PIX/ASA 7.x/FWSM 3.x: Traduza endereços IP globais múltiplos a um único endereço IP local usando a política estática NAT

Índice

Introdução

Este documento fornece uma configuração de exemplo de mapeamento entre um endereço IP local e dois ou mais endereços IP globais através da Tradução de Endereço da Rede (NAT) estática baseada em política no software PIX/Adaptive Security Appliance (ASA) 7.x.

Pré-requisitos

Requisitos

Assegure-se de que você cumpra esta exigência antes que você tente esta configuração:

- Assegure-se de que você tenha um conhecimento em funcionamento do PIX/ASA 7.x CLI e experiência prévia que configura listas de acesso e NAT estático.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Este exemplo específico usa um ASA 5520. Contudo as configurações de NAT da política trabalham em todo o dispositivo PIX ou ASA que executar 7.x.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

Este exemplo de configuração tem um servidor de Web interno em 192.168.100.50, situado atrás do ASA. A exigência é que o server precisa de ser acessível à relação de rede externa por seu endereço IP interno de 192.168.100.50 e por seu endereço externo de 172.16.171.125. Há igualmente uma exigência da política de segurança que o endereço IP privado de 192.168.100.50 pode somente ser alcançado pela rede 172.16.171.0/24. Adicionalmente, o Internet Control Message Protocol (ICMP) e o tráfego da porta 80 são os únicos protocolos permitiram de entrada ao servidor de Web interno. Desde que há dois endereços IP globais traçados a um endereço IP local, você precisa de usar a política NAT. Se não, o PIX/ASA rejeita as duas estatísticas lineares com um erro de endereço de sobreposição.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento usa esta instalação de rede

Configuração

Este documento usa esta configuração.

```
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
```

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração funciona adequadamente.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

1. No roteador ascendente 172.16.171.1 IOS®, verifique que você pode alcançar ambos os endereços IP globais do servidor de Web através do **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. No ASA, verifique que você vê as traduções que são construídas na tabela da tradução (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`**

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Se sua sibilo ou conexão são mal sucedido, tente usar Syslog para determinar se há algum problema com a configuração da tradução. Em uma rede levemente usada (tal como um ambiente de laboratório), o tamanho de logging buffer é geralmente suficiente para pesquisar defeitos o problema. Se não, você precisa de enviar os Syslog a um servidor syslog externo. Enable que registra ao buffer a nível 6 a fim ver se a configuração está correta nestas entradas do 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 você vê erros da tradução no log, verifique novamente suas configurações de NAT. Se você não observa nenhuns Syslog, use a função da captação no ASA para tentar capturar o tráfego na relação. A fim estabelecer uma captação, você deve primeiramente especificar uma lista de acesso para combinar em um tipo de tráfego ou em um fluxo de TCP específico. Em seguida, você deve aplicar esta captação a umas ou várias relações a fim começar capturar pacotes.

```
!--- 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
```

Informações Relacionadas

- Referência de comandos ASA 7.2
- Cisco PIX Firewall Software
- Referências do comando Cisco Secure PIX Firewall
- Avisos de campo de produto de segurança (incluindo PIX)
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems