PIX/ASA : exemple de configuration d'un doctoring DNS avec la commande static et deux interfaces NAT

Table des matières

Introduction

Ce document fournit un exemple de configuration pour effectuer le doctoring DNS (Domain Name System) sur l'appliance de sécurité adaptative de la gamme ASA 5500 ou l'appliance de sécurité de la gamme PIX 500 en utilisant des instructions NAT (Network Address Translation) statiques. 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.

Remarque : la configuration de ce document contient deux interfaces NAT : interne et externe. Pour un exemple de doctoring DNS avec statique et trois interfaces NAT (interne, externe et dmz), référez-vous à PIX/ASA : Perform DNS Doctoring with the static Command and Three NAT Interfaces Configuration Example.

Référez-vous à Instructions NAT et PAT de PIX/ASA 7.x et à Utilisation des commandes nat, global, static, conduit et access-list et redirection de port (transfert) sur PIX pour plus d'informations sur la façon d'utiliser NAT sur un dispositif de sécurité.

Conditions préalables

Exigences

L'inspection de DNS doit être activée afin d'effectuer le doctoring DNS sur l'appliance de sécurité. L'inspection de DNS est allumée par défaut. Si elle a été désactivée, consultez la section Configurer l'inspection DNS plus loin dans ce document pour la réactiver. Quand l'inspection de DNS est activée, l'appliance de sécurité effectue ces tâches:

- Traduit l'enregistrement DNS basé sur la configuration complétée en utilisant le routage statique et les commandes nat (réécriture de DNS). Le routage de traduction s'applique seulement à l'enregistrement A dans la réponse de DNS. Par conséquent, les recherches inverses qui demandent l'enregistrement PTR, ne sont pas affectées par la réécriture de DNS.

  Remarque : la réécriture DNS n'est pas compatible avec la traduction d'adresses de port (PAT) statique, car plusieurs règles PAT s'appliquent à chaque enregistrement A et 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 pour vérifier que la longueur du paquet est inférieure à la longueur maximale configurée. Le paquet est abandonné s'il dépasse la longueur maximale.

  Remarque : si vous exécutez la commande inspect dns sans l'option de longueur maximale, la taille de paquet DNS n'est pas cochée.

- 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 de ce document sont basées sur l'appliance de sécurité de la gamme ASA 5500, version 7.2(1).

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 l'Appliance de sécurité de la gamme Cisco PIX 500, version 6.2 ou ultérieures.

Remarque : la configuration de Cisco Adaptive Security Device Manager (ASDM) s'applique uniquement à la version 7.x.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

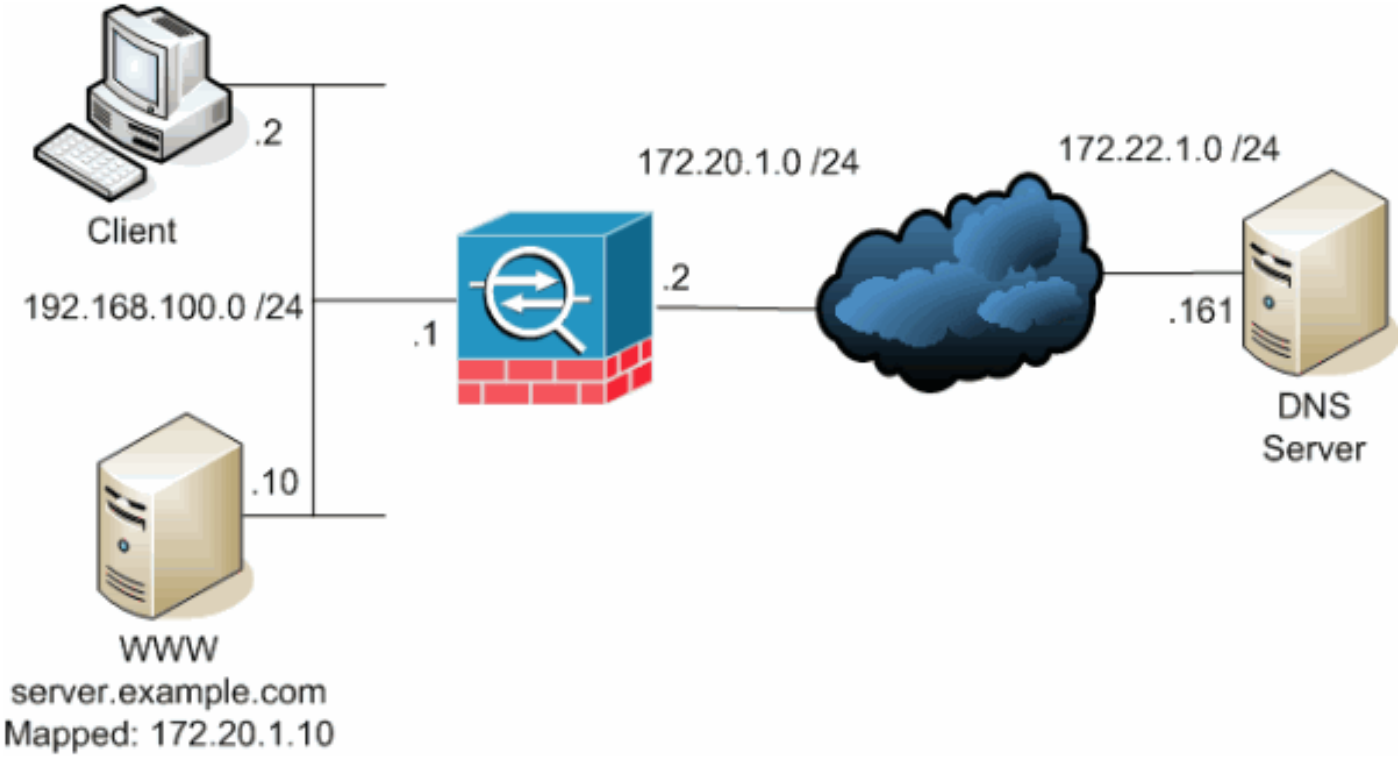
Informations générales

Dans un échange habituel DNS, un client de routage 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 : deux interfaces NAT (interne, externe)

Topologie

Dans ce scénario, le client et le serveur WWW que le client tente d'atteindre sont tous deux situés sur l'interface interne de l'ASA. Le PAT dynamique est configuré pour permettre l'accès client au routage Internet. NAT statique avec une liste d'accès est configurée pour permettre au serveur d'accéder à Internet et de permettre aussi aux hôtes Internet d'accéder au serveur WWWW.



Ce schéma illustre cette situation. Dans ce cas, le client à l'adresse 192.168.100.2 veut utiliser l'URL server.example.com pour accéder au serveur WWW à 192.168.100.10. 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. En effet, le client reçoit un enregistrement A qui contient l'adresse publique mappée : 172.20.1.10 du 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:

<#root>

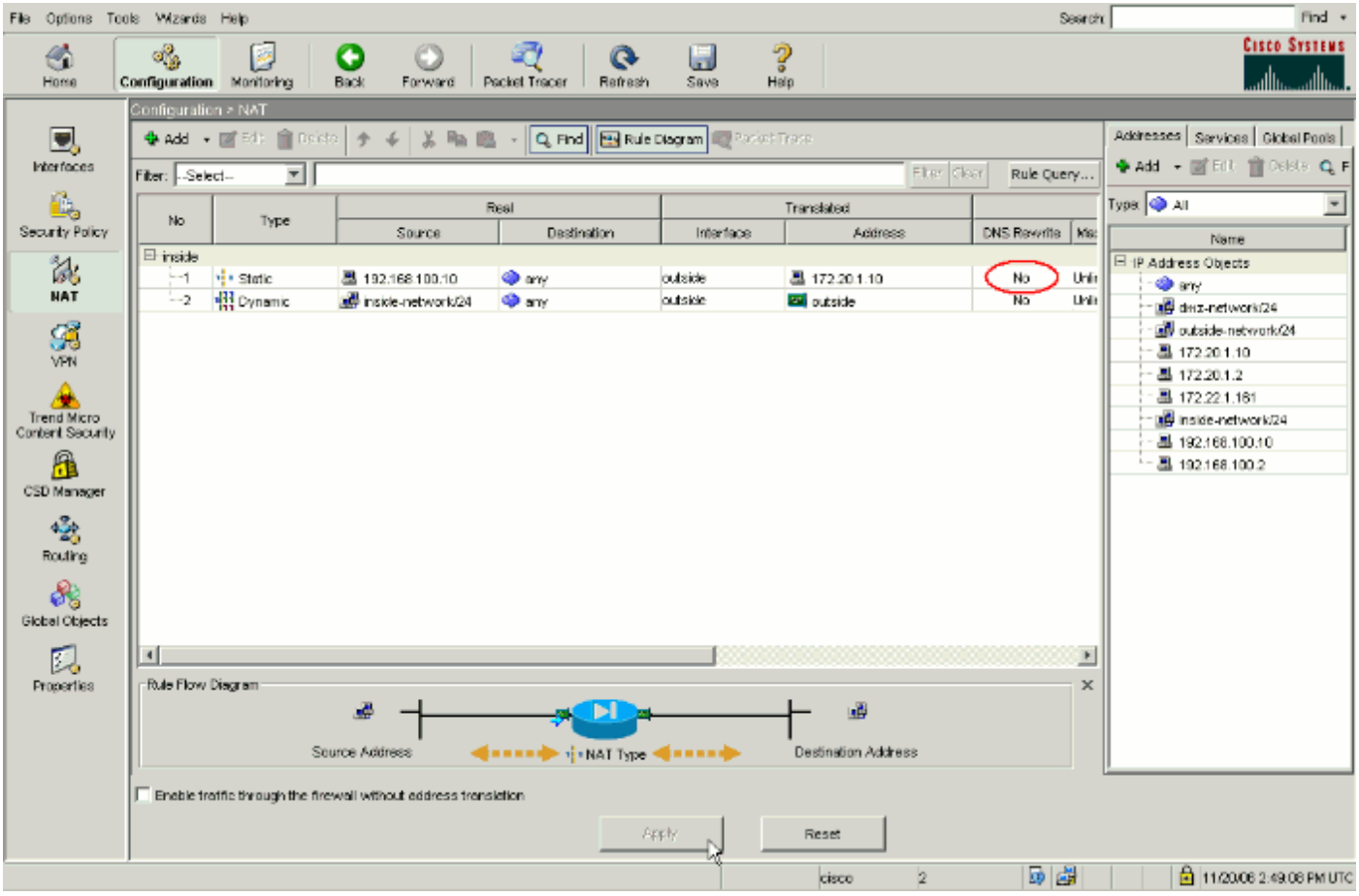
```
ciscoasa(config)#
```

show running-config

```
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa


!--- Output suppressed.
```

```
access-list OUTSIDE extended permit tcp any host 172.20.1.10 eq www


!--- Output suppressed.

global (outside) 1 interface
nat (inside) 1 192.168.100.0 255.255.255.0
static (inside,outside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255
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.

<#root>

```
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.

```
<#root>

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.

```
<#root>

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.

```
<#root>

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. A ce moment, le client de routage essaie d'accéder au serveur WWW à 172.20.1.10. L'ASA crée une entrée de routage de connexion pour cette communication. Cependant, comme elle ne permet pas au trafic de circuler de l'intérieur vers l'extérieur et de l'intérieur, la connexion expire. Les journaux ASA montrent ceci:

<#root>

```
%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 correctement

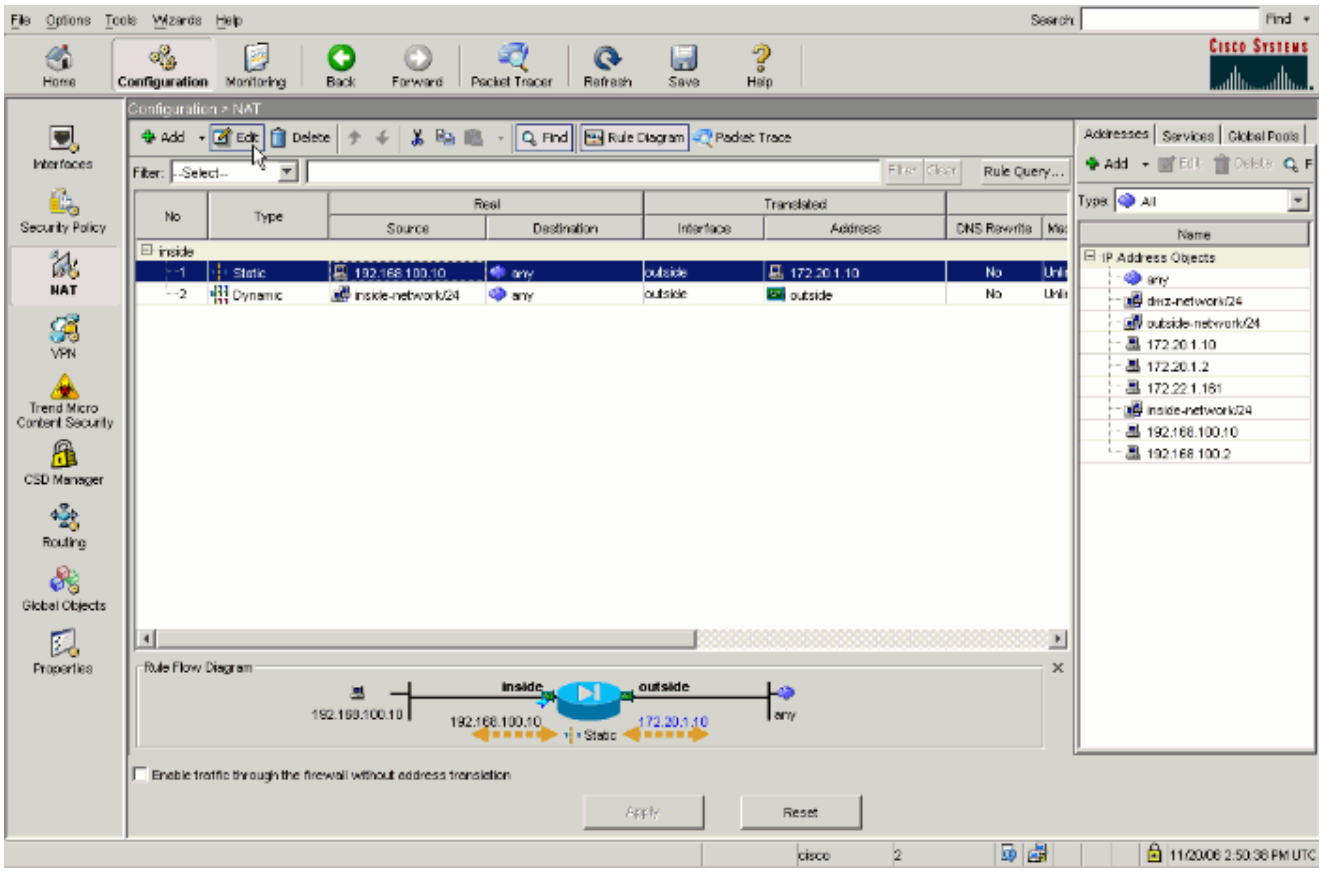
configuré, l'appliance de sécurité peut modifier l'enregistrement A pour permettre au client dans un scénario tel que discuté dans la section Problème : le client ne peut pas accéder au serveur WWW pour se connecter. Dans cette situation, avec le doctoring DNS activé, l'appliance de sécurité réécrit l'enregistrement A pour diriger le client de routage vers 192.168.100.10, au lieu de 172.20.1.10. Le doctoring DNS est activé quand vous ajoutez le mot clé de dns à une instruction NAT statique. Voici ce à quoi ressemble la partie NAT de la configuration quand le doctoring DNS es activé:

<#root>

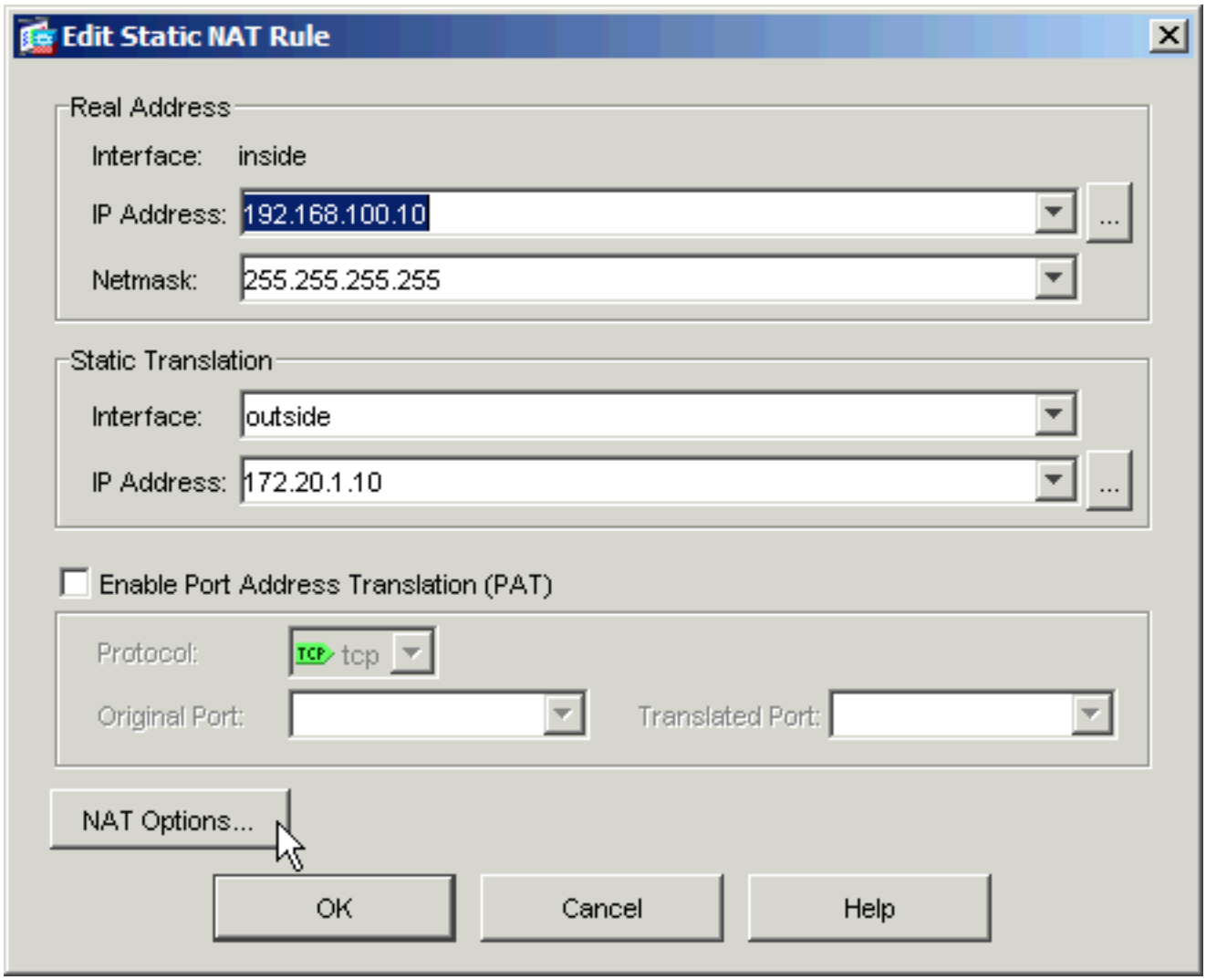
```
ciscoasa(config)#
show run

: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa


!--- Output suppressed.

access-list OUTSIDE extended permit tcp any host 172.20.1.10 eq www


!--- Output suppressed.

global (outside) 1 interface
nat (inside) 1 192.168.100.0 255.255.255.0
static (inside,outside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255
dns


!--- The "dns" keyword is added to instruct the security appliance to modify !--- DNS records related t

access-group OUTSIDE in interface outside


!--- Output suppressed.
```

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

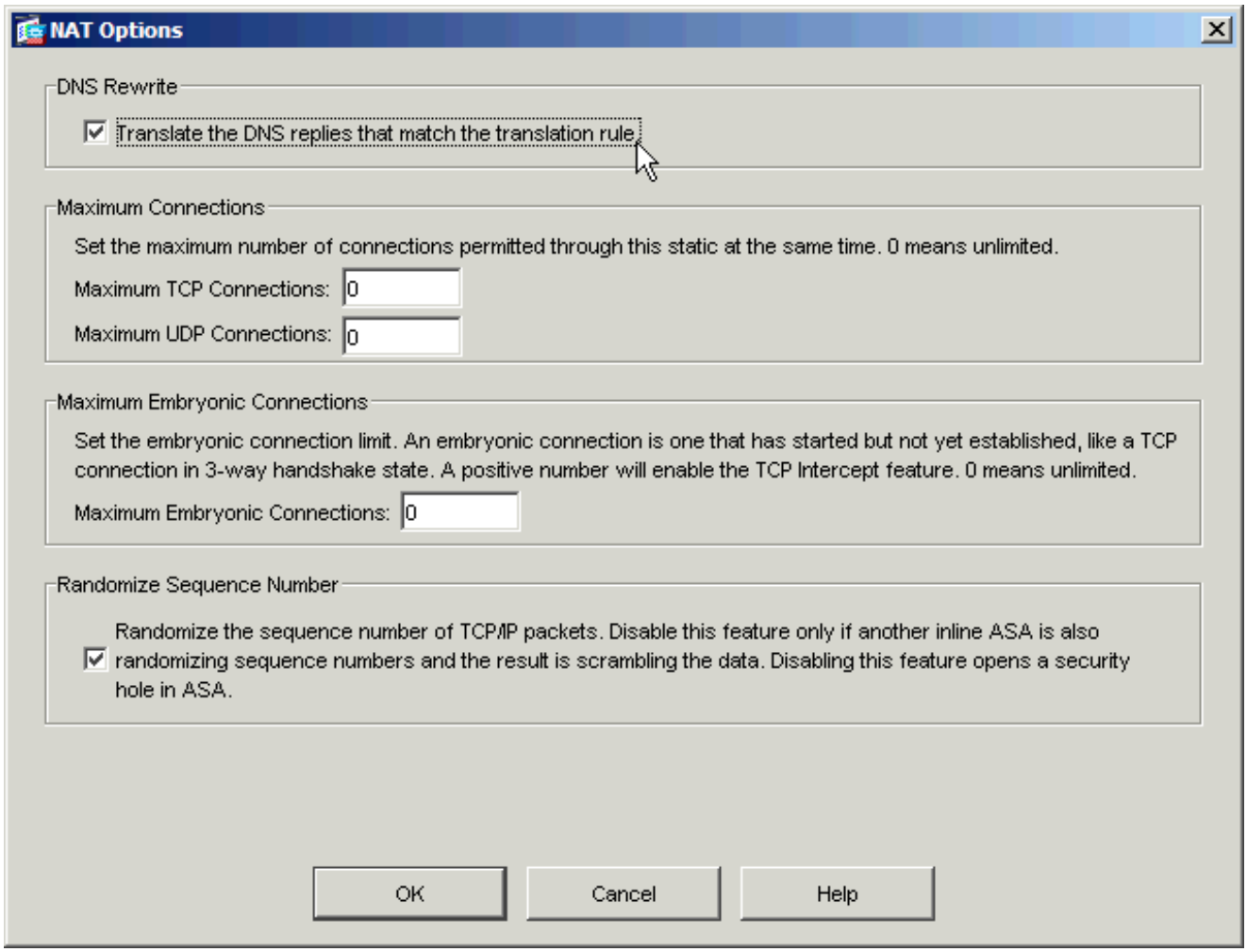
1. Naviguez vers la Configuration > NAT et choisissez que la règle NAT statique doit être modifiée. Cliquez sur Edit.



2. Cliquez surOptions NAT...



3. Sélectionnez la case à cocher Traduire les réponses de DNS qui correspondent à la règle de routage de traduction.



4. Cliquez sur OK pour quitter la fenêtre Options NAT. Cliquez sur OK pour quitter la fenêtre de la règle NAT statique. Cliquez sur Apply pour envoyer votre configuration à l'appliance de sécurité.

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

1. Le client de routage envoie la requête DNS.

<#root>

```
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.

<#root>

```
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.

<#root>

```
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.

```
<#root>

No.     Time      Source          Destination        Protocol Info
2       0.001251

172.22.1.161    192.168.100.2      DNS      Standard query response
                                                          A 192.168.100.10


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: 52985 (52985)
Domain Name System (response)
    [Request In: 1]
    [Time: 0.001251000 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 192.168.100.10
                Name: server.example.com
                Type: A (Host address)
                Class: IN (0x0001)
                Time to live: 1 hour
                Data length: 4
                Addr: 192.168.100.10


    !--- 172.20.1.10 has been rewritten to be 192.168.100.10.
```

5. A ce moment, le client de routage essaie d'accéder au serveur WWW à 192.168.100.10. La connexion réussit. Aucun trafic n'est capturé sur l'ASA car le client et le serveur se trouvent sur le même sous-réseau.

Configuration finale avec le mot clé de « dns »

Il s'agit de la configuration finale de l'ASA pour effectuer le doctoring DNS avec le mot clé dns et deux interfaces NAT.

Configuration finale ASA 7.2(1)
<#root> ciscoasa(config)# **show running-config** : Saved : ASA Version 7.2(1) ! 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
 shutdown
 no nameif
 no security-level
 no ip address
!
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


!--- Simple access-list that permits HTTP access to the mapped !--- address of the WWW server.

pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 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,outside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255 dns


!--- PAT and static NAT configuration. The DNS keyword instructs !--- the security appliance to rewrit


access-group OUTSIDE in interface outside


!--- The Access Control List (ACL) that permits HTTP access !--- to the WWW server is applied to the o

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


!--- DNS inspection map.

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 inspection is enabled using the configured 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:a4a38088109887c3ceb481efab3dcf32
: end
```

Solution alternative : Hairpinning

Hairpinning avec NAT statique

Attention : la reconnexion avec la NAT statique implique l'envoi de tout le trafic entre le client et le serveur WWW via l'appliance de sécurité. Avant de mettre en oeuvre cette solution, prenez soigneusement en compte le volume de trafic attendu et les fonctionnalités de votre appliance de sécurité.

L’épinglage est le processus par lequel le trafic est renvoyé par l’interface sur laquelle il est arrivé. Cette fonctionnalité a été introduite dans la version 7.0 du logiciel du dispositif de sécurité. Pour les versions antérieures à 7.2(1), il est nécessaire de chiffrer au moins une branche du trafic hairpin (entrant ou sortant). À partir de la version 7.2(1), cette exigence n'est plus en vigueur. Le

trafic entrant et le trafic sortant peuvent tous deux être non chiffrés lorsque vous utilisez 7.2(1).

L'épinglage, associé à une instruction NAT statique, peut être utilisé pour obtenir le même effet que le doctoring DNS. Cette méthode ne modifie pas le contenu de l'enregistrement A DNS qui est retourné du serveur DNS au client. Au lieu de cela, quand le hairpinning est utilisé, comme dans le scénario discuté dans ce document, le client peut utiliser l'adresse de 172.20.1.10 qui est retournée par le serveur DNS afin de se connecter.

Voici à quoi ressemble la partie appropriée de la configuration lorsque vous utilisez hairpinning et la NAT statique pour obtenir un effet de doctoring DNS. Les commandes en gras sont expliquées plus en détail à la fin de ce résultat :

<#root>

```
ciscoasa(config)#
```

show run

```
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa
```

!--- Output suppressed.

same-security-traffic permit intra-interface

!--- Enable hairpinning.

```
global (outside) 1 interface
```

!--- Global statement for client access to the Internet.

global (inside) 1 interface

!--- Global statment for hairpinned client access through !--- the security appliance.

```
nat (inside) 1 192.168.100.0 255.255.255.0
```

!--- The NAT statement defines which traffic should be natted. !--- The whole inside subnet in this cas

```
static (inside,outside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255
```

!--- Static NAT statement mapping the WWW server's real address to a !--- public address on the outside

static (inside,inside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255

!--- Static NAT statment mapping requests for the public IP address of !--- the WWW server that appear

- same-security-traffic : cette commande active le trafic du même niveau de sécurité pour le transit de l'appliance de sécurité. Les mots clés permit intra-interface permettent à ce même trafic de sécurité d'entrer et de quitter la même interface, ainsi le hairpinning est activé.

  Remarque : référez-vous à same-security-traffic pour plus d'informations sur hairpinning et la commande same-security-traffic.

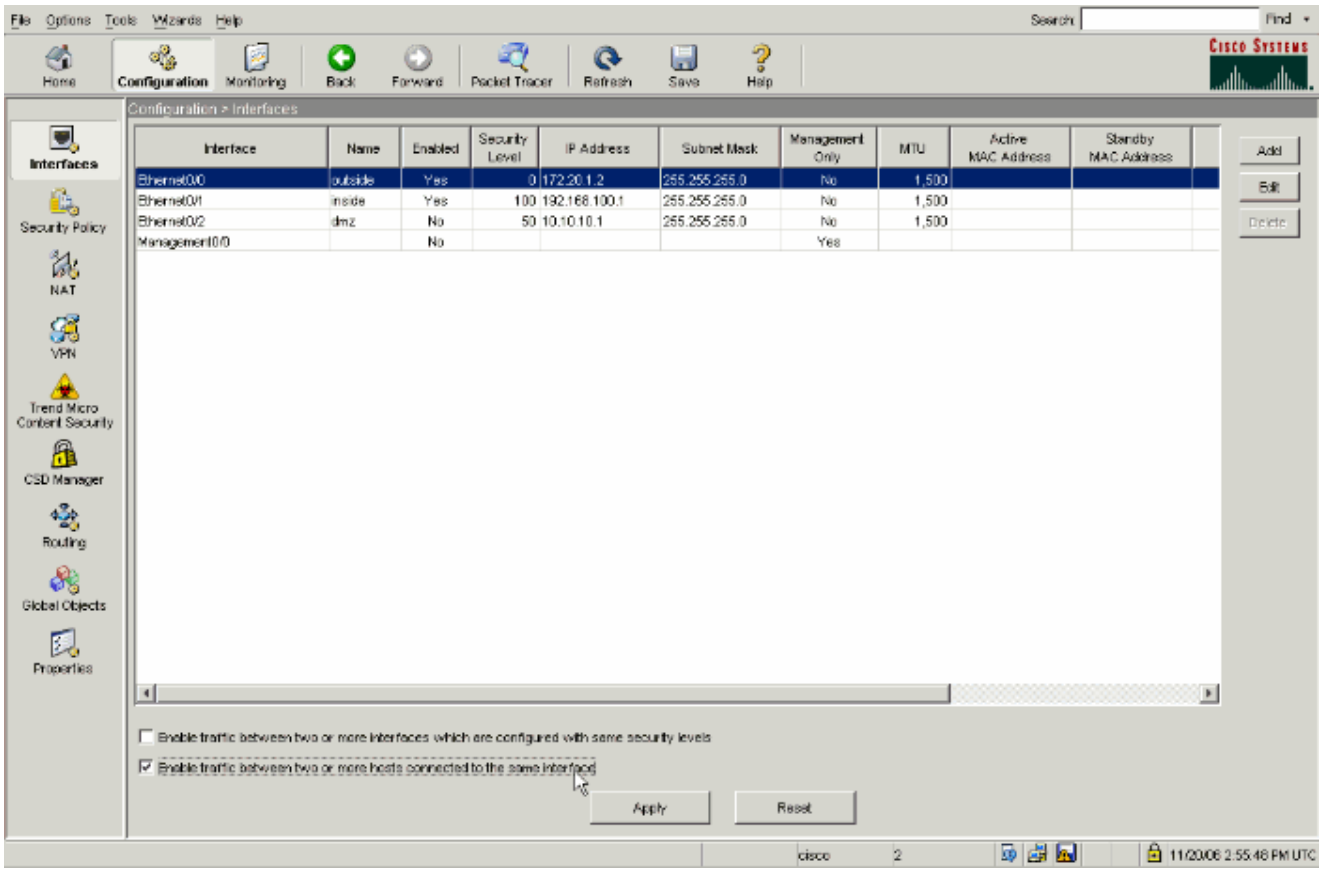
- interface globale (interne) 1 - Tout le trafic qui traverse l'appliance de sécurité doit subir la NAT. Cette commande utilise l'adresse d'interface interne de l'appliance de sécurité afin de permettre au trafic qui entre dans l'interface interne de subir la PAT pendant qu'il est reconnecté à l'interface interne.

- static (inside,inside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255 : cette entrée NAT statique crée un second mappage pour l'adresse IP publique du serveur WWW. Cependant, contrairement à la première entrée NAT statique, cette fois l'adresse 172.20.1.10 est mappée à l'interface interne de l'appliance de sécurité. Cela permet à l'appliance de sécurité de répondre aux requêtes qu'elle voit pour cette adresse sur l'interface interne. Ensuite, il redirige ces requêtes vers l'adresse réelle du serveur WWW via lui-même.

Complétez ces étapes afin de configurer la reconnexion avec la NAT statique dans l'ASDM :

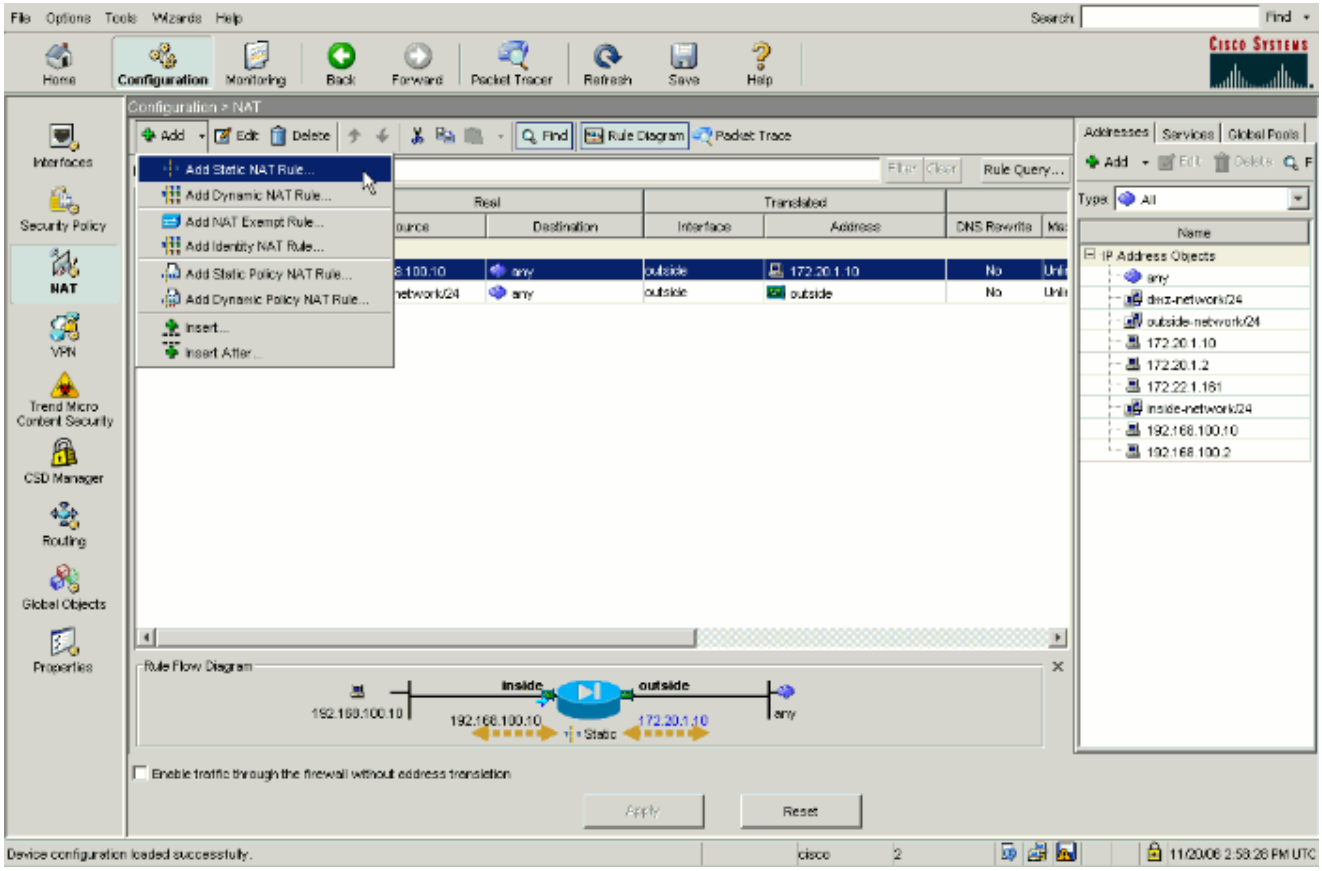
1. Accédez à Configuration > Interfaces.

2. Au bas de la fenêtre, cochez la case Enable traffic between two or more hosts connected to the same interface.



3. Cliquez sur Apply.

4. Naviguez vers la Configuration > NAT et choisissez Add > Add Static NAT Rule....

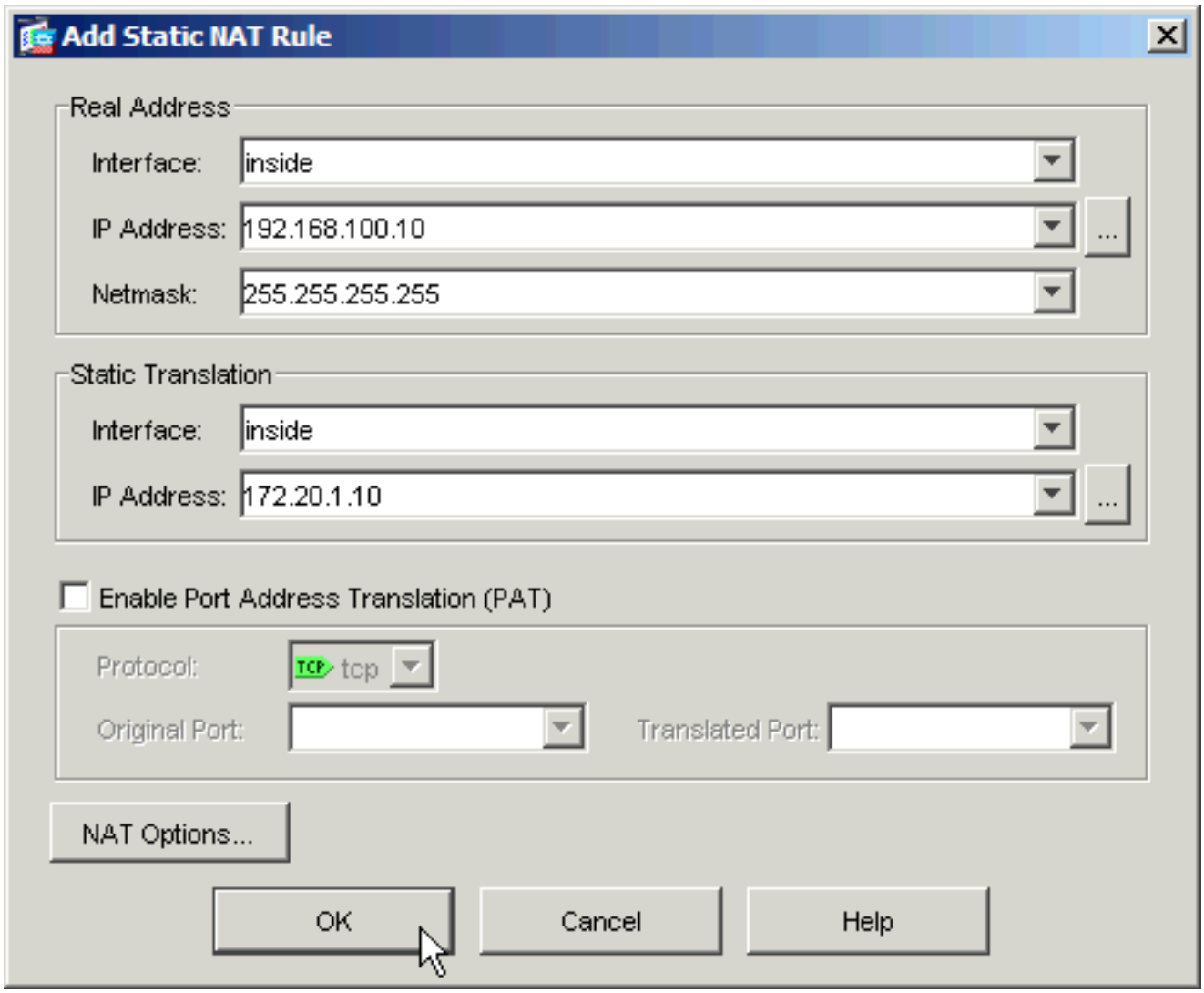


5. Complétez la configuration pour la nouveau routage de traduction statique.

    a. Remplissez la zone Véritable adresse avec les informations du serveur WWW.

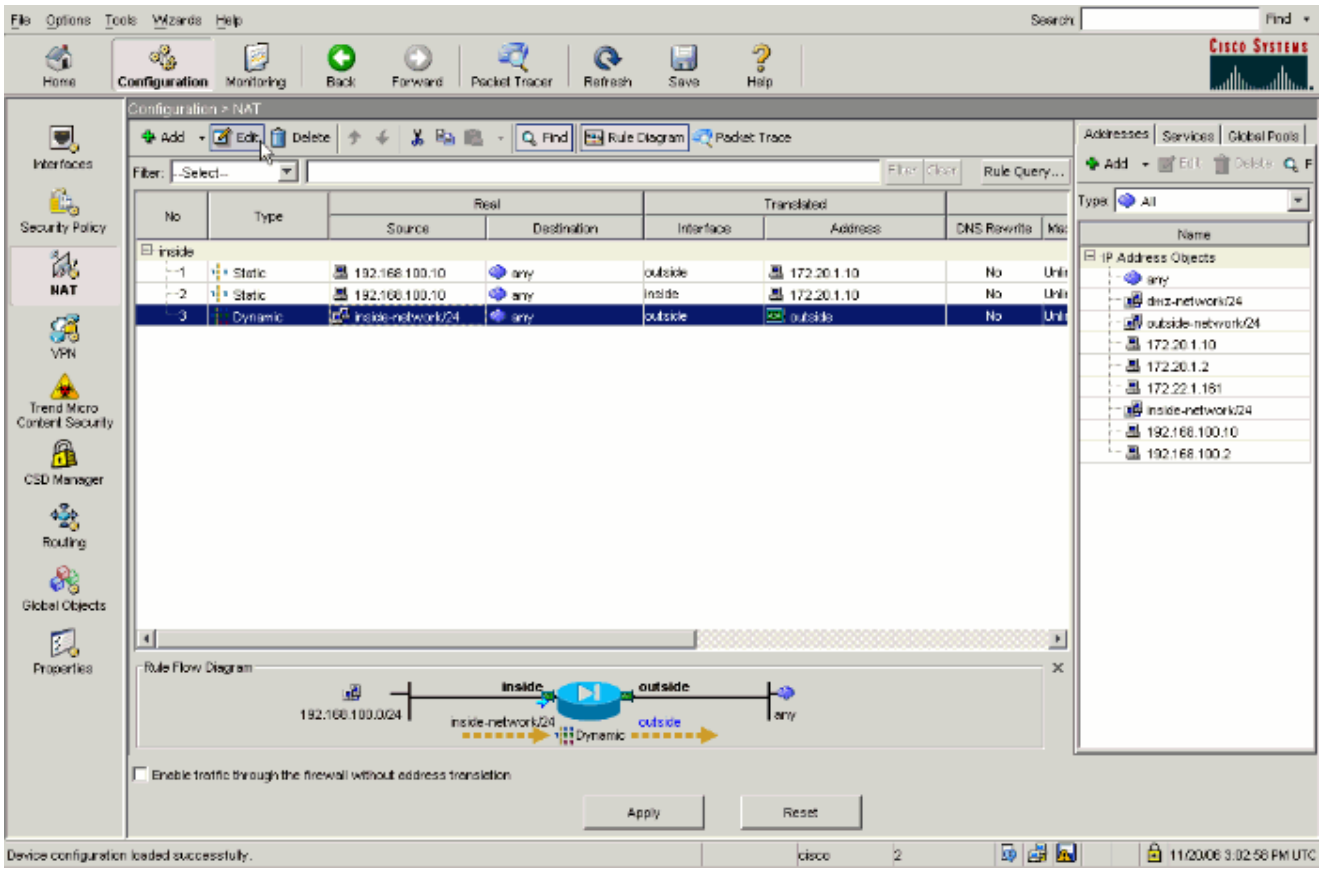
    b. Remplissez la zone Routage de traduction statique avec l'adresse et l'interface que vous souhaitez mapper au serveur WWW.

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.

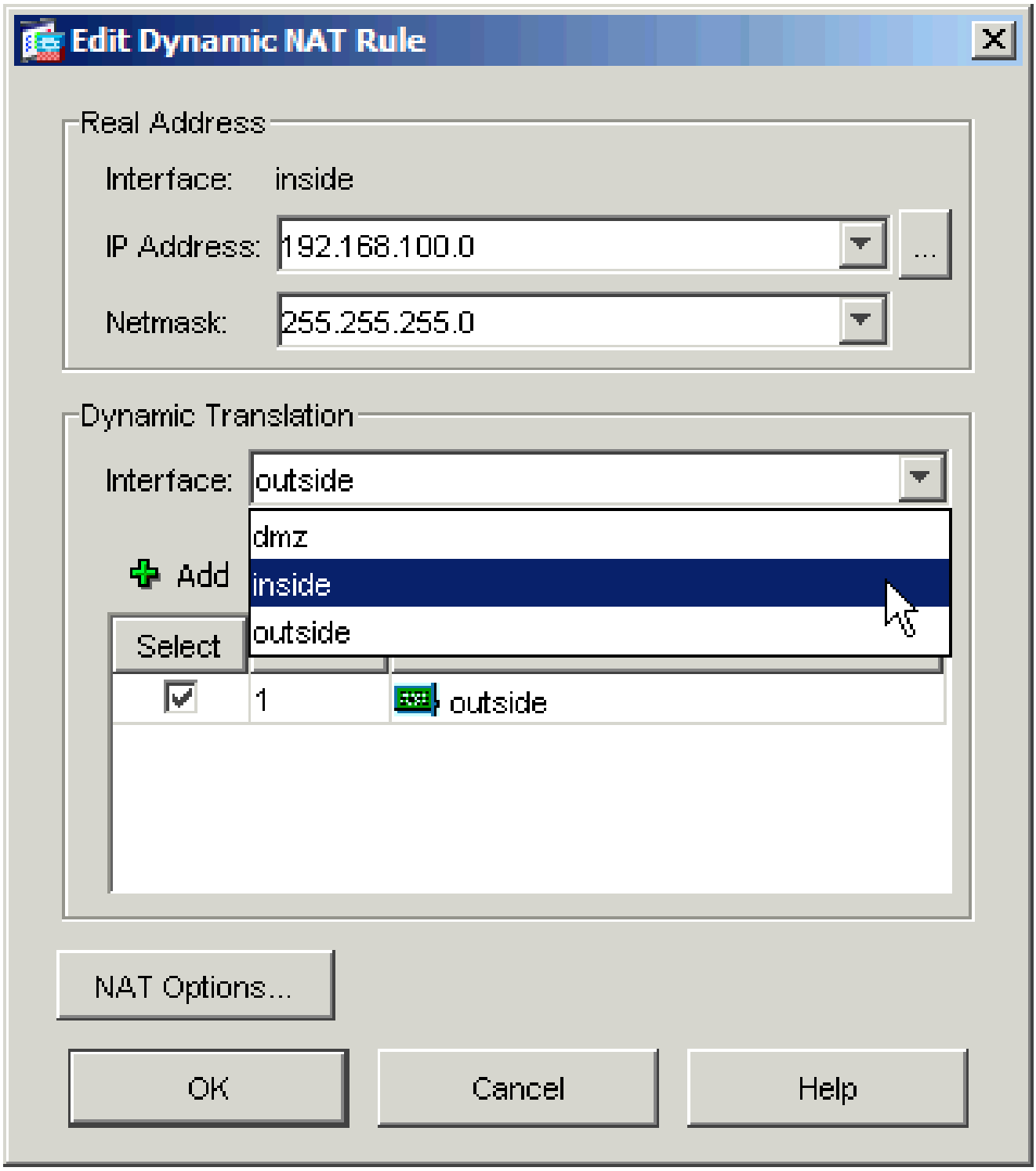


6. Cliquez surOK pour quitter la fenêtre Ajouter la règle NAT statique.

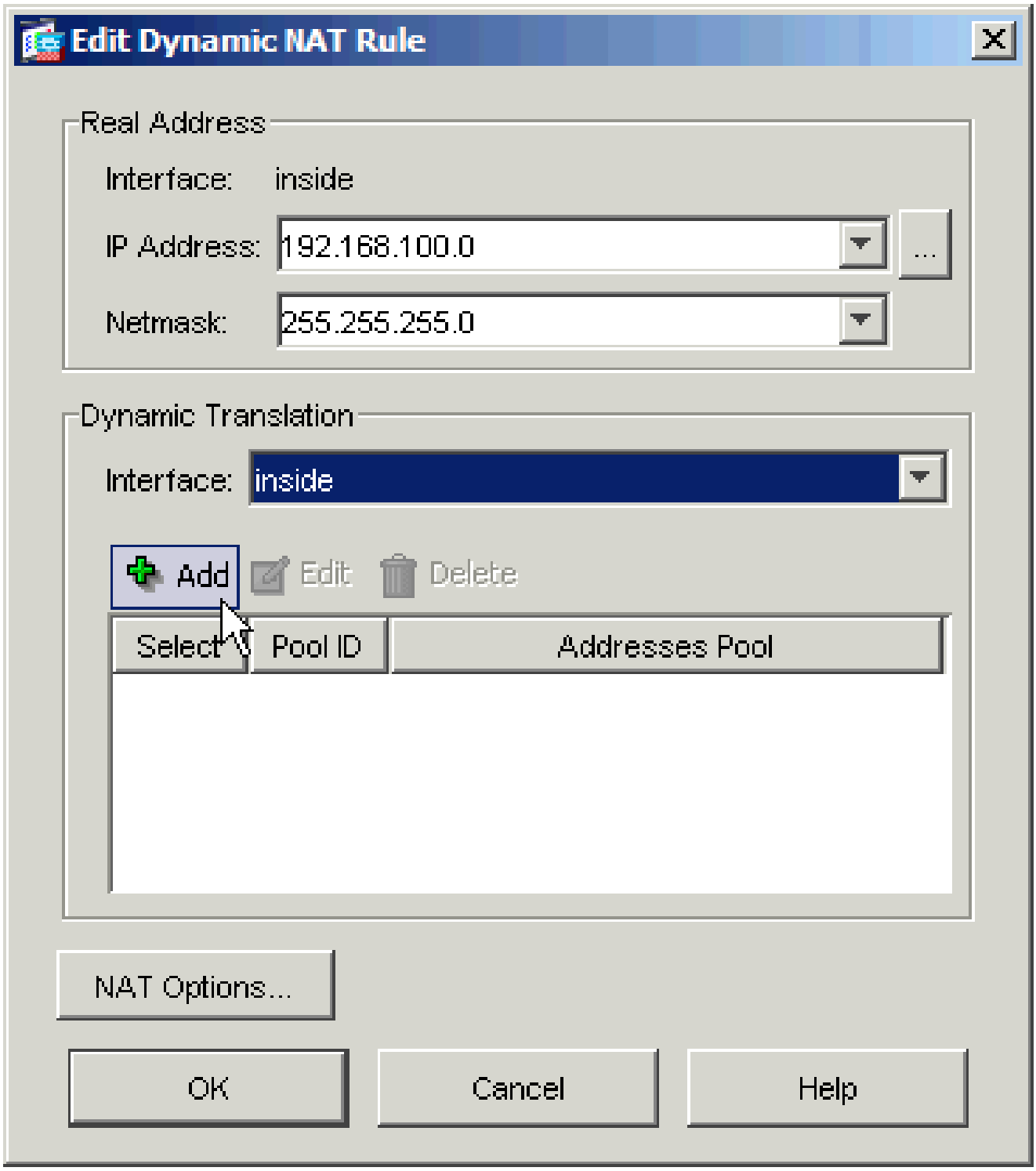
7. Choisissez la traduction PAT dynamique existante et cliquez sur Edit.



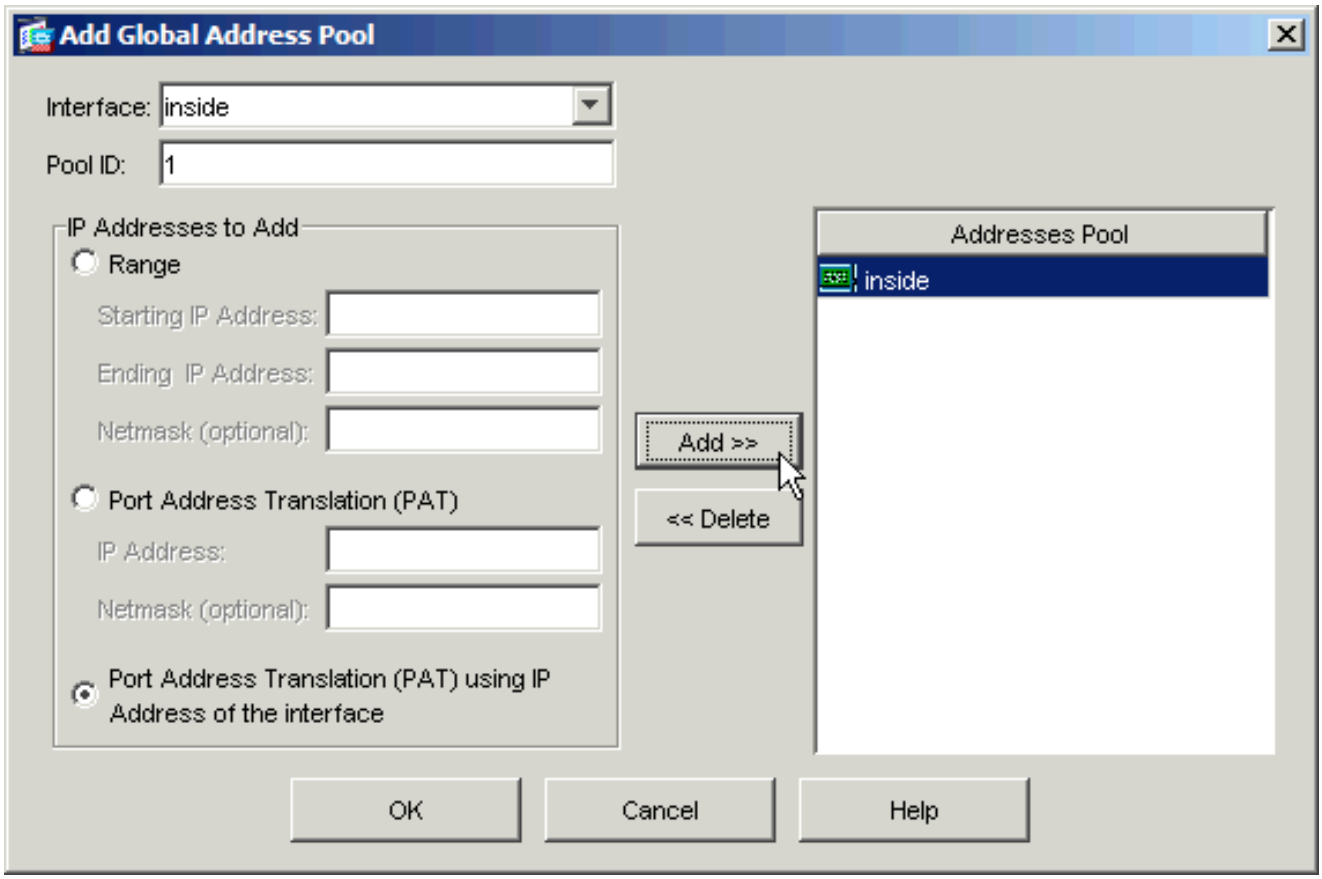
8. Choisissez inside dans la liste déroulante Interface.



9. Cliquez sur Add.



10. Sélectionnez la case d'option Port Address Translation (PAT) utilisant l'adresse IP de l'interface. Cliquez sur Add.



11. Cliquez sur OK pour quitter la fenêtre Ajouter un pool d'adresses globales. Cliquez sur OK pour quitter la fenêtre Edit Dynamic NAT Rule. Cliquez sur Apply pour envoyer votre configuration à l'appliance de sécurité.

Voici la séquence des événements qui se produisent lorsque la reconnexion 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 voit la requête et reconnaît que le serveur WWW se trouve à l'adresse 192.168.100.10.

```
%ASA-7-609001: Built local-host inside:192.168.100.10
```

3. L'appliance de sécurité crée une traduction PAT dynamique pour le client. La source du trafic client est désormais l'interface interne de l'appliance de sécurité : 192.168.100.1.

<#root>

```
%ASA-6-305011: Built dynamic TCP translation from inside:192.168.100.2/11012 to
inside:
```

192.168.100.1/1026

4. L'appliance de sécurité crée une connexion TCP entre le client et le serveur WWW via elle-même. Notez les adresses mappées de chaque hôte entre parenthèses.

<#root>

```
%ASA-6-302013: Built inbound TCP connection 67399 for inside:192.168.100.2/11012
```

(192.168.100.1/1026)

```
 to inside:192.168.100.10/80
```

(172.20.1.10/80)

5. 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.

<#root>

```
ciscoasa(config)#
```

show xlate

```
3 in use, 9 most used
Global 172.20.1.10 Local 192.168.100.10
Global 172.20.1.10 Local 192.168.100.10
```

PAT Global 192.168.100.1(1027) Local 192.168.100.2(11013)

6. La commande show conn sur l'appliance de sécurité vérifie que la connexion a réussi entre l'appliance de sécurité et le serveur WWW au nom du client. Notez l'adresse réelle du client entre parenthèses.

<#root>

```
ciscoasa#
```

show conn

```
TCP out 192.168.100.1
```

(192.168.100.2)

```
:11019 in 192.168.100.10:80
idle 0:00:03 bytes 1120 flags UIOB
```

Configuration finale avec Hairpinning et NAT statique

Il s'agit de la configuration finale de l'ASA qui utilise la reconnexion et la NAT statique pour obtenir un effet de doctoring DNS avec deux interfaces NAT.

Configuration finale ASA 7

<#root>

```
ciscoasa(config-if)#
show running-config

: Saved
:
ASA Version 7.2(1)
!
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
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
 management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
same-security-traffic permit intra-interface
access-list OUTSIDE extended permit tcp any host 172.20.1.10 eq www

!--- Simple access-list that permits HTTP access to the mapped !--- address of the WWW server.

pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
```

```
mtu inside 1500
asdm image disk0:/asdm512-k8.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface

!--- Global statement for client access to the Internet.

global (inside) 1 interface

!--- Global statment for hairpinned client access through !--- the security appliance.

nat (inside) 1 192.168.100.0 255.255.255.0

!--- The NAT statement defines which traffic should be natted. !--- The whole inside subnet in this ca

static (inside,outside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255

!--- Static NAT statement mapping the WWW server's real address to a public !--- address on the outsid

static (inside,inside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255

!--- Static NAT statement mapping requests for the public IP address of the !--- WWW server that appea

access-group OUTSIDE in interface outside

!--- The ACL that permits HTTP access to the WWW server is applied !--- to the outside interface.

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:7c9b4e3aff085ba90ee194e079111e1d
: end
```

Remarque : reportez-vous à cette vidéo, Épinglage des cheveux sur Cisco ASA (clients enregistrés uniquement) , pour plus d'informations sur les différents scénarios où l'épinglage des cheveux pourrait être utilisé.

Configurez l'inspection de DNS

Afin d'activer l'inspection DNS (si elle a été précédemment désactivée), effectuez ces étapes. 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. Consultez Utilisation d'un cadre de stratégie modulaire pour plus d'informations sur les stratégies et l'inspection des services.

1. Créez une carte de stratégie d'inspection pour le DNS.

   <#root>

   ciscoasa(config)#

   policy-map type inspect dns MY_DNS_INSPECT_MAP

2. A partir du mode de configuration de la carte de stratégie, entrez le mode de configuration de paramètre pour spécifier les paramètres pour le moteur d'inspection.

   <#root>

   ciscoasa(config-pmap)#

   parameters

3. En mode de configuration de paramètre de carte de stratégie, spécifiez la longueur maximum du message pour que les messages de DNS soient 512.

<#root>

```
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.

<#root>

```
ciscoasa(config-pmap-p)#
```

exit

```
ciscoasa(config-pmap)#
```

exit

5. Confirmez que la carte de stratégie d'inspection a été créée comme souhaité.

<#root>

```
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.

<#root>

```
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.

<#root>

```
ciscoasa(config-pmap)#
```

class inspection_default

```
ciscoasa(config-pmap-c)#
```

8. Dans le mode de configuration de la classe de carte de stratégie, spécifiez que le DNS devrait être inspecté en utilisant la carte de la stratégie d'inspection créée dans les étapes 1-3.

<#root>

```
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.

<#root>

```
ciscoasa(config-pmap-c)#
```

exit

```
ciscoasa(config-pmap)#
```

exit

10. Vérifiez que la carte de stratégie global_policy est configurée comme souhaité.

<#root>

```
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.

<#root>

```
ciscoasa(config)#

show run service-policy

service-policy global_policy global
```

Configuration du DNS fractionné

Émettez la commande split-dns en mode de configuration group-policy afin d'entrer une liste de domaines à résoudre par le biais du tunnel partagé. Utilisez non de cette commande afin de supprimer une liste.

En l'absence de listes de domaines de transmission tunnel partagée, les utilisateurs héritent de celles qui existent dans la stratégie de groupe par défaut. Émettez la commande split-dns none afin d'empêcher l'héritage des listes de domaines de transmission tunnel partagée.

Utilisez un espace unique afin de séparer chaque entrée dans la liste des domaines. Le nombre d'entrées est illimité, mais la chaîne entière ne peut pas comporter plus de 255 caractères. Vous ne pouvez utiliser que des caractères alphanumériques, des tirets (-) et des points (.). La commande no split-dns, lorsqu'elle est utilisée sans arguments, supprime toutes les valeurs actuelles, qui incluent une valeur Null créée lorsque vous émettez la commande split-dns none.

Cet exemple montre comment configurer les domaines Domain1, Domain2, Domain3 et Domain4 afin d'être résolus par la transmission tunnel partagée pour la stratégie de groupe nommée FirstGroup :

<#root>

```
hostname(config)#
group-policy FirstGroup attributes
hostname(config-group-policy)#
split-dns value Domain1 Domain2 Domain3 Domain4
```

Vérifier

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 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 la ou les instances de capture :

<#root>

```
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 la ou les captures.

   Voici ce à quoi ressemble l'exemple de capture après qu'une partie du trafic DNS a été passée:

<#root>

```
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 la ou les captures sur un serveur TFTP au format pcap pour les analyser dans une autre application.

   Les applications qui peuvent analyser le format pcap peuvent afficher des détails supplémentaires tels que le nom et l'adresse IP dans les enregistrements A DNS.

<#root>

```
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. Consultez la partie Configuration de l'inspection de DNS.

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 dmz:10.10.10.10/23
```

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

Supprimer la réponse DNS UDP

Il est possible que vous receviez ce message d'erreur en raison de la suppression de paquets DNS :

```
 %PIX|ASA-4-410001: UDP DNS request from source_interface:source_address/source_port
to dest_interface:dest_address/dest_port; (label length | domain-name length)
52 bytes exceeds remaining packet length of 44 bytes.
```

Augmentez la longueur du paquet DNS entre 512-65535 afin de résoudre ce problème.

Exemple :

```
<#root>
ciscoasa(config)#
policy-map type inspect dns MY_DNS_INSPECT_MAP

ciscoasa(config-pmap)#
parameters

ciscoasa(config-pmap-p)#
message-length maximum <512-65535>
```

Informations connexes

- Logiciels pare-feu Cisco PIX
- Références des commandes du pare-feu Cisco Secure PIX
- Notes de champ du produit de sécurité
- Request For Comments (RFC)
- Épinglage des cheveux sur Cisco ASA
- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.