

# Configurez le DNS Doctoring pour trois interfaces NAT sur la release 9.x ASA

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Produits connexes](#)

[Informations générales](#)

[Scénario : Trois interfaces NAT - À l'intérieur de, extérieur, DMZ](#)

[Topologie](#)

[Problème : Le client ne peut pas accéder au serveur de WWW](#)

[Solution : "mot clé « dns »](#)

[Doctoring DNS avec le mot clé « dns »](#)

[Version 8.2 et antérieures](#)

[Version 8.3 et ultérieures](#)

[Vérifiez](#)

[Configuration finale avec le mot clé de « dns »](#)

[Solution alternative: Adresse NAT de destination](#)

[Configuration finale avec la destination NAT](#)

[Configurez](#)

[Vérifiez](#)

[Saisissez le trafic DNS](#)

[Dépannez](#)

[La réécriture DNS n'est pas effectuée](#)

[La création de routage de traduction a échoué](#)

[Informations connexes](#)

## Introduction

Ce document fournit une configuration d'échantillon pour exécuter le Système de noms de domaine (DNS) soignant sur la gamme 5500-X ASA que l'apppliance de sécurité adaptable (ASA) cette des utilisations objectent/déclaration automatique de Traduction d'adresses de réseau (NAT). Le DNS doctoring permet à l'apppliance 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 déclare que l'inspection de DN doit être activée afin d'exécuter des DN soignant sur les dispositifs 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 basé sur la configuration terminée avec l'utilisation de l'objet/des commandes NAT automatiques (réécriture de DN). Le routage de traduction s'applique seulement à l'enregistrement A dans la réponse de DNS. Renversez par conséquent les consultations, qui demandent l'enregistrement du pointeur (PTR), ne sont pas affectés par réécriture de DN. Dans la version ASA 9.0(1) et plus tard, la traduction de l'enregistrement PTR de DN pour des consultations inverses de DN en utilisant l'ipv4 NAT, l'ipv6 nat, et le NAT64 avec l'inspection de DN activée pour la règle NAT. Remarque: 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 exécuté selon les besoins afin de vérifier que la longueur de paquet est moins que la longueur maximale configurée. Le paquet est abandonné s'il dépasse la longueur maximale. Remarque: Si vous entrez les **dn d'examiner** commandent sans option de longueur maximale, des DN que la longueur de paquet 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.

### [Composants utilisés](#)

Les informations dans ce document sont basées sur l'appliance de Sécurité de gamme 5500-X ASA, version 9.x.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

### [Produits connexes](#)

Cette configuration peut également être utilisée avec l'appliance de Sécurité de gamme de Cisco ASA 5500, version 8.4 ou ultérieures.

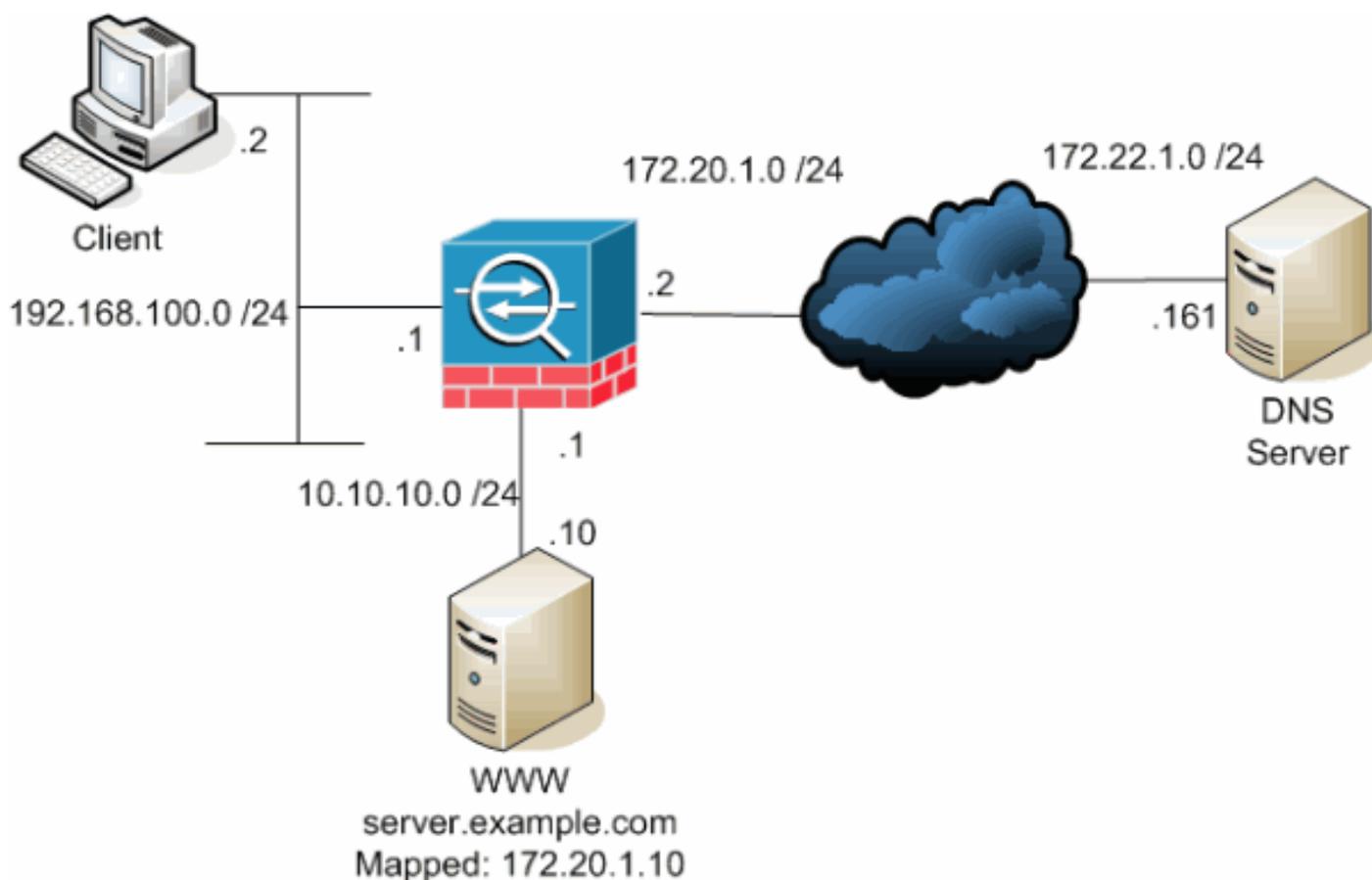
Remarque: La configuration ASDM s'applique à la version 7.x seulement.

## Informations générales

Dans un échange typique de DN, un client envoie un URL ou une adresse Internet à un serveur DNS afin de déterminer l'adresse IP de cet hôte. Le serveur DNS reçoit la requête de routage, vérifie 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 - À l'intérieur de, extérieur, DMZ

### Topologie



Ce schéma illustre cette situation. Dans ce cas, le client chez 192.168.100.2 veut employer l'URL de **server.example.com** afin d'accéder au serveur de WWW chez 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 de 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.

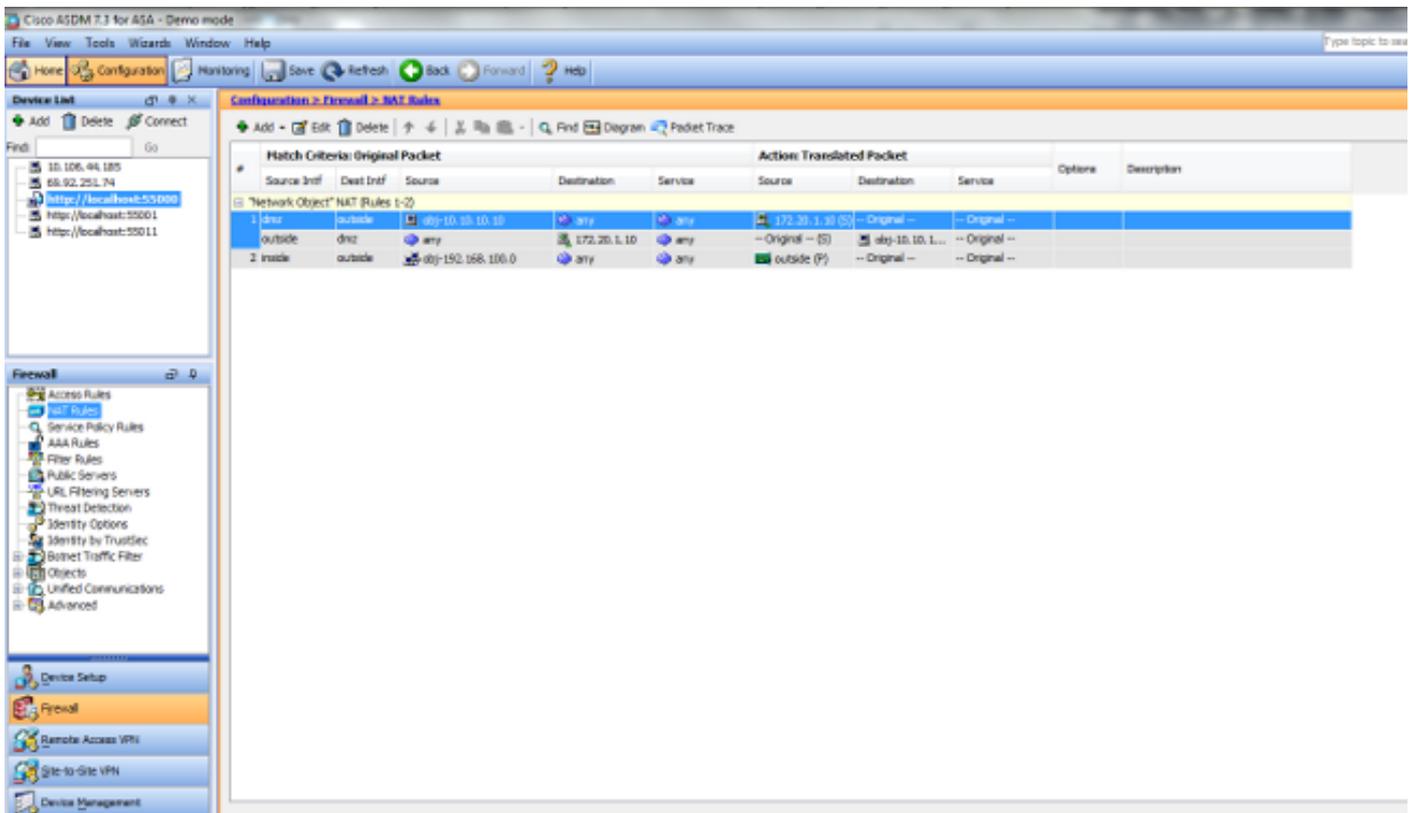
object network obj-192.168.100.0
network 192.168.100.0 255.255.255.0
nat (inside,outside) dynamic interface

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. En ce moment les essais de client pour accéder au serveur de WWW chez 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'apppliance de sécurité la capacité d'intercepter et réécrire les contenus des réponses du serveur DNS au client de routage. Une fois correctement configurés, les dispositifs de sécurité peuvent modifier l'Un-enregistrement afin de permettre le client dans un tel scénario comme évoqué dans le « problème : Le client ne peut pas section accéder à de WWW serveur » pour se connecter. Dans cette situation avec soigner de DN activé, les dispositifs de sécurité réécrivent l'Un-enregistrement pour diriger le client vers 10.10.10.10 au lieu de 172.20.1.10. Soigner de DN est activé quand vous ajoutez le mot clé de **dn** à une déclaration NAT statique (version 8.2 et antérieures) ou objectez/déclaration NAT automatique (version 8.3 et ultérieures).

## Version 8.2 et antérieures

C'est la configuration finale de l'ASA pour exécuter des DN soignant avec le mot clé de **dn** et trois interfaces NAT pour des 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 ultérieures

```

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 les **règles de Configuration > NAT** et choisissez l'objet/règle automatique d'être modifié. Cliquez sur **Edit**.
2. Clic **avancé...**

The screenshot shows the 'Edit Network Object' dialog box. The main configuration area includes:

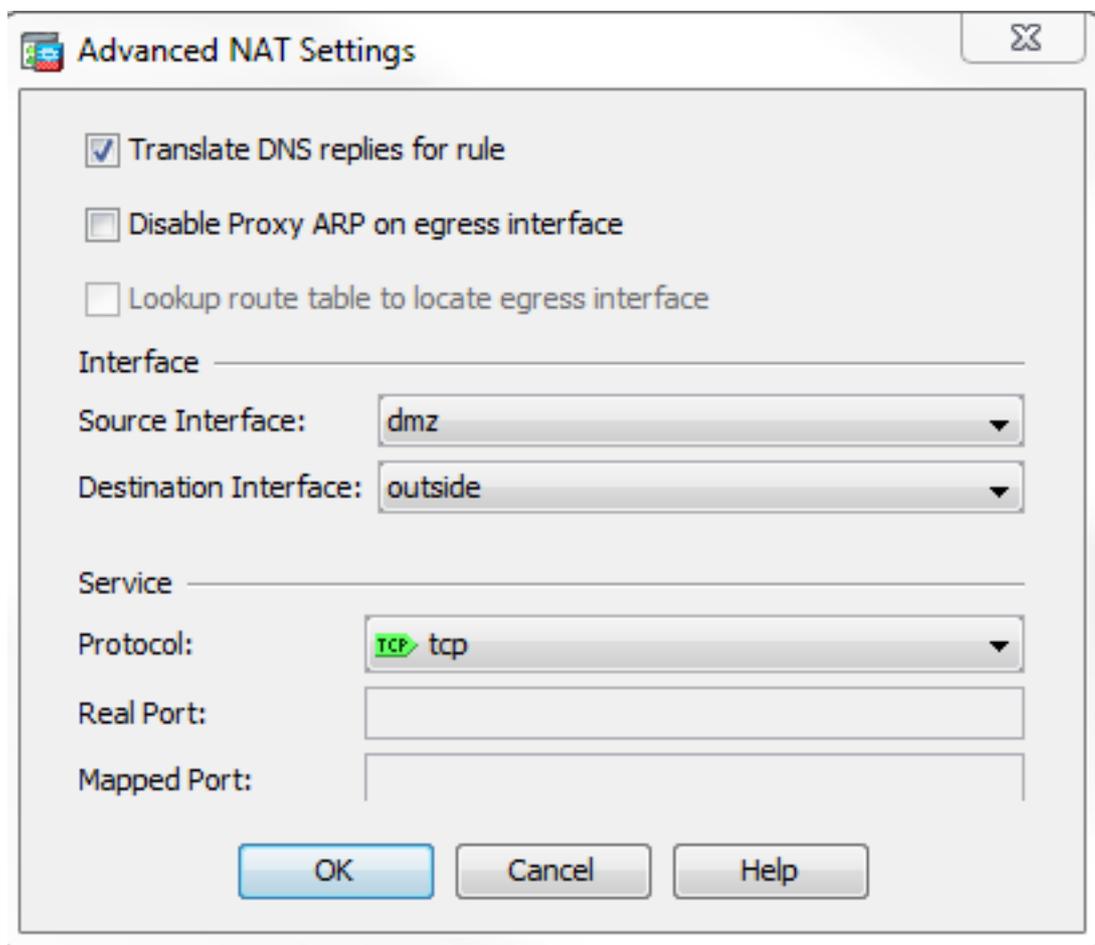
- Name: obj-10.10.10.10
- Type: Host
- IP Version:  IPv4  IPv6
- IP Address: 10.10.10.10
- Description: (empty)

The NAT configuration panel is expanded and shows:

- Add Automatic Address Translation Rules
- Type: Static
- Translated Addr: 172.20.1.10
- Use one-to-one address translation
- PAT Pool Translated Address: (empty)
- Round Robin
- Extend PAT uniqueness to per destination instead of per interface
- Translate TCP and UDP ports into flat range 1024-65535  Include range 1-1023
- Fall through to interface PAT(dest intf): dmz
- Use IPv6 for interface PAT

Buttons at the bottom: OK, Cancel, Help, and an 'Advanced...' button within the NAT panel.

3. Cochez les réponses de DN de traduire pour la case de



règle.

4. Cliquez sur OK afin de laisser la fenêtre NAT d'options.
5. Cliquez sur OK afin de laisser l'objet d'éditer/fenêtre automatique de règle NAT.
6. Cliquez sur Apply afin d'envoyer votre configuration aux dispositifs de sécurité.

## Vérifiez

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  |
|-----|----------|---------------|--------------|
| 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<br>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<br>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 réécrite pour être la véritable adresse du serveur de WWW.

```
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 destination NAT dans cette situation exige qu'un objet statique/traduction NAT automatique est créé entre l'annonce publique de serveur de WWW sur l'adresse intérieure et vraie sur le 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. L'objet statique/traduction automatique permet aux dispositifs de sécurité pour

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 réalisé avec le manuel/deux fois la déclaration 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

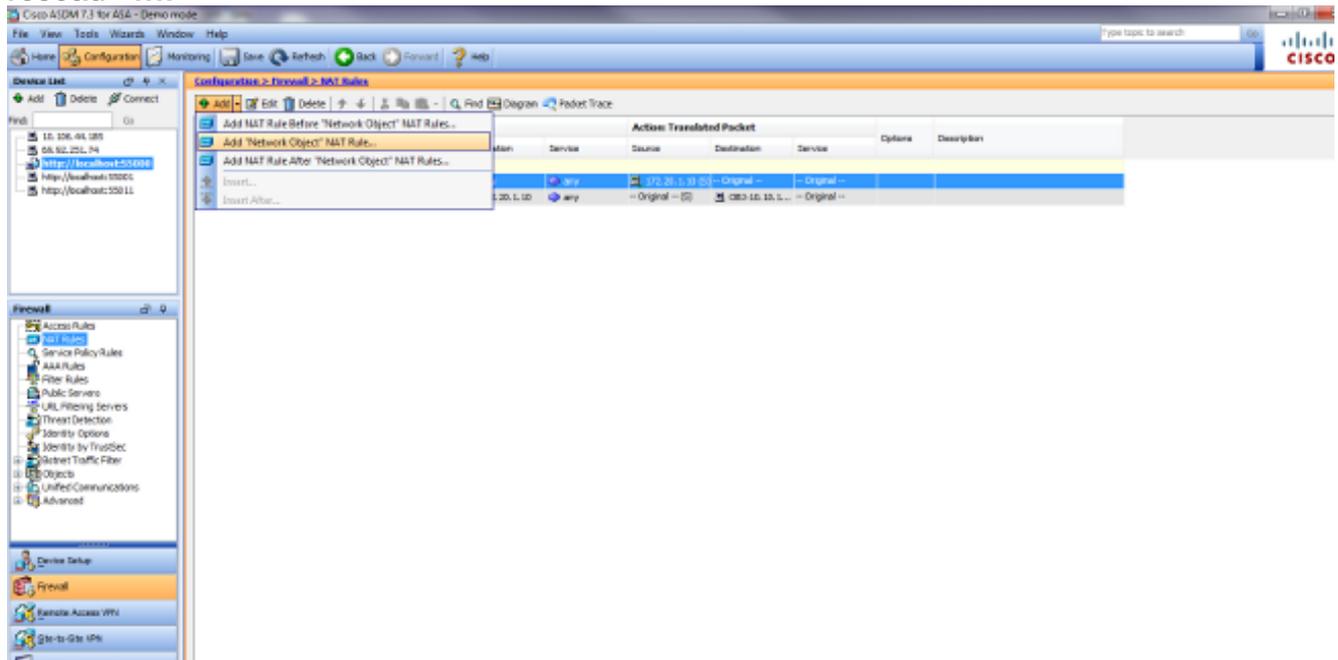
!--- Static translation to allow hosts on the inside access
!--- to the WWW server via its outside address.

access-group OUTSIDE in interface outside

!--- Output suppressed.
```

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

1. Choisissez les règles de Configuration > NAT et choisissez ajoutent > ajoutent la règle NAT de « objet de réseau »....



2. Complétez la configuration pour la nouveau routage de traduction statique. Dans la zone d'identification, écrivez **obj-10.10.10.10**. Dans le champ IP Address, introduisez l'adresse de l'adresse IP du serveur de WWW. De la liste déroulante de type, choisissez la **charge statique**. Dans le domaine traduit d'adr, écrivez l'adresse et l'interface que vous voulez tracer le serveur de WWW à. Cliquez sur **Advanced**.

**Add Network Object**

Name: obj-10.10.10.10

Type: Host

IP Version:  IPv4  IPv6

IP Address: 10.10.10.10

Description:

---

**NAT**

Add Automatic Address Translation Rules

Type: Static

Translated Addr: 172.20.1.10

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535  Include range 1-1023

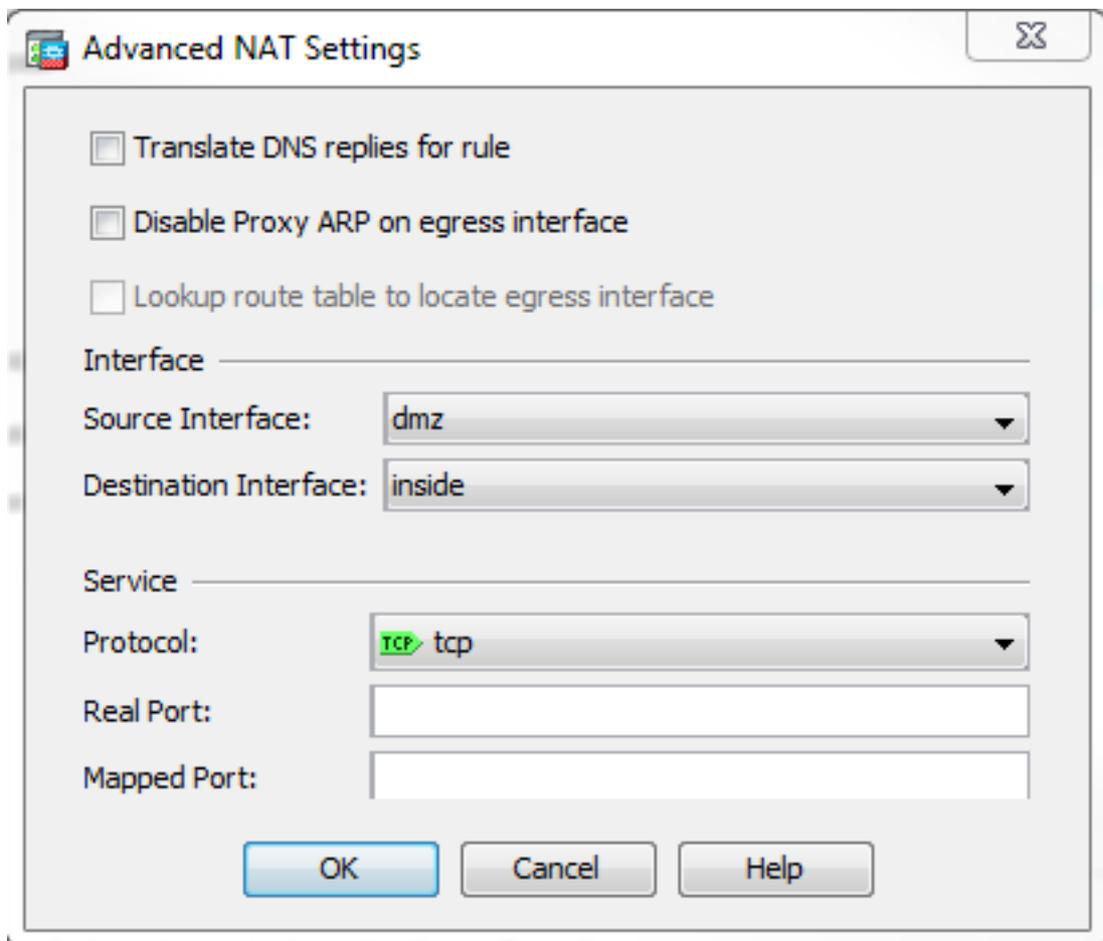
Fall through to interface PAT(dest intf): dmz

Use IPv6 for interface PAT

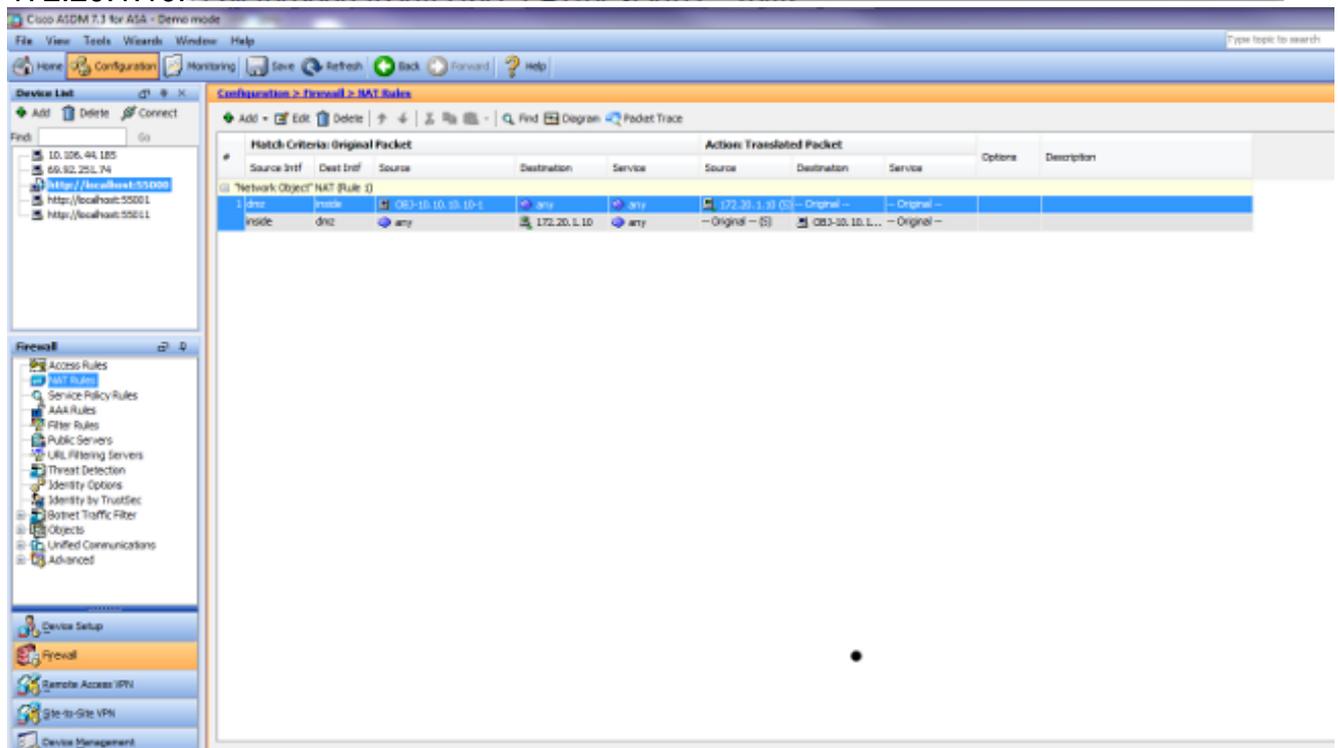
Advanced...

OK Cancel Help

Dans la liste déroulante d'interface de source, choisissez le **dmz**. Dans la liste déroulante d'interface de destination, choisissez **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



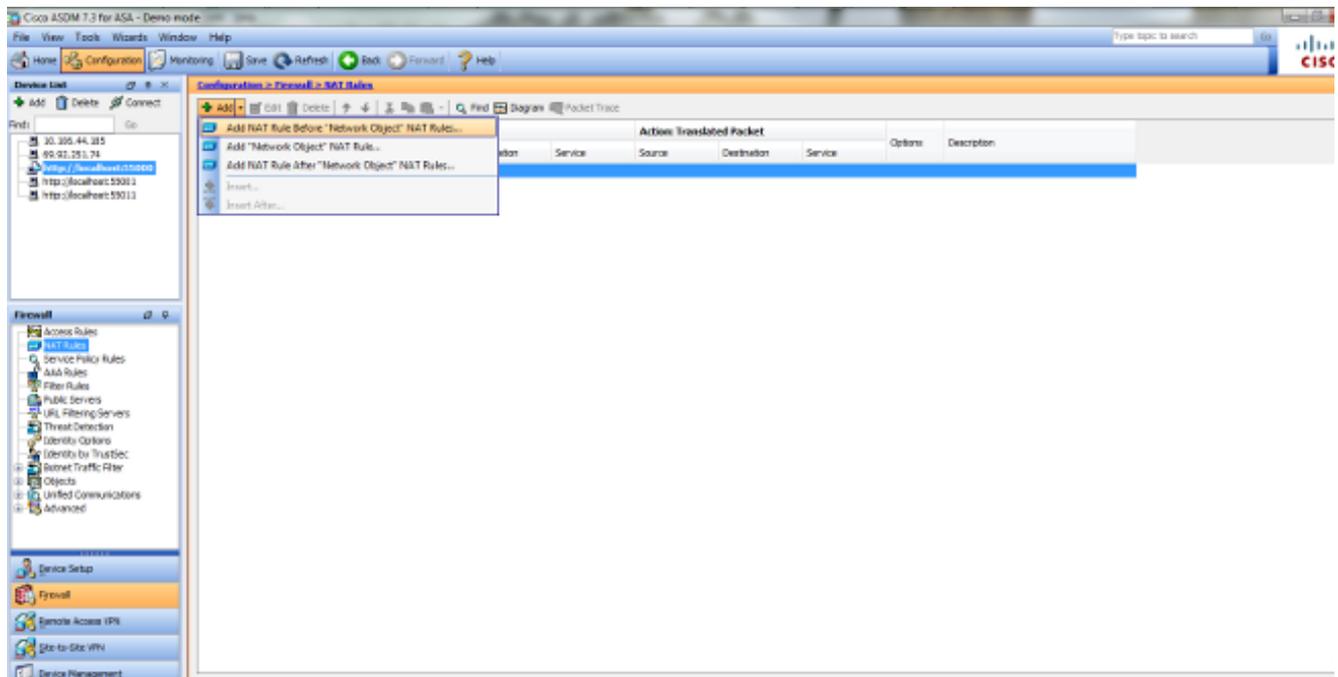
172.20.1.10.



Cliquez sur OK afin de laisser l'objet d'ajouter/fenêtre automatique de règle NAT. Cliquez sur Apply afin d'envoyer la configuration aux dispositifs de sécurité.

### Approche alternative avec le manuel/deux fois NAT et l'ASDM

1. Choisissez les règles de Configuration > NAT et choisissez ajoutent > ajoutent la règle nat avant règle NAT de « objet de réseau »....



2. Complétez la configuration pour le manuel/deux fois la traduction nat. Dans la liste déroulante d'interface de source, choisissez **à l'intérieur**. Dans la liste déroulante d'interface de destination, choisissez le **dmz**. Dans la zone adresse d'adresse source, écrivez l'objet de réseau intérieur (obj-192.168.100.0). Dans le champ d'adresse de destination, écrivez l'objet traduit IP de serveur DMZ (172.20.1.10). Dans la liste déroulante NAT de type de source, choisissez **PAT dynamique (peau)**. Dans l'adresse source [action : Le champ traduit de section de paquet], écrivent le **dmz**. Dans l'adresse de destination [action : Le champ traduit de section de paquet], écrivent le vrai objet IP de serveur DMZ (obj-10.10.10.10).

**Edit NAT Rule**

Match Criteria: Original Packet

Source Interface:  Destination Interface:

Source Address:  Destination Address:

Service:

Action: Translated Packet

Source NAT Type:

Source Address:  Destination Address:

Use one-to-one address translation

PAT Pool Translated Address:  Service:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535  Include range 1-1023

Fall through to interface PAT

Use IPv6 for source interface PAT  Use IPv6 for destination interface PAT

Options

Enable rule

Translate DNS replies that match this rule

Disable Proxy ARP on egress interface

Lookup route table to locate egress interface

Direction:

Description:

3. Cliquez sur OK afin de laisser la fenêtre de manuel/deux fois de règle NAT d'ajouter.

4. Cliquez sur Apply afin d'envoyer la configuration aux dispositifs 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'appareil 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'appareil 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'appareil de sécurité vérifie que le trafic de routage de client de routage est traduit par l'intermédiaire de l'appareil de sécurité. Dans ce cas, le premier

roulage 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-shal
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

```

## Configurez

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. Du mode de configuration de la carte de stratégie, écrivez le mode de configuration de paramètre afin de spécifier des paramètres pour l'engine d'inspection.  
`ciscoasa(config-pmap)#parameters`
3. Dans le mode de configuration de paramètre de policy-map, spécifiez la longueur de message maximum pour que les messages de DN soient 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. Dans le mode de configuration de classe de policy-map, employez la carte de stratégie d'inspection créée dans les étapes 1-3 afin de spécifier que des DN devraient être examinés.  
`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

## Vérifiez

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'apppliance 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 exemple de capture que vous voulez créer. L'ACL devrait spécifier le trafic de routage que vous voulez 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 exemples 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 vers un serveur TFTP dans le format pcap pour l'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
```

## Dépannez

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 de xlate, et puis retirez et réappliquez les déclarations NAT afin de résoudre cette erreur.

## [Informations connexes](#)

- [Guide de configuration de Cisco ASA 5500-x](#)
- [Références de commandes de gamme 5500-x de Cisco ASA](#)
- [Notes de terrain relatives aux produits de sécurité](#)
- [Request For Comments \(RFC\)](#)
- [Support et documentation techniques - Cisco Systems](#)