# PIX/ASA 7.2(1) en later: Intra-interfacecommunicatie

## Inhoud



## Inleiding

Dit document helpt gemeenschappelijke problemen op te lossen die zich voordoen wanneer u communicatie tussen interfaces mogelijk maakt op een adaptieve security applicatie (ASA) of PIX die actief is in softwarerelease 7.2(1) en hoger. IOS-softwarerelease 7.2(1)omvat de mogelijkheid om duidelijke tekstgegevens naar binnen of naar buiten dezelfde interface te sturen. Typ de **opdracht** voor **de intra-interface-toegangsvergunning** voor **hetzelfde verkeer** om deze functie in te schakelen. In dit document wordt ervan uitgegaan dat de netwerkbeheerder deze optie heeft ingeschakeld of dat hij van plan is dit in de toekomst te doen. Configuratie- en probleemoplossing worden geleverd met behulp van de opdrachtregel-interface (CLI).

**Opmerking:** dit document is gericht op duidelijke (niet-gecodeerde) gegevens die de ASA aankomen en verlaten. Versleutelde gegevens worden niet besproken.

Raadpleeg PIX/ASA en VPN-client voor PIX-interface-communicatie op ASA/PIX voor IPsec-configuratie op een voorbeeld van Stick Configuration.

Raadpleeg ASA 7.2(2) om communicatie tussen interfaces op ASA for SSL-configuratie mogelijk te maken: SSL VPN Client (SVC) voor Public Internet VPN op een tick Configuration Voorbeeld.

## Voorwaarden

## Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Toegangslijsten
- Routing
- Geavanceerde inspectie en preventie-security servicesmodule (AIP-SSM) voor inbraakpreventiesysteem (IPS) — kennis van deze module is alleen nodig als de module geïnstalleerd en gebruiksklaar is.
- IPS softwarerelease 5.x—kennis van IPS-software is niet vereist als AIP-SSM niet in gebruik is.

## Gebruikte componenten

- ASA 5510 7.2(1) en later
- AIP-SSM-10 dat IPS-software 5.1.1 exploiteert

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

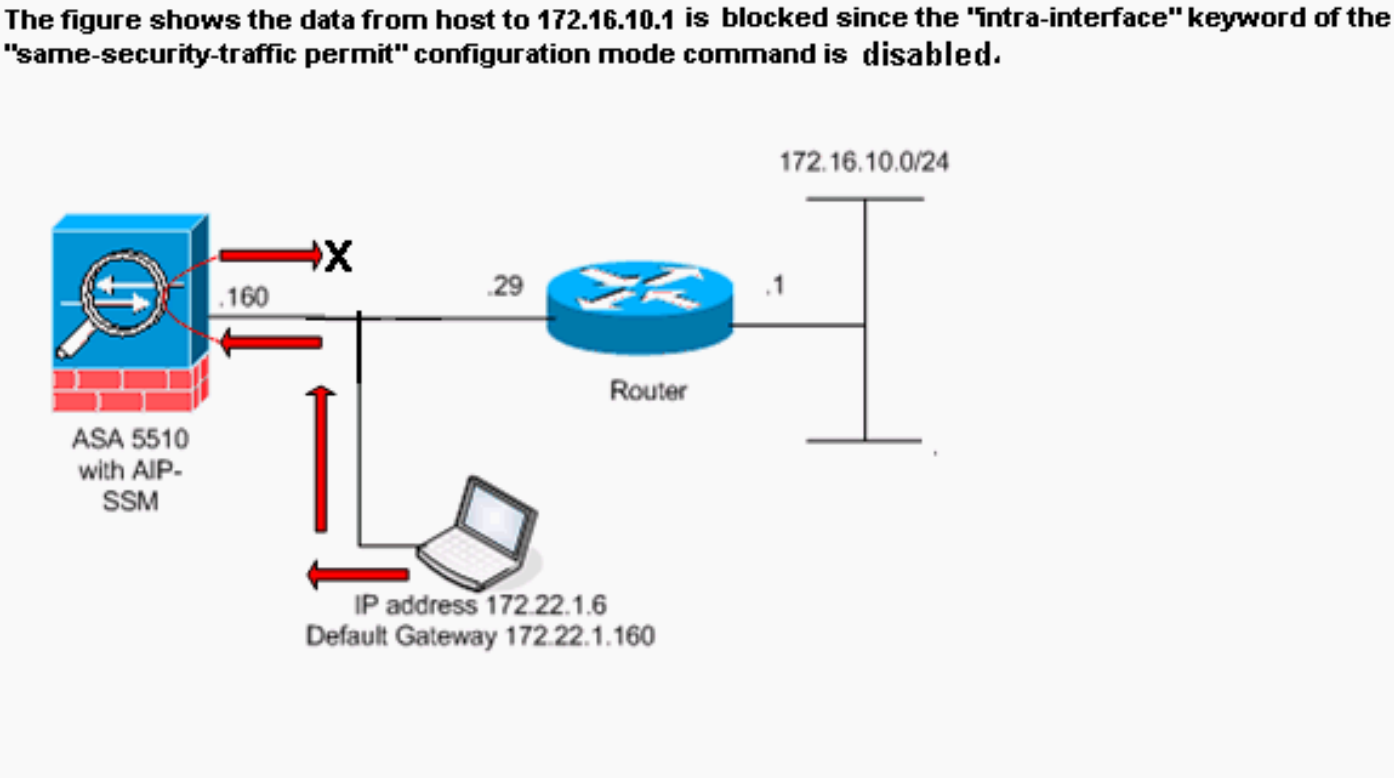
## Verwante producten

Deze configuratie kan ook worden gebruikt met Cisco 500 Series PIX, die versie 7.2(1) en hoger uitvoeren.

## Conventies

Raadpleeg Cisco Technical Tips Convention voor informatie over documentconventies.

# Achtergrondinformatie




**Opmerking:** de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Ze zijn RFC 1918 adressen die in een labomgeving gebruikt zijn.

Deze tabel toont de ASA startconfiguratie:

**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:
```

# Probleemoplossing

Deze secties illustreren verschillende configuratiescenario's, verwante syslg berichten, en pakkettracer output met betrekking tot intra-interface communicatie.

## Intra-interface communicatie niet ingeschakeld

In de ASA configuratie, host 172.22.1.6 pogingen om host 172.16.10.1 te pingelen. Host 172.22.1.6 stuurt een ICMP-echo-verzoekpakket naar de standaardgateway (ASA). Intra-interface communicatie is niet op de ASA ingeschakeld. De ASA laat het echo-verzoekpakket vallen. De test ping mislukt. ASA wordt gebruikt om het probleem op te lossen.

Dit voorbeeld toont de uitvoer van syslogberichten en een pakkettracer:

- Dit is het syslogbericht dat aan de buffer is ingelogd:

```
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)
```

- Dit is de uitvoer van de pakkettracer:

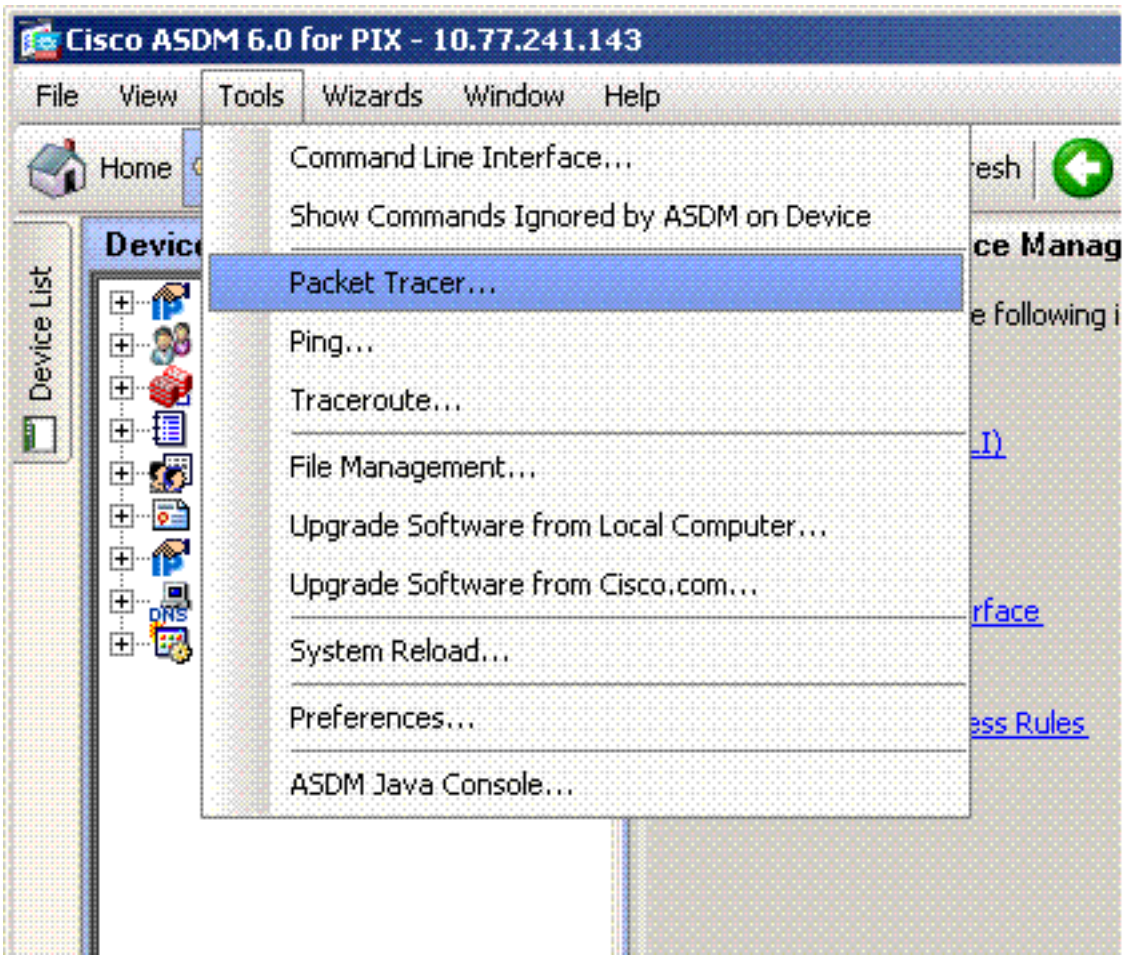
```
ciscoasa(config)#packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1 detailed
Phase: 1
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found no matching flow, creating a new flow

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**

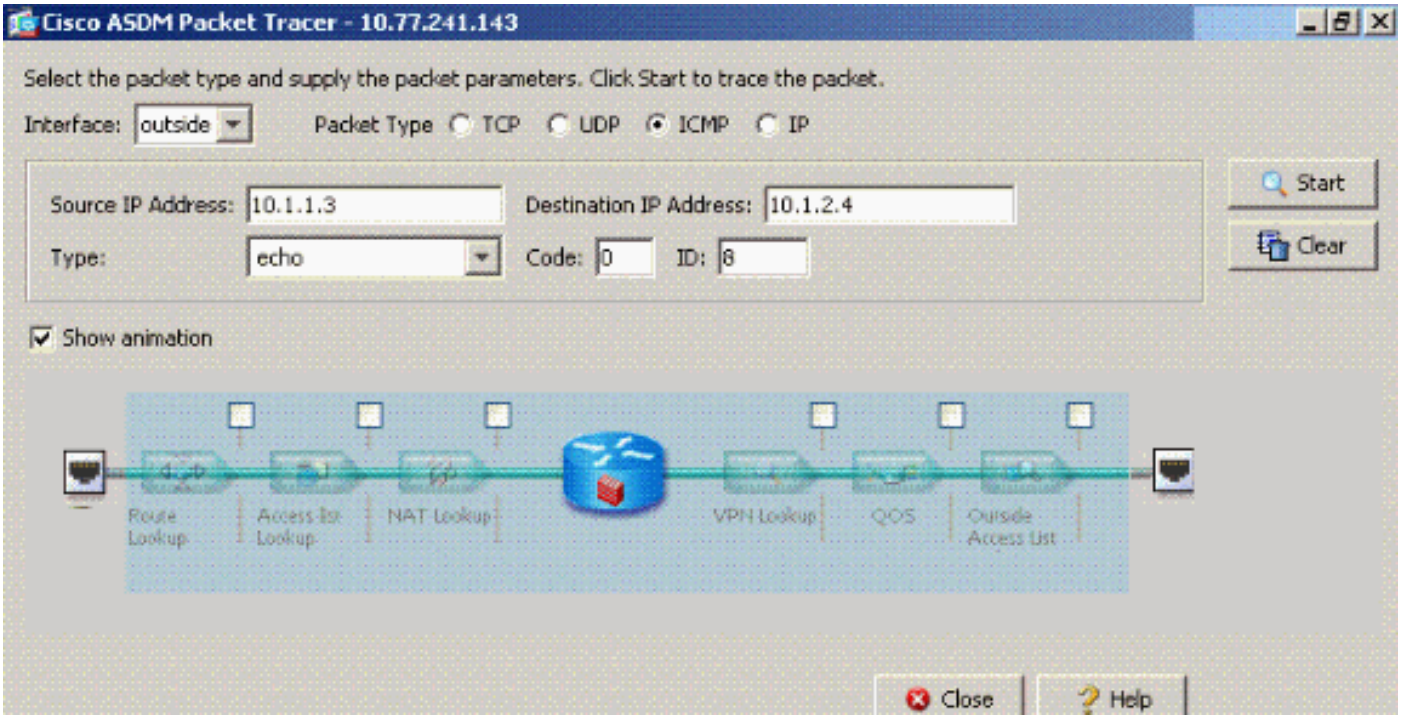
*!--- Implicit rule refers to configuration rules not configured !--- by the user. By default, intra-interface communication is not permitted. !--- In this example, the user has not enabled intra-interface communications !--- and therefore the traffic is implicitly denied.* Additional Information: Forward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

Het equivalent van de CLI-opdrachten in ASDM wordt in deze cijfers weergegeven:

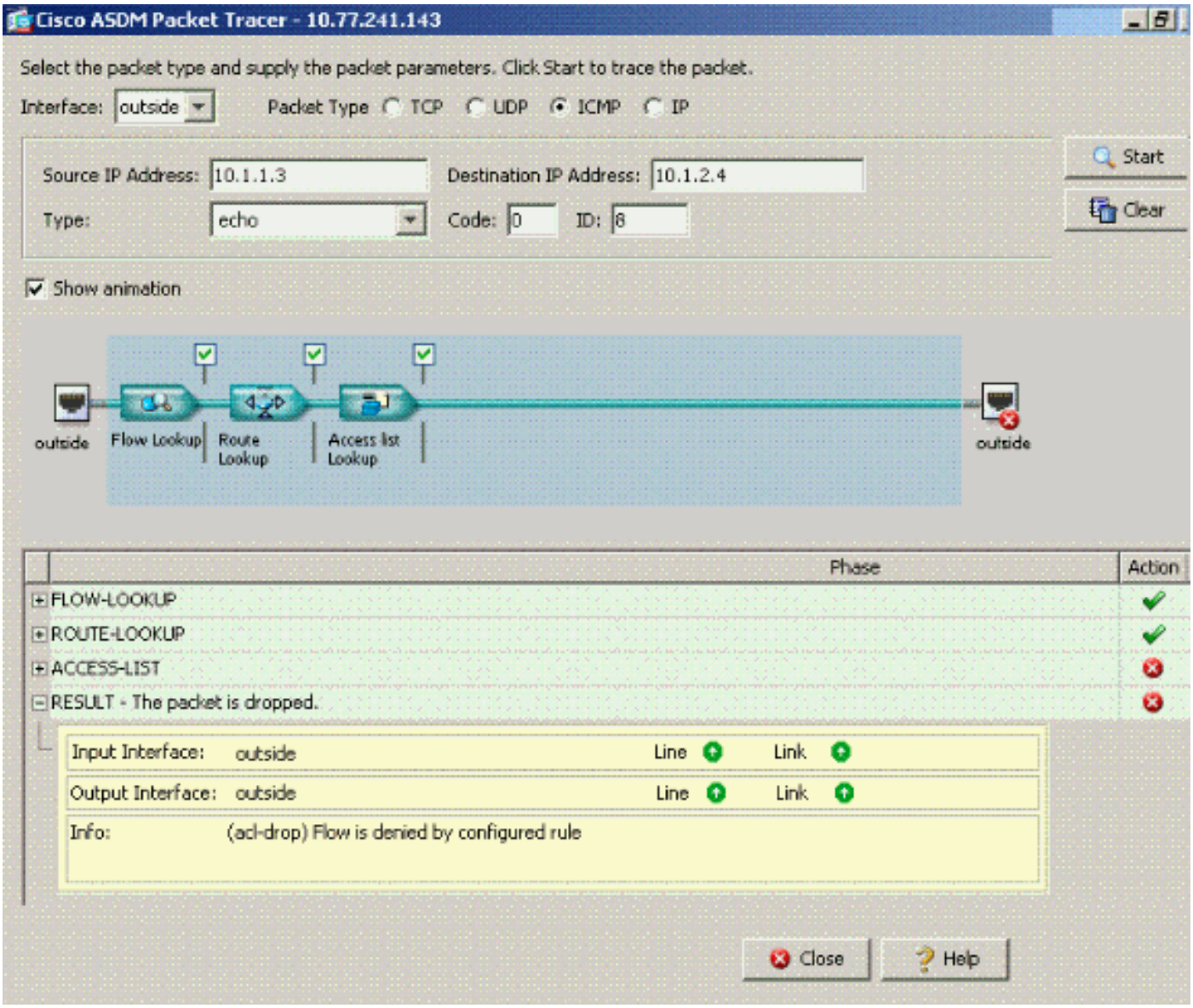
Stap 1:




Stap 2:




De uitvoer van de pakkettracer met de **optie-security-verkeer maakt de** opdracht **intra-interface** uit.



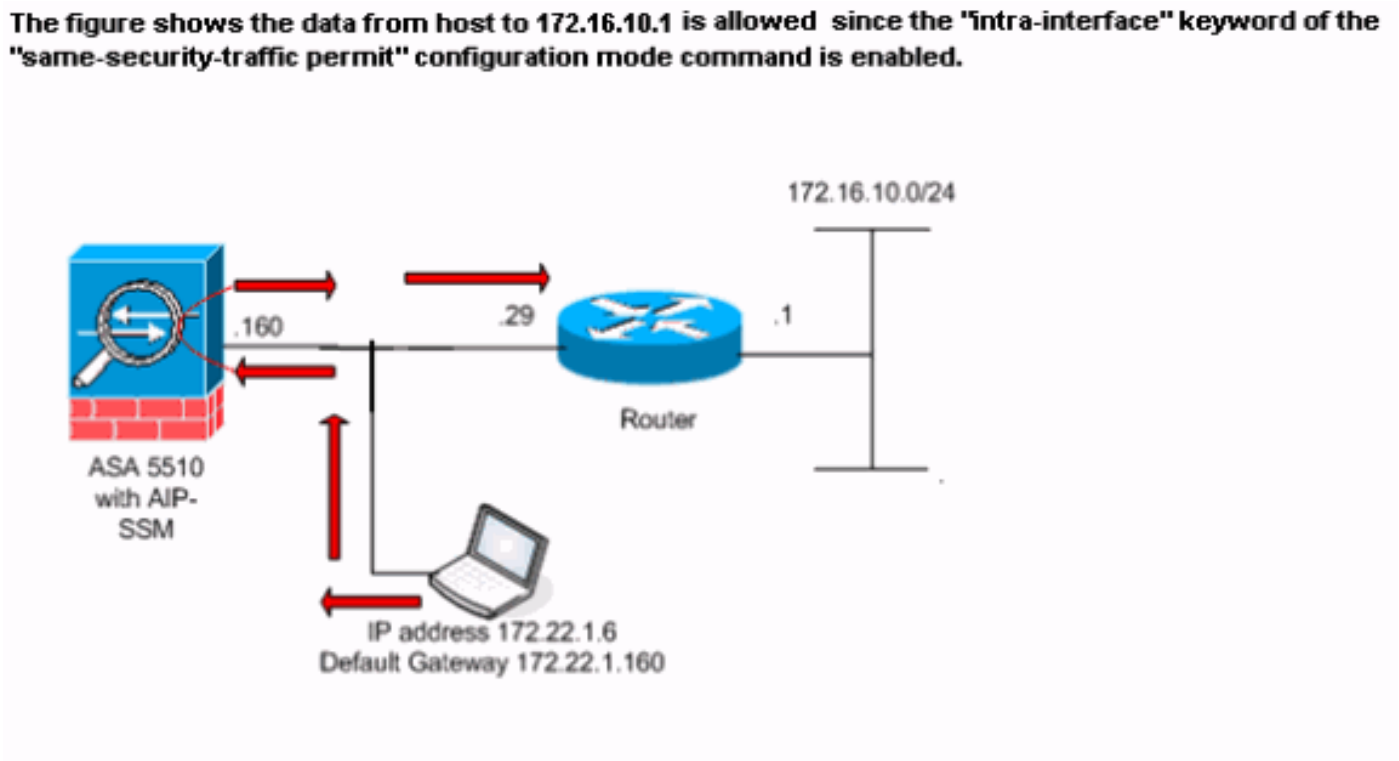
De pakkettracer uitvoer `daalt...De impliciete regel` suggereert dat een standaard configuratie instelling het verkeer blokkeert. De beheerder moet de actieve configuratie controleren om te verzekeren dat de intra-interface communicatie ingeschakeld is. In dit geval heeft de ASA configuratie interface-communicatie nodig om ingeschakeld te kunnen worden (**verbinding tussen hetzelfde beveiligingsverkeer en een andere 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 communicatie ingeschakeld

Intra-interface communicatie is nu ingeschakeld. De opdracht **voor** de **intra-interface-toegangsrechten voor hetzelfde beveiligingsverkeer** wordt aan de vorige configuratie toegevoegd. Host 172.22.1.6 probeert host 172.16.10.1 te pingelen. Host 172.22.1.6 stuurt een ICMP-echo-verzoekpakket naar de standaardgateway (ASA). Host 172.22.1.6 registreert succesvolle antwoorden van 172.16.10.1. De ASA geeft het ICMP-verkeer met succes door.

**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.**



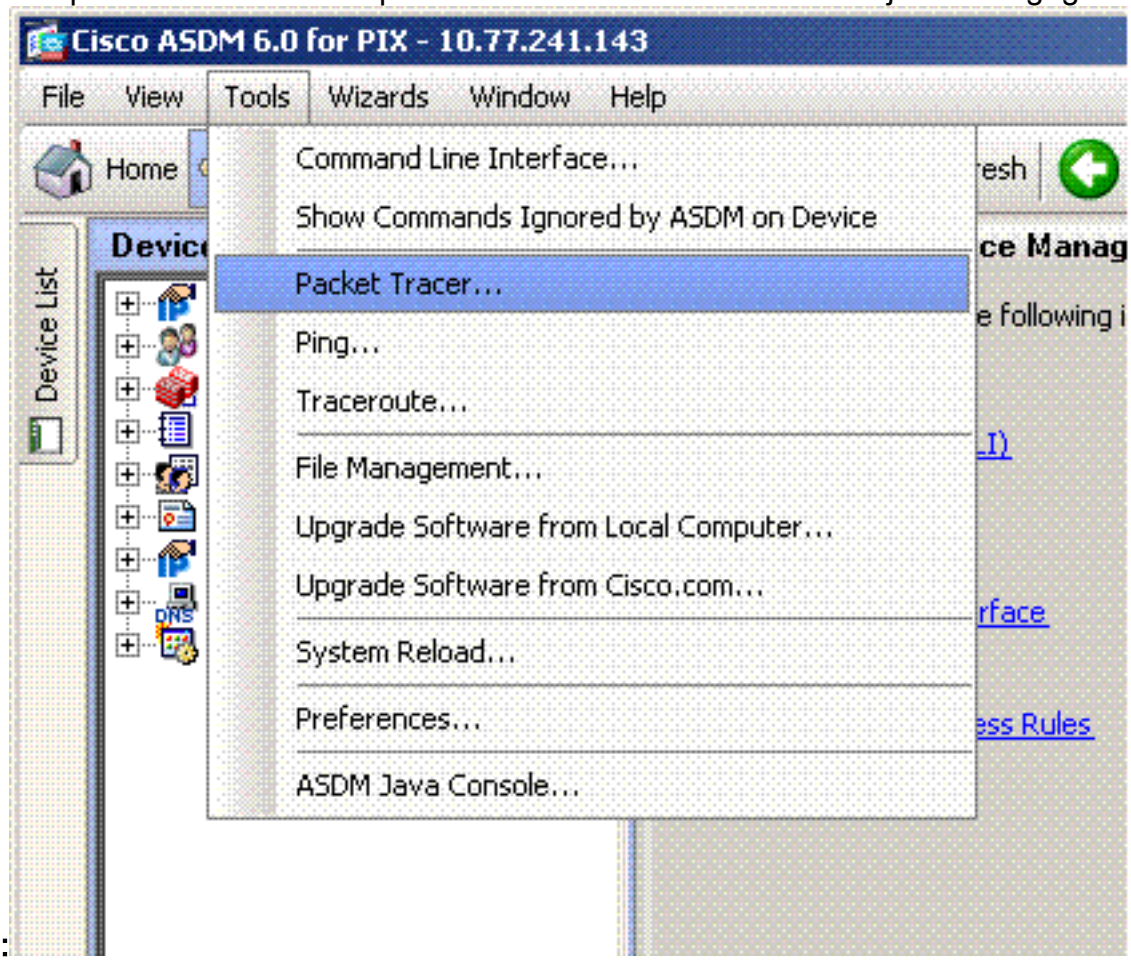

Deze voorbeelden tonen het ASA syslog bericht en de pakkettracer output:

- Dit zijn de syslogberichten die aan de buffer zijn aangemeld:
  ```
  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
  ```
- Dit is de uitvoer van de pakkettracer:

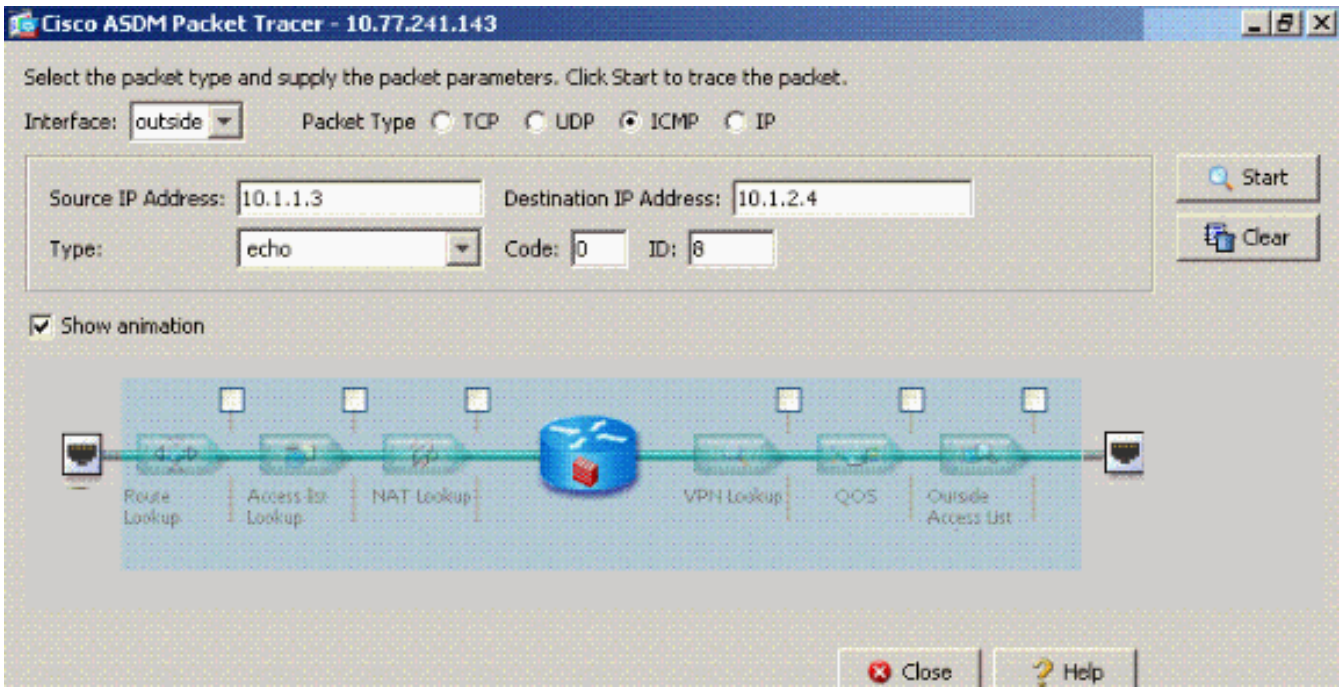
```
ciscoasa(config)#packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1

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
```

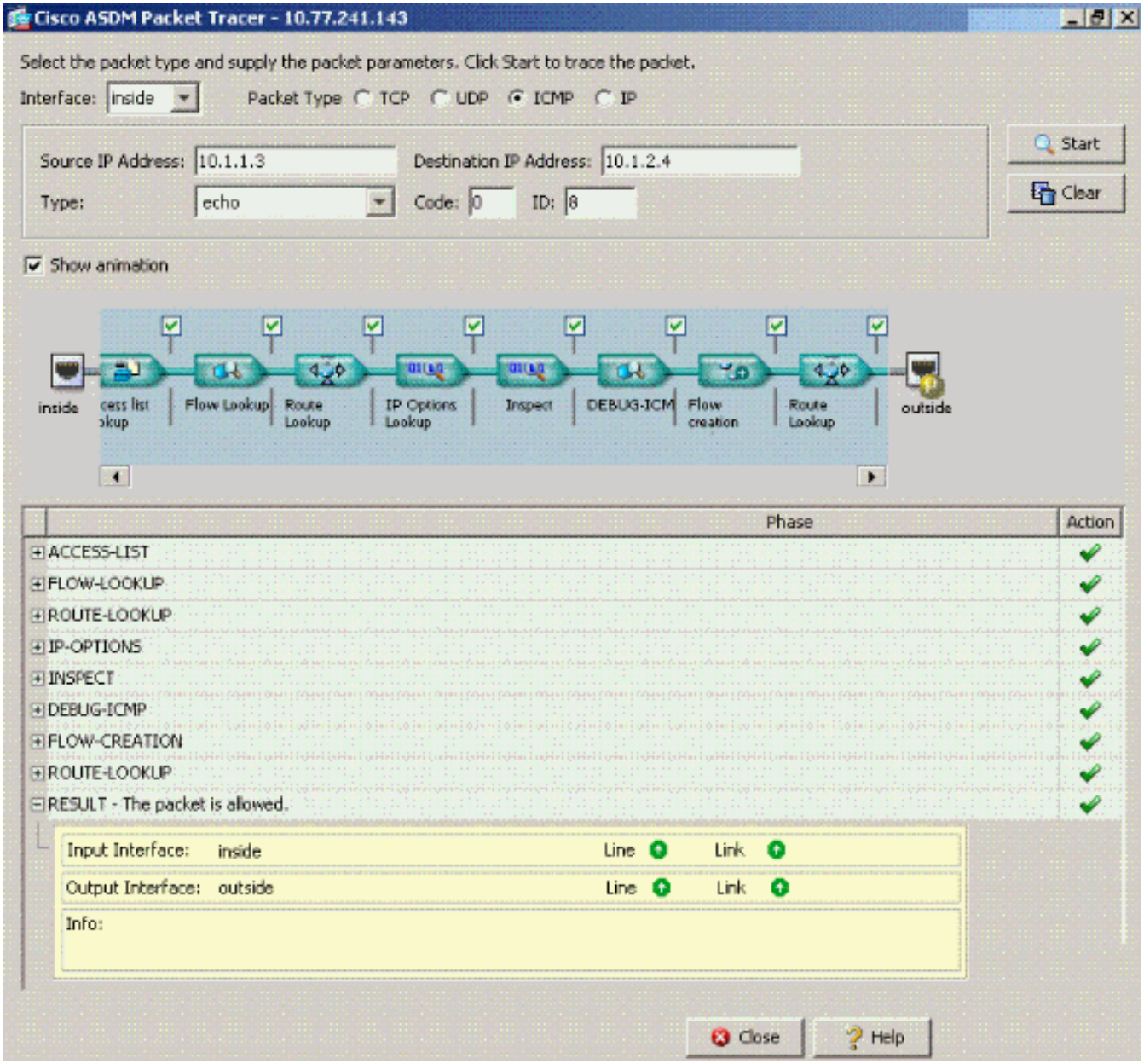
Het equivalent van de CLI-opdrachten in ASDM wordt in deze cijfers weergegeven:**Stap 1:**




**Stap 2:**




De [pakkettracer](#) uitvoer met de **optie-security-verkeer** intra-interface-opdracht ingeschakeld.




**Opmerking:** er is geen toegangslijst van toepassing op de externe interface. In de voorbeeldconfiguratie, wordt de externe interface toegewezen veiligheidsniveau 0. Standaard staat de firewall geen verkeer toe van een lage veiligheidsinterface naar een hoge veiligheidsinterface. Dit kan beheerders ertoe aanzetten om te geloven dat het intra-interface verkeer niet op de buitenkant (lage veiligheid) interface zonder toestemming van een access-list wordt toegestaan. Echter, het zelfde interfaceverkeer gaat vrij wanneer geen toegangslijst wordt toegepast op de interface.

## Intra-interface ingeschakeld en verkeer doorgeleid naar AIP-SSM voor inspectie

Intra-interfaceverkeer kan voor inspectie worden doorgegeven naar het AIP-SSM. In deze sectie wordt ervan uitgegaan dat de beheerder de ASA heeft ingesteld om verkeer naar AIP-SSM door te sturen en dat de beheerder weet hoe hij IPS 5.x software moet configureren.

Op dit punt bevat de ASA-configuratie de vorige voorbeeldconfiguratie, worden intra-interface-communicatie ingeschakeld en wordt al het (enige) verkeer naar AIP-SSM doorgestuurd. IPS signatuur 2004 wordt gewijzigd om het verkeer van echo-verzoeken te laten vallen. Host 172.22.1.6 probeert host 172.16.10.1 te pingelen. Host 172.22.1.6 stuurt een ICMP-echo-verzoekpakket naar de standaardgateway (ASA). ASA stuurt het echo-verzoekpakket naar het

AIP-SSM voor inspectie door. Het AIP-SSM daalt het gegevenspakket per de IPS configuratie.

Deze voorbeelden tonen het ASA syslogbericht en de pakkettracer uitvoer:

- Dit is het syslogbericht dat aan de buffer is ingelogd:

```
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.
```

- Dit is de uitvoer van de pakkettracer:

```
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.
```

Het is belangrijk om op te merken dat de beheerders zoveel mogelijk probleemoplossingsgereedschappen moeten gebruiken wanneer zij een probleem onderzoeken. Dit voorbeeld toont hoe twee verschillende gereedschappen voor het oplossen van problemen verschillende illustraties kunnen schilderen. Beide tools vertellen samen een compleet verhaal. Het ASA-configuratiebeleid maakt het verkeer mogelijk maar de IPS-configuratie niet.

## Intra-interface-enabled- en toegangslijsten die op een interface van toepassing zijn

In deze sectie worden de oorspronkelijke voorbeeldconfiguratie in dit document gebruikt, worden intra-interface-communicatie ingeschakeld en wordt een toegangslijst toegepast op de geteste interface. Deze lijnen worden aan de configuratie toegevoegd. De toegangslijst is bedoeld als een simpele weergave van wat er in een productiefirewall opgeslagen kan worden.

```
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 probeert host 172.16.10.1 te pingelen. Host 172.22.1.6 stuurt een ICMP-echo-verzoekpakket naar de standaardgateway (ASA). ASA laat het echo-verzoekpakket vallen volgens de toegangslijst regels. De host 172.22.1.6 test ping mislukt.

Deze voorbeelden tonen ASA syslogbericht en pakkettracer uitvoer:

- Dit is het syslogbericht dat aan de buffer is ingelogd:
  ```
  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]
  ```
- Dit is de uitvoer van de pakkettracer:
  ```
  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
```

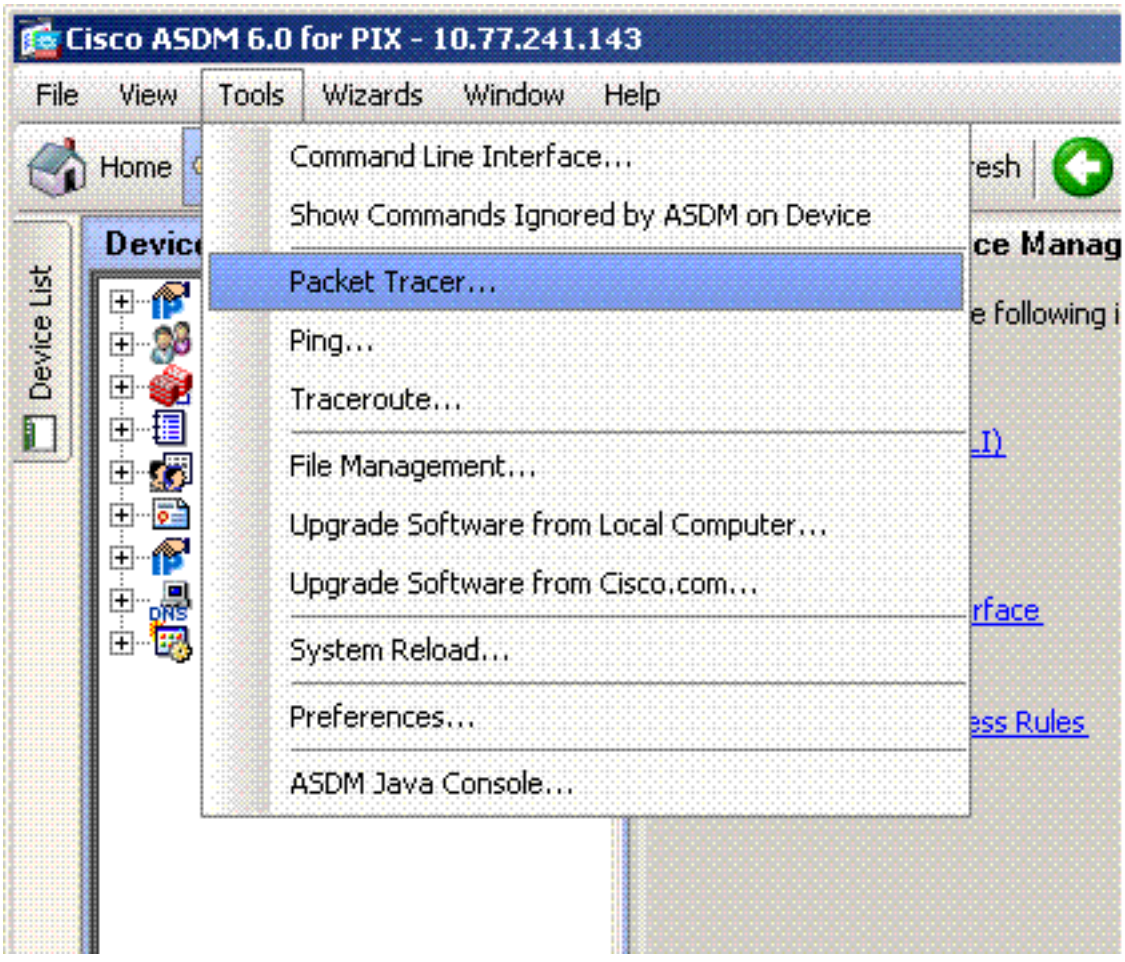
Raadpleeg pakkettracer voor meer informatie over de opdracht **pakkettracer**.

**Opmerking:** Voor het geval dat de toegangslijst die op de interface van toepassing is een ontkenningsverklaring bevat, verandert de uitvoer van de pakkettracer. Bijvoorbeeld:

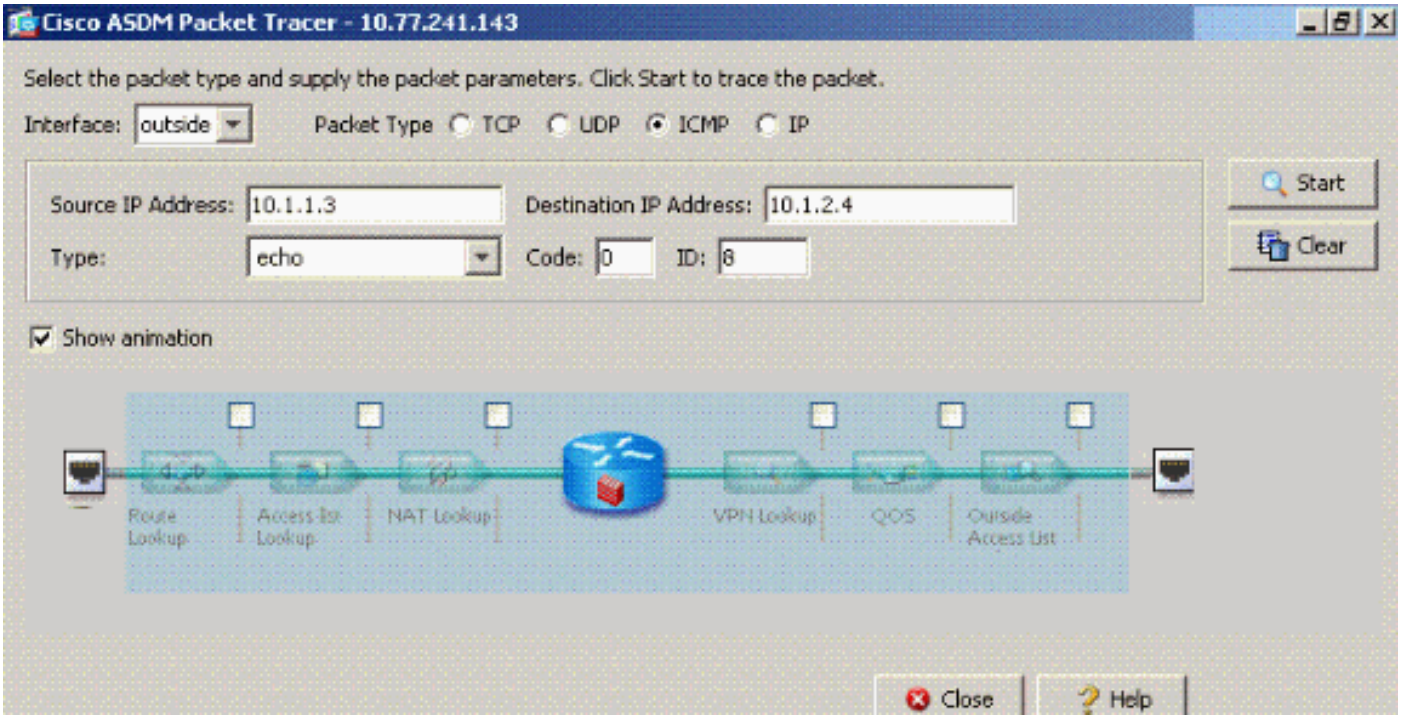
```
ciscoasa(config)#access-list outside_acl permit tcp any host 172.22.1.147 eq 80
ciscoasa(config)#access-list outside_acl deny ip any any
ciscoasa(config)#access-group outside_acl in interface outside
ciscoasa#packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1 detailed
!--- Output is suppressed.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

Het equivalent van de bovenstaande CLI-opdrachten in ASDM wordt in deze cijfers weergegeven:

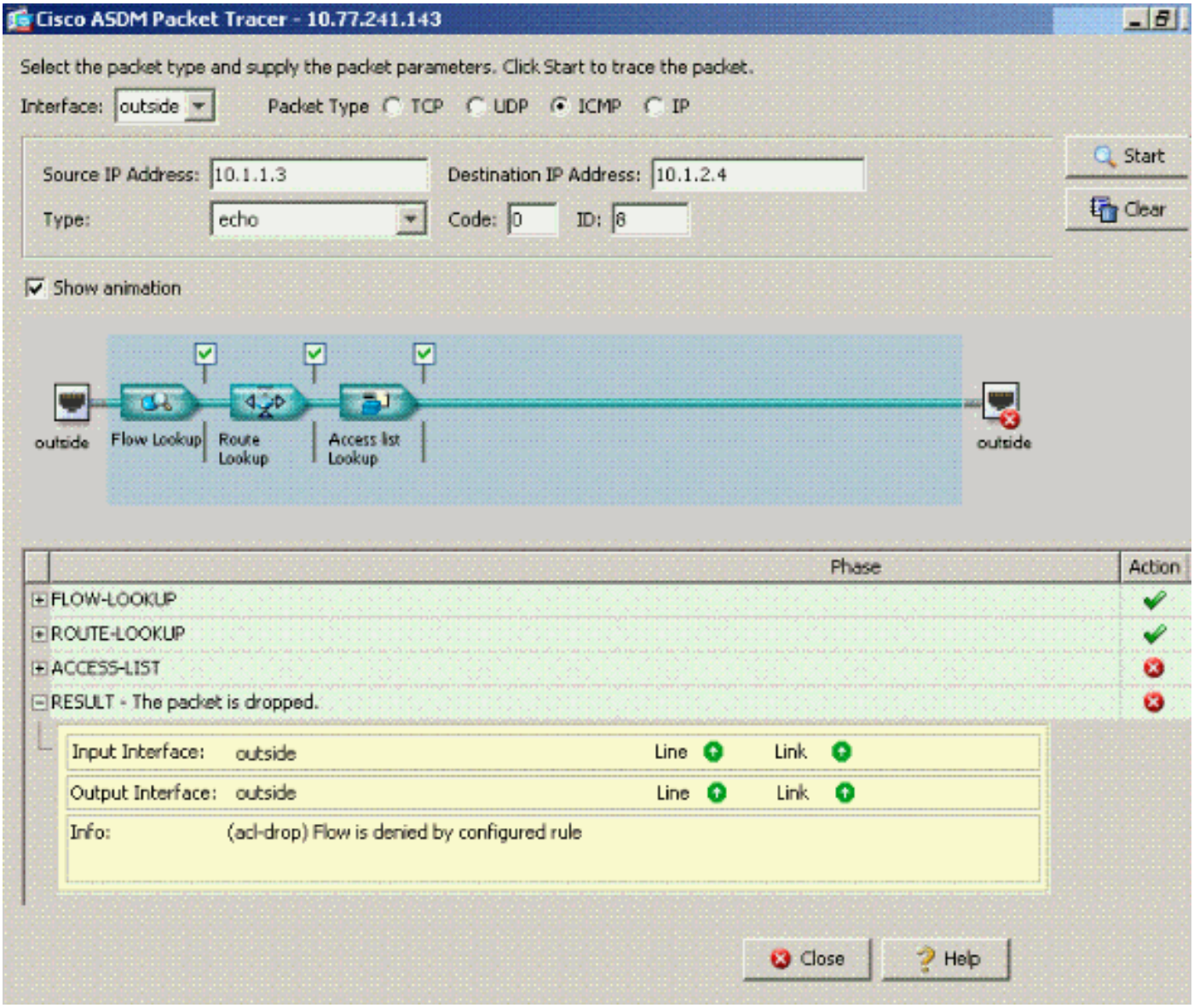
**Stap 1:**




**Stap 2:**




De Packet-tracer uitvoer met de **optie-security-traffic** file **licentie intra-interface** opdracht ingeschakeld en de **toegangslijst buiten_acl uitgebreid ontken elke** opdracht **die** is ingesteld om pakketten te ontkennen.

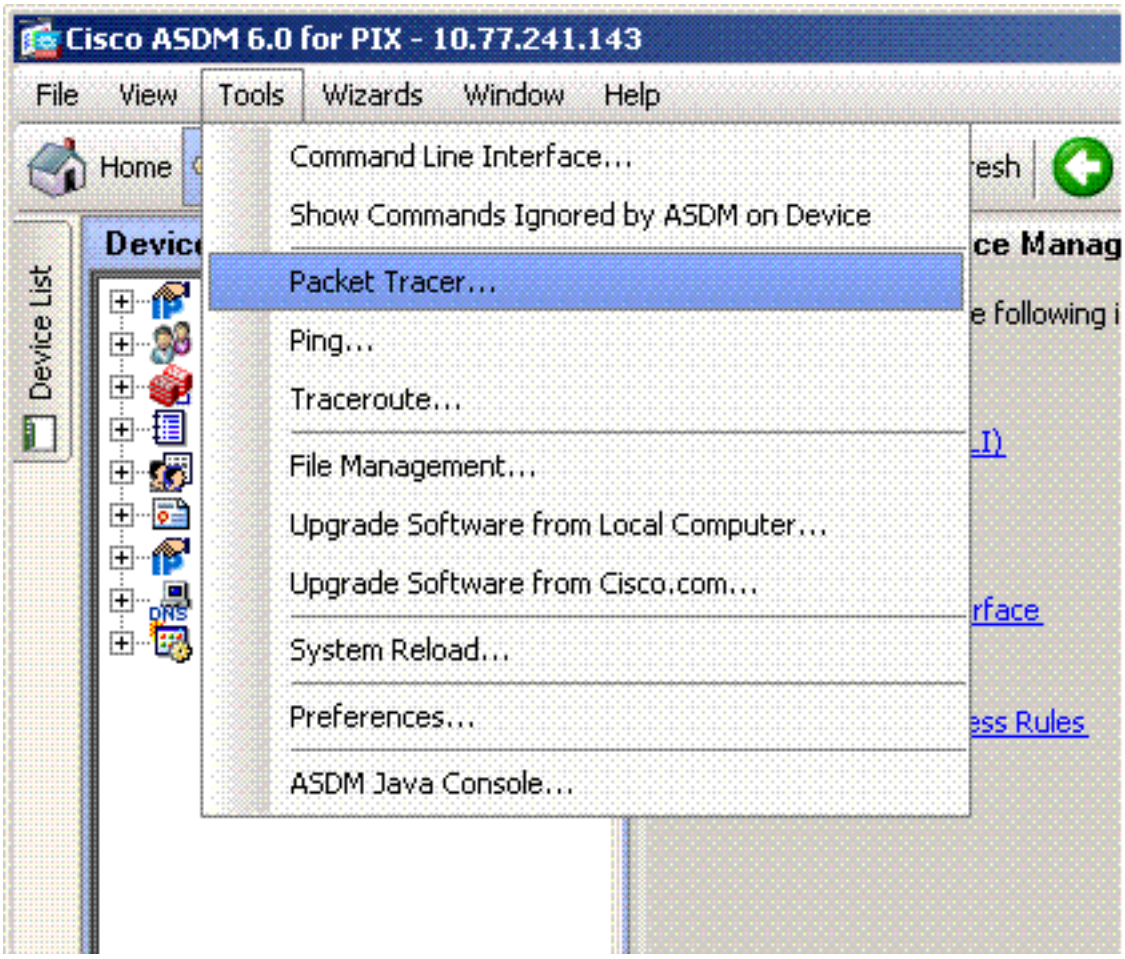



Als communicatie tussen interfaces op een bepaalde interface wordt gewenst en toegangslijsten op dezelfde interface worden toegepast, moeten de toegangslijsten het verkeer binnen de interface toestaan. Met behulp van de voorbeelden in dit deel moet de toegangslijst worden geschreven als:

