PIX/ASA 7.x/FWSM 3. x: Преобразование нескольких глобальных IP-адресов в один локальный IP-адрес с помощью статической политики NAT

Содержание

Введение

В этом документе представлен пример конфигурации для привязки одного локального IP-адреса к двум или нескольким глобальным IP-адресам посредством статического преобразования сетевых адресов на основе политик (NAT) в программном обеспечении устройств PIX / устройств адаптивной защиты (ASA) версии 7.x.

Предварительные условия

Требования

Перед попыткой применения конфигурации убедитесь в том, что следующие требования выполняются:

- Перед настройкой списков контроля доступа и статического преобразования NAT убедитесь в том, что вы владеете практическими знаниями интерфейса командной строки PIX/ASA 7.x и имеете опыт работы с ним.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного

обеспечения и оборудования:

- В данном конкретном примере используется модель ASA 5520, однако конфигурации NAT на основе политик работает с любым устройством PIX или ASA под управлением ПО версии 7.x.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Настройка

В этом примере конфигурации имеется внутренний web-сервер по адресу 192.168.100.50, расположенный за устройством ASA. Требуется, чтобы сервер был доступен для внешнего сетевого интерфейса по своему внутреннему IP-адресу 192.168.100.50 и внешнему адресу 172.16.171.125. Также имеется требование политики безопасности: частный IP-адрес 192.168.100.50 должен быть доступен исключительно из сети 172.16.171.0/24. Дополнительно входящие протоколы доступа ко внутреннему web-серверу ограничиваются межсетевым протоколом управляющих сообщений (ICMP) и трафиком на порт 80. Поскольку имеется два глобальных IP-адреса, привязанных к одному локальному IP-адресу, то необходимо использовать политики NAT. В противном случае устройство PIX/ASA отклонит два статических назначения «один к одному» по причине наложения адресов.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Схема сети

В настоящем документе используется следующая схема сети

!--- конфигурацию

В данном документе используется следующая конфигурация.

```
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
```

Проверка

В данном разделе содержатся сведения о проверке работы конфигурации.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

1. **На вышестоящем маршрутизаторе IOS® с адресом 172.16.171.1 убедитесь в доступности глобальных IP-адресов web-сервера по команде 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. На устройстве ASA проверьте, видны ли преобразования, построенные в таблице преобразований (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`

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

В случае непрохождения эхозапроса или подключения можно попробовать использовать системные журналы, чтобы проверить наличие проблем с конфигурацией преобразования. В активно используемой сети (например, лабораторной среде) размер буфера журнала обычно достаточен для диагностики проблемы. Если это не так, то журнальные сообщения следует отправлять на внешний сервер syslog. Чтобы проверить, верна ли конфигурация в этих записях syslog, разрешите ведение журналов в буфер на уровне 6.

```
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)
```

При наличии в журнале ошибок преобразования тщательно перепроверьте конфигурацию NAT. **Если сообщений в журнале syslog не наблюдается, воспользуйтесь функцией capture устройства ASA для перехвата трафика на интерфейсе.** Чтобы настроить перехват трафика, необходимо вначале определить список контроля доступа для сопоставления с определенным типом трафика или потоком TCP. Затем механизм перехвата трафика нужно применить к одному или нескольким интерфейсам, чтобы начать перехватывать пакеты.

```
!--- 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
```

Дополнительные сведения

- Справочник по командам ASA 7.2
- Cisco PIX Firewall Software
- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Уведомления о дефектах продуктов по безопасности (включая PIX)
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация