PIX/ASA Eseguire la funzionalità di documentazione DNS con il comando statico e due esempi di configurazione di interfacce NAT

Sommario

Introduzione

In questo documento viene fornita una configurazione di esempio per eseguire la documentazione DNS (Domain Name System) su ASA 5500 Series Adaptive Security Appliance o PIX 500 Security Appliance con istruzioni NAT (Network Address Translation) statiche. Il servizio di archiviazione DNS consente all'appliance di sicurezza di riscrivere i record A DNS.

La riscrittura DNS esegue due funzioni:

- Converte un indirizzo pubblico (l'indirizzo instradabile o mappato) in una risposta DNS in un indirizzo privato (l'indirizzo reale) quando il client DNS si trova su un'interfaccia privata.
- Converte un indirizzo privato in un indirizzo pubblico quando il client DNS si trova nell'interfaccia pubblica.

Nota: la configurazione in questo documento contiene due interfacce NAT; dentro e fuori. Per un esempio di dottorato DNS con statistiche e tre interfacce NAT (interna, esterna e dmz), fare riferimento a PIX/ASA: Eseguire la documentazione DNS con il comando statico e con l'esempio di configurazione a tre interfacce NAT.

Per ulteriori informazioni su come usare NAT su un appliance di sicurezza, fare riferimento alle istruzioni PIX/ASA 7.x NAT e PAT e Using nat, global, static, conduit, and access-list Commands and Port Redirection (Forwarding) on PIX.

Prerequisiti

Requisiti

Per eseguire il servizio di archiviazione DNS sull'accessorio di sicurezza, è necessario attivare l'ispezione DNS. L'ispezione DNS è attiva per impostazione predefinita. Se è stata disattivata, vedere la sezione Configurazione ispezione DNS più avanti in questo documento per riattivarla. Quando il controllo DNS è attivato, l'accessorio di protezione esegue le seguenti attività:

- Traduce il record DNS in base alla configurazione completata utilizzando i comandi **static** e **nat** (riscrittura DNS). La conversione si applica solo al record A nella risposta DNS. Le ricerche inverse, che richiedono il record PTR, non sono pertanto interessate dalla riscrittura del DNS.**Nota: la** riscrittura del DNS non è compatibile con PAT (Port Address Translation) statico perché per ogni record A sono applicabili più regole PAT e la regola PAT da utilizzare è ambigua.
- Applica la lunghezza massima dei messaggi DNS (il valore predefinito è 512 byte e la lunghezza massima è 65535 byte). Il riassemblaggio viene eseguito se necessario per verificare che la lunghezza del pacchetto sia inferiore alla lunghezza massima configurata. Il pacchetto viene scartato se supera la lunghezza massima.**Nota:** se si esegue il comando **inspect dns** senza l'opzione maximum-length, le dimensioni del pacchetto DNS non vengono controllate.
- Impone una lunghezza del nome di dominio di 255 byte e una lunghezza dell'etichetta di 63 byte.
- Verifica l'integrità del nome di dominio a cui fa riferimento il puntatore se vengono rilevati puntatori di compressione nel messaggio DNS.
- Verifica se esiste un loop del puntatore di compressione.

Componenti usati

Il riferimento delle informazioni contenute in questo documento è ASA serie 5500 Security Appliance, versione 7.2(1).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Questa configurazione può essere utilizzata anche con Cisco PIX serie 500 Security Appliance

versione 6.2 o successive.

Nota: la configurazione di Cisco Adaptive Security Device Manager (ASDM) è applicabile solo alla versione 7.x.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

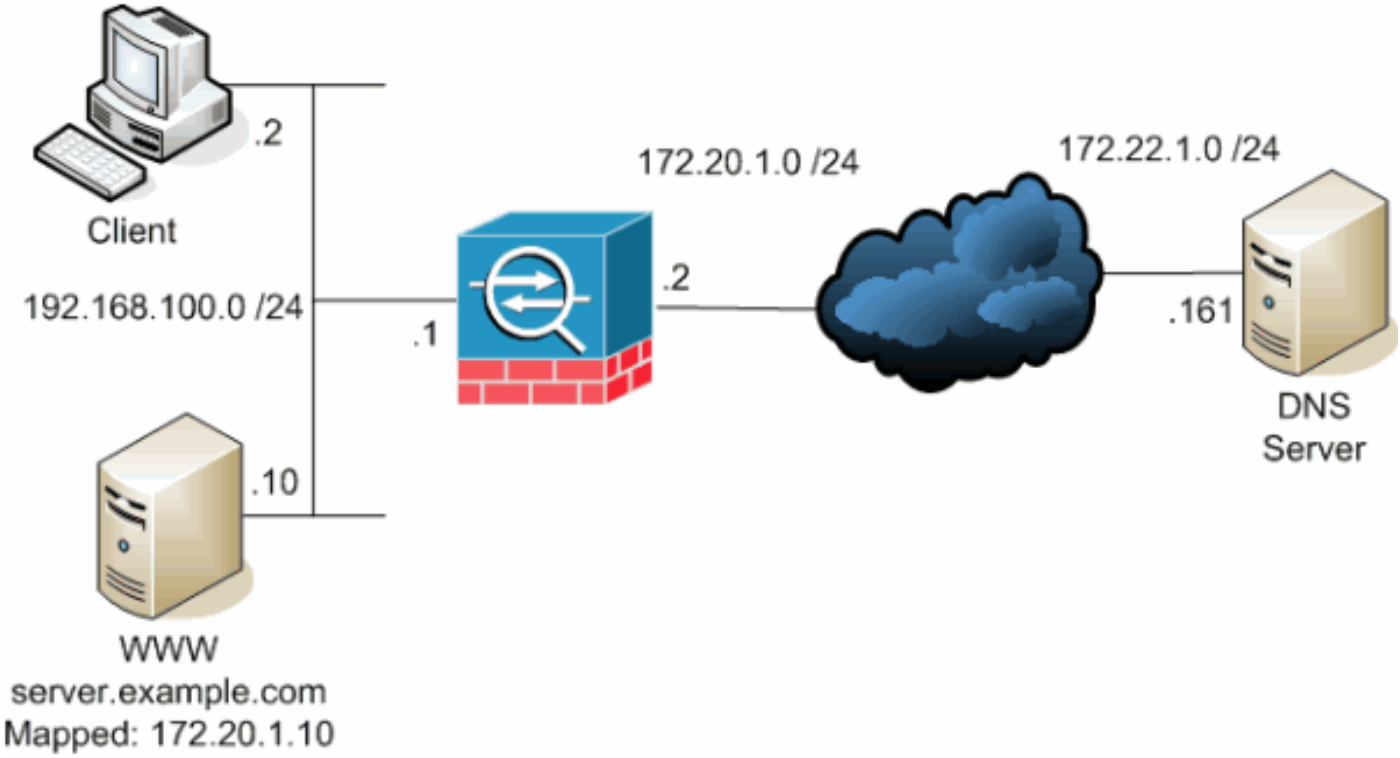
Premesse

In uno scambio DNS tipico un client invia un URL o un nome host a un server DNS per determinare l'indirizzo IP di tale host. Il server DNS riceve la richiesta, cerca il mapping nome-indirizzo IP per l'host e quindi fornisce il record A con l'indirizzo IP al client. Sebbene questa procedura funzioni bene in molte situazioni, possono verificarsi problemi. Questi problemi possono verificarsi quando il client e l'host che il client tenta di raggiungere si trovano entrambi nella stessa rete privata dietro NAT, ma il server DNS utilizzato dal client si trova in un'altra rete pubblica.

Scenario: Due interfacce NAT (interna, esterna)

Topologia

In questo scenario, il client e il server WWW che il client cerca di raggiungere si trovano entrambi sull'interfaccia interna dell'appliance ASA. PAT dinamico è configurato per consentire al client l'accesso a Internet. Il protocollo NAT statico con un elenco degli accessi è configurato per consentire al server l'accesso a Internet e agli host Internet di accedere al server WWW.



Questo diagramma è un esempio di questa situazione. In questo caso, il client in 192.168.100.2 desidera utilizzare l'URL di **server.example.com** per accedere al server WWW in 192.168.100.10. I

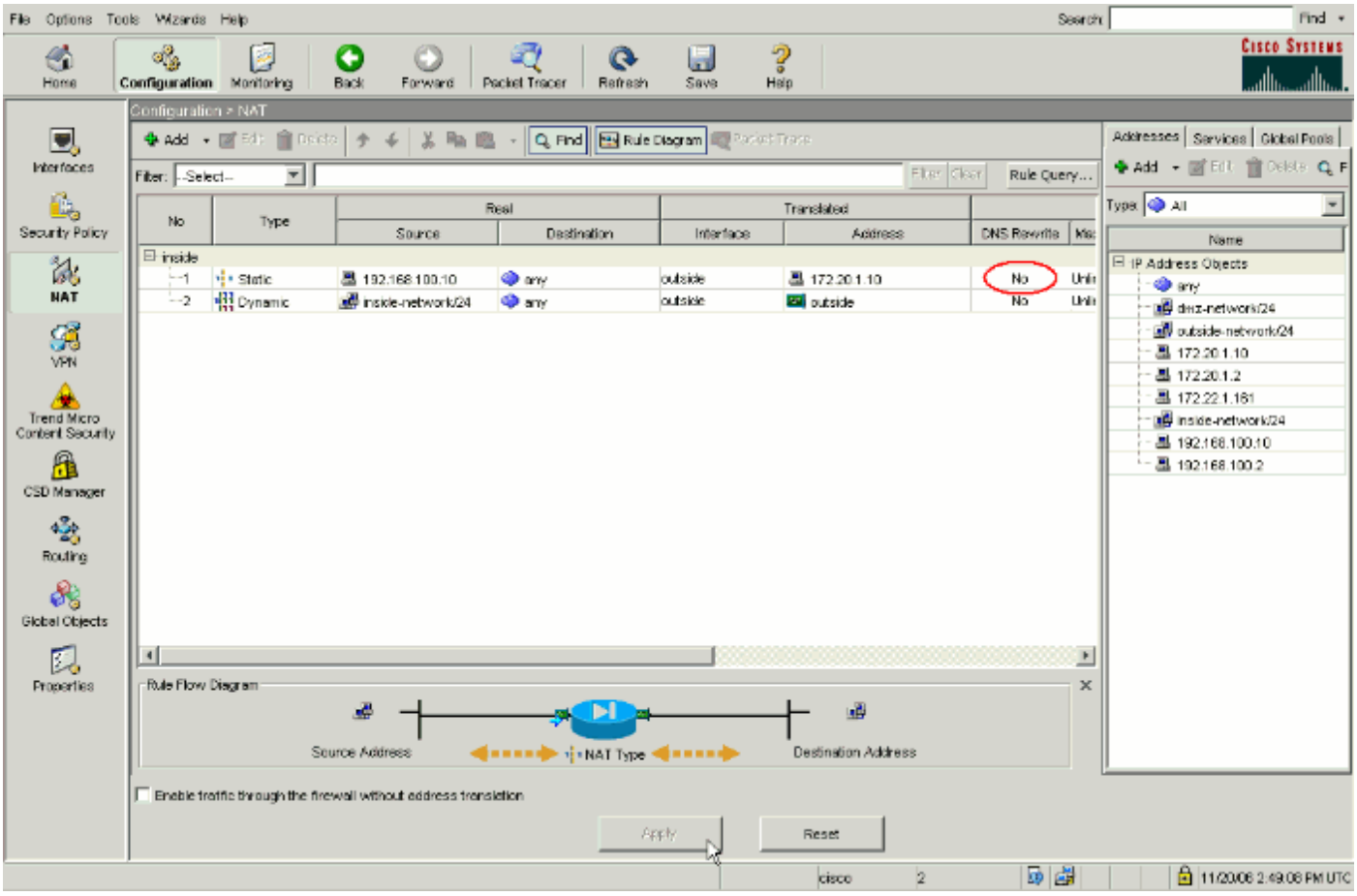
servizi DNS per il client vengono forniti dal server DNS esterno in 172.22.1.161. Poiché il server DNS si trova in un'altra rete pubblica, non conosce l'indirizzo IP privato del server WWW. Conosce invece l'indirizzo mappato del server WWW 172.20.1.10. Pertanto, il server DNS contiene il mapping da indirizzo IP a nome di **server.example.com** a **172.20.1.10**.

Problema: Il client non può accedere al server WWW

Se in questa situazione non è abilitata la funzionalità di protezione DNS o un'altra soluzione, il client non sarà in grado di accedere al server WWW se invia una richiesta DNS per l'indirizzo IP server.example.com. Il client riceve infatti un record A contenente l'indirizzo pubblico mappato: 172.20.1.10 del server WWW. Quando il client tenta di accedere a questo indirizzo IP, l'appliance di sicurezza scarta i pacchetti perché non consente il reindirizzamento dei pacchetti sulla stessa interfaccia. Di seguito è riportato l'aspetto della parte NAT della configurazione quando la funzionalità di gestione DNS non è abilitata:

```
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.
```

Questo è l'aspetto della configurazione in ASDM quando la funzionalità di archiviazione DNS non è abilitata:



Di seguito è riportata un'acquisizione di pacchetti degli eventi quando la funzionalità di archiviazione DNS non è abilitata:

1. Il client invia la query 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. Il PAT viene eseguito sulla query DNS dall'ASA e la query viene inoltrata. L'indirizzo di origine del pacchetto è stato modificato nell'interfaccia esterna dell'appliance 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. Il server DNS risponde con l'indirizzo mappato del server 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 annulla la conversione dell'indirizzo di destinazione della risposta DNS e inoltra il pacchetto al client. Si noti che se non è abilitata la funzionalità di archiviazione DNS, l'indirizzo nella risposta rimane l'indirizzo mappato del server 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 questo punto, il client tenta di accedere al server WWW all'indirizzo 172.20.1.10. L'ASA crea una voce di connessione per questa comunicazione. Tuttavia, poiché non consente il flusso del traffico dall'interno all'esterno all'interno, la connessione scade. I log ASA mostrano quanto segue:

```
%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
```

Soluzione: Parola chiave "dns"

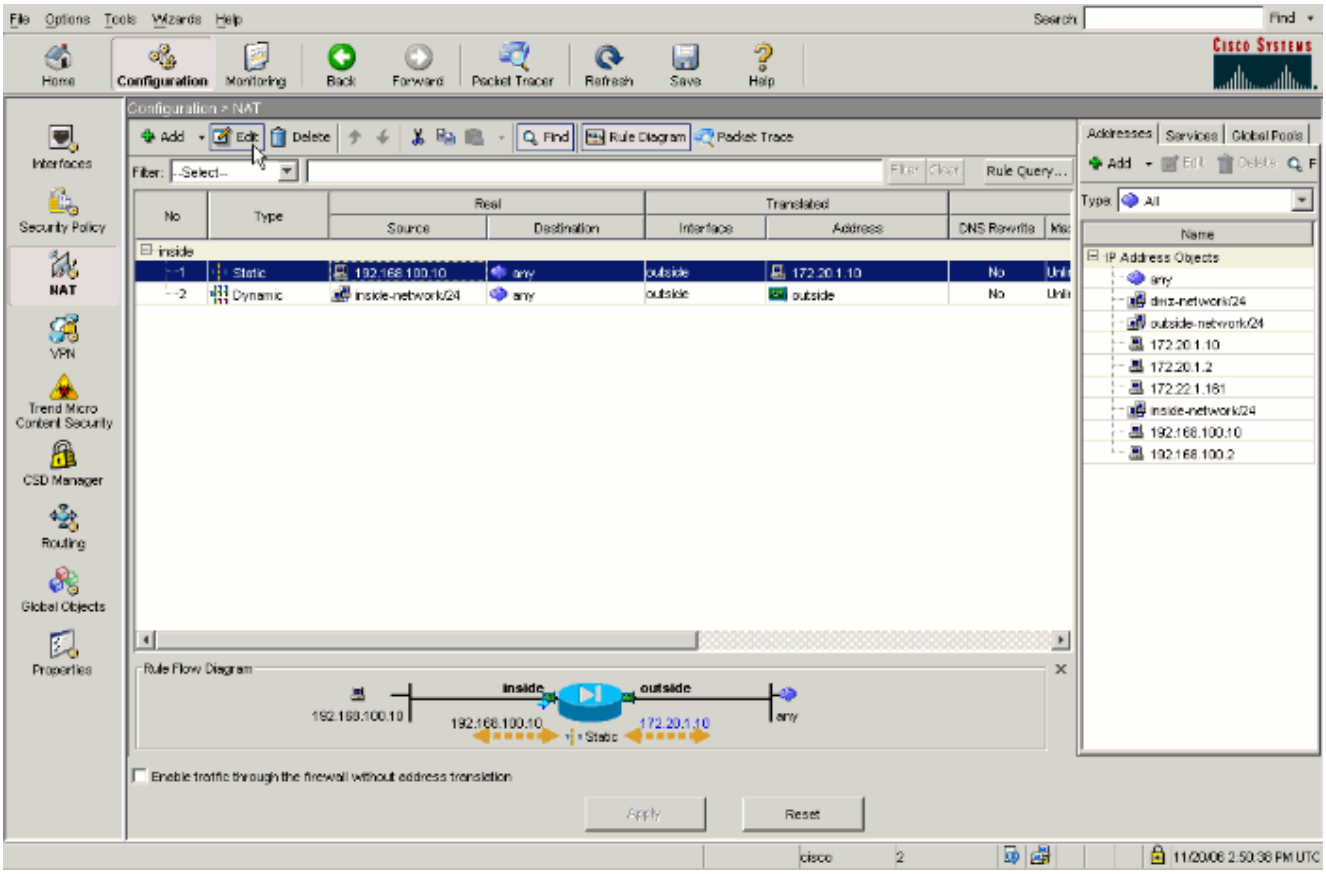
Documentazione DNS con la parola chiave "dns"

La funzione di archiviazione DNS con la parola chiave **dns** consente all'appliance di sicurezza di intercettare e riscrivere il contenuto delle risposte del server DNS al client. Quando è configurato correttamente, l'appliance di sicurezza può modificare il record A per consentire al client di procedere in uno scenario simile a quello illustrato nella sezione Problema: Il client non può accedere alla sezione del server WWW per connettersi. In questo caso, con la funzionalità di protezione DNS abilitata, l'appliance di sicurezza riscrive il record A per indirizzare il client a **192.168.100.10**, anziché a **172.20.1.10**. La funzionalità di protezione DNS viene abilitata quando si aggiunge la parola chiave **dns** a un'istruzione NAT statica. Di seguito è riportato l'aspetto della parte NAT della configurazione quando è abilitata la gestione del DNS:

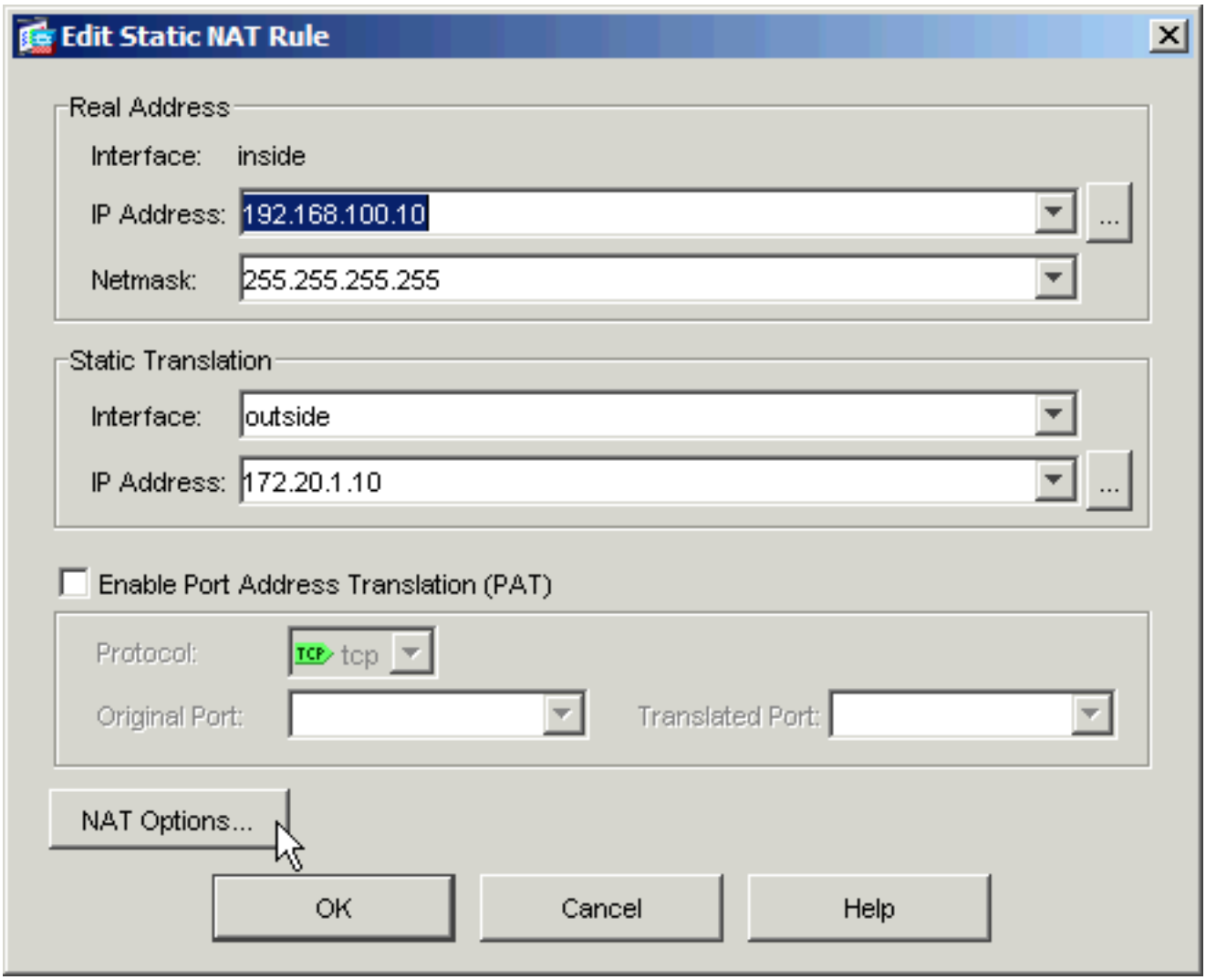
```
ciscoasa(config)#show run
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa

!--- 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.
```

Completare questa procedura per configurare la gestione del DNS in ASDM:

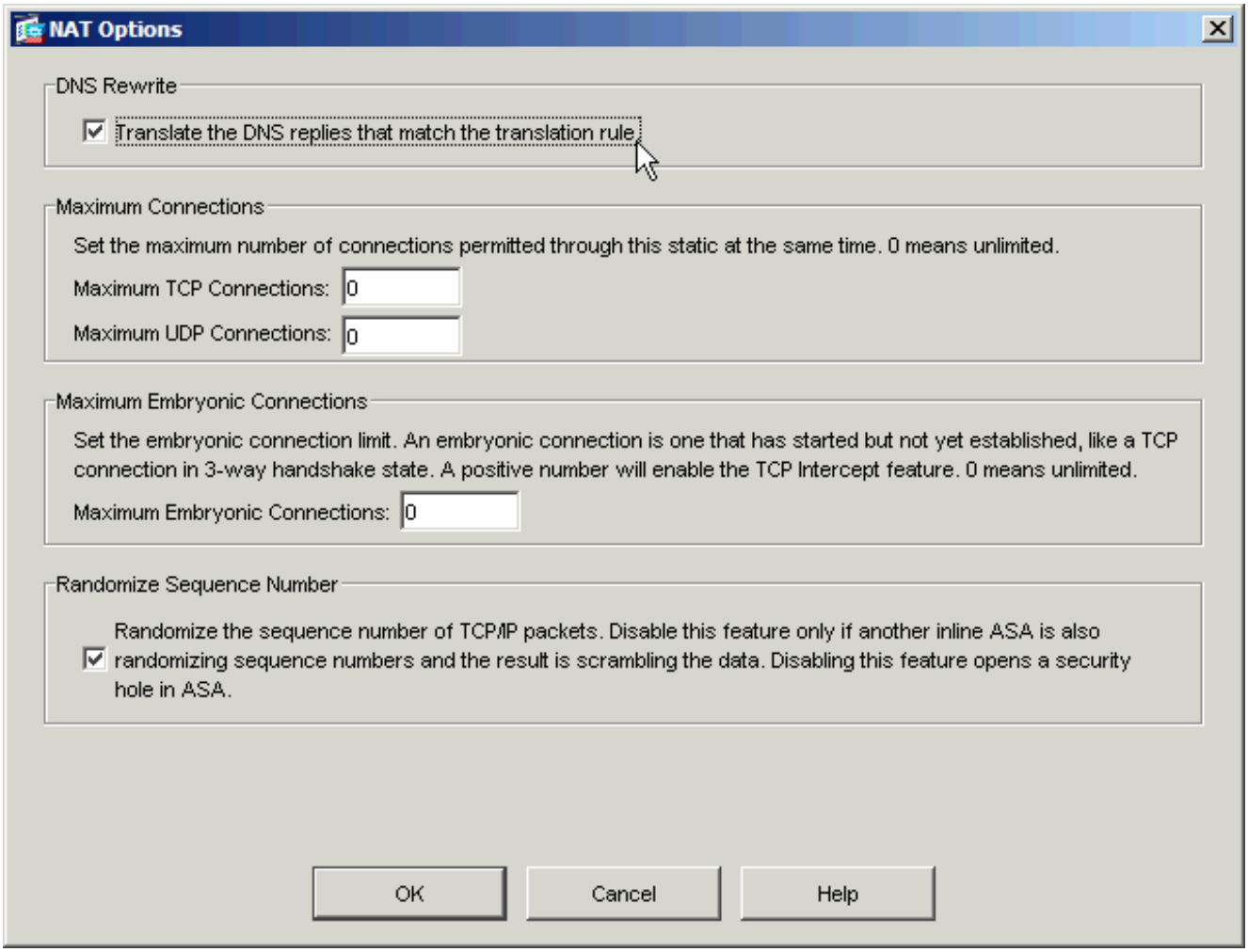
1. Passare a **Configurazione > NAT** e scegliere la regola NAT statica da modificare. Fare clic su **Modifica**.



2. Fare clic su **Opzioni NAT...**.



3. Selezionare la casella di controllo **Traduci risposte DNS corrispondenti alla regola di conversione**.



4. Fare clic su **OK** per uscire dalla finestra Opzioni NAT. Fare clic su **OK** per uscire dalla finestra Modifica regola NAT statica. Fare clic su **Applica** per inviare la configurazione all'appliance di sicurezza.

Di seguito è riportata un'acquisizione di pacchetti degli eventi quando è abilitata la gestione DNS:

1. Il client invia la query 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. Il PAT viene eseguito sulla query DNS dall'ASA e la query viene inoltrata. L'indirizzo di origine del pacchetto è stato modificato nell'interfaccia esterna dell'appliance 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. Il server DNS risponde con l'indirizzo mappato del server 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 annulla la conversione dell'indirizzo di destinazione della risposta DNS e inoltra il pacchetto al client. Si noti che se la funzionalità di gestione del DNS è abilitata, l'indirizzo **Addr** nella risposta viene riscritto in modo da corrispondere all'indirizzo reale del server 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. A questo punto, il client tenta di accedere al server WWW al numero 192.168.100.10. La connessione ha esito positivo. Sull'appliance ASA non viene acquisito alcun traffico perché il client e il server si trovano sulla stessa subnet.

Configurazione finale con la parola chiave "dns"

Questa è la configurazione finale dell'ASA per eseguire il docking DNS con la parola chiave **dns** e due interfacce NAT.

Configurazione finale di 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
```

Soluzione alternativa: Hairpinning

Hairpinning con NAT statico

Attenzione: l'hairpinning con NAT statico implica l'invio di tutto il traffico tra il client e il server WWW attraverso l'appliance di sicurezza. Prima di implementare questa soluzione, valutare attentamente la quantità di traffico prevista e le funzionalità dell'appliance di sicurezza.

L'hairpinning è il processo con il quale il traffico viene rimandato indietro dalla stessa interfaccia su cui è arrivato. Questa funzionalità è stata introdotta nel software per appliance di sicurezza versione 7.0. Per le versioni precedenti alla 7.2(1), è necessario crittografare almeno una parte del traffico bloccato (in entrata o in uscita). A partire dal punto 7.2(1), tale requisito non è più in vigore. Il traffico in entrata e il traffico in uscita potrebbero essere entrambi non crittografati quando si utilizza la versione 7.2(1).

L'hairpinning, in combinazione con un'istruzione NAT statica, può essere utilizzato per ottenere lo stesso effetto del doctoring DNS. Questo metodo non modifica il contenuto del record A DNS restituito dal server DNS al client. Quando si utilizza invece il hairpinning, come nello scenario illustrato in questo documento, il client può utilizzare l'indirizzo **172.20.1.10** restituito dal server DNS per connettersi.

Di seguito viene illustrato l'aspetto della parte rilevante della configurazione quando si utilizza il hairpinning e il protocollo NAT statico per ottenere un effetto di archiviazione DNS. I comandi in grassetto vengono spiegati più dettagliatamente alla fine di questo output:

```
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.
```

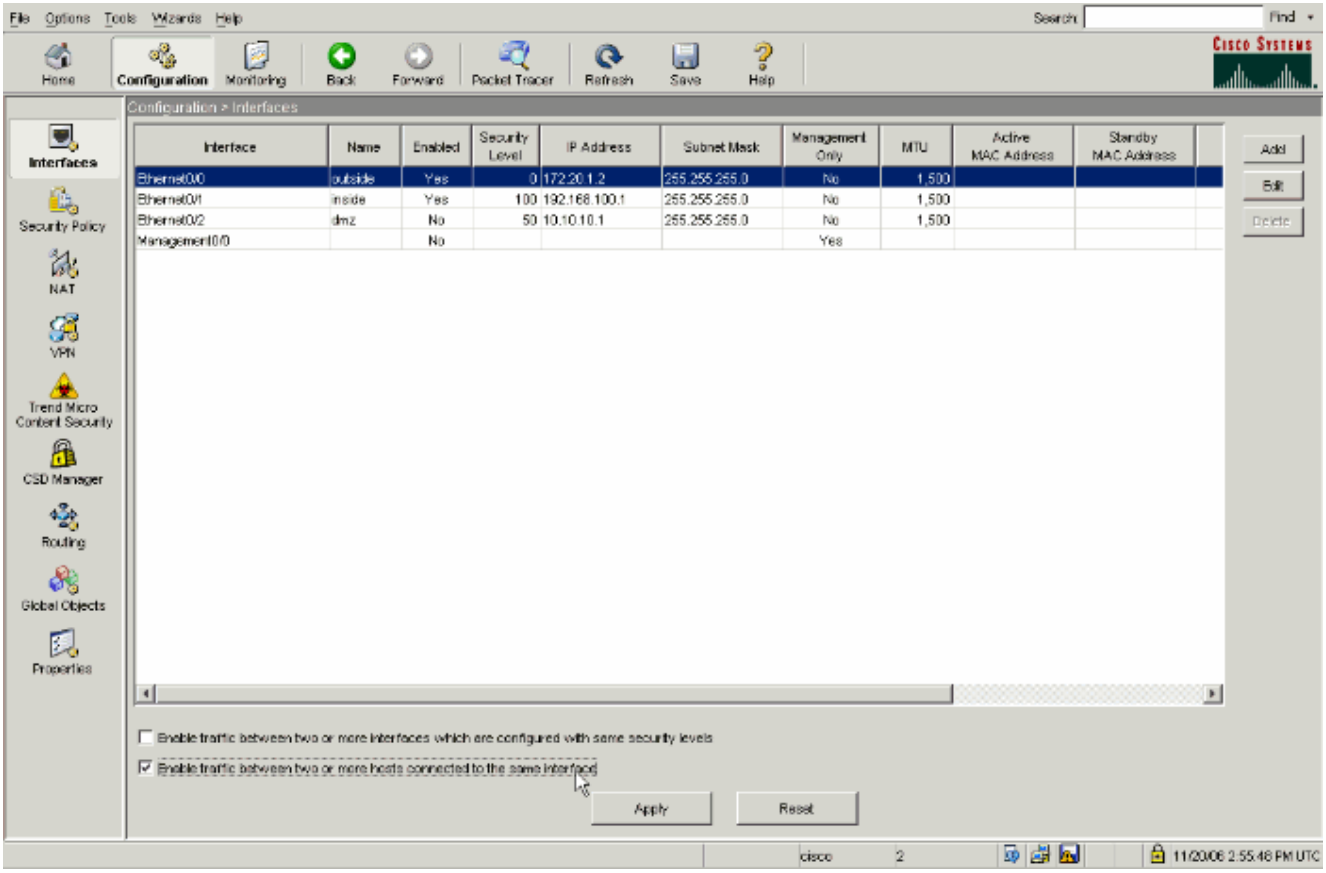
- **same-security-traffic**: questo comando consente al traffico con lo stesso livello di sicurezza di transitare sull'appliance di sicurezza. Le parole chiave **allow intra-interface** permettono a quel traffico di sicurezza stesso di entrare e uscire dalla stessa interfaccia, quindi è abilitato il hairpinning.**Nota: per** ulteriori informazioni sul hairpinning e sul comando **same-security-traffic,** fare riferimento a same-security-traffic.
- **interfaccia globale (interna) 1**: tutto il traffico che attraversa l'appliance di sicurezza deve

essere sottoposto a NAT. Questo comando utilizza l'indirizzo di interfaccia interno dell'appliance di sicurezza per bloccare il passaggio del traffico che entra nell'interfaccia interna mentre questa viene ritrasmessa verso l'esterno.

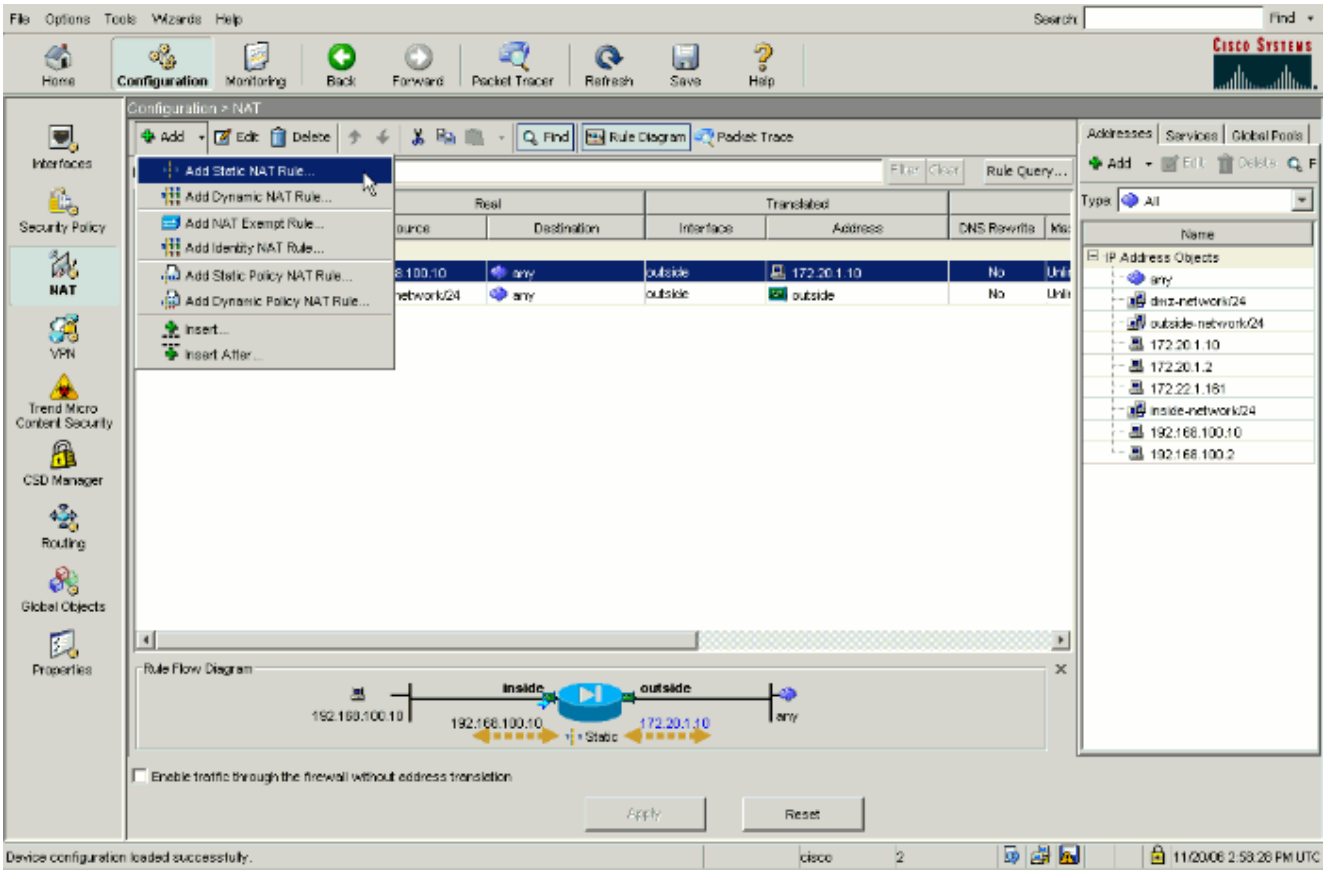
- **static (inside,inside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255**—Questa voce NAT statica crea una seconda mappatura per l'indirizzo IP pubblico del server WWW. Tuttavia, a differenza della prima voce NAT statica, questa volta l'indirizzo 172.20.1.10 è mappato sull'interfaccia interna dell'appliance di sicurezza. In questo modo l'appliance di sicurezza può rispondere alle richieste rilevate per questo indirizzo sull'interfaccia interna. Quindi, reindirizza tali richieste all'indirizzo reale del server WWW attraverso se stesso.

Completare questi passaggi per configurare il hairpinning con NAT statico in ASDM:

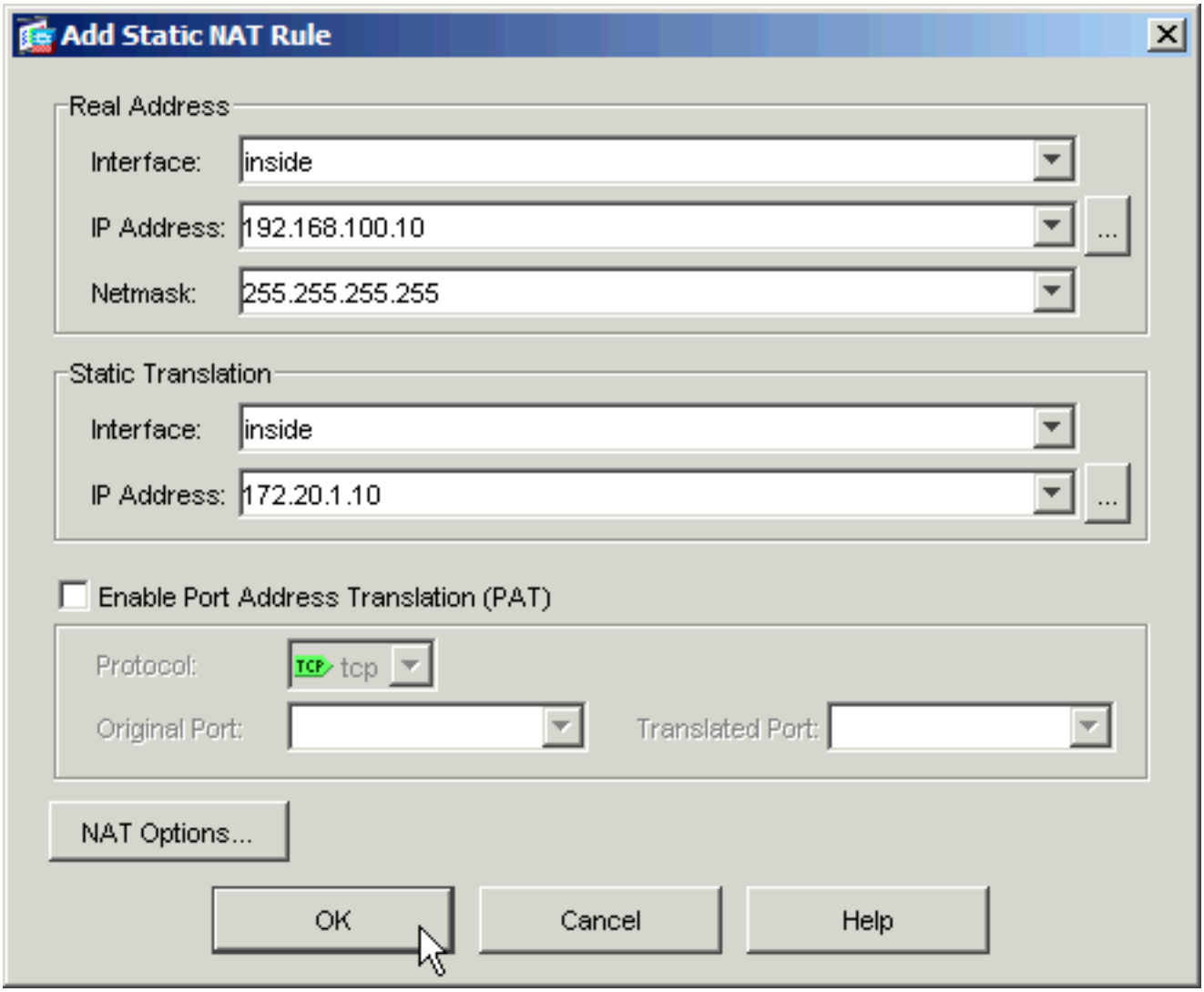
1. Selezionare **Configurazione > Interfacce**.
2. Nella parte inferiore della finestra selezionare la casella di controllo **Abilita traffico tra due o più host connessi alla stessa interfaccia**.



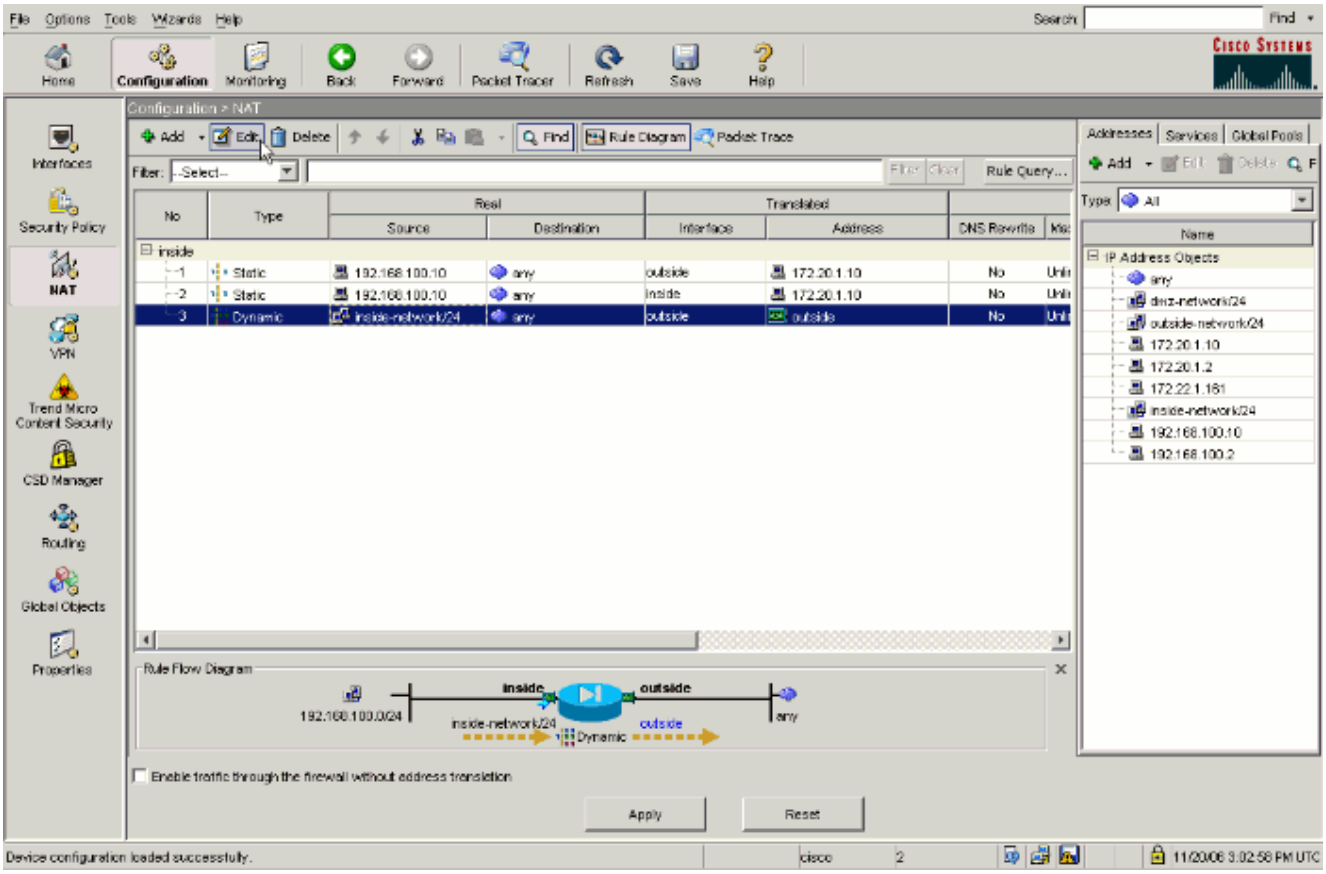
3. Fare clic su **Apply** (Applica).
4. Passare a **Configurazione > NAT** e scegliere **Aggiungi > Aggiungi regola NAT statica...**.



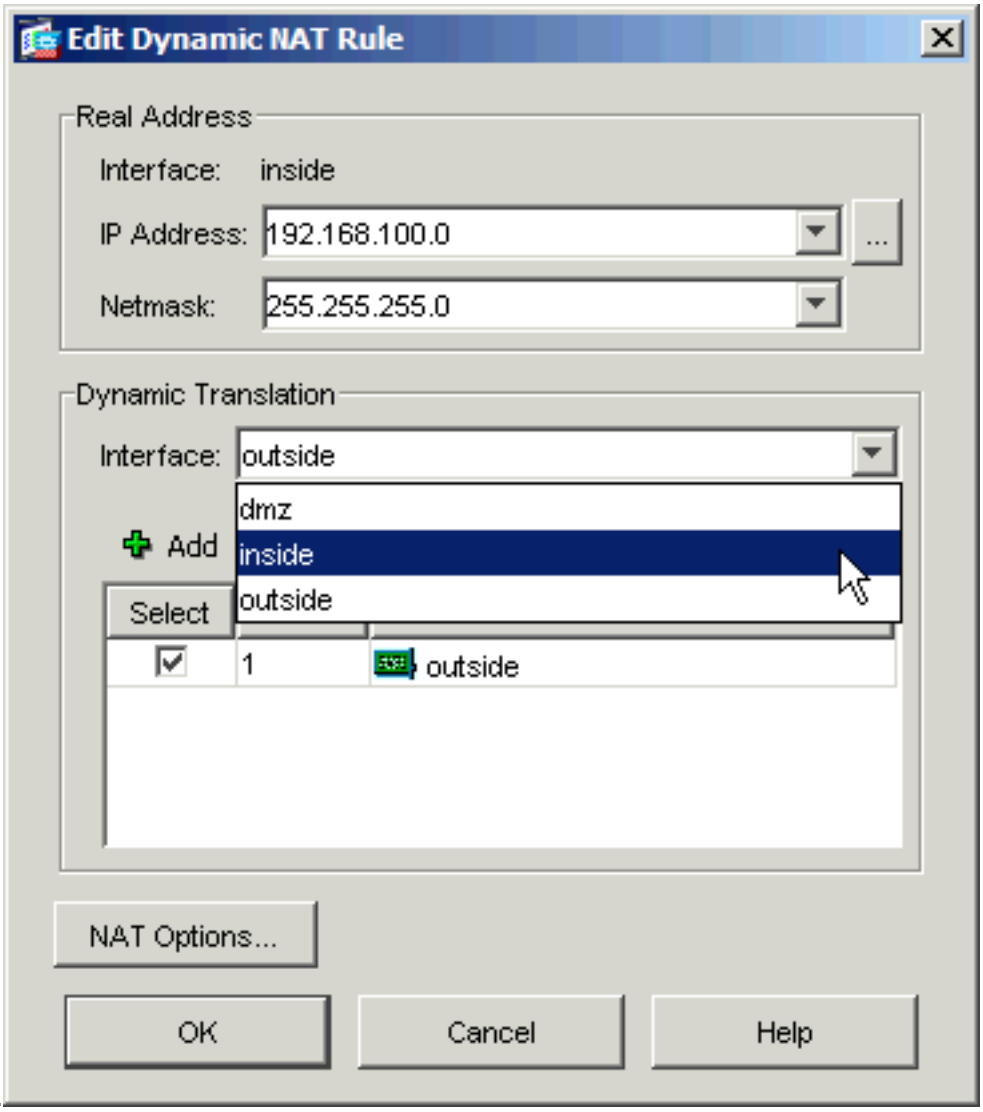
5. Completare la configurazione per la nuova traduzione statica.Popolare l'area **Real Address** con le informazioni sul server WWW.Popolare l'area **Traduzione statica** con l'indirizzo e l'interfaccia a cui si desidera mappare il server WWW.In questo caso, l'interfaccia interna è scelta per consentire agli host sull'interfaccia interna di accedere al server WWW tramite l'indirizzo mappato
   172.20.1.10.

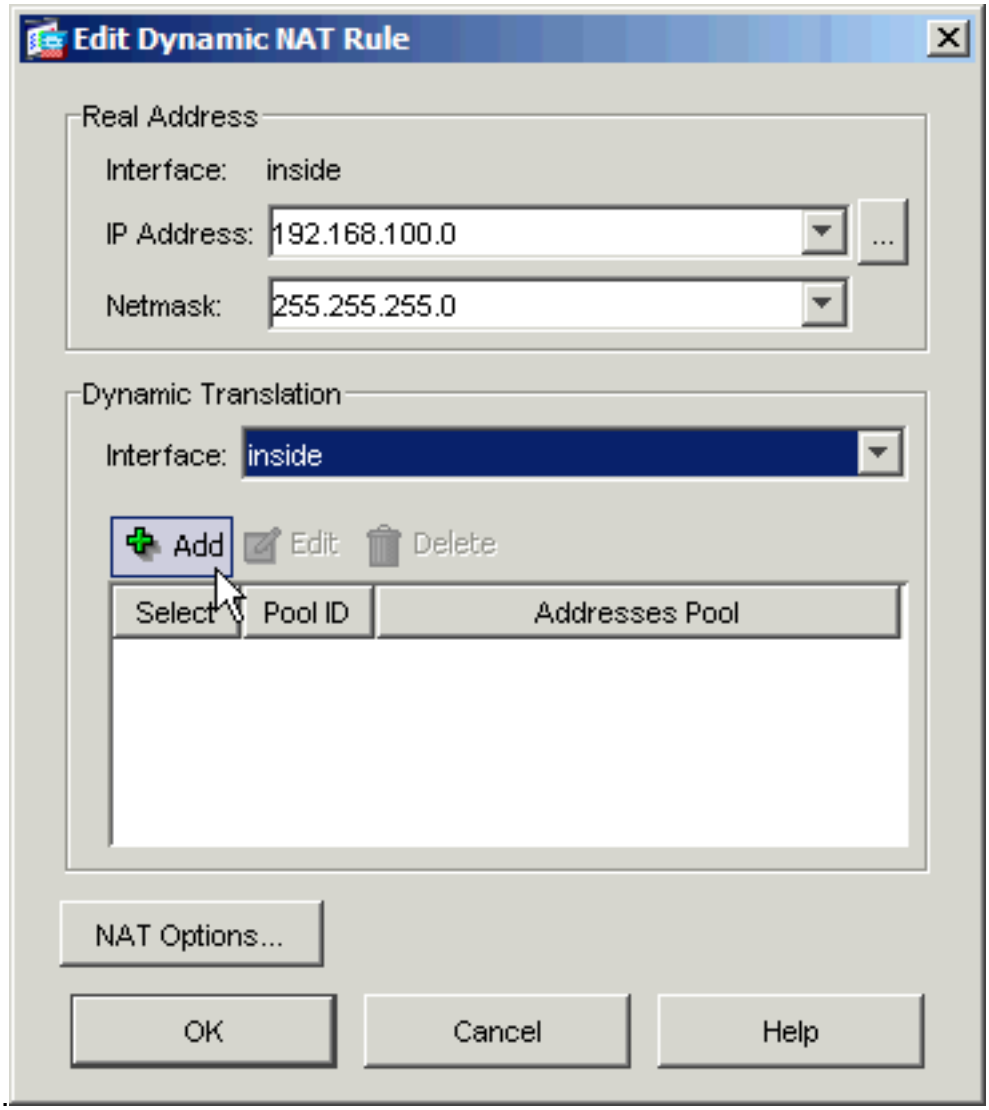


6. Fare clic su **OK** per uscire dalla finestra Aggiungi regola NAT statica.
7. Scegliete la traslazione dinamica PAT esistente e fate clic su **Modifica (Edit)**.

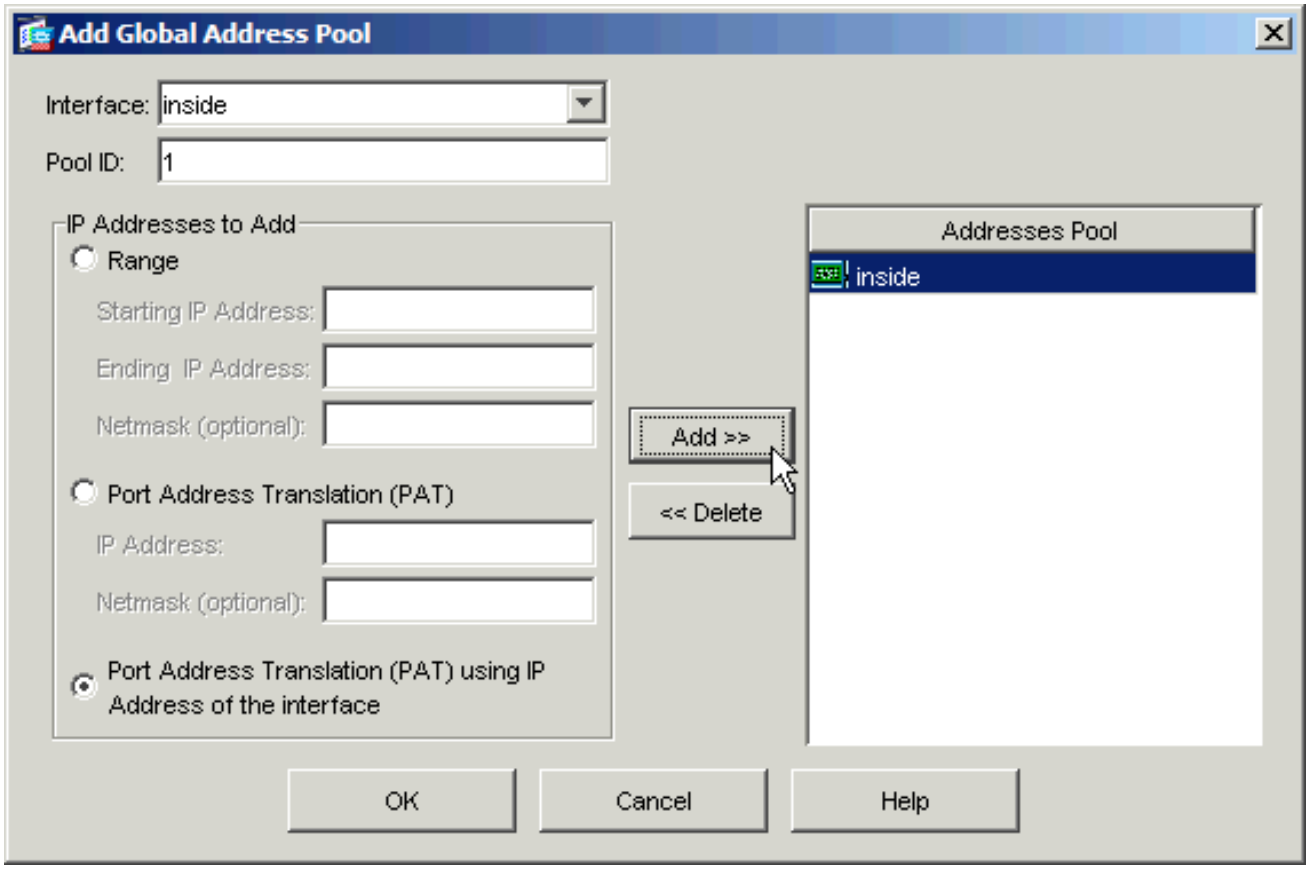


8. Selezionare **Inside** dal menu a discesa Interface (Interfaccia).





9. Fare clic su **Add**.
10. Scegliere il pulsante di opzione **PAT (Port Address Translation) utilizzando l'indirizzo IP dell'interfaccia**. Fare clic su **Add**.



11. Fare clic su **OK** per uscire dalla finestra Aggiungi pool di indirizzi globale. Fare clic su **OK** per uscire dalla finestra Modifica regola NAT dinamica. Fare clic su **Applica** per inviare la configurazione all'appliance di sicurezza.

Di seguito è riportata la sequenza di eventi che si verificano quando viene configurato il hairpinning. Si supponga che il client abbia già interrogato il server DNS e ricevuto una risposta di **172.20.1.10** per l'indirizzo del server WWW:

1. Il client tenta di contattare il server WWW all'indirizzo 172.20.1.10.
   ```
   %ASA-7-609001: Built local-host inside:192.168.100.2
   ```
2. L'appliance di sicurezza riconosce la richiesta e il server WWW è in corrispondenza di 192.168.100.10.
   ```
   %ASA-7-609001: Built local-host inside:192.168.100.10
   ```
3. L'appliance di sicurezza crea una traduzione dinamica PAT per il client. L'origine del traffico client è ora l'interfaccia interna dell'appliance di sicurezza: 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. L'appliance di sicurezza crea una connessione TCP tra il client e il server WWW tramite se stessa. Prendere nota degli indirizzi mappati di ciascun host tra parentesi.
   ```
   %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. Il comando **show xlate** sull'appliance di sicurezza verifica che il traffico del client passi attraverso l'appliance di sicurezza.
   ```
   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. Il comando **show conn** sull'appliance di sicurezza verifica che la connessione tra l'appliance di sicurezza e il server WWW sia stata stabilita correttamente per conto del client. Prendere nota dell'indirizzo reale del client tra parentesi.

```
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
```

Configurazione finale con hairpinning e NAT statico

Questa è la configurazione finale dell'ASA che usa il hairpinning e il protocollo NAT statico per raggiungere un effetto di dottorato DNS con due interfacce NAT.

Configurazione finale di 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
```

Nota: fare riferimento a questo video, Hair-pinning on Cisco ASA (solo utenti registrati) , per ulteriori informazioni su diversi scenari in cui potrebbe essere utilizzato lo hair-pinning.

Configura ispezione DNS

Per abilitare l'ispezione DNS (se è stata precedentemente disabilitata), eseguire la procedura seguente. Nell'esempio, l'ispezione DNS viene aggiunta al criterio di ispezione globale predefinito, che viene applicato globalmente da un comando **service-policy** come se l'ASA iniziasse con una configurazione predefinita. Per ulteriori informazioni sui criteri di servizio e sull'ispezione, fare riferimento a Utilizzo della struttura dei criteri modulari.

1. Creare una mappa dei criteri di ispezione per DNS.
   ```
   ciscoasa(config)#policy-map type inspect dns MY_DNS_INSPECT_MAP
   ```

2. In modalità di configurazione mappa dei criteri, accedere alla modalità di configurazione dei parametri per specificare i parametri per il motore di ispezione.
   ```
   ciscoasa(config-pmap)#parameters
   ```

3. In modalità di configurazione dei parametri della mappa dei criteri, specificare che la

lunghezza massima dei messaggi DNS sia 512.

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

4. Uscire dalla modalità di configurazione dei parametri della mappa dei criteri e dalla modalità di configurazione della mappa dei criteri.

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

5. Confermare che la mappa dei criteri di ispezione è stata creata come desiderato.

```
ciscoasa(config)#show run policy-map type inspect dns
!
policy-map type inspect dns MY_DNS_INSPECT_MAP
 parameters
  message-length maximum 512
!
```

6. Immettere la modalità di configurazione della mappa dei criteri per **global_policy**.

```
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#
```

7. In modalità di configurazione mappa dei criteri, specificate la mappa di classe predefinita del layer 3/4, **inspection_default**.

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

8. In modalità di configurazione delle classi con mapping dei criteri, specificare che il DNS deve essere ispezionato utilizzando il mapping dei criteri di ispezione creato nei passaggi da 1 a 3.

```
ciscoasa(config-pmap-c)#inspect dns MY_DNS_INSPECT_MAP
```

9. Uscire dalla modalità di configurazione della classe mappa dei criteri e dalla modalità di configurazione della mappa dei criteri.

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

10. Verificare che la mappa dei criteri **global_policy** sia configurata nel modo desiderato.

```
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. Verificare che global_policy sia applicato globalmente da un criterio-servizio.

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

Configurazione Split-DNS

Per immettere un elenco di domini da risolvere tramite il tunnel suddiviso, usare il comando **split-dns** in modalità di configurazione criteri di gruppo. Per eliminare un elenco, usare la forma *no* di questo comando.

Se non sono presenti elenchi di domini di tunneling divisi, gli utenti ereditano quelli esistenti nei Criteri di gruppo predefiniti. Usare il comando **split-dns none** per impedire che gli elenchi di domini con tunneling suddiviso vengano ereditati.

Utilizzare uno spazio singolo per separare ogni voce nell'elenco dei domini. Il numero di voci non è limitato, ma l'intera stringa non può superare i 255 caratteri. È possibile utilizzare solo caratteri alfanumerici, trattini (-) e punti (.). Se utilizzato senza argomenti, il comando **no split-dns** elimina tutti i valori correnti, incluso un valore null creato quando si esegue il comando **split-dns none**.

In questo esempio viene illustrato come configurare i domini Domain1, Domain2, Domain3 e Domain4 in modo che vengano risolti tramite il tunneling ripartito per i criteri di gruppo denominati FirstGroup:

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

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Acquisisci traffico DNS

Un metodo per verificare che l'accessorio di protezione riscriva correttamente i record DNS consiste nell'acquisire i pacchetti in questione, come illustrato nell'esempio precedente. Per acquisire il traffico sull'appliance ASA, completare i seguenti passaggi:

1. Creare un elenco degli accessi per ogni istanza di acquisizione che si desidera creare.L'ACL deve specificare il traffico che si desidera acquisire. Nell'esempio, sono stati creati due ACL.ACL per il traffico sull'interfaccia esterna:
   ```
   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.
   ```
   ACL per il traffico sull'interfaccia interna:
   ```
   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. Creare le istanze di acquisizione:
   ```
   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. Visualizzare le acquisizioni.Di seguito viene riportato l'aspetto dell'esempio catturato dopo il passaggio di traffico DNS:
   ```
   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. (Facoltativo) Copiare le acquisizioni su un server TFTP in formato pcap per analizzarle in un'altra applicazione.Le applicazioni in grado di analizzare il formato pcap possono visualizzare ulteriori dettagli, ad esempio il nome e l'indirizzo IP nei record A DNS.

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

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Riscrittura DNS non eseguita

Verificare che l'ispezione DNS sia configurata sull'appliance di sicurezza. Vedere la sezione Configurazione ispezione DNS.

Creazione della traduzione non riuscita

Se non è possibile creare una connessione tra il client e il server WWW, è possibile che la causa sia una configurazione errata di NAT. Controllare nei registri dell'accessorio di protezione se sono presenti messaggi che indicano che un protocollo non è riuscito a creare una traduzione tramite l'accessorio di protezione. Se vengono visualizzati messaggi di questo tipo, verificare che NAT sia stato configurato per il traffico desiderato e che nessun indirizzo sia errato.

```
%ASA-3-305006: portmap translation creation failed for tcp src
inside:192.168.100.2/11000 dst dmz:10.10.10.10/23
```

Cancellare le voci xlate, quindi rimuovere e riapplicare le istruzioni NAT per risolvere l'errore.

Elimina risposta DNS UDP

Èpossibile che venga visualizzato questo messaggio di errore a causa della perdita di pacchetti DNS:

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

Per risolvere il problema, aumentare la lunghezza del pacchetto DNS da 512 a 65535.

Esempio:

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

Informazioni correlate

- Software Cisco PIX Firewall
- Riferimenti per i comandi di Cisco Secure PIX Firewall
- Avvisi sui prodotti per la sicurezza
- RFC (Request for Comments)
- Accoppiamento capelli su Cisco ASA
- Cisco ASA serie 5500 Adaptive Security Appliance