PIX/ASA 7.2(1) والإصدارات الأحدث: الاتصالات الداخلية

المحتويات

المقدمة

يساعد هذا المستند على أستكشاف المشكلات الشائعة وإصلاحها والتي تحدث عند تمكين الاتصالات داخل الواجهة على جهاز الأمان القابل للتكيف (ASA) أو PIX الذي يعمل في الإصدار 7.2(1) من البرنامج والإصدارات الأحدث. يتضمن الإصدار 7.2(1) من البرنامج إمكانية توجيه بيانات نصية واضحة من الواجهة نفسها وإليها. أدخل الأمر **نفسه-security-traffic allowed intra-interface** لتمكين هذه الميزة. يفترض هذا المستند أن مسؤول الشبكة قد قام بتمكين هذه الميزة أو خطط لها في المستقبل. يتم توفير التكوين واستكشاف الأخطاء وإصلاحها باستخدام واجهة سطر الأوامر (CLI).

ملاحظة: يركز هذا المستند على البيانات الواضحة (غير المشفرة) التي تصل إلى ASA وتتركه. لا تتم مناقشة البيانات المشفرة.

لتمكين الاتصال بين الواجهات على ASA/PIX لتكوين IPsec، ارجع إلى PIX/ASA وعميل VPN لشبكة VPN العامة عبر الإنترنت على مثال تكوين العصا.

لتمكين الاتصال داخل الواجهة على ASA لتكوين SSL، ارجع إلى (ASA 7.2(2): SSL VPN Client (SVC لبروتوكول الإنترنت العام VPN على مثال تكوين العصا.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- قوائم الوصول
- توجيه
- بطاقة خدمات الأمان والفحص والمنع المتقدم (AIP-SSM) نظام منع التسلل (IPS)—لا تكون معرفة هذه الوحدة التعليمية ضرورية إلا في حالة تركيب الوحدة وتشغيلها.
- برنامج IPS الإصدار x.5—لا تكون معرفة برنامج IPS مطلوبة إذا لم يكن AIP-SSM قيد الاستخدام.

المكونات المستخدمة

- ASA 5510 7.2(1) والإصدارات الأحدث
- AIP-SSM-10 الذي يشغل برنامج IPS 5.1.1

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

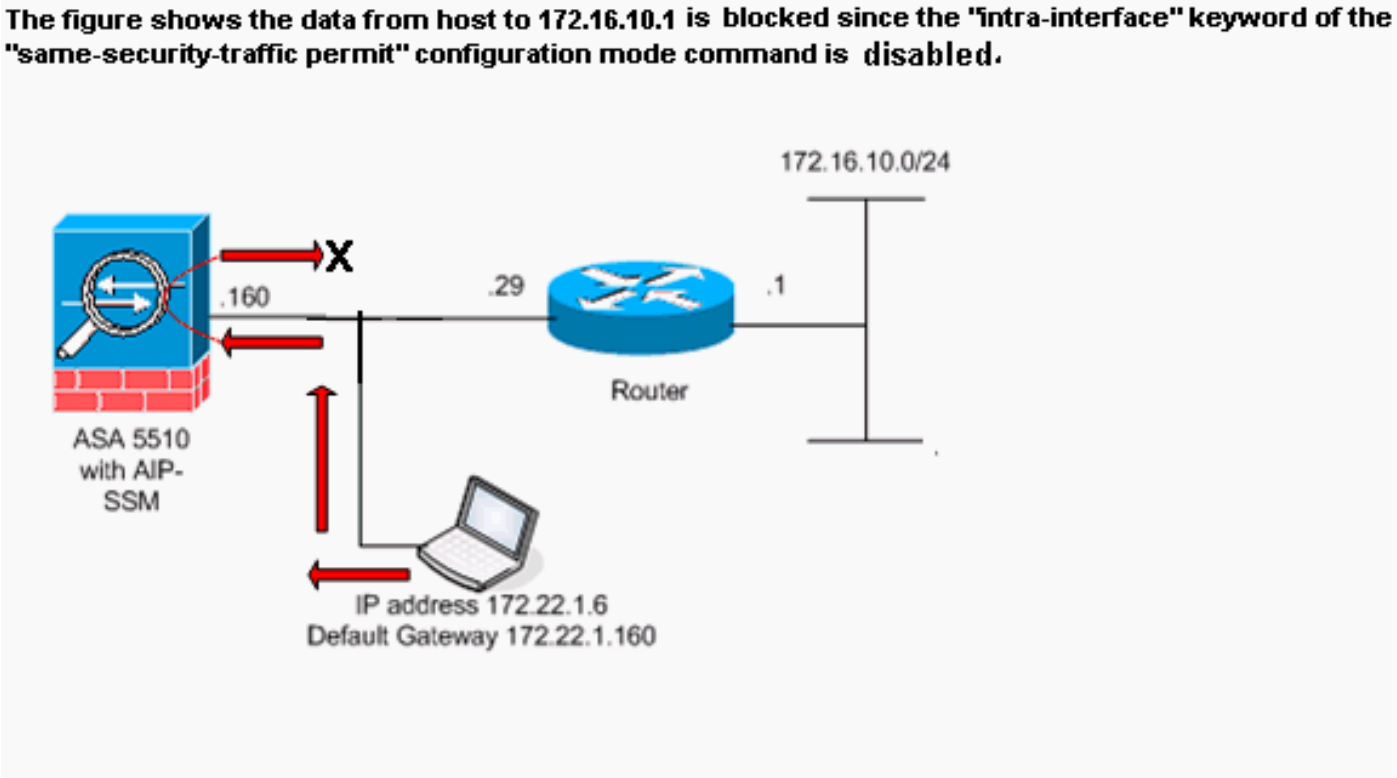
المنتجات ذات الصلة

كما يمكن إستخدام هذا التكوين مع Cisco 500 Series PIX الذي يشغل الإصدار 7.2(1) والإصدارات الأحدث.

الاصطلاحات

أحلت cisco فني طرف إتفاق لمعلومة على وثيقة إتفاق.

معلومات أساسية



ملاحظة: ال ip ليس يخاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. هم rfc 1918 عنوان أن يتلقى يكون استعملت في مختبر بيئة.

يوضح هذا الجدول تكوين ASA الذي بدأ:

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
```

استكشاف الأخطاء وإصلاحها

توضح هذه الأقسام العديد من سيناريوهات التكوين، ورسائل syslog ذات الصلة، ومخرجات packet-tracer فيما يتعلق بالاتصالات داخل الواجهة.

لم يتم تمكين إتصالات الواجهة الداخلية

في تكوين ASA، يحاول المضيف 172.22.1.6 إختبار الاتصال بالمضيف 172.16.10.1. يرسل المضيف 172.22.1.6 حزمة طلب صدى ICMP إلى البوابة الافتراضية (ASA). لم يتم تمكين الاتصالات الداخلية على ASA. يقوم ASA بإسقاط حزمة طلب الارتداد. فشل إختبار الاتصال. استعملت ال ASA أن يتحرى المشكلة.

يبدي هذا مثال الإنتاج من syslog رسالة و packet-tracer:

- هذه هي رسالة syslog التي تم تسجيلها إلى المخزن المؤقت:

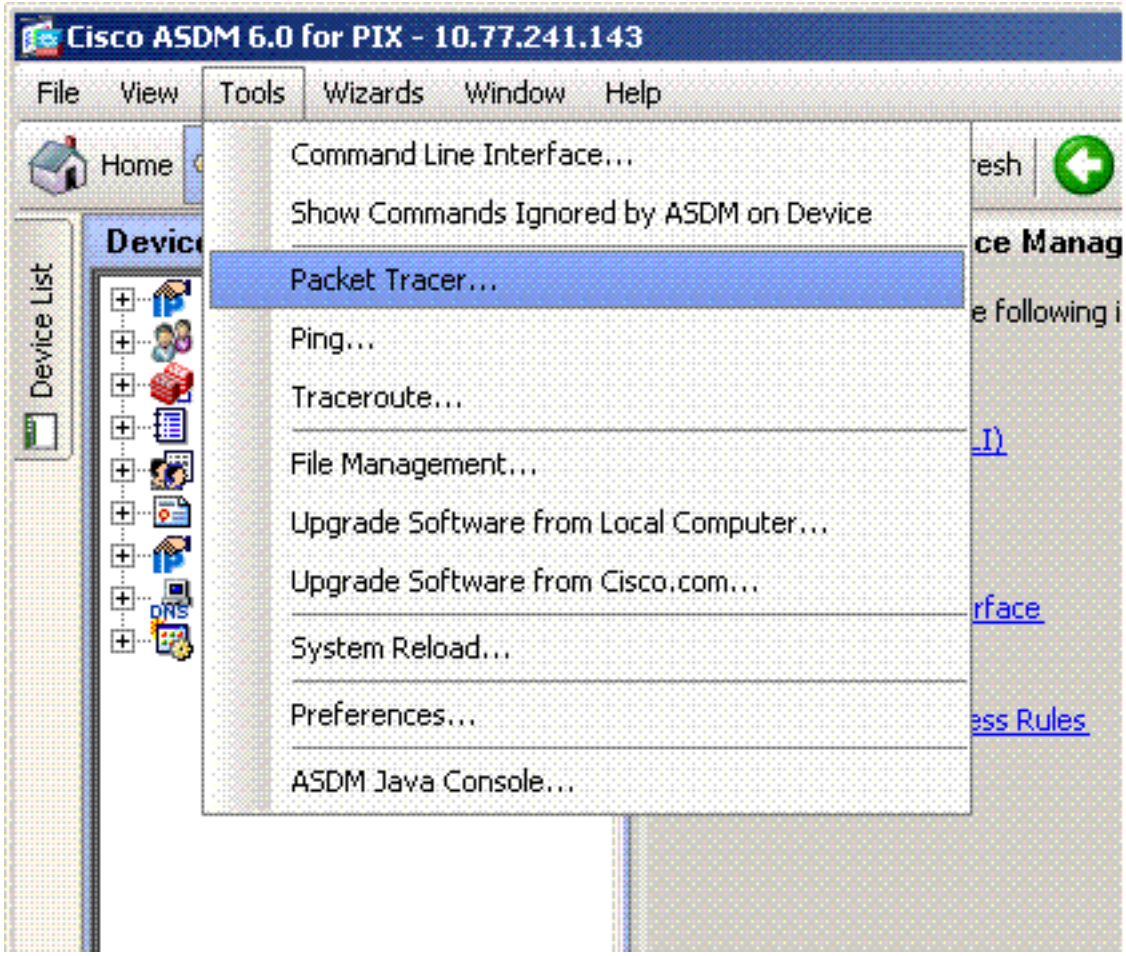
```
ciscoasa(config)#show logging
Output is suppressed. %ASA-3-106014: Deny inbound icmp src outside:172.22.1.6 dst ---!
(outside:172.16.10.1 (type 8, code 0
```

- هذا ال packet-tracer إنتاج:

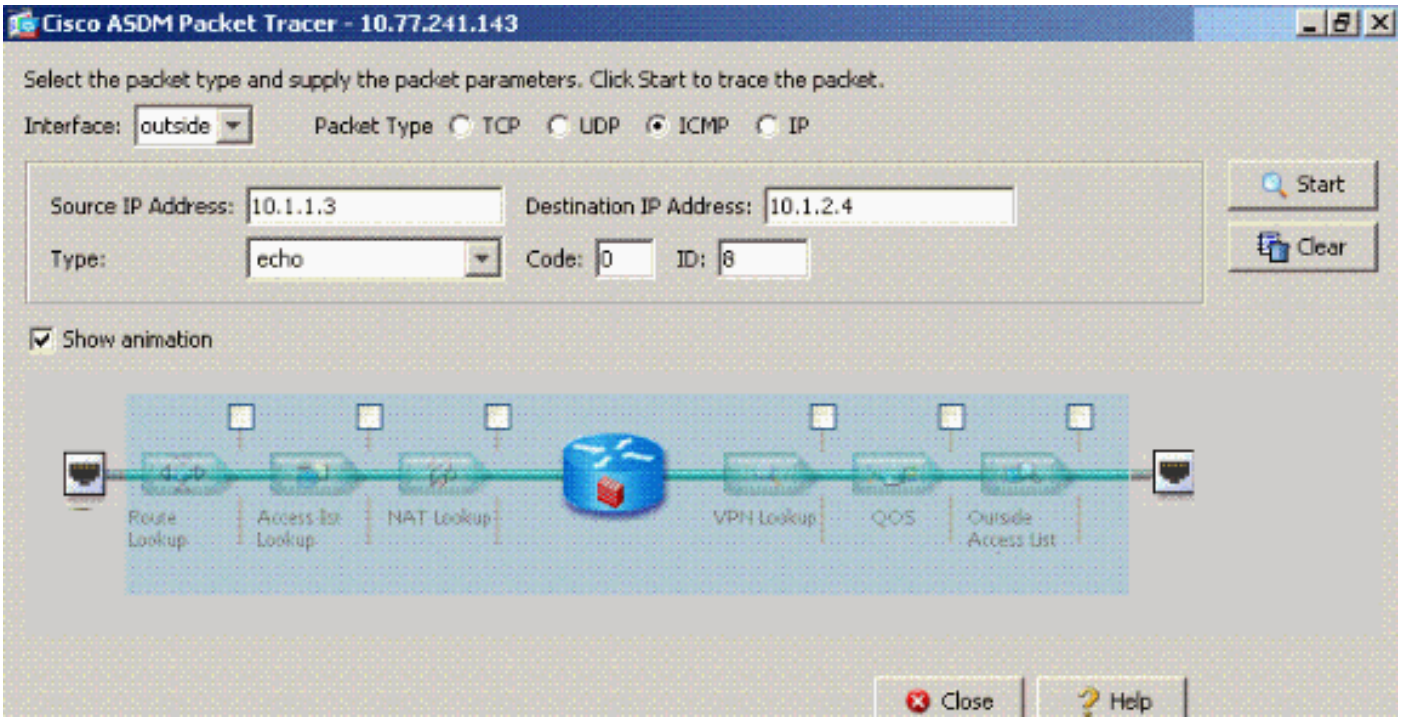
```
ciscoasa(config)#packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1 detailed
                                                                    Phase: 1
                                                              Type: FLOW-LOOKUP
                                                                      :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
```

يتم عرض مكافئ أوامر CLI في ASDM في الأشكال التالية:

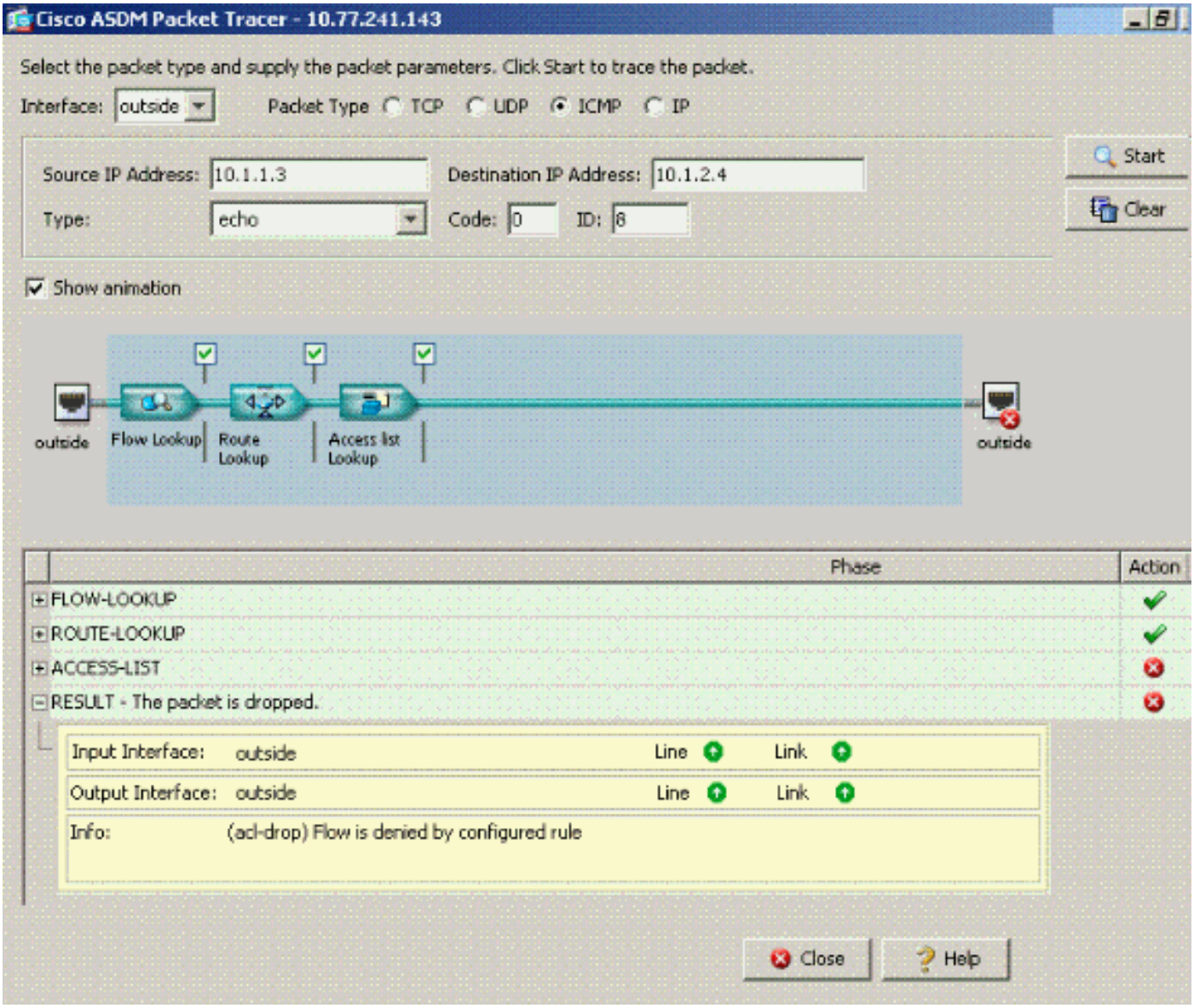
الخطوة 1:



الخطوة 2:



يتم تعطيل إخراج Packet-tracer باستخدام الأمر **نفسه-intra-interface** allowed **security-traffic**.



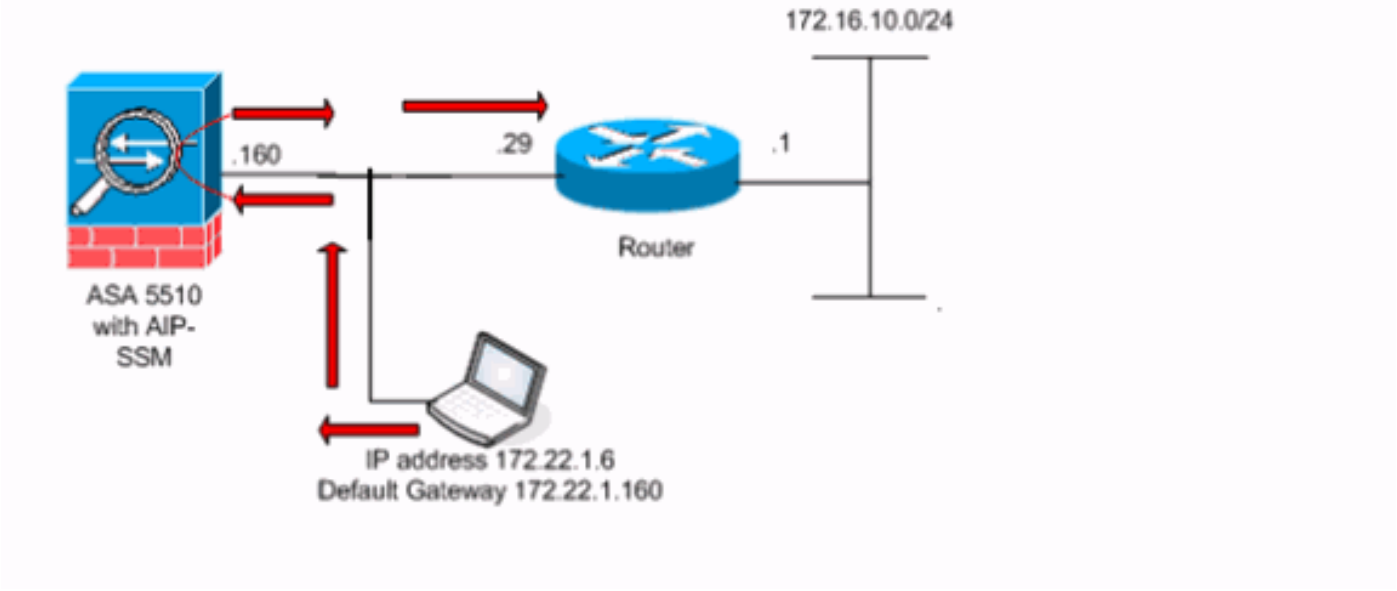
إخراج Packet-tracer. . .تشير إلى أن إعداد التكوين الافتراضي يقوم بحظر حركة المرور. يحتاج المسؤول إلى التحقق من التكوين الجاري تشغيله لضمان تمكين الاتصالات بين الواجهة. في هذه الحالة، يحتاج تكوين ASA إلى تمكين الاتصالات الداخلية للواجهة (**نفس** الأمر **security-traffic permit intra-interface**).

```
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
```

تم تمكين الاتصالات الداخلية

تم الآن تمكين الاتصالات بين الواجهات. تتم إضافة الأمر **نفسه-security-traffic permit intra-interface** إلى التكوين السابق. المضيف 172.22.1.6 محاولة إختبار الاتصال بالمضيف 172.16.10.1. يرسل المضيف 172.22.1.6 حزمة طلب صدى ICMP إلى البوابة الافتراضية (ASA). المضيف 172.22.1.6 يسجل الردود الناجحة من 172.16.10.1. يقوم ASA بتمرير حركة مرور ICMP بنجاح.

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.



تظهر هذه الأمثلة رسالة ASA syslog ومخرجات Packet-tracer:

- هذه هي رسائل syslog التي تم تسجيلها إلى المخزن المؤقت:

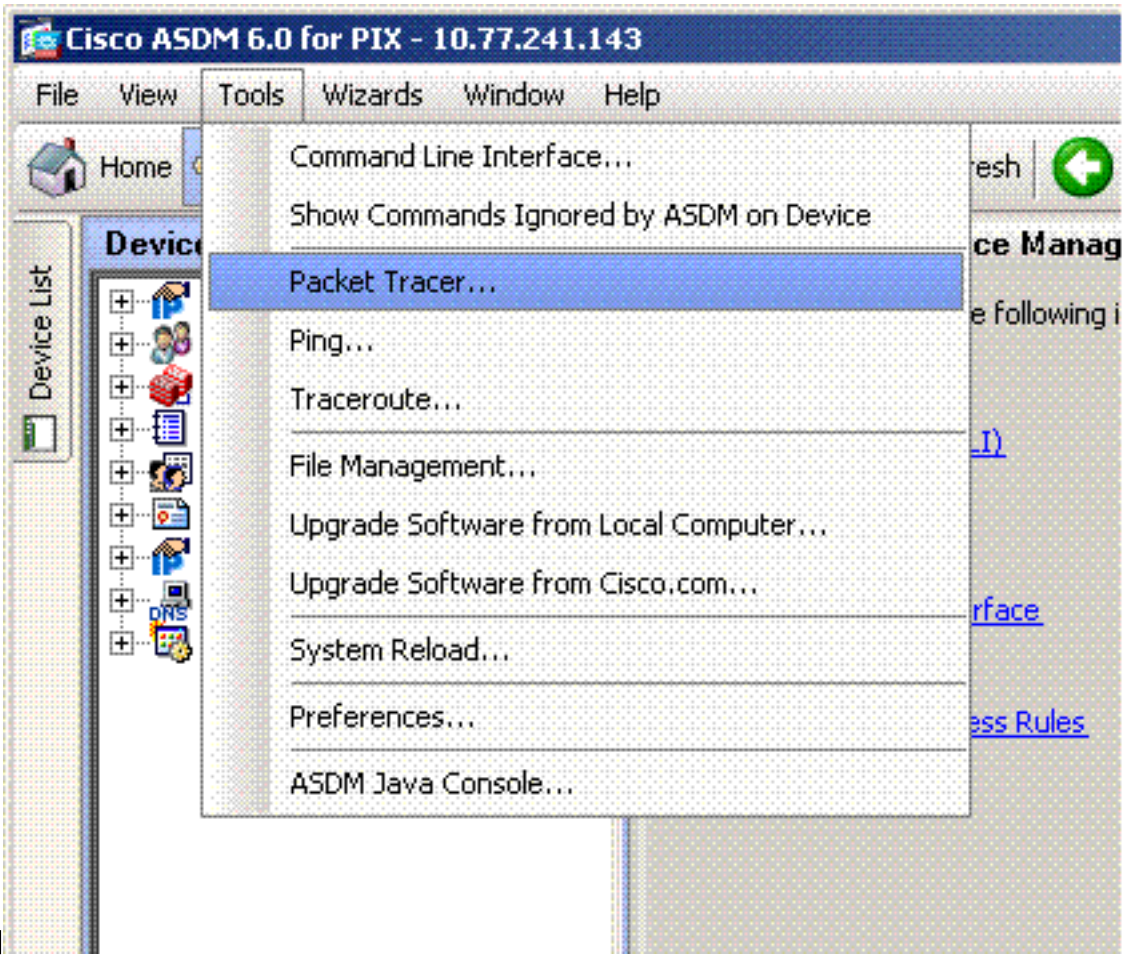
```
ciscoasa#show logging
Output is suppressed. %PIX-7-609001: Built local-host outside:172.22.1.6 %PIX-7-609001: ---!
        Built local-host outside:172.16.10.1 %PIX-6-302020: Built ICMP connection for faddr
      172.22.1.6/64560 gaddr 172.16.10.1/0 laddr 172.16.10.1/0 %PIX-6-302021: Teardown ICMP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

- هذا ال packet-tracer إنتاج:

```
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
```

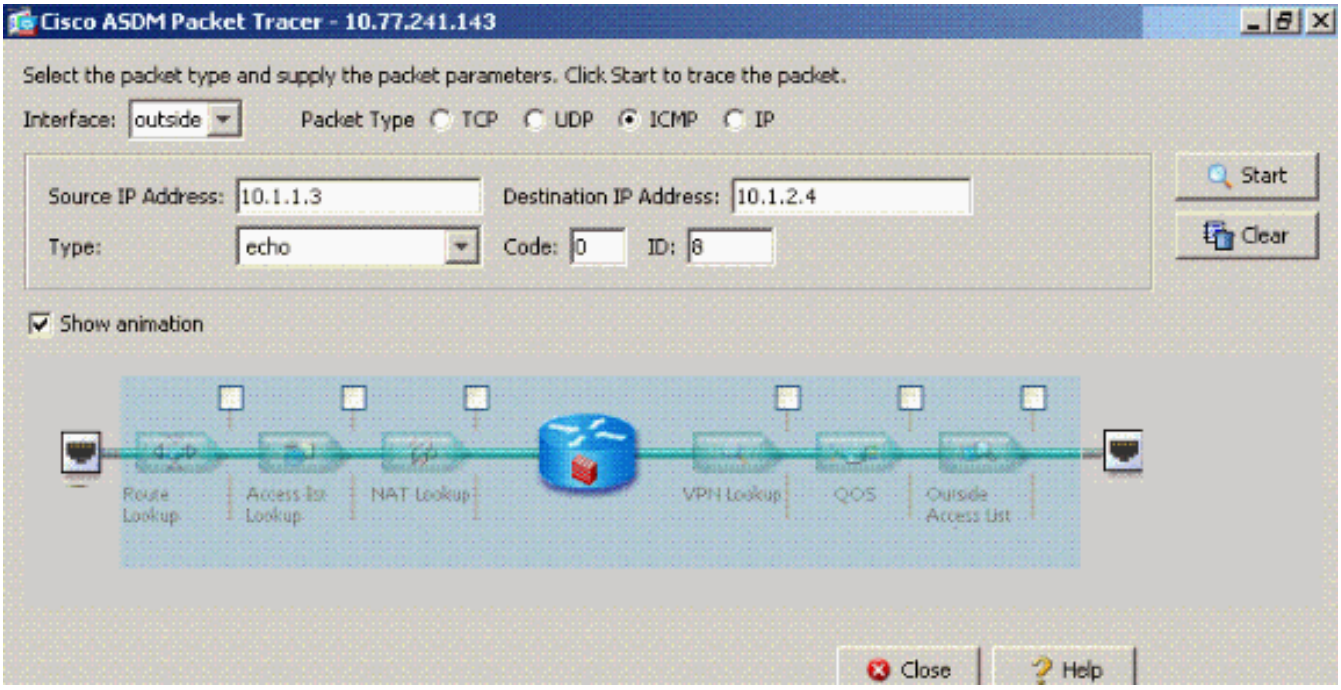
```
                                                Type: IP-OPTIONS
                                                        :Subtype
                                                   Result: ALLOW
                                                         :Config
                                               :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
```

يتم عرض مكافئ أوامر CLI في ASDM في الأشكال التالية:**الخطوة**

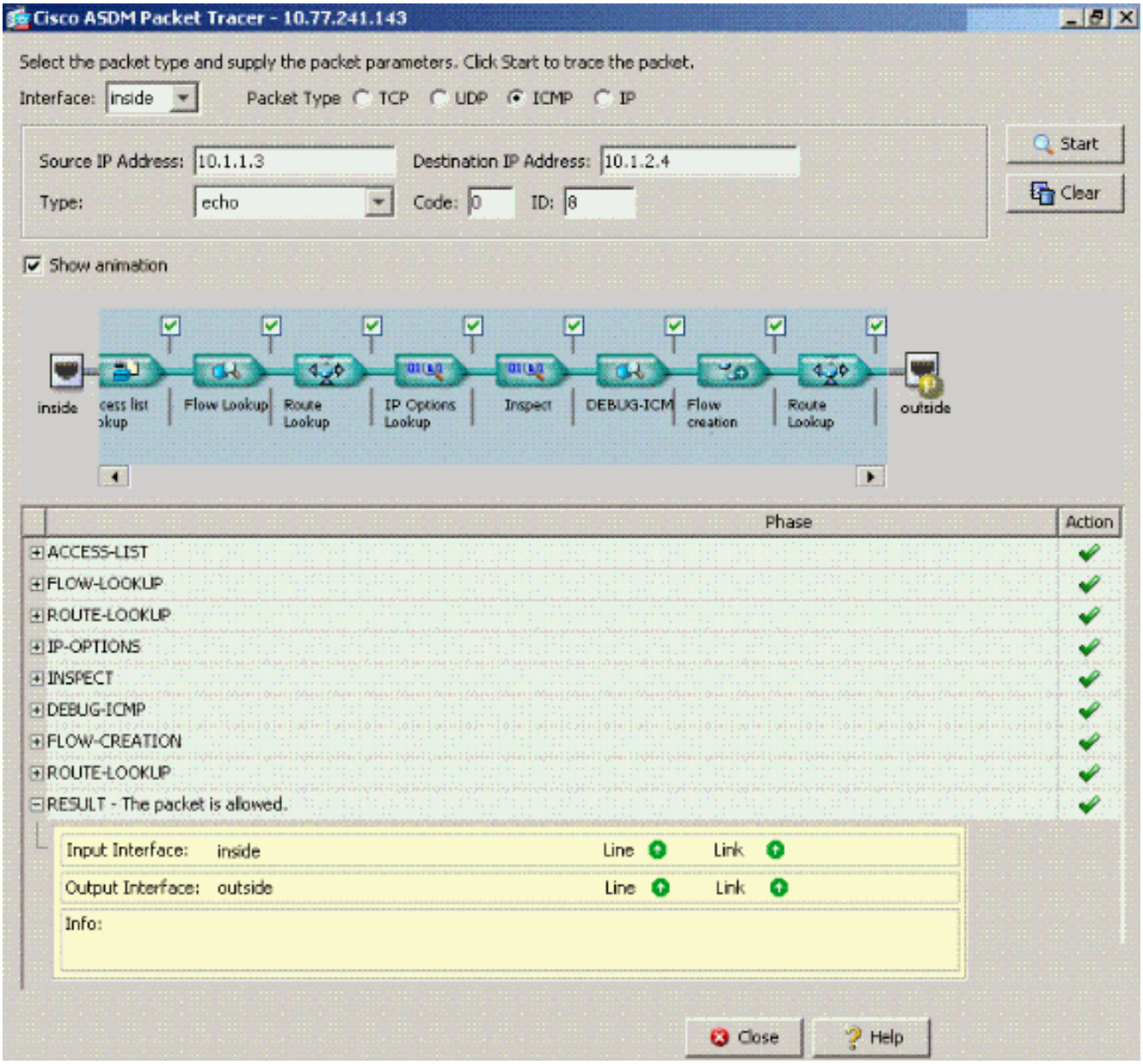


الخطوة 1:

الخطوة 2:



يتم إخراج packet-tracer مع تمكين الأمر **نفسه--security-traffic allowed intra** interface.



ملاحظة: لا يتم تطبيق قائمة الوصول على الواجهة الخارجية. في تكوين العينة، يتم تعيين مستوى الأمان 0 للواجهة الخارجية. وبشكل افتراضي، لا يسمح جدار الحماية بحركة المرور من واجهة أمان منخفضة إلى واجهة أمان عالية. قد يؤدي هذا إلى اعتقاد المسؤولين بأن حركة مرور البيانات داخل الواجهة غير مسموح بها على الواجهة الخارجية (ذات مستوى الأمان المنخفض) دون إذن من قائمة الوصول. ومع ذلك، تمر حركة مرور الواجهة نفسها بحرية عندما لا يتم تطبيق قائمة الوصول على الواجهة.

مكنت intra-interface ومرت حركة مرور إلى AIP-SSM للفحص

يمكن تمرير حركة مرور البيانات الداخلية للواجهة إلى AIP-SSM للفحص. يفترض هذا القسم أن المسؤول قام بتكوين ASA لإعادة توجيه حركة مرور البيانات إلى AIP-SSM وأن المسؤول يعرف كيفية تكوين برنامج IPS 5.x.

عند هذه النقطة يحتوي تكوين ASA على التكوين العينة السابقة، ويتم تمكين الاتصالات داخل الواجهة، وإعادة توجيه جميع (أي) حركة مرور إلى AIP-SSM. تم تعديل توقيع IPS 2004 لإسقاط حركة مرور طلب الارتداد. المضيف 172.22.1.6 محاولة إختبار الاتصال بالمضيف 172.16.10.1. يرسل المضيف 172.22.1.6 حزمة طلب صدى ICMP إلى البوابة الافتراضية (ASA). يرسل ال ASA ال echo طلب ربط إلى ال AIP-SSM لفحصه. تقوم AIP-SSM بإسقاط حزمة البيانات لكل تكوين IPS.

تظهر هذه الأمثلة رسالة ASA syslog ومخرج Packet-tracer:

- هذه هي رسالة syslog التي تم تسجيلها إلى المخزن المؤقت:

```
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
```

- هذا ال packet-tracer إنتاج:

```
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
```

من المهم ملاحظة أنه يجب على المسؤولين إستخدام أكبر عدد ممكن من أدوات أستكشاف الأخطاء وإصلاحها عند إجراء بحث عن مشكلة. يوضح هذا المثال كيف يمكن لأداتين مختلفتين لاستكشاف الأخطاء وإصلاحها طلاء صور مختلفة. وكل من الأداتين تحكي قصة كاملة معا. يسمح سياسة تكوين ASA بحركة المرور ولكن تكوين IPS لا يسمح بذلك.

تم تمكين الواجهة الداخلية وقوائم الوصول المطبقة على واجهة

يستخدم هذا القسم نموذج التكوين الأصلي في هذا المستند، مع تمكين الاتصالات داخل الواجهة، وقائمة الوصول التي تم تطبيقها على الواجهة التي تم إختبارها. تتم إضافة هذه الخطوط إلى التكوين. المقصود من قائمة الوصول أن تكون تمثيلا بسيطا لما يمكن تكوينه على جدار حماية الإنتاج.

```
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
```

المضيف 172.22.1.6 محاولة إختبار الاتصال بالمضيف 172.16.10.1. يرسل المضيف 172.22.1.6 حزمة طلب صدى ICMP إلى البوابة الافتراضية (ASA). يقوم ASA بإسقاط حزمة طلب الارتداد لكل قواعد قائمة الوصول. يفشل إختبار الاتصال للمضيف 172.22.1.6.

تظهر هذه الأمثلة رسالة ASA syslog ومخرج Packet-tracer:

- هذه هي رسالة syslog التي تم تسجيلها إلى المخزن المؤقت:

```
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
```

- هذا ال packet-tracer إنتاج:

```
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
```

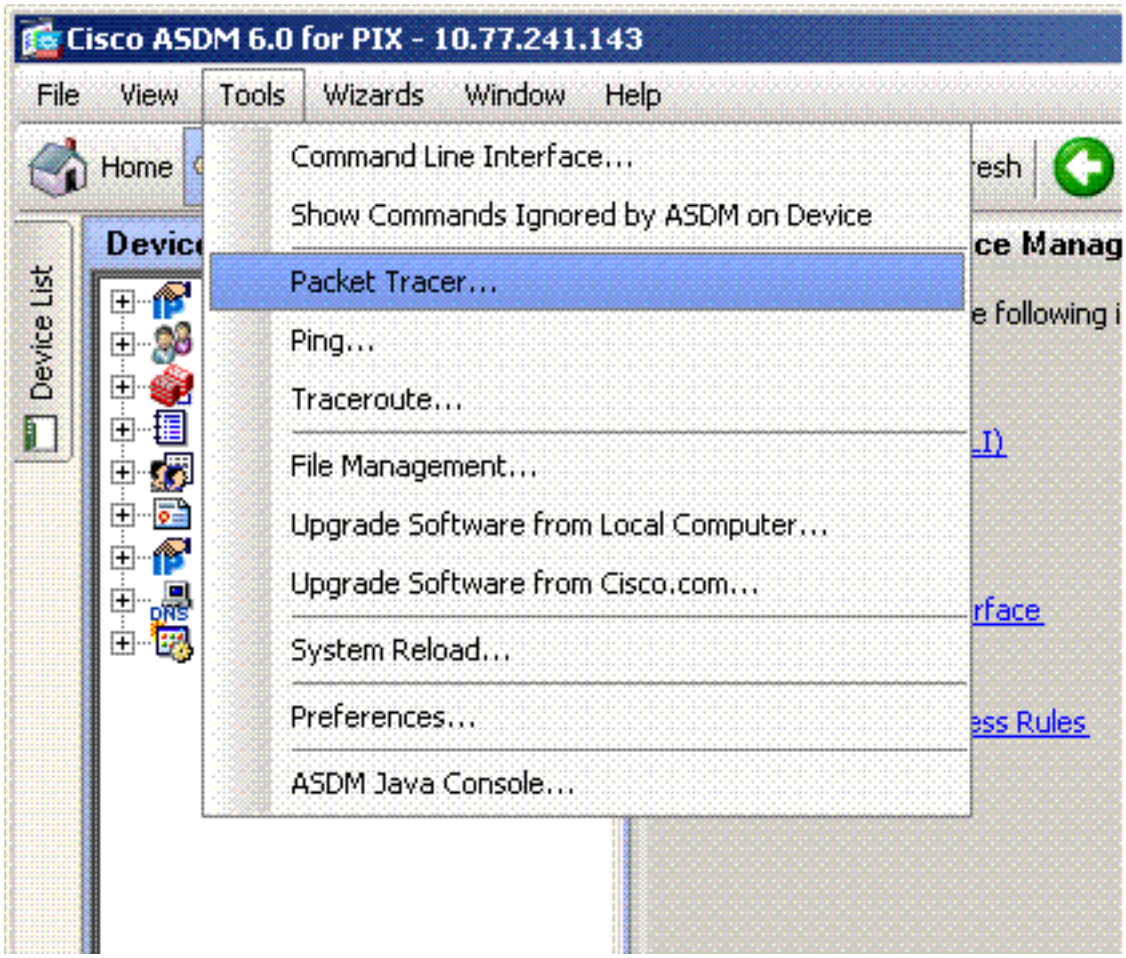
راجع packet-tracer للحصول على مزيد من المعلومات حول الأمر **packet-tracer**.

ملاحظة: في حالة ما إذا كانت قائمة الوصول المطبقة على الواجهة تتضمن عبارة رفض، فإن إخراج تغييرات أداة تتبع الحزم. على سبيل المثال:

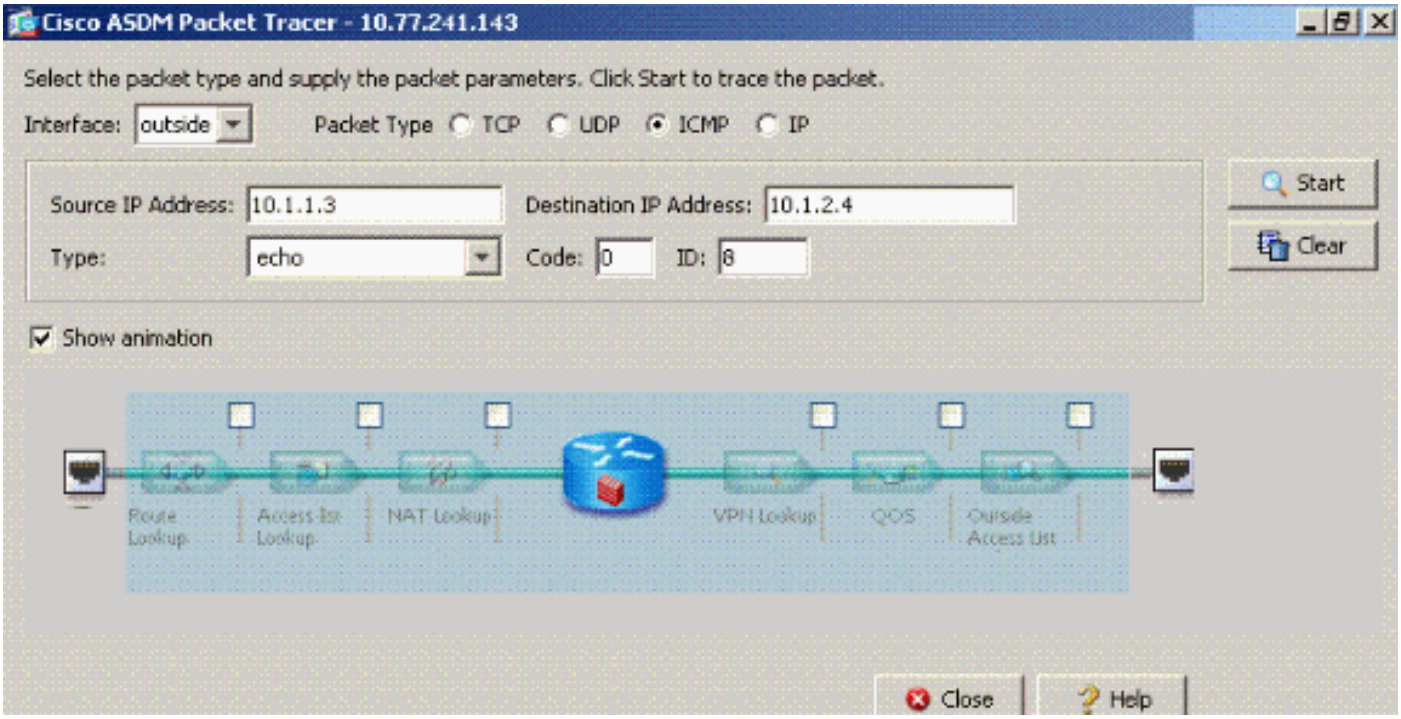
```
ciscoasa(config)#access-list outside_acl permit tcp any host 172.22.1.147 eq 80
ciscoasa(config)#access-list outside_acl deny ip any any
ciscoasa(config)#access-group outside_acl in interface outside
ciscoasa#packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1 detailed
Output is suppressed.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

يتم عرض ما يعادل أوامر CLI الواردة أعلاه في ASDM في الأشكال التالية:

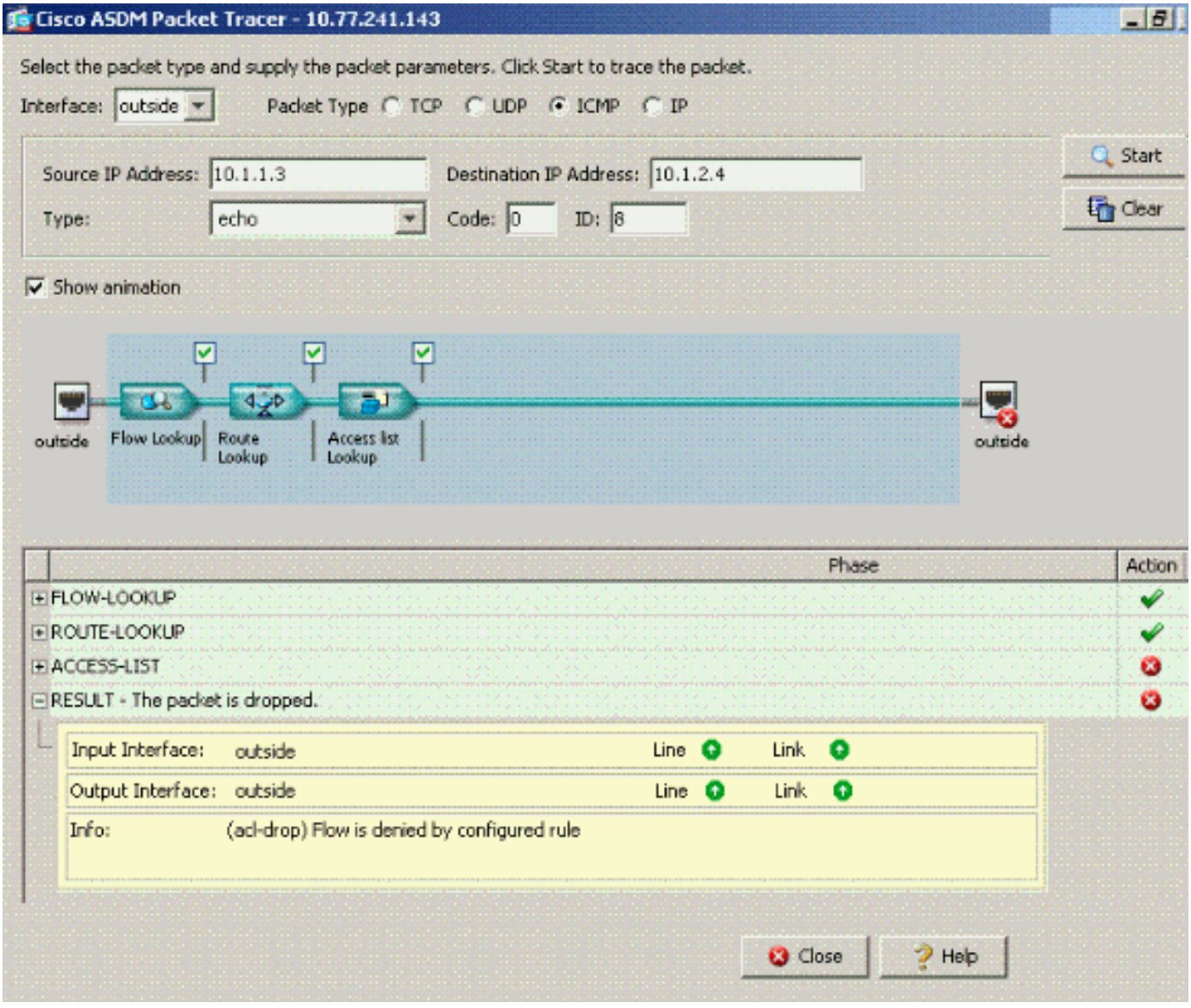
الخطوة 1:



الخطوة 2:



يتم تمكين الأمر packet-tracer output مع الأمر **نفسه-enabled** allowed-interface **security-traffic و-access** أمر تم تكوينه لرفض الحزم. **list outside_acl extended deny ip any**

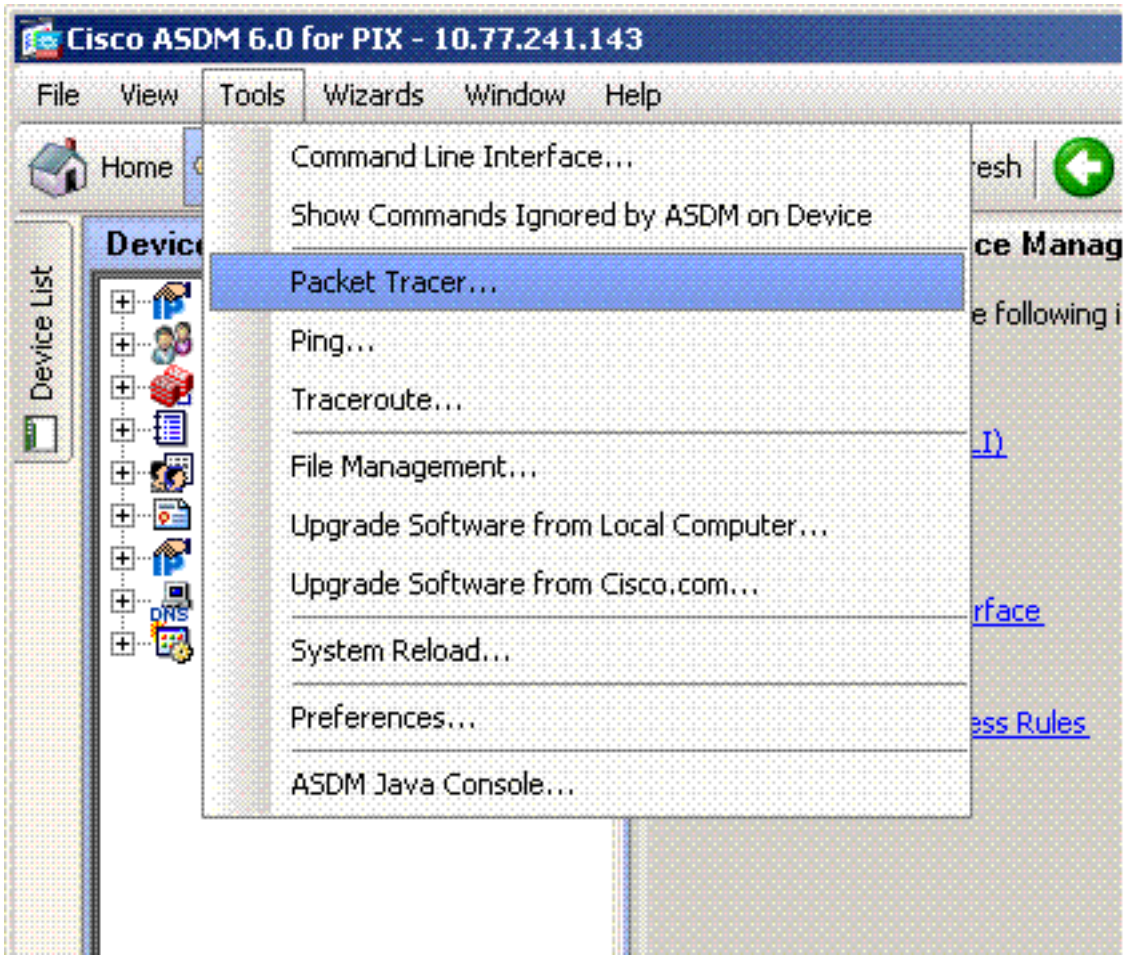


إذا كانت الاتصالات داخل الواجهة مطلوبة على واجهة معينة وتم تطبيق قوائم الوصول على نفس الواجهة، فيجب أن تسمح قواعد قائمة الوصول بحركة المرور داخل الواجهة. باستخدام الأمثلة الواردة في هذا القسم، يلزم كتابة قائمة الوصول على النحو التالي:

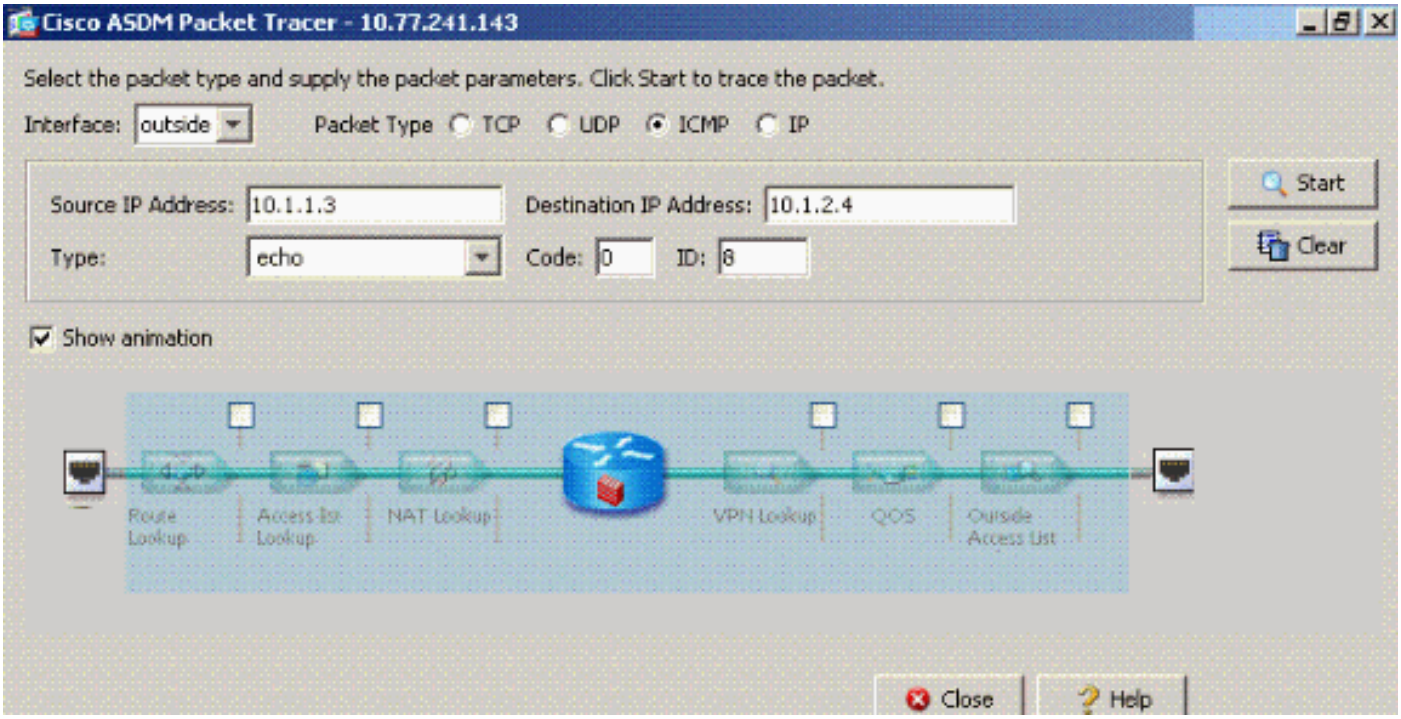
```
ciscoasa(config)#access-list outside_acl permit tcp any host 172.22.1.147 eq 80
ciscoasa(config)#access-list outside_acl permit ip 172.22.1.0 255.255.255.0 172.16.10.0
255.255.255.0
represents a locally !--- connected network on the ASA. !--- 255.255.255.0 172.22.1.0 ---!
172.16.10.0 255.255.255.0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

يتم عرض ما يعادل أوامر CLI الواردة أعلاه في ASDM في الأشكال التالية:

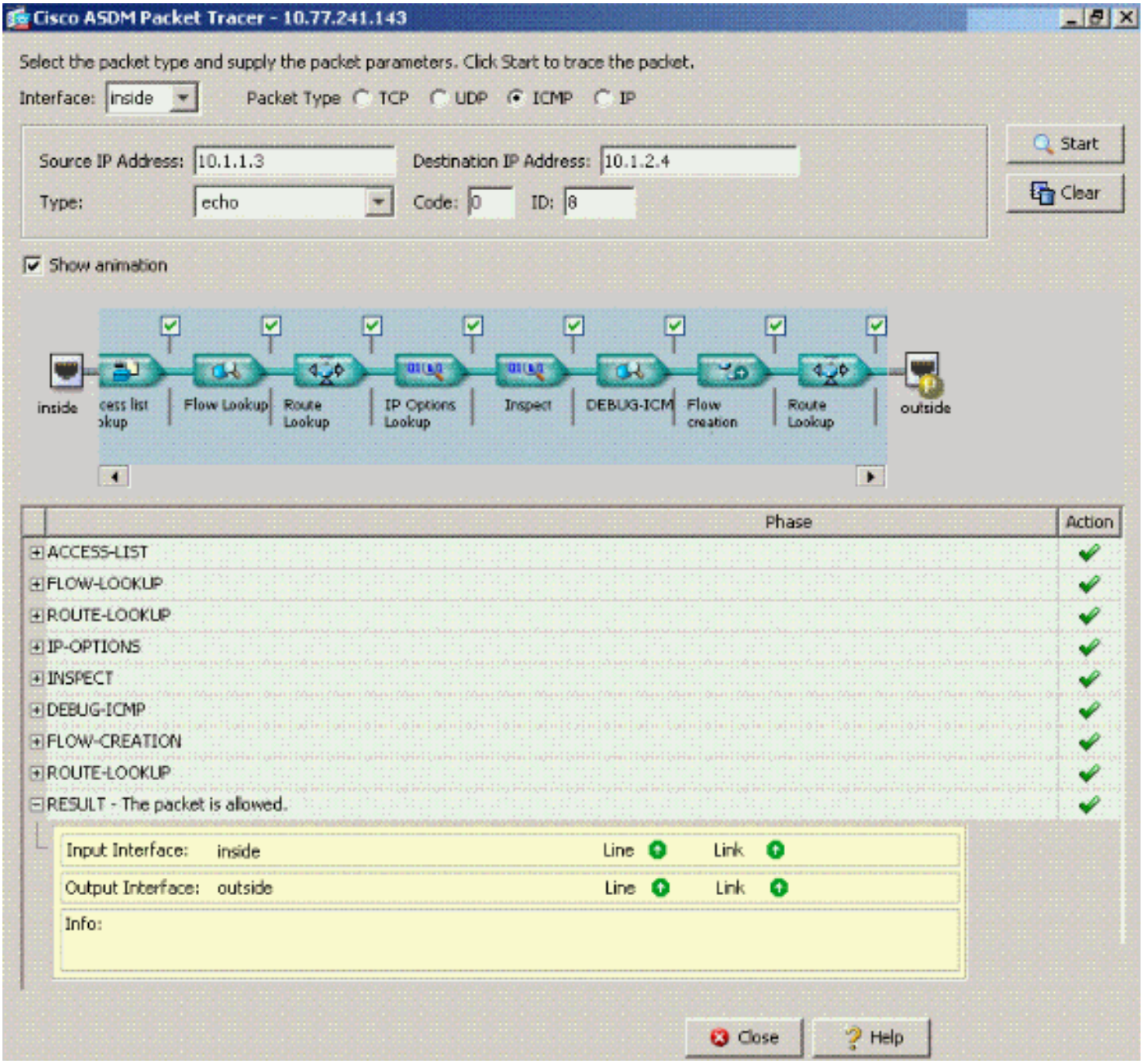
الخطوة 1:



الخطوة 2:



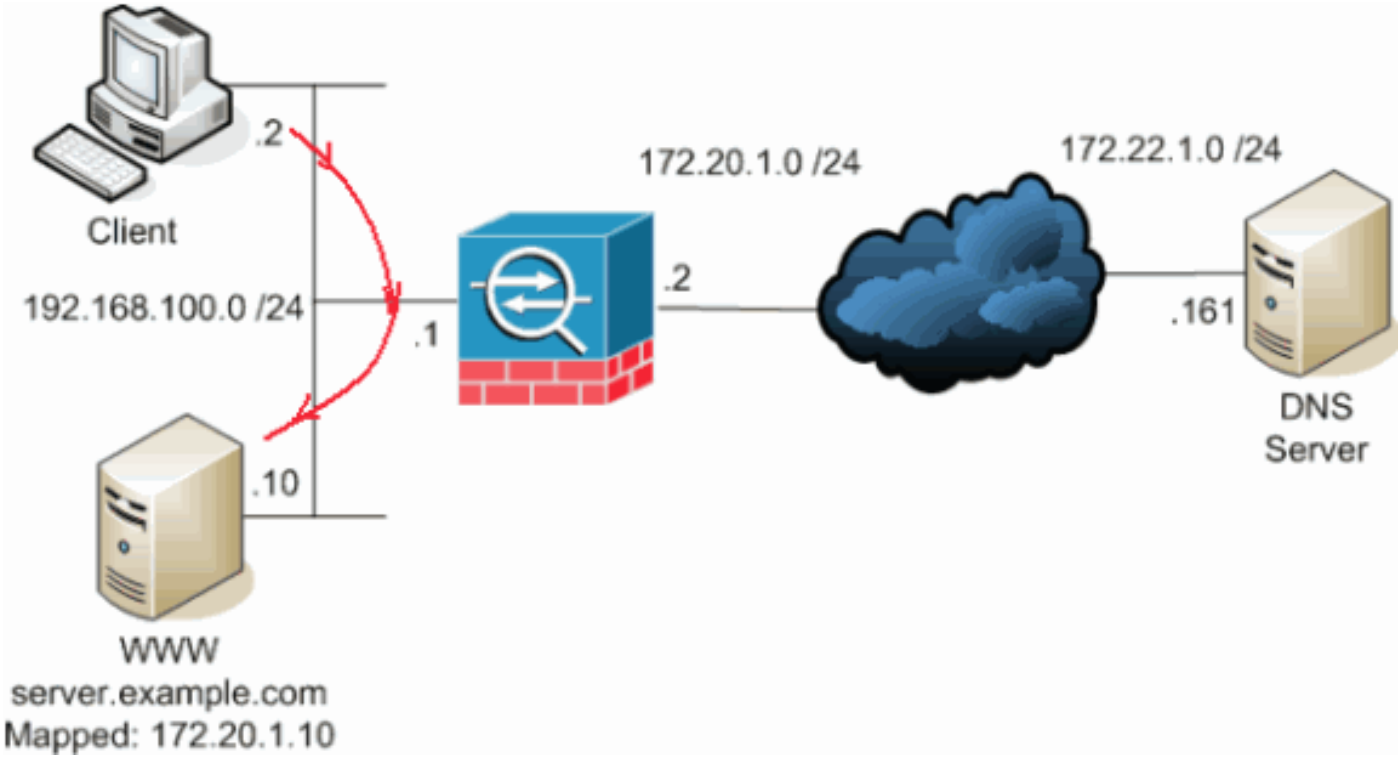
يتم تمكين الأمر **packet-tracer** الناتج مع الأمر **نفسه-enabled** allowed-interface **security-traffic والأمر** any **access-list outside_acl extended deny ip any** أمر تم تكوينه على الواجهة نفسها حيث تكون حركة مرور البيانات بين الواجهة مطلوبة.



ارجع إلى access-list extended وaccess-group للحصول على مزيد من المعلومات حول أوامر **access-list** و**access-group**.

Intra-Interface ممكن مع ساكن إستاتيكي و NAT

يشرح هذا القسم سيناريو يحاول فيه مستخدم داخلي الوصول إلى خادم ويب الداخلي باستخدام عنوانه العام.



في هذه الحالة، يريد العميل في 192.168.100.2 إستخدام العنوان العام لخادم WWW (على سبيل المثال، 172.20.1.10). يتم توفير خدمات DNS للعميل بواسطة خادم DNS الخارجي في 172.22.1.161. نظرا لوجود خادم DNS على شبكة عامة أخرى، فإنه لا يعرف عنوان IP الخاص لخادم WWW. بدلا من ذلك، يعرف خادم DNS العنوان المعين لخادم WWW 172.20.1.10.

هنا هذا حركة مرور من القارن داخلي ينبغي كنت ترجمت وأعدت من خلال القارن داخلي أن يبلغ ال WWW نادل. هذا يسمى تسريحة الشعر. يمكن تنفيذ هذا الإجراء من خلال الأوامر التالية:

```
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
```

للحصول على تفاصيل التكوين الكاملة والمزيد من المعلومات حول التصغير، ارجع إلى التصغير باستخدام الاتصال بين الواجهات.

تفكير تقدمي في قائمة الوصول

ليست جميع سياسات الوصول إلى جدار الحماية هي نفسها. بعض سياسات الوصول أكثر تحديدا من غيرها. في حالة تمكين الاتصالات داخل الواجهة وعدم وجود قائمة وصول مطبقة على جميع الواجهات في جدار الحماية، قد يكون من المفيد إضافة قائمة وصول في الوقت الذي يتم فيه تمكين الاتصالات داخل الواجهة. تحتاج قائمة الوصول المطبقة إلى السماح بالاتصالات داخل الواجهة وكذلك الحفاظ على متطلبات سياسة الوصول الأخرى.

يوضح هذا المثال هذه النقطة. يقوم ASA بتوصيل شبكة خاصة (داخل الواجهة) بالإنترنت (خارج الواجهة). لا تحتوي واجهة ASA الداخلية على قائمة وصول مطبقة. بشكل افتراضي، يتم السماح بجميع حركة مرور IP من الداخل إلى الخارج. يكمن الاقتراح في إضافة قائمة وصول تشبه هذا المخرج:

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

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

تستمر هذه المجموعة من قوائم الوصول في السماح بجميع حركة مرور IP. يذكر سطر (أسطر) قائمة الوصول المحددة للاتصالات داخل الواجهة المسؤولين بأنه يجب السماح بالاتصالات داخل الواجهة بواسطة قائمة وصول مطبقة.

معلومات ذات صلة

- مرجع أمر جهاز الأمان من Cisco، الإصدار 7.2
- رسائل سجل نظام جهاز الأمان من Cisco، الإصدار 7.2
- برنامج جدار حماية Cisco PIX
- ASA: إرسال حركة مرور الشبكة من ASA إلى مثال تكوين AIP SSM
- دعم منتجات أجهزة الأمان القابلة للتكيف ASA 5500 Series من Cisco
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).