Configurar o DNS Doctoring para três relações NAT na liberação 9.x ASA

Índice

Introdução

Este documento fornece uma configuração de exemplo para executar o Domain Name System (DNS) medicando na ferramenta de segurança adaptável do 5500-X Series ASA (ASA) essa usos objeta/auto indicação do Network Address Translation (NAT). Medicar DNS permite que a ferramenta de segurança reescreva Um-registros DNS.

A reescrita DNS executa duas funções:

- Traduz um endereço público (o roteável ou o endereço traçado) em uma resposta DNS a um endereço privado (o endereço real) quando o cliente de DNS está em uma interface

confidencial.
- Traduz um endereço privado a um endereço público quando o cliente de DNS está na interface pública.

Pré-requisitos

Requisitos

Cisco indica que a inspeção DNS deve ser permitida a fim executar o DNS que medica na ferramenta de segurança. A inspeção DNS está ligada à revelia.

Quando a inspeção DNS é permitida, a ferramenta de segurança executa estas tarefas:

- Traduz o registro DNS baseado na configuração terminada com o uso do objeto/auto comandos nat (reescrita DNS). A tradução aplica-se somente ao Um-registro na resposta DNS. Consequentemente as consultas reversas, que pedem o registro do ponteiro (PTR), não são afetadas pela reescrita DNS. Na versão ASA 9.0(1) e mais atrasado, na tradução do registro PTR DNS para pesquisas de DNS reversas ao usar o IPv4 NAT, no IPv6 NAT, e no NAT64 com a inspeção DNS permitida para a regra NAT.Nota: A reescrita DNS não é compatível com tradução de endereço da porta estática (PANCADINHA) porque as regras múltiplas da PANCADINHA são aplicáveis para cada Um-registro, e a regra da PANCADINHA a usar-se é ambígua.
- Reforça o tamanho da mensagem do máximo DNS (o padrão é 512 bytes e o comprimento máximo é 65535 bytes). A remontagem é executada como necessário a fim verificar que o comprimento do pacote é menos do que o comprimento máximo configurado. O pacote é deixado cair se excede o comprimento máximo.Nota: Se você incorpora o comando **dns da inspeção** sem a opção do comprimento máximo, o tamanho de pacote de DNS não está verificado.
- Reforça um comprimento do Domain Name de 255 bytes e um comprimento da etiqueta de 63 bytes.
- Verifica a integridade do Domain Name referido pelo ponteiro se os ponteiros da compressão são encontrados na mensagem DNS.
- Verifica para ver se um laço do ponteiro da compressão existe.

Componentes Utilizados

A informação neste documento é baseada no 5500-X Series ferramenta de segurança ASA, versão 9.x.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Produtos Relacionados

Esta configuração pode igualmente ser usada com o 5500 Series ferramenta de segurança de Cisco ASA, versão 8.4 ou mais recente.

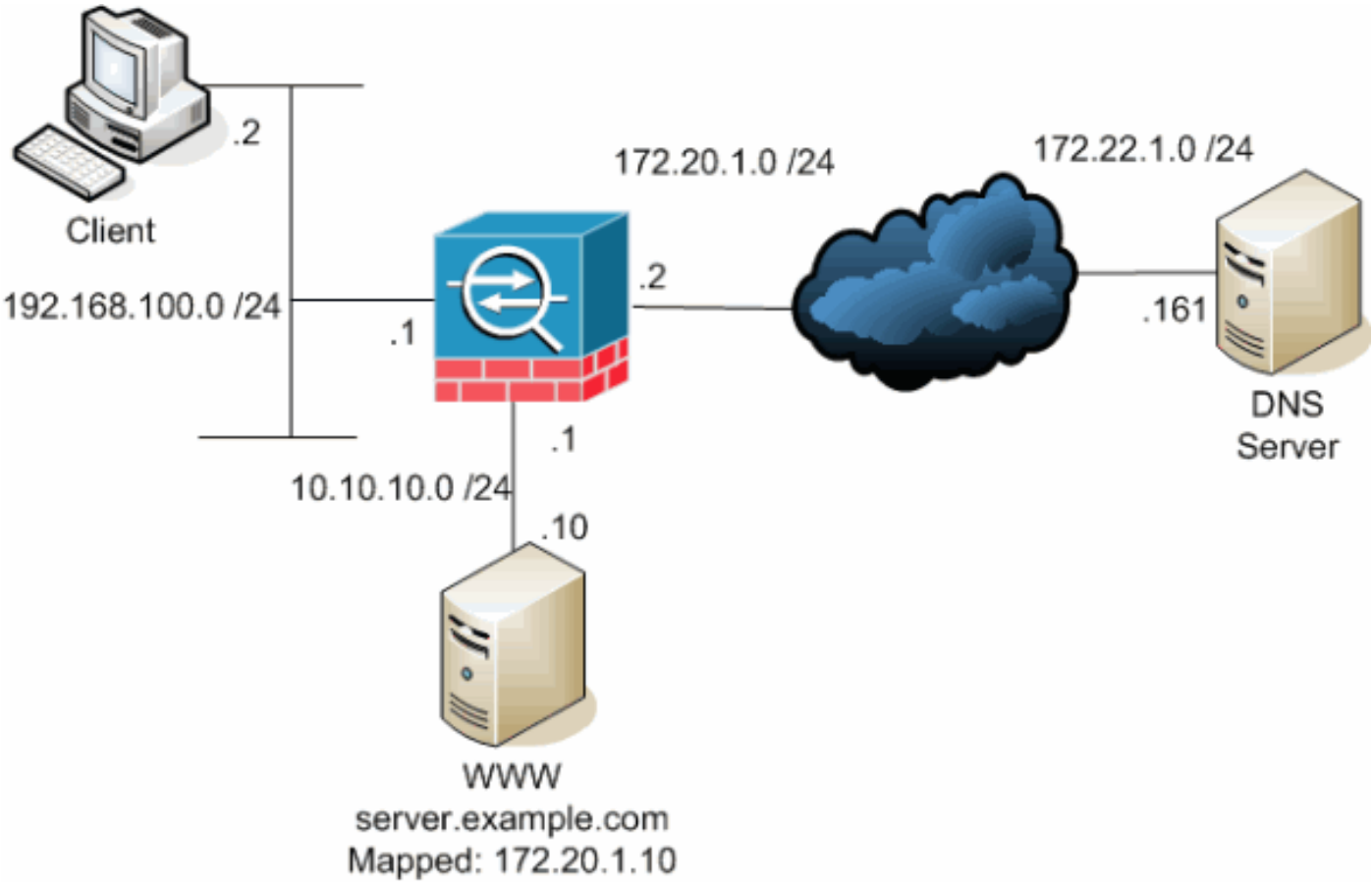
Nota: A configuração ASDM é aplicável à versão 7.x somente.

