Configuración de DNS Doctoring para Tres Interfaces NAT en ASA Versión 9.x

Contenido

Introducción

Este documento proporciona una configuración de ejemplo para realizar la documentación del sistema de nombres de dominio (DNS) en ASA 5500-X Series Adaptive Security Appliance (ASA) que utiliza instrucciones de traducción de direcciones de red automática (NAT)/objeto. La documentación DNS permite al dispositivo de seguridad reescribir los registros A de DNS.

La reescritura de DNS realiza dos funciones:

- Traduce una dirección pública (la enrutable o la asignada) en una respuesta DNS a una dirección privada (la dirección real) cuando el cliente DNS se encuentra en una interfaz

privada.
- Traduce una dirección privada a una dirección pública cuando el cliente DNS está en la interfaz pública.

Prerequisites

Requirements

Cisco afirma que la inspección de DNS debe estar habilitada para realizar la documentación de DNS en el dispositivo de seguridad. La inspección de DNS está activada de forma predeterminada.

Cuando se habilita la inspección de DNS, el dispositivo de seguridad realiza estas tareas:

- Traduce el registro DNS basándose en la configuración completada con el uso de comandos de objeto/NAT automática (reescritura DNS). La traducción sólo se aplica al registro A en la respuesta DNS. Por lo tanto, las búsquedas inversas, que solicitan el registro de puntero (PTR), no se ven afectadas por la reescritura de DNS. En la versión ASA 9.0(1) y posteriores, la traducción del registro DNS PTR para las búsquedas DNS inversas cuando se usa NAT IPv4, NAT IPv6 y NAT64 con la inspección DNS habilitada para la regla NAT.**Nota:** La reescritura de DNS no es compatible con la traducción estática de direcciones de puerto (PAT) porque se aplican varias reglas PAT para cada registro A y la regla PAT que se debe utilizar es ambigua.
- Aplica la longitud máxima del mensaje DNS (el valor predeterminado es 512 bytes y la longitud máxima es 65535 bytes). El reensamblado se realiza según sea necesario para verificar que la longitud del paquete es inferior a la longitud máxima configurada. El paquete se descarta si supera la longitud máxima.**Nota:** Si ingresa el comando **inspect dns** sin la opción maximum length, el tamaño del paquete DNS no se verifica.
- Aplica una longitud de nombre de dominio de 255 bytes y una longitud de etiqueta de 63 bytes.
- Verifica la integridad del nombre de dominio al que hace referencia el puntero si se encuentran punteros de compresión en el mensaje DNS.
- Comprueba si existe un loop de puntero de compresión.

Componentes Utilizados

La información de este documento se basa en ASA 5500-X Series Security Appliance, versión 9.x.

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.

Productos Relacionados

Esta configuración también se puede utilizar con Cisco ASA 5500 Series Security Appliance,

versión 8.4 o posterior.

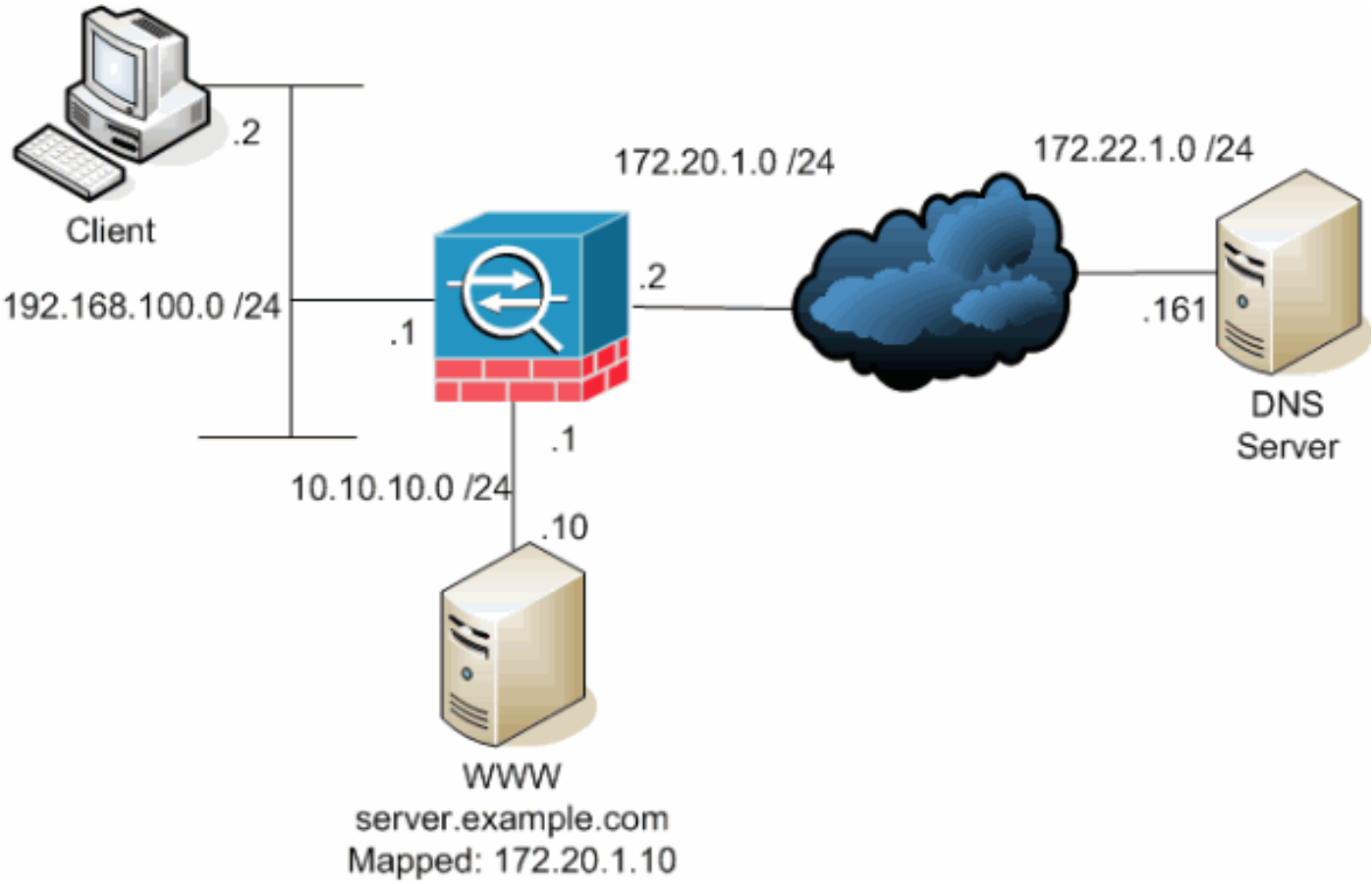
Nota: La configuración de ASDM sólo se aplica a la versión 7.x.

Antecedentes

En un intercambio DNS típico, un cliente envía una URL o un nombre de host a un servidor DNS para determinar la dirección IP de ese host. El servidor DNS recibe la solicitud, busca la asignación de nombre a dirección IP para ese host y luego proporciona el registro A con la dirección IP al cliente. Aunque este procedimiento funciona bien en muchas situaciones, pueden producirse problemas. Estos problemas pueden ocurrir cuando el cliente y el host al que el cliente intenta llegar están en la misma red privada detrás de NAT, pero el servidor DNS utilizado por el cliente está en otra red pública.

Situación: Tres interfaces NAT: interior, exterior, DMZ

Topología



Este diagrama es un ejemplo de esta situación. En este caso, el cliente en 192.168.100.2 desea utilizar la URL **server.example.com** para acceder al servidor WWW en 10.10.10.10. Los servicios DNS para el cliente los proporciona el servidor DNS externo en 172.22.1.161. Dado que el servidor DNS se encuentra en otra red pública, no conoce la dirección IP privada del servidor WWW. En su lugar, conoce la dirección asignada del servidor WWW de 172.20.1.10. Por lo tanto,

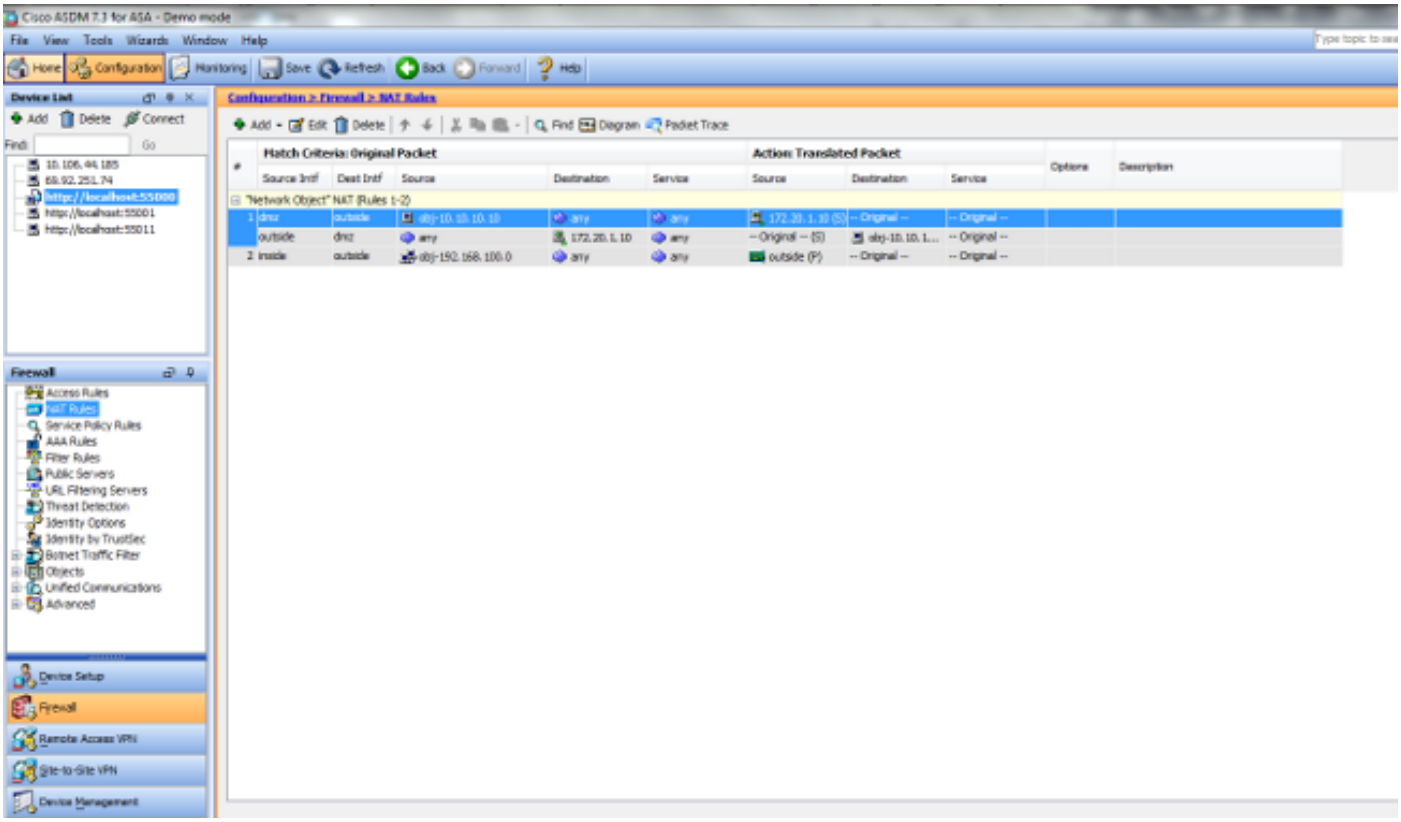
el servidor DNS contiene la asignación de dirección IP a nombre de **server.example.com** a **172.20.1.10**.

Problema: El cliente no puede acceder al servidor WWW

Sin la documentación DNS u otra solución habilitada en esta situación, si el cliente envía una solicitud DNS para la dirección IP de **server.example.com**, no podrá acceder al servidor WWW. Esto se debe a que el cliente recibe un registro A que contiene la dirección pública asignada de 172.20.1.10 para el servidor WWW. Cuando el cliente intenta acceder a esta dirección IP, el dispositivo de seguridad descarta los paquetes porque no permite la redirección de paquetes en la misma interfaz. A continuación, se muestra cómo se ve la parte NAT de la configuración cuando no está habilitada la documentación DNS:

```
ASA Version 9.x
!
hostname ciscoasa

!--- Output suppressed.

access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www
!--- Output suppressed.

object network obj-192.168.100.0
network 192.168.100.0 255.255.255.0
nat (inside,outside) dynamic interface

object network obj-10.10.10.10
host 10.10.10.10
nat (dmz,outside) static 172.20.1.10

!--- Static translation to allow hosts on the outside access
!--- to the WWW server.
access-group OUTSIDE in interface outside

!--- Output suppressed.
```

Así es como se ve la configuración en el ASDM cuando el doctorado DNS no está habilitado:



Aquí hay una captura de paquetes de los eventos cuando la documentación DNS no está habilitada:

1. El cliente envía la consulta DNS.

```
No.     Time        Source          Destination     Protocol Info
1 0.000000 192.168.100.2   172.22.1.161    DNS Standard query
A server.example.com

Frame 1 (78 bytes on wire, 78 bytes captured)
Ethernet II, Src: Cisco_c8:e4:00 (00:04:c0:c8:e4:00), Dst: Cisco_9c:c6:1f
(00:0a:b8:9c:c6:1f)
Internet Protocol, Src: 192.168.100.2 (192.168.100.2), Dst: 172.22.1.161
(172.22.1.161)
User Datagram Protocol, Src Port: 50879 (50879), Dst Port: domain (53)
Domain Name System (query)
[Response In: 2]
Transaction ID: 0x0004
Flags: 0x0100 (Standard query)
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
server.example.com: type A, class IN
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
```

2. El ASA realiza PAT en la consulta DNS y la consulta se reenvía. Observe que la dirección de origen del paquete ha cambiado a la interfaz exterior del ASA.

```
No.     Time        Source          Destination     Protocol Info
1 0.000000 172.20.1.2      172.22.1.161    DNS Standard query
A server.example.com

Frame 1 (78 bytes on wire, 78 bytes captured)
Ethernet II, Src: Cisco_9c:c6:1e (00:0a:b8:9c:c6:1e), Dst: Cisco_01:f1:22
(00:30:94:01:f1:22)
```

```
Internet Protocol, Src: 172.20.1.2 (172.20.1.2), Dst: 172.22.1.161
(172.22.1.161)
User Datagram Protocol, Src Port: 1044 (1044), Dst Port: domain (53)
Domain Name System (query)
[Response In: 2]
Transaction ID: 0x0004
Flags: 0x0100 (Standard query)
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
server.example.com: type A, class IN
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
```

3. El servidor DNS responde con la dirección asignada del servidor WWW.

```
No.     Time       Source         Destination       Protocol Info
2 0.005005 172.22.1.161   172.20.1.2        DNS Standard query response
A 172.20.1.10

Frame 2 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Cisco_01:f1:22 (00:30:94:01:f1:22), Dst: Cisco_9c:c6:1e
(00:0a:b8:9c:c6:1e)
Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 172.20.1.2
(172.20.1.2)
User Datagram Protocol, Src Port: domain (53), Dst Port: 1044 (1044)
Domain Name System (response)
[Request In: 1]
[Time: 0.005005000 seconds]
Transaction ID: 0x0004
Flags: 0x8580 (Standard query response, No error)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
server.example.com: type A, class IN
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
Answers
server.example.com: type A, class IN, addr 172.20.1.10
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
Time to live: 1 hour
Data length: 4
Addr: 172.20.1.10
```

4. El ASA deshace la traducción de la dirección de destino de la respuesta DNS y reenvía el paquete al cliente. Tenga en cuenta que sin la documentación DNS activada, la **dirección Addr** en la respuesta sigue siendo la dirección asignada del servidor WWW.

```
No.     Time       Source         Destination       Protocol Info
2 0.005264 172.22.1.161 192.168.100.2    DNS Standard query response
A 172.20.1.10

Frame 2 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Cisco_9c:c6:1f (00:0a:b8:9c:c6:1f), Dst: Cisco_c8:e4:00
(00:04:c0:c8:e4:00)
Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 192.168.100.2
(192.168.100.2)
User Datagram Protocol, Src Port: domain (53), Dst Port: 50879 (50879)
```

```
Domain Name System (response)
[Request In: 1]
[Time: 0.005264000 seconds]
Transaction ID: 0x0004
Flags: 0x8580 (Standard query response, No error)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
server.example.com: type A, class IN
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
Answers
server.example.com: type A, class IN, addr 172.20.1.10
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
Time to live: 1 hour
Data length: 4
Addr: 172.20.1.10
```

5. En este momento, el cliente intenta acceder al servidor WWW en 172.20.1.10. El ASA crea una entrada de conexión para esta comunicación. Sin embargo, debido a que no permite que el tráfico fluya de adentro hacia afuera hacia DMZ, la conexión se agota. Los registros de ASA muestran lo siguiente:

```
%ASA-6-302013: Built outbound TCP connection 54175 for
outside:172.20.1.10/80 (172.20.1.10/80) to inside:192.168.100.2/11001
(172.20.1.2/1024)

%ASA-6-302014: Teardown TCP connection 54175 for outside:172.20.1.10/80
to inside:192.168.100.2/11001 duration 0:00:30 bytes 0 SYN Timeout
```

Solución: Palabra clave "DNS"

Documentación de DNS con la palabra clave "dns"

La documentación DNS con la palabra clave **dns** proporciona al dispositivo de seguridad la capacidad de interceptar y reescribir el contenido de las respuestas del servidor DNS al cliente. Cuando se configura correctamente, el dispositivo de seguridad puede alterar el registro A para permitir al cliente en un escenario como el descrito en el problema ": El cliente no puede acceder a la sección WW Server" para conectarse. En esta situación con la documentación DNS activada, el dispositivo de seguridad reescribe el registro A para dirigir al cliente a 10.10.10.10 en lugar de a 172.20.1.10. La documentación de DNS se habilita cuando se agrega la palabra clave **dns** a una instrucción NAT estática (versión 8.2 y anteriores) o a una instrucción de objeto/NAT automática (versión 8.3 y posteriores) .

Versión 8.2 y anterior

Esta es la configuración final del ASA para realizar el doctorado DNS con la palabra clave **dns** y tres interfaces NAT para las versiones 8.2 y anteriores.

```
ciscoasa#show running-config
```

```
: Saved
:
ASA Version 8.2.x
!
hostname ciscoasa
enable password 9jNfZuG3TC5tCVH0 encrypted
names
dns-guard
!
interface Ethernet0/0
nameif outside
security-level 0
ip address 172.20.1.2 255.255.255.0
!
interface Ethernet0/1
nameif inside
security-level 100
ip address 192.168.100.1 255.255.255.0
!
interface Ethernet0/2
nameif dmz
security-level 50
ip address 10.10.10.1 255.255.255.0
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
access-list OUTSIDE extended permit tcp any host 172.20.1.10 eq www

pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
mtu dmz 1500
asdm image disk0:/asdm512-k8.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 192.168.100.0 255.255.255.0
static (inside,dmz) 192.168.100.0 192.168.100.0 netmask 255.255.255.0
static (dmz,outside) 172.20.1.10 10.10.10.10 netmask 255.255.255.255 dns

access-group OUTSIDE in interface outside

route outside 0.0.0.0 0.0.0.0 172.20.1.1 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
username cisco password ffIRPGpDSOJh9YLq encrypted
http server enable
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 MY_DNS_INSPECT_MAP
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
inspect esmtp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect dns MY_DNS_INSPECT_MAP
inspect icmp
policy-map type inspect dns migrated_dns_map_1
parameters
message-length maximum 512
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:d6637819c6ea981daf20d8c7aa8ca256
: end
```

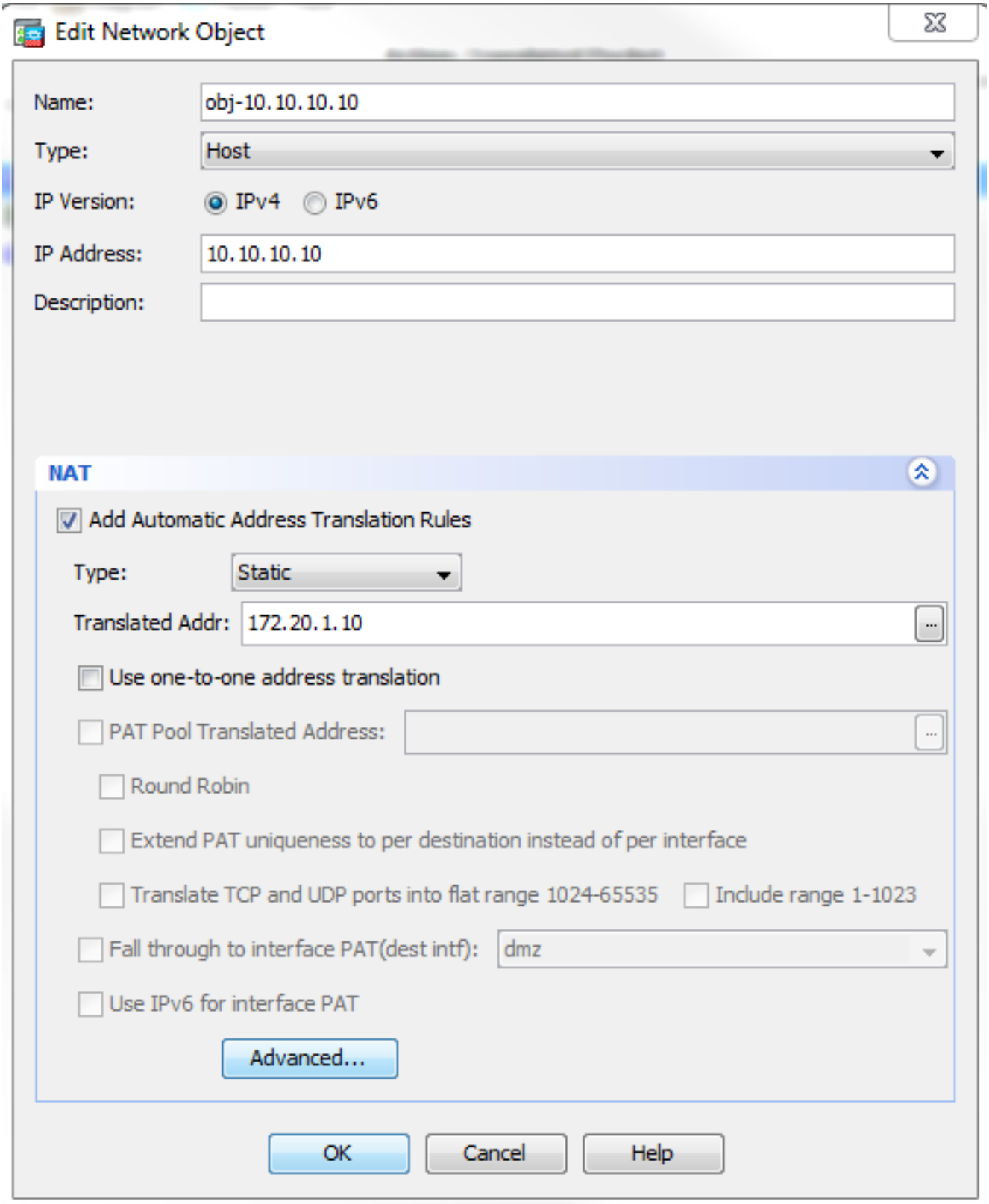
Versión 8.3 y posterior

```
ASA Version 9.x
!
hostname ciscoasa

!--- Output suppressed.

access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www

!--- Output suppressed.

object network obj-192.168.100.0
network 192.168.100.0 255.255.255.0
nat (inside,outside) dynamic interface

object network obj-10.10.10.10
host 10.10.10.10
nat (dmz,outside) static 172.20.1.10 dns

!--- Static translation to allow hosts on the outside access
!--- to the WWW server.

access-group OUTSIDE in interface outside

!--- Output suppressed.
```

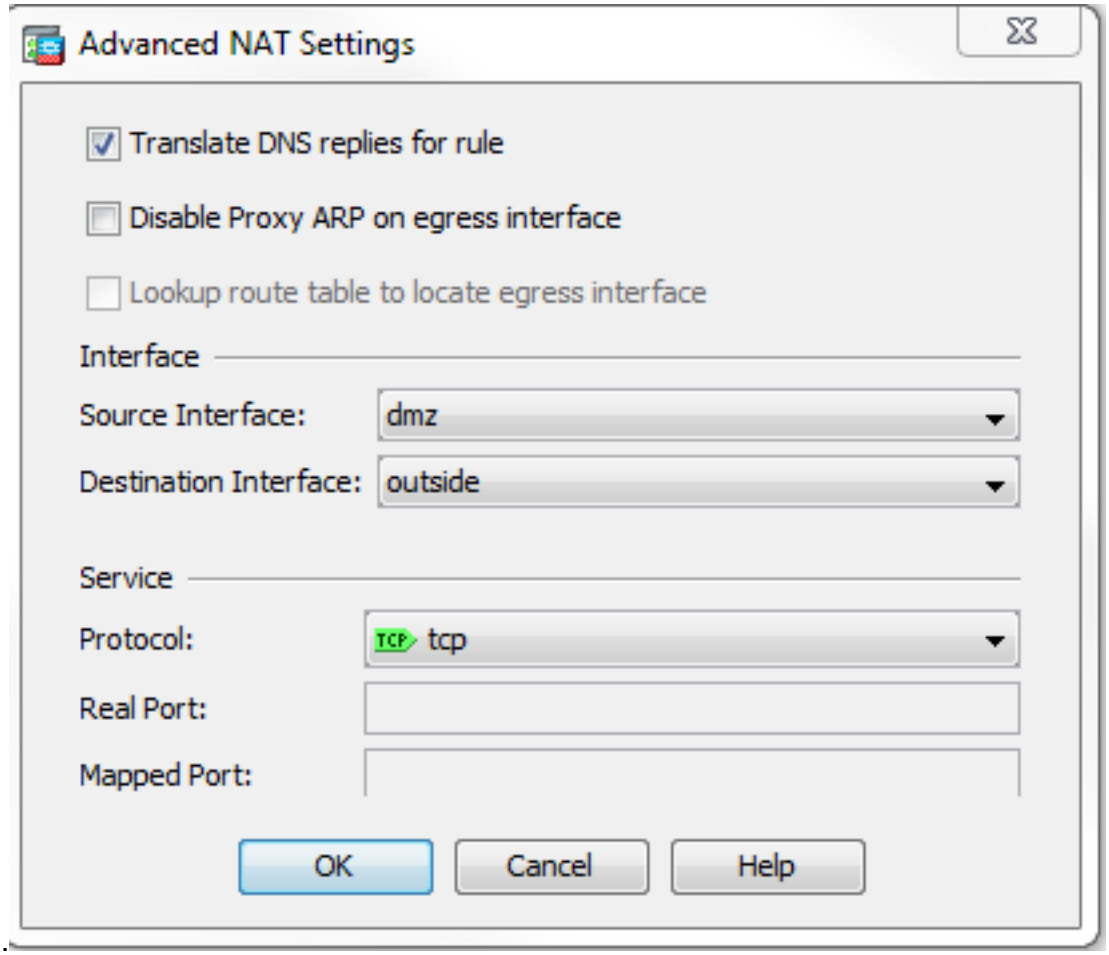
Configuración de ASDM

Complete estos pasos para configurar la documentación DNS en el ASDM:

1. Elija **Configuration > NAT Rules** y elija la regla Object/Auto que se modificará. Haga clic en **Editar**.
2. Haga clic en **Avanzado...**



3. Marque la casilla de verificación **Traducir respuestas DNS para la**



regla.

4. Haga clic en **Aceptar** para salir de la ventana Opciones de NAT.
5. Haga clic en **Aceptar** para salir de la ventana Edit Object/Auto NAT Rule .
6. Haga clic en **Aplicar** para enviar su configuración al dispositivo de seguridad.

Verificación

Esta es una captura de paquetes de los eventos cuando se habilita la documentación DNS:

1. El cliente envía la consulta DNS.

```
No.     Time        Source           Destination     Protocol Info
1 0.000000 192.168.100.2    172.22.1.161    DNS Standard query
A server.example.com

Frame 1 (78 bytes on wire, 78 bytes captured)
Ethernet II, Src: Cisco_c8:e4:00 (00:04:c0:c8:e4:00), Dst: Cisco_9c:c6:1f
(00:0a:b8:9c:c6:1f)
Internet Protocol, Src: 192.168.100.2 (192.168.100.2), Dst: 172.22.1.161
(172.22.1.161)
User Datagram Protocol, Src Port: 52985 (52985), Dst Port: domain (53)
Domain Name System (query)
[Response In: 2]
Transaction ID: 0x000c
Flags: 0x0100 (Standard query)
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
server.example.com: type A, class IN
Name: server.example.com
Type: A (Host address)
```

Class: IN (0x0001)

2. El ASA realiza PAT en la consulta DNS y la consulta se reenvía. Observe que la dirección de origen del paquete ha cambiado a la interfaz exterior del ASA.

```
No.     Time       Source          Destination       Protocol Info
1 0.000000 172.20.1.2      172.22.1.161      DNS  Standard query
A server.example.com

Frame 1 (78 bytes on wire, 78 bytes captured)
Ethernet II, Src: Cisco_9c:c6:1e (00:0a:b8:9c:c6:1e), Dst: Cisco_01:f1:22
(00:30:94:01:f1:22)
Internet Protocol, Src: 172.20.1.2 (172.20.1.2), Dst: 172.22.1.161
(172.22.1.161)
User Datagram Protocol, Src Port: 1035 (1035), Dst Port: domain (53)
Domain Name System (query)
[Response In: 2]
Transaction ID: 0x000c
Flags: 0x0100 (Standard query)
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
server.example.com: type A, class IN
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
```

3. El servidor DNS responde con la dirección asignada del servidor WWW.

```
No.     Time       Source         Destination     Protocol Info
2 0.000992 172.22.1.161   172.20.1.2      DNS Standard query response
A 172.20.1.10

Frame 2 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Cisco_01:f1:22 (00:30:94:01:f1:22), Dst: Cisco_9c:c6:1e
(00:0a:b8:9c:c6:1e)
Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 172.20.1.2
(172.20.1.2)
User Datagram Protocol, Src Port: domain (53), Dst Port: 1035 (1035)
Domain Name System (response)
[Request In: 1]
[Time: 0.000992000 seconds]
Transaction ID: 0x000c
Flags: 0x8580 (Standard query response, No error)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
server.example.com: type A, class IN
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
Answers
server.example.com: type A, class IN, addr 172.20.1.10
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
Time to live: 1 hour
Data length: 4
Addr: 172.20.1.10
```

4. El ASA deshace la traducción de la dirección de destino de la respuesta DNS y reenvía el paquete al cliente. Tenga en cuenta que con la documentación DNS activada, la dirección en la respuesta se reescribe para que sea la dirección real del servidor WWW.

```
No.     Time       Source         Destination     Protocol Info
6 2.507191 172.22.1.161   192.168.100.2   DNS Standard query response
A 10.10.10.10

Frame 6 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Cisco_9c:c6:1f (00:0a:b8:9c:c6:1f), Dst: Cisco_c8:e4:00
(00:04:c0:c8:e4:00)
Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 192.168.100.2
(192.168.100.2)
User Datagram Protocol, Src Port: domain (53), Dst Port: 50752 (50752)
Domain Name System (response)
[Request In: 5]
[Time: 0.002182000 seconds]
Transaction ID: 0x0004
Flags: 0x8580 (Standard query response, No error)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
server.example.com: type A, class IN
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
Answers
server.example.com: type A, class IN, addr 10.10.10.10
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
Time to live: 1 hour
Data length: 4
Addr: 10.10.10.10
```

5. En este punto, el cliente intenta acceder al servidor WWW en 10.10.10.10. La conexión se realiza correctamente.

Configuración final con la palabra clave "dns"

Esta es la configuración final del ASA para realizar el doctorado DNS con la palabra clave **dns** y tres interfaces NAT.

```
ciscoasa# sh running-config
: Saved
:
: Serial Number: JMX1425L48B
: Hardware:   ASA5510, 1024 MB RAM, CPU Pentium 4 Celeron 1600 MHz
:
ASA Version 9.1(5)4
!
hostname ciscoasa
enable password 9jNfZuG3TC5tCVH0 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
dns-guard
!
interface Ethernet0/0
 shutdown
 nameif outside
 security-level 0
 ip address 172.20.1.2 255.255.255.0
!
```

```
interface Ethernet0/1
 shutdown
 nameif inside
 security-level 100
 ip address 192.168.100.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 nameif dmz
 security-level 50
 ip address 10.10.10.1 255.255.255.0
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
 shutdown
 no nameif
 no security-level
 no ip address
!
ftp mode passive
object network obj-192.168.100.0
 subnet 192.168.100.0 255.255.255.0
object network obj-10.10.10.10
 host 10.10.10.10
access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www
pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm512-k8.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
!
object network obj-192.168.100.0
 nat (inside,outside) dynamic interface
object network obj-10.10.10.10
 nat (dmz,outside) static 172.20.1.10 dns
access-group OUTSIDE in interface outside
route outside 0.0.0.0 0.0.0.0 172.20.1.1 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
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
http server enable
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
```

```
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
no ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
 anyconnect-essentials
username cisco password ffIRPGpDSOJh9YLq encrypted
!
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
policy-map global_policy
 class inspection_default
 inspect dns preset_dns_map
 inspect ftp
 inspect h323 h225
 inspect h323 ras
 inspect rsh
 inspect rtsp
 inspect esmtp
 inspect sqlnet
 inspect skinny
 inspect sunrpc
 inspect xdmcp
 inspect sip
 inspect netbios
 inspect tftp
 inspect ip-options
 inspect icmp
policy-map type inspect dns MY_DNS_INSPECT_MAP
 parameters
 message-length maximum 512
policy-map type inspect dns migrated_dns_map_1
 parameters
 message-length maximum 512
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:3a8e3009aa3db1d6dba143abf25ee408
: end
```

Solución alternativa: NAT de destino

La NAT de destino puede proporcionar una alternativa a la documentación DNS. El uso de NAT de destino en esta situación requiere que se cree un objeto estático/traducción NAT automática entre la dirección pública del servidor WWW en el interior y la dirección real en la DMZ. La NAT de destino no cambia el contenido del registro A de DNS que se devuelve del servidor DNS al cliente. En su lugar, cuando utiliza NAT de destino en un escenario como el descrito en este documento, el cliente puede utilizar la dirección IP pública **172.20.1.10** que devuelve el servidor DNS para conectarse al servidor WWW. El objeto estático/traducción automática permite al

dispositivo de seguridad traducir la dirección de destino de 172.20.1.10 a 10.10.10.10. Esta es la parte relevante de la configuración cuando se utiliza NAT de destino:

```
ASA Version 9.x
!
hostname ciscoasa

!--- Output suppressed.

access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www

!--- Output suppressed.

object network obj-192.168.100.0
network 192.168.100.0 255.255.255.0
nat (inside,outside) dynamic interface

!--- The nat and global commands allow
!--- clients access to the Internet.

object network obj-10.10.10.10
host 10.10.10.10
nat (dmz,outside) static 172.20.1.10

!--- Static translation to allow hosts on the outside access
!--- to the WWW server.

object network obj-10.10.10.10-1
host 10.10.10.10
nat (dmz,inside) static 172.20.1.10
```

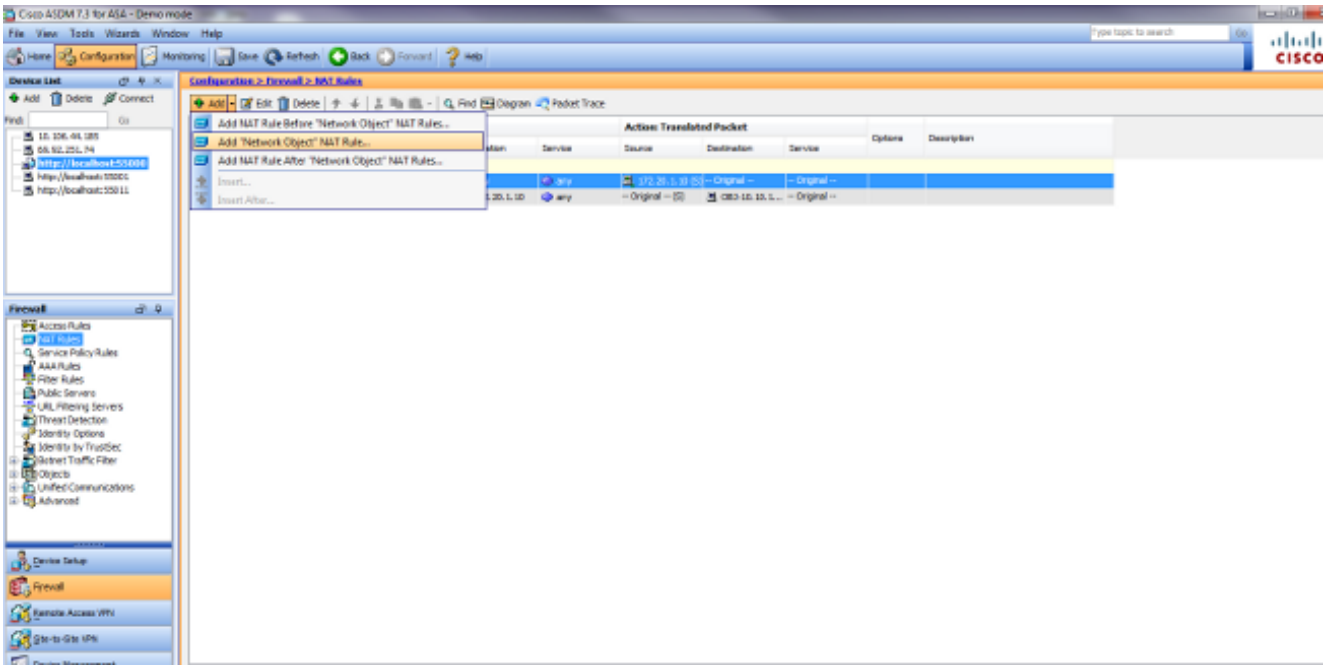
NAT de destino lograda con declaración NAT manual/doble

```
ASA Version 9.x
!
hostname ciscoasa

!--- Output suppressed.

access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www

!--- Output suppressed.

object network obj-192.168.100.0
network 192.168.100.0 255.255.255.0
nat (inside,outside) dynamic interface

object network obj-10.10.10.10
host 10.10.10.10

object network obj-172.20.1.10
host 172.20.1.10

nat (inside,dmz) source dynamic obj-192.168.100.0 interface
destination static obj-172.20.1.10 obj-10.10.10.10

!--- Static translation to allow hosts on the inside access
!--- to the WWW server via its outside address.

access-group OUTSIDE in interface outside
```

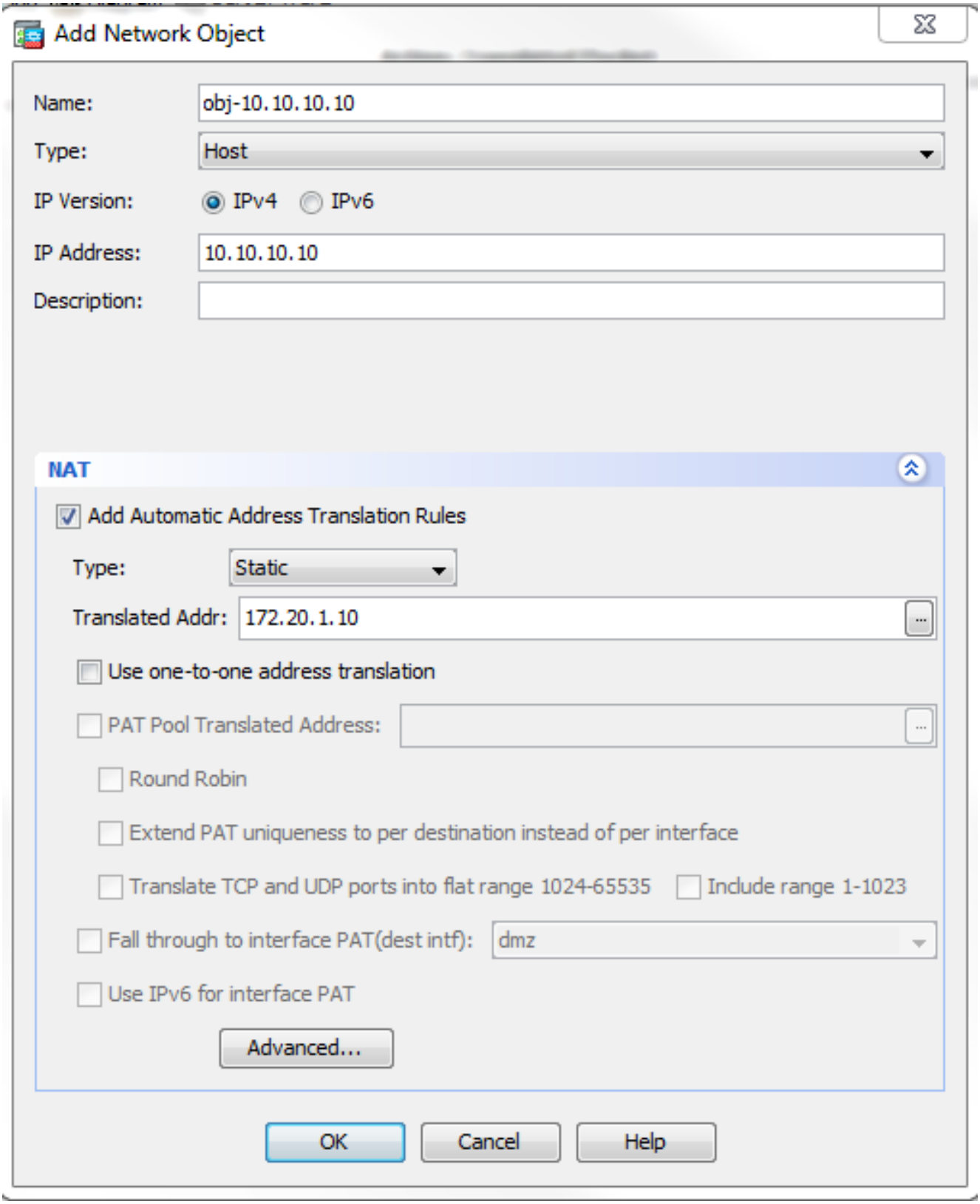
```
!--- Output suppressed.
```

Complete estos pasos para configurar la NAT de destino en el ASDM:

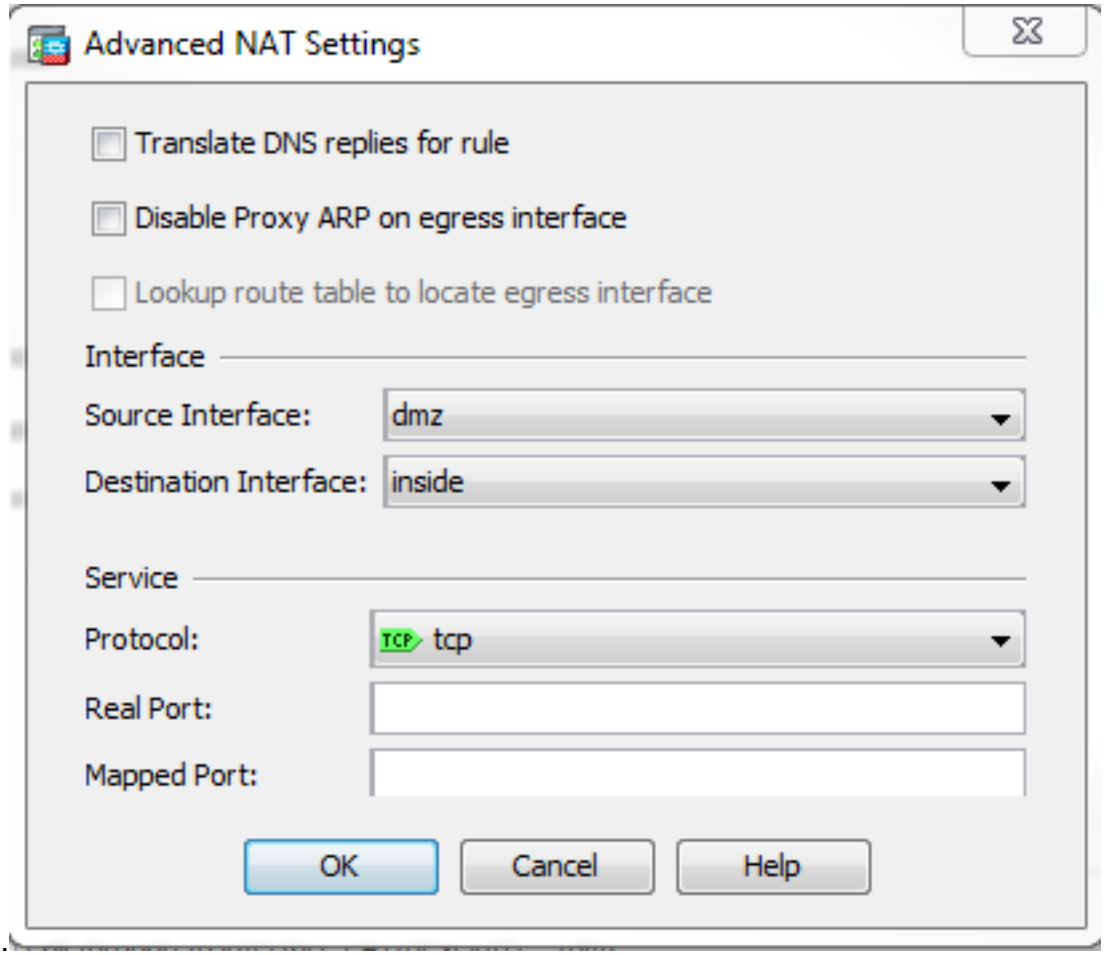
1. Elija **Configuration > NAT Rules** y elija **Add > Add "Network Object" NAT Rule...**.



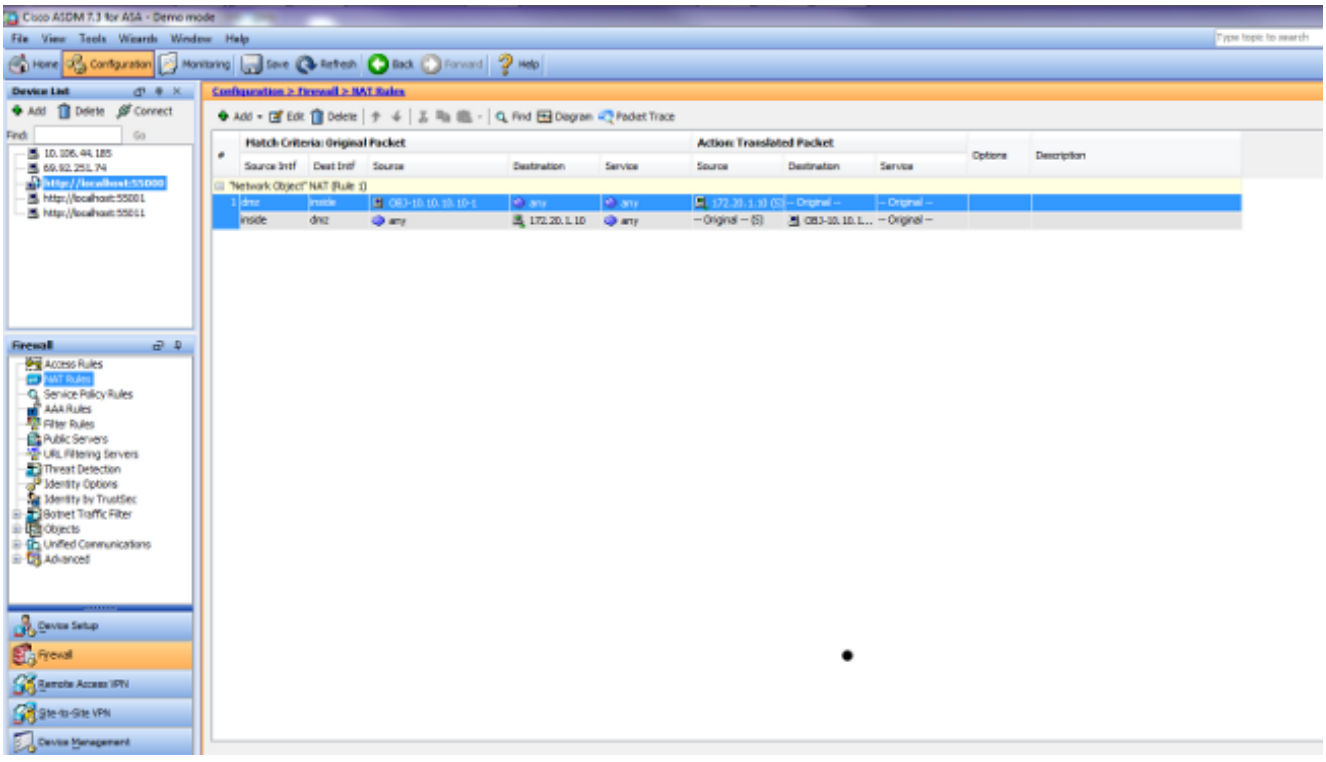
2. Complete la configuración para la nueva traducción estática. En el campo Nombre, introduzca **obj-10.10.10.10**.En el campo IP Address (Dirección IP), introduzca la dirección de la dirección IP del servidor WWW.En la lista desplegable Tipo, elija **Estático**.En el campo Dirección traducida, introduzca la dirección y la interfaz a la que desea asignar el servidor WWW.Haga clic en **Advanced**.



