Configurer le doctorage DNS pour trois interfaces NAT sur ASA version 9.x

Contenu

Introduction

Ce document fournit un exemple de configuration pour effectuer le doctoring DNS (Domain Name System) sur l'appliance ASA 5500-X Series Adaptive Security Appliance (ASA) qui utilise des instructions NAT (Object/Auto Network Address Translation). Le DNS doctoring permet à l'appliance de sécurité de réécrire les enregistrements A- DNS .

La réécriture DNS remplit deux fonctions:

- Elle traduit une adresse publique (l'adresse routable ou mappée) dans une réponse de DNS à une adresse privée (la véritable adresse) quand le client DNS est sur une interface privée.

- Elle traduit une adresse privée en une adresse publique quand le client DNS est sur l'interface publique.

Conditions préalables

Conditions requises

Cisco indique que l'inspection DNS doit être activée pour effectuer le doctoring DNS sur l'appliance de sécurité. L'inspection de DNS est allumée par défaut.

Quand l'inspection de DNS est activée, l'appliance de sécurité effectue ces tâches:

- Traduit l'enregistrement DNS en fonction de la configuration effectuée à l'aide des commandes NAT objet/auto (réécriture DNS). Le routage de traduction s'applique seulement à l'enregistrement A dans la réponse de DNS. Par conséquent, les recherches inversées, qui demandent l'enregistrement du pointeur (PTR), ne sont pas affectées par la réécriture DNS. Dans la version ASA 9.0(1) et les versions ultérieures, traduction de l'enregistrement PTR DNS pour les recherches DNS inversées lors de l'utilisation de NAT IPv4, NAT IPv6 et NAT64 avec inspection DNS activée pour la règle NAT.**Note**: La réécriture DNS n'est pas compatible avec la Traduction d'adresses de port statique (PAT) car plusieurs règles PAT sont applicables pour chaque enregistrement-A et car la règle PAT à utiliser est ambiguë.
- Impose la longueur maximale de message DNS (le routage par défaut est de 512 octets et la longueur maximale est de 65535 octets). Le réassemblage est effectué selon les besoins afin de vérifier que la longueur de paquet est inférieure à la longueur maximale configurée. Le paquet est abandonné s'il dépasse la longueur maximale.**Note**: Si vous entrez la commande **inspect dns** sans l'option de longueur maximale, la taille de paquet DNS n'est pas vérifiée.
- Impose une longueur de nom de domaine de 255 octets et une longueur d'étiquette de 63 octets.
- Vérifie l'intégrité du nom de domaine mentionnée par le pointeur situé si des pointeurs de compression sont rencontrés dans le message de DNS.
- Contrôle pour vérifier si une boucle de pointeur de compression existe.

Components Used

Les informations de ce document sont basées sur l'appliance de sécurité de la gamme ASA 5500-X, version 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.

Produits connexes

Cette configuration peut également être utilisée avec le dispositif de sécurité de la gamme Cisco ASA 5500, version 8.4 ou ultérieure.

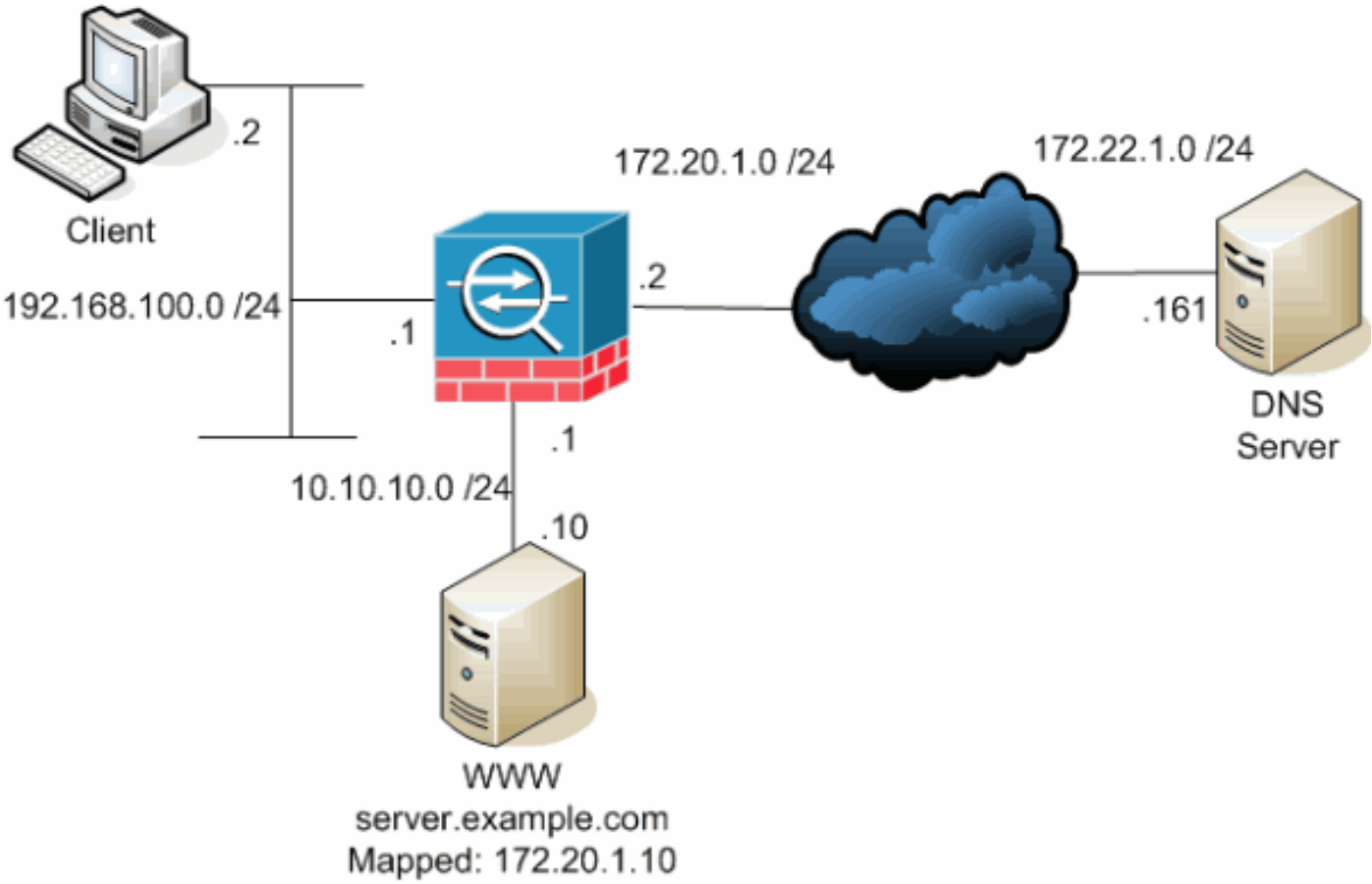
Note: La configuration ASDM s'applique à la version 7.x seulement.

Informations générales

Dans un échange DNS type, un client envoie une URL ou un nom d'hôte à un serveur DNS afin de déterminer l'adresse IP de cet hôte. Le serveur DNS reçoit la requête de routage, vérifie le consultations le mappage de nom-à-adresse-IP pour cet hôte et fournit à l'enregistrement A l'adresse IP au client de routage. Tandis que cette procédure fonctionne bien dans beaucoup de situations, les problèmes de routage peuvent se poser. Ces problèmes peuvent se poser quand le client de routage et l'hôte que le client de routage essaye d'atteindre sont tous deux sur le même réseau privé derrière NAT, mais le serveur DNS utilisé par le client de routage est sur un autre réseau public.

Scénario: Trois interfaces NAT : interne, externe, DMZ

Topologie



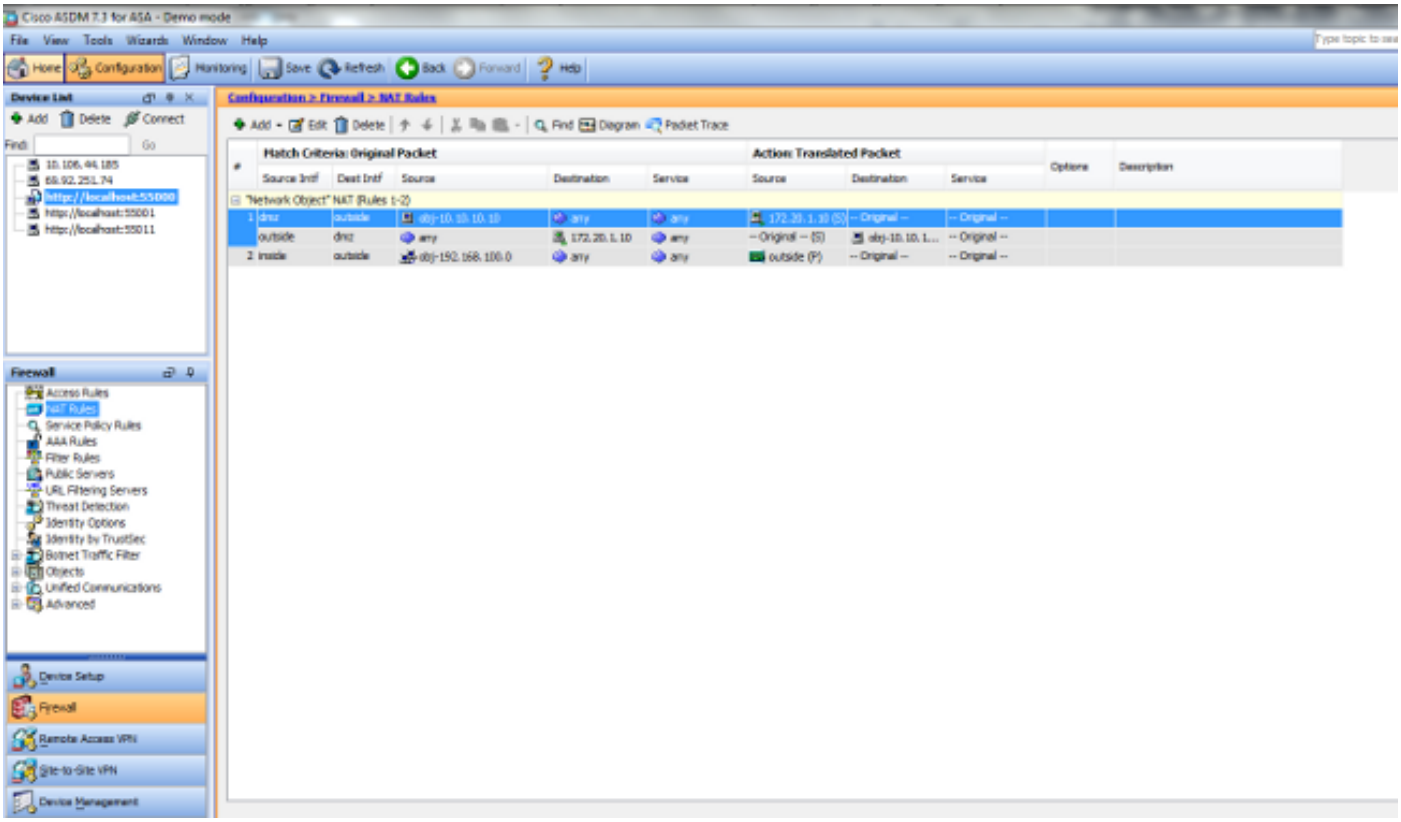
Ce schéma illustre cette situation. Dans ce cas, le client sur 192.168.100.2 veut utiliser l'URL **server.example.com** afin d'accéder au serveur WWW sur 10.10.10.10. Les services DNS pour le client sont fournis par le serveur DNS externe à l'adresse 172.22.1.161. Puisque le serveur DNS est situé sur un autre réseau public, il ne connaît pas l'adresse IP privée du serveur WWW. En revanche, il connaît l'adresse mappée du serveur WWW, à savoir 172.20.1.10. Ainsi, le serveur DNS contient le mappage de l'adresse IP à nommer **server.example.com à 172.20.1.10**.

Problème : Le client ne peut pas accéder au serveur WWW

Sans le doctoring DNS ou une autre solution de routage activée dans cette situation, si le client de routage envoie une demande DNS pour l'adresse IP de **server.example.com**, il ne peut pas accéder au serveur WWW. C'est parce que le client de routage reçoit un enregistrement A qui contient l'adresse publique mappée de 172.20.1.10 pour le serveur WWW. Quand le client de routage essaie d'accéder à cette adresse IP, l'appliance de sécurité supprime les paquets parce qu'elle ne permet pas la redirection de paquets sur la même interface. Voici ce à quoi ressemble la partie NAT de la configuration quand le doctoring DNS n'est pas activé:

```
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.
```

Voici ce à quoi la configuration ressemble dans l'ASDM quand le doctoring DNS n'est pas activé:



Voici une capture de paquets des événements quand le doctoring DNS n'est pas activé:

1. Le client de routage envoie la requête 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. PAT est effectué sur la requête DNS par l'ASA et la requête est transférée. Notez que l'adresse source du paquet a changé sur l'interface externe de l'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. Le serveur DNS répond avec l'adresse mappée du serveur 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. L'ASA annule le routage de traduction de l'adresse de destination de la réponse de DNS et transfère le paquet au client de routage. Notez que sans le doctoring DNS activé, l'adresse dans la réponse est toujours l'adresse mappée du serveur 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. Àce stade, le client tente d'accéder au serveur WWW à l'adresse 172.20.1.10. L'ASA crée une entrée de routage de connexion pour cette communication. Cependant, parce qu'elle ne permet pas au trafic de circuler de l'intérieur vers l'extérieur vers dmz, la connexion expire. Les journaux ASA montrent ceci:

```
%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
```

Solution : mot clé « dns »

Doctoring DNS avec le mot clé « dns »

Le doctoring DNS avec le mot clé de **dns donne à l'appliance de sécurité la capacité d'intercepter et réécrire les contenus des réponses du serveur DNS au client de routage.** Une fois configuré correctement, l'appliance de sécurité peut modifier l'enregistrement A afin de permettre au client dans un scénario tel que discuté dans le " Problème : Le client ne peut pas accéder à la section Serveur WWW » pour se connecter. Dans cette situation, lorsque le doctoring DNS est activé, le dispositif de sécurité réécrit l'enregistrement A pour diriger le client vers 10.10.10.10 au lieu de 172.20.1.10. Le doctoring DNS est activé lorsque vous ajoutez le mot clé **dns** à une instruction NAT statique (version 8.2 et antérieure) ou à une instruction NAT objet/auto (version 8.3 et ultérieure).

Version 8.2 et antérieure

Il s'agit de la configuration finale de l'ASA pour effectuer le doctoring DNS avec le mot clé **dns** et trois interfaces NAT pour les versions 8.2 et antérieures.

```
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
```

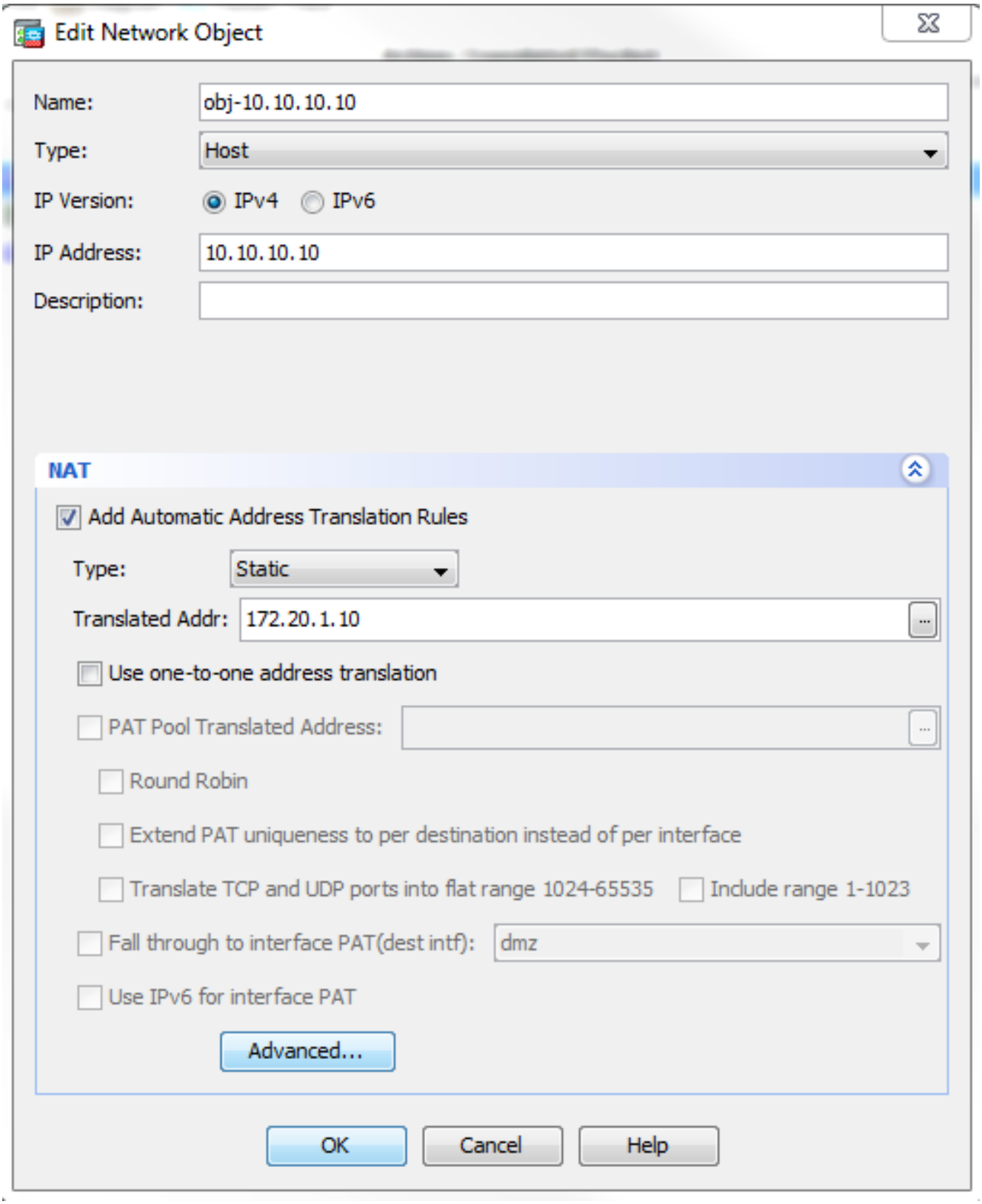
Version 8.3 et ultérieure

```
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.
```

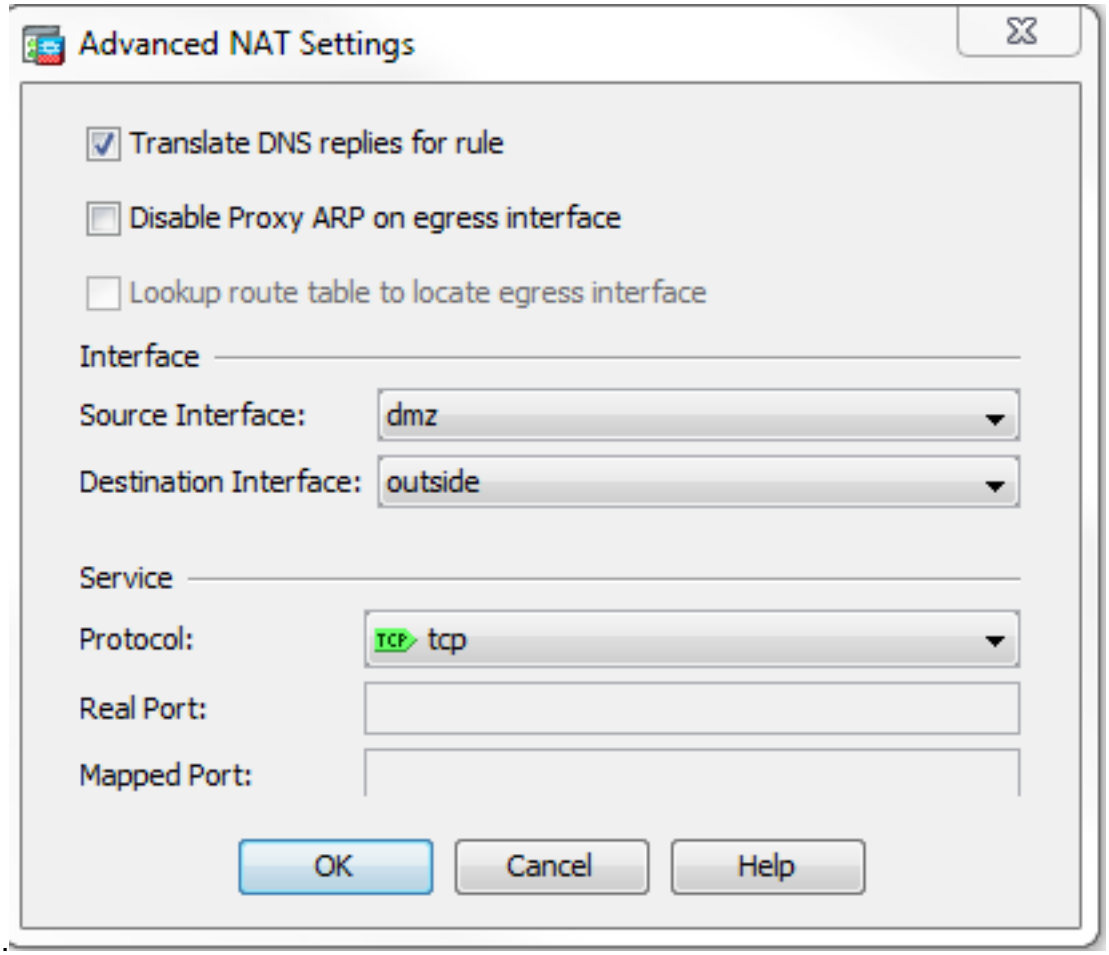
Configuration ASDM

Exécutez les étapes suivantes afin de configurer le doctoring DNS dans l'ASDM:

1. Choisissez **Configuration > NAT Rules** et choisissez la règle Objet/Auto à modifier. Cliquez sur **Edit**.
2. Cliquez sur **Avancé...**



3. Cochez la case **Traduire les réponses DNS pour la**



règle.

4. Cliquez sur **OK** afin de quitter la fenêtre Options NAT.
5. Cliquez sur **OK** afin de quitter la fenêtre Modifier l'objet/Règle NAT automatique.
6. Cliquez sur **Apply** afin d'envoyer votre configuration à l'appliance de sécurité.

Vérification

Voici une capture de paquets des événements quand le doctoring DNS est activé:

1. Le client de routage envoie la requête 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. PAT est effectué sur la requête DNS par l'ASA et la requête est transférée. Notez que l'adresse source du paquet a changé sur l'interface externe de l'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. Le serveur DNS répond avec l'adresse mappée du serveur 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. L'ASA annule le routage de traduction de l'adresse de destination de la réponse de DNS et transfère le paquet au client de routage. Notez qu'avec le doctoring de DNS activé, l'adresse dans la réponse est récrite pour être la véritable adresse du serveur de 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. A ce moment, le client de routage essaie d'accéder au serveur WWW à 10.10.10.10. La connexion réussit.

Configuration finale avec le mot clé de « dns »

C'est la configuration finale de l'ASA pour effectuer le doctoring DNS avec le mot clé **dns et trois 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
```

Solution alternative: Adresse NAT de destination

La destination NAT peut fournir une alternative au doctoring DNS. L'utilisation de la NAT de destination dans cette situation nécessite qu'une traduction NAT automatique/objet statique soit créée entre l'adresse publique du serveur WWW à l'intérieur et l'adresse réelle sur la DMZ. La destination NAT ne modifie pas les contenus de l'enregistrement A de DNS qui est renvoyé à partir du serveur DNS au client de routage. En revanche, quand vous utilisez la destination NAT dans un scénario tel que celui discuté dans ce document, le client de routage peut utiliser l'adresse IP publique **172.20.1.10 qui est retournée par le serveur DNS afin de se connecter au**

serveur WWW. La traduction automatique/objet statique permet au dispositif de sécurité de traduire l'adresse de destination de 172.20.1.10 à 10.10.10.10. Voici la partie appropriée de la configuration quand la destination NAT est utilisée:

```
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
```

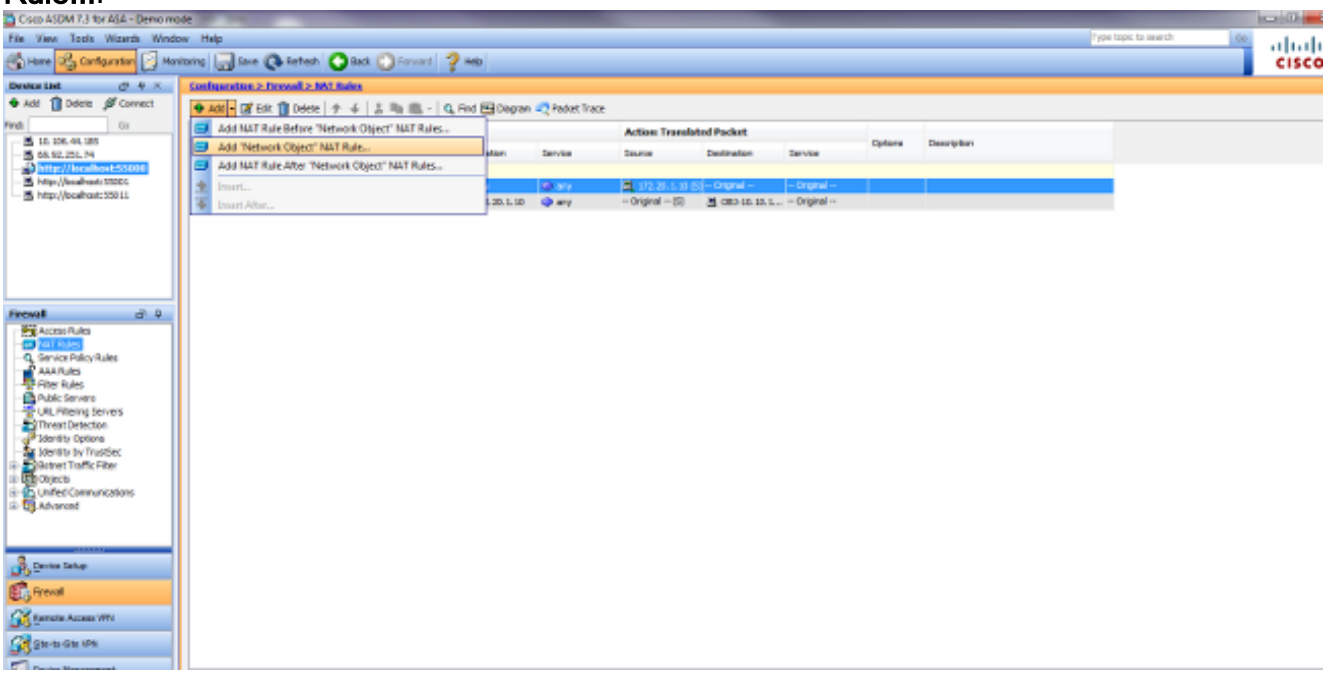
NAT de destination obtenu avec instruction NAT manuelle/double

```
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
```

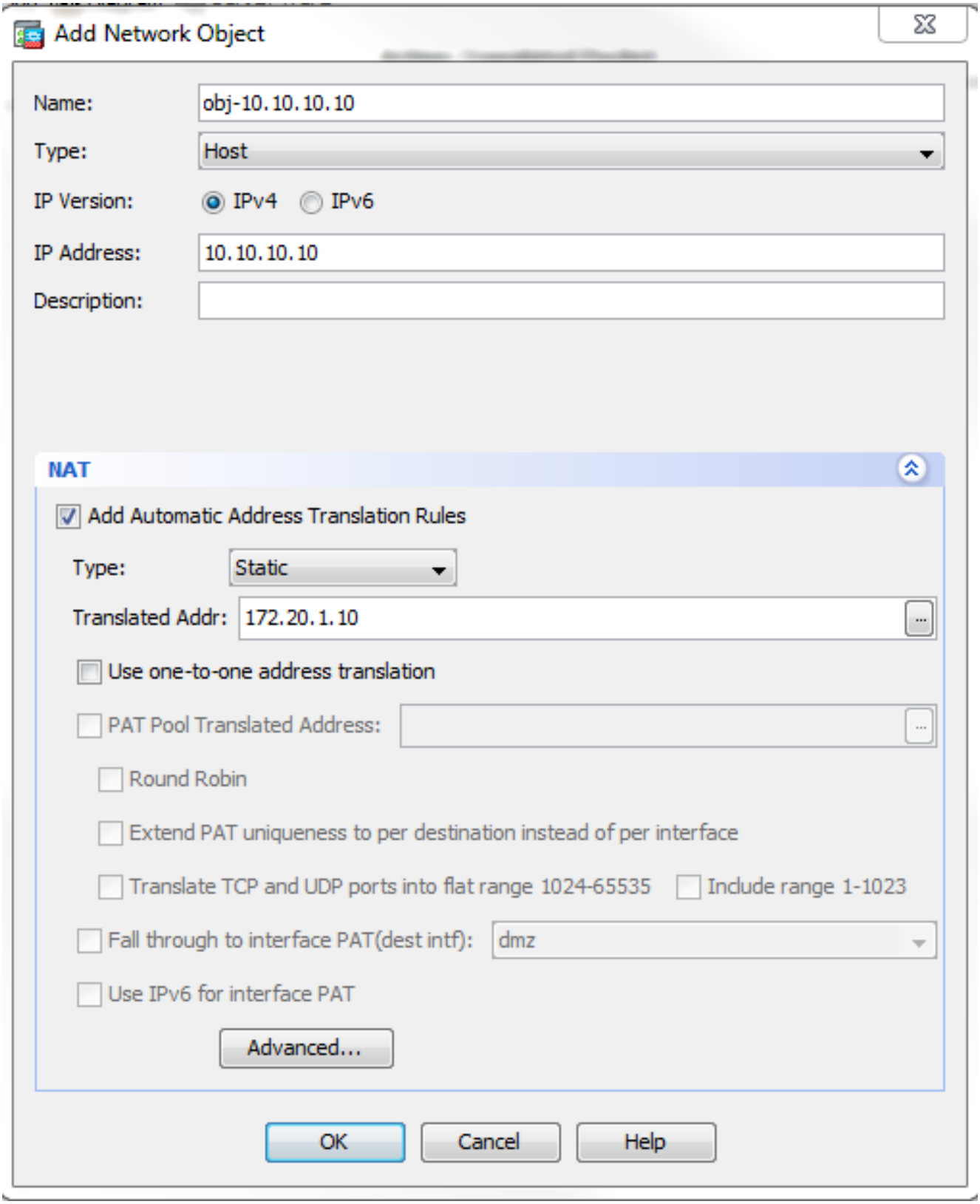
```
!--- Output suppressed.
```

Exécutez ces étapes afin de définir la configuration NAT dans l'ASDM:

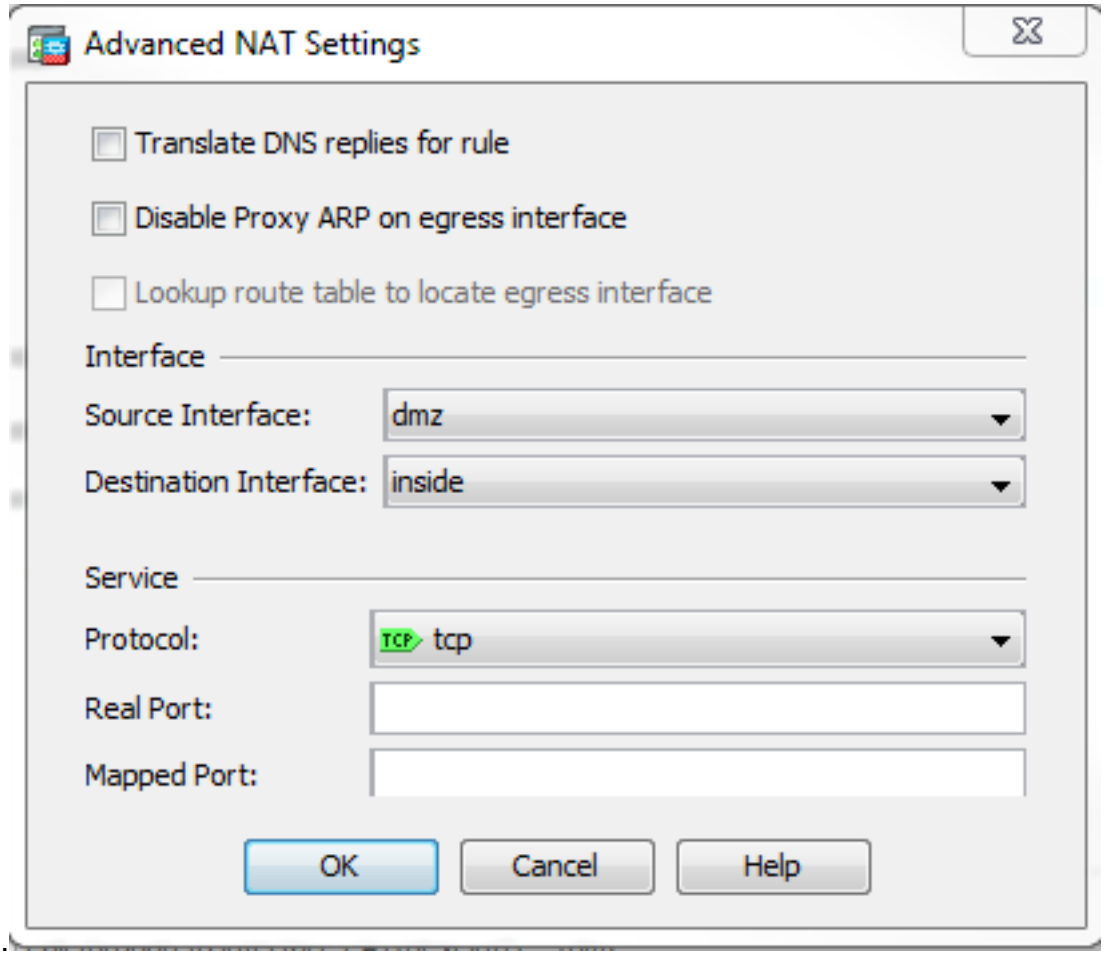
1. Choisissez **Configuration > NAT Rules** et choisissez **Add > Add « Network Object » NAT Rule...**.



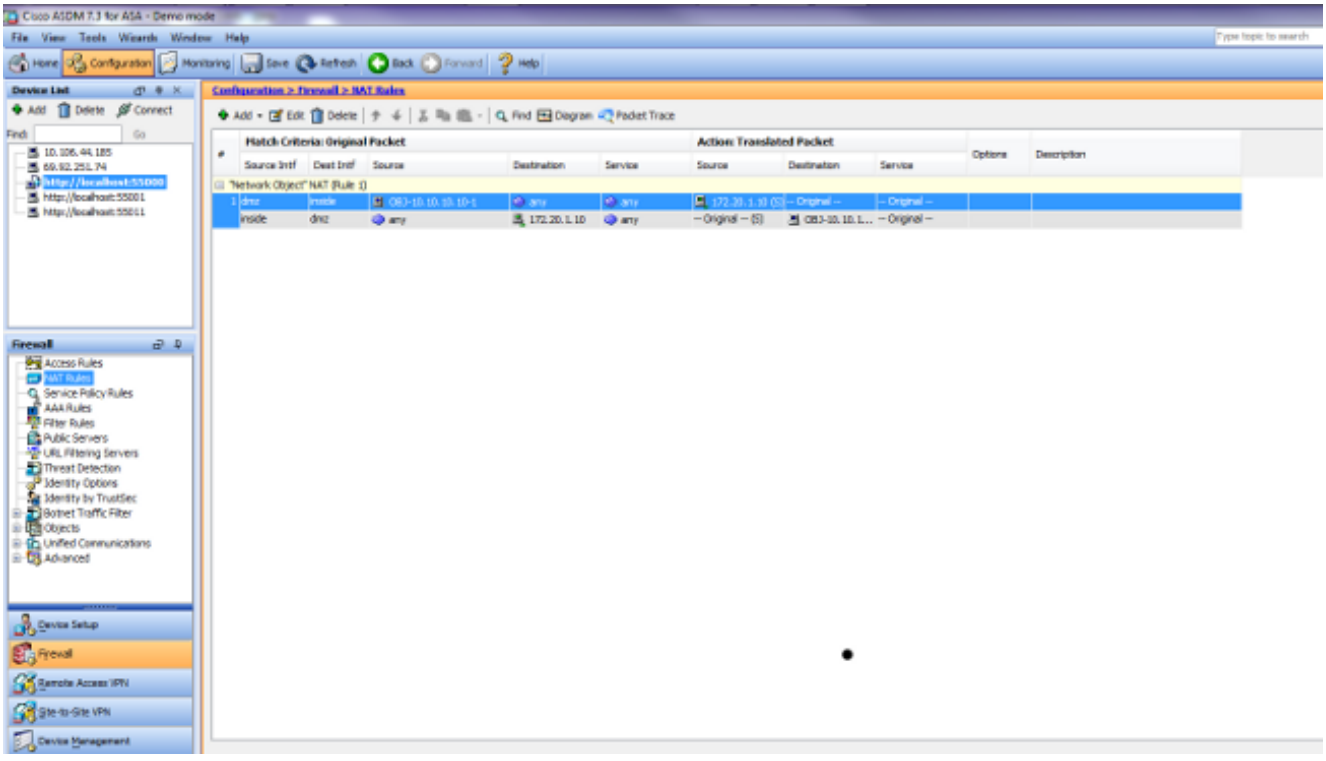
2. Complétez la configuration pour la nouveau routage de traduction statique. Dans le champ Nom, saisissez **obj-10.10.10.10**.Dans le champ IP Address, saisissez l'adresse IP du serveur WWW.Dans la liste déroulante Type, sélectionnez **Statique**.Dans le champ Adresse traduite, saisissez l'adresse et l'interface auxquelles vous souhaitez mapper le serveur WWW.Cliquez sur
Advanced.



Dans la liste déroulante Interface source, sélectionnez **dmz**.Dans la liste déroulante Interface de destination, sélectionnez **à l'intérieur**.Dans ce cas, l'interface interne est choisie pour permettre à des hôtes sur l'interface interne d'accéder au serveur WWW par l'intermédiaire de l'adresse mappée



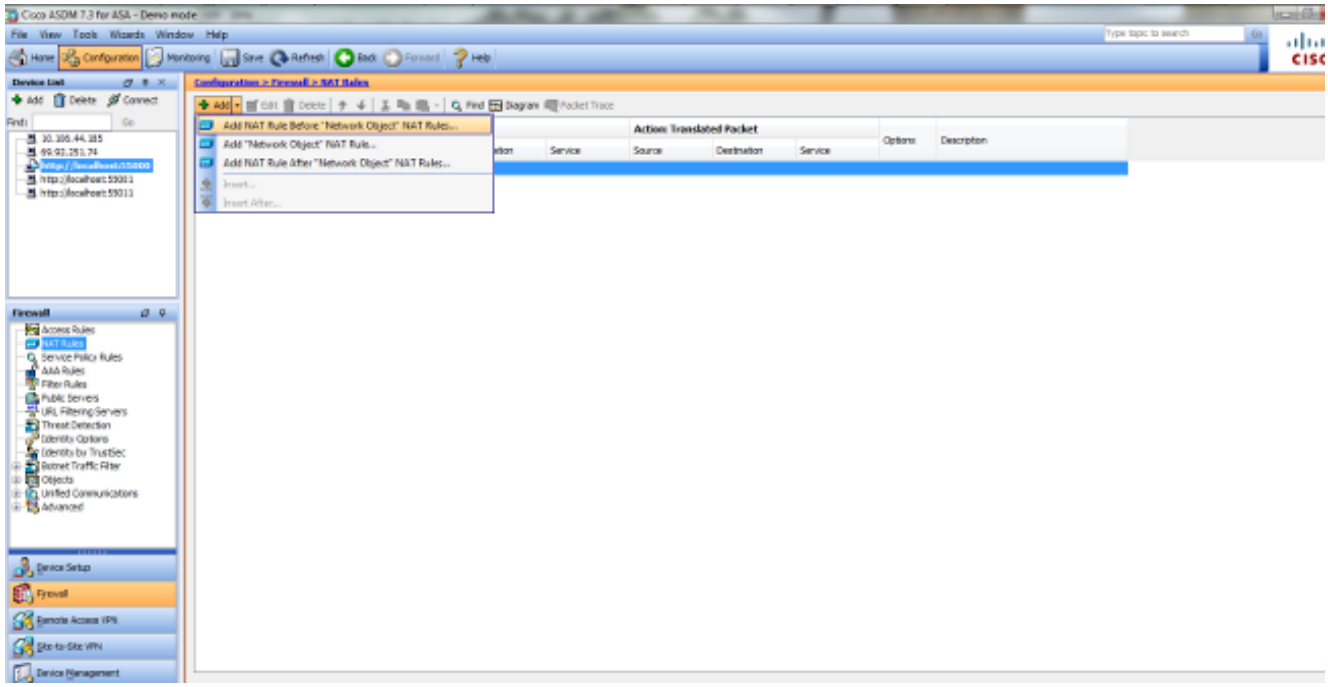
172.20.1.10.



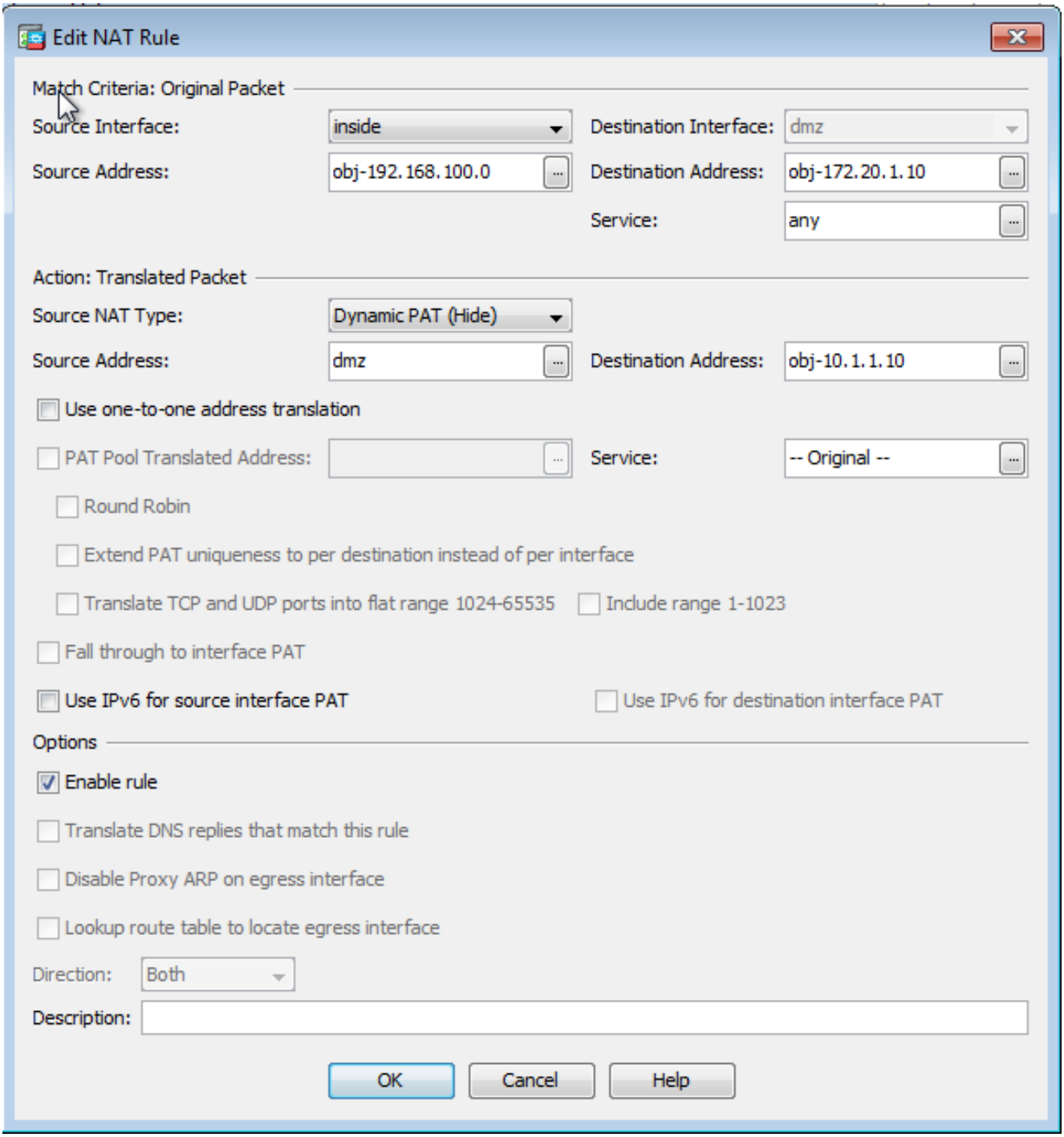
Cliquez sur **OK** afin de quitter la fenêtre Ajouter un objet/Règle NAT automatique.Cliquez sur **Apply** afin d'envoyer la configuration à l'appliance de sécurité.

Autre méthode avec NAT manuel/double et ASDM

1. Choisissez **Configuration > NAT Rules** et choisissez **Add > Add Nat rule avant « Network Object » NAT Rule...**.



2. Complétez la configuration de la traduction Manual/Twice Nat. Dans la liste déroulante Interface source, sélectionnez **à l'intérieur**.Dans la liste déroulante Interface de destination, sélectionnez **dmz**.Dans le champ Adresse source, saisissez l'objet réseau interne (obj-192.168.100.0).Dans le champ Adresse de destination, saisissez tObjet IP du serveur DMZ traduit (172.20.1.10).Dans la liste déroulante Type NAT source, sélectionnez **Dynamic PAT (Masquer).**.Dans l'adresse source [Action : Section Paquet traduit], saisissez **dmz**.Dans la zone Destination Adresse [Action : Section Paquet traduit] champ, saisissez l'objet IP réel du serveur DMZ (obj-10.10.10.10).



3. Cliquez sur **OK** afin de quitter la fenêtre Ajouter une règle NAT manuelle/double.
4. Cliquez sur **Apply** afin d'envoyer la configuration à l'appliance de sécurité.

Voici la séquence des événements qui ont lieu quand la destination NAT est configurée. Supposez que le client de routage a déjà questionné le serveur DNS et qu'il a obtenu une réponse de **172.20.1.10 pour l'adresse de serveur WWW:**

1. Le client de routage essaie de contacter le serveur WWW à 172.20.1.10.
   ```
   %ASA-7-609001: Built local-host inside:192.168.100.2
   ```
2. L'appliance de sécurité consulte la requête de routage et reconnaît que le serveur WWW est 10.10.10.10.
   ```
   %ASA-7-609001: Built local-host dmz:10.10.10.10
   ```
3. L'appliance de sécurité crée une connexion TCP entre le client de routage et le serveur WWW. Notez les adresses mappées de chaque hôte entre parenthèses.
   ```
   %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. La commande **show xlate sur l'appliance de sécurité vérifie que le trafic de routage de client**

de routage est traduit par l'intermédiaire de l'appliance de sécurité. Dans ce cas, le premier routage de traduction statique est en service.

```
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. La commande de **show conn sur l'appliance de sécurité vérifie que la connexion a réussi entre le client de routage et le serveur WWW par l'intermédiaire de l'appliance de sécurité.** Notez la véritable adresse du serveur WWW entre parenthèses.

```
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
```

Configuration finale avec la destination NAT

C'est la configuration finale de l'ASA pour effectuer le doctoring DNS avec la destination NAT et trois 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
```

Configuration

Exécutez ces étapes afin d'activer l'inspection de DNS (si elle a été précédemment désactivée). Dans cet exemple, l'inspection de DNS est ajoutée à la stratégie globale d'inspection par défaut, qui est appliqué globalement par une commande **service-policy comme si l'ASA avait commencé avec une configuration par défaut.**

1. Créez une carte de stratégie d'inspection pour le DNS.
   ```
   ciscoasa(config)#policy-map type inspect dns MY_DNS_INSPECT_MAP
   ```
2. Àpartir du mode de configuration policy-map, passez en mode de configuration des paramètres afin de spécifier les paramètres du moteur d'inspection.
   ```
   ciscoasa(config-pmap)#parameters
   ```
3. En mode de configuration des paramètres de mappage de stratégie, spécifiez la longueur maximale des messages DNS à 512.
   ```
   ciscoasa(config-pmap-p)#message-length maximum 512
   ```
4. Quittez le mode de configuration de paramètre de la carte de stratégie et le mode de configuration de la carte de stratégie.
   ```
   ciscoasa(config-pmap-p)#exit
   ciscoasa(config-pmap)#exit
   ```
5. Confirmez que la carte de stratégie d'inspection a été créée comme souhaité.
   ```
   ciscoasa(config)#show run policy-map type inspect dns
   !
   policy-map type inspect dns MY_DNS_INSPECT_MAP
   parameters
   message-length maximum 512
   !
   ```

6. Entrez le mode de configuration de la carte de stratégie pour la **stratégie globale**.
```
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#
```
7. En mode de configuration de la carte de stratégie, spécifiez la carte de classe de couche 3/4 par défaut, **inspection_default**.
```
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#
```
8. En mode de configuration de classe de carte de stratégie, utilisez la carte de stratégie d'inspection créée aux étapes 1 à 3 afin de spécifier que le DNS doit être inspecté.
```
ciscoasa(config-pmap-c)#inspect dns MY_DNS_INSPECT_MAP
```
9. Quittez le mode de configuration de la classe de la carte de stratégie et le mode de configuration de la carte de stratégie.
```
ciscoasa(config-pmap-c)#exit
ciscoasa(config-pmap)#exit
```
10. Vérifiez que la carte de stratégie **global_policy est configurée comme souhaité.**
```
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. Vérifiez que la stratégie globale est appliquée globalement par une stratégie de services.
```
ciscoasa(config)#show run service-policy
service-policy global_policy global
```

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show.** Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

Saisissez le trafic DNS

Une méthode pour vérifier que l'appliance de sécurité réécrit les enregistrements DNS consiste à capturer les paquets en question, comme évoqué dans l'exemple précédent. Exécutez ces étapes

afin de capturer le trafic de routage sur l'ASA:

1. Créez une liste d’accès pour chaque instance de capture que vous voulez créer.La liste de contrôle d’accès doit spécifier le trafic à capturer. Dans cet exemple, deux ACLs ont été créés. L'ACL pour le trafic de routage sur l'interface externe:
```
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.
```
   L'ACL pour le trafic de routage sur l'interface interne:
```
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. Créez les instances de capture :
```
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. Affichez les captures.Voici ce à quoi ressemble l'exemple de capture après qu'une partie du trafic DNS a été passée:
```
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. (Facultatif) Copiez les captures sur un serveur TFTP au format PCAP pour analyse dans une autre application.Les applications qui peuvent analyser le format de pcap peuvent montrer des détails supplémentaires tels que le nom et l'adresse IP dans des enregistrements A du DNS.
```
ciscoasa#copy /pcap capture:DNSINSIDE tftp
...
ciscoasa#copy /pcap capture:DNSOUTSIDE tftp
```

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

La réécriture DNS n'est pas effectuée

Assurez-vous que vous avez l'inspection de DNS configurée sur l'appliance de sécurité.

La création de routage de traduction a échoué

Si une connexion ne peut pas être créée entre le client de routage et le serveur WWW, elle pourrait être due à une erreur de configuration NAT. Vérifiez les journaux d'appliance de sécurité pour les messages qui indiquent qu'un protocole de routage n'a pas créé un routage de traduction par l'intermédiaire de l'appliance de sécurité. Si de tels messages apparaissent, vérifiez que NAT a été configuré pour le trafic de routage souhaité et qu'aucune adresse n'est incorrecte.

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

Effacez les entrées xlate, puis supprimez et réappliquez les instructions NAT afin de résoudre cette erreur.

Informations connexes

- Guide de configuration de Cisco ASA 5500-x
- Références des commandes de la gamme Cisco ASA 5500-x
- Avis de champs relatifs aux produits de sécurité
- Request For Comments (RFC)
- Support et documentation techniques - Cisco Systems