Network Working Group
Request for Comments: 3715
Category: Informational

B. Aboba
W. Dixon
Microsoft

March 2004

Требования по совместимости для трансляции IPsec NAT

IPsec-Network Address Translation (NAT) Compatibility Requirements

Статус документа

Этот документ содержит информацию для сообщества Internet и не задает каких-либо стандартов Internet. Документ может распространяться свободно.

Тезисы

В этом документе описаны известные случаи несовместимости между NAT[1] и IPsec, а также приведены требования по решению этой проблемы. Возможно наиболее распространенным применением IPsec является организация виртуальных частных сетей (VPN[2]). Одним из популярных приложений технологии VPN является обеспечение доступа удаленных пользователей в корпоративную сеть Intranet. Сегодня трансляторы NAT широко используются на домашних шлюзах, а также в других местах, откуда могут подключаться удаленные пользователи (гостиницы, кафе и т. п.). В результате несовместимости IPsec-NAT становятся основным препятствием распространению и практическом использованию технологий IPsec.

Оглавление

1. Введение

Возможно наиболее распространенным применением IPsec [RFC2401] являются виртуальные частные сети (VPN). Одним из наиболее популярных вариантов применения VPN является предоставление удаленным пользователям доступа в корпоративные сети Intranet. В настоящее время трансляторы сетевых адресов (NAT), как описано в [RFC3022] и [RFC2663], широко используются в домашних шлюзах, а также в других местах, откуда могут подключаться удаленные пользователя (например, в гостиницах). В результате несовместимости IPsec-NAT становятся главным препятствием распространению IPsec в одном из основных приложений. В этом документе описаны несовместимости между NAT и IPsec, а также требования по их преодолению.

1.1. Описание требований

Ключевые слова **возможно** (MAY), **необходимо** (MUST), **недопустимо** (MUST NOT), **необязательно** (OPTIONAL), **рекомендуется** (RECOMMENDED), **следует** (SHOULD), **не нужно** (SHOULD NOT) в данном документе интерпретируются в соответствии с [RFC2119].

Следует отметить, что приведенные в этом документе требования используются при оценке представляемых протоколов. По этой причине язык описания требований относится к возможностям таких протоколов, спецификации протоколов будут определять, какие из возможностей являются обязательными, рекомендуемыми или опциональными. Например, требование поддержки протоколом защиты конфиденциальности не тождественно требованию поддержки им шифрования.

Протокол считается не соответствующим требованиям, если в нем не выполняется одно или множество требований уровня **должно** или **недопустимо** для реализованных в протоколе возможностей. Протокол считается безусловно

[1]Network Address Translation — трансляция сетевых адресов.
[2]Virtual Private Network.

соответствующим, если в нем выполняются все требования уровня **должно**, **недопустимо**, **следует** и **не следует**. Если выполняются все требования уровня **должно** и **недопустимо**, но только часть требований уровня **следует** и **не следует**, протокол считается условно соответствующим.

2. Известные несовместимости между NA(P)T и IPsec

Несовместимости между NA(P)T и IPsec можно разделить на три категории, указанных ниже.

1) Внутренние проблемы NA(P)T. Несовместимости этого типа непосредственно связаны с функциональностью NA(P)T, описанной в [RFC3022], и, следовательно, присущи всем устройствам NA(P)T.

2) Недостатки реализации NA(P)T. Такие несовместимости не присущи природе NA(P)T, но присутствуют во многих реализациях NA(P)T. В эту категорию входит обработка входящих и исходящих фрагментов. Поскольку эти проблемы не связаны непосредственно с природой NA(P)T, они могут быть устранены в будущих реализациях NA(P)T. Однако в силу широкого распространения проблемных устройств их нужно принимать во внимание при реализации решений для работы через устройства NA(P)T.

3) Проблемы с «помощниками» (Helper). Эти несовместимости присутствуют в устройствах NA(P)T, которые пытаются побеспечить работу IPsec через трансляторы NA(P)T. Ирония состоит в том, что такие «помощники» создают новые проблемы совместимости, осложняя решение уже имевшихся проблем. Хотя функциональность «помощников» в работе IPsec через NA(P)T присутсвтует не во всех трансляторах, эти функции получили достаточное распространение и их нужно принимать во внимание при реализации решений для работы через устройства NA(P)T.

2.1. Внутренние проблемы NA(P)T

Присущие NA(P)T проблемы совместимости перечислены ниже.

a) Несовместимость IPsec AH [RFC2402] и NAT. Поскольку заголовок AH включает адреса отправителя и получателя в код контроля целостности, устройства NAT (включая reverse NAT), меняющие поля адресов, будут нарушать работу контроля целостности пакетов. Поскольку IPsec ESP [RFC2406] не включает адреса отправителя и получателя в код контроля целостности сообщений, этой проблемы не возникает для ESP.

b) Несовместимость контрольных сумм и NAT. Контрольные суммы TCP и UDP зависят от IP-адресов отправителя и получателя по причине включения «псевдозаголовка» в расчет контрольных сумм. В результате, при расчете и проверке контрольных сумм после прохождения через трансляторы NAT будет возникать отказ.

   По этой причине IPsec ESP[1] будет беспрепятственно работать через NAT только в случаях использования протоколов, отличных от TCP/UDP (например, туннельный режим IPsec или GRE с защитой IPsec), или отказа от проверки контрольных сумм (это возможно в IPv4 UDP). Как описано с [RFC793], расчет и проверка контрольных сумм TCP являются обязательными для протокола IPv4, а в IPv6 требуется расчет и проверка контрольных сумм UDP/TCP.

   Протокол SCTP[2], как определено в [RFC2960] и [RFC3309], использует алгоритм CRC32C только для пакета SCTP (общий заголовок и блоки данных), не включая заголовка IP. В результате трансляторы NAT не препятствуют использованию SCTP CRC и проблем не возникает.

   Отметим, что в результате защиты целостности и аутентификации трафика в транспортном режиме IPsec с использованием сильной криптографии изменение пакетов может быть обнаружено до проверки контрольных сумм UDP/TCP. Таким образом, проверка контрольных сумм в этом случае служит лишь для обнаружения ошибок при внутренней обработке.

c) Несовместимость адресных идентификаторов IKE с NAT. При использовании адресов IP в качестве идентификаторов на фазах 1 или 2 протокола IKE[3] [RFC2409] изменение адресов отправителя или получателя трансляторами NAT (или reverse NAT) будет приводить к несоответствию между протокольными идентификаторами и адресами в заголовках IP. В соответствии с [RFC2409] реализации IKE должны отбрасывать такие пакеты.

   Для отказа от применения адресов IP в качестве идентификаторов IKE (фаза 1 и фаза 2), можно воспользоваться значениями userID или именами FQDN[4]. Если желательна аутентификация пользователей, можно воспользоваться идентификаторами типа ID_USER_FQDN, описанными в [RFC2407]. Если желательна аутентификация машин, можно воспользоваться идентификаторами типа ID_FQDN. В любом случае требуется проверить, был ли предложенный идентификатор аутентифицирован в результате обработки сертификата конечного объекта (end-entity), если фаза 1 включает обмен сертификатами. Хотя использование идентификаторов типа USER_FQDN или FQDN возможно в IKE, существуют варианты (например, записи SPD[5] для подсетей), препятствующие такому применению.

   Поскольку в фазе 2 адреса отправителя зачастую применяются для формирования полных 5-элементных входящих селекторов SA, адрес получателя, протокол и номера портов отправителя и получателя могут использоваться в селекторах, чтобы не ослаблять обработку входящих SA.

d) Несовместимость фиксированных портов отправителя в IKE с NAPT. Когда множество расположенных за транслятором NAPT хостов инициирует связи IKE SA с одним ответчиком, требуется механизм, позволяющий устройству NAPT демультиплексировать входящие пакеты IKE от такого ответчика. Обычно это выполняется путем трансляции порта отправителя IKE UDP на исходящие пакеты от инициатора. В этом случае ответчики должны быть способны воспринимать пакеты IKE из порта отправителя UDP, отличающегося от 500 и передавать отклики в этот же порт. Здесь требуется аккуратность для предотвращений неожиданностей при

[1] Encapsulating Security Payload — инкапсулированные защищенные данные.
[2] Stream Control Transmission Protocol — протокол управления передачей потоков.
[3] Internet Key Exchange — обмен ключами в Internet.
[4] Полное доменное имя. *Прим. перев.*
[5] Security Policy Database — база данных о правилах безопасности.

смене ключей. Если «плавающий» порт отправителя не применяется в качестве порта получателя при смене ключа, транслятор NAT может оказаться не способным к передаче пакетов смены ключей нужному адресату.

e) Несовместимость между перекрывающимися записями SPD и NAT. При использовании хостами-инициаторами, расположенными за NAT своих адресов отправителя в качестве идентификаторов в фазе 2 возможно согласование перекрывающихся записей SPD с общим IP-адресом ответчика, который в таких случаях может передавать пакеты не в ту IPsec SA. Это обусловлено тем, что для отвечающего разные IPsec SA будут казаться эквивалентными, поскольку они соединяют одни и те же конечные точки и могут использоваться для передачи одного и того же трафика.

f) Несовместимость выбора IPsec SPI с NAT. Поскольку трафик IPsec ESP зашифрован и непрозрачен для NAT, трансляторы NAT должны использовать элементы заголовков IP и IPsec для демультиплексирования входящего трафика IPsec. Для этого обычно применяется комбинация IP-адреса получателя, протокол защиты (AH/ESP) и IPsec SPI.

Однако по причине независимого выбора входящих и исходящих SPI транслятор NAT не имеет возможности определить соответствие входящих SPI хостам-адресатам, проверяя лишь исходящий трафик. Таким образом, когда два расположенных за NAT хоста пытаются одновременно организовать связи IPsec SA с одним адресатом, транслятор NAT может доставлять входящие пакеты IPsec не тому получателю.

Отметим, что это является несовместимостью не с IPsec, самой по себе, а с типичными способами реализации. В протоколах AH и ESP передающий хост указывает значение SPI для использования в данной защищенной связи SA и выбор этого значения важен лишь для получателя. В настоящее время комбинации Destination IP, SPI и Security Protocol (AH, ESP) уникально идентифицируют защищенные связи SA. Значения SPI из диапазона 1 - 255 зарезервированы агентством IANA и могут быть использованы в будущем. Это означает, что при согласовании с одним внешним хостом или шлюзом внутренние хосты, расположенные за одним устройством NAPT могут выбрать одинаковые значения SPI - например, у одного хоста будет входящая SA с (SPI=470, Internal Dest IP=192.168.0.4), а у другого - с (SPI=470, Internal Dest IP=192.168.0.5). Принимающий пакеты транслятор NAPT не сможет определить какие из входящих пакетов IPsec с SPI=470 кому пересылать из этих двух хостов.

Принимающий хост может также выделить уникальное значение SPI для каждой индивидуальной (unicast) связи SA. В этом случае адрес Destination IP требуется проверять только для того, чтобы увидеть, является ли он индивидуальным адресом IP для данного хоста и не нужна проверка указания этого адреса удаленным хостом в поле Destination IP. Используя такой метод, транслятор NA(P)T может обеспечить малую (но отличную от 0) вероятность пересылки пакетов не тому внутреннему хосту даже при организации несколькими внутренними хостами связей SA с одним внешним хостом.

Такое решение полностью совместимо с предшествующими версиями и требует на конкретном принимающем хосте лишь изменения политики выделения SPI и кода IPsec_esp_input(). Однако устройства NA(P)T могут оказаться не способны детектировать такое поведение без проблем, связанных с разбором элементов данных IKE. А от хоста может потребоваться использование резервных значений SPI из числа выделенных IANA.

g) Несовместимость вложенных адресов IP с NAT. Поскольку данные защищены криптографически, все адреса IP, вложенные в пакеты IPsec, не будут транслироваться устройствами NAT. Это препятствует работе шлюзов прикладного уровня (ALG[1]), реализуемых в трансляторах NAT. К протоколам, использующим вложенные адреса IP относятся FTP, IRC, SNMP, LDAP, H.323, SIP, SCTP (не всегда) и многие игры. Для решения этой проблемы требуется устанавливать шлюзы ALG на хостах или защитных шлюзах, которые могут обрабатывать трафик приложений до инкапсуляции IPsec и после декапсуляции IPsec.

h) Неявная направленность NA(P)T. Трансляторы NA(P)T зачастую требуют прохождения через них начального исходящего пакета для создания входного отображения. Направленность препятствует незапрошенной организации связей IPsec SA для хостов, расположенных за устройством NA(P)T.

i) Проверка входных селекторов SA. В предположении, что IKE согласует селекторы фазы 2, обработка входных SA будет приводить к отбрасыванию декапсулированного пакета, поскольку [RFC2401] требует соответствия адреса отправителя пакета значению селектора SA, которое NA(P)T будет менять при обработке пакетов ESP.

2.2. Недостатки реализаций NA(P)T

Ниже перечислены проблемы, встречающиеся во многих реализациях NA(P)T.

j) Неспособность обслуживания трафика, отличного от UDP/TCP. Некоторые системы NA(P)T отбрасывают трафик, не относящийся к UDP/TCP, или выполняют трансляцию только адресов в случаях, когда за NAT находится единственный хост. Такие системы NAPT не поддерживают трафик SCTP, ESP (протокол 50) и AH (протокол 51).

k) Тайм-ауты отображений NAT. Трансляторы NA(P)T различаются по времени, в течение которого будет поддерживаться отображения UDP при отсутствии трафика. В результате даже при корректной трансляции пакетов IKE возможно преждевременное удаление состояний трансляции.

l) Невозможность обработки исходящих фрагментов. Большинство трансляторов NA(P)T могут корректно фрагментировать исходящие пакеты IP в тех случаях, когда размер пакета превышает значение MTU на выходном интерфесе. Однако корректная трансляция исходящих пакетов, которые уже были фрагментированы, достаточно сложна и многие устройства NAPT не поддерживают этого. Как отмечено в параграфе 6.3 работы [RFC3022], в случае, когда два хоста передают фрагментированные пакеты одному получателю, идентификаторы фрагментов могут перекрываться. Поскольку хост-получатель использует при сборке идентификаторы и смещения фрагментов, результатом такого перекрытия будет повреждение данных. Некоторые трансляторы NA(P)T обеспечивают защиту от описанного перекрытия с помощью трансляции идентификаторов фрагментов. Конфликты идентификаторов не вызывают проблем в тех случаях, когда фрагментацию выполняет сам транслятор NAT, поскольку уникальность идентификаторов должна обеспечиваться только для данной пары адресов отправителя и получателя.

[1]Application Layer Gateway.

Поскольку фрагмент может иметь размер даже в 68 октетов (или больше) [RFC791], нет гарантии присутствия в первом фрагменте полного заголовка TCP. Поэтому транслятору NA(P)T для перерасчета контрольной суммы TCP может потребоваться изменение следующего фрагмента. Поскольку порядок следования фрагментов может нарушаться, а адреса IP могут оказаться в разных фрагментах (даже один адрес может быть разделен), транслятору NA(P)T потребуется выполнить сборку фрагментов для выполнения трансляции. Далеко не все устройства NA(P)T поддерживают это.

m) Невозможность обработки входящих фрагментов. Поскольку полный заголовок IP/UDP/SCTP/TCP обычно содержится лишь в первом фрагменте, от устройств NAPT требуется способность трансляции на основе адресов отправителя и получателя, а также по идентификаторам фрагментов. Поскольку порядок следования фрагментов может нарушаться, заголовки для фрагмента с данным идентификатором могут быть не известны на момент его прибытия. Кроме того, заголовок может оказаться разделенным между фрагментами. В результате устройству NAPT потребуется перед трансляцией выполнить полную сблорку пакета, что поддерживают далеко не все устройства NAPT.

   Отметим, что в NAT адресов отправителя и получателя достаточно для трансляции и описанной проблемы не возникает. Однако заголовки IPsec и IKE могут быть разделены между фрагментами и сборка снова потребуется.

2.3. Несовместимости «помощников»

Ниже перечислены несовместимости IPsec с функциональностью «помощников» NAT.

n) Проверка заголовков ISAKMP[1]. Сегодня некоторые реализации NAT пытаются использовать значения IKE cookie для демультиплексирования трафика IKE. Как и при демультиплексировании по порту отправителя такое решение сталкивается с проблемами при смене ключей, поскольку в фазе 1 при смене ключей используются обычно не те значения cookie, которые применялись для предшествующего трафика.

o) Специальная трактовка для порта 500. Поскольку некоторые реализации IKE не могут работать с портами отправителя, отличными от UDP 500, некоторые устройства NAT не транслируют пакеты, отправленные из порта UDP 500. Это означает, что такой транслятор NAT не позволит работать нескольким клиентам IPsec с одним удаленным шлюзом, если он не обрабатывает заголовки ISAKMP для работы со значениями cookie, что создает другую проблему, описанную выше.

p) Проверка данных ISAKMP. Реализации NA(P)T, пытающиеся разбирать элементы данных ISAKMP, могут не обрабатывать все комбинации порядка этих элементов или не поддерживать элементы vendor_id для согласования опции IKE.

3. Требования по совместимости IPsec-NAT

Решение по совместимости IPsec-NAT предназначено для расширения сферы применения функциональности IPsec за пределы использования решения на основе совместимых с NAT туннелей IPsec, описанного в параграфе 2.3.

При оценке решений для совместимости IPsec-NAT следует принимать во внимание перечисленные ниже аспекты.

Развертывание

Поскольку IPv6 будет решать проблему нехватки адресов, зачастую вынуждающую использовать NA(P)T для IPv4, вопрос совместимости IPsec-NAT можно считать временным, решение которого нужно лишь до широкого развертывания IPv6. Следовательно, для того, чтобы решение IPsec-NAT было полезным, оно **должно** быть развернуто до перехода на IPv6.

Поскольку развертывание IPv6 требует изменений как на маршрутизаторах, так и на хостах, требующие подобных изменений решения по совместимости IPsec-NAT будут разворачиваться примерно с такой же скоростью, как IPv6. По этой причине для совместимости IPsec-NAT **следует** находить решения, которые потребуют изменений только на хостах без изменения в маршрутизаторах.

Наряду с прочим это означает, что решению по совместимости IPsec-NAT **не следует** требовать коммуникаций между хостом и транслятором NA(P)T, поскольку такое взаимодействие потребует изменения трансляторов NA(P)T и проверки интероперабельности между реализациями хостов и NA(P)T. Для быстрого развертывания требуется решение, которое будет работать с имеющимися маршрутизаторами и трансляторами NA(P)T в уже развернутой инфраструктуре.

Совместимость протоколов

От решения по работе IPsec через NAT не ожидается решение проблем для протоколов, которые не могут работать через трансляторы NA(P)T без защиты IPsec. Следовательно, сохранится потребность в шлюзах ALG для некоторых протоколов даже при наличии решения для работы IPsec через трансляторы NAT.

Безопасность

Поскольку NA(P)T напрямую обслуживает функции защиты, решениям по работе IPsec через NA(P)T не следует пропускать произвольный входящий трафик IPsec или IKE с любого адреса IP на хост за транслятором NA(P)T, хотя после организации двухсторонней связи IKE и IPsec следует сохранять отображение.

Удаленные пользователи

Поскольку основным применением IPsec является удаленный доступ в корпоративные сети (Intranet), решение для работы через трансляторы NA(P)T **должно** поддерживать туннельный режим IPsec или транспортный режим L2TP over IPsec [RFC3193], включая возможность прохождения через множество трансляторов NA(P)T между удаленным клиентом и шлюзом VPN.

[1] Internet Security Association and Key Management Protocol — протокол защищенных связей и обмена ключами в Internet.

Клиент может иметь маршрутизируемый адрес, а шлюз VPN может размещаться за одним или несколькими трансляторами NA(P)T или оба (клиент и шлюз VPN) могут находиться за одним или множеством трансляторов NA(P)T. Удаленные пользователи, подключающиеся к одному шлюзу VPN, могут работать с одинаковыми приватными адресами IP, находясь каждый за своим устройством NA(P)T, или множество удаленных пользователей может находиться в частной сети за одним транслятором NA(P)T с выдачей каждому уникального приватного адреса. Поскольку IKE использует порт UDP 500 для получателя, не требуется применять множество шлюзов VPN, расположенных за общим внешним адресом IP.

Взаимодействие между шлюзами

В варианте «шлюз-шлюз» между корпоративной сетью и Internet может размещаться сеть с адресами из приватного блока (DMZ[1]). В таких случаях защитные шлюзы IPsec, подключающие части корпоративной сети, могут размещаться в DMZ и использовать приватные адреса на своих внешних (в DMZ) интерфейсах. Транслятор NA(P)T соединяет сеть DMZ с Internet.

Сквозное взаимодействие

Решение NAT-IPsec **должно** разрешать защищенные коммуникации TCP/IP между парами хостов с использованием IPsec, а также коммуникации между хостами и шлюзами. Хост частной сети **должен** быть способен организовать одно или множество защищенных с помощью IPsec соединений TCP или сессий UDP с другим хостом, отделенным от первого одним или множеством устройств NA(P)T. Например, трансляторы NA(P)T могут размещаться в сетях филиалов, соединенных с корпоративной сетью, а также в центральном офисе для подключения корпоративной сети к Internet. Точно также трансляторы NA(P)T могут развертываться в корпоративной сети для беспроводного подключения или доступа удаленных клиентов. Это может потребовать на хосте специальной обработки трафика TCP и UDP.

Организация соединений SCTP с другим хостом через один или множество трансляторов NA(P)T может создавать дополнительные проблемы. Протокол SCTP поддерживает многодомность. Если применяется более одного адреса IP, эти адреса передаются, как часть пакета SCTP в процессе создания ассоциации (в блоках INIT и INIT-ACK). Для случая использования только однодомных конечных точек SCTP в параграфе 3.3.2.1 работы [RFC2960] сказано:

Отметим, что отсутствие параметров IP address в блоках INIT и INIT-ACK упрощает организацию ассоциаций при работе с использованием NAT.

Это означает, что без необходимости адреса IP не следует помещать в пакеты SCTP. Если присутствует транслятор NAT и адреса IP помещены в пакет, организация соединения завершится отказом. Недавно было внесено предложение [AddIP], позволяющее менять адрес IP после создания ассоциации. Сообщения о таком изменении также передают адреса IP в пакете SCTP и это будет вызывать конфликт с трансляторами NAT.

Совместимость с межсетевыми экранами

По причине широкого использования межсетевых экранов решение для совместимости NAT-IPsec **должно** позволять администраторам этих экранов создавать простые, статические правила доступа, разрешающие или запрещающие трафик IKE и IPsec, проходящий через трансляторы NA(P)T. Это позволяет, например, избежать динамического выделения портов получателя для IKE и IPsec.

Масштабирование

Решение проблемы совместимости IPsec-NAT должно подходить для использования в системах с тысячами удаленных пользователей. В таких ситуациях нельзя предполагать, что единственный хост работает с данным получателем в каждый момент времени. В силу этого решение по совместимости IPsec-NAT **должно** решать вопрос перекрывающихся записей SPD и демультиплексирования входящих пакетов.

Поддержка режимов

По минимуму решение для совместимости IPsec-NAT **должно** поддерживать работу режимов IKE и IPsec, требуемых в [RFC2409] и [RFC2401]. Например, шлюз IPsec **должен** поддерживать туннельный режим ESP через трансляторы NA(P)T, а хост IPsec **должен** поддерживать работу через NA(P)T в транспортном режиме IPsec. Целью AH является защита неизменяемых полей в заголовках IP (включая адреса), а NA(P)T транслирует адреса, аннулируя проверку целостности AH. В результате NA(P)T и AH принципиально не совместимы и поэтому не вводится требования поддержки решением по совместимости IPsec-NAT протокола AH в транспортном или туннельном режиме.

Совместимость и взаимодействие со старыми версиями

Решение IPsec-NAT **должно** быть совместимо с имеющимися реализациями IKE/IPsec, чтобы они могли взаимодействовать через трансляторы NA(P)T, если таковые присутствуют. Это предполагает, что решение IPsec-NAT **должно** быть совместимо со старыми версиями IPsec [RFC2401] и IKE [RFC2409]. Кроме того, **следует** также обеспечивать возможность обнаружения устройств NA(P)T, чтобы решения NA(P)T не применялись без необходимости. Это означает, что **должна** обеспечиваться возможность определить, что существующая реализация IKE не поддерживает работу через NA(P)T, чтобы организовать работу IKE, как описано в [RFC2407], [RFC2408] и [RFC2409]. Отметим, что хотя это означает инициирование IKE через порт 500, требование выбора конкретного порта отправителя не задается, поэтому отправителю не обязательно использовать порт UDP 500.

Безопасность

Недопустимо внесение решением по совместимости IPsec-NAT дополнительных уязвимостей в защиту IKE или IPsec. Например, подходящее решение должно продемонстрировать, что оно не создает новых возможностей для атак на службы или использования обманок (spoofing). Протоколу IKE **должна** быть разрешена смена ключей, инициируемая любой стороной, как описано в [RFC2408].

[1] «Демилитаризованная» зона.

4. Существующие решения

4.1. Туннельный режим IPsec

В ограниченном числе случаев для работы через NA(P)T можно использовать туннельный режим IPsec (см., например, [DHCP]). Однако предъявляемые требования, перечисленные ниже, вносят существенные ограничения и не снижают потребности в общем решении.

1) IPsec ESP. Туннели IPsec ESP не учитывают внешний заголовок IP при расчете кода контроля целостности, поэтому трансляция адресов не приводит к отказам аутентификации. В туннелях IPsec не должна использоваться проверка контрольных сумм.

2) Отказ от проверки адресов. Большинство современных реализаций туннельного режима IPsec не проверяет адрес отправителя, поэтому несоответствие этих адресов с идентификаторами IKE не обнаруживается. Это создает уязвимости, описанные в разделе 5.

3) Записи Any to Any в SPD. Клиенты туннельного режима IPsec могут согласовывать SPD вида any to any (каждый с каждым), которые не становятся неприемлемыми в результате трансляции адресов, Это фактически исключает использование SPD для фильтрации туннелируемого трафика.

4) Работа с одним клиентом. Если за транслятором NAT размещается единственный клиент, риска перекрытия SPD не возникает. Поскольку устройству NAT не требуется разделять трафик между несколькими клиентами, не возникает риска при смене ключей или некорректного демультиплексирования входящих SPI и cookie.

5) Фрагментация. При использовании аутентификации по сертификатам может возникнуть потребность фрагментации пакетов IKE. Это может происходить при использовании цепочек сертификатов или даже обного сертификата, если размер ключа или иных полей сертификата (например, отличительное имя и другие расширения) достаточно велик. Однако при использовании аутентификации на основе заранее распространенного общего ключа вероятность фрагментации снижается.

6) Активные сессии. Большинство сессий VPN обычно поддерживают поток входящего трафика в течение всего срока существования, поэтому вероятность удаления отображений портов UDP в действующей сессии достаточно мала.

4.2. RSIP

Метод RSIP, описанный в [RSIP] и [RSIPFrame], включает механизмы для работы IPsec через трансляторы, описанные в [RSIPsec]. За счет поддержки связи между хостом и транслятором NA(P)T метод RSIP решает проблемы демультплексирования SPI и перекрытия SPD в приложениях IPsec. Метод подходит для использования в корпоративных и домашних сетях. Позволяя расположенным за транслятором NAT хостам использовать общий внешний адрес транслятора NA(P)T (шлюз RSIP), этот метод обеспечивает совместимость с протоколами, передающими вложенные в пакеты адреса IP.

За счет туннелирования пакетов IKE и IPsec метод RSIP позволяет обойтись без изменения протоколов IKE и IPsec, хотя в реализациях IKE и IPsec на хостах требуются серьезные изменения для обеспечения совместимости с RSIP. В результате будет обеспечиваться совместимость со всеми имеющимися протоколами (AH/ESP) и режимами (транспортный и туннельный).

Для обеспечения демультиплексирования при смене ключей IKE в RSIP требуется использовать «плавающий» порт отправителя IKE, а также смена ключей с «плавающим» портом. В результате совместимость с имеющимися реализациями IPsec не гарантируется.

RSIP не удовлетворяет требованиям к развертыванию решений по совместимости IPsec-NAT, поскольку хостам с поддержкой RSIP требуется соответствующий шлюз RSIP для организации IPsec SA с другим хостом. Поскольку RSIP требует менять только клиентов и маршрутизатора, а не серверы, это несколько снижает сложность развертывания по сравнению с IPv6. Однако от разработчиков реализация RSIP потребует существенной части ресурсовЮ нужных для поддержки IPv6. По этой причине RSIP может служить лишь временным решением, которое не имеет долгосрочной перспективы.

4.3. 6to4

Метод 6to4, описанный в [RFC3056], может служить основой для решения IPsec-NAT. В этой модели транслятор NAT обеспечивает хостам IPv6 префикс IPv6, созданный на основе внешнего адреса IPv4 транслятора NAT, и инкапсулирует пакеты IPv6 в IPv4 для передачи другим хостам или трансляторам 6to4. Это позволяет хостам IPv6, использующим IPsec, свободно обмениваться данными с другими хостами в облаке IPv6 или 6to4.

Решение 6to4 изящно и отказоустойчиво для случая одного транслятора NA(P)T между клиентом и шлюзом VPN, но оно не обеспечивает универсальности применения. Поскольку в 6to4 требуется выделение маршрутизируемого адреса IPv4 транслятору NA(P)T для того, чтобы он мог сформировать префикс IPv6, это решение не может быть использовано при наличии нескольких устройств NA(P)T между клиентом и шлюзом VPN. Например, трансляторы NA(P)T с приватными адресами на внешнем интерфейсе не могут использоваться находящимися за ними клиентами для получения префикса IPv6 с помощью 6to4.

Хотя 6to4 не требует существенной поддержки от хостов, которые уже поддерживают IPv6, этот метод требует существенного обновления трансляторов NAT. В результате 6to4 не может служить для быстрого решения проблемы.

5. Вопросы безопасности

По определению решение IPsec-NAT требует от всех хостов и маршрутизаторов, поддерживающих IPsec, способности безопасно обрабатывать пакеты, чьи заголовки IP не имеют криптографической защиты. Это вызывает множество проблем, которые требуется обсудить.

Поскольку IPsec AH не может работать через NAT, одним из побочных эффектов решения по совместимости IPsec-NAT может быть использование IPsec ESP с null-шифрованием (бех шифрования) взамен AH при наличии трансляторов

NAT между отправителем и получателем. Однако следует отметить, что ESP с null-шифрованием не обеспечивает таких же защитных свойств, как AH. Например, риски, связанные с IPv6 source routing, предотвращаются в AH, но сохраняются в ESP с null-шифрованием.

Кроме того, по причине отсутствия в ESP с любыми преобразованиями защиты от подмены адресов отправителя, требуется та или иная проверка корректности адреса отправителя. Важность такой проверки понимают далеко не все. Обычно проверка подмены IP-адреса отправителя выполняется, как часть IPsec_{esp,ah}_input(). Это позволяет убедиться, что пакет отправлен с того же адреса, который заявлен в исходных защитных связях IKE для фаз 1 и 2. Когда принимающих хост расположен за транслятором NAT, такая проверка не имеет большого смысла для индивидуальных (unicast) сессий, но в глобальной сети Internet она важна для индивидуальных сессий в туннельном режиме с целью предотвращения spoofing-атак, описанных в [AuthSource], которые могут возникать в тех случаях, когда контроль доступа на приемной стороне зависит от IP-адреса отправителя проверенных пакетов ESP после декапсуляции. Схемам IPsec-NAT следует обеспечивать защиту от атак с подменой адресов отправителя, если эти адреса применяются для контроля доступа.

Рассмотрим два хоста A и C, находящихся за (разными) трансляторами NAT, которые согласуют туннельные связи IPsec SA с маршрутизатором B. Хосты A и C могут иметь разные привилегии — например, A может принадлежать сотруднику доверенной компании с доступом в корпоративную сеть Intranet, а C — заказчику с доступом лишь к конкретному web-сайту.

Если C отправит туннельный пакет от имени хоста A (обманный адрес отправителя), важно, чтобы такой пакет не получил привилегий, соответствующих A. Если выполняется аутентификация и защита целостности но без проверки обманных адресов (соответствия между адресом отправителя и SPI), хост C может получить доступ в ту часть сети, которая для него не предназначена. По этой причине схема решения для совместимости IPsec-NAT **должна** обеспечивать ту или иную защиту от подмены адреса отправителя.

6. Литература

6.1. Нормативные документы

[RFC791] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.

[RFC793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, September 1981.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2401] Atkinson, R. and S. Kent, "Security Architecture for the Internet Protocol", RFC 2401[1], November 1998.

[RFC2402] Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402[2], November 1998.

[RFC2406] Kent,S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406[3], November 1998.

[RFC2407] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407[4], November 1998.

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409[4], November 1998.

[RFC2663] Srisuresh, P. and M. Holdredge, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, August 1999.

[RFC3022] Srisuresh, P. and K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)", RFC 3022, January 2001.

6.2. Дополнительная литература

[RFC2408] Maughan, D., Schertler, M., Schneider, M. and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408[4], November 1998.

[RFC2960] Stewart, R., Xie, Q., Morneault, K., Sharp, C., Schwarzbauer, H., Taylor, T., Rytina, I., Kalla, M., Zhang, M. and V. Paxson, "Stream Control Transmission Protocol", RFC 2960, October 2000.

[RFC3056] Carpenter, B. and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds", RFC 3056, February 2001.

[RFC3193] Patel, B., Aboba, B., Dixon, W., Zorn, G. and S. Booth, "Securing L2TP using IPsec", RFC 3193, November 2001.

[RFC3309] Stone, J., Stewart, R. and D. Otis, "Stream Control Transmission Protocol (SCTP) Checksum Change", RFC 3309, September 2002.

[RSIPFrame] Borella, M., Lo, J., Grabelsky, D. and G. Montenegro, "Realm Specific IP: Framework", RFC 3102, October 2001.

[RSIP] Borella, M., Grabelsky, D., Lo, J. and K. Taniguchi, "Realm Specific IP: Protocol Specification", RFC 3103, October 2001.

[RSIPsec] Montenegro, G. and M. Borella, "RSIP Support for End-to-End IPsec", RFC 3104, October 2001.

[DHCP] Patel, B., Aboba, B., Kelly, S. and V. Gupta, "Dynamic Host Configuration Protocol (DHCPv4) Configuration of IPsec Tunnel Mode", RFC 3456, January 2003.

[AuthSource] Kent, S., "Authenticated Source Addresses", IPsec WG Archive (ftp://ftp.ans.net/pub/archive/IPsec), Message-Id: <v02130517ad121773c8ed@[128.89.0.110]>, January 5, 1996.

[1]Этот документ признан устаревшим и заменен RFC 4301. *Прим. перев.*
[2]Этот документ признан устаревшим и заменен RFC 4302 и RFC 4305. *Прим. перев.*
[3]Этот документ признан устаревшим и заменен RFC 4303 и RFC 4305. *Прим. перев.*
[4]Этот документ признан устаревшим и заменен RFC 4306, который заменен RFC 5996, а затем - RFC 7296. *Прим. перев.*

[AddIP] Stewart, R., et al., "Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration", Work in Progress[5].

7. Благодарности

Спасибо Steve Bellovin из AT&T Research, Michael Tuexen из Siemens, Peter Ford из Microsoft, Ran Atkinson из Extreme Networks и Daniel Senie за полезные обсуждения проблемы.

8. Адреса авторов

Bernard Aboba

Microsoft Corporation

One Microsoft Way

Redmond, WA 98052

Phone: +1 425 706 6605

Fax: +1 425 936 7329

EMail: bernarda@microsoft.com

William Dixon

V6 Security, Inc.

601 Union Square, Suite #4200-300

Seattle, WA 98101

EMail: ietf-wd@v6security.com

Перевод на русский язык

Николай Малых

nmalykh@gmail.com

9. Полное заявление авторских прав

Подтверждение

Финансирование функций RFC Editor обеспеченоInternet Society.

[5]Работа завершена и опубликована в RFC 5061. *Прим. перев.*