PIX/ASA 7.2(1)及更高版本：介面內通訊

目錄

簡介

本文檔有助於排除以下常見問題：在運行於軟體版本7.2(1)及更高版本的自適應安全裝置(ASA)或PIX上啟用介面內通訊。軟體版本7.2(1)具有將明文資料路由進和路由出同一介面的功能。輸入**same-security-traffic permit intra-interface**命令以啟用此功能。本檔案假設網路管理員已啟用此功能或計畫將來啟用。使用命令列介面(CLI)提供配置和故障排除。

注意：本文檔重點介紹到達和離開ASA的清晰（未加密）資料。加密資料不會討論。

要在ASA/PIX for IPsec配置上啟用介面內通訊，請參閱PIX/ASA和VPN Client for Public Internet VPN on a Stick配置示例。

要在ASA上啟用介面內通訊以進行SSL配置，請參閱ASA 7.2(2):用於單臂公共網際網路VPN的SSL VPN客戶端(SVC)配置示例。

必要條件

需求

思科建議您瞭解以下主題：

- 存取清單
- 路由

- 高級檢測和防禦 — 安全服務模組(AIP-SSM)入侵防禦系統(IPS) — 僅當模組已安裝且運行正常時，才需要瞭解此模組。
- IPS軟體版本5.x — 如果未使用AIP-SSM，則不需要瞭解IPS軟體。

採用元件

- ASA 5510 7.2(1)及更高版本
- 運行IPS軟體5.1.1的AIP-SSM-10

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

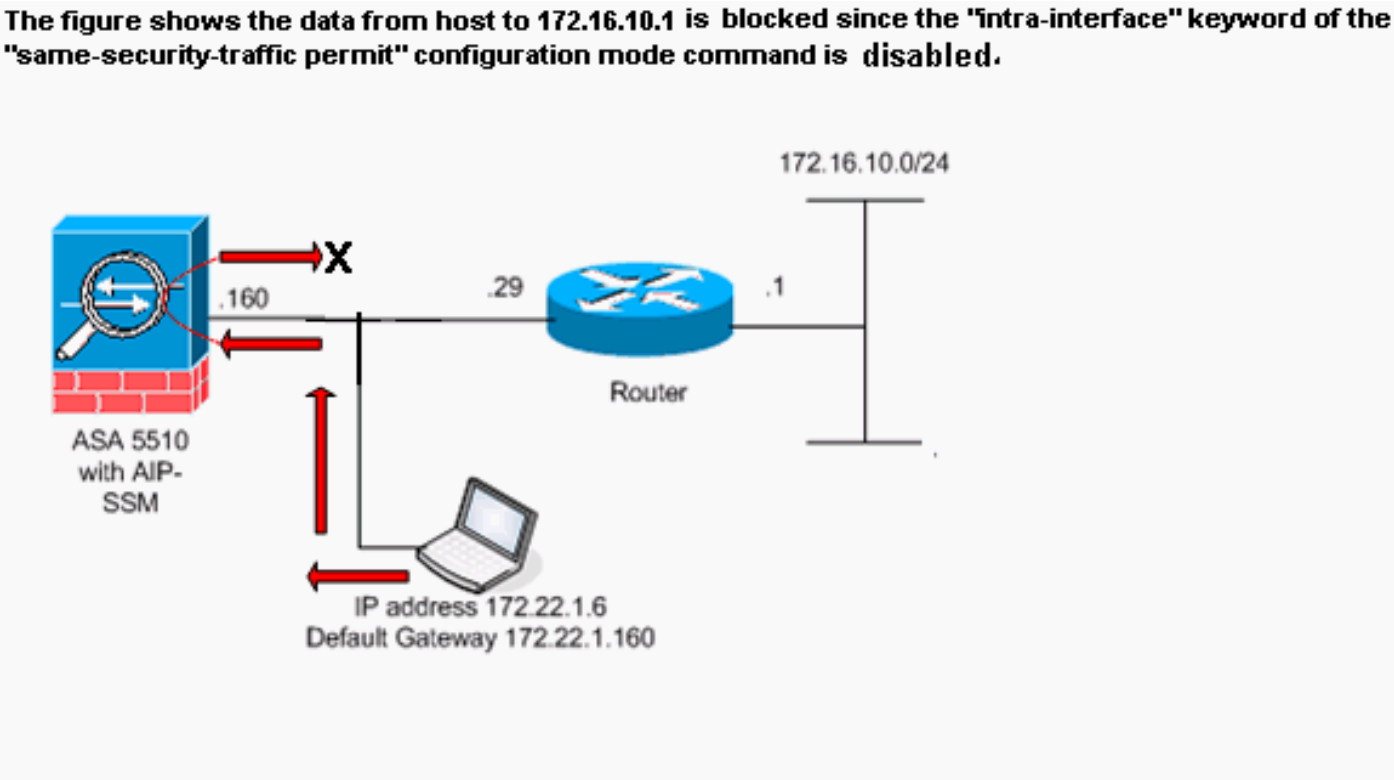
相關產品

此配置還可以與運行7.2(1)及更高版本的Cisco 500系列PIX一起使用。

慣例

如需檔案慣例的相關資訊，請參閱思科技術提示慣例。

背景資訊



注意：此配置中使用的IP編址方案在Internet上不能合法路由。這些地址是RFC 1918 ，已在實驗室環境中使用。

此表顯示了ASA啟動配置：

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:
```

疑難排解

以下各節說明了與介面內通訊有關的幾個配置場景、相關系統日誌消息和Packet Tracer輸出。

介面內通訊未啟用

在ASA配置中，主機172.22.1.6嘗試ping主機172.16.10.1。主機172.22.1.6向預設網關(ASA)傳送ICMP回應請求資料包。 尚未在ASA上啟用介面內通訊。ASA丟棄回應要求資料包。測試ping失敗。ASA用於排除故障。

此示例顯示系統日誌消息和Packet Tracer的輸出：

- 這是記錄到緩衝區的系統日誌消息：

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

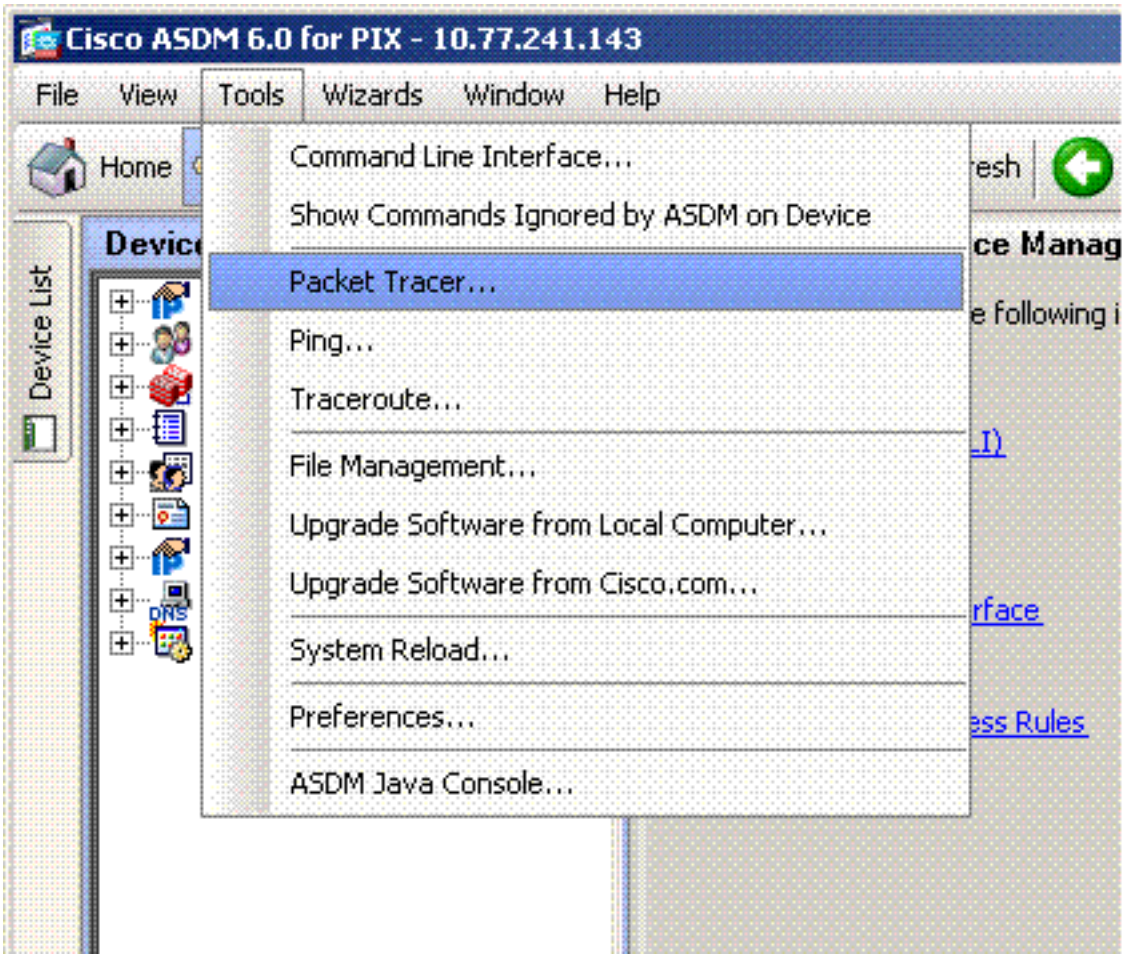
```
outside:172.16.10.1 (type 8, code 0)
```

- 以下是Packet Tracer輸出：

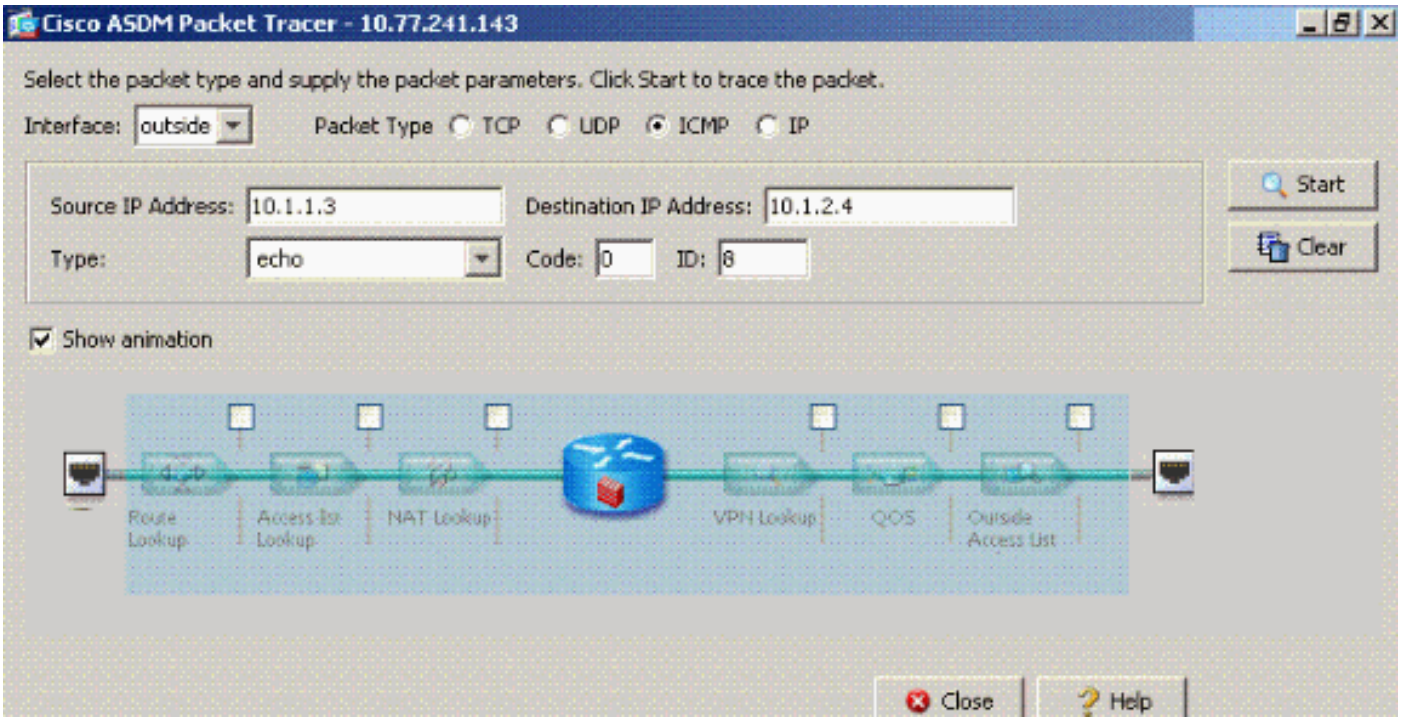
```
ciscoasa(config)#packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1 detailed
Phase: 1
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found no matching flow, creating a new flow

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中等效的CLI命令如下圖所示：

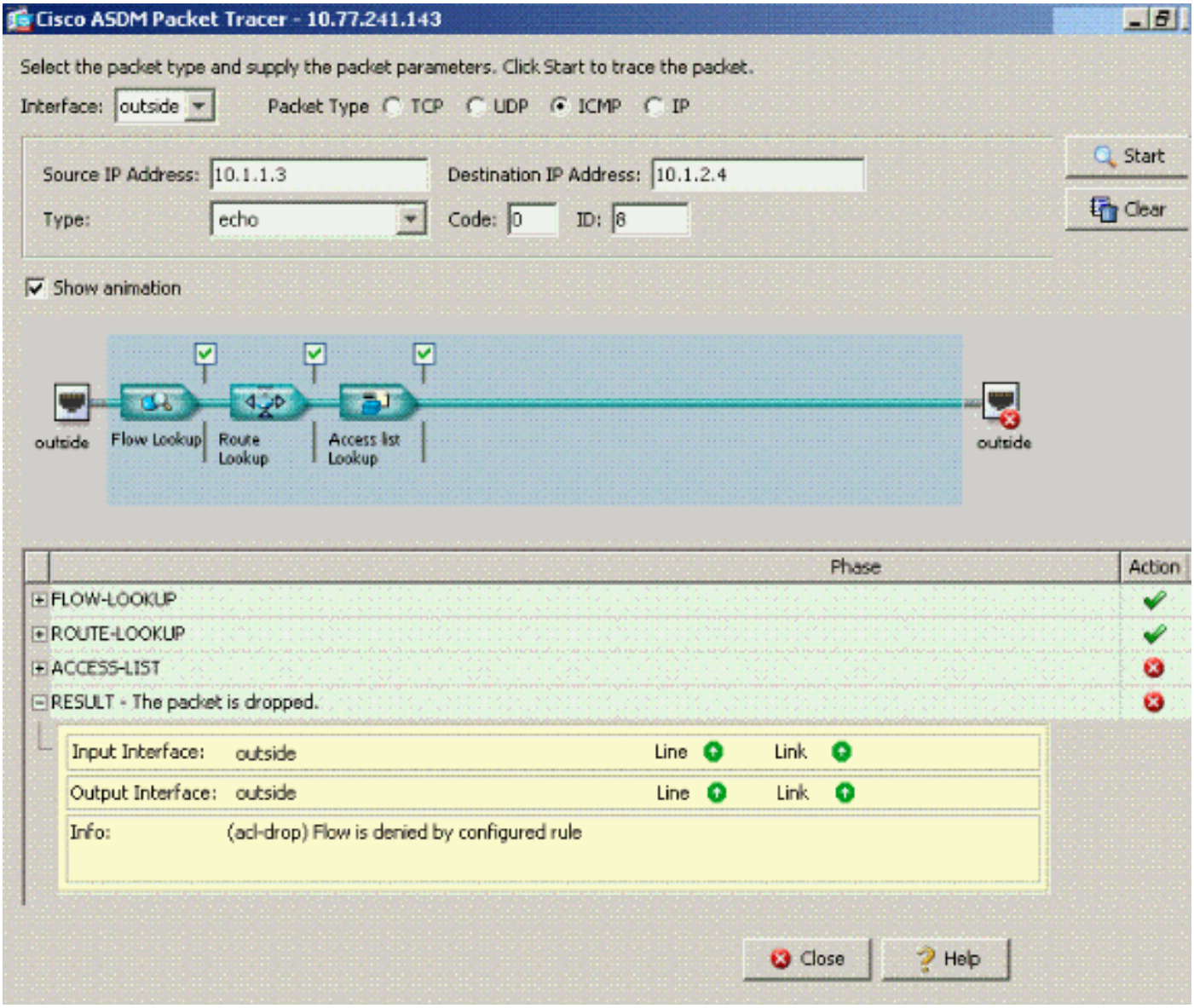
第1步：



第2步：



禁用**same-security-traffic permit intra-interface**命令的Packet Tracer輸出。



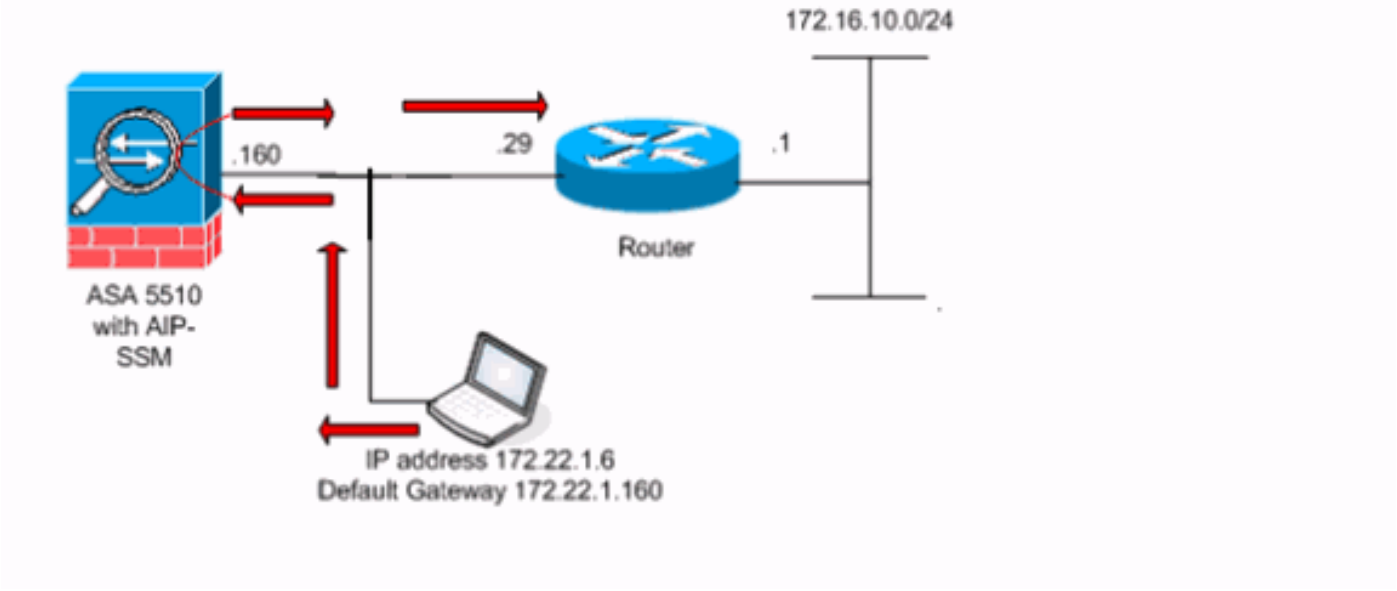
Packet Tracer輸出丟……`implicit rule`示預設配置設定正在阻止流量。管理員需要檢查運行配置，以確保啟用介面內通訊。在這種情況下，ASA配置需要啟用介面內通訊(**same-security-traffic permit intra-interface**)。

```
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...
```

已啟用介面內通訊

現已啟用介面內通訊。將**same-security-traffic permit intra-interface**命令新增到先前的配置中。主機172.22.1.6嘗試ping主機172.16.10.1。主機172.22.1.6將ICMP回應請求資料包傳送到預設網關(ASA)。 主機172.22.1.6記錄來自172.16.10.1的成功應答。ASA成功通過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.



以下示例顯示ASA系統日誌消息和Packet Tracer輸出：

- 以下是記錄到緩衝區的系統日誌訊息：

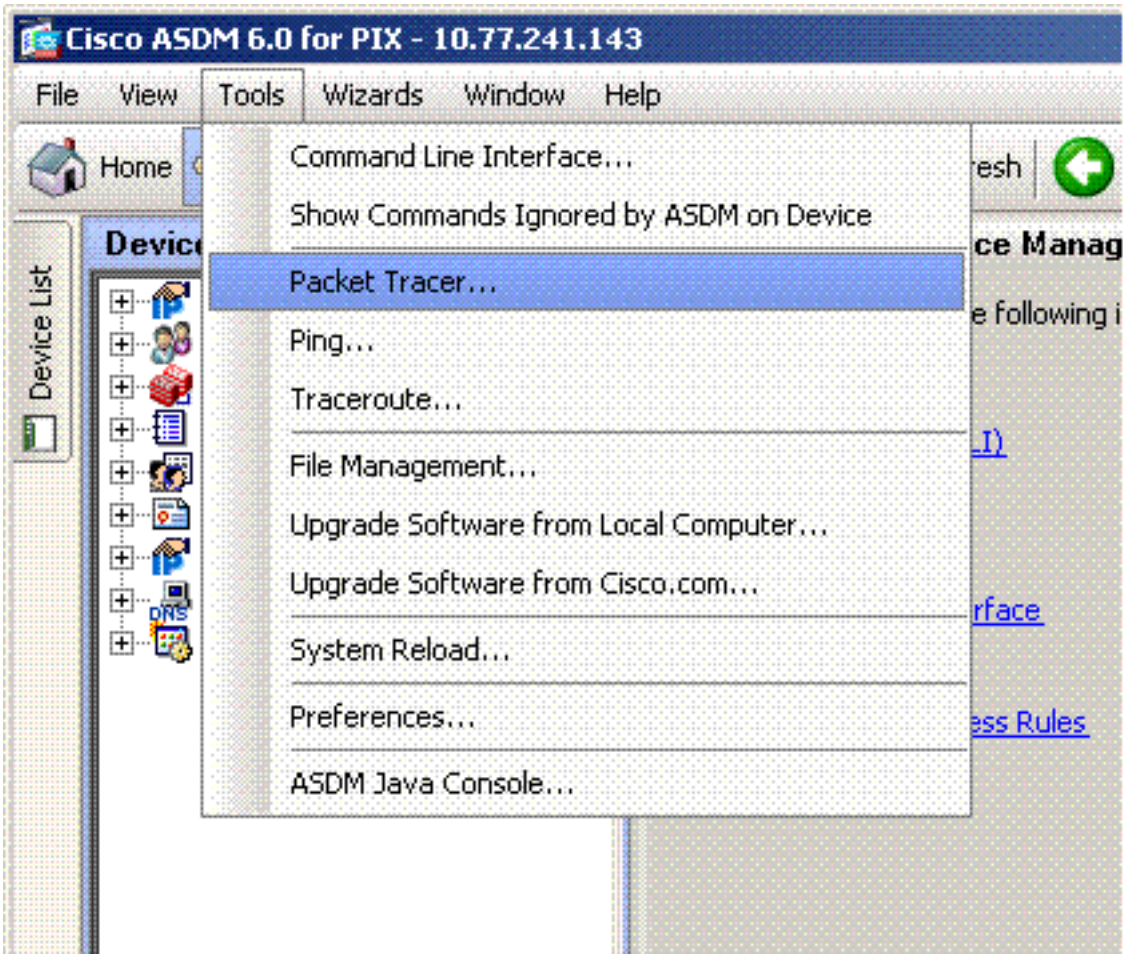
```
ciscoasa#show logging
!--- Output is suppressed. %PIX-7-609001: Built local-host outside:172.22.1.6 %PIX-7-609001:
Built local-host outside:172.16.10.1 %PIX-6-302020: Built ICMP connection for faddr
172.22.1.6/64560 gaddr 172.16.10.1/0 laddr 172.16.10.1/0 %PIX-6-302021: Teardown ICMP
connection for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

```
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      (
```

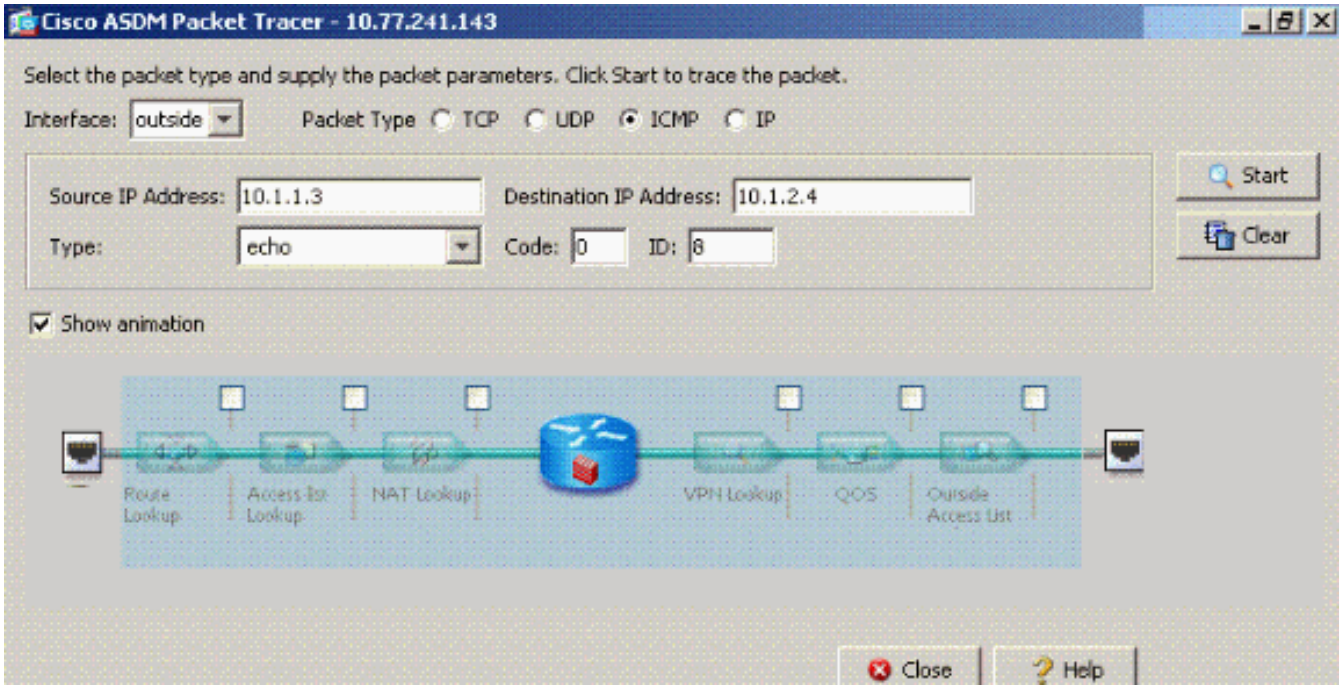
```
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

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中等效的CLI命令如下圖所示：**第1步**

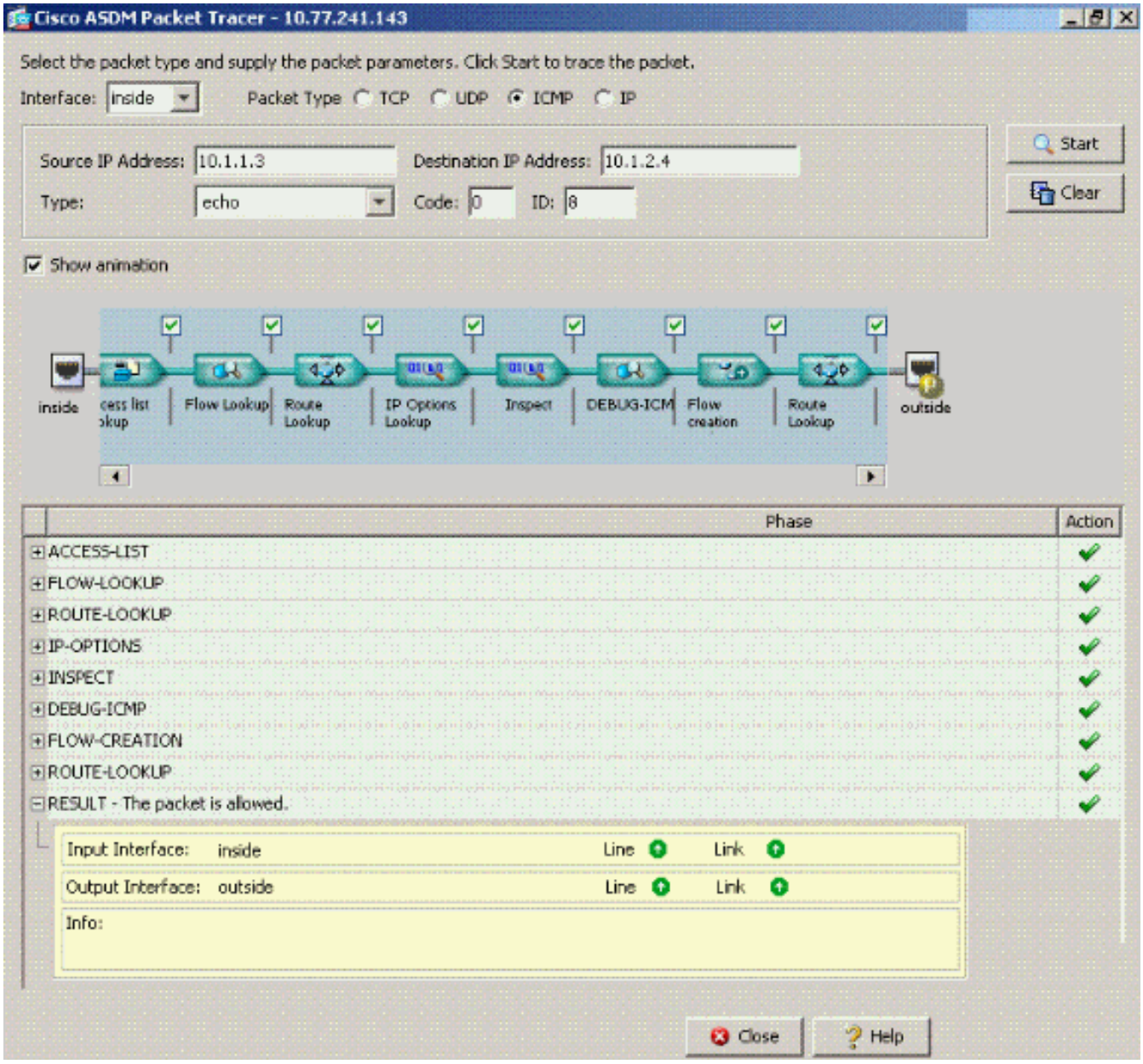


: **第2步**

:



已啟用**same-security-traffic permit intra-interface**命令的[packet-tracer](#)輸出。



注意：外部介面未應用任何訪問清單。在示例配置中，外部介面被分配安全級別0。預設情況下，防火牆不允許從低安全介面到高安全介面的流量。這可能使管理員認為在未經存取清單允許的情況下，外部（低安全性）介面不允許內部流量。但是，當介面未應用訪問清單時，相同的介面流量可自由通過。

介面內已啟用且流量已傳遞到AIP-SSM以進行檢測

介面內流量可以傳遞到AIP-SSM進行檢測。本節假設管理員已將ASA配置為將流量轉發到AIP-SSM，並且管理員知道如何配置IPS 5.x軟體。

此時，ASA配置包含先前的示例配置，介面內通訊已啟用，所有（任何）流量轉發到AIP-SSM。IPS特徵碼2004被修改為丟棄回應要求流量。主機172.22.1.6嘗試ping主機172.16.10.1。主機172.22.1.6將ICMP回應請求資料包傳送到預設網關(ASA)。 ASA將回應要求資料包轉發到AIP-SSM以供檢查。AIP-SSM根據IPS配置丟棄資料包。

以下示例顯示ASA系統日誌消息和Packet Tracer輸出：

- 這是記錄到緩衝區的系統日誌消息：

```
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輸出：

```
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.
```

必須注意的是，管理員在研究問題時應該使用儘可能多的故障排除工具。此示例說明兩種不同的故

障排除工具如何繪製不同的圖片。這兩種工具共同講述了一個完整的故事。ASA配置策略允許流量，但IPS配置不允許。

啟用介面內和應用於介面的訪問清單

本節使用本文檔中的原始示例配置、啟用的介面內通訊以及應用於測試介面的訪問清單。這些行將新增到配置中。訪問清單旨在簡單表示在生產防火牆上可能配置的內容。

```
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.
```

主機172.22.1.6嘗試ping主機172.16.10.1。主機172.22.1.6將ICMP回應請求資料包傳送到預設網關(ASA)。 ASA根據訪問清單規則丟棄回應要求資料包。主機172.22.1.6測試ping失敗。

以下示例顯示ASA系統日誌消息和Packet Tracer輸出：

- 這是記錄到緩衝區的系統日誌消息：

  ```
  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輸出：

  ```
  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
  ```

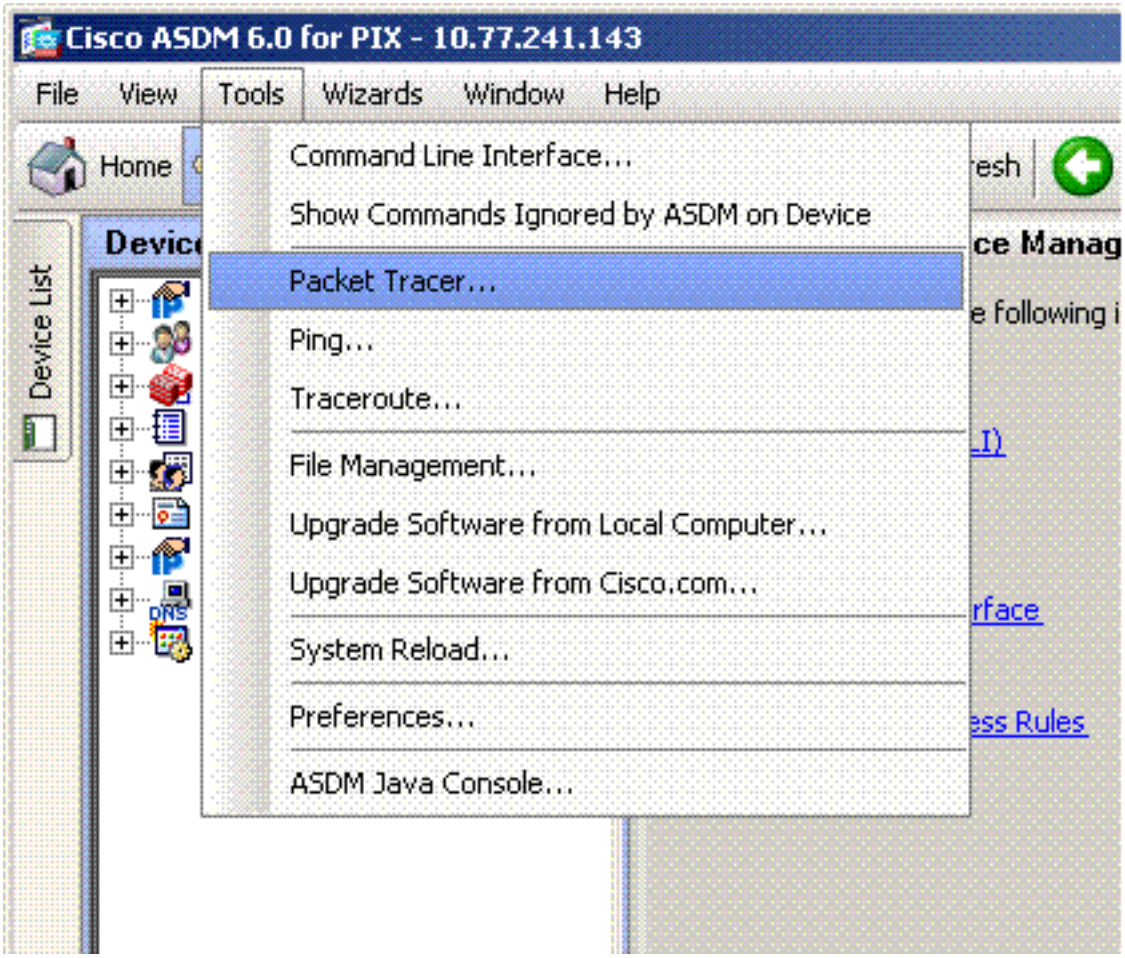
有關**packet tracer**命令的詳細資訊，請參閱packet-tracer。

註：如果應用到介面的訪問清單包含拒絕語句，則Packet Tracer的輸出將發生變化。例如：

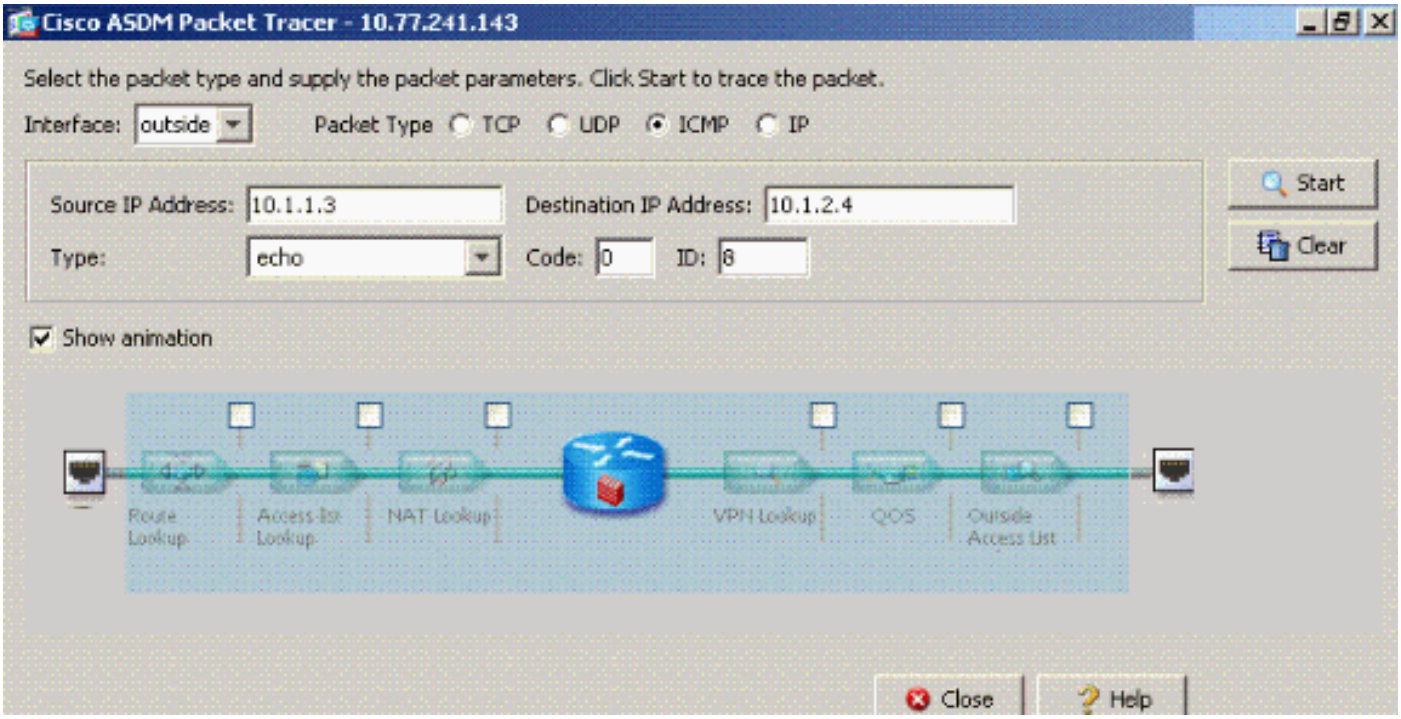
```
ciscoasa(config)#access-list outside_acl permit tcp any host 172.22.1.147 eq 80
ciscoasa(config)#access-list outside_acl deny ip any any
ciscoasa(config)#access-group outside_acl in interface outside
ciscoasa#packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1 detailed
!--- Output is suppressed. 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:
```

下圖所示為上述ASDM中CLI命令的等效命令：

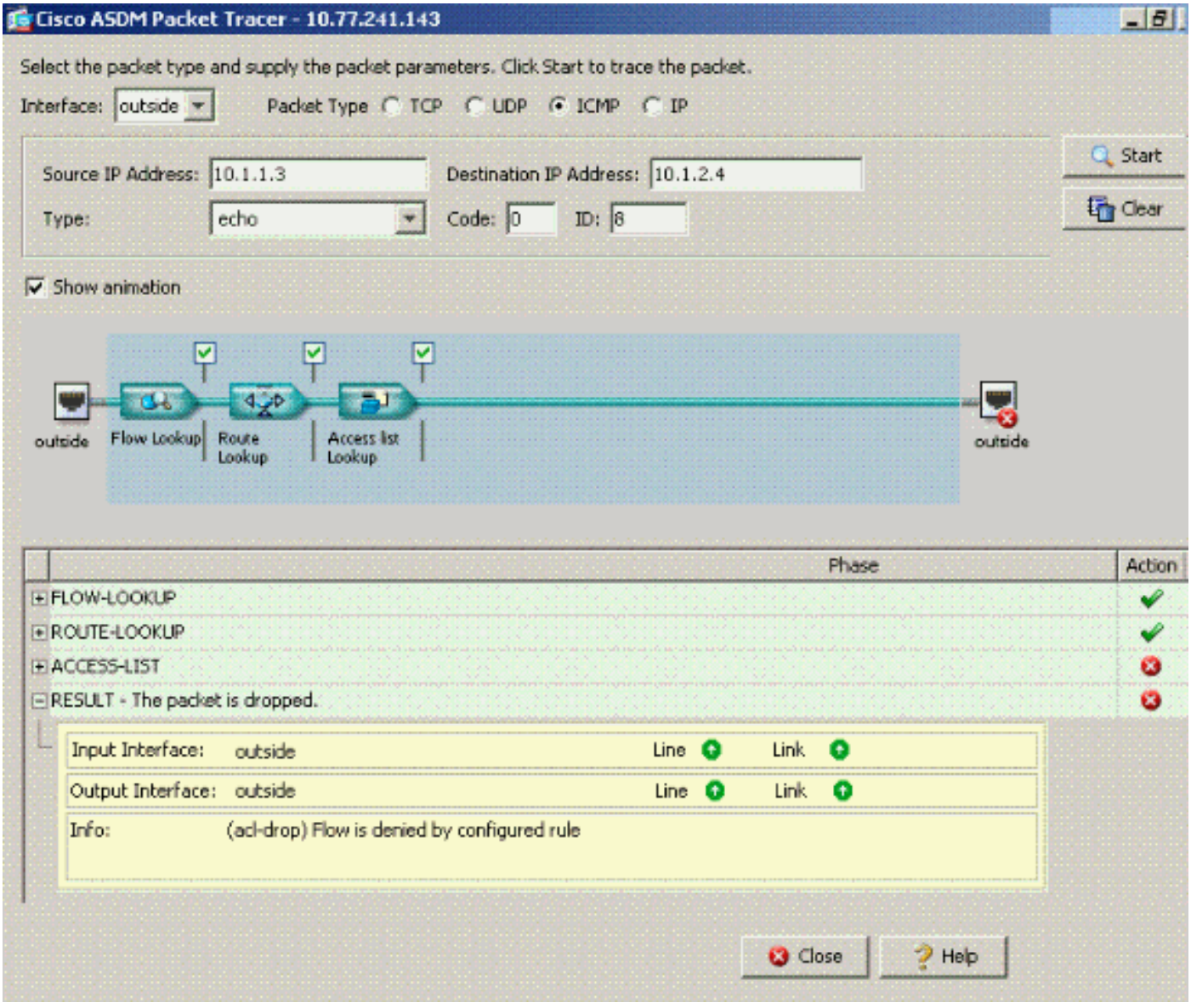
第1步：



第2步：



已啟用**same-security-traffic permit intra-interface**命令的packet Tracer輸出以及已配置為拒絕資料包的**access-list outside_acl extended deny ip any any**命令。

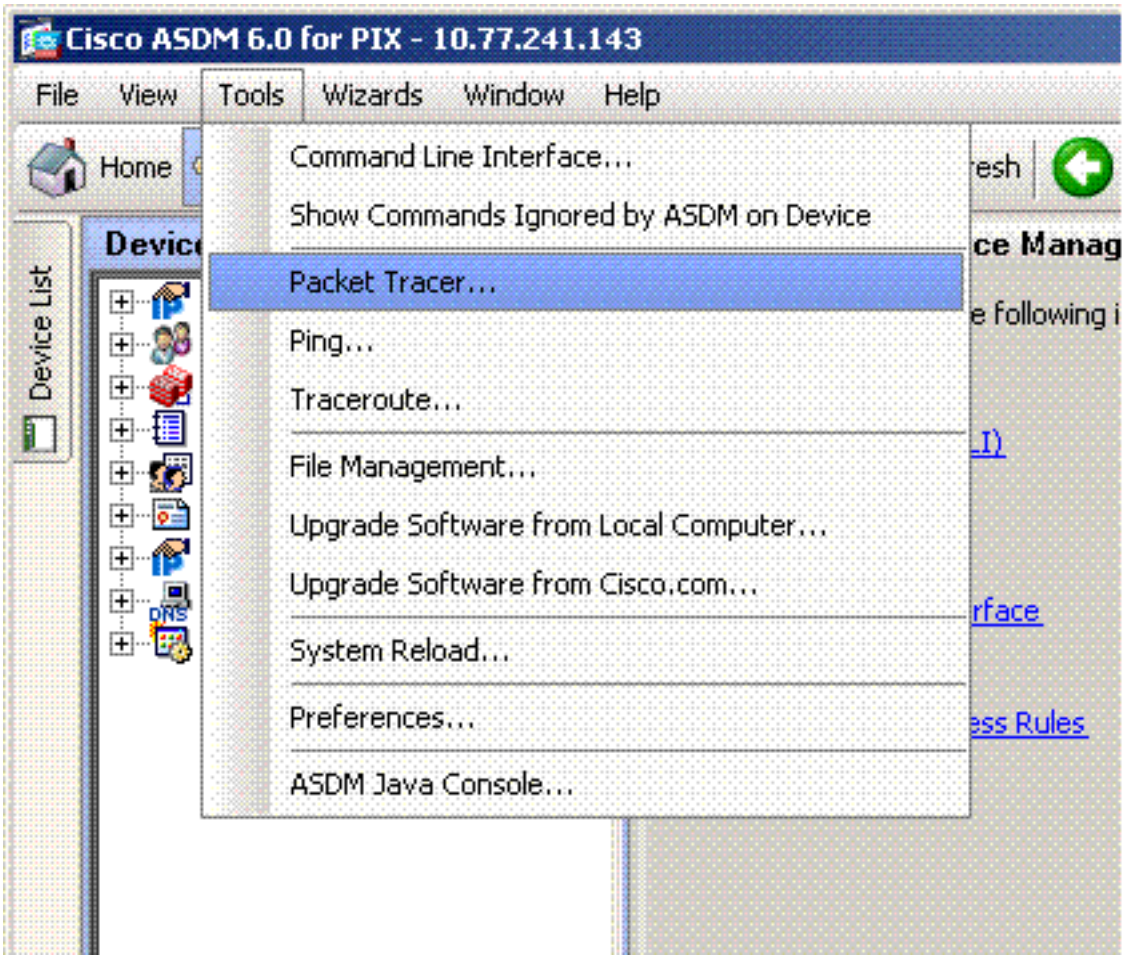


如果在特定介面上需要介面內通訊，且訪問清單應用於同一介面，則訪問清單規則必須允許介面內流量。使用本節中的範例時，存取清單需要寫為：

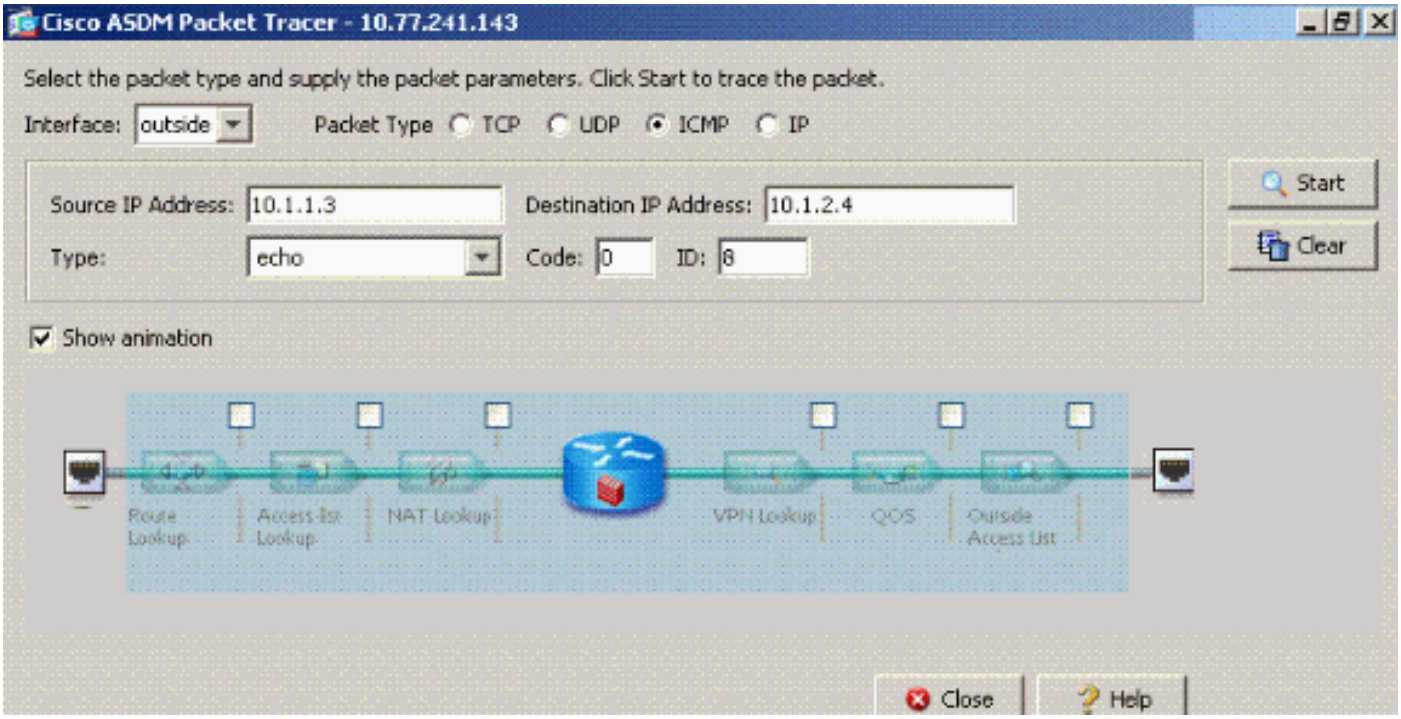
```
ciscoasa(config)#access-list outside_acl permit tcp any host 172.22.1.147 eq 80
ciscoasa(config)#access-list outside_acl permit ip 172.22.1.0 255.255.255.0 172.16.10.0
255.255.255.0
!--- 172.22.1.0 255.255.255.0 represents a locally !--- connected network on the ASA. !---
172.16.10.0 255.255.255.0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

下圖所示為上述ASDM中CLI命令的等效命令：

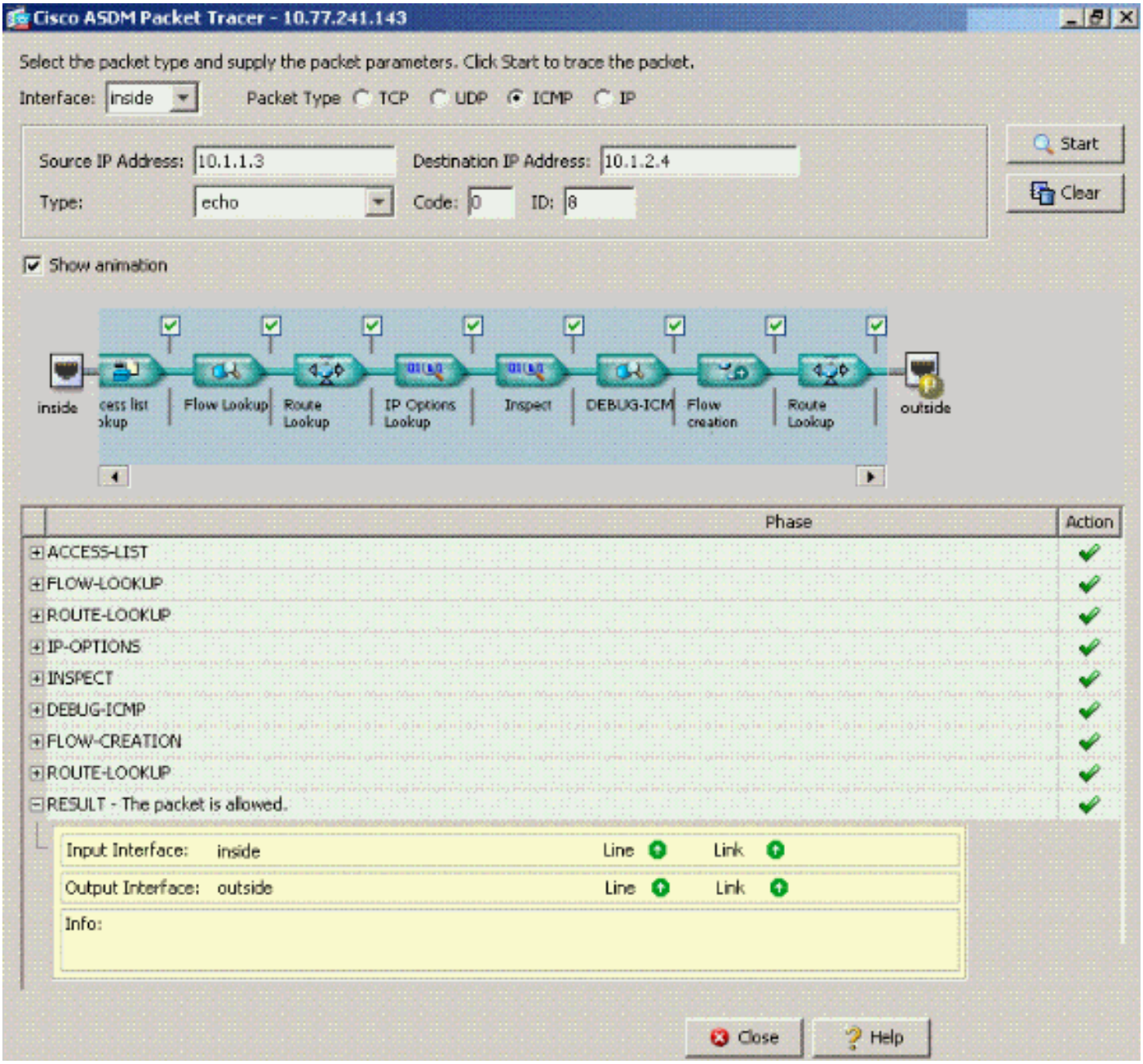
第1步：



第2步：



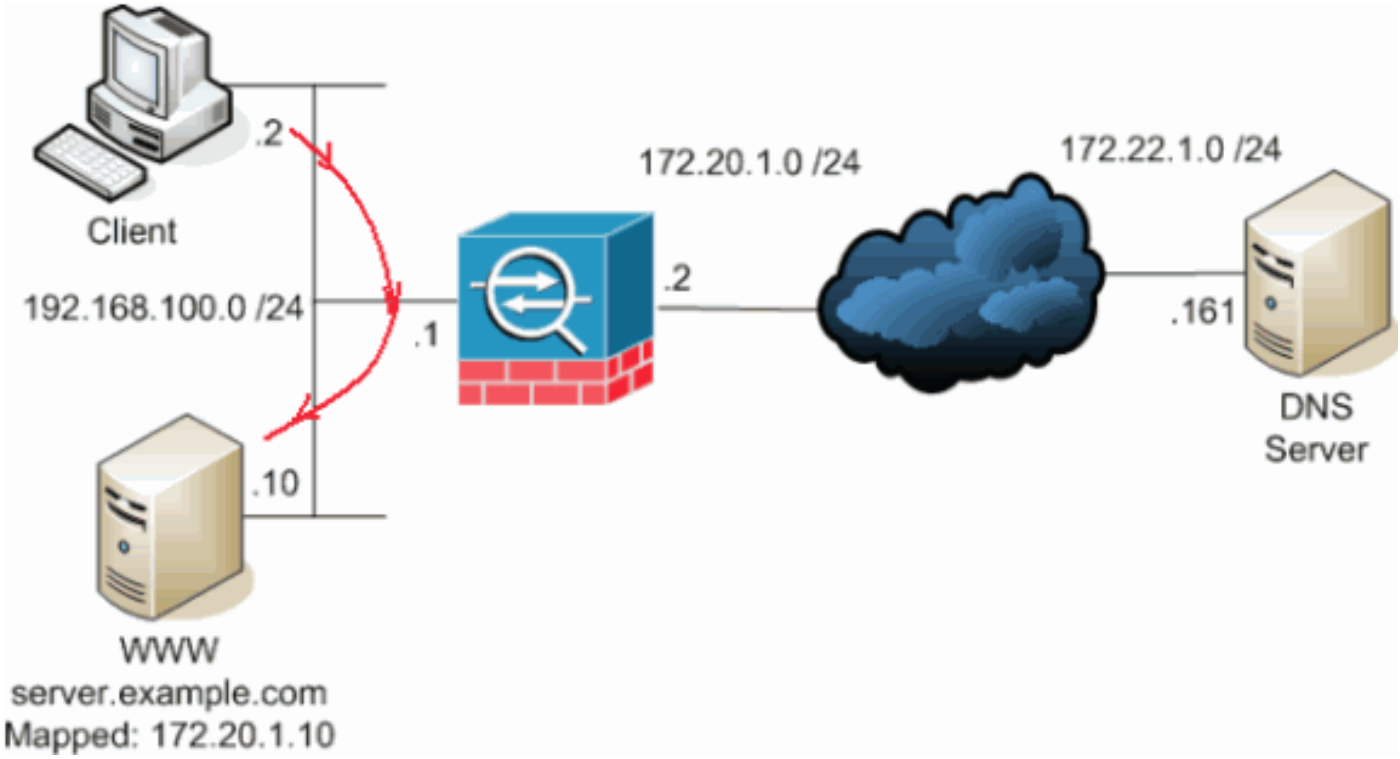
已啟用**same-security-traffic permit intra-interface**命令的packet Tracer輸出和在需要介面內流量的同一介面上配置的**access-list outside_acl extended deny ip any any**命令。



如需**access-list**和access-group命令的詳細資訊，請參閱access-list extended和access-group。

通過靜態和NAT啟用介面內

本節介紹內部使用者嘗試使用其公用位址存取內部Web伺服器的案例。



在本例中，位於192.168.100.2的客戶端希望使用WWW伺服器的公有地址（例如172.20.1.10）。客戶端的DNS服務由位於172.22.1.161的外部DNS伺服器提供。因為DNS伺服器位於另一個公共網路上，所以它不知道WWW伺服器的專用IP地址。相反，DNS伺服器知道WWW伺服器對映地址172.20.1.10。

在這裡，來自內部介面的此流量必須轉換並通過內部介面重新路由才能到達WWW伺服器。這稱為迴轉傳輸。這可以通過以下命令執行：

```
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
```

有關髮夾的完整配置詳細資訊和詳細資訊，請參閱使用介面內通訊的髮夾。

訪問清單轉發思考

並非所有防火牆訪問策略都相同。某些訪問策略比其他訪問策略更加具體。如果啟用了介面內通訊，並且防火牆沒有將訪問清單應用於所有介面，則可能值得在啟用介面內通訊時新增訪問清單。應用的訪問清單需要允許介面內通訊並維護其他訪問策略要求。

此示例說明了這一點。ASA將專用網路（內部介面）連線到Internet（外部介面）。 ASA內部介面未應用訪問清單。預設情況下，所有IP流量都允許從內部到外部。建議新增類似於以下輸出的訪問清單：

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

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

這組存取清單繼續允許所有IP流量。介面內通訊的特定訪問清單行提醒管理員，應用的訪問清單必須允許介面內通訊。

相關資訊

- 思科安全裝置命令參考7.2版
- 思科安全裝置系統日誌消息版本7.2
- Cisco PIX防火牆軟體
- ASA:從ASA向AIP SSM傳送網路流量配置示例
- Cisco ASA 5500系列自適應安全裝置產品支援
- 技術支援與文件 - Cisco Systems