PIX/ASA 7.2(1) and later: Intra-Interface Communications

Contents

Introduction

This document helps to troubleshoot common problems that occur when you enable intra-interface communications on an Adaptive Security Appliance (ASA) or PIX that operates in software release 7.2(1) and later. Software release 7.2(1) includes the capability to route clear text data in and out of the same interface. Enter the **same-security-traffic permit intra-interface** command in order to enable this feature. This document assumes the network administrator has either enabled this feature or plans to in the future. Configuration and troubleshooting are provided using the command line interface (CLI).

Note: This document focuses on clear (unencrypted) data that arrives and leaves the ASA. Encrypted data is not discussed.

In order to enable intra-interface communication on ASA/PIX for IPsec configuration, refer to [PIX/ASA and VPN Client for Public Internet VPN on a Stick Configuration Example](#).

In order to enable intra-interface communication on ASA for SSL configuration, refer to [ASA 7.2(2): SSL VPN Client (SVC) for Public Internet VPN on a Stick Configuration Example](#).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Access lists
- Routing
- Advanced Inspection and Prevention-Security Services Module (AIP-SSM) Intrusion Prevention System (IPS)—Knowledge of this module is only necessary if the module is installed and operational.
- IPS software release 5.x—Knowledge of IPS software is not required if the AIP-SSM is not in use.

Components Used

- ASA 5510 7.2(1) and later
- AIP-SSM-10 that operates IPS software 5.1.1

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. If your network is live, make sure that you understand the potential impact of any command.

Related Products

This configuration can also be used with the Cisco 500 Series PIX which runs version 7.2(1) and later.

Conventions

Refer to Cisco Technical Tips Conventions for information on document conventions.

Background Information

The figure shows the data from host to 172.16.10.1 is blocked since the "intra-interface" keyword of the "same-security-traffic permit" configuration mode command is disabled.
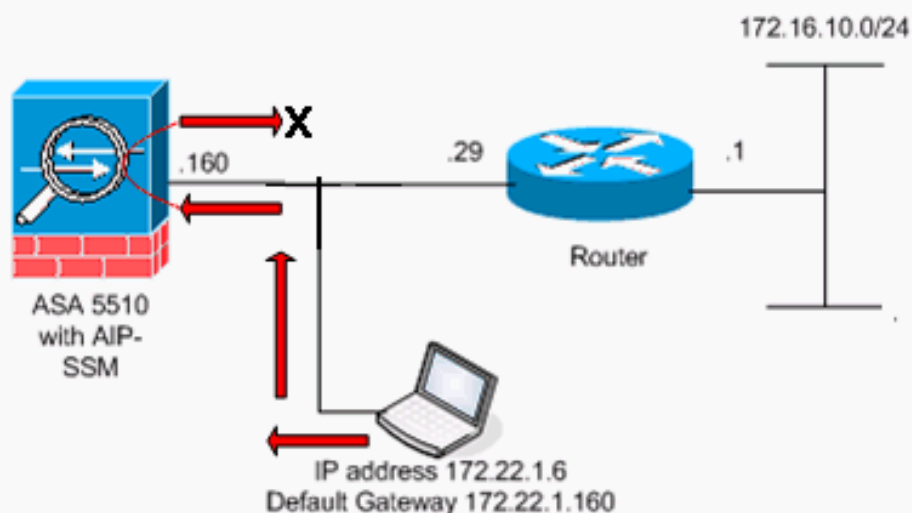
Note: The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 ☑ addresses that have been used in a lab environment.

This table shows the ASA starting configuration:

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:
```

Troubleshooting

These sections illustrate several configuration scenarios, related syslog messages, and packet-tracer outputs in relation to intra-interface communications.

Intra-Interface Communications Not Enabled

In the ASA configuration, host 172.22.1.6 attempts to ping host 172.16.10.1. Host 172.22.1.6 sends an ICMP echo request packet to the default gateway (ASA). Intra-interface communications have not been enabled on the ASA. The ASA drops the echo request packet. The test ping fails. The ASA is used to troubleshoot the problem.

This example shows the output of syslog messages and a packet-tracer:

- This is the syslog message logged to the buffer: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)
- This is the packet-tracer output: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

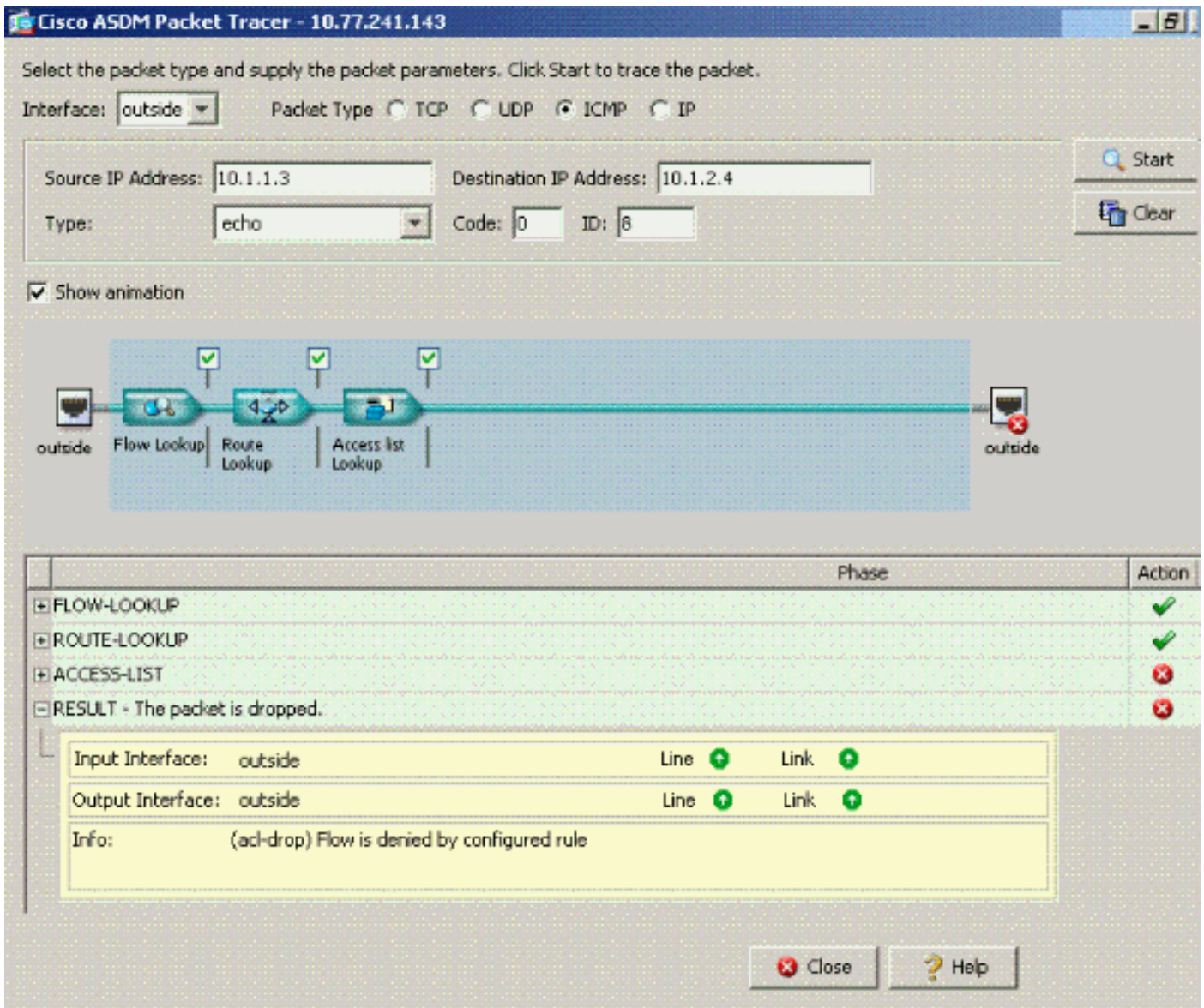The equivalent of the CLI commands in ASDM is shown in these figures:
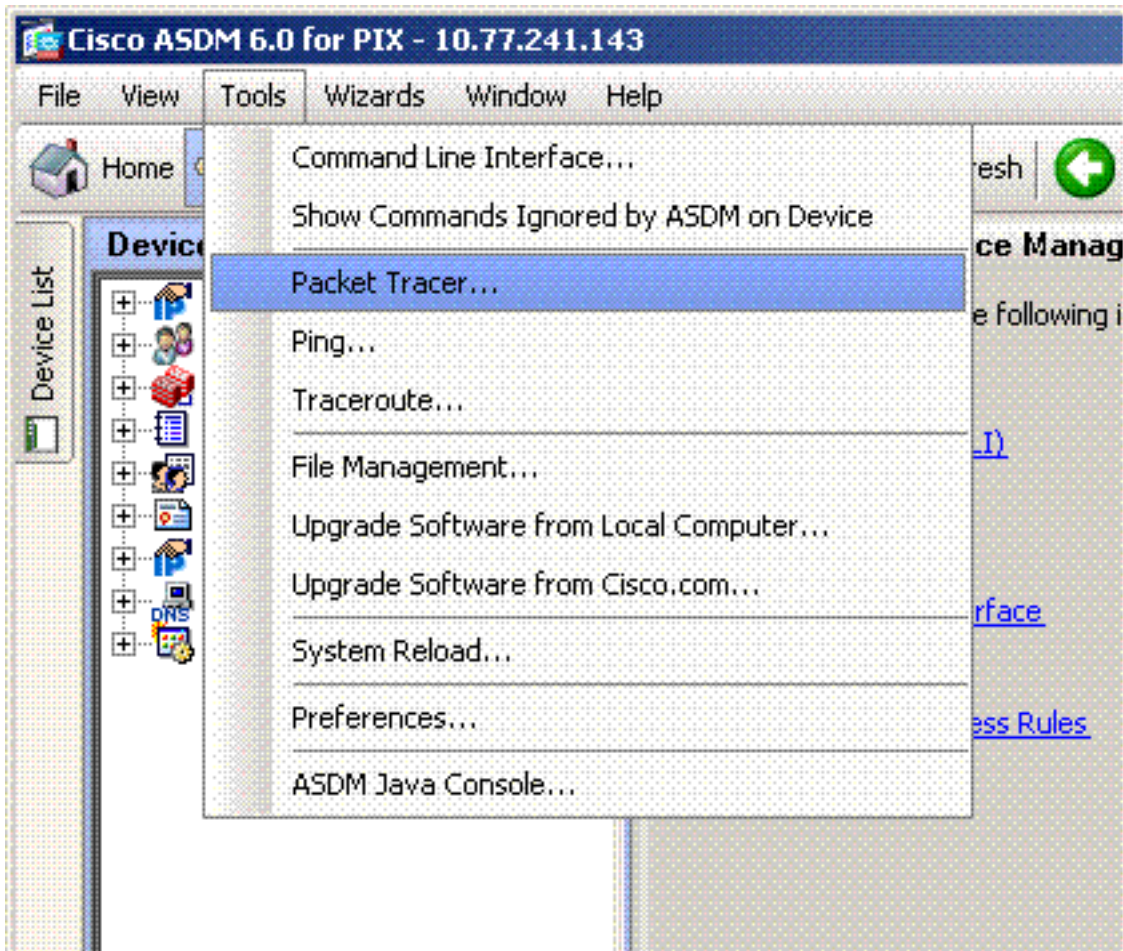
Step 1:

Step 2:
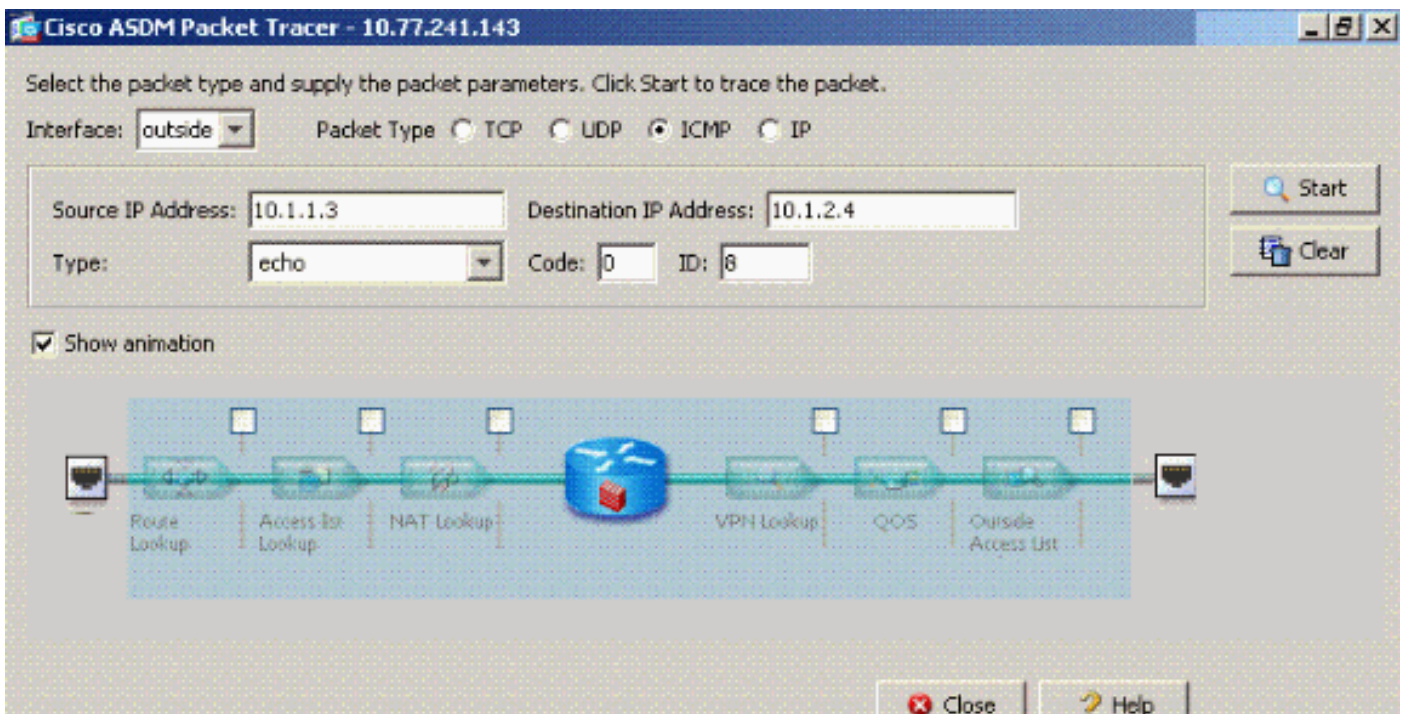
The packet-tracer output with the **same-security-traffic permit intra-interface** command disabled.

The packet-tracer output `drop...implicit rule` suggests that a default configuration setting is blocking the traffic. The administrator needs to check the running configuration in order to ensure intra-interface communications are enabled. In this case, the ASA configuration needs intra-interface communications to be enabled (**same-security-traffic permit intra-interface**).

```
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...
```

Intra-Interface Communications Enabled

Intra-interface communications are now enabled. The **same-security-traffic permit intra-interface** command is added to the previous configuration. Host 172.22.1.6 attempts to ping host 172.16.10.1. Host 172.22.1.6 sends an ICMP echo request packet to the default gateway (ASA). Host 172.22.1.6 records successful replies from 172.16.10.1. The ASA passes the ICMP traffic successfully.

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.
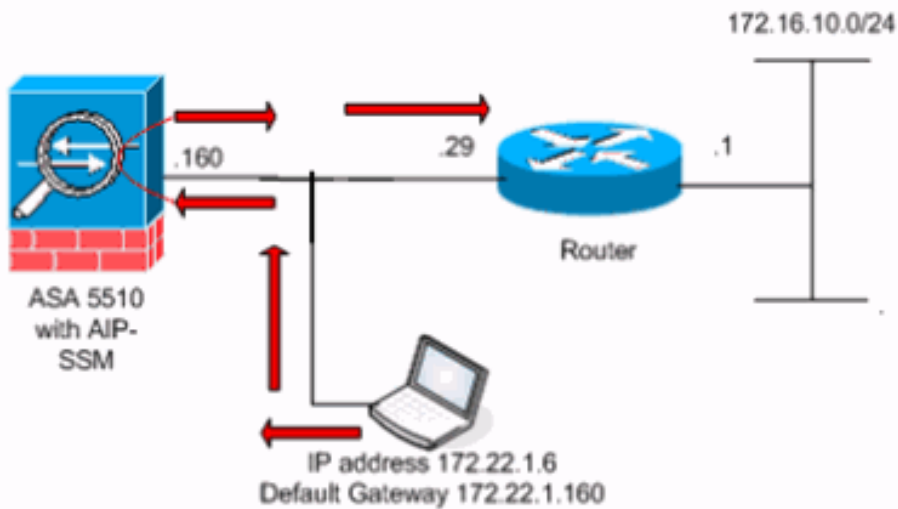

These examples show the ASA syslog message and packet-tracer outputs:

- These are the syslog messages logged to the buffer: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

- This is the packet-tracer output: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*The equivalent of the CLI commands in ASDM is shown in these figures:**Step**
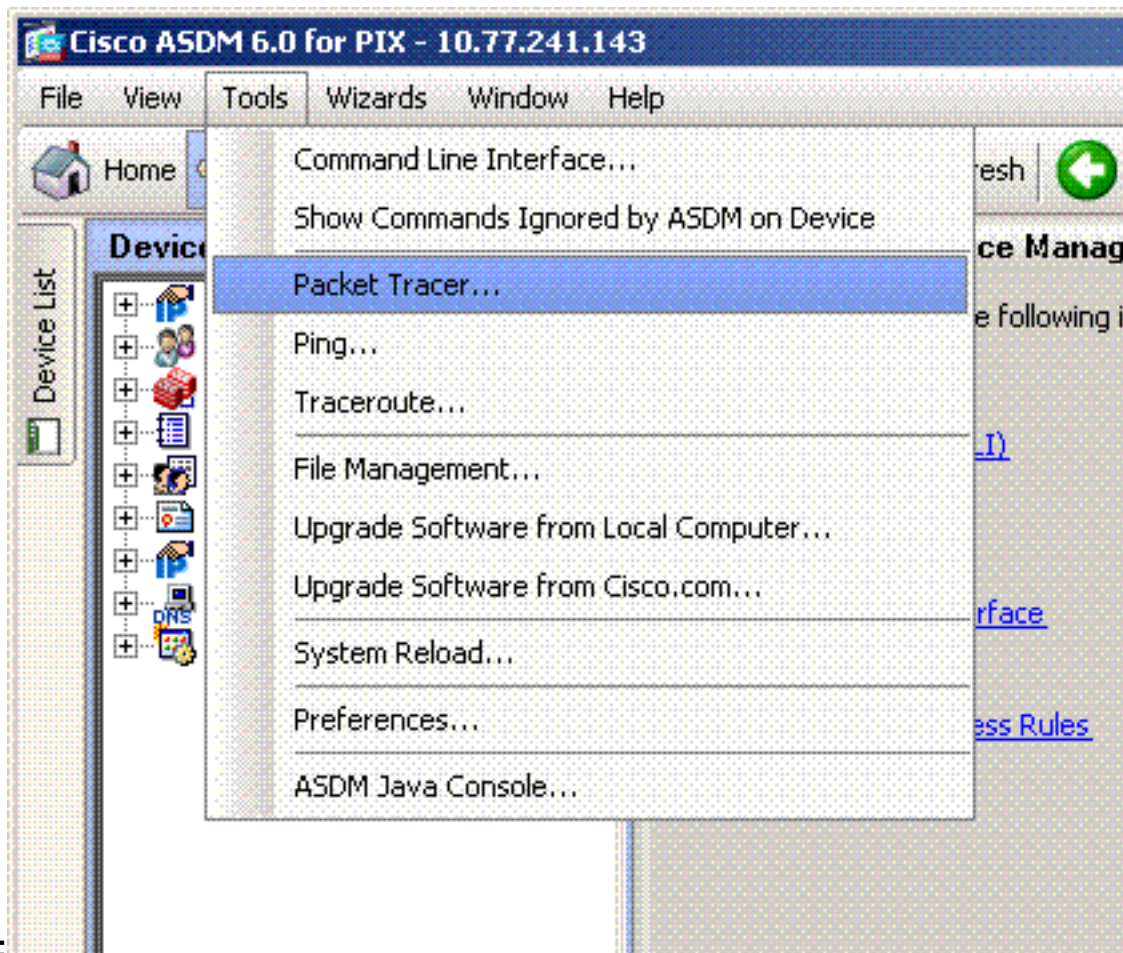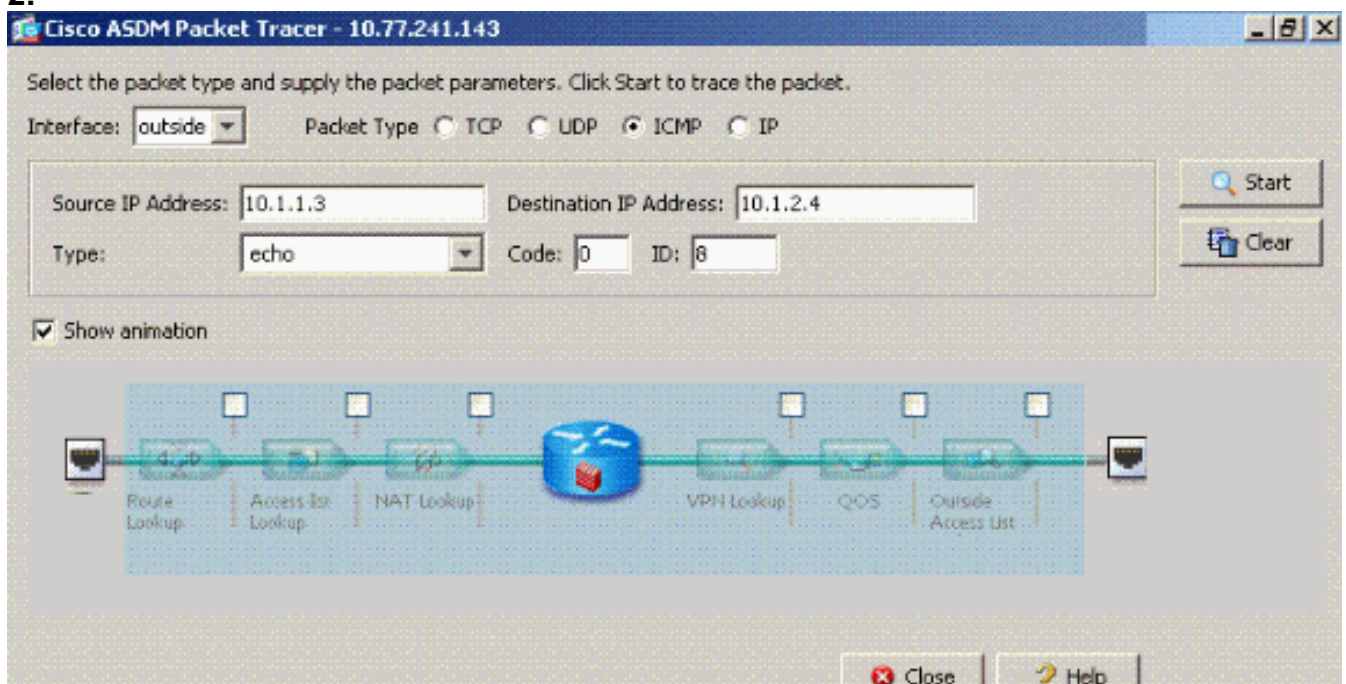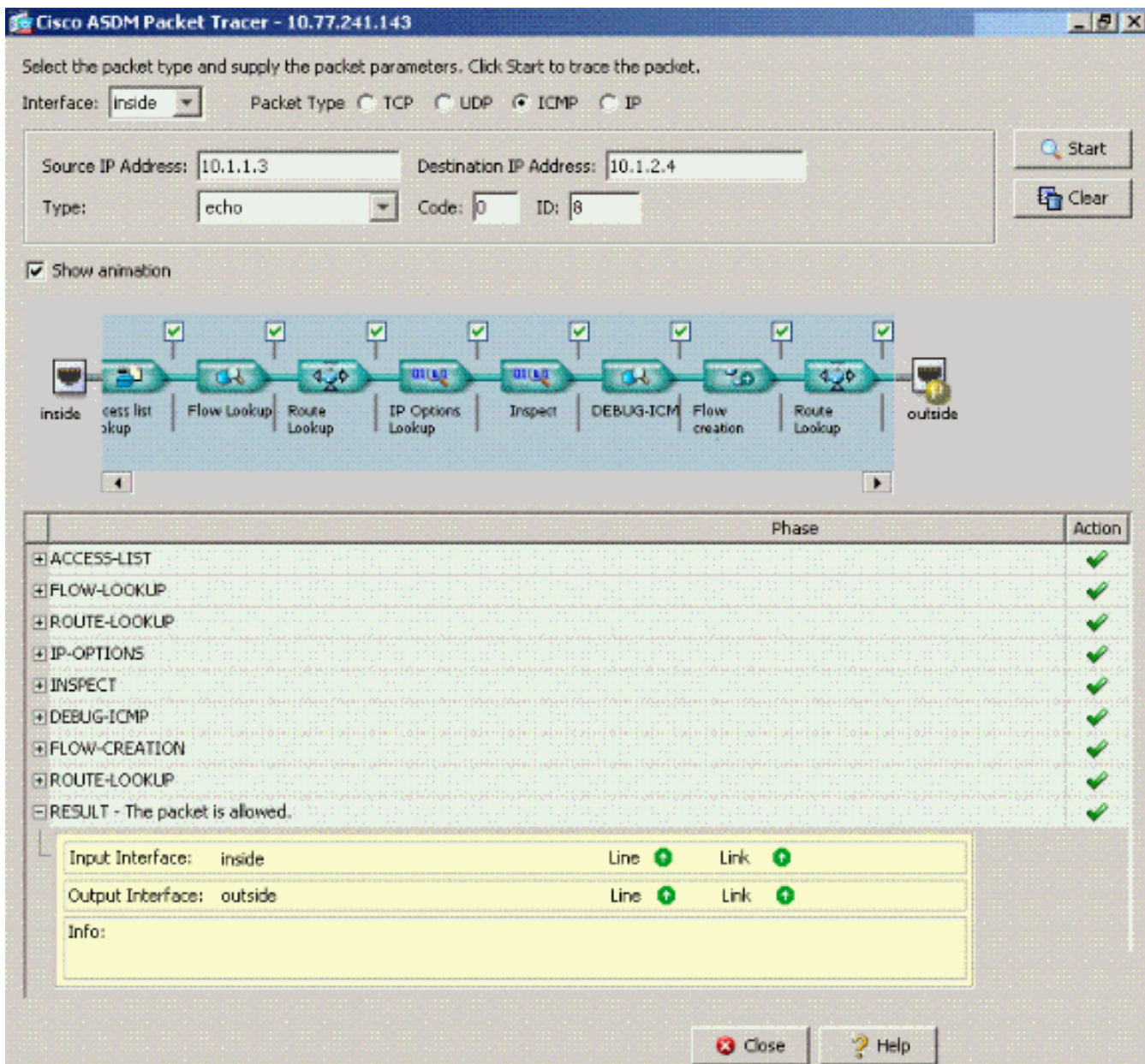
1: **Step 2:**

The packet-tracer output with the **same-security-traffic permit intra-interface** command enabled.

Note: No access-list is applied to the outside interface. In the sample configuration, the outside interface is assigned security level 0. By default, the firewall does not permit traffic from a low security interface to a high security interface. This might lead administrators to believe that intra-interface traffic is not permitted on the outside (low security) interface without permission from an access-list. However, the same interface traffic passes freely when no access-list is applied to the interface.

Intra-Interface Enabled and Traffic Passed to the AIP-SSM for Inspection

Intra-interface traffic can be passed to the AIP-SSM for inspection. This section assumes the administrator has configured the ASA to forward traffic to the AIP-SSM and the administrator knows how to configure IPS 5.x software.

At this point the ASA configuration contains the previous sample configuration, intra-interface communications are enabled, and all (any) traffic is forwarded to the AIP-SSM. IPS signature 2004 is modified to drop echo request traffic. Host 172.22.1.6 attempts to ping host 172.16.10.1. Host 172.22.1.6 sends an ICMP echo request packet to the default gateway (ASA). The ASA forwards the echo request packet to the AIP-SSM for inspection. The AIP-SSM drops the data packet per the IPS configuration.

These examples show the ASA syslog message and packet-tracer output:

- This is the syslog message logged to the buffer: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.*
- This is the packet-tracer output: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.*

It is important to note that administrators should use as many troubleshooting tools as possible when they research a problem. This example shows how two different troubleshooting tools can paint different pictures. Both tools together tell a complete story. The ASA configuration policy permits the traffic but the IPS configuration does not.

Intra-Interface Enabled and Access Lists Applied to an Interface

This section uses the original sample configuration in this document, intra-interface communications enabled, and an access-list applied to the tested interface. These lines are added to the configuration. The access-list is intended to be a simple representation of what might be configured on a production firewall.

```
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.
```

Host 172.22.1.6 attempts to ping host 172.16.10.1. Host 172.22.1.6 sends an ICMP echo request packet to the default gateway (ASA). The ASA drops the echo request packet per the access-list rules. The host 172.22.1.6 test ping fails.

These examples show ASA syslog message and packet-tracer output:

- This is the syslog message logged to the buffer: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]
- This is the packet-tracer output: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
```

Refer to [packet-tracer](#) for more information on the **packet-tracer** command.

Note: In the event the access-list applied to the interface includes a deny statement, the output of the packet-tracer changes. For example:

```
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:
```

The equivalent of the above CLI commands in ASDM is shown in these figures:
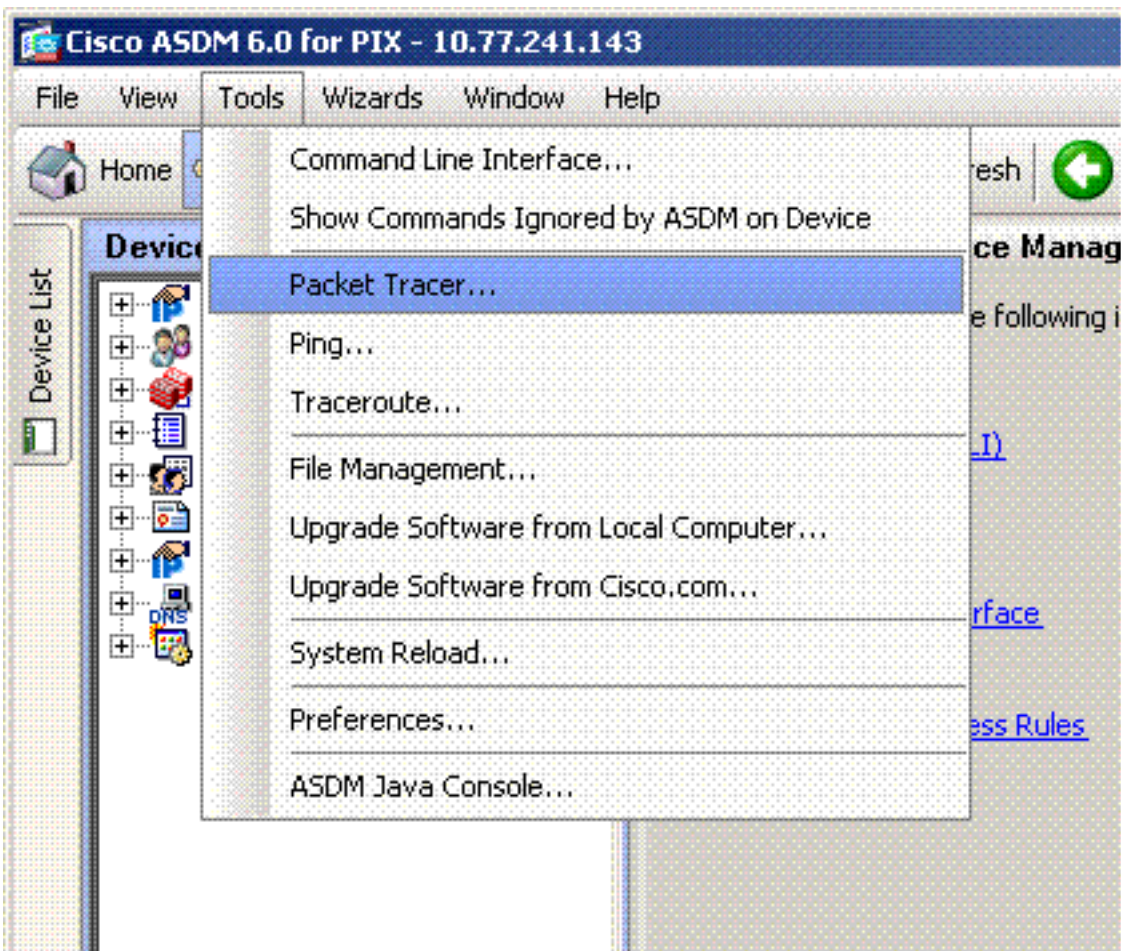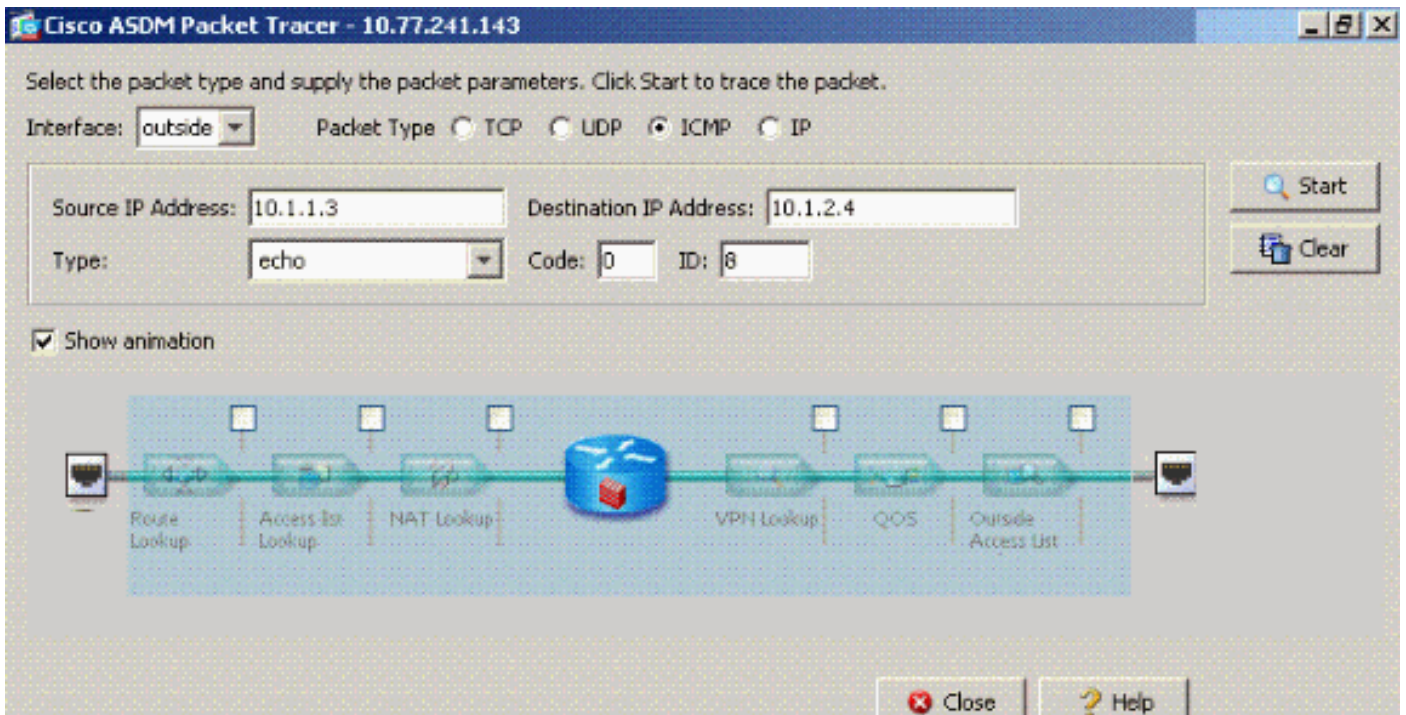
Step 1:

Step 2:

The packet-tracer output with the **same-security-traffic permit intra-interface** command enabled and the **access-list outside_acl extended deny ip any any** command configured to deny packets.

If intra-interface communications are desired on a particular interface and access-lists are applied to the same interface, the access-list rules must permit the intra-interface traffic. With the use of the examples in this section, the access-list needs to be written as:

```
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
```
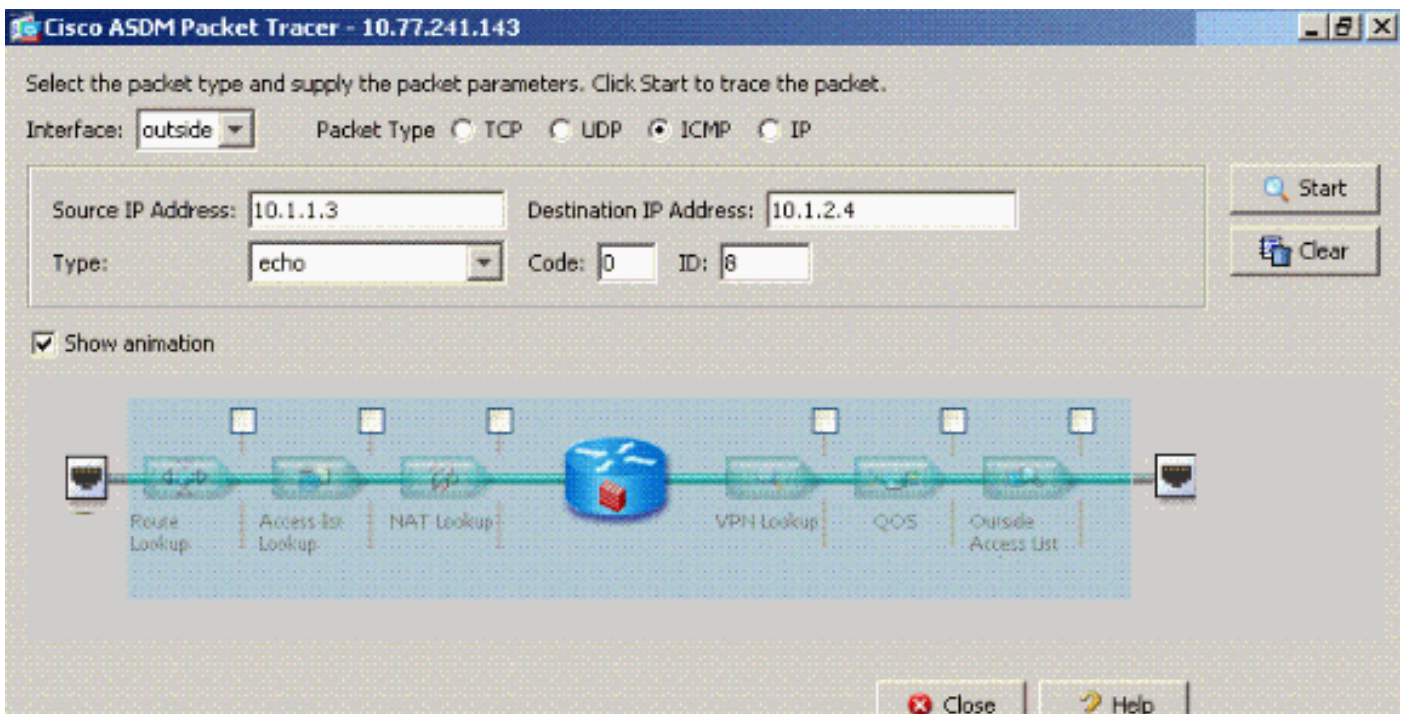
The equivalent of the above CLI commands in ASDM is shown in these figures:
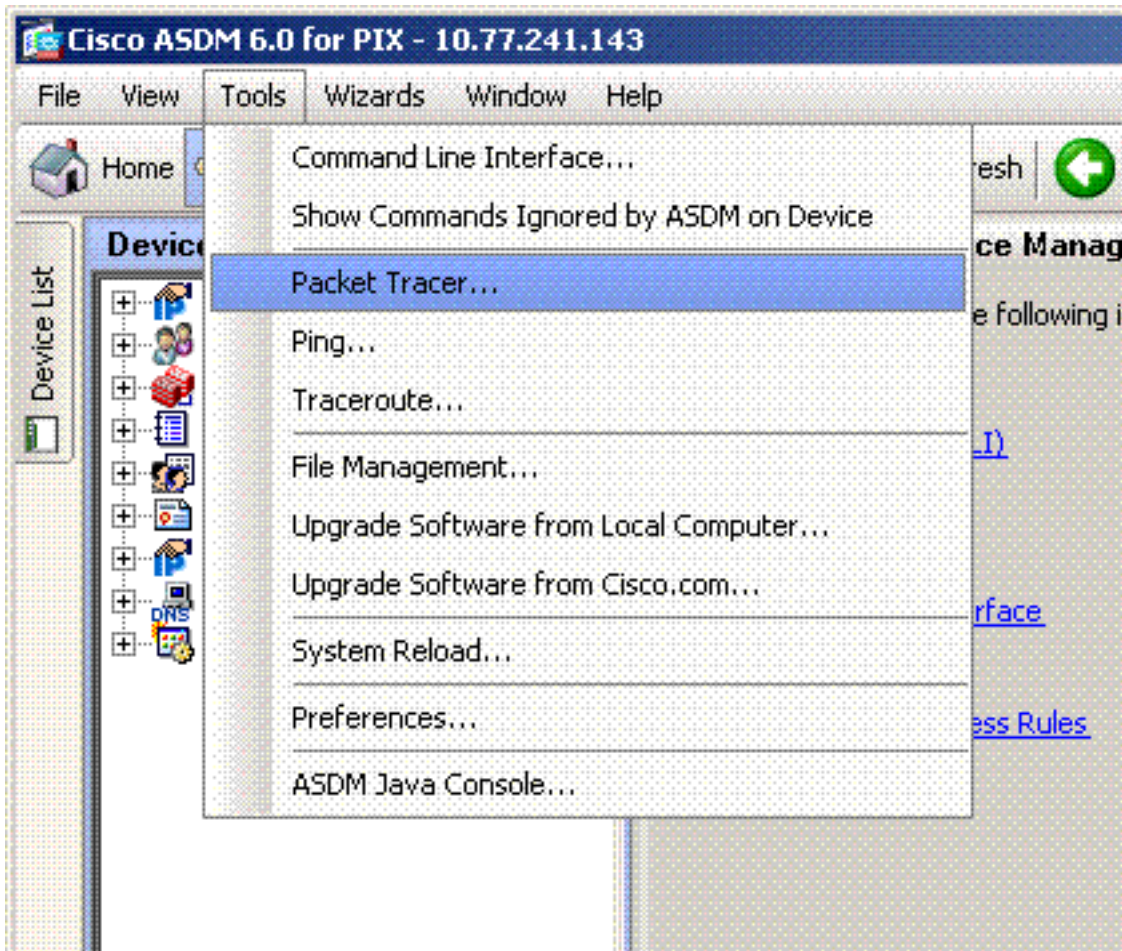
Step 1:

Step 2:

The packet-tracer output with the **same-security-traffic permit intra-interface** command enabled and the **access-list outside_acl extended deny ip any any** command configured on the same interface where intra-interface traffic is desired.

Refer to access-list extended and access-group for more information on the **access-list** and **access-group** commands.

Intra-Interface Enabled with Static and NAT

This section explains a scenario where an inside user is trying to access the internal Web server with its public address.
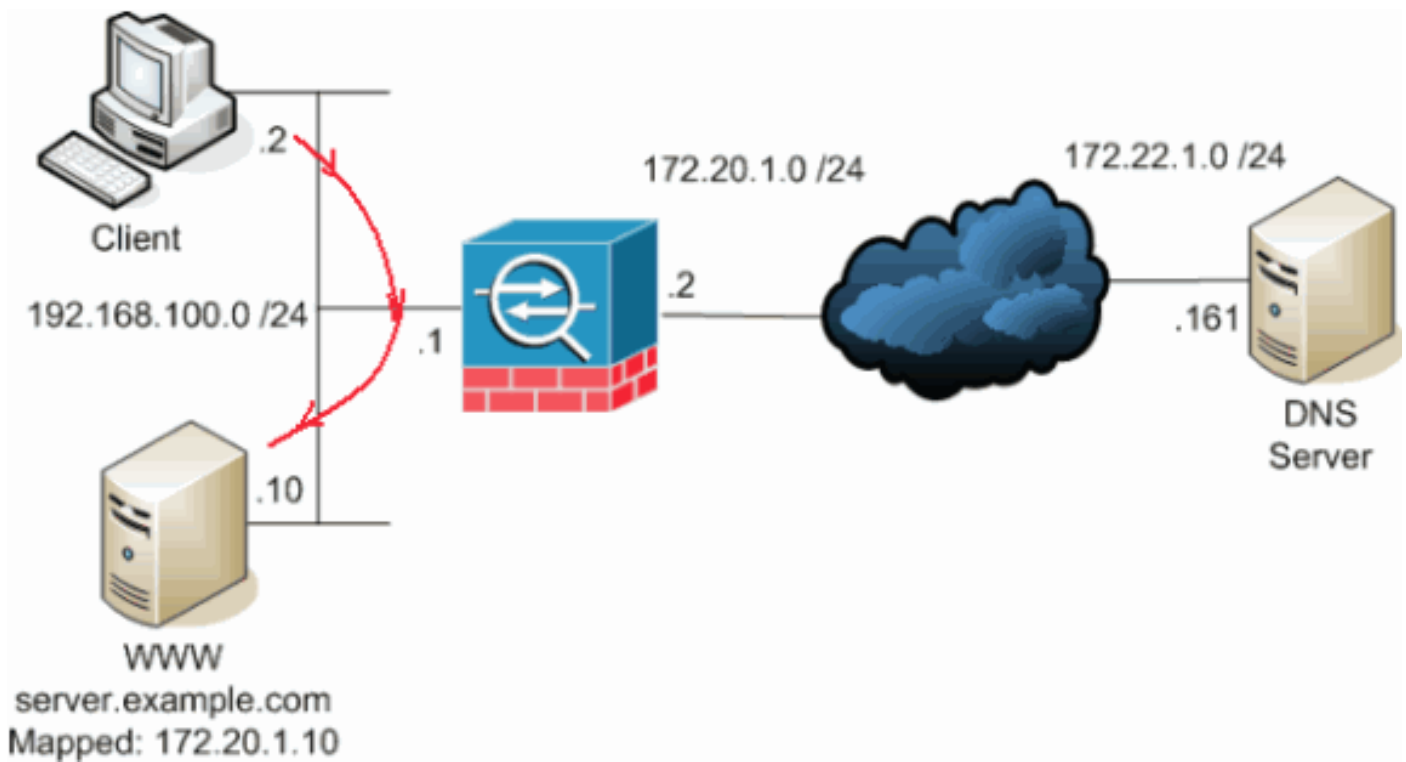
In this case, the client at 192.168.100.2 wants to use the public address of the WWW server (for example, 172.20.1.10). The DNS services for the client are provided by the external DNS server at 172.22.1.161. Because the DNS server is located on another public network, it does not know the private IP address of the WWW server. Instead, the DNS server knows the WWW server mapped address of 172.20.1.10.

Here this traffic from the inside interface has to be translated and re-routed through the inside interface to reach the WWW server. This is called hairpinning. This can be performed through these commands:

```
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
```

For complete configuration details and more information about hairpinning, refer to Hairpinning with Intra-interface communication.

Access-List Forward Thinking

Not all firewall access policies are the same. Some access policies are more specific than others. In the event intra-interface communications are enabled and the firewall does not have an access-list applied to all interfaces, it might be worth adding an access-list at the time intra-interface communications are enabled. The applied access-list needs to permit intra-interface communications as well as maintain other access policy requirements.

This example illustrates this point. The ASA connects a private network (inside interface) to the Internet (outside interface). The ASA inside interface does not have an access-list applied. By default, all IP traffic is permitted from the inside to outside. The suggestion is to add an access-list that looks something like this output:

```
access-list inside_acl permit ip <locally connected network> <all other internal
```

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

This set of access-lists continue to permit all IP traffic. The specific access-list line(s) for intra-interface communications reminds administrators that intra-interface communications must be permitted by an applied access-list.

Related Information

- **Cisco Security Appliance Command Reference, Version 7.2**
- **Cisco Security Appliance System Log Messages, Version 7.2**
- **Cisco PIX Firewall Software**
- **ASA: Send Network Traffic from the ASA to the AIP SSM Configuration Example**
- **Cisco ASA 5500 Series Adaptive Security Appliances Product Support**
- **Technical Support & Documentation - Cisco Systems**