Configurar o DNS Doctoring para Três Interfaces NAT no ASA versão 9.x

Contents

Introduction

Este documento fornece uma configuração de exemplo para executar o documento de DNS (Domain Name System) no ASA 5500-X Series Adaptive Security Appliance (ASA) que usa instruções de NAT (Object/Auto Network Address Translation). O acoplamento DNS permite que o Security Appliance regrave registros A de DNS.

A regravação de DNS executa duas funções:

- Converte um endereço público (o endereço roteável ou mapeado) em uma resposta DNS para um endereço privado (o endereço real) quando o cliente DNS está em uma interface

privada.
- Converte um endereço privado em um endereço público quando o cliente DNS está na interface pública.

Prerequisites

Requirements

A Cisco afirma que a inspeção de DNS deve ser habilitada para executar o doping de DNS no Security Appliance. A inspeção de DNS está ativada por padrão.

Quando a inspeção de DNS está habilitada, o Security Appliance executa estas tarefas:

- Converte o registro DNS com base na configuração concluída com o uso de comandos de NAT de objeto/automático (regravação de DNS). A tradução aplica-se somente ao registro A na resposta DNS. Portanto, as pesquisas reversas, que solicitam o registro de Ponteiro (PTR), não são afetadas pela regravação de DNS. Na versão ASA 9.0(1) e posterior, a conversão do registro PTR de DNS para pesquisas de DNS reverso ao usar NAT IPv4, NAT IPv6 e NAT64 com inspeção de DNS habilitada para a regra de NAT.**Note**: A regravação de DNS não é compatível com a Conversão de Endereço de Porta (PAT - Port Address Translation) estática porque várias regras de PAT são aplicáveis para cada registro A e a regra de PAT a ser usada é ambígua.
- Aplica o comprimento máximo da mensagem DNS (o padrão é 512 bytes e o comprimento máximo é 65535 bytes). A remontagem é executada conforme necessário para verificar se o comprimento do pacote é menor que o comprimento máximo configurado. O pacote será descartado se exceder o comprimento máximo.**Note**: Se você inserir o comando **inspect dns** sem a opção de comprimento máximo, o tamanho do pacote DNS não será verificado.
- Aplica um comprimento de nome de domínio de 255 bytes e um comprimento de rótulo de 63 bytes.
- Verifica a integridade do nome de domínio referido pelo ponteiro se houver ponteiros de compressão na mensagem DNS.
- Verifica se existe um loop de ponteiro de compressão.

Componentes Utilizados

As informações neste documento são baseadas no ASA 5500-X Series Security Appliance, versão 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.

Produtos Relacionados

Essa configuração também pode ser usada com o Cisco ASA 5500 Series Security Appliance, versão 8.4 ou posterior.

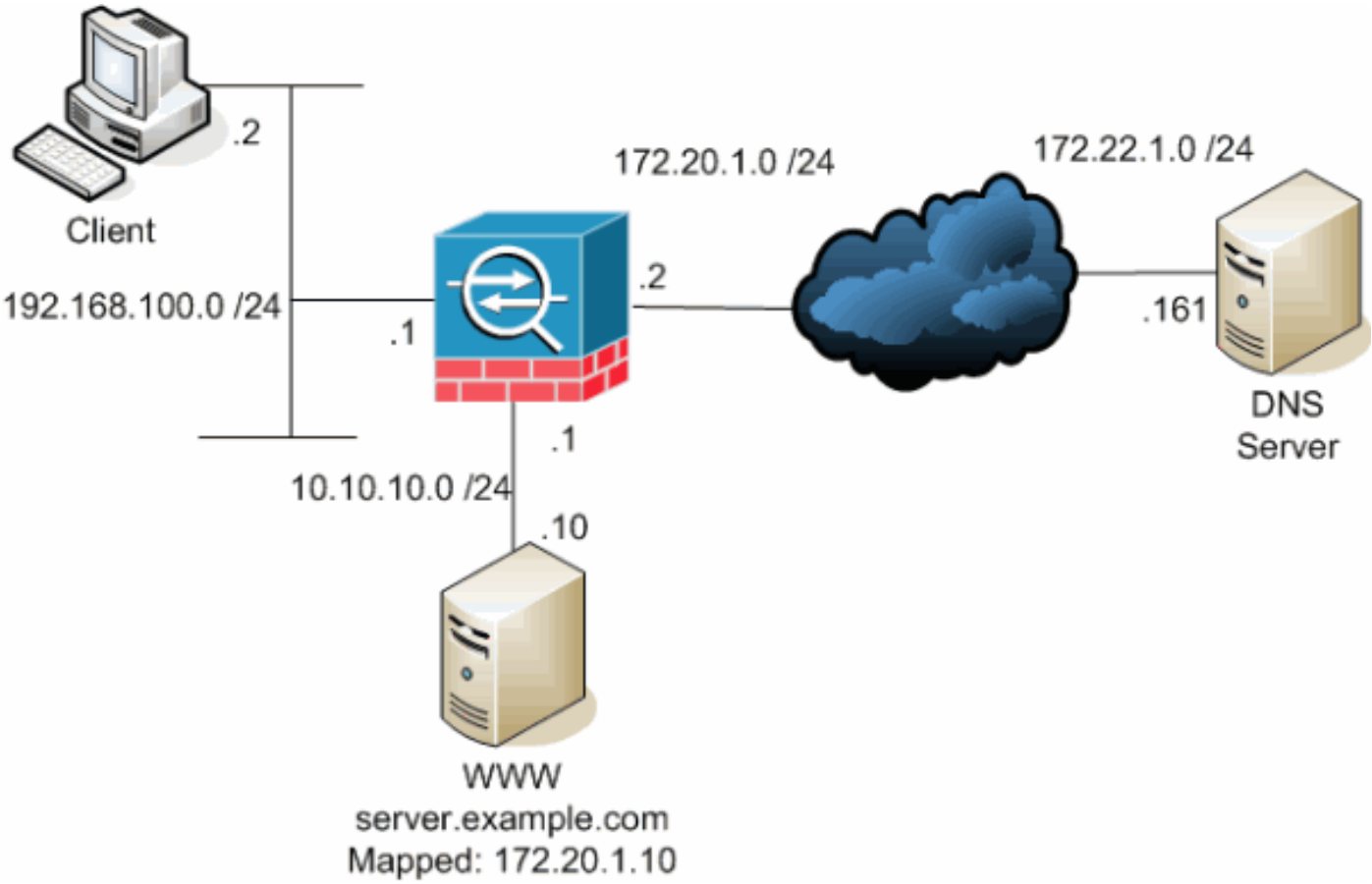
Note: A configuração do ASDM é aplicável somente à versão 7.x.

Informações de Apoio

Em uma troca DNS típica, um cliente envia um URL ou nome de host a um servidor DNS para determinar o endereço IP desse host. O servidor DNS recebe a solicitação, procura o mapeamento de nome para endereço IP para esse host e, em seguida, fornece o registro A com o endereço IP para o cliente. Embora esse procedimento funcione bem em muitas situações, podem ocorrer problemas. Esses problemas podem ocorrer quando o cliente e o host que o cliente tenta acessar estão na mesma rede privada atrás do NAT, mas o servidor DNS usado pelo cliente está em outra rede pública.

Cenário: Três interfaces NAT - Interno, Externo, DMZ

Topologia



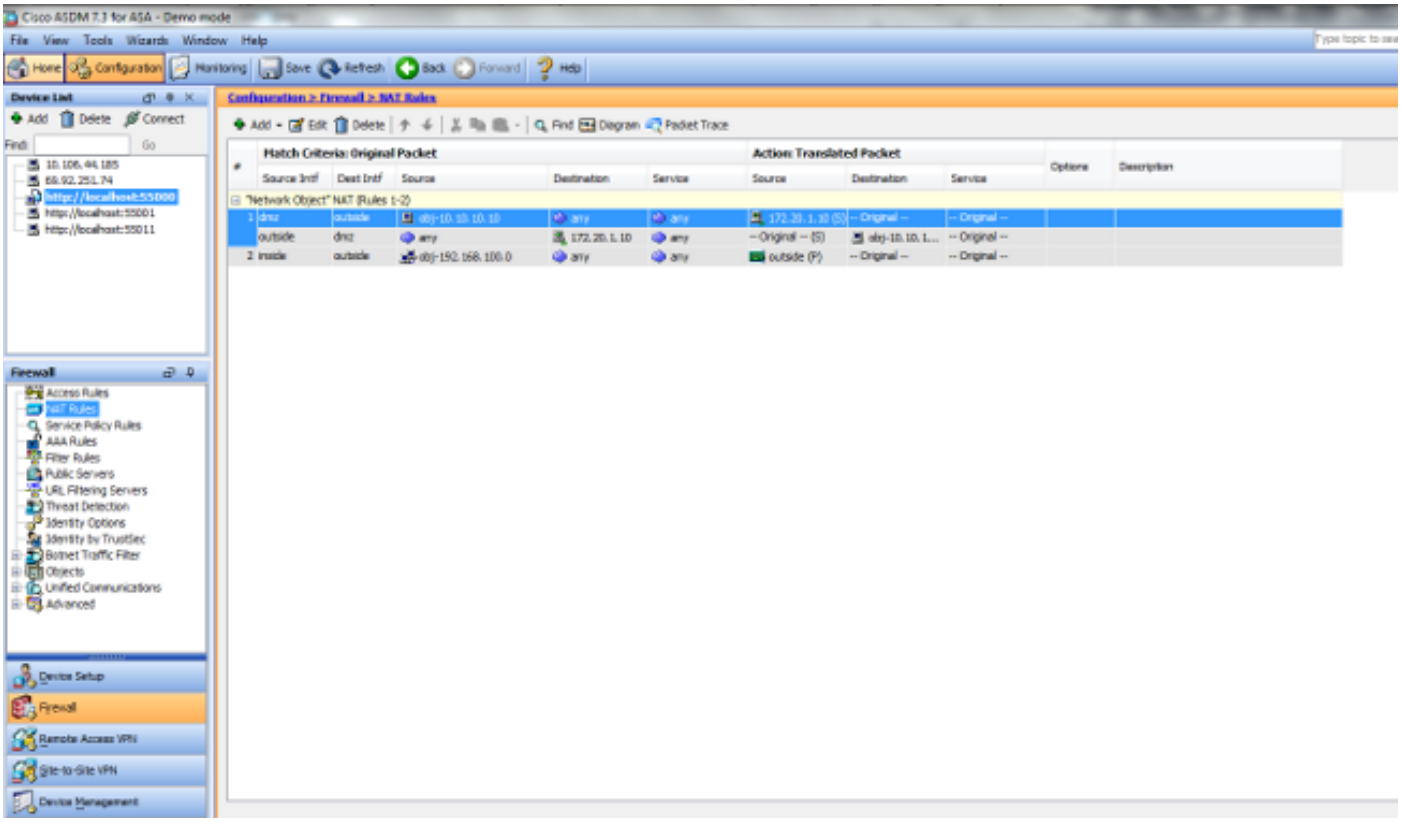
Este diagrama é um exemplo dessa situação. Nesse caso, o cliente em 192.168.100.2 deseja usar a URL **server.example.com** para acessar o servidor WWW em 10.10.10.10. Os serviços DNS para o cliente são fornecidos pelo servidor DNS externo em 172.22.1.161. Como o servidor DNS está localizado em outra rede pública, ele não sabe o endereço IP privado do servidor WWW. Em vez disso, ele conhece o endereço mapeado do servidor WWW 172.20.1.10. Assim, o servidor DNS contém o mapeamento de endereço IP para nome de **server.example.com** para **172.20.1.10**.

Problema: O cliente não pode acessar o servidor WWW

Sem o encaixe DNS ou outra solução habilitada nessa situação, se o cliente enviar uma solicitação DNS para o endereço IP de **server.example.com**, ele não poderá acessar o servidor WWW. Isso ocorre porque o cliente recebe um registro A que contém o endereço público mapeado de 172.20.1.10 para o servidor WWW. Quando o cliente tenta acessar esse endereço IP, o Security Appliance descarta os pacotes porque não permite o redirecionamento de pacotes na mesma interface. Aqui está a aparência da parte NAT da configuração quando o encaixe DNS não está ativado:

```
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.
```

Essa é a aparência da configuração no ASDM quando o acoplamento de DNS não está habilitado:



Aqui está uma captura de pacotes dos eventos quando o encaixe de DNS não está ativado:

1. O cliente envia a 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. O PAT é executado na consulta DNS pelo ASA e a consulta é encaminhada. Observe que o endereço de origem do pacote foi alterado para a interface externa do 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. O servidor DNS responde com o endereço mapeado do 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. O ASA desfaz a tradução do endereço de destino da resposta DNS e encaminha o pacote ao cliente. Observe que sem o encaixe DNS habilitado, o **Addr** na resposta ainda é o endereço mapeado do 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. Neste ponto, o cliente tenta acessar o servidor WWW em 172.20.1.10. O ASA cria uma entrada de conexão para esta comunicação. No entanto, como não permite que o tráfego flua de dentro para fora para DMZ, a conexão expira. Os registros do ASA mostram o seguinte:

```
%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
```

Solução: Palavra-chave "dns"

Documentação de DNS com a palavra-chave "dns"

O acoplamento DNS com a palavra-chave **dns** dá ao Security Appliance a capacidade de interceptar e regravar o conteúdo das respostas do servidor DNS ao cliente. Quando configurado corretamente, o Security Appliance pode alterar o registro A para permitir que o cliente em um cenário como discutido no " Problema: O cliente não pode acessar a seção WWW Server" para conectar. Nessa situação com o encaixe DNS habilitado, o Security Appliance regrava o registro A para direcionar o cliente para 10.10.10.10, em vez de 172.20.1.10. O encaixe de DNS é ativado quando você adiciona a palavra-chave **dns** a uma instrução NAT estática (Versão 8.2 e anterior) ou à instrução object/auto NAT (Versão 8.3 e posterior) .

Versão 8.2 e anterior

Esta é a configuração final do ASA para executar o acoplamento de DNS com a palavra-chave **dns** e três interfaces NAT para as versões 8.2 e 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
```

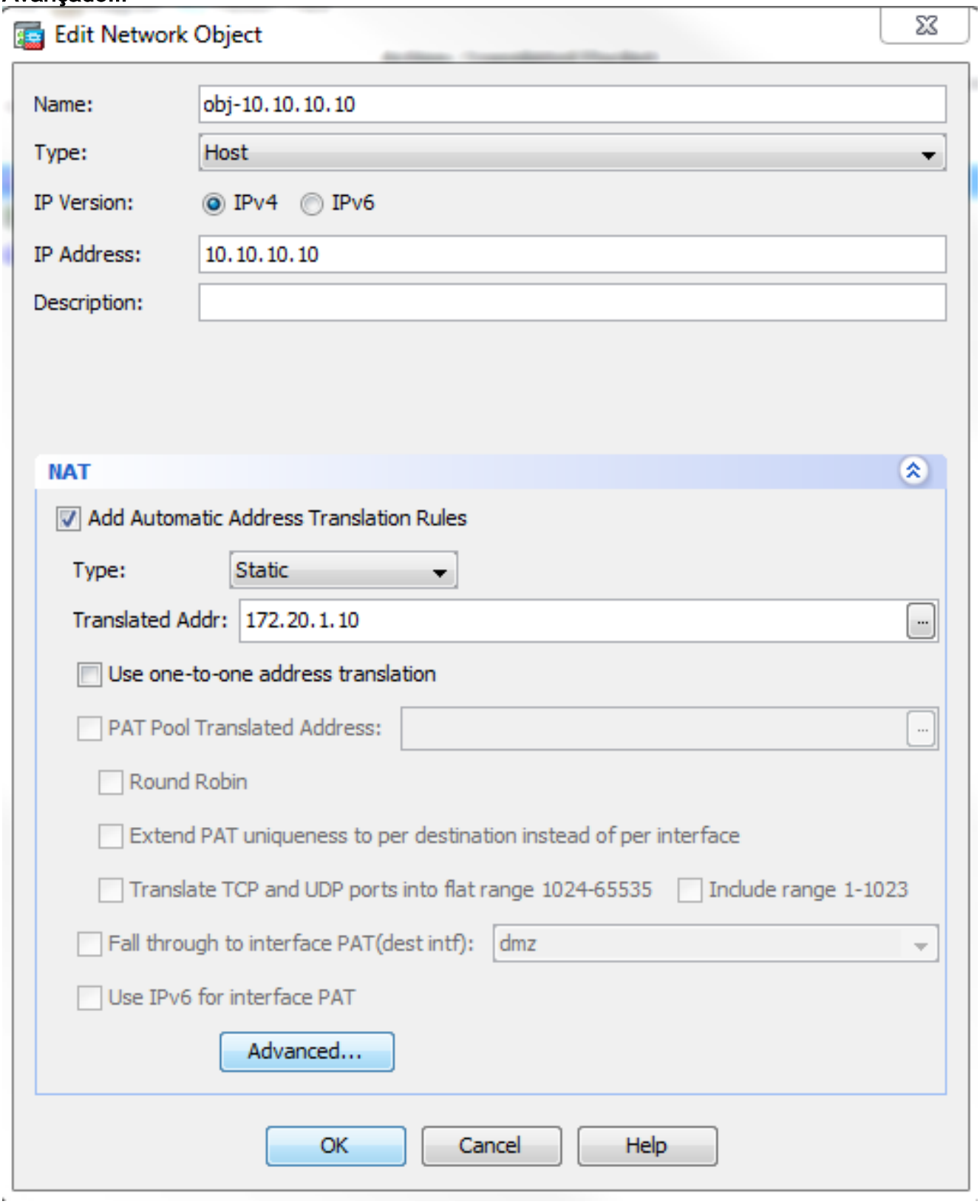
Versão 8.3 e posterior

```
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.
```

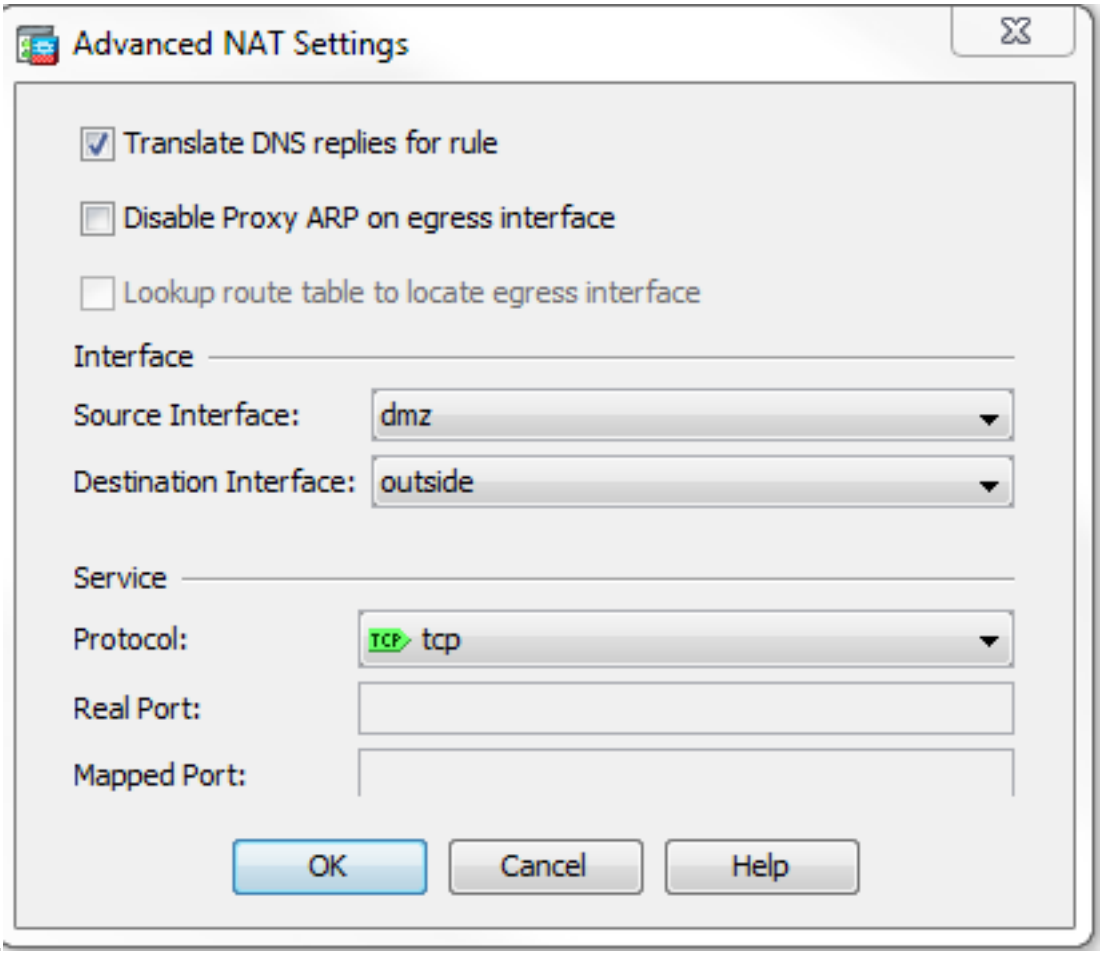
Configuração do ASDM

Conclua estes passos para configurar o encaixe DNS no ASDM:

1. Escolha **Configuration > NAT Rules** e escolha a regra Object/Auto a ser modificada. Clique em **Editar**.
2. Clique em **Avançado...**



3. Marque a caixa de seleção **Traduzir respostas de DNS para**



regra.

4. Clique em **OK** para sair da janela Opções de NAT.
5. Clique em **OK** para sair da janela Editar objeto/regra de NAT automática.
6. Clique em **Apply** para enviar sua configuração para o Security Appliance.

Verificar

Aqui está uma captura de pacotes dos eventos quando o encaixe DNS está ativado:

1. O cliente envia a 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. O PAT é executado na consulta DNS pelo ASA e a consulta é encaminhada. Observe que o endereço de origem do pacote foi alterado para a interface externa do 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. O servidor DNS responde com o endereço mapeado do 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. O ASA desfaz a tradução do endereço de destino da resposta DNS e encaminha o pacote ao cliente. Observe que com o encaixe DNS habilitado, o **Addr** na resposta é reescrito para ser o endereço real do 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. Neste ponto, o cliente tenta acessar o servidor WWW em 10.10.10.10. A conexão foi bem-sucedida.

Configuração final com a palavra-chave "dns"

Esta é a configuração final do ASA para executar o acoplamento de DNS com a palavra-chave **dns** e três 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
```

Solução alternativa: NAT de destino

O NAT de destino pode fornecer uma alternativa para o doctoring DNS. O uso do NAT de destino nessa situação exige que uma conversão de objeto estático/NAT automático seja criada entre o endereço público do servidor WWW no endereço interno e real no DMZ. O NAT de destino não altera o conteúdo do registro A DNS que é retornado do servidor DNS para o cliente. Em vez disso, quando você usa o NAT de destino em um cenário como discutido neste documento, o cliente pode usar o endereço IP público **172.20.1.10** retornado pelo servidor DNS para se conectar ao servidor WW. A tradução automática/objeto estático permite que o Security Appliance

converta o endereço de destino de 172.20.1.10 para 10.10.10.10. Aqui está a parte relevante da configuração quando o NAT de destino é usado:

```
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
```

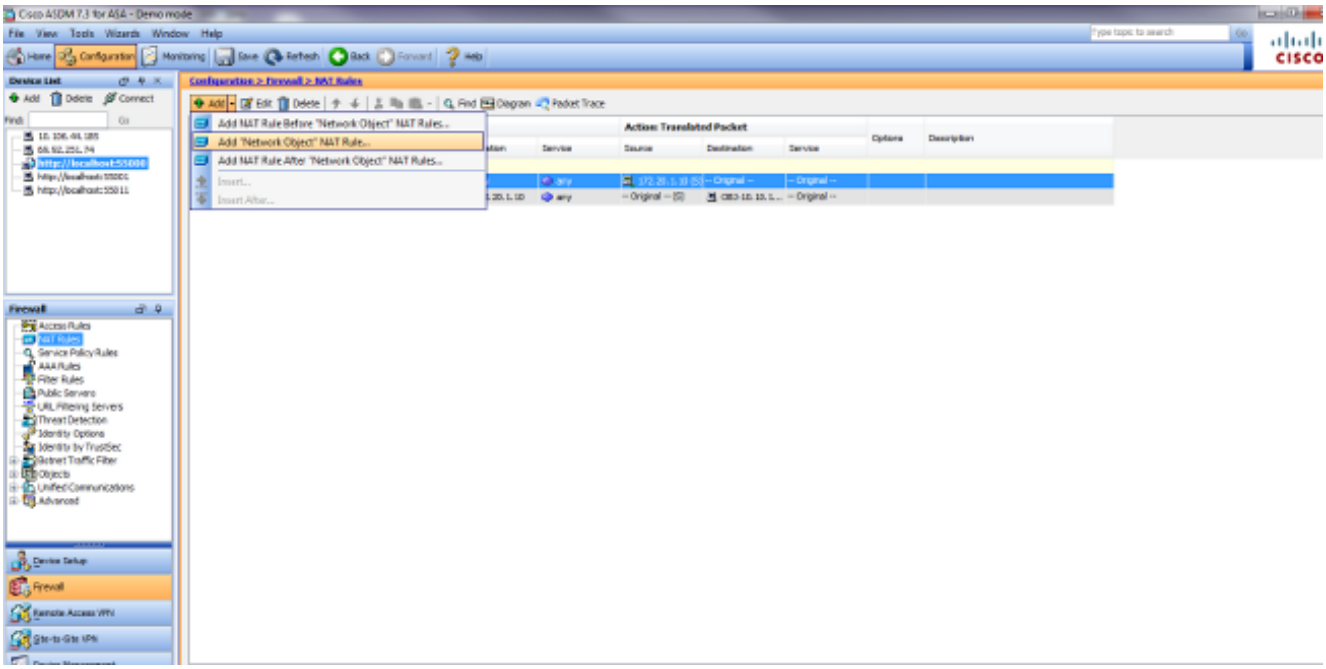
NAT de destino alcançado com declaração de NAT manual/duas vezes

```
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
```

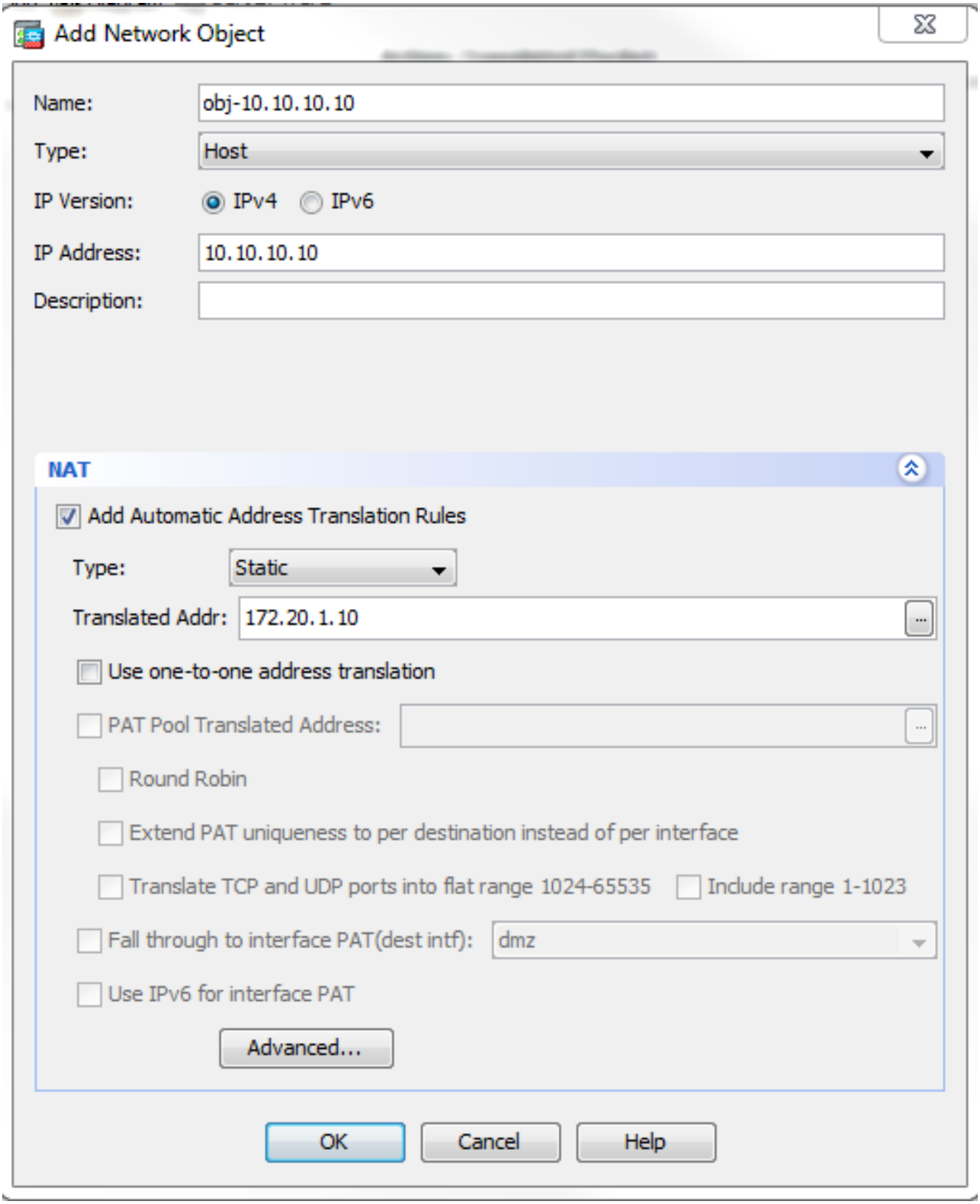
```
!--- Output suppressed.
```

Conclua estes passos para configurar o NAT de destino no ASDM:

