Configuración del ASA para el acceso al servidor de correo SMTP en redes DMZ, internas y externas

Contenido

Introducción

Este documento describe cómo configurar un Cisco Adaptive Security Appliance (ASA) para acceder a un servidor SMTP (protocolo simple de transferencia de correo) ubicado en la zona desmilitarizada (DMZ), la red interna o la red externa.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco ASA que ejecuta la versión de software 9.1 o posterior
- Router de la serie Cisco 2800C con Cisco IOS® Software Release 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.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configurar

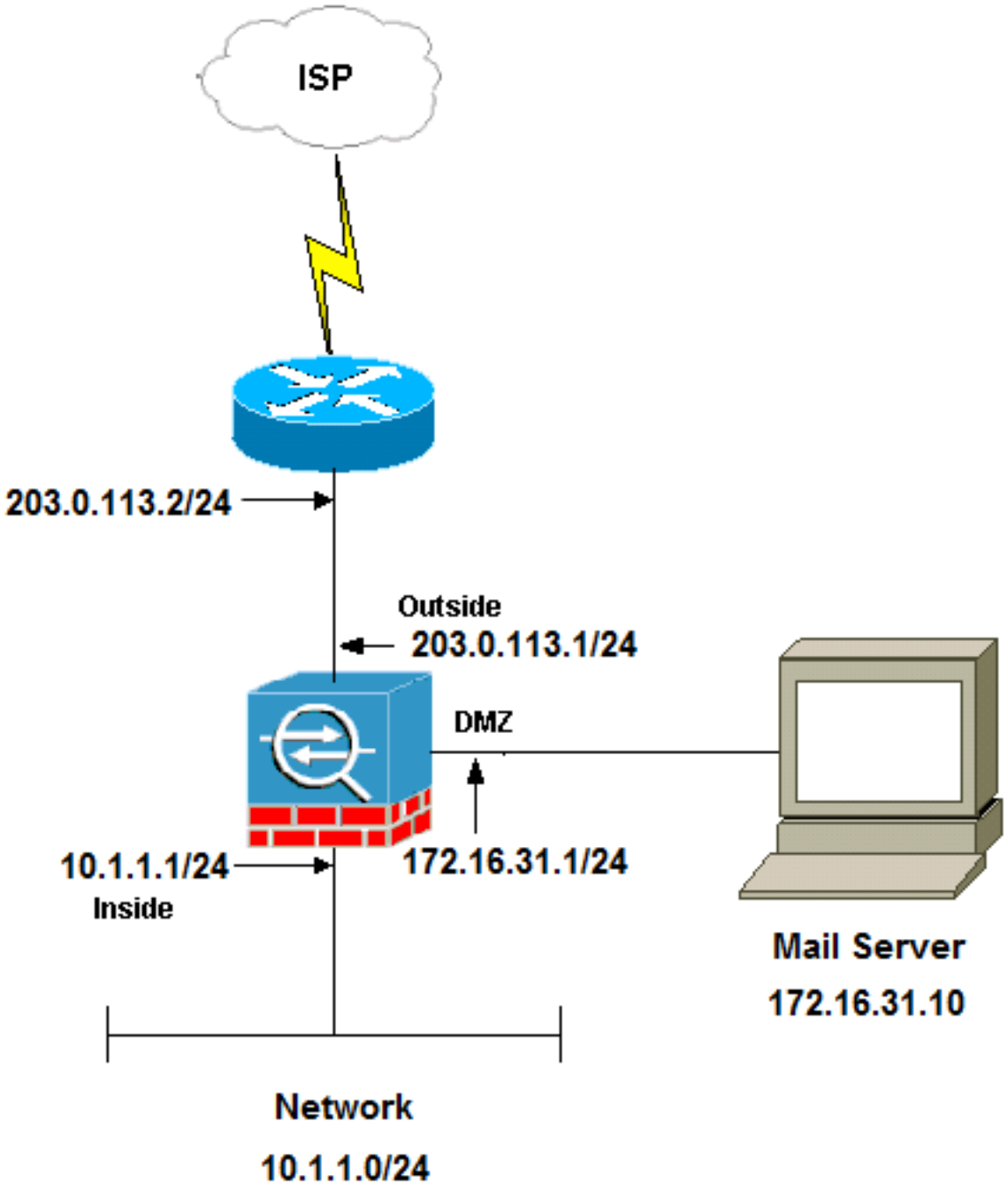
Esta sección describe cómo configurar el ASA para alcanzar el servidor de correo en la red DMZ, la red interna o la red externa.

Nota: Utilice la Command Lookup Tool (sólo clientes registrados) para obtener más información sobre los comandos que se utilizan en esta sección.

Servidor de correo en la red DMZ

Diagrama de la red

La configuración que se describe en esta sección utiliza esta configuración de red:



Nota: Los esquemas de direccionamiento IP que se utilizan en este documento no son legalmente enrutables en Internet. Son las direcciones RFC1918 que se han utilizado en un

entorno de laboratorio.

La configuración de red que se utiliza en este ejemplo tiene el ASA con una red interna en **10.1.1.0/24** y una red externa en **203.0.113.0/24**. El servidor de correo con la dirección IP **172.16.31.10** se encuentra en la red DMZ. Para que la red interna pueda acceder al servidor de correo, debe configurar la identidad de traducción de direcciones de red (NAT).

Para que los usuarios externos accedan al servidor de correo, debe configurar una NAT estática y una lista de acceso, que es **outside_int** en este ejemplo, para permitir que los usuarios externos accedan al servidor de correo y enlacen la lista de acceso a la interfaz exterior.

Configuración ASA

Esta es la configuración ASA para este ejemplo:

```
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
```

Configuración de ESMTP TLS

Si utiliza el cifrado de seguridad de la capa de transporte (TLS) para la comunicación por correo electrónico, la función de inspección de protocolo simple extendido de transferencia de correo (ESMTP) (activada de forma predeterminada) en el ASA descarta los paquetes. Para permitir los correos electrónicos con TLS habilitado, inhabilite la función de inspección ESMTP como se muestra en el siguiente ejemplo.

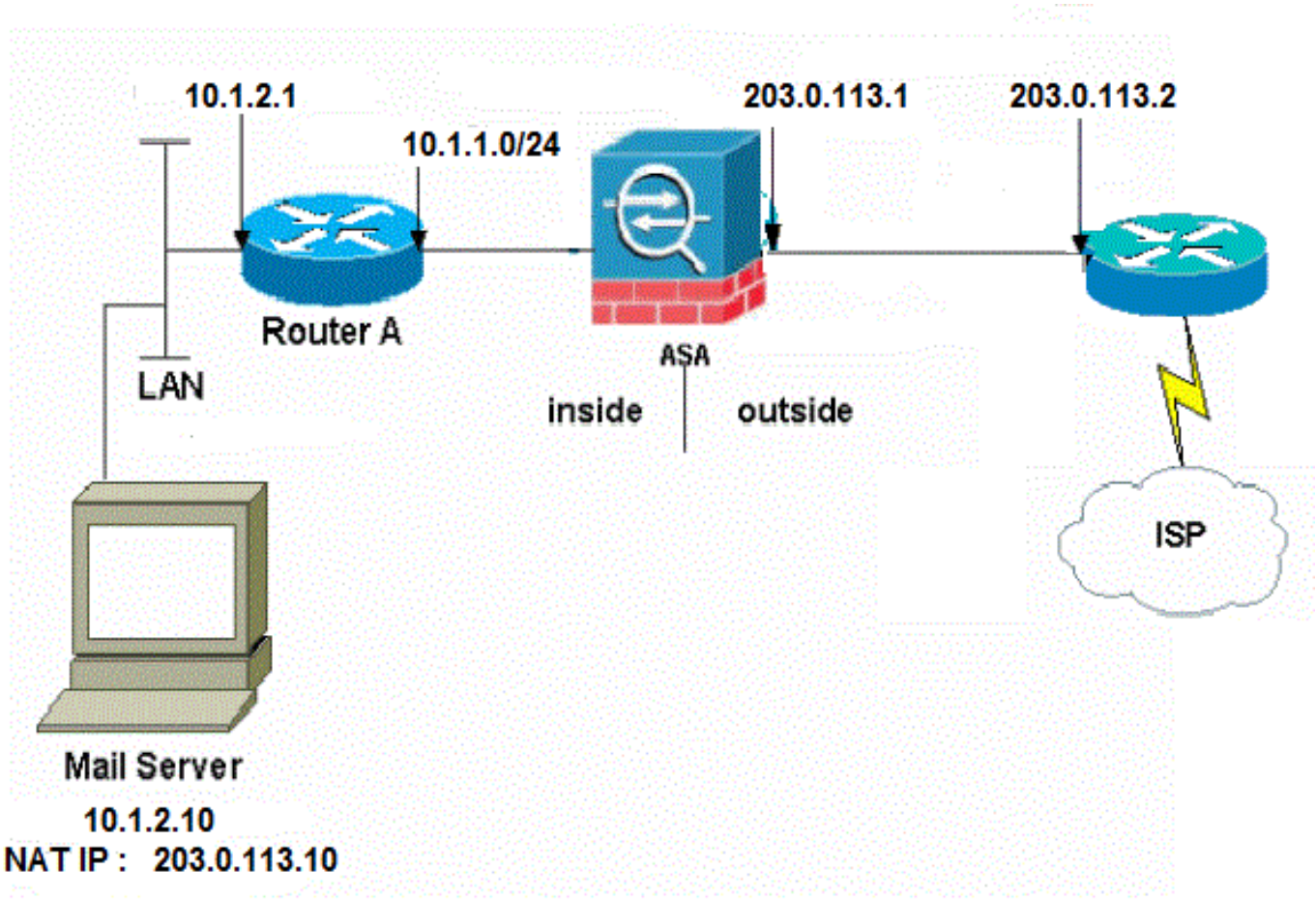
> **Nota:** Consulte Cisco bug ID CSCtn08326 (sólo clientes registrados) para obtener más información.

```
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
```

Servidor de correo en la red interna

Diagrama de la red

La configuración que se describe en esta sección utiliza esta configuración de red:



La configuración de red que se utiliza en este ejemplo tiene el ASA con una red interna en **10.1.1.0/24** y una red externa en **203.0.113.0/24**. El servidor de correo con la dirección IP **10.1.2.10** se encuentra en la red interna.

Configuración ASA

Esta es la configuración ASA para este ejemplo:

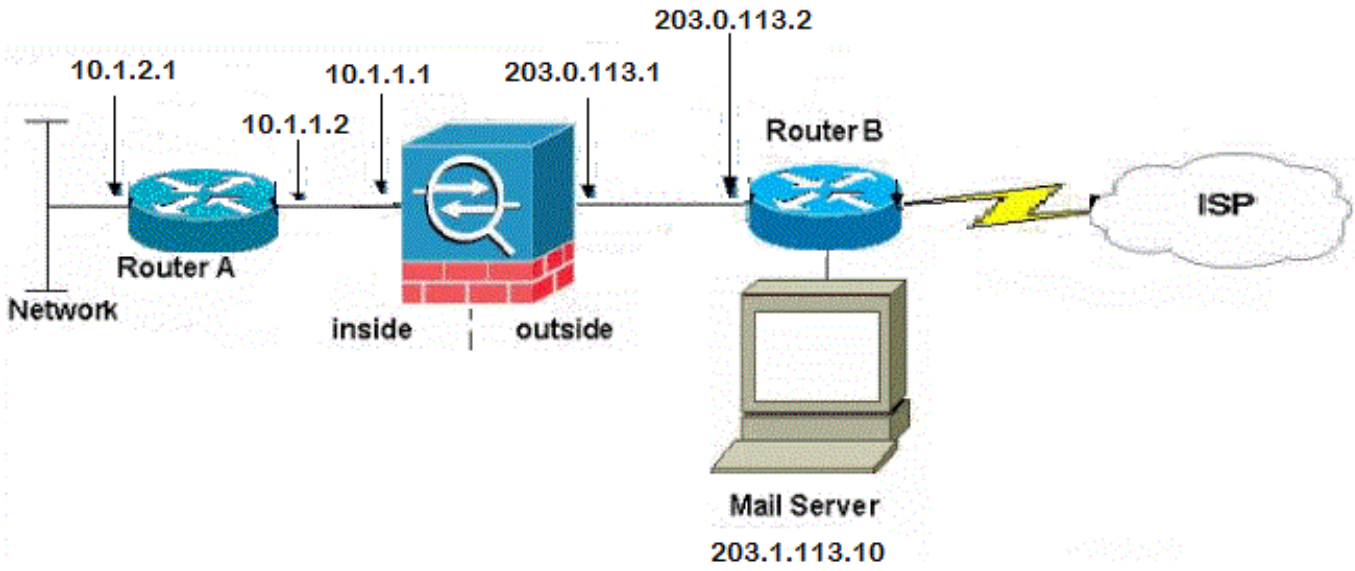
```
ASA#show run
: Saved
:
ASA Version 9.1(2)
!
--Omitted--
!

!--- 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
```

Servidor de correo en la red externa

Diagrama de la red

La configuración que se describe en esta sección utiliza esta configuración de red:



Configuración ASA

Esta es la configuración ASA para este ejemplo:

```
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
```

Verificación

Utilice la información proporcionada en esta sección para verificar que su configuración funcione correctamente.

Servidor de correo en la red DMZ

Ping TCP

El ping TCP prueba una conexión sobre TCP (el valor predeterminado es Protocolo de mensajes de control de Internet (ICMP)). Un ping TCP envía paquetes SYN y considera el ping exitoso si el dispositivo de destino envía un paquete SYN-ACK. Puede ejecutar como máximo dos pings TCP simultáneos a la vez.

Aquí tiene un ejemplo:

```
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
```

Conexión

El ASA es un firewall con información de estado y se permite devolver el tráfico del servidor de correo a través del firewall porque coincide con una conexión en la tabla de conexión del firewall. El tráfico que coincide con una conexión actual se permite a través del firewall sin ser bloqueado por una lista de control de acceso (ACL) de interfaz.

En el siguiente ejemplo, el cliente en la interfaz exterior establece una conexión al host 203.0.113.10 de la interfaz DMZ. Esta conexión se realiza con el protocolo TCP y ha estado inactiva durante dos segundos. Los indicadores de conexión indican el estado actual de esta

conexión:

```
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
```

Registro

El firewall de ASA genera syslogs durante el funcionamiento normal. El nivel de detalle de los syslogs depende de la configuración de registro. Esta salida muestra dos syslogs que aparecen en el nivel seis (el nivel *informativo*) y el nivel siete (el *nivel de depuración*):

```
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)
```

El segundo syslog en este ejemplo indica que el firewall ha generado una conexión en su tabla de conexión para este tráfico específico entre el cliente y el servidor. Si el firewall se configuró para bloquear este intento de conexión, o algún otro factor inhibió la creación de esta conexión (restricciones de recursos o una posible configuración incorrecta), el firewall no generaría un registro que indique que la conexión se ha generado. En su lugar, registraría una razón para que se negara la conexión o una indicación sobre el factor que impedía que se creara la conexión.

Por ejemplo, si la ACL en el exterior no está configurada para permitir **172.16.31.10** en el puerto 25, entonces verá este registro cuando se niegue el tráfico:

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

Esto ocurriría cuando falta una ACL o se configura mal, como se muestra aquí:

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

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

Traducciones NAT (Xlate)

Para confirmar que se han creado las traducciones, puede verificar la tabla Xlate (traducción). El comando **show xlate**, cuando se combina con la palabra clave local y la dirección IP interna del host, muestra todas las entradas que están presentes en la tabla de traducción para ese host. La siguiente salida muestra que hay una traducción actualmente construida para este host entre la DMZ y las interfaces externas. La dirección IP del servidor DMZ se traduce a la dirección 203.0.113.10 por la configuración anterior. Los indicadores que se enumeran (**s** en este ejemplo) indican que la traducción es *estática*.

```
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
```

Servidor de correo en la red interna

Ping TCP

A continuación se muestra un ejemplo de resultado de 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
```

Conexión

A continuación se muestra un ejemplo de verificación de conexión:

```
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
```

Registro

Este es un ejemplo 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)
```

Traducciones NAT (Xlate)

A continuación se muestran algunos ejemplos de resultados de los comandos **show nat detail** y **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
```

Servidor de correo en la red externa

Ping TCP

A continuación se muestra un ejemplo de resultado de 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
```

Conexión

A continuación se muestra un ejemplo de verificación de conexión:

```
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
```

Registro

Este es un ejemplo 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)
```

Traducciones NAT (Xlate)

A continuación se muestra un ejemplo de salida del comando **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
```

Troubleshoot

ASA proporciona varias herramientas con las que resolver problemas de conectividad. Si el problema persiste después de verificar la configuración y verificar los resultados descritos en la sección anterior, estas herramientas y técnicas pueden ayudarle a determinar la causa de su falla de conectividad.

Servidor de correo en la red DMZ

Packet-Tracer

La funcionalidad de seguimiento de paquetes en el ASA le permite especificar un paquete *simulado* y ver todos los pasos, verificaciones y funciones por los que pasa el firewall cuando procesa el tráfico. Con esta herramienta, es útil identificar un ejemplo de tráfico que cree *debería* permitirse pasar a través del Firewall, y usar ese tipo de cinco tubos para simular el tráfico. En el siguiente ejemplo, se utiliza el trazador de paquetes para simular un intento de conexión que cumple estos criterios:

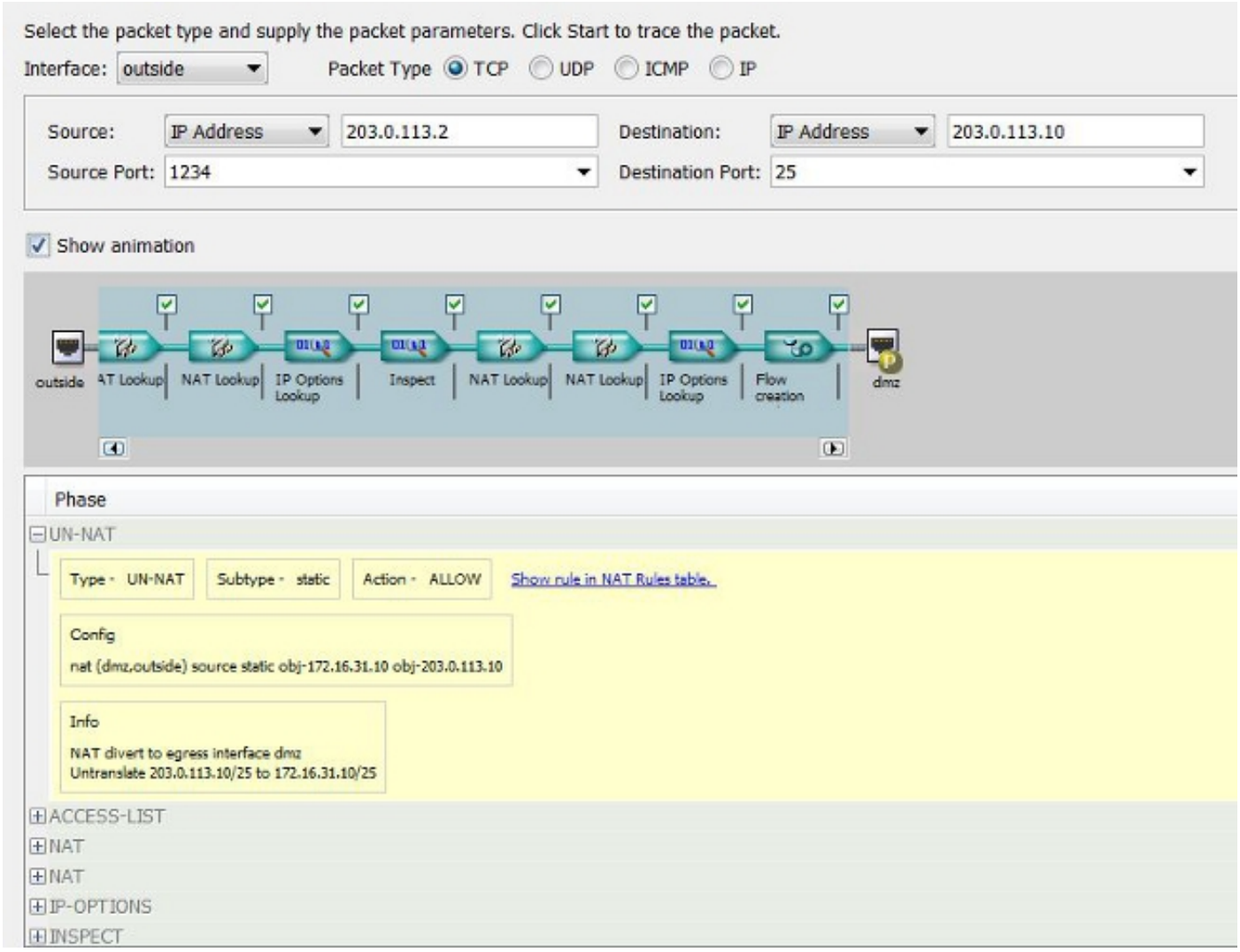
- El paquete simulado llega al **exterior**.
- El protocolo que se usa es TCP.
- La dirección IP del cliente simulado es 203.0.113.2.
- El cliente envía el tráfico que se origina en el puerto 1234.
- El tráfico se destina a un servidor en la dirección IP 203.0.113.10.

- El tráfico está destinado al puerto 25.

A continuación se muestra un ejemplo de resultado del trazador de paquetes:

```
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
```

A continuación se muestra un ejemplo de Cisco Adaptive Security Device Manager (ASDM):



Observe que no se menciona la interfaz *DMZ* en las salidas anteriores. Esto es por diseño de Packet Tracer. La herramienta le indica cómo el firewall procesa ese tipo de intento de conexión, que incluye cómo lo rutearía y desde qué interfaz.

> **Consejo:** Para obtener información adicional sobre la función de seguimiento de paquetes, refiérase a la sección Seguimiento de Paquetes con Packet Tracer de la *Guía de Configuración de Cisco ASA 5500 Series con la CLI, 8.4 y 8.6*.

Captura de paquete

El firewall ASA puede capturar el tráfico que entra o sale de sus interfaces. Esta funcionalidad de captura es muy útil porque puede probar definitivamente si el tráfico llega a un firewall o sale de él. El siguiente ejemplo muestra la configuración de dos capturas denominadas **capd** y **capout** en las interfaces DMZ y externas, respectivamente. Los comandos capture utilizan una palabra clave match, que le permite ser específico sobre el tráfico que desea capturar.

Para el **Capd de captura** en este ejemplo, se indica que desea hacer coincidir el tráfico visto en la interfaz DMZ (entrada o salida) que coincide con el host TCP 172.16.31.10/host 203.0.113.2. En otras palabras, desea capturar cualquier tráfico TCP que se envíe del host 172.16.31.10 al host 203.0.113.2, o viceversa. El uso de la palabra clave match permite que el firewall capture ese tráfico bidireccionalmente. El comando capture que se define para la interfaz externa no hace referencia a la dirección IP del servidor de correo interno porque el firewall realiza una NAT en esa dirección IP del servidor de correo. Como resultado, no puede coincidir con esa dirección IP del servidor. En cambio, el siguiente ejemplo utiliza la palabra **any** para indicar que todas las direcciones IP posibles coincidirían con esa condición.

Después de configurar las capturas, debe intentar establecer una conexión de nuevo y continuar con la vista de las capturas con el comando **show capture <capture_name>**. En este ejemplo, puede ver que el host externo pudo conectarse al servidor de correo, como lo evidencia el intercambio de señales tridireccional TCP que se ve en las capturas:

```
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
```

Servidor de correo en la red interna

Packet-Tracer

A continuación se muestra un ejemplo de resultado del trazador de paquetes:

```
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
```

Servidor de correo en la red externa

Packet-Tracer

A continuación se muestra un ejemplo de resultado del trazador de paquetes:

```
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
```

Información Relacionada

- Mensajes de Syslog de la serie ASA de Cisco
- Ejemplo de Configuración de Capturas de Paquetes ASA con CLI y ASDM
- Guía de Configuración de Cisco ASA Series CLI, 9.0 - Configuración de Network Object NAT
- Soporte técnico y documentación - Cisco Systems