PIX/ASA 7.2(1) et versions ultérieures : Communications intra-interface

Contenu

Introduction

Ce document aide à dépanner les problèmes communs qui se posent quand vous activez les communications intra-interface sur un dispositif de sécurité ASA (Adaptive Security Appliance) ou PIX qui fonctionne dans la version de logiciel 7.2(1) et ultérieure. La version de logiciel 7.2(1) inclut la capacité de router des données de texte en clair à l'intérieur et à l'extérieur de la même interface. Entrez la commande **same-security-traffic permit intra-interface** afin d'activer cette fonction. Ce document suppose que l'administrateur réseau a activé cette fonction ou qu'il a l'intention de le faire. La configuration et le dépannage sont fournis à l'aide de l'interface de ligne de commande (CLI).

Remarque: Ce document se concentre sur les données en clair (non cryptées) qui arrivent et partent du dispositif ASA. Les données cryptées ne sont pas discutées.

Afin d'activer la communication intra-interface sur une configuration ASA/PIX pour IPsec, référez-vous à Exemple de configuration de PIX/ASA et du client VPN pour le VPN Internet public sur une barrette.

Afin d'activer la communication intra-interface sur une configuration ASA pour SSL, référez-vous à ASA 7.2(2) : Exemple de configuration du client VPN SSL (SVC) pour le VPN Internet public sur une barrette.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Listes d'accès
- Acheminement
- Module de services de sécurité Advanced Inspection and Prevention (AIP-SSM) Système de protection contre les intrusions (IPS) - la connaissance de ce module est seulement nécessaire si le module est installé et opérationnel.
- Version de logiciel IPS 5.x - La connaissance du logiciel IPS n'est pas requise si l'AIP-SSM n'est pas utilisé.

Composants utilisés

- ASA 5510 7.2(1) et ultérieure
- AIP-SSM-10 qui exécute le logiciel IPS 5.1.1

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

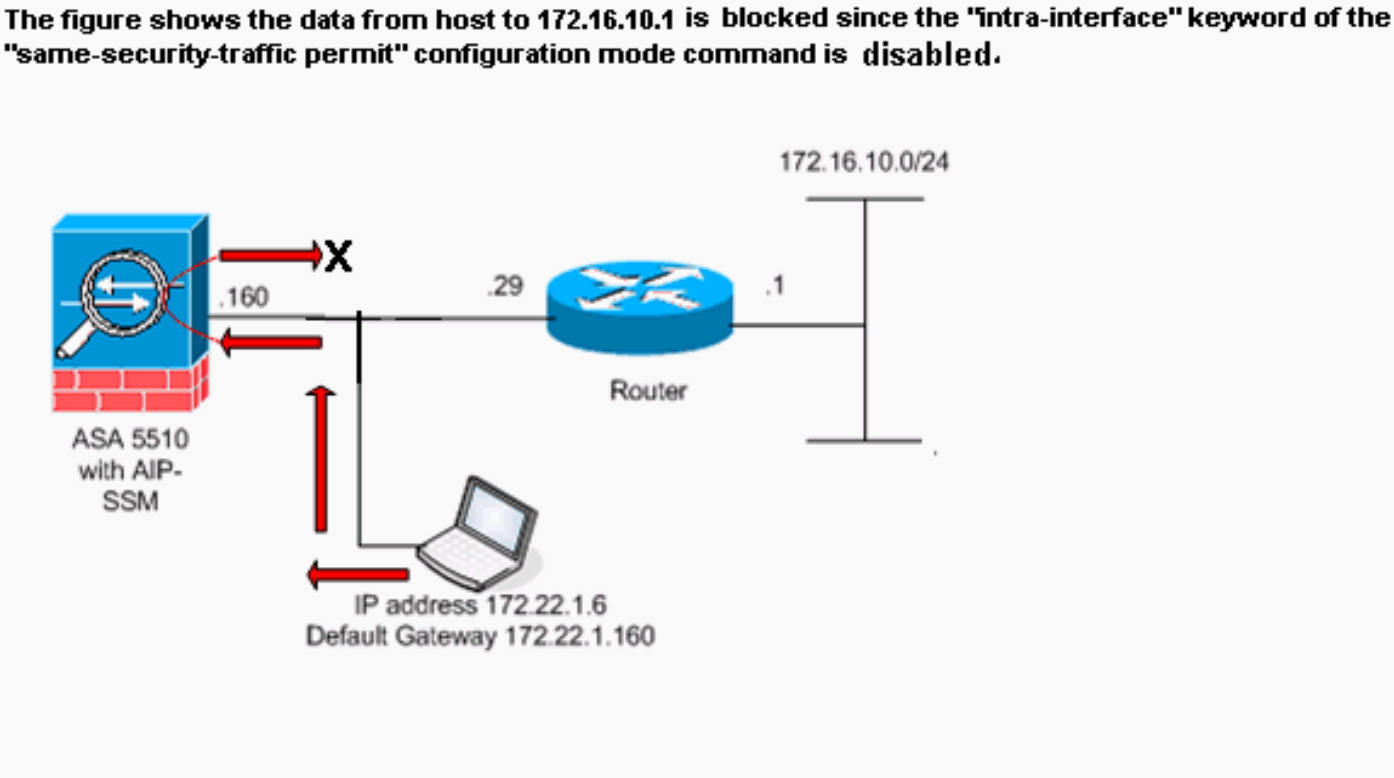
Produits connexes

Cette configuration peut également être utilisée avec un dispositif de sécurité PIX de la gamme Cisco 500 qui exécute la version 7.2(1) et ultérieure.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales



Remarque: Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisées dans un environnement de laboratoire.

Cette table montre le début de la configuration de l'ASA :

ASA

```
ciscoasa#show running-config : Saved : ASA Version
7.2(1) ! hostname ciscoasa enable password
8Ry2YjIyt7RRXU24 encrypted names ! !--- The IP
addressing assigned to interfaces. interface Ethernet0/0
nameif inside security-level 100 ip address 10.1.1.2
255.255.255.0 ! interface Ethernet0/1 nameif outside
security-level 0 ip address 172.22.1.160 255.255.255.0 !
interface Ethernet0/2 shutdown no nameif no security-
level no ip address ! interface Management0/0 shutdown
no nameif no security-level no ip address ! passwd
2KFQnbNIdI.2KYOU encrypted ftp mode passive !--- Notice
that there are no access-lists. pager lines 24 logging
enable logging buffered debugging mtu inside 1500 mtu
outside 1500 no asdm history enable arp timeout 14400 !-
-- There are no network address translation (NAT) rules.
!--- The static routes are added for test purposes.
route inside 10.2.2.0 255.255.255.0 10.1.1.100 1 route
outside 172.16.10.0 255.255.255.0 172.22.1.29 1 timeout
xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00
udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323
0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute no
snmp-server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart telnet timeout 5 ssh timeout 5 console timeout
0 ! class-map inspection_default match default-
inspection-traffic ! ! policy-map type inspect dns
preset_dns_map parameters message-length maximum 512
```

```
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323 h225
inspect h323 ras inspect netbios inspect rsh inspect
rtsp inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global prompt hostname context
Cryptochecksum:
```

Dépannage

Ces sections illustrent plusieurs scénarios de configuration, les messages syslog associés et les sorties du traceur de paquet par rapport aux communications intra-interface.

