PIX/ASA 7.x/FWSM 3.x: Conversione di più indirizzi IP globali in un singolo indirizzo IP locale utilizzando il protocollo NAT dei criteri statici

Sommario

Introduzione

In questo documento viene fornita una configurazione di esempio per il mapping di un indirizzo IP locale a due o più indirizzi IP globali tramite NAT (Network Address Translation) statico basato su criteri sul software PIX/Adaptive Security Appliance (ASA) 7.x.

Prerequisiti

Requisiti

Prima di provare la configurazione, verificare che sia soddisfatto il seguente requisito:

- Accertarsi di avere una conoscenza operativa della CLI di PIX/ASA 7.x e una precedente esperienza nella configurazione degli elenchi degli accessi e del NAT statico.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- In questo esempio specifico viene usato un'ASA 5520. Tuttavia, le configurazioni NAT delle policy funzionano su qualsiasi appliance PIX o ASA con versione 7.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.

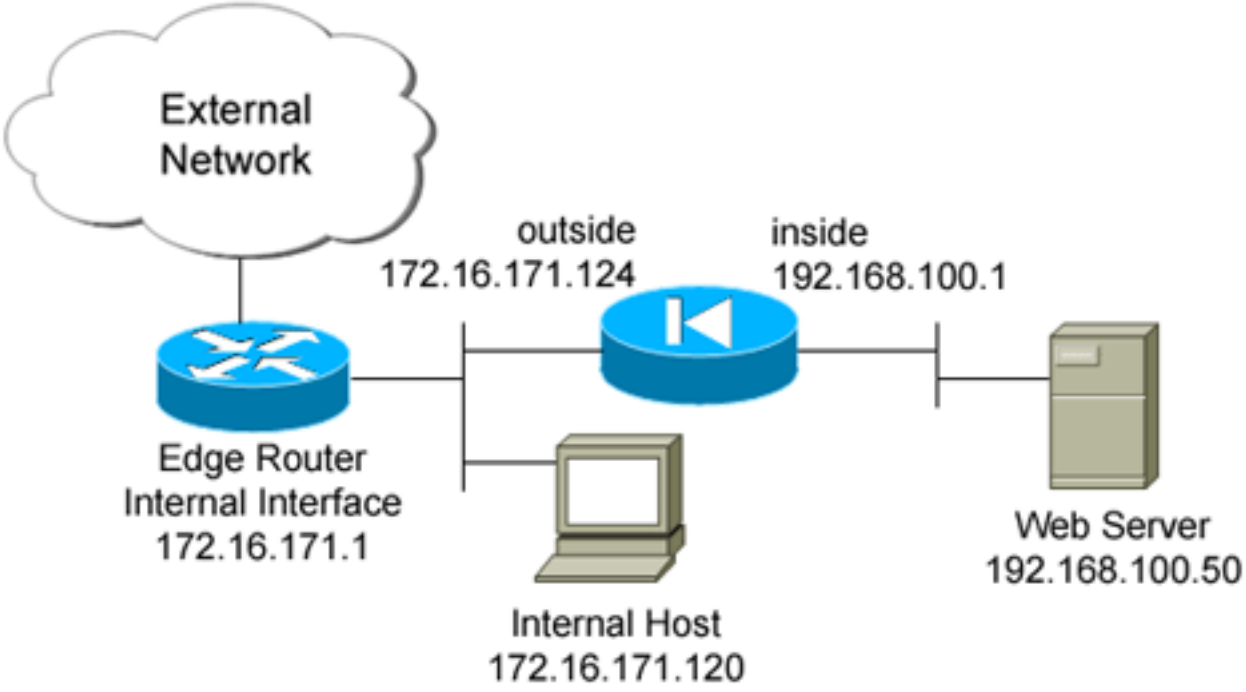
Configurazione

Nell'esempio di configurazione, il server Web interno è situato alla posizione 192.168.100.50, dietro l'appliance ASA. Il requisito è che il server deve essere accessibile all'interfaccia della rete esterna tramite l'indirizzo IP interno 192.168.100.50 e l'indirizzo esterno 172.16.171.125. Esiste anche un requisito dei criteri di sicurezza che prevede che l'indirizzo IP privato 192.168.100.50 sia accessibile solo dalla rete 172.16.171.0/24. Inoltre, il protocollo ICMP (Internet Control Message Protocol) e il traffico della porta 80 sono gli unici protocolli consentiti in entrata nel server Web interno. Poiché esistono due indirizzi IP globali mappati a un indirizzo IP locale, è necessario utilizzare il criterio NAT. In caso contrario, PIX/ASA rifiuta le due statistiche uno-a-uno con un errore di indirizzo sovrapposto.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete



Configurazione

Nel documento viene usata questa configurazione.

```
ciscoasa(config)#show run
: Saved
:
ASA Version 7.2(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.16.171.124 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.100.1 255.255.255.0
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 nameif management
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive


!--- policy_nat_web1 and policy_nat_web2 are two access-
lists that match the source !--- address we want to
translate on. Two access-lists are required, though they
!--- can be exactly the same. access-list
policy_nat_web1 extended permit ip host 192.168.100.50
any
access-list policy_nat_web2 extended permit ip host
192.168.100.50 any

!--- The inbound_outside access-list defines the
security policy, as previously described. !--- This
access-list is applied inbound to the outside interface.
access-list inbound_outside extended permit tcp
172.16.171.0 255.255.255.0
   host 192.168.100.50 eq www
access-list inbound_outside extended permit icmp
172.16.171.0 255.255.255.0
   host 192.168.100.50 echo-reply
access-list inbound_outside extended permit icmp
```

```
172.16.171.0 255.255.255.0
   host 192.168.100.50 echo
access-list inbound_outside extended permit tcp any host
172.16.171.125 eq www
access-list inbound_outside extended permit icmp any
host 172.16.171.125 echo-reply
access-list inbound_outside extended permit icmp any
host 172.16.171.125 echo
pager lines 24
logging asdm informational
mtu management 1500
mtu inside 1500
mtu outside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400

!--- This first static allows users to reach the
translated global IP address of the !--- web server.
Since this static appears first in the configuration,
for connections !--- initiated outbound from the
internal web server, the ASA translates the source !---
address to 172.16.171.125. static (inside,outside)
172.16.171.125  access-list policy_nat_web1

!--- The second static allows networks to access the web
server by its private !--- IP address of 192.168.100.50.
static (inside,outside) 192.168.100.50  access-list
policy_nat_web2

!--- Apply the inbound_outside access-list to the
outside interface. access-group inbound_outside in
interface outside

route outside 0.0.0.0 0.0.0.0 172.16.171.1 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
http server enable
http 192.168.1.0 255.255.255.0 management
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 preset_dns_map
 parameters
  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
!
service-policy global_policy global
prompt hostname context
```

Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

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

1. Sul router upstream IOS® 172.16.171.1, verificare di poter raggiungere entrambi gli indirizzi IP globali del server Web con il comando **ping**.

```
router#ping 172.16.171.125

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.171.125, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
router#ping 192.168.100.50

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.50, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

2. Sull'appliance ASA, verificare di vedere le traduzioni create nella tabella delle traduzioni (xlate).

```
ciscoasa(config)#show xlate global 192.168.100.50
2 in use, 28 most used
Global 192.168.100.50 Local 192.168.100.50
ciscoasa(config)#show xlate global 172.16.171.125
2 in use, 28 most used
Global 172.16.171.125 Local 192.168.100.50
```

Risoluzione dei problemi

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

Se il ping o la connessione ha esito negativo, provare a utilizzare syslogs per determinare se vi sono problemi con la configurazione di conversione. In una rete poco utilizzata, ad esempio in un

ambiente lab, le dimensioni del buffer di registrazione sono in genere sufficienti per la risoluzione del problema. In caso contrario, è necessario inviare i syslog a un server syslog esterno. Abilitare la registrazione nel buffer al livello 6 per verificare se la configurazione è corretta in queste voci di syslog.

```
ciscoasa(config)#logging buffered 6
ciscoasa(config)#logging on

!--- From 172.16.171.120, initiate a TCP connection to port 80 to both the external !---
(172.16.171.125) and internal addresses (192.168.100.50). ciscoasa(config)#show log
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: level debugging, 4223 messages logged
    Trap logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: level informational, 4032 messages logged
%ASA-5-111008: User 'enable_15' executed the 'clear logging buffer' command.
%ASA-7-609001: Built local-host outside:172.16.171.120
%ASA-7-609001: Built local-host inside:192.168.100.50
%ASA-6-302013: Built inbound TCP connection 67 for outside:172.16.171.120/33687
(172.16.171.120/33687) to inside:192.168.100.50/80 (172.16.171.125/80)
%ASA-6-302013: Built inbound TCP connection 72 for outside:172.16.171.120/33689
(172.16.171.120/33689) to inside:192.168.100.50/80 (192.168.100.50/80)
```

Se nel registro vengono visualizzati errori di conversione, verificare le configurazioni NAT. Se non si osserva alcun syslog, usare la funzione **capture** sull'appliance ASA per tentare di catturare il traffico sull'interfaccia. Per configurare un'acquisizione, è necessario prima specificare un elenco degli accessi che corrisponda a un tipo specifico di traffico o flusso TCP. Quindi, applicare questa acquisizione a una o più interfacce per avviare l'acquisizione dei pacchetti.

```
!--- Create a capture access-list to match on port 80 traffic to !--- the external IP address of
172.16.171.125. !--- Note: These commands are over two lines due to spatial reasons.

ciscoasa(config)#access-list acl_capout permit tcp host 172.16.171.120
     host 172.16.171.125 eq 80
ciscoasa(config)#access-list acl_capout permit tcp host 172.16.171.125
    eq 80 host 172.16.171.120
ciscoasa(config)#

!--- Apply the capture to the outside interface.

ciscoasa(config)#capture capout access-list acl_capout interface outside

!--- After you initiate the traffic, you see output similar to this when you view !--- the
capture. Note that packet 1 is the SYN packet from the client, while packet !--- 2 is the SYN-
ACK reply packet from the internal server. If you apply a capture !--- on the inside interface,
in packet 2 you should see the server reply with !--- 192.168.100.50 as its source address.

ciscoasa(config)#show capture capout
```

```
4 packets captured
   1: 13:17:59.157859 172.16.171.120.21505 > 172.16.171.125.80: S
      2696120951:2696120951(0) win 4128 <mss 1460>
   2: 13:17:59.159446 172.16.171.125.80 > 172.16.171.120.21505: S
      1512093091:1512093091(0) ack 2696120952 win 4128 <mss 536>
   3: 13:17:59.159629 172.16.171.120.21505 > 172.16.171.125.80: .
      ack 1512093092 win 4128
   4: 13:17:59.159873 172.16.171.120.21505 > 172.16.171.125.80: .
      ack 1512093092 win 4128
```

Informazioni correlate

- Guida di riferimento ai comandi di ASA 7.2
- Software Cisco PIX Firewall
- Riferimenti per i comandi di Cisco Secure PIX Firewall
- Avvisi sui prodotti per la sicurezza (inclusi PIX)
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems