PIX/ASA 7.2(1) y posteriores: Comunicaciones dentro de la interfaz

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Productos Relacionados
Convenciones
Antecedentes
Resolución de problemas
Comunicaciones intra-interfaz no habilitadas
Comunicaciones internas habilitadas
Intra-Interface Enabled y Traffic Passed to the AIP-SSM para su Inspección
Listas de Acceso y Habilitadas Intra-Interface Aplicadas a una Interfaz
Interfaz interna habilitada con NAT y estática
Pensamiento de Reenvío de Lista de Acceso
Información Relacionada

Introducción

Este documento ayuda a resolver problemas comunes que ocurren cuando se habilitan las comunicaciones internas de la interfaz sobre un Adaptive Security Appliance (ASA) o PIX que ejecuta la versión 7.2(1) y posteriores del software. La versión de software 7.2(1) incluye la capacidad de rutear datos de texto sin cifrar dentro y fuera de la misma interfaz. Ingrese el comando **same-security-traffic permit intra-interface** para habilitar esta función. Este documento asume que el administrador de red ha habilitado esta función o planea hacerlo en el futuro. La configuración y la resolución de problemas se proporcionan mediante la interfaz de línea de comandos (CLI).

Nota: Este documento se centra en los datos claros (no cifrados) que llegan y salen del ASA. Los datos cifrados no se discuten.

Para habilitar la comunicación dentro de la interfaz en ASA/PIX para la configuración de IPSec, refiérase a Ejemplo de Configuración de PIX/ASA y VPN Client para la VPN de Internet Pública en un Palo.

Para habilitar la comunicación dentro de la interfaz en ASA para la configuración SSL, consulte ASA 7.2(2): Ejemplo de Configuración de SSL VPN Client (SVC) para Public Internet VPN on a Stick.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Listas de acceso
- Ruteo
- Sistema de prevención de intrusiones (IPS) de Advanced Inspection and Prevention Security Services Module (AIP-SSM): el conocimiento de este módulo solo es necesario si está instalado y en funcionamiento.
- Software IPS versión 5.x: el conocimiento del software IPS no es necesario si el AIP-SSM no está en uso.

Componentes Utilizados

- ASA 5510 7.2(1) y posterior
- AIP-SSM-10 que opera el 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.

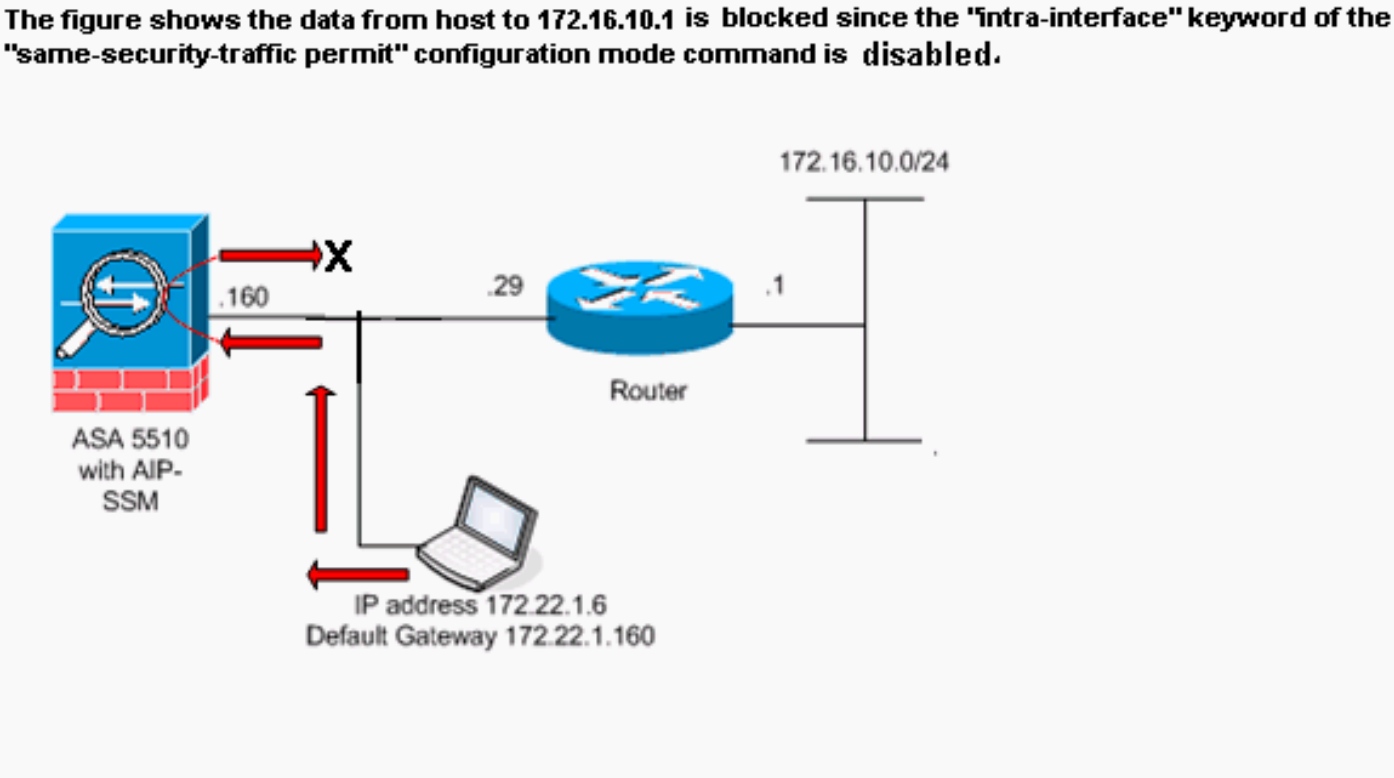
Productos Relacionados

Esta configuración también se puede utilizar con Cisco 500 Series PIX que ejecuta la versión 7.2(1) y posterior.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener información sobre las convenciones sobre documentos.

Antecedentes



Nota: Los esquemas de direccionamiento IP utilizados en esta configuración no son legalmente enrutables en Internet. Son direcciones RFC 1918 que se han utilizado en un entorno de laboratorio.

Esta tabla muestra la configuración inicial de 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:
```

Resolución de problemas

Estas secciones ilustran varios escenarios de configuración, mensajes de syslog relacionados y salidas de packet-tracer en relación con las comunicaciones dentro de la interfaz.

Comunicaciones intra-interfaz no habilitadas

En la configuración ASA, el host 172.22.1.6 intenta hacer ping al host 172.16.10.1. El host 172.22.1.6 envía un paquete de solicitud de eco ICMP al gateway predeterminado (ASA). Las comunicaciones dentro de la interfaz no se han habilitado en el ASA. El ASA descarta el paquete de solicitud de eco. El ping de prueba falla. El ASA se utiliza para solucionar el problema.

Este ejemplo muestra el resultado de los mensajes syslog y un packet-tracer:

- Este es el mensaje syslog registrado en el 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 es la salida de packet-tracer:

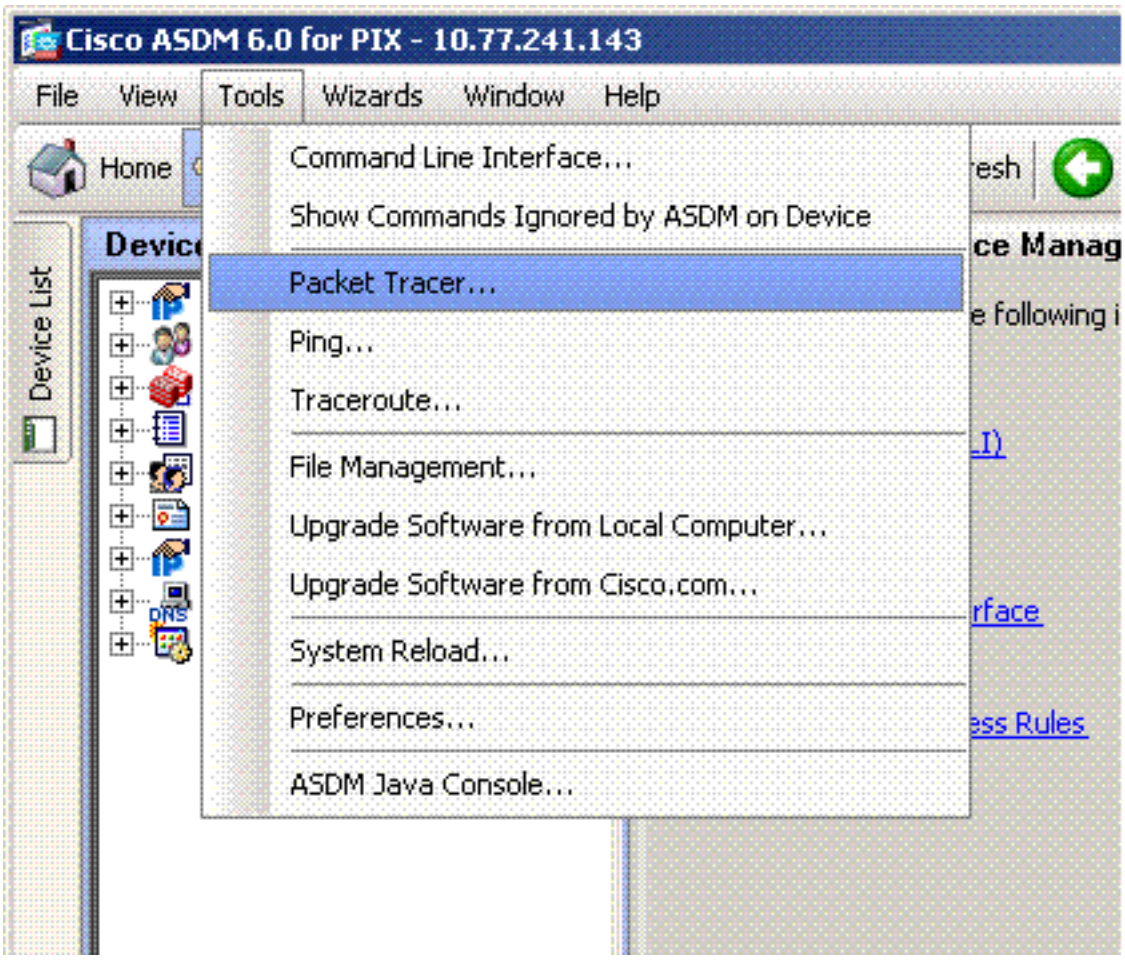
```
ciscoasa(config)#packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1 detailed
Phase: 1
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found no matching flow, creating a new flow

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

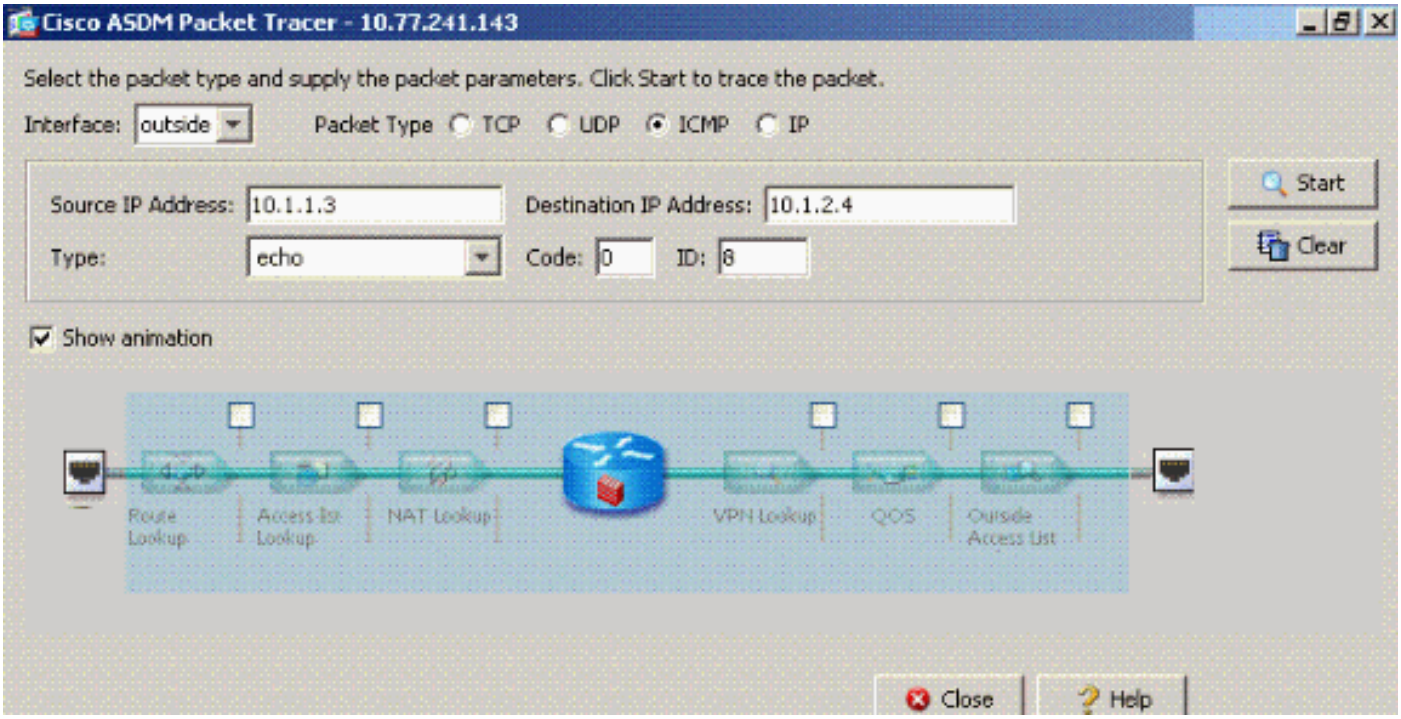
!--- Implicit rule refers to configuration rules not configured !--- by the user. By default, intra-interface communication is not permitted. !--- In this example, the user has not enabled intra-interface communications !--- and therefore the traffic is implicitly denied. Additional Information: Forward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

El equivalente de los comandos CLI en ASDM se muestra en estas figuras:

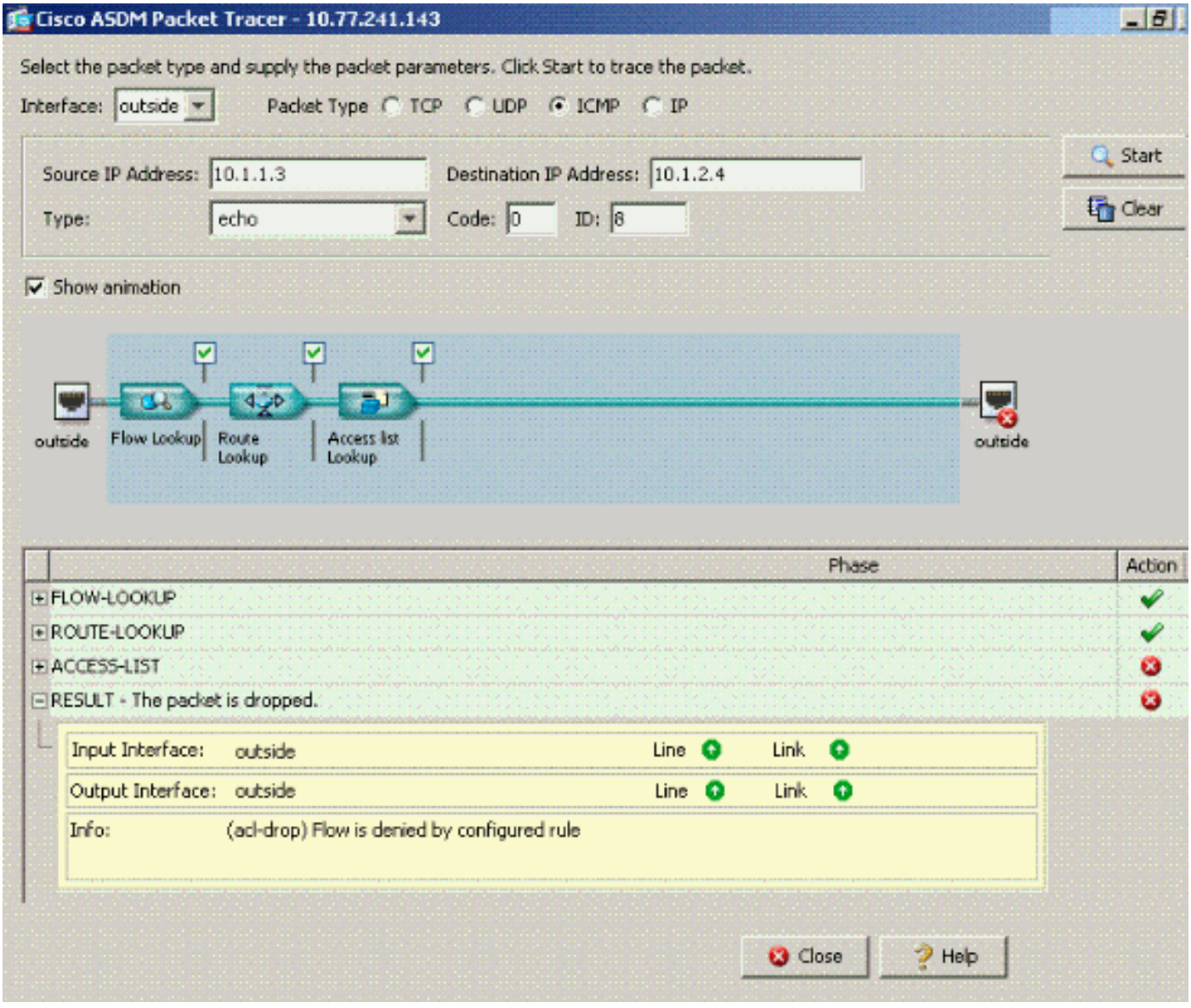
Paso 1:



Paso 2:



El resultado de packet-tracer con el comando **same-security-traffic permit intra-interface** inhabilitado.



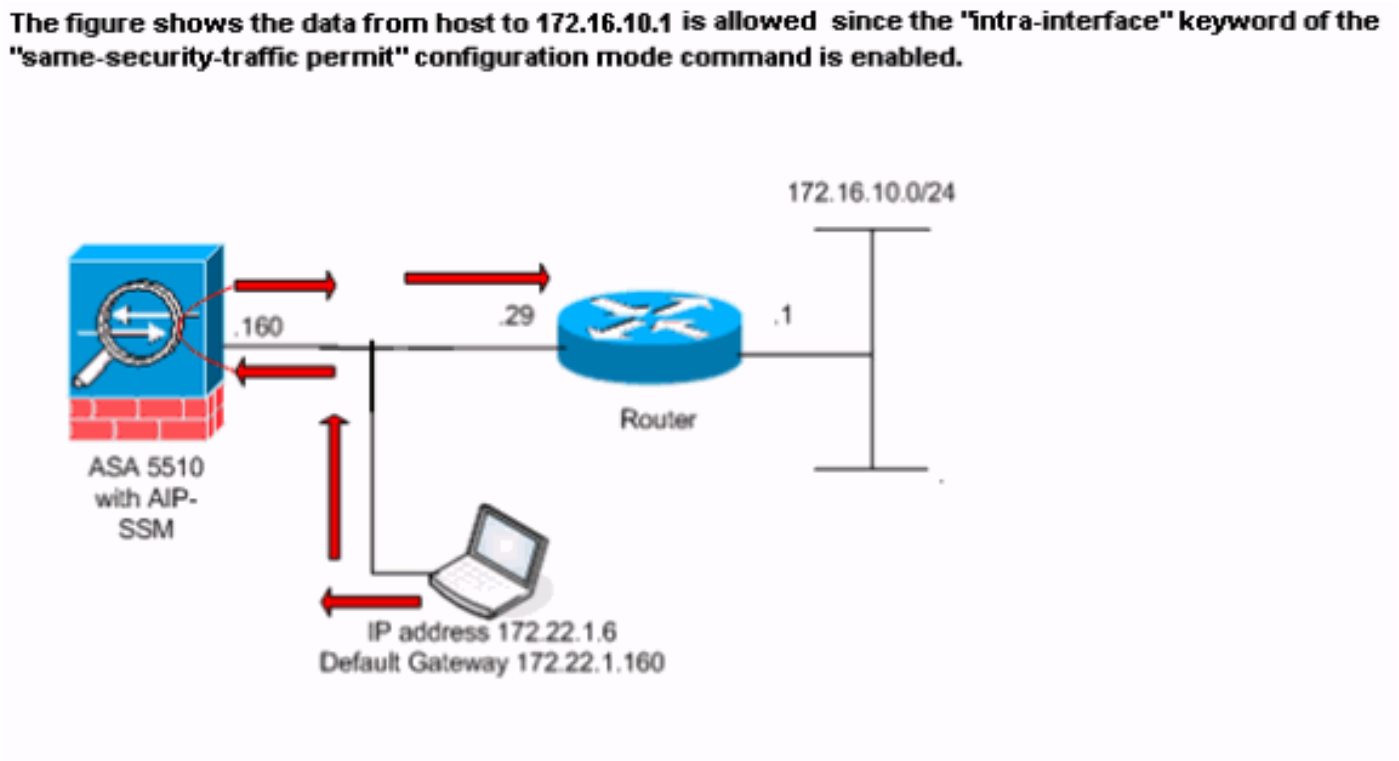
La salida de packet-tracer `cae...regla implícita` sugiere que una configuración predeterminada está bloqueando el tráfico. El administrador debe verificar la configuración en ejecución para asegurarse de que las comunicaciones dentro de la interfaz estén habilitadas. En este caso, la configuración de ASA necesita que se habiliten las comunicaciones dentro de la interfaz (**el tráfico de la misma seguridad permite el tráfico dentro de la interfaz**).

```
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...
```

Comunicaciones internas habilitadas

Las comunicaciones dentro de la interfaz ahora están habilitadas. El comando **same-security-traffic permit intra-interface** se agrega a la configuración anterior. El host 172.22.1.6 intenta hacer ping al host 172.16.10.1. El host 172.22.1.6 envía un paquete de solicitud de eco ICMP al gateway predeterminado (ASA). El host 172.22.1.6 registra las respuestas exitosas de 172.16.10.1. El ASA pasa el tráfico ICMP correctamente.

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.



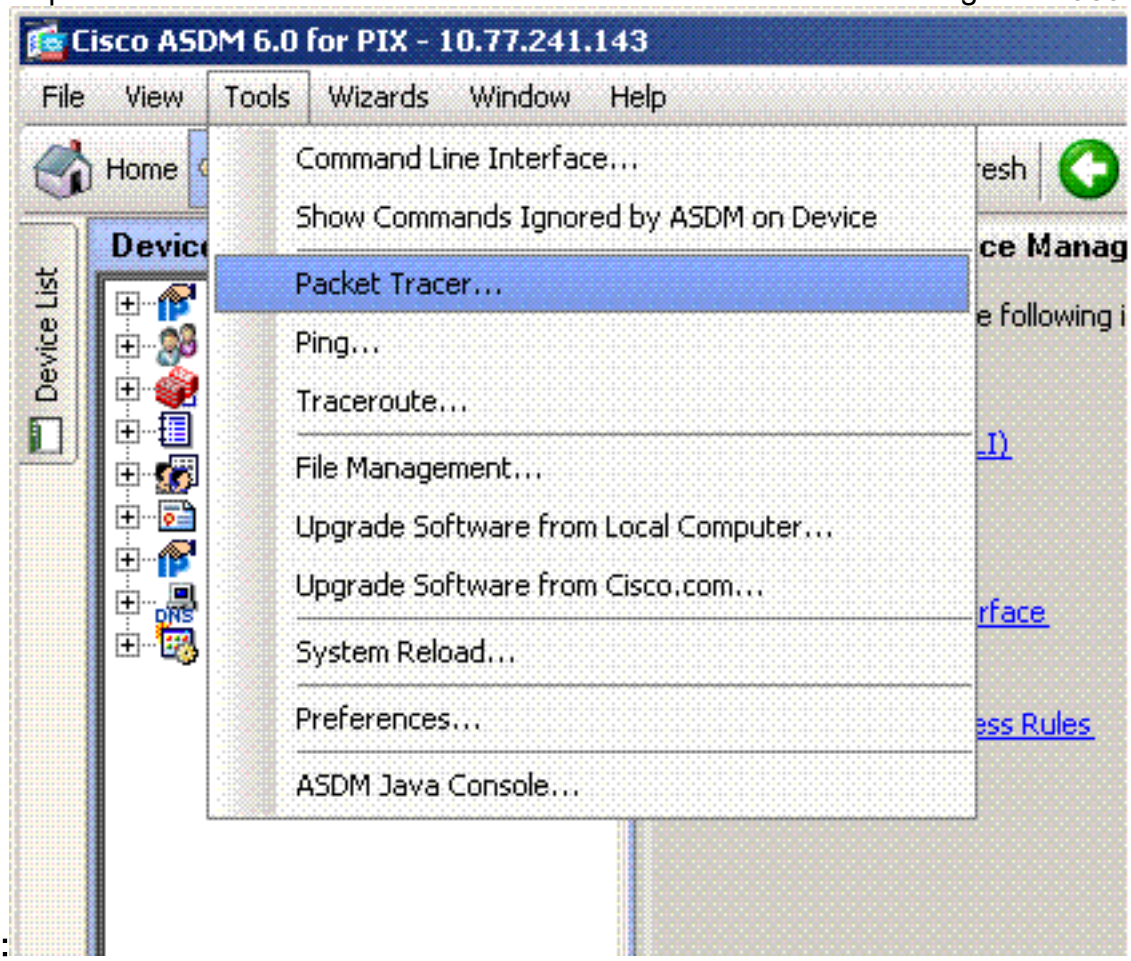
Estos ejemplos muestran el mensaje de syslog ASA y las salidas de packet-tracer:

- Estos son los mensajes syslog registrados en el 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 es la salida de packet-tracer:

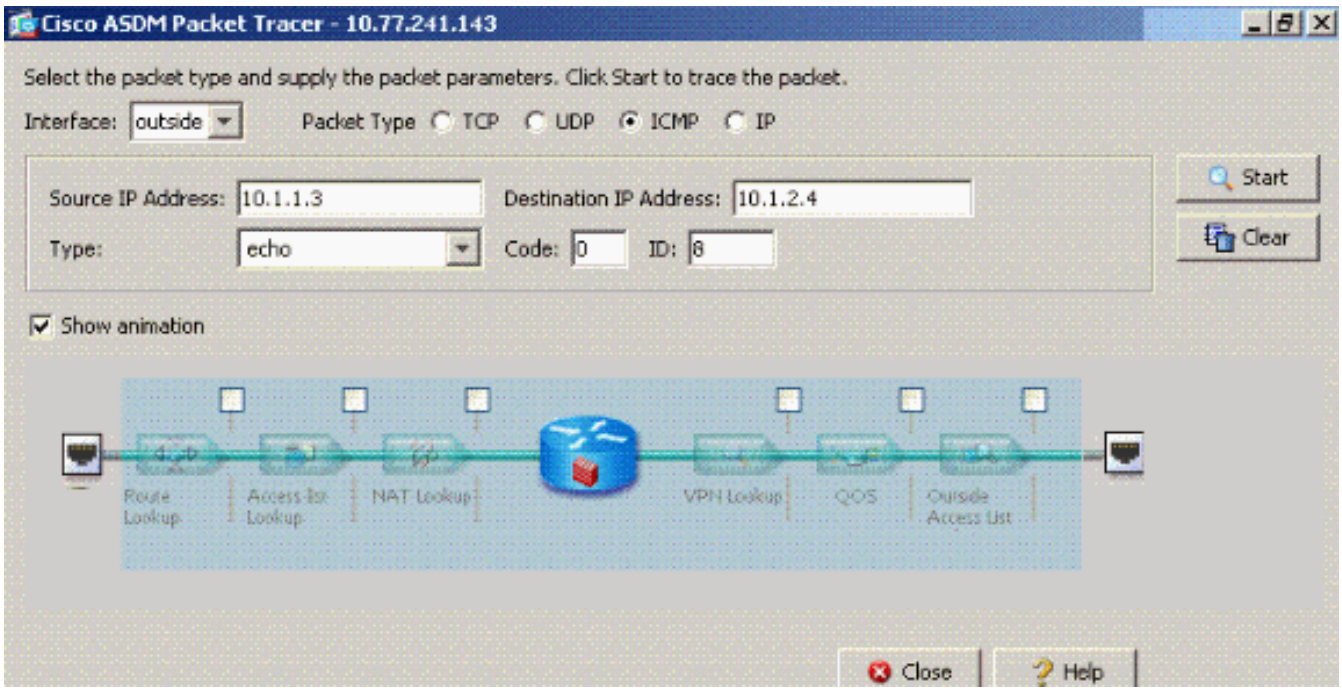
```
ciscoasa(config)#packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1

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
```

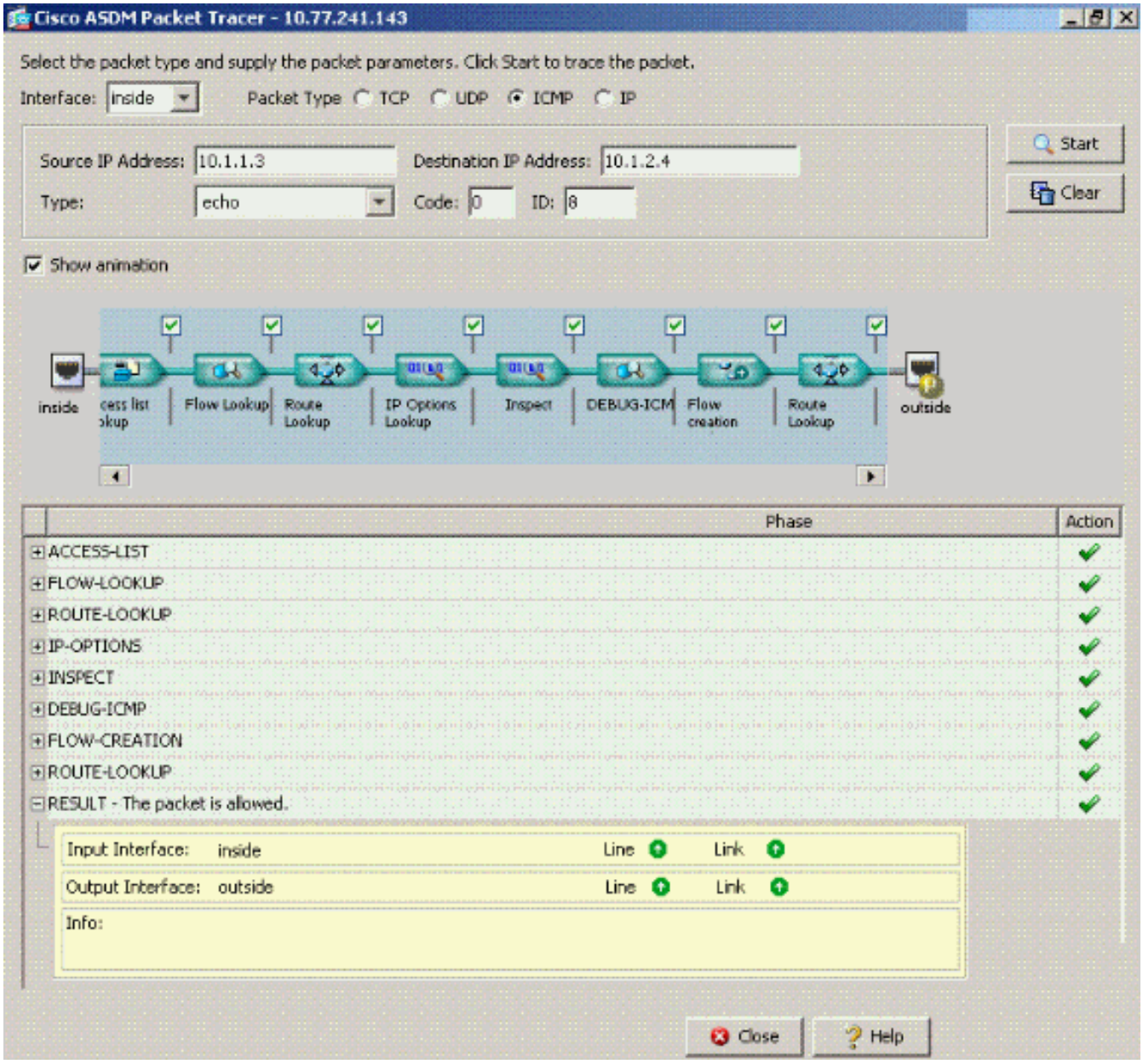
El equivalente de los comandos CLI en ASDM se muestra en estas figuras:**Paso 1:**



Paso 2:



La salida packet-tracer con el comando **same-security-traffic permit intra-interface** habilitado.



Nota: No se aplica ninguna lista de acceso a la interfaz externa. En la configuración de ejemplo, a la interfaz externa se le asigna el nivel de seguridad 0. De forma predeterminada, el firewall no permite el tráfico desde una interfaz de seguridad baja a una interfaz de seguridad alta. Esto podría llevar a los administradores a creer que el tráfico dentro de la interfaz no está permitido en la interfaz externa (baja seguridad) sin permiso de una lista de acceso. Sin embargo, el mismo tráfico de interfaz pasa libremente cuando no se aplica ninguna lista de acceso a la interfaz.

Intra-Interface Enabled y Traffic Passed to the AIP-SSM para su Inspección

El tráfico dentro de la interfaz se puede pasar al AIP-SSM para su inspección. En esta sección se asume que el administrador ha configurado el ASA para reenviar el tráfico al AIP-SSM y que el administrador sabe configurar el software IPS 5.x.

En este punto, la configuración ASA contiene la configuración de ejemplo anterior, se habilitan las comunicaciones dentro de la interfaz y todo el tráfico (cualquiera) se reenvía al AIP-SSM. La firma IPS 2004 se modifica para descartar el tráfico de solicitud de eco. El host 172.22.1.6 intenta hacer ping al host 172.16.10.1. El host 172.22.1.6 envía un paquete de solicitud de eco ICMP al gateway predeterminado (ASA). El ASA reenvía el paquete de solicitud de eco al AIP-SSM para

su inspección. El AIP-SSM descarta el paquete de datos según la configuración IPS.

Estos ejemplos muestran el mensaje de syslog ASA y la salida de packet-tracer:

- Este es el mensaje syslog registrado en el 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 es la salida de 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.
```

Es importante tener en cuenta que los administradores deben utilizar tantas herramientas de resolución de problemas como sea posible cuando investiguen un problema. Este ejemplo muestra cómo dos herramientas de resolución de problemas diferentes pueden pintar imágenes diferentes. Ambas herramientas juntas cuentan una historia completa. La política de configuración de ASA permite el tráfico, pero la configuración de IPS no.

Listas de Acceso y Habilitadas Intra-Interface Aplicadas a una Interfaz

Esta sección utiliza la configuración de ejemplo original en este documento, las comunicaciones dentro de la interfaz habilitadas y una lista de acceso aplicada a la interfaz probada. Estas líneas se agregan a la configuración. La lista de acceso está pensada para ser una representación simple de lo que se podría configurar en un firewall de producción.

```
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.
```

El host 172.22.1.6 intenta hacer ping al host 172.16.10.1. El host 172.22.1.6 envía un paquete de solicitud de eco ICMP al gateway predeterminado (ASA). El ASA descarta el paquete de solicitud de eco según las reglas de la lista de acceso. El ping de prueba de host 172.22.1.6 falla.

Estos ejemplos muestran el mensaje de syslog ASA y la salida de packet-tracer:

- Este es el mensaje syslog registrado en el 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 es la salida de 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
```

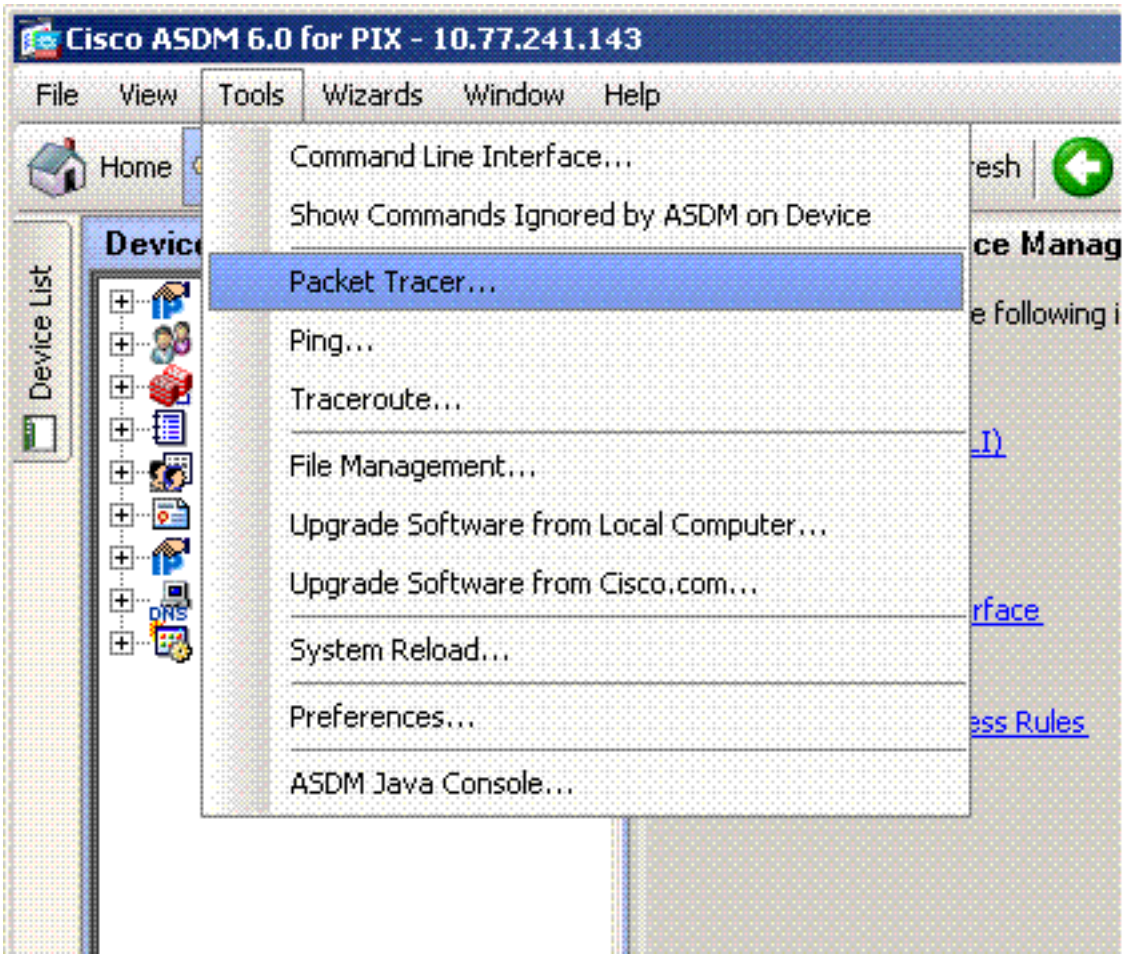
Refiérase a packet-tracer para obtener más información sobre el **comando packet-tracer**.

Nota: En el caso de que la lista de acceso aplicada a la interfaz incluya una sentencia deny, cambia el resultado del packet-tracer. Por ejemplo:

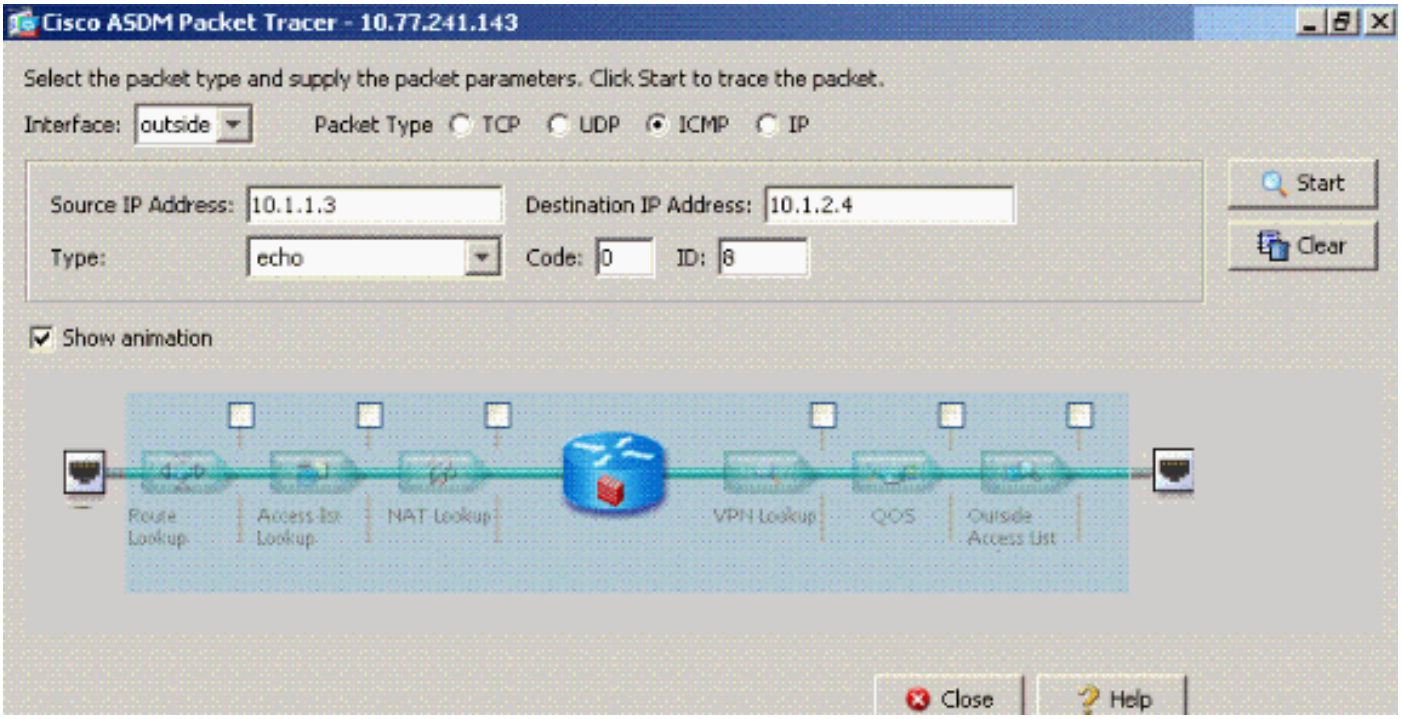
```
ciscoasa(config)#access-list outside_acl permit tcp any host 172.22.1.147 eq 80
ciscoasa(config)#access-list outside_acl deny ip any any
ciscoasa(config)#access-group outside_acl in interface outside
ciscoasa#packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1 detailed
!--- Output is suppressed.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

El equivalente de los comandos CLI anteriores en ASDM se muestra en estas figuras:

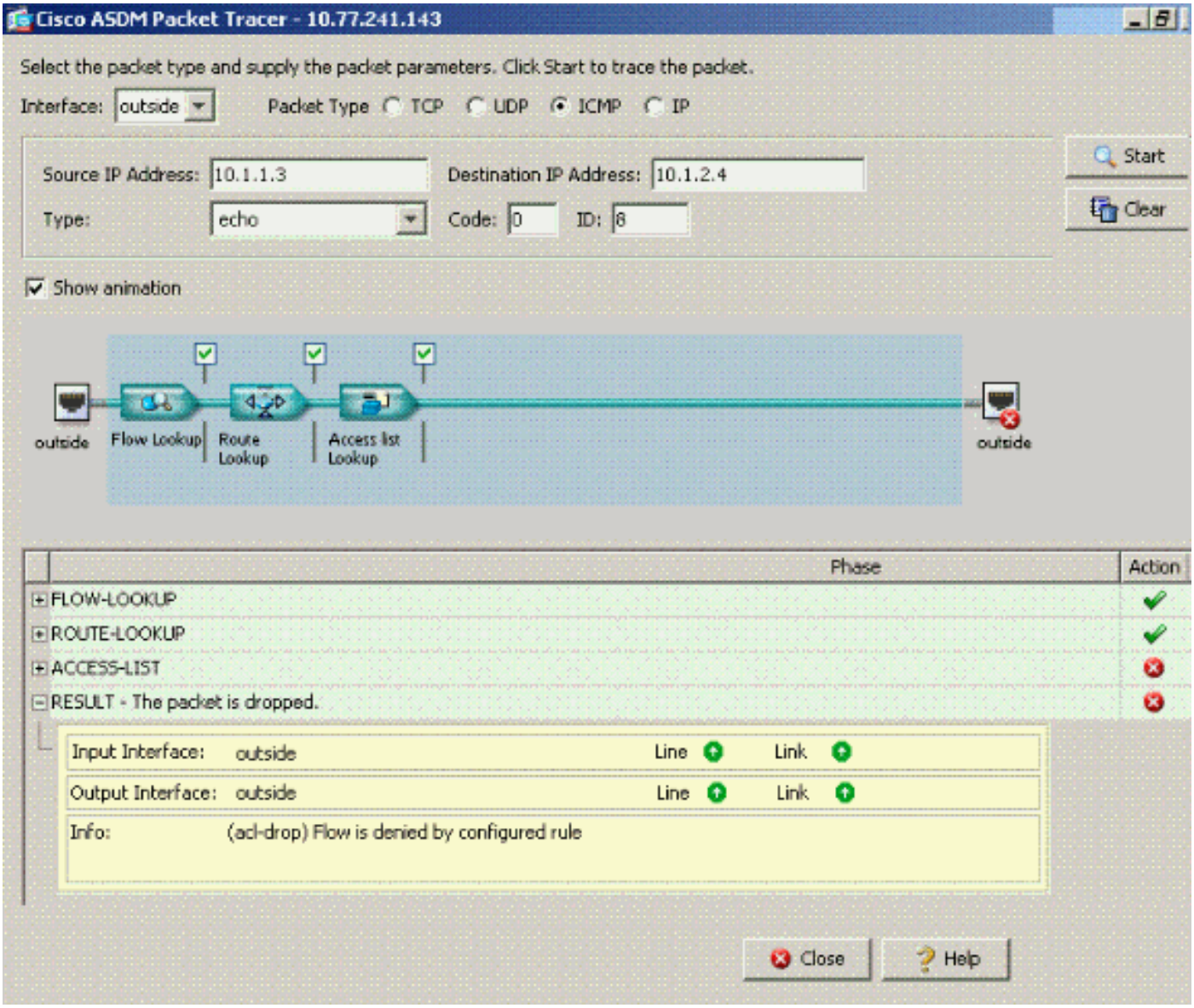
Paso 1:



Paso 2:



El resultado de packet-tracer con el comando **same-security-traffic permit intra-interface** habilitado y el **comando access-list outside_acl extended deny ip any any** configurado para denegar paquetes.

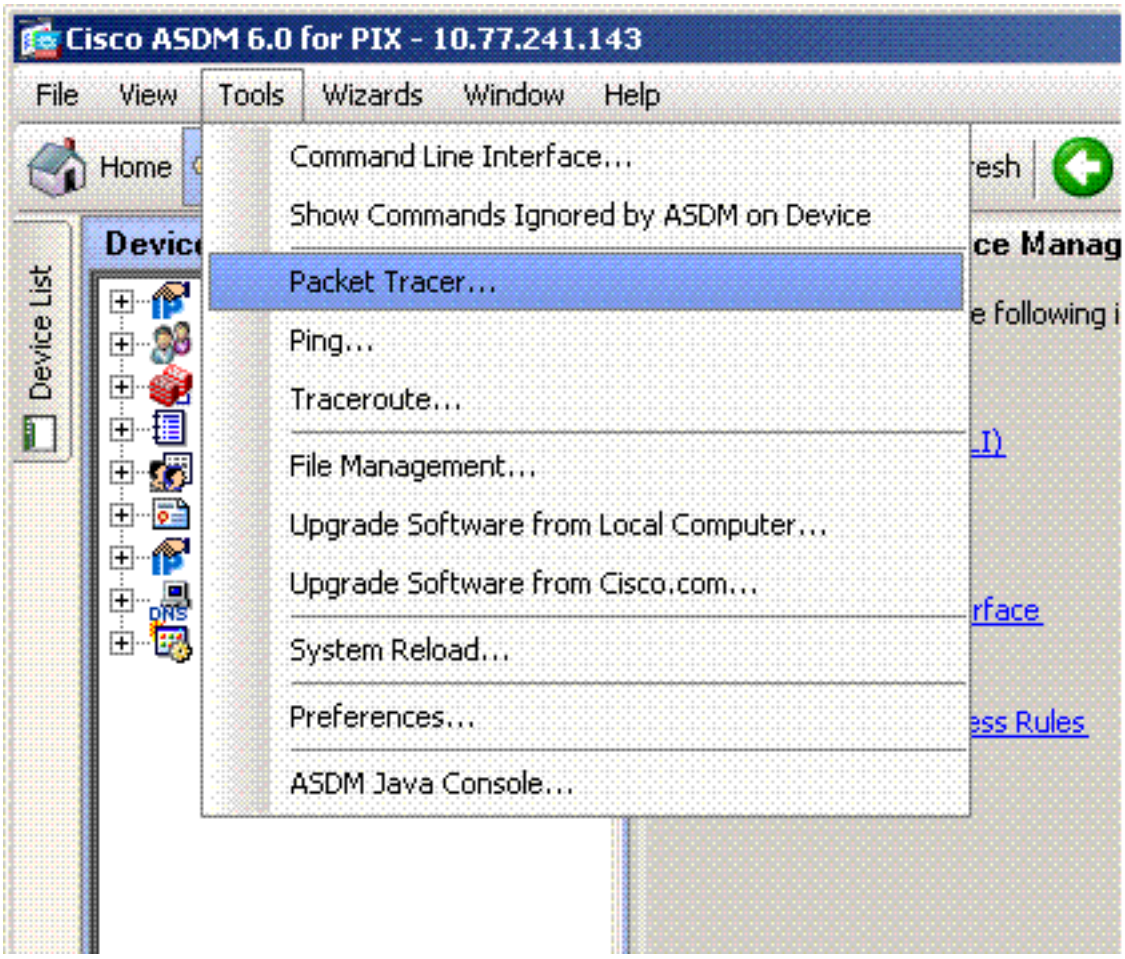


Si se desean las comunicaciones dentro de la interfaz en una interfaz determinada y las listas de acceso se aplican a la misma interfaz, las reglas de la lista de acceso deben permitir el tráfico dentro de la interfaz. Con el uso de los ejemplos de esta sección, la lista de acceso debe escribirse como:

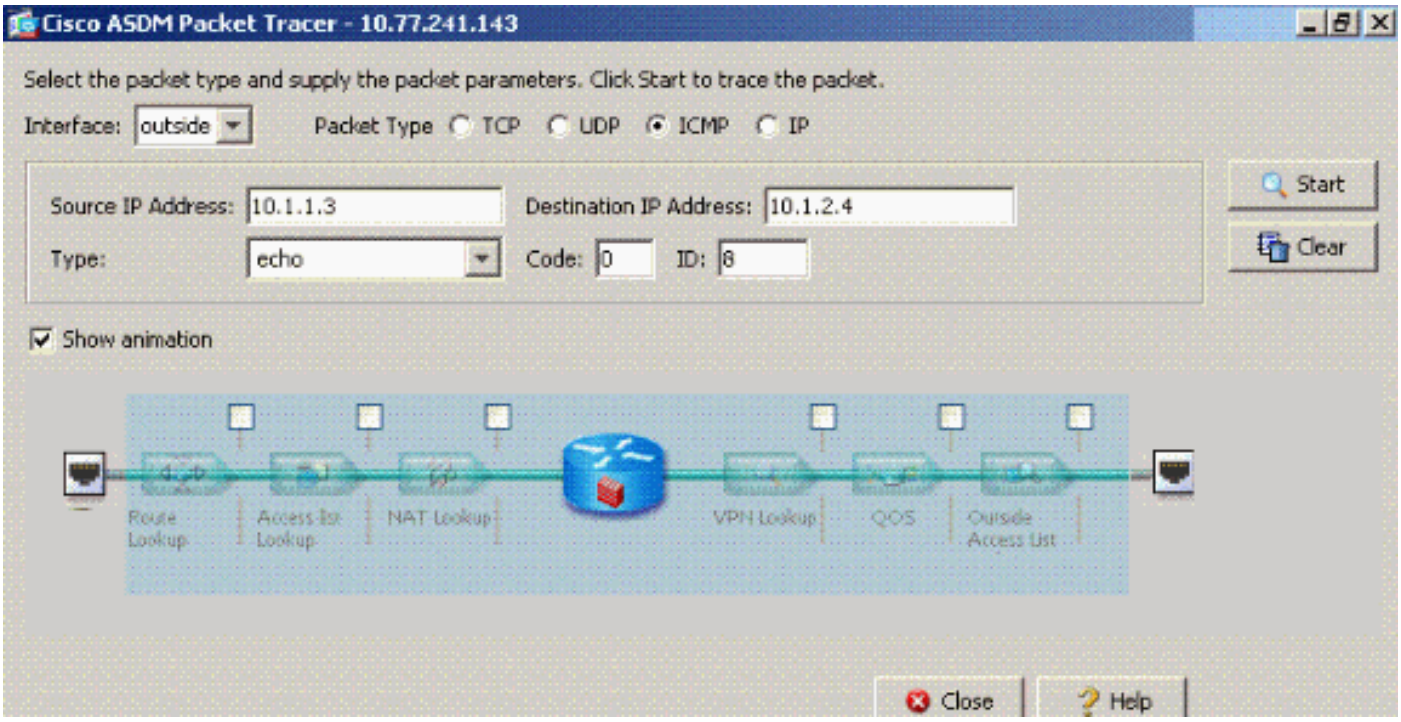
```
ciscoasa(config)#access-list outside_acl permit tcp any host 172.22.1.147 eq 80
ciscoasa(config)#access-list outside_acl permit ip 172.22.1.0 255.255.255.0 172.16.10.0
255.255.255.0
!--- 172.22.1.0 255.255.255.0 represents a locally !--- connected network on the ASA. !---
172.16.10.0 255.255.255.0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

El equivalente de los comandos CLI anteriores en ASDM se muestra en estas figuras:

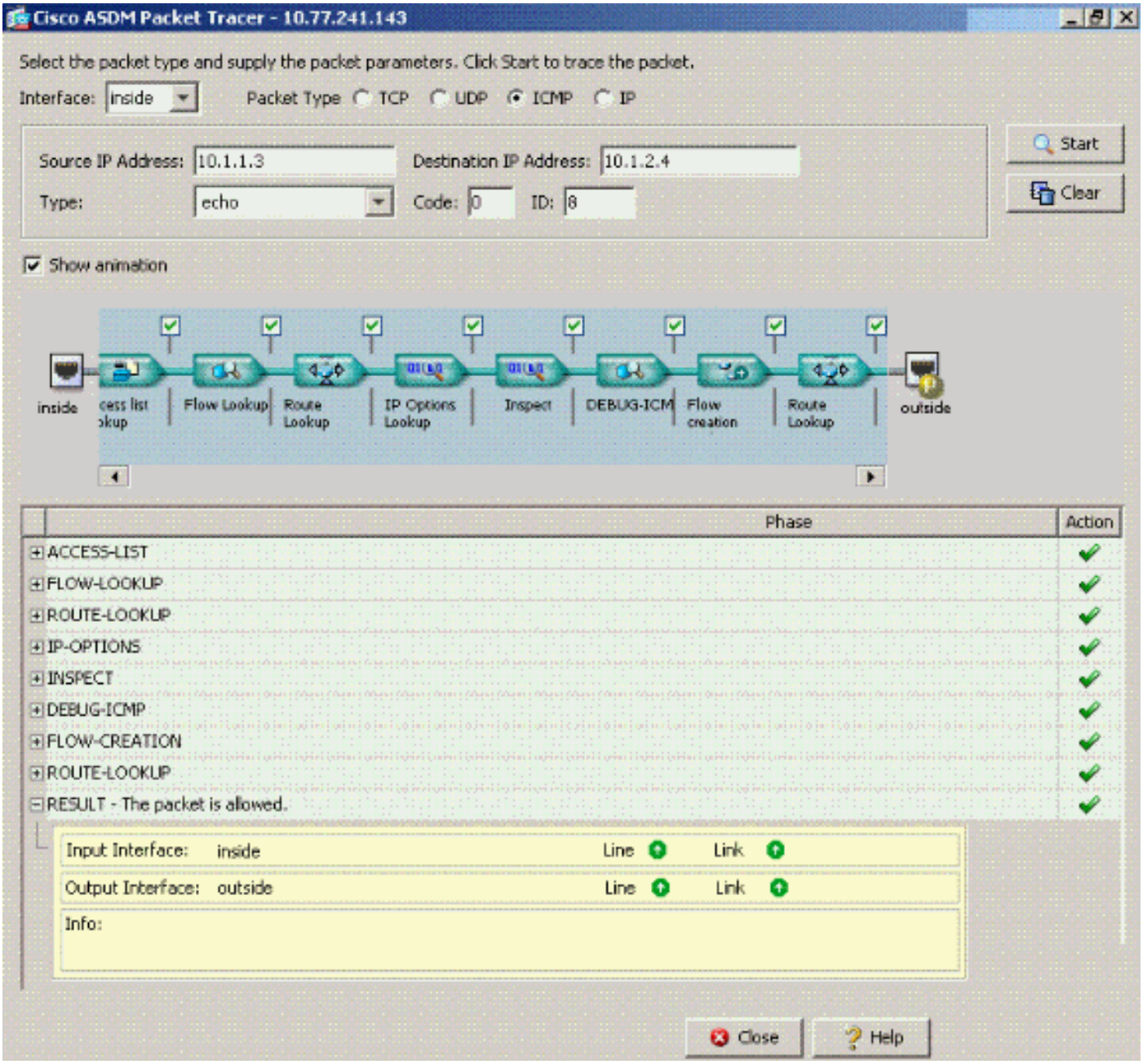
Paso 1:



Paso 2:



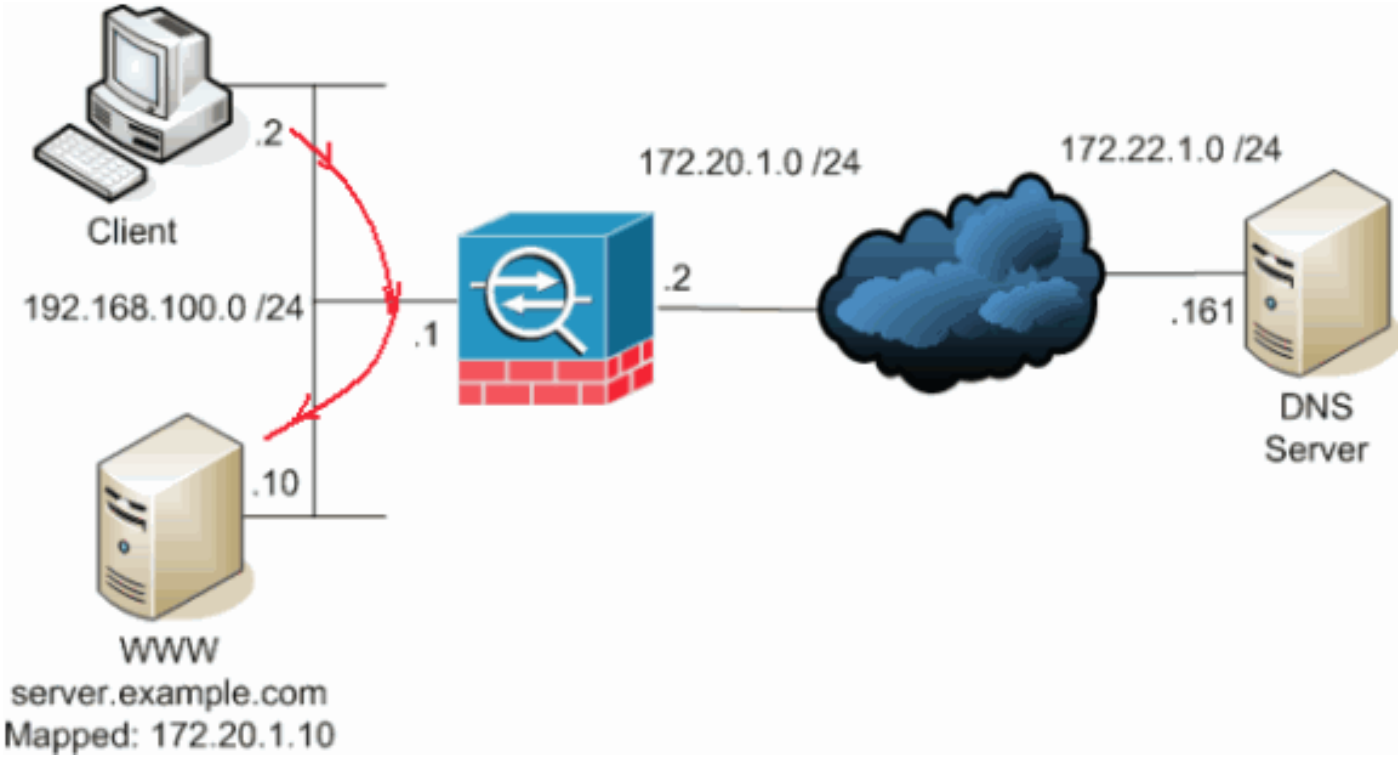
El resultado de packet-tracer con el comando **same-security-traffic permit intra-interface** habilitado y el **comando access-list outside_acl extended deny ip any any** configurado en la misma interfaz donde se desea tráfico dentro de la interfaz.



Consulte access-list extended y access-group para obtener más información sobre los comandos **access-list y access-group .**

Interfaz interna habilitada con NAT y estática

Esta sección explica un escenario en el que un usuario interno intenta acceder al servidor Web interno con su dirección pública.



En este caso, el cliente en 192.168.100.2 desea utilizar la dirección pública del servidor WWW (por ejemplo, 172.20.1.10). Los servicios DNS para el cliente son proporcionados por el servidor DNS externo en 172.22.1.161. Dado que el servidor DNS se encuentra en otra red pública, no conoce la dirección IP privada del servidor WWW. En su lugar, el servidor DNS conoce la dirección asignada al servidor WWW de 172.20.1.10.

Aquí, este tráfico de la interfaz interna debe ser traducido y reenrutado a través de la interfaz interna para llegar al servidor WWW. Esto se llama hairpinning . Esto se puede realizar a través de estos 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 obtener detalles completos de la configuración y más información sobre hairpinning, refiérase a Hairpinning with Intra-interface Communication.

Pensamiento de Reenvío de Lista de Acceso

No todas las políticas de acceso al firewall son iguales. Algunas políticas de acceso son más específicas que otras. En el caso de que se habiliten las comunicaciones dentro de la interfaz y el firewall no tenga una lista de acceso aplicada a todas las interfaces, puede ser conveniente agregar una lista de acceso en el momento en que se habiliten las comunicaciones dentro de la interfaz. La lista de acceso aplicada debe permitir las comunicaciones dentro de la interfaz, así como mantener otros requisitos de políticas de acceso.

Este ejemplo ilustra este punto. ASA conecta una red privada (interfaz interna) a Internet (interfaz externa). La interfaz interna de ASA no tiene una lista de acceso aplicada. De forma predeterminada, todo el tráfico IP se permite desde el interior al exterior. La sugerencia es agregar una lista de acceso que se parezca a este resultado:

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

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

Este conjunto de listas de acceso continúa permitiendo todo el tráfico IP. Las líneas de lista de acceso específicas para las comunicaciones dentro de la interfaz recuerdan a los administradores que las comunicaciones dentro de la interfaz deben estar permitidas por una lista de acceso aplicada.

Información Relacionada

- Referencia de Comandos de Dispositivos de Seguridad de Cisco, Versión 7.2
- Mensajes de registro del sistema del dispositivo de seguridad de Cisco, versión 7.2
- Cisco PIX Firewall Software
- ASA: Ejemplo de Configuración de Enviar Tráfico de Red desde ASA a AIP SSM
- Soporte de producto para dispositivos de seguridad adaptable Cisco ASA de la serie 5500
- Soporte Técnico y Documentación - Cisco Systems