PIX/ASA 7.2(1) und höher: Schnittstellenübergreifende Kommunikation

Inhalt

Einführung

Dieses Dokument unterstützt Sie bei der Behebung gängiger Probleme, die auftreten, wenn Sie die Kommunikation innerhalb der Schnittstelle auf einer Adaptive Security Appliance (ASA) oder PIX aktivieren, die in Softwareversion 7.2(1) und höher ausgeführt wird. Softwareversion 7.2(1) enthält die Funktion zum Weiterleiten von Klartextdaten in und aus derselben Schnittstelle. Geben Sie den Befehl **allow intra-interface (Datenverkehr mit identischer Sicherheit zulassen) ein**, um diese Funktion zu aktivieren. In diesem Dokument wird davon ausgegangen, dass der Netzwerkadministrator diese Funktion aktiviert hat oder dies in Zukunft planen wird. Die Konfiguration und Fehlerbehebung erfolgt über die Befehlszeilenschnittstelle (CLI).

Hinweis: Im Mittelpunkt dieses Dokuments stehen klare (unverschlüsselte) Daten, die bei der ASA eintreffen und diese verlassen. Verschlüsselte Daten werden nicht behandelt.

Informationen zum Aktivieren der Kommunikation zwischen den Schnittstellen auf ASA/PIX für die IPsec-Konfiguration finden Sie unter PIX/ASA und VPN-Client für Public Internet VPN in einem Stick-Konfigurationsbeispiel.

Informationen zum Aktivieren der Kommunikation zwischen den Schnittstellen auf ASA für die SSL-Konfiguration finden Sie in ASA 7.2(2): SSL VPN Client (SVC) für Public Internet VPN auf einem Stick-Konfigurationsbeispiel.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Zugriffslisten
- Routing
- Advanced Inspection and Prevention-Security Services Module (AIP-SSM) Intrusion Prevention System (IPS) - Dieses Modul ist nur bekannt, wenn das Modul installiert und betriebsbereit ist.
- IPS Software Release 5.x - Kenntnisse der IPS-Software sind nicht erforderlich, wenn das AIP-SSM nicht verwendet wird.

Verwendete Komponenten

- ASA 5510 7.2(1) und höher
- AIP-SSM-10, der IPS-Software 5.1.1 betreibt

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

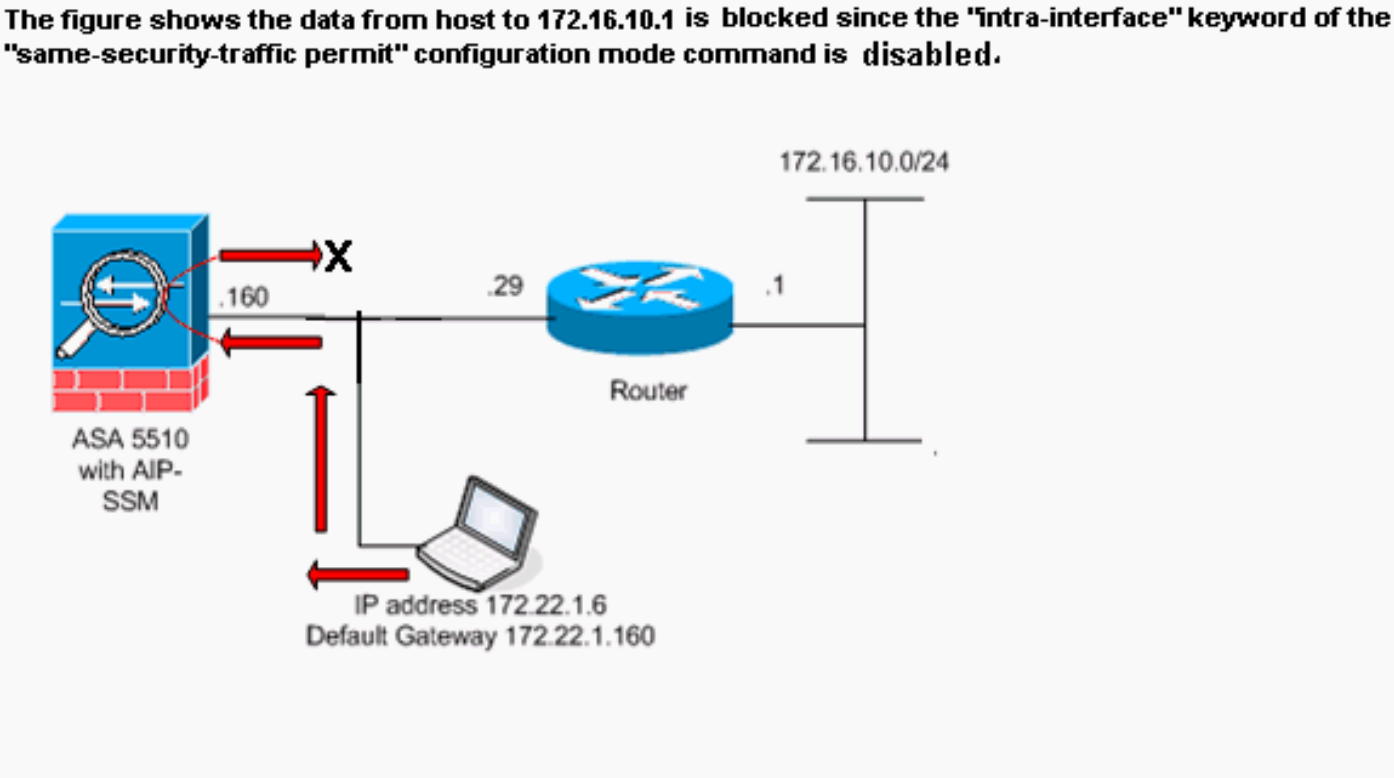
Zugehörige Produkte

Diese Konfiguration kann auch mit dem Cisco PIX der Serie 500 verwendet werden, auf dem Version 7.2(1) und höher ausgeführt werden.

Konventionen

Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Hintergrundinformationen



Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Sie sind RFC 1918 -Adressen, die in einer Laborumgebung verwendet wurden.

Diese Tabelle zeigt die ASA-Startkonfiguration:

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:
```

Fehlerbehebung

In diesen Abschnitten werden verschiedene Konfigurationsszenarien, zugehörige Syslog-Meldungen und Paket-Tracer-Ausgaben im Zusammenhang mit der Kommunikation innerhalb der Schnittstelle erläutert.

Kommunikation innerhalb der Schnittstelle nicht aktiviert

In der ASA-Konfiguration versucht Host 172.22.1.6, Host 172.16.10.1 zu pingen. Host 172.22.1.6 sendet ein ICMP-Echoanforderungspaket an das Standard-Gateway (ASA). Die Kommunikation über interne Schnittstellen wurde auf der ASA nicht aktiviert. Die ASA verwirft das Echo-Anforderungspaket. Der Test-Ping schlägt fehl. Die ASA wird zur Fehlerbehebung verwendet.

Dieses Beispiel zeigt die Ausgabe von Syslog-Meldungen und einem Paket-Tracer:

- Dies ist die im Puffer protokollierte Syslog-Meldung:

```
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)
```

- Dies ist die Pakettracer-Ausgabe:

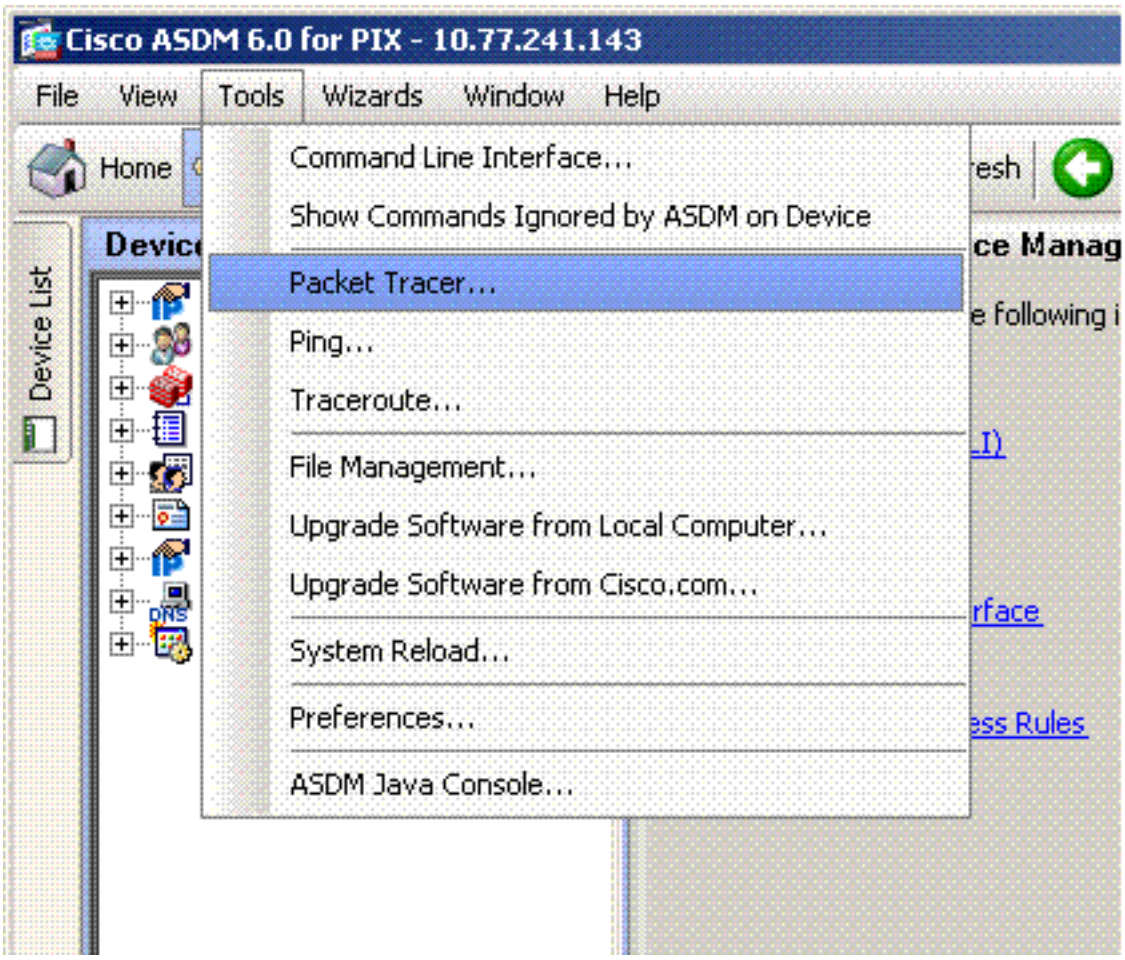
```
ciscoasa(config)#packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1 detailed
Phase: 1
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found no matching flow, creating a new flow

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

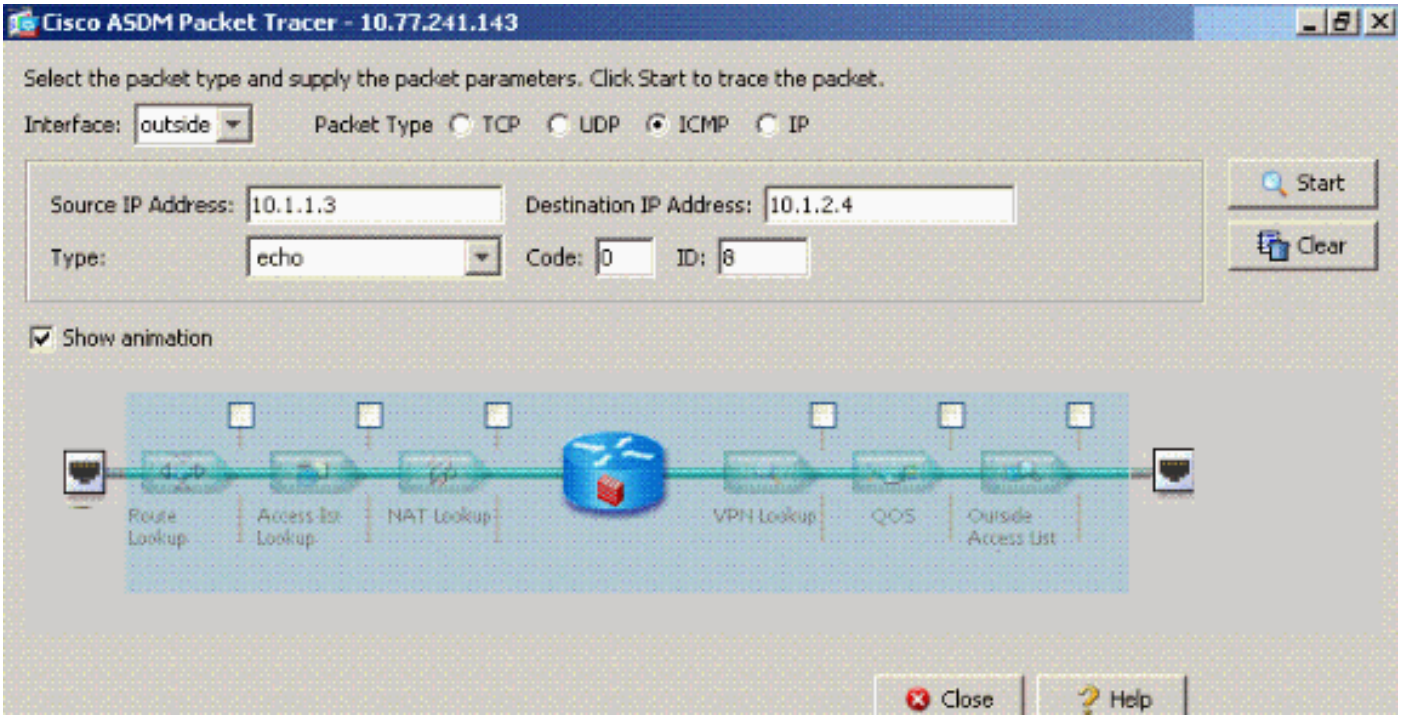
!--- Implicit rule refers to configuration rules not configured !--- by the user. By default, intra-interface communication is not permitted. !--- In this example, the user has not enabled intra-interface communications !--- and therefore the traffic is implicitly denied. Additional Information: Forward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

Die Entsprechung der CLI-Befehle in ASDM wird in den folgenden Zahlen dargestellt:

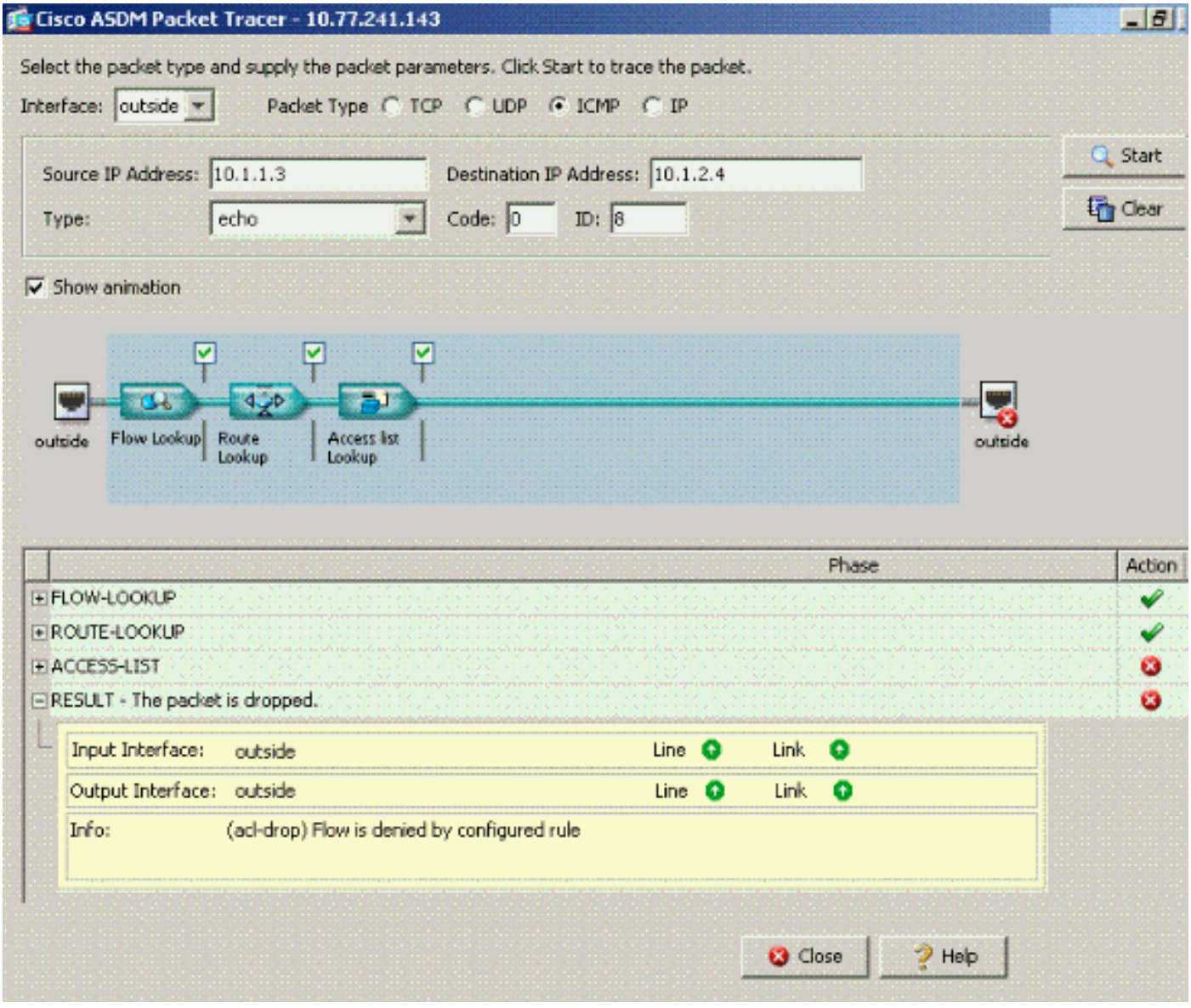
Schritt 1:



Schritt 2:



Die Packet-Tracer-Ausgabe mit deaktiviertem Befehl **für den Datenverkehr mit der gleichen** Sicherheit **(**permit intra-interface).



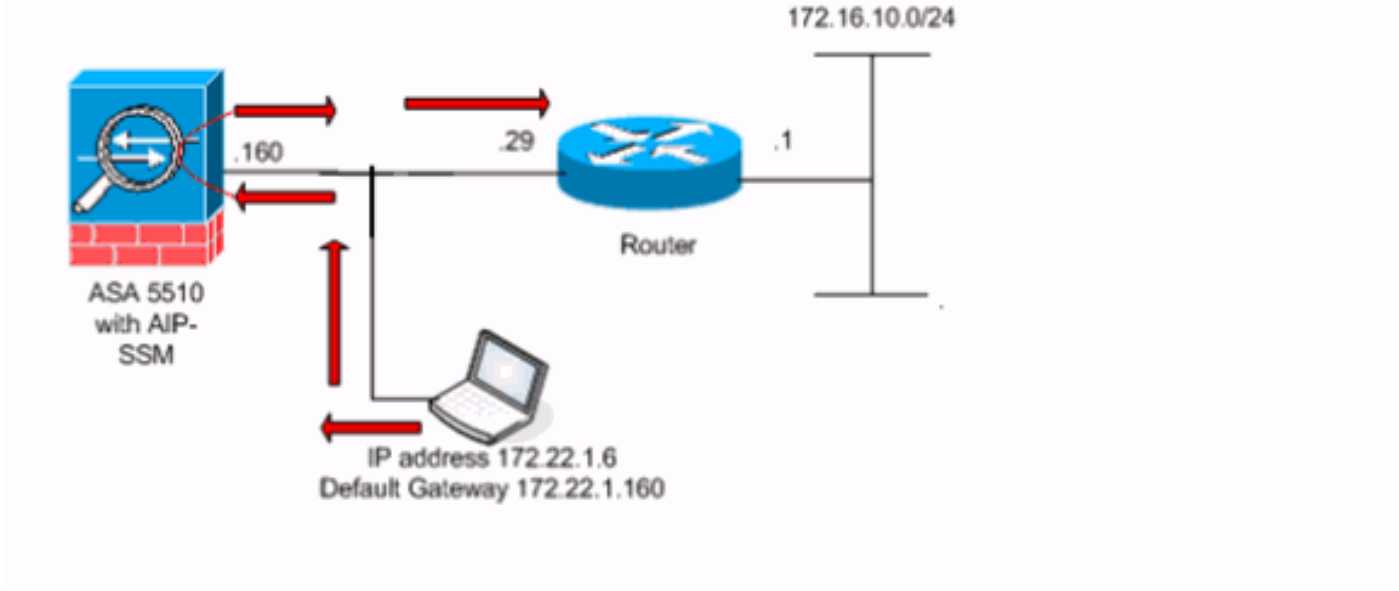
Die Packet-Tracer-Ausgabe-`Drop..implizite Regel` legt nahe, dass eine Standardkonfigurationseinstellung den Datenverkehr blockiert. Der Administrator muss die aktuelle Konfiguration überprüfen, um sicherzustellen, dass die Kommunikation innerhalb der Schnittstelle aktiviert ist. In diesem Fall muss für die ASA-Konfiguration die Kommunikation innerhalb der Schnittstelle aktiviert sein (**Intra-Interface-Zulassung für gleichen Sicherheitsdatenverkehr**).

```
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...
```

Kommunikation innerhalb der Schnittstelle aktiviert

Schnittstelleninterne Kommunikation ist jetzt aktiviert. Der Befehl **allow intra-interface (Datenverkehr zulassen, gleiche Sicherheit)** wird der vorherigen Konfiguration hinzugefügt. Host 172.22.1.6 versucht, Host 172.16.10.1 zu pingen. Host 172.22.1.6 sendet ein ICMP-Echoanforderungspaket an das Standard-Gateway (ASA). Host 172.22.1.6 zeichnet erfolgreiche Antworten von 172.16.10.1 auf. Die ASA leitet den ICMP-Datenverkehr erfolgreich weiter.

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.



Diese Beispiele zeigen die Ausgaben für ASA-Syslog-Meldungen und Paket-Tracer:

- Dies sind die im Puffer protokollierten Syslog-Meldungen:

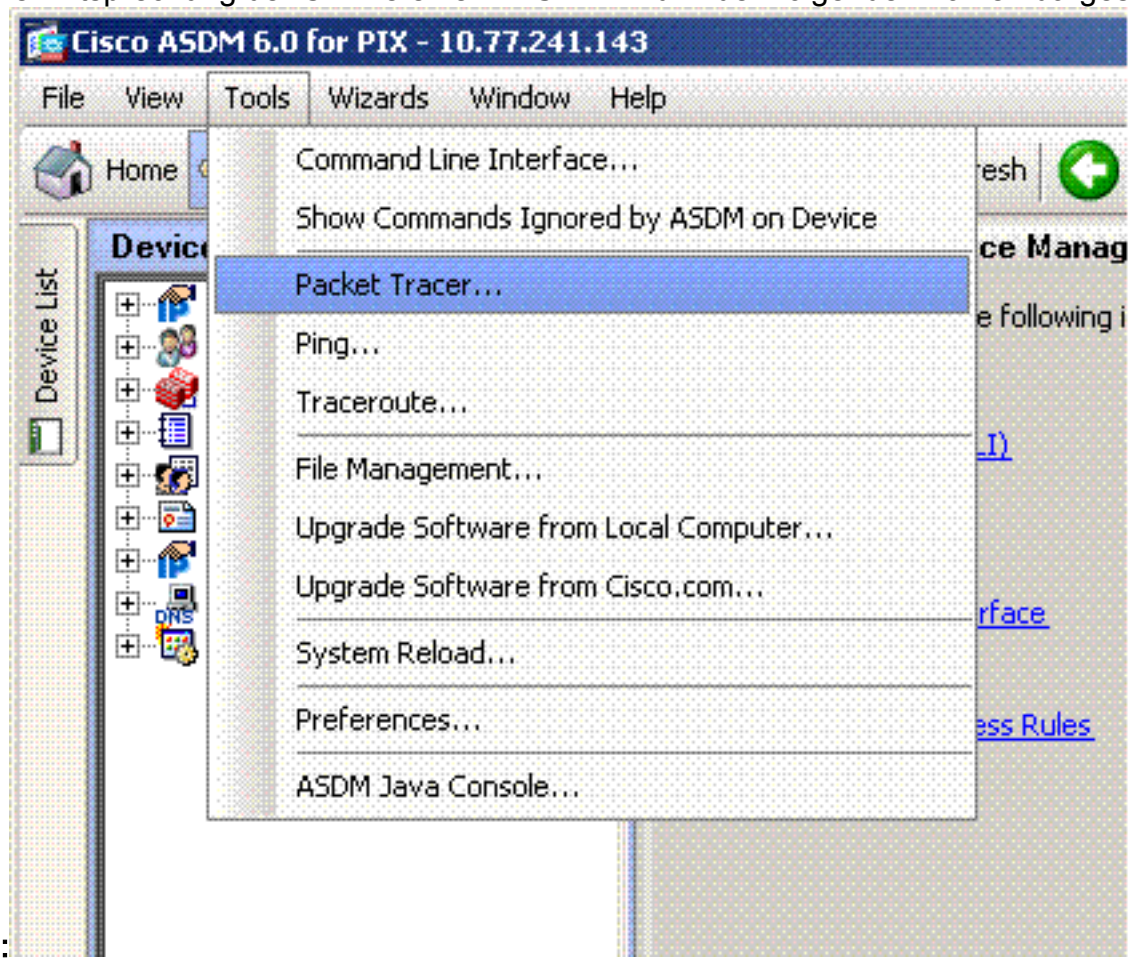
```
ciscoasa#show logging
!--- Output is suppressed. %PIX-7-609001: Built local-host outside:172.22.1.6 %PIX-7-609001:
Built local-host outside:172.16.10.1 %PIX-6-302020: Built ICMP connection for faddr
172.22.1.6/64560 gaddr 172.16.10.1/0 laddr 172.16.10.1/0 %PIX-6-302021: Teardown ICMP
connection for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

- Dies ist die Pakettracer-Ausgabe:

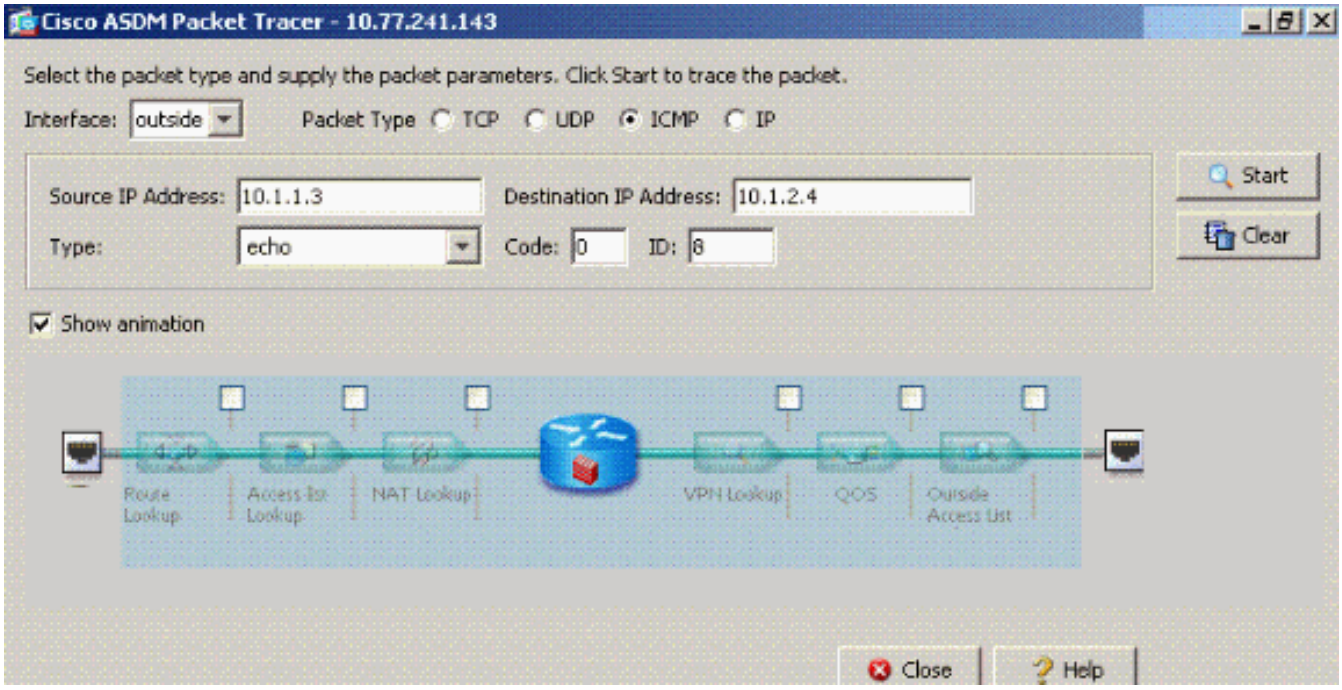
```
ciscoasa(config)#packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1

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
```

Die Entsprechung der CLI-Befehle in ASDM wird in den folgenden Zahlen dargestellt:**Schritt 1:**

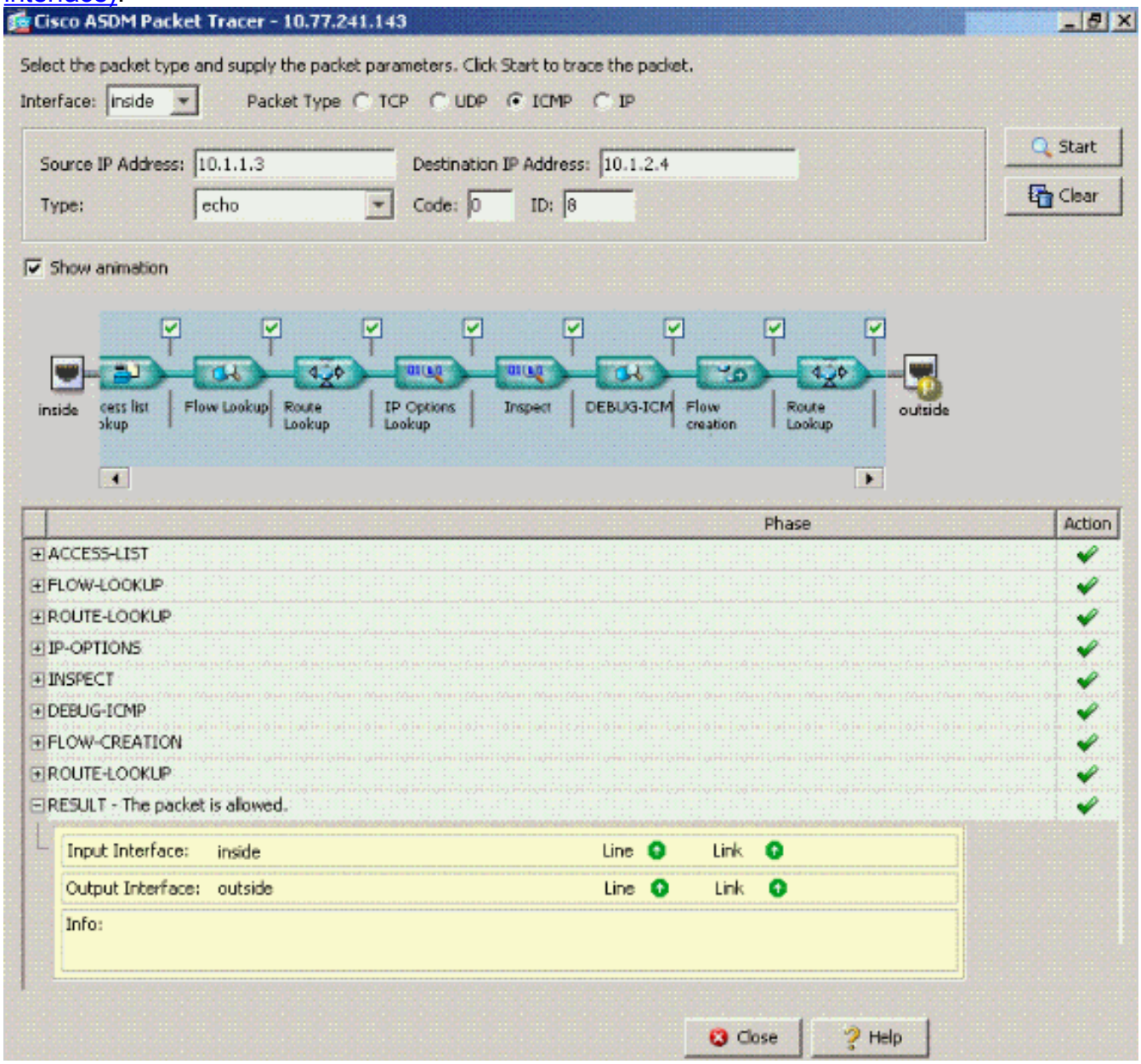


Schritt 2:



Die [Packet-Tracer-](#)Ausgabe mit dem Befehl **für den Datenverkehr mit der gleichen Sicherheitsstufe** ([allow intra-](#)

interface).



Hinweis: Auf die externe Schnittstelle wird keine Zugriffsliste angewendet. In der Beispielkonfiguration wird der externen Schnittstelle die Sicherheitsstufe 0 zugewiesen. Standardmäßig lässt die Firewall keinen Datenverkehr von einer Schnittstelle mit niedriger Sicherheit zu einer Schnittstelle mit hoher Sicherheit zu. Dies kann dazu führen, dass Administratoren glauben, dass Schnittstelleninterner Datenverkehr auf der externen Schnittstelle (Schnittstelle mit niedriger Sicherheit) ohne Genehmigung einer Zugriffsliste nicht zulässig ist. Derselbe Schnittstellenverkehr verläuft jedoch frei, wenn keine Zugriffsliste auf die Schnittstelle angewendet wird.

Intra-Interface aktiviert und Datenverkehr zur Überprüfung an AIP-SSM weitergeleitet

Schnittstelleninterner Datenverkehr kann zur Überprüfung an das AIP-SSM weitergeleitet werden. In diesem Abschnitt wird davon ausgegangen, dass der Administrator die ASA für die Weiterleitung des Datenverkehrs an das AIP-SSM konfiguriert hat und der Administrator weiß, wie die IPS 5.x-Software konfiguriert wird.

Zu diesem Zeitpunkt enthält die ASA-Konfiguration die vorherige Beispielkonfiguration, die

Kommunikation innerhalb der Schnittstelle ist aktiviert, und der gesamte (beliebige) Datenverkehr wird an das AIP-SSM weitergeleitet. Die IPS-Signatur 2004 wird geändert, um den Echo-Anforderungsverkehr zu verwerfen. Host 172.22.1.6 versucht, Host 172.16.10.1 zu pingen. Host 172.22.1.6 sendet ein ICMP-Echoanforderungspaket an das Standard-Gateway (ASA). Die ASA leitet das Echo-Anforderungspaket zur Überprüfung an den AIP-SSM weiter. Das AIP-SSM verwirft das Datenpaket pro IPS-Konfiguration.

In diesen Beispielen werden die ASA-Syslog-Meldung und die Packet-Tracer-Ausgabe angezeigt:

- Dies ist die im Puffer protokollierte Syslog-Meldung:

```
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.
```

- Dies ist die Pakettracer-Ausgabe:

```
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 ist wichtig zu beachten, dass Administratoren möglichst viele Tools zur Fehlerbehebung verwenden sollten, wenn sie ein Problem recherchieren. Dieses Beispiel zeigt, wie zwei verschiedene Tools zur Fehlerbehebung verschiedene Bilder zeichnen können. Beide Tools vermitteln gemeinsam eine vollständige Geschichte. Die ASA-Konfigurationsrichtlinie erlaubt den Datenverkehr, die IPS-Konfiguration jedoch nicht.

Intra-Interface aktiviert und auf eine Schnittstelle angewendete Zugriffslisten

In diesem Abschnitt wird die ursprüngliche Beispielkonfiguration in diesem Dokument verwendet. Schnittstelleninterne Kommunikation ist aktiviert, und auf die getestete Schnittstelle wird eine Zugriffsliste angewendet. Diese Posten werden der Konfiguration hinzugefügt. Die Zugriffsliste soll eine einfache Darstellung dessen darstellen, was auf einer Produktions-Firewall konfiguriert werden kann.

```
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 versucht, Host 172.16.10.1 zu pingen. Host 172.22.1.6 sendet ein ICMP-Echoanforderungspaket an das Standard-Gateway (ASA). Die ASA verwirft das Echo-Anforderungspaket gemäß den Zugriffslistenregeln. Der Test-Ping für den Host 172.22.1.6 ist fehlgeschlagen.

In diesen Beispielen werden die ASA-Syslog-Meldung und die Packet-Tracer-Ausgabe angezeigt:

- Dies ist die im Puffer protokollierte Syslog-Meldung:
  ```
  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]
  ```
- Dies ist die Pakettracer-Ausgabe:
  ```
  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
```

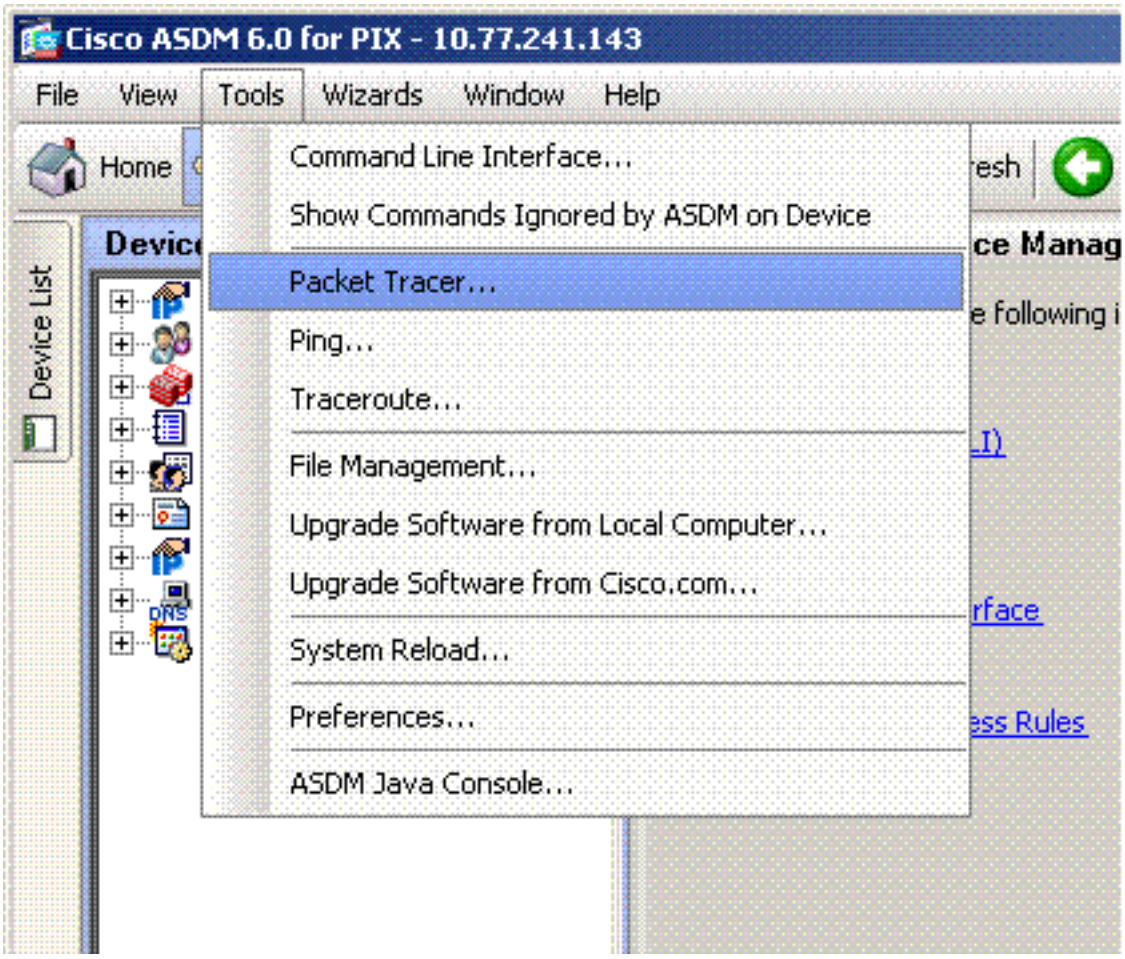
Weitere Informationen zum Befehl Packet-Tracer finden Sie unter Packet-Tracer.

Hinweis: Falls die auf die Schnittstelle angewendete Zugriffsliste eine deny-Anweisung enthält, ändert sich die Ausgabe der Paket-Tracer. Beispiel:

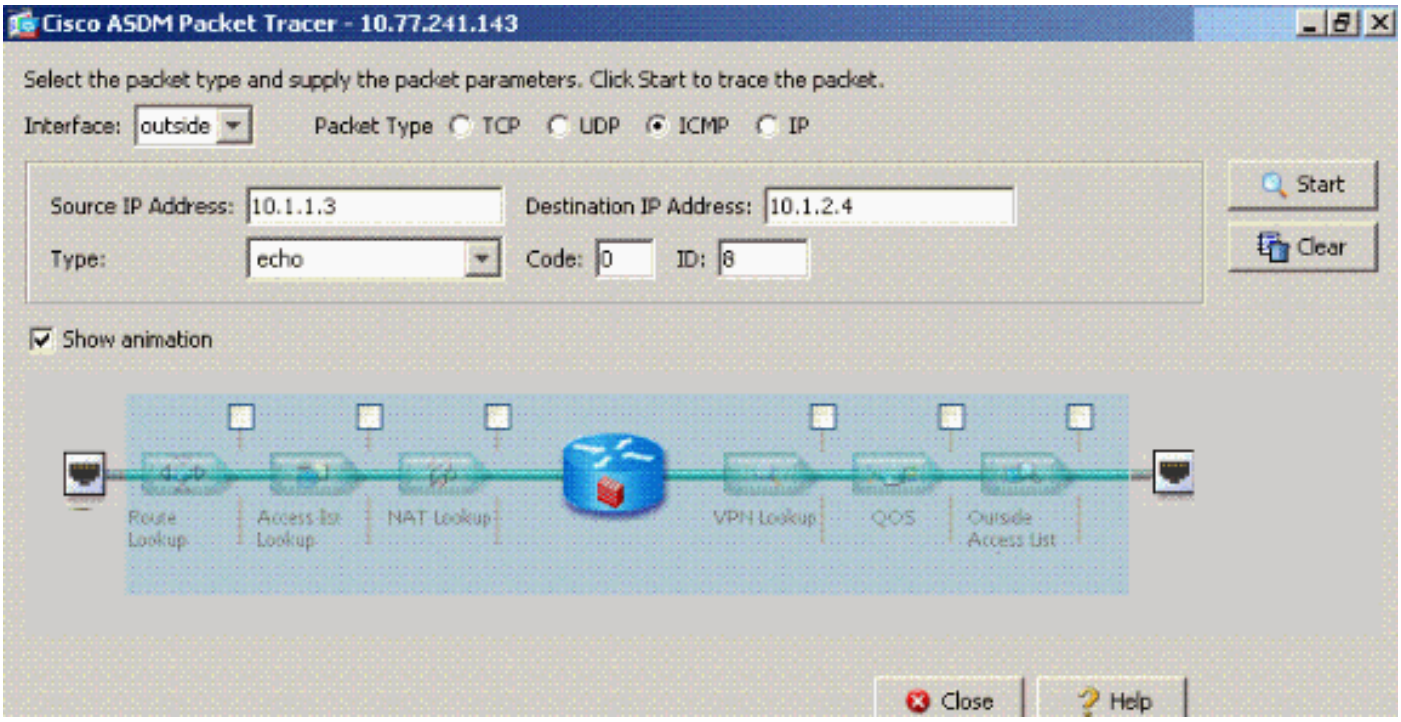
```
ciscoasa(config)#access-list outside_acl permit tcp any host 172.22.1.147 eq 80
ciscoasa(config)#access-list outside_acl deny ip any any
ciscoasa(config)#access-group outside_acl in interface outside
ciscoasa#packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1 detailed
!--- Output is suppressed.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

Die Entsprechung der obigen CLI-Befehle in ASDM wird in den folgenden Zahlen dargestellt:

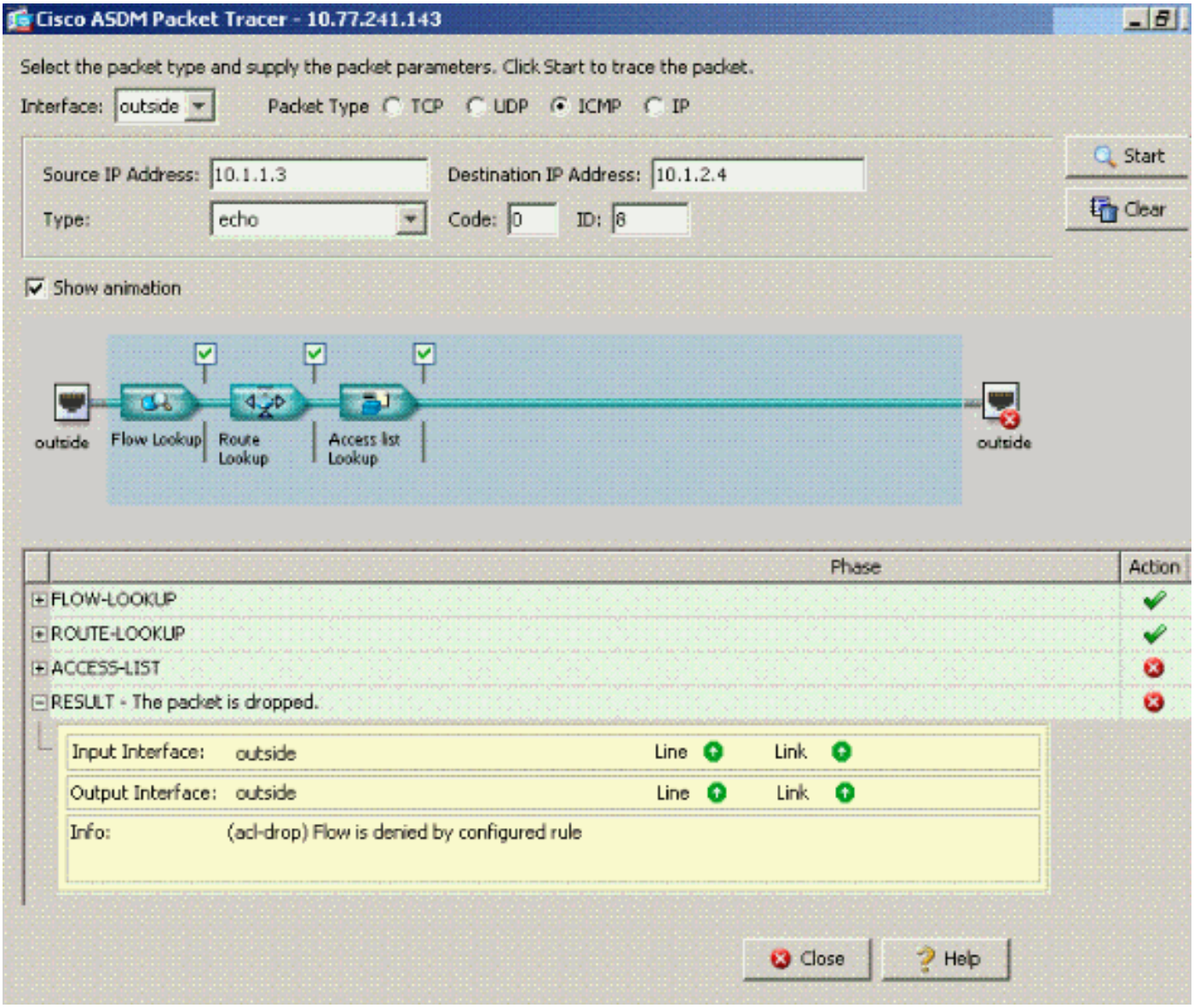
Schritt 1:



Schritt 2:



Die Pakettracer-Ausgabe mit aktiviertem Befehl **für** den **Datenverkehr mit der gleichen** Sicherheit (**allow intra-interface)** und die **Zugriffsliste "outside_acl" erweitert deny ip any** command, um Pakete zu verweigern.

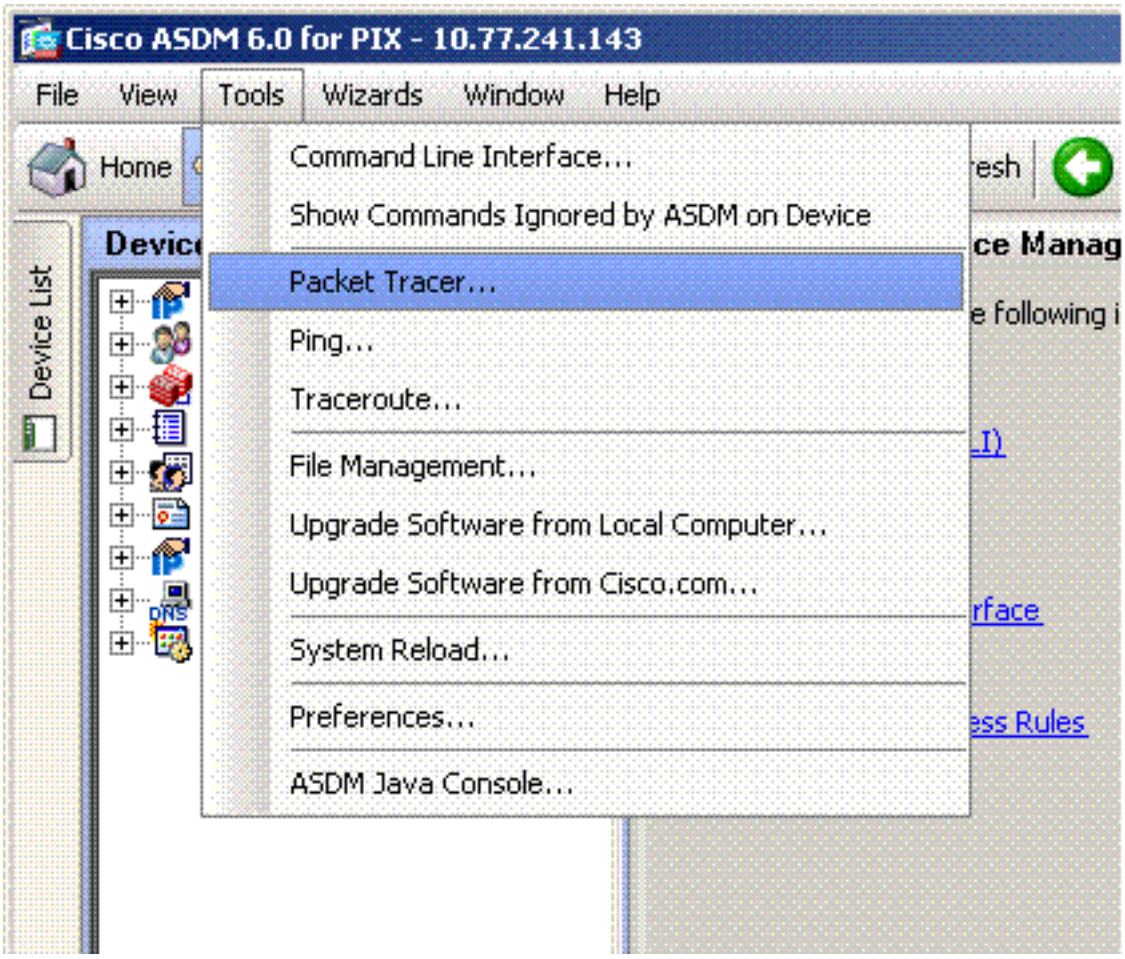


Wenn Schnittstelleninterne Kommunikation über eine bestimmte Schnittstelle gewünscht wird und Zugriffslisten auf dieselbe Schnittstelle angewendet werden, müssen die Zugriffslistenregeln den Schnittstelleninternen Datenverkehr zulassen. Bei Verwendung der Beispiele in diesem Abschnitt muss die Zugriffsliste wie folgt geschrieben werden:

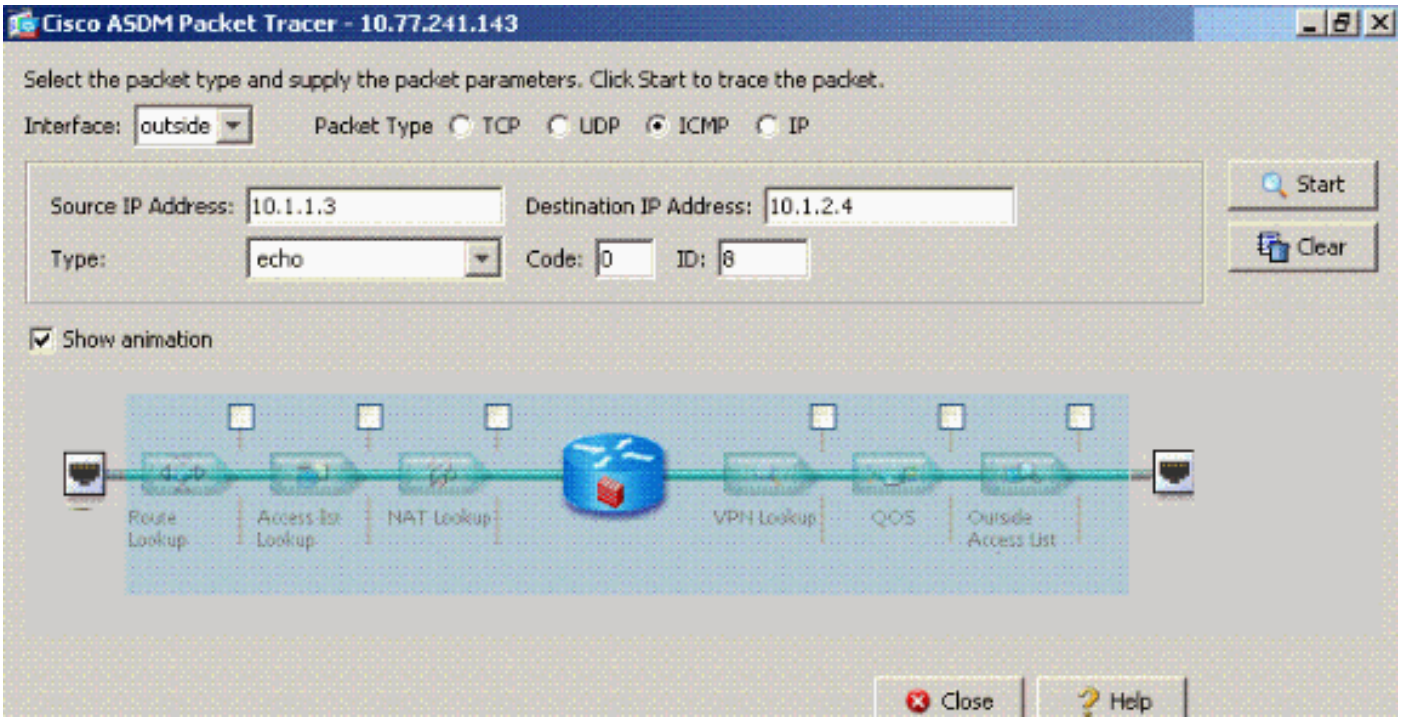
```
ciscoasa(config)#access-list outside_acl permit tcp any host 172.22.1.147 eq 80
ciscoasa(config)#access-list outside_acl permit ip 172.22.1.0 255.255.255.0 172.16.10.0
255.255.255.0
!--- 172.22.1.0 255.255.255.0 represents a locally !--- connected network on the ASA. !---
172.16.10.0 255.255.255.0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

Die Entsprechung der obigen CLI-Befehle in ASDM wird in den folgenden Zahlen dargestellt:

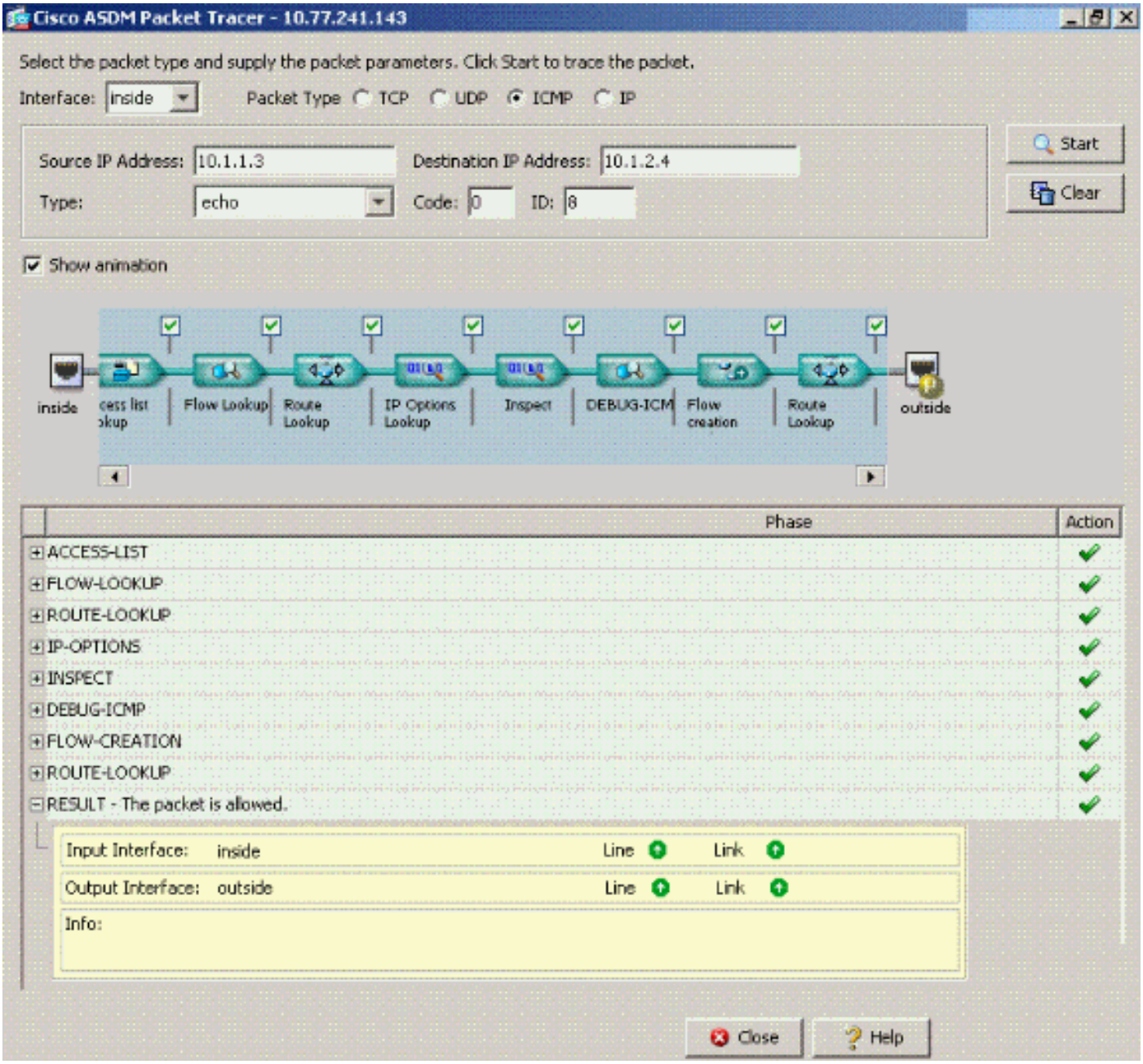
Schritt 1:



Schritt 2:



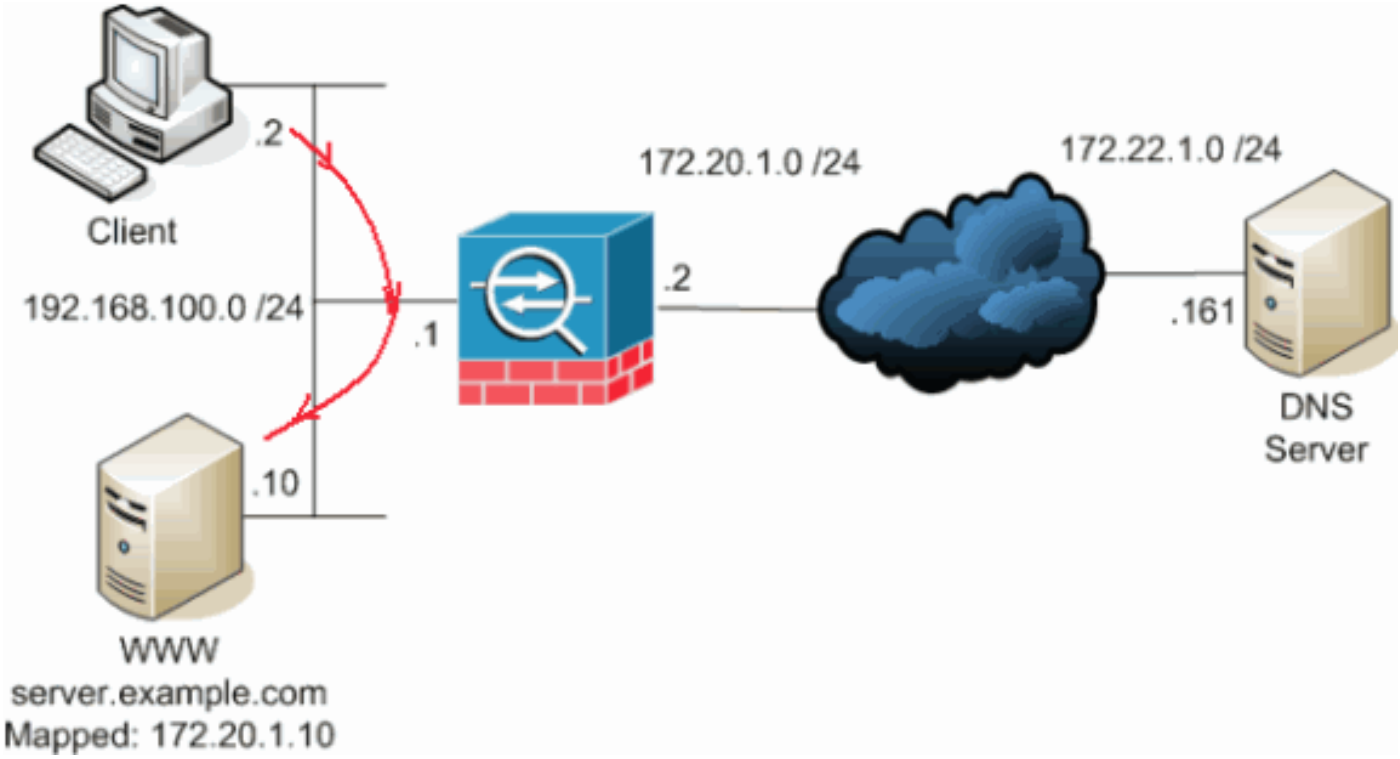
Die Pakettracer-Ausgabe mit aktiviertem Befehl **für** den **Datenverkehr mit der gleichen Sicherheit (allow intra-interface) und die Zugriffsliste "outside_acl" erweitert deny ip any any** command, die auf derselben Schnittstelle konfiguriert sind, auf der der Datenverkehr innerhalb der Schnittstelle gewünscht wird.



Weitere Informationen zu den Befehlen für die **Zugriffsliste** und die **Zugriffsgruppe** finden Sie unter Erweiterte Zugriffslisten- und Zugriffsgruppen-Zugriffslisten.

Interne Schnittstelle mit statischer und NAT-Funktion

In diesem Abschnitt wird ein Szenario erläutert, in dem ein interner Benutzer versucht, mit seiner öffentlichen Adresse auf den internen Webserver zuzugreifen.



In diesem Fall möchte der Client unter 192.168.100.2 die öffentliche Adresse des WWW-Servers verwenden (z. B. 172.20.1.10). Die DNS-Dienste für den Client werden vom externen DNS-Server unter 172.22.1.161 bereitgestellt. Da sich der DNS-Server in einem anderen öffentlichen Netzwerk befindet, kennt er die private IP-Adresse des WWW-Servers nicht. Stattdessen kennt der DNS-Server die WWW-Server-zugeordnete Adresse 172.20.1.10.

Hier muss dieser Datenverkehr von der internen Schnittstelle übersetzt und über die interne Schnittstelle umgeleitet werden, um den WWW-Server zu erreichen. Das nennt man Hairpinning. Dies kann mithilfe der folgenden Befehle durchgeführt werden:

```
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
```

Vollständige Konfigurationsdetails und weitere Informationen über Hairpinning finden Sie unter Hairpinning with Intra-Interface Communication.

Weiterleiten von Zugriffslisten

Nicht alle Firewall-Zugriffsrichtlinien sind identisch. Einige Zugriffsrichtlinien sind spezifischerer als andere. Wenn die Kommunikation innerhalb der Schnittstelle aktiviert ist und für die Firewall keine Zugriffsliste auf alle Schnittstellen angewendet wurde, empfiehlt es sich möglicherweise, eine Zugriffsliste hinzuzufügen, wenn die Kommunikation innerhalb der Schnittstelle aktiviert ist. Die angewendete Zugriffsliste muss die Kommunikation innerhalb der Schnittstelle sowie andere Anforderungen an die Zugriffsrichtlinien zulassen.

Dieses Beispiel veranschaulicht diesen Punkt. Die ASA verbindet ein privates Netzwerk (interne Schnittstelle) mit dem Internet (externe Schnittstelle). Auf die interne ASA-Schnittstelle wird keine Zugriffsliste angewendet. Standardmäßig ist der gesamte IP-Datenverkehr von innen nach außen zulässig. Es wird vorgeschlagen, eine Zugriffsliste hinzuzufügen, die etwa der folgenden Ausgabe

entspricht:

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

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

Diese Zugriffslisten erlauben weiterhin den gesamten IP-Datenverkehr. Die spezifischen Zugriffslisten für die Kommunikation innerhalb der Schnittstelle erinnern Administratoren daran, dass die Kommunikation innerhalb der Schnittstelle von einer angewendeten Zugriffsliste zugelassen werden muss.

Zugehörige Informationen

- Cisco Security Appliance Command Reference, Version 7.2
- Systemprotokollmeldungen der Cisco Security Appliance, Version 7.2
- Cisco PIX Firewall-Software
- ASA: Netzwerkverkehr von der ASA an das AIP SSM-Konfigurationsbeispiel senden
- Produkt-Support für Cisco Adaptive Security Appliances der Serie ASA 5500
- Technischer Support und Dokumentation - Cisco Systems