PIX/ASA 7.x/FWSM 3.x：使用静态策略 NAT 将多个全局 IP 地址转换为单个本地 IP 地址

目录

简介

本文档提供了一个示例配置，在 PIX/自适应安全设备 (ASA) 7.x 软件中通过基于策略的静态网络地址转换 (NAT) 将一个本地 IP 地址映射到两个或更多全局 IP 地址。

先决条件

要求

在尝试进行此配置之前，请确保满足以下要求：

- 确保您熟悉 PIX/ASA 7.x CLI 并且以前配置过访问列表和静态 NAT。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 这一特定示例使用 ASA 5520。但是，策略 NAT 配置适用于所有运行 7.x 的 PIX 或 ASA 设备。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

本配置示例中有一个内部 Web 服务器，它位于 ASA 之后，地址为 192.168.100.50。要求是：服务器需要通过其内部 IP 地址 192.168.100.50 和外部地址 172.16.171.125 访问外部网络接口。还有一项安全策略要求：专用 IP 地址 192.168.100.50 只能通过 172.16.171.0/24 网络访问。另外，互联网控制消息协议(ICMP)和端口80流量是唯一的协议允许入站到内部网络服务器。因为有两个全局 IP 地址映射到一个本地 IP 地址，所以您需要使用策略 NAT。否则， PIX/ASA 会因重迭地址错误拒绝两个一对一的静态映射。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置

配置

本文档使用以下配置。

```
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
```

验证

本部分提供的信息可帮助您确认您的配置是否可正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

1. 在上游 IOS® 路由器 172.16.171.1 上，请通过 **ping** 命令验证您是否能够访问 Web 服务器的两个全局 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 在，请验证您是否看到在转换 (xlate) 表里建立的转换。`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`**

故障排除

本部分提供的信息可用于对配置进行故障排除。

如果 ping 命令或连接失败，请尝试使用 syslog 确定转换配置是否有问题。在负荷很轻的网络（例

如实验室环境）中，日志缓冲区大小通常足以满足排除故障的需要。否则，您需要将 syslog 发送到外部 syslog 服务器中。在第 6 级对缓冲区启用日志记录以便在这些 syslog 条目中查看配置是否正确。

```
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)
```

如果在日志中看到转换错误，请仔细检查您的 NAT 配置。如果未看到任何系统日志，请使用 ASA 中的**捕获**功能尝试捕获接口上的数据流。为了设置捕获，您必须首先指定一个访问列表以匹配特定类型的数据流或 TCP 流。接下来，您必须将此捕获应用到一个或多个接口以便开始捕获数据包。

```
!--- 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
```

相关信息

- ASA 7.2 命令参考
- Cisco PIX 防火墙软件
- Cisco Secure PIX 防火墙命令参考
- 安全产品 Field Notices（包括 PIX）
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems