PIX/ASA 7.2(1) 以降：インターフェイス内通信

内容

概要

このドキュメントは、Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）やソフトウェア リリース 7.2(1) 以降で稼働している PIX でインターフェイス内通信をイネーブルにした場合に発生する、一般的な問題のトラブルシューティングに役立ちます。ソフトウェア リリース 7.2(1) には、同じインターフェイスでクリア テキスト データをルーティングする機能があります。この機能をイネーブルにするには、**same-security-traffic permit intra-interface** コマンドを入力します。このドキュメントでは、すでにネットワーク管理者によってこの機能がイネーブルにされているか、将来イネーブルにする予定であるものと想定しています。設定やトラブルシューティングには、コマンドライン インターフェイス（CLI）を使用します。

注：このドキュメントでは、ASAに到着してASAから送信されるクリアデータ（暗号化なし）に焦点を当てます。暗号化されたデータは対象としていません。

IPsec 用の ASA/PIX の設定でインターフェイス内通信をイネーブルにするには、『パブリック インターネット VPN on a Stick のための PIX/ASA および VPN Client の設定例』を参照してください。

SSL 用の ASA の設定でインターフェイス内通信をイネーブルにするには、『ASA 7.2(2)：パブリック インターネット VPN on a Stick のための SSL VPN Client（SVC）の設定例』を参照してください。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- アクセス リスト
- ルーティング
- AIP-SSM（Advanced Inspection and Prevention-Security Services Module）IPS（Intrusion Prevention System）：このモジュールがインストールされていて稼働している場合にのみ、このモジュールについての知識が必要となります。
- IPSソフトウェアリリース5.x:AIP-SSMが使用されていない場合、IPSソフトウェアに関する知識は必要ありません。

使用するコンポーネント

- ASA 5510 7.2(1) 以降
- IPS ソフトウェア 5.1.1 が稼働している AIP-SSM-10

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

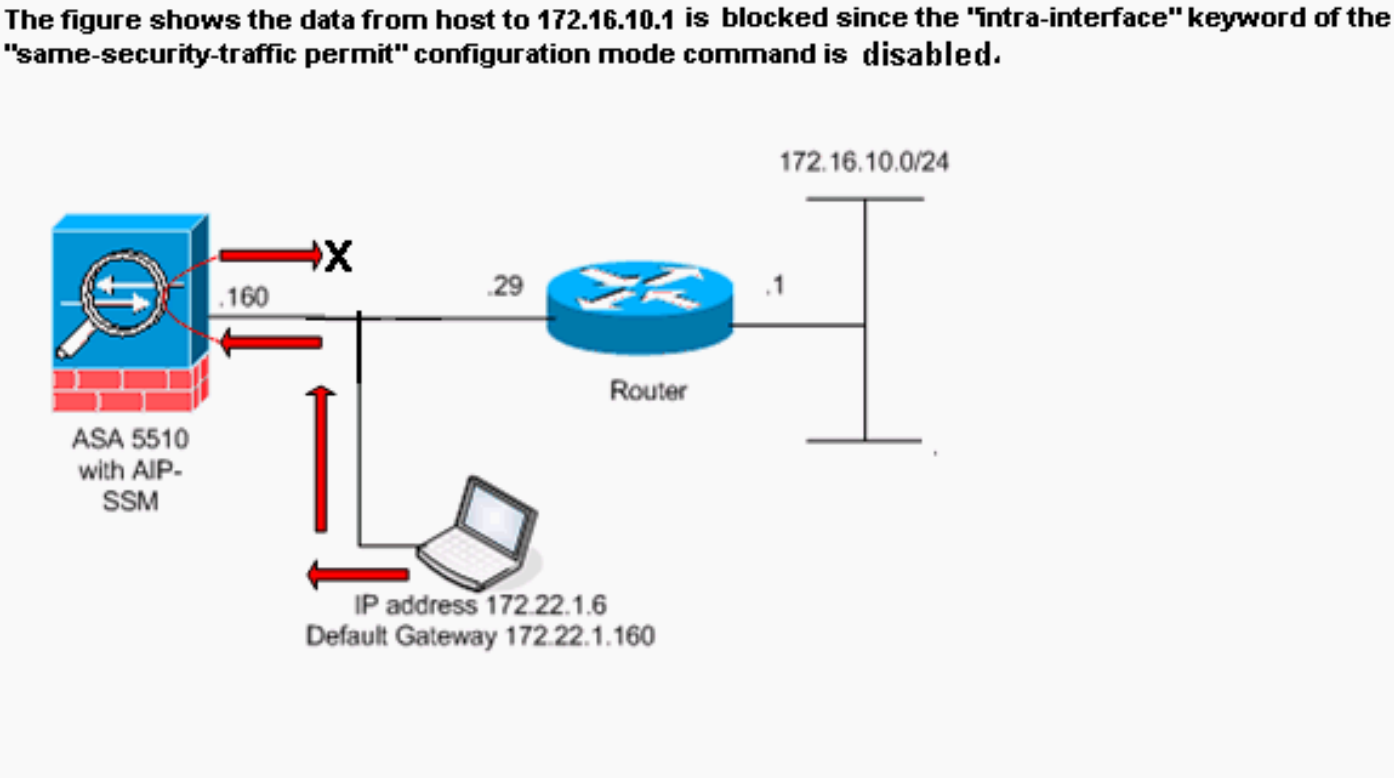
関連製品

この設定は、バージョン 7.2(1) 以降が稼働する Cisco 500 シリーズ PIX にも適用できます。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明



注：この設定で使用されるIPアドレッシング方式は、インターネット上で正式にルーティング可能なものではありません。これらは RFC 1918 で使用されているアドレスであり、ラボ環境で使用されたものです。

この表は、ASA の開始設定を示しています。

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:
```

トラブルシューティング

ここからのセクションでは、インターフェイス内通信に関連する、いくつかの設定シナリオ、関連 syslog メッセージ、およびパケットトレーサの出力を説明しています。

インターフェイス内通信がイネーブルになっていない

ASA設定で、ホスト172.22.1.6はホスト172.16.10.1へのpingを試みます。ホスト172.22.1.6はICMPエコー要求パケットをデフォルトゲートウェイ(ASA)に送信します。 ASA ではインターフェイス内通信がイネーブルになっていません。ASA ではエコー要求パケットがドロップされます。テスト ping が失敗します。ASA を使用して、問題のトラブルシューティング行います。

次の例には、syslog メッセージとパケットトレーサの出力が示されています。

- バッファには次の syslog メッセージが記録されています。

```
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)
```

- パケットトレーサの出力は次のようになっています。

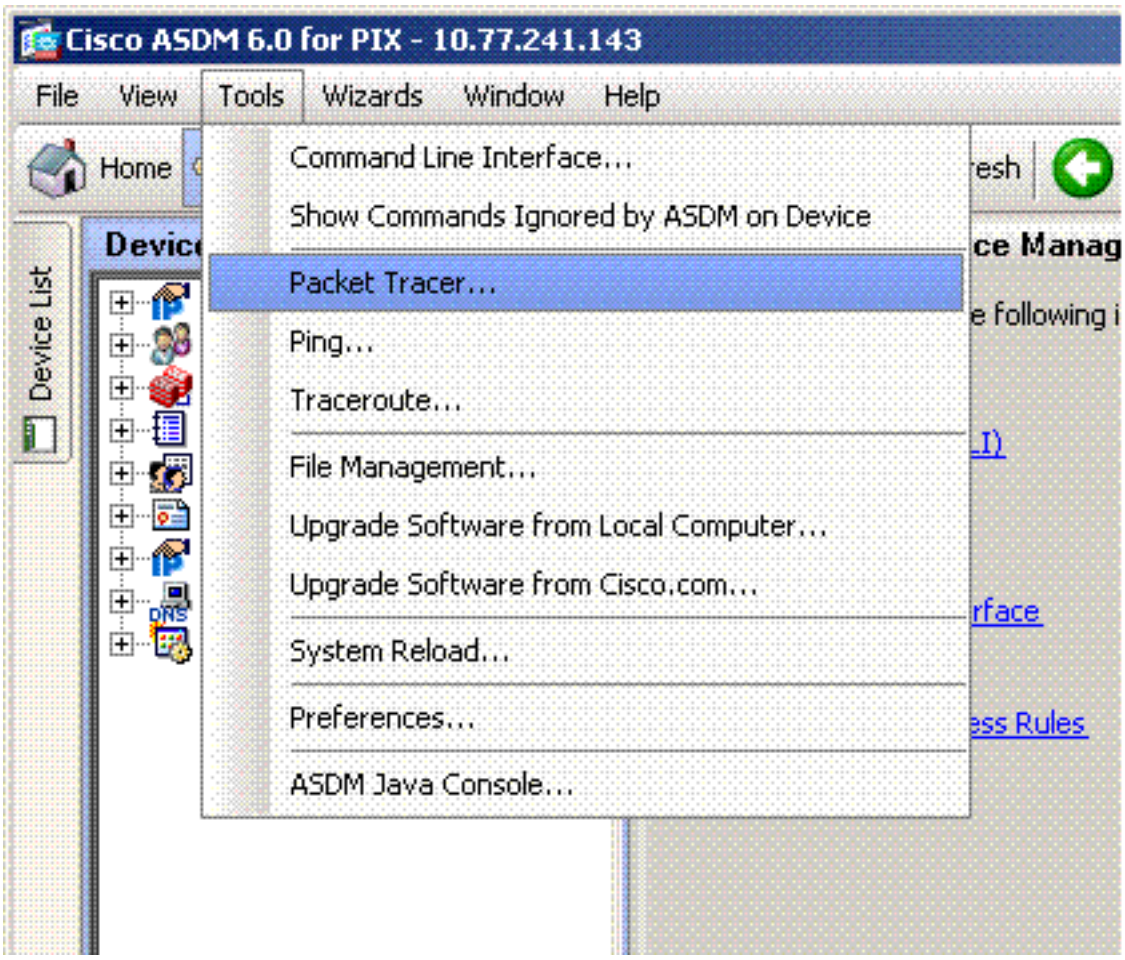
```
ciscoasa(config)#packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1 detailed
Phase: 1
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found no matching flow, creating a new flow

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

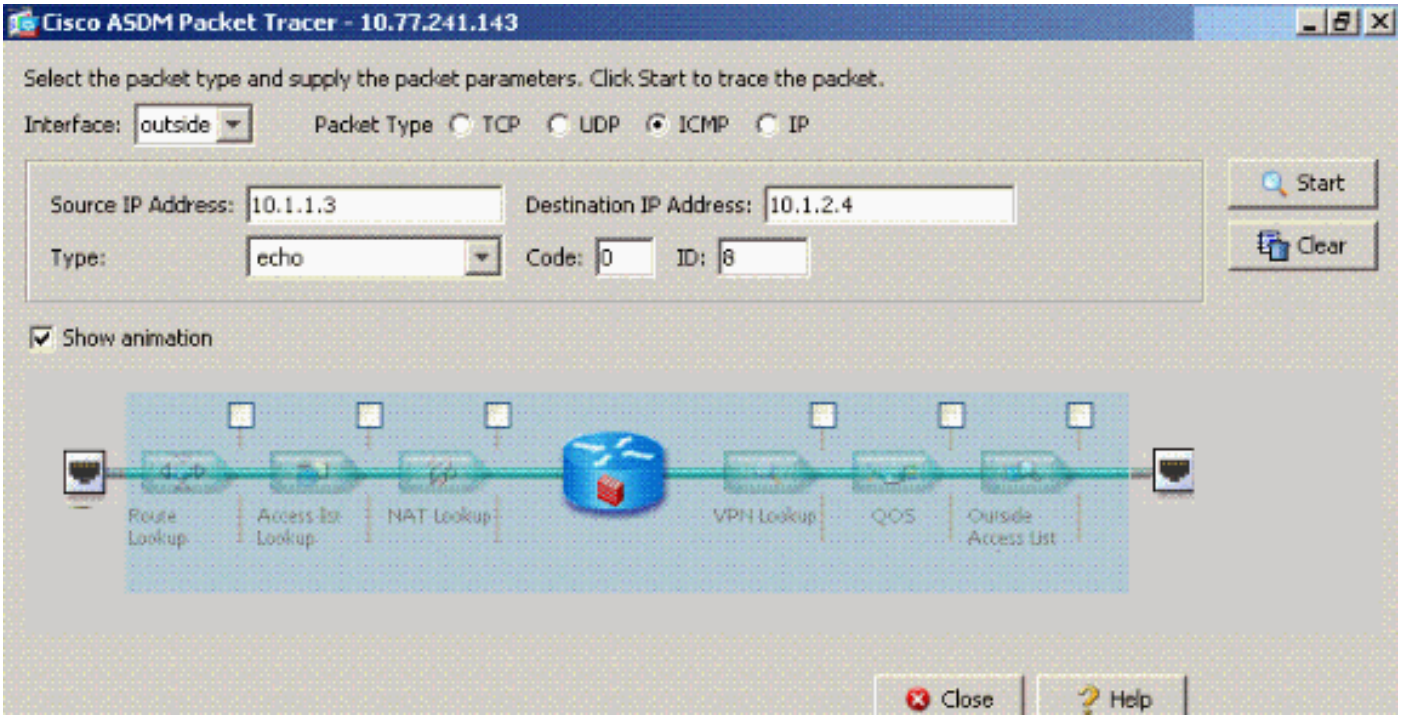
!--- Implicit rule refers to configuration rules not configured !--- by the user. By default, intra-interface communication is not permitted. !--- In this example, the user has not enabled intra-interface communications !--- and therefore the traffic is implicitly denied. Additional Information: Forward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

次の図には、ASDM での CLI コマンドと同等の操作が示されています。

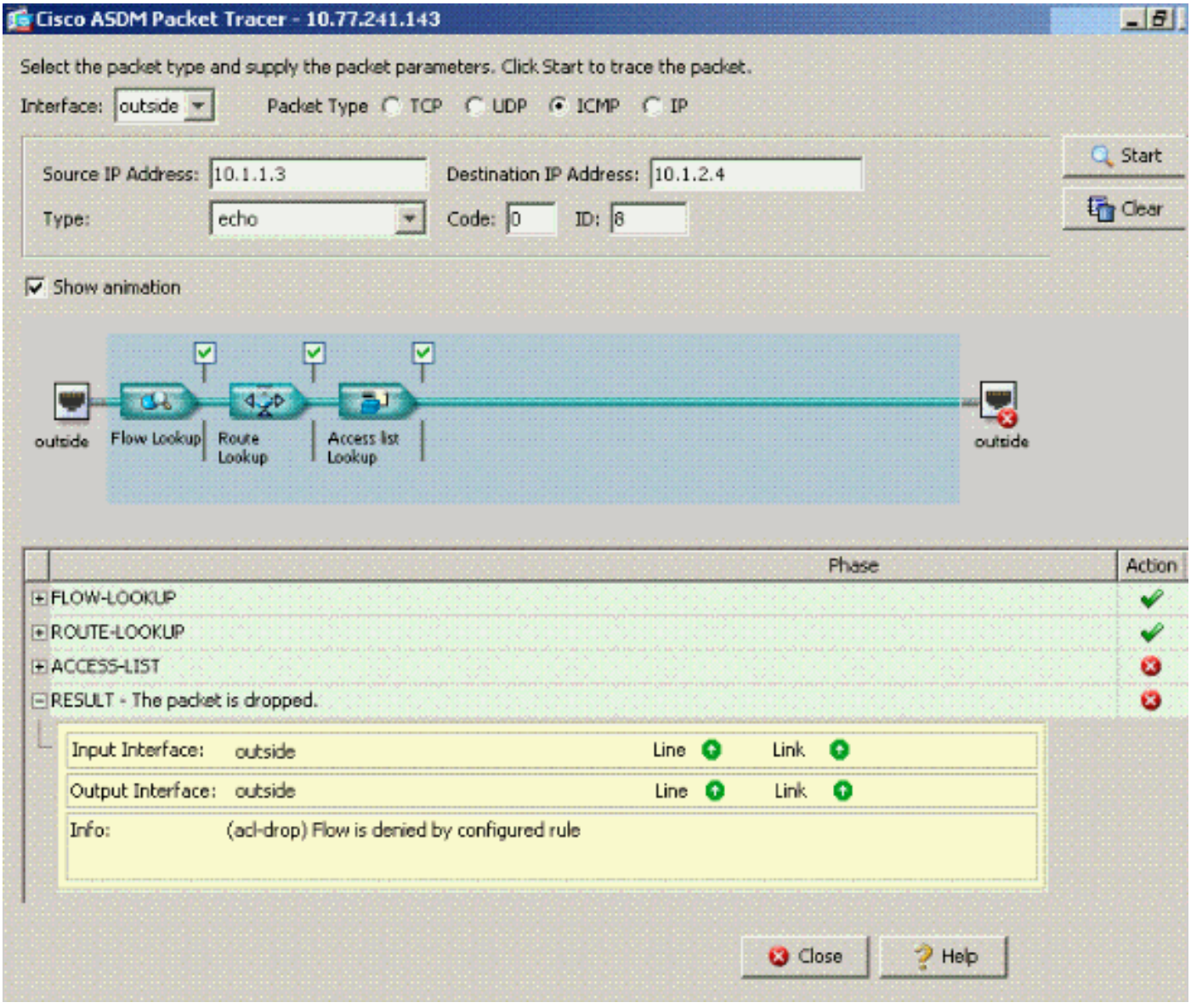
ステップ 1：



ステップ 2：



same-security-traffic permit intra-interface コマンドがディセーブルになっているパケットトレーサの出力。



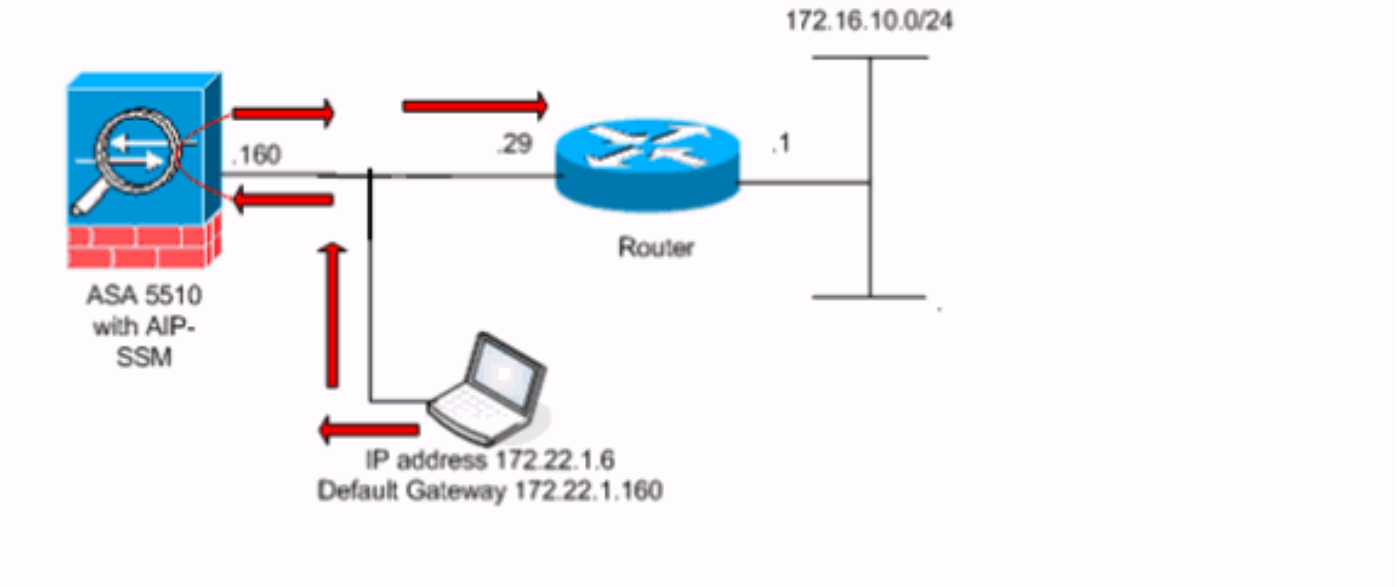
パケットトレーサの出力…は、デフォルトの構成設定がトラフィックをブロックしていることを示しています。管理者は、稼働中の設定を調べて、インターフェイス内通信がイネーブルになっていることを確認する必要があります。この場合、ASA 設定でインターフェイス内通信を有効にする必要があります（same-security-traffic permit intra-interface コマンド）。

```
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...
```

インターフェイス内通信がイネーブルになっている

現在、インターフェイス内通信がイネーブルになっています。以前の設定に same-security-traffic permit intra-interface コマンドを追加します。ホスト172.22.1.6はホスト172.16.10.1へのpingを試みます。ホスト172.22.1.6はICMPエコー要求パケットをデフォルトゲートウェイ(ASA)に送信します。 ホスト172.22.1.6は、172.16.10.1からの正常な応答を記録します。ASAはICMPトラフィックを正常に渡します。

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.



次の例には、ASA の syslog メッセージとパケットトレーサ出力が示されています。

- バッファには次の syslog メッセージが記録されています。

```
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
```

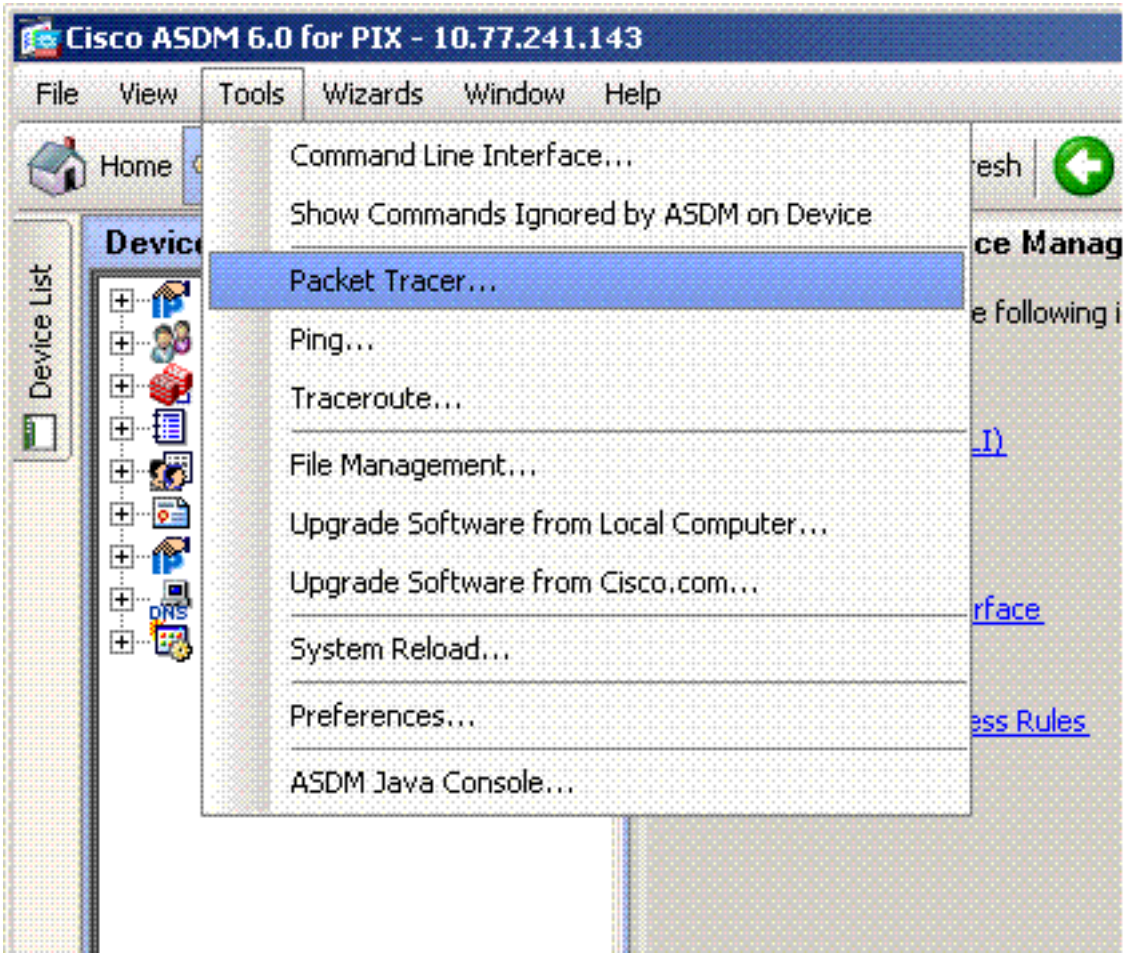
- パケットトレーサの出力は次のようになっています。

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

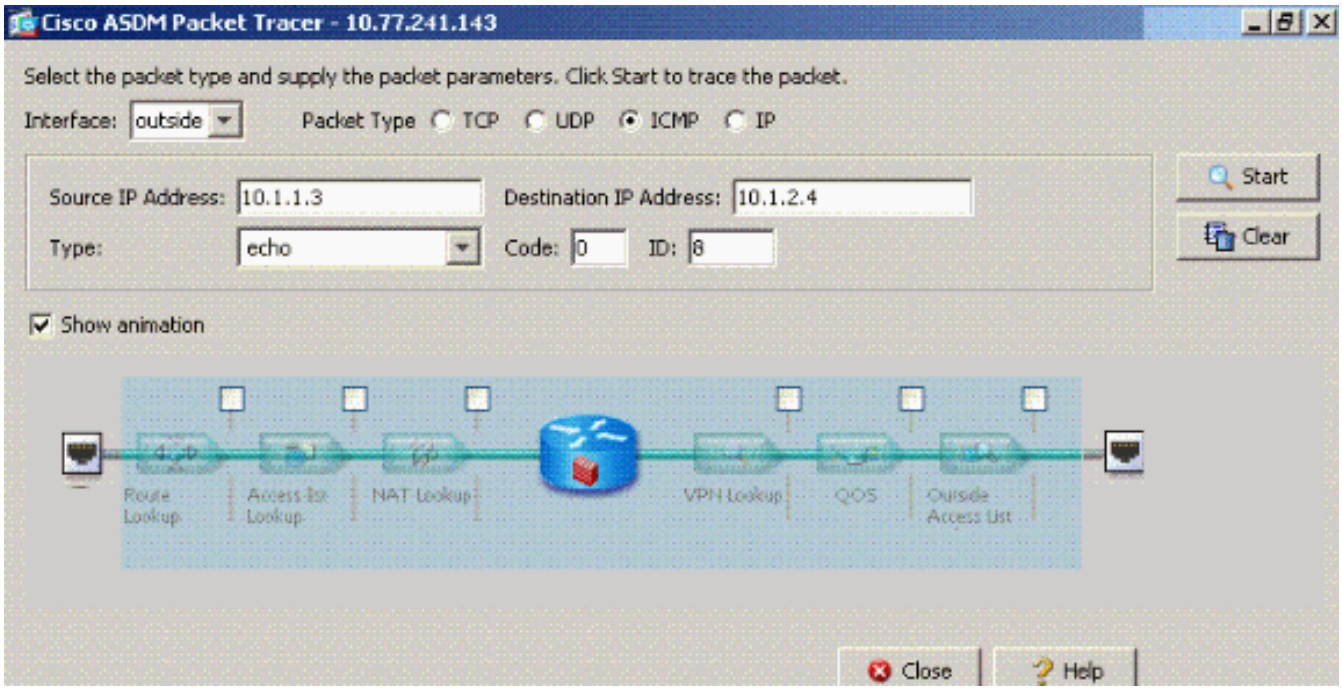
```
Phase: 1
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found no matching flow, creating a new flow

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
```

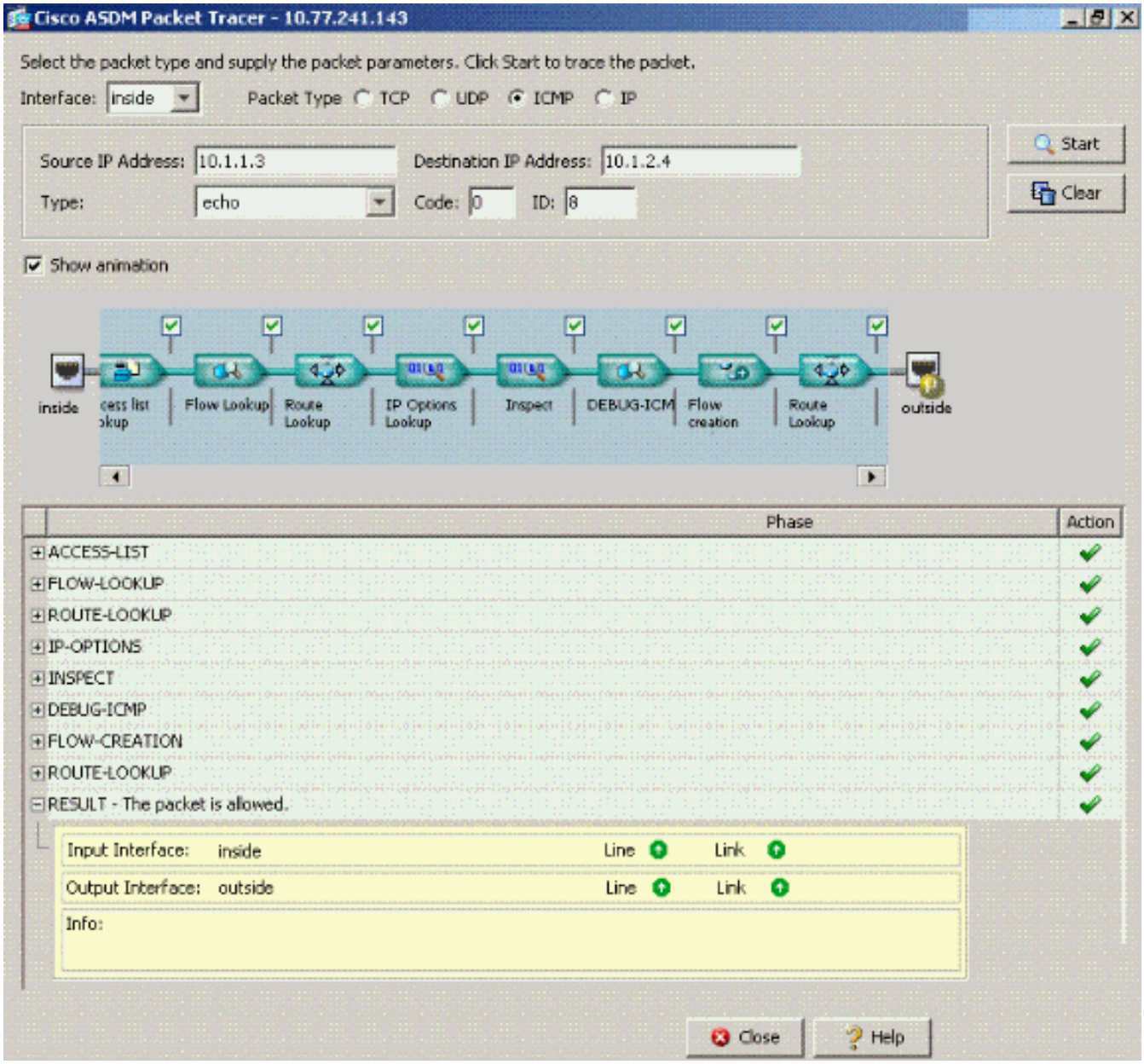
次の図には、ASDM での CLI コマンドと同等の操作が示されています。**ステップ 1：**



ステップ 2：



same-security-traffic permit intra-interface コマンドがイネーブルになっているパケットトレーサの出力。



注：外部インターフェイスにはアクセスリストは適用されません。設定例では、Outside インターフェイスにはセキュリティ レベル 0 が割り当てられています。デフォルトでは、低セキュリティ インターフェイスから高セキュリティ インターフェイスへのトラフィックは、ファイアウォールでは許可されません。このため管理者は、外部（低セキュリティの）インターフェイスではアクセスリストによる許可がないと、インターフェイス内のトラフィックは許可されないと思い込んでしまう可能性があります。ところが、インターフェイスに適用されるアクセスリストがない場合は、同じインターフェイス トラフィックが制限なく渡されます。

インターフェイス内通信がイネーブルになっていてトラフィックは AIP-SSM に渡されて検査される

インターフェイス内トラフィックを検査のために AIP-SSM に渡すことができます。このセクションでは、ASA がトラフィックを AIP-SSM に転送するように管理者によって設定されていることと、管理者に IPS 5.x ソフトウェアの設定方法についての知識があることを前提としています。

この時点では、ASA 設定には以前のサンプル設定が含まれていて、インターフェイス内通信はイネーブルになっており、すべてのトラフィックが AIP-SSM に転送されます。IPS シグニチャ

2004 は、エコー要求トラフィックをドロップするように変更されています。ホスト172.22.1.6はホスト172.16.10.1へのpingを試みます。ホスト172.22.1.6はICMPエコー要求パケットをデフォルトゲートウェイ(ASA)に送信します。 ASA によってエコー要求パケットが AIP-SSM に転送されて検査されます。AIP-SSM では IPS 設定によってデータ パケットをドロップします。

次の例には、ASA の syslog メッセージとパケットトレーサ出力が示されています。

- バッファには次の syslog メッセージが記録されています。

```
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.
```

- パケットトレーサの出力は次のようになっています。

```
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.
```

問題を調査する際には、管理者ができるだけ多くのトラブルシューティング ツールを使用することが重要です。この例では、2 種類の異なるトラブルシューティング ツールを使用した場合の違いを示しています。どちらのツールでも、筋書きが欠落なく報告されています。ASA 設定ポリシーではトラフィックが許可されていますが、IPS 設定では許可されていません。

インターフェイス内通信がイネーブルになっていてインターフェイスにアクセスリストが適用される

このセクションでは、このドキュメント内独自のサンプル設定を使用しています。インターフェイス内通信はイネーブルになっており、テスト済みのインターフェイスにアクセスリストが適用されています。次に示す行が設定に追加されます。アクセスリストは、実稼働中のファイアウォールで設定されている可能性のあるもの簡潔に表現するようになっています。

```
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.
```

ホスト172.22.1.6はホスト172.16.10.1へのpingを試みます。ホスト172.22.1.6はICMPエコー要求パケットをデフォルトゲートウェイ(ASA)に送信します。 ASA では、アクセスリスト ルールによってエコー要求パケットがドロップされます。ホスト 172.22.1.6 のテスト ping が失敗します。

次の例には、ASA の syslog メッセージとパケットトレーサ出力が示されています。

- バッファには次の syslog メッセージが記録されています。

```
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]
```

- パケットトレーサの出力は次のようになっています。

```
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
```

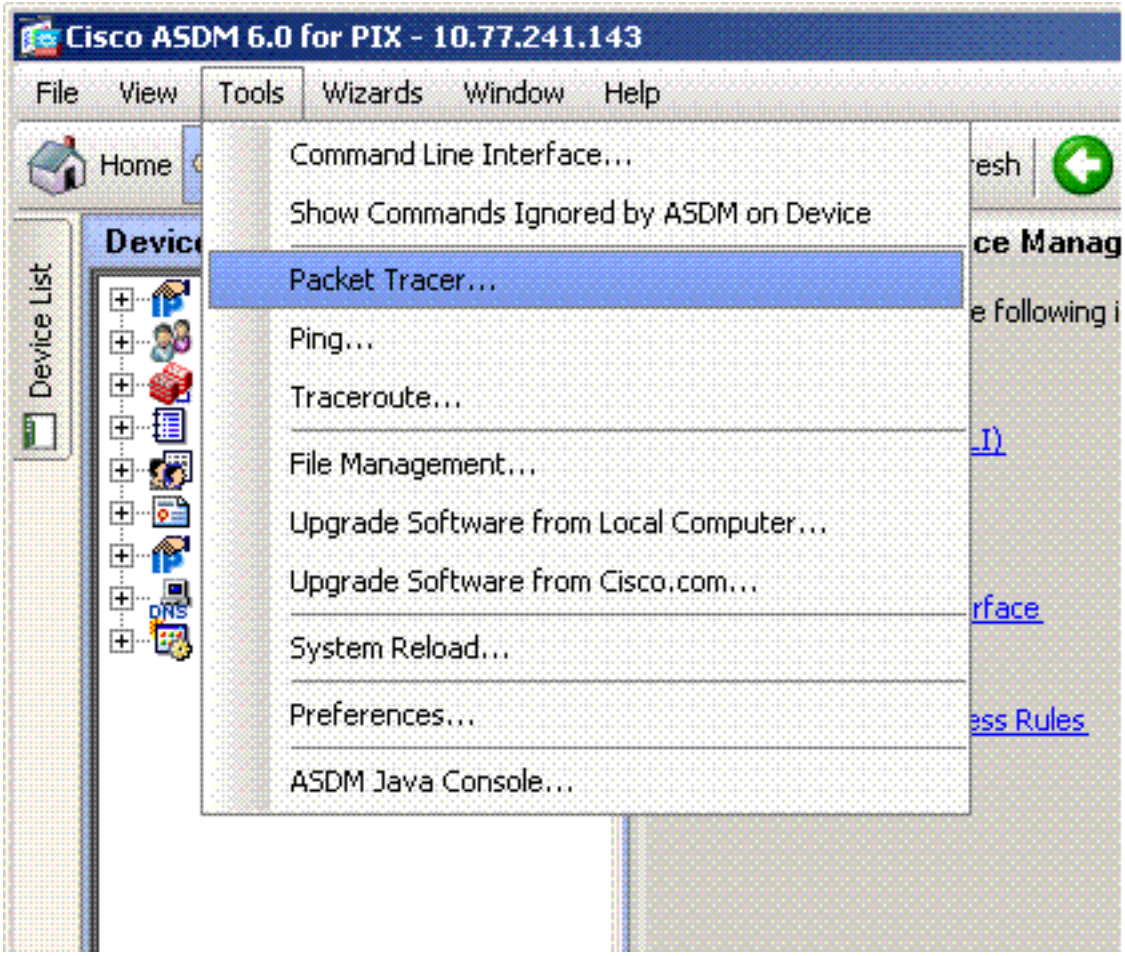
パケットトレーサのコマンドについての詳細は、『パケットトレーサ』を参照してください。

注：インターフェイスに適用されるアクセスリストにdeny文が含まれている場合、パケットトレーサの出力が変更されます。以下に、いくつかの例を示します。

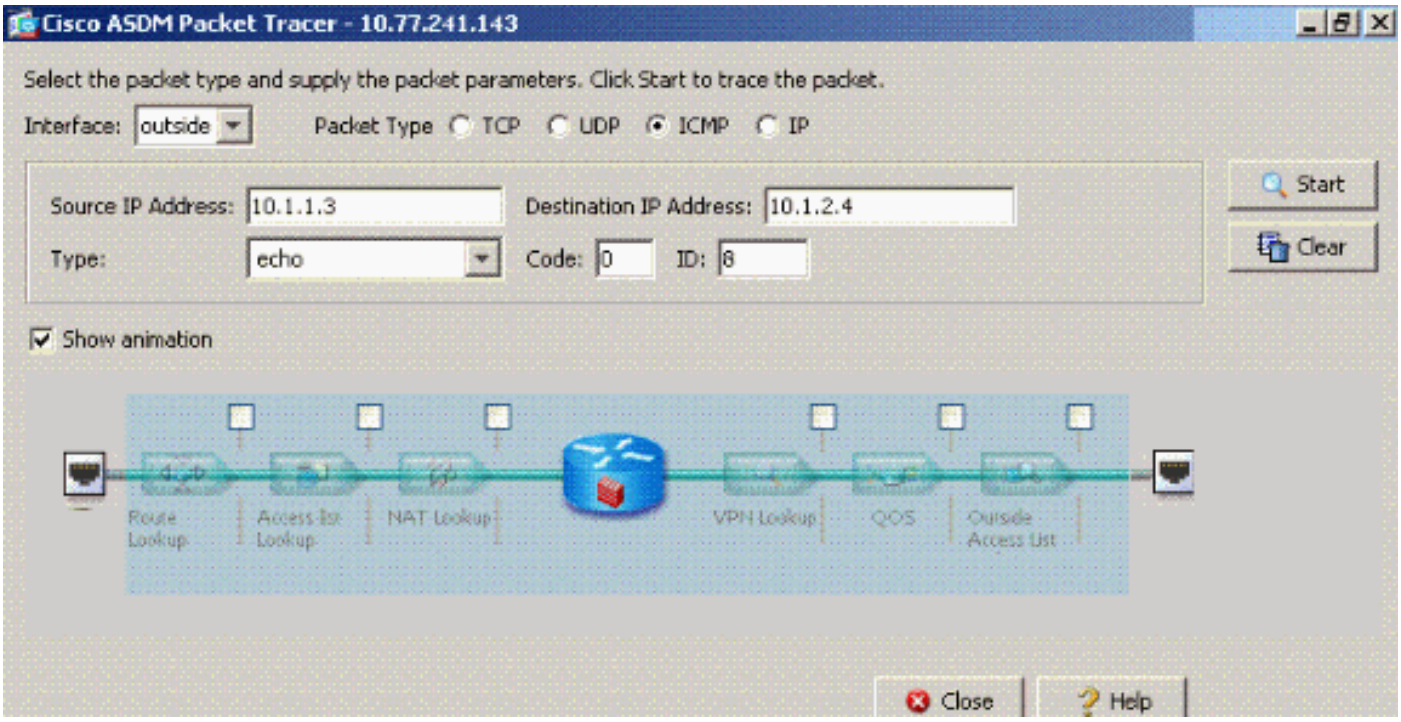
```
ciscoasa(config)#access-list outside_acl permit tcp any host 172.22.1.147 eq 80
ciscoasa(config)#access-list outside_acl deny ip any any
ciscoasa(config)#access-group outside_acl in interface outside
ciscoasa#packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1 detailed
!--- Output is suppressed.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

次の図には、ASDM での上記 CLI コマンドと同等の操作が示されています。

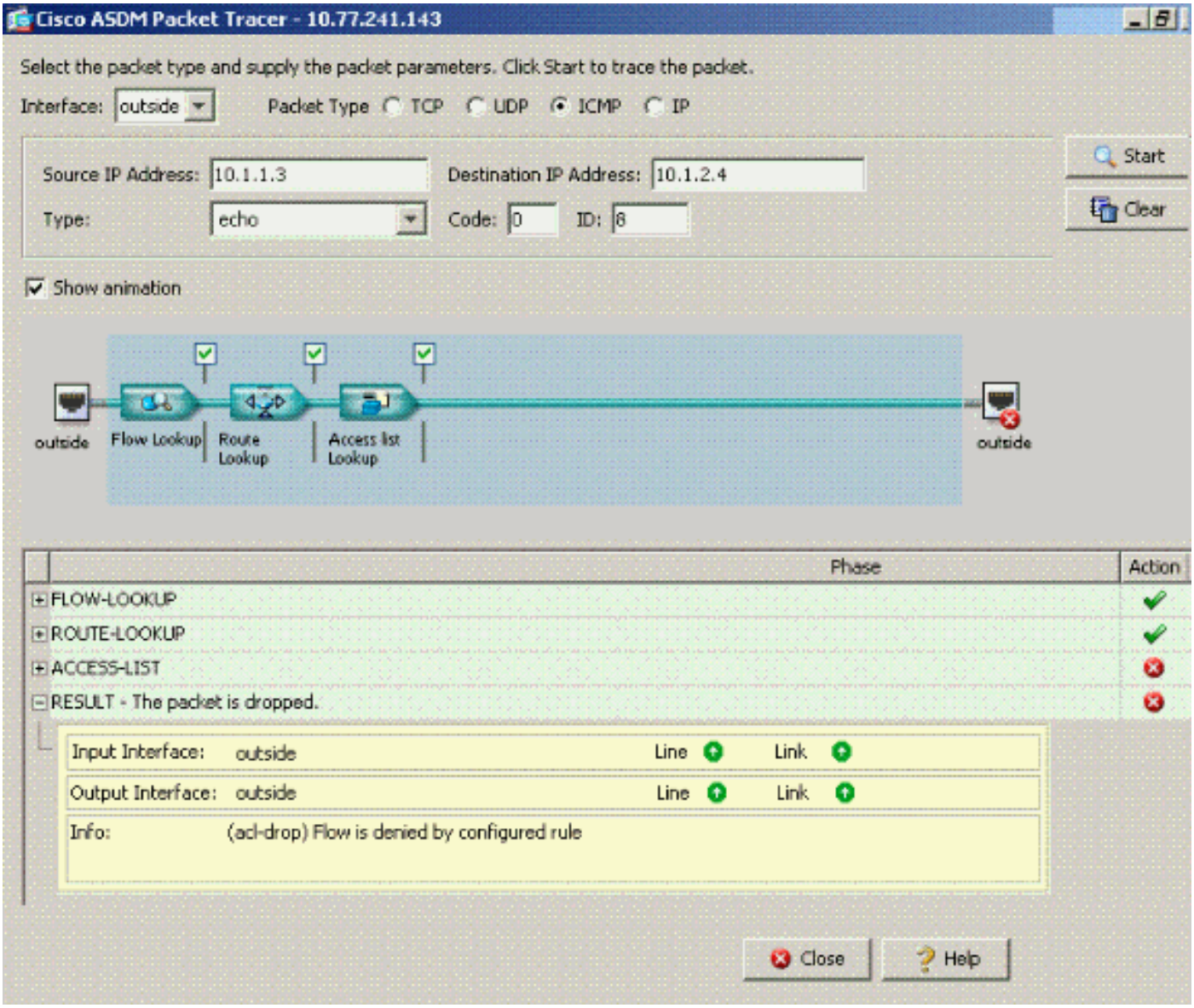
ステップ 1：



ステップ 2：



same-security-traffic permit intra-interface コマンドがイネーブルになっていて、パケットを拒否するように access-list outside_acl extended deny ip any any コマンドが設定されたパケットトレーサの出力。

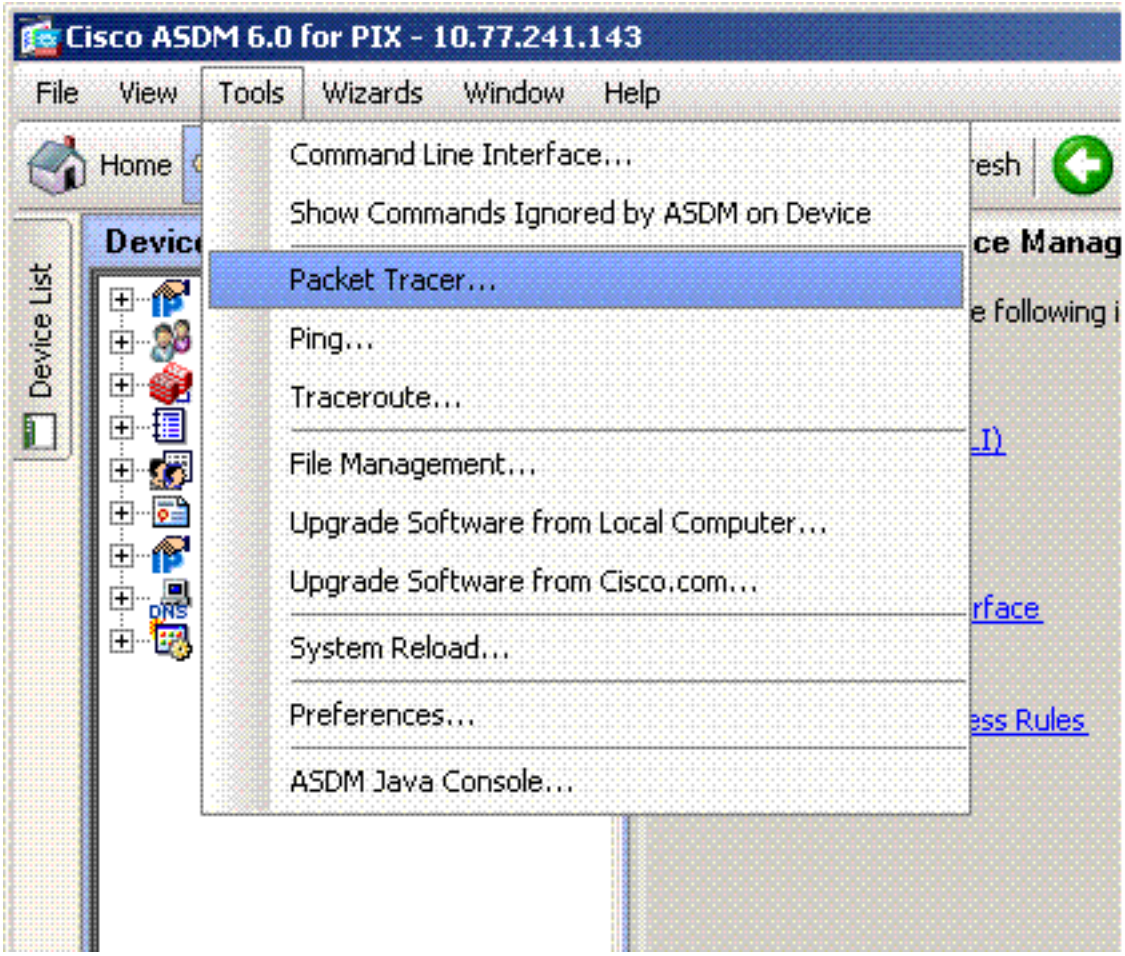


特定のインターフェイスでインターフェイス内通信が必要で、同じインターフェイスにアクセスリストを適用する場合、インターフェイス内トラフィックはアクセスリスト ルールで許可される必要があります。このセクションの例では、アクセスリストを次のように書く必要があります。

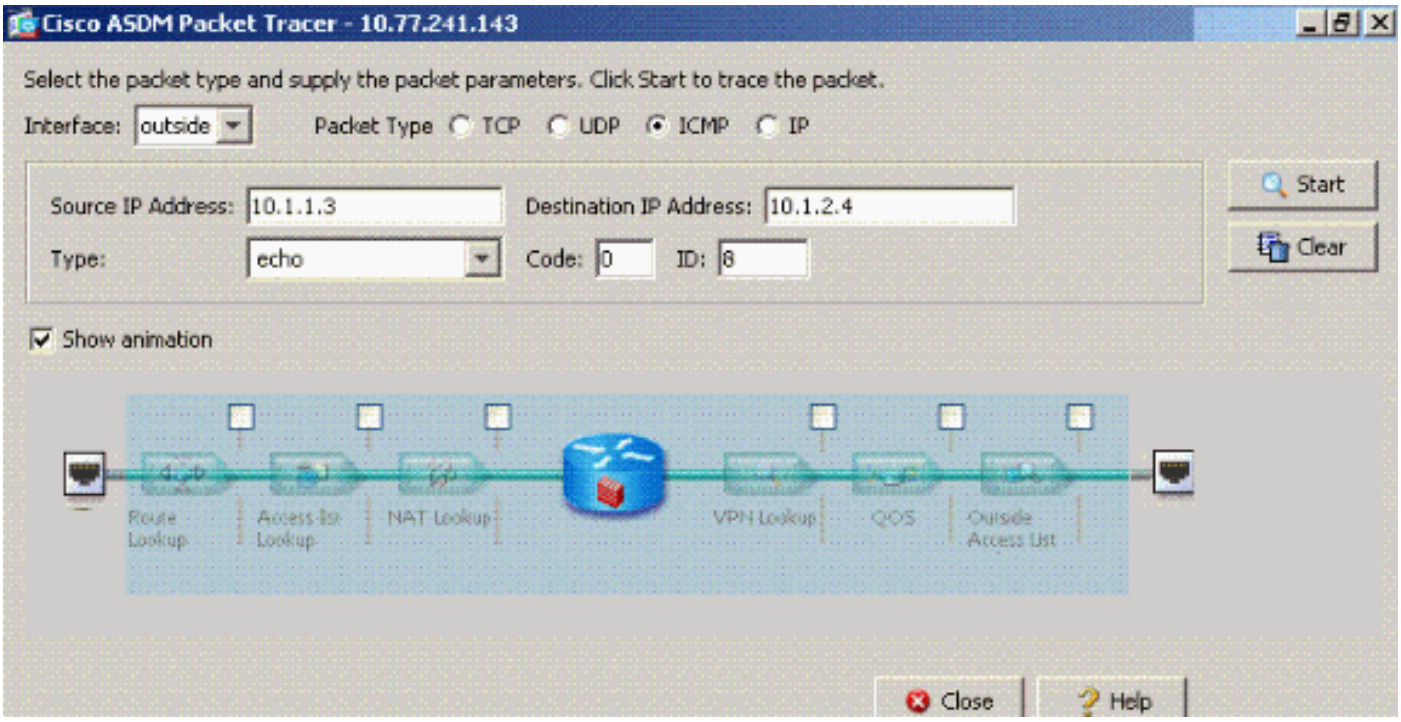
```
ciscoasa(config)#access-list outside_acl permit tcp any host 172.22.1.147 eq 80
ciscoasa(config)#access-list outside_acl permit ip 172.22.1.0 255.255.255.0 172.16.10.0
255.255.255.0
!--- 172.22.1.0 255.255.255.0 represents a locally !--- connected network on the ASA. !---
172.16.10.0 255.255.255.0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

次の図には、ASDM での上記 CLI コマンドと同等の操作が示されています。

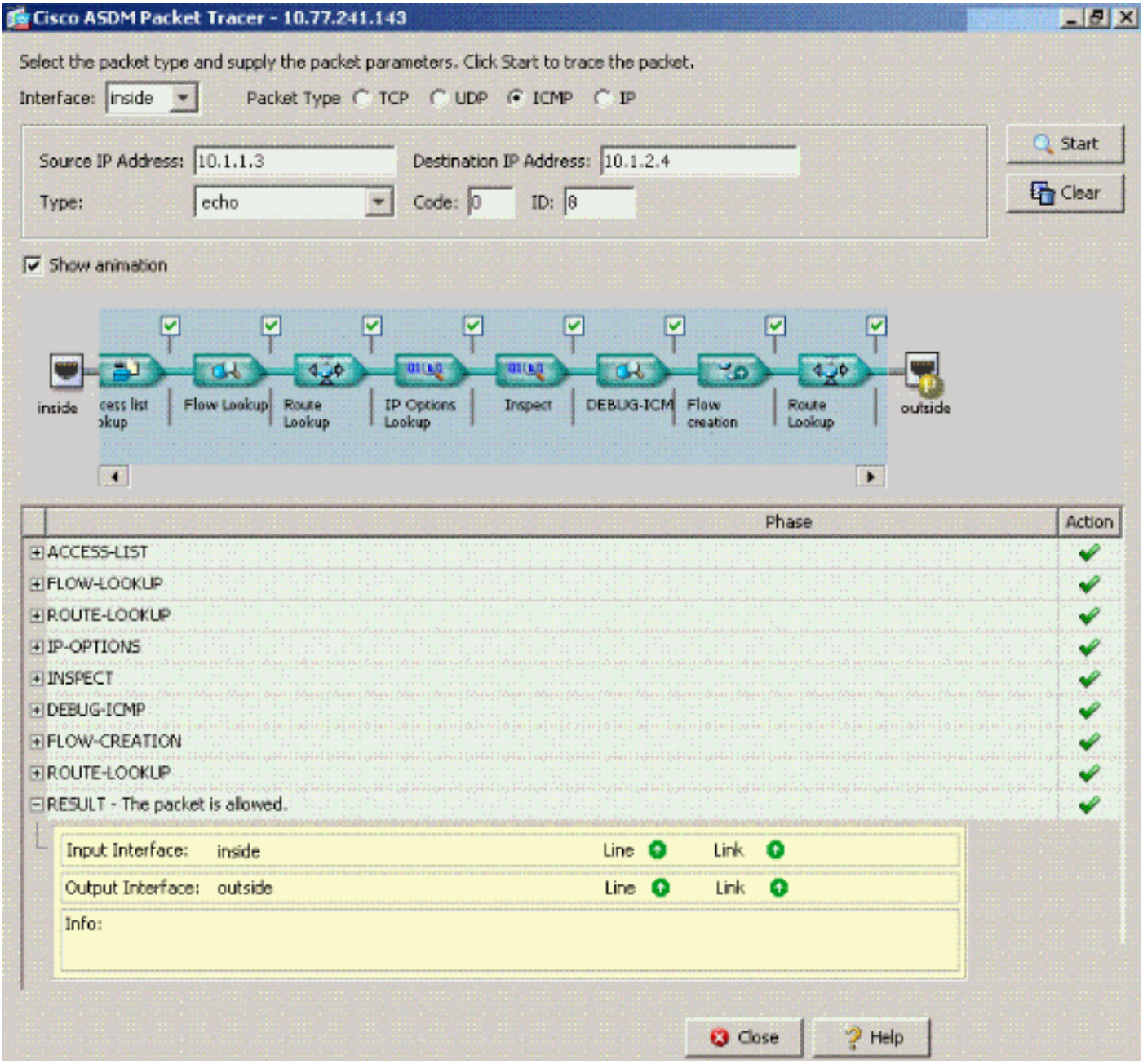
ステップ 1：



ステップ 2：



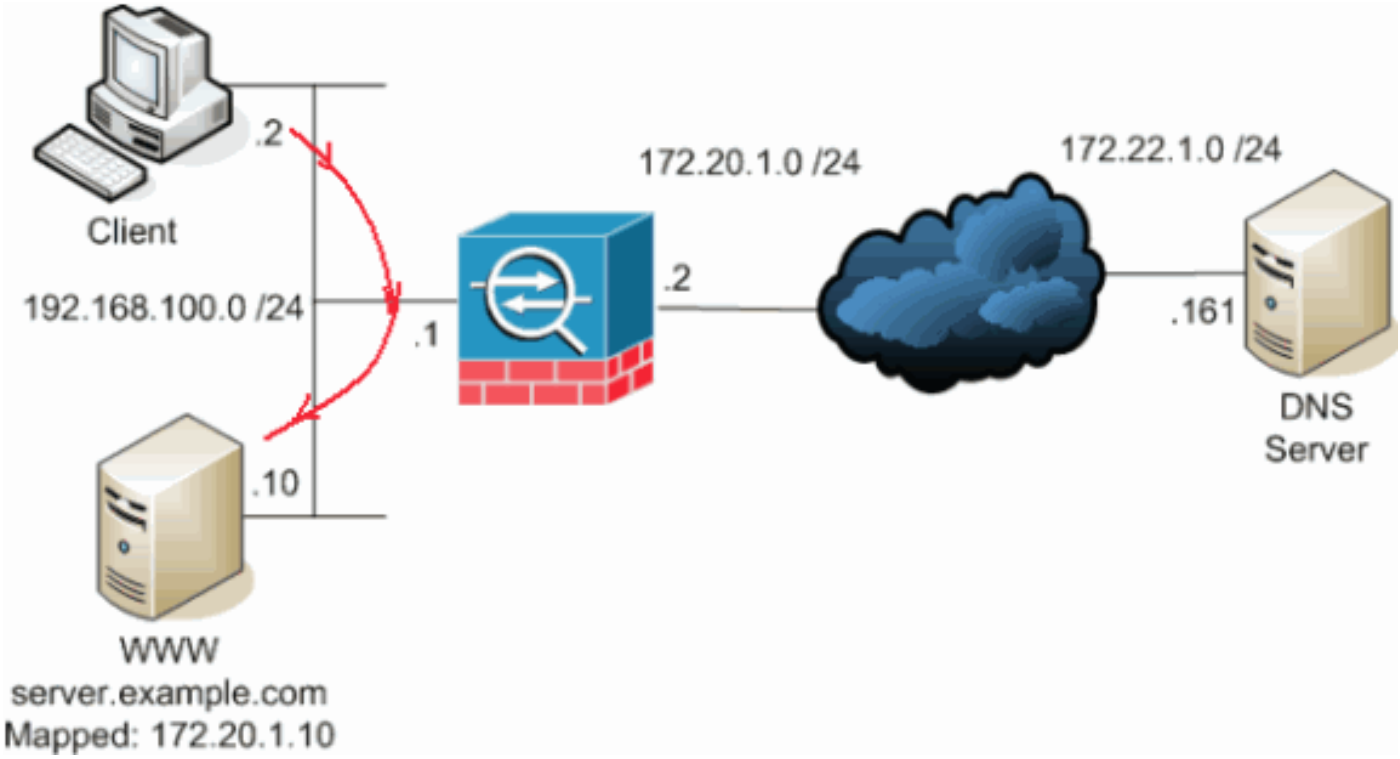
same-security-traffic permit intra-interface コマンドがイネーブルにされていて、インターフェイス内トラフィックが要求されている同じインターフェイスに **access-list outside_acl extended deny ip any any** コマンドが設定されたパケットトレーサの出力。



access-list コマンドと access-group コマンドについての詳細は、『拡張アクセスリスト』と『アクセスグループ』を参照してください。

インターフェイス内通信がスタティックおよび NAT とともにイネーブルになっている

ここでは、内部ユーザが内部 Web サーバにそのパブリック アドレスでアクセスを試みるシナリオについて説明します。



この場合、192.168.100.2 のクライアントが WWW サーバのパブリック アドレス (例 ：172.20.1.10) を使用しようとしています。 クライアントのDNSサービスは、172.22.1.161の外部DNSサーバーによって提供されます。DNSサーバーは別のパブリックネットワーク上にあるため、WWWサーバーのプライベートIPアドレスを知りません。ただし、DNS サーバは WWW サーバのマップ アドレス (172.20.1.10) は認識しています。

この例では、内部インターフェイスからのトラフィックが変換され、内部インターフェイスを経由して WWW サーバに到達するように再ルーティングされます。これは、ヘアピニングと呼ばれます。これは次のコマンドを使用して実行できます。

```
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
```

設定の詳細とヘアピニングに関する詳細については、『インターフェイス内通信を使用したヘアピニング』を参照してください。

アクセスリストの積極的な利用

すべてのファイアウォールのアクセス ポリシーが同一というわけではありません。一部のアクセス ポリシーには、他のものよりも詳細なものがあります。インターフェイス内通信がイネーブルで、すべてのインターフェイスに適用されるアクセスリストがファイアウォールにない場合、インターフェイス内通信がイネーブルにされる時点でアクセスリストの追加を検討してください。適用されるアクセスリストでは、インターフェイス内通信を許可し、さらに他のアクセス ポリシー要件も維持する必要があります。

次の例は、この点について説明しています。ASA によって、プライベート ネットワーク (インターフェイスの内部) がインターネット (インターフェイスの外部) に接続されています。 インターフェイス内の ASA に適用されているアクセスリストはありません。デフォルトでは、内部から外部へのすべての IP トラフィックが許可されます。次に示す出力のようなアクセスリストを追加

することが提言されます。

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

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

この一連のアクセスリストではすべての IP トラフィックが許可され続けます。インターフェイス内通信用の特定のアクセスリスト行により、適用されるアクセスリストによってインターフェイス内通信を許可する必要があることが管理者に示されています。

関連情報

- Cisco セキュリティ アプライアンス コマンド リファレンス、バージョン 7.2
- Cisco セキュリティ アプライアンス システム ログ メッセージ、バージョン 7.2
- Cisco PIX Firewall ソフトウェア
- ASA：ASA から AIP SSM にネットワーク トラフィックを送信する設定例
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス製品のサポート
- テクニカル サポートとドキュメント – Cisco Systems