PIX/ASA 7.x/FWSM 3.x:使用靜態策略NAT將多個全域性IP地址轉換為單個本地IP地址

目錄

簡介

本文檔提供在PIX/自適應安全裝置(ASA)7.x軟體上通過基於策略的靜態網路地址轉換(NAT)將一個本地IP地址對映到兩個或多個全域性IP地址的示例配置。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 確保您瞭解PIX/ASA 7.x CLI的工作知識和配置訪問清單和靜態NAT的先前經驗。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 此特定示例使用ASA 5520。但是，策略NAT配置在運行7.x的任何PIX或ASA裝置上均可運行。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

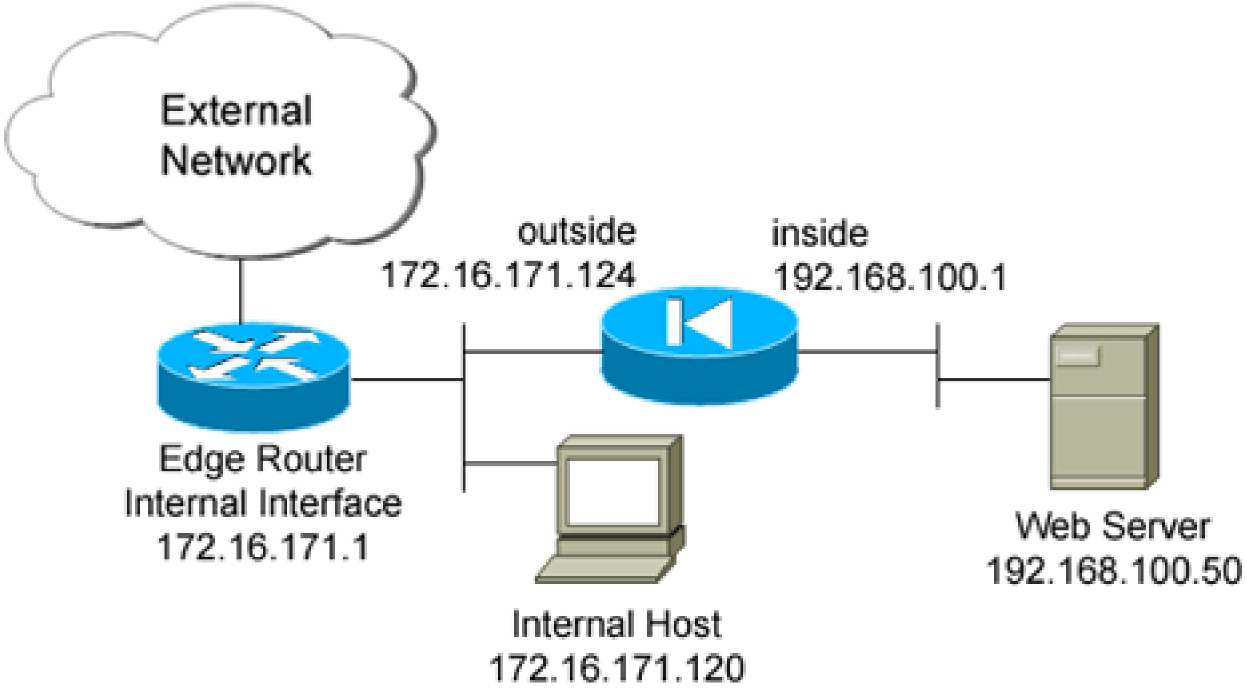
設定

此配置示例有一個位於ASA後方192.168.100.50的內部Web伺服器。要求是伺服器需要通過其內部IP地址192.168.100.50及其外部地址172.16.171.125來訪問外部網路介面。還有一項安全策略要求，即只有通過172.16.171.0/24網路才能訪問私有IP地址192.168.100.50。此外，網際網路控制訊息通訊協定(ICMP)和連線埠80流量是允許傳入內部Web伺服器的唯一通訊協定。由於有兩個全域性IP地址對映到一個本地IP地址，因此需要使用策略NAT。否則，PIX/ASA會拒絕帶有重疊地址錯誤的兩個一對一靜態圖。

註：使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

網路圖表

本文使用此網路設定



組態

本檔案會使用此組態。

```
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
```

驗證

本節提供的資訊可用於確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析
。

1. 在上游IOS®路由器172.16.171.1上，驗證您是否可以通過**ping**命令到達Web伺服器的兩個全域性IP地址。

   ```
   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. 在ASA上，驗證您是否看到轉換(xlate)表中構建的轉換。

   ```
   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
   ```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

如果ping或連線失敗，則嘗試使用syslog來確定轉換配置是否存在任何問題。在少量使用的網路（如實驗室環境）中，日誌記錄緩衝區大小通常足以用於排除故障。否則，您需要將系統日誌傳送到外部系統日誌伺服器。啟用到第6級緩衝區的日誌記錄，以檢視這些系統日誌條目中的配置是否正確。

```
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)
```

如果在日誌中看到轉換錯誤，請仔細檢查NAT配置。如果未觀察到任何系統日誌，請使用ASA上的**capture**功能嘗試捕獲介面上的流量。為了設定捕獲，必須首先指定訪問清單以匹配特定型別的流量或TCP流。接下來，您必須將此捕獲應用到一個或多個介面，才能開始捕獲資料包。

```
!--- 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
```

相關資訊

- ASA 7.2命令參考
- Cisco PIX防火牆軟體
- Cisco Secure PIX防火牆命令參考
- 安全產品現場通知（包括PIX）
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems