

Configurazione della documentazione DNS per tre interfacce NAT su ASA release 9.x

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Prodotti correlati](#)

[Premesse](#)

[Scenario: Tre interfacce NAT - Interna, Esterna, DMZ](#)

[Topologia](#)

[Problema: Il client non può accedere al server WWW](#)

[Soluzione: Parola chiave "dns"](#)

[Documentazione DNS con la parola chiave "dns"](#)

[Versione 8.2 e precedente](#)

[Versione 8.3 e successive](#)

[Verifica](#)

[Configurazione finale con la parola chiave "dns"](#)

[Soluzione alternativa: NAT destinazione](#)

[Configurazione finale con NAT di destinazione](#)

[Configurazione](#)

[Verifica](#)

[Acquisisci traffico DNS](#)

[Risoluzione dei problemi](#)

[Riscrittura DNS non eseguita](#)

[Creazione della traduzione non riuscita](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene fornita una configurazione di esempio per eseguire la documentazione del DNS (Domain Name System) sull'appliance ASA 5500-X Adaptive Security (ASA) che utilizza istruzioni Object/Auto Network Address Translation (NAT). 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.

Prerequisiti

Requisiti

Cisco afferma che l'ispezione DNS deve essere abilitata per eseguire la documentazione DNS sull'appliance di sicurezza. L'ispezione DNS è attiva per impostazione predefinita.

Quando il controllo DNS è attivato, l'accessorio di protezione esegue le seguenti attività:

- Traduce il record DNS in base alla configurazione completata con l'utilizzo dei comandi NAT object/auto (riscrittura DNS). La conversione si applica solo al record A nella risposta DNS. Le ricerche inverse, che richiedono il record Pointer (PTR), non sono pertanto interessate dalla riscrittura del DNS. Nella versione ASA 9.0(1) e successive, conversione del record PTR DNS per ricerche DNS inverse quando si utilizza IPv4 NAT, IPv6 NAT e NAT64 con ispezione DNS abilitata per la regola NAT.**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). Se necessario, il riassemblaggio viene eseguito 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 immette 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

Per la stesura del documento, è stata usata l'appliance ASA serie 5500-X Security, versione 9.x.

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 ASA serie 5500 Security Appliance, versione 8.4 o successive.

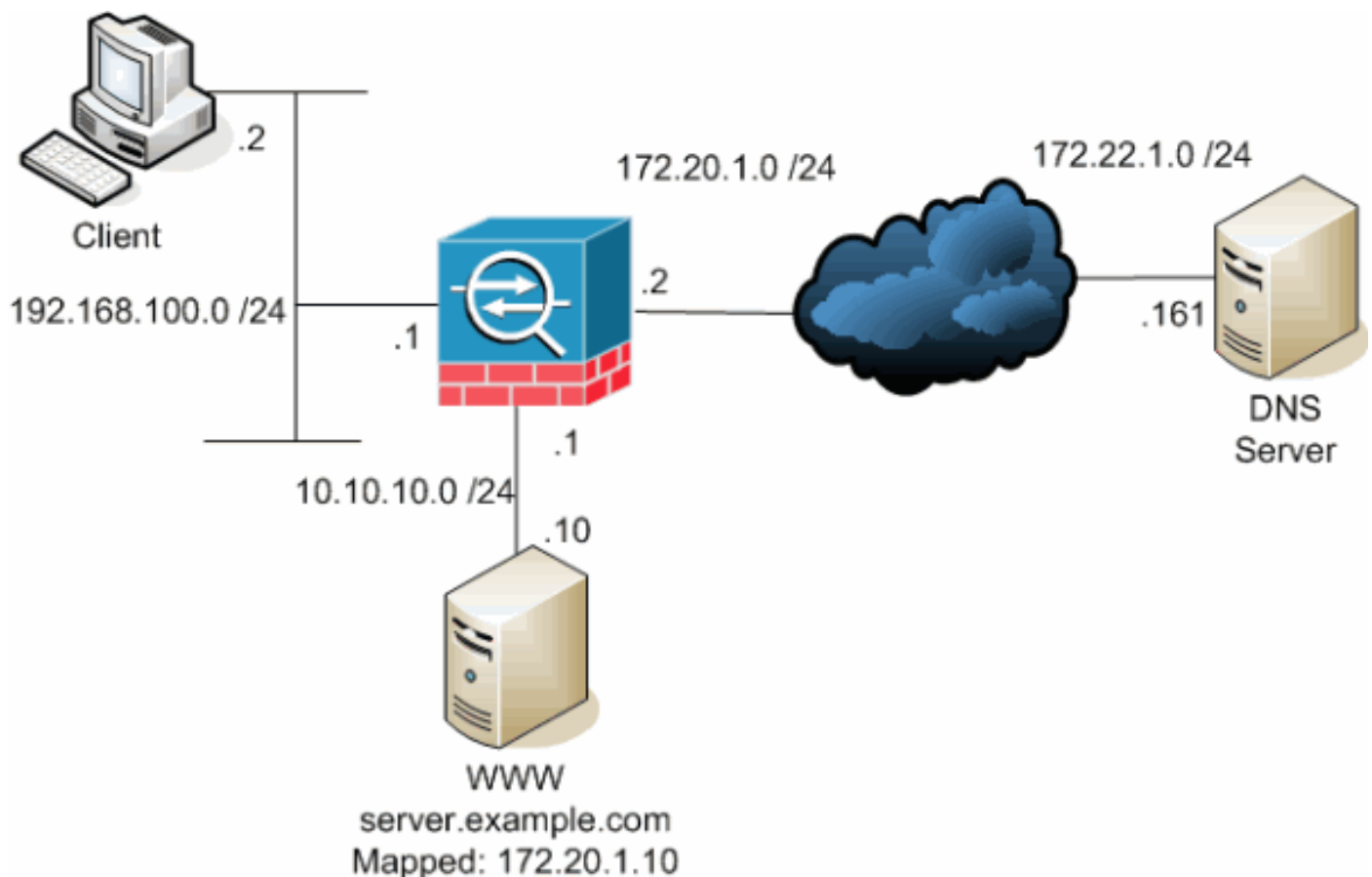
Nota: La configurazione ASDM è applicabile solo alla versione 7.x.

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: Tre interfacce NAT - Interna, Esterna, DMZ

Topologia



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 10.10.10.10. 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

Senza la funzionalità di doctoring DNS o un'altra soluzione abilitata in questa situazione, se il client invia una richiesta DNS per l'indirizzo IP di **server.example.com**, non è in grado di accedere al server WWW. Questo perché il client riceve un record A che contiene l'indirizzo pubblico mappato 172.20.1.10 per il 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:

```
ASA Version 9.x
!
hostname ciscoasa

!--- Output suppressed.

access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www
!--- Output suppressed.

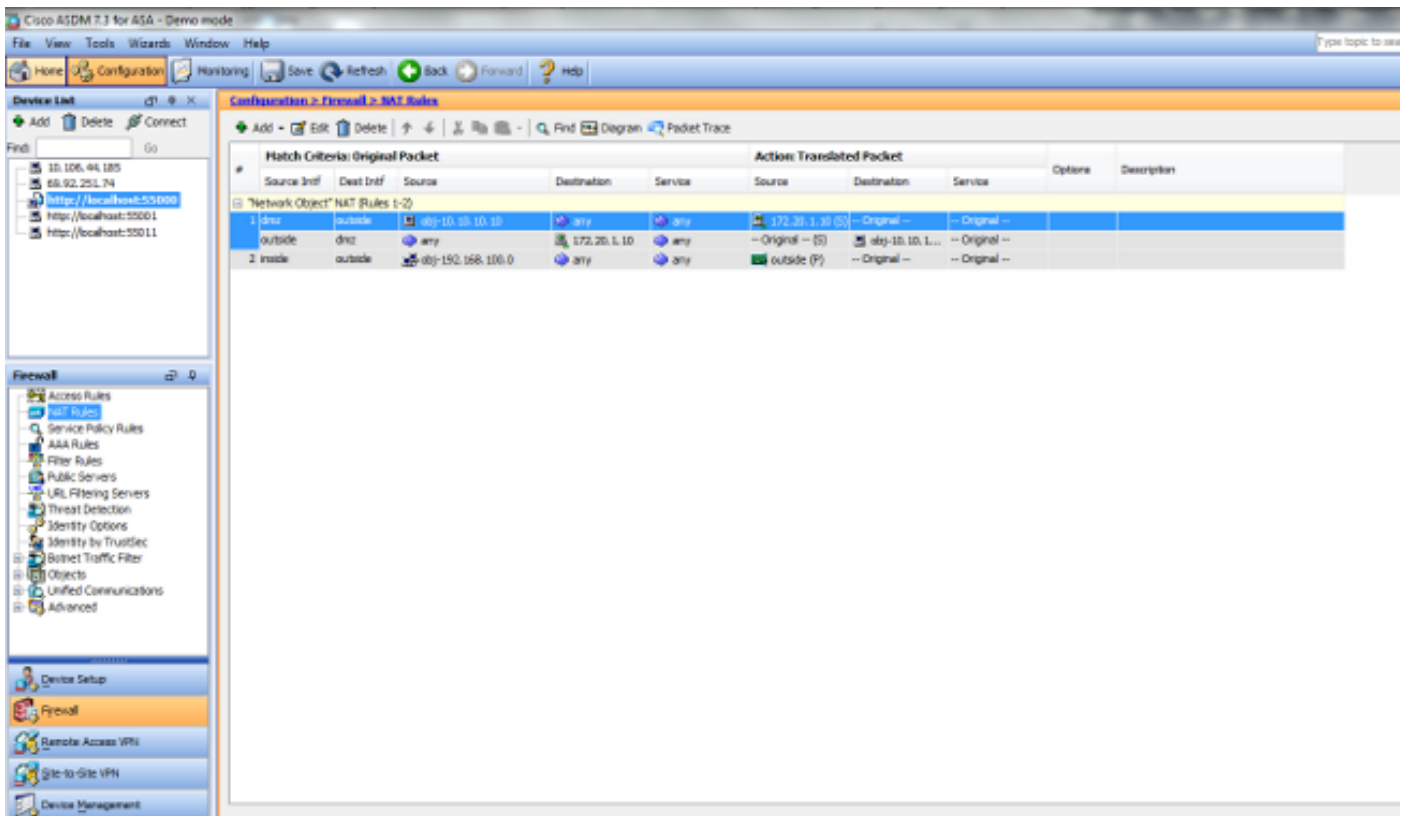
object network obj-192.168.100.0
network 192.168.100.0 255.255.255.0
nat (inside,outside) dynamic interface

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.
```

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 della DMZ, 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. Se configurato correttamente, l'appliance di sicurezza può modificare il record A per consentire al client di operare in uno scenario simile a quello descritto nella sezione "Problema: Il client non può accedere alla sezione "Server WWW" per connettersi. In questo caso, quando la funzionalità di protezione DNS è abilitata, l'appliance di sicurezza riscrive il record A per indirizzare il client alla versione 10.10.10.10 anziché alla versione 172.20.1.10. La funzionalità di protezione DNS è abilitata quando si aggiunge la parola chiave **dns** a un'istruzione NAT statica (versione 8.2 e precedenti) o a un'istruzione NAT object/auto (versione 8.3 e successive).

Versione 8.2 e precedente

Questa è la configurazione finale dell'ASA per eseguire il dottorato DNS con la parola chiave **dns** e tre interfacce NAT per le versioni 8.2 e precedenti.

```
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
```

Versione 8.3 e successive

```
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.

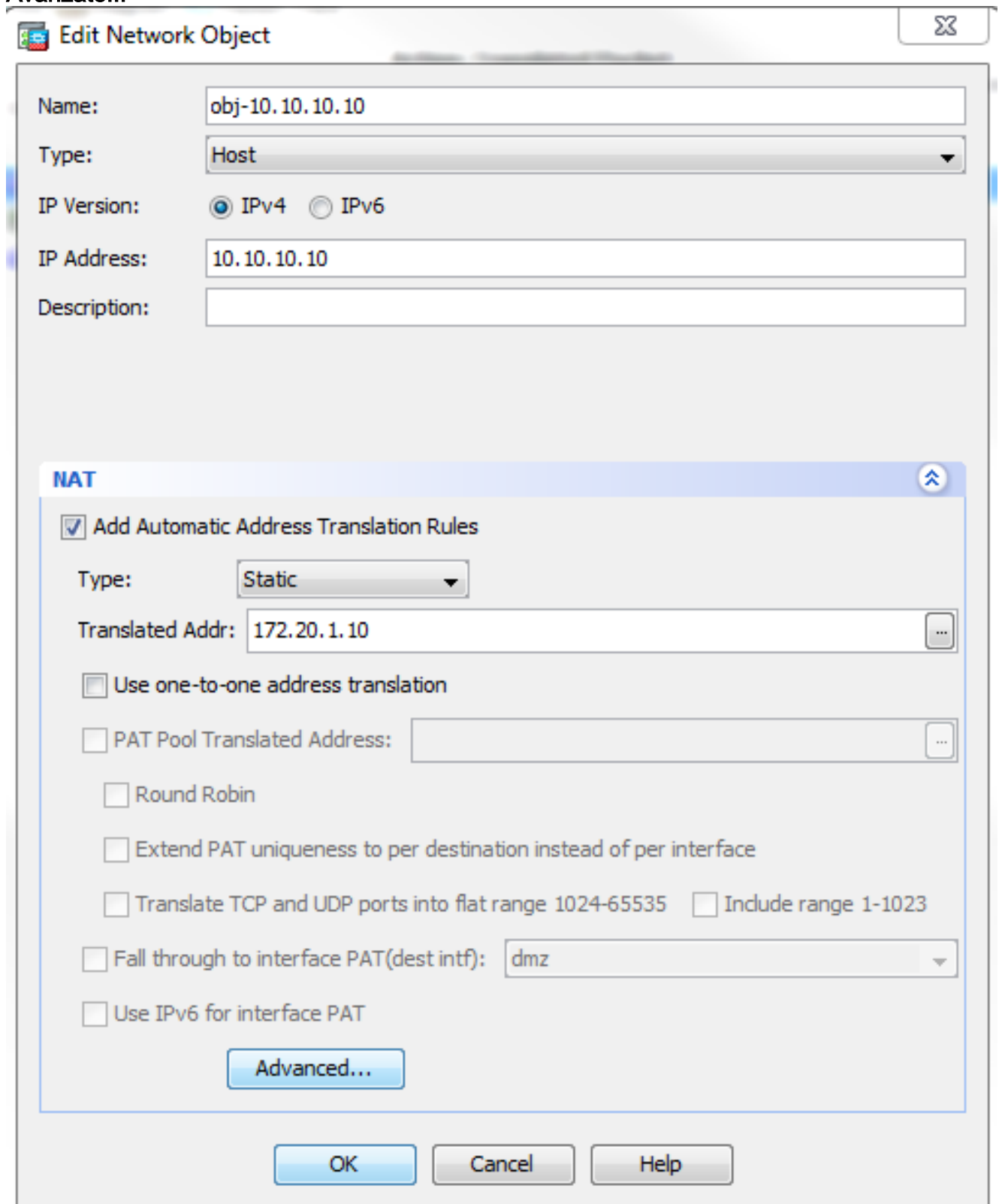
access-group OUTSIDE in interface outside

!--- Output suppressed.
```

Configurazione ASDM

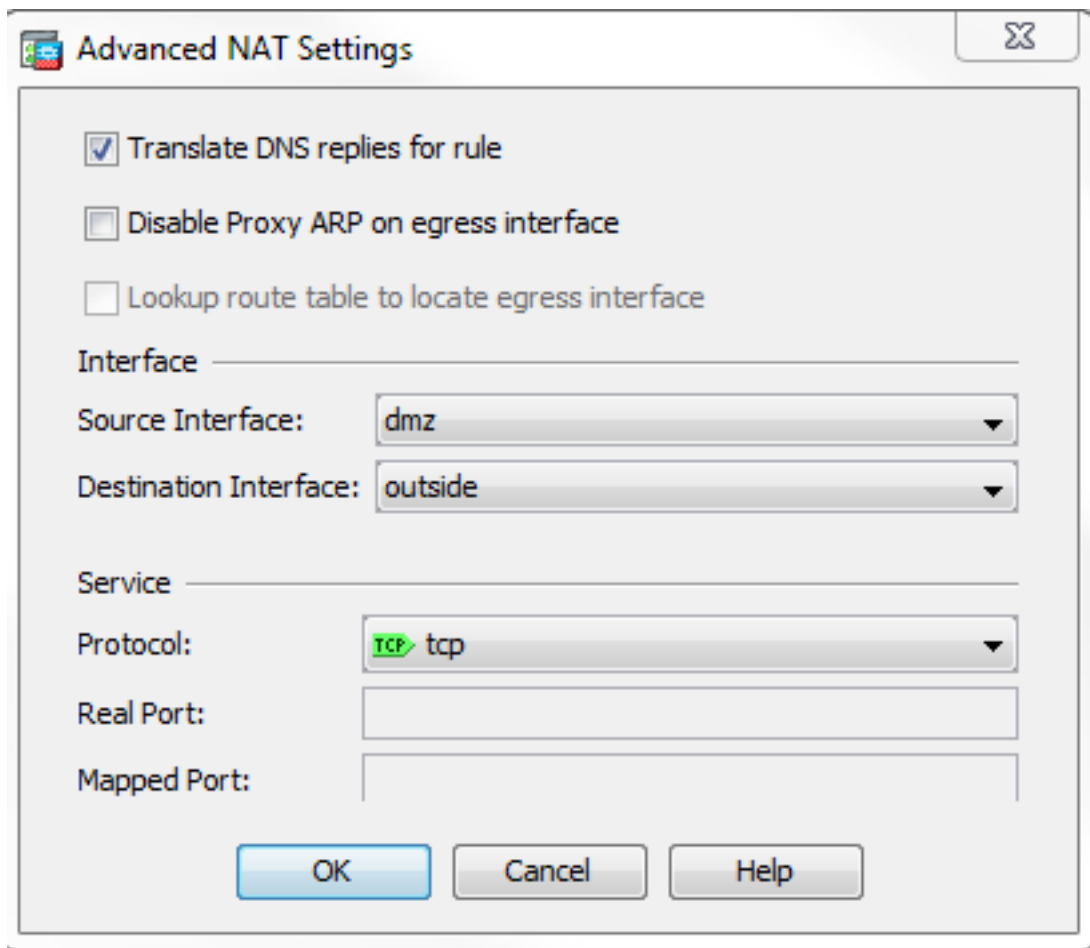
Completare questa procedura per configurare la gestione del DNS in ASDM:

1. Scegliere **Configurazione > Regole NAT** e scegliere la regola oggetto/automatico da modificare. Fare clic su **Modifica**.
2. Fare clic su **Avanzate...**



The screenshot shows the 'Edit Network Object' dialog box in ASDM. The 'Name' field is 'obj-10.10.10.10', 'Type' is 'Host', 'IP Version' is 'IPv4', and 'IP Address' is '10.10.10.10'. The 'Description' field is empty. The 'NAT' section is expanded, showing the 'Add Automatic Address Translation Rules' checkbox checked. The 'Type' is 'Static', and the 'Translated Addr' is '172.20.1.10'. Other options like 'Use one-to-one address translation', 'PAT Pool Translated Address', 'Round Robin', 'Extend PAT uniqueness to per destination instead of per interface', 'Translate TCP and UDP ports into flat range 1024-65535', 'Include range 1-1023', 'Fall through to interface PAT(dest intf): dmz', and 'Use IPv6 for interface PAT' are all unchecked. An 'Advanced...' button is visible at the bottom of the NAT section. At the bottom of the dialog are 'OK', 'Cancel', and 'Help' buttons.

3. Selezionare la casella di controllo **Traduci risposte DNS** per la



regola.

4. Per uscire dalla finestra Opzioni NAT, fare clic su **OK**.
5. Per uscire dalla finestra Modifica oggetto/Regola NAT automatica, fare clic su **OK**.
6. Per inviare la configurazione all'appliance di sicurezza, fare clic su **Apply** (Applica).

Verifica

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
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. A questo punto, il client tenta di accedere al server WWW all'indirizzo 10.10.10.10. La connessione ha esito positivo.

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 tre interfacce NAT.

```
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

```

Soluzione alternativa: NAT destinazione

Il protocollo NAT di destinazione può fornire un'alternativa alla gestione DNS. L'uso del NAT di destinazione in questa situazione richiede la creazione di una conversione NAT automatica/oggetto statico tra l'indirizzo pubblico del server WWW all'interno e l'indirizzo reale sulla DMZ. Il NAT di destinazione non modifica il contenuto del record A DNS restituito dal server DNS al client. Quando si utilizza invece il NAT di destinazione in uno scenario come quello illustrato in questo documento, il client può utilizzare l'indirizzo IP pubblico **172.20.1.10** restituito

dal server DNS per connettersi al server WWW. La conversione automatica o dell'oggetto statico consente all'appliance di sicurezza di convertire l'indirizzo di destinazione da **172.20.1.10** a **10.10.10.10**. Di seguito è riportata la parte rilevante della configurazione quando si utilizza il protocollo NAT di destinazione:

```
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
```

NAT di destinazione raggiunto con istruzione NAT manuale/doppia

```
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

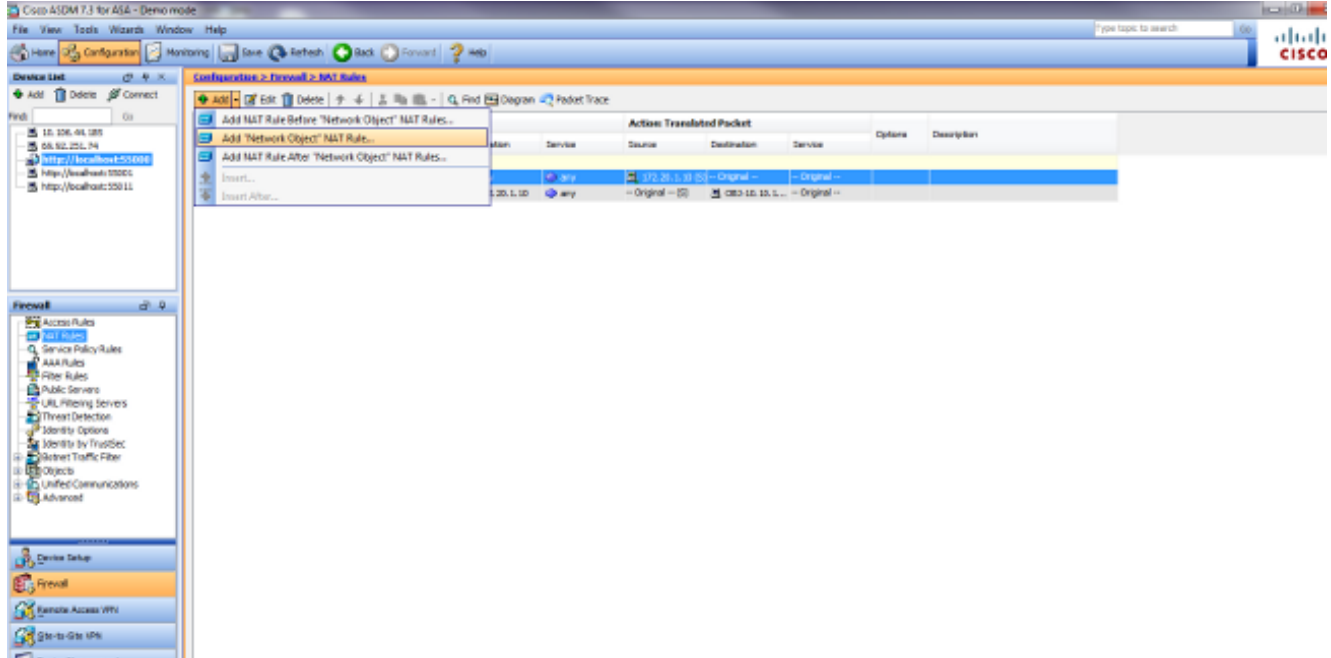
!--- Static translation to allow hosts on the inside access
!--- to the WWW server via its outside address.
```


access-group OUTSIDE in interface outside

!--- Output suppressed.

Completare questa procedura per configurare il NAT di destinazione nell'ASDM:

1. Scegliere **Configurazione > Regole NAT** e scegliere **Aggiungi > Aggiungi regola NAT "Oggetto di rete"...**



2. Completare la configurazione per la nuova traduzione statica. Nel campo Nome, immettere **obj-10.10.10.10**. Nel campo Indirizzo IP, immettere l'indirizzo IP del server WWW. Dall'elenco a discesa Tipo (Type), selezionate **Statico (Static)**. Nel campo Indirizzo tradotto immettere l'indirizzo e l'interfaccia a cui si desidera mappare il server WWW. Fare clic su **Avanzate**.

Add Network Object [X]

Name:

Type:

IP Version: IPv4 IPv6

IP Address:

Description:

NAT [^]

Add Automatic Address Translation Rules

Type:

Translated Addr:

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

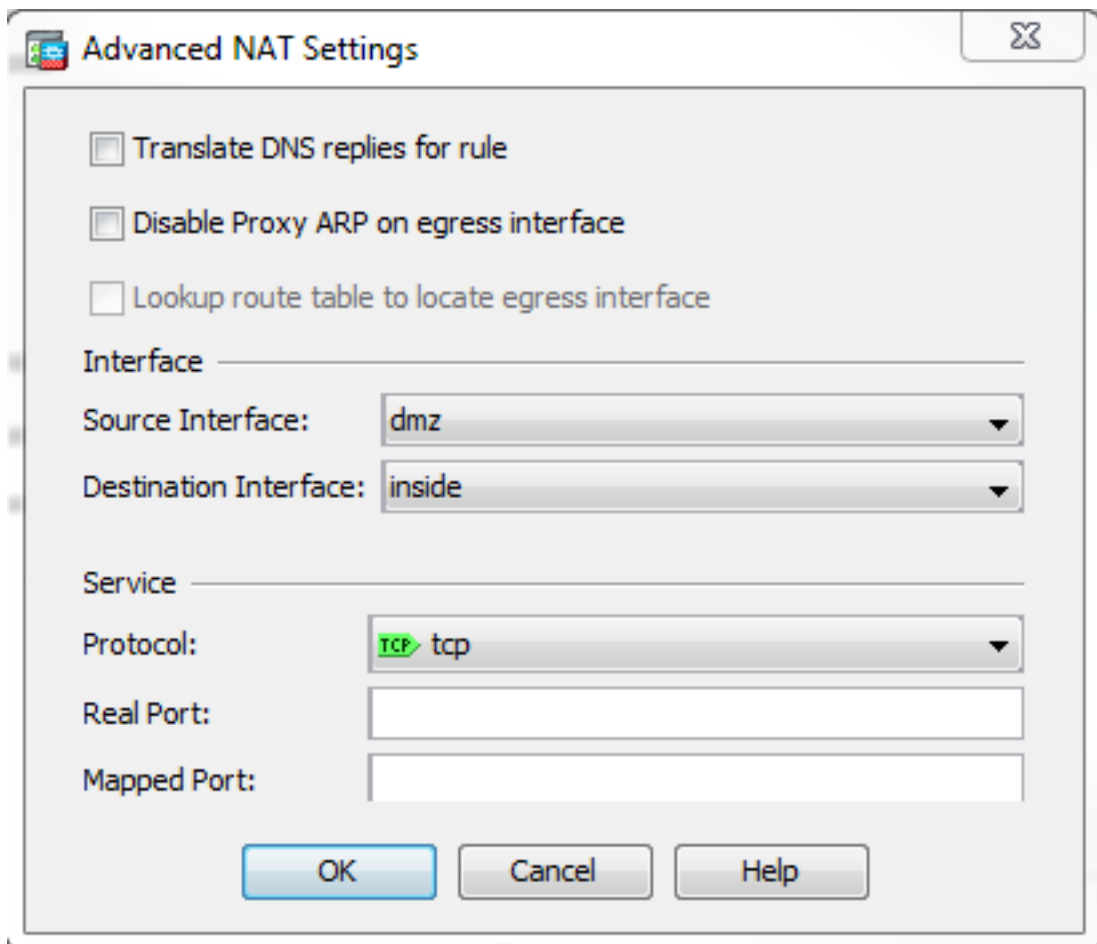
Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

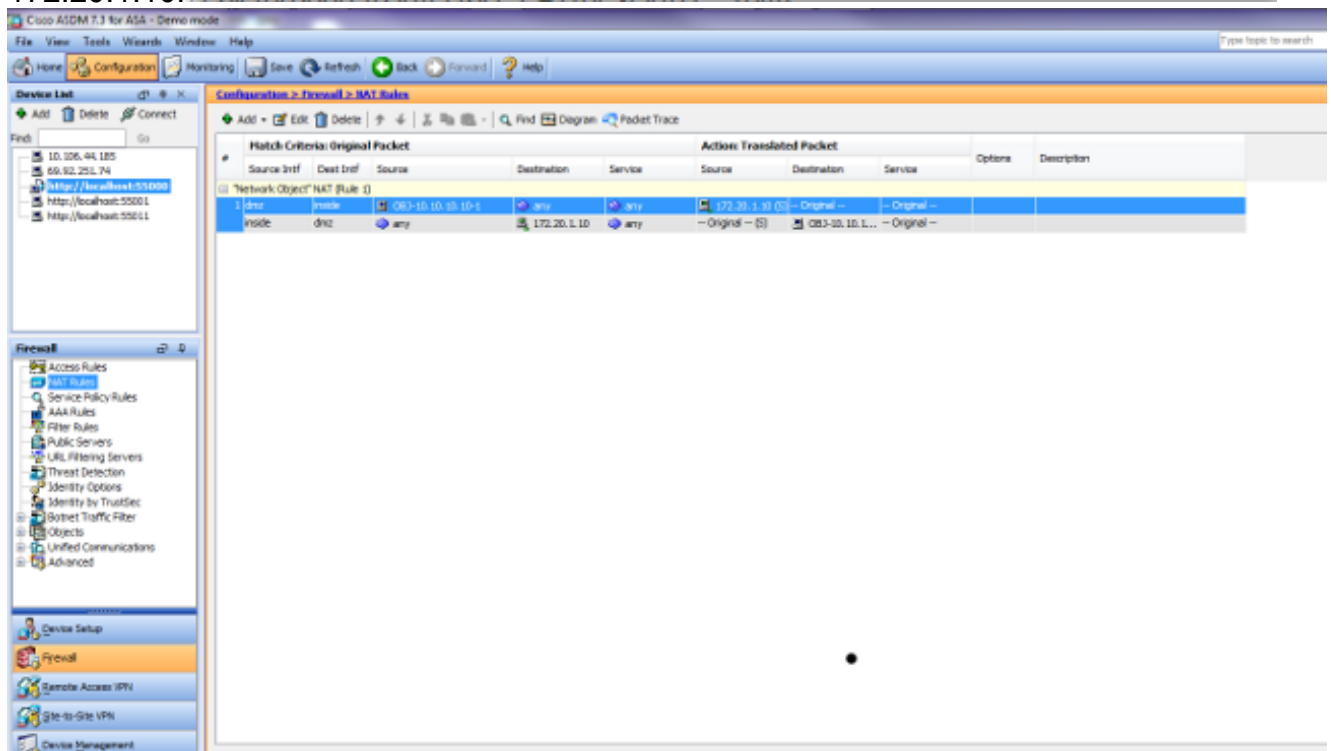
Fall through to interface PAT(dest intf):

Use IPv6 for interface PAT

Nell'elenco a discesa Source Interface (Interfaccia di origine), selezionare **dmz**. Nell'elenco a discesa Interfaccia di destinazione, scegliere **dall'interno**. In questo caso, l'interfaccia interna è scelta per consentire agli host sull'interfaccia interna di accedere al server WWW tramite l'indirizzo mappato



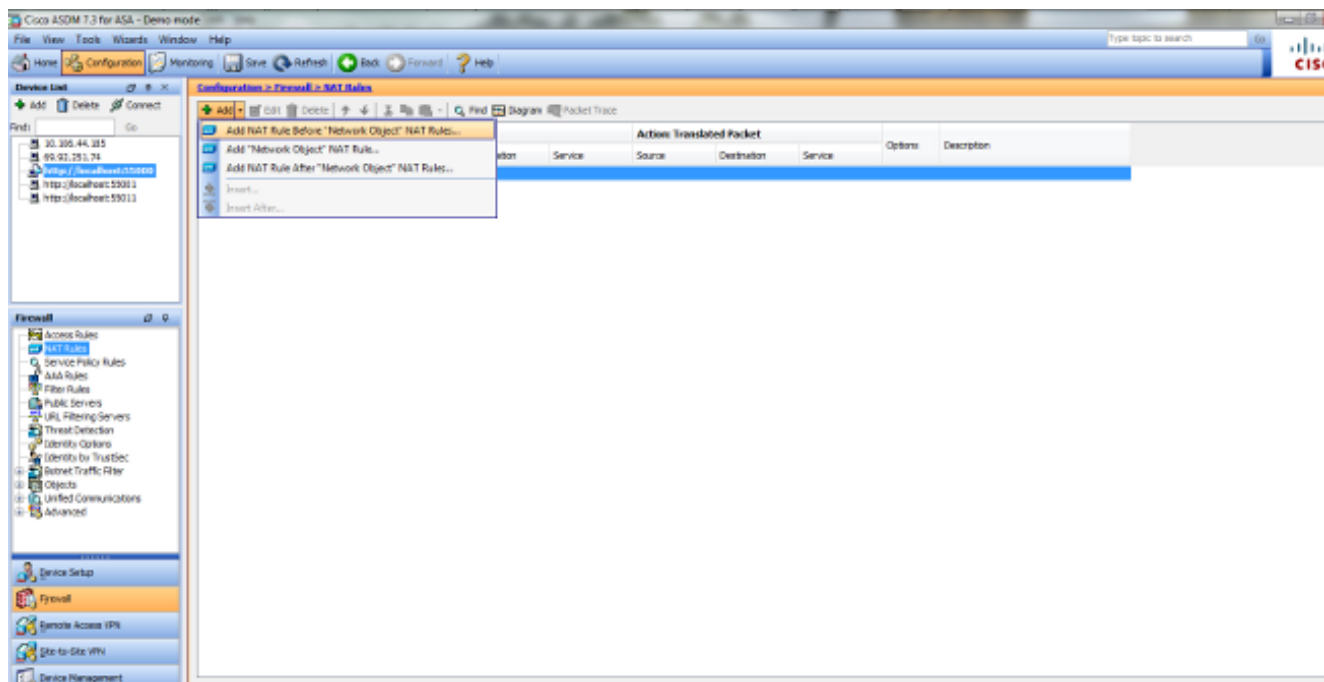
172.20.1.10.



Per uscire dalla finestra Aggiungi oggetto/regola NAT automatica, fare clic su **OK**. Per inviare la configurazione all'appliance di sicurezza, fare clic su **Apply** (Applica).

Metodo alternativo con NAT manuale/doppio e ASDM

1. Scegliere **Configurazione > Regole NAT e Aggiungi > Aggiungi regola NAT prima di Regola NAT "Oggetto di rete"....**



2. Completare la configurazione per la traduzione manuale/doppia Nat. Nell'elenco a discesa Source Interface (Interfaccia di origine), selezionare **inside** (Interno). Nell'elenco a discesa Interfaccia di destinazione, scegliere **dmz**. Nel campo Source Address (Indirizzo di origine), immettere l'oggetto di rete interno (obj-192.168.100.0). Nel campo Indirizzo di destinazione, immettere la tOggetto IP del server DMZ tradotto (172.20.1.10). Nell'elenco a discesa Source NAT Type (Tipo NAT di origine), selezionare **Dynamic PAT (Nascondi)**. Nel campo Source Address [Azione: Translated Packet section], immettere **dmz**. Nella destinazione Address [Azione: Translated Packet section] campo, immettere l'oggetto IP reale del server DMZ (obj-10.10.10.10).

Edit NAT Rule

Match Criteria: Original Packet

Source Interface: Destination Interface:

Source Address: Destination Address:

Service:

Action: Translated Packet

Source NAT Type:

Source Address: Destination Address:

Use one-to-one address translation

PAT Pool Translated Address:

Service:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

Fall through to interface PAT

Use IPv6 for source interface PAT Use IPv6 for destination interface PAT

Options

Enable rule

Translate DNS replies that match this rule

Disable Proxy ARP on egress interface

Lookup route table to locate egress interface

Direction:

Description:

3. Fare clic su **OK** per uscire dalla finestra Aggiungi regola NAT manuale/doppia.

4. Per inviare la configurazione all'appliance di sicurezza, fare clic su **Apply** (Applica).

Di seguito è riportata la sequenza di eventi che hanno luogo quando viene configurato il NAT di destinazione. 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 10.10.10.10.

```
%ASA-7-609001: Built local-host dmz:10.10.10.10
```

3. L'appliance di sicurezza crea una connessione TCP tra il client e il server WWW. Prendere nota degli indirizzi mappati di ciascun host tra parentesi.

```
%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. Il comando **show xlate** sull'appliance di sicurezza verifica che il traffico del client passi attraverso l'appliance di sicurezza. In questo caso, viene utilizzata la prima traslazione

statica.

```
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. Il comando **show conn** sull'appliance di sicurezza verifica che la connessione tra il client e il server WWW sia stata stabilita correttamente tramite l'appliance di sicurezza. Prendere nota dell'indirizzo reale del server WWW tra parentesi.

```
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
```

Configurazione finale con NAT di destinazione

Questa è la configurazione finale dell'ASA per eseguire il dottorato DNS con il NAT di destinazione e tre interfacce NAT.

```
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-shal
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

```

Configurazione

Completare questi passaggi per abilitare l'ispezione DNS (se è stata precedentemente disabilitata). 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.

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, utilizzare la mappa dei criteri di ispezione creata nei passaggi 1-3 per specificare che il DNS deve essere ispezionato.

```
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
```

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 da 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.

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 inside:192.168.100.10/80
```

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

Informazioni correlate

- [Guida alla configurazione di Cisco ASA 5500-x](#)
- [Riferimenti per i comandi di Cisco ASA serie 5500-x](#)
- [Avvisi sui prodotti per la sicurezza](#)
- [RFC \(Request for Comments\)](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)