Configurazione dell'ASA per le due reti interne

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Convenzioni](#)
[Premesse](#)
[Configurazione](#)
[Esempio di rete](#)
[Configurazione di ASA 9.x](#)
[Consenti agli host interni l'accesso alle reti esterne con PAT](#)
[Configurazione router B](#)
[Verifica](#)
[Connessione](#)
[Risoluzione dei problemi](#)
[Syslog](#)
[Packet Tracer](#)
[Acquisisci](#)
[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare una Cisco Adaptive Security Appliance (ASA) con software versione 9.x per l'utilizzo di due reti interne.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni di questo documento si basano sull'appliance Cisco ASA con software 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.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Premesse

Quando si aggiunge una seconda rete interna dietro un firewall ASA, tenere presenti le seguenti informazioni importanti:

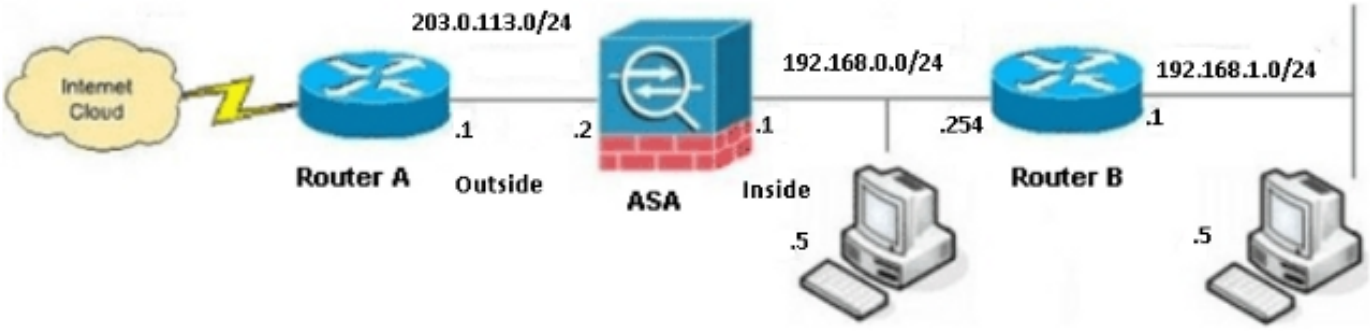
- L'ASA non supporta l'indirizzamento secondario.
- Ènecessario usare un router dietro l'ASA per ottenere il routing tra la rete corrente e la rete appena aggiunta.
- Il gateway predefinito per tutti gli host deve puntare al router interno.
- Ènecessario aggiungere un percorso predefinito sul router interno che punti all'appliance ASA.
- Ènecessario cancellare la cache ARP (Address Resolution Protocol) sul router interno.

Configurazione

Per configurare l'ASA, usare le informazioni descritte in questa sezione.

Esempio di rete

Di seguito è riportata la topologia utilizzata per gli esempi in questo documento:



Nota: Gli schemi di indirizzamento IP utilizzati in questa configurazione non sono indirizzabili

legalmente su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

Configurazione di ASA 9.x

se il dispositivo Cisco restituisce i risultati del comando **write terminal**, è possibile usare lo strumento Output Interpreter (solo utenti registrati) per visualizzare i potenziali errori e correggerli.

Di seguito è riportata la configurazione dell'appliance ASA con software versione 9.x:

```
ASA Version 9.3(2)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!

!--- This is the configuration for the outside interface.

!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 203.0.113.2 255.255.255.0

!--- This is the configuration for the inside interface.

!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!

boot system disk0:/asa932-smp-k8.bin

!--- This creates an object called OBJ_GENERIC_ALL.
!--- Any host IP address that does not already match another configured
!--- object will get PAT to the outside interface IP address
!--- on the ASA (or 10.1.5.1), for Internet-bound traffic.


object network OBJ_GENERIC_ALL
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic interface
!
route inside 192.168.1.0 255.255.255.0 192.168.0.254 1
route outside 0.0.0.0 0.0.0.0 203.0.113.1
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 sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.0.0 255.255.254.0 inside
no snmp-server location
```

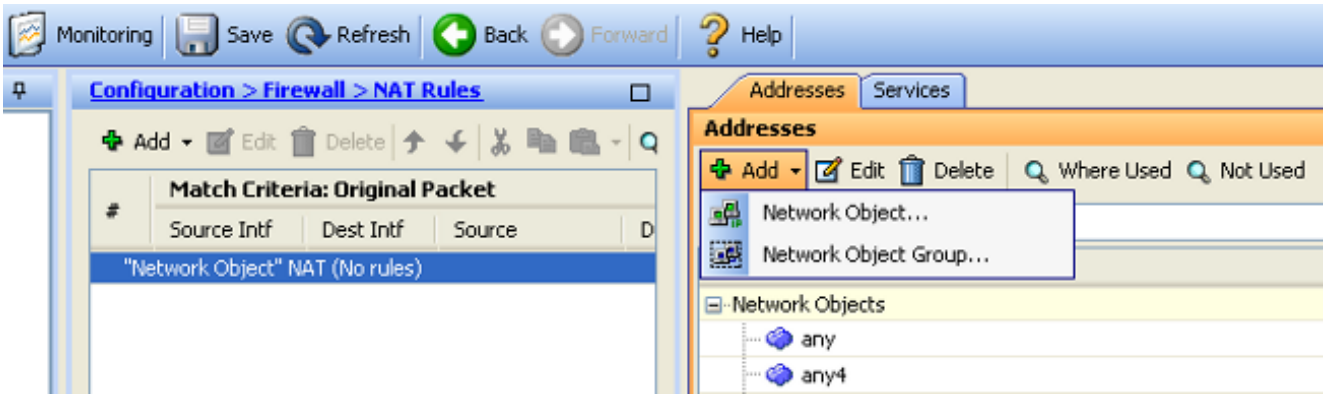
```
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
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
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:6fffbd3dc9cb863fd71c71244a0ecc5f
: end
```

Consenti agli host interni l'accesso alle reti esterne con PAT

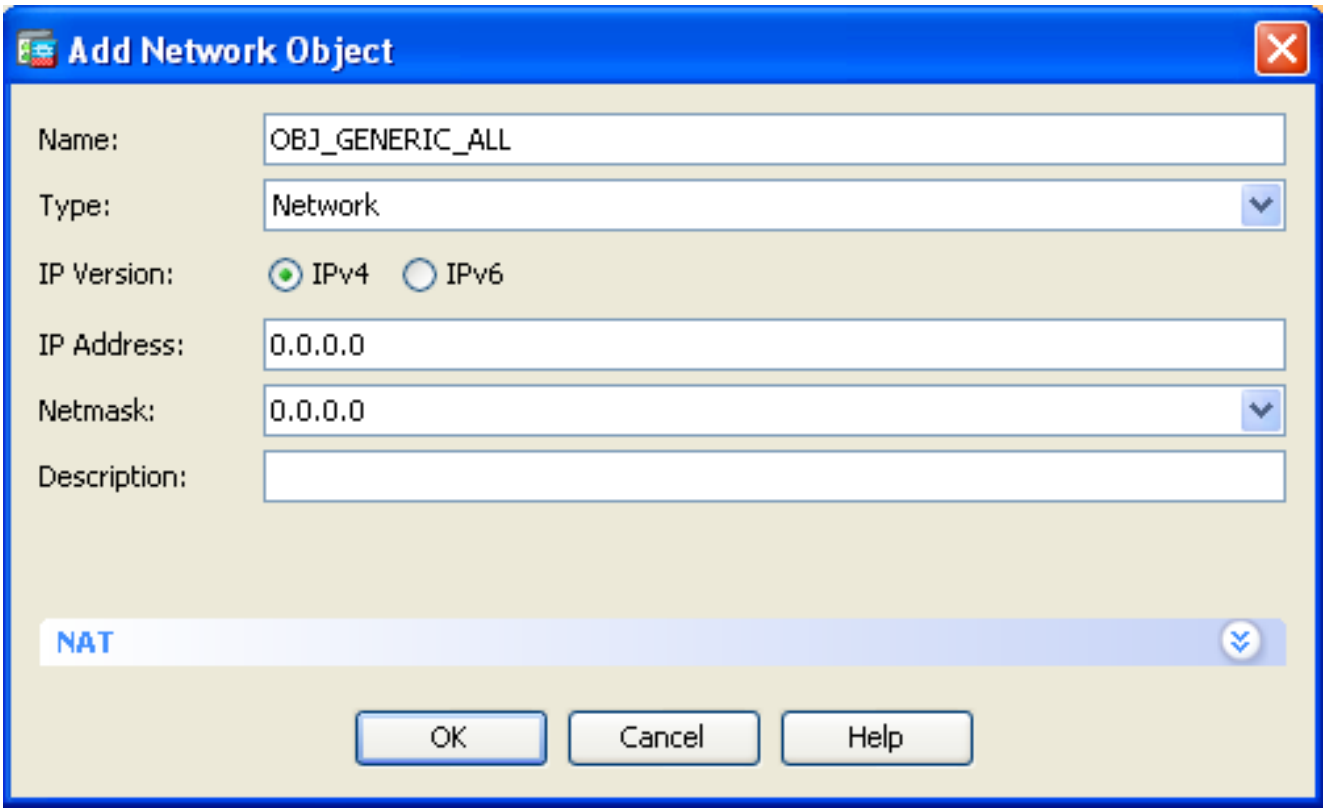
Se si desidera che gli host interni condividano un unico indirizzo pubblico per la traduzione, utilizzare Port Address Translation (PAT). Una delle configurazioni PAT più semplici prevede la conversione di tutti gli host interni in modo che sembrino essere l'IP dell'interfaccia esterna. Si tratta della configurazione tipica utilizzata quando il numero di indirizzi IP instradabili disponibili presso l'ISP è limitato a pochi o a uno solo.

Completare questi passaggi per consentire agli host interni di accedere alle reti esterne con PAT:

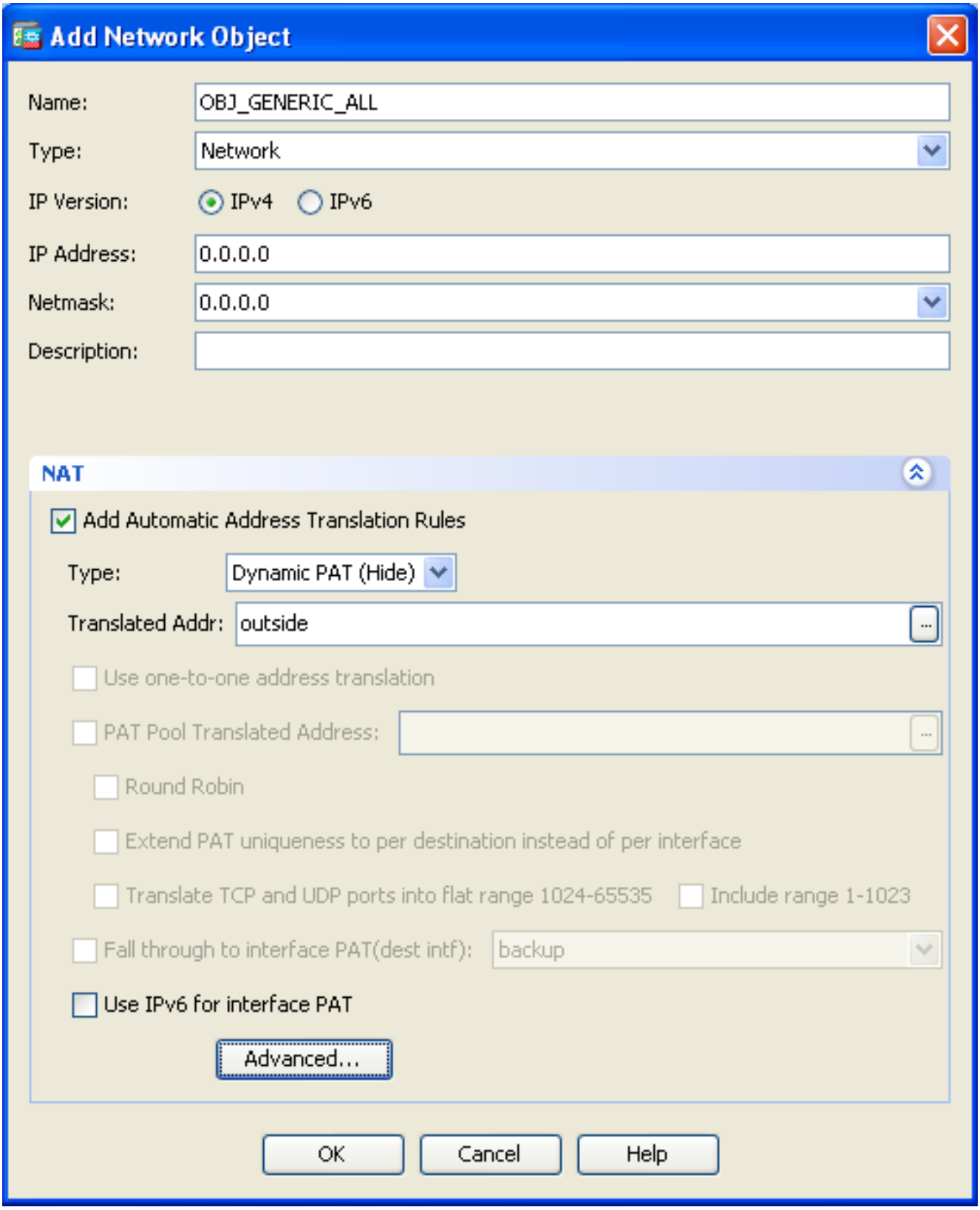
1. Passare a Configurazione **> Firewall > Regole NAT**, fare clic su **Aggiungi**, quindi scegliere **Oggetto di rete** per configurare una regola NAT dinamica:



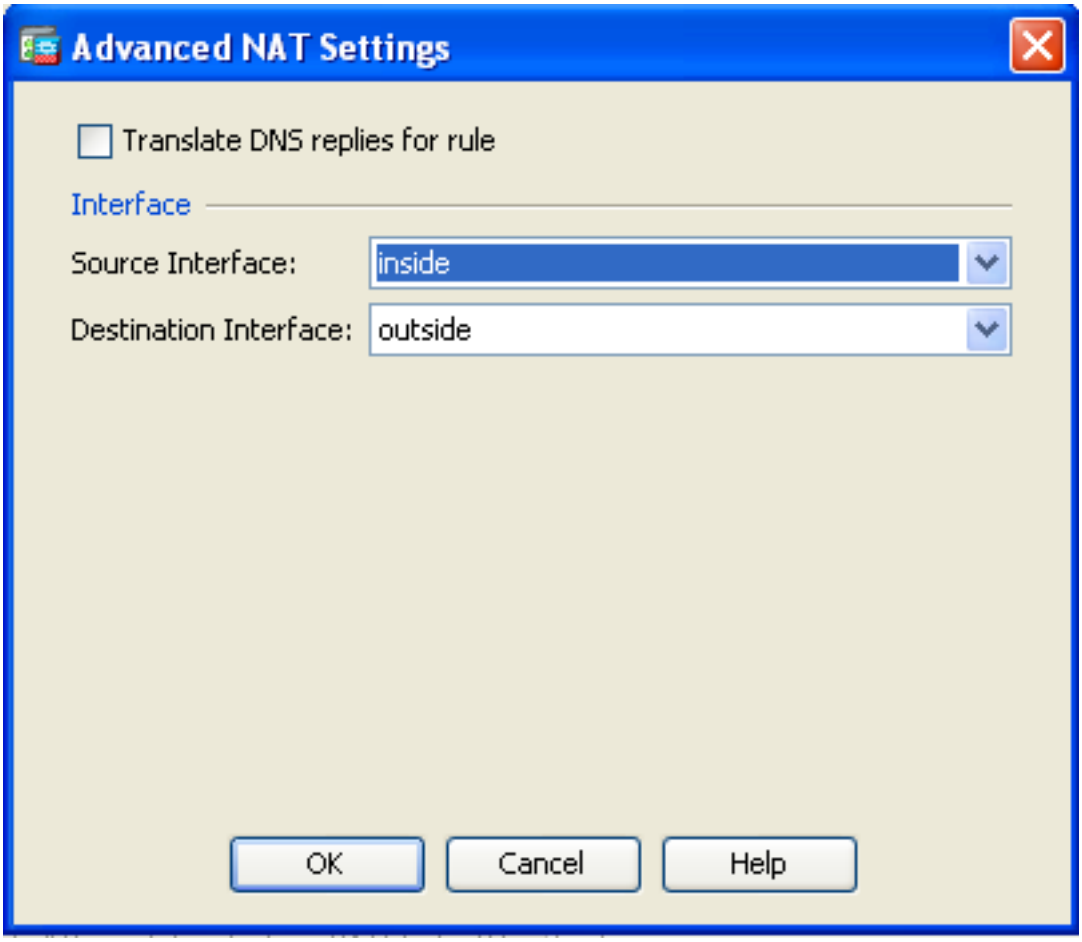
2. Configurare la rete/l'host/l'intervallo per cui è richiesta la parte dinamica. In questo esempio sono state selezionate tutte le subnet interne. Questo processo deve essere ripetuto per le subnet specifiche che si desidera tradurre nel modo seguente:



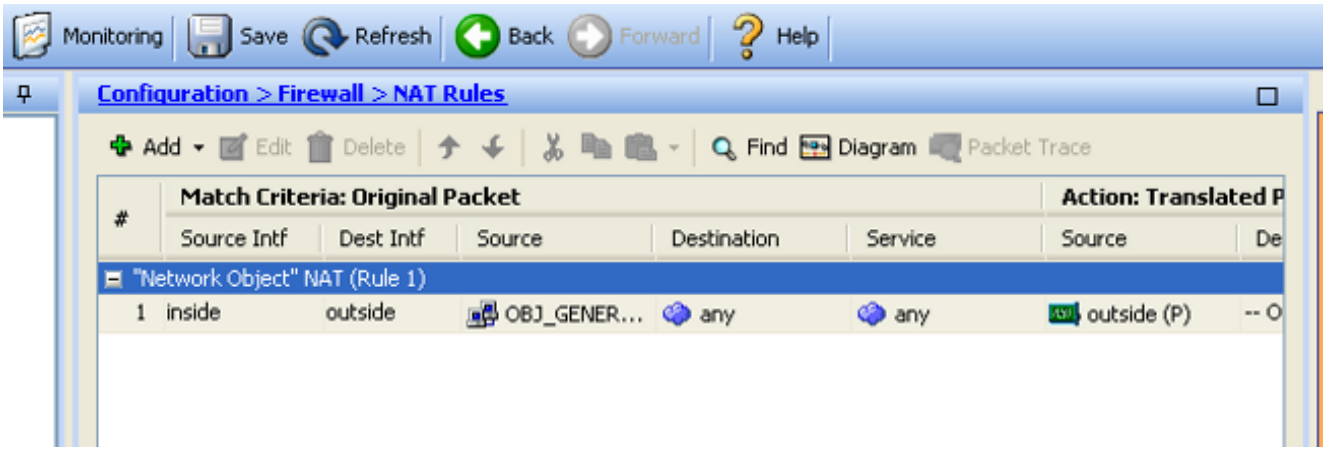
3. Fare clic su **NAT**, selezionare la casella di controllo **Aggiungi regola di conversione automatica degli indirizzi**, immettere **Dynamic** (Dinamico) e impostare l'**opzione Translated Addr** in modo che rifletta l'interfaccia esterna. Facendo clic sul pulsante con i puntini di sospensione, è possibile scegliere un oggetto preconfigurato, ad esempio l'interfaccia esterna:



4. Per selezionare un'interfaccia di origine e di destinazione, fare clic su **Advanced** (Avanzate):



5. Per applicare le modifiche, fare clic su **OK**, quindi su **Applica**. Al termine, Adaptive Security Device Manager (ASDM) visualizza la regola NAT:



Configurazione router B

Di seguito è riportata la configurazione del router B:

```
Building configuration...

Current configuration:
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
```

```
!
hostname Router B
!
!
username cisco password 0 cisco
!
!
!
!
ip subnet-zero
ip domain-name cisco.com
!
isdn voice-call-failure 0
!

!
interface Ethernet0/0
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast
!
interface Ethernet0/1

!--- This assigns an IP address to the ASA-facing Ethernet interface.

ip address 192.168.0.254 255.255.255.0
no ip directed-broadcast

ip classless

!--- This route instructs the inside router to forward all of the
!--- non-local packets to the ASA.

ip route 0.0.0.0 0.0.0.0 192.168.0.1
no ip http server
!
!
line con 0
exec-timeout 0 0
length 0
transport input none
line aux 0
line vty 0 4
password ww
login
!
end
```

Verifica

Per verificare il corretto funzionamento della configurazione, accedere a un sito Web tramite HTTP tramite un browser Web.

Questo esempio utilizza un sito ospitato all'indirizzo IP *198.51.100.100*. Se la connessione ha esito positivo, gli output forniti nelle sezioni seguenti possono essere visualizzati sulla CLI dell'ASA.

Connessione

Immettere il comando **show connection address** per verificare la connessione:

```
ASA(config)# show connection address 172.16.11.5
6 in use, 98 most used
TCP outside 198.51.100.100:80 inside 192.168.1.5:58799, idle 0:00:06, bytes 937,
flags UIO
```

L'ASA è un firewall con stato e il traffico di ritorno dal server Web può attraversare nuovamente il firewall perché corrisponde a una ***connessione*** nella tabella delle connessioni del firewall. Il traffico che corrisponde a una connessione preesistente può passare attraverso il firewall senza essere bloccato da un Access Control List (ACL) di interfaccia.

Nell'output precedente, il client sull'interfaccia interna ha stabilito una connessione con l'host 198.51.100.100 dall'interfaccia esterna. Questa connessione viene effettuata con il protocollo TCP ed è rimasta inattiva per sei secondi. I flag di connessione indicano lo stato corrente della connessione.

> **Nota:** Per ulteriori informazioni sui flag di connessione, consultare il documento Cisco ASA TCP Connection Flags (Connection build-up and teardown).

Risoluzione dei problemi

Utilizzare le informazioni descritte in questa sezione per risolvere i problemi relativi alla configurazione.

Syslog

Immettere il comando **show log** per visualizzare i syslog:

```
ASA(config)# show log | in 192.168.1.5

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
192.168.1.5/58799 to outside:203.0.113.2/58799

Apr 27 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside:
198.51.100.100/80 (198.51.100.100/80) to inside:192.168.1.5/58799 (203.0.113.2/58799)
```

Il firewall ASA genera syslog durante il normale funzionamento. L'intervallo dei syslog è espresso in dettaglio in base alla configurazione di registrazione. L'output mostra due syslog visualizzati al livello sei o al livello *informativo*.

In questo esempio vengono generati due syslog. Il primo è un messaggio di registro che indica che il firewall ha creato una traduzione; in particolare, una conversione TCP dinamica (PAT). Indica l'indirizzo IP e la porta di origine, nonché l'indirizzo IP e la porta convertiti, quando il traffico attraversa le interfacce interna ed esterna.

Il secondo syslog indica che il firewall ha creato una connessione nella relativa tabella di connessione per il traffico specifico tra il client e il server. Se il firewall è stato configurato per bloccare questo tentativo di connessione o altri fattori hanno impedito la creazione della connessione (vincoli di risorse o una possibile configurazione errata), il firewall non genera un

registro per indicare che la connessione è stata creata. Registra invece un motivo per cui la connessione viene negata o un'indicazione relativa al fattore che ha impedito la creazione della connessione.

Packet Tracer

Immettere questo comando per abilitare la funzionalità di traccia dei pacchetti:

```
ASA(config)# packet-tracer input inside tcp 192.168.1.5 1234 198.51.100.100 80


--Omitted--

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

La funzionalità di tracciamento dei pacchetti sull'appliance ASA consente di specificare un pacchetto *simulato* e di visualizzare tutte le varie fasi, i controlli e le funzioni completati dal firewall quando elabora il traffico. Con questo strumento, è utile identificare un esempio del traffico che si ritiene *debba* essere autorizzato a passare attraverso il firewall e utilizzare quel 5-tuple per simulare il traffico. Nell'esempio precedente, il packet tracer viene usato per simulare un tentativo di connessione che soddisfa i seguenti criteri:

- Il pacchetto simulato arriva all'interfaccia interna.
- Il protocollo utilizzato è TCP.
- L'indirizzo IP del client simulato è 192.168.1.5.
- Il client invia il traffico proveniente dalla porta 1234.
- Il traffico è destinato a un server all'indirizzo IP 198.51.100.100.
- Il traffico è destinato al porto 80.

Nel comando non è stata menzionata alcuna interfaccia esterna. Ciò è dovuto alla progettazione del tracer dei pacchetti. Lo strumento indica il modo in cui il firewall elabora il tipo di tentativo di connessione, incluse le modalità di instradamento e di uscita dall'interfaccia.

> **Suggerimento**: Per ulteriori informazioni sulla funzionalità di traccia dei pacchetti, consultare la sezione Traccia dei pacchetti con Packet Tracer nella *guida alla configurazione di Cisco ASA serie 5500 dalla CLI, versione 8.4 e 8.6*.

Acquisisci

Per applicare un'acquisizione, immettere i seguenti comandi:

```
ASA# capture capin interface inside match tcp host 192.168.1.5 host 198.51.100.100
ASA# capture capout interface outside match tcp any host 198.51.100.100

ASA#show capture capin

3 packets captured

1: 11:31:23.432655 192.168.1.5.58799 > 198.51.100.100.80: S 780523448:
780523448(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
2: 11:31:23.712518 198.51.100.100.80 > 192.168.1.5.58799: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712884 192.168.1.5.58799 > 198.51.100.100.80: . ack 2123396068
win 32768

ASA#show capture capout

3 packets captured

1: 11:31:23.432869 203.0.113.2.58799 > 198.51.100.100.80: S 1633080465:
1633080465(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>
2: 11:31:23.712472 198.51.100.100.80 > 203.0.113.2.58799: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712914 203.0.113.2.58799 > 198.51.100.100.80: . ack 95714630
win 32768/pre>
```

Il firewall ASA può acquisire il traffico in entrata o in uscita dalle interfacce. Questa funzionalità di acquisizione è fantastica perché può dimostrare in modo definitivo se il traffico arriva a un firewall o se ne esce. L'esempio precedente mostra la configurazione di due clip denominate **capin** e **capout** rispettivamente sulle interfacce interna ed esterna. I comandi **capture** utilizzano la parola chiave **match**, che consente di specificare il traffico da acquisire.

Nell'esempio di acquisizione *capin*, viene indicato che si desidera far corrispondere il traffico visualizzato sull'interfaccia interna (in entrata o in uscita) che corrisponde all'*host tcp 192.168.1.5 host 198.51.100.100*. In altre parole, si desidera acquisire tutto il traffico TCP inviato dall'host *192.168.1.5* all'host *198.51.100.10*, o viceversa. L'utilizzo della parola chiave **match** consente al firewall di acquisire il traffico in modo bidirezionale. Il comando **capture** definito per l'interfaccia esterna non fa riferimento all'indirizzo IP del client interno perché il firewall esegue PAT su tale indirizzo IP del client. Di conseguenza, non è possibile stabilire una corrispondenza con l'indirizzo IP del client. Nell'esempio viene invece utilizzato **any** per indicare che tutti gli indirizzi IP possibili soddisferanno la condizione.

Dopo aver configurato le clip, è possibile tentare di stabilire nuovamente la connessione e continuare a visualizzarle con il comando **show capture***<nome_acquisizione>*. In questo esempio, è possibile vedere che il client è in grado di connettersi al server, come dimostra l'handshake TCP a 3 vie rilevato nelle acquisizioni.

Informazioni correlate

- Cisco Adaptive Security Device Manager
- Cisco ASA serie 5500-X Next-Generation Firewall

- RFC (Requests for Comments)
- Cisco ASA Series CLI Configuration Guide, 9.0ÂÂ Configurazione delle route statiche e predefinite
- Documentazione e supporto tecnico ÂÂ Cisco Systems