PIX/ASA 7.2(1) e posterior: Comunicações Intra-Interface

Contents

Introduction

Este documento ajuda a resolver problemas comuns que ocorrem ao habilitar as comunicações entre interfaces em um Mecanismo de Segurança Adaptável (ASA) ou PIX que opera na versão de software 7.2(1) e mais recente. A versão 7.2(1) do software inclui a capacidade de rotear dados de texto não criptografado para dentro e para fora da mesma interface. Para habilitar este recurso, execute o comando **same-security-traffic permit intra-interface**. Este documento pressupõe que o administrador de rede ativou este recurso ou planeja ativá-lo no futuro. A configuração e a solução de problemas são fornecidas usando a interface de linha de comando (CLI).

Nota:Este documento concentra-se em dados não criptografados que chegam e saem do ASA. Os dados criptografados não são discutidos.

Para habilitar a comunicação entre interfaces na configuração do ASA/PIX para IPsec, consulte Exemplo de Configuração de PIX/ASA e VPN Client para VPN de Internet Pública em um Stick.

Para habilitar a comunicação entre interfaces no ASA para configuração SSL, consulte o ASA 7.2(2): Exemplo de configuração de SSL VPN Client (SVC) para VPN de Internet Pública em um Stick.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Listas de acesso
- Roteamento
- Sistema de prevenção de intrusão (IPS - Intrusion Prevention Prevention System) AIP-SSM (Advanced Inspection and Prevention-Security Services Module)—O conhecimento deste módulo só é necessário se ele estiver instalado e operacional.
- Software IPS versão 5.x—O conhecimento do software IPS não é necessário se o AIP-SSM não estiver em uso.

Componentes Utilizados

- ASA 5510 7.2(1) e posterior
- AIP-SSM-10 que opera o software IPS 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.

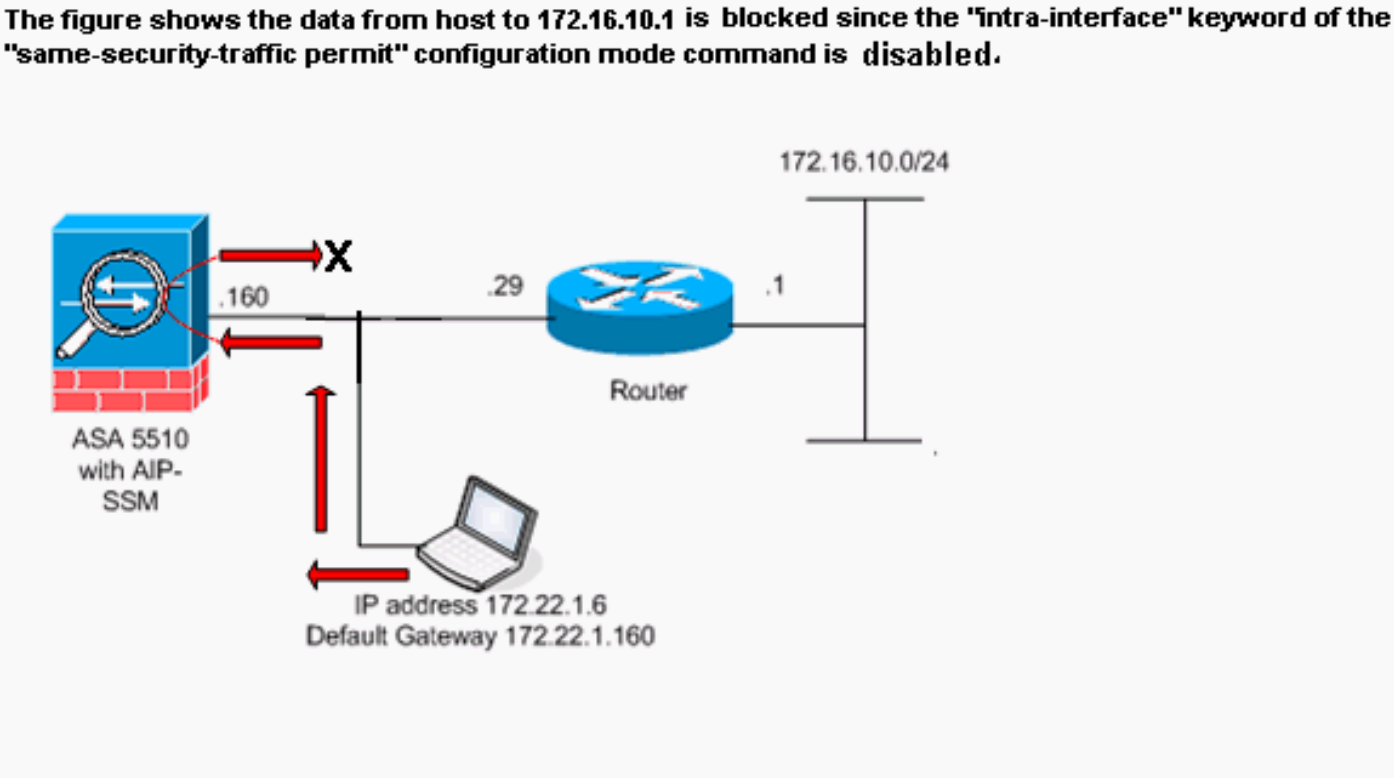
Produtos Relacionados

Essa configuração também pode ser usada com o Cisco 500 Series PIX que executa a versão 7.2(1) e posterior.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter informações sobre convenções de documentos.

Informações de Apoio



Observação: os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São endereços RFC 1918 que foram usados em um ambiente de laboratório.

Esta tabela mostra a configuração inicial do 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:
```

Troubleshooting

Essas seções ilustram vários cenários de configuração, mensagens de syslog relacionadas e saídas de packet-tracer em relação às comunicações entre interfaces.

Comunicação IntraInterface Não Habilitada

Na configuração do ASA, o host 172.22.1.6 tenta fazer ping no host 172.16.10.1. O host 172.22.1.6 envia um pacote de solicitação de eco ICMP para o gateway padrão (ASA). As comunicações intrainterface não foram habilitadas no ASA. O ASA descarta o pacote de solicitação de eco. O ping de teste falha. O ASA é usado para solucionar o problema.

Este exemplo mostra a saída de mensagens syslog e um packet-tracer:

- Esta é a mensagem de syslog registrada no 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)
```

- Esta é a saída do packet-tracer:

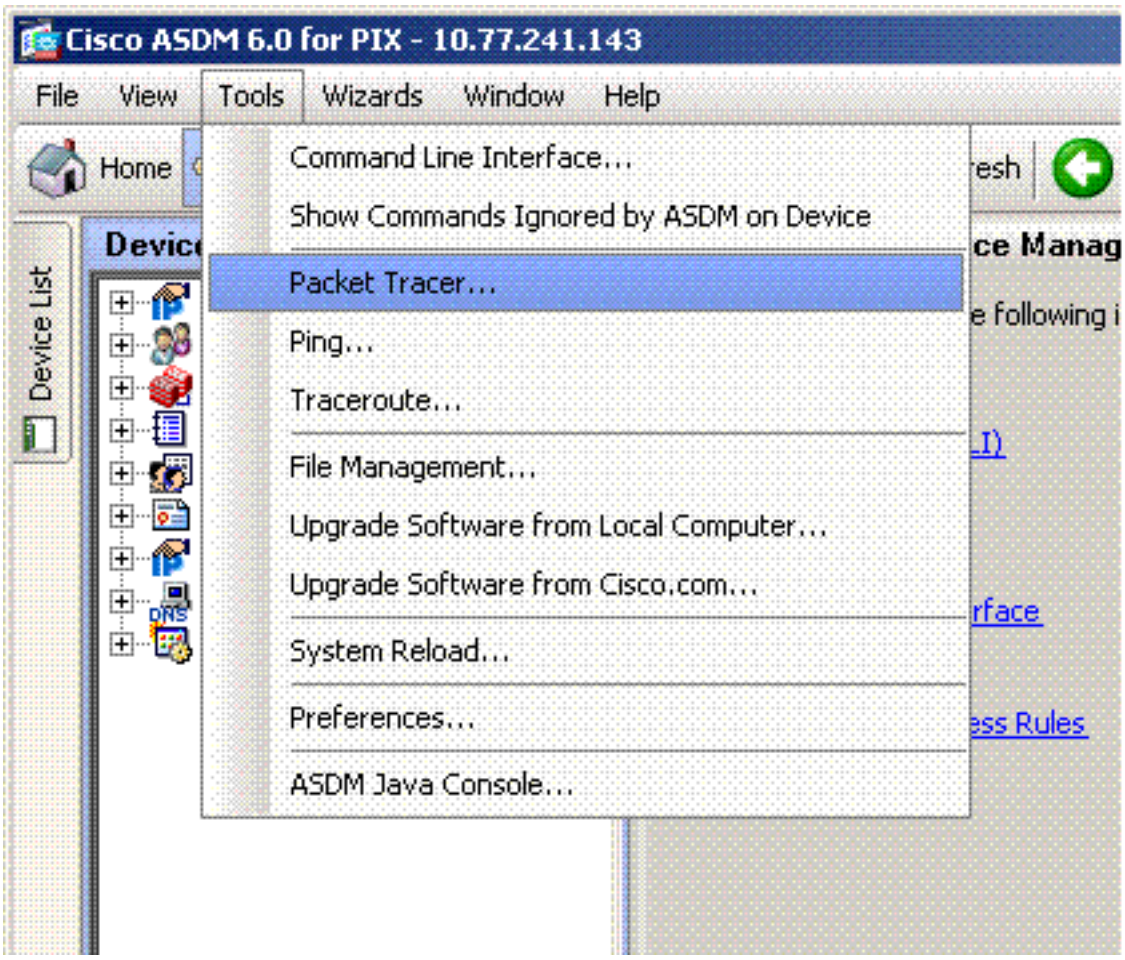
```
ciscoasa(config)#packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1 detailed
Phase: 1
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found no matching flow, creating a new flow

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

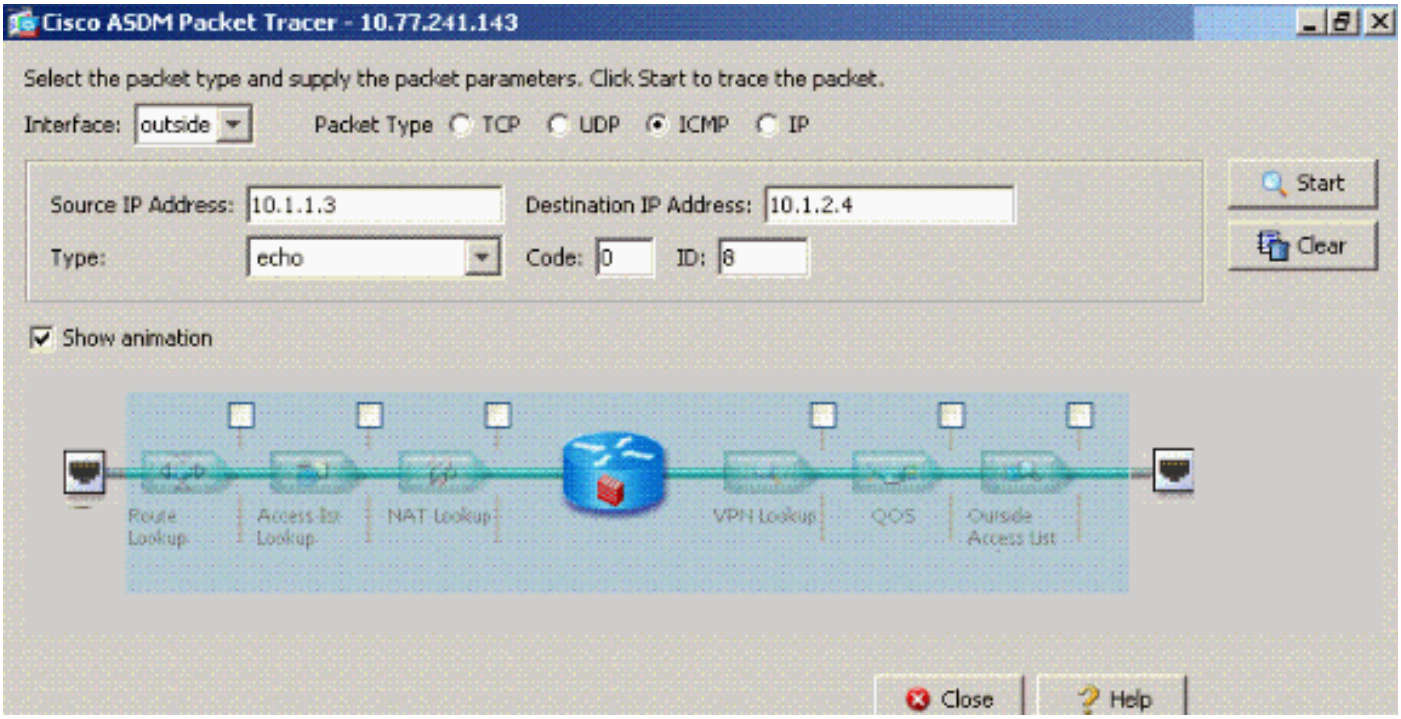
```
!--- Implicit rule refers to configuration rules not configured !--- by the user. By
default, intra-interface communication is not permitted. !--- In this example, the user has
not enabled intra-interface communications !--- and therefore the traffic is implicitly
denied. Additional Information: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

O equivalente dos comandos CLI no ASDM é mostrado nas seguintes figuras:

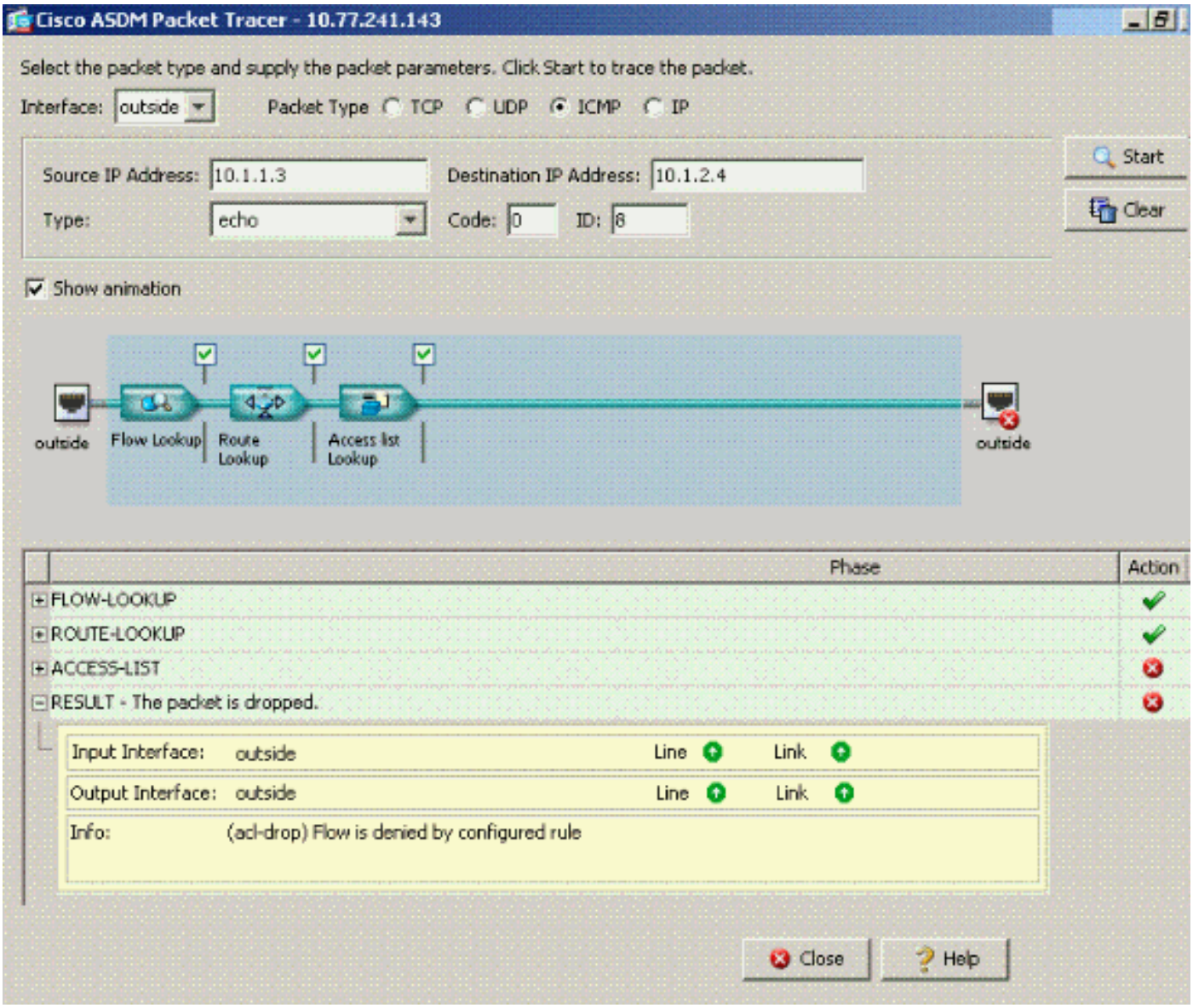
Passo 1:



Passo 2:



A saída do packet-tracer com o comando **same-security-traffic permit intrainterface** desabilitado.



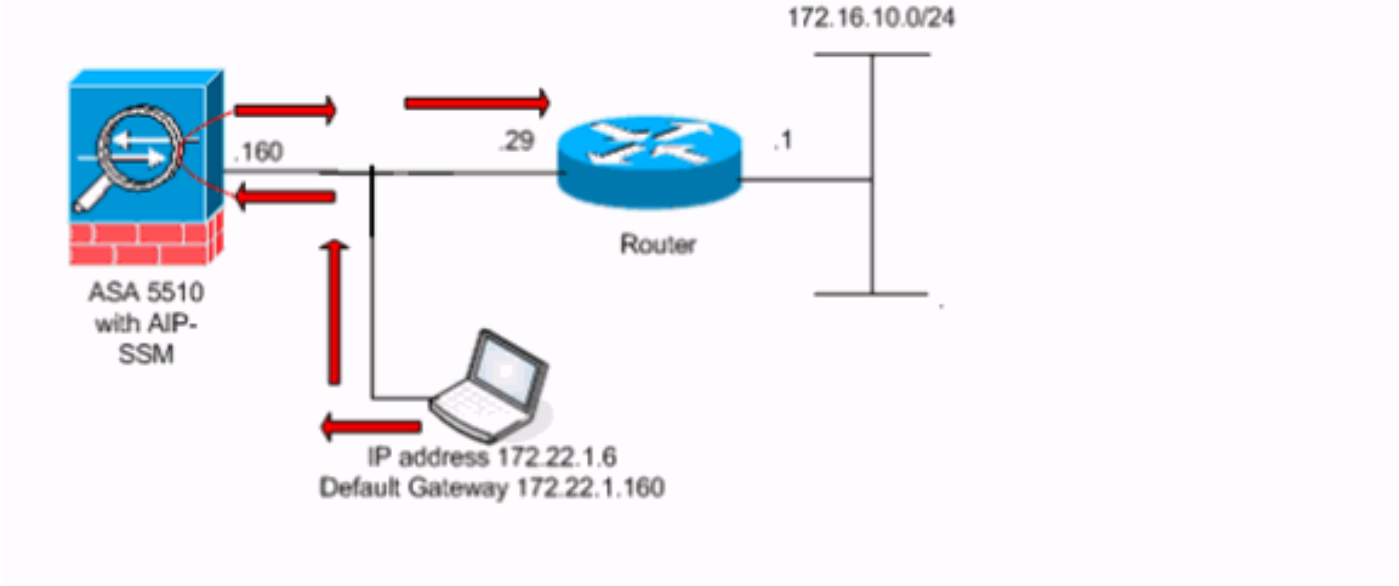
A saída do packet-tracer `caiu...regra implícita` sugere que uma configuração padrão está bloqueando o tráfego. O administrador precisa verificar a configuração atual para garantir que as comunicações entre interfaces estejam habilitadas. Nesse caso, a configuração do ASA precisa que as comunicações intrainterface sejam habilitadas (**mesma interface de permissão de tráfego de segurança**).

```
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...
```

Comunicações IntraInterface Habilitadas

As comunicações intrainterface agora estão ativadas. O comando **same-security-traffic permit intra-interface** é adicionado à configuração anterior. O host 172.22.1.6 tenta fazer ping no host 172.16.10.1. O host 172.22.1.6 envia um pacote de solicitação de eco ICMP para o gateway padrão (ASA). O host 172.22.1.6 registra respostas bem-sucedidas de 172.16.10.1. O ASA passa o tráfego ICMP com êxito.

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.



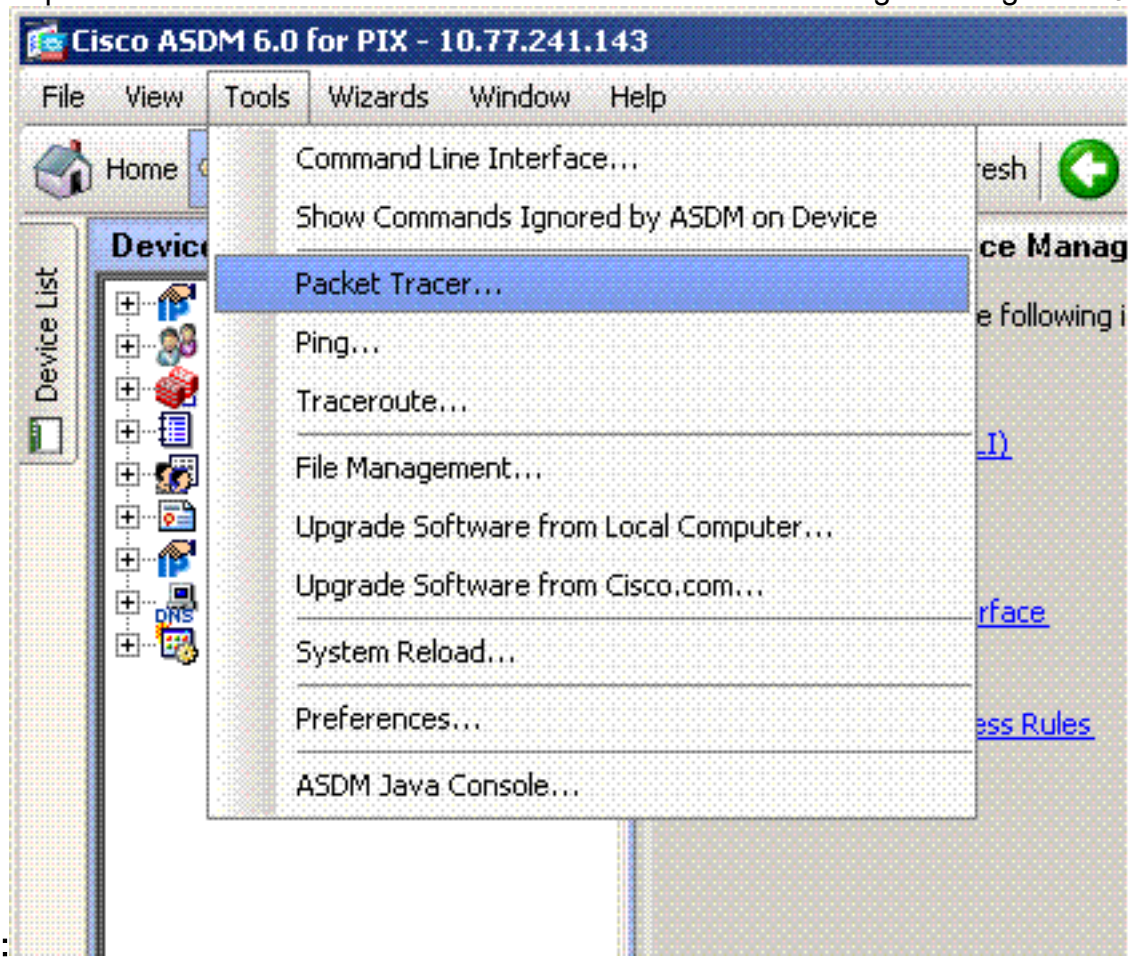
Estes exemplos mostram a mensagem do Syslog ASA e as saídas do packet-tracer:

- Estas são as mensagens de syslog registradas no 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
  ```
- Esta é a saída do packet-tracer:

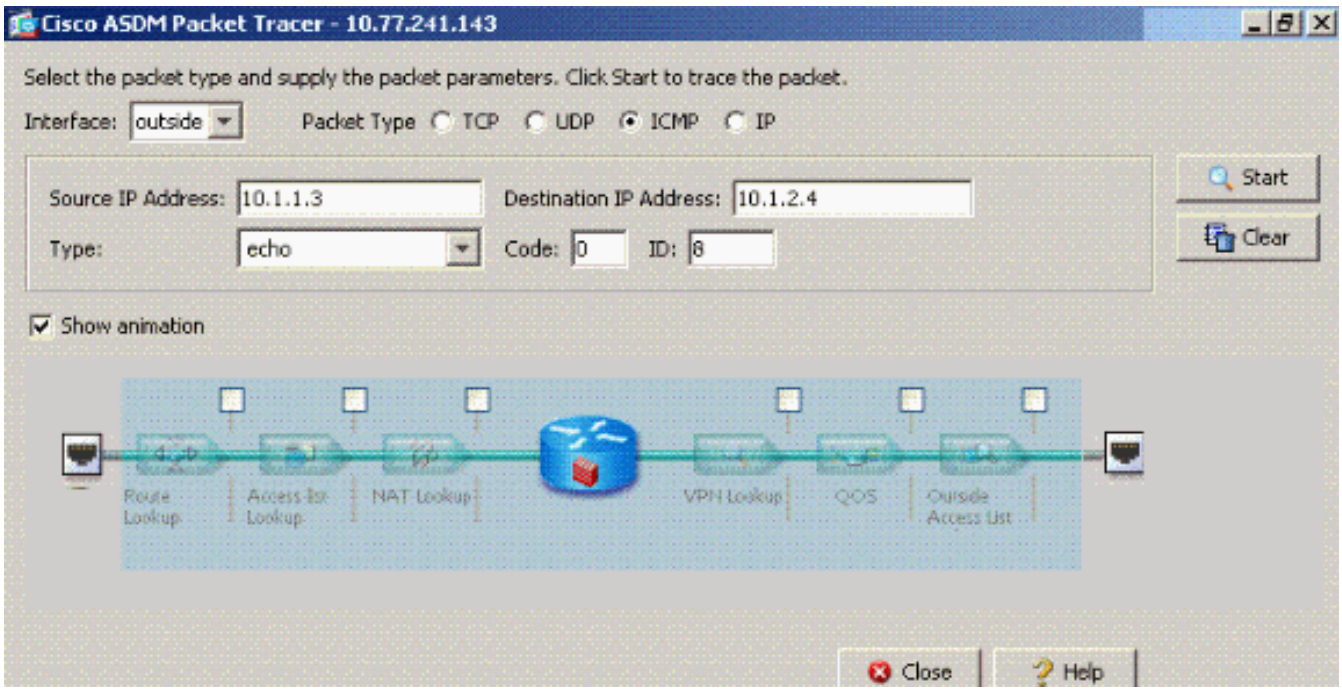
```
ciscoasa(config)#packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1

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
```

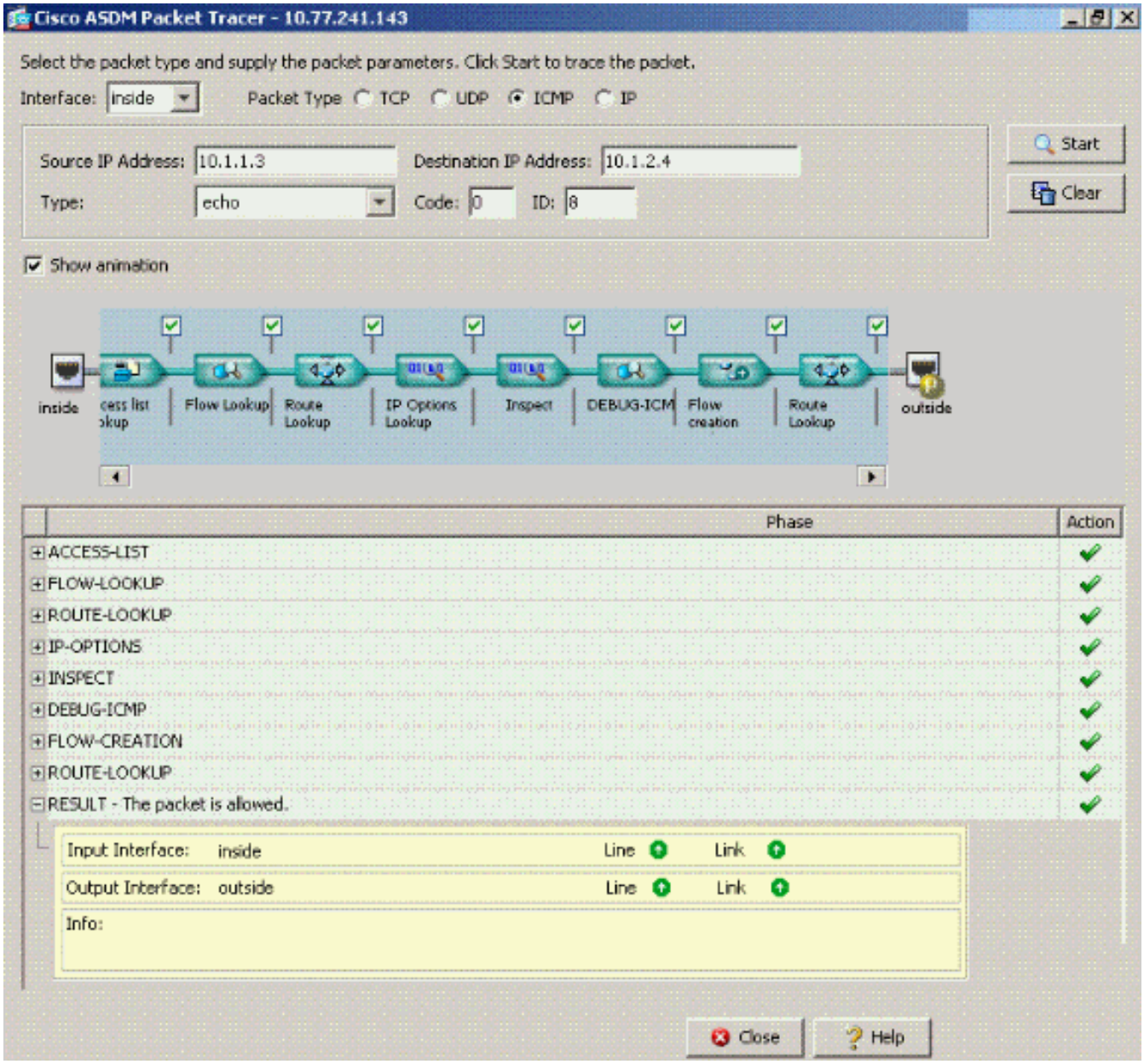
O equivalente dos comandos CLI no ASDM é mostrado nas seguintes figuras:**Passo 1:**



Passo 2:



A saída do packet-tracer com o comando **same-security-traffic permit intrainterface** ativado.



Nota:Nenhuma lista de acesso é aplicada à interface externa. Na configuração de exemplo, a interface externa recebe o nível de segurança 0. Por padrão, o firewall não permite o tráfego de uma interface de segurança baixa para uma interface de segurança alta. Isso pode levar os administradores a acreditar que o tráfego intrainterface não é permitido na interface externa (de baixa segurança) sem permissão de uma lista de acesso. No entanto, o mesmo tráfego de interface passa livremente quando nenhuma lista de acesso é aplicada à interface.

IntraInterface Habilitada e Tráfego Passado para o AIP-SSM para Inspeção

O tráfego intrainterface pode ser passado ao AIP-SSM para inspeção. Esta seção pressupõe que o administrador configurou o ASA para encaminhar o tráfego para o AIP-SSM e que o administrador sabe como configurar o software IPS 5.x.

Nesse ponto, a configuração do ASA contém a configuração de exemplo anterior, as comunicações intrainterface estão habilitadas e todo o tráfego (qualquer) é encaminhado para o AIP-SSM. A assinatura do IPS 2004 é modificada para descartar o tráfego de solicitação de eco. O host 172.22.1.6 tenta fazer ping no host 172.16.10.1. O host 172.22.1.6 envia um pacote de solicitação de eco ICMP para o gateway padrão (ASA). O ASA encaminha o pacote de solicitação de eco ao AIP-SSM para inspeção. O AIP-SSM descarta o pacote de dados de acordo com a configuração do IPS.

Estes exemplos mostram a mensagem do Syslog ASA e a saída do packet-tracer:

- Esta é a mensagem de syslog registrada no 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.
```

- Esta é a saída do 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.
```

Éimportante observar que os administradores devem usar o máximo possível de ferramentas de solução de problemas ao pesquisar um problema. Este exemplo mostra como duas diferentes ferramentas de solução de problemas podem pintar diferentes imagens. As duas ferramentas juntas contam uma história completa. A política de configuração do ASA permite o tráfego, mas a configuração do IPS não.

IntraInterface habilitada e listas de acesso aplicadas a uma interface

Esta seção usa a configuração de exemplo original neste documento, comunicações intrainterface habilitadas e uma lista de acesso aplicada à interface testada. Essas linhas são adicionadas à configuração. A lista de acesso tem como objetivo ser uma representação simples do que pode ser configurado em um firewall de produção.

```
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.
```

O host 172.22.1.6 tenta fazer ping no host 172.16.10.1. O host 172.22.1.6 envia um pacote de solicitação de eco ICMP para o gateway padrão (ASA). O ASA descarta o pacote de solicitação de eco de acordo com as regras da lista de acesso. O ping de teste do host 172.22.1.6 falha.

Estes exemplos mostram a mensagem do Syslog ASA e a saída do packet-tracer:

- Esta é a mensagem de syslog registrada no 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]
  ```
- Esta é a saída do 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
```

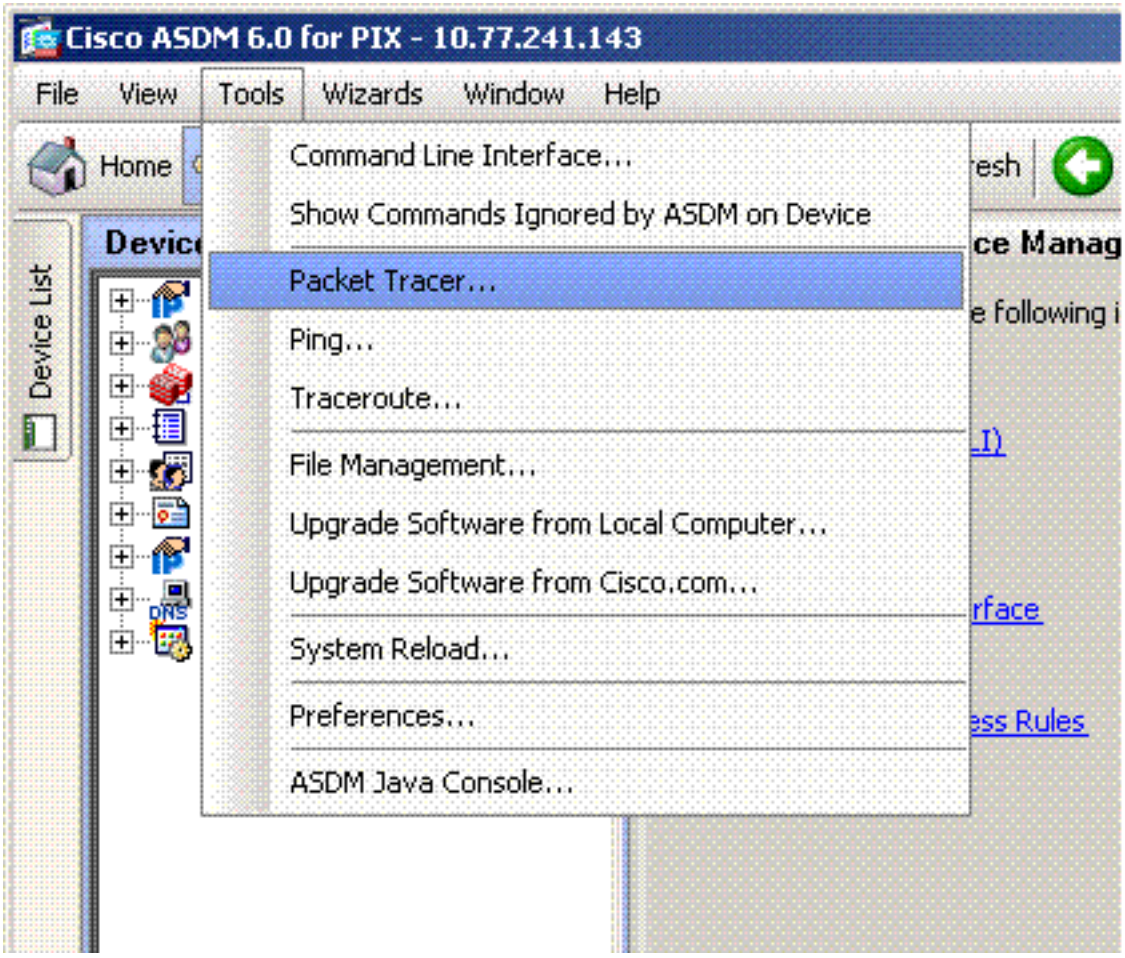
Consulte o packet-tracer para obter mais informações sobre o comando **packet-tracer**.

Nota:No caso de uma lista de acesso aplicada à interface incluir uma instrução de negação, a saída do rastreador de pacotes é alterada. Por exemplo:

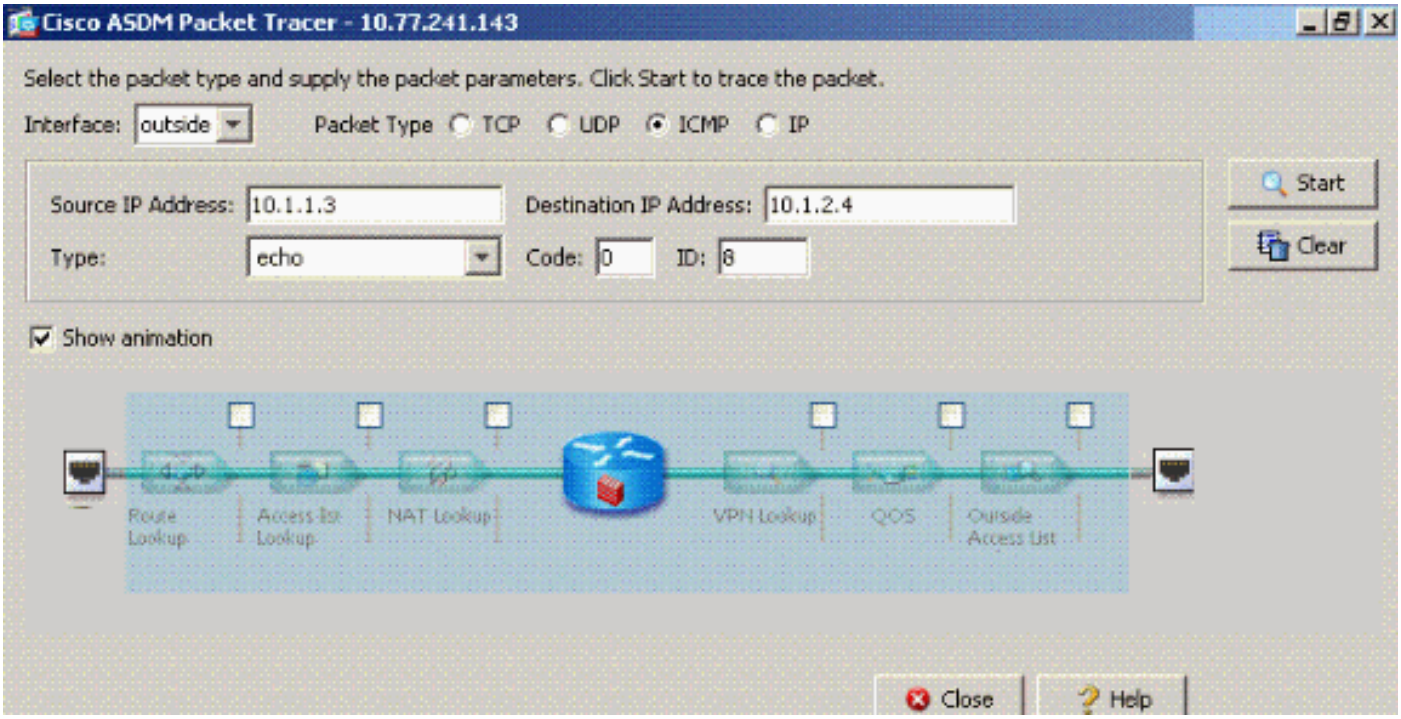
```
ciscoasa(config)#access-list outside_acl permit tcp any host 172.22.1.147 eq 80
ciscoasa(config)#access-list outside_acl deny ip any any
ciscoasa(config)#access-group outside_acl in interface outside
ciscoasa#packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1 detailed
!--- Output is suppressed.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

O equivalente dos comandos CLI acima no ASDM é mostrado nas seguintes figuras:

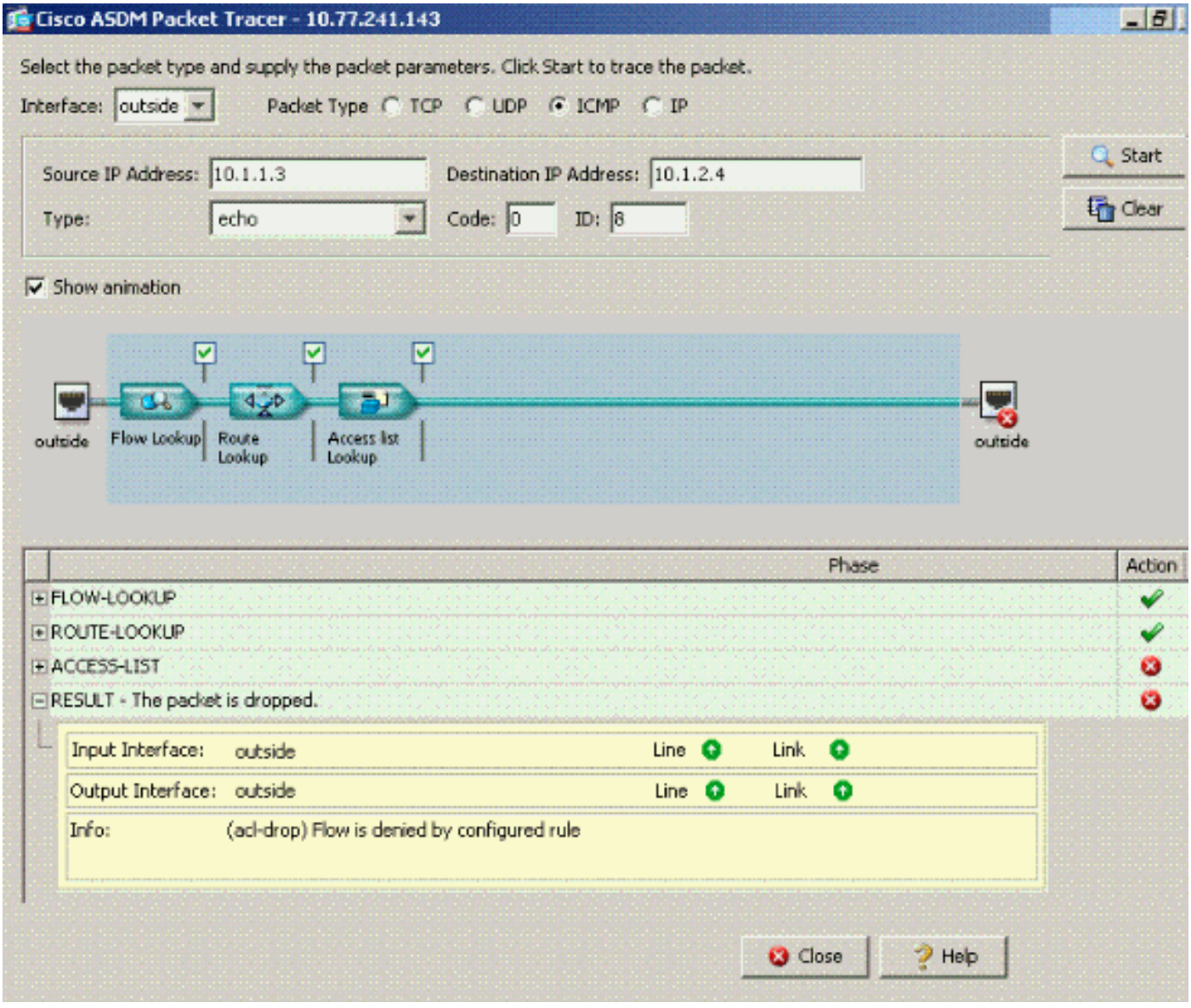
Passo 1:



Passo 2:



A saída do packet-tracer com o comando **same-security-traffic permit intra-interface** enabled e o **comando access-list outside_acl extended deny ip any any any** configurado para negar pacotes.

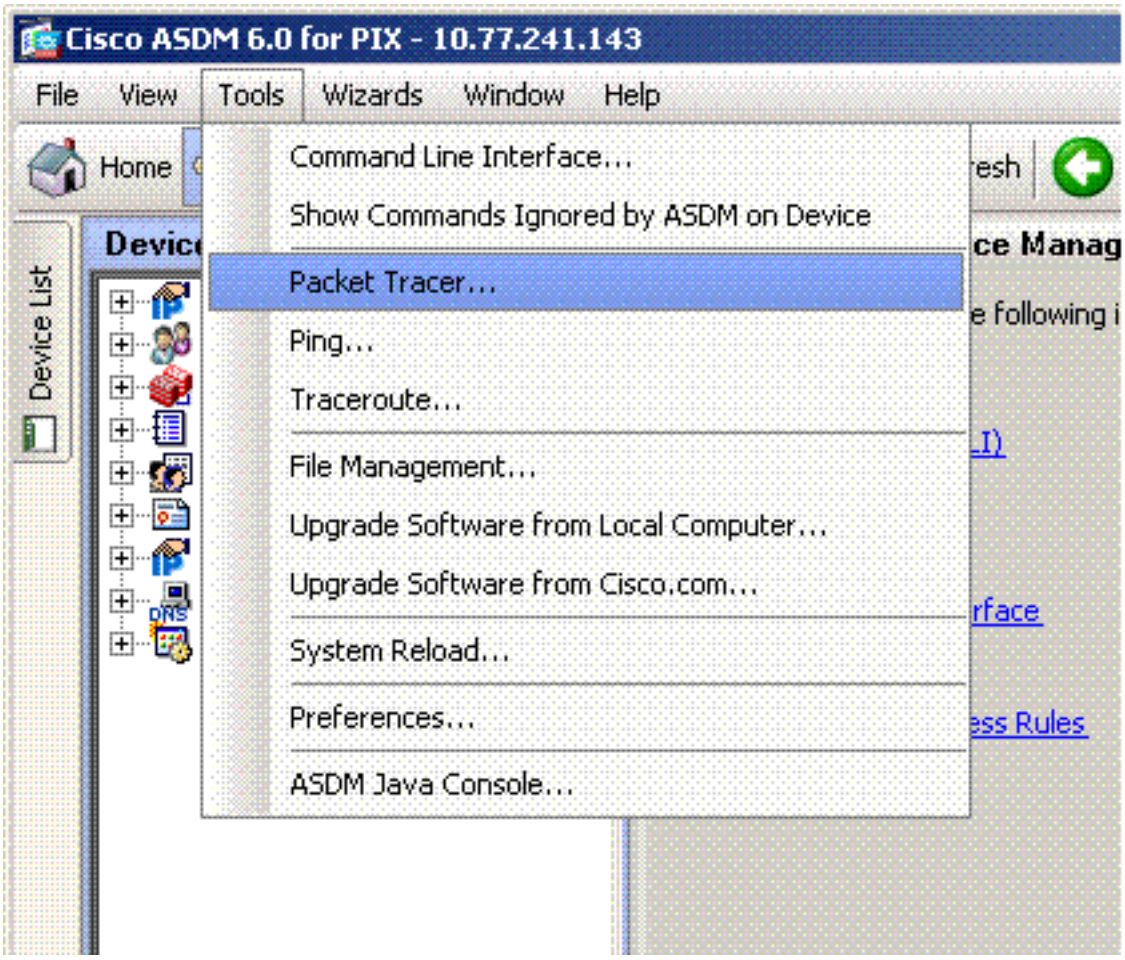


Se as comunicações intrainterface forem desejadas em uma interface específica e as listas de acesso forem aplicadas à mesma interface, as regras da lista de acesso devem permitir o tráfego intrainterface. Com o uso dos exemplos nesta seção, a lista de acesso precisa ser escrita como:

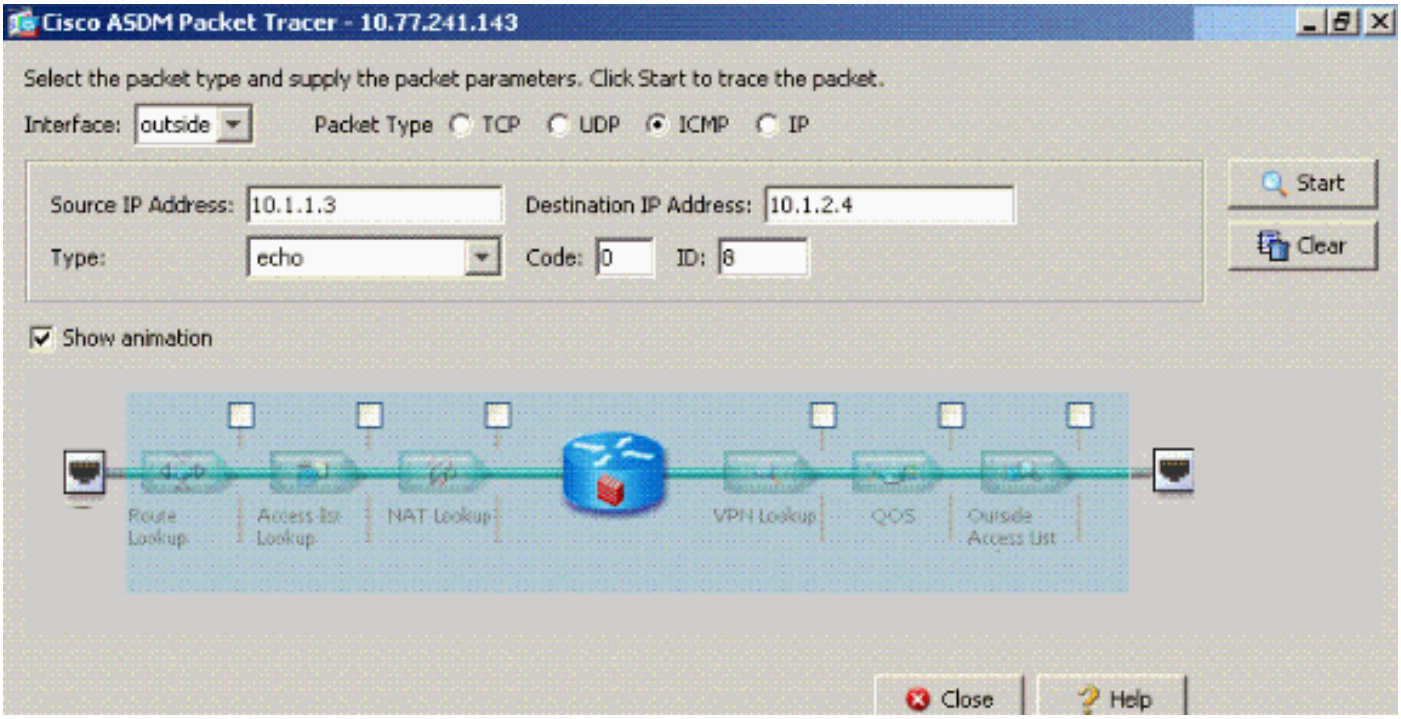
```
ciscoasa(config)#access-list outside_acl permit tcp any host 172.22.1.147 eq 80
ciscoasa(config)#access-list outside_acl permit ip 172.22.1.0 255.255.255.0 172.16.10.0
255.255.255.0
!--- 172.22.1.0 255.255.255.0 represents a locally !--- connected network on the ASA. !---
172.16.10.0 255.255.255.0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

O equivalente dos comandos CLI acima no ASDM é mostrado nas seguintes figuras:

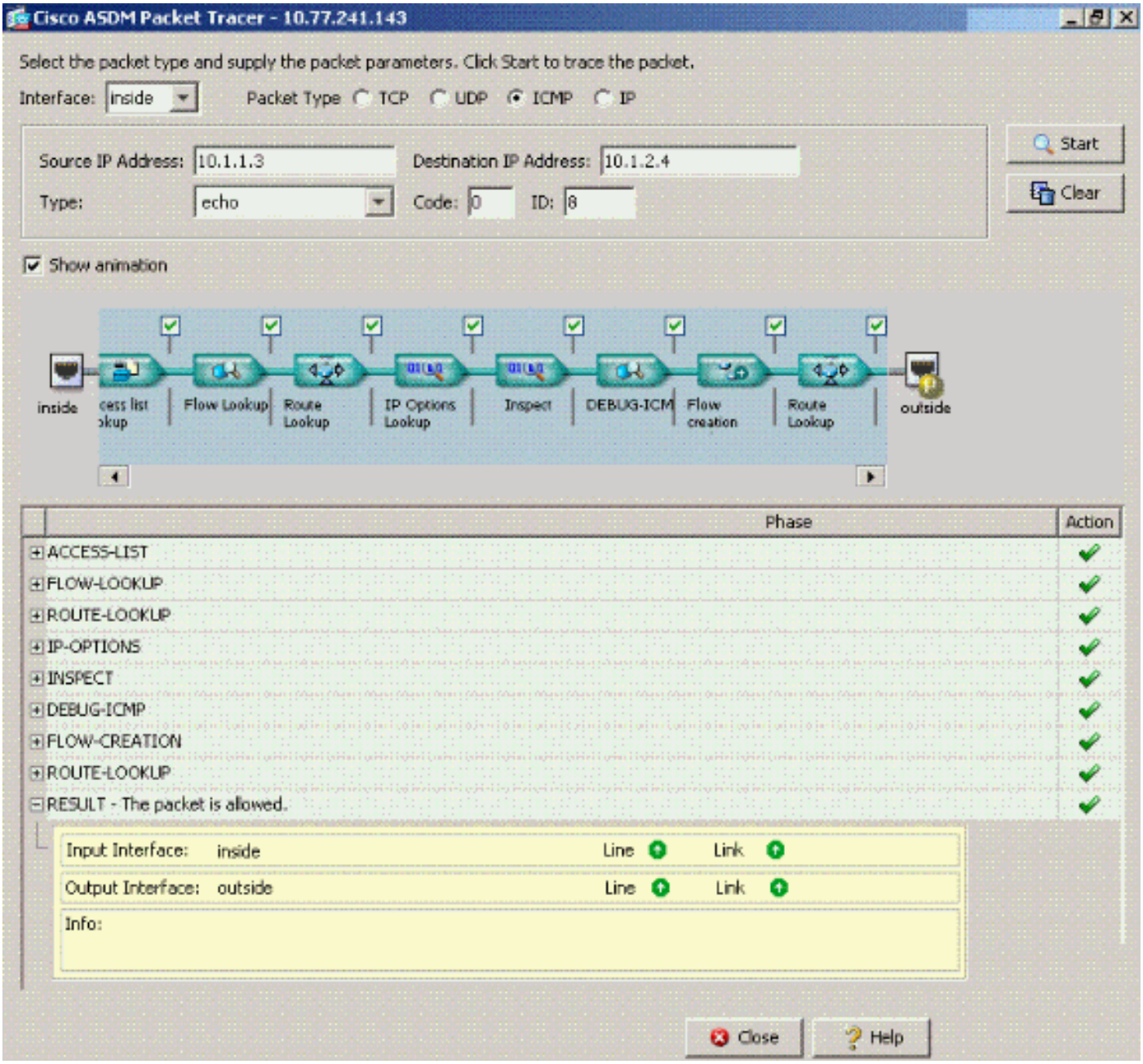
Passo 1:



Passo 2:



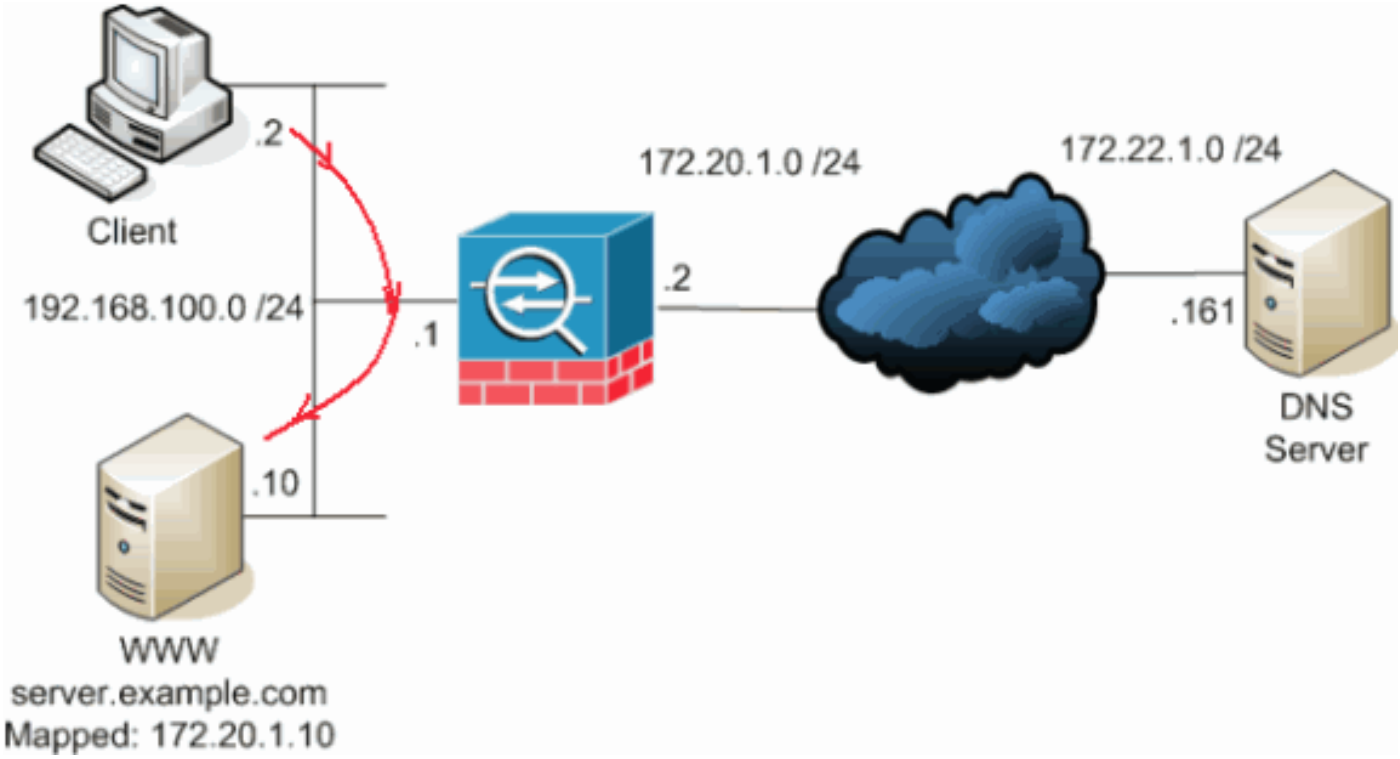
A saída do packet-tracer com o comando **same-security-traffic permit intra-interface** enabled e o **comando access-list outside_acl extended deny ip any any any** configurado na mesma interface onde o tráfego intrainterface é desejado.



Consulte access-list extended e access-group para obter mais informações sobre os comandos **access-list** e **access-group**.

Intra-interface habilitada com estática e NAT

Esta seção explica um cenário em que um usuário interno está tentando acessar o servidor Web interno com seu endereço público.



Nesse caso, o cliente em 192.168.100.2 deseja usar o endereço público do servidor WW (por exemplo, 172.20.1.10). Os serviços DNS para o cliente são fornecidos pelo servidor DNS externo em 172.22.1.161. Como o servidor DNS está localizado em outra rede pública, ele não sabe o endereço IP privado do servidor WWW. Em vez disso, o servidor DNS conhece o endereço mapeado do servidor WWW 172.20.1.10.

Aqui, esse tráfego da interface interna deve ser convertido e reroteado através da interface interna para acessar o servidor WW. Isso é chamado hairpinning. Isso pode ser realizado através destes comandos:

```
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
```

Para obter detalhes completos da configuração e mais informações sobre hairpinning, consulte Hairpinning com comunicação Intra-interface.

Pensamento de encaminhamento de lista de acesso

Nem todas as políticas de acesso a firewall são iguais. Algumas políticas de acesso são mais específicas do que outras. Caso as comunicações entre interfaces estejam habilitadas e o firewall não tenha uma lista de acesso aplicada a todas as interfaces, pode valer a pena adicionar uma lista de acesso no momento em que as comunicações entre interfaces estão ativadas. A lista de acesso aplicada precisa permitir a comunicação entre interfaces, bem como manter outros requisitos de política de acesso.

Este exemplo ilustra este ponto. O ASA conecta uma rede privada (interface interna) à Internet (interface externa). A interface interna do ASA não tem uma lista de acesso aplicada. Por padrão, todo o tráfego IP é permitido de dentro para fora. A sugestão é adicionar uma lista de acesso que se pareça com esta saída:

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

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

Esse conjunto de listas de acesso continua a permitir todo o tráfego IP. as linhas da lista de acesso específicas para as comunicações intra-interface lembram aos administradores que as comunicações intra-interface devem ser permitidas por uma lista de acesso aplicada.

Informações Relacionadas

- Referência de comando do Cisco Security Appliance, versão 7.2
- Mensagens de registro do sistema do Cisco Security Appliance, versão 7.2
- Cisco PIX Firewall Software
- ASA: Exemplo de Configuração para Envio de Tráfego de Rede do ASA para o AIP-SSM
- Suporte de produto dos dispositivos de segurança adaptável Cisco ASA 5500 Series
- Suporte Técnico e Documentação - Cisco Systems