PIX/ASA 7.2(1) e versioni successive: Comunicazioni intra-interfaccia

Sommario

Introduzione

Questo documento aiuta a risolvere i problemi più comuni che si verificano quando si abilitano le comunicazioni intra-interfaccia su un'appliance ASA (Adaptive Security Appliance) o su un PIX compatibile con il software versione 7.2(1) e successive. Il software versione 7.2(1) offre la possibilità di instradare dati non crittografati in entrata e in uscita dalla stessa interfaccia. Per abilitare questa funzione, immettere il comando **intra-interface same-security-traffic-allow**. in questo documento si presume che l'amministratore di rete abbia abilitato questa funzione o lo faccia in futuro. La configurazione e la risoluzione dei problemi vengono fornite mediante l'interfaccia della riga di comando (CLI).

Nota: questo documento è incentrato sui dati non crittografati che arrivano e lasciano l'appliance ASA. I dati crittografati non vengono trattati.

Per abilitare la comunicazione intra-interfaccia su ASA/PIX per la configurazione IPsec, fare riferimento agli esempi di configurazione di PIX/ASA e VPN Client per VPN Internet pubblica su Memory Stick.

Per abilitare la comunicazione intra-interfaccia sull'appliance ASA per la configurazione SSL, fare riferimento alla sezione ASA 7.2(2): Esempio di configurazione su Memory Stick del client VPN SSL (SVC) per VPN Internet pubblica.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Elenchi di accesso
- Routing
- Advanced Inspection and Prevention-Security Services Module (AIP-SSM) Intrusion Prevention System (IPS): la conoscenza di questo modulo è necessaria solo se il modulo è installato e operativo.
- Software IPS release 5.x: la conoscenza del software IPS non è necessaria se AIP-SSM non è in uso.

Componenti usati

- ASA 5510 7.2(1) e versioni successive
- AIP-SSM-10 con software IPS 5.1.1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

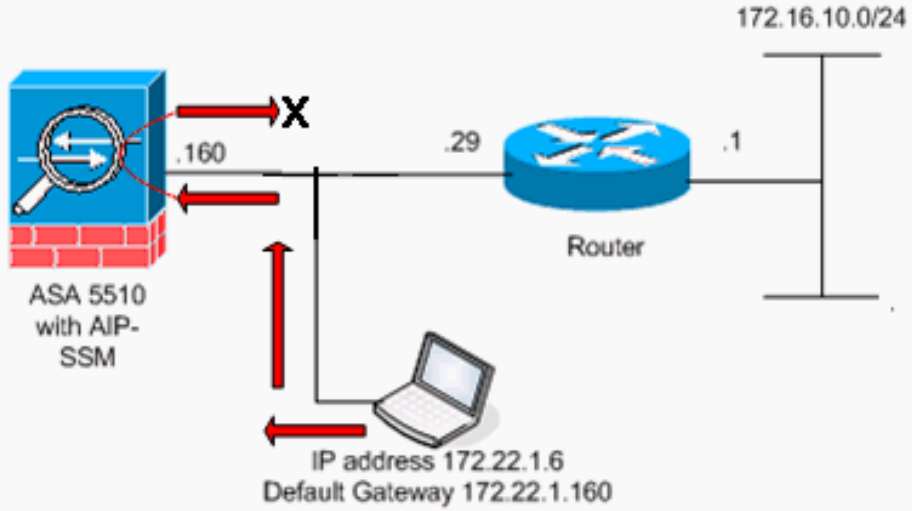
Questa configurazione può essere utilizzata anche con Cisco serie 500 PIX con versione 7.2(1) e successive.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

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.



Nota: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

La tabella mostra la configurazione iniziale dell'ASA:

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:
```

Risoluzione dei problemi

Nelle sezioni seguenti vengono illustrati diversi scenari di configurazione, messaggi syslog correlati e output di packet-tracer in relazione alle comunicazioni intra-interfaccia.

Comunicazioni intra-interfaccia non abilitate

Nella configurazione ASA, l'host 172.22.1.6 tenta di eseguire il ping tra l'host 172.16.10.1. L'host 172.22.1.6 invia un pacchetto di richiesta echo ICMP al gateway predefinito (ASA). Le comunicazioni intra-interfaccia non sono state abilitate sull'appliance ASA. L'ASA rifiuta il pacchetto di richiesta echo. Il ping di test non ha esito positivo. L'appliance ASA viene usata per risolvere il problema.

Nell'esempio viene mostrato l'output dei messaggi syslog e di un pacchetto-tracer:

- Questo è il messaggio syslog registrato nel 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)
```

- Questo è l'output del comando packet-tracer:

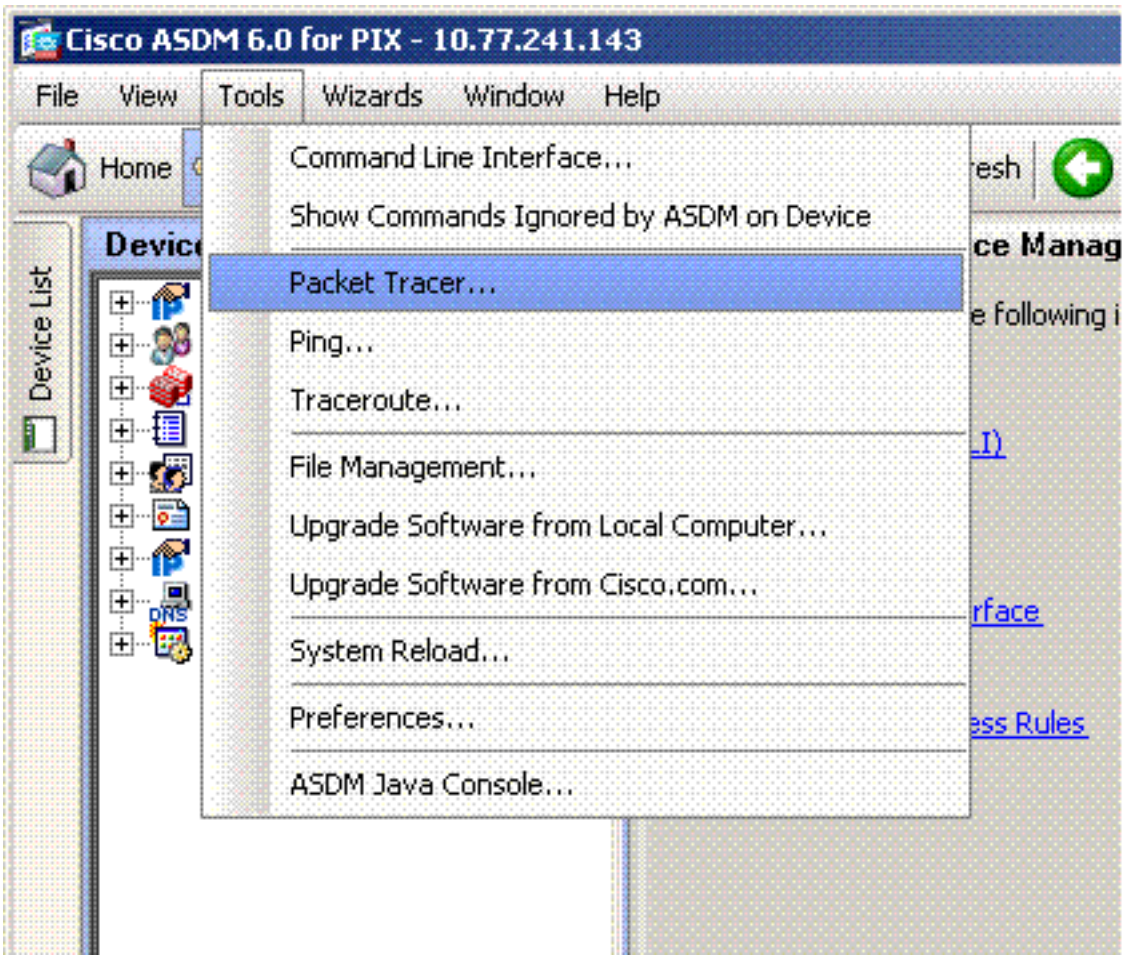
```
ciscoasa(config)#packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1 detailed
Phase: 1
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found no matching flow, creating a new flow

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

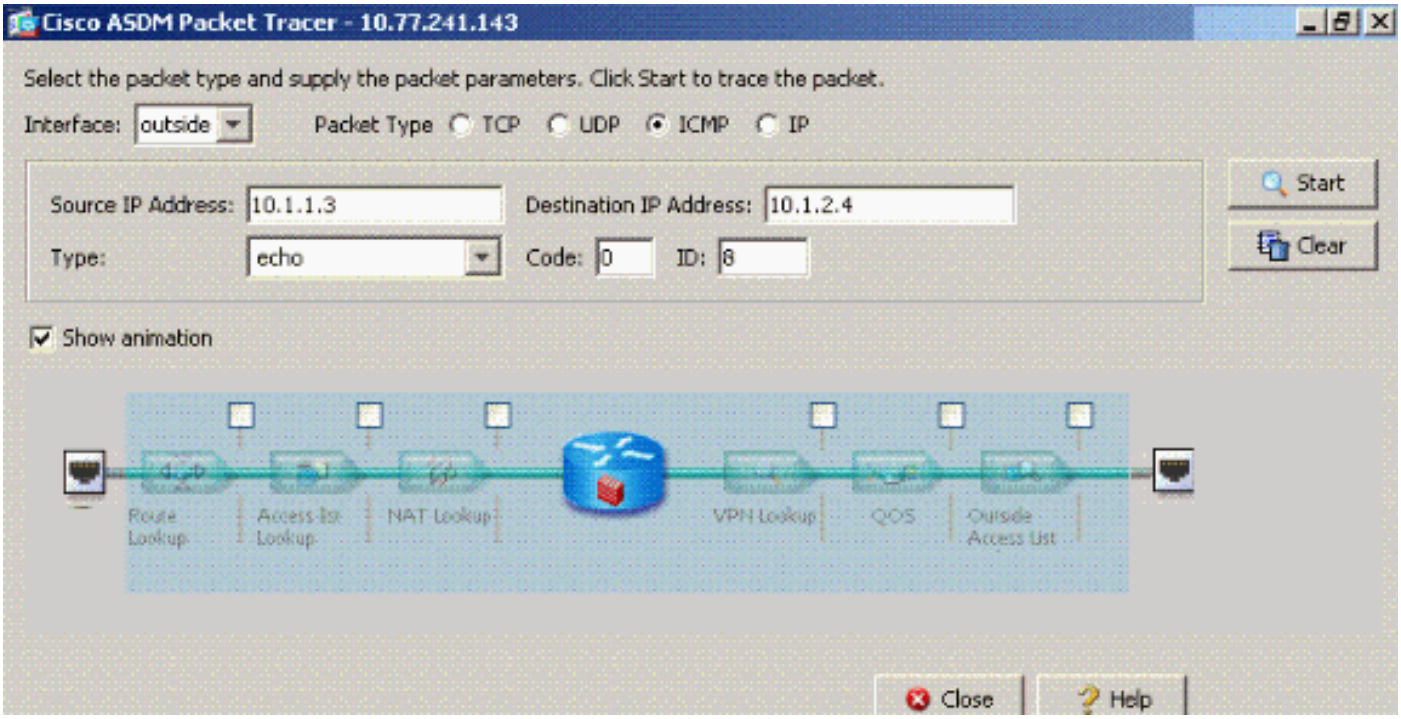
```
!--- Implicit rule refers to configuration rules not configured !--- by the user. By
default, intra-interface communication is not permitted. !--- In this example, the user has
not enabled intra-interface communications !--- and therefore the traffic is implicitly
denied. Additional Information: 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
```

L'equivalente dei comandi CLI in ASDM è mostrato nelle seguenti figure:

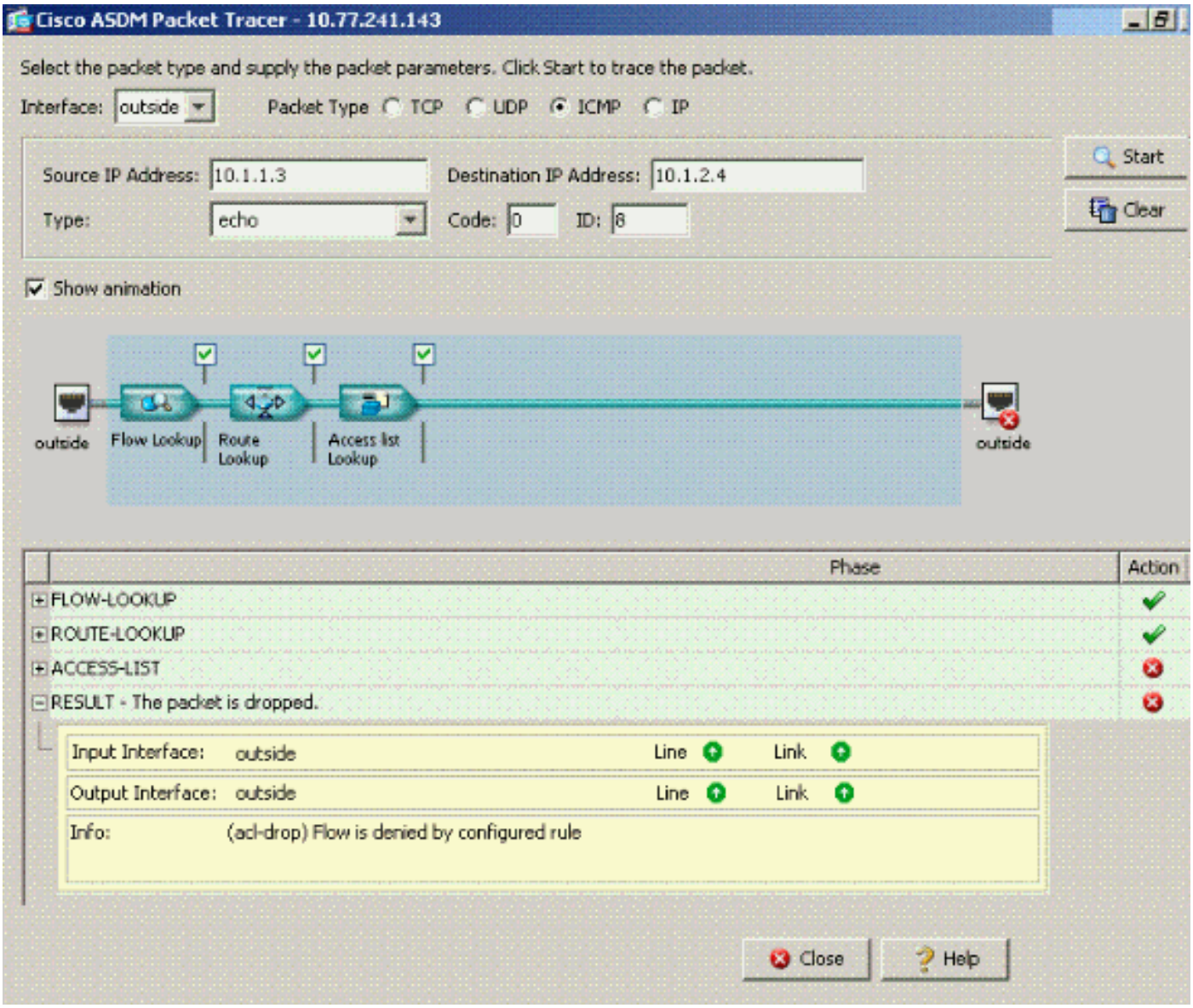
Passaggio 1:



Passaggio 2:



L'output packet-tracer con il comando **intra-interface** show-**security-traffic** permette.



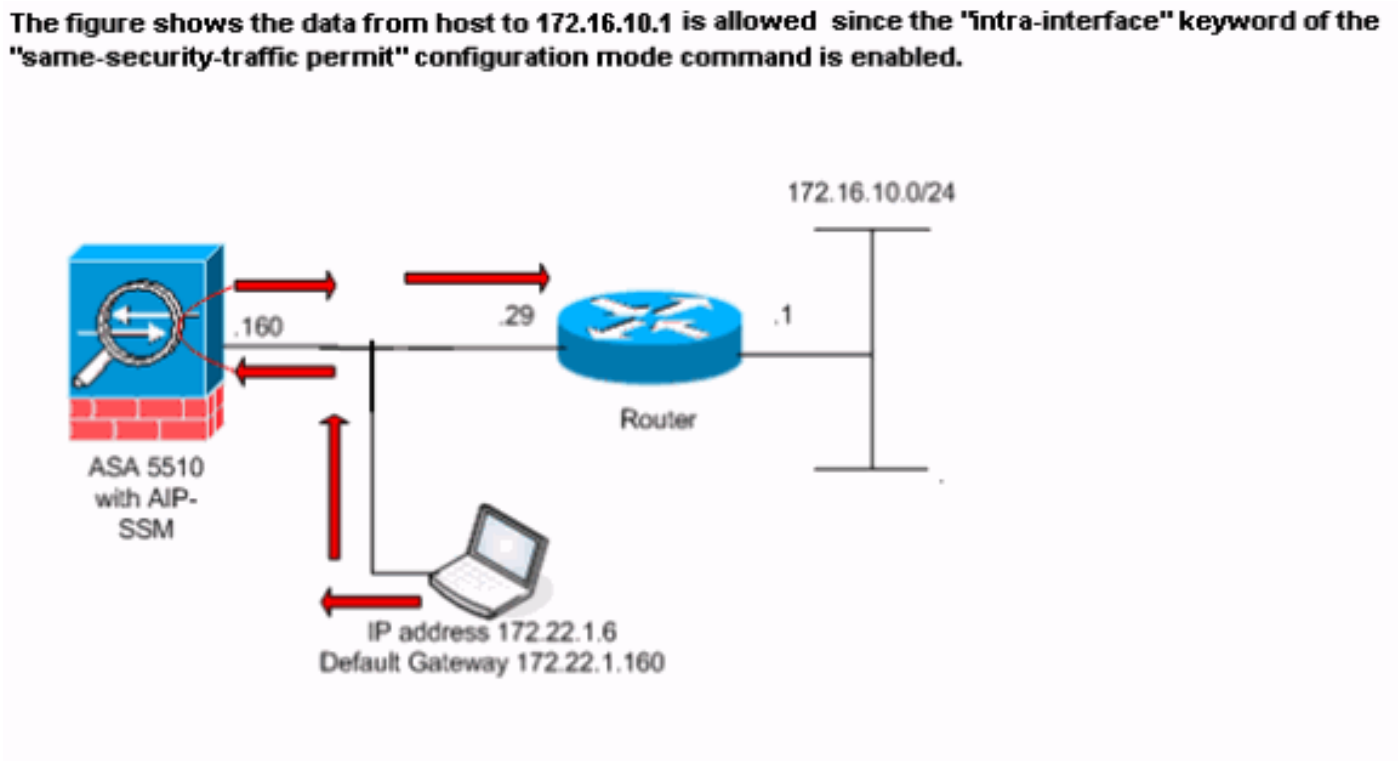
Il pacchetto-tracer output `drop...una regola implicita` suggerisce che un'impostazione di configurazione predefinita blocca il traffico. L'amministratore deve controllare la configurazione in esecuzione per garantire che le comunicazioni tra le interfacce siano abilitate. In questo caso, per abilitare le comunicazioni tra le interfacce della configurazione ASA (**lo stesso tipo di traffico di sicurezza permette le comunicazioni tra le interfacce**).

```
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...
```

Comunicazioni intra-interfaccia abilitate

Le comunicazioni intra-interfaccia sono ora abilitate. alla configurazione precedente, è stato aggiunto il comando **same-security-traffic allow intra-interface**. L'host 172.22.1.6 tenta di eseguire il ping tra l'host 172.16.10.1. L'host 172.22.1.6 invia un pacchetto di richiesta echo ICMP al gateway predefinito (ASA). L'host 172.22.1.6 registra le risposte riuscite della versione 172.16.10.1. L'ASA supera correttamente il traffico ICMP.

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.



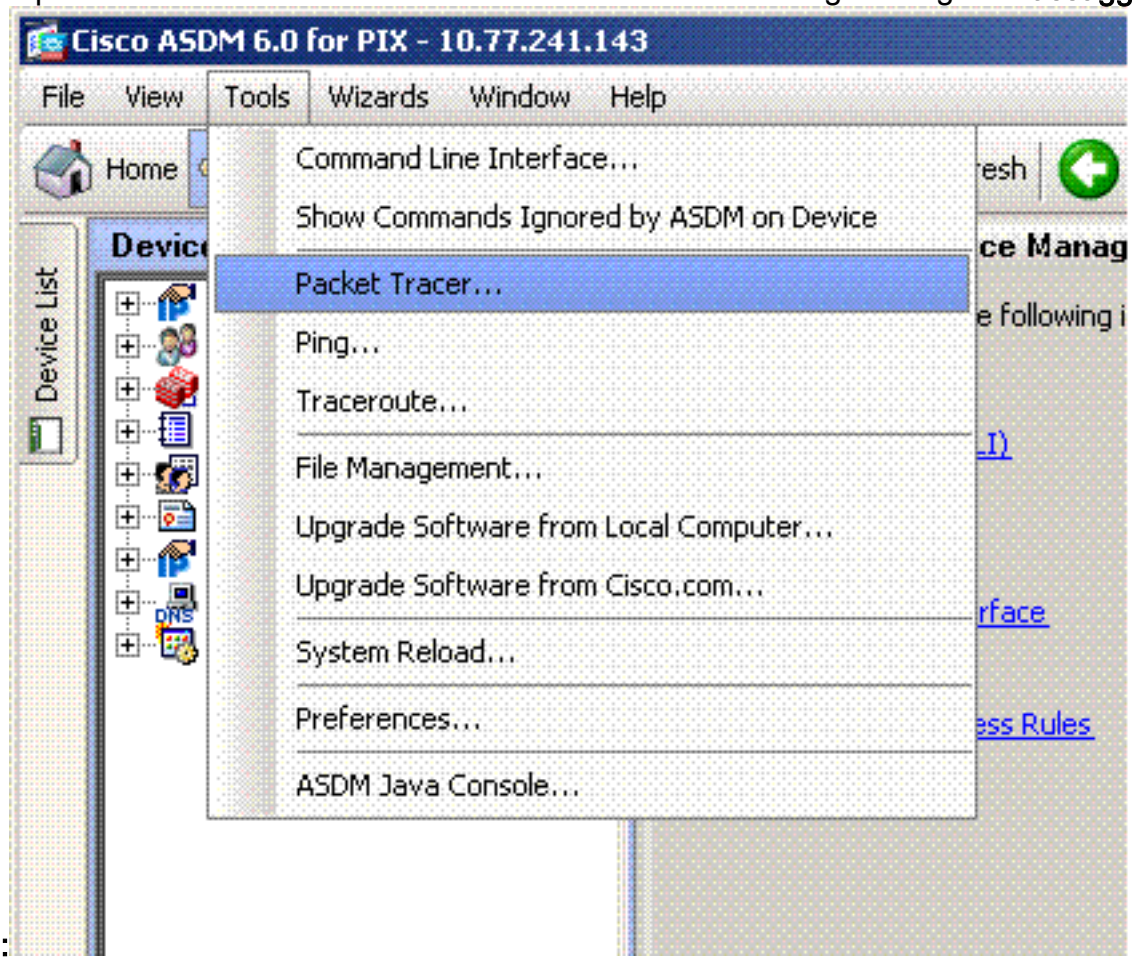
Gli esempi mostrano gli output del messaggio syslog ASA e del comando packet-tracer:

- Questi sono i messaggi syslog registrati nel 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
  ```
- Questo è l'output del comando packet-tracer:

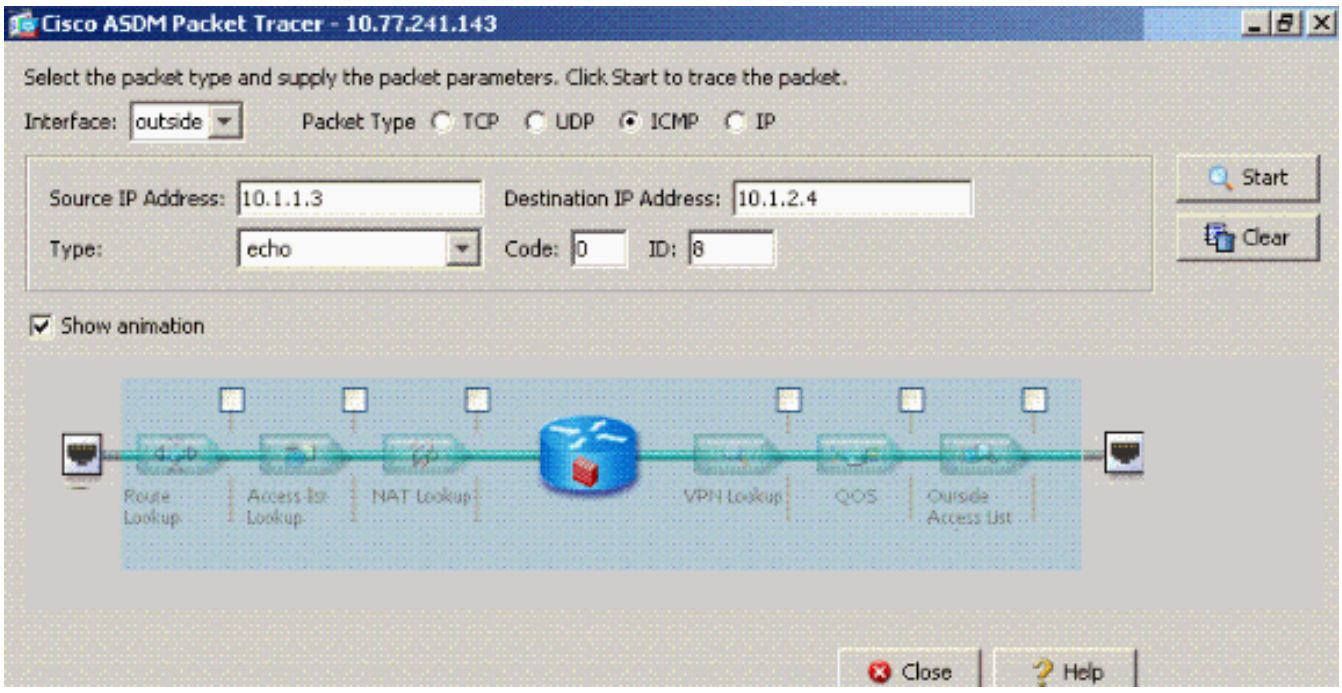
```
ciscoasa(config)#packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1

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
```

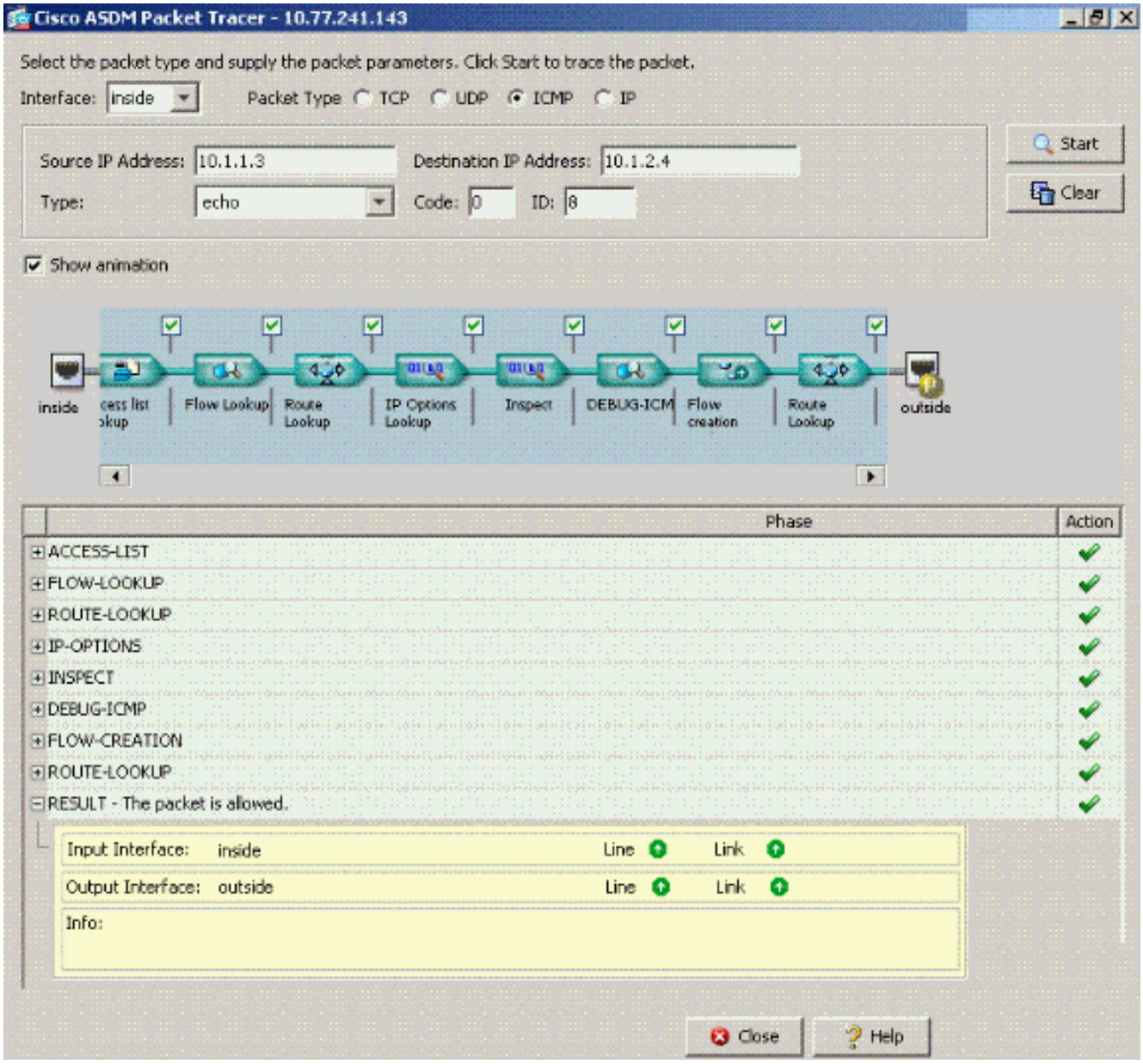
L'equivalente dei comandi CLI in ASDM è mostrato nelle seguenti figure:**Passaggio 1:**



Passaggio 2:



L'output [packet-tracer] con il comando **same-security-traffic permette di intra-interface** è abilitato.



Nota: all'interfaccia esterna non è applicato alcun elenco degli accessi. Nella configurazione di esempio, all'interfaccia esterna viene assegnato il livello di protezione 0. Per impostazione predefinita, il firewall non consente il traffico da un'interfaccia con un livello di protezione basso a un'interfaccia con un livello di protezione alto. Ciò potrebbe portare gli amministratori a credere che il traffico all'interno dell'interfaccia non sia autorizzato sull'interfaccia esterna (a bassa sicurezza) senza l'autorizzazione di un elenco degli accessi. Tuttavia, lo stesso traffico di interfaccia passa liberamente quando all'interfaccia non viene applicato alcun elenco degli accessi.

Traffico e abilitazione intra-interfaccia passati all'AIP-SSM per l'ispezione

Il traffico intra-interfaccia può essere trasmesso all'AIP-SSM per ispezione. In questa sezione si presume che l'amministratore abbia configurato l'ASA per inoltrare il traffico all'AIP-SSM e che sappia come configurare il software IPS 5.x.

A questo punto, la configurazione ASA contiene l'esempio di configurazione precedente, le comunicazioni tra le interfacce sono abilitate e tutto il traffico (qualsiasi) viene inoltrato all'AIP-SSM. La firma IPS 2004 viene modificata in modo da eliminare il traffico delle richieste echo. L'host 172.22.1.6 tenta di eseguire il ping tra l'host 172.16.10.1. L'host 172.22.1.6 invia un

pacchetto di richiesta echo ICMP al gateway predefinito (ASA). L'ASA inoltra il pacchetto di richiesta echo all'AIP-SSM per un'ispezione. AIP-SSM scarta il pacchetto dati per la configurazione IPS.

Gli esempi mostrano il messaggio syslog ASA e l'output del comando packet-tracer:

- Questo è il messaggio syslog registrato nel 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.
```
- Questo è l'output del comando packet-tracer:
```
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.
```

Èimportante notare che gli amministratori devono utilizzare il maggior numero possibile di strumenti di risoluzione dei problemi quando ricercano un problema. Nell'esempio viene mostrato come due diversi strumenti di risoluzione dei problemi possono colorare immagini diverse. Entrambi gli strumenti insieme raccontano una storia completa. Il criterio di configurazione ASA consente il traffico, a differenza della configurazione IPS.

Elenchi accessi intra-interfaccia abilitati e applicati a un'interfaccia

In questa sezione viene usata la configurazione di esempio originale illustrata in questo documento, le comunicazioni intra-interfaccia abilitate e un elenco degli accessi applicato all'interfaccia testata. Queste linee vengono aggiunte alla configurazione. L'elenco degli accessi deve essere una semplice rappresentazione di ciò che potrebbe essere configurato su un firewall di produzione.

```
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.
```

L'host 172.22.1.6 tenta di eseguire il ping tra l'host 172.16.10.1. L'host 172.22.1.6 invia un pacchetto di richiesta echo ICMP al gateway predefinito (ASA). L'ASA rifiuta il pacchetto di richiesta echo in base alle regole dell'elenco degli accessi. Il ping di test dell'host 172.22.1.6 non è riuscito.

Gli esempi mostrano il messaggio syslog ASA e l'output del comando packet-tracer:

- Questo è il messaggio syslog registrato nel 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]
  ```
- Questo è l'output del comando packet-tracer:
  ```
  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
```

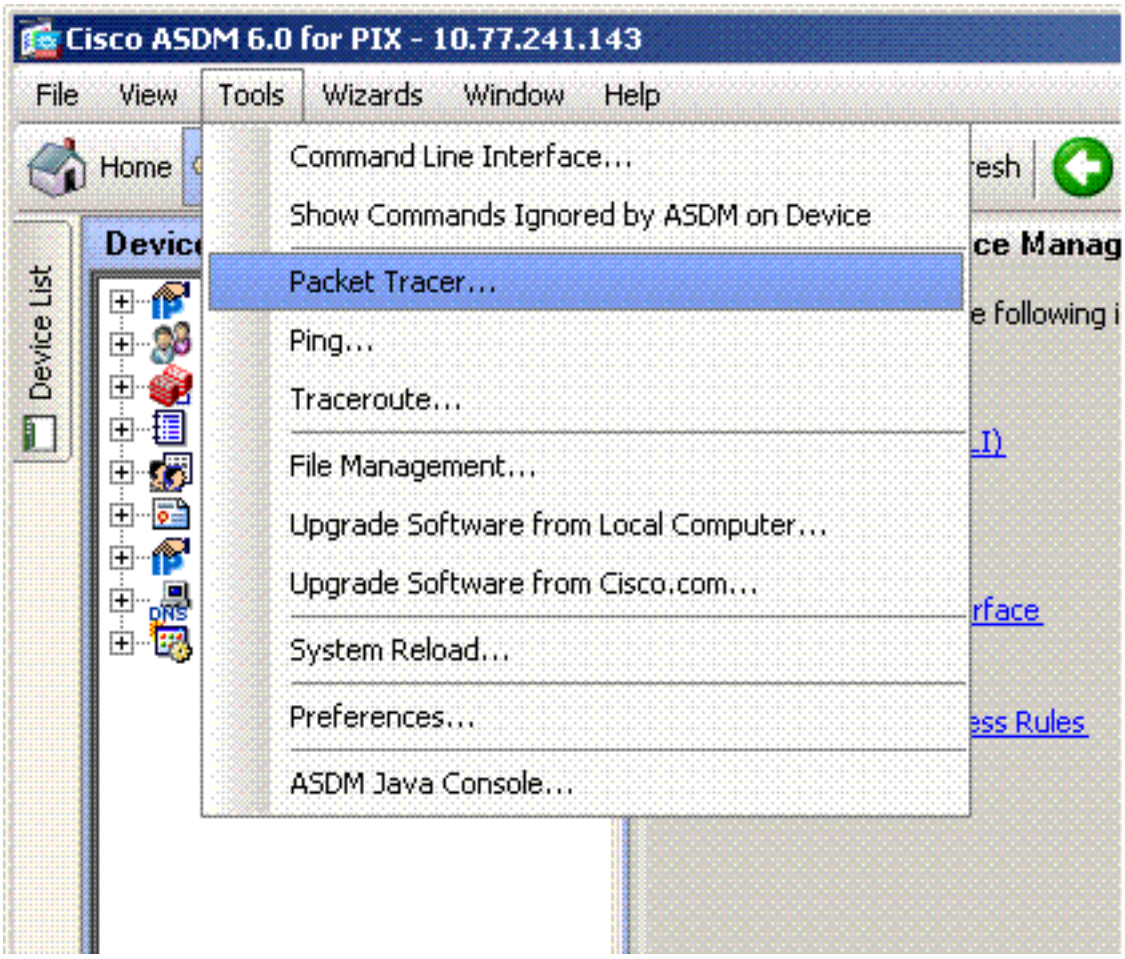
Per ulteriori informazioni sul comando **packet-tracer**, consultare il documento packet-tracer.

Nota: se l'elenco degli accessi applicato all'interfaccia include un'istruzione deny, l'output del comando packet-tracer cambia. Ad esempio:

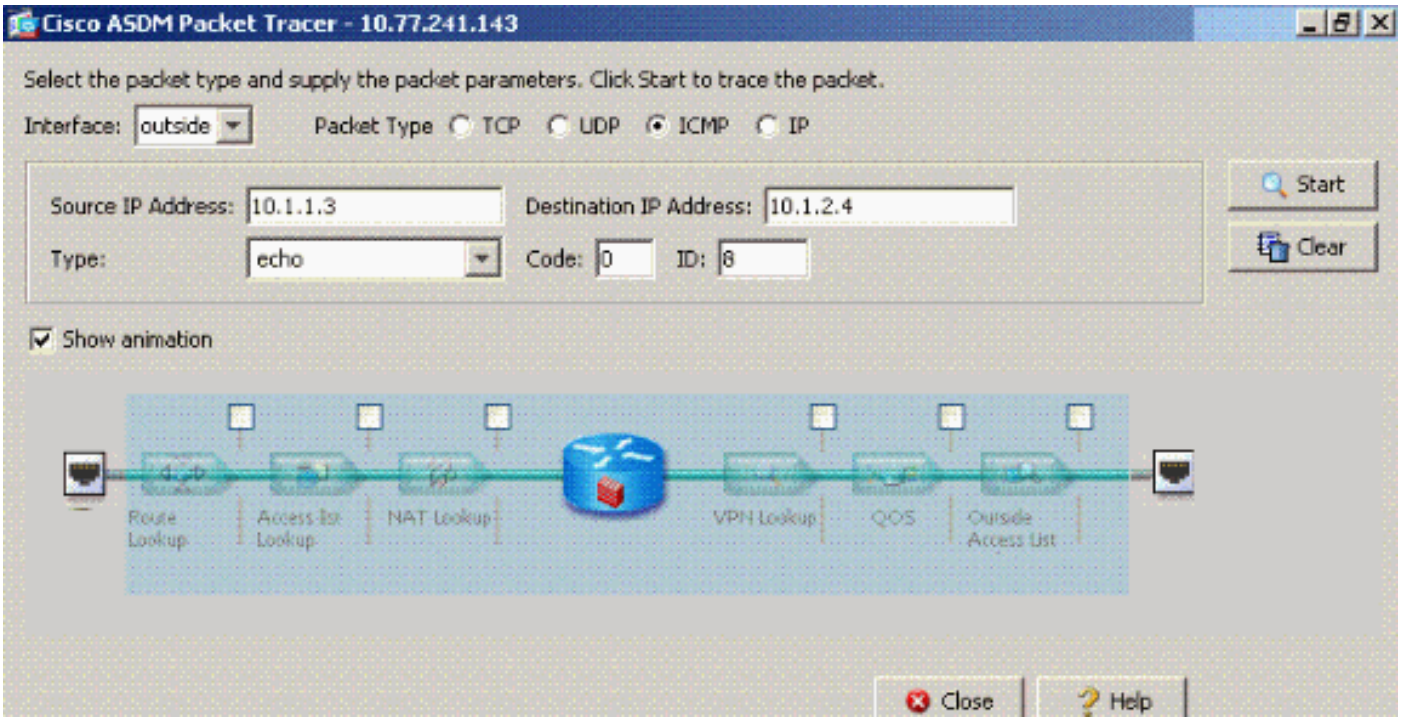
```
ciscoasa(config)#access-list outside_acl permit tcp any host 172.22.1.147 eq 80
ciscoasa(config)#access-list outside_acl deny ip any any
ciscoasa(config)#access-group outside_acl in interface outside
ciscoasa#packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1 detailed
!--- Output is suppressed.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

L'equivalente dei comandi CLI precedenti in ASDM è mostrato nelle seguenti figure:

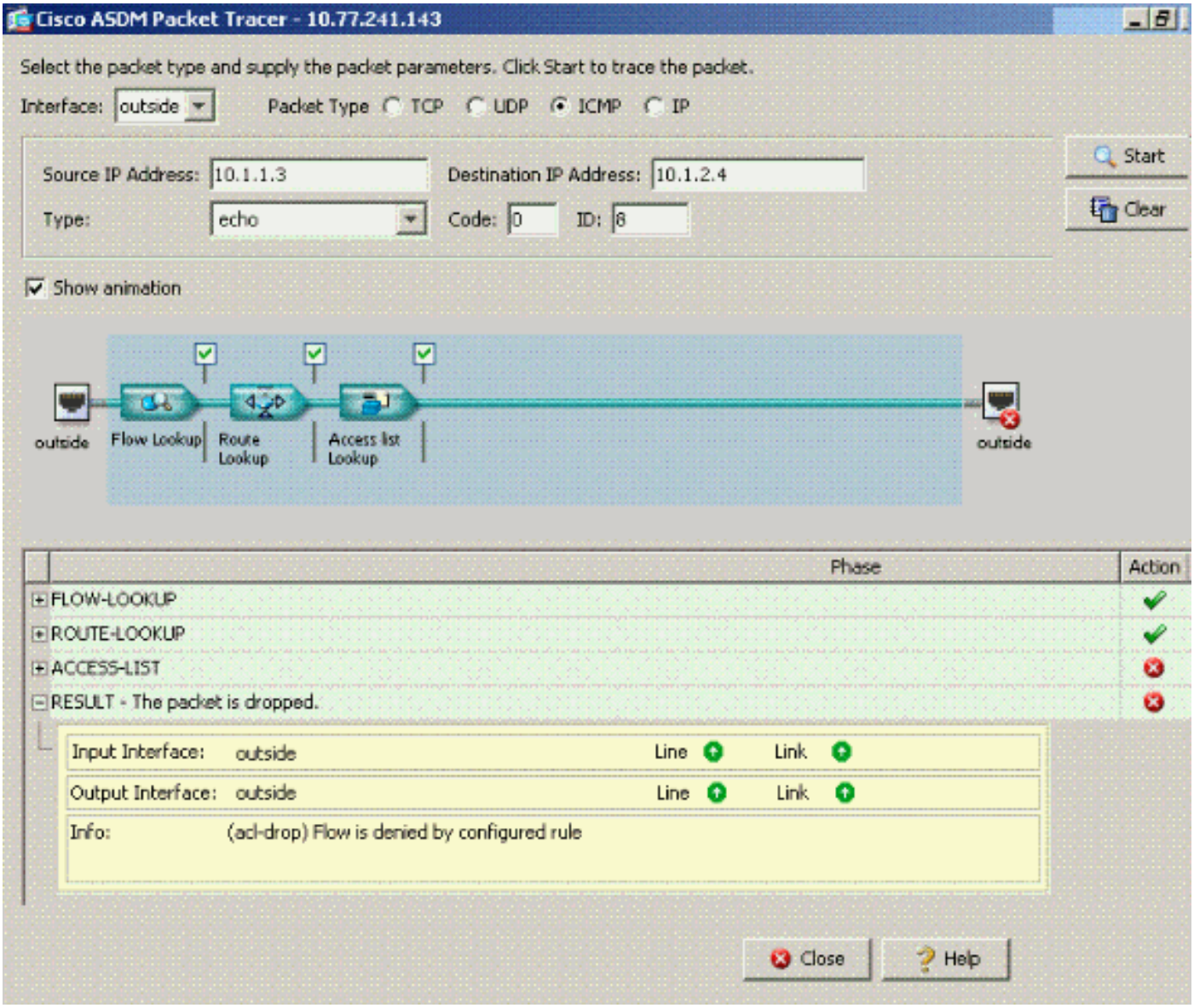
Passaggio 1:



Passaggio 2:



L'output packet-tracer con il comando **same-security-traffic** permette di **interfacciarsi** e il comando **access-list outside_acl extended deny ip any** è configurato per rifiutare i pacchetti.

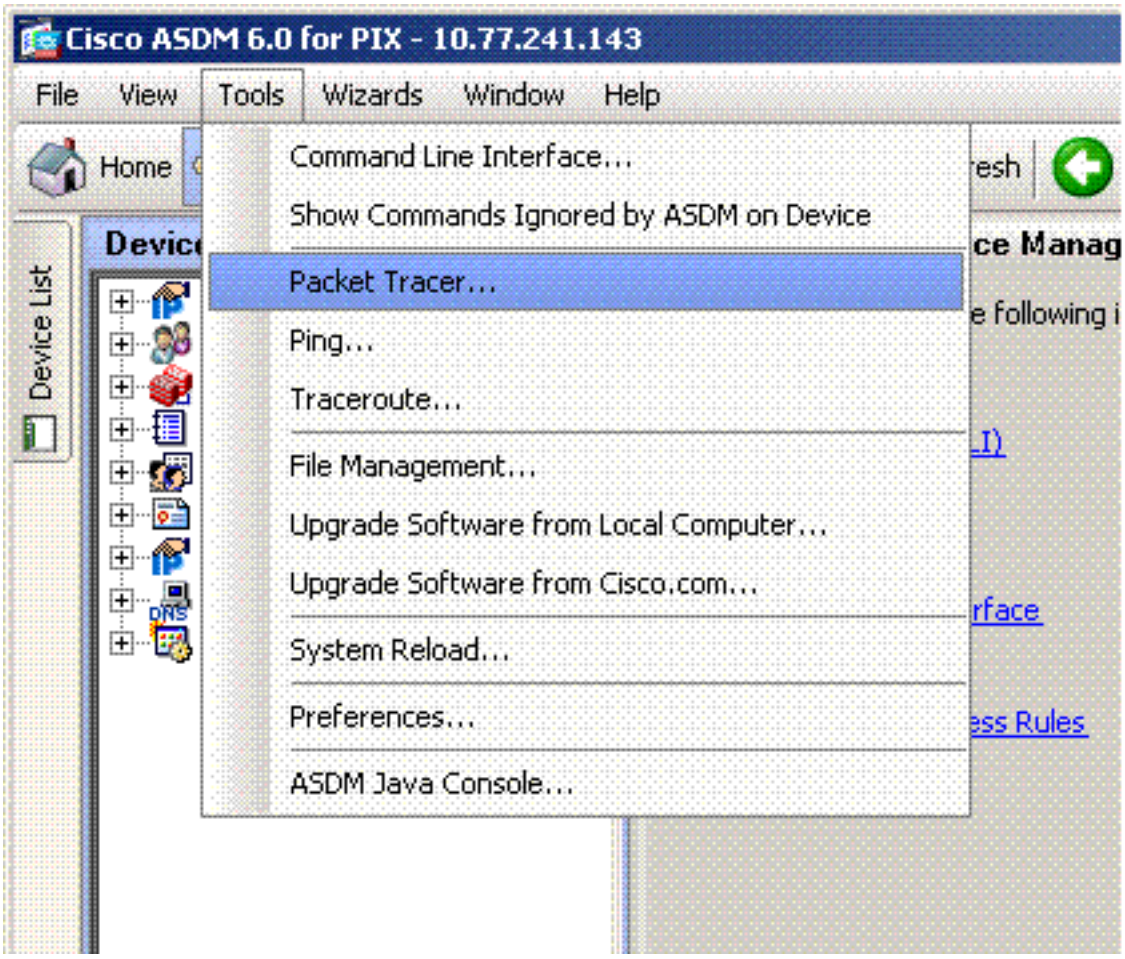


Se si desidera che le comunicazioni all'interno dell'interfaccia abbiano luogo su una determinata interfaccia e gli elenchi degli accessi siano applicati alla stessa interfaccia, le regole sugli elenchi degli accessi devono consentire il traffico all'interno dell'interfaccia. Se si usano gli esempi riportati in questa sezione, l'elenco degli accessi deve essere scritto come segue:

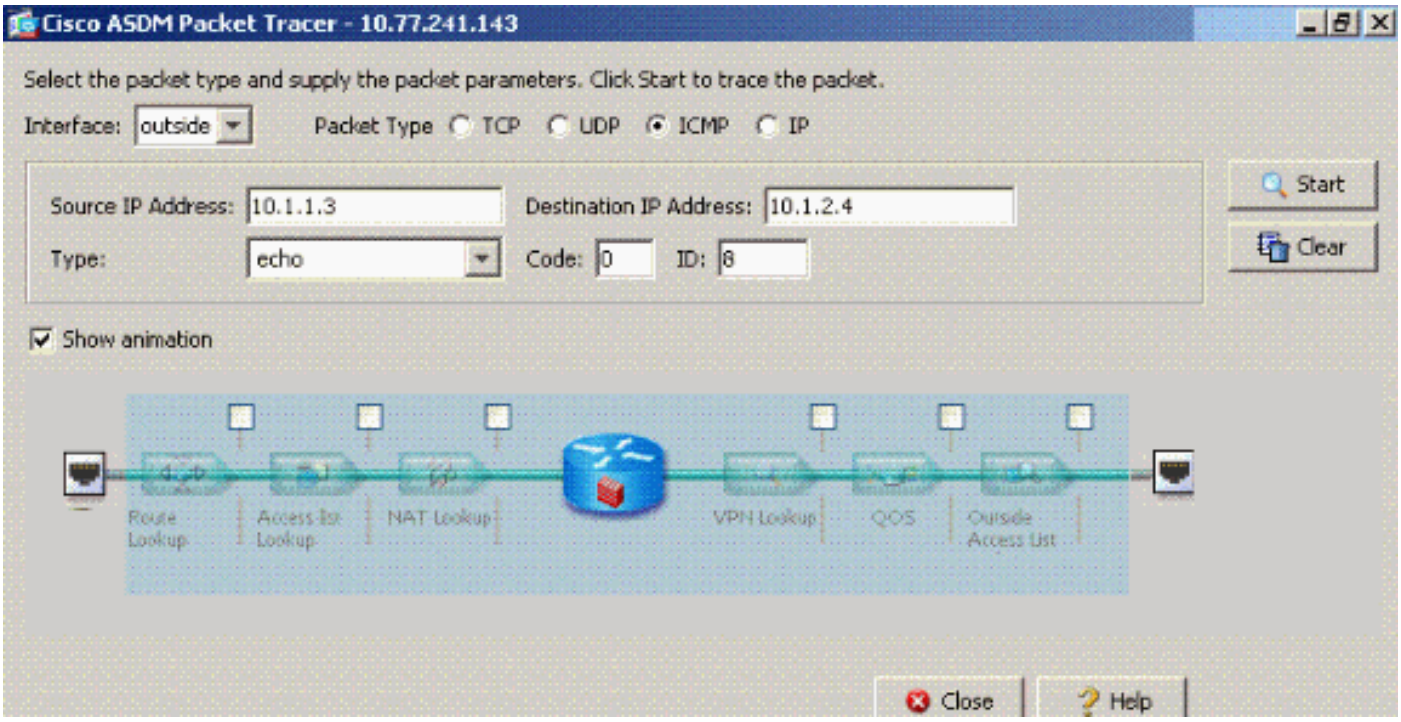
```
ciscoasa(config)#access-list outside_acl permit tcp any host 172.22.1.147 eq 80
ciscoasa(config)#access-list outside_acl permit ip 172.22.1.0 255.255.255.0 172.16.10.0
255.255.255.0
!--- 172.22.1.0 255.255.255.0 represents a locally !--- connected network on the ASA. !---
172.16.10.0 255.255.255.0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

L'equivalente dei comandi CLI precedenti in ASDM è mostrato nelle seguenti figure:

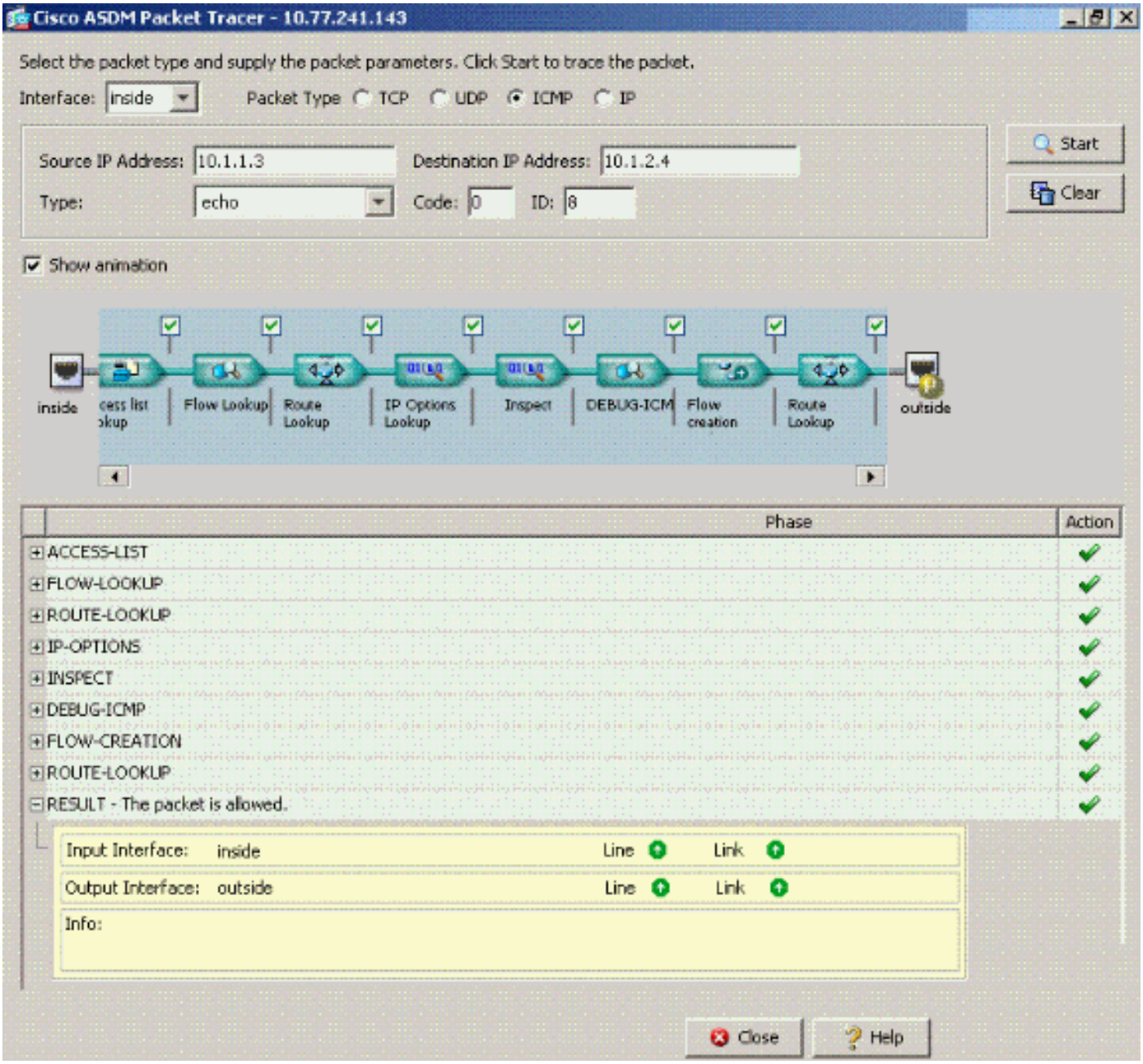
Passaggio 1:



Passaggio 2:



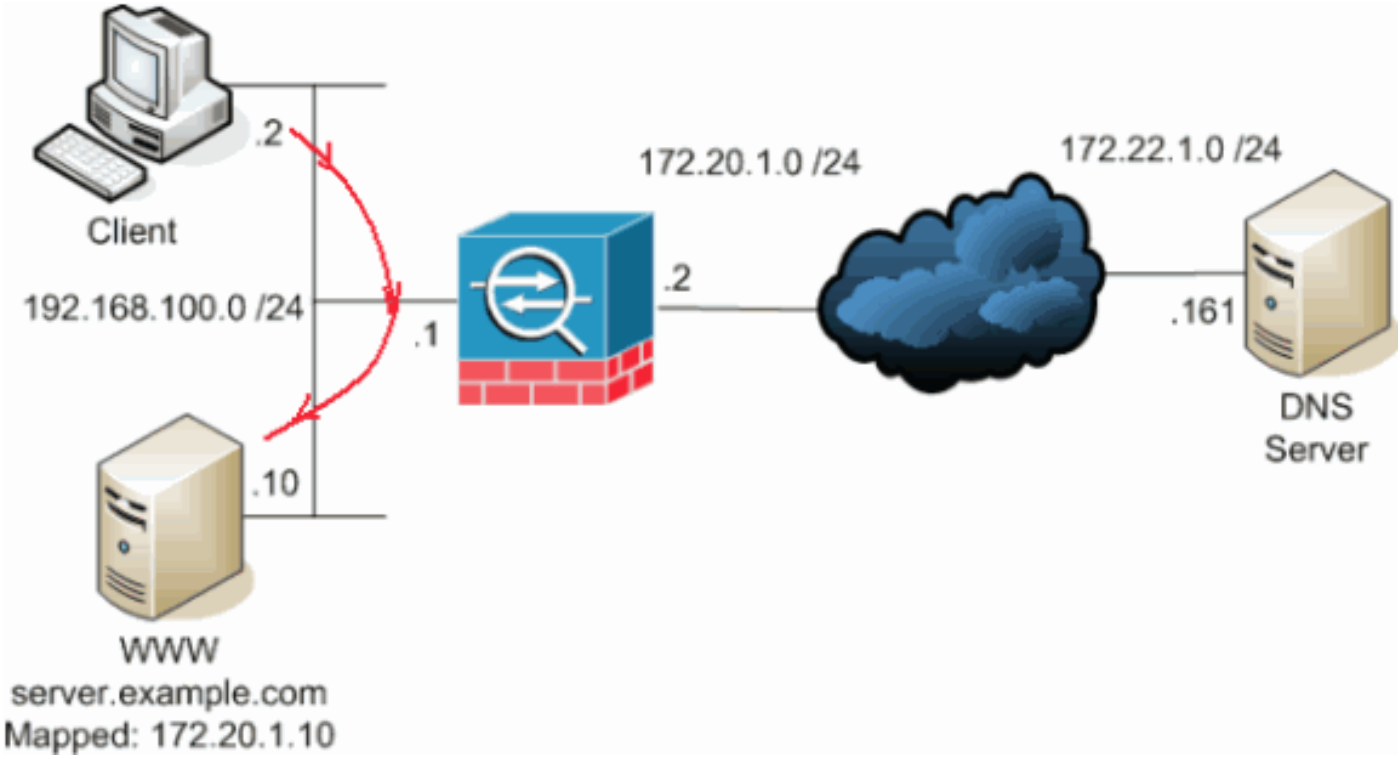
L'output del comando packet-tracer con lo **stesso traffico di sicurezza permette il** comando **intra-interfaccia** abilitato e il comando **access-list outside_acl extended deny ip any** configurato sulla stessa interfaccia, dove si desidera il traffico intra-interfaccia.



Per ulteriori informazioni sui comandi access-list-extended e **access-group**, consultare il documento.

Interfaccia intra-abilitata con statico e NAT

In questa sezione viene illustrato uno scenario in cui un utente interno tenta di accedere al server Web interno con il relativo indirizzo pubblico.



In questo caso, il client in 192.168.100.2 desidera utilizzare l'indirizzo pubblico del server WWW (ad esempio, 172.20.1.10). I servizi DNS per il client vengono forniti dal server DNS esterno all'indirizzo 172.22.1.161. Poiché il server DNS si trova in un'altra rete pubblica, non conosce l'indirizzo IP privato del server WWW. Il server DNS conosce invece l'indirizzo mappato del server WWW 172.20.1.10.

In questo caso, il traffico proveniente dall'interfaccia interna deve essere convertito e instradato nuovamente attraverso l'interfaccia interna per raggiungere il server WWW. Questo si chiama hairpinning. A tale scopo, è possibile utilizzare i seguenti comandi:

```
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
```

Per dettagli completi sulla configurazione e ulteriori informazioni sul hairpinning, fare riferimento a Hairpinning con comunicazione tra interfacce.

Access-List Forward Thinking

Non tutti i criteri di accesso firewall sono uguali. Alcuni criteri di accesso sono più specifici di altri. Nel caso in cui le comunicazioni tra interfacce siano abilitate e il firewall non abbia un elenco degli accessi applicato a tutte le interfacce, potrebbe essere utile aggiungere un elenco degli accessi nel momento in cui le comunicazioni tra interfacce sono abilitate. L'elenco degli accessi applicato deve consentire le comunicazioni all'interno dell'interfaccia e deve mantenere altri requisiti in materia di politica di accesso.

Questo esempio illustra questo punto. L'ASA connette una rete privata (interfaccia interna) a Internet (interfaccia esterna). All'interfaccia interna dell'ASA non è applicato un elenco degli accessi. Per impostazione predefinita, tutto il traffico IP è autorizzato dall'interno all'esterno. Il suggerimento è quello di aggiungere un elenco degli accessi simile al seguente output:

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

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

Questo gruppo di elenchi degli accessi continua a consentire tutto il traffico IP. La riga o le righe specifiche dell'elenco degli accessi per le comunicazioni intra-interfaccia ricordano agli amministratori che le comunicazioni intra-interfaccia devono essere consentite da un elenco degli accessi applicato.

Informazioni correlate

- Guida di riferimento ai comandi di Cisco Security Appliance, versione 7.2
- Messaggi del registro di sistema di Cisco Security Appliance, versione 7.2
- Software Cisco PIX Firewall
- ASA: Invio del traffico di rete dall'ASA all'esempio di configurazione di SSM AIP
- Cisco ASA serie 5500 Adaptive Security Appliance - Supporto dei prodotti
- Documentazione e supporto tecnico – Cisco Systems