PIX/ASA:使用static命令和兩個NAT介面配置示例執行DNS修正

目錄

簡介

本文檔提供使用靜態網路地址轉換(NAT)語句在ASA 5500系列自適應安全裝置或PIX 500系列安全裝置上執行域名系統(DNS)修補的示例配置。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。

注意：本文檔中的配置包含兩個NAT介面；內外兼備。有關使用靜態和三個NAT介面（內部、外部和dmz）進行DNS修正示例，請參閱PIX/ASA:使用static命令和三個NAT介面配置示例執行DNS修正。

有關如何在安全裝置上使用NAT的詳細資訊，請參閱PIX/ASA 7.x NAT和PAT語句以及在PIX上使用

nat、global、static、conduit和access-list命令和埠重定向（轉發）。

必要條件

需求

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。如果已將其關閉，請參閱本文檔後面的配置DNS檢測部分以重新啟用它。啟用DNS檢查後，安全裝置將執行以下任務：

- 根據使用**static**和**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PTR記錄的反向查詢不受DNS重寫的影響。**注意**：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，將執行重組，以驗證資料包長度是否小於配置的最大長度。如果封包超過最大長度，就會將其捨棄。**注意**：如果發出不帶maximum-length選項的**inspect dns**命令，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系列安全裝置7.2(1)版。

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 PIX 500系列安全裝置6.2版或更高版本配合使用。

注意：思科自適應安全裝置管理器(ASDM)配置僅適用於版本7.x。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

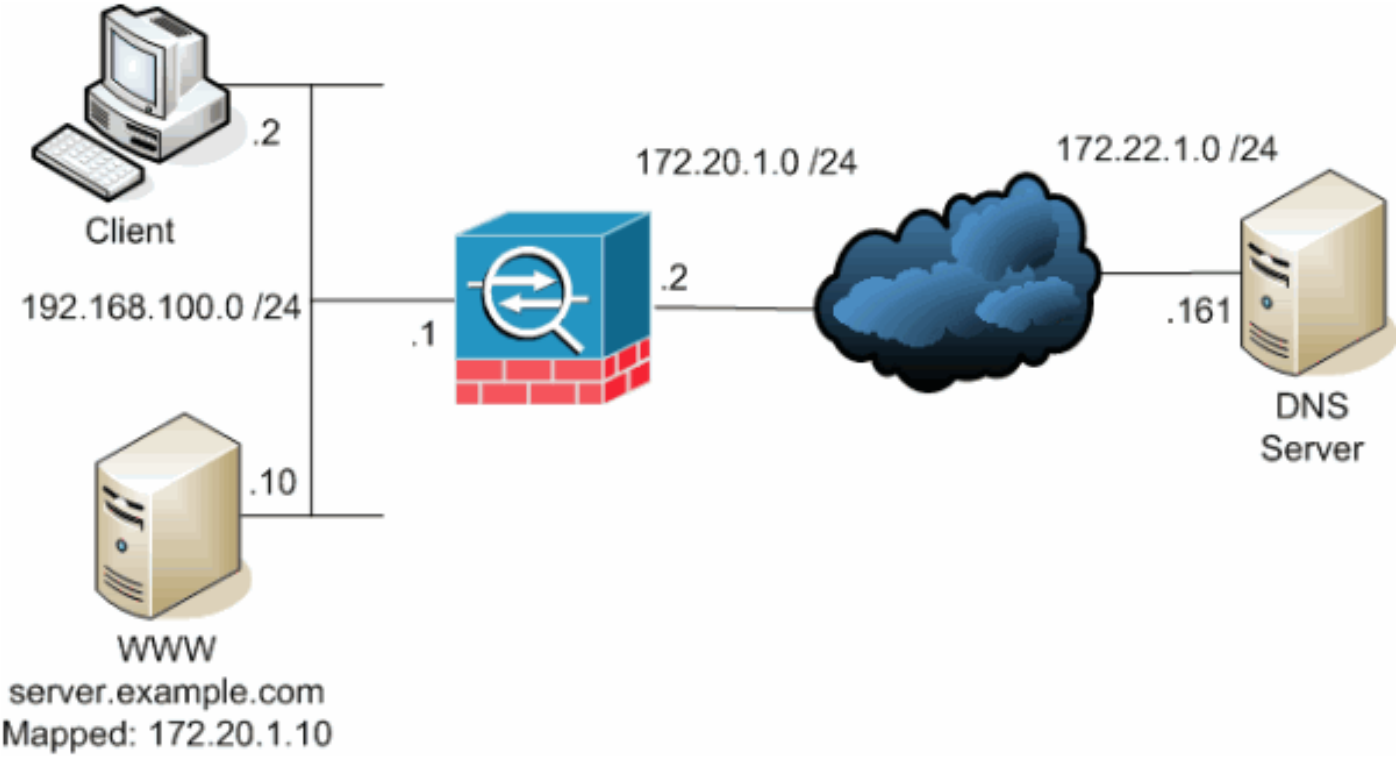
背景資訊

在典型的DNS交換中，客戶端會向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：兩個NAT介面（內部、外部）

拓撲

在此場景中，客戶端和客戶端嘗試訪問的WWW伺服器都位於ASA的內部介面上。動態PAT配置為允許客戶端訪問Internet。具有訪問清單的靜態NAT配置為允許伺服器訪問Internet，以及允許Internet主機訪問WWW伺服器。



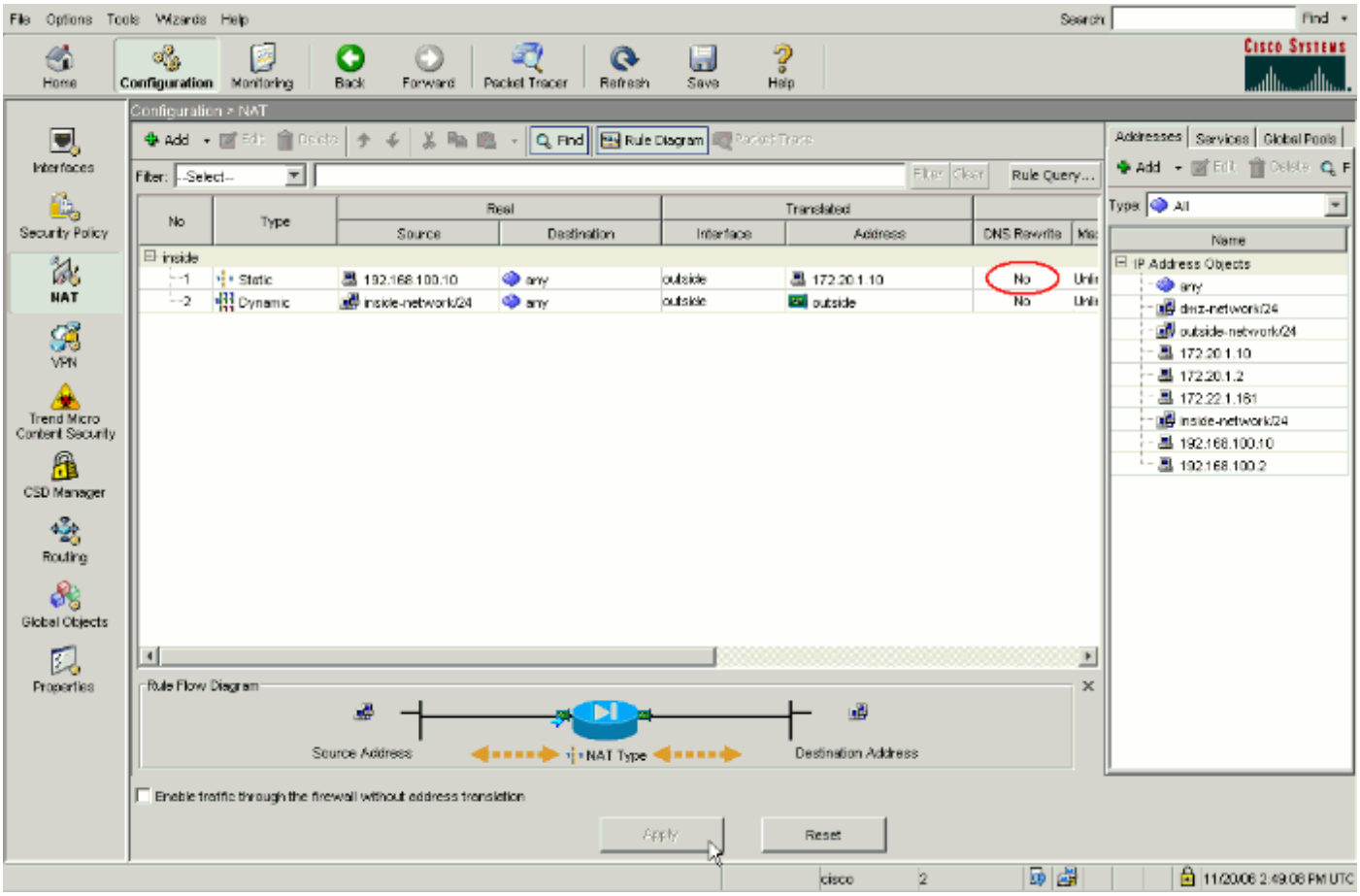
此圖是這種情況的一個示例。在本例中，位於192.168.100.2的客戶端希望使用**server.example.com** URL來訪問位於192.168.100.10的WWW伺服器。客戶端的DNS服務由位於172.22.1.161的外部DNS伺服器提供。由於DNS伺服器位於另一個公共網路上，因此它不知道WWW伺服器的專用IP地址。相反，它知道WWW伺服器對映地址172.20.1.10。因此，DNS伺服器包含**server.example.com**到**172.20.1.10**的IP地址到名稱對映。

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，則如果客戶端傳送對server.example.com的IP地址的DNS請求，它將無法訪問WWW伺服器。這是因為客戶端收到包含對映公有地址的A記錄：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：

```
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.
```

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，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

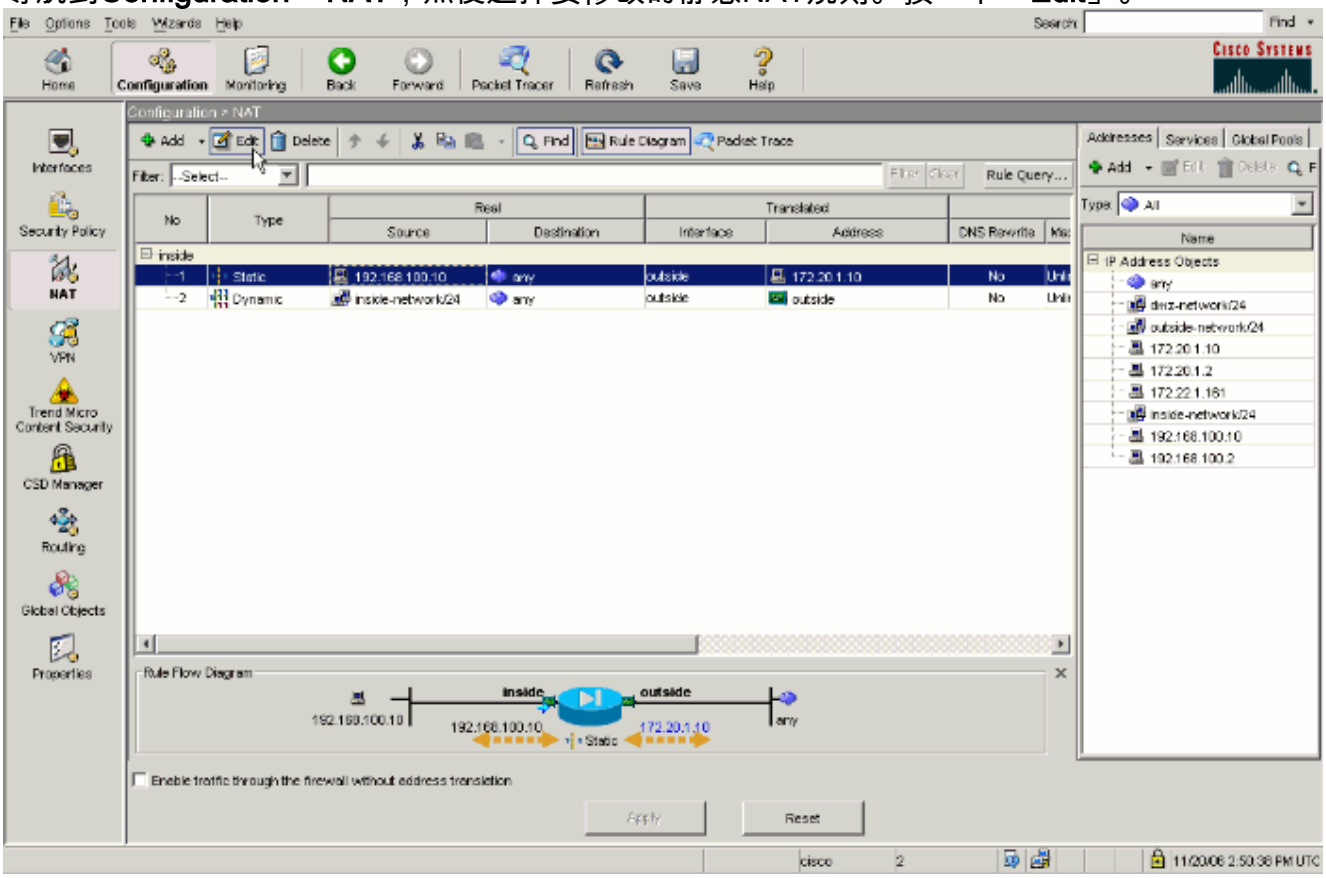
使用「dns」關鍵字進行DNS修正

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，安全裝置可以更改A記錄，以便在問題：客戶端無法訪問WWW服務器部分進行連線。在這種情況下，啟用DNS修正後，安全裝置會重寫A記錄以將客戶端定向到**192.168.100.10**，而不是**172.20.1.10**。將**dns**關鍵字新增到靜態NAT語句中時，DNS修正會啟用。以下是啟用DNS修正後，配置的NAT部分的外觀：

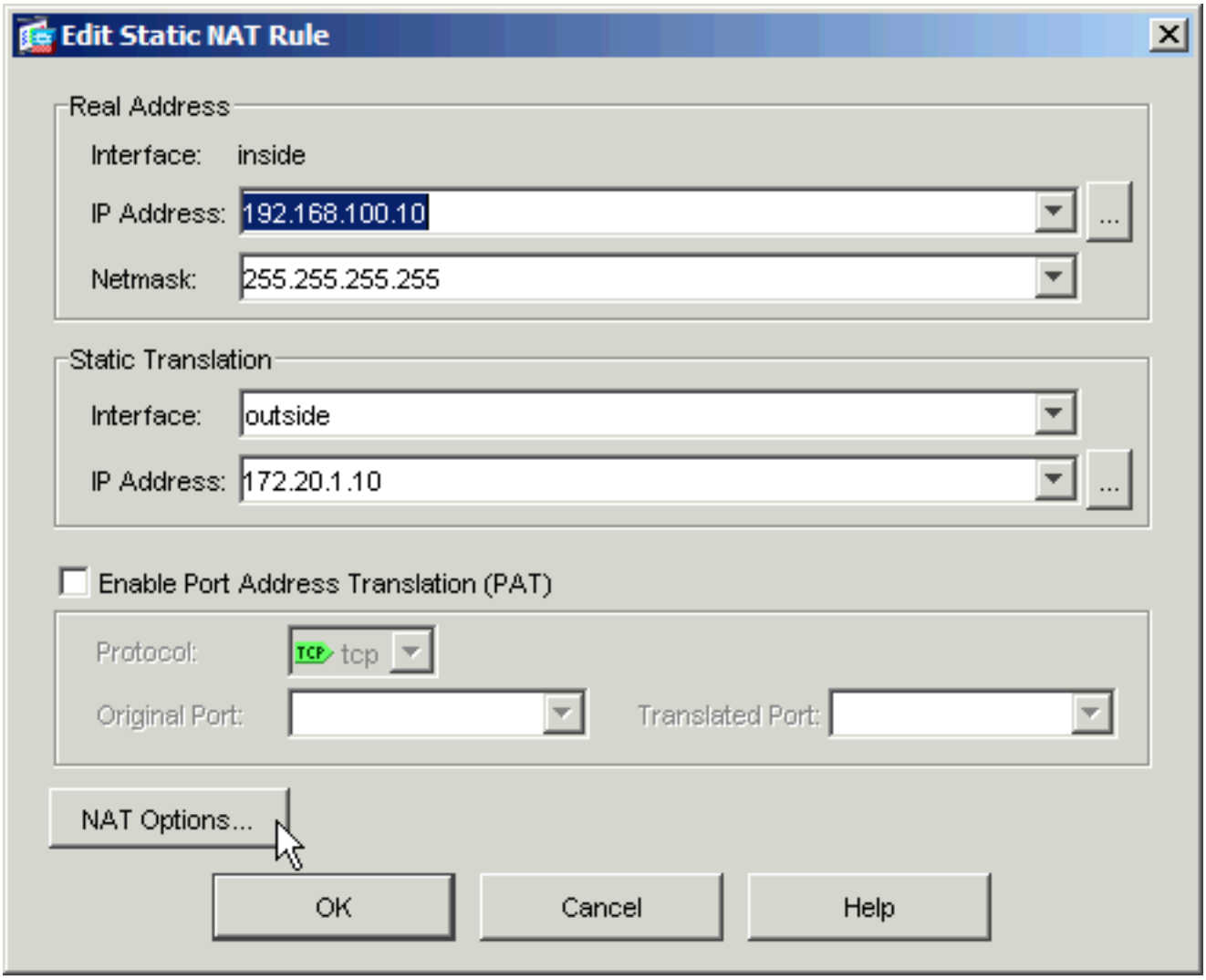
```
ciscoasa(config)#show run
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa

!--- 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.
```

完成以下步驟，以便在ASDM中配置DNS修正：

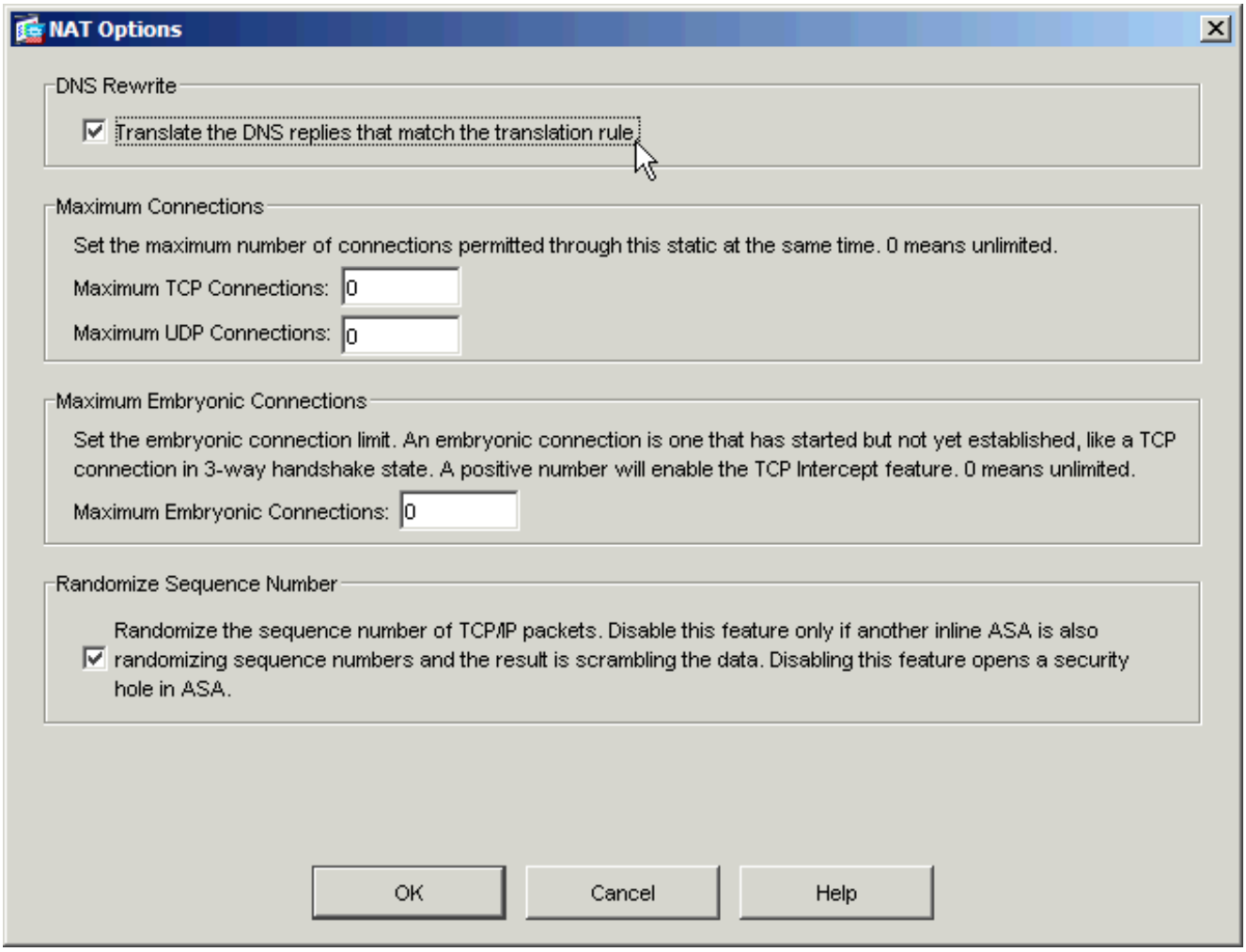
1. 導航到**Configuration > NAT**，然後選擇要修改的靜態NAT規則。按一下「**Edit**」。



2. 按一下**NAT Options...**。



3. 選中**Translate DNS replies that match the translation rule**覈取方塊。



4. 按一下**OK**以離開NAT Options視窗。按一下**OK**以離開Edit Static NAT Rule視窗。按一下**Apply**將配置傳送到安全裝置。

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
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. 此時，客戶端嘗試訪問地址為192.168.100.10的WWW伺服器。連線成功。由於客戶端和伺服器位於同一子網中，因此ASA上不會捕獲任何流量。

使用「dns」關鍵字的最終配置

這是使用**dns**關鍵字和兩個NAT介面執行DNS修補的ASA的最終配置。

最終ASA 7.2(1)配置

```
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
```

備選解決方案：迴轉傳輸

使用靜態NAT的迴轉傳輸

注意：使用靜態NAT的迴轉工作包括通過安全裝置在客戶端和WWW伺服器之間傳送所有流量。實施此解決方案之前，請仔細考慮預期流量和安全裝置的功能。

迴轉是流量從到達的同一介面傳回的過程。此功能已在安全裝置軟體7.0版中引入。對於7.2(1)之前的版本，要求至少對髮夾流量（入站或出站）的一個分支進行加密。從7.2(1)及更高版本開始，此要求不再適用。使用7.2(1)時，傳入流量和傳出流量可能均未加密。

使用髮夾功能，結合靜態NAT語句，可以獲得與DNS修正相同的效果。此方法不會更改從DNS伺服器返回到客戶端的DNS A記錄的內容。反之，當使用迴轉時（例如本檔案所討論的情境），使用者端可以使用DNS伺服器傳回的**172.20.1.10位址進行連線。**

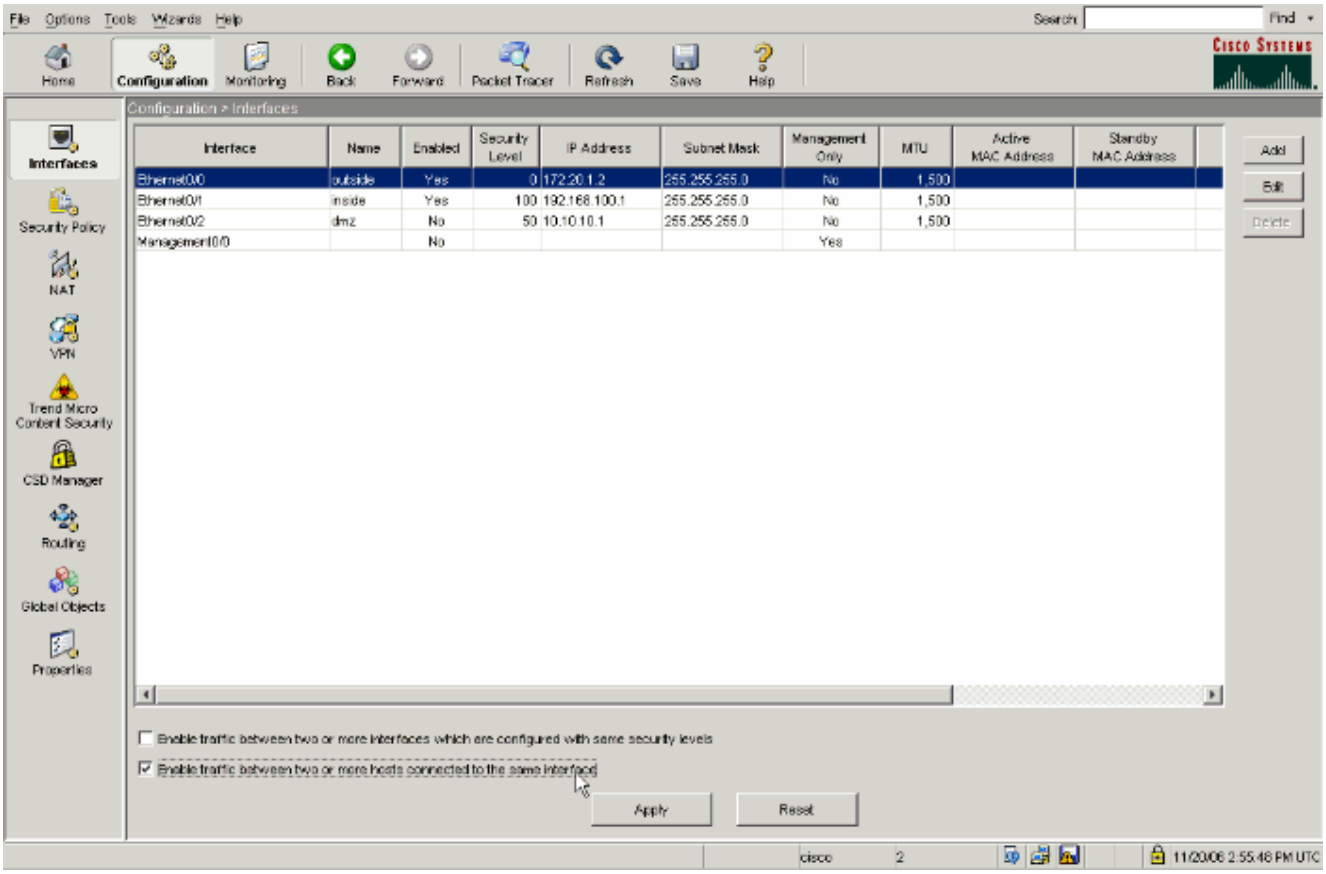
以下是使用迴轉和靜態NAT實現DNS修正效果時，配置的相關部分的外觀。以粗體顯示的命令在本輸出末尾有更詳細的說明：

```
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.
```

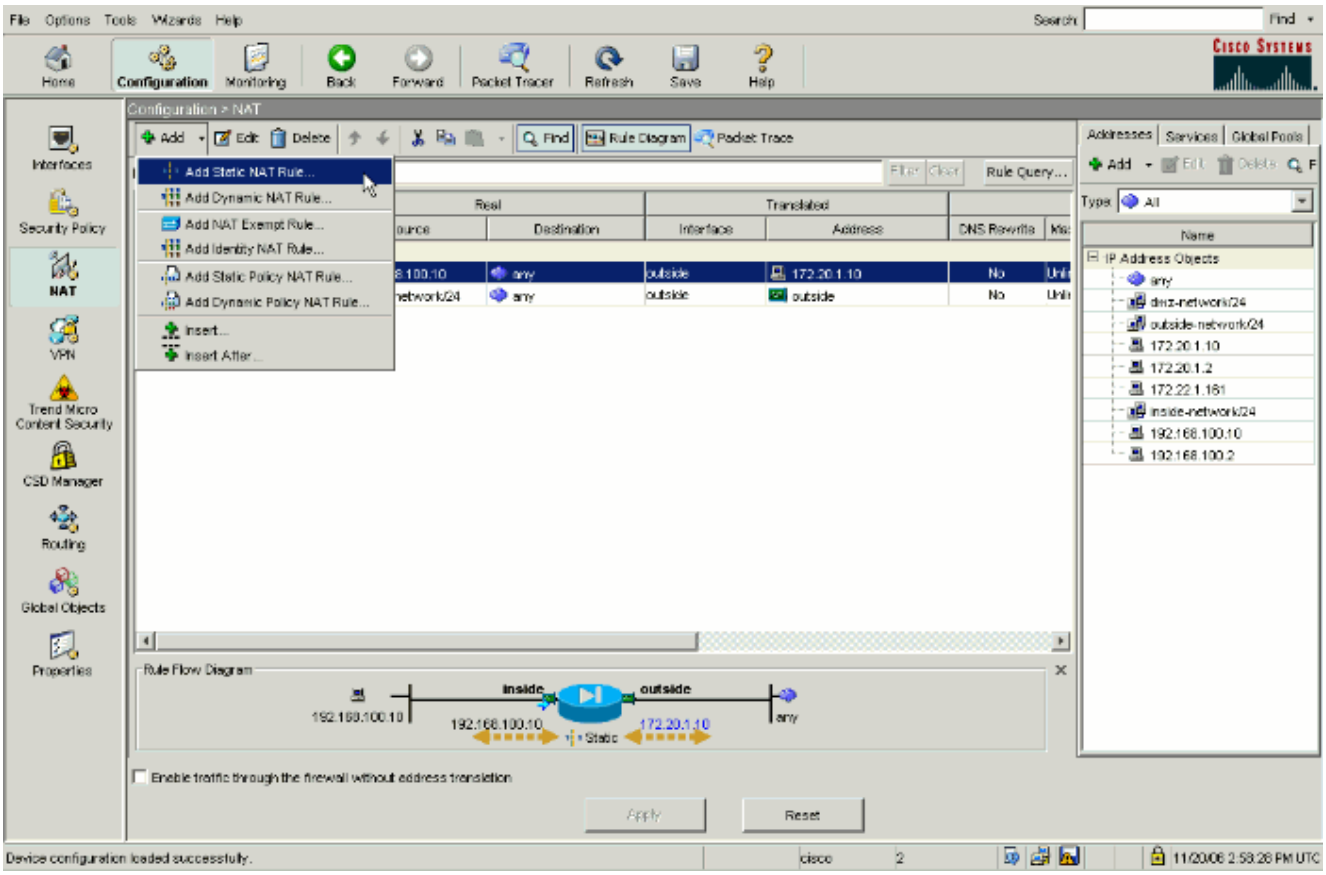
- **same-security-traffic** — 此命令允許安全級別相同的流量傳輸安全裝置。**permit intra-interface**關鍵字允許相同安全流量進入和離開相同介面，因此啟用迴轉功能。**注意：**請參閱 same-security-traffic，瞭解有關迴轉分析和**same-security-traffic命令的詳細**資訊。
- **global(inside)1介面** — 通過安全裝置的所有流量都必須進行NAT。此命令使用安全裝置的內部介面地址，以使進入內部介面的流量在從其內部介面重新髮夾時進行PAT。
- **static(inside，inside)172.20.1.10 192.168.100.10 netmask 255.255.255.255** — 此靜態NAT條目為WWW伺服器的公共IP地址建立第二個對映。但是，與第一個靜態NAT條目不同，這次地址172.20.1.10對映到安全裝置的內部介面。這樣，安全裝置就可以響應在內部介面上看到的此地址請求。然後，它通過自身將這些請求重定向到WWW伺服器的實際地址。

完成以下步驟，以便在ASDM中使用靜態NAT配置迴轉傳輸：

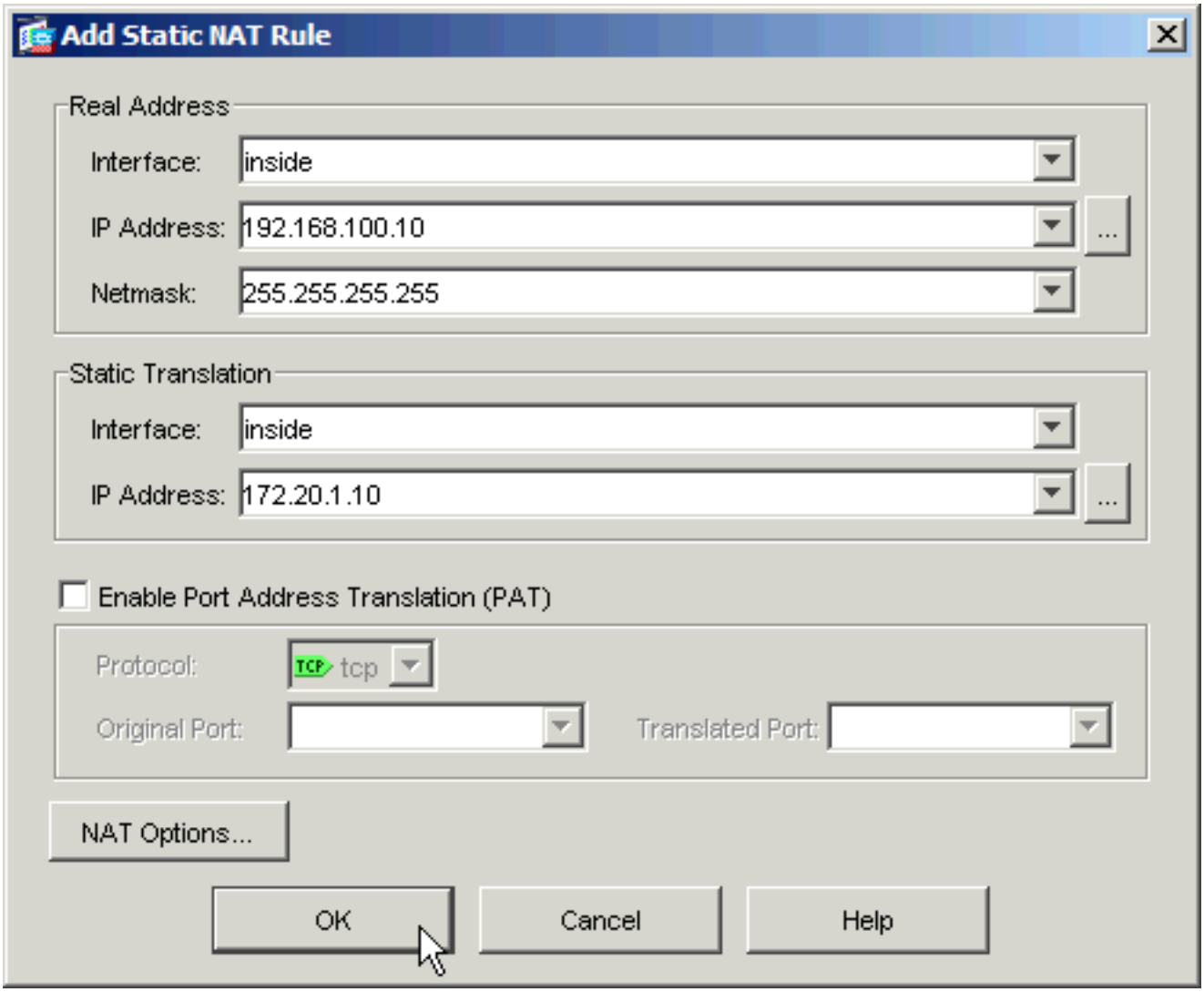
1. 導覽至**Configuration > Interfaces**。
2. 在視窗底部，選中**Enable traffic between two or more hosts connected to same interface**覈取方塊。



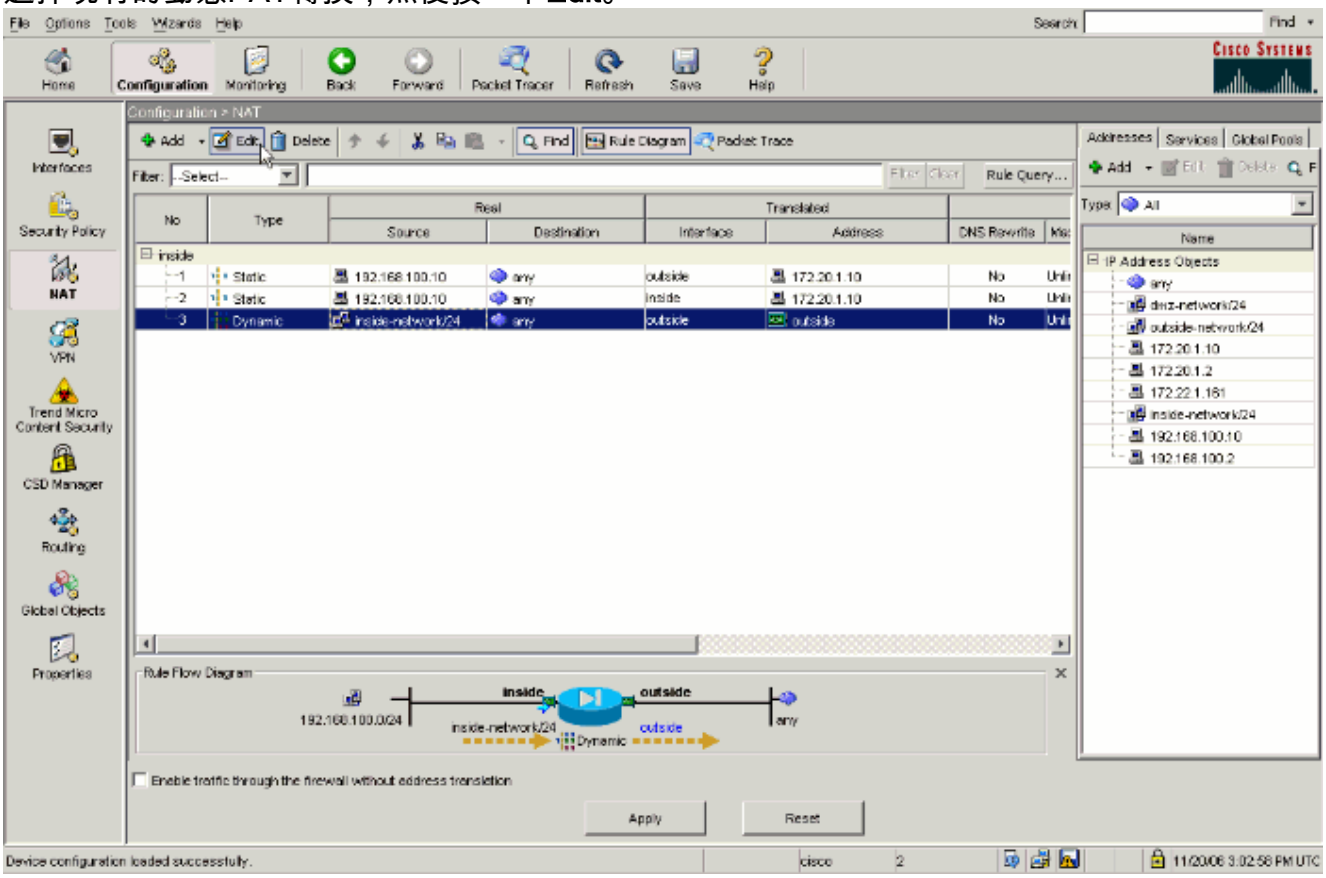
3. 按一下「**Apply**」。
4. 導航到**Configuration > NAT**，然後選擇**Add > Add Static NAT Rule...**。



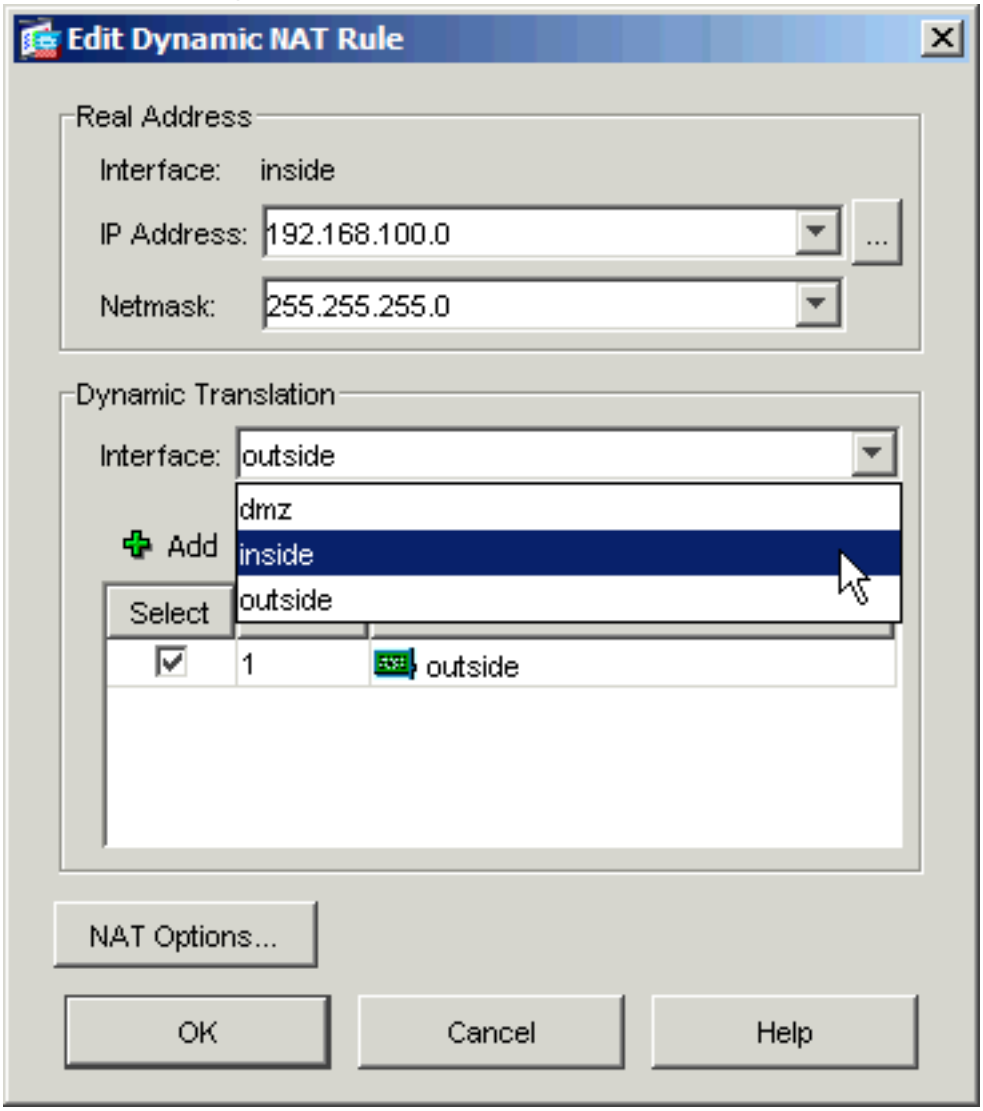
5. 填寫新靜態轉換的配置。使用WWW伺服器資訊填充**Real Address**區域。使用要將WWW伺服器對映到的地址和介面填充**靜態轉換**區域。在這種情況下，選擇內部介面以允許內部介面上的主機通過對映地址172.20.1.10訪問WWW伺服器。

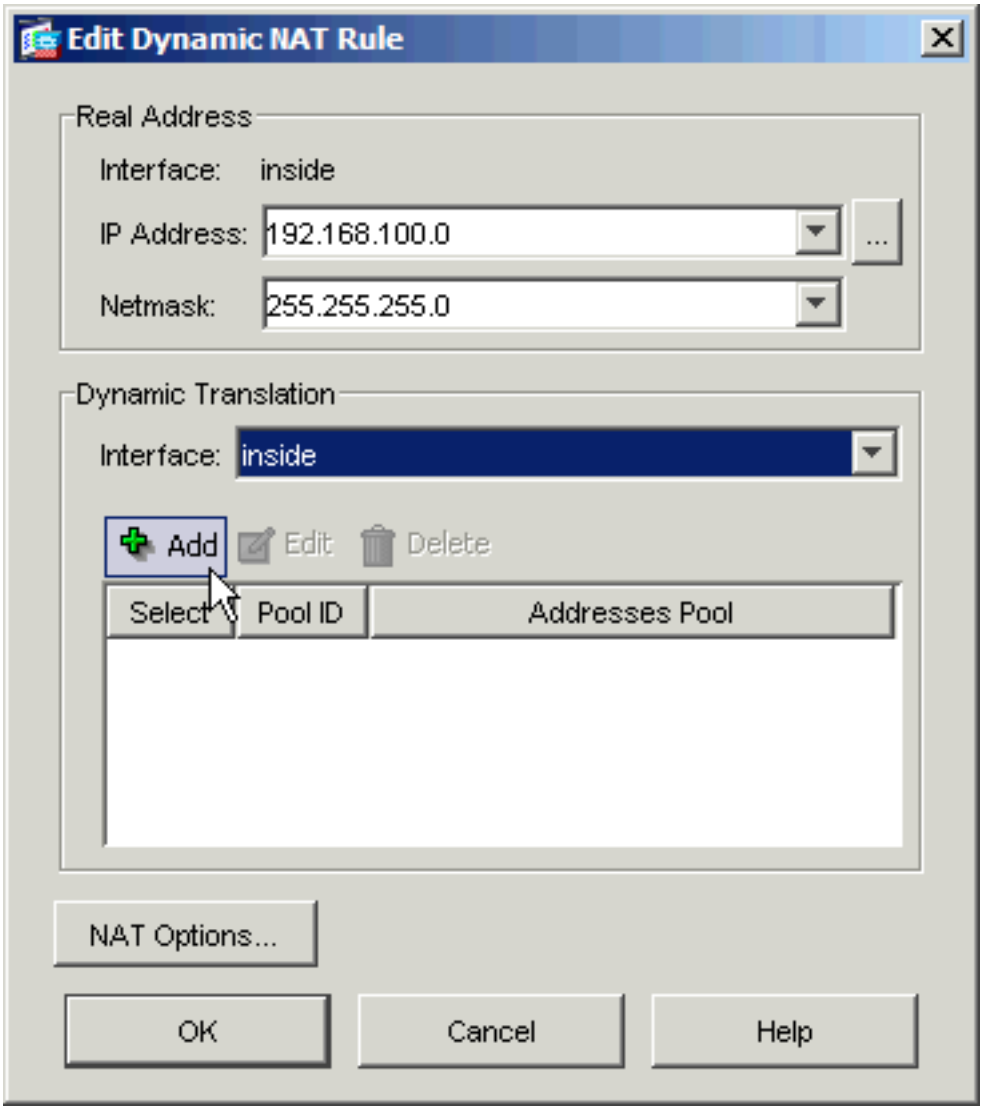


6. 按一下**OK**以離開Add Static NAT Rule視窗。
7. 選擇現有的動態PAT轉換，然後按一下**Edit**。

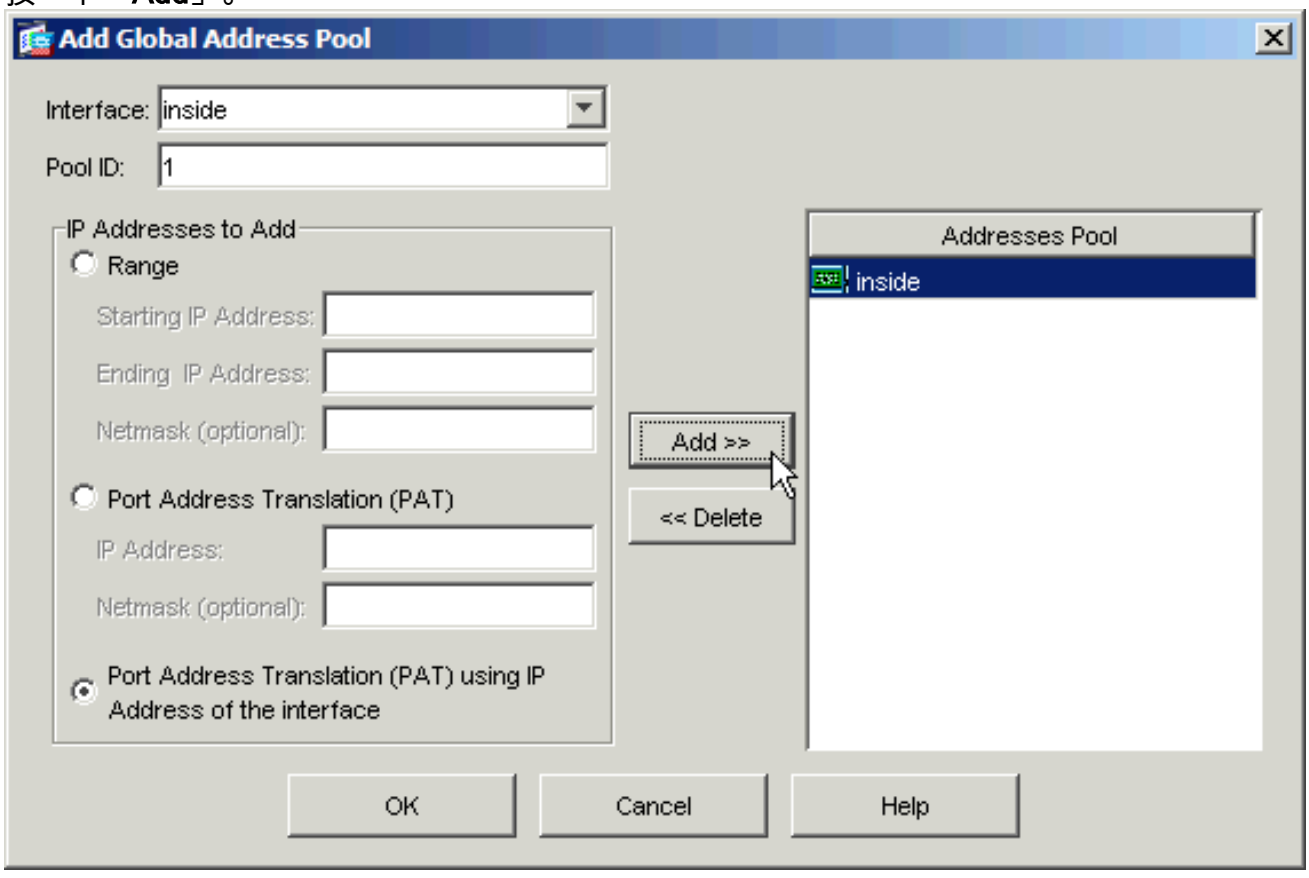


8. 從Interface下拉框中選擇**inside**。





9. 按一下「**Add**」。
10. 選擇標有**Port Address Translation(PAT) using the IP address of the interface**的單選按鈕。按一下「**Add**」。



11. 按一下**OK**以退出「新增全域性地址池」視窗。按一下**OK**以離開Edit Dynamic NAT Rule視窗。按一下**Apply**將配置傳送到安全裝置。

以下是配置髮夾時發生的事件序列。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伺服器位於192.168.100.10。
   ```
   %ASA-7-609001: Built local-host inside:192.168.100.10
   ```
3. 安全裝置為客戶端建立動態PAT轉換。客戶端流量的源現在是安全裝置的內部介面：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. 安全裝置通過自身在客戶端和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 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. 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。
   ```
   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. 安全裝置上的**show conn**命令驗證安全裝置和WWW伺服器之間是否已成功代表客戶端進行連線。在括弧中記下客戶端的實際地址。
   ```
   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
   ```

使用迴轉和靜態NAT的最終配置

這是ASA的最終配置，它使用迴轉和靜態NAT通過兩個NAT介面實現DNS修正效果。

最終ASA 7.2(1)配置

```
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
```

注意：請參閱此影片Hair-pinning on Cisco ASA (僅限註冊客戶)，瞭解有關可以使用髮夾的不同方案的詳細資訊。

配置DNS檢測

要啟用DNS檢查（如果之前已禁用），請執行以下步驟。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。有關服務策略和檢查的詳細資訊，請參閱使用模組化策略框架。

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指定檢查引擎的引數。
   ```
   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，指定應使用步驟1-3中建立的檢查策略對映檢查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
```

拆分DNS配置

在組策略配置模式下發出**split-dns**命令，以輸入通過拆分隧道解析的域清單。使用此命令的***no***形式可刪除清單。

如果沒有拆分隧道域清單，使用者將繼承預設組策略中存在的任何清單。發出**split-dns none**命令可防止繼承分割隧道域清單。

使用單個空格分隔域清單中的每個條目。條目數沒有限制，但整個字串長度不能超過255個字元。只能使用字母數字字元、連字元(-)和句點(.)。 不帶引數的**no split-dns**命令將刪除所有當前值，其中包括在您發出**split-dns none**命令時建立的空值。

此示例說明如何配置域Domain1、Domain2、Domain3和Domain4，以便通過名為FirstGroup的組策略的拆分隧道進行解析：

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

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）以pcap格式將捕獲複製到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。請參閱配置DNS檢測部分。

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 dmz:10.10.10.10/23
```

清除xlate條目，然後刪除並重新應用NAT語句以解決此錯誤。

丟棄UDP DNS回覆

由於DNS封包捨棄，您可能會收到此錯誤訊息：

```
 %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.
```

增加512-65535之間的DNS資料包長度以解決此問題。

範例：

```
ciscoasa(config)#policy-map type inspect dns MY_DNS_INSPECT_MAP
ciscoasa(config-pmap)#parameters
ciscoasa(config-pmap-p)#message-length maximum <512-65535>
```

相關資訊

- Cisco PIX防火牆軟體
- Cisco Secure PIX防火牆命令參考
- 安全產品現場通知
- 要求建議(RFC)
- 在Cisco ASA上固定頭髮
- Cisco ASA 5500系列調適型安全裝置