasa(config)#access-list outside_acl permit tcp any host 172.22.1.147 eq 80
ciscoasa(config)#access-list outside_acl deny ip any any
ciscoasa(config)#access-group outside_acl in interface outside
ciscoasa#packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1 detailed
!--- Output is suppressed. Phase: 3 Type: ACCESS-LIST Subtype: log Result: DROP Config: access-
group outside_acl in interface outside access-list outside_acl extended deny ip any any

Additional Information:
 Forward Flow based lookup yields rule:
```

ASDM의 위 CLI 명령과 동일한 명령이 다음 그림에 나와 있습니다.

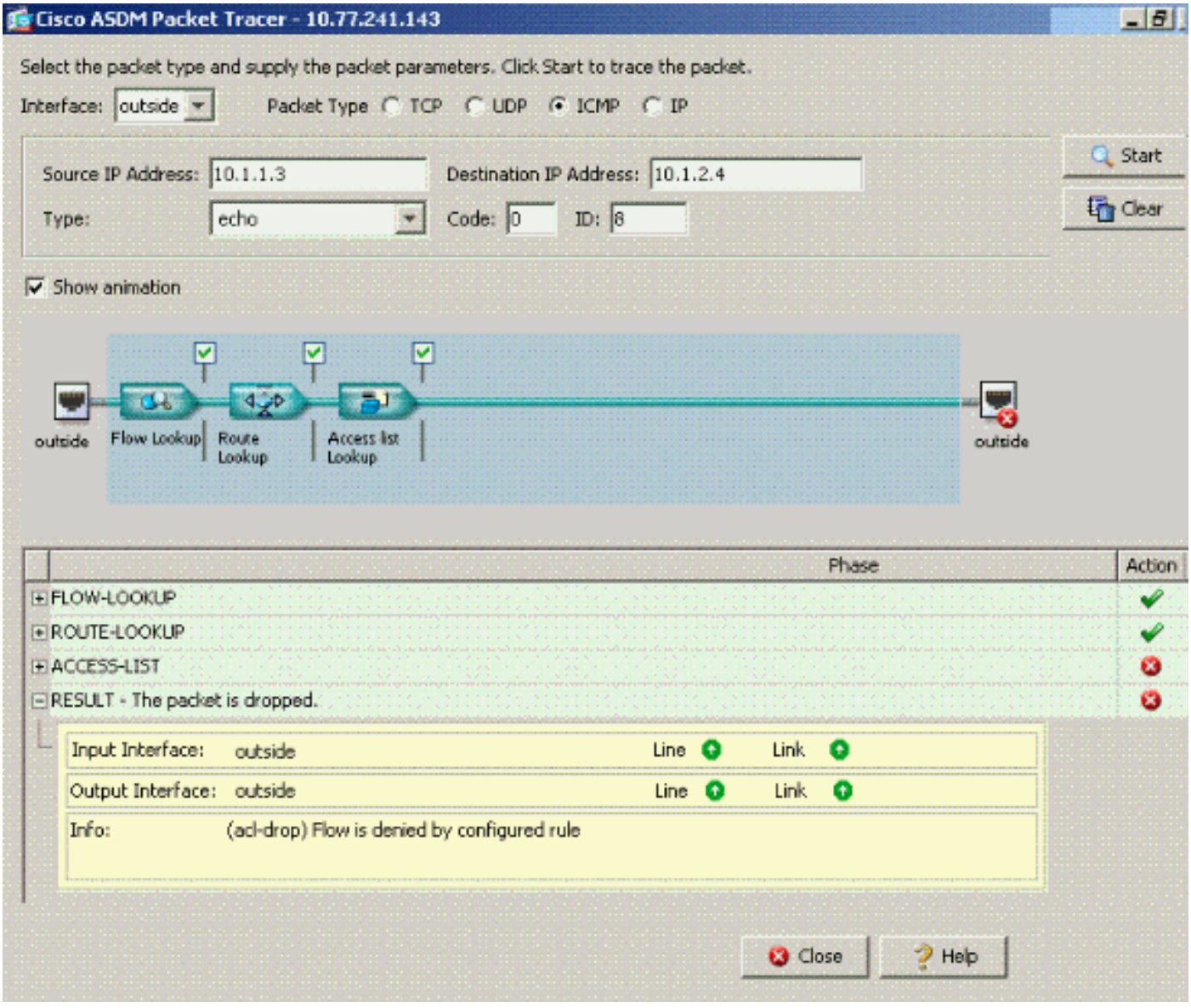
1단계:



2단계:



same-security-traffic을 사용하는 패킷 추적기 출력은 intra-**interface** 명령**을 활성화하고 access-list outside_acl extended deny ip any any** 명령**을** 패킷**을** 거부하도록 구성된 **any** 명령입니다.

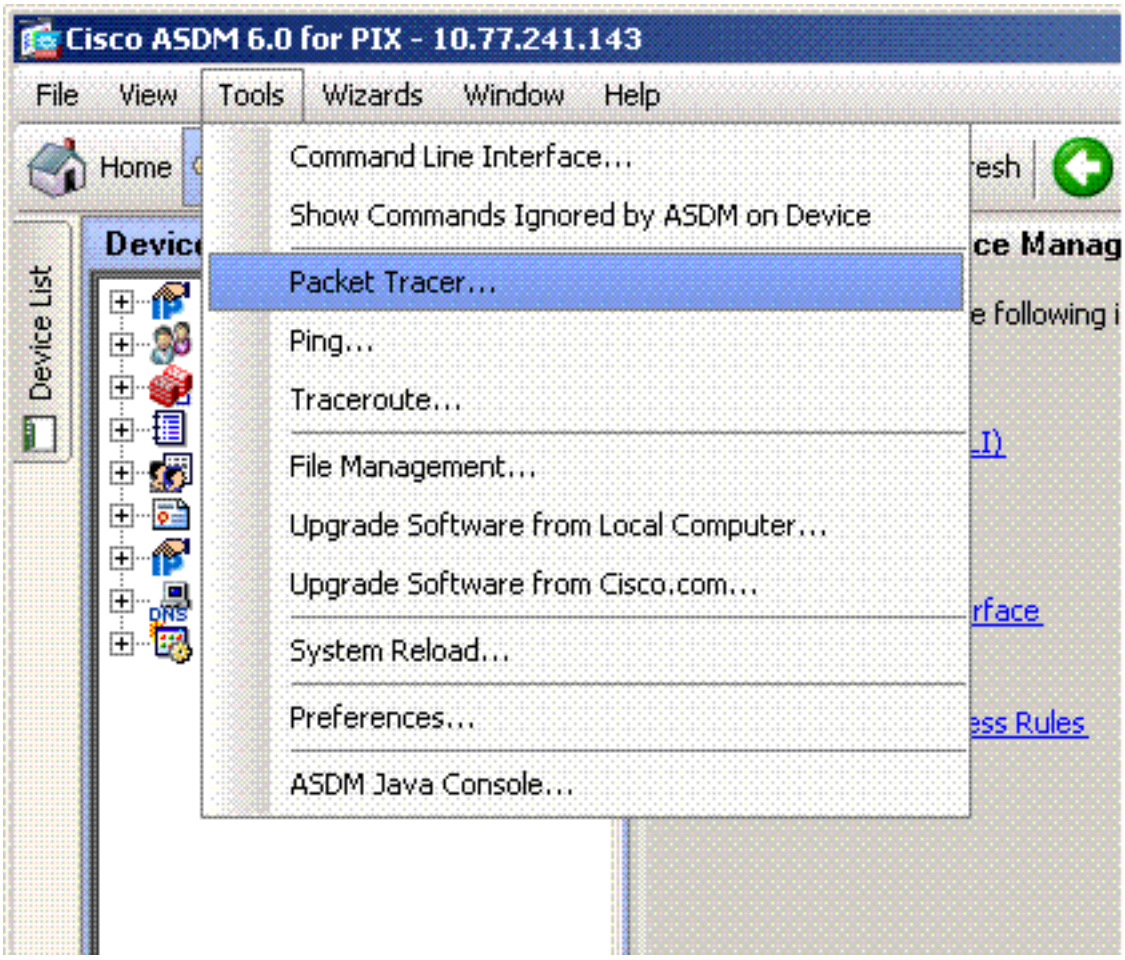


특정 인터페이스에서 인터페이스 내 통신이 필요하고 액세스 목록이 동일한 인터페이스에 적용되는 경우 access-list 규칙은 인터페이스 내 트래픽을 허용해야 합니다.이 섹션의 예제를 사용하여 액세스 목록을 다음과 같이 작성해야 합니다.

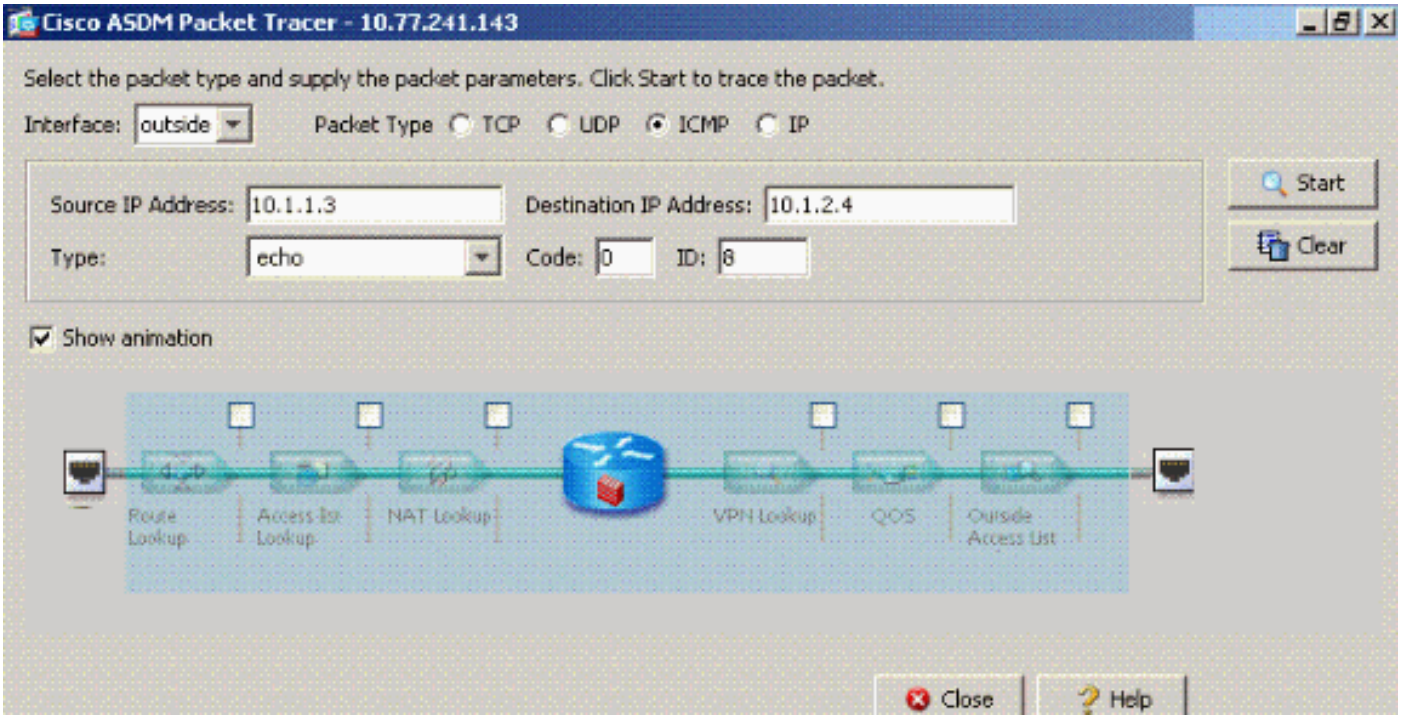
```
ciscoasa(config)#access-list outside_acl permit tcp any host 172.22.1.147 eq 80
ciscoasa(config)#access-list outside_acl permit ip 172.22.1.0 255.255.255.0 172.16.10.0
255.255.255.0
!--- 172.22.1.0 255.255.255.0 represents a locally !--- connected network on the ASA. !---
172.16.10.0 255.255.255.0 represents any network that !--- 172.22.1.0/24 needs to access.
ciscoasa(config)#access-list outside_acl deny ip any any
ciscoasa(config)#access-group outside_acl in interface outside
```

ASDM의 위 CLI 명령과 동일한 명령이 다음 그림에 나와 있습니다.

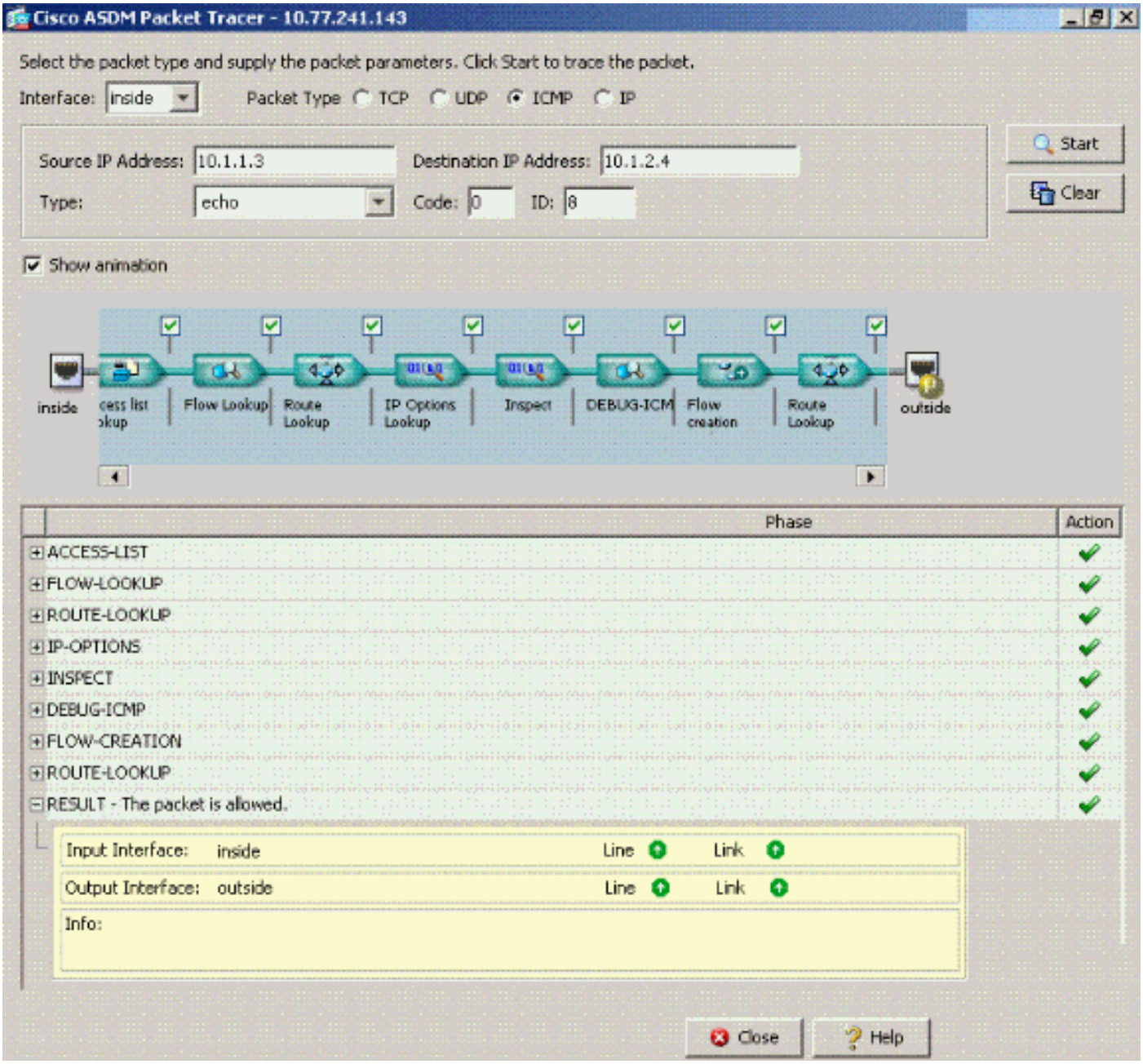
1단계:



2단계:



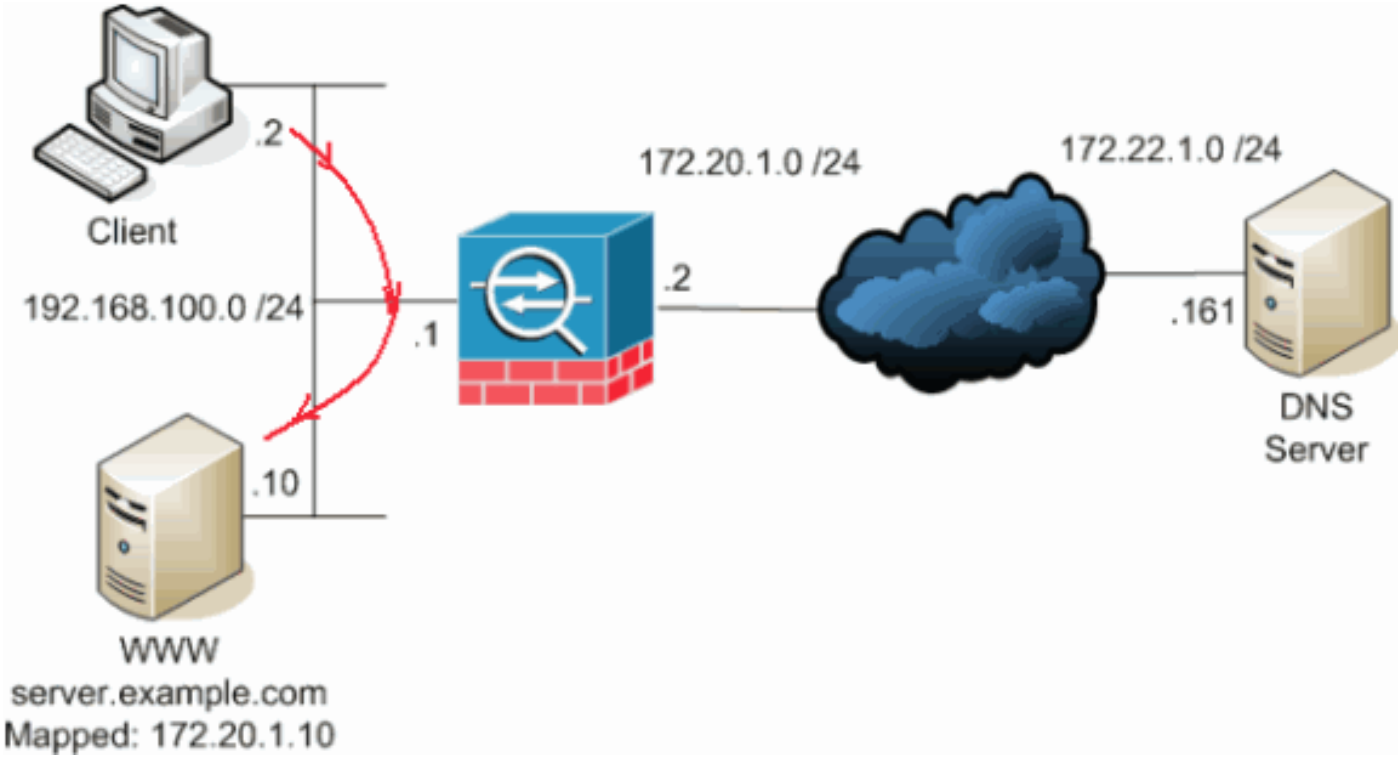
same-security-traffic을 사용하는 패킷 추적기 출력은 intra-**interface** 명령**을 활성화하고 access-list outside_acl extended deny ip any any** 명령이 **필요한** 인터페이스 내 트래픽이 필요한 동일한 인터페이스**에 구성된** any 명령을 **허용합니다**.



access-list 및 access-group 명령에 대한 자세한 내용은 access-list extended and access-group을 참조하십시오.

고정 및 NAT로 인터페이스 내 활성화

이 섹션에서는 내부 사용자가 공용 주소를 사용하여 내부 웹 서버에 액세스하려고 시도하는 시나리오를 설명합니다.



이 경우 192.168.100.2의 클라이언트는 WWW 서버의 공용 주소(예: 172.20.1.10)을 사용하려고 합니다. 클라이언트에 대한 DNS 서비스는 외부 DNS 서버 172.22.1.161에서 제공합니다. DNS 서버는 다른 공용 네트워크에 있으므로 WWW 서버의 개인 IP 주소를 모르는 것입니다.대신 DNS 서버는 WWW 서버 매핑 주소 172.20.1.10을 알고 있습니다.

여기서 내부 인터페이스에서 오는 이 트래픽은 내부 인터페이스를 통해 변환되고 다시 라우팅되어 WWW 서버에 도달해야 합니다.이를 헤어핀이라고 합니다.이 작업은 다음 명령을 통해 수행할 수 있습니다.

```
same-security-traffic permit intra-interface
global (inside) 1 interface
nat (inside) 1 192.168.100.0 255.255.255.0
static (inside,inside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255
```

헤어피닝에 대한 자세한 컨피그레이션 및 자세한 내용은 Intra-interface 통신으로 헤어피닝 을 참조하십시오.

Access-List Forward Thinking(액세스 목록 전달 사고)

모든 방화벽 액세스 정책이 동일한 것은 아닙니다.일부 액세스 정책은 다른 액세스 정책보다 더 구체적입니다.인터페이스 내 통신이 활성화되고 방화벽에 모든 인터페이스에 적용되는 액세스 목록이 없는 경우, 인터페이스 내 통신이 활성화될 때 액세스 목록을 추가할 필요가 있습니다.적용된 액세스 목록은 인터페이스 내 통신을 허용하고 다른 액세스 정책 요구 사항을 유지해야 합니다.

이 예에서는 이 점을 설명합니다.ASA는 사설 네트워크(내부 인터페이스)를 인터넷(외부 인터페이스)에 연결합니다. ASA 내부 인터페이스에 액세스 목록이 적용되지 않았습니다.기본적으로 모든 IP 트래픽은 내부에서 외부로 허용됩니다.다음 출력과 비슷한 액세스 목록을 추가하는 것이 좋습니다.

```
access-list inside_acl permit ip
```

```
access-list inside_acl permit ip any any
access-group inside_acl in interface inside
```

이 액세스 목록 집합은 모든 IP 트래픽을 계속 허용합니다.인터페이스 내 커뮤니케이션을 위한 특정 액세스 목록 라인은 관리자가 인터페이스 내 통신을 적용된 액세스 목록에서 허용해야 함을 상기시킵니다.

관련 정보

- Cisco Security Appliance 명령 참조, 버전 7.2
- Cisco Security Appliance 시스템 로그 메시지, 버전 7.2
- Cisco PIX 방화벽 소프트웨어
- ASA:ASA에서 AIP SSM 컨피그레이션으로 네트워크 트래픽 전송 예시
- Cisco ASA 5500 Series Adaptive Security Appliances 제품 지원
- 기술 지원 및 문서 – Cisco Systems