Configurer l'accès ASA pour le serveur de messagerie SMTP dans les réseaux DMZ, internes et externes

Contenu

Introduction

Ce document décrit comment configurer un dispositif de sécurité adaptatif Cisco (ASA) pour l'accès à un serveur SMTP (Simple Mail Transfer Protocol) situé dans la zone démilitarisée (DMZ), le réseau interne ou le réseau externe.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco ASA qui exécute le logiciel version 9.1 ou ultérieure
- Routeur de la gamme Cisco 2800C avec logiciel Cisco IOS® version 15.1(4)M6

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Configuration

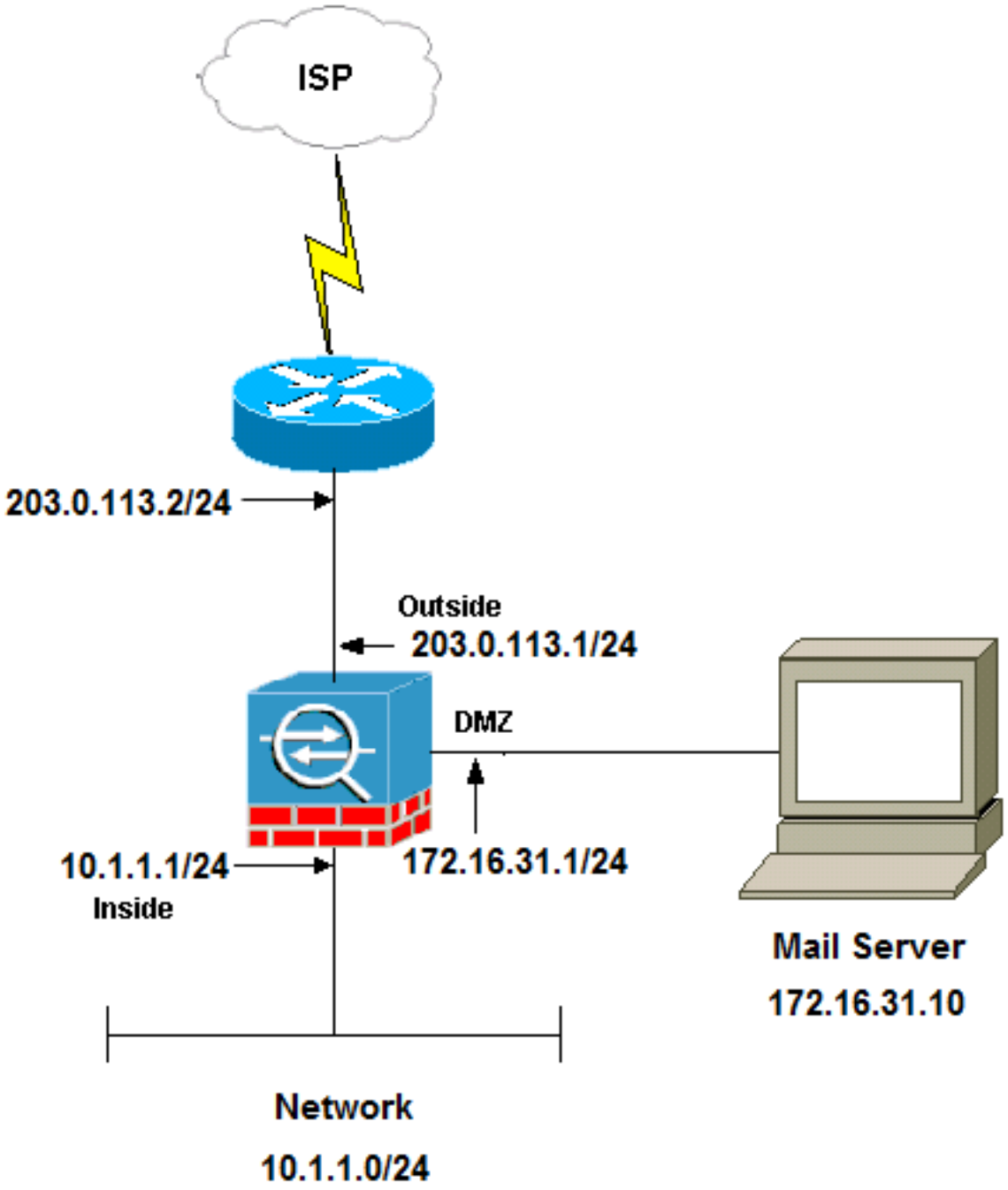
Cette section décrit comment configurer l'ASA afin d'atteindre le serveur de messagerie dans le réseau DMZ, le réseau interne ou le réseau externe.

Note: Utilisez l'outil de recherche de commandes (clients enregistrés uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Serveur de messagerie du réseau DMZ

Diagramme du réseau

La configuration décrite dans cette section utilise cette configuration réseau :



Note: Les schémas d'adressage IP utilisés dans ce document ne sont pas routables légalement sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisées dans un

environnement de laboratoire.

La configuration de réseau utilisée dans cet exemple a l'ASA avec un réseau interne à **10.1.1.0/24** et un réseau externe à **203.0.113.0/24**. Le serveur de messagerie dont l'adresse IP est **172.16.31.10** se trouve dans le réseau DMZ. Pour que le serveur de messagerie soit accessible par le réseau interne, vous devez configurer la traduction d'adresses de réseau (NAT) d'identité.

Pour que les utilisateurs externes puissent accéder au serveur de messagerie, vous devez configurer une NAT statique et une liste d'accès, qui est **outside_int** dans cet exemple, afin de permettre aux utilisateurs externes d'accéder au serveur de messagerie et de lier la liste d'accès à l'interface externe.

Configuration ASA

Voici la configuration ASA pour cet exemple :

```
show run
: Saved
:
ASA Version 9.1(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
passwd 2KFQnbNIdI.2KYOU encrypted
names

!--- Configure the dmz interface.

interface GigabitEthernet0/0
nameif dmz
security-level 50
ip address 172.16.31.1 255.255.255.0
!

!--- Configure the outside interface.

interface GigabitEthernet0/1
nameif outside
security-level 0
ip address 203.0.113.1 255.255.255.0

!--- Configure inside interface.

interface GigabitEthernet0/2
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
boot system disk0:/asa912-k8.bin
```

```
ftp mode passive

!--- This access list allows hosts to access
!--- IP address 172.16.31.10 for the SMTP port from outside.

access-list outside_int extended permit tcp any4 host 172.16.31.10 eq smtp

object network obj1-10.1.1.0
 subnet 10.1.1.0 255.255.255.0
nat (inside,outside) dynamic interface

!--- This network static does not use address translation.
!--- Inside hosts appear on the DMZ with their own addresses.

object network obj-10.1.1.0
subnet 10.1.1.0 255.255.255.0
nat (inside,dmz) static obj-10.1.1.0

!--- This Auto-NAT uses address translation.
!--- Hosts that access the mail server from the outside
!--- use the 203.0.113.10 address.

object network obj-172.16.31.10
host 172.16.31.10
nat (dmz,outside) static 203.0.113.10

access-group outside_int in interface outside

route outside 0.0.0.0 0.0.0.0 203.0.113.2 1

timeout xlate 3:00:00
timeout pat-xlate 0:00:30
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 sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512

!--- The inspect esmtp command (included in the map) allows
!--- SMTP/ESMTP to inspect the application.

policy-map global_policy
class inspection_default
inspect dns maximum-length 512
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
!

!--- The inspect esmtp command (included in the map) allows
!--- SMTP/ESMTP to inspect the application.

service-policy global_policy global
```

Configuration TLS ESMTP

Si vous utilisez le chiffrement TLS (Transport Layer Security) pour les communications par e-mail, la fonction d'inspection ESMTP (Extended Simple Mail Transfer Protocol) (activée par défaut) de l'ASA supprime les paquets. Afin d'autoriser les e-mails avec TLS activé, désactivez la fonction d'inspection ESMTP comme indiqué dans l'exemple suivant.

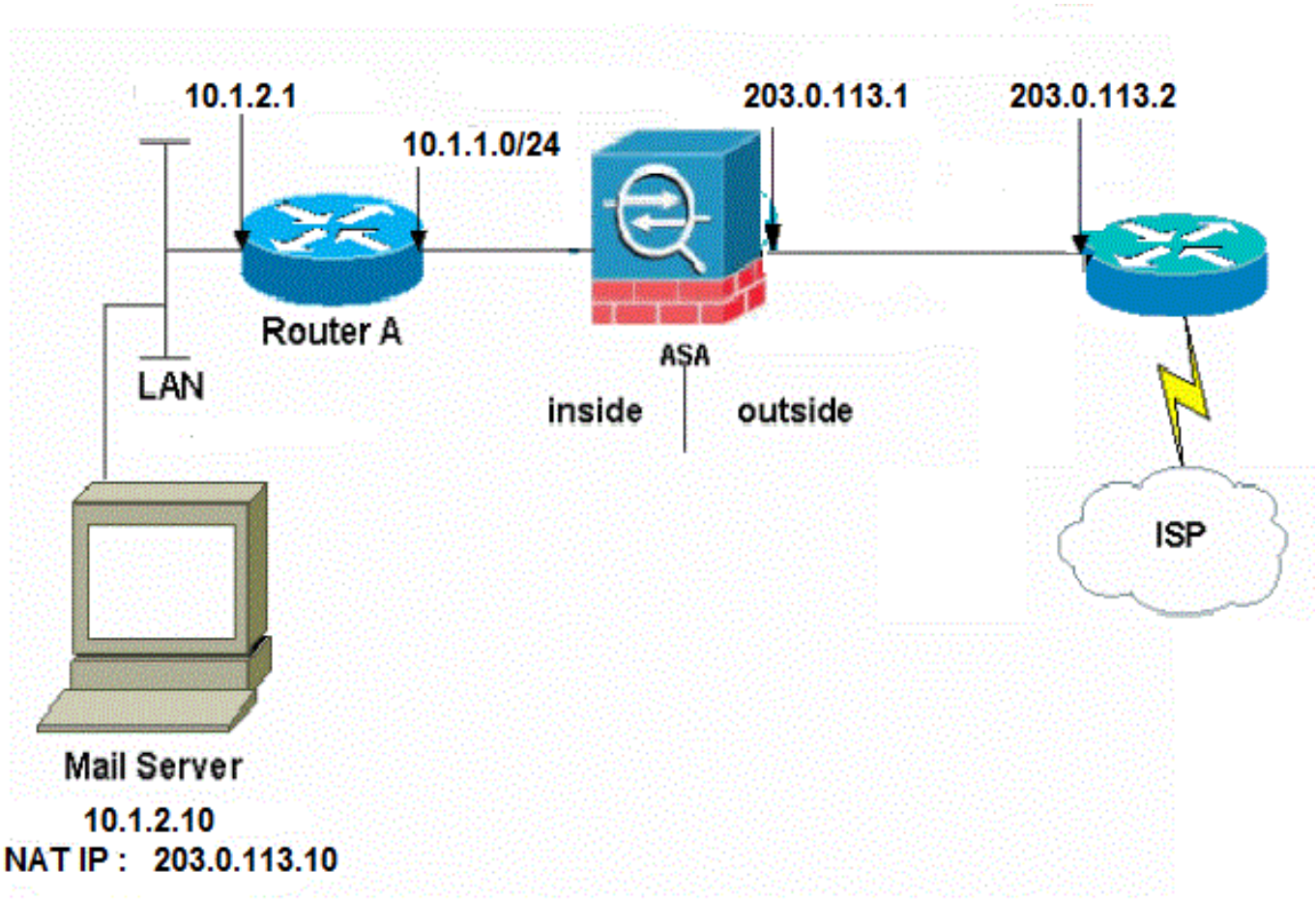
> **Note**: Référez-vous à l'ID de bogue Cisco CSCtn08326 (clients enregistrés uniquement) pour plus d'informations.

```
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#no inspect esmtp
ciscoasa(config-pmap-c)#exit
ciscoasa(config-pmap)#exit
```

Serveur de messagerie du réseau interne

Diagramme du réseau

La configuration décrite dans cette section utilise cette configuration réseau :



La configuration de réseau utilisée dans cet exemple a l'ASA avec un réseau interne à **10.1.1.0/24** et un réseau externe à **203.0.113.0/24**. Le serveur de messagerie avec l'adresse IP **10.1.2.10** se trouve dans le réseau interne.

Configuration ASA

Voici la configuration ASA pour cet exemple :

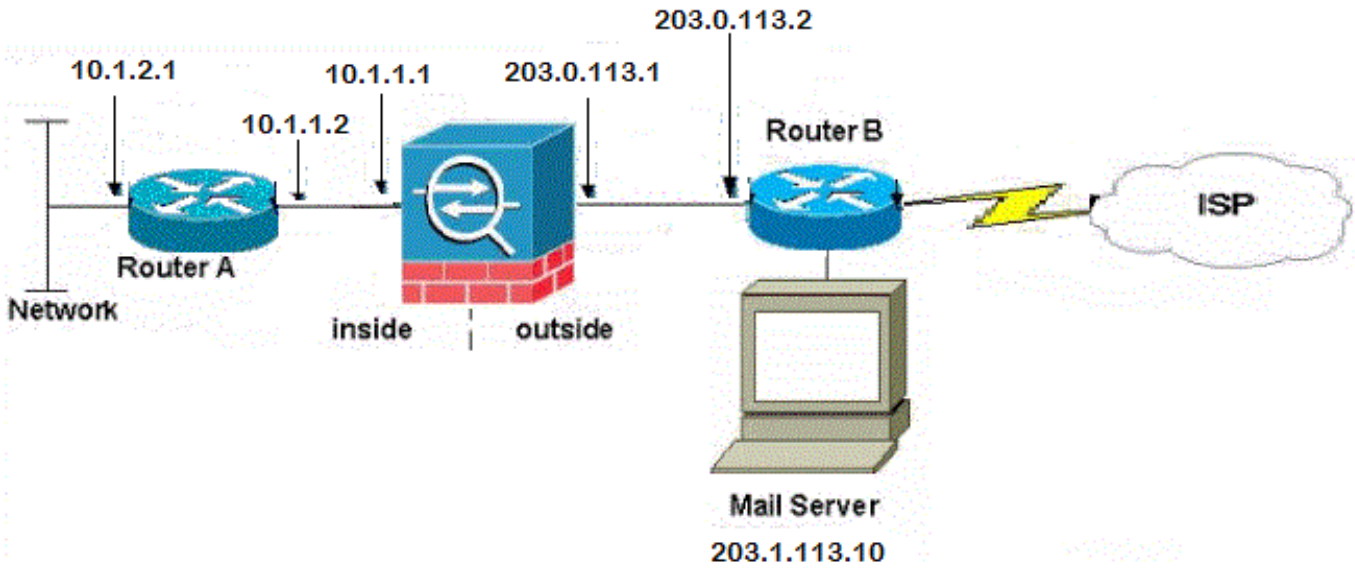
```
ASA#show run
: Saved
:
ASA Version 9.1(2)
!
--Omitted--
!

!--- Define the IP address for the inside interface.

interface GigabitEthernet0/2
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0

!--- Define the IP address for the outside interface.

interface GigabitEthernet0/1
nameif outside
security-level 0
```

```
ip address 203.0.113.1 255.255.255.0
!
--Omitted--

!--- Create an access list that permits Simple
!--- Mail Transfer Protocol (SMTP) traffic from anywhere
!--- to the host at 203.0.113.10 (our server). The name of this list is
!--- smtp. Add additional lines to this access list as required.
!--- Note: There is one and only one access list allowed per
!--- interface per direction, for example, inbound on the outside interface.
!--- Because of limitation, any additional lines that need placement in
!--- the access list need to be specified here. If the server
!--- in question is not SMTP, replace the occurrences of SMTP with
!--- www, DNS, POP3, or whatever else is required.

access-list smtp extended permit tcp any host 10.1.2.10 eq smtp

--Omitted--

!--- Specify that any traffic that originates inside from the
!--- 10.1.2.x network NATs (PAT) to 203.0.113.9 if
!--- such traffic passes through the outside interface.

object network obj-10.1.2.0
subnet 10.1.2.0 255.255.255.0
nat (inside,outside) dynamic 203.0.113.9

!--- Define a static translation between 10.1.2.10 on the inside and
!--- 203.0.113.10 on the outside. These are the addresses to be used by
!--- the server located inside the ASA.

object network obj-10.1.2.10
host 10.1.2.10
nat (inside,outside) static 203.0.113.10

!--- Apply the access list named smtp inbound on the outside interface.

access-group smtp in interface outside

!--- Instruct the ASA to hand any traffic destined for 10.1.2.0
!--- to the router at 10.1.1.2.

route inside 10.1.2.0 255.255.255.0 10.1.1.2 1

!--- Set the default route to 203.0.113.2.
!--- The ASA assumes that this address is a router address.

route outside 0.0.0.0 0.0.0.0 203.0.113.2 1
```

Serveur de messagerie du réseau externe

Diagramme du réseau

La configuration décrite dans cette section utilise cette configuration réseau :



Configuration ASA

Voici la configuration ASA pour cet exemple :

```
ASA#show run
: Saved
:
ASA Version 9.1(2)
!
--Omitted--
!--- Define the IP address for the inside interface.

interface GigabitEthernet0/2
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0

!--- Define the IP address for the outside interface.

interface GigabitEthernet0/1
nameif outside
security-level 0
ip address 203.0.113.1 255.255.255.0
!
--Omitted--

!--- This command indicates that all addresses in the 10.1.2.x range
!--- that pass from the inside (GigabitEthernet0/2) to a corresponding global
!--- destination are done with dynamic PAT.
!--- As outbound traffic is permitted by default on the ASA, no
!--- static commands are needed.

object network obj-10.1.2.0
subnet 10.1.2.0 255.255.255.0
nat (inside,outside) dynamic interface

!--- Creates a static route for the 10.1.2.x network.
!--- The ASA forwards packets with these addresses to the router
```

```
!--- at 10.1.1.2
route inside 10.1.2.0 255.255.255.0 10.1.1.2 1

!--- Sets the default route for the ASA Firewall at 203.0.113.2

route outside 0.0.0.0 0.0.0.0 203.0.113.2 1

--Omitted--

: end
```

Vérification

Utilisez les informations fournies dans cette section afin de vérifier que votre configuration fonctionne correctement.

Serveur de messagerie du réseau DMZ

TCP Ping

La requête ping TCP teste une connexion sur TCP (la valeur par défaut est ICMP (Internet Control Message Protocol)). Une requête ping TCP envoie des paquets SYN et considère que la requête ping réussit si le périphérique de destination envoie un paquet SYN-ACK. Vous pouvez exécuter au maximum deux requêtes ping TCP simultanées à la fois.

Voici un exemple :

```
ciscoasa(config)# ping tcp
Interface: outside
Target IP address: 203.0.113.10
Destination port: [80] 25
Specify source? [n]: y
Source IP address: 203.0.113.2
Source port: [0] 1234
Repeat count: [5] 5
Timeout in seconds: [2] 2
Type escape sequence to abort.
Sending 5 TCP SYN requests to 203.0.113.10 port 25
from 203.0.113.2 starting port 1234, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Connexion

L'ASA est un pare-feu dynamique et le trafic de retour du serveur de messagerie est autorisé à revenir par le pare-feu car il correspond à une connexion dans la table de connexion du pare-feu. Le trafic qui correspond à une connexion actuelle est autorisé via le pare-feu sans être bloqué par une liste de contrôle d'accès (ACL) d'interface.

Dans l'exemple suivant, le client de l'interface externe établit une connexion à l'hôte 203.0.113.10 de l'interface DMZ. Cette connexion est établie avec le protocole TCP et est inactive depuis deux secondes. Les indicateurs de connexion précisent l’état actuel de la connexion:

```
ciscoasa(config)# show conn  address  172.16.31.10
1 in use, 2 most used
TCP outside  203.0.113.2:16678 dmz  172.16.31.10:25, idle 0:00:02, bytes 921, flags UIO
```

Journalisation

Le pare-feu de l'ASA génère des SYSLOG pendant le fonctionnement normal. Les SYSLOG varient en verbosité selon la configuration de la journalisation. Cette sortie montre deux syslogs qui apparaissent au niveau 6 (le niveau *informationnel*) et au niveau 7 (le niveau *de débogage*) :

```
ciscoasa(config)# show logging  | i 172.16.31.10

%ASA-7-609001: Built local-host dmz:172.16.31.10

%ASA-6-302013: Built inbound TCP connection 11 for outside:203.0.113.2/16678
(203.0.113.2/16678) to dmz:172.16.31.10/25 (203.0.113.10/25)
```

Le deuxième syslog de cet exemple indique que le pare-feu a créé une connexion dans sa table de connexion pour ce trafic spécifique entre le client et le serveur. Si le pare-feu a été configuré afin de bloquer cette tentative de connexion, ou si un autre facteur a empêché la création de cette connexion (contraintes de ressources ou une éventuelle erreur de configuration), le pare-feu ne génère pas de journal indiquant que la connexion a été créée. Au lieu de cela, il consigne une raison pour laquelle la connexion est refusée ou une indication sur le facteur qui empêche la création de la connexion.

Par exemple, si la liste de contrôle d'accès de l'extérieur n'est pas configurée pour autoriser **172.16.31.10** sur le port 25, ce journal s'affiche lorsque le trafic est refusé :

%ASA-4-106100 : access-list outside_int refusée tcp outside/203.0.113.2(3756) -> dmz/172.16.31.10(25) hit-cnt 5 intervalle de 300 secondes

Cela se produit lorsqu'une liste de contrôle d'accès est manquante ou mal configurée, comme indiqué ici :

```
access-list outside_int extended permit tcp any4 host 172.16.31.10 eq http

access-list outside_int extended deny ip any4 any4
```

Traductions NAT (Xlate)

Afin de confirmer que les traductions sont créées, vous pouvez vérifier la table Xlate (traduction). La commande **show xlate**, lorsqu'elle est associée au mot clé local et à l'adresse IP de l'hôte interne, affiche toutes les entrées qui figurent dans la table de traduction de cet hôte. La sortie suivante montre qu'une traduction est actuellement créée pour cet hôte entre la DMZ et les interfaces externes. L'adresse IP du serveur DMZ est traduite en adresse 203.0.113.10 selon la configuration précédente. Les indicateurs répertoriés (**s** dans cet exemple) indiquent que la traduction est *statique*.

```
ciscoasa(config)# show nat detail
Manual NAT Policies (Section 1)
1 (dmz) to (outside) source static obj-172.16.31.10 obj-203.0.113.10
   translate_hits = 7, untranslate_hits = 6
```

```
   Source - Origin: 172.16.31.10/32, Translated: 203.0.113.10/32

Auto NAT Policies (Section 2)
1 (dmz) to (outside) source static obj-172.16.31.10 203.0.113.10
   translate_hits = 1, untranslate_hits = 5
   Source - Origin: 172.16.31.10/32, Translated: 203.0.113.10/32
2 (inside) to (dmz) source static obj-10.1.1.0 obj-10.1.1.0
   translate_hits = 0, untranslate_hits = 0
   Source - Origin: 10.1.1.0/24, Translated: 10.1.1.0/24
3 (inside) to (outside) source dynamic obj1-10.1.1.0 interface
   translate_hits = 0, untranslate_hits = 0
   Source - Origin: 10.1.1.0/24, Translated: 203.0.113.1/24

ciscoasa(config)# show xlate
4 in use, 4 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
      s - static, T - twice, N - net-to-net
NAT from dmz:172.16.31.10 to outside:203.0.113.10
   flags s idle 0:10:48 timeout 0:00:00
NAT from inside:10.1.1.0/24 to dmz:10.1.1.0/24
   flags sI idle 79:56:17 timeout 0:00:00
NAT from dmz:172.16.31.10 to outside:203.0.113.10
   flags sT idle 0:01:02 timeout 0:00:00
NAT from outside:0.0.0.0/0 to dmz:0.0.0.0/0
   flags sIT idle 0:01:02 timeout 0:00:00
```

Serveur de messagerie du réseau interne

TCP Ping

Voici un exemple de résultat de la commande ping TCP :

```
ciscoasa(config)# PING TCP
Interface: outside
Target IP address: 203.0.113.10
Destination port: [80] 25
Specify source? [n]: y
Source IP address: 203.0.113.2
Source port: [0] 1234
Repeat count: [5] 5
Timeout in seconds: [2] 2
Type escape sequence to abort.
Sending 5 TCP SYN requests to 203.0.113.10 port 25
from 203.0.113.2 starting port 1234, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Connexion

Voici un exemple de vérification de connexion :

```
ciscoasa(config)# show conn  address  10.1.2.10
1 in use, 2 most used
TCP outside  203.0.113.2:5672 inside  10.1.2.10:25, idle 0:00:05, bytes 871, flags UIO
```

Journalisation

Voici un exemple de syslog :

```
%ASA-6-302013: Built inbound TCP connection 553 for outside:203.0.113.2/19198
(203.0.113.2/19198) to inside:10.1.2.10/25 (203.0.113.10/25)
```

Traductions NAT (Xlate)

Voici quelques exemples de sorties de commande **show nat detail** et **show xlate** :

```
ciscoasa(config)# show nat detail

Auto NAT Policies (Section 2)
1 (inside) to (outside) source static obj-10.1.2.10 203.0.113.10
   translate_hits = 0, untranslate_hits = 15
   Source - Origin: 10.1.2.10/32, Translated: 203.0.113.10/32
2 (inside) to (dmz) source static obj-10.1.1.0 obj-10.1.1.0
   translate_hits = 0, untranslate_hits = 0
   Source - Origin: 10.1.1.0/24, Translated: 10.1.1.0/24
3 (inside) to (outside) source dynamic obj1-10.1.1.0 interface
   translate_hits = 0, untranslate_hits = 0
   Source - Origin: 10.1.1.0/24, Translated: 203.0.113.1/24

ciscoasa(config)# show xlate

NAT from inside:10.1.2.10 to outside:203.0.113.10
   flags s idle 0:00:03 timeout 0:00:00
```

Serveur de messagerie du réseau externe

TCP Ping

Voici un exemple de résultat de la commande ping TCP :

```
ciscoasa# PING TCP
Interface: inside
Target IP address: 203.1.113.10
Destination port: [80] 25
Specify source? [n]: y
Source IP address: 10.1.2.10
Source port: [0] 1234
Repeat count: [5] 5
Timeout in seconds: [2] 2
Type escape sequence to abort.
Sending 5 TCP SYN requests to 203.1.113.10 port 25
from 10.1.2.10 starting port 1234, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Connexion

Voici un exemple de vérification de connexion :

```
ciscoasa# show conn address 203.1.113.10
1 in use, 2 most used
TCP inside 10.1.2.10:13539 outside 203.1.113.10:25, idle 0:00:02, bytes 898, flags UIO
```

Journalisation

Voici un exemple de syslog :

```
ciscoasa# show logging | i 203.1.113.10

%ASA-6-302013: Built outbound TCP connection 590 for outside:203.1.113.10/25
(203.1.113.10/25) to inside:10.1.2.10/1234 (203.0.113.1/1234)
```

Traductions NAT (Xlate)

Voici un exemple de sortie de commande **show xlate** :

```
ciscoasa# show xlate | i 10.1.2.10

TCP PAT from inside:10.1.2.10/1234 to outside:203.0.113.1/1234 flags ri idle
0:00:04 timeout 0:00:30
```

Dépannage

L'ASA fournit plusieurs outils pour dépanner la connectivité. Si le problème persiste après avoir vérifié la configuration et vérifié les sorties décrites dans la section précédente, ces outils et techniques peuvent vous aider à déterminer la cause de votre échec de connectivité.

Serveur de messagerie du réseau DMZ

Packet Tracer

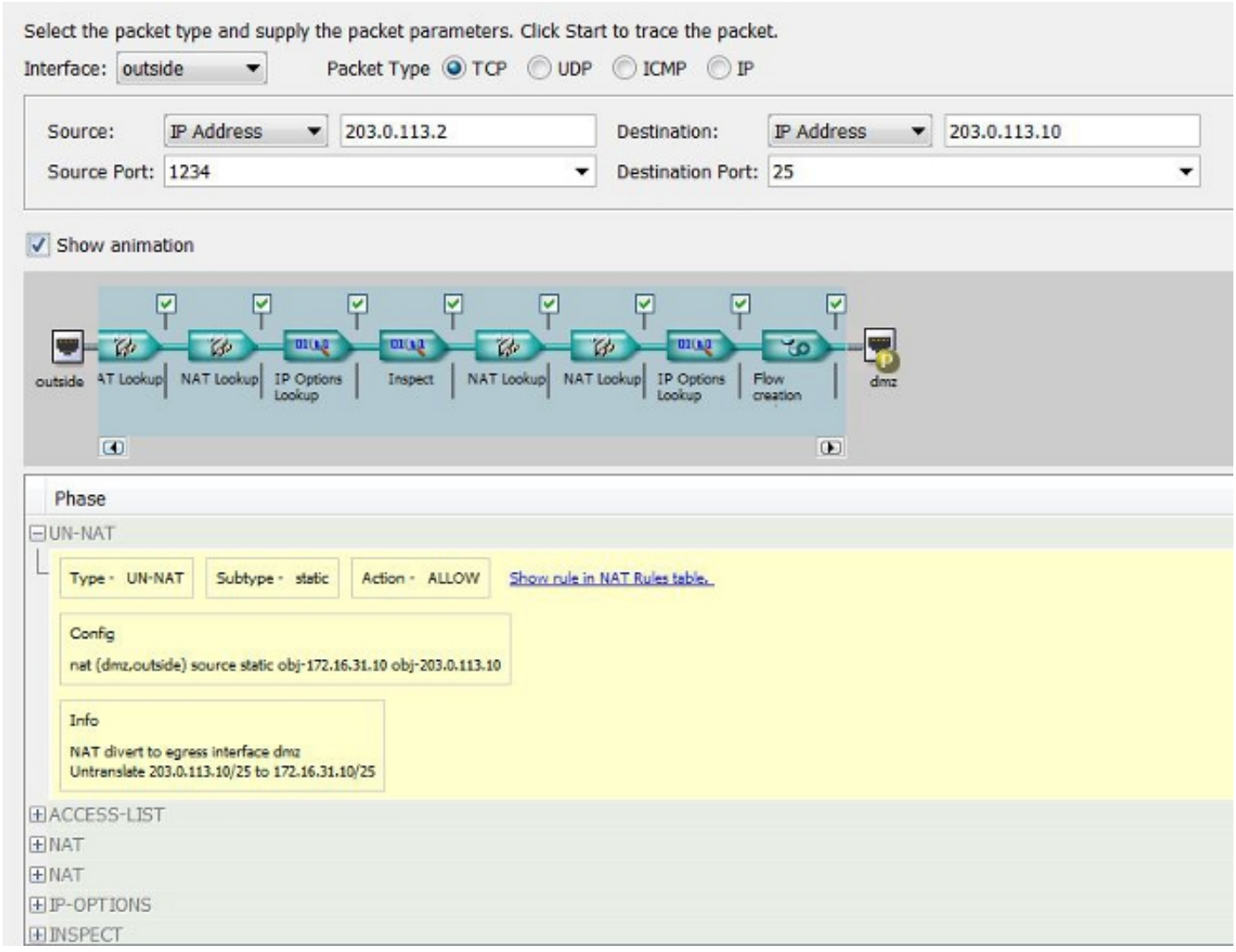
La fonctionnalité Packet Tracer de l'ASA vous permet de spécifier un paquet *simulé* et d'afficher toutes les étapes, vérifications et fonctions que le pare-feu exécute lorsqu'il traite le trafic. Avec cet outil, il est utile d'identifier un exemple de trafic qui, selon vous, *devrait* être autorisé à passer par le pare-feu, et d'utiliser ce cinq-tuple afin de simuler le trafic. Dans l'exemple suivant, packet tracer est utilisé afin de simuler une tentative de connexion qui répond à ces critères :

- Le paquet simulé arrive à l'**extérieur**.
- Le protocole utilisé est TCP.
- L’adresse IP du client simulé est 203.0.113.2.
- Le client envoie le trafic provenant du port 1234.
- Le trafic est destiné à un serveur ayant l’adresse IP 203.0.113.10.
- Le trafic est destiné au port 25.

Voici un exemple de sortie Packet Tracer :

```
packet-tracer input outside tcp 203.0.113.2 1234 203.0.113.10 25 detailed

--Omitted--

Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (dmz,outside) source static obj-172.16.31.10 obj-203.0.113.10
Additional Information:
NAT divert to egress interface dmz
Untranslate 203.0.113.10/25 to 172.16.31.10/25

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: dmz
output-status: up
output-line-status: up
Action: allow
```

Voici un exemple sur Cisco Adaptive Security Device Manager (ASDM) :



Notez qu'il n'est pas fait mention de l'interface *DMZ* dans les sorties précédentes. C'est par

conception Packet Tracer. L'outil vous explique comment le pare-feu traite ce type de tentative de connexion, ce qui inclut la manière dont il l'acheminerait et à partir de quelle interface.

> **Astuce** : Pour plus d'informations sur la fonctionnalité Packet Tracer, reportez-vous à la section Tracing Packets with Packet Tracer du *Guide de configuration de la gamme Cisco ASA 5500 à l'aide de l'interface de ligne de commande, 8.4 et 8.6*.

Capture de paquets

Le pare-feu ASA peut capturer le trafic entrant ou sortant de ses interfaces. Cette fonctionnalité de capture est très utile, car elle peut prouver de manière définitive si le trafic arrive ou quitte un pare-feu. L'exemple suivant montre la configuration de deux captures nommées **capd** et **capout** sur les interfaces DMZ et externes, respectivement. Les commandes de capture utilisent un mot clé match, qui vous permet d'être spécifique au trafic que vous voulez capturer.

Pour la **capture capd** dans cet exemple, il est indiqué que vous voulez faire correspondre le trafic affiché sur l'interface DMZ (entrée ou sortie) qui correspond à l'hôte TCP 172.16.31.10/host 203.0.113.2. Autrement dit, vous souhaitez capter tout trafic TCP envoyé de l'hôte 172.16.31.10 à l'hôte 203.0.113.2, ou inversement. L'utilisation du mot-clé match permet au pare-feu de capter ce trafic dans les deux sens. La commande capture définie pour l'interface externe ne fait pas référence à l'adresse IP du serveur de messagerie interne, car le pare-feu effectue une NAT sur cette adresse IP du serveur de messagerie. Par conséquent, vous ne pouvez pas correspondre à cette adresse IP de serveur. L'exemple suivant utilise plutôt le mot **any** afin d'indiquer que toutes les adresses IP possibles correspondent à cette condition.

Après avoir configuré les captures, essayez de rétablir une connexion et passez à l'affichage des captures à l'aide de la commande **show capture <nom_capture>**. Dans cet exemple, vous pouvez voir que l'hôte externe a pu se connecter au serveur de messagerie, comme le montre la connexion en trois étapes TCP qui est visible dans les captures :

```
ASA#  capture capd interface dmz match tcp host 172.16.31.10 any
ASA#  capture capout interface outside match tcp any host 203.0.113.10

ASA#   show capture capd

3 packets captured

  1: 11:31:23.432655       203.0.113.2.65281 > 172.16.31.10.25: S 780523448:
  780523448(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
  2: 11:31:23.712518       172.16.31.10.25 > 203.0.113.2.65281: S 2123396067:
  2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712884       203.0.113.2.65281 > 172.16.31.10.25. ack 2123396068
  win 32768

ASA# show capture capout

3 packets captured

  1: 11:31:23.432869       203.0.113.2.65281 > 203.0.113.10.25: S 1633080465:
  1633080465(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>
  2: 11:31:23.712472       203.0.113.10.25 > 203.0.113.2.65281: S 95714629:
  95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712914        203.0.113.2.65281 > 203.0.113.10.25: . ack 95714630
```

```
  win 32768
```

Serveur de messagerie du réseau interne

Packet Tracer

Voici un exemple de sortie Packet Tracer :

```
CLI : packet-tracer input outside tcp 203.0.113.2 1234 203.0.113.10 25 detailed

--Omitted--

Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network obj-10.1.2.10
 nat (inside,outside) static 203.0.113.10
Additional Information:
NAT divert to egress interface inside
Untranslate 203.0.113.10/25 to 10.1.2.10/25

Phase: 3
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group smtp in interface outside
access-list smtp extended permit tcp any4 host 10.1.2.10 eq smtp
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0x77dd2c50, priority=13, domain=permit, deny=false
       hits=1, user_data=0x735dc880, cs_id=0x0, use_real_addr, flags=0x0, protocol=6
       src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0
       dst ip/id=10.1.2.10, mask=255.255.255.255, port=25, tag=0, dscp=0x0
       input_ifc=outside, output_ifc=any
```

Serveur de messagerie du réseau externe

Packet Tracer

Voici un exemple de sortie Packet Tracer :

```
CLI :  packet-tracer input inside tcp 10.1.2.10 1234 203.1.113.10 25 detailed

--Omitted--

Phase: 2
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
```

```
in 203.1.113.0 255.255.255.0 outside

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
object network obj-10.1.2.0
nat (inside,outside) dynamic interface
Additional Information:
Dynamic translate 10.1.2.10/1234 to 203.0.113.1/1234
Forward Flow based lookup yields rule:
in id=0x778b14a8, priority=6, domain=nat, deny=false
hits=11, user_data=0x778b0f48, cs_id=0x0, flags=0x0, protocol=0
src ip/id=10.1.2.0, mask=255.255.255.0, port=0, tag=0
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0, dscp=0x0
input_ifc=inside, output_ifc=outside
```

Informations connexes

- Messages Syslog de la gamme Cisco ASA
- Exemple de configuration des captures de paquets ASA avec CLI et ASDM
- Guide de configuration de l'interface de ligne de commande de la gamme Cisco ASA, 9.0 - Configuration de la NAT d'objet réseau
- Assistance technique et documentation - Cisco Systems