PIX/ASA 7.2 (1) и последующие версии: Внутриинтерфейсные коммуникации

Содержание

Введение

Этот документ помогает решить типичные проблемы, возникающие при включении связи внутри интерфейса на устройстве адаптивной защиты (ASA) или PIX с выпуском ПО 7.2(1) или более поздним. Выпуск ПО 7.2 (1) включает возможность направить данные открытого текста в и из того же интерфейса. **Чтобы включить данную функцию, введите команду same-security-traffic permit intra-interface.** Этот документ предполагает, что администратор сети или активировал эту опцию или планирует к в будущем. Конфигурация и устранение проблем предоставлена с помощью интерфейса командной строки (CLI).

Примечание: Внимание этого документа на ясные (незашифрованные) данные, которые поступают и оставляют ASA. Зашифрованные данные не обсуждены.

Для включения внутриинтерфейсной связи на ASA/PIX для Конфигурации IPSec обратитесь к PIX/ASA и Клиенту VPN для VPN Общедоступного Интернета на Примере конфигурации Палки.

Для включения внутриинтерфейсной связи на ASA для конфигурации SSL обратитесь к ASA 7.2 (2): Пример настройки SSL клиента VPN (SVC) для общедоступного Интернета "on a stick".

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Списки доступа
- Маршрутизация
- Если модуль установлен и в рабочем состоянии, усовершенствованный Контроль и Модуль Сервисов безопасности предотвращения (SSM AIP) Система предотвращения вторжений (IPS) — Знание этого модуля только необходимо.
- Если SSM AIP не используется, выпуск ПО IPS 5.x — Знание программного обеспечения IPS не требуется.

Используемые компоненты

- ASA 5510 7.2 (1) и позже
- AIP-SSM-10, который управляет программным обеспечением IPS 5.1.1

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

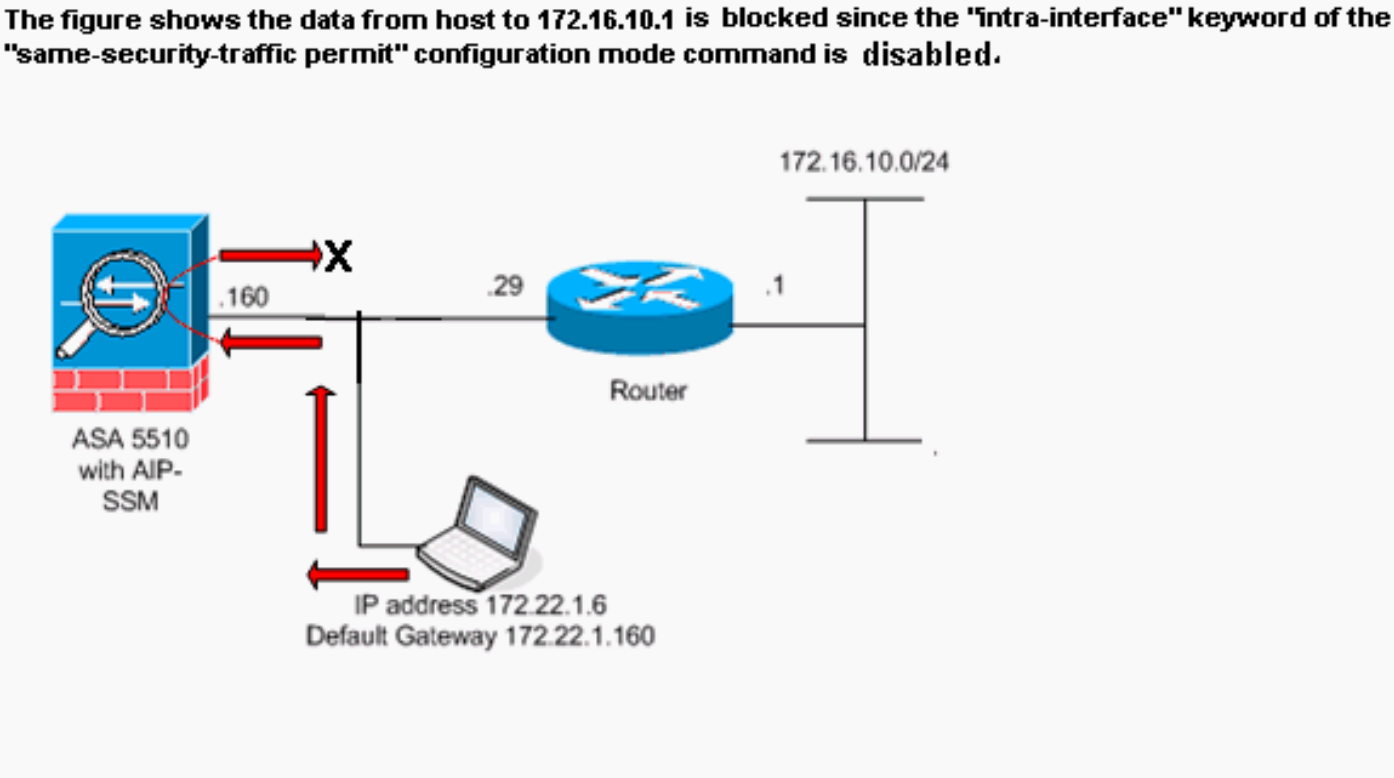
Родственные продукты

Эта конфигурация может также использоваться с Cisco PIX серии 500, который выполняет версию 7.2 (1) и позже.

Условные обозначения

Сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Общие сведения



Примечание: Схемы IP-адресации, которые использованы в данной конфигурации, не поддерживаются официальной маршрутизацией в Интернете. Это адреса RFC 1918, которые использовались в лабораторной среде.

Эта таблица показывает ASA стартовая конфигурация:

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:
```

Устранение неисправностей

Эти разделы иллюстрируют несколько сценариев конфигурации, отнесенных сообщений системного журнала и выходных данных packet-tracer относительно внутриинтерфейсной связи.

Внутриинтерфейсная связь, не включенная

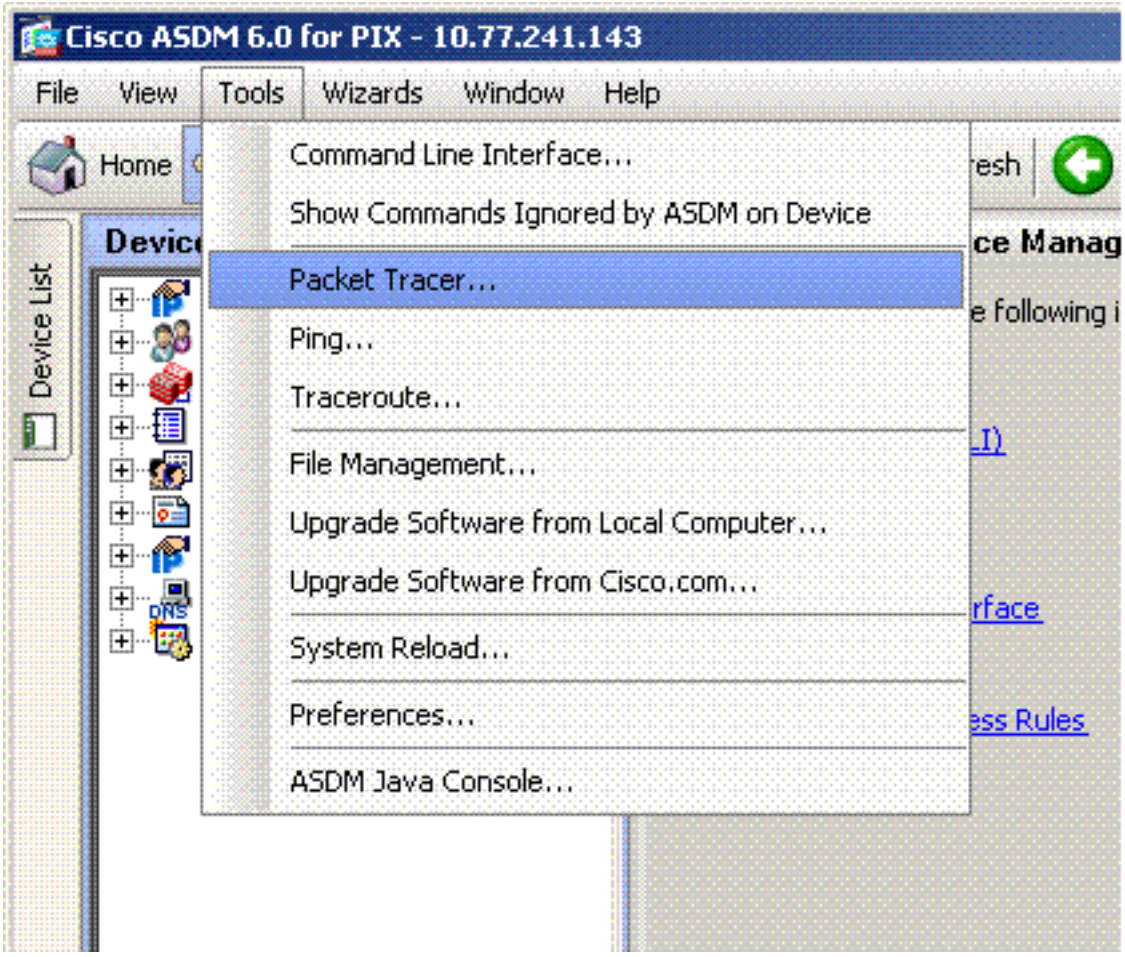
В конфигурации ASA хост 172.22.1.6 пытается пропинговать хост 172.16.10.1. Хост 172.22.1.6 передает пакет эхо-запроса протокола ICMP к шлюзу по умолчанию (ASA). Внутриинтерфейсная связь не была включена на ASA. ASA отбрасывает пакет эхо-запроса. Тестовые сбои эхо-запроса. ASA используется для устренения проблемы.

Данный пример показывает выходные данные сообщений системного журнала и пакетного трассировщика:

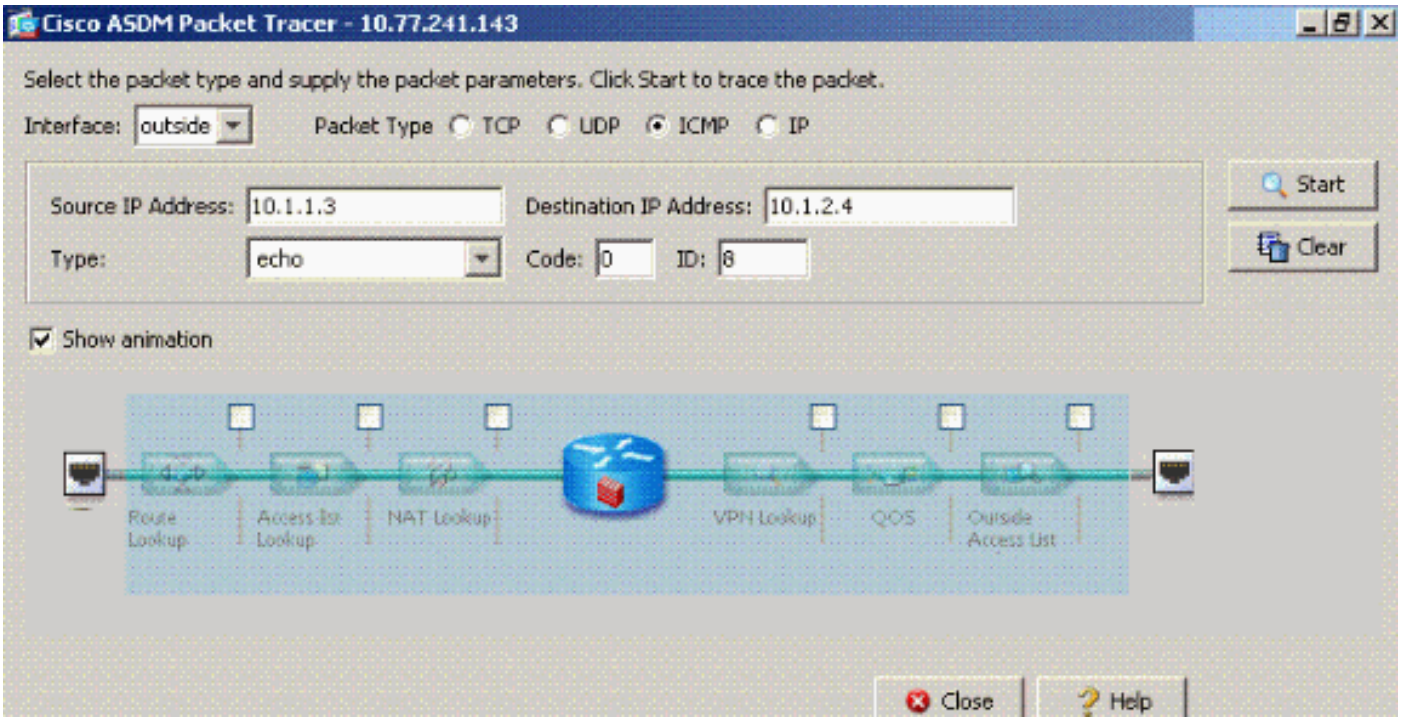
- Это - сообщение системного журнала, зарегистрированное к буферу:`ciscoasa(config)#`**`show logging`** *`!--- Output is suppressed.`* `%ASA-3-106014: Deny inbound icmp src outside:172.22.1.6 dst outside:172.16.10.1 (type 8, code 0)`
- Это - выходные данные packet-tracer:`ciscoasa(config)#`**`packet-tracer 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`

Эквивалент команд CLI в ASDM показывают на этих рисунках:

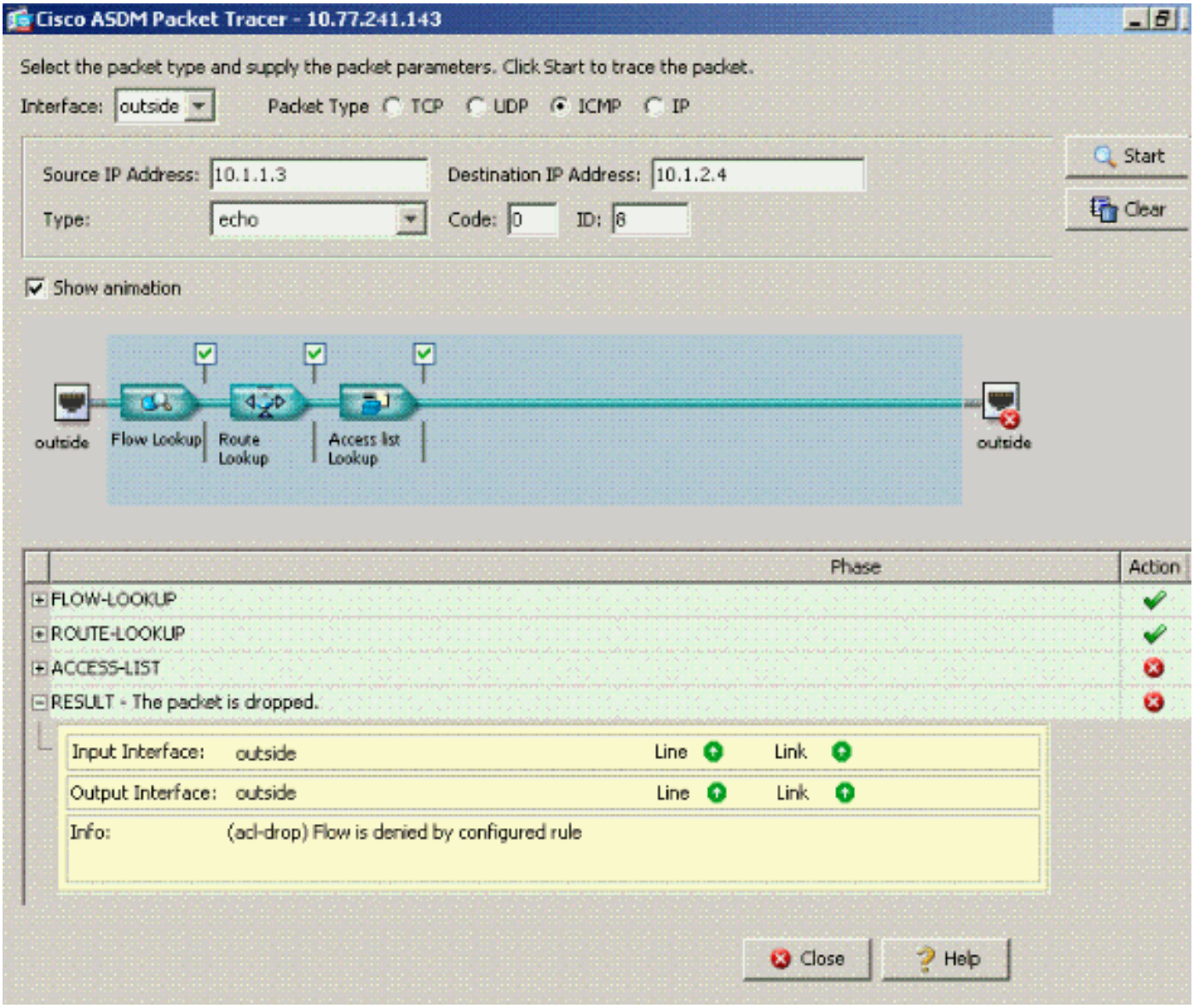
Шаг 1:



Шаг 2:



Выходные данные packet-tracer с отключенной **командой same-security-traffic permit intra-interface**.



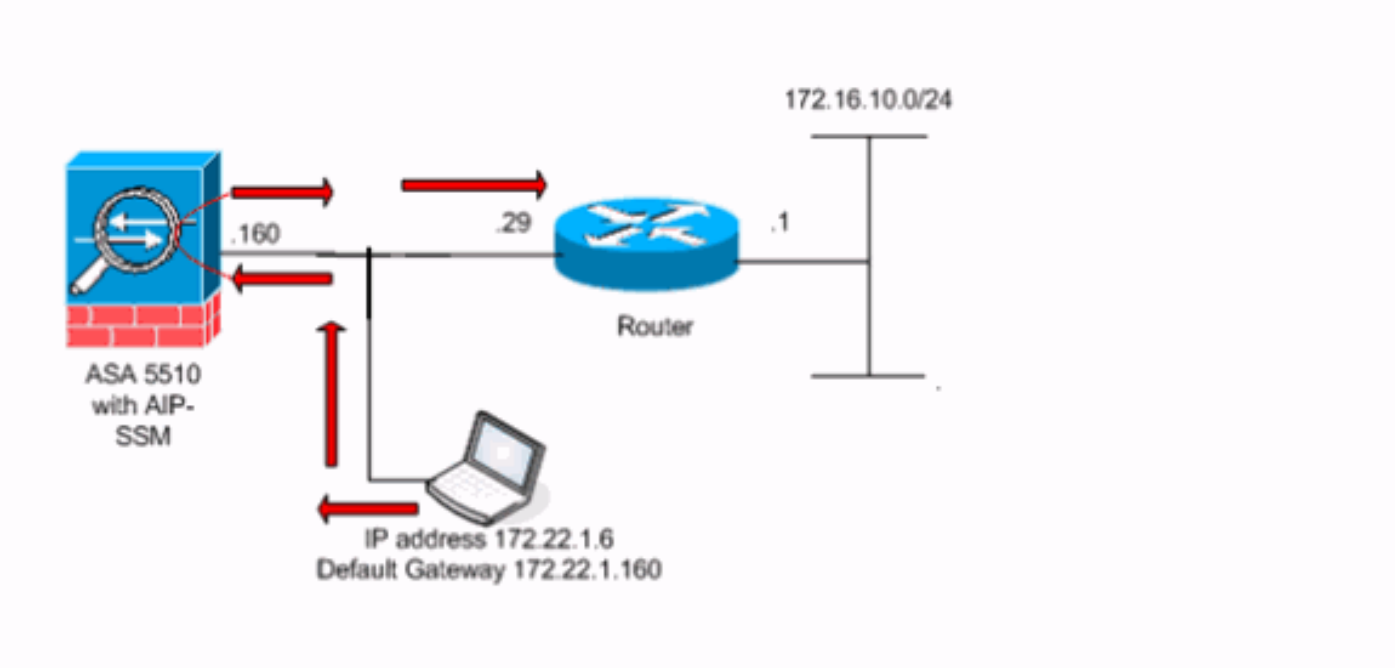
Выходной packet-tracer `drop...implicit rule` предполагает, что значение конфигурации по умолчанию блокирует трафик. Администратор должен проверить рабочую конфигурацию, чтобы гарантировать, что включена внутриинтерфейсная связь. **В данном случае для конфигурации ASA необходимо включить функцию межинтерфейсной и внутриинтерфейсной связи (same-security-traffic permit intra-interface).**

```
ciscoasa#show running-config !--- Output is suppressed. interface Ethernet5 shutdown no nameif
no security-level no ip address ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode passive same-
security-traffic permit intra-interface !--- When intra-interface communications are enabled,
the line !--- highlighted in bold font appears in the configuration. The configuration line !---
appears after the interface configuration and before !--- any access-list configurations.
access-list... access-list...
```

Включена внутриинтерфейсная связь

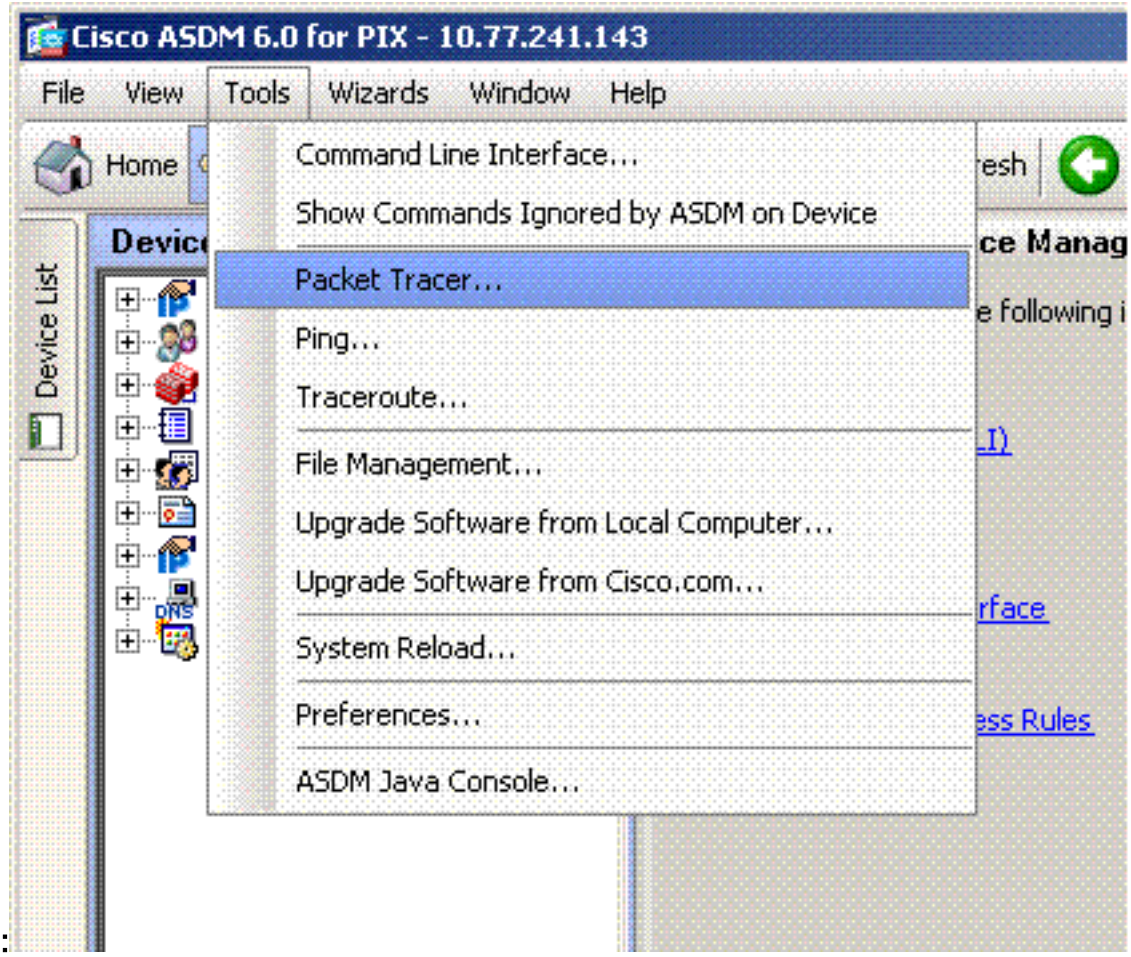
Внутриинтерфейсная связь теперь включена. **К предыдущей конфигурации добавляется команда same-security-traffic permit intra-interface**. Хост 172.22.1.6 пытается пропинговать хост 172.16.10.1. Хост 172.22.1.6 передает пакет эхо-запроса протокола ICMP к шлюзу по умолчанию (ASA). Хост 172.22.1.6 делает запись успешных ответов от 172.16.10.1. ASA передает трафик ICMP успешно.

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.

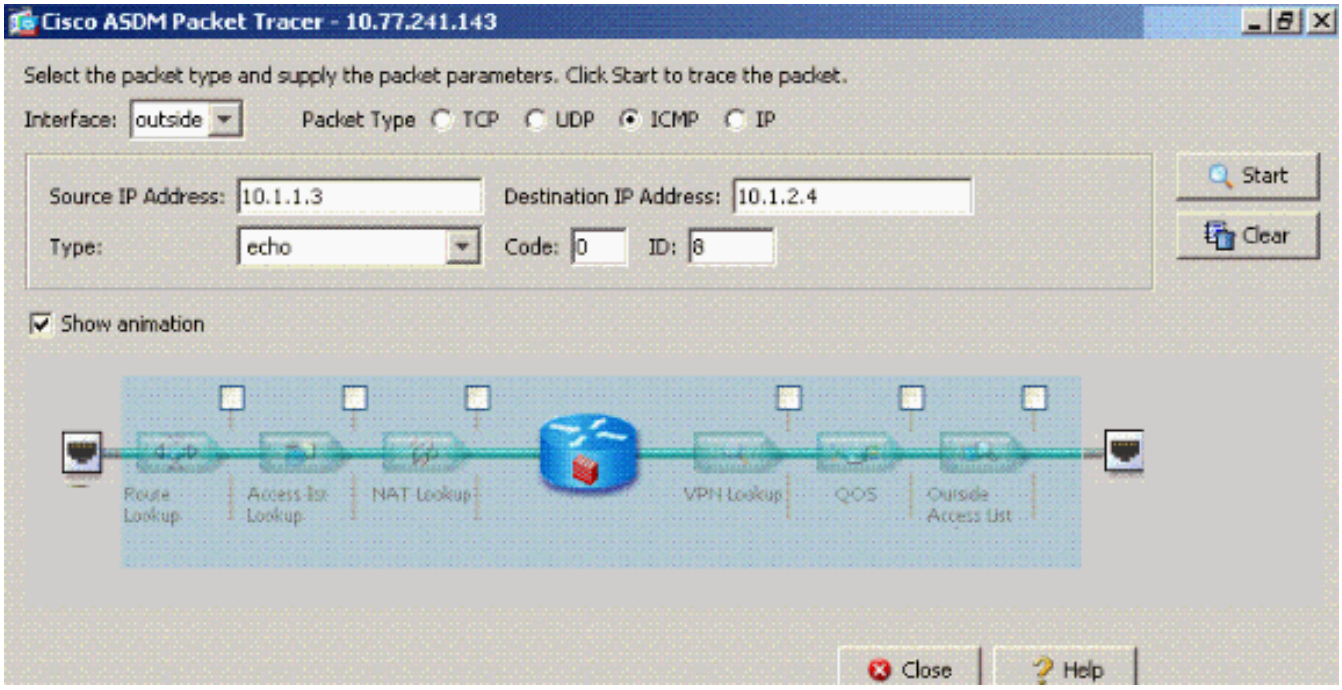


Эти примеры показывают сообщение системного журнала ASA и выходные данные packet-tracer:

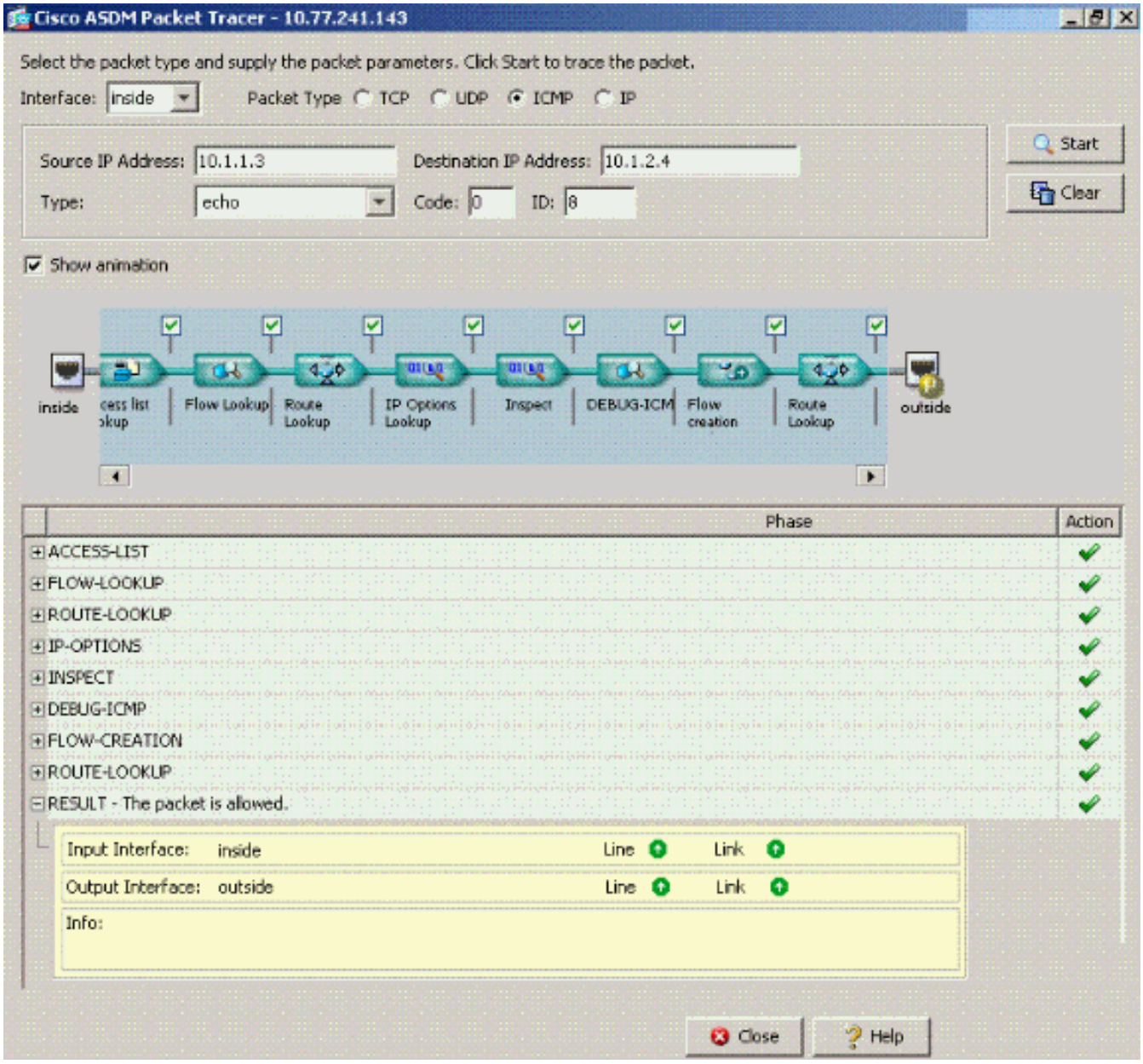
- Это сообщения системного журнала, зарегистрированные к буферу:`ciscoasa#`**`show logging`** *`!--- Output is suppressed.`* `%PIX-7-609001: Built local-host outside:172.22.1.6 %PIX-7-609001: Built local-host outside:172.16.10.1 %PIX-6-302020: Built ICMP connection for faddr 172.22.1.6/64560 gaddr 172.16.10.1/0 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`
- Это - выходные данные 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`*** Эквивалент команд CLI в ASDM показывают на этих рисунках:Шаг



1: Шаг 2:



Выходные данные packet-tracer с включенной **командой same-security-traffic permit intra-interface**.



Примечание: Никакой access-list не применен к внешнему интерфейсу. В примере конфигурации внешний интерфейс является назначенным уровнем безопасности 0. По умолчанию межсетевой экран не разрешает трафик с низкого безопасного интерфейса на интерфейс высокого уровня безопасности. Это могло бы вести администраторов полагать, что внутриинтерфейсный трафик не разрешен на внешней стороне (низкая безопасность) интерфейс без разрешений от access-list. Когда никакой access-list не применен к интерфейсу, Однако тот же интерфейсный трафик проходит свободно.

Внутриинтерфейс включил, и трафик прошел к SSM AIP для контроля

Внутриинтерфейсный трафик можно передать к SSM AIP для контроля. Этот раздел предполагает, что администратор настроил ASA для передачи трафика к SSM AIP, и администратор знает, как настроить программное обеспечение IPS 5.x.

На этом этапе конфигурация ASA содержит предыдущий пример конфигурации, внутриинтерфейсная связь включена, и весь (любой) трафик передан к SSM AIP. Подпись 2004 IPS модифицируется для отбрасывания трафика запроса эха. Хост 172.22.1.6 пытается пропинговать хост 172.16.10.1. Хост 172.22.1.6 передает пакет эхо-запроса протокола ICMP к шлюзу по умолчанию (ASA). ASA вперед пакет эхо-запроса к SSM AIP для

контроля. SSM AIP отбрасывает пакет данных на конфигурацию IPS.

Эти примеры показывают сообщение системного журнала ASA и выходные данные packet-tracer:

- Это - сообщение системного журнала, зарегистрированное к буферу:`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.`*
- Это - выходные данные 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.`*

Следует отметить, что администраторы должны использовать как можно больше средств устранения проблем, когда они исследуют проблему. Данный пример показывает, как два других средства устранения проблем могут нарисовать другие изображения. Оба программных средства вместе рассказывают завершенную историю. Политика конфигурации ASA разрешает трафик, но конфигурация IPS не делает.

Внутриинтерфейс включил, и списки доступа применились к интерфейсу

Этот раздел использует исходный пример конфигурации в этом документе, внутриинтерфейсная связь включила, и access-list применился к протестированному интерфейсу. Эти линии добавлены к конфигурации. Access-list предназначен, чтобы быть простым представлением того, что могло бы быть настроено на производственном межсетевом экране.

```
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.
```

Хост 172.22.1.6 пытается пропинговать хост 172.16.10.1. Хост 172.22.1.6 передает пакет эхо-запроса протокола ICMP к шлюзу по умолчанию (ASA). ASA отбрасывает пакет эхо-запроса на правила access-list. Тест хоста 172.22.1.6 пропинговывает сбои.

Эти примеры показывают сообщение системного журнала ASA и выходные данные packet-tracer:

- Это - сообщение системного журнала, зарегистрированное к буферу:`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]`

- Это - выходные данные 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`

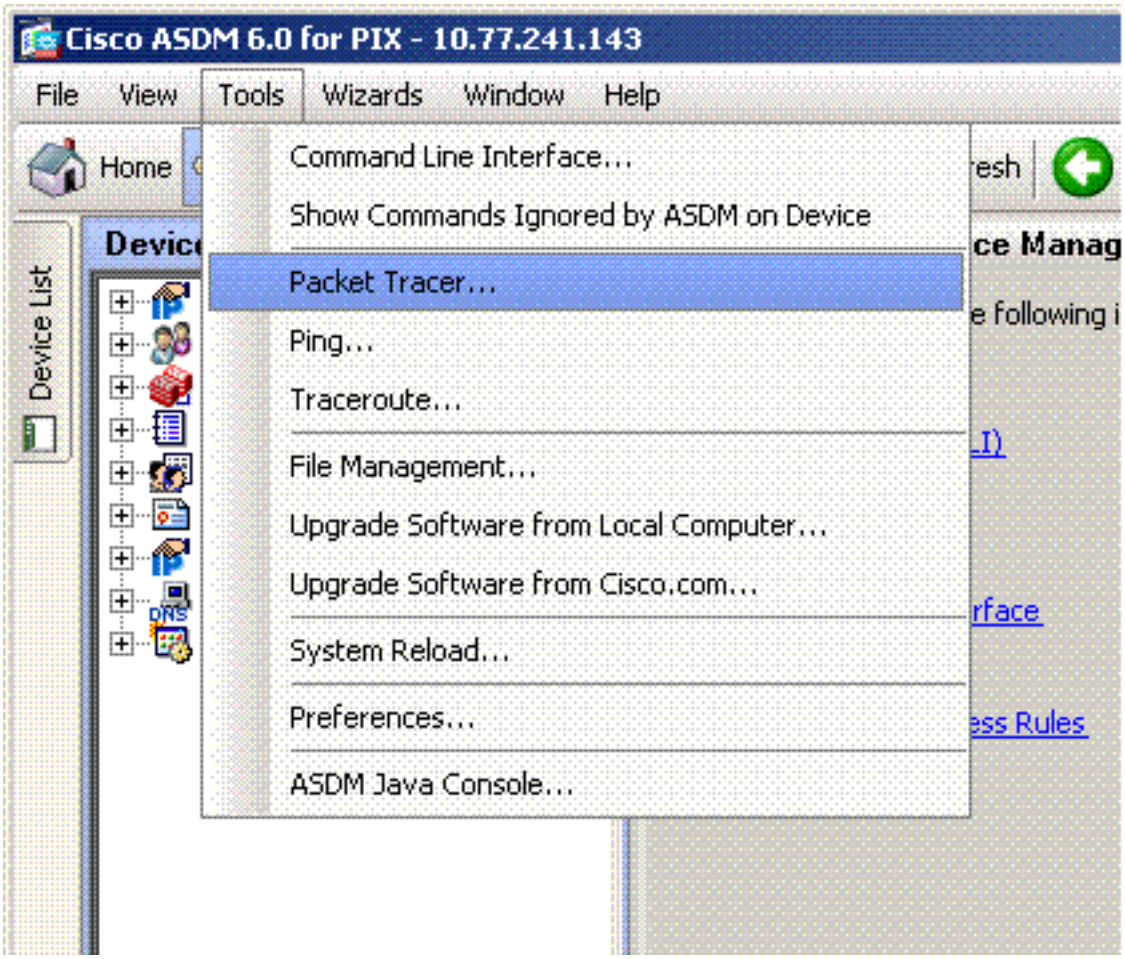
См. пакетного трассировщика для получения дополнительной информации о **команде packet-tracer**.

Примечание: В конечном счете access-list применился к интерфейсу, включает инструкцию deny, выходные данные изменений пакетного трассировщика. Пример:

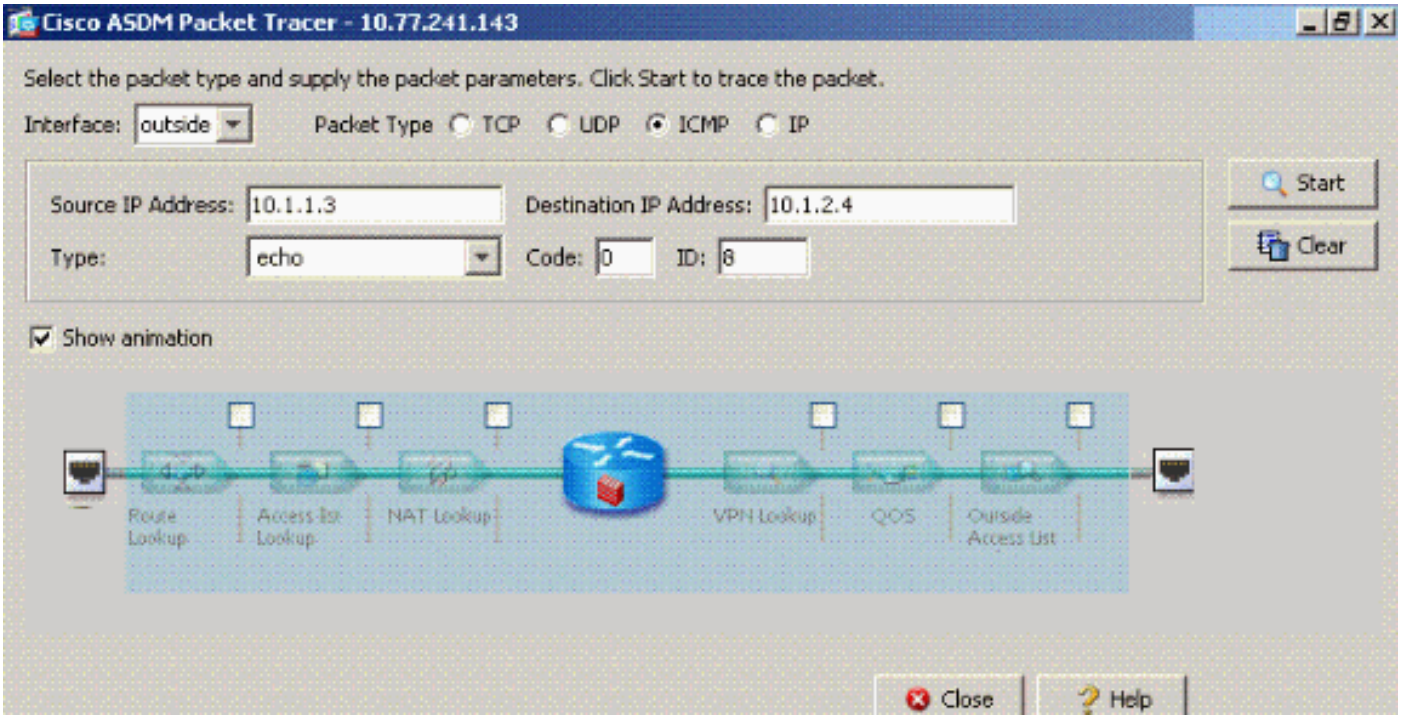
`ciscoasa(config)#`**`access-list outside_acl permit tcp any host 172.22.1.147 eq 80`**
`ciscoasa(config)#`**`access-list outside_acl deny ip any any`** `ciscoasa(config)#`**`access-group outside_acl in interface outside`** `ciscoasa#`**`packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1 detailed`**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

Эквивалент вышеупомянутых команд CLI в ASDM показывают на этих рисунках:

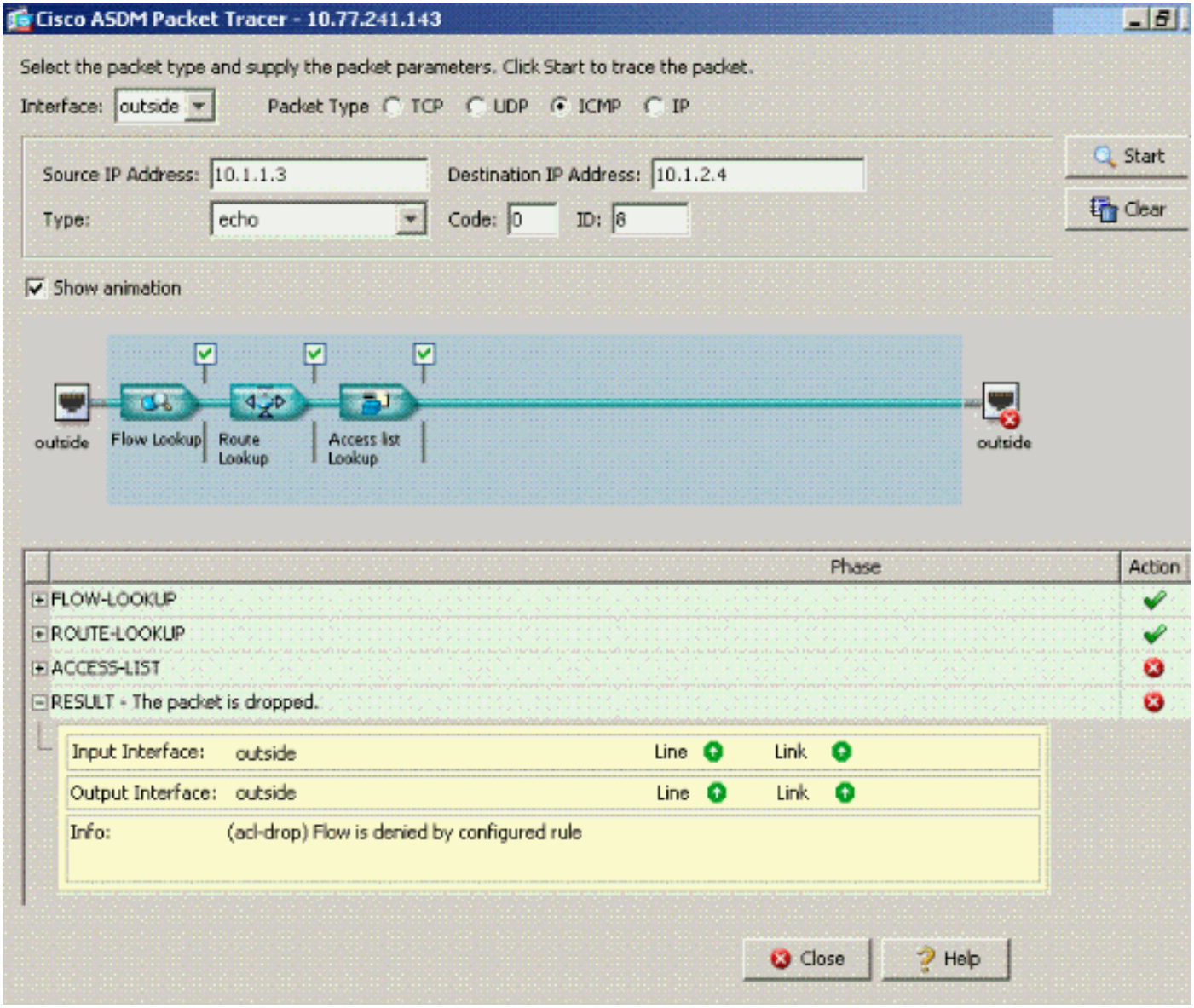
Шаг 1:



Шаг 2:



Выходные данные packet-tracer с включенной **командой same-security-traffic permit intra-interface** и **командой access-list outside_acl extended deny ip any any**, настроенной для запрета пакетов.

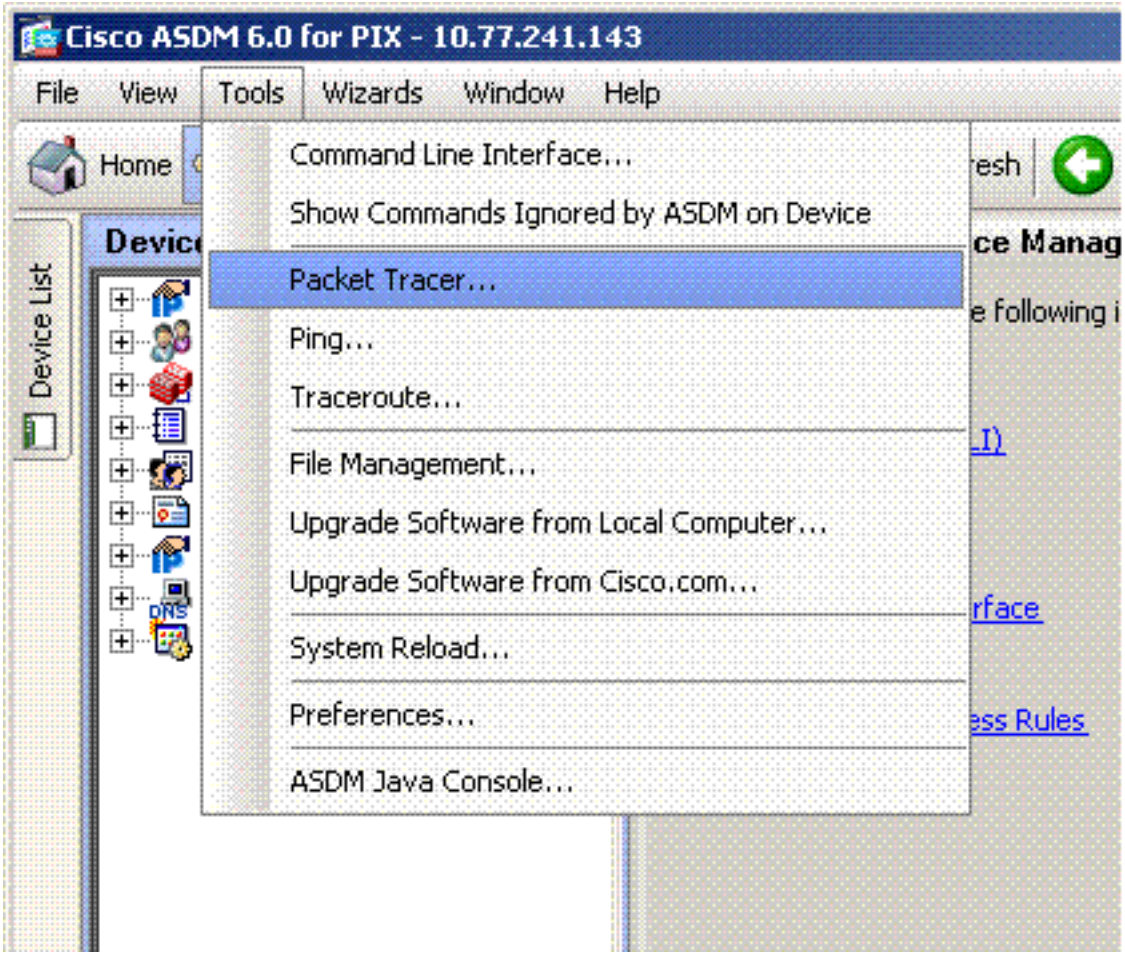


Если внутриинтерфейсная связь желаема на определенном интерфейсе, и access-lists применены к тому же интерфейсу, правила access-list должны разрешить внутриинтерфейсный трафик. С использованием примеров в этом разделе access-list должен быть записан как:

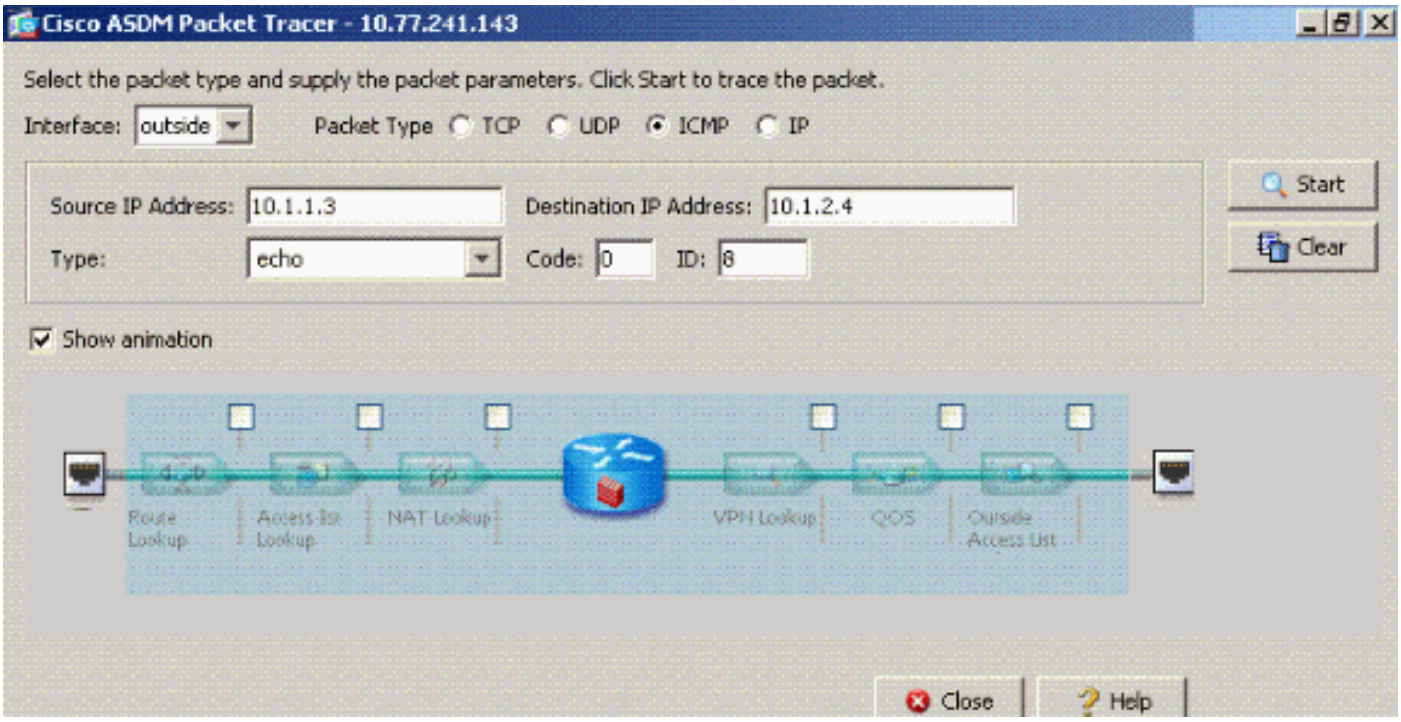
```
ciscoasa(config)#access-list outside_acl permit tcp any host 172.22.1.147 eq 80
ciscoasa(config)#access-list outside_acl permit ip 172.22.1.0 255.255.255.0 172.16.10.0
255.255.255.0 !--- 172.22.1.0 255.255.255.0 represents a locally !--- connected network on the
ASA. !--- 172.16.10.0 255.255.255.0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

Эквивалент вышеупомянутых команд CLI в ASDM показывают на этих рисунках:

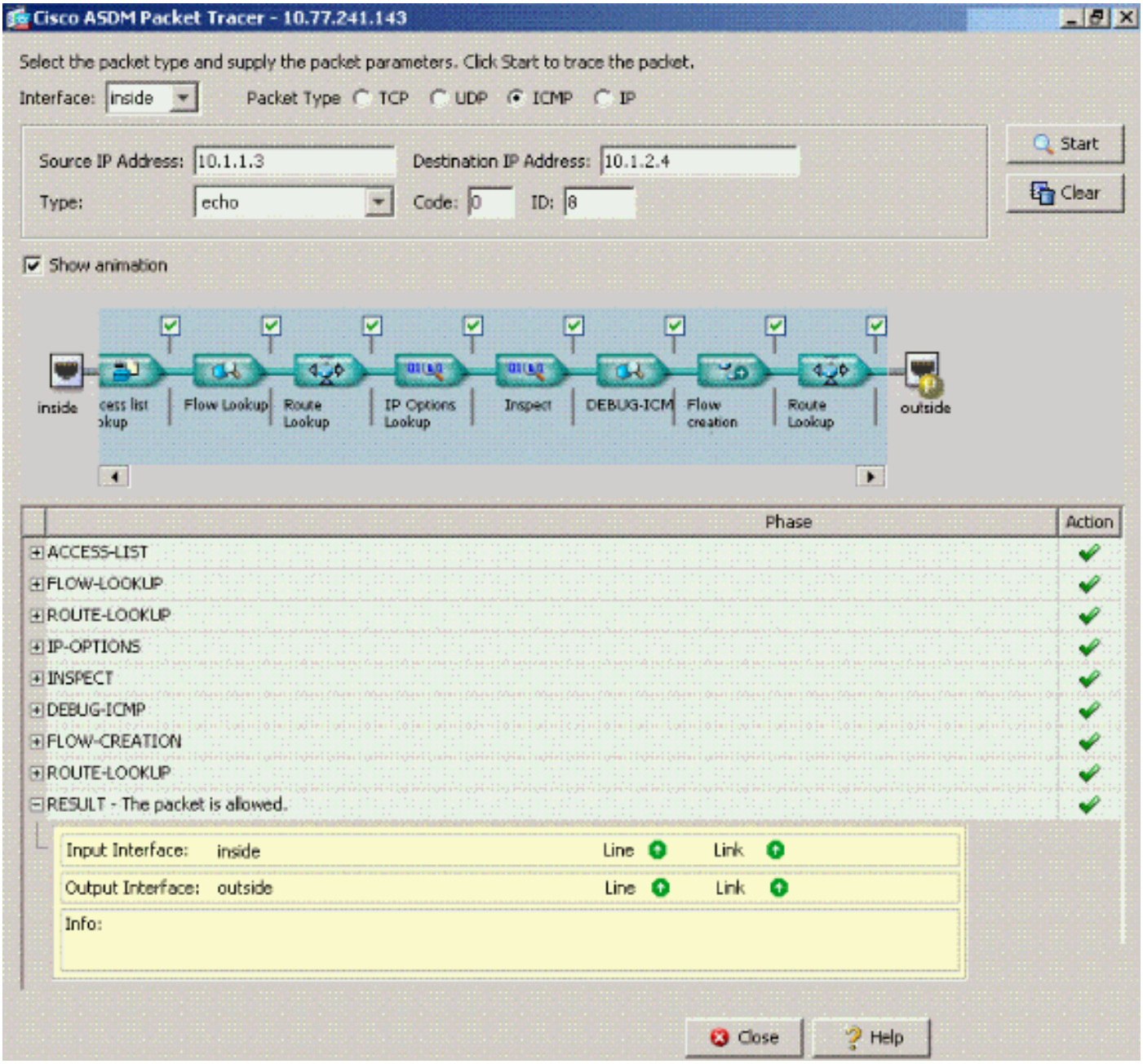
Шаг 1:



Шаг 2:



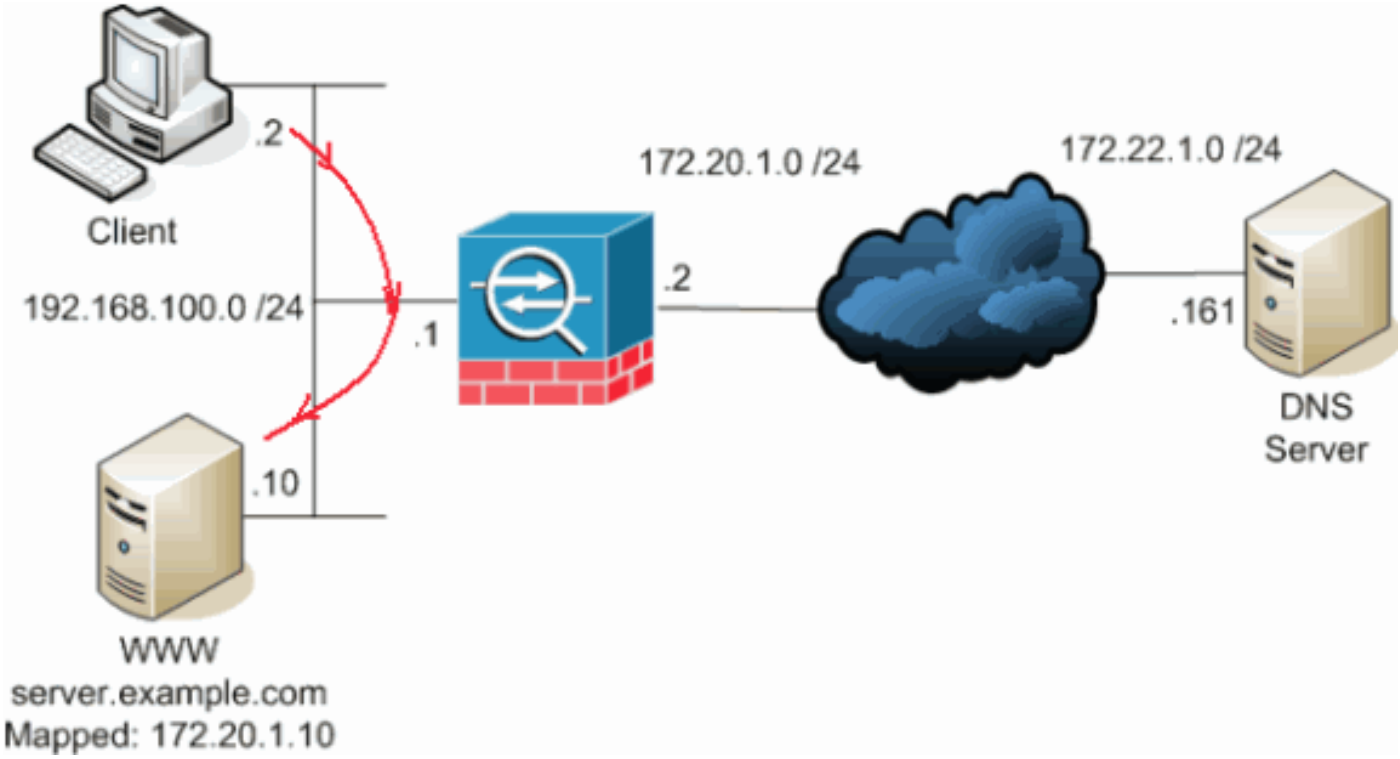
Выходные данные packet-tracer с включенной **командой same-security-traffic permit intra-interface** и **командой access-list outside_acl extended deny ip any any** настроили на том же интерфейсе, где желаем внутриинтерфейсный трафик.



Дополнительные сведения по командам access-list и access-group см. в документах access-list extended и access-group.

Внутриинтерфейс включил со статическим и NAT

Этот раздел объясняет сценарий, где внутренний пользователь пытается обратиться к внутреннему веб-серверу с его общим адресом.



В этом случае клиент в 192.168.100.2 хочет использовать общий адрес сервера WWW (например, 172.20.1.10). Сервисы DNS для клиента предоставлены внешним сервером DNS в 172.22.1.161. Так как DNS-сервер расположен в другой общедоступной сети, ему неизвестен частный IP-адрес сервера WWW. Вместо этого сервер DNS знает, что сервер WWW сопоставил адрес 172.20.1.10.

Здесь этот трафик от внутреннего интерфейса должен быть преобразован и перенаправлен через внутренний интерфейс для достижения сервера WWW. Это называют прикреплением. Это может быть выполнено посредством этих команд:

```
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
```

Для завершенных элементов конфигурации и дополнительных сведений о прикреплении, обратитесь к Прикреплению с Внутриинтерфейсной связью.

Дальновидный Access-List

Не вся политика доступа межсетевого экрана является тем же. Некоторая политика доступа является более определенной, чем другие. В конечном счете внутриинтерфейсная связь включена, и межсетевому экрану не применились к access-list все интерфейсы, могло бы стоить добавить access-list в то время, когда включена внутриинтерфейсная связь. Прикладной access-list должен разрешить внутриинтерфейсную связь, а также поддержать другие требования политики доступа.

Этот вопрос представлен в следующем примере. ASA подключает частную сеть (внутренний интерфейс) с Интернетом (внешний интерфейс). Внутреннему интерфейсу ASA не применили access-list. По умолчанию весь IP - трафик разрешен от внутренней части до внешней стороны. Предложение должно добавить access-list, который выглядит примерно так выходные данные:

```
access-list inside_acl permit ip <locally connected network> <all other internal networks>
access-list inside_acl permit ip any any access-group inside_acl in interface inside
```

Этот набор access-lists продолжает разрешать весь IP - трафик. Определенная линия (линии) access-list для внутриинтерфейсной связи напоминает администраторам, что внутриинтерфейсная связь должна быть разрешена прикладным access-list.

Дополнительные сведения

- Справочник по командам Cisco Security Appliance, версия 7.2
- Сообщения журнала системы Cisco Security Appliance, версия 7.2
- Cisco PIX Firewall Software
- ASA: Пример конфигурации для отправки трафика из ASA в AIP SSM
- Поддержка устройств адаптивной безопасности Cisco ASA серии 5500
- Cisco Systems – техническая поддержка и документация