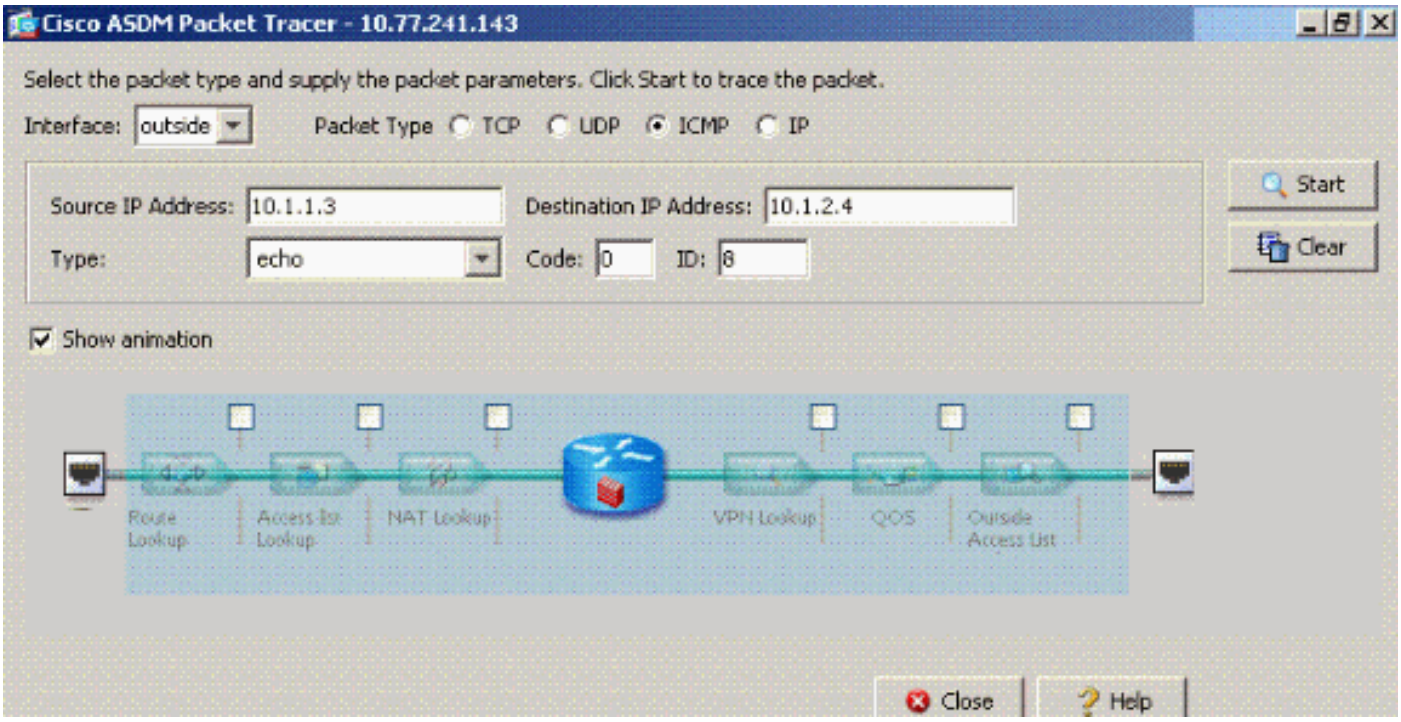
```
ciscoasa(config)#access-list outside_acl permit tcp any host 172.22.1.147 eq 80
ciscoasa(config)#access-list outside_acl permit ip 172.22.1.0 255.255.255.0 172.16.10.0
255.255.255.0
!--- 172.22.1.0 255.255.255.0 represents a locally !--- connected network on the ASA. !---
172.16.10.0 255.255.255.0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

Het equivalent van de bovenstaande CLI-opdrachten in ASDM wordt in deze cijfers weergegeven:

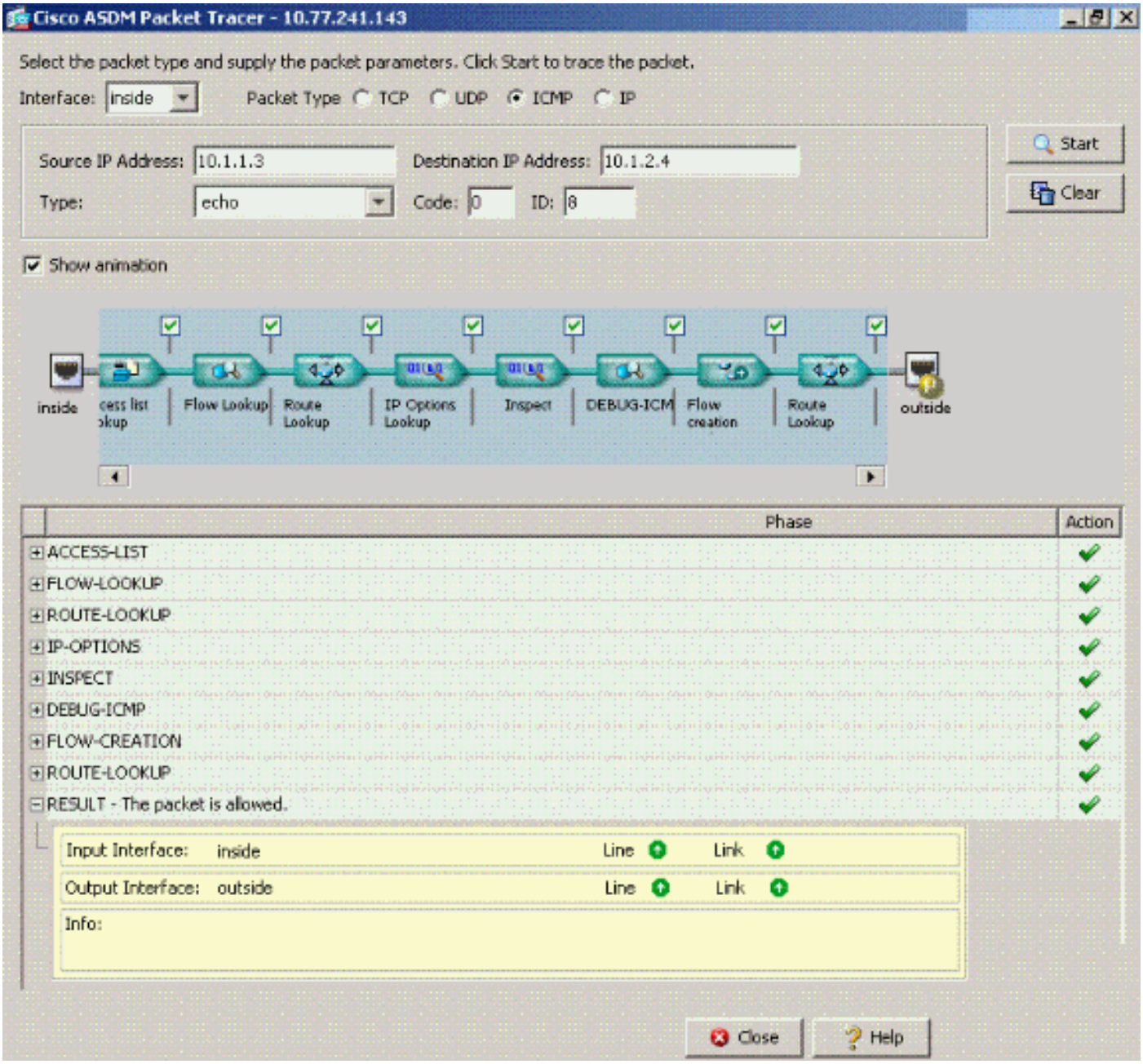
**Stap 1:**




Stap 2:



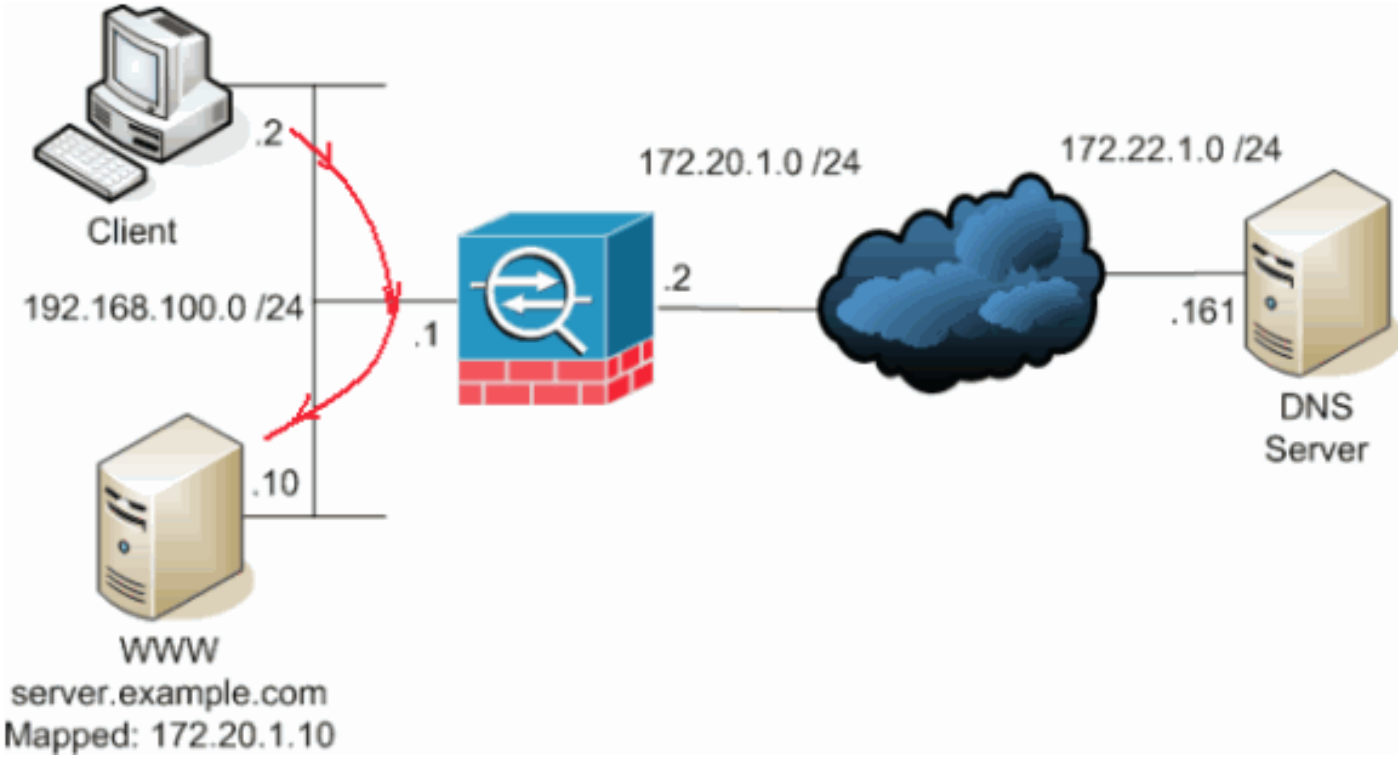

De Packet-tracer uitvoer met de **optie-security-verkeer maakt de** opdracht **intra-interface** mogelijk en de **toegangslijst externe_acl** ontkent **elke** opdracht **die** op dezelfde interface is ingesteld waar intra-interfaceverkeer is gewenst.




Raadpleeg de uitgebreid toegangslijst en toegangsgroep voor meer informatie over de opdrachten **toegangslijst** en **toegangsgroep**.

## Intra-interface ingeschakeld met statische en NAT

In deze sectie wordt een scenario uitgelegd waarin een binnengebruiker probeert om toegang te krijgen tot de interne webserver met het openbare adres.




In dit geval wil de klant op 192.168.100.2 het openbare adres van de WW server gebruiken (bijvoorbeeld 172.20.1.10). De DNS-services voor de client worden geleverd door de externe DNS-server op 172.22.1.161. Omdat de DNS-server zich op een ander openbaar netwerk bevindt, kent de server niet het privéIP-adres van de WW-server. In plaats daarvan weet de DNS-server het WW server-in kaart gebrachte adres van 172.20.1.10.

Hier moet dit verkeer van de binneninterface worden vertaald en opnieuw verstuurd door de binneninterface om de WW server te bereiken. Dit heet kapsel. U kunt deze opdrachten als volgt uitvoeren:

```
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
```

Voor volledige configuratiegegevens en meer informatie over het haarspelden kunt u Hairling met Intra-interface communicatie raadplegen.

## Voorwaarts denken op toegangslijst

Niet alle firewalltoegangsbeleid is hetzelfde. Sommige toegangsbeleid is specifieker dan andere. In de gebeurtenis zijn de intra-interface mededelingen toegelaten en de firewall heeft geen toegang-lijst van toepassing op alle interfaces, het kan de moeite waard zijn om een toegang-lijst toe te voegen op het moment dat de intra-interface communicatie wordt toegelaten. De toegepaste toegangslijst moet communicatie tussen interfaces mogelijk maken en andere eisen van het toegangsbeleid handhaven.

Dit voorbeeld illustreert dit punt. ASA sluit een privaat netwerk (binneninterface) aan op het internet (externe interface). ASA interne interface heeft geen toegangslijst. Standaard is al het IP-verkeer van binnenuit naar buiten toegestaan. De suggestie is om een toegangslijst toe te voegen die er ongeveer als deze output uitziet:

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

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

Deze reeks toegangslijsten blijft al IP-verkeer toestaan. De specifieke toegangslijst(s) voor communicatie tussen interfaces herinnert beheerders eraan dat communicatie tussen interfaces moet worden toegestaan door een toegepaste toegangslijst.

## Gerelateerde informatie

- Cisco Security Appliance Opdracht Ref, versie 7.2
- Cisco Security applicatie System Log Messaging, versie 7.2
- Cisco PIX-firewallsoftware
- ASA: Netwerkverkeer vanuit de ASA naar het AIP SSM-configuratievoorbeeld verzenden
- Cisco ASA 5500 Series productondersteuning voor adaptieve security applicaties
- Technische ondersteuning en documentatie – Cisco Systems