PIX/ASA: Выполните Врачевание DNS со статической Командой и Тремя Примерами Конфигурации Интерфейсов NAT

Содержание

Введение

Этот документ обеспечивает типовую конфигурацию для выполнения врачевания Системы доменных имен (DNS) на ряду ASA 5500 Адаптивный прибор PIX 500 безопасности Прибора или Ряда безопасности, который использует статические заявления Сетевого перевода адреса (NAT). Врачевание DNS позволяет прибору безопасности переписывать A-отчеты DNS.

DNS переписывают, выполняет две функции:

- Переводит общественный адрес (routable, или нанесенный на карту адрес) в DNS отвечают на частный адрес (реальный адрес), когда клиент DNS находится в частном интерфейсе.
- Когда клиент DNS находится в общественном интерфейсе, переводит частное обращение к общественному адресу.

Примечание: конфигурация в этом документе содержит три интерфейса NAT: внутри, снаружи, и dmz. Для примера врачевания DNS со статикой и двумя интерфейсами NAT, обратитесь к PIX/ASA: Как Выполнить Врачевание DNS Со статической Командой и Двумя Примерами Конфигурации Интерфейсов NAT.

Обратитесь к PIX/ASA 7.x NAT и Заявления PAT и Используя туземный, глобальное, статическое, трубопровод и список доступа Команды и Переназначение Порта (Отправление) на PIX для получения дополнительной информации о том, как использовать NAT на Приборе безопасности PIX/ASA.

Обратитесь к Использованию туземного, глобального, статичного, трубопровод и список доступа Команды и Переназначение Порта (Отправление) на PIX для получения дополнительной информации о **туземном**, **глобальном**, **статическом**, **трубопроводе**, и командах **списка доступа** и переназначении порта (Отправление) на PIX.

Предпосылки

Требования

- Контроль DNS должен быть позволен для выполнения врачевания DNS на приборе безопасности. Контроль DNS идет по умолчанию. Однако, если это было выключено, посмотрите Формирование секции Контроля DNS позже в этом документе, чтобы повторно позволить его. Когда контроль DNS позволен, прибор безопасности выполняет эти задачи:

- Переводит отчет DNS, основанный на конфигурации, законченной с помощью **статических** и **туземных** команд (DNS переписывают). Перевод только относится к A-отчету в ответе DNS. Поэтому, полностью измените поиски, которые просят отчет PTR, не затронуты DNS, переписывают.

  Примечание: DNS переписывают, не совместимо со статическим Переводом адреса порта (PAT), потому что многократные правила PAT применимы для каждого A-отчета, и правило PAT использовать неоднозначно.

- Проводит в жизнь максимальную длину сообщения DNS (неплатеж составляет 512 байтов, и максимальная длина составляет 65535 байтов). Повторная сборка выполнена по мере необходимости, чтобы проверить, что длина пакета является меньше, чем максимальная формируемая длина. Пакет уронен, если он превышает максимальную длину.

  Примечание: при издании **осматривания dns** команда без выбора максимальной длины размер пакета DNS не проверен.

- Проводит в жизнь длину доменного имени 255 байтов и длину этикетки 63 байтов.
- Если с указателями сжатия сталкиваются в сообщении DNS, проверяет целостность доменного имени, упомянутого указателем.
- Проверки, чтобы видеть, существует ли петля указателя сжатия.

- Дополнительный: выпуск 5.2.1 Адаптивного диспетчера устройств безопасности (ASDM) Cisco или позже

Примечание: Обратитесь к Разрешению Доступа HTTPS для ASDM, чтобы позволить ASA формироваться ASDM.

Используемые компоненты

Информация в этом документе основана на Серийном приборе ASA 5500 безопасности, версии 7.2 (1).

Информация в этом документе была создана из устройств в определенной окружающей среде лаборатории. Все устройства, используемые в этом документе, начали с очищенного (неплатеж) конфигурацию. Если ваша сеть жива, удостоверьтесь, что вы понимаете потенциальное воздействие любой команды.

Связанные продукты

Эта конфигурация может также использоваться с Cisco PIX 500 Серийный Прибор безопасности, версия 6.2 или позже.

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

Соглашения

Направьте в Cisco Технические Соглашения Подсказок для получения дополнительной информации о соглашениях документа.

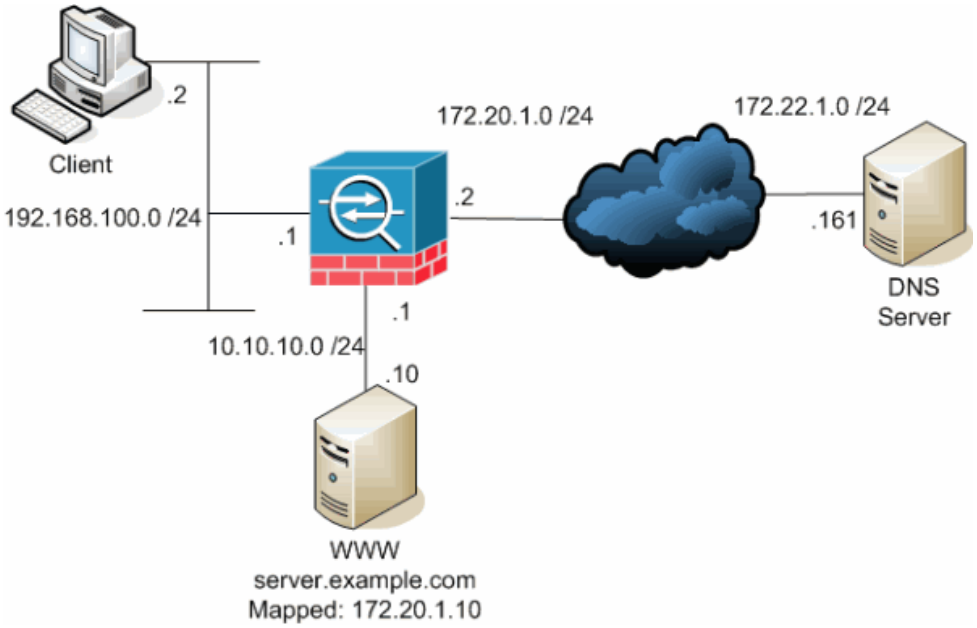
Справочная информация

В типичном обмене DNS клиент посылает URL или hostname к серверу DNS для определения IP-адреса того хозяина. Сервер DNS получает запрос, ищет отображение name-to-IP-address для того хозяина, и затем предоставляет A-отчету IP-адрес клиенту. В то время как эта процедура работает хорошо во многих ситуациях, проблемы могут произойти. Эти проблемы могут произойти, когда клиент и хозяин, которого клиент пытается достигнуть, находятся оба на той же самой частной сети позади NAT, но сервер DNS, используемый клиентом, находится на другой общедоступной сети.

Сценарий: Три Интерфейса NAT (внутри, снаружи, dmz)

Топология

В этом сценарии клиент расположен во внутреннем интерфейсе ASA. WWW-сервер, которого клиент пытается достигнуть, расположен в dmz интерфейсе ASA. Динамический PAT формируется для разрешения доступа клиента к Интернету. Статический NAT со списком доступа формируется, чтобы позволить доступ сервера к Интернету, а также позволить интернет-хозяевам получать доступ к WWW-серверу.



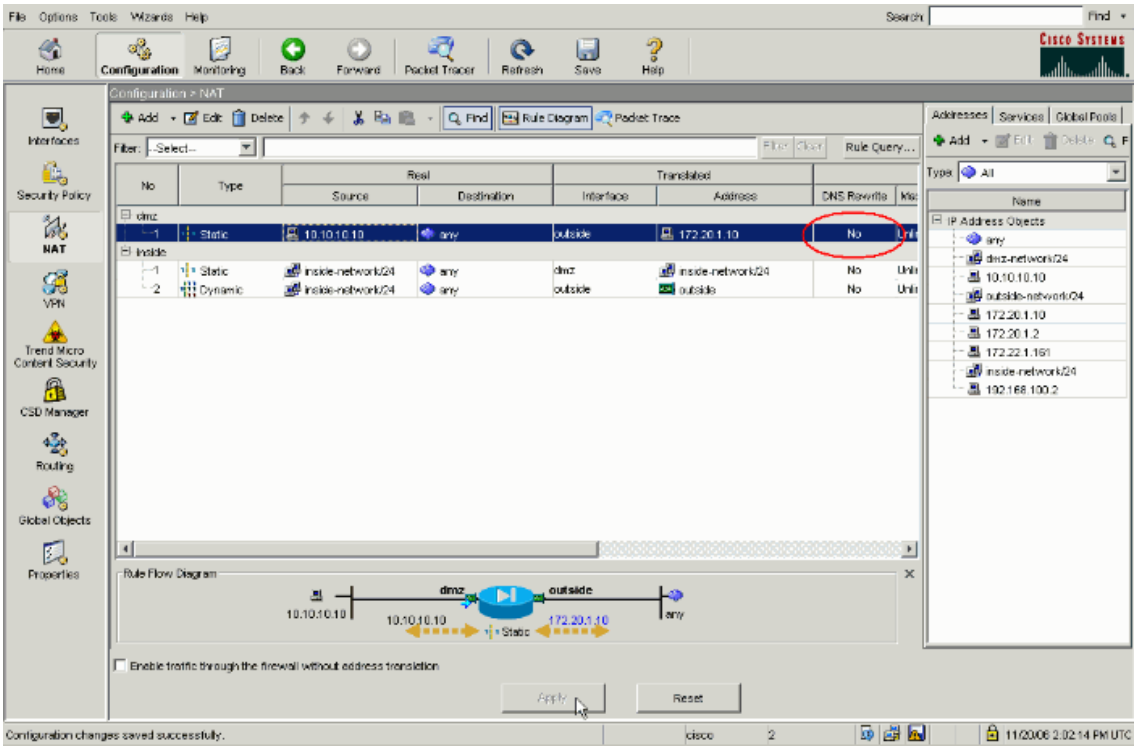
Эта диаграмма является примером этой ситуации. В этом случае клиент в 192.168.100.2 хочет использовать **server.example.com** URL для доступа к WWW-серверу в 10.10.10.10. Услуги DNS для клиента предоставлены внешним сервером DNS в 172.22.1.161. Поскольку сервер DNS расположен на другой общедоступной сети, он не знает частный IP-адрес WWW-сервера. Вместо этого это знает, что WWW-сервер нанес на карту адрес 172.20.1.10. Таким образом сервер DNS содержит отображение IP-address-to-name **server.example.com** к **172.20.1.10**.

Проблема: клиент не может получить доступ к WWW-серверу

Без врачевания DNS или другого решения, позволенного в этой ситуации, если клиент отправляет запрос DNS для IP-адреса **server.example.com**, это неспособно получить доступ к WWW-серверу. Это вызвано тем, что клиент получает A-отчет, который содержит нанесенный на карту общественный адрес 172.20.1.10 для WWW-сервера. Когда клиент пытается получить доступ к этому IP-адресу, прибор безопасности уронил пакеты, потому что это не позволяет переназначение пакета в том же самом интерфейсе. Вот то, на что похожа часть NAT конфигурации, когда не позволено врачевание DNS:

```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa

!--- Output suppressed.

access-list OUTSIDE extended permit tcp any host 172.20.1.10 eq www

!--- Output suppressed.

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 translation to allow hosts on the inside access to
!--- hosts on the dmz.

static (dmz,outside) 172.20.1.10 10.10.10.10 netmask 255.255.255.255

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

access-group OUTSIDE in interface outside

!--- Output suppressed.
```

Это - то, на что конфигурация похожа в ASDM, когда не позволено врачевание DNS:



Когда врачевание DNS не позволено, вот захват пакета событий:

1. Клиент посылает вопрос 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. PAT выполнен на вопросе DNS ASA, и вопрос отправлен. Обратите внимание на то, что адрес источника 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. Сервер DNS отвечает с нанесенным на карту адресом WWW-сервера.

```
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 перевод адреса получателя ответа DNS и вперед пакета клиенту. Обратите внимание на то, что без врачевания DNS позволил, **Addr** в ответе является все еще нанесенным на карту адресом WWW-сервера.

```
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. В этом пункте клиент пытается получить доступ к WWW-серверу в 172.20.1.10. ASA создает вход связи для этой коммуникации. Однако, потому что это не позволяет движению течь изнутри к внешней стороне к dmz, времена связи. Регистрации ASA показывают это:

```
%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"

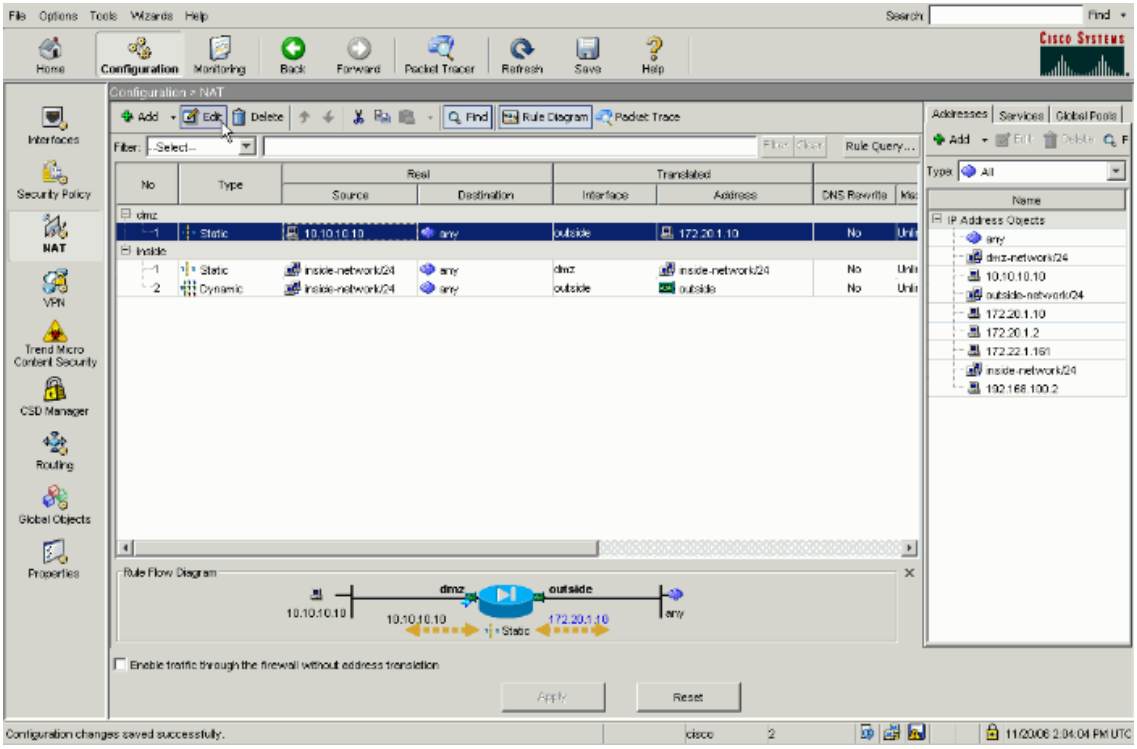
Врачевание DNS с "dns" ключевым словом

Врачевание DNS с **dns** ключевым словом дает прибору безопасности способность перехватить и переписать содержание ответов сервера DNS клиенту. Когда должным образом формируется, прибор безопасности может изменить A-отчет, чтобы позволить клиенту в таком сценарии, как обсуждено в проблеме: Клиент не Может Получить доступ к секции WWW-сервера для соединения. В этой ситуации, с позволенным врачеванием DNS, прибор безопасности переписывает A-отчет для направления клиента к 10.10.10.10, вместо 172.20.1.10. Когда вы добавляете **dns** ключевое слово к статическому заявлению NAT, врачевание DNS позволено. Вот то, на что похожа часть NAT конфигурации, когда позволено врачевание DNS:

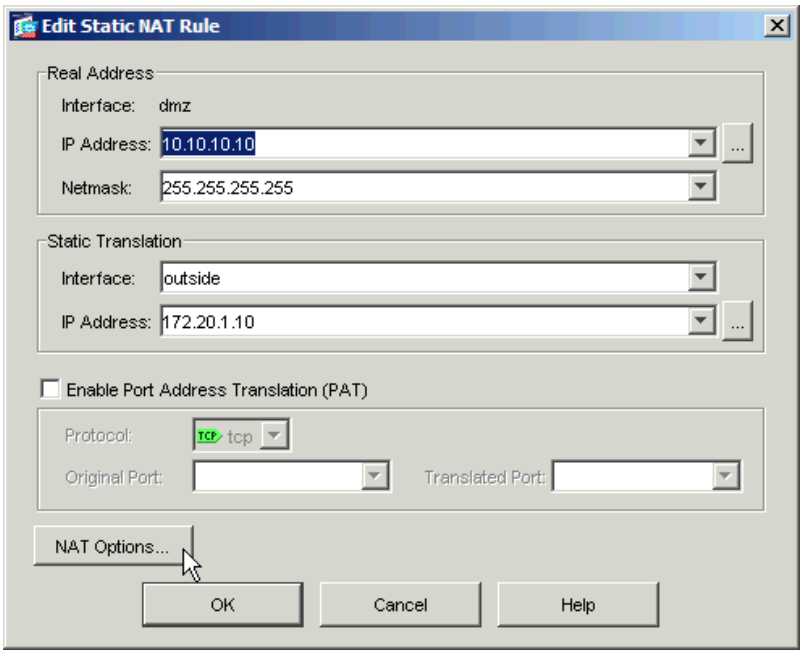
```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa

!--- Output suppressed.

access-list OUTSIDE extended permit tcp any host 172.20.1.10 eq www

!--- Output suppressed.

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 translation to allow hosts on the inside access to
!--- hosts on the dmz.

static (dmz,outside) 172.20.1.10 10.10.10.10 netmask 255.255.255.255 dns

!--- The "dns" keyword is added to instruct the security appliance
!--- to modify DNS records related to this entry.

access-group OUTSIDE in interface outside

!--- Output suppressed.
```

Закончите эти шаги для формирования врачевания DNS в ASDM:

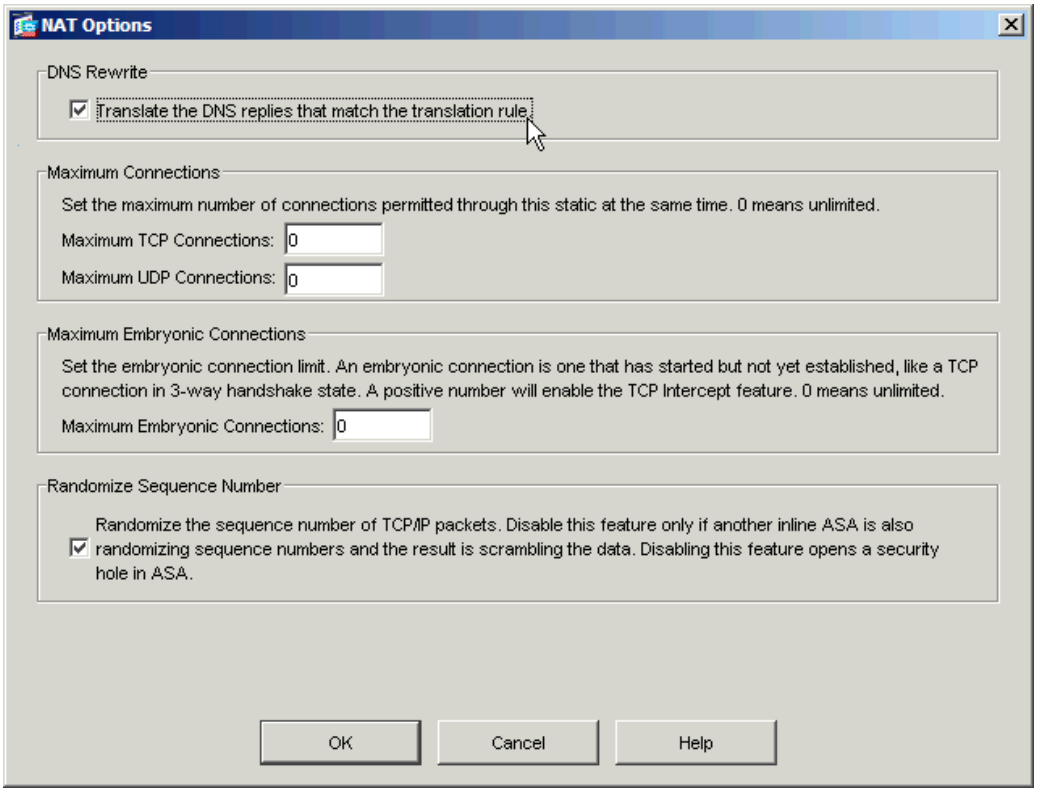
1. Проведите к **Конфигурации> NAT** и выберите статическое правило NAT, которое будет изменено. Нажмите **Edit**.



2. Нажмите **NAT Options....**



3. Проверьте**, что Переведение DNS отвечает, что соответствуют** флажку **правила перевода**.



4. **Нажмите OK** для отъезда окна Вариантов NAT. **Нажмите OK** для отъезда Редактировать Статическое окно Правила NAT. Нажмите **Apply** для отправки конфигурации в прибор безопасности.

Когда врачевание DNS позволено, вот захват пакета событий:

1. Клиент посылает вопрос 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. PAT выполнен на вопросе DNS ASA, и вопрос отправлен. Обратите внимание на то, что адрес источника 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. Сервер DNS отвечает с нанесенным на карту адресом WWW-сервера.

```
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 перевод адреса получателя ответа DNS и вперед пакета клиенту. Обратите внимание на то, что с позволенным врачеванием DNS, **Addr** в ответе переписан, чтобы быть реальным адресом WWW-сервера.

```
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. В этом пункте клиент пытается получить доступ к WWW-серверу в 10.10.10.10. Связь преуспевает.

Заключительная конфигурация с "dns" ключевым словом

Это - заключительная конфигурация ASA для выполнения врачевания DNS с **dns** ключевым словом и тремя интерфейсами NAT.

Заключительный ASA 7.2 (1) конфигурация

```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 7.2(1)
!
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

!--- Simple access-list that permits HTTP access to the mapped
!--- address of the WWW server.

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

!--- PAT and static NAT configuration. The DNS keyword instructs
!--- the security appliance to rewrite DNS records related to this entry.

access-group OUTSIDE in interface outside

!--- The Access Control List (ACL) that permits HTTP access to the
!--- WWW server is applied to the outside interface.

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

!--- DNS inspection is enabled using the configured 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
```

Альтернативное решение: место назначения NAT

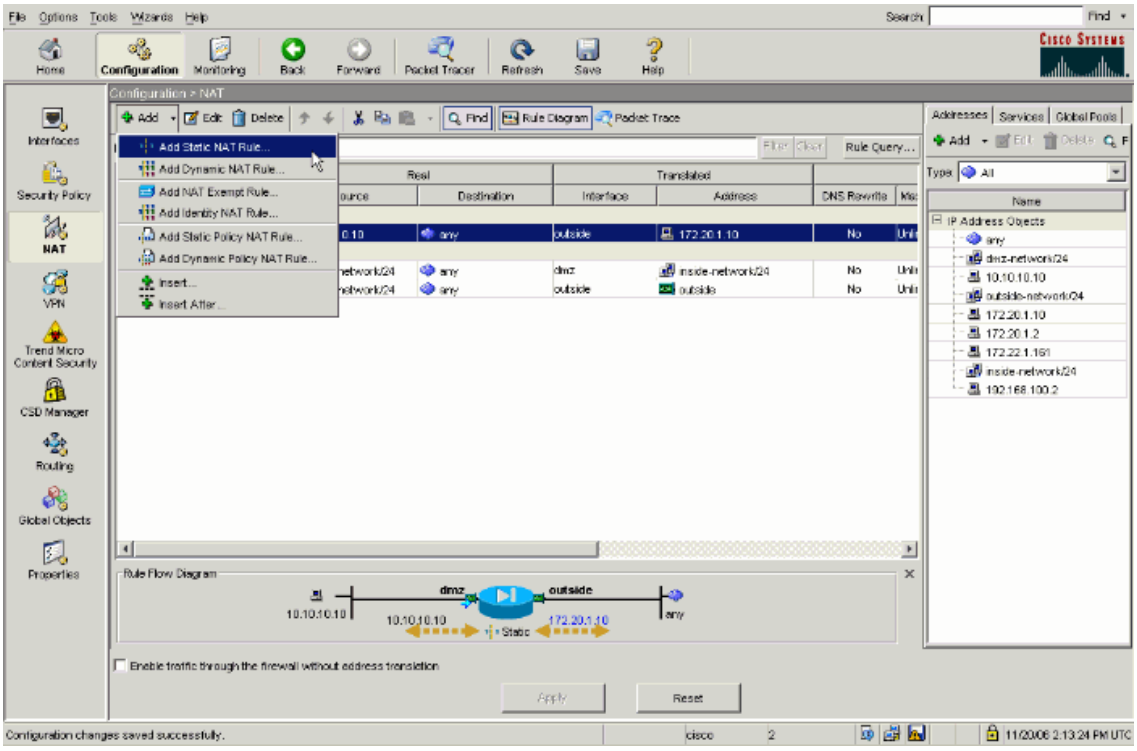
Место назначения NAT может обеспечить альтернативу врачеванию DNS. Использование места назначения, NAT в этой ситуации требует, чтобы статический перевод NAT был создан между общественным адресом WWW-сервера на внутреннем и реальном адресе на dmz. NAT назначения не изменяет содержание A-отчета DNS, который возвращен от сервера DNS до клиента. Вместо этого когда вы используете место назначения NAT в сценарии такой, как обсуждено в этом документе, клиент может использовать общественный IP-адрес **172.20.1.10**, который возвращен сервером DNS для соединения с WWW-сервером. Статический перевод позволяет прибору безопасности переводить адрес получателя от **172.20.1.10** до **10.10.10.10**. Когда место назначения NAT используется, вот соответствующая часть конфигурации:

```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 7.2(1)
```

```
!
hostname ciscoasa

!--- Output suppressed.

access-list OUTSIDE extended permit tcp any host 172.20.1.10 eq www

!--- Output suppressed.

global (outside) 1 interface
nat (inside) 1 192.168.100.0 255.255.255.0

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

static (inside,dmz) 192.168.100.0 192.168.100.0 netmask 255.255.255.0

!--- Static translation to allow hosts on the inside access to
!--- hosts on the dmz.

static (dmz,outside) 172.20.1.10 10.10.10.10 netmask 255.255.255.255

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

static (dmz,inside) 172.20.1.10 10.10.10.10 netmask 255.255.255.255

!--- 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.
```

Закончите эти шаги для формирования места назначения NAT в ASDM:

1. Проведите к **Конфигурации> NAT** и выберите**, Добавляют>, Добавляет Статическое Правило NAT....**

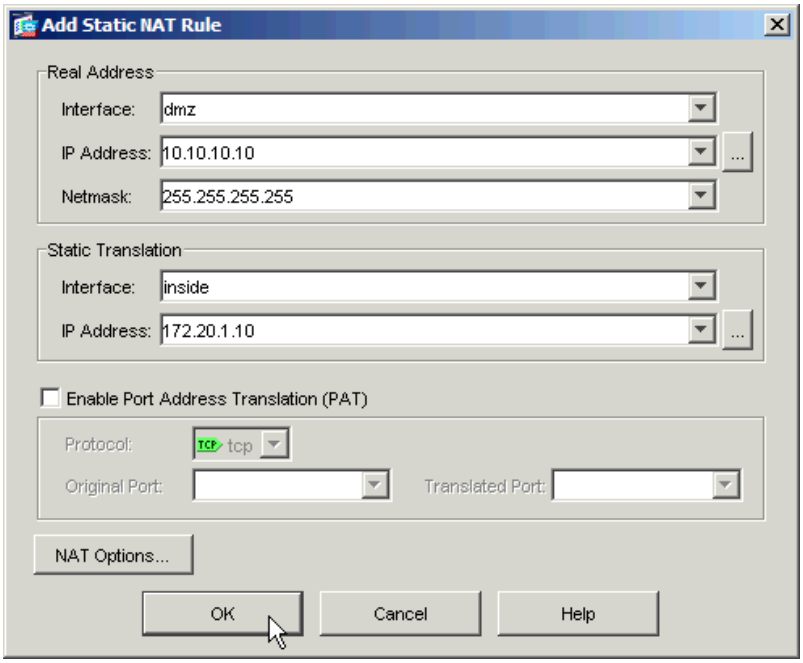


2. Заполните конфигурацию для нового статического перевода.

   a. Населите **Реальную** область **Адреса** с информацией о WWW-сервере.

   b. Населите **Статическую** область **Перевода** с адресом и интерфейсом, к которому вы хотите нанести на карту WWW-сервер.

В этом случае внутренний интерфейс выбран, чтобы позволить хозяевам во внутреннем интерфейсе получать доступ к WWW-серверу через нанесенный на карту адрес 172.20.1.10.



3. **Нажмите OK** для отъезда Добавления Статического окна Правила NAT.

4. Нажмите **Apply** для отправки конфигурации в прибор безопасности.

Вот последовательность событий, которые имеют место, когда формируется место назначения NAT. Предположите, что клиент уже подверг сомнению сервер DNS и получил ответ **172.20.1.10** для адреса WWW-сервера:

1. Клиент пытается связаться с WWW-сервером в 172.20.1.10.

```
%ASA-7-609001: Built local-host inside:192.168.100.2
```

2. Прибор безопасности видит запрос и признает, что WWW-сервер 10.10.10.10.

```
%ASA-7-609001: Built local-host dmz:10.10.10.10
```

3. Прибор безопасности создает связь TCP между клиентом и WWW-сервером. Отметьте нанесенные на карту адреса каждого хозяина в круглых 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. **Шоу xlate** команда на приборе безопасности проверяет, что движение клиента переводит через прибор безопасности. В этом случае первый статический перевод используется.

```
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. **Шоу ведет** команду на приборе безопасности, проверяет, что связь преуспела между клиентом и WWW-сервером через прибор безопасности. Отметьте реальный адрес WWW-сервера в круглых 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
```

Заключительная конфигурация с местом назначения NAT

Это - заключительная конфигурация ASA для выполнения врачевания DNS с местом назначения NAT и три интерфейса NAT.

Заключительный ASA 7.2 (1) конфигурация

```
ciscoasa#show running-config
: Saved
:
ASA Version 7.2(1)
!
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

!--- Simple access-list that permits HTTP access to the mapped
!--- address of the WWW server.

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

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

static (inside,dmz) 192.168.100.0 192.168.100.0 netmask 255.255.255.0

!--- Static translation to allow hosts on the inside access to
!--- hosts on the dmz.

static (dmz,outside) 172.20.1.10 10.10.10.10 netmask 255.255.255.255

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

static (dmz,inside) 172.20.1.10 10.10.10.10 netmask 255.255.255.255

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

access-group OUTSIDE in interface outside

!--- The ACL that permits HTTP access to the WWW server is applied
!--- to the outside interface.

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
```

Формируйте контроль DNS

Закончите эти шаги для предоставления возможности контроля DNS (если он был ранее отключен). В этом примере контроль DNS добавлен к неплатежу глобальная инспекционная политика, которая применена глобально командой **обслуживания**, как будто ASA начался с конфигурации по умолчанию. Обратитесь к Использованию Модульной стратегической Структуры для получения дополнительной информации об обслуживаниях и контроле.

1. Создайте инспекционную стратегическую карту для DNS.

```
ciscoasa(config)#policy-map type inspect dns MY_DNS_INSPECT_MAP
```

2. От способа конфигурации стратегической карты войдите в способ конфигурации параметра для определения параметров для инспекционного двигателя.

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

3. В способе конфигурации параметра стратегической карты определите maxiumum длину сообщения для сообщений DNS, чтобы быть 512.

```
ciscoasa(config-pmap-p)#message-length maximum 512
```

4. Выход из способа конфигурации параметра стратегической карты и способа конфигурации стратегической карты.

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

5. Подтвердите, что инспекционная стратегическая карта была создана, как желаемый.

```
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 способ конфигурации стратегической карты для **global_policy**.

```
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#
```

7. В способе конфигурации стратегической карты определите слой по умолчанию 3/4 карта класса, **inspection_default**.

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

8. В способе конфигурации класса стратегической карты определите, что DNS должен быть осмотрен с помощью инспекционной стратегической карты, созданной в шагах 1-3.

```
ciscoasa(config-pmap-c)#inspect dns MY_DNS_INSPECT_MAP
```

9. Выход из способа конфигурации класса стратегической карты и способа конфигурации стратегической карты.

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

10. Проверьте, что **global_policy** стратегическая карта формируется, как желаемый.

```
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. Проверьте, что global_policy применен глобально обслуживанием.

```
ciscoasa(config)#show run service-policy
service-policy global_policy global
```

Проверить

Используйте эту секцию, чтобы подтвердить, что ваша конфигурация работает должным образом.

Переводчик Продукции Тул (только зарегистрированные клиенты) (OIT) поддерживает определенные **выставочные** команды. Используйте OIT для просмотра анализа **выставочной** продукции команды.

Захватите движение DNS

Один метод, чтобы проверить, что прибор безопасности переписывает отчеты DNS правильно, должен захватить рассматриваемые пакеты, как обсуждено в предыдущем примере. Закончите эти шаги для завоевания движения на ASA:

1. Создайте список доступа для каждого случая захвата, который вы хотите создать.

   ACL должен определить движение, которое вы хотите захватить. В этом примере были созданы два ACLs.

   - ACL для движения во 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 движения во 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 случай (и) 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. Рассмотрите захват (ы).

   Вот то, на что похожи захваты в качестве примера после того, как было передано некоторое движение DNS:

```
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. (Дополнительная) Копия захват (ы) к серверу TFTP в pcap форматирует для анализа в другом применении.

   Заявления, которые могут разобрать формат pcap, могут показать дополнительные детали, такие как имя и IP-адрес в DNS отчеты.

```
ciscoasa#copy /pcap capture:DNSINSIDE tftp
...
ciscoasa#copy /pcap capture:DNSOUTSIDE tftp
```

Расследовать

Эта секция предоставляет информацию, которую можно использовать для поиска неисправностей конфигурации.

DNS переписывают, не выполнен

Удостоверьтесь, что у вас есть контроль DNS, формируемый на приборе безопасности. Посмотрите Формирование секции Контроля DNS.

Неудавшееся создание перевода

Если связь не может быть создана между клиентом и WWW-сервером, это могло бы произойти из-за неверной конфигурации NAT. Проверьте регистрации прибора безопасности на сообщения, которые указывают, что протокол не создал перевод через прибор безопасности. Если такие сообщения появляются, проверяют, что NAT формировался для желаемого движения и что никакие адреса не являются неправильными.

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

Очистите xlate записи, и затем удалите и повторно используйте заявления NAT для решения этой ошибки.

Соответствующая информация

- **Запрос о комментариях (RFCs)**
- **Примеры конфигурации и технические примечания**

Дата генерации PDF файла: 26 декабря 2014

http://www.cisco.com/cisco/web/support/RU/104/1041/1041927_dns-doctoring-3zones.html