PIX/ASA : Exemple de configuration de DNS Doctoring avec la commande static et deux interfaces NAT

Contenu

Introduction

Ce document fournit une configuration d'échantillon pour exécuter le Système de noms de domaine (DNS) soignant sur l'appliance de sécurité adaptable de la gamme ASA 5500 ou l'appliance de Sécurité de gamme 500 PIX utilisant des déclarations (NAT) de traduction d'adresses de réseau statique. 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 dans ce document contient deux interfaces NAT ; à l'intérieur et dehors. Pour un exemple des DN soignant avec la statique et trois interfaces NAT (à l'intérieur, extérieur et dmz), référez-vous à PIX/ASA : Exécutez le DNS Doctoring avec l'exemple statique de commande et de configuration de trois interfaces NAT.

Référez-vous à PIX/ASA 7.x NAT et TAPOTEZ les déclarations et utilisation nat, globales, statiques, le conduit, et les commandes access-list et le Port Redirection(Forwarding) sur PIX pour plus d'informations sur la façon utiliser NAT sur des dispositifs de sécurité.

Conditions préalables

Conditions requises

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. S'il a été arrêté, voyez la section d'inspection de DN de configurer plus tard dans ce document pour le 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 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 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 lancez la commande **inspect dns** sans l'option de longueur maximum, la taille du 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.

Composants utilisés

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

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 la gamme Cisco PIX 500, version 6.2 ou ultérieures.

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

Conventions

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

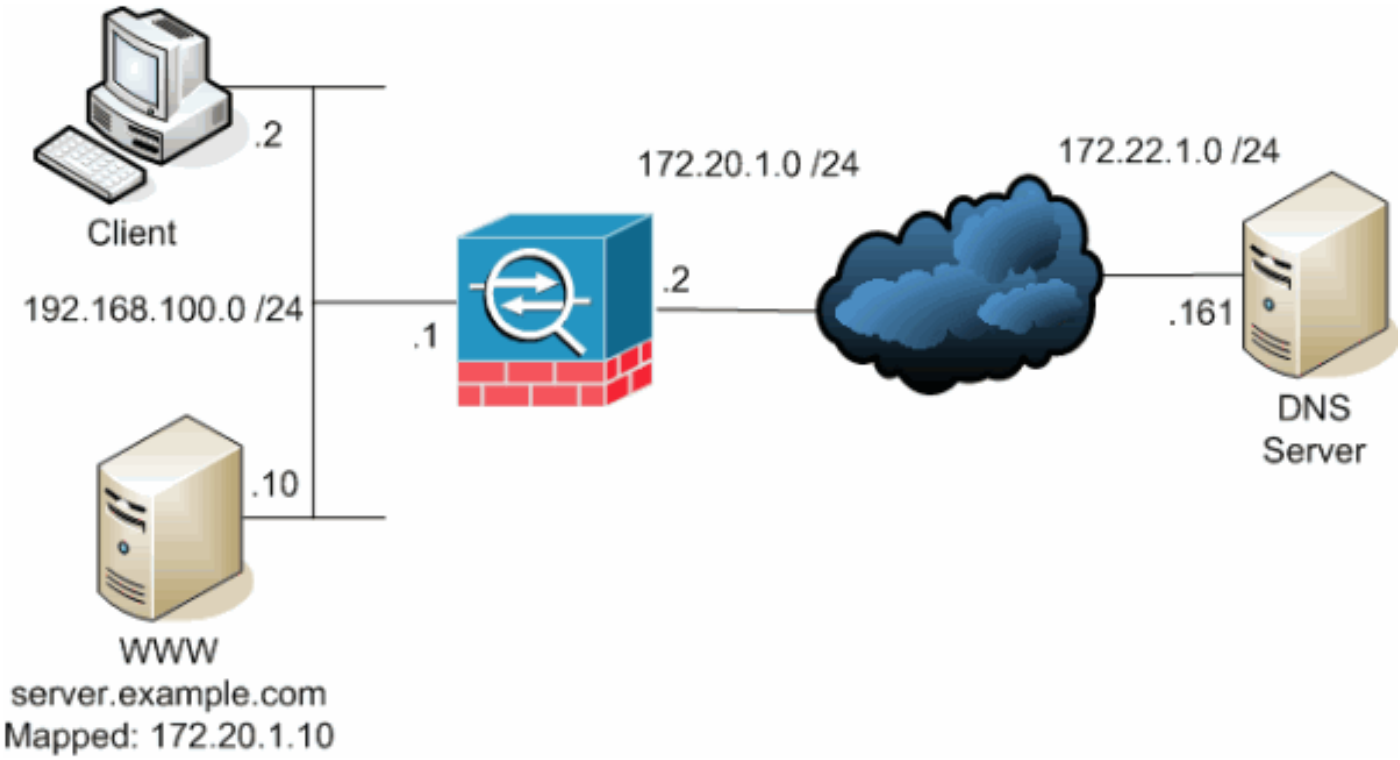
Informations générales

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 (à l'intérieur, dehors)

Topologie

Dans ce scénario, le client et le serveur de WWW que le client essaye 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.



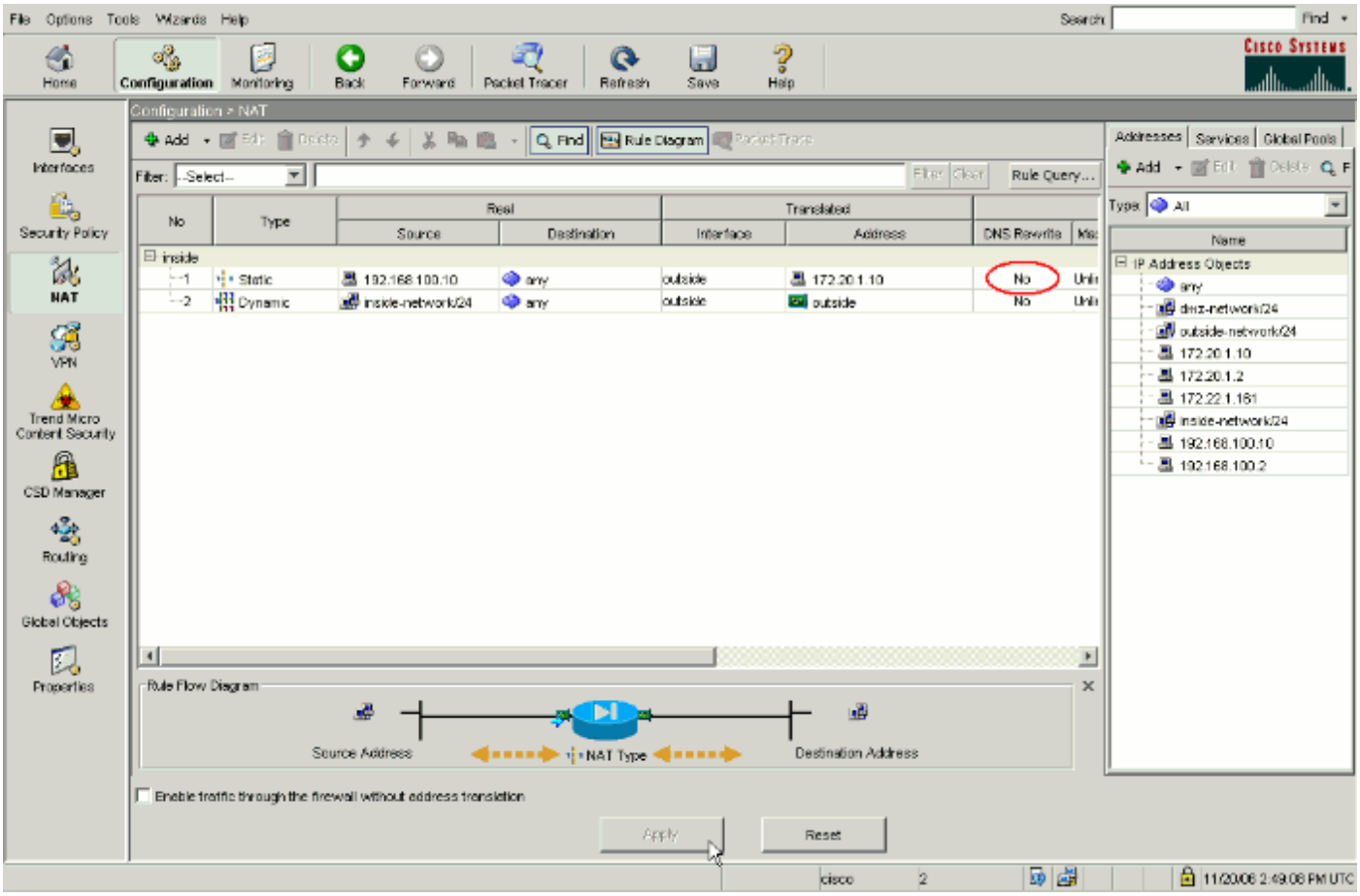
Ce schéma illustre cette situation. Dans ce cas, le client chez 192.168.100.2 veut employer l'URL de **server.example.com** pour accéder au serveur de WWW chez 192.168.100.10. Les services DNS pour le client sont fournis par le serveur DNS externe à l'adresse 172.22.1.161. Puisque le serveur DNS est 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 de routage 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 reçoit un Un-enregistrement qui contient l'annonce publique tracée : 172.20.1.10 du serveur de 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:

```
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.`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. 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, parce qu'il ne permet pas au trafic pour circuler de l'intérieur à l'externe vers interne, les temps de connexion. 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 »

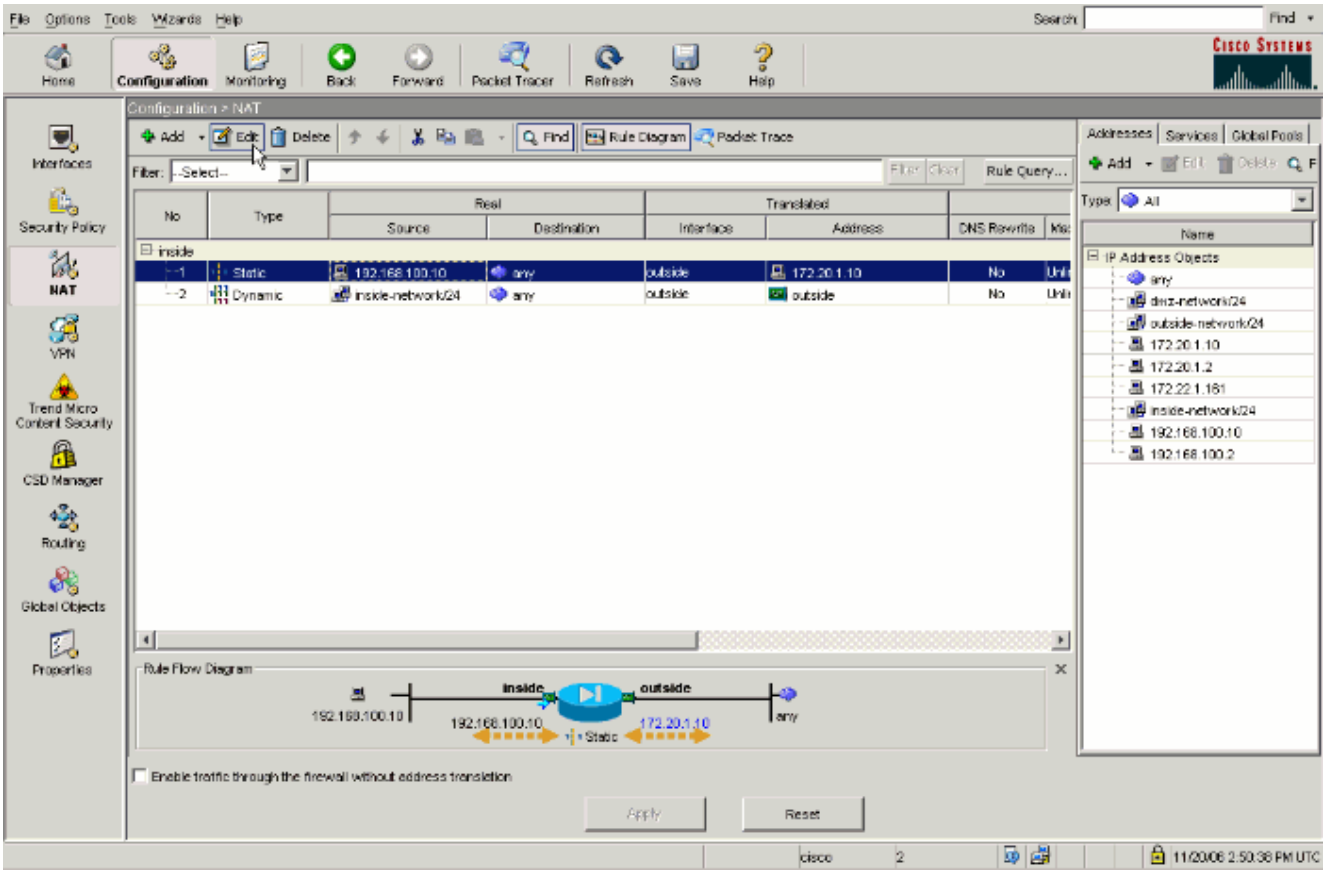
Doctoring DNS avec le mot clé « dns »

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 correctement configurée, l'appliance de sécurité peut modifier l'enregistrement A pour autoriser le client de routage dans un scénario comme celui évoqué dans le problème de routage : Le client de routage ne peut pas accéder à la partie Serveur WWW pour se connecter. Dans cette situation, avec soigner de DN activé, les dispositifs de sécurité réécrivent l'Un-enregistrement pour diriger le client 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:

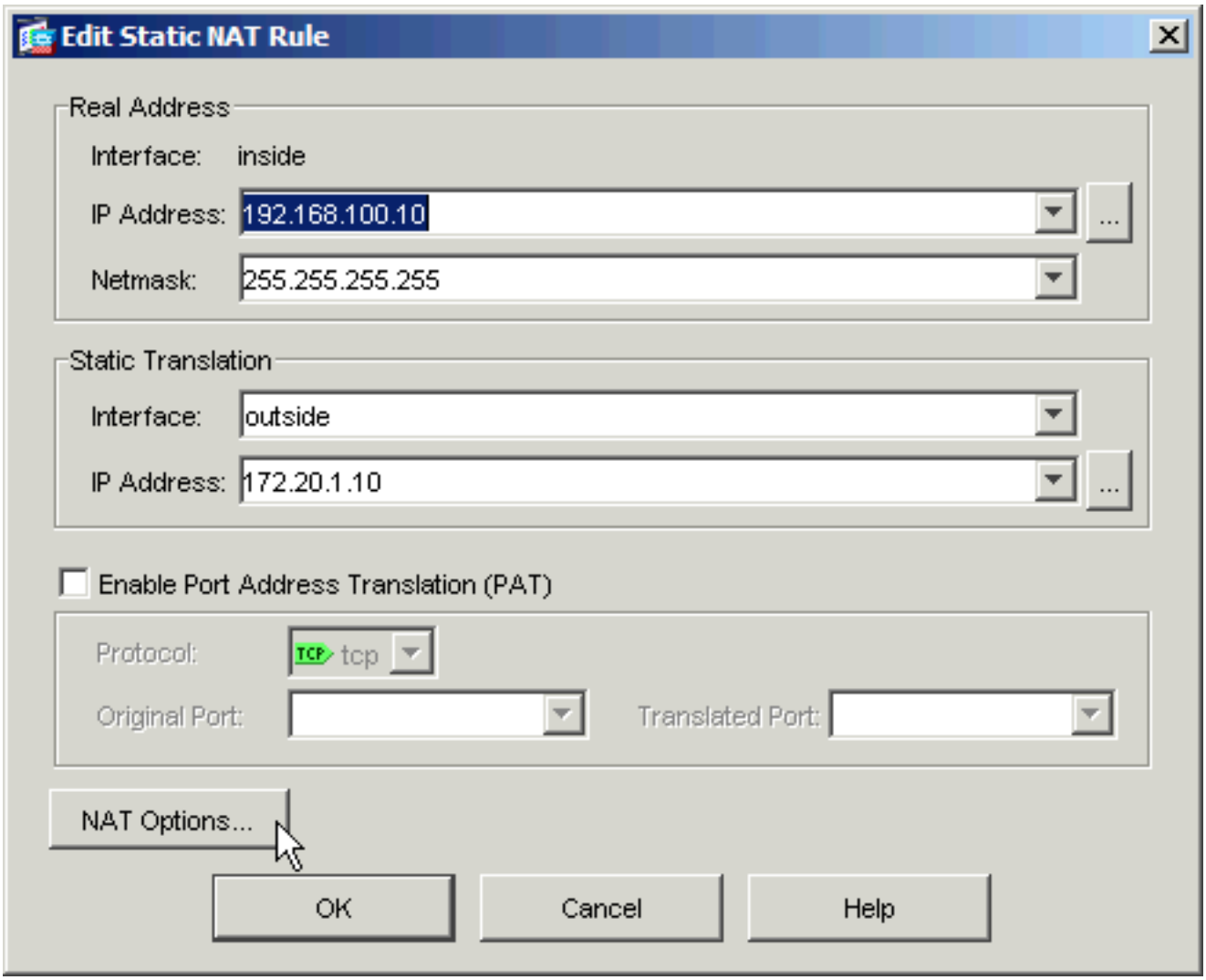
```
ciscoasa(config)#show run : Saved : ASA Version 7.2(1) ! hostname ciscoasa !--- Output
suppressed. access-list OUTSIDE extended permit tcp any host 172.20.1.10 eq www !--- Output
suppressed. global (outside) 1 interface nat (inside) 1 192.168.100.0 255.255.255.0 static
(inside,outside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255 dns !--- The "dns" keyword
is added to instruct the security appliance to modify !--- DNS records related to this entry.
access-group OUTSIDE in interface outside !--- Output suppressed.
```

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

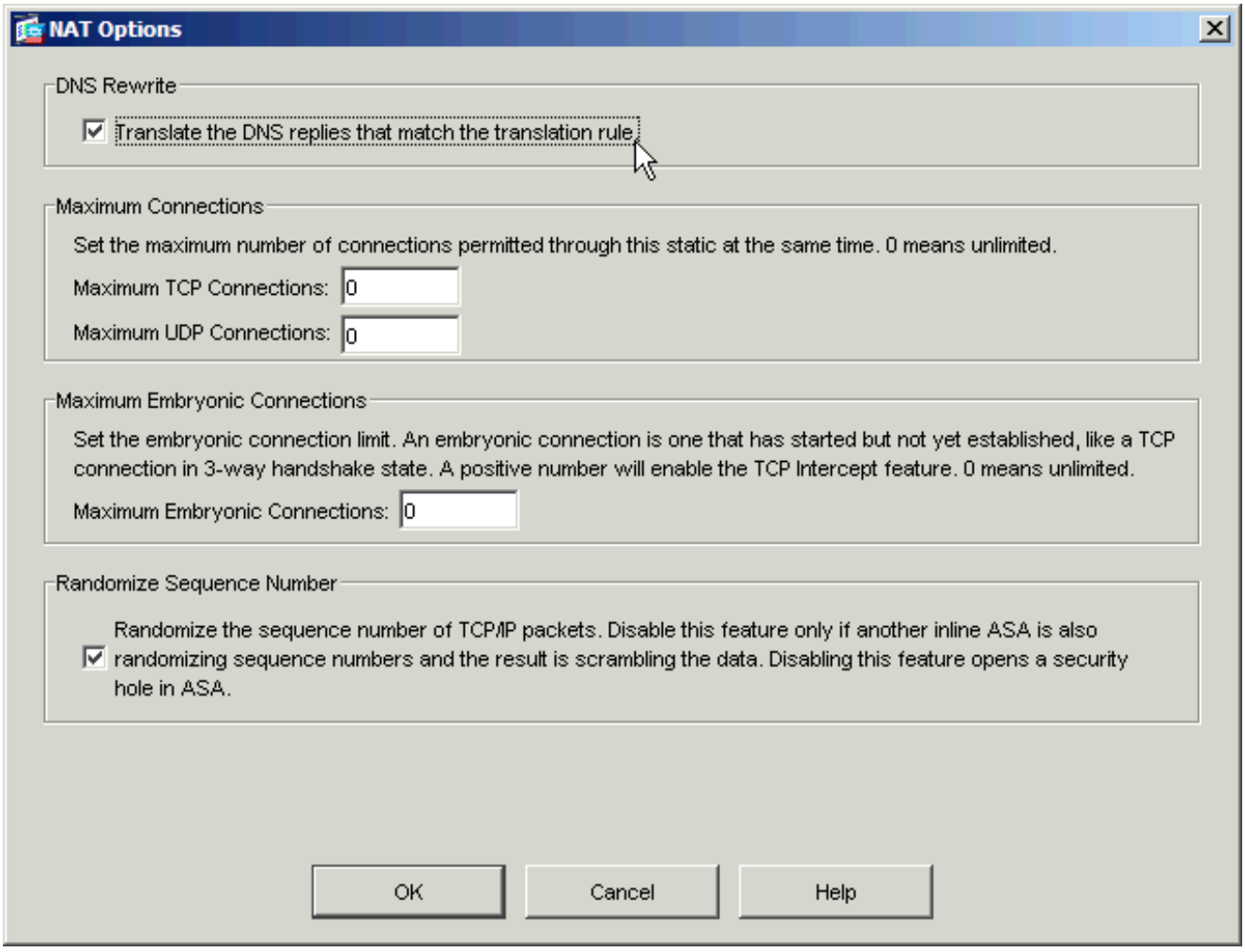
1. Naviguez vers la **Configuration > NAT** et choisissez que la règle NAT statique doit être modifiée. Cliquez sur
Edit.



2. Cliquez sur**Options 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.`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
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. En ce moment, les essais de client pour accéder au serveur de WWW chez 192.168.100.10. La connexion réussit. Aucun trafic n'est capturé sur l'ASA parce que le client et serveur sont sur le même sous-réseau.

Configuration finale avec le mot clé de « dns »

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

Configuration finale ASA 7.2(1)

```
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 rewrite DNS records related to
this entry. access-group OUTSIDE in interface outside !-
-- The Access Control List (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 !--- 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 : Le hairpinning avec NAT statique implique d'envoyer tout le trafic entre le client et le serveur de WWW par les dispositifs de sécurité. Considérez soigneusement le niveau de trafic prévu et les capacités de vos dispositifs de sécurité avant que vous implémentiez cette solution.

Le hairpinning est le processus par lequel le trafic est envoyé soutiennent la même interface sur laquelle il est arrivé. Cette caractéristique a été introduite dans la version de logiciel 7.0 d'appareils de Sécurité. Pour des versions plus tôt que 7.2(1), on l'exige qu'au moins un bras du trafic hairpinned (d'arrivée ou sortant) soit chiffré. De 7.2(1) et plus tard, cette condition requise n'est plus en place. Le trafic d'arrivée et le trafic sortant pourraient être décryptés quand vous l'utilisation 7.2(1).

Le hairpinning, en même temps qu'une déclaration NAT statique, peut être utilisé pour réaliser le même effet que soigner de DN. Cette méthode ne change pas le contenu du l'Un-enregistrement de DN 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 connecter.

Voici ce qui ressemble à la partie appropriée de la configuration quand vous employez le hairpinning et NAT statique pour réaliser des DN soignant l'effet. Les commandes en gras sont expliquées plus en détail à l'extrémité de cette sortie :

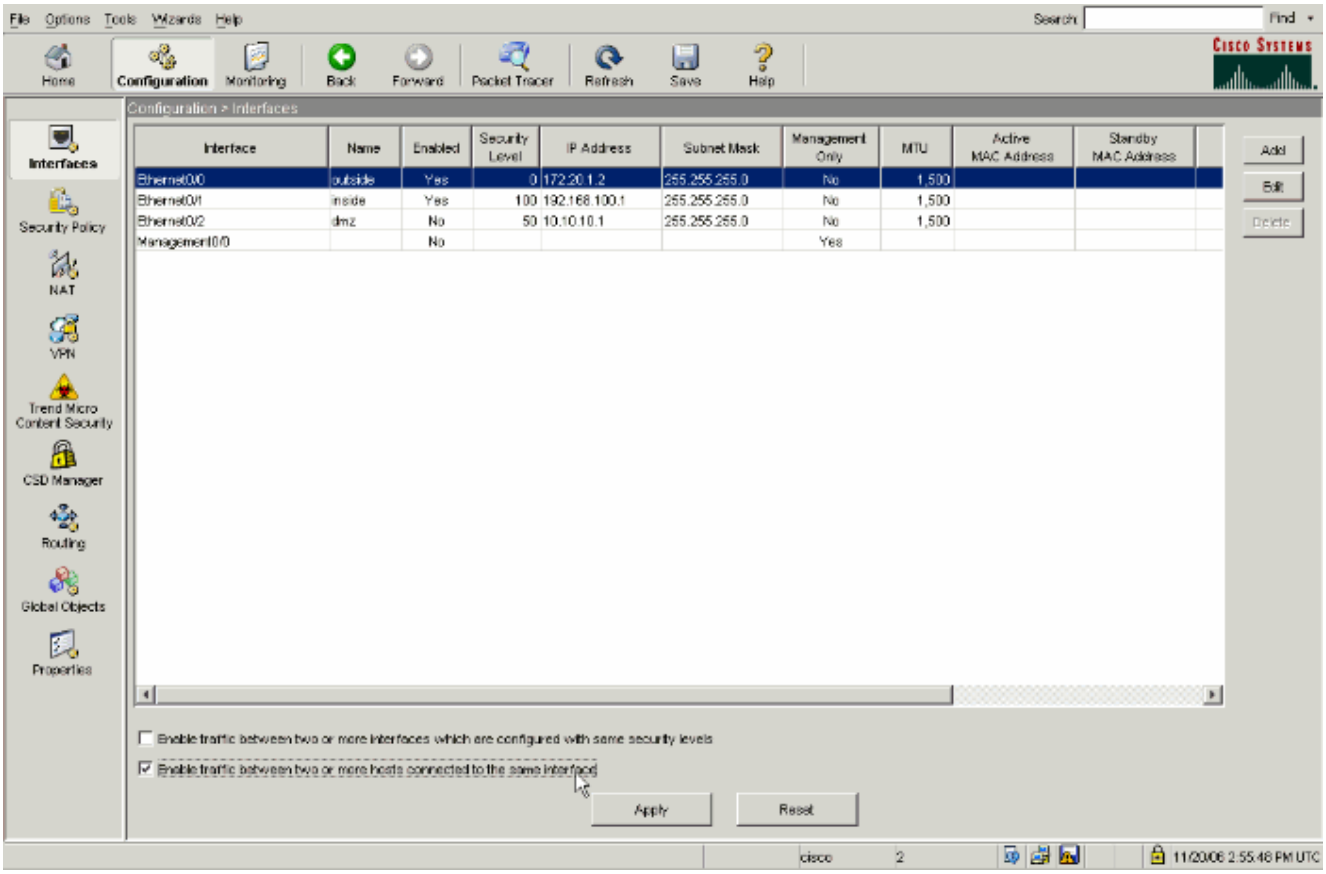
```
ciscoasa(config)#show run : Saved : ASA Version 7.2(1) ! hostname ciscoasa !--- Output
suppressed. same-security-traffic permit intra-interface !--- Enable hairpinning. global
(outside) 1 interface !--- Global statement for client access to the Internet. global (inside) 1
```

```
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 case. 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 interface. 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 on the inside interface to the WWW server's !---
real address of 192.168.100.10.
```

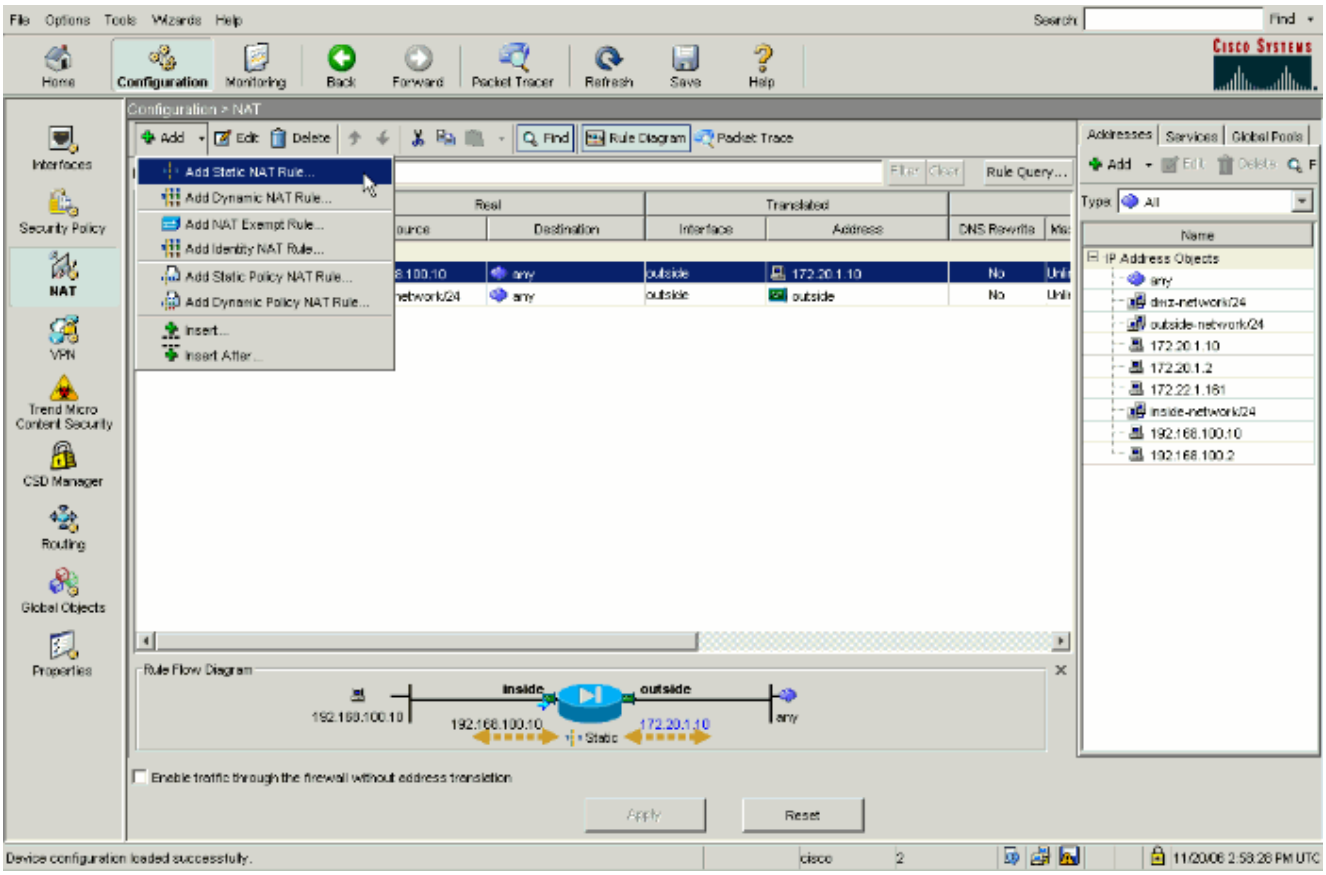
- **le même-Sécurité-trafic** — Ce trafic de commandes enables du même niveau de Sécurité pour transiter les dispositifs de sécurité. Les mots clé **intra-interface d'autorisation** admettent que le même-Sécurité-trafic pour écrire et partir de la même interface, ainsi le hairpinning est activé.**Remarque:** Référez-vous au même-Sécurité-trafic pour plus d'informations sur le hairpinning et la commande du même-Sécurité-**trafic**.
- **(à l'intérieur) 1 interface globale** — Tout le trafic qui croise les dispositifs de sécurité doit subir NAT. Cette commande emploie l'adresse d'interface interne des dispositifs de sécurité afin d'activer le trafic qui écrit l'interface interne pour subir PAT pendant qu'elle hairpinned soutiennent l'interface interne.
- **(à l'intérieur, à l'intérieur) netmask statique 255.255.255.255 de 172.20.1.10 192.168.100.10** — cette entrée NAT statique crée un deuxième mappage pour l'adresse IP publique du serveur de WWW. Cependant, à la différence de la première entrée NAT statique, cette fois l'adresse 172.20.1.10 est tracée à l'interface interne des dispositifs de sécurité. Ceci permet aux dispositifs de sécurité pour répondre aux demandes qu'ils voient pour cette adresse sur l'interface interne. Puis, il réoriente ces demandes à la vraie adresse du serveur de WWW par lui-même.

Terminez-vous ces étapes afin de configurer le hairpinning avec NAT statique dans l'ASDM :

1. Naviguez vers le **Configuration > Interfaces**.
2. Au bas de la fenêtre, cochez le **trafic d'enable entre deux hôtes ou plus connectés dans la même** case d'**interface**.

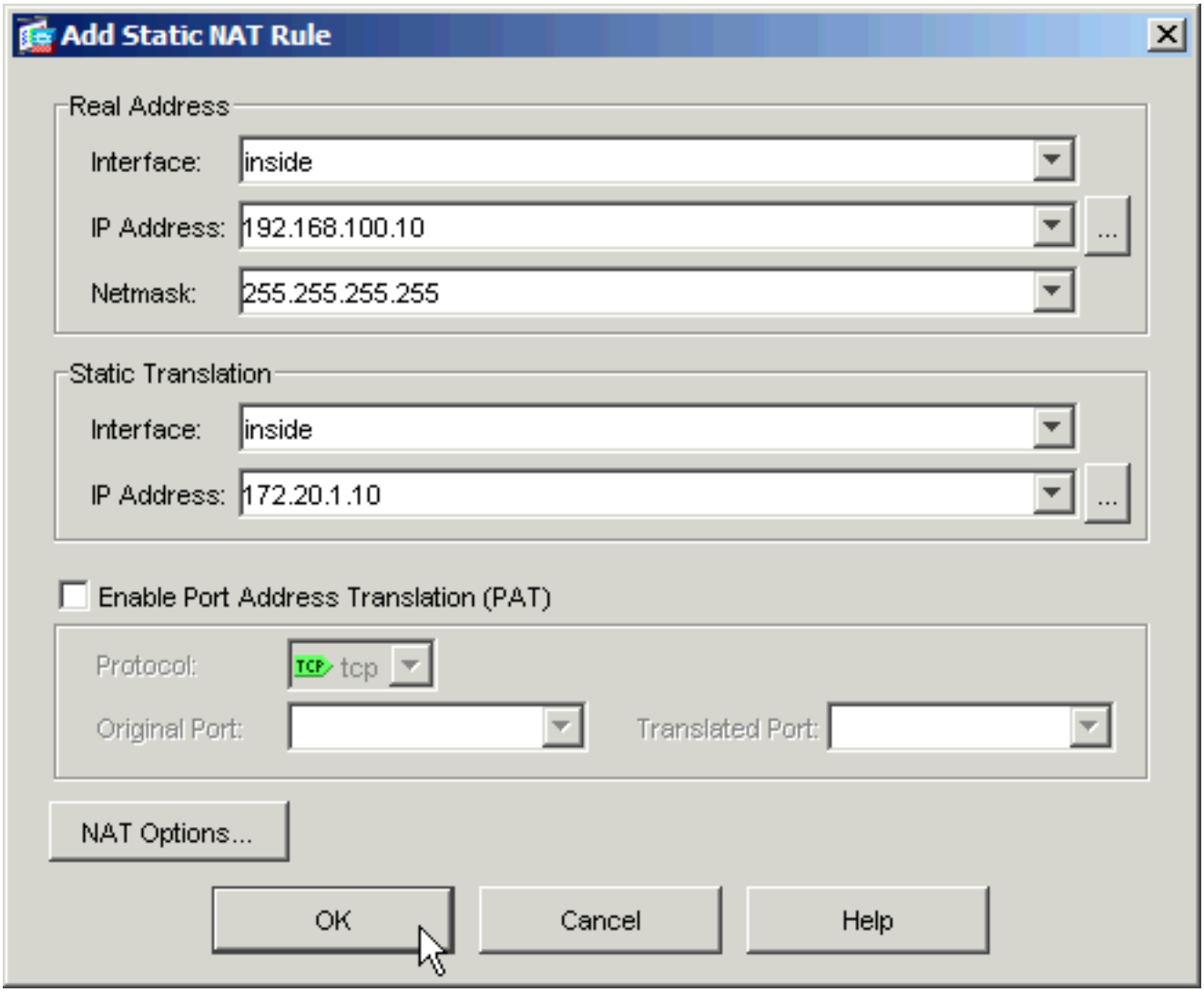


3. Cliquez sur **Apply**.
4. Naviguez vers la **Configuration > NAT** et choisissez **Add > Add Static NAT Rule....**

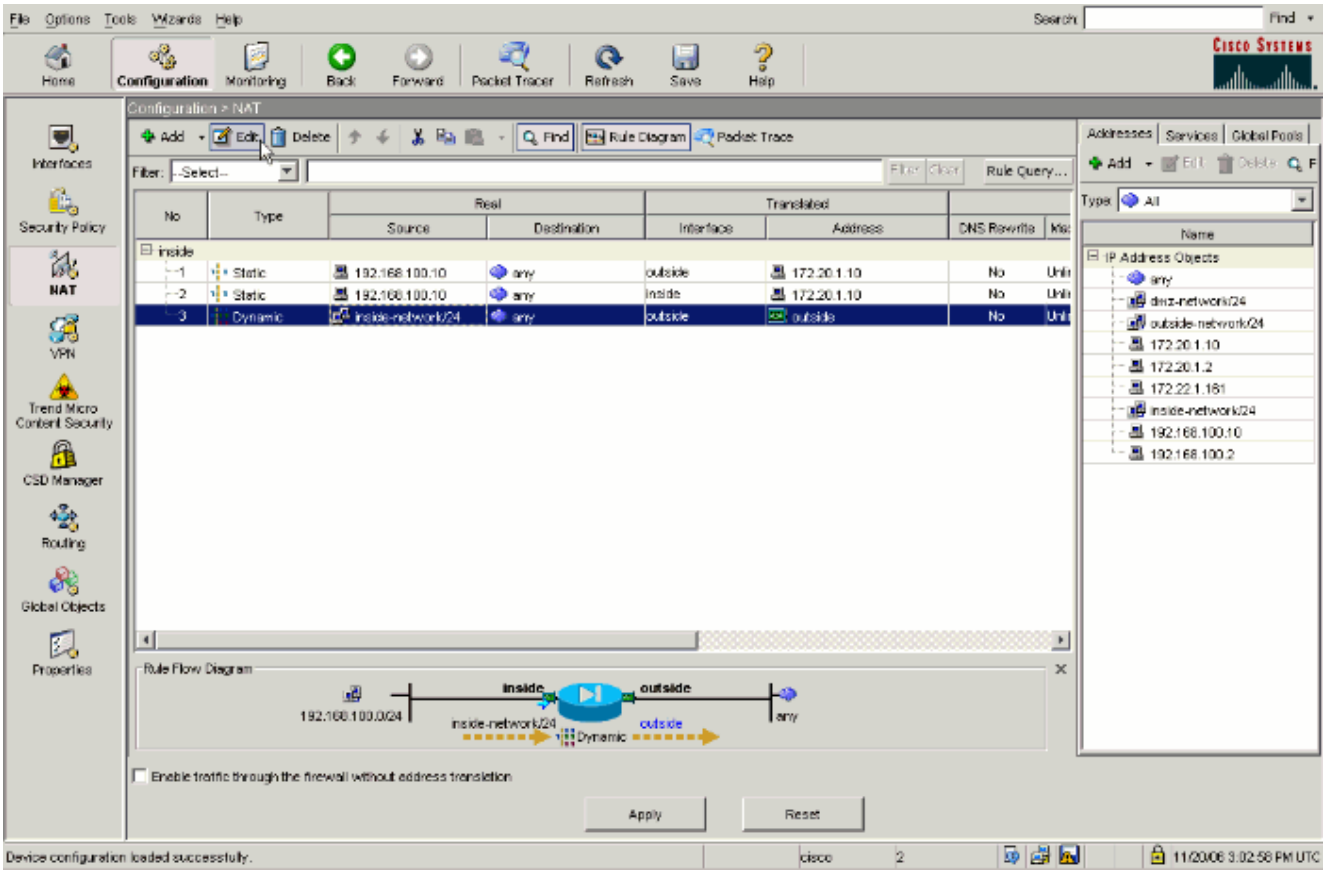


5. Complétez la configuration pour la nouveau routage de traduction statique.Remplissez la zone **Véritable adresse** avec les informations du serveur WWW.Remplissez la zone **Routage de traduction statique** avec l'adresse et l'interface que vous souhaitez mapper au serveur WWW.Dans ce cas, l'interface interne est choisie pour permettre à des hôtes sur l'interface

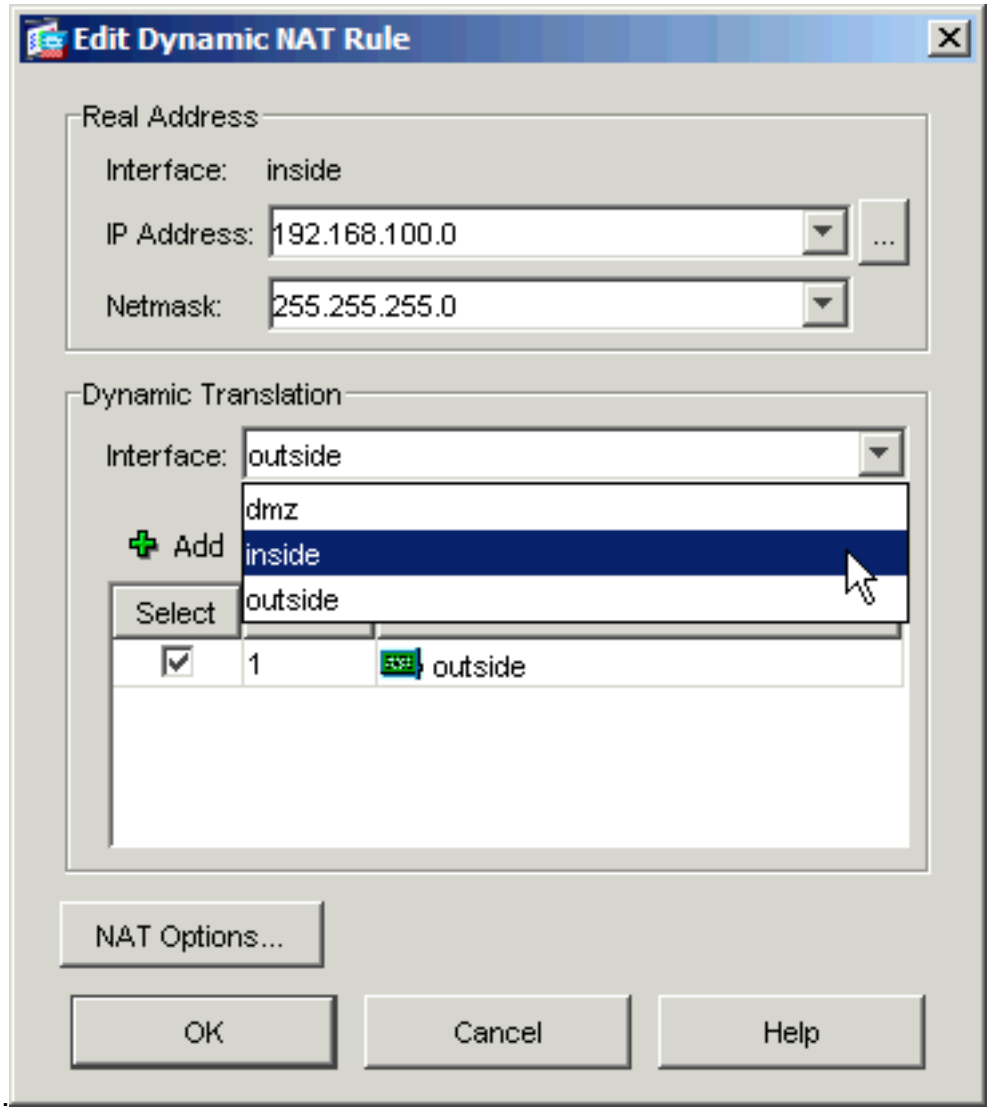
interne d'accéder au serveur WWW par l'intermédiaire de l'adresse mappée 172.20.1.10.

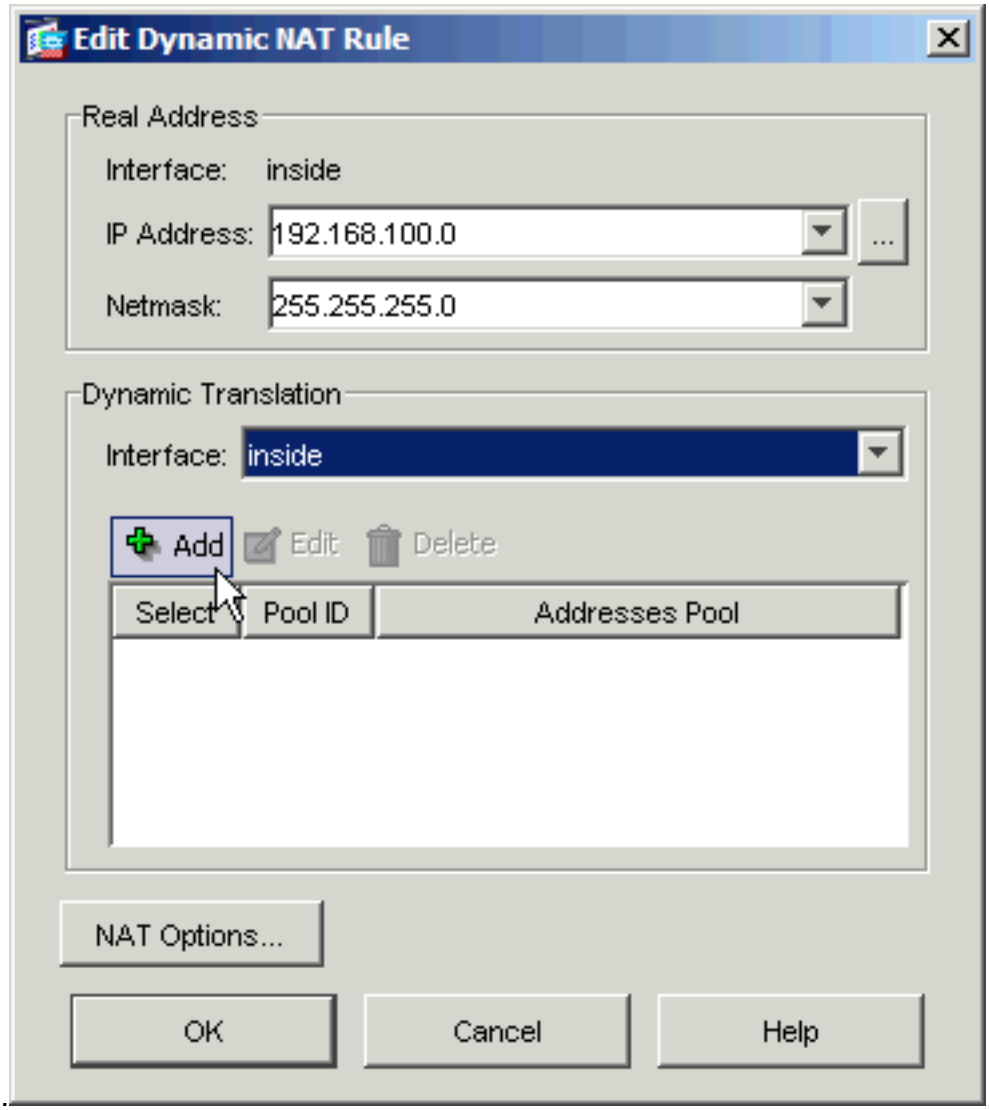


6. Cliquez sur**OK** pour quitter la fenêtre Ajouter la règle NAT statique.
7. Choisissez la traduction PAT dynamique existante et cliquez sur Edit.

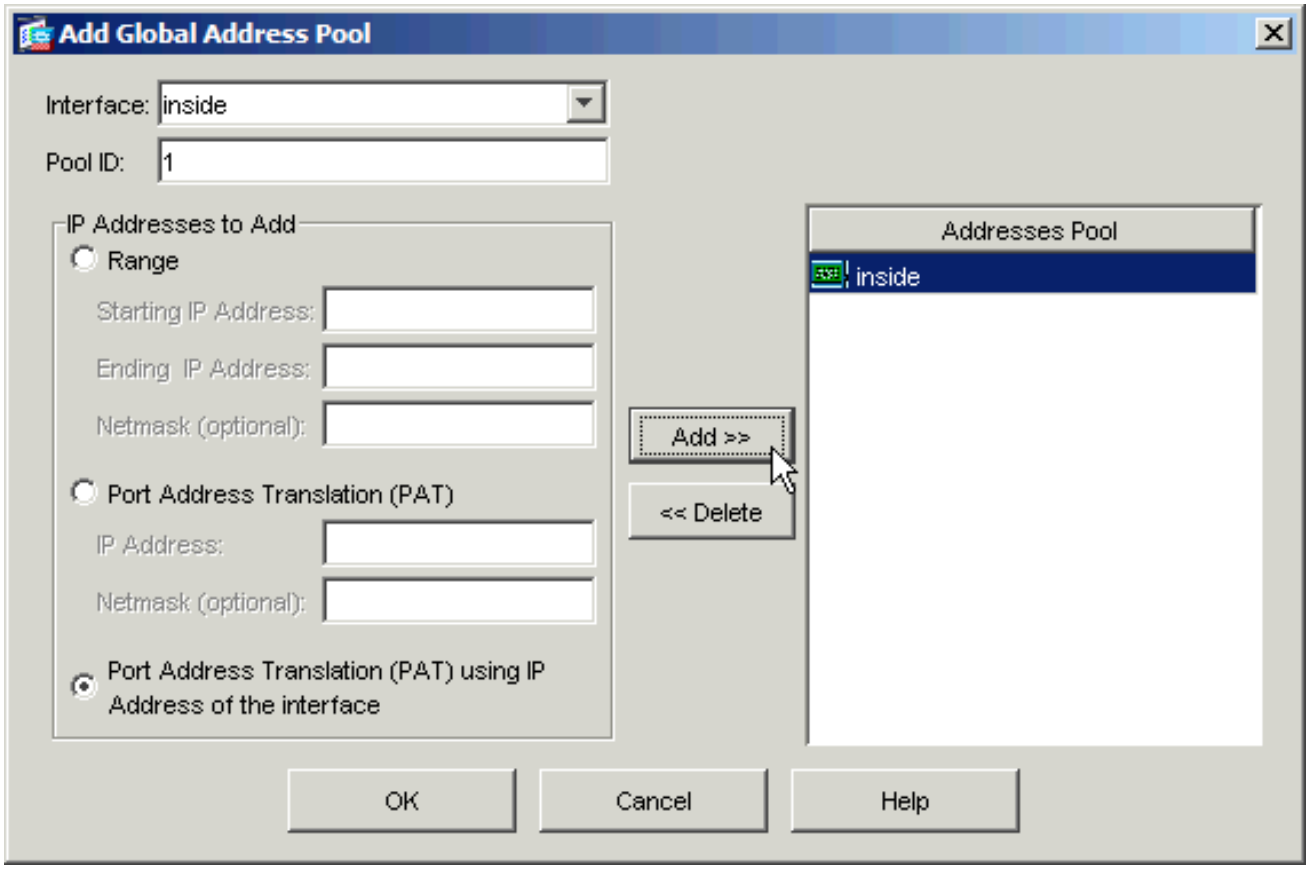


8. Choisissez **à l'intérieur de la** case de menu déroulant d'interface.





9. Cliquez sur **Add**.
10. Choisissez la **translation d'adresses d'adresse du port** marquée par case d'option **(PAT) utilisant l'adresse IP de l'interface**. Cliquez sur **Add**.



11. Cliquez sur OK pour laisser la fenêtre de pool d'adresses globales d'ajouter. Cliquez sur OK pour laisser à l'éditer la fenêtre dynamique de règle NAT. Cliquez sur **Apply** pour envoyer votre configuration à l'appliance de sécurité.

Voici la séquence d'opérations qui ont lieu quand le hairpinning est configuré. 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. Les dispositifs de sécurité voient la demande et identifient que le serveur de WWW est chez 192.168.100.10.`%ASA-7-609001: Built local-host inside:192.168.100.10`
3. Les dispositifs de sécurité créent une traduction PAT dynamique pour le client. La source de trafic de client est maintenant l'interface interne des dispositifs de sécurité : 192.168.100.1.`%ASA-6-305011: Built dynamic TCP translation from inside:192.168.100.2/11012 to inside:`**`192.168.100.1/1026`**
4. Les dispositifs de sécurité créent une connexion TCP entre le client et le serveur de WWW par lui-même. Notez les adresses mappées de chaque hôte entre parenthèses.`%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.`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 de **show conn** sur les dispositifs de sécurité vérifie que la connexion a réussi entre les dispositifs de sécurité et le serveur de WWW au nom du client. Notez la vraie adresse du client entre parenthèses.`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 le hairpinning et NAT statique]

C'est la configuration finale de l'ASA qui emploie le hairpinning et NAT statique pour réaliser des DN soignant l'effet avec deux interfaces NAT.

Configuration finale ASA 7.2(1)

```
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 case. 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 interface. 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 appear on the inside
interface to the WWW server's real address !--- of
192.168.100.10. 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: Référez-vous à ce vidéo, Cheveu-goupillant sur Cisco ASA (clients enregistrés seulement), pour plus d'informations sur différents scénarios où cheveu-goupiller pourrait être utilisé.

Configurez l'inspection de DNS

Afin d'activer l'inspection de DN (si elle a été précédemment désactivée), exécutez 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.`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.`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.`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 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.`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`

Configuration de split-dns

Émettez le **split-dns** commandent dans le mode de configuration de stratégie de groupe afin d'écrire une liste de domaines à résoudre par le tunnel partagé. Utilisez le ***forme no de*** cette commande afin de supprimer une liste.

Quand il n'y a aucun domain list de Segmentation de tunnel, les utilisateurs en héritent qui existent dans la stratégie de groupe par défaut. Émettez le **split-dns qu'aucun** ne commande afin d'empêcher l'héritage des domains lists de Segmentation de tunnel.

Employez un espace simple afin de séparer chaque entrée dans la liste de domaines. Il n'y a aucune limite sur le nombre d'entrées, mais la chaîne entière peut être plus que 255 caractères. Vous pouvez utiliser seulement des caractères alphanumériques, des traits d'union (-), et des périodes (.). **L'aucun split-dns** ne commande, une fois utilisé sans arguments, supprime toutes les valeurs courantes, qui inclut une valeur nulle créée quand vous émettez le **split-dns qu'aucun** ne commande.

Cet exemple affiche comment configurer les domaines Domain1, Domain2, Domain3 et Domain4 afin de pour être résolu par la Segmentation de tunnel pour la stratégie de groupe nommée FirstGroup :

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

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'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 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

afficher des détails supplémentaires tels que le nom et l'adresse IP dans des Un-enregistrements de DN.`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. 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 de xlate, et puis retirez et réappliquez les déclarations NAT afin de résoudre cette erreur.

Réponse de DN d'UDP de baisse

Il est possible que vous receviez ce message d'erreur dû à la perte de paquets de DN :

```
 %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 de paquet de DN entre 512-65535 afin de résoudre ce problème.

Exemple :

```
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 terrain relatives aux produits de sécurité
- Request For Comments (RFC)
- Cheveux goupillant sur Cisco ASA
- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Support et documentation techniques - Cisco Systems