Настройте исправление DNS для трех интерфейсов NAT на выпуске 9 ASA. x

Содержание

Введение

Этот документ предоставляет пример конфигурации для выполнения врачевания Системы доменных имен (DNS) на ASA Устройство адаптивной защиты (ASA) серии 5500-X, которое использует Объектные/Автоматические операторы Технологии NAT. Исправление DNS позволяет устройству защиты перезаписывать A-записи DNS.

Перезапись DNS выполняет две функции:

- Преобразует публичный адрес (маршрутизируемый или сопоставляемый адрес) в отклик DNS на частный адрес (реальный адрес), когда клиент DNS находится на

частном интерфейсе.
- Преобразует частный адрес в публичный адрес, когда клиент DNS находится на публичном интерфейсе.

Предварительные условия

Требования

Cisco сообщает, что проверка DNS должна быть включена для выполнения исправления DNS на устройстве безопасности. Проверка DNS по умолчанию включена.

Когда проверка DNS включена, устройство защиты выполняет следующие задачи:

- Преобразовывает запись DNS на основе конфигурации, завершенной с использованием объектных/автоматических команд NAT (перезапись DNS). Преобразование применяется только к A-записи в отклике DNS. Поэтому на обратные просмотры, которые запрашивают Указатель (PTR) запись, не влияет перезапись DNS. В версии ASA 9.0 (1) и позже, трансляция PTR DNS делает запись для обратных поисков DNS при использовании IPv4 NAT, IPv6 NAT и NAT64 с проверкой DNS, включенной для правила NAT.**Примечание:** Перезапись DNS не совместима с преобразованием адреса статического порта (PAT), потому что множественные правила PAT применимы для каждой A-записи, и правило PAT использовать неоднозначно.
- Задает максимальную длину сообщения DNS (по умолчанию 512 байт, максимум 65535 байт). Повторная сборка выполнена по мере необходимости, чтобы проверить, что длина пакета является меньше, чем настроенная максимальная длина. Пакет сбрасывается, если его длина превышает максимальную.**Примечание:** При вводе **команды inspect dns** без опции максимальной длины размер Пакета DNS не проверен.
- Задает длину доменного имени в 255 байт и длину метки в 63 байта.
- Проверяет целостность доменного имени, на которое ссылается указатель, если в сообщении DNS встречаются указатели сжатия.
- Проверяет наличие петли указателя сжатия.

Используемые компоненты

Сведения в этом документе основываются на ASA Устройство безопасности серии 5500-X, Версия 9. 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.

Родственные продукты

Эта конфигурация может также использоваться с Устройством безопасности серии 5500 Cisco ASA, Версией 8.4 или позже.

Примечание: Конфигурация ASDM применима к версии 7.x только.

Общие сведения

При обычном DNS-обмене клиент отправляет URL или имя хоста на DNS-сервер, чтобы определить IP-адрес этого хоста. DNS-сервер получает запрос, ищет сопоставление имя — IP-адрес для данного хоста и предоставляет A-запись с IP-адресом клиенту. Хотя эта процедура хорошо работает во многих ситуациях, могут возникать и проблемы. Проблемы могут возникнуть, когда клиент и хост, с которым клиент пытается связаться, находятся в одной частной сети за NAT, а DNS-сервер, используемый клиентом, находится в другой, общедоступной сети.

Сценарий: Три интерфейса NAT (внутренний, внешний, dmz)

Топология

Эта схема является примером данной ситуации. В этом случае клиент в 192.168.100.2 хочет использовать **сервер. пример.** URL **com** для доступа к серверу WWW в 10.10.10.10. Сервисы DNS для клиента предоставлены внешним DNS-сервером по адресу 172.22.1.161. Так как DNS-сервер расположен в другой общедоступной сети, ему неизвестен частный IP-адрес сервера WWW. Вместо этого он располагает адресом сопоставления сервера WWW 172.20.1.10. **Таким образом, DNS-сервер содержит сопоставление имя — IP-адрес в виде server.example.com — 172.20.1.10.**

Проблема: Клиент не может обратиться к серверу WWW

Без исправления DNS или другого решения, пригодного в данной ситуации, если клиент отправит DNS-запрос IP-адреса для имени server.example.com, он не сможет получить доступ к серверу WWW. Это произойдет потому, что клиент получит A-запись, содержащую сопоставленный публичный адрес сервера WWW 172.20.1.10. Когда клиент попытается обратиться к этому IP-адресу, устройство защиты отбрасывает пакеты, так как оно не разрешает перенаправление пакетов на тот же интерфейс. Вот как выглядит область NAT в конфигурации, когда исправление DNS не включено:

```
ASA Version 9.x
!
hostname ciscoasa

!--- Output suppressed.

access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www
!--- Output suppressed.

object network obj-192.168.100.0
network 192.168.100.0 255.255.255.0
nat (inside,outside) dynamic interface

object network obj-10.10.10.10
```

```
host 10.10.10.10
nat (dmz,outside) static 172.20.1.10

!--- Static translation to allow hosts on the outside access
!--- to the WWW server.
access-group OUTSIDE in interface outside

!--- Output suppressed.
```

Вот как выглядит конфигурация в ASDM, когда исправление DNS не включено:

Вот захват пакета событий, когда исправление DNS не включено:

1. Клиент отправляет запрос DNS.
```
No.     Time       Source           Destination
Protocol Info
1 0.000000 192.168.100.2 172.22.1.161 DNS Standard query
A server.example.com

Frame 1 (78 bytes on wire, 78 bytes captured)
Ethernet II, Src: Cisco_c8:e4:00 (00:04:c0:c8:e4:00), Dst: Cisco_9c:c6:1f
(00:0a:b8:9c:c6:1f)
Internet Protocol, Src: 192.168.100.2 (192.168.100.2), Dst: 172.22.1.161
(172.22.1.161)
User Datagram Protocol, Src Port: 50879 (50879), Dst Port: domain (53)
Domain Name System (query)
[Response In: 2]
Transaction ID: 0x0004
Flags: 0x0100 (Standard query)
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
server.example.com: type A, class IN
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
```
2. ASA выполняет PAT для DNS-запроса, и запрос пересылается. Заметьте, что исходный адрес пакета изменился на внешний интерфейс ASA.
```
No.     Time       Source
Destination     Protocol Info
1 0.000000 172.20.1.2 172.22.1.161 DNS Standard query
A server.example.com

Frame 1 (78 bytes on wire, 78 bytes captured)
Ethernet II, Src: Cisco_9c:c6:1e (00:0a:b8:9c:c6:1e), Dst: Cisco_01:f1:22
(00:30:94:01:f1:22)
Internet Protocol, Src: 172.20.1.2 (172.20.1.2), Dst: 172.22.1.161
(172.22.1.161)
User Datagram Protocol, Src Port: 1044 (1044), Dst Port: domain (53)
Domain Name System (query)
[Response In: 2]
Transaction ID: 0x0004
Flags: 0x0100 (Standard query)
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
server.example.com: type A, class IN
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
```

3. DNS-сервер отвечает сопоставленным адресом сервера WWW.No. Time Source Destination Protocol Info
2 0.005005 **172.22.1.161 172.20.1.2 DNS Standard query response A 172.20.1.10**

Frame 2 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Cisco_01:f1:22 (00:30:94:01:f1:22), Dst: Cisco_9c:c6:1e (00:0a:b8:9c:c6:1e)
Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 172.20.1.2 (172.20.1.2)
User Datagram Protocol, Src Port: domain (53), Dst Port: 1044 (1044)
Domain Name System (response)
[Request In: 1]
[Time: 0.005005000 seconds]
Transaction ID: 0x0004
Flags: 0x8580 (Standard query response, No error)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
server.example.com: type A, class IN
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
Answers
server.example.com: type A, class IN, addr 172.20.1.10
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
Time to live: 1 hour
Data length: 4
Addr: 172.20.1.10

4. ASA отменяет преобразование адреса назначения ответа DNS и пересылает пакет клиенту. **Заметьте, что при отключенном исправлении DNS запись Addr в ответе все еще является сопоставленным адресом сервера WWW.**No. Time Source Destination Protocol Info
2 0.005264 172.22.1.161 **192.168.100.2** DNS Standard query response A 172.20.1.10

Frame 2 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Cisco_9c:c6:1f (00:0a:b8:9c:c6:1f), Dst: Cisco_c8:e4:00 (00:04:c0:c8:e4:00)
Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 192.168.100.2 (192.168.100.2)
User Datagram Protocol, Src Port: domain (53), Dst Port: 50879 (50879)
Domain Name System (response)
[Request In: 1]
[Time: 0.005264000 seconds]
Transaction ID: 0x0004
Flags: 0x8580 (Standard query response, No error)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
server.example.com: type A, class IN
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
Answers
server.example.com: type A, class IN, addr 172.20.1.10

```
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
Time to live: 1 hour
Data length: 4
Addr: 172.20.1.10
```

5. На этом этапе клиент пытается обратиться к серверу WWW по адресу 172.20.1.10. ASA создает запись соединения для этого обмена данными. Однако, так как ASA не разрешает прохождение трафика с внутреннего интерфейса на внешний и на dmz, соединение простаивает. Записи журнала ASA выглядят следующим образом:`%ASA-6-302013: Built outbound TCP connection 54175 for outside:172.20.1.10/80 (172.20.1.10/80) to inside:192.168.100.2/11001 (172.20.1.2/1024)`

   `%ASA-6-302014: Teardown TCP connection 54175 for outside:172.20.1.10/80 to inside:192.168.100.2/11001 duration 0:00:30 bytes 0` **`SYN Timeout`**

Решение: Ключевое слово "dns"

Исправление DNS с помощью ключевого слова "dns"

Исправление DNS с помощью ключевого слова dns дает устройству защиты возможность перехватывать и перезаписывать содержимое ответов DNS-сервера клиенту. Когда должным образом настроено, устройство безопасности может изменить A-запись, чтобы позволить клиенту в таком сценарии, как обсуждено в "проблеме: Клиент не может получить доступ к серверу WWW. В этой ситуации, если исправление DNS включено, устройство безопасности перезаписывает A-запись, чтобы направить клиента на адрес 10.10.10.10 вместо 172.20.1.10. Когда вы добавляете ключевое слово **dns** к статической инструкции NAT (Версия 8.2 и ранее) или объектное/автоматическое Выражение NAT (Версия 8.3 и позже), исправление DNS включено.

Версия 8.2 и ранее

Это - окончательная конфигурация ASA для выполнения исправления DNS с ключевым словом **dns** и тремя интерфейсами NAT для версий 8.2 и ранее.

```
ciscoasa#show running-config
: Saved
:
ASA Version 8.2.x
!
hostname ciscoasa
enable password 9jNfZuG3TC5tCVH0 encrypted
names
dns-guard
!
interface Ethernet0/0
nameif outside
security-level 0
ip address 172.20.1.2 255.255.255.0
!
interface Ethernet0/1
nameif inside
security-level 100
ip address 192.168.100.1 255.255.255.0
```

```
!
interface Ethernet0/2
nameif dmz
security-level 50
ip address 10.10.10.1 255.255.255.0
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
access-list OUTSIDE extended permit tcp any host 172.20.1.10 eq www

pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
mtu dmz 1500
asdm image disk0:/asdm512-k8.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 192.168.100.0 255.255.255.0
static (inside,dmz) 192.168.100.0 192.168.100.0 netmask 255.255.255.0
static (dmz,outside) 172.20.1.10 10.10.10.10 netmask 255.255.255.255 dns

access-group OUTSIDE in interface outside

route outside 0.0.0.0 0.0.0.0 172.20.1.1 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
username cisco password ffIRPGpDSOJh9YLq encrypted
http server enable
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 MY_DNS_INSPECT_MAP
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
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
inspect dns MY_DNS_INSPECT_MAP
inspect icmp
policy-map type inspect dns migrated_dns_map_1
parameters
message-length maximum 512
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:d6637819c6ea981daf20d8c7aa8ca256
: end
```

Версия 8.3 и позже

```
ASA Version 9.x
!
hostname ciscoasa

!--- Output suppressed.

access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www

!--- Output suppressed.

object network obj-192.168.100.0
network 192.168.100.0 255.255.255.0
nat (inside,outside) dynamic interface

object network obj-10.10.10.10
host 10.10.10.10
nat (dmz,outside) static 172.20.1.10 dns

!--- Static translation to allow hosts on the outside access
!--- to the WWW server.

access-group OUTSIDE in interface outside

!--- Output suppressed.
```

Настройка посредством ASDM

Чтобы настроить исправление DNS в ASDM, выполните следующие действия:

1. Выберите **Configuration> NAT Rules** и выберите Объектное/Автоматическое правило, которое будет модифицироваться. **Нажмите Edit.**
2. **Нажмите кнопку Advanced...**
3. Проверьте **Преобразовывать ответы DNS для** флажка **правила**.
4. Нажмите **OK** для отъезда окна NAT Options.
5. Нажмите **OK** для отъезда окна Edit Object/Auto NAT Rule.
6. Нажмите **Apply** для передачи конфигурации к устройству безопасности.

Проверка

Вот захват пакета событий, когда исправление DNS включено:

1. Клиент отправляет запрос DNS.No. Time Source Destination Protocol Info
1 0.000000 **192.168.100.2 172.22.1.161 DNS Standard query A server.example.com**

Frame 1 (78 bytes on wire, 78 bytes captured)
Ethernet II, Src: Cisco_c8:e4:00 (00:04:c0:c8:e4:00), Dst: Cisco_9c:c6:1f (00:0a:b8:9c:c6:1f)
Internet Protocol, Src: 192.168.100.2 (192.168.100.2), Dst: 172.22.1.161 (172.22.1.161)
User Datagram Protocol, Src Port: 52985 (52985), Dst Port: domain (53)
Domain Name System (query)
[Response In: 2]
Transaction ID: 0x000c
Flags: 0x0100 (Standard query)
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
server.example.com: type A, class IN
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)

2. ASA выполняет PAT для DNS-запроса, и запрос пересылается. Заметьте, что исходный адрес пакета изменился на внешний интерфейс ASA.No. Time Source Destination Protocol Info
1 0.000000 **172.20.1.2** 172.22.1.161 DNS Standard query A server.example.com

Frame 1 (78 bytes on wire, 78 bytes captured)
Ethernet II, Src: Cisco_9c:c6:1e (00:0a:b8:9c:c6:1e), Dst: Cisco_01:f1:22 (00:30:94:01:f1:22)
Internet Protocol, Src: 172.20.1.2 (172.20.1.2), Dst: 172.22.1.161 (172.22.1.161)
User Datagram Protocol, Src Port: 1035 (1035), Dst Port: domain (53)
Domain Name System (query)
[Response In: 2]
Transaction ID: 0x000c
Flags: 0x0100 (Standard query)
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
server.example.com: type A, class IN
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)

3. DNS-сервер отвечает сопоставленным адресом сервера WWW.No. Time Source Destination Protocol Info
2 0.000992 **172.22.1.161 172.20.1.2 DNS Standard query response A 172.20.1.10**

Frame 2 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Cisco_01:f1:22 (00:30:94:01:f1:22), Dst: Cisco_9c:c6:1e (00:0a:b8:9c:c6:1e)
Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 172.20.1.2 (172.20.1.2)
User Datagram Protocol, Src Port: domain (53), Dst Port: 1035 (1035)
Domain Name System (response)
[Request In: 1]

```
[Time: 0.000992000 seconds]
Transaction ID: 0x000c
Flags: 0x8580 (Standard query response, No error)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
server.example.com: type A, class IN
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
Answers
server.example.com: type A, class IN, addr 172.20.1.10
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
Time to live: 1 hour
Data length: 4
Addr: 172.20.1.10
```

4. ASA отменяет преобразование адреса назначения ответа DNS и пересылает пакет клиенту. **Заметьте, что при включенном исправлении DNS запись Addr в ответе перезаписана реальным адресом сервера WWW.**

```
No.     Time        Source
Destination     Protocol Info
6 2.507191 172.22.1.161 192.168.100.2 DNS Standard query response
A 10.10.10.10

Frame 6 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Cisco_9c:c6:1f (00:0a:b8:9c:c6:1f), Dst: Cisco_c8:e4:00
(00:04:c0:c8:e4:00)
Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 192.168.100.2
(192.168.100.2)
User Datagram Protocol, Src Port: domain (53), Dst Port: 50752 (50752)
Domain Name System (response)
[Request In: 5]
[Time: 0.002182000 seconds]
Transaction ID: 0x0004
Flags: 0x8580 (Standard query response, No error)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
server.example.com: type A, class IN
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
Answers
server.example.com: type A, class IN, addr 10.10.10.10
Name: server.example.com
Type: A (Host address)
Class: IN (0x0001)
Time to live: 1 hour
Data length: 4
Addr: 10.10.10.10
```

5. На этом этапе клиент пытается обратиться к серверу WWW по адресу 10.10.10.10. Соединение устанавливается.

Окончательная конфигурация с ключевым словом "dns"

Это окончательная конфигурация ASA для выполнения исправления DNS с ключевым

словом dns и тремя интерфейсами NAT.

```
ciscoasa# sh running-config
: Saved
:
: Serial Number: JMX1425L48B
: Hardware:  ASA5510, 1024 MB RAM, CPU Pentium 4 Celeron 1600 MHz
:
ASA Version 9.1(5)4
!
hostname ciscoasa
enable password 9jNfZuG3TC5tCVH0 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
dns-guard
!
interface Ethernet0/0
 shutdown
 nameif outside
 security-level 0
 ip address 172.20.1.2 255.255.255.0
!
interface Ethernet0/1
 shutdown
 nameif inside
 security-level 100
 ip address 192.168.100.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 nameif dmz
 security-level 50
 ip address 10.10.10.1 255.255.255.0
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
 shutdown
 no nameif
 no security-level
 no ip address
!
ftp mode passive
object network obj-192.168.100.0
 subnet 192.168.100.0 255.255.255.0
object network obj-10.10.10.10
 host 10.10.10.10
access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www
pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm512-k8.bin
no asdm history enable
```

```
arp timeout 14400
no arp permit-nonconnected
!
object network obj-192.168.100.0
 nat (inside,outside) dynamic interface
object network obj-10.10.10.10
 nat (dmz,outside) static 172.20.1.10 dns
access-group OUTSIDE in interface outside
route outside 0.0.0.0 0.0.0.0 172.20.1.1 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
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 sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
http server enable
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
no ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
 anyconnect-essentials
username cisco password ffIRPGpDSOJh9YLq encrypted
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
 message-length maximum client auto
 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
 inspect ip-options
 inspect icmp
policy-map type inspect dns MY_DNS_INSPECT_MAP
```

```
 parameters
 message-length maximum 512
policy-map type inspect dns migrated_dns_map_1
 parameters
 message-length maximum 512
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:3a8e3009aa3db1d6dba143abf25ee408
: end
```

Альтернативное решение: NAT получателя

NAT получателя может стать альтернативным решением исправления DNS. Использование преобразования сетевых адресов назначения в этой ситуации требует, чтобы статический объект / автоматическое преобразование NAT был создан между общим адресом сервера WWW на внутреннем и действительном адресе на DMZ. NAT получателя не изменяет содержимое A-записи DNS, которая возвращается от DNS-сервера клиенту. **Вместо этого, при использовании NAT получателя, например в сценарии, рассматриваемом в этом документе, клиент может использовать для соединения с сервером WWW публичный IP-адрес 172.20.1.10, возвращенный DNS-сервером.** Статический объект / автоматическая трансляция позволяет устройству безопасности преобразовывать адрес назначения (DA) от **172.20.1.10** до **10.10.10.10**. Вот соответствующая часть конфигурации при использованиии NAT получателя:

```
ASA Version 9.x
!
hostname ciscoasa

!--- Output suppressed.

access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www

!--- Output suppressed.

object network obj-192.168.100.0
network 192.168.100.0 255.255.255.0
nat (inside,outside) dynamic interface

!--- The nat and global commands allow
!--- clients access to the Internet.

object network obj-10.10.10.10
host 10.10.10.10
nat (dmz,outside) static 172.20.1.10

!--- Static translation to allow hosts on the outside access
!--- to the WWW server.

object network obj-10.10.10.10-1
host 10.10.10.10
nat (dmz,inside) static 172.20.1.10
```

Преобразование сетевых адресов назначения, Достигнутое с Ручным/Дважды Выражением NAT

```
ASA Version 9.x
!
hostname ciscoasa
```

```
!--- Output suppressed.

access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www

!--- Output suppressed.

object network obj-192.168.100.0
network 192.168.100.0 255.255.255.0
nat (inside,outside) dynamic interface

object network obj-10.10.10.10
host 10.10.10.10

object network obj-172.20.1.10
host 172.20.1.10

nat (inside,dmz) source dynamic obj-192.168.100.0 interface
destination static obj-172.20.1.10 obj-10.10.10.10

!--- Static translation to allow hosts on the inside access
!--- to the WWW server via its outside address.

access-group OUTSIDE in interface outside

!--- Output suppressed.
```

Чтобы настроить NAT получателя в ASDM, выполните следующие действия:

1. Выберите **Configuration> NAT Rules** и выберите **Add> Add "Сетевой объект" Правило NAT....**
2. Введите данные конфигурации для нового статического преобразования. В Поле имени введите **obj-10.10.10.10**.В поле IP Address введите адрес IP-адреса сервера WWW.От выпадающего списка Типа выберите **Static**.В поле Translated Addr введите адрес и интерфейс, с которым вы хотите сопоставить сервер WWW.**Нажмите кнопку Advanced.**В выпадающем списке Исходного интерфейса выберите **dmz**.В выпадающем списке Интерфейса назначения выберите **внутри**.В этом случае внутренний интерфейс выбирается так, чтобы разрешить узлам на внутреннем интерфейсе обращаться к серверу WWW через сопоставленный адрес 172.20.1.10.Нажмите **OK** для отъезда окна Add Object/Auto NAT Rule.Нажмите **Apply** для передачи конфигурации к устройству безопасности.

Альтернативный метод с Руководством/Дважды NAT и ASDM

1. Выберите **Configuration> NAT Rules** и выберите **Add> правило Add Nat перед "Сетевым объектом" Правило NAT....**
2. Заполните конфигурацию для Ручной/Дважды трансляции NAT. В выпадающем списке Исходного интерфейса выберите **внутри**.В выпадающем списке Интерфейса назначения выберите **dmz**.В Поле исходного адреса введите объект (obj-192.168.100.0) внутренней сети.В Поле адреса точки назначения введите преобразованный объект (172.20.1.10) IP сервера DMZ.В Источнике выпадающий список Типа NAT выберите **Dynamic PAT (Hide)**.В Адресе источника [Действие: Преобразованный Пакетный раздел] поле, введите **dmz**.В Адресе назначения (DA) [Действие: Преобразованный Пакетный раздел] поле, введите реальный объект (obj-10.10.10.10) IP сервера DMZ.
3. Нажмите **OK** для отъезда окна Add Manual/Twice NAT Rule.
4. Нажмите **Apply** для передачи конфигурации к устройству безопасности.

Вот последовательность событий, которые происходят, когда настроен NAT получателя.

Предположим, что клиент уже запросил DNS-сервер и получил ответ в виде адреса 172.20.1.10 для сервера WWW:

1. Клиент пытается обратиться к серверу WWW по адресу 172.20.1.10.`%ASA-7-609001: Built local-host inside:192.168.100.2`
2. Устройство безопасности принимает запрос и определяет, что сервер WWW находится по адресу 10.10.10.10.`%ASA-7-609001: Built local-host dmz:10.10.10.10`
3. Устройство безопасности создает TCP-соединение между клиентом и сервером WWW. Обратите внимание на сопоставленные адреса узлов в скобках.`%ASA-6-302013: Built outbound TCP connection 67956 for dmz:10.10.10.10/80` **`(172.20.1.10/80)`** `to inside:192.168.100.2/11001` **`(192.168.100.2/11001)`**
4. **Команда show xlate на устройстве защиты проверяет, преобразуется ли клиентский трафик через устройство защиты.** В этом случае используется первое статическое преобразование.`ciscoasa#`**`show xlate`**
   `3 in use, 9 most used`
   `Global 192.168.100.0 Local 192.168.100.0`
   `Global 172.20.1.10 Local 10.10.10.10`
   `Global 172.20.1.10 Local 10.10.10.10`
5. **Команда show conn на устройстве безопасности проверяет, что соединение между клиентом и сервером WWW установлено через устройство безопасности.** Обратите внимание на реальный адрес сервера WWW в скобках.`ciscoasa#`**`show conn`**
   `TCP out 172.20.1.10`**`(10.10.10.10)`**`:80 in 192.168.100.2:11001`
   `idle 0:01:38 bytes 1486 flags UIO`

Окончательная конфигурация с NAT получателя

Это окончательная конфигурация ASA для выполнения исправления DNS с NAT получателя и тремя интерфейсами NAT.

```
ASA Version 9.x
!
hostname ciscoasa
enable password 9jNfZuG3TC5tCVH0 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
dns-guard
!
interface Ethernet0/0
 shutdown
 nameif outside
 security-level 0
 ip address 172.20.1.2 255.255.255.0
!
interface Ethernet0/1
 shutdown
 nameif inside
 security-level 100
 ip address 192.168.100.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 nameif dmz
 security-level 50
 ip address 10.10.10.1 255.255.255.0
!
interface Ethernet0/3
 shutdown
 no nameif
```

```
 no security-level
 no ip address
!
interface Management0/0
 management-only
 shutdown
 no nameif
 no security-level
 no ip address
!
ftp mode passive
object network obj-192.168.100.0
 subnet 192.168.100.0 255.255.255.0
object network obj-10.10.10.10
 host 10.10.10.10
object network obj-10.10.10.10-1
 host 10.10.10.10
object network obj-172.20.1.10
 host 172.20.1.10
access-list OUTSIDE extended permit tcp any host 10.10.10.10 eq www
pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm512-k8.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
!
object network obj-192.168.100.0
 nat (inside,outside) dynamic interface
object network obj-10.10.10.10
 nat (dmz,outside) static 172.20.1.10
object network obj-10.10.10.10-1
 nat (dmz,inside) static 172.20.1.10
access-group OUTSIDE in interface outside
route outside 0.0.0.0 0.0.0.0 172.20.1.1 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
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 sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
http server enable
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
no ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
```

```
no threat-detection statistics tcp-intercept
webvpn
 anyconnect-essentials
username cisco password ffIRPGpDSOJh9YLq encrypted
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
 message-length maximum client auto
 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
 inspect ip-options
 inspect icmp
policy-map type inspect dns MY_DNS_INSPECT_MAP
 parameters
 message-length maximum 512
policy-map type inspect dns migrated_dns_map_1
 parameters
 message-length maximum 512
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:2cdcc45bfc13f9e231f3934b558f1fd4
: end
```

Настройка

Чтобы включить проверку DNS (если она была отключена ранее), выполните следующие действия. **В этом примере проверка DNS добавляется в глобальную политику проверки по умолчанию, которая применяется глобально командой service-policy, как при начале работы ASA с конфигурацией по умолчанию.**

1. Создайте карту политик проверки для DNS.`ciscoasa(config)#`**`policy-map type inspect dns MY_DNS_INSPECT_MAP`**
2. От режима конфигурации карты политик перейдите в режим настройки параметров для определения параметров для инспекционного механизма.`ciscoasa(config-pmap)#`**`parameters`**
3. В режиме настройки параметров policy-map задайте максимальную длину сообщения для сообщений DNS, чтобы быть 512.`ciscoasa(config-pmap-p)#`**`message-length maximum 512`**
4. Выйдите из режима настройки параметров карты политик и из режима настройки карты политик.`ciscoasa(config-pmap-p)#`**`exit`**

```
ciscoasa(config-pmap)#exit
```

5. Подтвердите создание карты политик проверки.`ciscoasa(config)#show run policy-map type inspect dns`

```
!
policy-map type inspect dns MY_DNS_INSPECT_MAP
parameters
message-length maximum 512
!
```

6. Войдите в режим настройки карты политик для global_policy.`ciscoasa(config)#policy-map global_policy`

```
ciscoasa(config-pmap)#
```

7. В режиме настройки карты политик задайте карту класса уровней 3/4 по умолчанию, inspection_default.`ciscoasa(config-pmap)#class inspection_default`

```
ciscoasa(config-pmap-c)#
```

8. В режиме конфигурации класса policy-map используйте карту политики проверки, созданную в шагах 1-3, чтобы указать, что должен быть осмотрен DNS.`ciscoasa(config-pmap-c)#inspect dns MY_DNS_INSPECT_MAP`
9. Выйдите из режима настройки класса карты политик и из режима настройки карты политик.`ciscoasa(config-pmap-c)#exit`

```
ciscoasa(config-pmap)#exit
```

10. Убедитесь, что карта политик global_policy настроена как требуется.`ciscoasa(config)#show run policy-map`

```
!

!--- The configured DNS inspection policy map.

policy-map type inspect dns MY_DNS_INSPECT_MAP
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
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
inspect dns MY_DNS_INSPECT_MAP

!--- DNS application inspection enabled.
```

11. Убедитесь, что политика global_policy применяется глобально служебной политикой.`ciscoasa(config)#show run service-policy`

```
service-policy global_policy global
```

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

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

команд show.

Захват трафика DNS

Одним из методов проверки правильной перезаписи записей DNS устройством защиты является захват соответствующих пакетов, как рассматривалось в предыдущем примере. Для захвата трафика на ASA выполните следующие действия:

1. Создайте список доступа для каждого экземпляра захвата, который планируется создать. ACL должен задавать трафик, который планируется захватывать. В этом примере создаются два ACL. ACL для трафика на внешнем интерфейсе:
```
access-list DNSOUTCAP extended permit ip host 172.22.1.161 host
172.20.1.2

!--- All traffic between the DNS server and the ASA.

access-list DNSOUTCAP extended permit ip host 172.20.1.2 host
172.22.1.161

!--- All traffic between the ASA and the DNS server.
```
ACL для трафика на внутреннем интерфейсе:
```
access-list DNSINCAP extended permit ip host 192.168.100.2 host
172.22.1.161

!--- All traffic between the client and the DNS server.

access-list DNSINCAP extended permit ip host 172.22.1.161 host
192.168.100.2

!--- All traffic between the DNS server and the client.
```
2. Создайте экземпляры захвата:
```
ciscoasa#capture DNSOUTSIDE access-list DNSOUTCAP interface
outside

!--- This capture collects traffic on the outside interface that matches
!--- the ACL DNSOUTCAP.

ciscoasa# capture DNSINSIDE access-list DNSINCAP interface inside

!--- This capture collects traffic on the inside interface that matches
!--- the ACL DNSINCAP.
```
3. Просмотрите захваты.Вот как должны выглядеть примеры захватов после прохождения DNS-трафика:
```
ciscoasa#show capture DNSOUTSIDE
2 packets captured
1: 14:07:21.347195 172.20.1.2.1025 > 172.22.1.161.53: udp 36
2: 14:07:21.352093 172.22.1.161.53 > 172.20.1.2.1025: udp 93
2 packets shown
ciscoasa#show capture DNSINSIDE
2 packets captured
1: 14:07:21.346951 192.168.100.2.57225 > 172.22.1.161.53: udp 36
2: 14:07:21.352124 172.22.1.161.53 > 192.168.100.2.57225: udp 93
2 packets shown
```
4. (Необязательно) Скопируйте захваты на сервер TFTP в формате pcap для анализа в другом приложении.Приложения, которые могут анализировать формат pcap, могут показывать дополнительные данные, например имя и IP-адрес в A-записях DNS.
```
ciscoasa#copy /pcap capture:DNSINSIDE tftp
...
ciscoasa#copy /pcap capture:DNSOUTSIDE tftp
```

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Перезапись DNS не выполняется

Убедитесь, что на устройстве защиты настроена проверка DNS.

Создание преобразования не выполняется

Причиной невозможности создания соединения между клиентом и сервером WWW может быть неправильная конфигурация NAT. Проверьте журналы устройства защиты на предмет сообщений, показывающих, что протокол не может создать преобразование через устройство защиты. При наличии таких сообщений убедитесь, что NAT настроен на требуемый трафик и все адреса правильные.

```
%ASA-3-305006: portmap translation creation failed for tcp src
inside:192.168.100.2/11000 dst inside:192.168.100.10/80
```

Очистите записи xlate, и затем удалите и повторно примените Выражения NAT для решения этой ошибки.

Дополнительные сведения

- Cisco ASA 5500-x руководство по конфигурации
- Cisco ASA 5500-x Справочники по командам серии
- Уведомления о дефекте для специалистов по продуктам безопасности
- Запрос на комментарии (RFC)
- Cisco Systems – техническая поддержка и документация