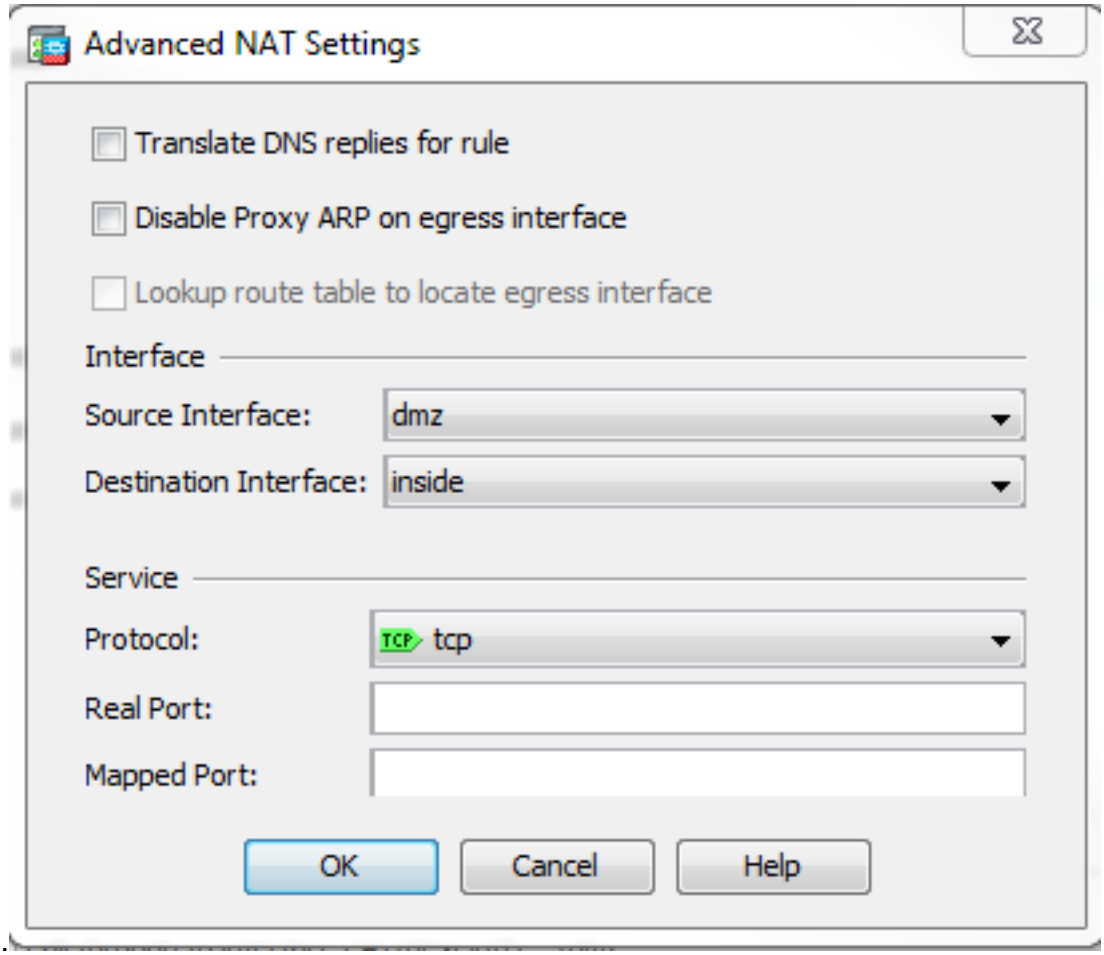
1. Escolha **Configuration > NAT Rules** e escolha **Add > Add "Network Object" NAT Rule...**.



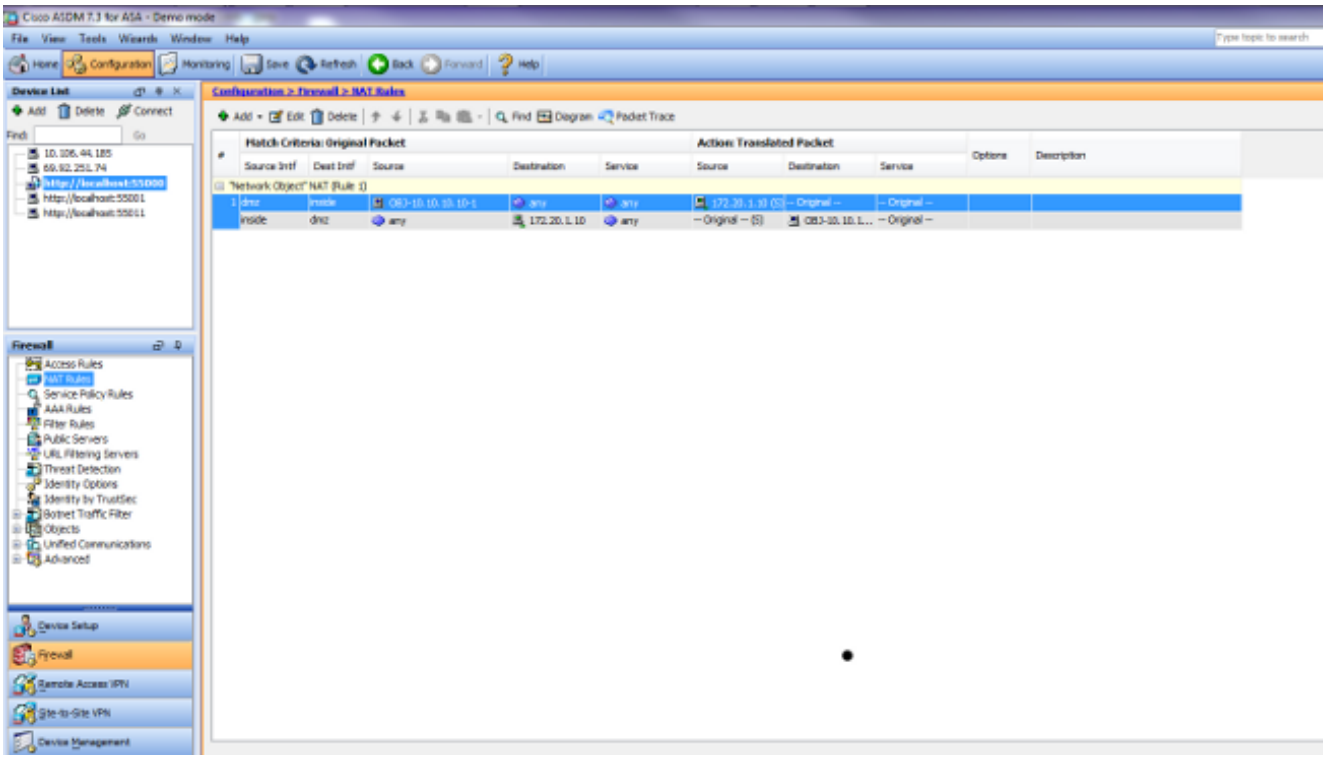
2. Preencha a configuração para a nova tradução estática. No campo Nome, insira **obj-10.10.10.10**.No campo Endereço IP, insira o endereço IP do servidor WWW.Na lista suspensa Tipo, escolha **Estático**.No campo Endereço traduzido, insira o endereço e a interface para os quais deseja mapear o servidor WWW.Clique em **Advanced** (Avançado).



Na lista suspensa Interface de origem, escolha **dmz**.Na lista suspensa Interface de destino, escolha **dentro**.Nesse caso, a interface interna é escolhida para permitir que os hosts na interface interna acessem o servidor WWW através do endereço mapeado



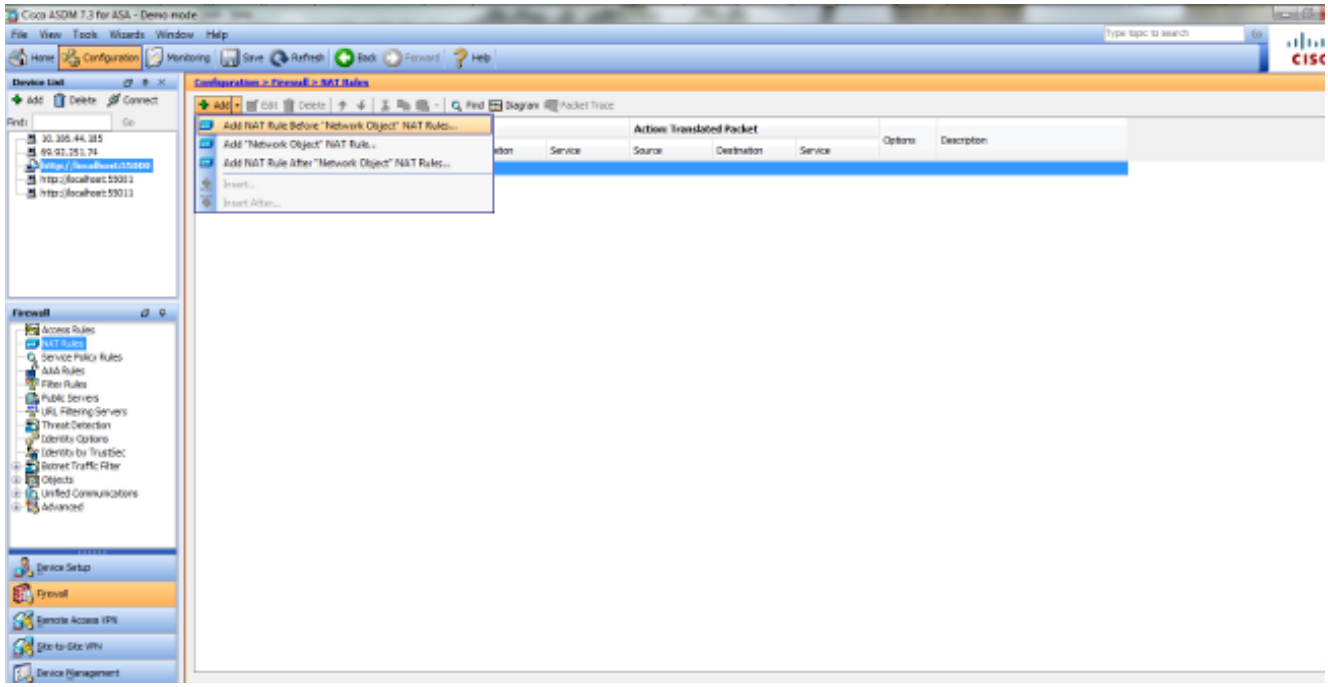
172.20.1.10.



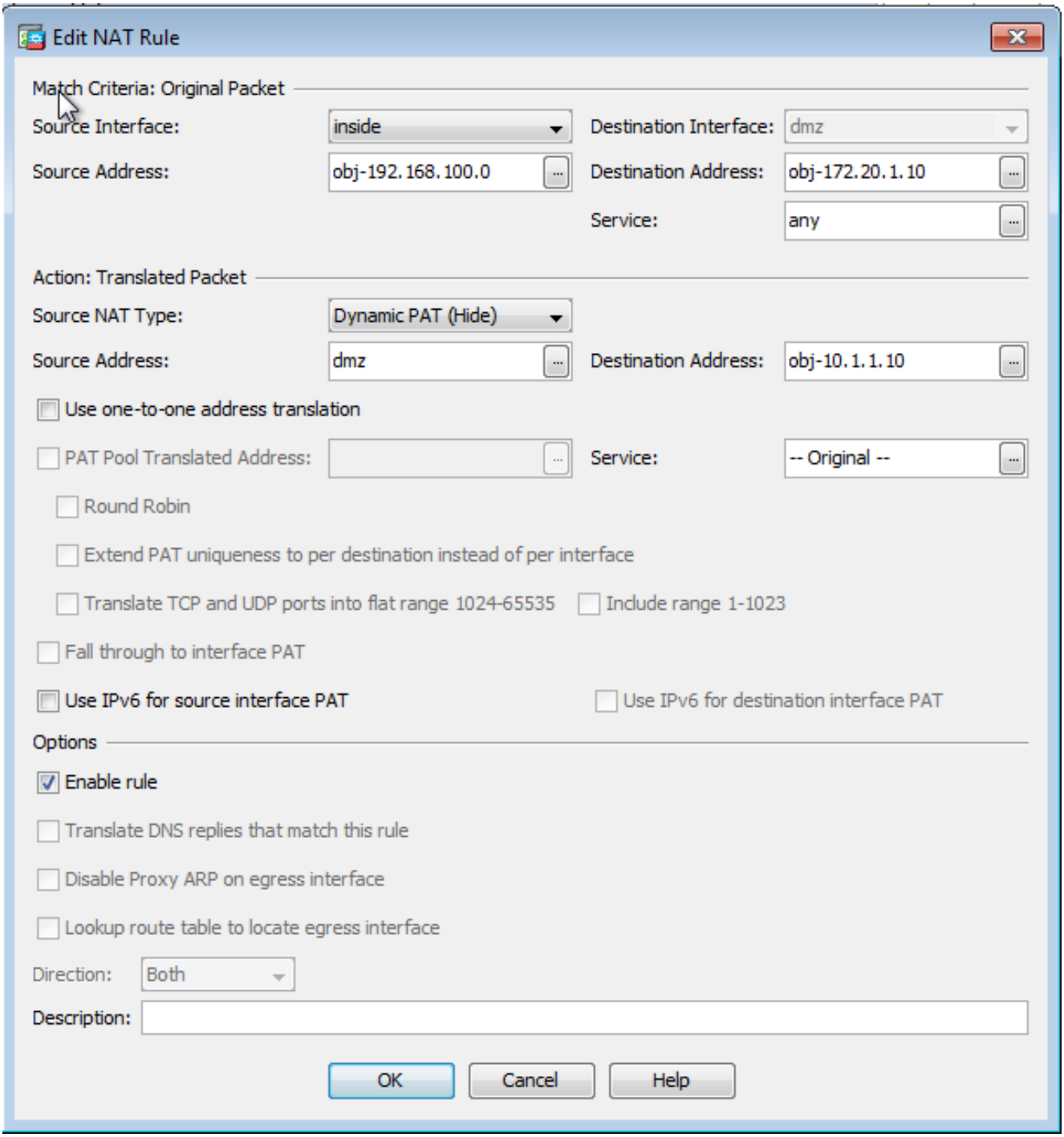
Clique em **OK** para sair da janela Add Object/Auto NAT Rule.Clique em **Apply** para enviar a configuração para o Security Appliance.

Método alternativo com NAT manual/duas vezes e ASDM

1. Escolha **Configuration > NAT Rules** e escolha **Add > Add Nat rule antes de "Network Object" NAT Rule...**.



2. Preencha a configuração para a tradução Manual/Duas Vezes Nat. Na lista suspensa Interface de origem, escolha **dentro**.Na lista suspensa Interface de destino, escolha **dmz**.No campo Endereço de origem, insira o objeto de rede interno (obj-192.168.100.0).No campo Endereço de destino, insira o tObjeto IP do servidor DMZ traduzido (172.20.1.10).Na lista suspensa Tipo de NAT de origem, escolha **PAT dinâmico (Ocultar)**.No Endereço de Origem [Ação: Translated Packet section], insira **dmz**.No destino Endereço [Ação: Seção Pacote traduzido] campo, insira o objeto IP real do servidor DMZ (obj-10.10.10.10).



3. Clique em **OK** para sair da janela Add Manual/Twice NAT Rule.
4. Clique em **Apply** para enviar a configuração para o Security Appliance.

Esta é a sequência de eventos que ocorrem quando o NAT de destino é configurado. Suponha que o cliente já consultou o servidor DNS e recebeu uma resposta de **172.20.1.10** para o endereço do servidor WWW:

1. O cliente tenta entrar em contato com o servidor WWW em 172.20.1.10.
   ```
   %ASA-7-609001: Built local-host inside:192.168.100.2
   ```
2. O Security Appliance vê a solicitação e reconhece que o servidor WWW é 10.10.10.10.
   ```
   %ASA-7-609001: Built local-host dmz:10.10.10.10
   ```
3. O Security Appliance cria uma conexão TCP entre o cliente e o servidor WWW. Observe os endereços mapeados de cada host entre parênteses.
   ```
   %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. O comando **show xlate** no Security Appliance verifica se o tráfego do cliente é convertido através do Security Appliance. Nesse caso, a primeira tradução estática está em 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. O comando **show conn** no Security Appliance verifica se a conexão foi bem-sucedida entre o cliente e o servidor WWW através do Security Appliance. Observe o endereço real do servidor WWW entre parênteses.

```
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
```

Configuração final com NAT de destino

Essa é a configuração final do ASA para executar o acoplamento de DNS com NAT de destino e três 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

Conclua estes passos para habilitar a inspeção de DNS (se ela tiver sido desabilitada anteriormente). Neste exemplo, a inspeção de DNS é adicionada à política de inspeção global padrão, que é aplicada globalmente por um comando **service-policy** como se o ASA começasse com uma configuração padrão.

1. Crie um mapa de política de inspeção para DNS.
   ```
   ciscoasa(config)#policy-map type inspect dns MY_DNS_INSPECT_MAP
   ```
2. No modo de configuração do mapa de política, insira o modo de configuração do parâmetro para especificar parâmetros para o mecanismo de inspeção.
   ```
   ciscoasa(config-pmap)#parameters
   ```
3. No modo de configuração de parâmetro de mapa de política, especifique o comprimento máximo da mensagem para as mensagens DNS como 512.
   ```
   ciscoasa(config-pmap-p)#message-length maximum 512
   ```
4. Saia do modo de configuração de parâmetro policy-map e do modo de configuração policy-map.
   ```
   ciscoasa(config-pmap-p)#exit
   ciscoasa(config-pmap)#exit
   ```
5. Confirme se o mapa da política de inspeção foi criado conforme desejado.
   ```
   ciscoasa(config)#show run policy-map type inspect dns
   !
   policy-map type inspect dns MY_DNS_INSPECT_MAP
   parameters
   message-length maximum 512
   !
   ```
6. Entre no modo de configuração do mapa de política para **global_policy**.
   ```
   ciscoasa(config)#policy-map global_policy
   ciscoasa(config-pmap)#
   ```

7. No modo de configuração de mapa de política, especifique o mapa de classe padrão da camada 3/4, **inspection_default**.
```
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#
```
8. No modo de configuração de classe de mapa de política, use o mapa de política de inspeção criado nas etapas 1 a 3 para especificar que o DNS deve ser inspecionado.
```
ciscoasa(config-pmap-c)#inspect dns MY_DNS_INSPECT_MAP
```
9. Saia do modo de configuração de classe de mapa de política e do modo de configuração de mapa de política.
```
ciscoasa(config-pmap-c)#exit
ciscoasa(config-pmap)#exit
```
10. Verifique se o mapa de políticas **global_policy** está configurado conforme desejado.
```
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 se global_policy é aplicada globalmente por uma service-policy.
```
ciscoasa(config)#show run service-policy
service-policy global_policy global
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Capturar tráfego DNS

Um método para verificar se o Security Appliance regrava registros DNS corretamente é capturar os pacotes em questão, conforme discutido no exemplo anterior. Conclua estes passos para capturar o tráfego no ASA:

1. Crie uma lista de acesso para cada instância de captura que deseja criar.A ACL deve especificar o tráfego que deseja capturar. Neste exemplo, duas ACLs foram criadas. A ACL para tráfego na interface externa:

```
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.
```

   A ACL para tráfego na interface 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. Crie a(s) instância(s) 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. Exibir as capturas.Aqui está o aspecto das capturas de exemplo após a passagem de algum tráfego 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 a(s) captura(s) para um servidor TFTP no formato PCAP para análise em outro aplicativo.Os aplicativos que podem analisar o formato PCAP podem mostrar detalhes adicionais, como o nome e o endereço IP nos registros DNS A.

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

Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

A regravação de DNS não é executada

Verifique se você tem a inspeção de DNS configurada no Security Appliance.

Falha na criação da tradução

Se não for possível criar uma conexão entre o cliente e o servidor WWW, isso pode ser devido a uma configuração incorreta de NAT. Verifique os registros do Security Appliance em busca de mensagens que indicam que um protocolo não conseguiu criar uma tradução através do Security Appliance. Se essas mensagens forem exibidas, verifique se o NAT foi configurado para o tráfego desejado e se nenhum endereço está incorreto.

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

Limpe as entradas xlate e remova e reaplique as instruções NAT para resolver esse erro.

Informações Relacionadas

- Guia de configuração do Cisco ASA 5500-x
- Referências de comandos do Cisco ASA 5500-x Series
- Avisos de campo do produto de segurança
- Solicitação de comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems