NAT: вопросы и ответы

Вопросы

Введение

Этот документ содержит ответы на некоторые наиболее часто задаваемые вопросы о трансляции сетевых адресов Cisco IOS® (NAT).

Дополнительные сведения об условных обозначениях в документах см. в разделе Технические советы Cisco. Условные обозначения.

В. Что такое NAT?

Ответ: NAT означает преобразование сетевых адресов. NAT предназначен для упрощения и сохранения IP-адресов. Он позволяет частным IP-сетям, которые используют незарегистрированные IP-адреса, подключаться к Интернету. NAT

работает на маршрутизаторе, который обычно соединяет две сети, и преобразует частные (а не глобально уникальные) адреса во внутренней сети в действительные адреса перед отправкой пакетов в другую сеть. Поскольку данная функция является частью возможностей маршрутизатора, трансляцию сетевых адресов (NAT) можно настроить для отображения только одного адреса всей сети для внешнего мира. Это обеспечивает дополнительную безопасность и позволяет скрыть внутреннюю сеть от доступа извне. NAT поддерживает совместные функции обеспечения безопасности и сохранения адресов и обычно устанавливается в средах удаленного доступа. Дополнительные сведения о работе NAT содержатся в документе Принципы работы NAT.

В. Каковы основные различия между Cisco IOS NAT® и реализацией NAT брандмауэром Cisco PIX?

Ответ: Функция NAT, основанная на ПО Cisco IOS, не намного отличается от функций NAT, доступных в брандмауэре PIX. Главные отличия включают в себя различные типы трафика, поддерживаемые в Cisco IOS NAT и реализации NAT в PIX. Подробная информация о настройке функций NAT в PIX (содержит описание типов поддерживаемых трафиков) содержится в документах Брандмауэры Cisco PIX серии 500 и Примеры настройки NAT.

В. Для каких платформ маршрутизации Cisco доступна система Cisco IOS NAT? Как оформляется заказ?

Ответ: Средство Cisco Software Advisor (только для зарегистрированных пользователей) (поиск по функции) предоставляет инструменты для идентификации выпуска и платформы, для которых доступны возможности Cisco IOS. Чтобы проверить, поддерживается ли NAT на определенной платформе, перейдите к Software Advisor (только для зарегистрированных пользователей), выберите функцию **Найти ПО с нужными функциями**, укажите информацию о продукте и ПО, затем укажите функцию NAT и выберите платформу. Затем данное средство сообщает о ПО Cisco IOS, которое поддерживает данную функцию на этой платформе.

Для информации:

- Когда функция NAT впервые появилась в ПО Cisco IOS версии 11.2, она была доступна только в образах Plus.
- В Cisco IOS версии 11.3 функции PAT доступны на всех IP-образах, а все функции NAT (1-1 и PAT) доступны только на образах Enterprise Plus.
- В Cisco IOS версии 12.0 функции PAT доступны на всех IP-образах.

Представленная ниже таблица содержит сведения о поддержке Cisco IOS и NAT.

Версия ПО Cisco IOS	Поддержка NAT в базовых образах	Поддержка NAT в образах Plus	Простая поддержка IP	Поддерживаемые аппаратные платформы
11.2	-	NAT	-	Cisco 1000, 2500, 4x00, AS5200, 7200, RSP7000, 7500
11.2P	-	NAT	-	Cisco 1000, 1600, 2500, 3620, 3640, 4x00, AS5200, AS5300, Cat5000 RSM, 7200, RSP7000, 7500
11.3	Только PAT	NAT	Фаза 1	Cisco 1000, 1600, 2500, 3620, 3640, 4x00, AS5200, 7200, RSP7000, 7500
11.3T	Только PAT	NAT	Фаза 1	Cisco 1000, 1600, 2500, 2600, 3620, 3640, 4x00, AS5200, AS5300, Cat5000 RSM, 7200, RSP7000, 7500
12.0	NAT	NAT	Фаза 1	Cisco 1600, 2500, 2600, 3620, 3640, 4000, 4500, 4700, AS5x00, Cat5000 RSM, 7200, RSP7000, 7500
				Cisco 800[1], 1400, 1600, 1700, 2500[2],

12.0T	NAT	NAT	Фаза 2	2600, 36x0,MC3810, C4x00, AS5x00,Cat5000 RSM, Cat5000 RSFC, 7100, 7200, uBR9x0, uBR7200[3], RSP7000, 7500
12.1	NAT	NAT	Фаза 2	Cisco 800[1], 1400, 1600, 1700, 2500[2], 2600, 36x0, MC3810, C4x00, AS5x00, Cat5000 RSM, Cat5000 RSFC, 7100, 7200, ubr9x0, uBR7200[3], RSP7000, 7500, RPM
12.1T	NAT	NAT	Фаза 2	Cisco 800[1], 1400, 1600[4], 1700[2,4], 2500, 2600, 36x0, MC3810, C4x00, AS5x00, Cat5000 RSM, Cat5000 RSFC, 7100, 7200, ubr9x0, uBR7200[3], RSP7000, 7500, RPM
12.2	NAT	NAT	Фаза 2	Cisco1400, 1601-1604, 1601R-1605R,1720,1750,2501-2525,2610XM-2611XM,2620-2621, 2620XM-2621XM, 2650XM-2651XM, 2650-2651, 3620,3640,3640A, 3660, 4500,7100, 7200,7500,800,8850RPM-PR,AS5300, AS5400,CAT4500-AGM, CAT5000-RSM, ICS7700,MC3810,SLT,UBR910, 920
12.2T	NAT	NAT	Фаза 2	Cisco 1710, 1721,1751,1751-V,1760,1720,1750,2501-2525,2610XM-2611XM,2620-2621, 2620XM-2621XM, 2650XM-2651XM, 2650-2651, 3620,3640,3640A, 3660, 3725,3745,6400-NPR-1, 6400-NPR-2SV,6400-NSP,7100, 7200,7400,7500,800,8850RPM-PR,AS5300, AS5350,AS5400,AS5400HPX, CAT4500-AGM, CVA 120, CAT5000-RSM, ICS7700,MC3810,SLT, SOHO76, 77, 78, UBR7200,UBR905,925.
12.3	NAT	NAT	Фаза 2	Cisco 1400, 1601-1604, 1601R-1605R,1710,1720,1721,1750,1751-V,1751,1760,2501-2525,2610XM-2611XM, 2620XM-2621XM, 2650XM-2651XM, 2650-2651,2691, 3620,3631,3640,3640A, 3660, 3725,3745,6400-NRP1, 6400-NRP-2SV, 6400- NSP, 7200,7301,7400,7500,800,8850RPM-PR,AS5300, AS5350, AS5400,AS5400HPX, AS5850-RSC,CAT4224,CAT4500-AGM, CVA120, ICS7700,MC3810,SCT, SOHO76,77,78, UBR905, 925.
12.3T	NAT	NAT	Фаза 2	Cisco 1701,1710,1711, 1712,1720,1721,1751-V,1751,1760, 2610XM-2611XM, 2620XM-2621XM, 2650XM-2651XM, 2691, 28X1,3620,3631,3640,3640A, 3660, 3725,3745,6400-NRP1, 6400-NRP-2SV, 6400- NSP, 7200,7301,7400,7500,800,8850RPM-PR,AS5300, AS5350, AS5400,AS5400HPX, AS5850-RSC,CAT4224,CAT4500-AGM, CVA120, ICS7700,MC3810,SCT, SOHO78, SOHO91, 96,97, UBR905, 925, VG224.,

Примечание: Эта информация получена с помощью инструмента Навигатор функций (только для зарегистрированных клиентов) .

- Функция NAT отсутствует на uBR7200 в образе программного обеспечения поставщика услуг (-p). Функциональность протокола DHCP для сервера доступна на uBR7200 в образе ПО провайдера (-p).
- В серии 2500, начиная с ПО Cisco IOS версии 11.2, поддерживается образ Enterprise plus. Образы Enterprise не поддерживают NAT.
- В серии 2600, начиная с ПО Cisco IOS версии 12.2T, поддерживается образ Enterprise Base.
- В серии 3620, начиная с ПО Cisco IOS версии 11.2P, поддерживается образ Enterprise plus. Образы Enterprise не поддерживают NAT.
- В серии 3640, начиная с ПО Cisco IOS версии 11,3, поддерживается образ Enterprise plus. Образы Enterprise не поддерживают NAT.
- В серии 4000, начиная с ПО Cisco IOS версии 11.2, поддерживается образ Enterprise plus. Образы Enterprise не поддерживают NAT.
- В серии 4500, начиная с ПО Cisco IOS версии 11.2, поддерживается образ Enterprise plus. Образы Enterprise не поддерживают NAT.
- В серии AS5300, начиная с ПО Cisco IOS версии 11.2P, поддерживается образ Enterprise. AS5800 предоставляет поддержку для NAT, SIP и NAT, директории NetMeeting.
- В серии Catalyst 5000 RSM, начиная с ПО Cisco IOS версии 11.3T, поддерживается образ Enterprise. В серии 7200 NAT поддерживается, начиная с версии ПО Cisco IOS 11.2.
- В версии 7500 NAT поддерживается, начиная с версии ПО Cisco IOS 11.2.
- В Cisco 3825 и 3845 поддерживается образ IP Base, начиная с ПО Cisco IOS версии 12.3T.
- В серии 1600, начиная с ПО Cisco IOS версии 11.3 IP base и в серии 2500, начиная с ПО Cisco IOS версии 11.3 IP base, функция NAT поддерживается.
- [1]NAT поддерживается всеми образами программного обеспечения Cisco IOS для Cisco 800, начиная с Cisco IOS версии 12.0(3)T.
- [2]NAT поддерживается всеми образами программного обеспечения Cisco IOS для Cisco 1700, начиная с Cisco IOS версии 12.2ZH.
- [3] Функции NAT и протокола DHCP для сервера доступны только на платформе на uBR7200 в образе ПО провайдера (-ps), начиная с ПО Cisco IOS версии 12.0(3)T.
- [4] Чтобы обеспечить поддержку приложения NetMeeting Microsoft в Cisco IOS NAT для всех платформ, кроме uBR7200, необходим образ J или O (Enterprise или брандмауэр Cisco, соответственно).

B. NAT происходит до или после маршрутизации?

Ответ. Трансляция изнутри-наружу происходит после маршрутизации, а трансляция снаружи-внутрь происходит перед маршрутизацией. Дополнительная информация содержится в документе Порядок работы NAT.

B. Как при помощи NAT достигается осведомленность маршрутизатора об IP-адресах?

Ответ. Маршрутизация для IP-адресов, созданных при помощи NAT, распознается в следующих случаях:

- Внутренний пул глобальных адресов формируется в подсети маршрутизатора следующего узла.
- Запись статического маршрута настраивается на следующем маршрутизаторе и перераспределяется в пределах маршрутизируемой сети.

B. Сколько параллельных сеансов NAT поддерживается в NAT Cisco IOS?

Ответ. Количество сеансов NAT ограничено количеством доступных DRAM в маршрутизаторе. На каждое преобразование сетевых адресов (NAT) выделяется около 150 байт DRAM. В итоге на 10 000 трансляций (больше, чем обычно обрабатывает один маршрутизатор) выделяется около 1,6 МБ. Следовательно, у стандартной платформы маршрутизации более чем достаточно памяти для поддержки тысяч трансляций NAT.

Вопрос. Какую эффективность маршрутизации можно ожидать при использовании Cisco IOS NAT?

Ответ. Cisco IOS NAT поддерживает коммутацию Cisco Express Forwarding (CEF), быструю коммутацию и коммутацию процессов.

Производительность зависит от следующих факторов:

- Тип приложения и тип его трафика (содержит ли он встроенный IP-адрес?)
- Выполняется ли обмен сообщениями, которые подлежат проверке?
- Используется ли выделенный порт или происходит согласование портов?
- Количество преобразований.
- Что еще выполняется на сервере в это время?
- Тип платформы и процессора.

Для большинства приложений ухудшение производительности, связанное с NAT, должно быть незначительным.

В. Можно ли применить Cisco IOS NAT к подинтерфейсам?

Ответ. Да. Преобразования NAT источника или назначения могут применяться к любому интерфейсу или подинтерфейсу с IP-адресом (включая интерфейсы программы набора номера).

В. Может ли Cisco IOS NAT использоваться вместе с протоколом HSRP для прокладывания избыточных каналов к поставщику Интернет-услуг (ISP)?

Ответ. Нет. В этом сценарии и в более ранних версиях ПО Cisco IOS маршрутизатор в режиме ожидания не использует таблицу преобразования активного маршрутизатора. Поэтому, когда происходит переброс, подключения блокируются по времени и дают отказ.

В ПО Cisco IOS версии 12.2(13)T и позднее можно настроить функцию Stateful Failover of Network Address Translation для обеспечения избыточности впесте с протоколом HSRP. Дополнительная информация содержится в документе NAT - Поддержка отображения статических таблиц NAT с помощью HSRP для обеспечения высокой доступности.

В. Поддерживает ли Cisco IOS NAT входящие преобразования на последовательной магистрали, использующей Frame Relay, и исходящую трансляцию на стороне Ethernet?

Ответ. Да.

В. Может ли один маршрутизатор, поддерживающий NAT, позволить некоторым пользователям использовать NAT, а другим пользователям в том же интерфейсе Ethernet продолжать работать с их собственными IP-адресами?

Ответ. Да. Это возможно с помощью списка управления доступом ACL, в которых представлены наборы узлов или сетей, для которых необходимо преобразование NAT. Все сеансы на одном и том же узле будут либо преобразованы, либо пройдут через маршрутизатор без преобразования.

ACL, расширенные ACL и карты маршрутов можно использовать для определения правил трансляции IP-устройств. Всегда задавайте сетевой адрес и соответствующую маску подсети. Не используйте ключевое слово "**any**" вместо сетевого адреса и маски подсети.

```
ip nat inside source static 10.1.1.10 140.16.1.254
!--- Статическое преобразование для сервера ns.bar.com DNS.

ip nat outside source static 10.1.1.10 192.168.1.254
!--- Статическое преобразование для сервера ns.foo.com DNS.

ip nat pool iga 140.16.1.1 140.16.1.253 netmask 255.255.255.0
!--- Динамическая команда IL->IG address xlations.

ip nat pool ola 192.168.1.1 192.168.1.253 netmask 255.255.255.0
!--- Динамическая команда OG->OL address xlations.

ip nat inside source list 1 pool iga
ip nat outside source list 2 pool ola
access-list 1 permit 10.2.17.0 .255.255.255.0
!--- Преобразовать весь трафик, поступающий с внутренних узлов 10.2.17.

access-list 2 permit 10.0.0.0 255.0.0.0
!--- Преобразовать весь трафик, созданный извне.
```

В. Что такое перегрузка PAT или NAT?

Ответ. PAT, или перегрузка NAT, — это функция NAT в Cisco IOS, которую можно использовать для трансляции внутренних (внутренних локальных) частных адресов в один или несколько внешних (внутренних глобальных, обычно зарегистрированных) IP-адресов. Уникальные номера портов источника для каждого преобразования позволяют отличать один диалог от другого.

При перегрузке NAT создается запись таблицы преобразования, содержащая полный адрес и информацию об исходном порте.

В. Каково максимальное количество переводов, которое может быть выполнено для каждого внутреннего IP адреса при конфигурировании для PAT (перегрузка трансляции сетевых номеров)?

Ответ. PAT (перегрузка NAT) разделяет доступные порты в соответствии с глобальными IP-адресами на три диапазона: 0-511, 512-1023 и 1024-65535. PAT (перегрузка NAT) присваивает уникальный исходный порт для каждого протокола дейтаграммы пользователя (UDP) или сеансов протокола управления передачей (TCP). Он пытается присвоить одно и то же значение порта исходного запроса. Однако если исходный порт уже используется, будет произведено сканирование от начала определенного диапазона портов для поиска первого доступного порта и его назначения для разговора.

B. Принципы работы трансляции адресов портов.

Ответ. PAT с одним IP-адресом:

1. NAT/PAT проверяет трафик и находит соответствия с правилом преобразования.
2. Это правило соответствует конфигурации PAT.
3. Известен ли PAT тип трафика, и есть ли у этого типа трафика конкретный набор портов или согласуемых им портов, которые он будет использовать? Если это так, не распределяйте их в качестве уникальных идентификаторов.
4. Сессии без особых требований к портам стремятся разъединиться. PAT осуществляет преобразование IP-адреса источника и проверяет доступность исходного порта источника (например 433). Используются следующие группы: 1-511, 512-1023 и 1024-65535.
   Примечание: Для TCP и UDP используются следующие группы: 1-511, 512-1023, 1024-65535. Для ICMP первая группа начинается с 0.

5. Если запрошенный порт отправителя доступен, он присваивает порт источника и сеанс продолжается.
6. Если запрашиваемый исходный порт недоступен, NAT начинает поиск с начала соответствующей группы. В этом примере поиск начинается с 1 для TCP или UDP и с 0 для ICMP.
7. При наличии доступного порта выполняется назначение, и сеанс продолжается.
8. Если нет доступных портов, пакет отбрасывается.

A2. PAT с несколькими IP-адресами.

Используйте ту же логику, что и при одном IP-адресе (выше приведенные шаги 1-8) и:

1. Если в релевантной группе на первом IP-адресе недоступен ни один порт, NAT переходит на следующий IP-адрес в пуле и пытается выделить запрошенный порт источника.
2. Если запрошенный порт отправителя доступен, он присваивает порт источника и сеанс продолжается.
3. Если запрашиваемый исходный порт недоступен, NAT начинает поиск с начала соответствующей группы. В этом примере поиск начинается с 1 для TCP или UDP и с 0 для ICMP.
4. При наличии доступного порта выполняется назначение, и сеанс продолжается.
5. Если доступных портов нет, а в пуле нет другого IP-адреса, то пакет отбрасывается, и так до тех пор, пока не будут проверены все IP-адреса.

B. Каково максимальное число реконфигурируемых IP пулов NAT (используя команду ip nat pool <name>)?

Ответ. Ограничения не существует. Впрочем, на практике максимальное число настраиваемых IP-пулов ограничивается объемом свободной памяти DRAM на конкретном используемом маршрутизаторе.

B. Что означает наложение IP-адресов в контексте NAT?

Ответ. Совмещение IP-адреса относится к ситуации, когда два местоположения для внутреннего соединения между собой используют схему одного IP-адреса. Это не стандартная ситуация и происходит чаще всего при слиянии компаний или

приобретении одной компанией другой. Без специальной поддержки установка связи и сеансов между двумя расположениями невозможна. Перекрывающиеся IP-адреса могут быть публичными адресами, назначенными другим компаниям, частными адресами, уже назначенными другим компаниям, или входить в диапазон частных адресов, как определено в RFC 1918 . Частные IP-адреса не являются маршрутизируемыми и требуют преобразований NAT для подключения к внешнему миру. Решение подразумевает перехват ответов на запросы имени DNS от внешней среды к внутренней, настройку преобразования внешнего адреса и корректировку ответа DNS перед пересылкой его на внутренний хост. Чтобы позволить пользователям подключаться к обеим сетям, необходимо использовать сервер DNS на обеих сторонах устройства NAT.

Преобразование NAT может проверять и выполнять преобразование адресов для содержимого DNS A и записей PTR. Подробнее см. в документе Использование NAT в перекрывающихся сетях.

B. Можно ли создать конфигурацию с динамической и статической трансляцией сетевых адресов?

Ответ. Да, это возможно. Ограничение, которое глобальные адреса используют в статических преобразованиях, не исключаются автоматически с помощью динамических пулов, содержащих эти глобальные адреса. Необходимо создать динамические пулы, чтобы исключить адреса, назначенные через статические записи.

B. Может ли Cisco IOS поддерживать множественные внешние таблицы NAT?

Ответ. Да, это можно сделать с помощью карт маршрутов. Команда динамического преобразования **dynamic translation** может теперь указать карту маршрутов, которая обрабатывается вместо ACL. Карта маршрута позволяет пользователю подбирать комбинации ACL, IP-адресов следующего узла и выходных интерфейсов, чтобы определить, какой пул нужно использовать. Дополнительная информация о настройке NAT с помощью карт маршрута содержится в документе Поддержка преобразования сетевых адресов (NAT) для нескольких пулов с использованием карт маршрутов.

Вопрос:Почему нужно указывать маску подсети при настройке пула адресов NAT?

Ответ. Маска подсети используется для проверки адресов, назначенных из пула (то есть, к примеру, не нужно назначать широковещательные адреса подсети). Маска подсети должна совпадать с размером подсети, в которую производится преобразование.

B. Можно ли распределить IP-адреса из подсети внешнего интерфейса маршрутизатора NAT динамическому пулу NAT?

Ответ. Да. Маршуртизатор NAT отвечает на запросы ARP к этим IP-адресам в динамическом пуле.

B. Правильно ли обрабатывает маршрутизатор NAT перенаправления протокола ICMP?

Ответ. Да

В. Поддерживает ли Cisco NAT весь трафик приложения?

Ответ. Трафик приложения прозрачен для Cisco IOS NAT, если не выполняются следующие условия:

- В части данных встроены IP-адреса.
- Приложение требует предварительно заданных или согласованных значений порта источника/назначения.

NAT Cisco IOS выполняет проверку трафика "потоком" и должен обладать информацией обо всех приложениях, которые встроены и/или для которых необходимы конкретные порты источника.

К примеру, Cisco поддерживает преобразование встроенных IP-адресов в записях DNS A и PTR, а также поддерживает FTP и NetMeeting версии 2.11 (4.3.2519) и 3.01 (4.4.3385), выделяя необходимые для них значения исходного порта. Cisco не назначает эти значения при использовании PAT или функции перегрузки Cisco IOS NAT.

При работе со встроенными IP-адресами Cisco IOS NAT должен обладать информацией о сообщениях, которые содержат встроенные адреса и о смещении в этих сообщениях. Если встроенные адреса совпадают с настроенными правилами, они транслируются в соответствии с конфигурацией. Приложение, внедряющее IP-адреса (о которых Cisco IOS NAT не известно), не будет нормально работать в конфигурации Cisco IOS NAT.

Возможно исключение при использовании туннельного протокола, например протокол туннельного соединения двух точек (PPTP). В данном случае встроенный IP-адрес пакетов, проходящих по туннелю, не будет транслироваться. Однако у пользователя есть виртуальное расширение домашней сети, и он использует схему адресации домашних сетей. Если пользователю требуется выйти за пределы домашней сети, он может выбрать использование NAT.

Проблема встроенных IP-адресов существует вне зависимости от настроенного типа трансляции NAT в Cisco IOS (простая, расширенная, перегрузка и т. д.).

При преобразовании пакетов, направленных на хорошо известные порты, NAT проверяет полезную информацию пакетов, преобразовывает встроенные IP-адреса и создает полностью расширенное преобразование. Это происходит в статических и динамических конфигурациях NAT. Этот набор функций выполняется на пути с коммутацией процессов и является стандартным поведением для всех протоколов, для которых необходимо преобразование встроенных IP-адресов, включая FTP, DNS, IRC, SNMP, LDAP, H.323 и SIP.

Предварительно настроенные или согласованные значения портов источника учитываются только при использовании PAT или функции перегрузки Cisco IOS NAT. PAT мультиплексирует множественные преобразования IP с помощью 1 или нескольких IP-адресов, а также использует исходный порт для точной идентификации преобразований для каждого IP-адреса. Функция PAT должна выделить все известные значения портов на тот случай, если происходит преобразование этих типов приложений (FTP, NetMeeting и т.д.).

В. Почему Cisco IOS NAT не поддерживает трафик SNMP?

Ответ. Формат пакета SNMP зависит от используемого MIB и не может определяться самостоятельно. Нет единого формата для запросов и ответов SNMP, который можно обрабатывать обычным путем.

В. Как обрабатываются протоколы ARP для IP-адресов, созданных NAT?

Ответ. Cisco IOS NAT создает запись ARP для IP-адресов, созданных NAT, указывающих на MAC-адрес интерфейса, с которыми связан пул IP-адресов NAT.

Например, при выполнении внутреннего преобразования источника, если внутренний пул глобальных адресов связан с подсетью внешнего интерфейса (например, S0), то тогда записи ARP для этих IP-адресов будут использовать MAC-адреса S0.

B. Поддерживает ли Cisco IOS NAT запросы DNS?

Ответ. Да, Cisco IOS NAT не преобразовывает адреса, которые появляются в ответах DNS на поиск имени (запросы A) и инверсивные запросы (запросы PTR). Таким образом, внешний хост отправляет внутреннему DNS-серверу запрос на поиск имени, и этот сервер отвечает внутренним адресом, программа NAT преобразует этот локальный адрес в глобальный. Противоположное поведение также встречается при поддержке Cisco совпадающих IP-адресов. Внутренний хост запрашивает внешний сервер DNS, ответ содержит адрес, соответствующий списку управления доступом, указанному в команде outside source, и код преобразует внешний глобальный адрес во внешний локальный адрес.

Значения TTL на всех записях ресурсов (RR) DNS, которые получают преобразования адресов в полезных сведениях RR, автоматически приравниваются к нулю.

Cisco IOS NAT не преобразовывает IP-адреса, встроенные в зону передачи DNS.

B. Поддерживает ли Cisco IOS NAT списки управления доступом, которые разрешают выход в Интернет некоторым или всем пакетам?

Ответ. При настройке Cisco IOS NAT для динамического преобразования NAT, для идентификации пакетов, которые могут быть преобразованы, используется список управления доступом. Текущая архитектура NAT не поддерживает использование какого-либо или всех пакетов в ACL, используемых NAT. Использование всех или некоторых пакетов может привести к неожиданному поведению.

B. Почему активный FTP работает со статической / расширенной (переадресацией) и не работает с PAT?

Ответ. Причина в том, что при открытии доступа FTP происходит подключении к порту 21 удаленного сервера FTP. Но при использовании команд "ls", "put", get" или других, для которых необходимо порт данных, сервер устаналивает другое соединение с клиентом. При открытии исходного соединения FTP изнутри маршрутизатор распознает этот запрос в качестве определенного внешнего IP-адреса и выбирает случайный номер порта, в этом случае сервер FTP общается с этим IP-адресом и номером порта. Следовательно, когда сервер хочет вновь открыть подключение данных при использовании команд "get" or "ls" и т.д., он пытается открыть подключение TCP с порта 20 на какой-либо случайный порт, который выбирает сервер. В то время как сервер считает, что общается с внешним IP-адресом, маршрутизатор определяет трафик, направляемый на внешний IP-адрес, но не может найти соответствия PAT с номером порта, выбранным сервером. Следовательно, он не определяет, что данный трафик должен вернуться к клиенту.

Порт 20 не устанавливается. Чтобы решить эту проблему, можно использовать режим "passive FTP". Этот режим заставляет клиента открыть соединения через порты 21 и 20 с самого начала. Маршрутизатор видит оба порта и позволяет серверу открыть порт 20.

Дополнительная информация о сервер FTP содержится в документе Анализ протокола FTP .

Необходимо провести расширенные преобразования для портов 20 и 21 со статическими отображениями (пример адреса)

```
ip nat inside source static tcp 192.168.0.4 20 66.46.64.82 20 extendable
ip nat inside source static tcp 192.168.0.4 21 66.46.64.82 21 extendable
```

Режим, в котором работает активный FTP, не позволяет использовать динамический NAT. В этом случае может использоваться только статический NAT. Это ограничение FTP.

Дополнительные сведения

- **Страница поддержки технологии NAT**
- **Техническая поддержка и документация - Cisco Systems**

Дата генерации PDF файла: Jan 05, 2010

---

http://www.cisco.com/support/RU/customer/content/9/92029/nat-faq.shtml

---