# 在ASA 9.x版上為三個NAT介面配置DNS修正

## 目錄



## 簡介

本文提供在使用對象/自動網路地址轉換(NAT)語句的ASA 5500-X系列自適應安全裝置(ASA)上執行域名系統(DNS)修正的配置示例。DNS修正允許安全裝置重寫DNS A記錄。

DNS重寫執行兩種功能：

- 當DNS客戶端位於專用介面上時，將DNS應答中的公共地址（可路由或對映地址）轉換為專用地址（實際地址）。
- 當DNS客戶端位於公共介面上時，將私有地址轉換為公共地址。

## 必要條件

### 需求

Cisco宣告必須啟用DNS檢查才能在安全裝置上執行DNS修正。預設情況下，DNS檢查處於開啟狀態。

啟用DNS檢查後，安全裝置將執行以下任務：

- 根據使用object/auto NAT命令（DNS重寫）完成的配置轉換DNS記錄。 轉換僅適用於DNS回覆中的A記錄。因此，請求指標(PTR)記錄的反向查詢不會受DNS重寫的影響。在ASA 9.0(1)及更高版本中，在使用IPv4 NAT、IPv6 NAT和NAT64並啟用NAT規則的DNS檢查時，轉換用於反向DNS查詢的DNS PTR記錄。**附註**：DNS重寫與靜態埠地址轉換(PAT)不相容，因為多個PAT規則適用於每個A記錄，而要使用的PAT規則不明確。
- 實施最大DNS消息長度(預設值為512位元組，最大長度為65535位元組)。 如有必要，會執行重組，以驗證封包長度是否小於設定的最大長度。如果封包超過最大長度，就會將其捨棄。**附註**：如果您輸入**inspect dns**命令而不使用最大長度選項，則不會檢查DNS資料包大小。
- 強制域名長度為255個位元組，標籤長度為63個位元組。
- 如果DNS消息中遇到壓縮指標，則驗證指標引用的域名的完整性。
- 檢查是否存在壓縮指標循環。

### 採用元件

本文檔中的資訊基於ASA 5500-X系列安全裝置版本9.x。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

### 相關產品

此配置還可以與Cisco ASA 5500系列安全裝置8.4版或更高版本配合使用。

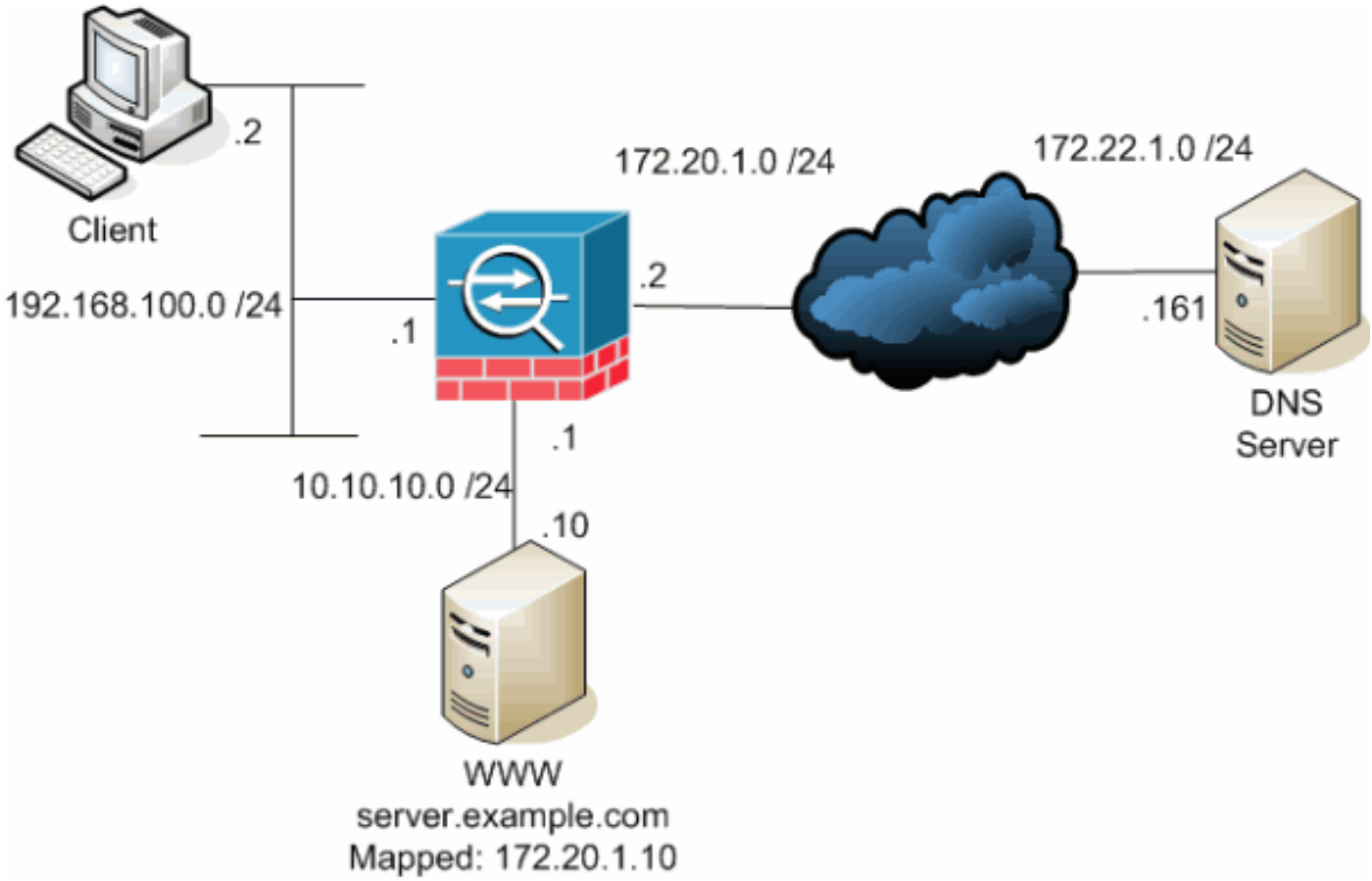
**附註**：ASDM配置僅適用於版本7.x。

## 背景資訊

在典型的DNS交換中，客戶端向DNS伺服器傳送URL或主機名以確定該主機的IP地址。DNS伺服器收到請求，查詢該主機的名稱到IP地址的對映，然後向客戶端提供具有IP地址的A記錄。儘管此過程在許多情況下都運行良好，但也可能會出現問題。當客戶端和客戶端嘗試連線的主機都位於NAT後的同一專用網路上，但客戶端使用的DNS伺服器位於另一個公共網路上時，便會出現這些問題。

## 案例：三個NAT介面 — 內部、外部、DMZ

### 拓撲




此圖是這種情況的一個示例。在這種情況下，位於192.168.100.2的客戶端希望使用**server.example.com** URL來訪問10.10.10.10的WWW伺服器。客戶端的DNS服務由位於172.22.1.161的外部DNS伺服器提供。由於DNS伺服器位於另一個公共網路上，因此它不知道WWW伺服器的專用IP地址。相反，它知道WWW伺服器對映地址172.20.1.10。因此，DNS伺服器包含**server.example.com**到**172.20.1.10**的IP地址到名稱對映。

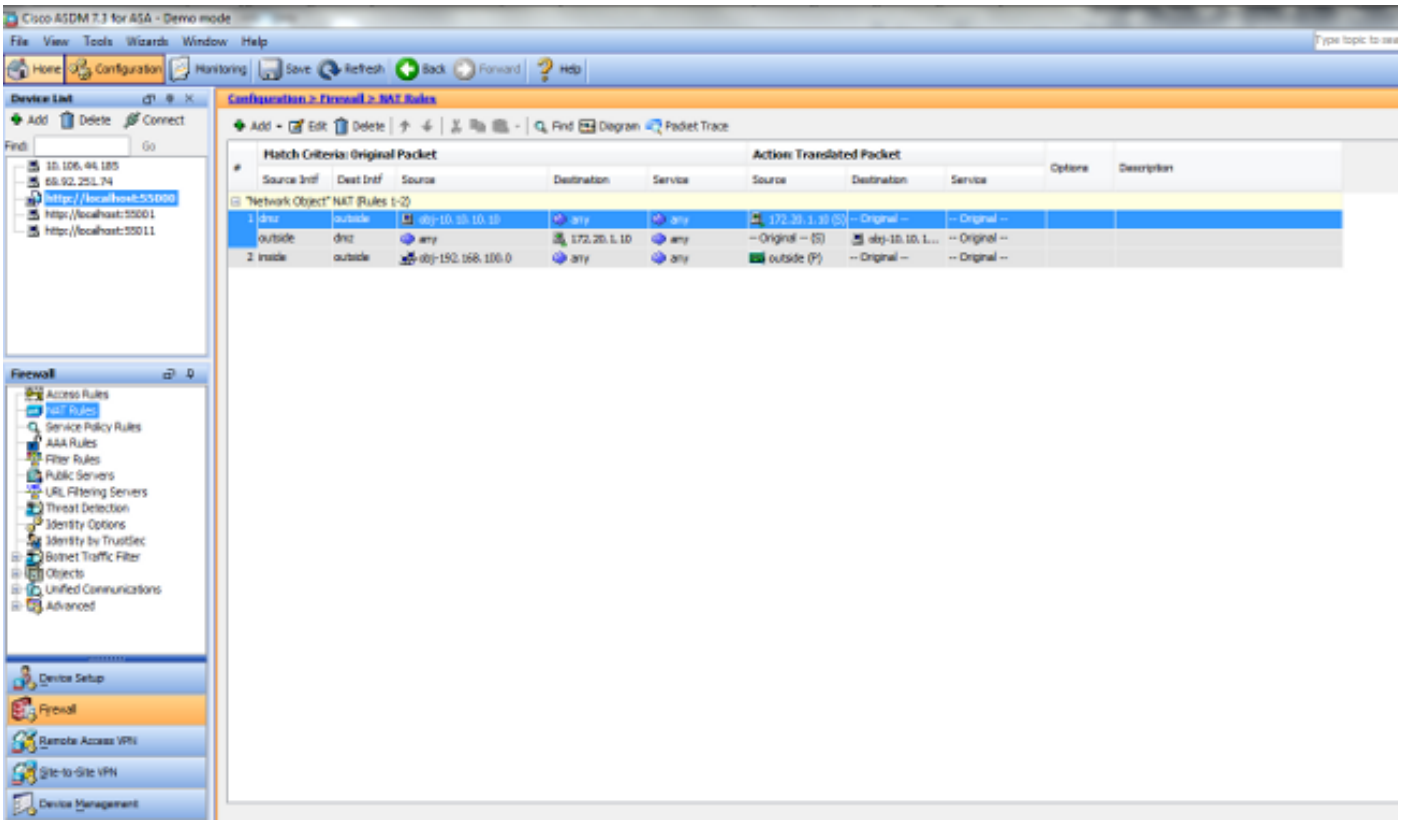
## 問題：客戶端無法訪問WWW伺服器

如果在此情況下未啟用DNS修正或其他解決方案，則如果客戶端傳送針對**server.example.com** IP地址的DNS請求，則無法訪問WWW伺服器。這是因為客戶端收到一個A記錄，其中包含用於WWW伺服器的對映公有地址172.20.1.10。當客戶端嘗試訪問此IP地址時，安全裝置會丟棄資料包，因為它不允許在同一介面上重定向資料包。以下是未啟用DNS修正時，配置的NAT部分的外觀：

```
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.
```

未啟用DNS修正時，ASDM中的配置如下所示：



以下是未啟用DNS修正時事件的封包擷取：

1. 客戶端傳送DNS查詢。

```
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. ASA對DNS查詢執行PAT並轉發查詢。請注意，資料包的源地址已更改為ASA的外部介面。

```
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. DNS伺服器使用WWW伺服器的對映地址進行應答。

```
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. ASA會解除DNS響應的目標地址的轉換，並將資料包轉發到客戶端。請注意，如果沒有啟用DNS修正，則應答中的Addr仍是WWW伺服器的對映地址。

```
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. 此時，客戶端嘗試訪問地址為172.20.1.10的WWW伺服器。ASA為此通訊建立連線條目。但是，由於它不允許流量從內部流向外部到DMZ，因此連線超時。ASA日誌顯示：

```
%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
```

## 解決方案："dns"關鍵字

### 使用「dns」關鍵字進行DNS修正

使用**dns**關鍵字進行DNS修正使安全裝置能夠截獲和重寫DNS伺服器回復到客戶端的內容。正確配置後，安全裝置可以修改A記錄，以便在「問題：客戶端無法訪問WWW伺服器」部分進行連線。在啟用DNS修正的情況下，安全裝置會重寫A記錄以將客戶端定向到10.10.10.10而不是172.20.1.10。將**dns**關鍵字新增到靜態NAT語句（8.2版及更低版本）或對象/自動NAT語句（8.3版及更高版本）時，會啟用DNS修正。

## 8.2及更低版本

這是使用**dns**關鍵字執行DNS修正的ASA的最終配置，以及版本8.2及更低版本的三個NAT介面。

```
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
```

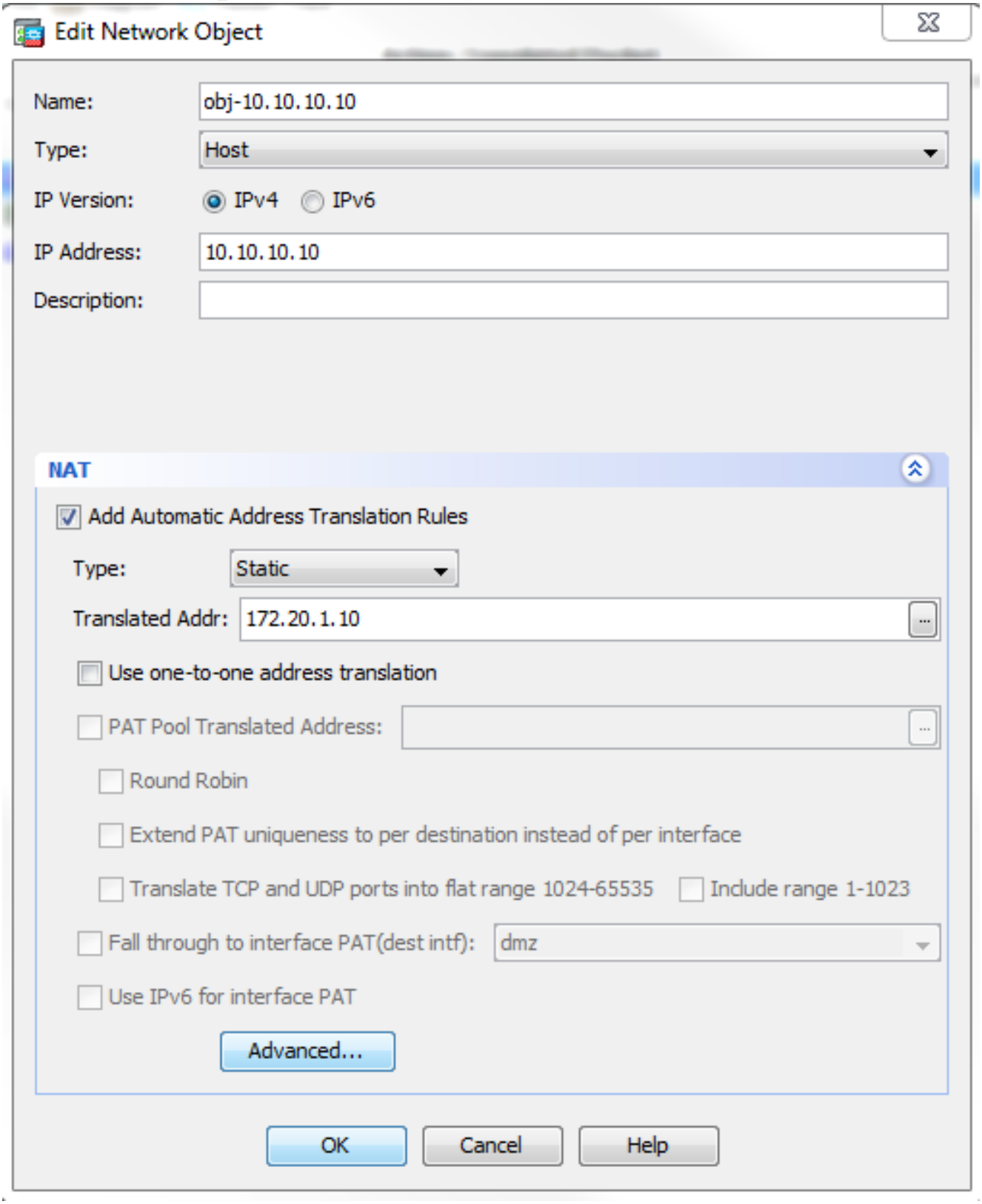
## 8.3及更新版本

```
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.
```

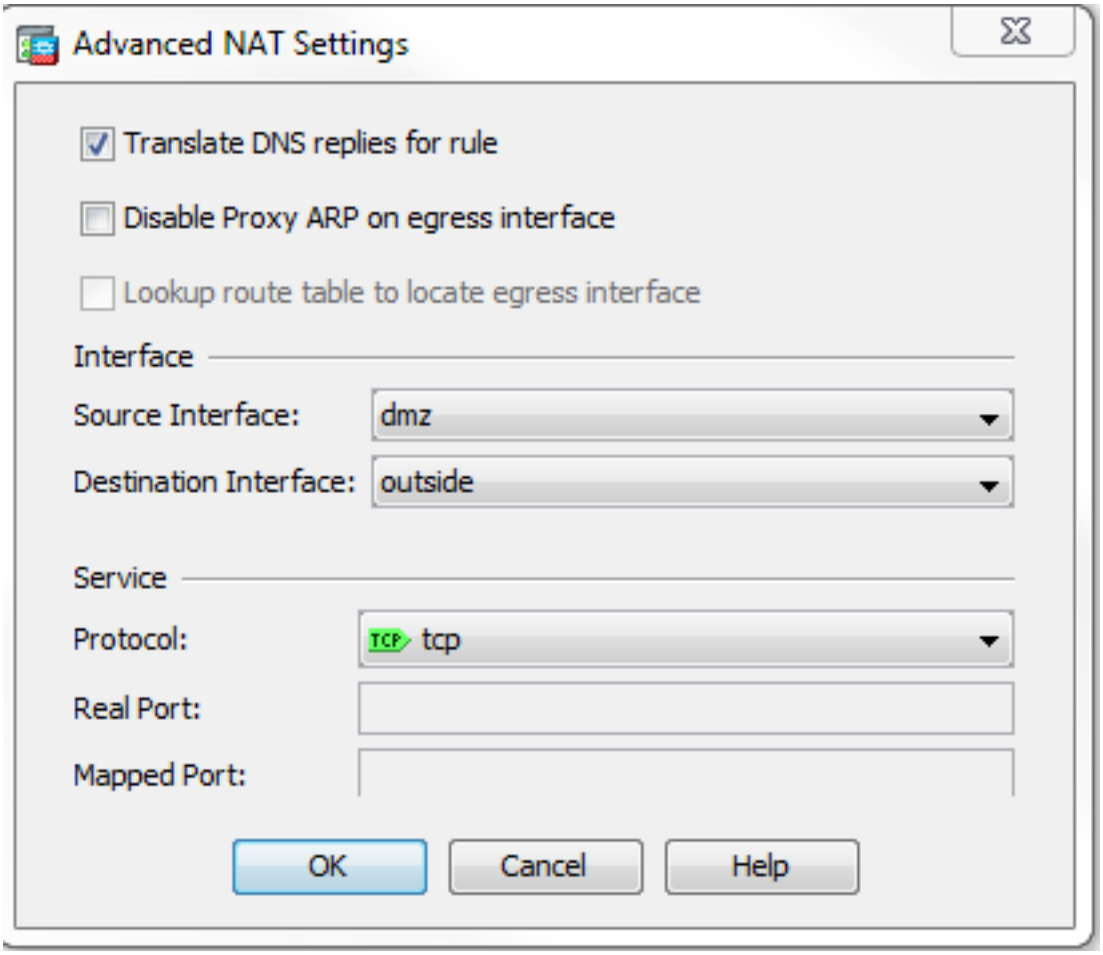
## ASDM配置

完成以下步驟，以便在ASDM中配置DNS修正：

1. 選擇Configuration > NAT Rules，然後選擇要修改的對象/自動規則。按一下「Edit」。
2. 按一下「Advanced..」




3. 選中Translate DNS replies for rule覈取方塊。




4. 按一下**OK**以退出「NAT選項」視窗。
5. 按一下**OK**以退出Edit Object/Auto NAT Rule視窗。
6. 按一下「**Apply**」將組態傳送到安全裝置。

## 驗證

以下是啟用DNS修正後事件的封包擷取：

1. 客戶端傳送DNS查詢。

```
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. ASA對DNS查詢執行PAT並轉發查詢。請注意，資料包的源地址已更改為ASA的外部介面。

```
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. DNS伺服器使用WWW伺服器的對映地址進行應答。

```
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. ASA會解除DNS響應的目標地址的轉換，並將資料包轉發到客戶端。請注意，啟用DNS修正後，應答中的Addr將重寫為WWW伺服器的實際地址。

```
No.     Time       Source         Destination     Protocol Info
6 2.507191 172.22.1.161   192.168.100.2   DNS Standard query response
```

```
A 10.10.10.10

Frame 6 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Cisco_9c:c6:1f (00:0a:b8:9c:c6:1f), Dst: Cisco_c8:e4:00
(00:04:c0:c8:e4:00)
Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 192.168.100.2
(192.168.100.2)
User Datagram Protocol, Src Port: domain (53), Dst Port: 50752 (50752)
Domain Name System (response)
[Request In: 5]
[Time: 0.002182000 seconds]
Transaction ID: 0x0004
Flags: 0x8580 (Standard query response, No error)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
server.example.com: type A, class IN
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
Answers
server.example.com: type A, class IN, addr 10.10.10.10
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
Time to live: 1 hour
Data length: 4
Addr: 10.10.10.10
```

5. 此時，客戶端嘗試訪問位於10.10.10.10的WWW伺服器。連線成功。

## 使用「dns」關鍵字的最終配置

這是使用**dns**關鍵字和三個NAT介面執行DNS修正的ASA的最終配置。

```
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
```

## 備選解決方案：目標NAT

目標NAT可以替代DNS修正。在此情況下使用目標NAT要求在內部的WWW伺服器公有地址和DMZ上的實際地址之間建立靜態對象/自動NAT轉換。目標NAT不會更改從DNS伺服器返回到客戶端的DNS A記錄的內容。相反，當您在本文檔所討論的場景中使用目標NAT時，客戶端可以使用DNS伺服器返回的公共IP地址**172.20.1.10**來連線到WWW伺服器。靜態對象/自動轉換允許安全裝置將目標地址從**172.20.1.10**轉換為**10.10.10.10**。以下是使用目標NAT時的相關配置部分：

```
ASA Version 9.x
!
hostname ciscoasa

!--- Output suppressed.
```

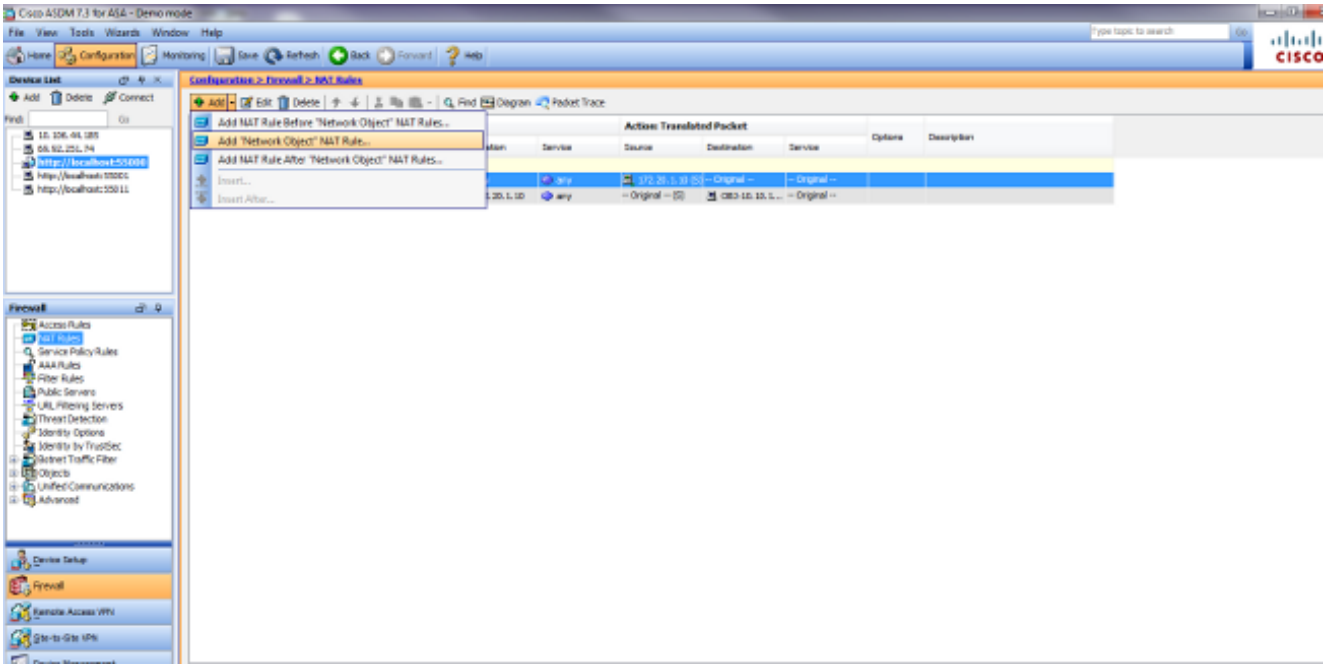
```
access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www

!--- 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
```

## 使用手動/兩次NAT語句實現目標NAT

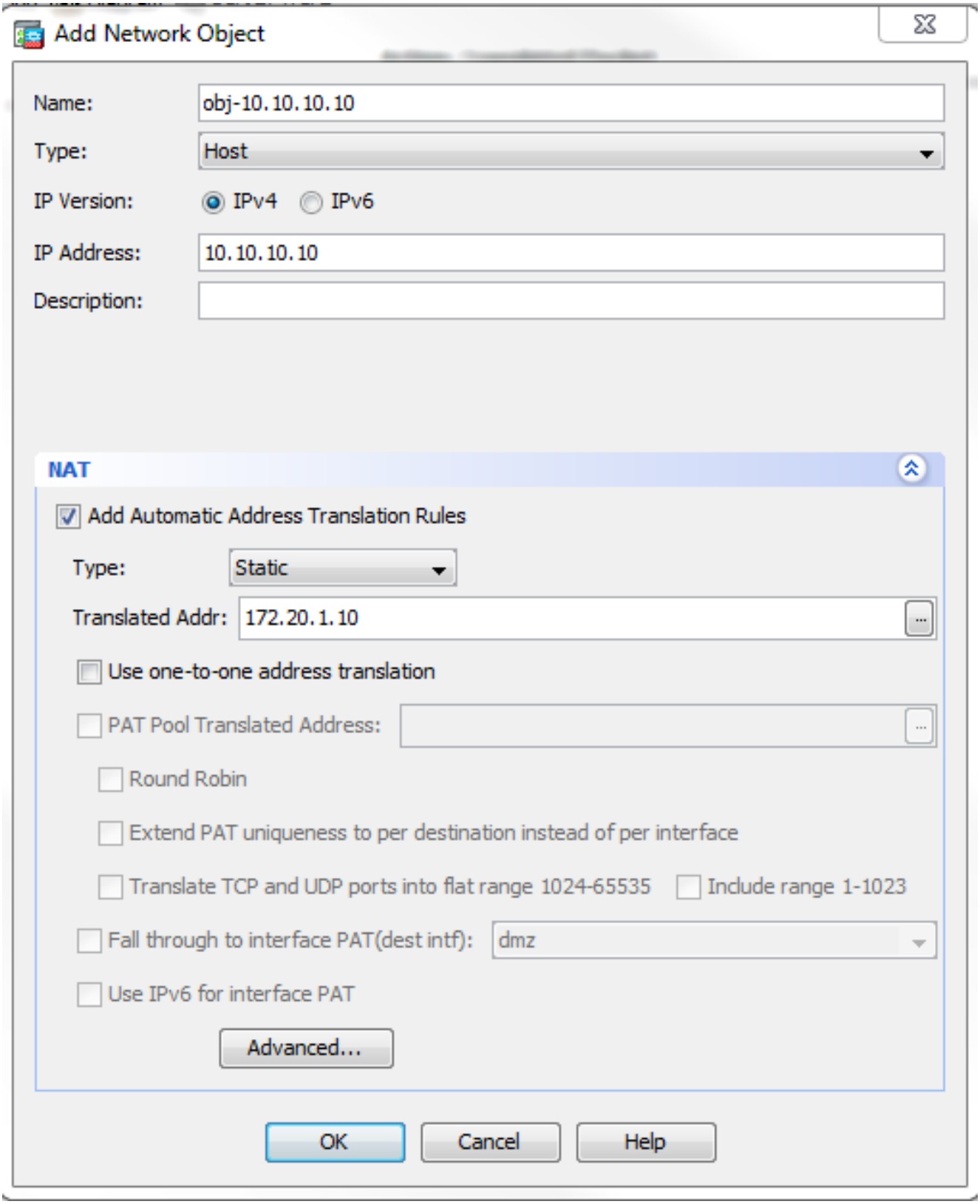
```
ASA Version 9.x
!
hostname ciscoasa

!--- 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.
```

完成以下步驟，以便在ASDM中配置目標NAT:

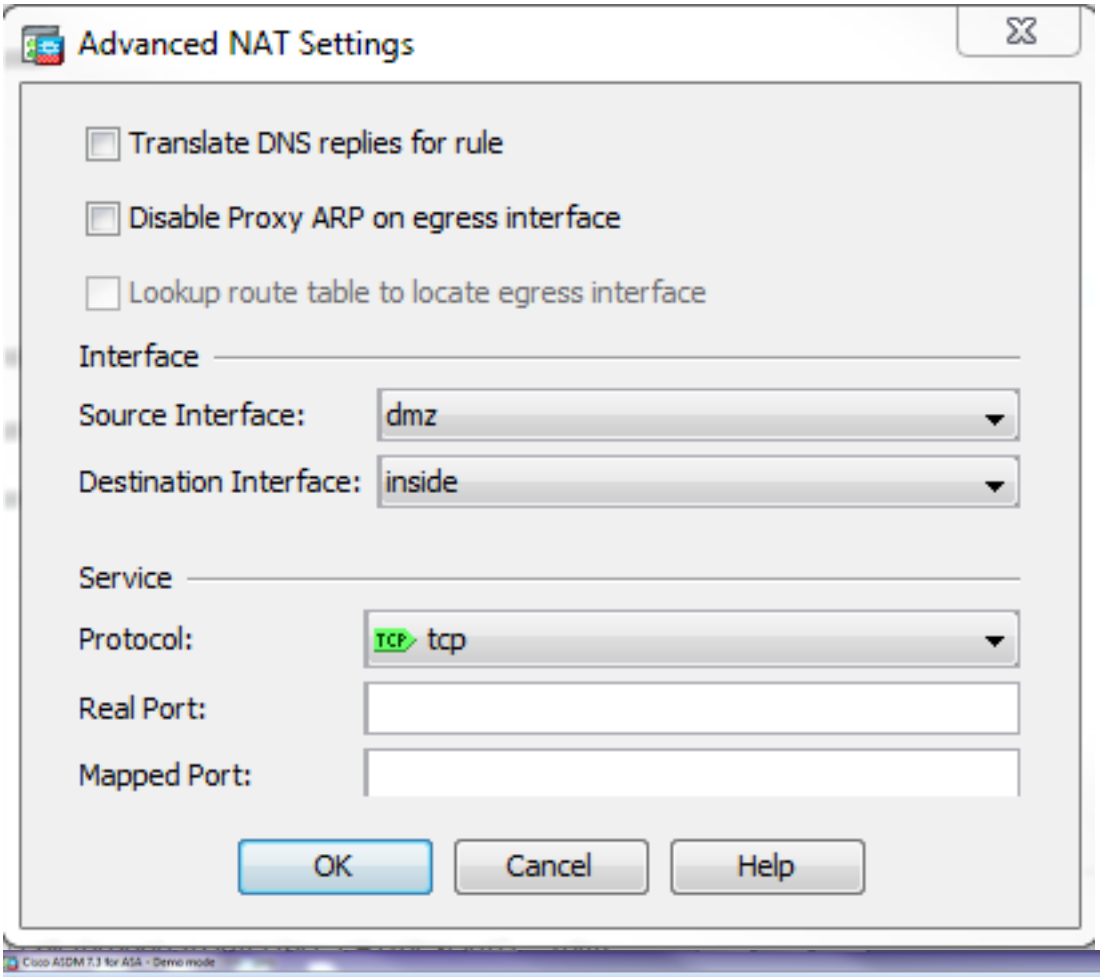
1. 選擇**Configuration > NAT Rules**，然後選擇**Add > Add "Network Object" NAT Rule...**.

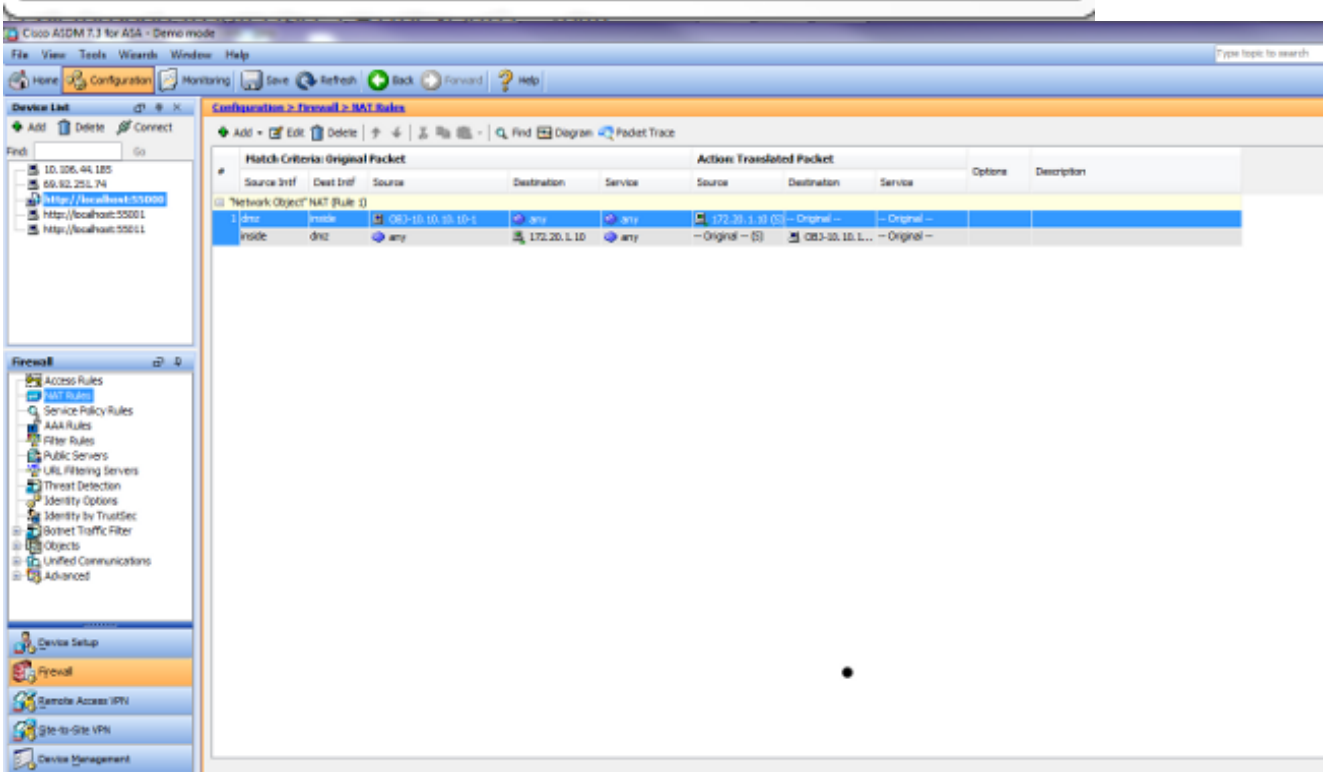


2. 填寫新靜態轉換的配置。 在「名稱」欄位中，輸入**obj-10.10.10.10**。在IP Address欄位中，輸入WWW伺服器IP地址的地址。在「型別」下拉式清單中選擇**「靜態」**。在Translated Addr欄位中，輸入要將WWW伺服器對映到的地址和介面。按一下「**Advanced**」。




在「Source Interface」下拉式清單中選擇**dmz**。在Destination Interface下拉選單中，選擇**inside**。在這種情況下，選擇內部介面以允許內部介面上的主機通過對映地址172.20.1.10訪問WWW伺服器。

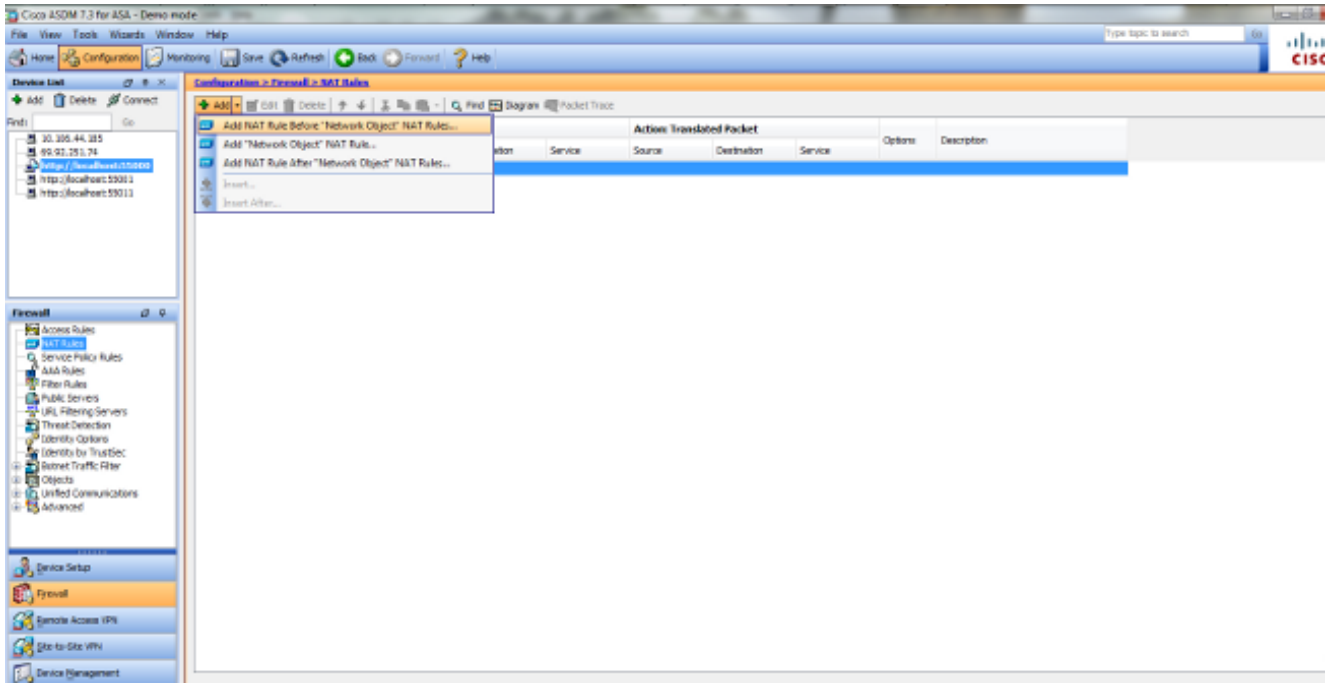


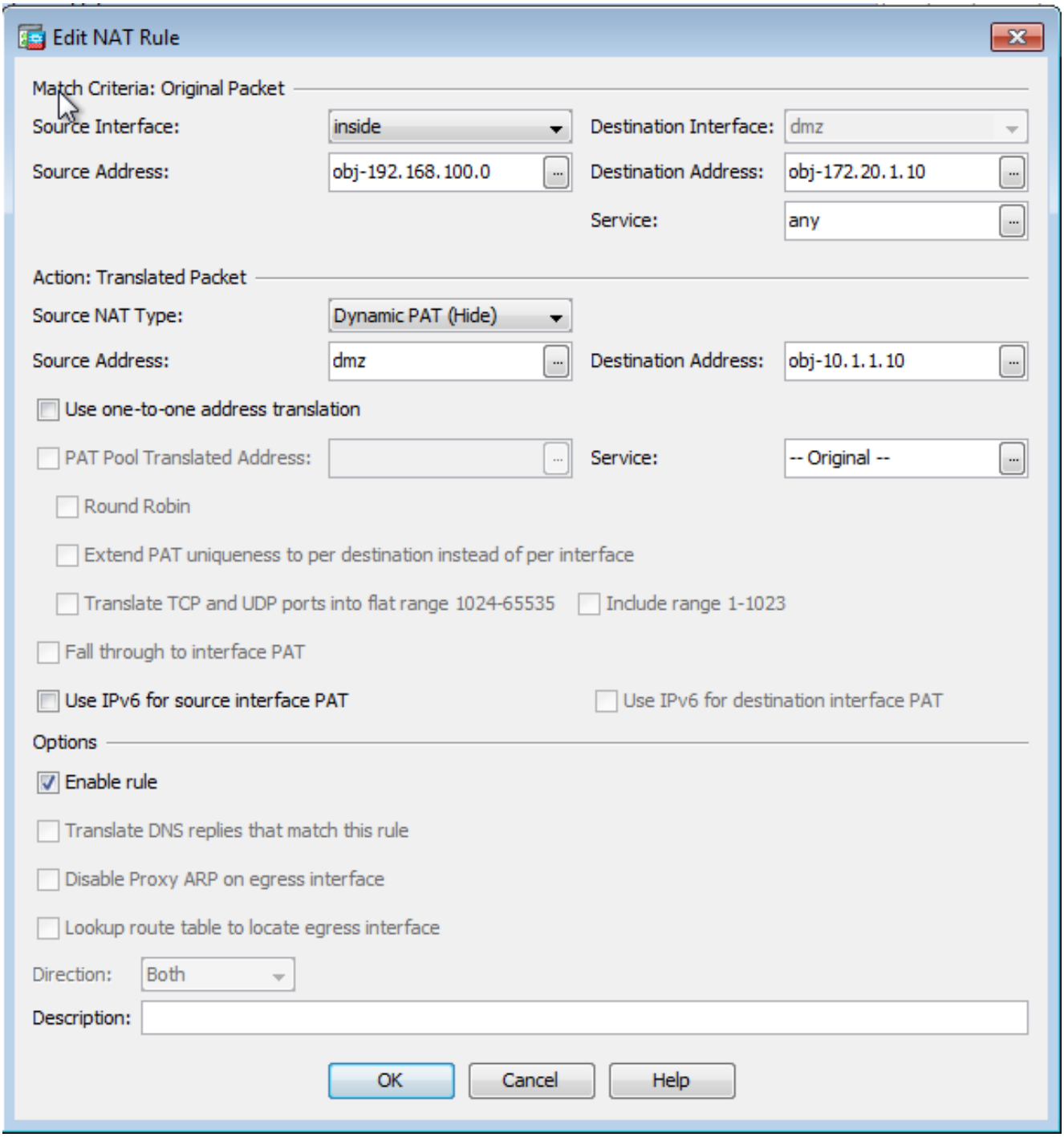
按一下**OK**以退出Add Object/Auto NAT Rule視窗。按一下「**Apply**」將組態傳送到安全裝置。

**使用手動/兩次NAT和ASDM的替代方法**

1. 選擇**Configuration > NAT Rules**，然後選擇**Add > Add Nat rule before "Network Object" NAT Rule...**.




2. 填寫手動/兩次Nat轉換的配置。 在Source Interface下拉選單中，選擇**inside**。在「Destination Interface」下拉式清單中選擇**dmz**.在「源地址」欄位中，輸入內部網路對象(obj-192.168.100.0)。在「目標地址」欄位中，輸入轉換的DMZ伺服器IP對象(172.20.1.10)。在Source NAT Type下拉選單中，選擇**Dynamic PAT(Hide)**.在源地址[Action:Translated Packet section]欄位，輸入**dmz**。在目標中 地址[Action:轉換後的資料包部分] 欄位，輸入DMZ伺服器實際IP對象(obj-10.10.10.10)。




3. 按一下**OK**以退出Add Manual/Two NAT Rule視窗。
4. 按一下「**Apply**」將組態傳送到安全裝置。

以下是配置目標NAT時發生的事件序列。假設使用者端已查詢DNS伺服器，並收到**172.20.1.10**的WWW伺服器位址：

1. 客戶端嘗試聯絡地址為172.20.1.10的WWW伺服器。
   ```
   %ASA-7-609001: Built local-host inside:192.168.100.2
   ```
2. 安全裝置會看到該請求並識別WWW伺服器是10.10.10.10。
   ```
   %ASA-7-609001: Built local-host dmz:10.10.10.10
   ```
3. 安全裝置在客戶端和WWW伺服器之間建立TCP連線。請注意括弧中每個主機的對映地址。
   ```
   %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. 安全裝置上的**show xlate**命令用於驗證客戶端流量是否通過安全裝置轉換。在這種情況下，正在使用第一個靜態轉換。
   ```
   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. 安全裝置上的**show conn**命令會驗證通過安全裝置在客戶端和WWW伺服器之間的連線是否成功。請將WWW伺服器的實際地址用括弧註明。

```
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
```

## 使用目標NAT的最終配置

這是ASA使用目標NAT和三個NAT介面執行DNS修正的最終配置。

```
ASA Version 9.x
!
hostname ciscoasa
enable password 9jNfZuG3TC5tCVH0 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
dns-guard
!
interface Ethernet0/0
 shutdown
 nameif outside
 security-level 0
 ip address 172.20.1.2 255.255.255.0
!
interface Ethernet0/1
 shutdown
 nameif inside
 security-level 100
 ip address 192.168.100.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 nameif dmz
 security-level 50
 ip address 10.10.10.1 255.255.255.0
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
 shutdown
 no nameif
 no security-level
 no ip address
!
ftp mode passive
object network obj-192.168.100.0
 subnet 192.168.100.0 255.255.255.0
object network obj-10.10.10.10
 host 10.10.10.10
object network obj-10.10.10.10-1
 host 10.10.10.10
object network obj-172.20.1.10
 host 172.20.1.10
```

```
access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www
pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm512-k8.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
!
object network obj-192.168.100.0
 nat (inside,outside) dynamic interface
object network obj-10.10.10.10
 nat (dmz,outside) static 172.20.1.10
object network obj-10.10.10.10-1
 nat (dmz,inside) static 172.20.1.10
access-group OUTSIDE in interface outside
route outside 0.0.0.0 0.0.0.0 172.20.1.1 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
http server enable
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
no ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
 anyconnect-essentials
username cisco password ffIRPGpDSOJh9YLq encrypted
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
 message-length maximum client auto
 message-length maximum 512
policy-map global_policy
 class inspection_default
 inspect dns preset_dns_map
 inspect ftp
 inspect h323 h225
 inspect h323 ras
```

```
 inspect rsh
 inspect rtsp
 inspect esmtp
 inspect sqlnet
 inspect skinny
 inspect sunrpc
 inspect xdmcp
 inspect sip
 inspect netbios
 inspect tftp
 inspect ip-options
 inspect icmp
policy-map type inspect dns MY_DNS_INSPECT_MAP
 parameters
 message-length maximum 512
policy-map type inspect dns migrated_dns_map_1
 parameters
 message-length maximum 512
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:2cdcc45bfc13f9e231f3934b558f1fd4
: end
```

# 設定

完成以下步驟以啟用DNS檢查（如果之前已禁用）。 在本示例中，DNS檢查被新增到預設全域性檢查策略中，該策略通過**service-policy**命令全域性應用，就像ASA以預設配置開始一樣。

1. 為DNS建立檢查策略對映。
   ```
   ciscoasa(config)#policy-map type inspect dns MY_DNS_INSPECT_MAP
   ```
2. 在策略對映配置模式下，進入引數配置模式以便為檢查引擎指定引數。
   ```
   ciscoasa(config-pmap)#parameters
   ```
3. 在策略對映引數配置模式下，將DNS消息的最大消息長度指定為512。
   ```
   ciscoasa(config-pmap-p)#message-length maximum 512
   ```
4. 退出策略對映引數配置模式和策略對映配置模式。
   ```
   ciscoasa(config-pmap-p)#exit
   ciscoasa(config-pmap)#exit
   ```
5. 確認已根據需要建立檢查策略對映。
   ```
   ciscoasa(config)#show run policy-map type inspect dns
   !
   policy-map type inspect dns MY_DNS_INSPECT_MAP
   parameters
   message-length maximum 512
   !
   ```
6. 進入**global**_policy的策略對映**配置模式。**
   ```
   ciscoasa(config)#policy-map global_policy
   ciscoasa(config-pmap)#
   ```
7. 在策略對映配置模式下，指定預設第3/4層類對映**inspection_default**。
   ```
   ciscoasa(config-pmap)#class inspection_default
   ciscoasa(config-pmap-c)#
   ```
8. 在策略對映類配置模式下，使用在步驟1-3中建立的檢查策略對映指定應檢查DNS。
   ```
   ciscoasa(config-pmap-c)#inspect dns MY_DNS_INSPECT_MAP
   ```
9. 退出策略對映類配置模式和策略對映配置模式。
   ```
   ciscoasa(config-pmap-c)#exit
   ciscoasa(config-pmap)#exit
   ```
10. 驗證**global_policy**策略對映是否已根據需要配置。
    ```
    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. 驗證global_policy是否由服務策略全域性應用。

```
ciscoasa(config)#show run service-policy
service-policy global_policy global
```

# 驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析。

## 捕獲DNS流量

驗證安全裝置是否正確重寫DNS記錄的方法之一是捕獲有問題的資料包，如上例所述。完成以下步驟，以便捕獲ASA上的流量：

1. 為要建立的每個捕獲例項建立訪問清單。ACL應指定要捕獲的流量。在此範例中，已建立兩個ACL。 外部介面上流量的ACL:

```
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.
```

內部介面上流量的ACL:

```
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. 建立捕獲例項：

```
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. 檢視捕獲。以下是一些DNS流量通過後擷取範例的樣子：

```
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. （可選）將捕獲以PCAP格式複製到TFTP伺服器，以便在其他應用程式中進行分析。可以分析PCAP格式的應用程式可以顯示其他詳細資訊，例如DNS A記錄中的名稱和IP地址。

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

# 疑難排解

本節提供的資訊可用於對組態進行疑難排解。

## 未執行DNS重寫

確保在安全裝置上配置了DNS檢查。

## 翻譯建立失敗

如果無法在客戶端和WWW伺服器之間建立連線，則可能是因為NAT配置錯誤。檢查安全裝置日誌，查詢指示協定無法通過安全裝置建立轉換的消息。如果出現此類消息，請檢驗是否已針對所需流量配置了NAT，以及沒有地址不正確。

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

清除xlate條目，然後刪除並重新應用NAT語句以解決此錯誤。

# 相關資訊

- Cisco ASA 5500-x配置指南
- Cisco ASA 5500-x系列命令參考
- 安全產品現場通知
- 要求建議(RFC)
- 技術支援與文件 - Cisco Systems