PIX/ASA: Пример исправления DNS с помощью статической команды и двух интерфейсов NAT

Содержание

Введение

В этом документе приведен пример конфигурации для исправления системы доменных имен (DNS) на устройстве адаптивной безопасности серии ASA 5500 или устройстве безопасности серии PIX 500 с помощью утверждений статической таблицы преобразования сетевых адресов (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.

Примечание: Конфигурация в этом документе содержит два интерфейса NAT; внутри и снаружи. Пример исправления DNS со статикой и тремя интерфейсами NAT (внутренним, внешним и dmz) см. в разделе PIX/ASA: Пример исправления DNS с помощью статической команды и трех интерфейсов NAT.

Дополнительные сведения об использовании NAT на устройстве безопасности см. в разделах Утверждения PIX/ASA 7.x NAT и PAT и Использование команд nat, global, static, conduit и access-list, а также перенаправление портов (пересылка) на PIX.

Предварительные условия

Требования

Чтобы выполнить исправление DNS, на устройстве защиты должна быть включена проверка DNS. Проверка DNS по умолчанию включена. Если она была отключена, обратитесь к параграфу Настройка проверки DNS далее в этом разделе, чтобы снова включить ее. Когда проверка DNS включена, устройство защиты выполняет следующие задачи:

- **Преобразует запись DNS на основании конфигурации, выполненной с помощью команд static и nat (перезапись DNS).** Преобразование применяется только к A-записи в отклике DNS. Поэтому обратные поиски, запрашивающие запись PTR, не затрагиваются перезаписью DNS.**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). Сборка выполняется при необходимости проверить, что длина пакета меньше, чем заданная максимальная длина. Пакет сбрасывается, если его длина превышает максимальную.**Примечание:** При запуске **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, содержащиеся в данном документе, относятся к устройству безопасности серии ASA 5500, версия 7.2(1).

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 также может быть использована с устройством безопасности серии Cisco

PIX 500 версии 6.2 или более поздней.

Примечание: Cisco Adaptive Security Device Manager (ASDM) конфигурация применим к версии 7.x только.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

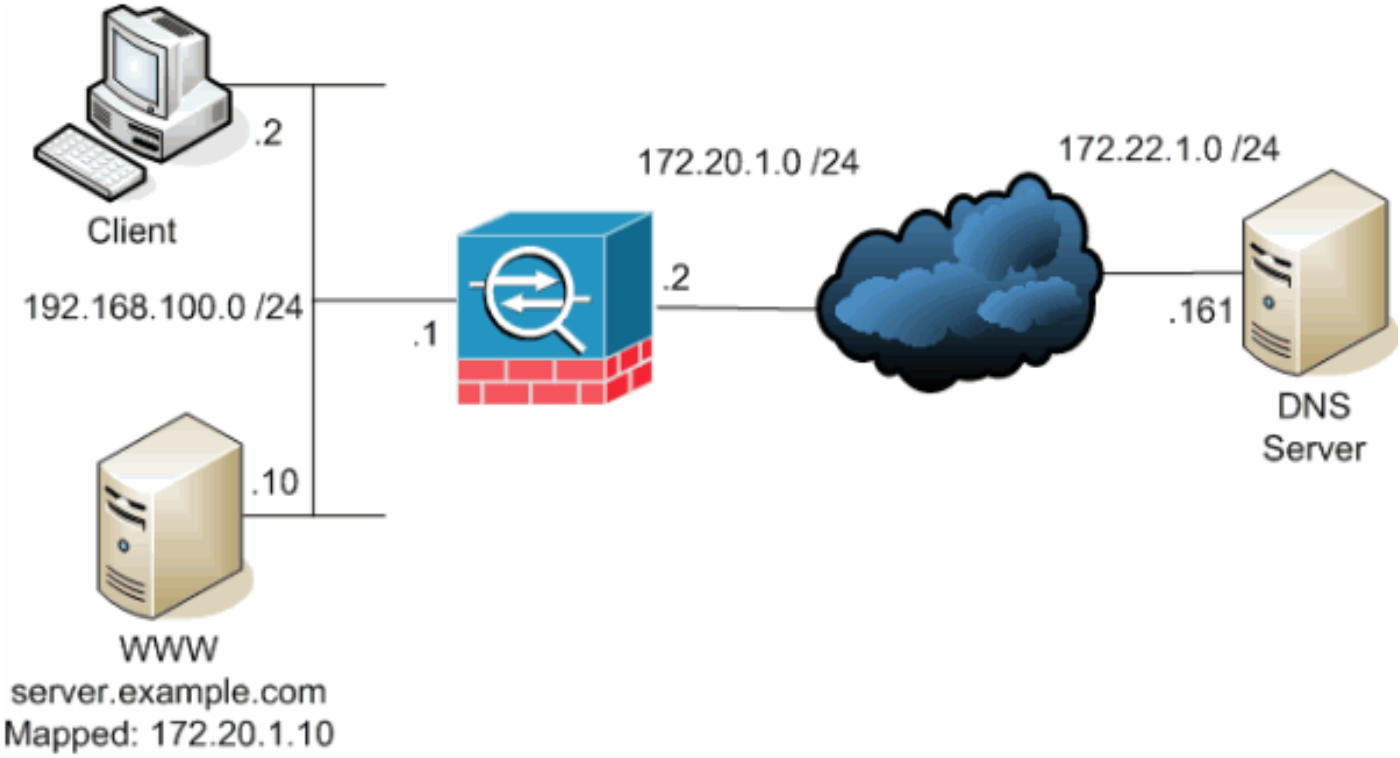
Общие сведения

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: Два интерфейса NAT (внутренний, внешний)

Топология

В этом сценарии клиент и сервер WWW, который клиент пытается достичь, находятся на внутреннем интерфейсе ASA. Динамический PAT настроен на разрешение клиенту доступа в Интернет. Статический NAT со списком доступа настроен на разрешение серверу доступа в Интернет, а также на разрешение узлам Интернета доступа к серверу WWW.



Эта схема является примером данной ситуации. **В этом случае клиент с адресом**

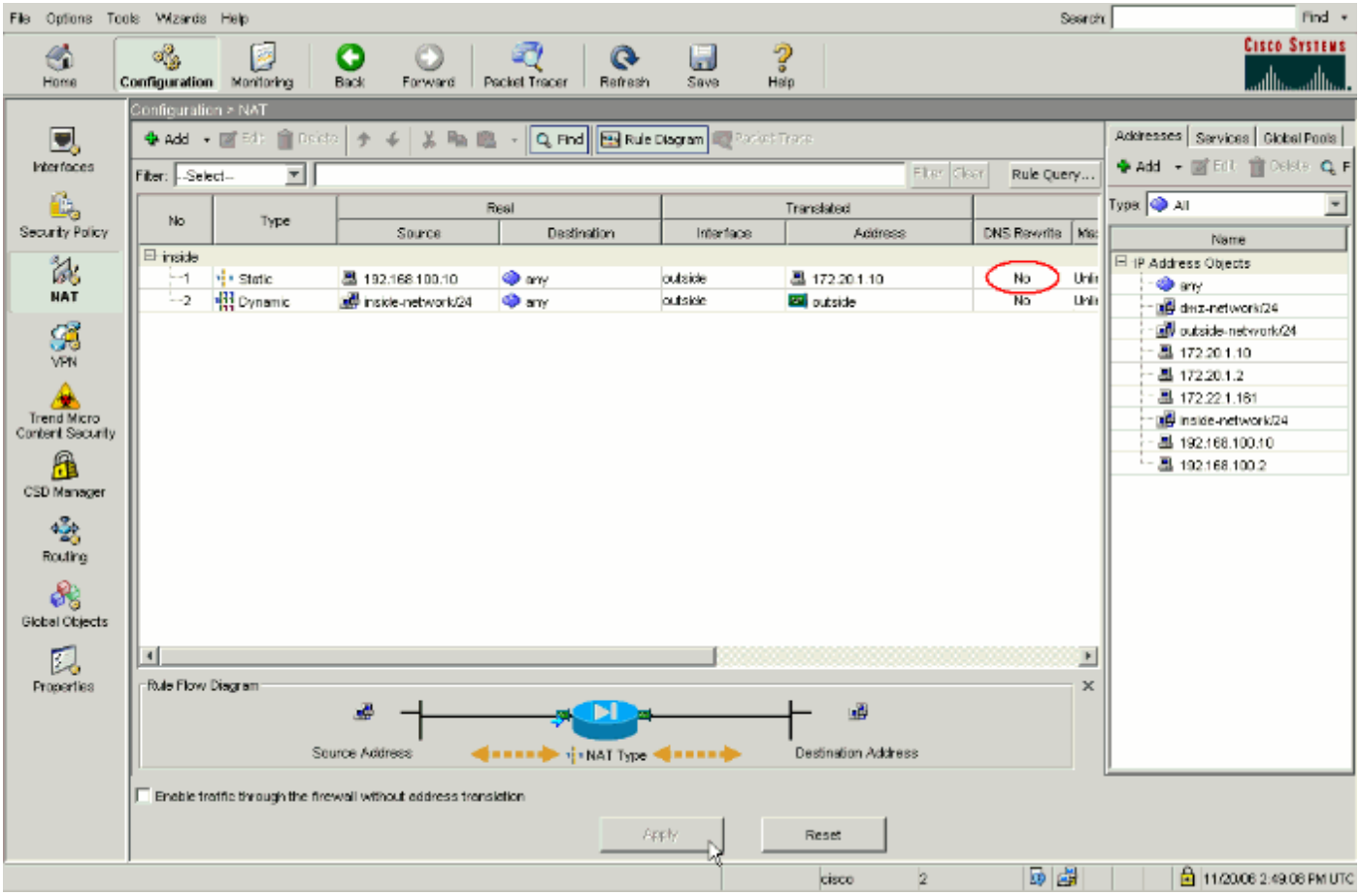
192.168.100.2 пытается использовать URL server.example.com для доступа к серверу WWW по адресу 192.168.100.10. Сервисы DNS для клиента предоставлены внешним DNS-сервером по адресу 172.22.1.161. Так как DNS-сервер расположен в другой общедоступной сети, ему неизвестен частный IP-адрес сервера WWW. Вместо 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 получить доступ 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: 172.20.1.10 сервера WWW. 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:

```
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,outside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255 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 обратно, 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"

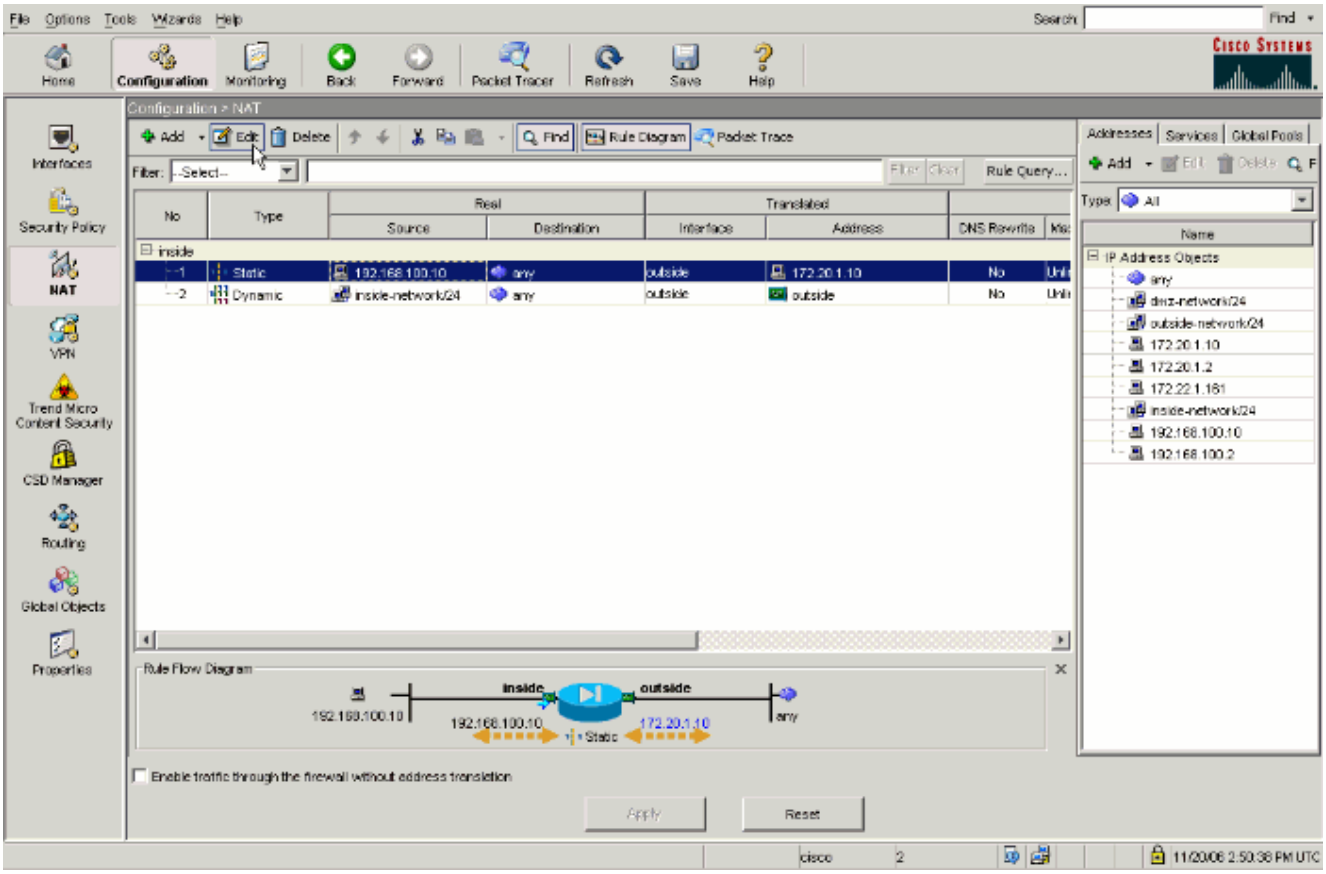
Исправление DNS с помощью ключевого слова "dns"

Исправление DNS с помощью ключевого слова dns дает устройству защиты возможность перехватывать и перезаписывать содержимое ответов DNS-сервера клиенту. [При правильной настройке устройство защиты может изменить A-запись, чтобы разрешить клиенту подключение в сценарии, который рассматривался в разделе Проблема: 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 192.168.100.10 вместо 172.20.1.10. Исправление DNS включается, если добавить ключевое слово dns в утверждение NAT static.** Вот как выглядит область NAT в конфигурации, когда исправление DNS включено:

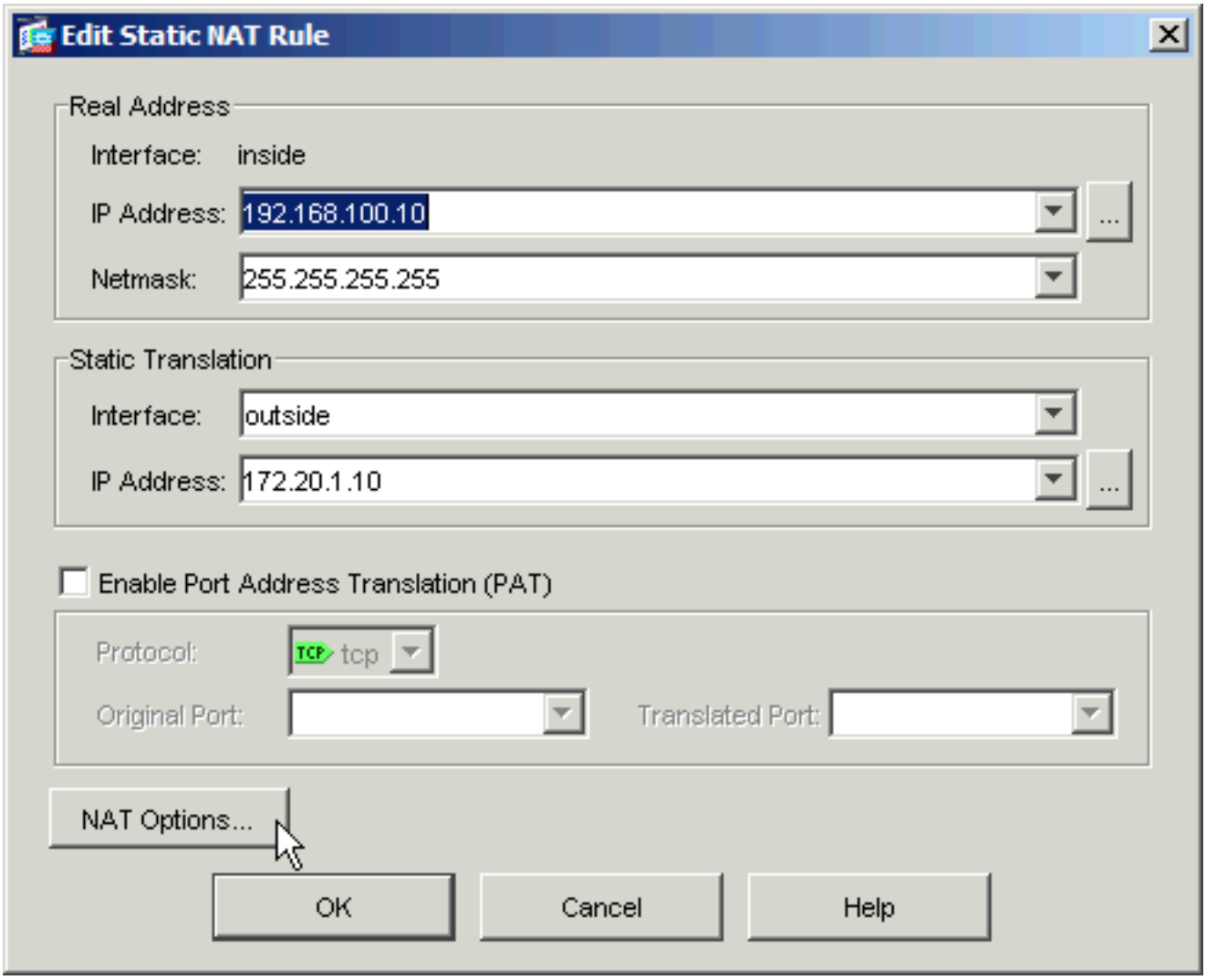
```
ciscoasa(config)#show run : Saved : ASA Version 7.2(1) ! hostname ciscoasa !--- Output
suppressed. access-list OUTSIDE extended permit tcp any host 172.20.1.10 eq www !--- Output
suppressed. global (outside) 1 interface nat (inside) 1 192.168.100.0 255.255.255.0 static
(inside,outside) 172.20.1.10 192.168.100.10 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.
```

Чтобы настроить исправление DNS в ASDM, выполните следующие действия:

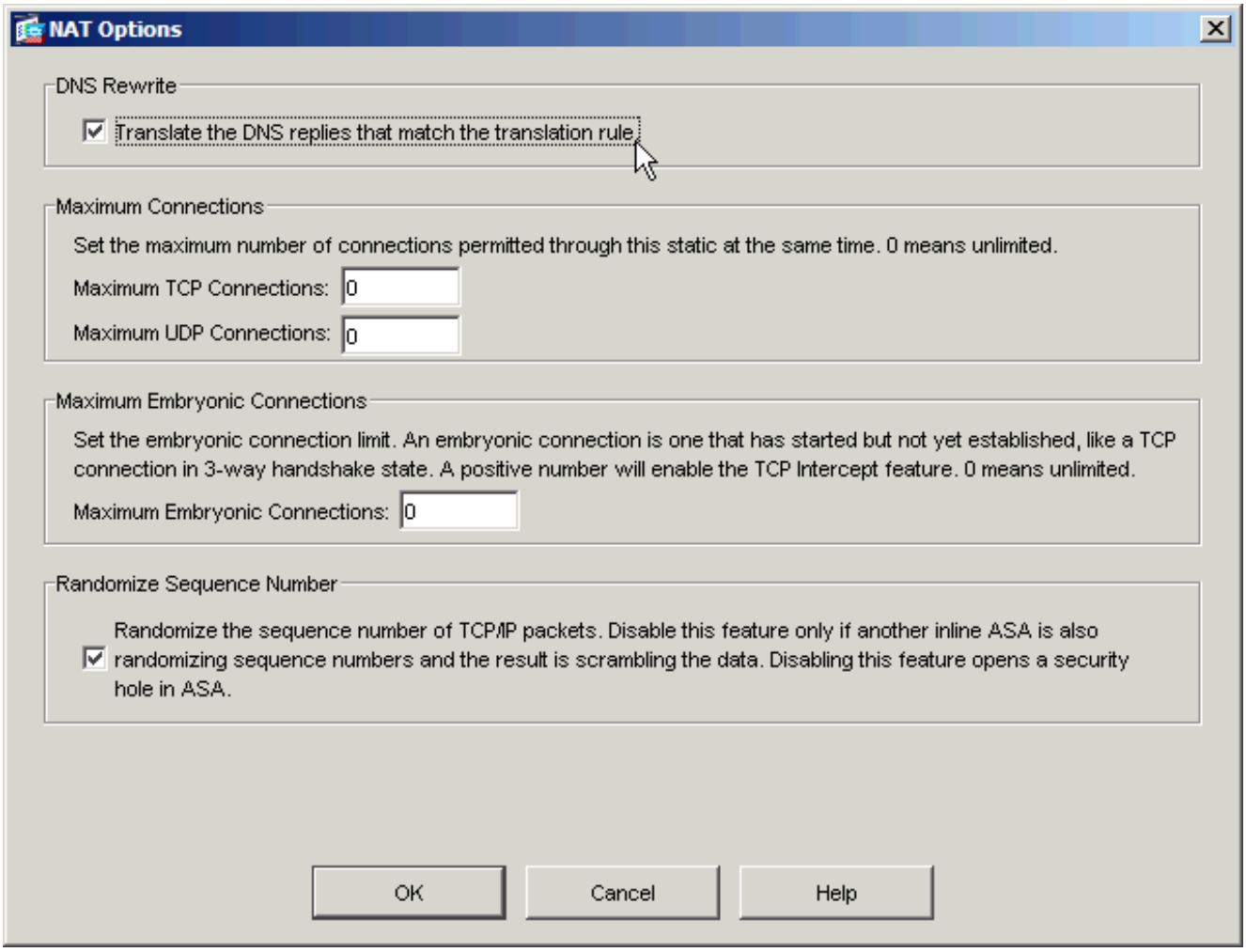
1. **Перейдите в Configuration > NAT и выберите статическое правило NAT для изменения. Нажмите Edit.**



2. **Нажмите NAT Options....**



3. Установите флажок Translate DNS replies that match the translation rule.



4. **Нажмите OK, чтобы покинуть окно "NAT Options" (Параметры NAT). Нажмите OK, чтобы покинуть окно "Edit Static NAT Rule" (Изменение статического правила NAT). Нажмите Apply, чтобы отправить конфигурацию на устройство защиты.**

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
2 0.001251 **172.22.1.161 192.168.100.2 DNS Standard query response A 192.168.100.10** 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: 52985 (52985) Domain Name System (response) [Request In: 1] [Time: 0.001251000 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 192.168.100.10 Name: server.example.com Type: A (Host address) Class: IN (0x0001) Time to live: 1 hour Data length: 4 Addr: 192.168.100.10** *!--- 172.20.1.10 has been rewritten to be 192.168.100.10.*
5. На этом этапе клиент пытается обратиться к серверу WWW по адресу 192.168.100.10. Соединение устанавливается. Трафик не перехватывается в ASA, так как клиент и сервер находятся в одной подсети.

Окончательная конфигурация с ключевым словом "dns"

Это окончательная конфигурация ASA для выполнения исправления DNS с ключевым словом dns и двумя интерфейсами NAT.

Окончательная конфигурация ASA 7.2(1)
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 shutdown no nameif no security-level no ip address ! 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 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,outside) 172.20.1.10 192.168.100.10 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 !--- DNS inspection map. 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:a4a38088109887c3ceb481efab3dcf32 : end
```

Альтернативное решение: Прикрепление

Прикрепление со статическим NAT

Внимание. : Прикрепление со статическим NAT включает передачу всего трафика между клиентом и сервером WWW через устройство безопасности. Тщательно оцените ожидаемый объем трафика и возможности устройства безопасности, прежде чем применять это решение.

Прикрепление — это процесс, который отправляет трафик обратно на тот интерфейс, с которого он поступил. Эта функция была добавлена в ПО устройств безопасности версии 7.0. Для версий ниже 7.2(1) по крайней мере одна ветвь прикрепленного трафика (входящая или исходящая) обязательно должна быть зашифрована. Начиная с версии 7.2(1) это требование не действует. При использовании версии 7.2(1) обе ветви трафика могут быть незашифрованы.

Прикрепление в сочетании с утверждением NAT static можно использовать для достижения того же эффекта, что и исправление DNS. Этот метод не изменяет содержимое A-записи DNS, которая возвращается от DNS-сервера клиенту. **Вместо этого, при использовании прикрепления, например в сценарии, рассматриваемом в этом документе, клиент может использовать для соединения адрес 172.20.1.10, возвращенный DNS-сервером.**

Вот как выглядит соответствующая часть конфигурации при использовании прикрепления и статического NAT для достижения эффекта исправления DNS. Команды, выделенные полужирным шрифтом, объясняются более подробно в конце этих выходных данных:

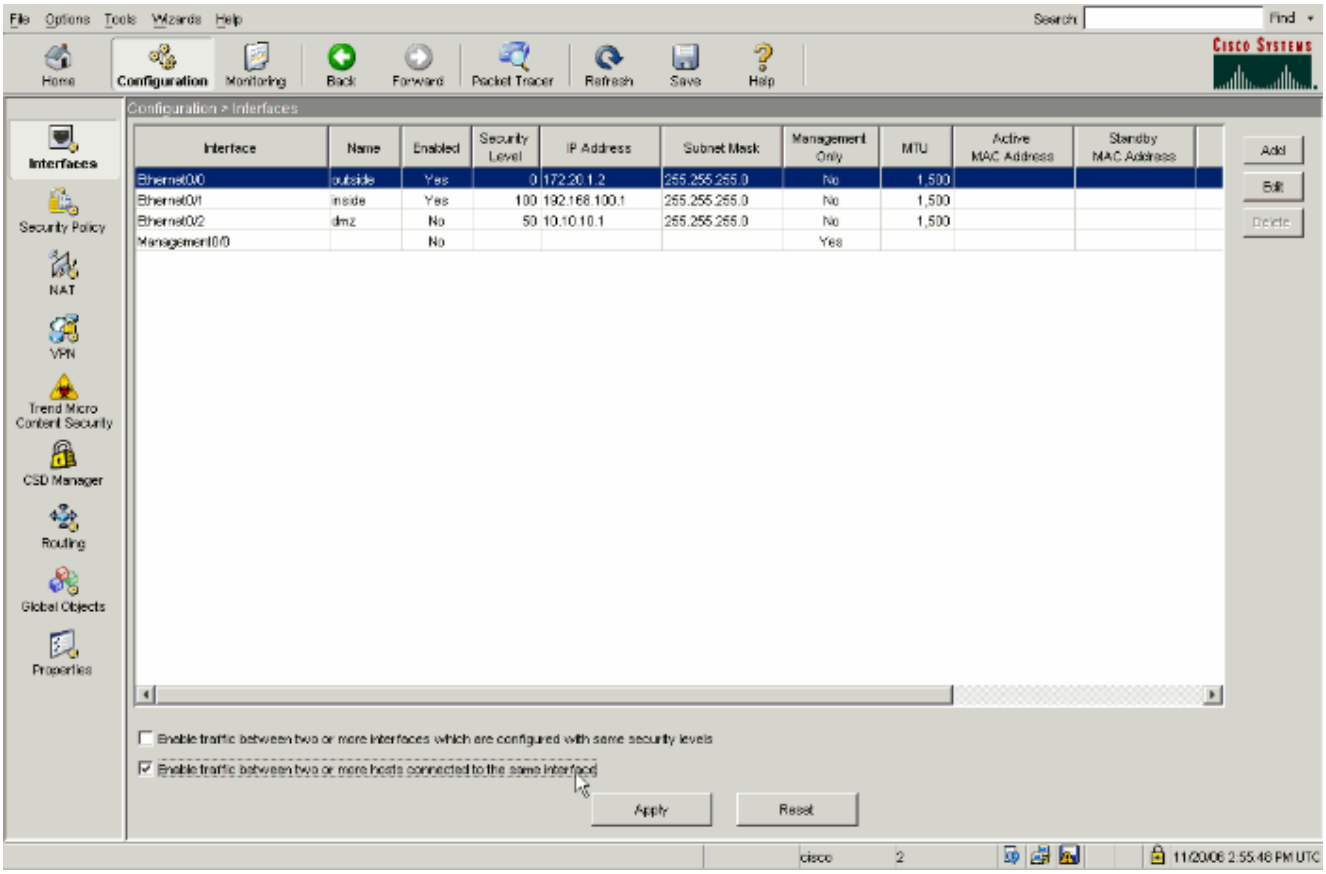
```
ciscoasa(config)#show run : Saved : ASA Version 7.2(1) ! hostname ciscoasa !--- Output
suppressed. same-security-traffic permit intra-interface !--- Enable hairpinning. global
(outside) 1 interface !--- Global statement for client access to the Internet. global (inside) 1
interface !--- Global statment for hairpinned client access through !--- the security appliance.
nat (inside) 1 192.168.100.0 255.255.255.0 !--- The NAT statement defines which traffic should
be natted. !--- The whole inside subnet in this case. static (inside,outside) 172.20.1.10
```

```
192.168.100.10 netmask 255.255.255.255 !--- Static NAT statement mapping the WWW server's real address to a !--- public address on the outside interface. static (inside,inside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255 !--- Static NAT statment mapping requests for the public IP address of !--- the WWW server that appear on the inside interface to the WWW server's !--- real address of 192.168.100.10.
```

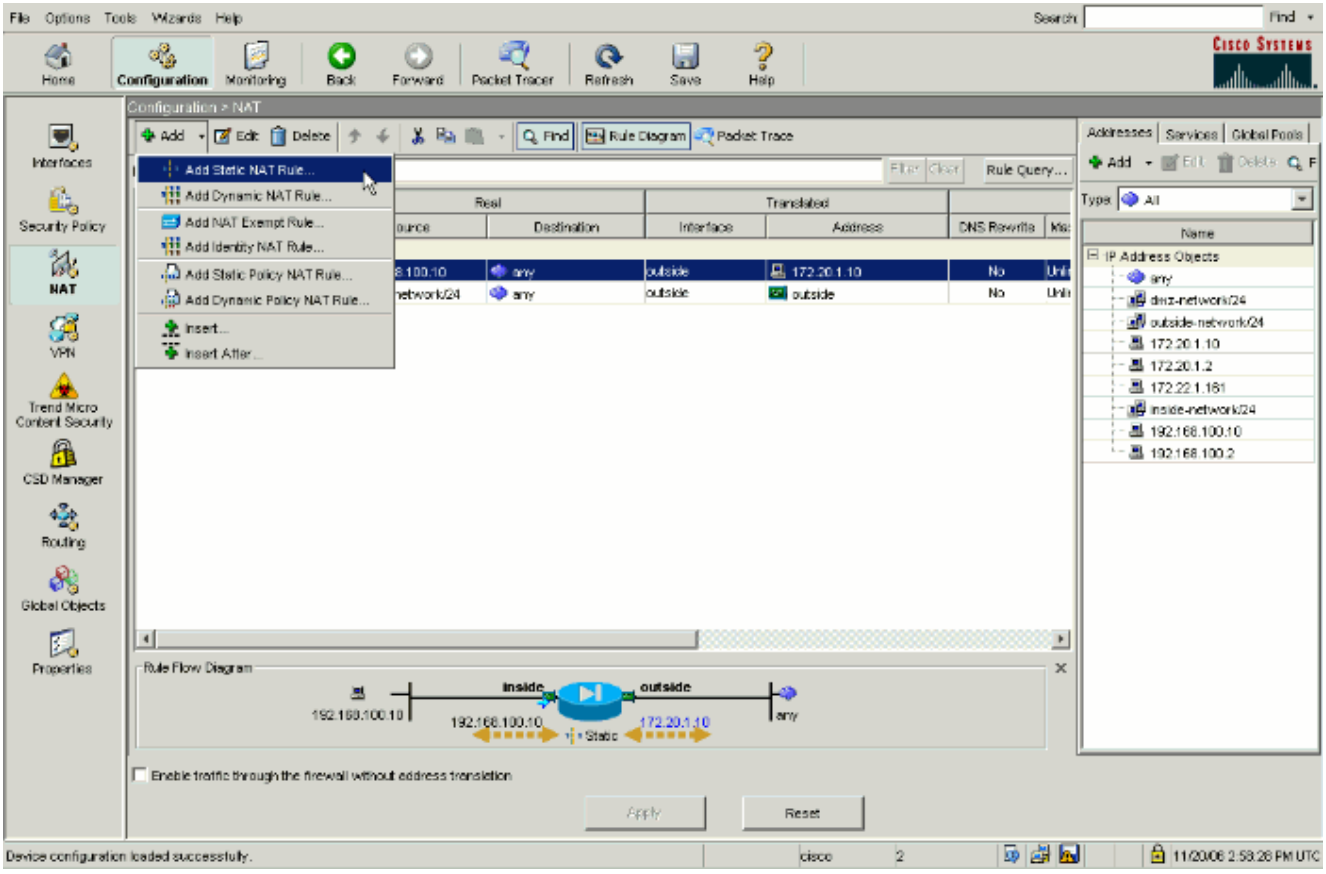
- **same-security-traffic—Эта команда позволяет трафику того же уровня безопасности проходить через устройство безопасности. Ключевые слова permit intra-interface позволяют трафику одного уровня безопасности поступать и исходить с одного и того же интерфейса, таким образом включая прикрепление.Примечание:** См. same-security-traffic для получения дополнительной информации о прикреплении и **команде same-security-traffic**.
- **global (inside) 1 interface—Весь трафик, проходящий через устройство безопасности, должен пройти через NAT. Эта команда использует адрес внутреннего интерфейса устройства безопасности, чтобы позволить трафику, поступающему на внутренний интерфейс, пройти через PAT, как бы прикрепляя его снаружи внутреннего интерфейса.**
- **static (inside,inside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255—Эта статическая запись NAT создает второе сопоставление для публичного IP-адреса сервера WWW.** Однако, в отличие от первой статической записи NAT, на этот раз адрес 172.20.1.10 сопоставляется внутреннему интерфейсу устройства безопасности. Это позволяет устройству безопасности отвечать на запросы, которые оно получает для этого адреса на внутренний интерфейс. Затем устройство безопасности перенаправляет эти запросы на реальный адрес сервера WWW через себя.

Чтобы настроить прикрепление со статическим NAT в ASDM, выполните следующие действия:

1. **Перейдите на Configuration > Interfaces.**
2. **В нижней части окна установите флажок Enable traffic between two or more hosts connected to the same interface.**

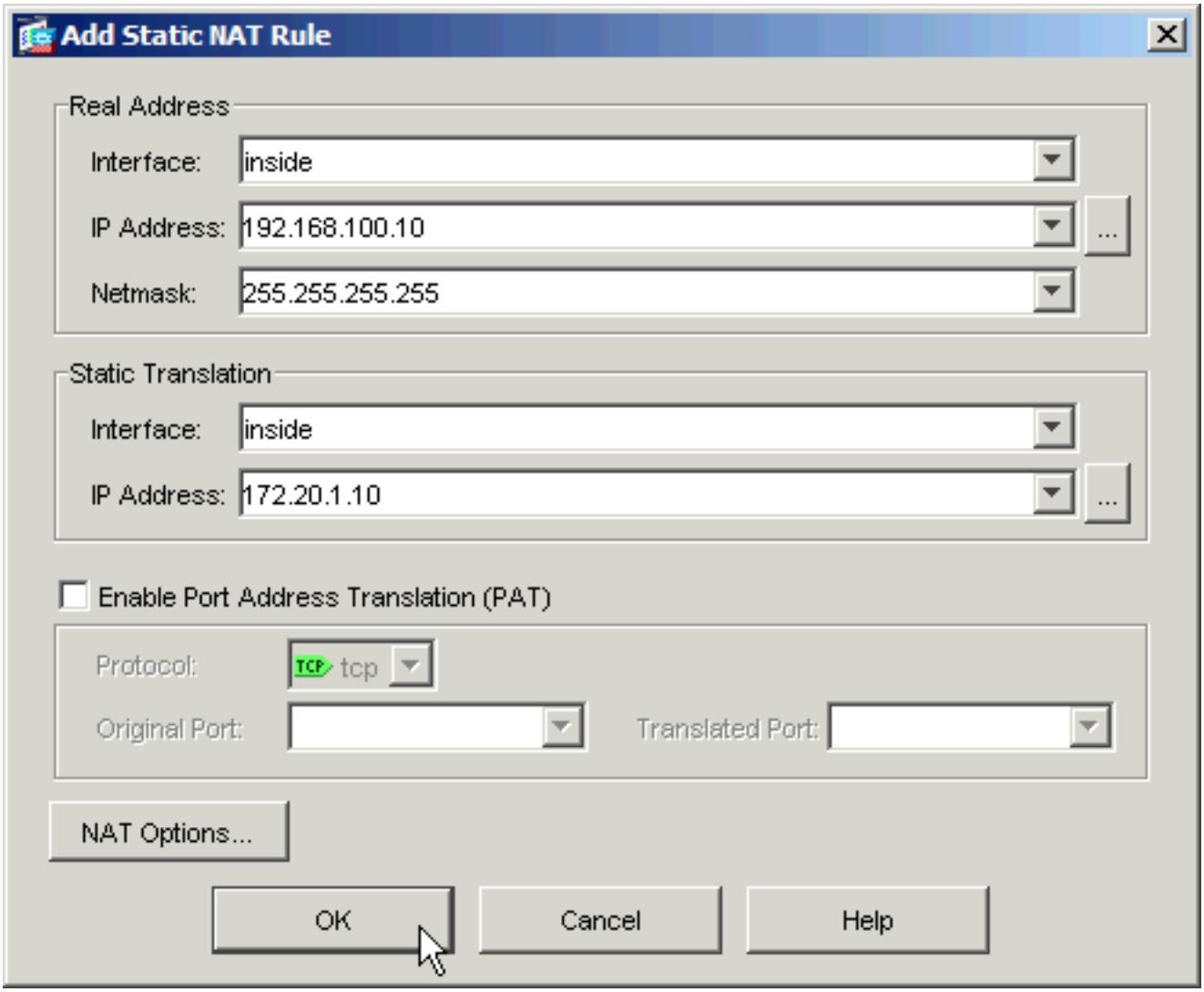


3. **Щелкните "Применить".**
4. **Перейдите на Configuration > NAT и выберите Add > Add Static NAT Rule....**

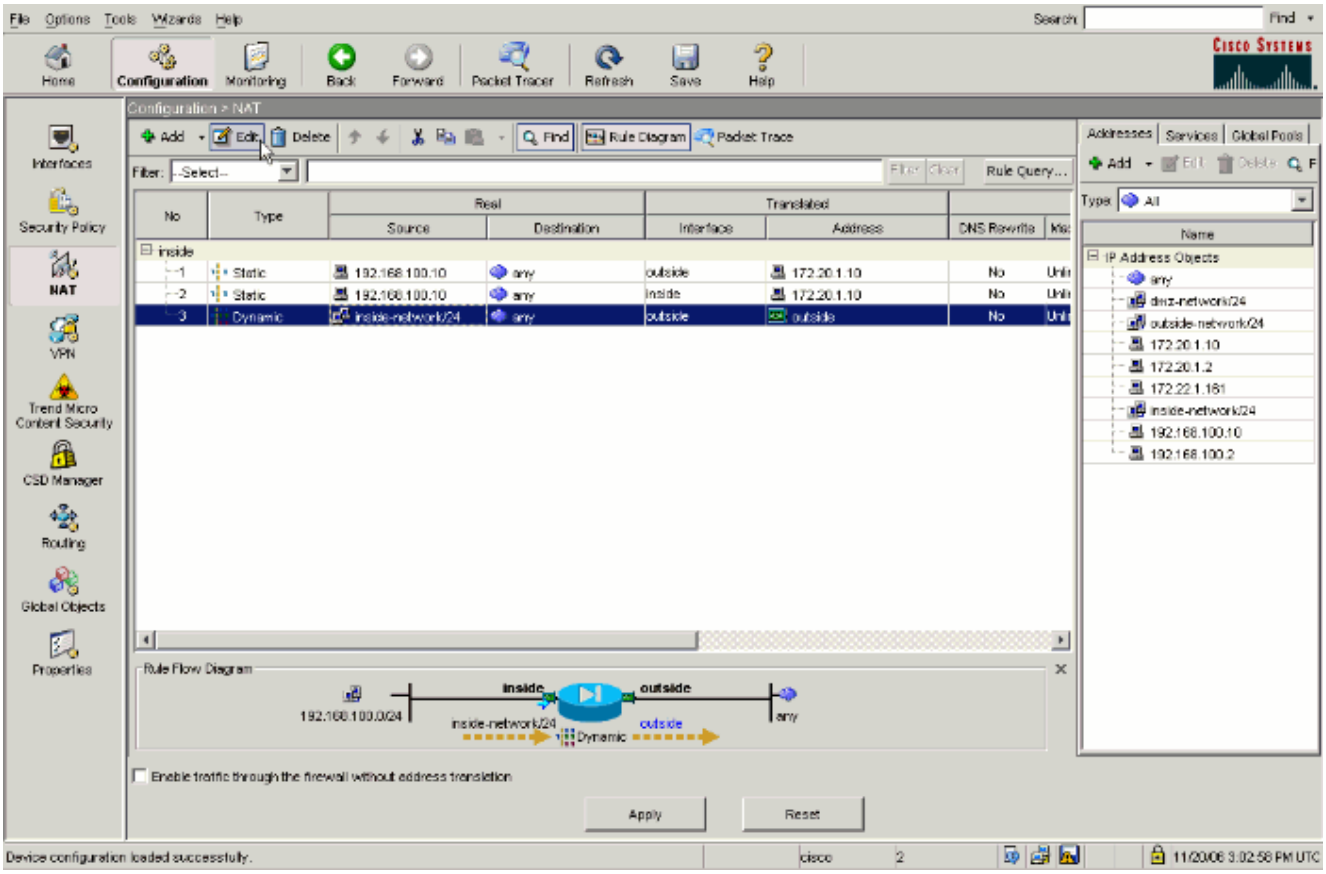


5. Введите данные конфигурации для нового статического преобразования.**Заполните область Real Address данными сервера WWW.Заполните область Static Translation данными адреса и интерфейса, которые необходимо сопоставить серверу WWW.**В этом случае внутренний интерфейс выбирается так, чтобы разрешить узлам на

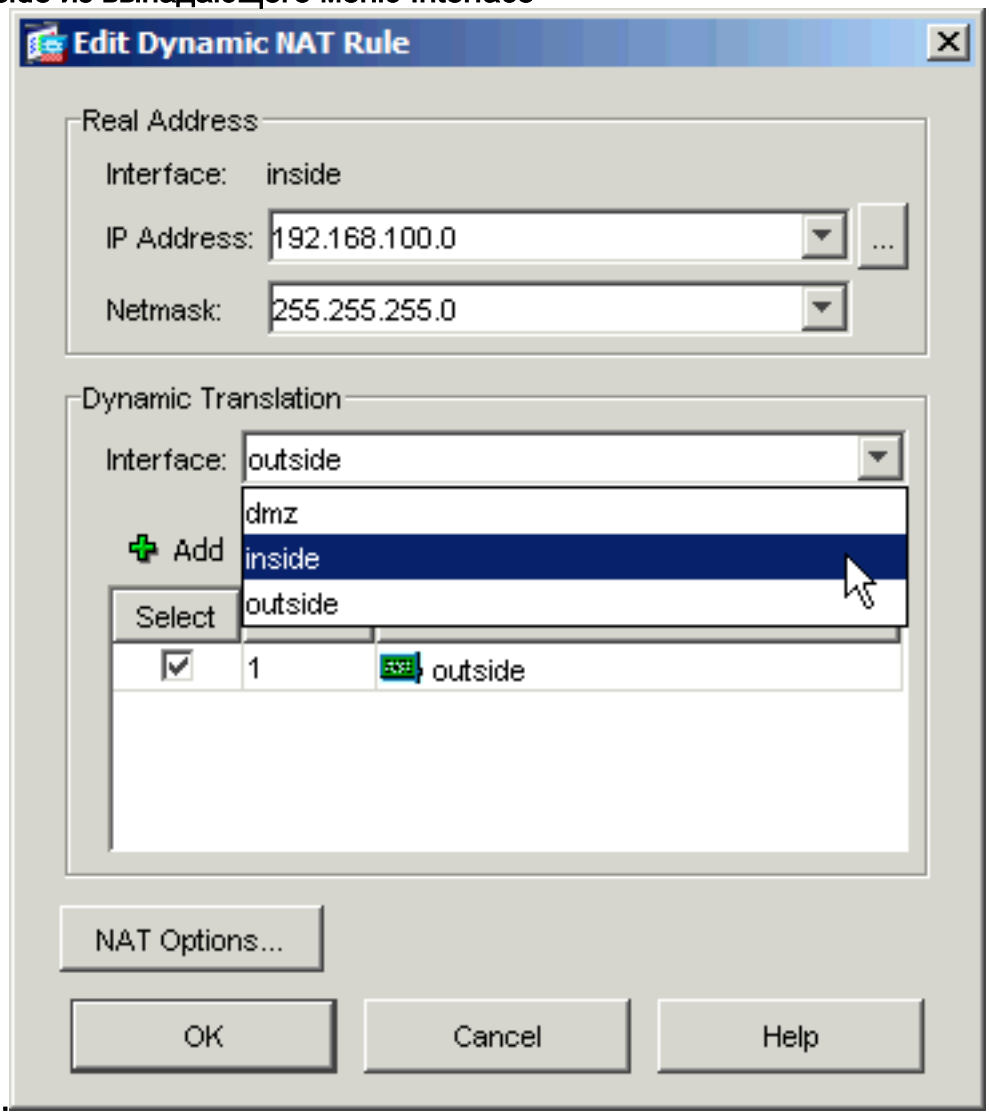
внутреннем интерфейсе обращаться к серверу WWW через сопоставленный адрес 172.20.1.10.

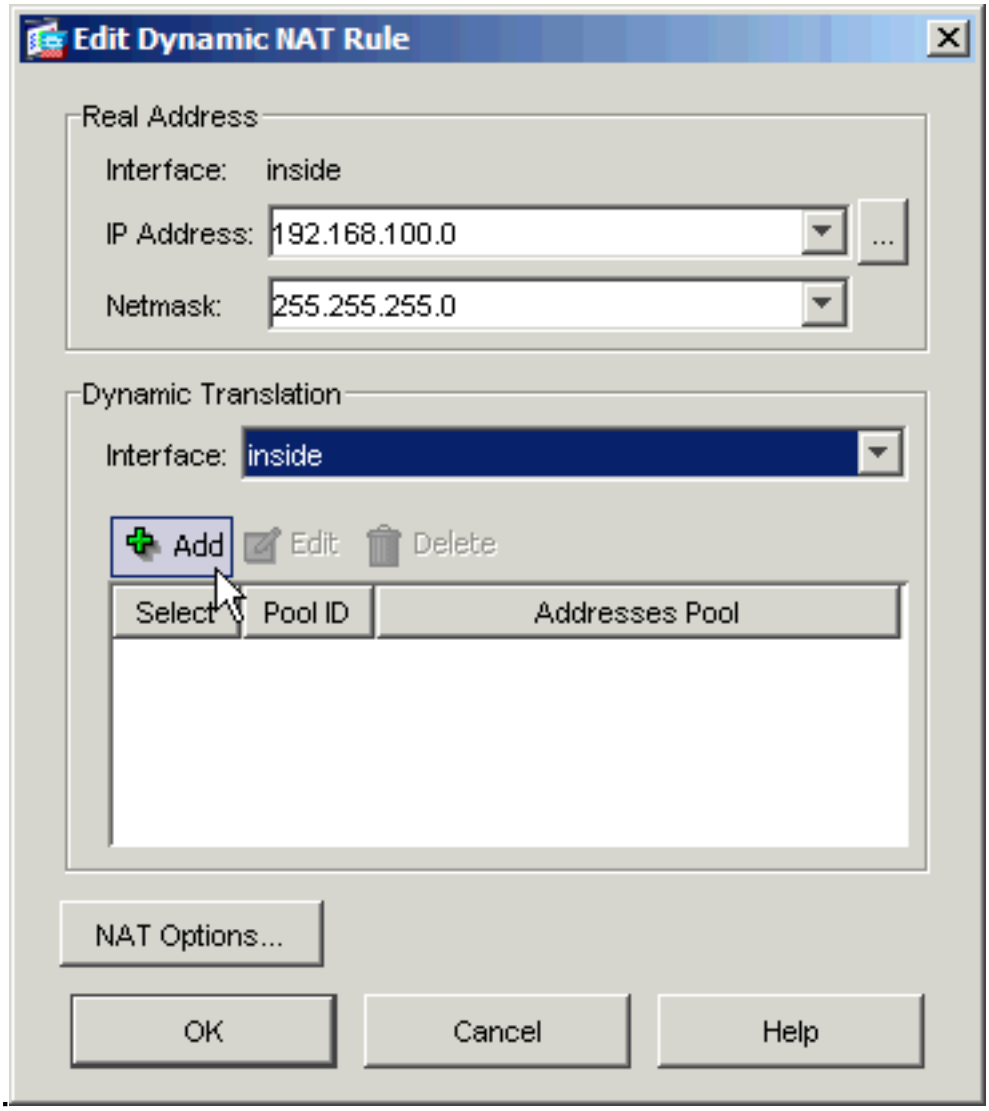


6. Нажмите OK, чтобы покинуть окно "Add Static NAT Rule" (Добавление статического правила NAT).
7. Выберите существующее динамическое преобразование PAT и нажмите Edit.

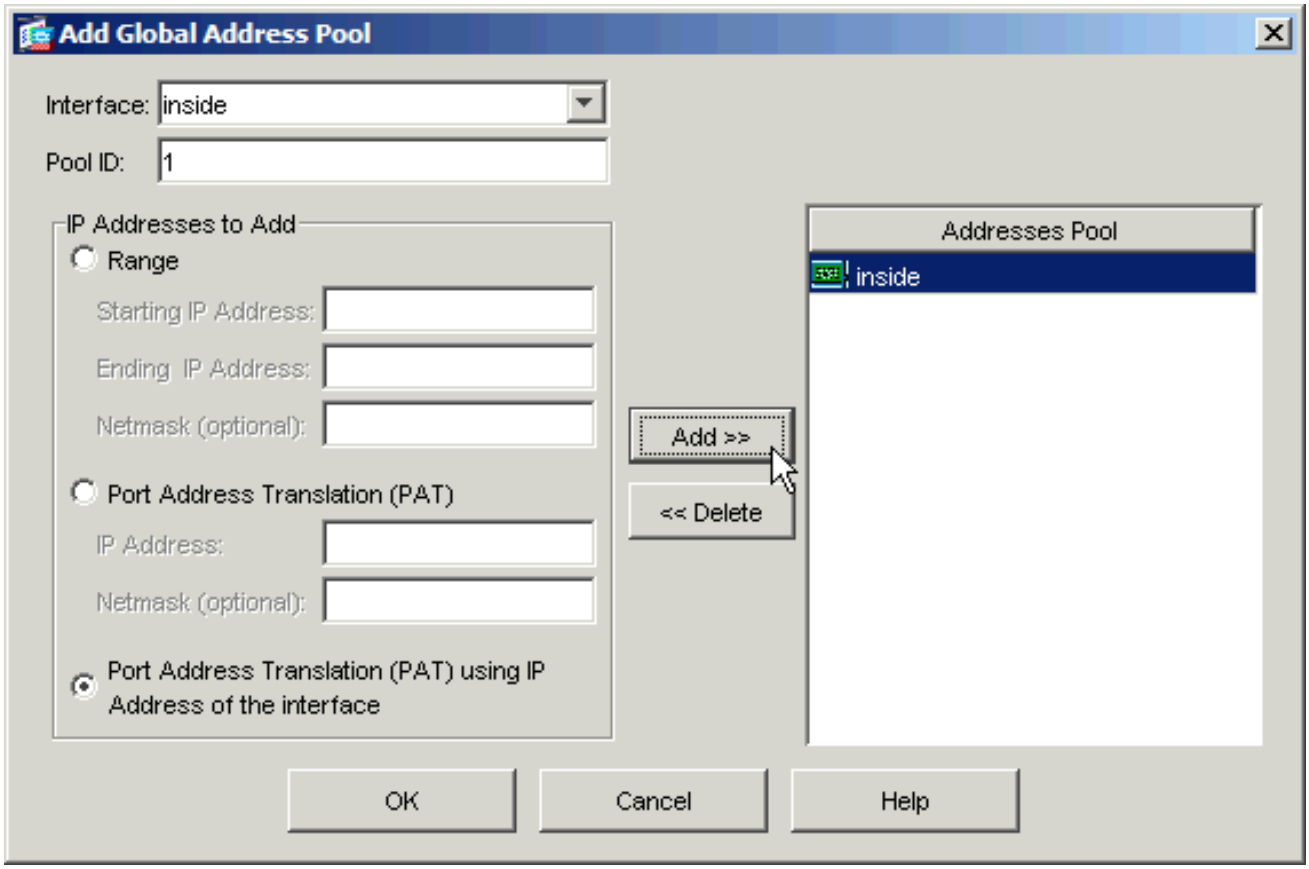


8. **Выберите inside из выпадающего меню Interface (Интерфейс).**





9. Нажмите Add.
10. Выберите переключатель Port Address Translation (PAT) using IP address of the interface. Нажмите
    Add.



11. **Нажмите OK, чтобы покинуть окно "Add Global Address Pool" (Добавление глобального пула адресов). Нажмите OK, чтобы покинуть окно "Edit Dynamic NAT Rule" (Изменение динамического правила NAT). Нажмите Apply, чтобы отправить конфигурацию на устройство защиты.**

Вот последовательность событий, которые происходят, когда настроено прикрепление. **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 192.168.100.10.`%ASA-7-609001: Built local-host inside:192.168.100.10`
3. Устройство безопасности создает динамическое преобразование PAT для клиента. Источником клиентского трафика теперь является внутренний интерфейс устройства безопасности: 192.168.100.1.`%ASA-6-305011: Built dynamic TCP translation from inside:192.168.100.2/11012 to inside:`**`192.168.100.1/1026`**
4. Устройство безопасности создает TCP-соединение между клиентом и сервером WWW через себя. Обратите внимание на сопоставленные адреса узлов в скобках.`%ASA-6-302013: Built inbound TCP connection 67399 for inside:192.168.100.2/11012 `**`(192.168.100.1/1026)`**` to inside:192.168.100.10/80 `**`(172.20.1.10/80)`**
5. **Команда show xlate на устройстве защиты проверяет, преобразуется ли клиентский трафик через устройство защиты.**`ciscoasa(config)#`**`show xlate`**` 3 in use, 9 most used Global 172.20.1.10 Local 192.168.100.10 Global 172.20.1.10 Local 192.168.100.10 `**`PAT Global 192.168.100.1(1027) Local 192.168.100.2(11013)`**
6. **Команда show conn на устройстве безопасности проверяет, что соединение между устройством безопасности и сервером WWW установлено от имени клиента.** Обратите внимание на реальный адрес клиента в скобках.`ciscoasa#`**`show conn`**` TCP out 192.168.100.1`**`(192.168.100.2)`**`:11019 in 192.168.100.10:80 idle 0:00:03 bytes 1120 flags UIOB`

Окончательная конфигурация с прикреплением и статическим NAT

Это окончательная конфигурация ASA, которая использует прикрепление и статический NAT для достижения эффекта исправления DNS с двумя интерфейсами NAT.

Окончательная конфигурация ASA 7.2(1)

```
ciscoasa(config-if)#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 shutdown no nameif
no security-level no ip address ! interface
Management0/0 shutdown no nameif no security-level no ip
address management-only ! passwd 2KFQnbNIdI.2KYOU
encrypted ftp mode passive same-security-traffic permit
intra-interface 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 asdm
image disk0:/asdm512-k8.bin no asdm history enable arp
timeout 14400 global (outside) 1 interface !--- Global
statement for client access to the Internet. global
(inside) 1 interface !--- Global statment for hairpinned
client access through !--- the security appliance. nat
(inside) 1 192.168.100.0 255.255.255.0 !--- The NAT
statement defines which traffic should be natted. !---
The whole inside subnet in this case. static
(inside,outside) 172.20.1.10 192.168.100.10 netmask
255.255.255.255 !--- Static NAT statement mapping the
WWW server's real address to a public !--- address on
the outside interface. static (inside,inside)
172.20.1.10 192.168.100.10 netmask 255.255.255.255 !---
Static NAT statement mapping requests for the public IP
address of the !--- WWW server that appear on the inside
interface to the WWW server's real address !--- of
192.168.100.10. 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:7c9b4e3aff085ba90ee194e079111e1d
: end
```

Примечание: См. это видео, Прикрепление на Cisco ASA (только зарегистрированные клиенты), для получения дополнительной информации о других сценариях, где могло использоваться прикрепление.

Настройка проверки DNS

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.** Дополнительные сведения о политиках обслуживания и проверке см. в разделе Использование модульной системы политик.

1. Создайте карту политик проверки для DNS.`ciscoasa(config)#`**`policy-map type inspect dns MY_DNS_INSPECT_MAP`**
2. Из режима настройки карты политик войдите в режим настройки параметров, чтобы задать параметры для механизма проверки.`ciscoasa(config-pmap)#`**`parameters`**
3. В режиме настройки параметров карты политик задайте для максимальной длины сообщения DNS значение 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 настройки класса карты политик укажите, что DNS должен проверяться с помощью карты политик проверки, созданной на шагах 1-3.`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`

Настройка раздельных DNS

Выполните команду split-dns в режиме настройки групповой политики, чтобы ввести список доменов, разрешающихся через раздельные туннели. ***Используйте форму по этой команды, чтобы удалить список.***

Если списки доменов раздельного туннелирования отсутствуют, пользователи наследуют списки, существующие в групповой политике по умолчанию. **Выполните команду split-dns none, чтобы предотвратить наследование списков доменов раздельного туннелирования.**

Для разделения записей в списке доменов используйте одиночные пробелы. Число записей не ограничено, но длина всей строки не может превышать 255 символов. Можно использовать только алфавитно-цифровые символы, дефисы (-) и точки (.).). **Команда no split-dns, при использовании без аргументов, удаляет все текущие значения, включая нулевые значения, созданные при выполнении команды split-dns none.**

В этом примере показано, как настроить домены Domain1, Domain2, Domain3 и Domain4, чтобы они разрешались через раздельное туннелирование для групповой политики с именем FirstGroup:

```
hostname(config)#group-policy FirstGroup attributes hostname(config-group-policy)#split-dns
value Domain1 Domain2 Domain3 Domain4
```

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. См. раздел Настройка проверки 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 dmz:10.10.10.10/23
```

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

Сброс отклика UDP DNS

При сбросе пакета DNS возможно получение следующего сообщения об ошибке:

```
 %PIX|ASA-4-410001: UDP DNS request from source_interface:source_address/source_port
to dest_interface:dest_address/dest_port; (label length | domain-name length)
52 bytes exceeds remaining packet length of 44 bytes.
```

Чтобы решить эту проблему, увеличьте длину пакета DNS в диапазоне 512-65535.

Пример:

```
ciscoasa(config)#policy-map type inspect dns MY_DNS_INSPECT_MAP ciscoasa(config-pmap)#parameters
ciscoasa(config-pmap-p)#message-length maximum <512-65535>
```

Дополнительные сведения

- Cisco PIX Firewall Software
- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Уведомления о дефекте для специалистов по продуктам безопасности
- Запрос на комментарии (RFC)
- Прикрепление на Cisco ASA
- CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES
- Cisco Systems – техническая поддержка и документация