Communications intra-interface non activées

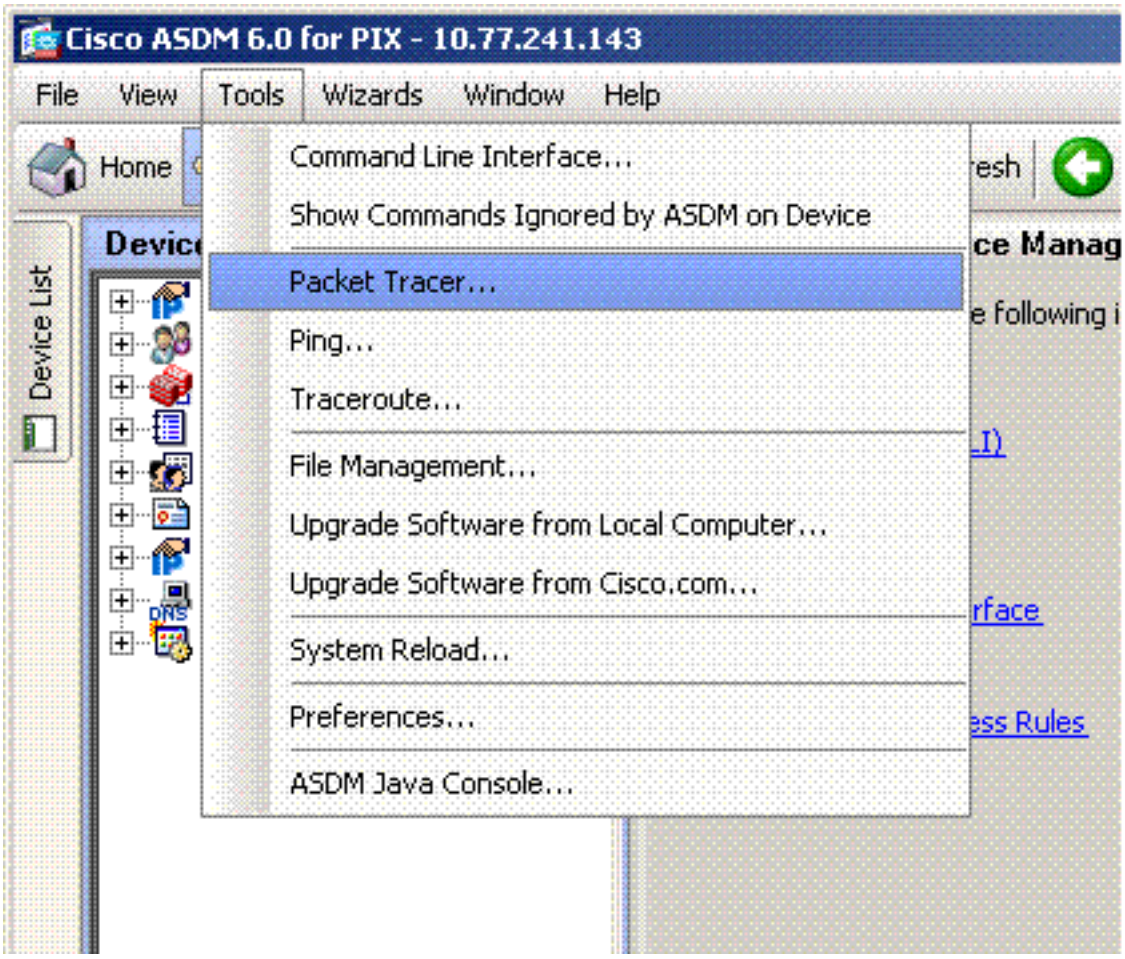
Dans ASA Configuration, l'hôte 172.22.1.6 essaye d'envoyer un ping à l'hôte 172.16.10.1. L'hôte 172.22.1.6 envoie un paquet de demande d'écho ICMP à la passerelle par défaut (ASA). Les communications intra-interface n'ont pas été activées sur l'ASA. L'ASA supprime le paquet de demande d'écho. Le ping de test échoue. L'ASA est utilisé pour dépanner le problème.

Cet exemple montre la sortie des messages syslog et d'un traceur de paquets :

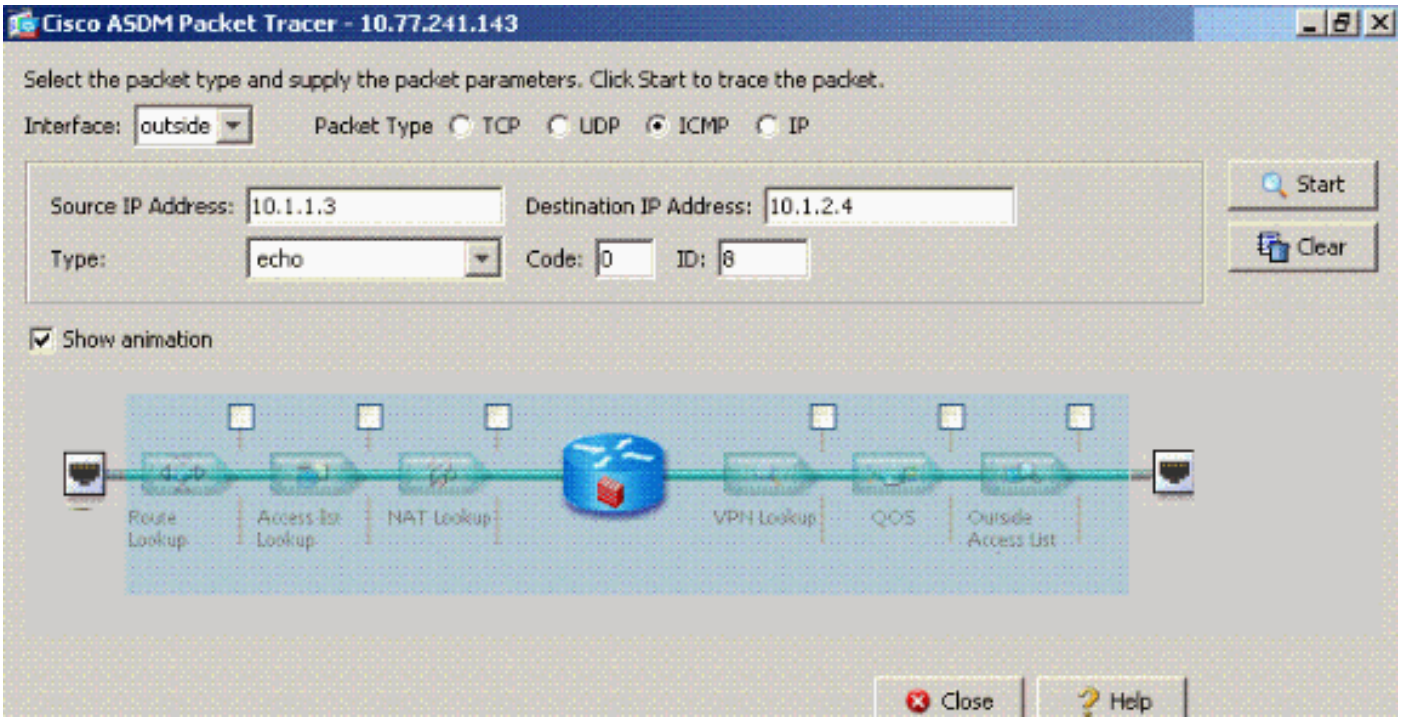
- Voici le message syslog enregistré dans la mémoire tampon :`ciscoasa(config)#`**`show logging`** *`!-- Output is suppressed.`* `%ASA-3-106014: Deny inbound icmp src outside:172.22.1.6 dst outside:172.16.10.1 (type 8, code 0)`
- Voici la sortie du traceur de paquets :`ciscoasa(config)#`**`packet-tracer 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`

L'équivalent des commandes CLI dans l'ASDM est montré dans ces figures :

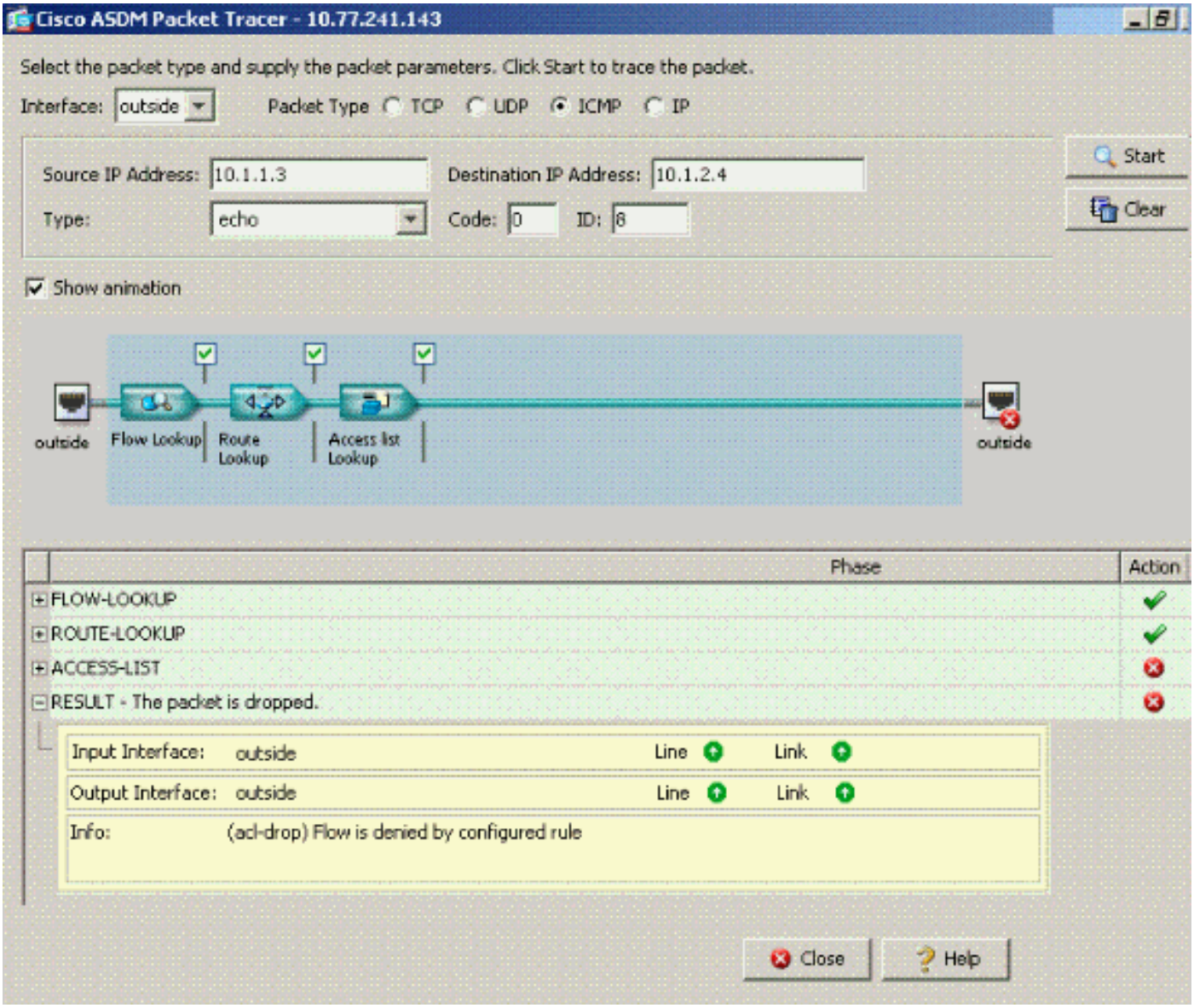
Étape 1 :



Étape 2 :



La sortie du traceur de paquets avec la commande **same-security-traffic permit intra-interface** désactivée.



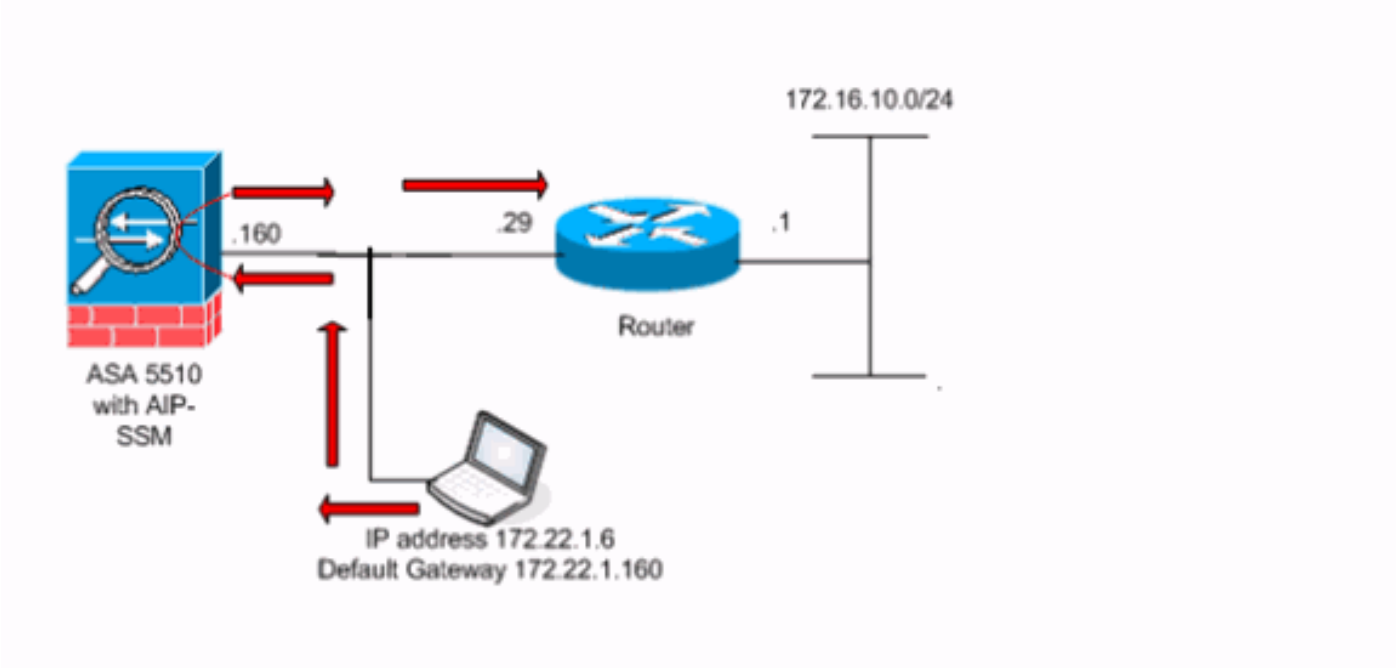
La sortie du traceur de paquets drop… implicit rule suggère qu'un paramètre de configuration par défaut bloque le trafic. L'administrateur doit vérifier la configuration en cours afin de s'assurer que les communications intra-interface sont activées. Dans ce cas, la configuration de l'ASA a besoin que les communications intra-interface soient activées (**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...
```

Communications intra-interface activées

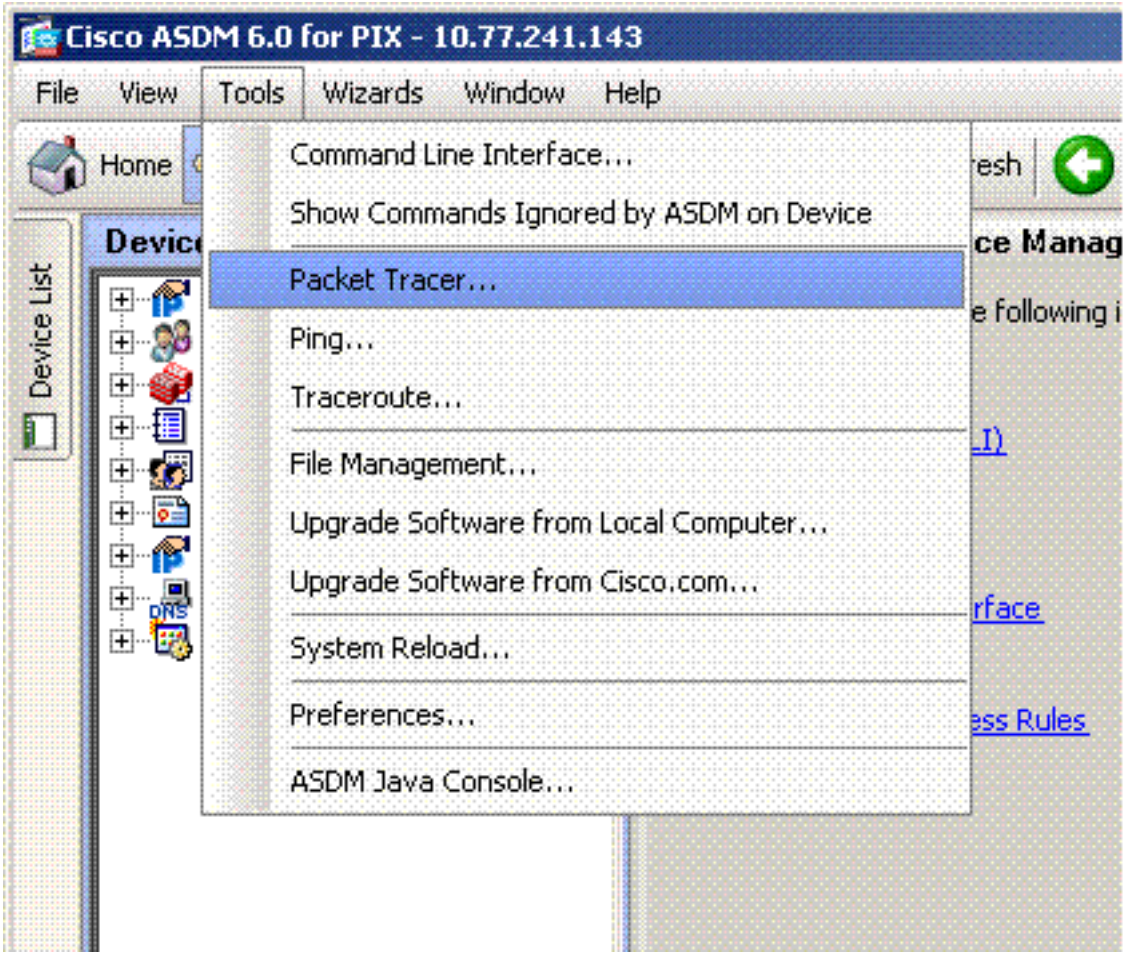
Les communications intra-interface sont maintenant activées. La commande **same-security-traffic permit intra-interface** est ajoutée à la configuration précédente. L'hôte 172.22.1.6 essaye d'envoyer un ping à l'hôte 172.16.10.1. L'hôte 172.22.1.6 envoie un paquet de demande d'écho ICMP à la passerelle par défaut (ASA). L'hôte 172.22.1.6 enregistre des réponses réussies en provenance de 172.16.10.1. L'ASA transmet le trafic ICMP avec succès.

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.

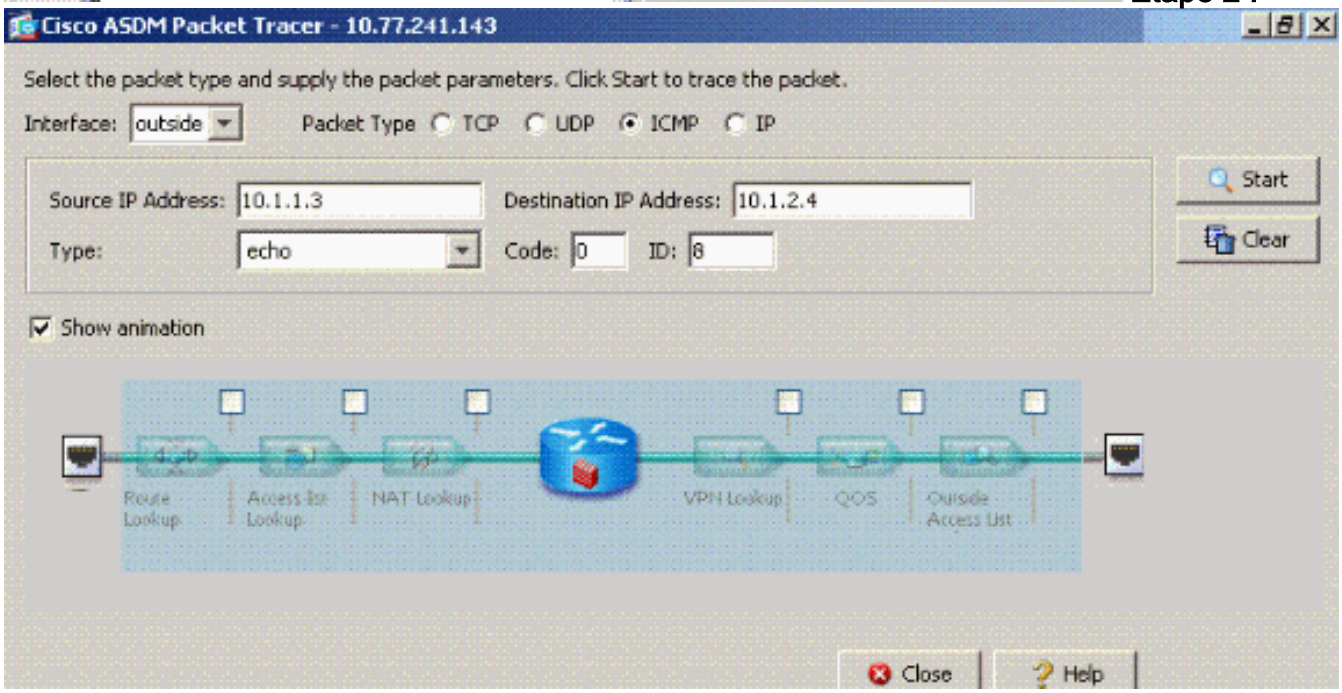


Ces exemples montrent le message syslog d'ASA et les sorties du traceur de paquets :

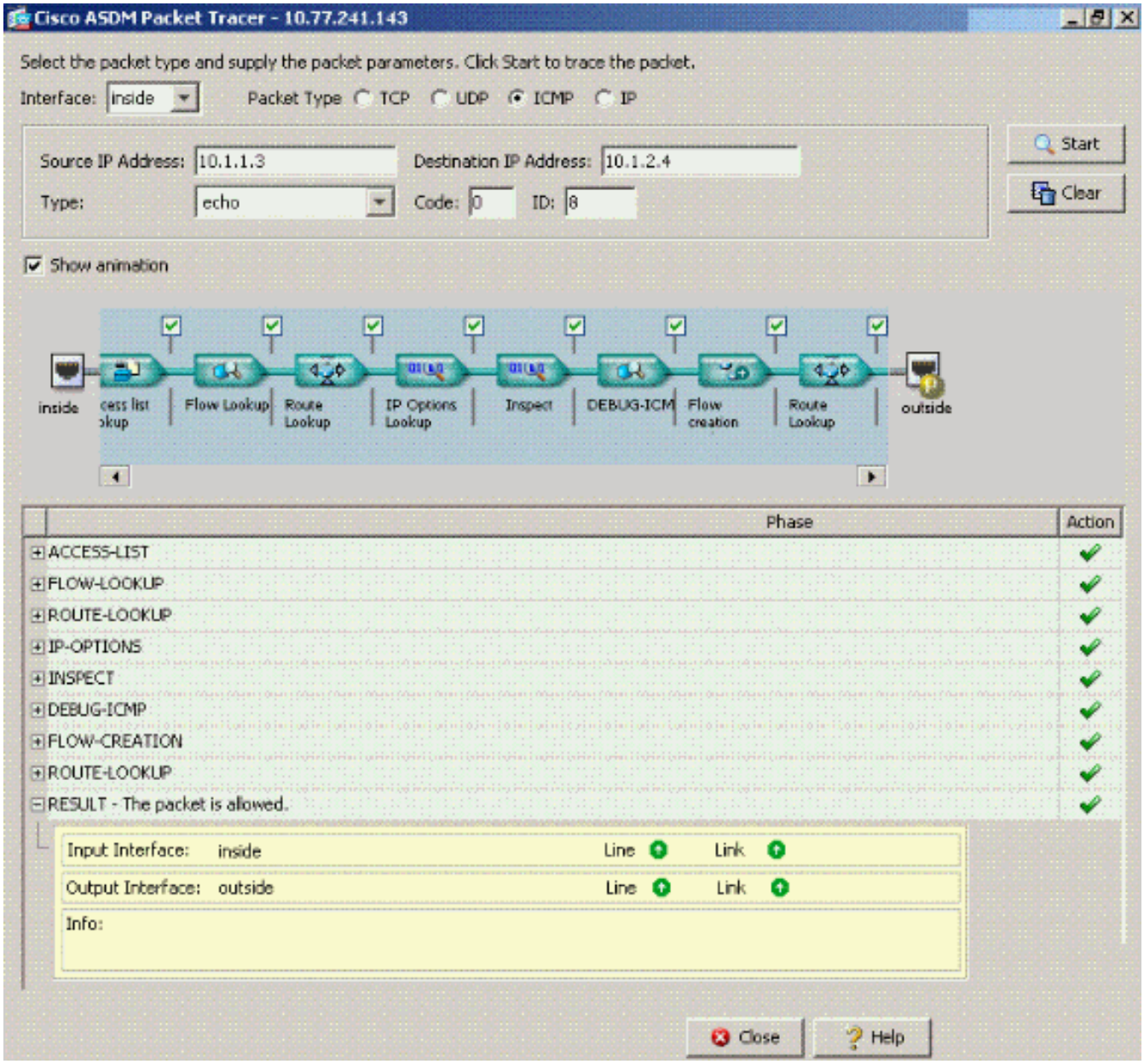
- Voici les messages syslog enregistré dans la mémoire tampon :`ciscoasa#`**`show logging`** *`!--- Output is suppressed.`* `%PIX-7-609001: Built local-host outside:172.22.1.6 %PIX-7-609001: Built local-host outside:172.16.10.1 %PIX-6-302020: Built ICMP connection for faddr 172.22.1.6/64560 gaddr 172.16.10.1/0 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`
- Voici la sortie du traceur de paquets :`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`*** L'équivalent des commandes CLI dans l'ASDM est montré dans ces figures :**Étape 1 :**



Étape 2 :



La sortie du traceur de paquets avec la commande **same-security-traffic permit intra-interface** activée.



Remarque: Aucune liste d'accès n'est appliquée à l'interface externe. Dans l'exemple de configuration, l'interface externe a reçu le niveau de sécurité 0. Par défaut, le pare-feu n'autorise pas le trafic d'une interface à faible sécurité vers une interface à haute sécurité. Cela pourrait amener les administrateurs à croire que le trafic intra-interface n'est pas permis sur l'interface extérieure (basse sécurité) sans l'autorisation d'une liste d'accès. Cependant, le trafic d'une même interface est transmis librement lorsqu'aucune liste d'accès n'est appliquée à l'interface.

Intra-interface activé et trafic transmis au module AIP-SSM pour inspection

Le trafic intra-interface peut être transmis à l'AIP-SSM pour inspection. Cette section suppose que l'administrateur a configuré l'ASA pour acheminer le trafic vers l'AIP-SSM et qu'il sait configurer le logiciel IPS 5.x.

Àce stade, la configuration ASA contient l'exemple de configuration précédent, les communications intra-interface sont activées, et tout le trafic est acheminé vers l'AIP-SSM. La signature IPS 2004 est modifiée pour supprimer le trafic lié à la demande d'écho. L'hôte 172.22.1.6 essaye d'envoyer un ping à l'hôte 172.16.10.1. L'hôte 172.22.1.6 envoie un paquet de demande d'écho ICMP à la passerelle par défaut (ASA). L'ASA achemine le paquet de demande

d'écho vers l'AIP-SSM pour inspection. L'AIP-SSM supprime le paquet de données en fonction de la configuration IPS.

Ces exemples montrent le message syslog d'ASA et la sortie du traceur de paquets :

- Voici le message syslog enregistré dans la mémoire tampon :`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.`*
- Voici la sortie du traceur de paquets :`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.`*

Il est important de noter que les administrateurs devraient utiliser autant d'outils de dépannage que possible quand ils recherchent un problème. Cette exemple montre comment deux outils de dépannage différents peuvent décrire des tableaux différents. Les deux outils racontent ensemble une histoire complète. La stratégie de configuration ASA autorise le trafic, mais la configuration d'IPS ne l'autorise pas.

Intra-interface activé et listes d'accès appliquées à une interface

Cette section utilise l'exemple de configuration initial de ce document, avec communications intra-interface activées, et une liste d'accès appliquée à l'interface testée. Ces lignes sont ajoutées à la configuration. La liste d'accès est destinée à être une simple représentation de ce qui pourrait être configuré sur un pare-feu de production.

```
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.
```

L'hôte 172.22.1.6 essaye d'envoyer un ping à l'hôte 172.16.10.1. L'hôte 172.22.1.6 envoie un paquet de demande d'écho ICMP à la passerelle par défaut (ASA). L'ASA supprime le paquet de demande d'écho en fonction des règles de liste d'accès. Le ping de test de l'hôte 172.22.1.6 échoue.

Ces exemples montrent le message syslog d'ASA et la sortie du traceur de paquets :

- Voici le message syslog enregistré dans la mémoire tampon :`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]`
- Voici la sortie du traceur de paquets :`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
```

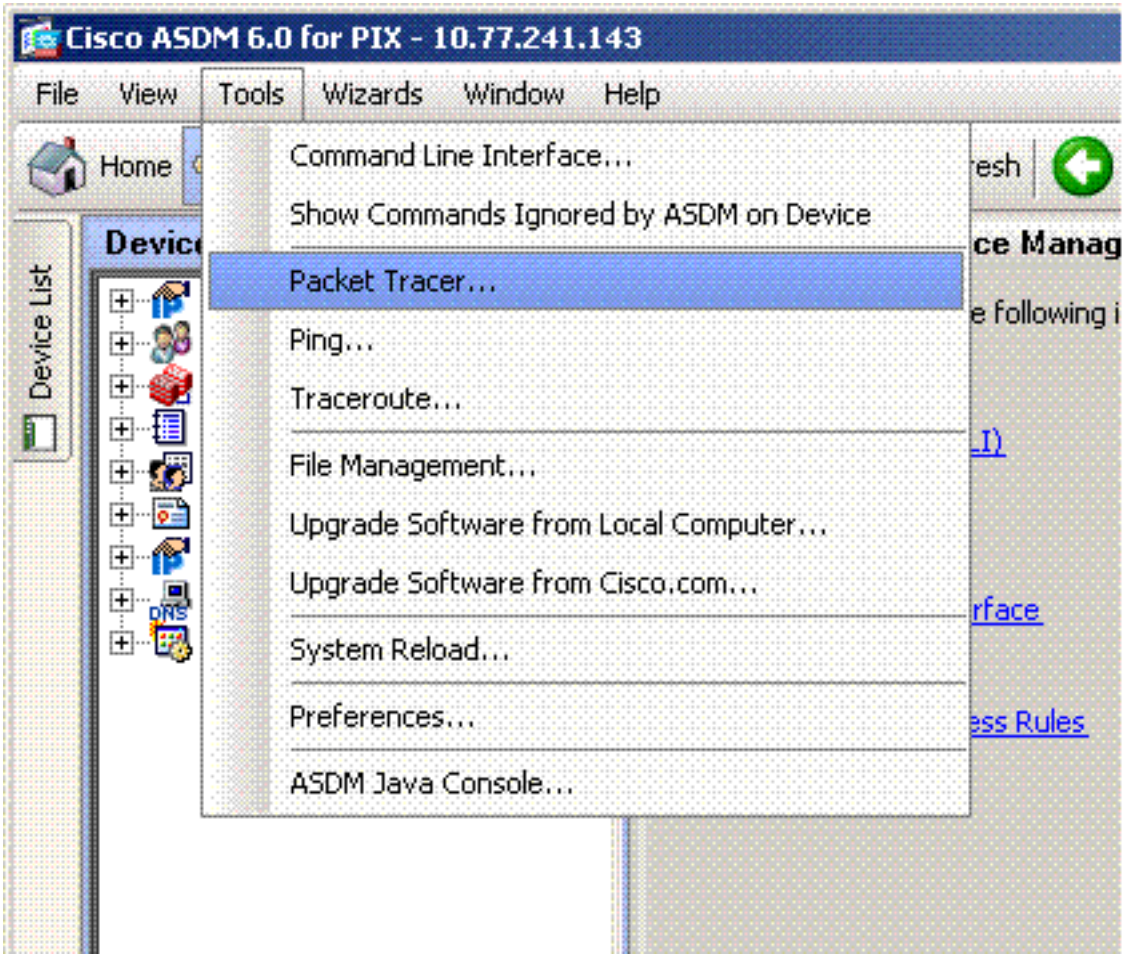
Référez-vous à traceur de paquets pour plus d'informations sur la commande **packet-tracer** .

Remarque: Dans le cas où la liste d'accès appliquée à l'interface inclut une déclaration de refus, la sortie du traceur de paquets change. Exemple :

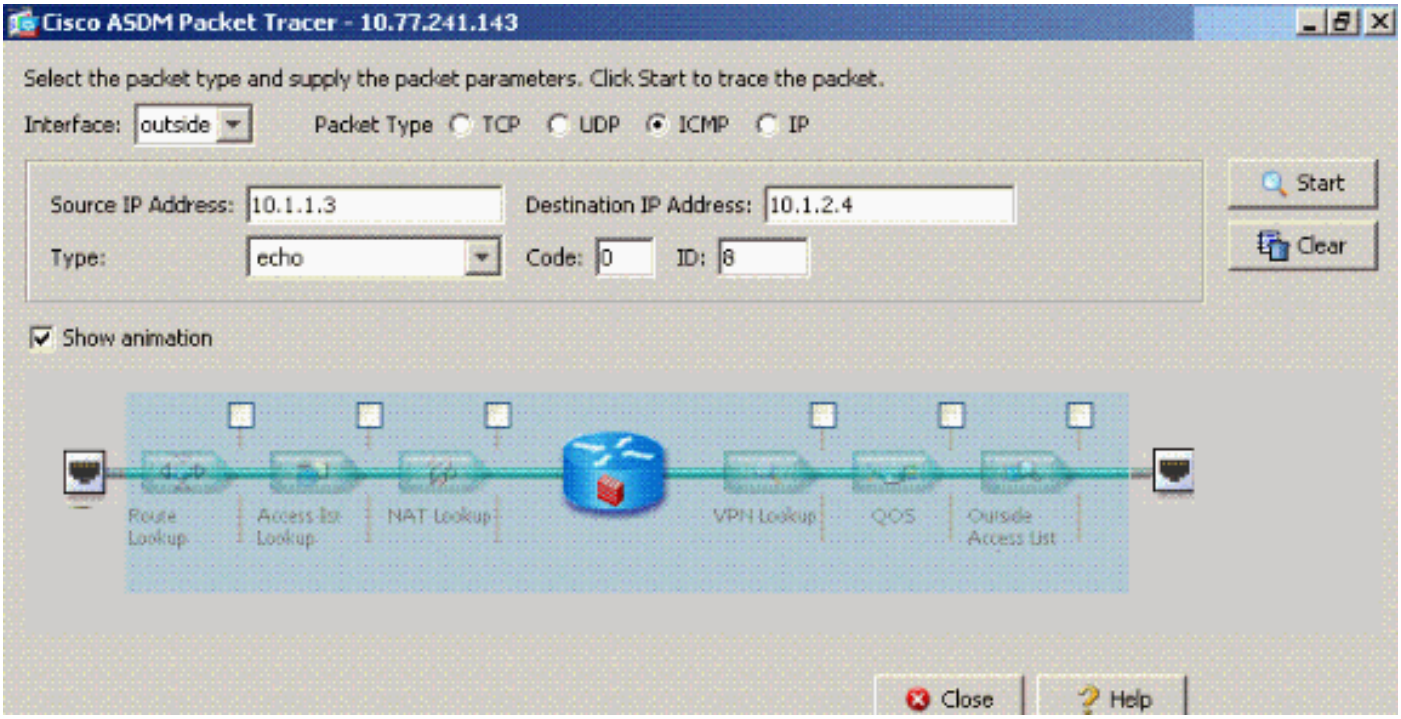
```
ciscoasa(config)#access-list outside_acl permit tcp any host 172.22.1.147 eq 80
ciscoasa(config)#access-list outside_acl deny ip any any ciscoasa(config)#access-group
outside_acl in interface outside ciscoasa#packet-tracer input outside icmp 172.22.1.6 8 0
172.16.10.1 detailed !--- Output is suppressed.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

L'équivalent des commandes CLI ci-dessus dans l'ASDM est montré dans ces figures :

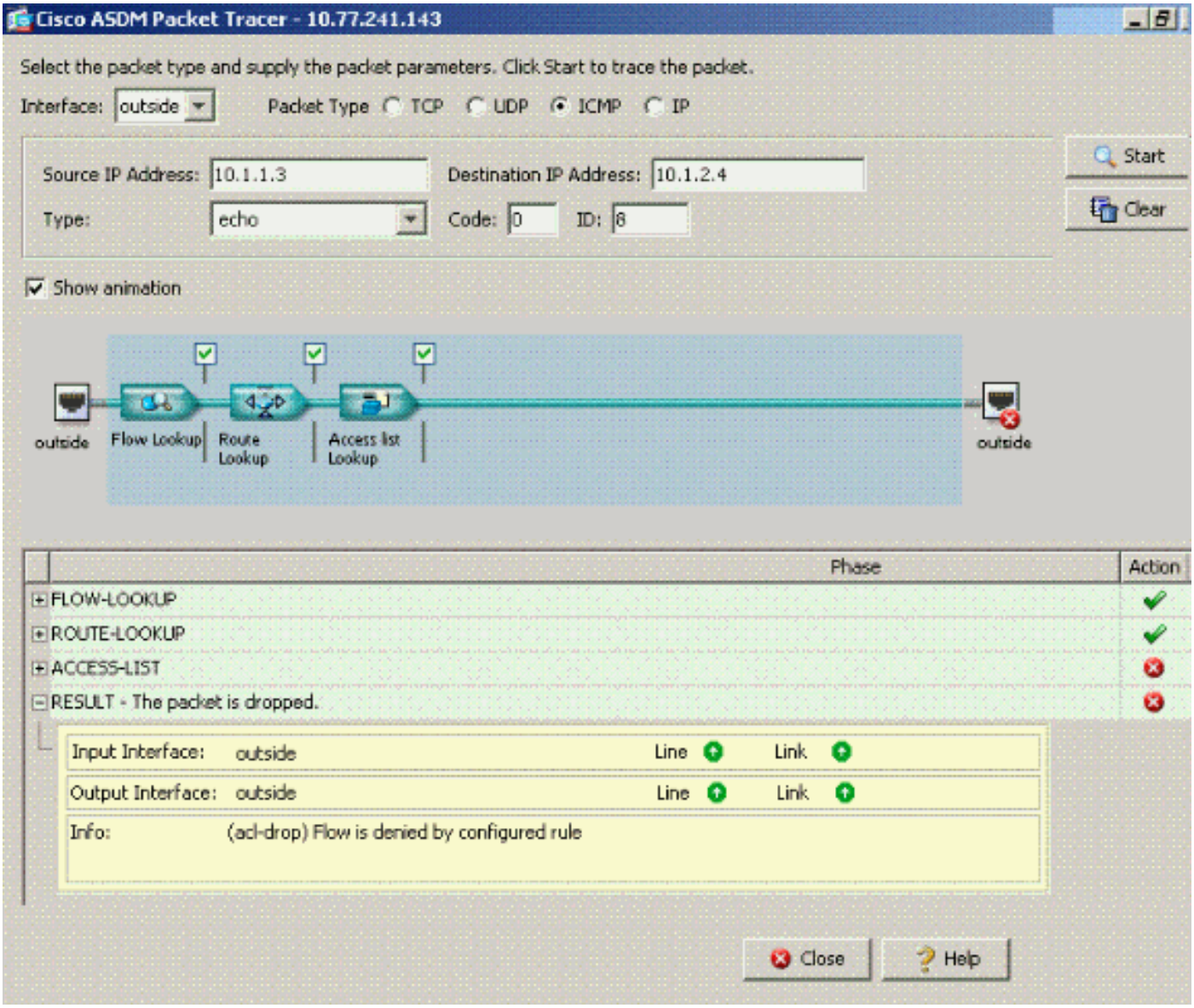
Étape 1 :



Étape 2 :



La sortie du traceur de paquets avec la commande **same-security-traffic permit intra-interface** activée et la commande **access-list outside_acl extended deny ip any any** configurée pour refuser les paquets.

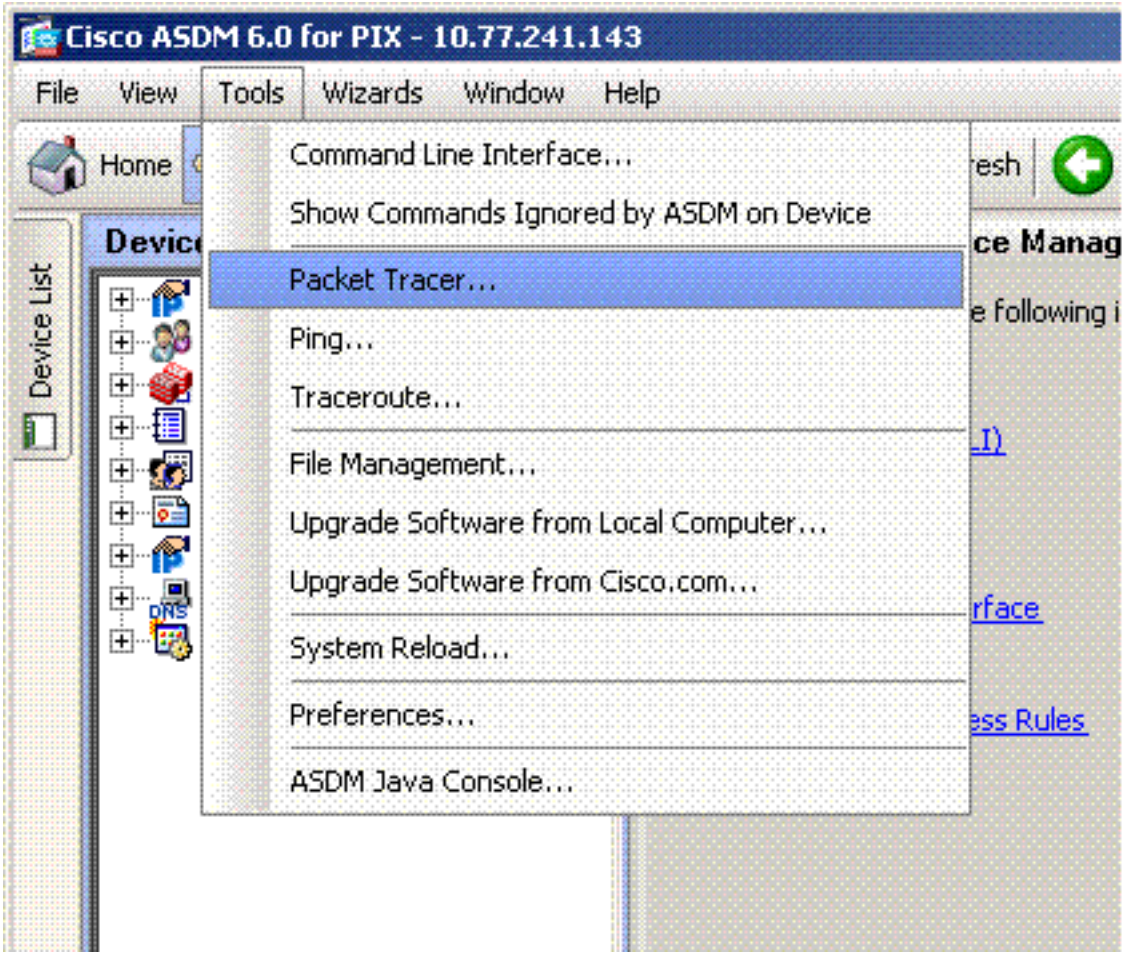


Si les communications intra-interface sont désirées sur une interface particulière et que des listes d'accès sont appliquées à la même interface, les règles de liste d'accès doivent autoriser le trafic intra-interface. Avec l'utilisation des exemples de cette section, la liste d'accès doit être écrite comme suit :

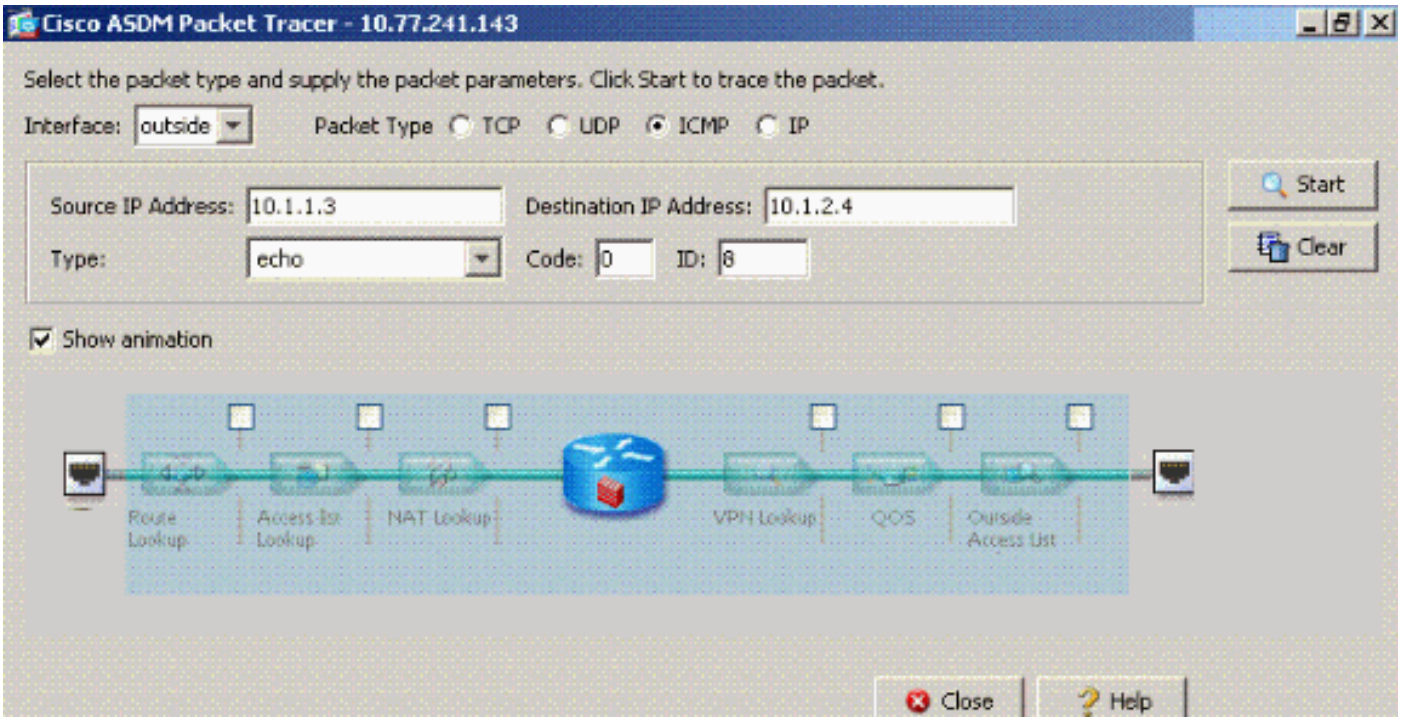
```
ciscoasa(config)#access-list outside_acl permit tcp any host 172.22.1.147 eq 80
ciscoasa(config)#access-list outside_acl permit ip 172.22.1.0 255.255.255.0 172.16.10.0
255.255.255.0 !--- 172.22.1.0 255.255.255.0 represents a locally !--- connected network on the
ASA. !--- 172.16.10.0 255.255.255.0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

L'équivalent des commandes CLI ci-dessus dans l'ASDM est montré dans ces figures :

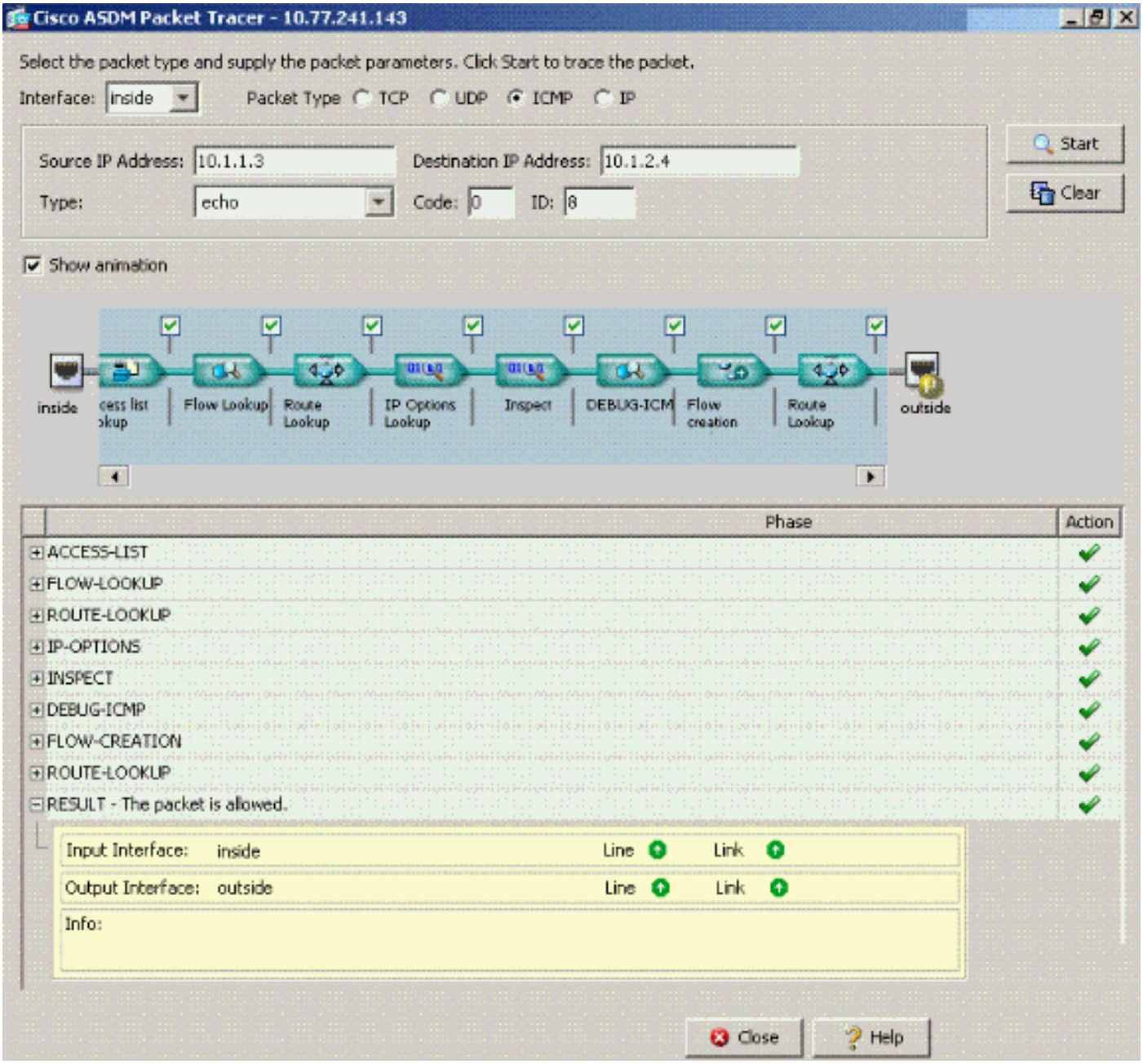
Étape 1 :



Étape 2 :



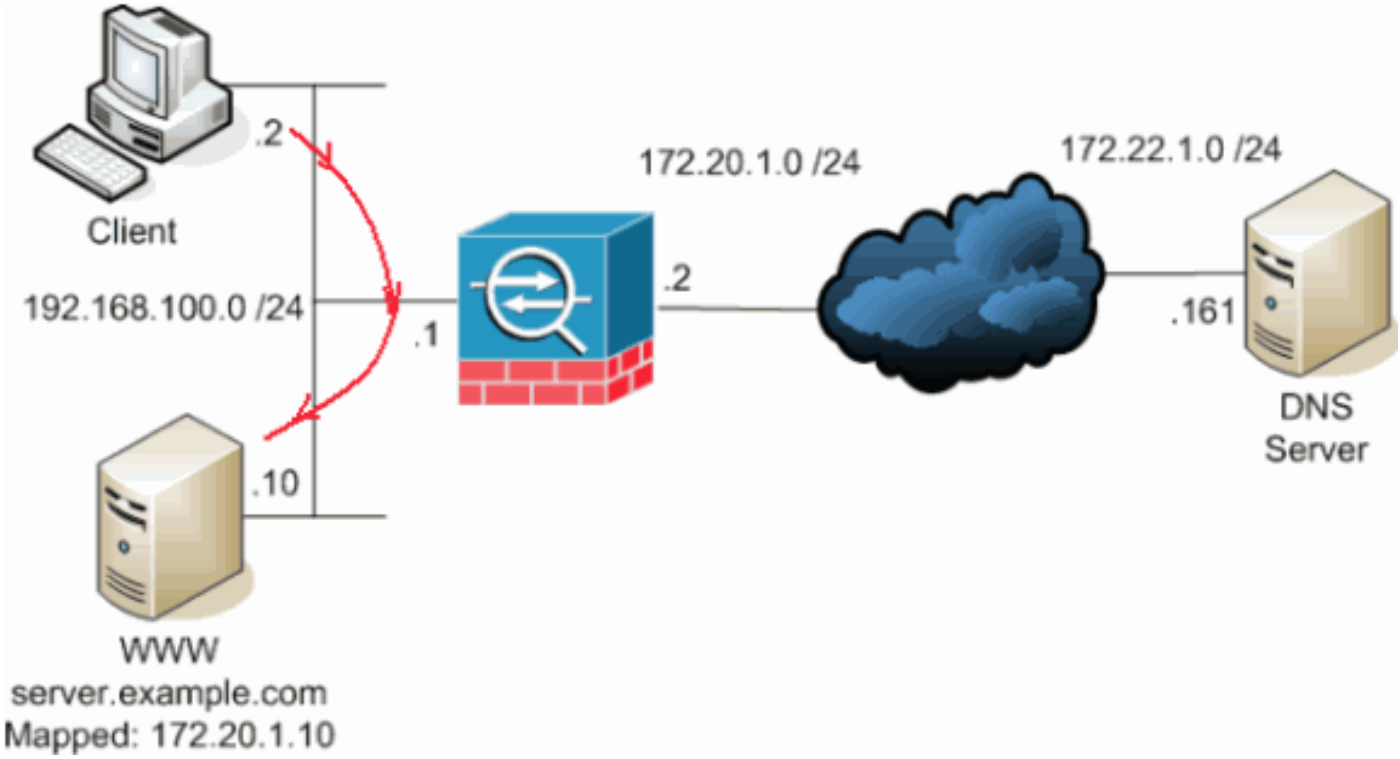
La sortie du traceur de paquets avec la commande **same-security-traffic permit intra-interface** activée et la commande **access-list outside_acl extended deny ip any any** configurée sur la même interface où le trafic intra-interface est désiré.



Référez-vous à la liste d'accès étendue et au groupe d'accès pour plus d'informations sur les commandes **access-list** et **access-group**.

Intra-interface activé avec la fonction NAT statique

Cette section explique un scénario dans lequel un utilisateur interne essaye d'accéder au serveur Web interne avec son adresse publique.



Dans ce cas, le client à l'adresse 192.168.100.2 veut utiliser l'adresse publique du serveur WWW (par exemple, 172.20.1.10). Les services DNS pour le client sont fournis par le serveur DNS externe à l'adresse 172.22.1.161. Puisque le serveur DNS est situé sur un autre réseau public, il ne connaît pas l'adresse IP privée du serveur WWW. En revanche, le serveur DNS connaît l'adresse mappée du serveur WWW, à savoir 172.20.1.10.

Ici, ce trafic provenant de l'interface interne doit être traduit et réacheminé via l'interface interne pour atteindre le serveur WWW. Cela s'appelle le « hairpinning ». Cette méthode peut être effectuée à l'aide de ces commandes :

```
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
```

Pour les détails de configuration complets et pour plus d'informations sur le « hairpinning », référez-vous à « Hairpinning » avec communication intra-interface.

Anticipation des listes d'accès

Toutes les stratégies d'accès de pare-feu ne sont pas identiques. Quelques stratégies d'accès sont plus spécifiques que d'autres. Dans le cas où les communications intra-interface sont activées et où le pare-feu n'applique pas une liste d'accès à toutes les interfaces, il peut être utile d'ajouter une liste d'accès au moment où les communications intra-interface sont activées. La liste d'accès appliquée doit autoriser les communications intra-interface, de même que gérer d'autres conditions de stratégie d'accès.

L'exemple ci-dessous illustre ce point. L'ASA connecte un réseau privé (interface interne) à l'Internet (interface externe). L'interface interne ASA n'a pas de liste d'accès appliquée. Par défaut, tout trafic IP est autorisé de l'intérieur vers l'extérieur. La suggestion est d'ajouter une liste d'accès qui ressemble à la sortie suivante :

```
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
```

Cet ensemble de listes d'accès continue à autoriser tout le trafic IP. La ligne de la liste d'accès spécifique aux communications intra-interface rappelle aux administrateurs que les communications intra-interface doivent être autorisées par une liste d'accès appliquée.

Informations connexes

- Référence des commandes des dispositifs de sécurité Cisco, version 7.2
- Messages du journal système des dispositifs de sécurité Cisco, version 7.2
- Logiciels pare-feu Cisco PIX
- ASA : Exemple de configuration pour l'acheminement de trafic réseau entre l'ASA et l'AIP SSM
- Assistance produit des dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500
- Support et documentation techniques - Cisco Systems