En la lista desplegable Interfaz de origen, elija **dmz**.En la lista desplegable Destination Interface , elija **inside**.En este caso, se elige la interfaz interna para permitir que los hosts en la interfaz interna accedan al servidor WWW a través de la dirección asignada



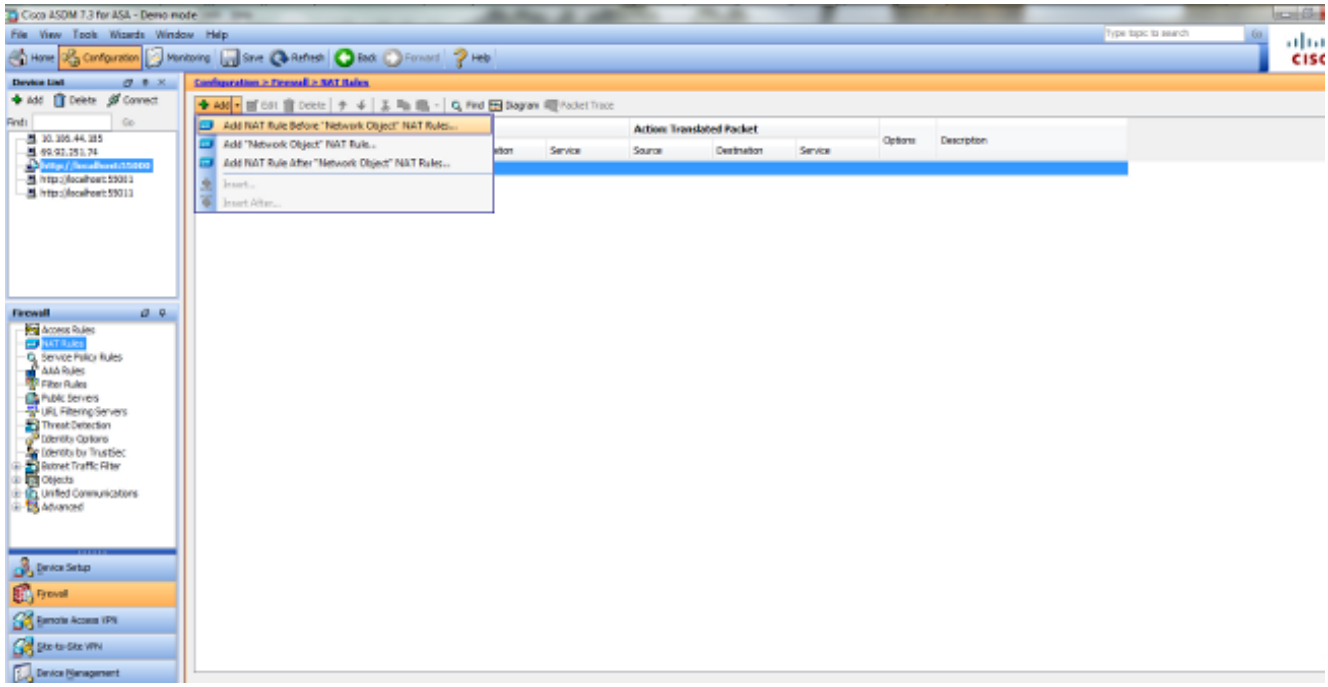
172.20.1.10.



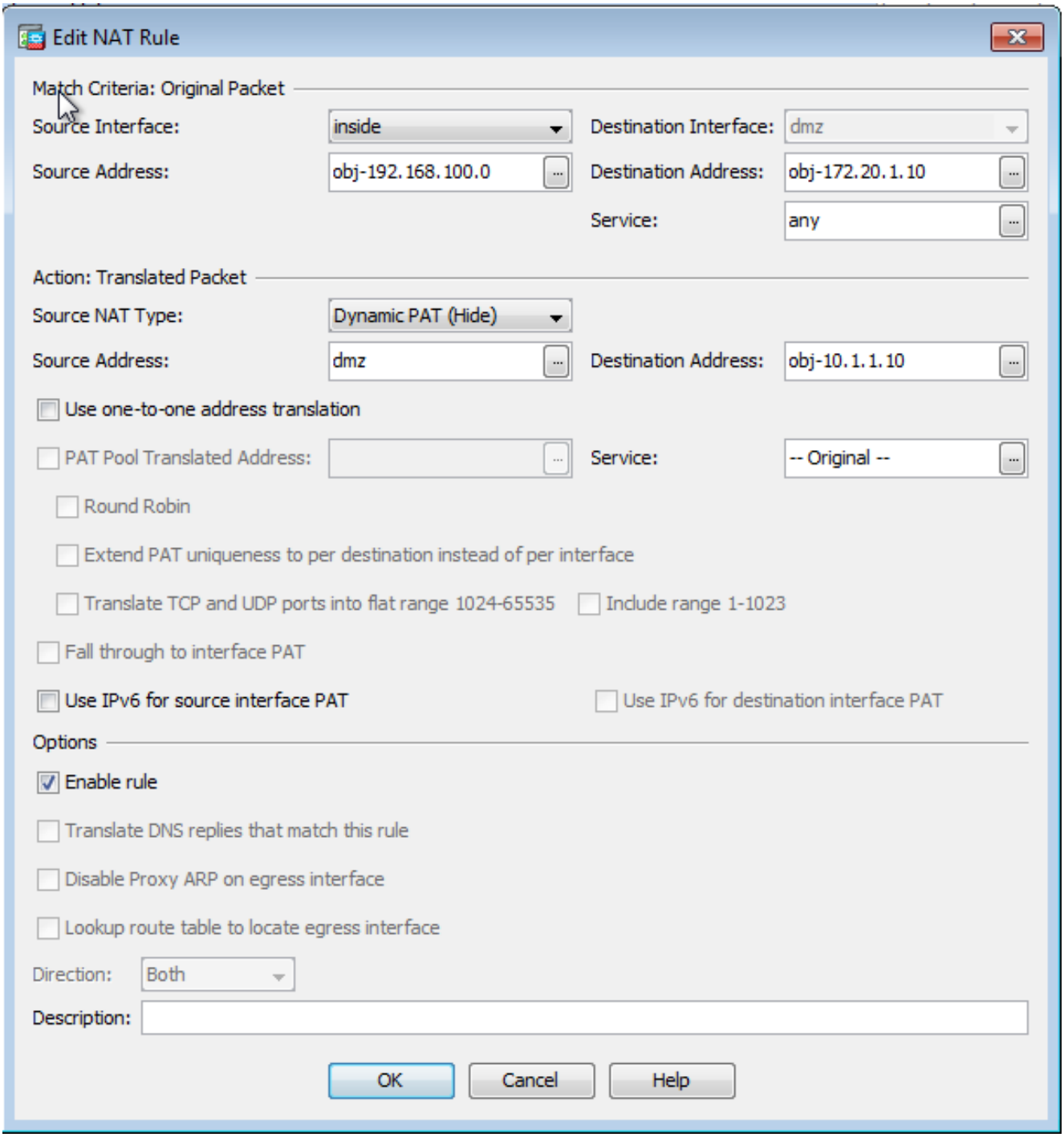
Haga clic en **Aceptar** para salir de la ventana Add Object/Auto NAT Rule .Haga clic en **Aplicar** para enviar la configuración al dispositivo de seguridad.

Método alternativo con NAT manual/doble y ASDM

1. Elija **Configuration > NAT Rules** y elija **Add > Add Nat rule antes "Network Object" NAT Rule...**.



2. Complete la configuración para la traducción Manual/Dos veces Nat. En la lista desplegable Interfaz de origen, elija **interior**.En la lista desplegable Destination Interface , elija **dmz**.En el campo Dirección de origen, introduzca el objeto de red interno (obj-192.168.100.0).En el campo Destination Address (Dirección de destino), introduzca elobjeto IP del servidor DMZ traducido (172.20.1.10).En la lista desplegable Tipo de NAT de Origen, elija **PAT Dinámico (Ocultar)**.En la dirección de origen [Acción: sección Paquete traducido], introduzca **dmz**.En el destino Dirección [Acción: Sección de paquetes traducidos] campo, introduzca el objeto IP real del servidor DMZ (obj-10.10.10.10).



3. Haga clic en **Aceptar** para salir de la ventana Add Manual/Twice NAT Rule .
4. Haga clic en **Aplicar** para enviar la configuración al dispositivo de seguridad.

Esta es la secuencia de eventos que tienen lugar cuando se configura la NAT de destino. Suponga que el cliente ya ha consultado al servidor DNS y ha recibido una respuesta de **172.20.1.10** para la dirección del servidor WWW:

1. El cliente intenta comunicarse con el servidor WWW en 172.20.1.10.
   ```
   %ASA-7-609001: Built local-host inside:192.168.100.2
   ```
2. El dispositivo de seguridad ve la solicitud y reconoce que el servidor WWW es 10.10.10.10.
   ```
   %ASA-7-609001: Built local-host dmz:10.10.10.10
   ```
3. El dispositivo de seguridad crea una conexión TCP entre el cliente y el servidor WWW. Observe las direcciones asignadas de cada host entre paréntesis.
   ```
   %ASA-6-302013: Built outbound TCP connection 67956 for dmz:10.10.10.10/80
   (172.20.1.10/80) to inside:192.168.100.2/11001 (192.168.100.2/11001)
   ```
4. El comando **show xlate** en el dispositivo de seguridad verifica que el tráfico del cliente se traduce a través del dispositivo de seguridad. En este caso, la primera traducción estática

está en uso.

```
ciscoasa#show xlate
3 in use, 9 most used
Global 192.168.100.0 Local 192.168.100.0
Global 172.20.1.10 Local 10.10.10.10
Global 172.20.1.10 Local 10.10.10.10
```

5. El comando **show conn** en el dispositivo de seguridad verifica que la conexión se ha realizado correctamente entre el cliente y el servidor WWW a través del dispositivo de seguridad. Observe la dirección real del servidor WWW entre paréntesis.

```
ciscoasa#show conn
TCP out 172.20.1.10(10.10.10.10):80 in 192.168.100.2:11001
idle 0:01:38 bytes 1486 flags UIO
```

Configuración final con NAT de destino

Esta es la configuración final del ASA para realizar el doctorado DNS con NAT de destino y tres interfaces NAT.

```
ASA Version 9.x
!
hostname ciscoasa
enable password 9jNfZuG3TC5tCVH0 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
dns-guard
!
interface Ethernet0/0
 shutdown
 nameif outside
 security-level 0
 ip address 172.20.1.2 255.255.255.0
!
interface Ethernet0/1
 shutdown
 nameif inside
 security-level 100
 ip address 192.168.100.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 nameif dmz
 security-level 50
 ip address 10.10.10.1 255.255.255.0
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
 shutdown
 no nameif
 no security-level
 no ip address
!
ftp mode passive
object network obj-192.168.100.0
```

```
 subnet 192.168.100.0 255.255.255.0
object network obj-10.10.10.10
 host 10.10.10.10
object network obj-10.10.10.10-1
 host 10.10.10.10
object network obj-172.20.1.10
 host 172.20.1.10
access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www
pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm512-k8.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
!
object network obj-192.168.100.0
 nat (inside,outside) dynamic interface
object network obj-10.10.10.10
 nat (dmz,outside) static 172.20.1.10
object network obj-10.10.10.10-1
 nat (dmz,inside) static 172.20.1.10
access-group OUTSIDE in interface outside
route outside 0.0.0.0 0.0.0.0 172.20.1.1 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
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
http server enable
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
no ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
 anyconnect-essentials
username cisco password ffIRPGpDSOJh9YLq encrypted
!
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
policy-map global_policy
 class inspection_default
 inspect dns preset_dns_map
 inspect ftp
 inspect h323 h225
 inspect h323 ras
 inspect rsh
 inspect rtsp
 inspect esmtp
 inspect sqlnet
 inspect skinny
 inspect sunrpc
 inspect xdmcp
 inspect sip
 inspect netbios
 inspect tftp
 inspect ip-options
 inspect icmp
policy-map type inspect dns MY_DNS_INSPECT_MAP
 parameters
 message-length maximum 512
policy-map type inspect dns migrated_dns_map_1
 parameters
 message-length maximum 512
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:2cdcc45bfc13f9e231f3934b558f1fd4
: end
```

Configurar

Complete estos pasos para habilitar la inspección de DNS (si se ha desactivado previamente). En este ejemplo, la inspección de DNS se agrega a la política de inspección global predeterminada, que se aplica globalmente mediante un comando **service-policy** como si el ASA comenzara con una configuración predeterminada.

1. Cree un mapa de política de inspección para DNS.
   ```
   ciscoasa(config)#policy-map type inspect dns MY_DNS_INSPECT_MAP
   ```
2. Desde el modo de configuración policy-map, ingrese el modo de configuración de parámetros para especificar los parámetros para el motor de inspección.
   ```
   ciscoasa(config-pmap)#parameters
   ```
3. En el modo de configuración de parámetro policy-map, especifique la longitud máxima de mensaje para los mensajes DNS que será 512.
   ```
   ciscoasa(config-pmap-p)#message-length maximum 512
   ```
4. Salga del modo de configuración de parámetro policy-map y del modo de configuración de policy-map.
   ```
   ciscoasa(config-pmap-p)#exit
   ciscoasa(config-pmap)#exit
   ```
5. Confirme que el policy-map de inspección se ha creado como desee.
   ```
   ciscoasa(config)#show run policy-map type inspect dns
   !
   policy-map type inspect dns MY_DNS_INSPECT_MAP
   parameters
   message-length maximum 512
   !
   ```
6. Ingrese el modo de configuración policy-map para **global_policy**.

```
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#
```

7. En el modo de configuración de policy-map, especifique el mapa de clase predeterminado de capa 3/4, **inspection_default**.
```
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#
```
8. En el modo de configuración de clase de policy-map, utilice el mapa de política de inspección creado en los pasos 1-3 para especificar que se debe inspeccionar el DNS.
```
ciscoasa(config-pmap-c)#inspect dns MY_DNS_INSPECT_MAP
```
9. Salga del modo de configuración de clase de policy-map y del modo de configuración de policy-map.
```
ciscoasa(config-pmap-c)#exit
ciscoasa(config-pmap)#exit
```
10. Verifique que el policy-map **global_policy** esté configurado como desee.
```
ciscoasa(config)#show run policy-map
!

!--- The configured DNS inspection policy map.

policy-map type inspect dns MY_DNS_INSPECT_MAP
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
inspect esmtp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect dns MY_DNS_INSPECT_MAP

!--- DNS application inspection enabled.
```
11. Verifique que global_policy se aplique globalmente mediante una política de servicio.
```
ciscoasa(config)#show run service-policy
service-policy global_policy global
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Captura de tráfico DNS

Un método para verificar que el dispositivo de seguridad vuelva a escribir los registros DNS correctamente es capturar los paquetes en cuestión, como se mencionó en el ejemplo anterior. Complete estos pasos para capturar el tráfico en el ASA:

1. Cree una lista de acceso para cada instancia de captura que desee crear.La ACL debe especificar el tráfico que desea capturar. En este ejemplo, se han creado dos ACL. La ACL para el tráfico en la interfaz exterior:

```
access-list DNSOUTCAP extended permit ip host 172.22.1.161 host
172.20.1.2

!--- All traffic between the DNS server and the ASA.

access-list DNSOUTCAP extended permit ip host 172.20.1.2 host
172.22.1.161

!--- All traffic between the ASA and the DNS server.
```

   La ACL para el tráfico en la interfaz interna:

```
access-list DNSINCAP extended permit ip host 192.168.100.2 host
172.22.1.161

!--- All traffic between the client and the DNS server.

access-list DNSINCAP extended permit ip host 172.22.1.161 host
192.168.100.2

!--- All traffic between the DNS server and the client.
```

2. Cree las instancias de captura:

```
ciscoasa#capture DNSOUTSIDE access-list DNSOUTCAP interface outside

!--- This capture collects traffic on the outside interface that matches
!--- the ACL DNSOUTCAP.

ciscoasa# capture DNSINSIDE access-list DNSINCAP interface inside

!--- This capture collects traffic on the inside interface that matches
!--- the ACL DNSINCAP.
```

3. Vea las capturas.A continuación se muestra cómo se ven las capturas de ejemplo después de que se haya pasado algo de tráfico DNS:

```
ciscoasa#show capture DNSOUTSIDE
2 packets captured
1: 14:07:21.347195 172.20.1.2.1025 > 172.22.1.161.53: udp 36
2: 14:07:21.352093 172.22.1.161.53 > 172.20.1.2.1025: udp 93
2 packets shown
ciscoasa#show capture DNSINSIDE
2 packets captured
1: 14:07:21.346951 192.168.100.2.57225 > 172.22.1.161.53: udp 36
2: 14:07:21.352124 172.22.1.161.53 > 192.168.100.2.57225: udp 93
2 packets shown
```

4. (Opcional) Copie las capturas a un servidor TFTP en formato PCAP para su análisis en otra aplicación.Las aplicaciones que pueden analizar el formato PCAP pueden mostrar detalles adicionales como el nombre y la dirección IP en los registros DNS A.

```
ciscoasa#copy /pcap capture:DNSINSIDE tftp
...
ciscoasa#copy /pcap capture:DNSOUTSIDE tftp
```

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

No se realiza la reescritura de DNS

Asegúrese de que la inspección de DNS está configurada en el dispositivo de seguridad.

Error al crear la traducción

Si no se puede crear una conexión entre el cliente y el servidor WWW, puede deberse a una configuración incorrecta de NAT. Verifique los registros del dispositivo de seguridad en busca de mensajes que indiquen que un protocolo no pudo crear una traducción a través del dispositivo de seguridad. Si aparecen tales mensajes, verifique que NAT se haya configurado para el tráfico deseado y que ninguna dirección sea incorrecta.

```
%ASA-3-305006: portmap translation creation failed for tcp src
inside:192.168.100.2/11000 dst inside:192.168.100.10/80
```

Borre las entradas de xlate y luego quite y vuelva a aplicar las sentencias NAT para resolver este error.

Información Relacionada

- Guía de configuración de Cisco ASA 5500-x
- Referencias de Comandos de Cisco ASA 5500-x Series
- Avisos de campo de productos de seguridad
- Solicitud de comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems