PIX/ASA 7.2 (1)及以后：接口内通信

目录

简介

本文档为您启用在软件版本 7.2(1) 及以上版本中运行的自适应安全设备 (ASA) 或 PIX 上的接口内通信时遇到的常见问题提供故障排除帮助。软件版本 7.2(1) 包括路由明文数据进出同一接口的能力。输入 **same-security-traffic permit intra-interface** 命令以便启用该功能。本文档假设网络管理员已经或计划在将来启用该功能。使用命令行界面 (CLI) 进行配置和故障排除。

注意：本文当重点介绍到达和离开 ASA 的明确（未加密）数据。未讨论已加密数据。

要启用 ASA/PIX 上的接口内通信以便进行 IPSec 配置，请参阅单接口上的公共 Internet VPN 的 PIX/ASA 和 VPN 客户端配置示例。

要启用 ASA 上的接口内通信以便进行 SSL 配置，请参阅 ASA 7.2(2)：单接口上的公共 Internet VPN 的 SSL VPN 客户端 (SVC) 配置示例。

先决条件

要求

Cisco 建议您了解以下主题：

- 访问列表
- 路由

- 高级检查和防御-安全服务模块 (AIP-SSM) 入侵防御系统 (IPS) - 仅在安装并运行此模块后，才需要了解此模块。
- IPS 软件版本 5.x - 如果没有使用 AIP-SSM，则不要求了解 IPS 软件。

使用的组件

- ASA 5510 7.2(1) 及以上版本
- 运行 IPS 软件 5.1.1 的 AIP-SSM-10

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

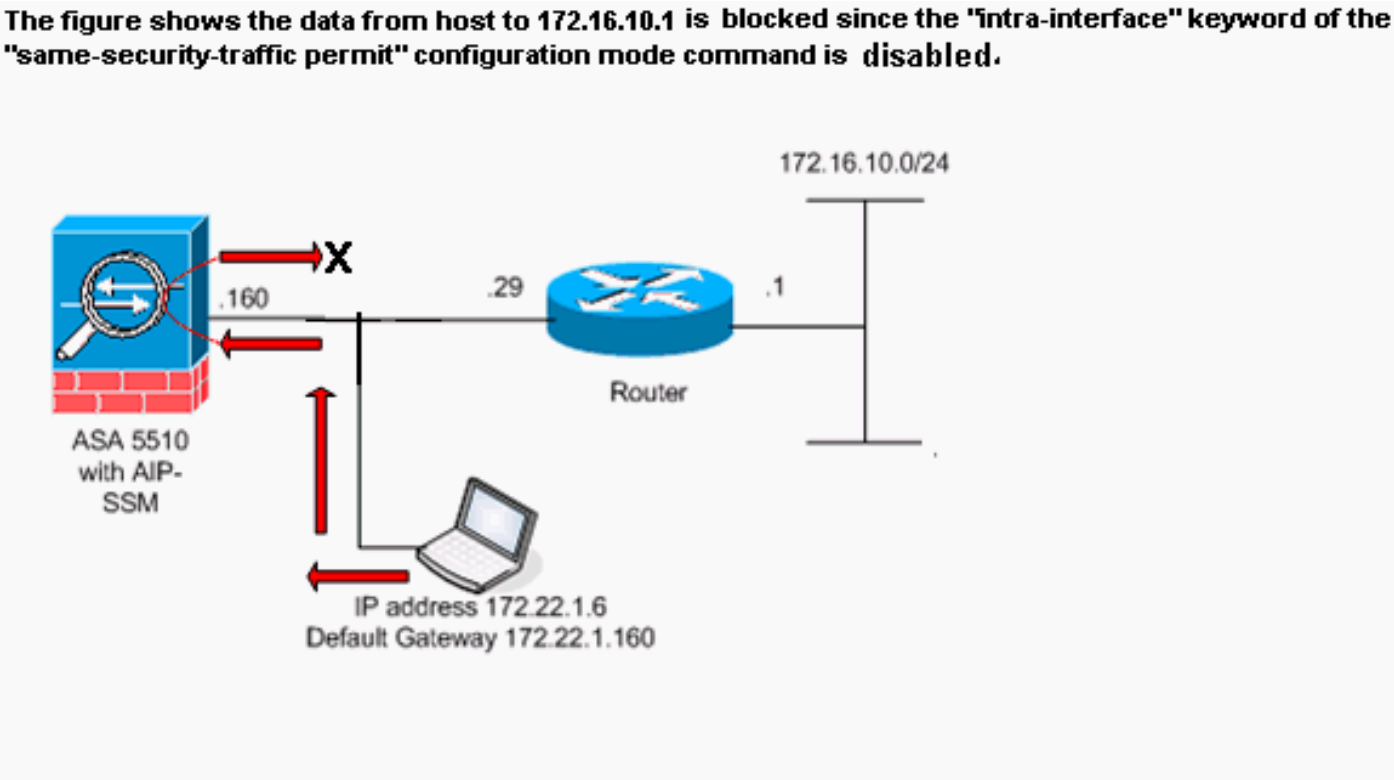
相关产品

此配置还可用于运行版本 7.2(1) 及以上版本的 Cisco 500 系列 PIX。

规则

有关文档规则的信息，请参阅 Cisco 技术提示规则。

背景信息



注意： 此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

下表显示 ASA 的启动配置：

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:
```

排除故障

以下部分介绍与接口内通信相关的几种配置方案、相关 syslog 消息和 Packet Tracer 输出。

接口内通信未启用

在 ASA 配置中，主机 172.22.1.6 尝试 ping 主机 172.16.10.1。主机 172.22.1.6 发送 ICMP Echo 请求数据包到默认网关 (ASA)。ASA 上未启用接口内通信。ASA 丢弃 Echo 请求数据包。测试 ping 发生故障。ASA 用于排除该问题的故障。

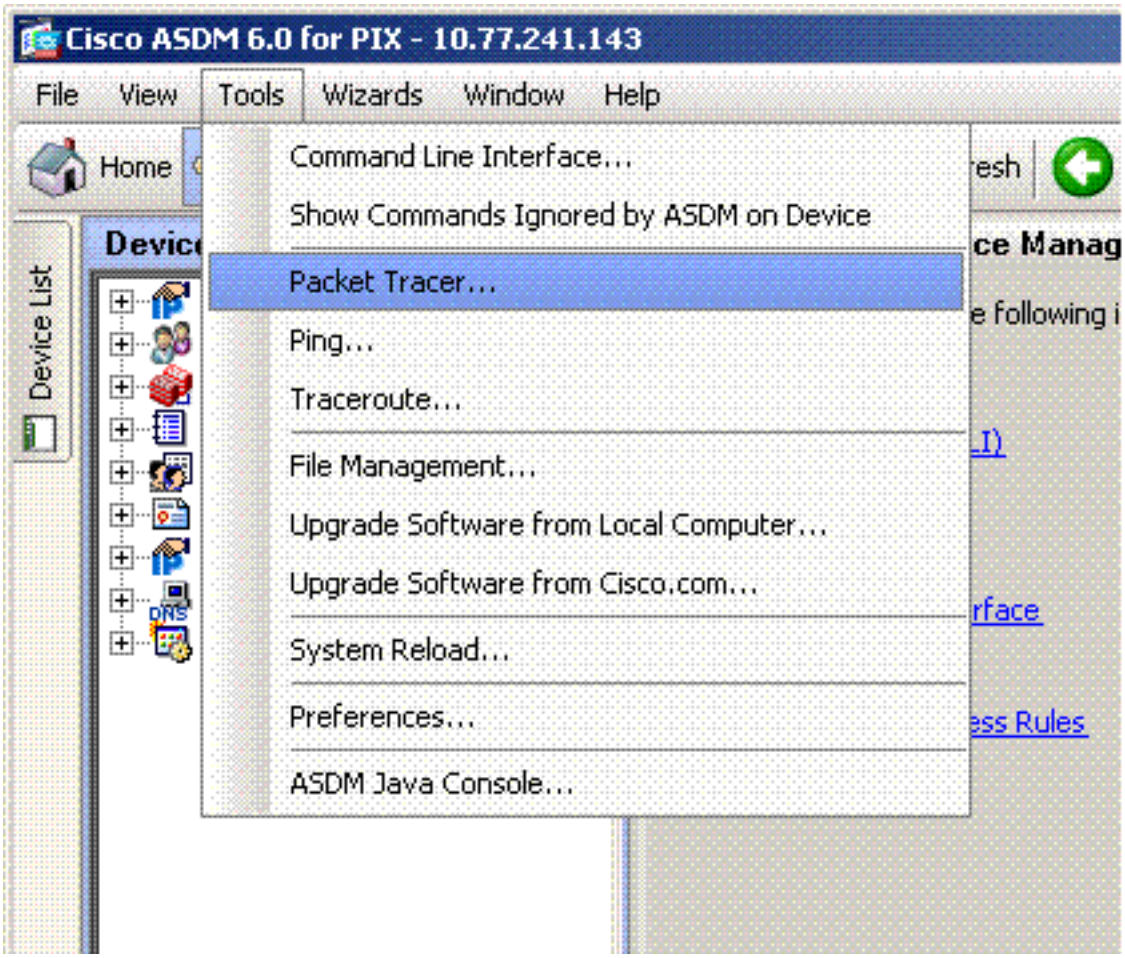
此示例显示 syslog 消息和 Packet Tracer 的输出：

- 以下是记录到缓冲区的 syslog 消息：`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)`
- 以下是 Packet Tracer 输出：`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.`*

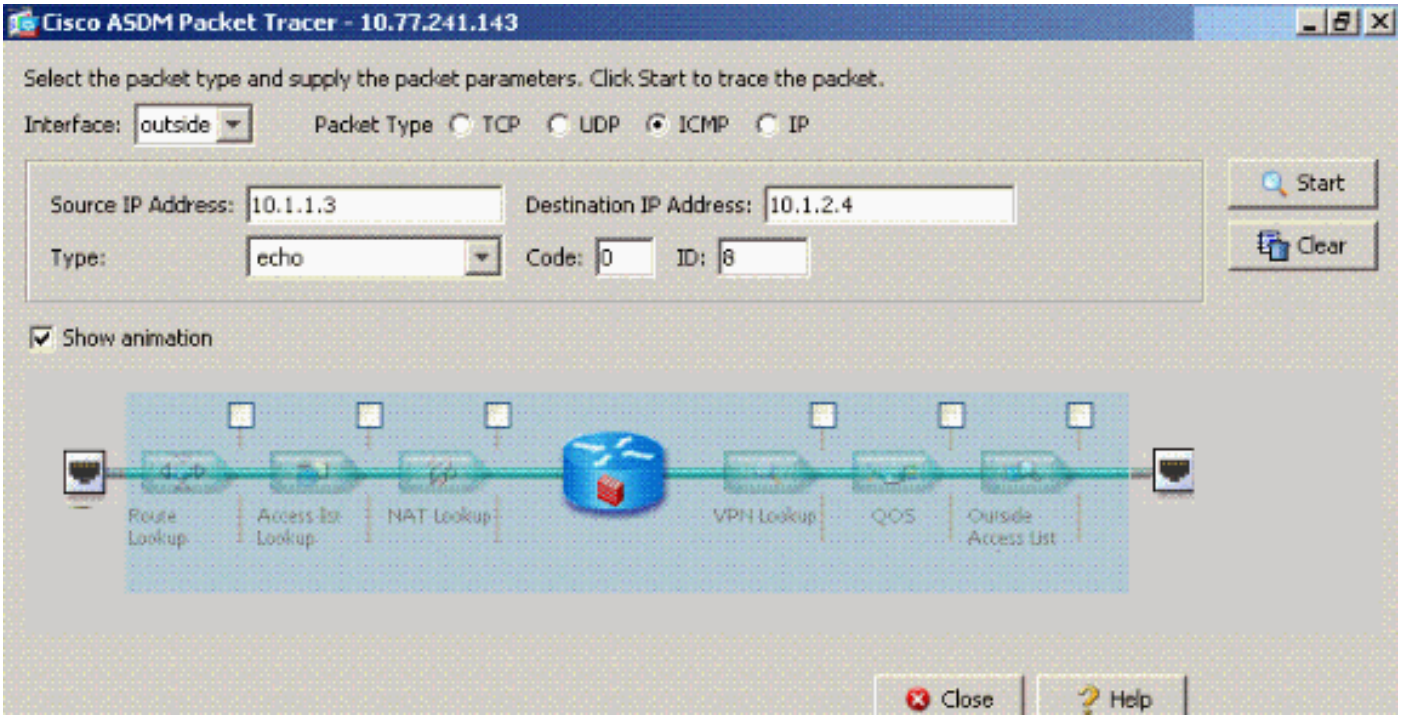
```
Additional Information: Forward Flow based lookup yields rule: in id=0x3bd8480,
priority=111, domain=permit, deny=true hits=0, user_data=0x0, cs_id=0x0, flags=0x4000,
protocol=0 src ip=0.0.0.0, mask=0.0.0.0, port=0 dst ip=0.0.0.0, mask=0.0.0.0, port=0 Result:
input-interface: outside input-status: 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
```

ASDM 中与 CLI 命令等效的命令如下图所示：

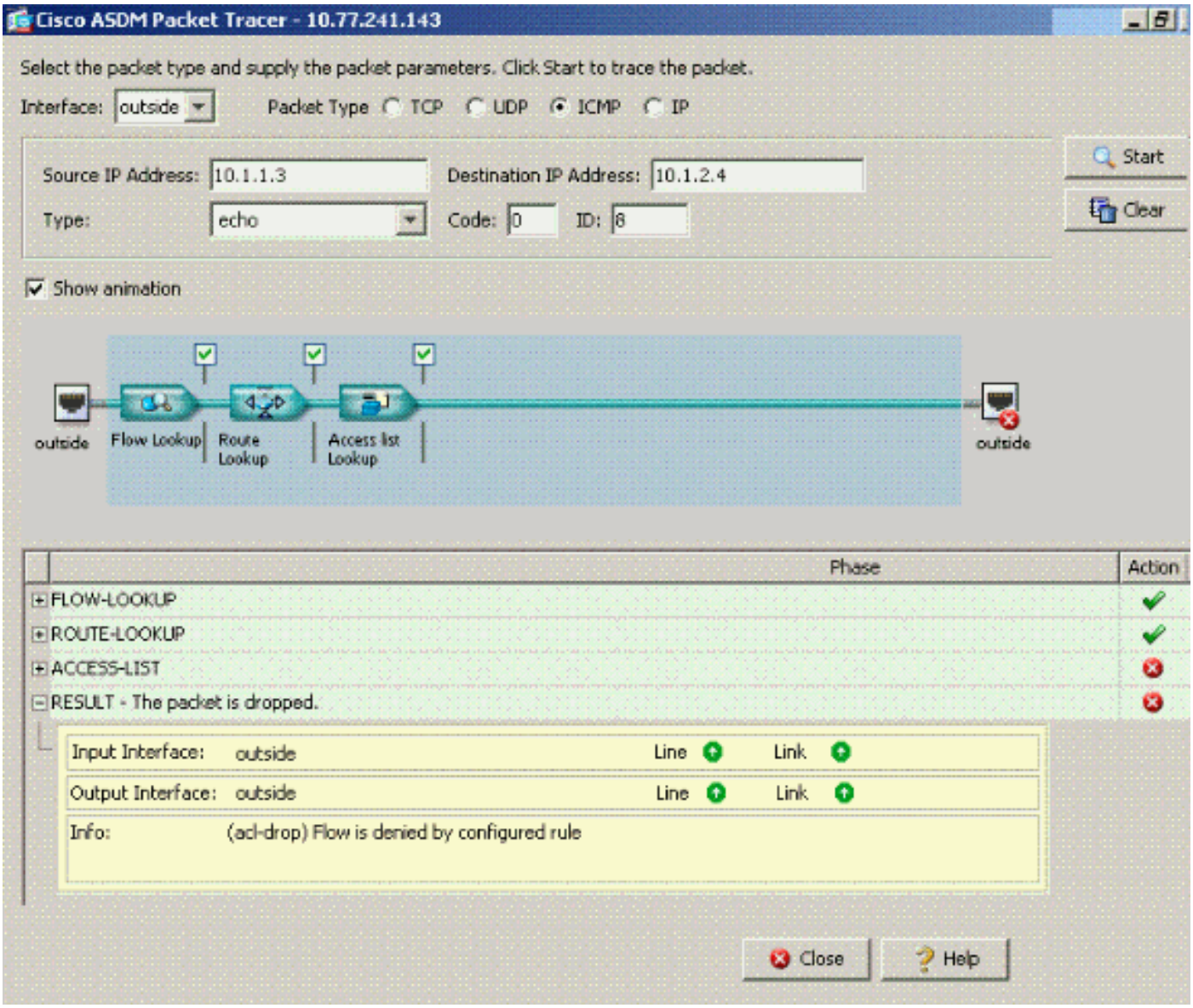
步骤 1：



步骤 2：



same-security-traffic permit intra-interface 命令的 Packet Tracer 输出已禁用。



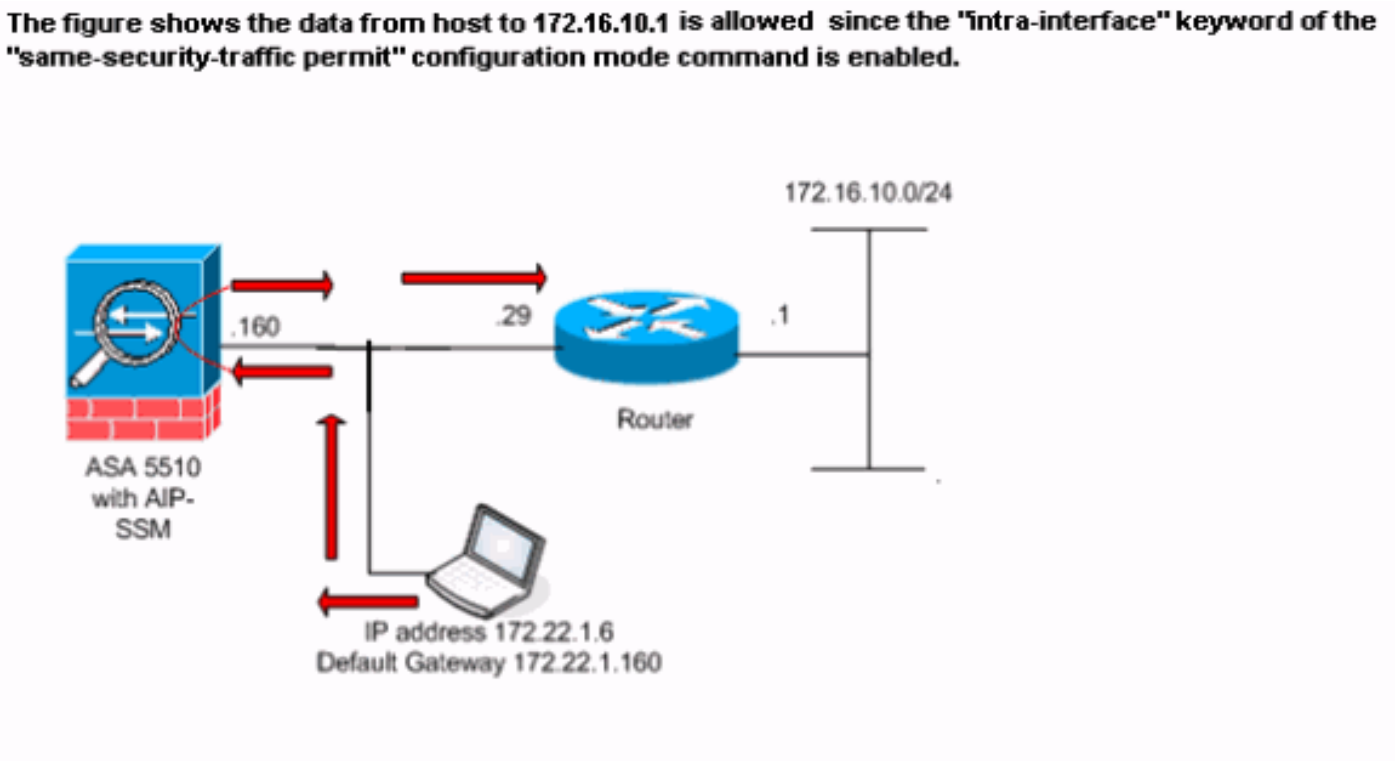
Packet Tracer 输出 drop...implicit rule 表示默认配置设置正在阻塞流量。管理员需要检查正在运行的配置以确保接口内通信已启用。在这种情况下，ASA 配置需要启用接口内通信 (**ame-security-traffic permit intra-interface**)。

```
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...
```

接口内通信已启用

接口内通信当前已启用。**same-security-traffic permit intra-interface** 命令已添加到先前的配置。主机 172.22.1.6 尝试 ping 主机 172.16.10.1。主机 172.22.1.6 发送 ICMP Echo 请求数据包到默认网关 (ASA)。主机 172.22.1.6 记录来自 172.16.10.1的成功回复。ASA 成功传递 ICMP 流量。

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.

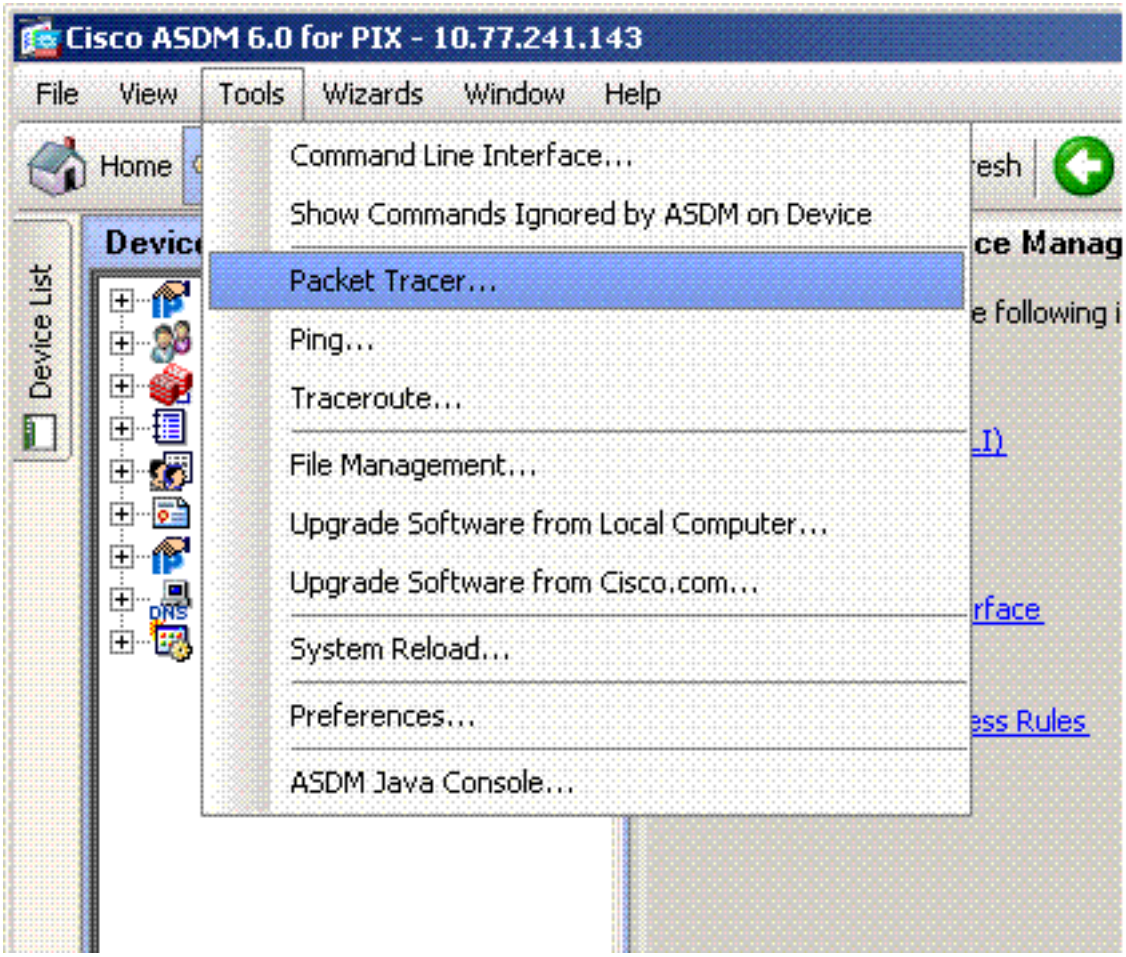


以下示例显示 ASA syslog 消息和 Packet Tracer 输出：

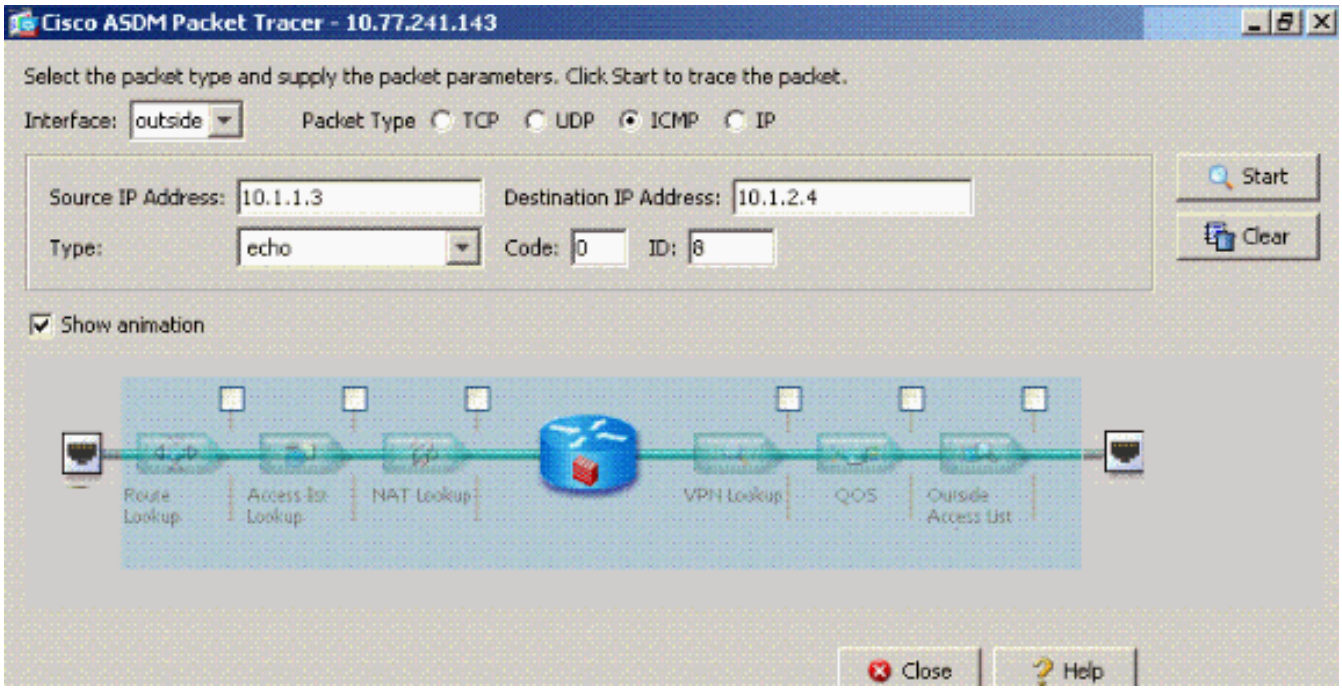
- 以下是记录到缓冲区的 syslog 消息：`ciscoasa#show logging !--- Output is suppressed. %PIX-7-609001: Built local-host outside:172.22.1.6 %PIX-7-609001: Built local-host outside:172.16.10.1 %PIX-6-302020: Built ICMP connection for faddr 172.22.1.6/64560 gaddr 172.16.10.1/0 laddr 172.16.10.1/0 %PIX-6-302021: Teardown 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`
- 以下是 Packet Tracer 输出：`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
```

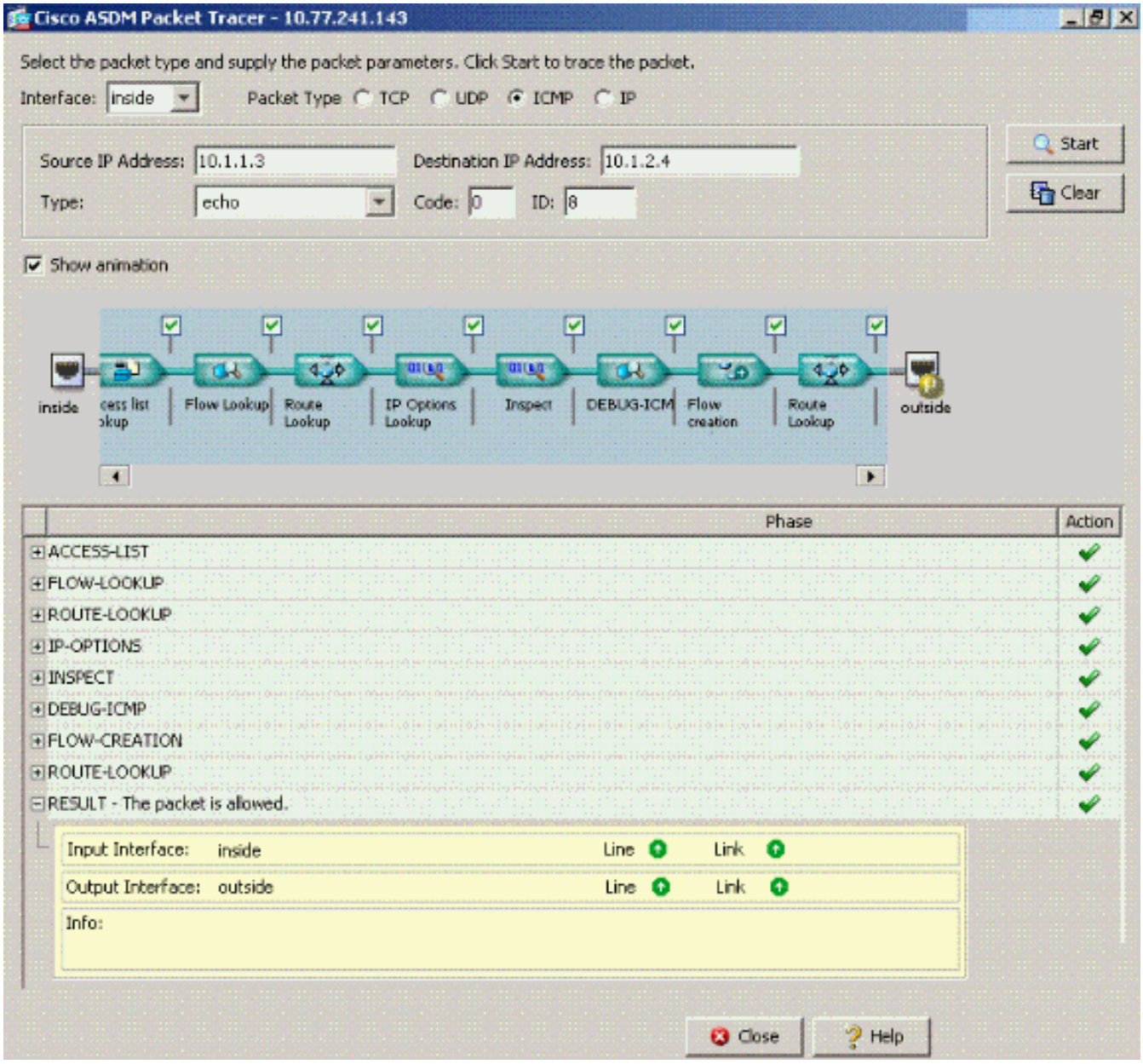
ASDM 中与 CLI 命令等效的命令如下图所示：**步骤 1：**



步骤 2：



same-security-traffic permit intra-interface 命令的 Packet Tracer 输出已禁用。



注意： 没有访问列表适用于外部接口。在该配置示例中，外部接口的安全级别分配为 0。默认情况下，防火墙不允许从低安全接口到高安全接口的流量。这可能会导致管理员认为，如果没有访问列表的允许，则外部（低安全）接口上不允许接口内流量。然而，当接口没有应用访问列表时，同一接口流量可以自由通过。

接口内已启用并且流量已传递到 AIP-SSM 以便检查

接口内流量可传递到 AIP-SSM 以便检查。本部分假设管理员已将 ASA 配置为转发流量到 AIP-SSM，并且管理员知道如何配置 IPS 5.x 软件。

这时 ASA 配置包含先前的配置示例，接口内通信已启用，并且所有（任何）流量都被转发到 AIP-SSM。修改 IPS 签名 2004 以丢弃 Echo 请求流量。主机 172.22.1.6 尝试 ping 主机 172.16.10.1。主机 172.22.1.6 发送 ICMP Echo 请求数据包到默认网关 (ASA)。ASA 将 Echo 请求数据包转发给 AIP-SSM 以便检查。AIP-SSM 会丢弃每个 IPS 配置的数据包。

以下示例显示 ASA syslog 消息和 Packet Tracer 输出：

- 以下是记录到缓冲区的 syslog 消息：`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.

- 以下是 Packet Tracer 输出：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.*

请务必注意，管理员在研究问题时，应使用尽可能多的故障排除工具。以下示例显示两种不同的故障排除工具可如何产生不同的结果。使用两个工具可以有一个完整的了解。ASA 配置策略允许流量，但是 IPS 配置不允许。

接口内已启用并且访问列表已应用于接口

本部分使用本文档中的原始配置示例、启用接口内通信以及应用到测试接口的访问列表。这些线路已添加到配置。访问列表意图简单地展示生产防火墙上可能配置的内容。

```
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.
```

主机 172.22.1.6 尝试 ping 主机 172.16.10.1。主机 172.22.1.6 发送 ICMP Echo 请求数据包到默认网关 (ASA)。ASA 会丢弃每个访问列表规则的 Echo 请求数据包。主机 172.22.1.6 测试 ping 发生故障。

以下示例显示 ASA syslog 消息和 Packet Tracer 输出：

- 以下是记录到缓冲区的 syslog 消息：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]
- 以下是 Packet Tracer 输出：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

有关 **packet-tracer** 命令的详细信息，请参阅 Packet Tracer。

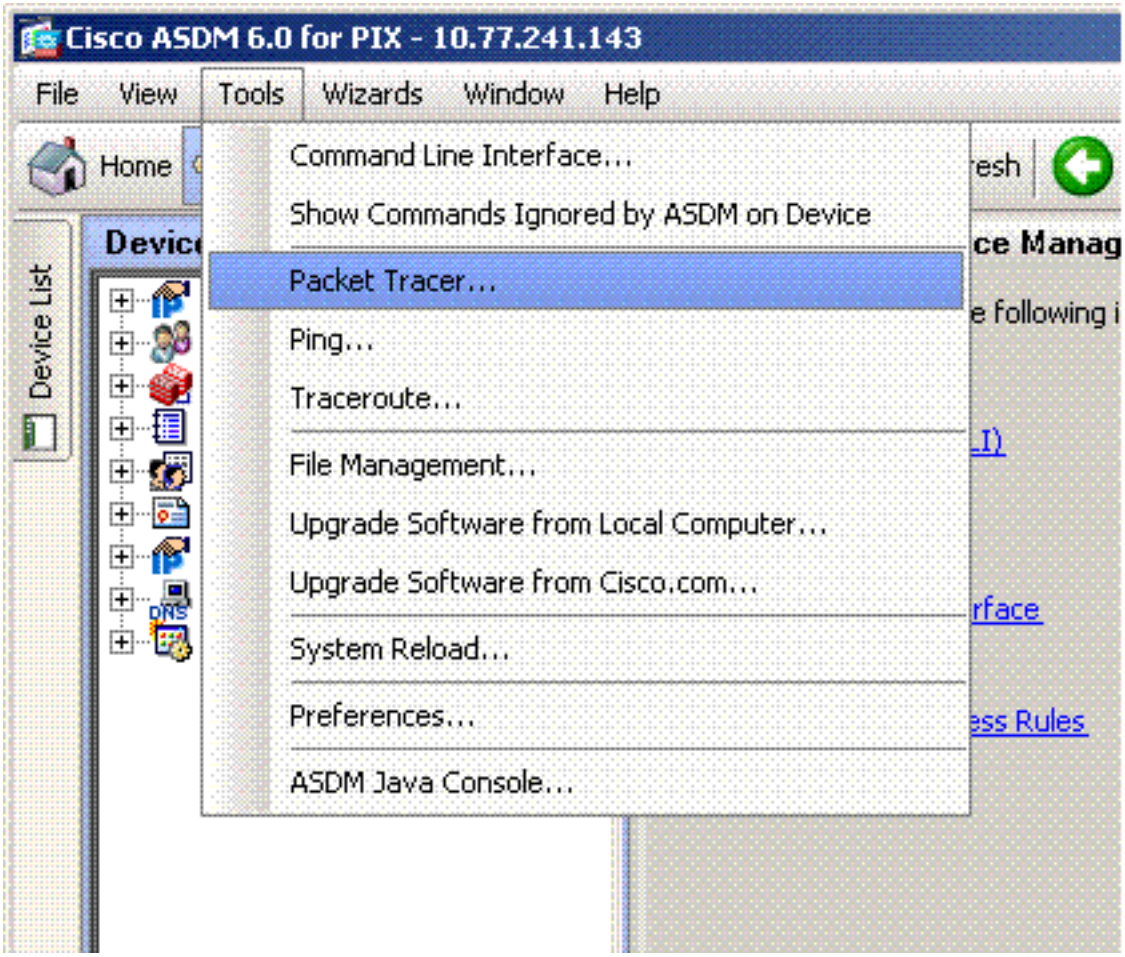
注意： 如果应用到接口的访问列表包含拒绝语句，则 Packet Tracer 的输出会更改。例如：

```
ciscoasa(config)#access-list outside_acl permit tcp any host 172.22.1.147 eq 80
```

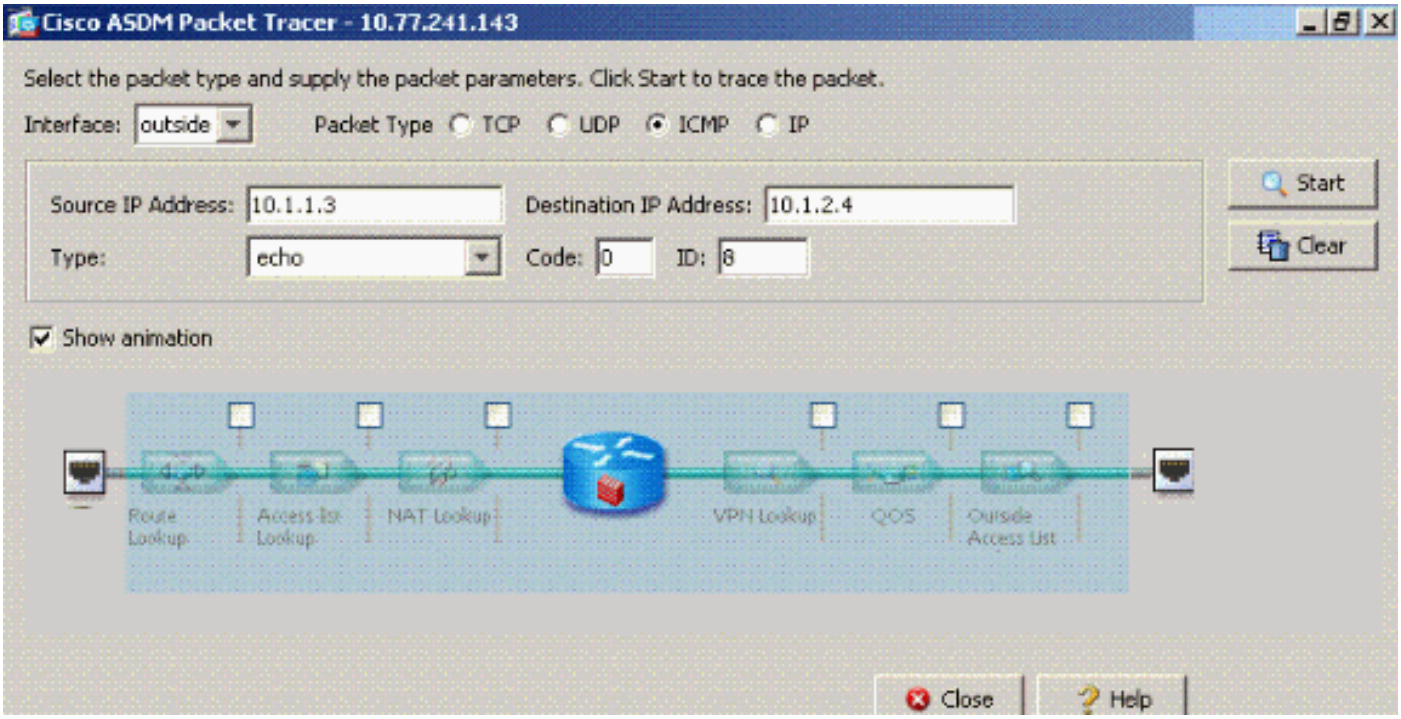
```
ciscoasa(config)#access-list outside_acl deny ip any any ciscoasa(config)#access-group
outside_acl in interface outside ciscoasa#packet-tracer input outside icmp 172.22.1.6 8 0
172.16.10.1 detailed !--- Output is suppressed. Phase: 3 Type: ACCESS-LIST Subtype: log Result:
DROP Config: access-group outside_acl in interface outside access-list outside_acl extended deny
ip any any Additional Information: Forward Flow based lookup yields rule:
```

ASDM 中与上述 CLI 命令等效的命令如下图所示：

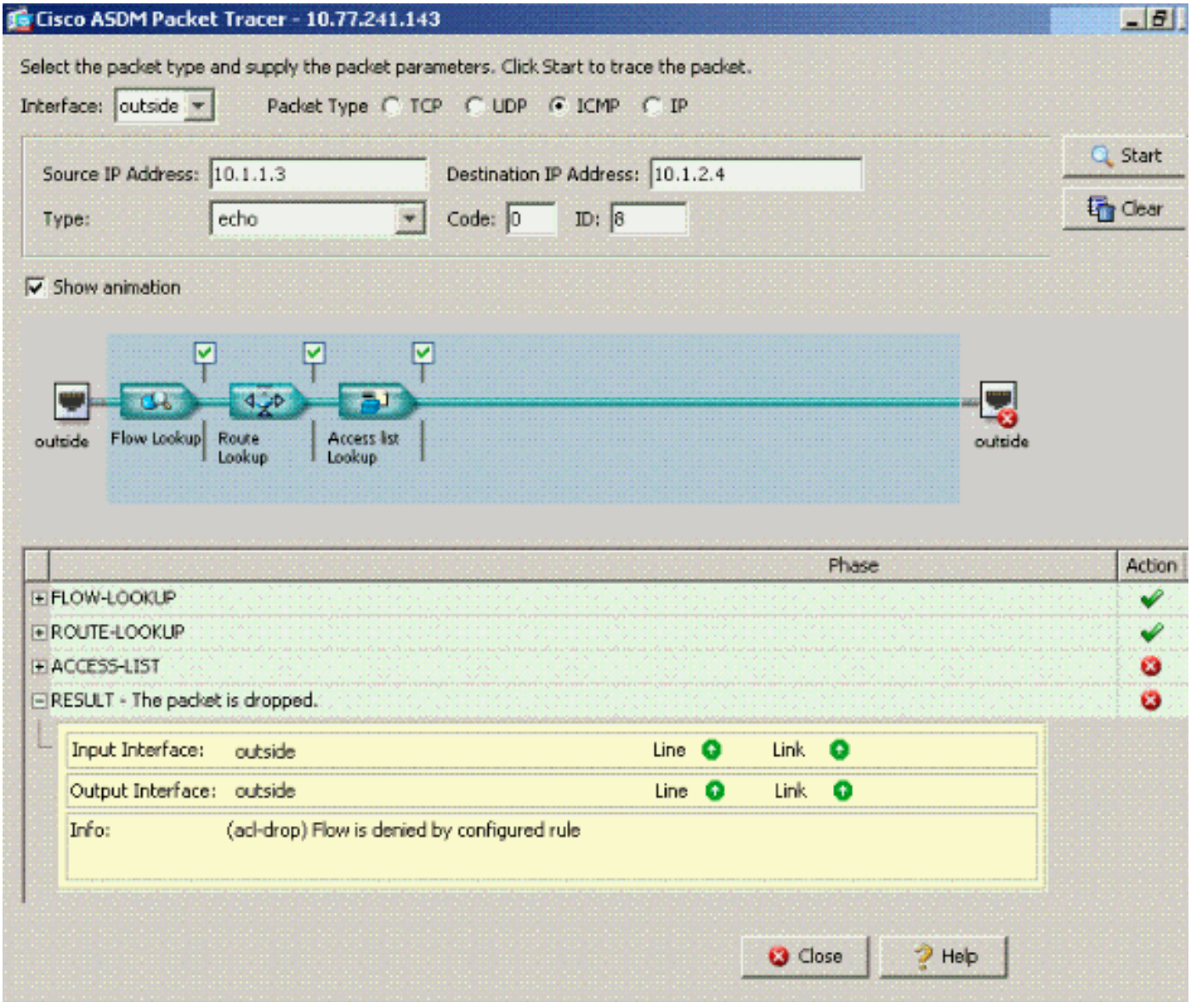
步骤 1：



步骤 2：



已启用 **same-security-traffic permit intra-interface** 命令并且已将 **access-list outside_acl extended deny ip any any** 命令配置为拒绝数据包的 Packet Tracer 输出。

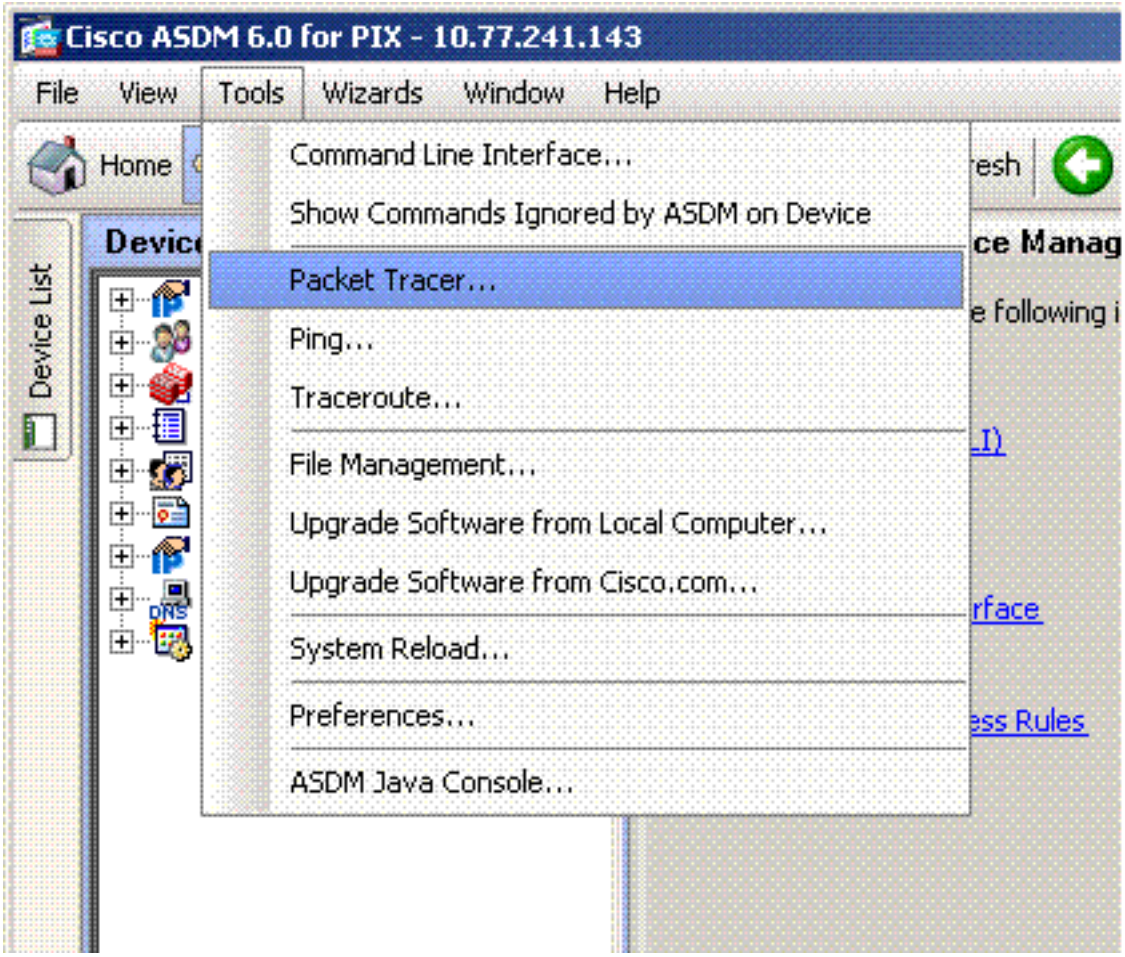


如果特定接口需要接口内通信，并且访问列表应用到同一接口，则访问列表规则必须允许接口内流量。使用本部分中的示例，需要将访问列表写为：

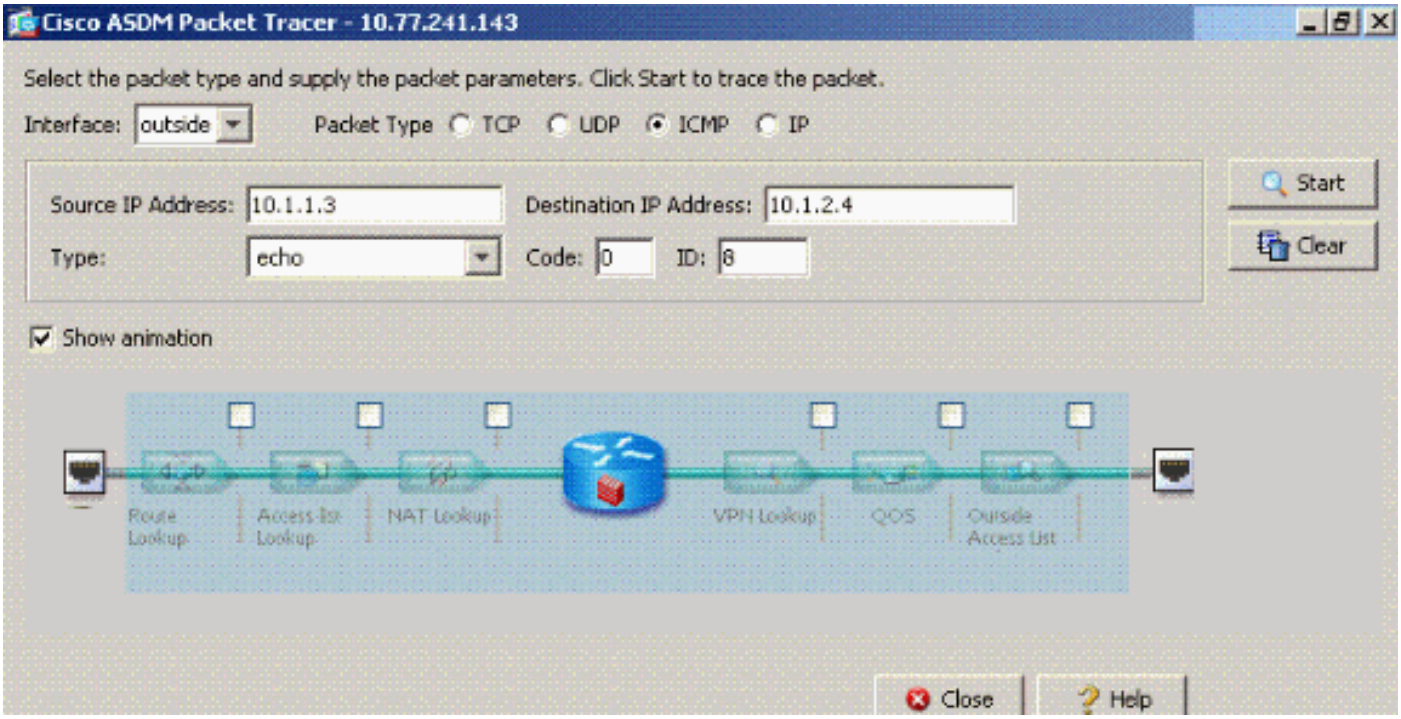
```
ciscoasa(config)#access-list outside_acl permit tcp any host 172.22.1.147 eq 80
ciscoasa(config)#access-list outside_acl permit ip 172.22.1.0 255.255.255.0 172.16.10.0
255.255.255.0 !--- 172.22.1.0 255.255.255.0 represents a locally !--- connected network on the
ASA. !--- 172.16.10.0 255.255.255.0 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
```

ASDM 中与上述 CLI 命令等效的命令如下图所示：

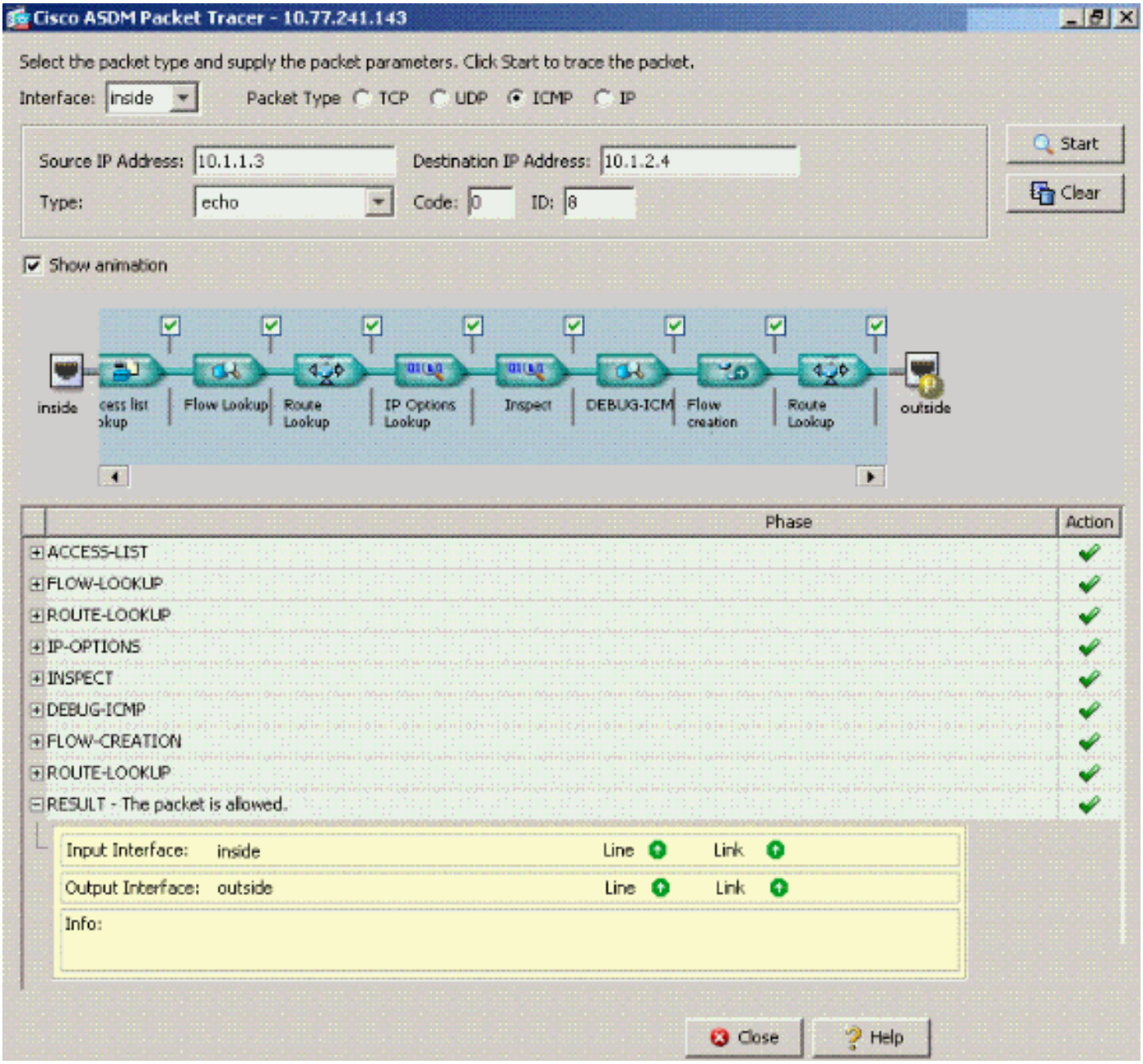
步骤 1：



步骤 2：



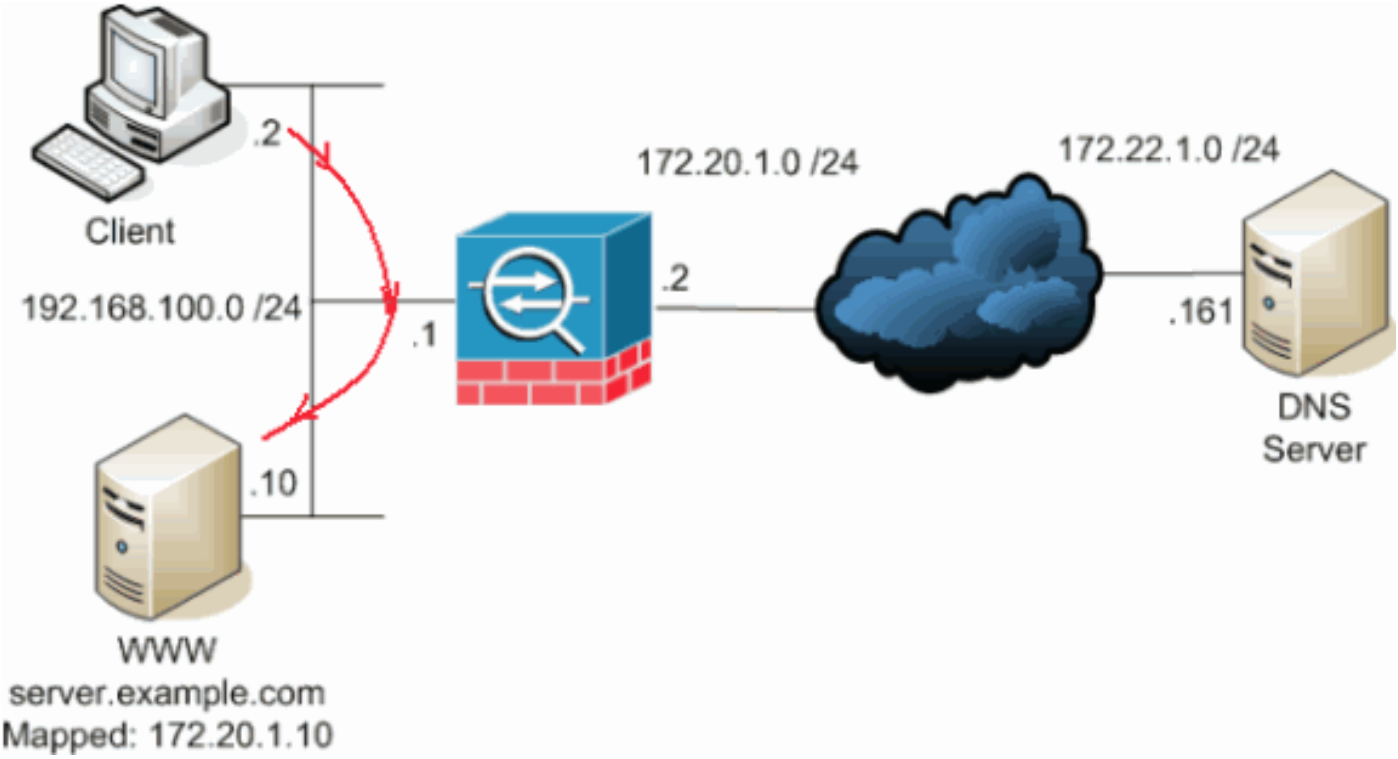
已启用 **same-security-traffic permit intra-interface** 命令并且在需要接口内流量的同一接口上配置 **access-list outside_acl extended deny ip any any** 命令的 Packet Tracer 输出。



有关 **access-list** 和 **access-group** 命令的详细信息，请参阅 access-list extended 和 access-group 。

接口内已启用静态和 NAT

本部分介绍内部用户尝试访问位于其公共地址的内部 Web 服务器的方案。



在这种情况下，192.168.100.2 处的客户端想要使用 WWW 服务器的公共地址（例如，172.20.1.10）。客户端的 DNS 服务由地址为 172.22.1.161 的外部 DNS 服务器提供。由于 DNS 服务器位于另一个公共网络上，因此，它不知道 WWW 服务器的专用 IP 地址。然而，DNS 服务器知道 WWW 服务器的映射地址 172.20.1.10。

此时，内部接口的流量必须通过内部接口进行翻译和重新路由才能到达 WWW 服务器。这称为发夹。可通过以下命令完成发夹：

```
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
```

有关完整的配置详细信息和发夹的详细信息，请参阅带有接口内通信的发夹。

对访问列表的前瞻性思考

不是所有的防火墙访问策略都相同。一些访问策略要比其它的访问策略更特别。如果接口内通信已启用，并且防火墙没有将访问列表应用到所有接口，则可能需要在接口内通信启用时添加访问列表。应用的访问列表需要允许接口内通信并保持其他访问策略要求。

以下示例说明了这一点。ASA 将私有网络（内部接口）连接到 Internet（外部接口）。ASA 内部接口没有应用访问列表。默认情况下，允许所有 IP 流量从内部流向外部。建议添加与以下输出类似的访问列表：

```
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
```

此访问列表集会继续允许所有 IP 流量。接口内通信的特定access-list线路提醒管理员必须由应用的允许接口内通信access-list。

相关信息

- Cisco 安全设备命令参考 7.2 版
- Cisco 安全设备系统日志消息 7.2 版
- Cisco PIX 防火墙软件
- ASA ：从 ASA 向 AIP SSM 发送网络流量的配置示例
- Cisco ASA 5500 系列自适应安全设备产品支持
- 技术支持和文档 - Cisco Systems