Informações de Apoio

Em uma troca típica DNS, um cliente envia uma URL ou um hostname a um servidor DNS a fim determinar o endereço IP de Um ou Mais Servidores Cisco ICM NT desse host. O servidor DNS recebe o pedido, olha acima o mapeamento do nome-à-IP-endereço para esse host, e fornece então o Um-registro o endereço IP de Um ou Mais Servidores Cisco ICM NT ao cliente. Quando este procedimento trabalhar bem em muitas situações, os problemas podem ocorrer. Estes problemas podem ocorrer quando o cliente e o host que o cliente tenta alcançar são ambos na mesma rede privada atrás do NAT, mas o servidor DNS usado pelo cliente está em uma outra rede pública.

Encenação: Três relações NAT - Dentro de, exterior, DMZ

Topologia



Este diagrama é um exemplo desta situação. Neste caso, o cliente em 192.168.100.2 quer usar **server.example.com** URL a fim alcançar o servidor WWW em 10.10.10.10. Os serviços DNS para o cliente são proporcionados pelo servidor DNS externo em 172.22.1.161. Porque o servidor DNS

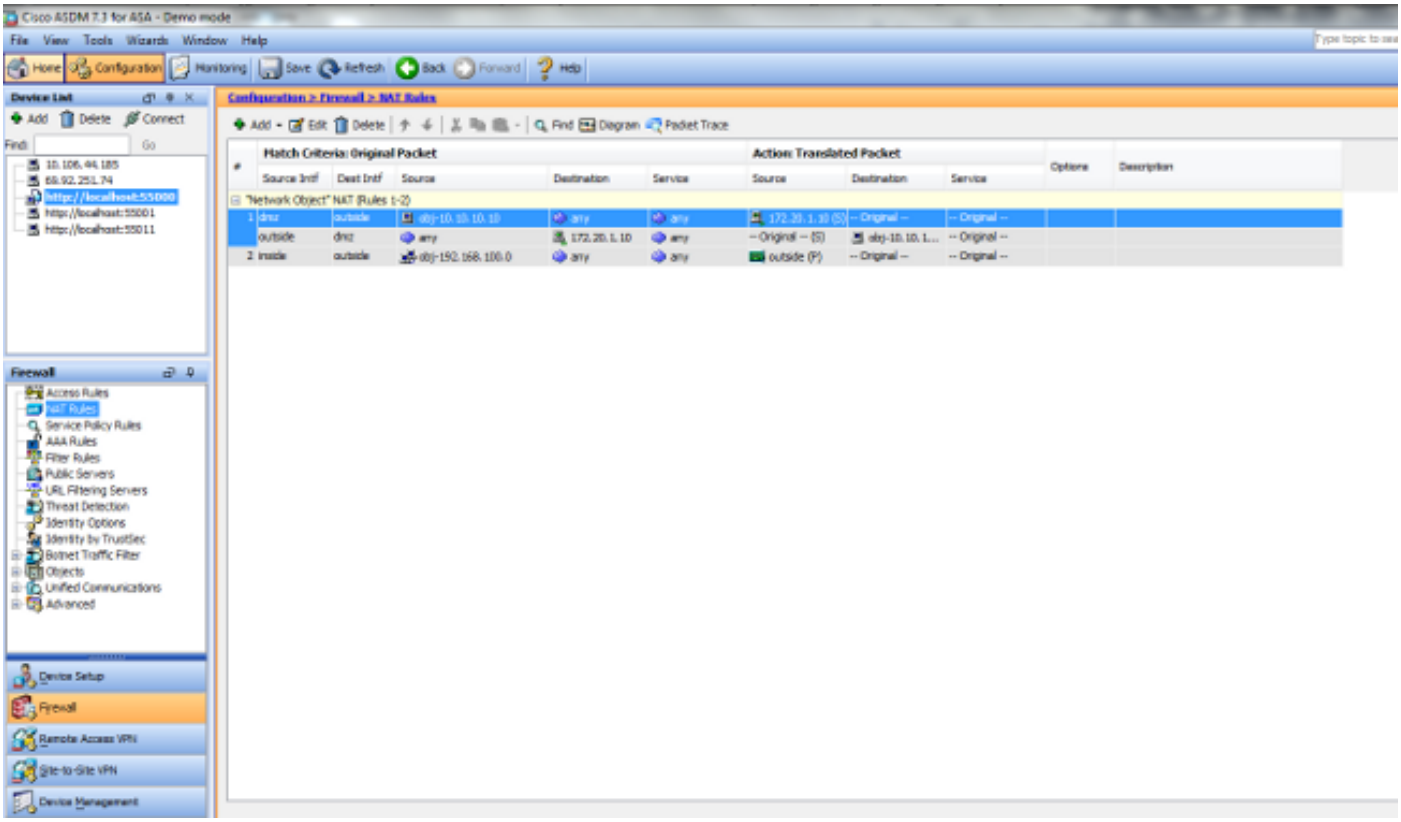
é ficado situado em uma outra rede pública, não conhece o endereço IP privado do servidor WWW. Em lugar de, conhece o endereço traçado servidor WWW de 172.20.1.10. Assim, o servidor DNS contém o mapeamento do IP-endereço-à-nome de **server.example.com a 172.20.1.10**.

Problema: O cliente não pode alcançar o servidor WWW

Sem medicar DNS ou uma outra solução permitido nesta situação, se o cliente envia um pedido DNS para o endereço IP de Um ou Mais Servidores Cisco ICM NT de **server.example.com**, é incapaz de alcançar o servidor WWW. Isto é porque o cliente recebe um Um-registro que contenha o endereço público traçado de 172.20.1.10 para o servidor WWW. Quando o cliente tenta alcançar este endereço IP de Um ou Mais Servidores Cisco ICM NT, a ferramenta de segurança deixa cair os pacotes porque não permite o redirecionamento de pacote na mesma relação. É aqui o que a parcela NAT da configuração olha como quando medicar DNS não é permitido:

```
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.
```

Este é o que a configuração olha como no ASDM quando medicar DNS não é permitido:



Está aqui uma captura de pacote de informação dos eventos quando medicar DNS não é permitido:

1. O cliente envia a pergunta 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. A PANCADINHA é executada na pergunta DNS pelo ASA e a pergunta é enviada. Note que o endereço de origem do pacote mudou à 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 traçado 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 desabotoa a tradução do endereço de destino da resposta de DNS e para a frente do pacote ao cliente. Note que sem medicar DNS permitido, o ADDR na resposta é ainda o endereço traçado 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 momento o cliente tenta alcançar o servidor WWW em 172.20.1.10. O ASA cria uma entrada de conexão para esta comunicação. Contudo, porque não permite que o tráfego flua do interior à parte externa ao DMZ, o tempo de conexão para fora. Os logs ASA mostram este:

```
%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”

DNS Doctoring com a palavra-chave “dns”

O DNS que medica com a palavra-chave **dns** dá à ferramenta de segurança a capacidade para interceptar e para reescrever os índices do servidor DNS responde ao cliente. Quando configurada corretamente, a ferramenta de segurança pode alterar o Um-registro a fim permitir o cliente em tal encenação como discutido no “problema: O cliente não pode alcançar seção do servidor WWW” para conectar. Nesta situação com medicar DNS permitido, a ferramenta de segurança reescreve o Um-registro para dirigir o cliente a 10.10.10.10 em vez de 172.20.1.10. Medicar DNS está permitido quando você adiciona a palavra-chave **dns a uma** indicação do NAT estático (versão 8.2 e anterior) ou ao objeto/auto declaração NAT (versão 8.3 e mais recente).

Versão 8.2 e anterior

Esta é a configuração final do ASA para executar o DNS que medica com a palavra-chave **dns** e as três relações NAT para versões 8.2 e anterior.

```
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
```

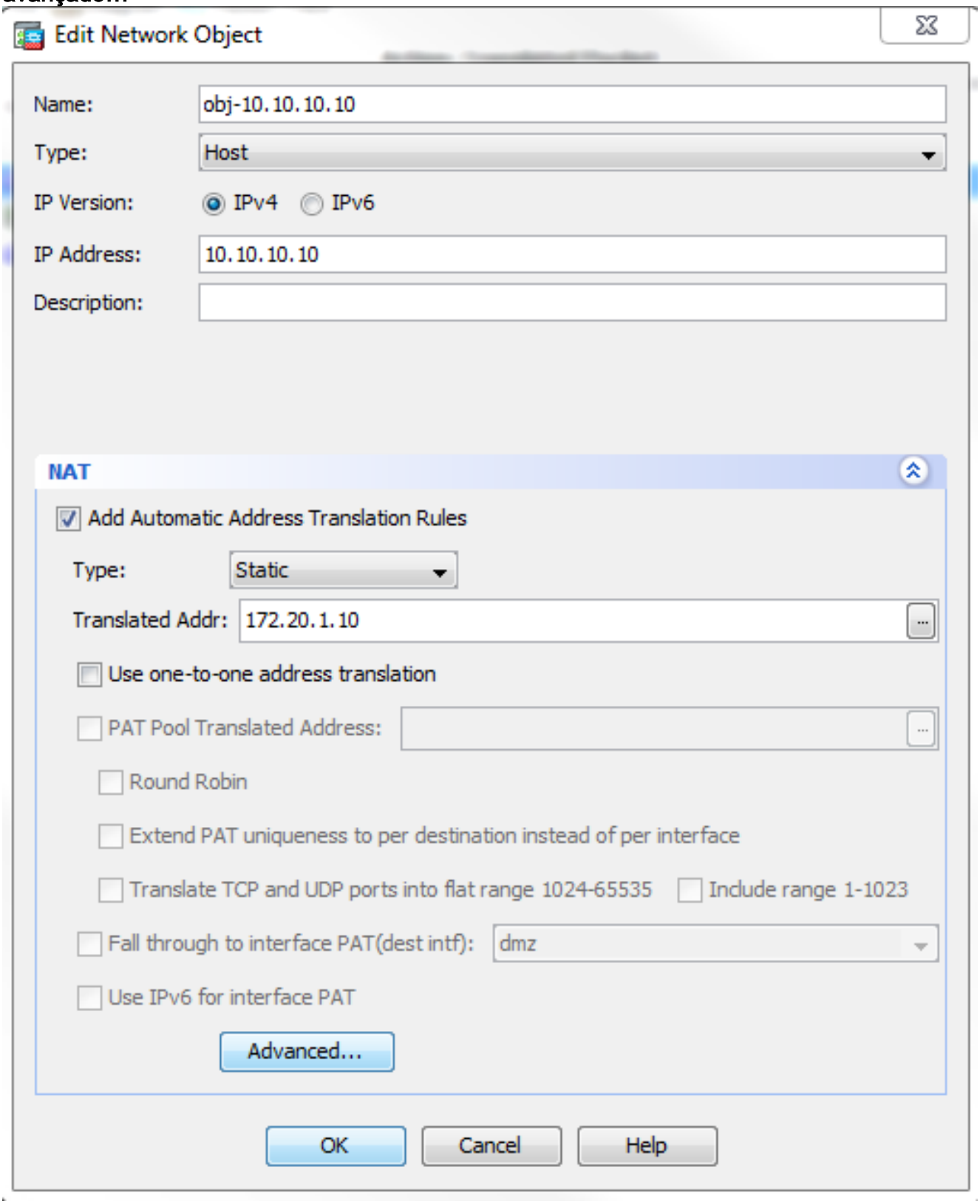
Versão 8.3 e mais recente

```
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.
```

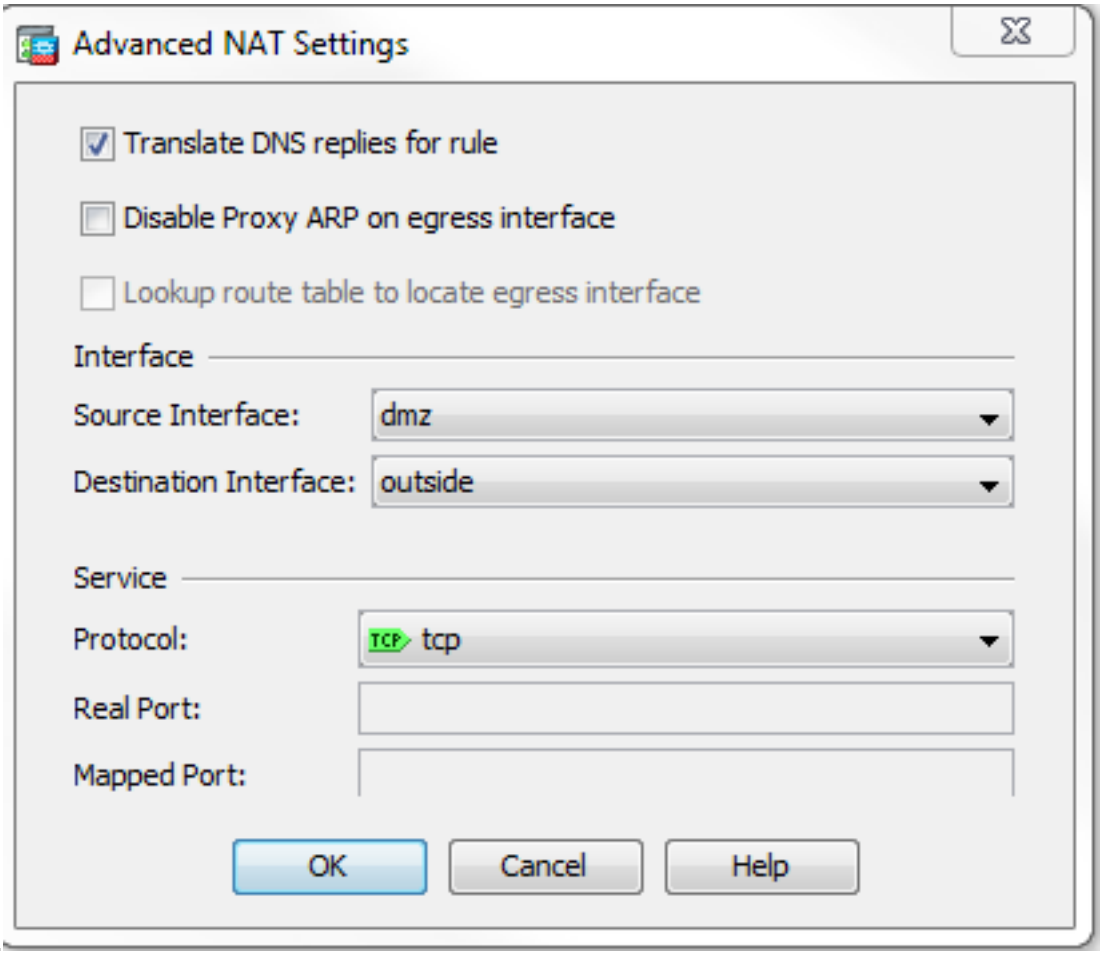
Configuração ASDM

Termine estas etapas a fim configurar o DNS que medica no ASDM:

1. Escolha a **configuração > as regras NAT** e escolha o objeto/auto regra a ser alterado. O clique **edita**.
2. Clique **avançado...**



3. Verifique as **respostas da tradução DNS para ver se há a** caixa de verificação de



regra.

4. Clique a **APROVAÇÃO** a fim deixar o indicador das opções NAT.
5. Clique a **APROVAÇÃO** a fim deixar o objeto da edição/auto indicador da regra NAT.
6. O clique **aplica-se** a fim enviar sua configuração à ferramenta de segurança.

Verificar

Está aqui uma captura de pacote de informação dos eventos quando medicar DNS é permitido:

1. O cliente envia a pergunta 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. A PANCADINHA é executada na pergunta DNS pelo ASA e a pergunta é enviada. Note que o endereço de origem do pacote mudou à 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 traçado 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 desabotoa a tradução do endereço de destino da resposta de DNS e para a frente do pacote ao cliente. Note que com medicar DNS permitido, o **ADDR na** resposta está 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 momento, o cliente tenta alcançar o servidor WWW em 10.10.10.10. A conexão sucede.

Configuração final com a palavra-chave “dns”

Esta é a configuração final do ASA para executar o DNS que medica com a palavra-chave **dns** e as três relações 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 a medicar DNS. O uso do NAT de destino exige nesta situação que um objeto estático/auto tradução NAT está criado entre o endereço público do servidor WWW no interior e o endereço real no DMZ. O NAT de destino não muda os índices do Um-registro DNS que é retornado do servidor DNS ao cliente. Em lugar de, quando você usa o NAT de destino em uma encenação tal como discutido neste documento, o cliente pode usar o endereço IP público **172.20.1.10** que é retornado pelo servidor DNS a fim conectar ao servidor WWW. O objeto estático/auto tradução permite que a ferramenta de segurança traduza o endereço de destino de **172.20.1.10 a 10.10.10.10**. Está aqui a porção relevante da configuração

quando o NAT de destino é usado:

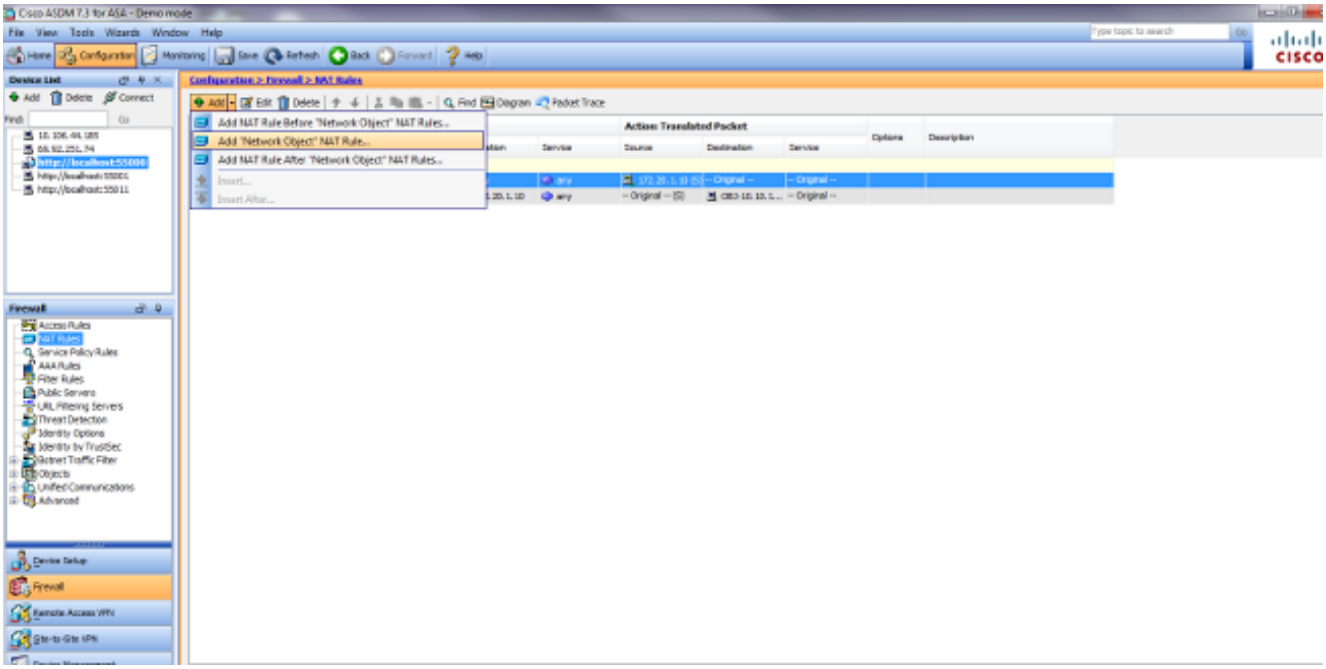
```
ASA Version 9.x
!
hostname ciscoasa

!--- 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 conseguido com manual/duas vezes declaração NAT

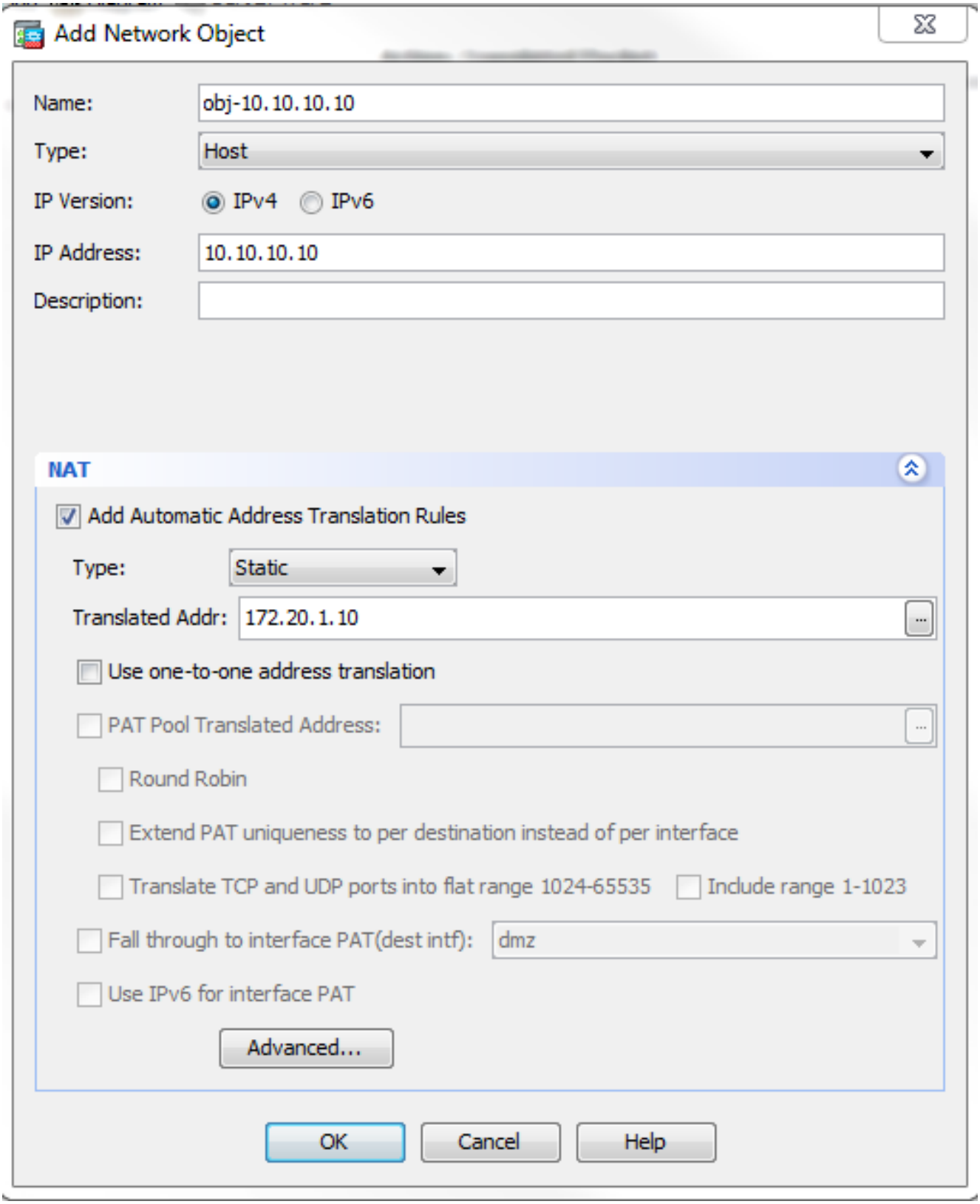
```
ASA Version 9.x
!
hostname ciscoasa

!--- 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.
```

Termine estas etapas a fim configurar o NAT de destino no ASDM:

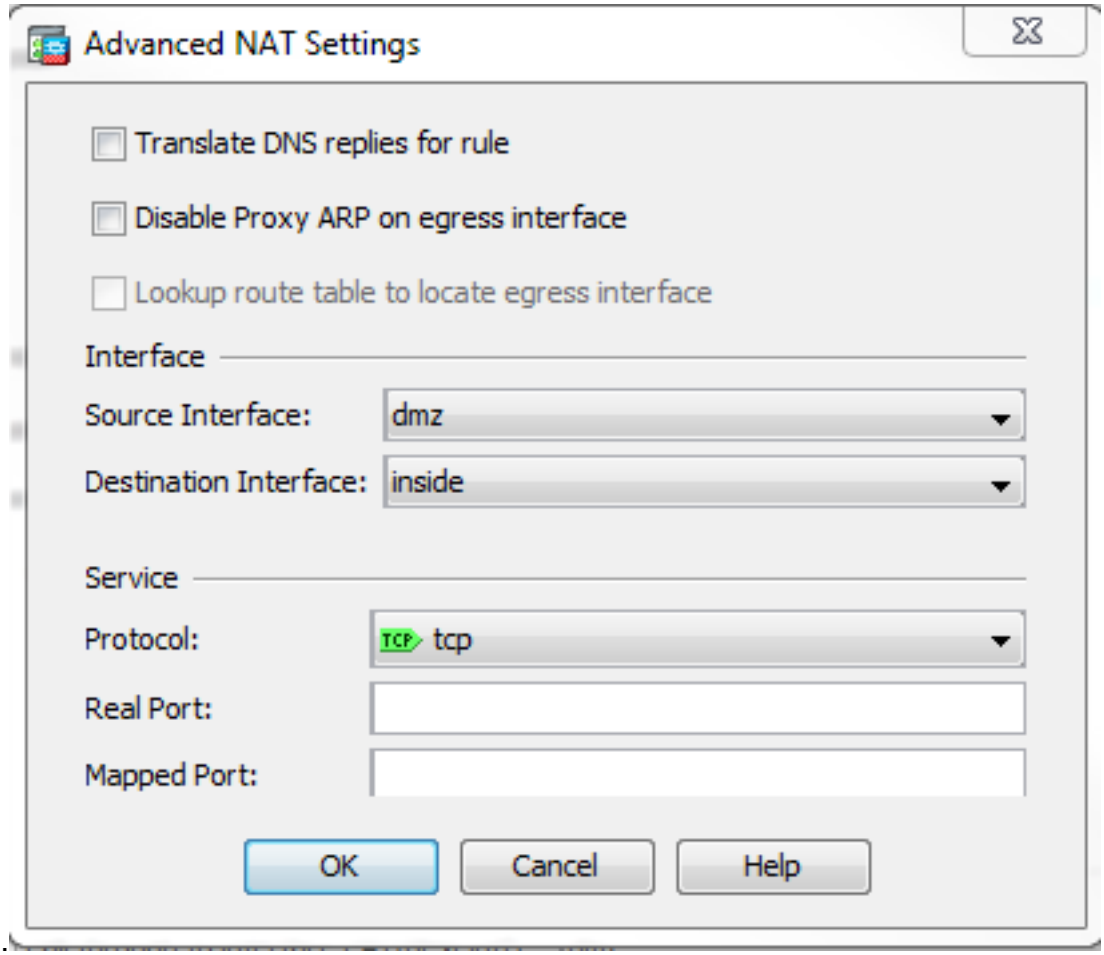
1. Escolha a **configuração > as regras NAT** e escolha-os **adicionam a regra NAT do "objeto de rede" do > Add….**



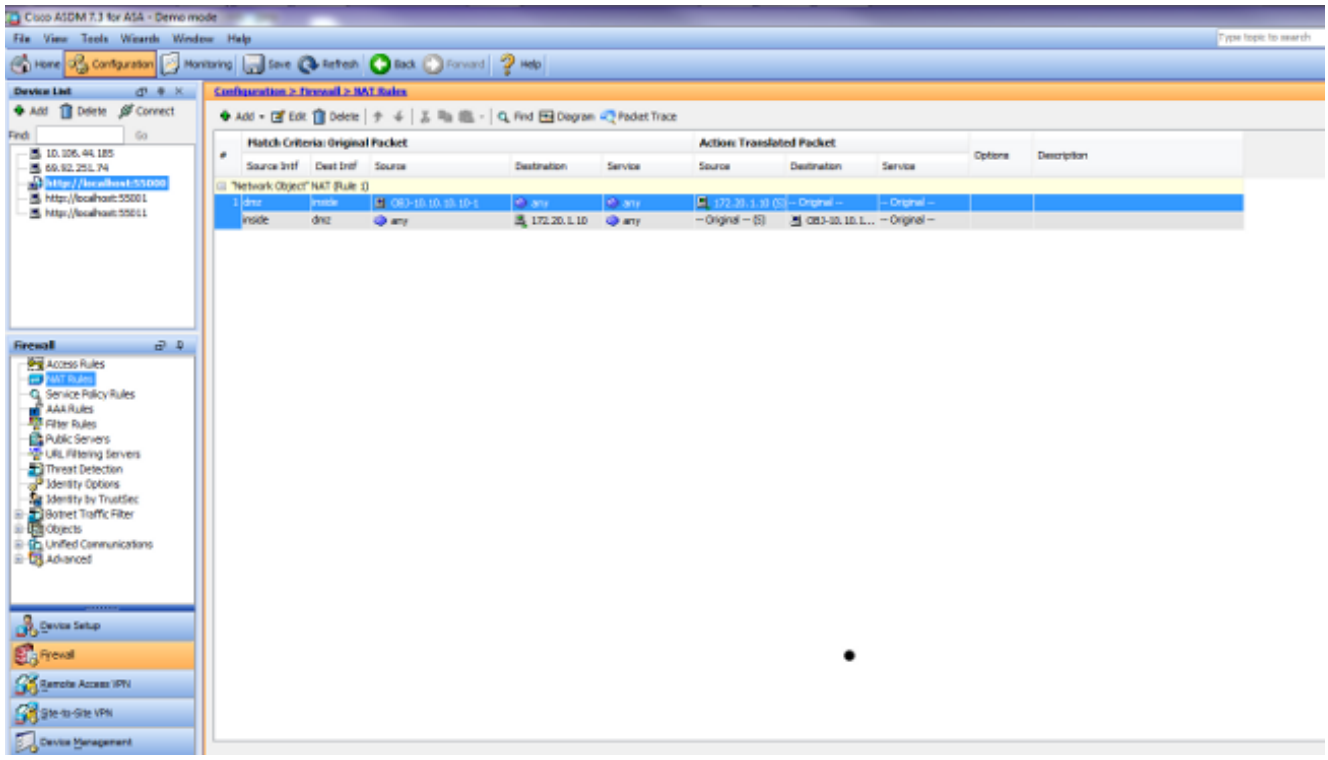
2. Preencha a configuração para a tradução estática nova. No campo de nome, incorpore **obj-10.10.10.10**.No campo do endereço IP de Um ou Mais Servidores Cisco ICM NT, incorpore o endereço do endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor WWW.Do tipo lista de drop-down, escolha a **estática**.No campo traduzido do ADDR, incorpore o endereço e conecte-o que você quer traçar o servidor WWW a.Clique **avançado**.



Na lista de drop-down da interface de origem, escolha o **dmz**.Na lista de drop-down da interface de destino, escolha **para dentro**.Neste caso, a interface interna é escolhida permitir que os anfitriões na interface interna alcancem o servidor WWW através do endereço traçado



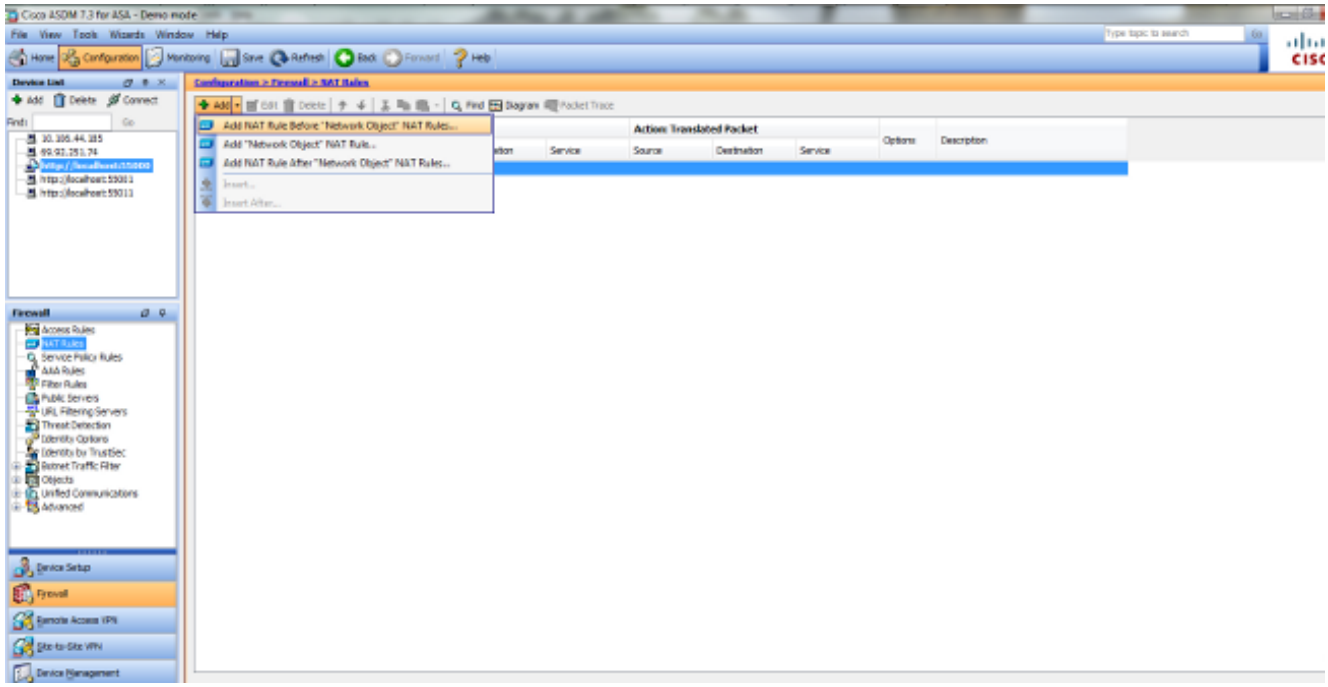
172.20.1.10.



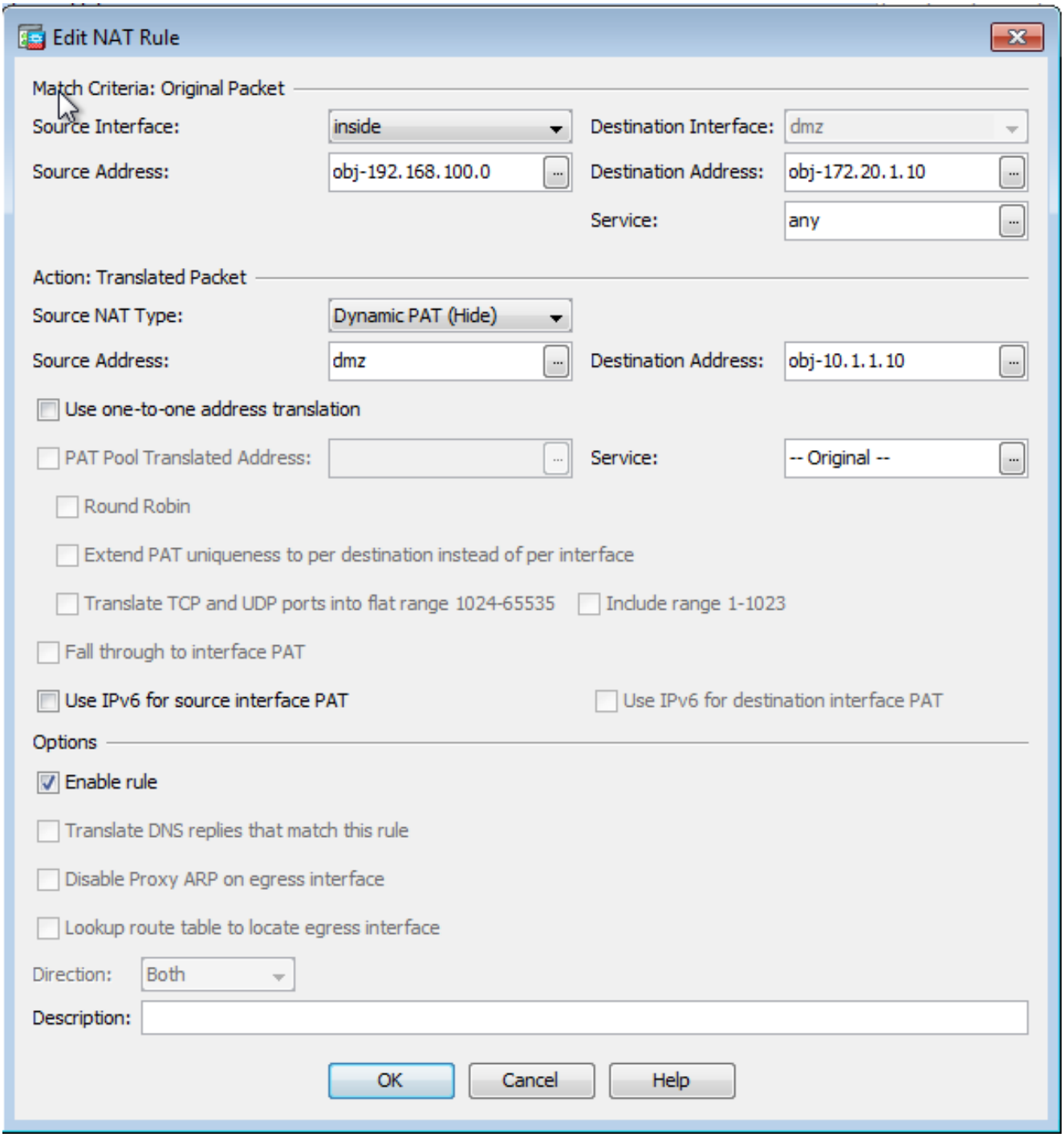
Clique a **APROVAÇÃO** a fim deixar o objeto adicionar/auto indicador da regra NAT.O clique **aplica-se** a fim enviar a configuração à ferramenta de segurança.

Método alternativo com manual/duas vezes NAT e o ASDM

1. Escolha a **configuração > as regras NAT** e escolha-os **adicionam a regra Nat do > Add antes da regra NAT do "objeto de rede"….**



2. Preencha a configuração para a tradução manual/duas vezes Nat. Na lista de drop-down da interface de origem, escolha **para dentro**.Na lista de drop-down da interface de destino, escolha o **dmz**.No campo de endereço de origem, incorpore o objeto de rede interna (obj-192.168.100.0).No campo de endereço de destino, incorpore o objeto traduzido IP do servidor DMZ (172.20.1.10).Na fonte NAT datilografe a lista de drop-down, escolhem a **PANCADINHA dinâmica (couro cru)**.No endereço de origem [ação: O campo traduzido da seção do pacote], incorpora o **dmz**.No endereço de destino [ação: O campo traduzido da seção do pacote], incorpora o objeto real IP do servidor DMZ (obj-10.10.10.10).



3. Clique a **APROVAÇÃO** a fim deixar adicionar indicador a manual/duas vezes NAT da regra.
4. O clique **aplica-se** a fim enviar a configuração à ferramenta de segurança.

Está aqui a sequência de evento que ocorre quando o NAT de destino é configurado. Supõe que o cliente tem perguntado o servidor DNS e tem recebido já uma resposta de **172.20.1.10** para o endereço do servidor WWW:

1. O cliente tenta contactar o servidor WWW em 172.20.1.10.`%ASA-7-609001: Built local-host inside:192.168.100.2`
2. A ferramenta de segurança vê o pedido e reconhece que o servidor WWW é 10.10.10.10.`%ASA-7-609001: Built local-host dmz:10.10.10.10`
3. A ferramenta de segurança cria uma conexão de TCP entre o cliente e o servidor WWW. Note os endereços traçados 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 na** ferramenta de segurança verifica que o tráfego do cliente traduz através da ferramenta de segurança. Neste caso, a primeira tradução estática está no

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 na ferramenta de segurança verifica que a conexão sucedeu entre o cliente e o servidor WWW através da ferramenta de segurança. Note 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

Esta é a configuração final do ASA para executar o DNS que medica com o NAT de destino e as três relações 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

Termine estas etapas a fim permitir a inspeção DNS (se tem sido desabilitada previamente). Neste exemplo, a inspeção DNS é adicionada à política global da inspeção do padrão, que é aplicada globalmente por um **comando service-policy** como se o ASA começou com uma configuração padrão.

1. Crie um mapa de política da inspeção para o DNS.`ciscoasa(config)#`**`policy-map type inspect dns MY_DNS_INSPECT_MAP`**
2. Do modo da configuração de mapa de política, entre no modo da configuração de parâmetro a fim especificar parâmetros para o motor da inspeção.`ciscoasa(config-pmap)#`**`parameters`**
3. No modo da configuração de parâmetro do mapa de política, especifique o tamanho da mensagem máximo para que as mensagens DNS sejam 512.`ciscoasa(config-pmap-p)#`**`message-length maximum 512`**
4. Retire fora do modo da configuração de parâmetro do mapa de política e do modo da configuração de mapa de política.`ciscoasa(config-pmap-p)#`**`exit`**
   `ciscoasa(config-pmap)#`**`exit`**
5. Confirme que o mapa de política da inspeção esteve criado como 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 da configuração de mapa de política para o **global_policy**.`ciscoasa(config)#`**`policy-map global_policy`**
   `ciscoasa(config-pmap)#`
7. No modo da configuração de mapa de política, especifique o mapa da classe da camada 3/4 do padrão, **inspection_default**.`ciscoasa(config-pmap)#`**`class inspection_default`**
   `ciscoasa(config-pmap-c)#`

8. No modo de configuração de classe do mapa de política, use o mapa de política da inspeção criado nas etapas 1-3 a fim especificar que o DNS deve ser inspecionado.`ciscoasa(config-pmap-c)#`**`inspect dns MY_DNS_INSPECT_MAP`**
9. Retire fora do modo de configuração de classe do mapa de política e do modo da configuração de mapa de política.`ciscoasa(config-pmap-c)#`**`exit`**
`ciscoasa(config-pmap)#`**`exit`**
10. Verifique que o mapa de política do **global_policy** está configurado como 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 que o global_policy está aplicado globalmente por uma serviço-política.`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 (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Capture o tráfego DNS

Um método para verificar que os registros das reescritas DNS da ferramenta de segurança são corretamente capturar os pacotes na pergunta, como discutido no exemplo anterior. Termine estas etapas a fim capturar o tráfego no ASA:

1. Crie uma lista de acessos para cada exemplo que da captação você quer criar. O ACL deve especificar o tráfego que você quer capturar. Neste exemplo, dois ACL foram criados. O ACL para o 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.
```

O ACL para o 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 os exemplos da captação:`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. Veja as captações.Éaqui o que as captações do exemplo olham como depois que algum tráfego DNS foi passado:`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 as captações a um servidor TFTP no formato PCAP para a análise em um outro aplicativo.Os aplicativos que podem analisar gramaticalmente o formato PCAP podem mostrar detalhes adicionais tais como o nome e o endereço IP de Um ou Mais Servidores Cisco ICM NT em registros DNS A.`ciscoasa#`**`copy /pcap capture:DNSINSIDE tftp`**

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

Troubleshooting

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

A reescrita DNS não é executada

Certifique-se de que você tem a inspeção DNS configurada na ferramenta de segurança.

Criação da tradução falhada

Se uma conexão não pode ser criada entre o cliente e o servidor WWW, pôde ser devido a um misconfiguration NAT. Verifique os logs da ferramenta de segurança para ver se há mensagens que indicam que um protocolo não criou uma tradução através da ferramenta de segurança. Se tais mensagens aparecem, verifique que o NAT esteve configurado para o tráfego desejado e que 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
```

Cancele as entradas do xlate, e então remova e reaplique as declarações NAT a fim resolver este erro.

Informações Relacionadas

- Manual de configuração de Cisco ASA 5500-x
- Referências de comandos do 5500-x Series de Cisco ASA
- Field Notice de produto de segurança
- Request For Comments (RFC)
- Suporte Técnico e Documentação - Cisco Systems