PIX/ASA 7.x/FWSM 3.x: Übertragen mehrerer globaler IP-Adressen in eine einzige lokale IP-Adresse mithilfe von Static Policy NAT

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration für die Zuordnung einer lokalen IP-Adresse zu zwei oder mehr globalen IP-Adressen mithilfe der richtlinienbasierten statischen Network Address Translation (NAT) auf der PIX/Adaptive Security Appliance (ASA) 7.x-Software.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderung erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Vergewissern Sie sich, dass Sie über Kenntnisse der CLI von PIX/ASA 7.x verfügen und über Erfahrungen bei der Konfiguration von Zugriffslisten und statischen NATs verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- In diesem speziellen Beispiel wird eine ASA 5520 verwendet. Die Richtlinien-NAT-Konfigurationen funktionieren jedoch auf allen PIX- oder ASA-Appliances, die 7.x ausführen.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

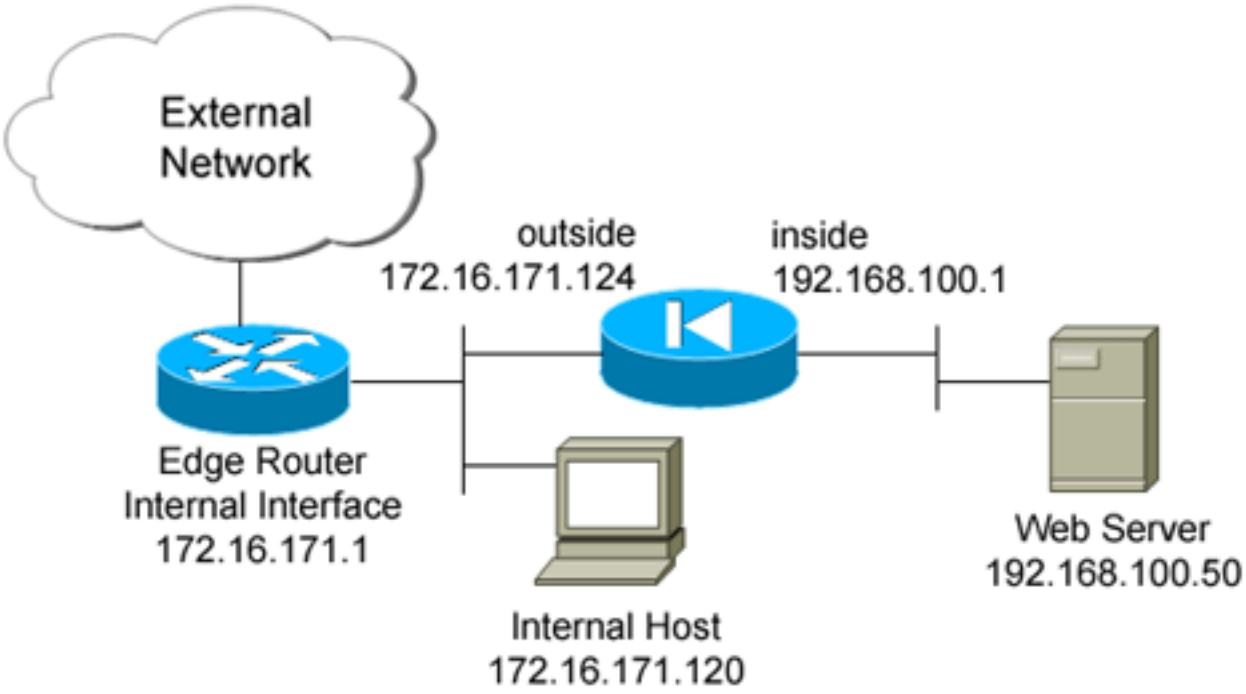
Konfigurieren

In diesem Konfigurationsbeispiel befindet sich hinter der ASA ein interner Webserver mit der Adresse 192.168.100.50. Der Server muss über die interne IP-Adresse 192.168.100.50 und die externe Adresse 172.16.171.125 für die externe Netzwerkschnittstelle zugänglich sein. Es besteht außerdem die Anforderung einer Sicherheitsrichtlinie, dass auf die private IP-Adresse 192.168.100.50 nur vom Netzwerk 172.16.171.0/24 zugegriffen werden kann. Darüber hinaus sind Internet Control Message Protocol (ICMP)- und Port 80-Datenverkehr die einzigen Protokolle, die eingehende Anrufe an den internen Webserver zulassen. Da zwei globale IP-Adressen einer lokalen IP-Adresse zugeordnet sind, müssen Sie die Richtlinie NAT verwenden. Andernfalls weist PIX/ASA die beiden Eins-zu-Eins-Statistiken mit einem sich überschneidenden Adressfehler zurück.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

Dieses Dokument verwendet diese Netzwerkeinrichtung.



Konfiguration

In diesem Dokument wird diese Konfiguration verwendet.

```
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
```

Überprüfen

Dieser Abschnitt enthält Informationen zur Bestätigung, dass Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

1. Überprüfen Sie auf dem Upstream-IOS®-Router 172.16.171.1, ob Sie über den Befehl **ping** beide globalen IP-Adressen des Webservers erreichen können.
```
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. Vergewissern Sie sich auf der ASA, dass Sie die Übersetzungen sehen, die in der Übersetzungstabelle (Xlate) enthalten sind.
```
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
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Wenn Ihr Ping oder Ihre Verbindung nicht erfolgreich ist, versuchen Sie, mithilfe von Syslogs festzustellen, ob Probleme mit der Übersetzungskonfiguration vorliegen. In einem wenig genutzten Netzwerk (z. B. in einer Laborumgebung) reicht die Größe des Protokollierungspuffers normalerweise aus, um das Problem zu beheben. Andernfalls müssen Sie die Syslogs an einen externen Syslog-Server senden. Aktivieren Sie die Protokollierung auf Stufe 6 im Puffer, um festzustellen, ob die Konfiguration in diesen Syslog-Einträgen korrekt ist.

```
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)
```

Wenn Übersetzungsfehler im Protokoll angezeigt werden, überprüfen Sie Ihre NAT-Konfigurationen. Wenn Sie keine Syslogs beobachten, verwenden Sie die Capture-Funktion auf der ASA, um den Datenverkehr auf der Schnittstelle zu erfassen. Um eine Erfassung einzurichten, müssen Sie zunächst eine Zugriffsliste für einen bestimmten Datenverkehr oder TCP-Datenfluss angeben. Anschließend müssen Sie diese Erfassung auf eine oder mehrere Schnittstellen anwenden, um Pakete zu erfassen.

```
!--- 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
```

Zugehörige Informationen

- ASA 7.2 Befehlsreferenz
- Cisco PIX Firewall-Software
- Cisco Secure PIX Firewall - Befehlsreferenzen
- Problemhinweise zu Sicherheitsprodukten (einschließlich PIX)
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems