Network Working Group
Request for Comments: 3947
Category: Standards Track

T. Kivinen
SafeNet
B. Swander
Microsoft
A. Huttunen
F-Secure Corporation
V. Volpe
Cisco Systems

January 2005

Работа IKE через трансляторы NAT

Negotiation of NAT-Traversal in the IKE

Статус документа

Этот документ содержит спецификацию проекта стандартного протокола Internet и служит приглашением к дискуссии в целях развития протокола. Текущее состояние стандартизации и статус протокола можно узнать из документа Internet Official Protocol Standards (STD 1). Документ может распространяться свободно.

Авторские права

Copyright (C) The Internet Society (2005).

Аннотация

Этот документ описывает способы обнаружения трансляторов сетевых адресов (NAT[1]) между хостами IPsec и согласования применения инкапсуляции в UDP пакетов IPsec, передаваемых через NAT при обмене ключами (IKE[2]).

Оглавление

1. Введение

Этот документ состоит из двух частей. Первая часть описывает, что требуется сделать в фазе 1 IKE (Phase 1) для работы через трансляторы сетевых адресов (NAT-Traversal), включая обнаружение поддержки NAT-Traversal на другой стороне и обнаружения устройств NAT между партнёрами.

Во второй части описано использование инкапсулированных в UDP пакетов IPsec в ускоренном режиме[3] IKE. Рассматриваются также способы передачи партнёру исходных адресов отправителя и получателя, если они требуются. Эти адреса используются в транспортном режиме для инкрементального обновления контрольных сумм TCP/IP с целью сохранения их корректности после прохождения через устройства NAT (само устройство NAT не может сделать этого, поскольку контрольные суммы NAT TCP/IP находятся внутри пакета IPsec, инкапсулированного в UDP).

В [RFC3948] описаны детали инкапсуляции в UDP, а в [RFC3715] приведена базовая информация и мотивировка NAT-Traversal в целом. В комбинации с [RFC3948] данный документ представляет безусловно совместимое решение в части требований, определённых в [RFC3715].

В базовом сценарии для этого документа инициатор размещается за устройством NA(P)T, а отвечающая сторона имеет фиксированный адрес IP.

[1]Network address translation.
[2]Internet Key Exchange.
[3]Quick Mode.

Этот документ определяет протокол, который будет работать даже при размещении обеих сторон за трансляторами NAT, но обработка случаев, когда отвечающая сторона также размещается за транслятором адресов, выходит за рамки этого документа. В одном варианте отвечающая сторона размещается за транслятором NAT со статическим адресом (для одного адреса IP может быть только один ответчик, поскольку нет возможности использовать порт получателя, отличающийся от 500/4500). Такая ситуация известна из конфигурационных параметров.

2. Уровни требований

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

3. Фаза 1

Обнаружение поддержки работы через NAT (NAT-Traversal) и присутствия устройств NAT на пути между двумя партнёрами. IKE выполняется в фазе 1 IKE [RFC2409] .

Транслятор NAT может сменить порт отправителя IKE UDP и получатели **должны** быть способны обрабатывать пакеты IKE, в которых номер порта отправителя отличается от 500. Трансляторы NAT меняют порт отправителя с учётом приведённых ниже условий.

- порт не меняется, если за устройством NAT размещается только один хост IPsec;
- для первого хоста IPsec устройство NAT может сохранить порт 500 и менять его только для соединений других хостов.

Получатели **должны** отвечать по адресу отправителя из пакета (см. [RFC3715], параграф 2.1, п. d). Это означает, что при смене исходным ответчиком ключей или отправке уведомлений исходному оператору исходный ответчик **должен** отправлять пакеты с тем же номером порта и адресом IP, которые использовались при последнем обращении к IKE SA.

Например, когда инициатор передаёт пакет с номерами портов отправителя и получателя 500, транслятор NAT может заменить порт отправителя на 12312, сохранив порт получателя 500. Отвечающий должен быть способен обработать пакет, отправленный из порта 12312 и отвечать на него пакетом из порта 500 в порт 12312. Устройство NAT тогда будет транслировать этого пакет, устанавливая для портов отправителя и получателя значение 500.

3.1. Детектирование поддержки работы через NAT

Возможность работы удалённого хоста через NAT (NAT-Traversal) определяется путём обмена идентификаторами производителей. В двух первых сообщениях фазы 1 (Phase 1) элемент данных с идентификатором производителя (vendor id payload) для данной спецификации **должен** передаваться, если он поддерживается (и он **должен** приниматься обеими сторонами) для проб NAT-Traversal. Содержимое этого элемента данных является хэш-суммой MD5 для

```
RFC 3947
```

или (в шестнадцатеричной форме)

```
4a131c81070358455c5728f20e95452f
```

3.2. Обнаружение присутствия NAT

Элемент данных NAT-D[1] не только позволяет обнаружить присутствие NAT между партнёрами. IKE, но и определяет место расположения трансляторов NAT. Это имеет важное значение для передачи пакетов keepalive от устройств, расположенных «за» трансляторами NAT.

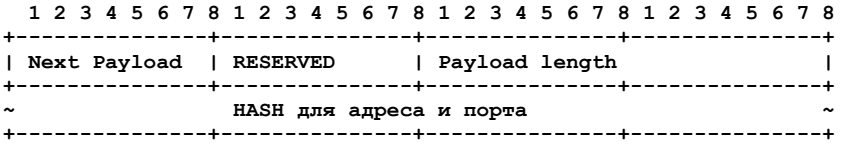
Для обнаружения устройств NAT между двумя хостами проверяется изменение адресов IP или номеров портов на пути доставки. Это выполняется путём передачи хэш-значений для адресов IP и номеров портов обоих партнёров IKE с каждой из сторон на другую. Если обе стороны рассчитывают эти хэш-значения и получают одинаковые результаты, это говорит об отсутствии преобразований NAT между ними. Если хэш-значения различаются, это говорит о том, что адрес или номер порта был где-то изменён. Это означает, что для передачи пакетов IPsec будет использоваться NAT-Traversal.

Если отправитель пакета не знает своего адреса IP (при наличии множества интерфейсов реализация может не знать конкретный интерфейс, через который будет отправлен пакет), отправитель может включить в пакет множество локальных хэш-значений (в виде отдельных элементов NAT-D). В таких случаях о наличии NAT говорит несоответствие всех таких значений.

Хэш-значения передаются в форме серий элементов NAT-D. Каждый элемент содержит одно хэш-значение, поэтому при передаче множества значений используется соответствующее число элементов NAT-D. В обычно ситуации применяется только два элемента NAT-D.

Элементы данных NAT-D включаются в третий и четвёртый пакеты основного режима (Main Mode) и во второй и третий - агрессивного режима (Aggressive Mode).

Формат пакетов NAT-D показан на рисунке.



Идентификатор типа для элемента данных NAT-D имеет значение 20.

Значение HASH рассчитывается по формуле

[1]NAT discovery - обнаружение NAT.

```
HASH = HASH(CKY-I | CKY-R | IP | Port)
```

Здесь используется согласованный алгоритм хэширования (HASH). Все данные в HASH представляются в сетевом порядке байтов. IP представляет 4 октета адреса IPv4 или 16 октетов адреса IPv6. Номер порта указывается 2-октетным значением с сетевым порядком байтов. Первый элемент NAT-D содержит IP-адрес и номер порта удалённой стороны (т. е., адрес получателя пакета UDP). Остальные элементы NAT-D содержат возможные адреса IP и номера портов для локальной стороны (т. е., все возможные адреса отправителя в пакетах UDP).

Если на пути нет устройств NAT первый полученный элемент NAT-D будет совпадать с одним из локальных элементов NAT-D (т. е., элементов NAT-D, передаваемых данным хостом), а один из оставшихся элементов NAT-D должен совпадать с адресом и портом удалённой стороны. Если первая проверка даёт несовпадение (т. е., первый элемент NAT-D не соответствует ни одному из локальных адресов IP и портов), это говорит о динамическом преобразовании NAT на пути между партнёрами., поэтому данной стороне соединения следует начать передачу пакетов keepalive, как описано в [RFC3948] (эта сторона расположена за NAT).

CKY-I и CKY-R указывают значения cookie инициатора и ответчика, которые добавляются при расчёте хэш-функции для предотвращения атак с предварительным расчётом (precomputation attack), делающих адреса IP и порты недоступными.

Ниже приведён пример обмена Phase 1 с использованием NAT-Traversal в основном режиме (Main Mode - аутентификация с подписями).

```
Инициатор                           Ответчик
------------                        ------------
HDR, SA, VID                -->
                                    <-- HDR, SA, VID
HDR, KE, Ni, NAT-D, NAT-D   -->
                                    <-- HDR, KE, Nr, NAT-D, NAT-D
HDR*#, IDii, [CERT, ] SIG_I -->
```

Ниже приведён пример обмена Phase 1 с использованием NAT-Traversal в агрессивном режиме (Aggressive Mode - аутентификация с подписями).

```
Инициатор                           Ответчик
------------                        ------------
HDR, SA, KE, Ni, IDii, VID  -->
                                    <-- HDR, SA, KE, Nr, Idir, [CERT, ], VID, NAT-D,
                                            NAT-D, SIG_R
HDR*#, [CERT, ], NAT-D, NAT-D,
                      SIG_I  -->
```

Знак # указывает, что такие пакеты передаются в изменённый порт, если обнаружено присутствие NAT.

4. Смена портов

Осведомленные об IPsec трансляторы NAT могут вызывать проблемы (см. параграф 2.3 в [RFC3715]). Некоторые устройства NAT не будут менять порт отправителя IKE 500 даже при наличии за транслятором NAT множества клиентов ([RFC3715], параграф 2.3, п. n). Они также могут применять для демультиплексирования трафика IKE cookie вместо номера порта отправителя ([RFC3715], параграф 2.3, п. m). Обе эти ситуации являются проблематичными для базовой прозрачности NAT, поскольку протоколу IKE трудно определить возможности транслятора NAT. Лучшим решением будет просто максимально быстрый перенос трафика IKE из порта 500 для предотвращения описанных выше ситуаций в осведомленных об IPsec трансляторах NAT.

Наиболее часто встречаются ситуации с размещением инициатора за устройством NAT. Инициатор должен быстро переключиться на работу через порт 4500 после обнаружения присутствия NAT для минимизации окна проблем, связанных с осведомленными об IPsec трансляторами NAT.

В основном режиме (Main Mode) инициатор **должен** сменить порты при передаче элемента данных ID, если между хостами имеется устройство NAT. Инициатор **должен** установить для портов отправителя и получателя значения UDP 4500. Все последующие пакеты для этого партнёра (включая информационные уведомления) **должны** передаваться в порт 4500. В дополнение к этому перед данными IKE **должен** помещаться маркер non-ESP, позволяющий демультиплексировать трафик, как описано в [RFC3948].

Таким образом, пакет IKE будет иметь вид

```
IP UDP(4500,4500) <non-ESP marker> HDR*, IDii, [CERT, ] SIG_I
```

Это предполагает аутентификацию с использованием подписей. 4-байтовый маркер non-ESP определён в [RFC3948].

При получении этого пакета ответчиком он выполняет обычную расшифровку и обработку различных элементов данных. После успешного завершения ответчик **должен** обновить своё локальное состояние так, что все последующие пакеты (включая информационные уведомления) для партнёра использовали новый номер порта и, возможно, новый адрес IP, полученные из корректного входящего пакета. Номера портов в общем случае будут различаться, поскольку NAT будет отображать UDP(500,500) в UDP(X,500), а UDP(4500,4500) в UDP(Y,4500). Адрес IP будет иногда отличаться от заранее изменённого IP-адреса. Ответчик должен направлять все последующие пакеты IKE данному партнёру, используя UDP(4500,Y).

Аналогично, если ответчик меняет ключи Phase 1 SA, согласование замены **должно** начинаться с использованием UDP(4500,Y). Все реализации, обеспечивающие работу через NAT, **должны** поддерживать согласование, начинающееся через порт 4500. если согласование начинается через порт 4500, номер порта не потребуется менять в течение обмена.

После смены порта получение пакета на порту 500 будет говорить о том, сто это старый пакет. Если пакет является информационным, его **можно** обработать в соответствии с локальной политикой (если она разрешает это). Если пакет относится к Main Mode или Aggressive Mode (с теми же значениями cookie, что и в предыдущем пакете), его **следует** отбросить. Если пакет относится к новому обмену основного или агрессивного режима, он обрабатывается обычным путём (другая сторона могла быть перезагружена и начала обмен по этой причине).

Ниже приведён пример обмена Phase 1 с использованием NAT-Traversal в основном режиме (аутентификация с подписями) с заменой порта.

```
Инициатор                          Ответчик
------------                       ------------
UDP(500,500) HDR, SA, VID -->
                                   <-- UDP(500,X) HDR, SA, VID
UDP(500,500) HDR, KE, Ni,
             NAT-D, NAT-D -->
                                   <-- UDP(500,X) HDR, KE, Nr, NAT-D, NAT-D
UDP(4500,4500) HDR*#, IDii,
            [CERT, ]SIG_I -->
                                   <-- UDP(4500,Y) HDR*#, Idir, [ CERT, ], SIG_R
```

Процедура для Aggressive Mode очень похожа. После обнаружения NAT инициатор передаёт пакет IP UDP(4500,4500) вида <4-байтовый маркер non-ESP> HDR*, [CERT,], NAT-D, NAT-D, SIG_I. Ответчик выполняет обработку, подобную описанной выше, и при её успешном завершении **должен** обновить свои внутренние порты IKE. Ответчик **должен** отправлять все последующие пакеты IKE этому партнёру, используя UDP(4500,Y).

```
Инициатор                          Ответчик
------------                       ------------
UDP(500,500) HDR, SA, KE,
              Ni, IDii, VID -->
                                   <-- UDP(500,X) HDR, SA, KE, Nr, IDir, [CERT, ],
                                          VID, NAT-D, NAT-D, SIG_R
UDP(4500,4500) HDR*#, [CERT, ],
        NAT-D, NAT-D, SIG_I -->
                                   <-- UDP(4500, Y) HDR*#, ...
```

При включённой поддержке работы через NAT поле номера порта в элементе данных ID для режимов Main Mode/Aggressive Mode **должно** иметь значение 0.

Наиболее распространенным вариантом размещения ответчика за NAT является простое преобразование адресов 1:1 в трансляторе NAT. В этом случае инициатор так же меняет номера обоих портов на 4500. Ответчик применяет алгоритм, аналогичный вышеописанному, хотя в этом случае Y = 4500 и трансляции портов не происходит.

Другой случай смены портов включает определение используемых портов внешними средствами (out-of-band), рассмотрение которых выходит за рамки этого документа. Например, если ответчик находится за устройством NAT, транслирующим номера портов, а инициатору нужно связаться с таким ответчиком, обычно инициатор определяет используемые порты через некий другой сервер. После того, как инициатор узнает номера портов, используемые для работы через NAT (обычно что-то типа UDP(Z,4500)), он инициирует соединения, используя эти порты. Это похоже на описанный выше случай смены ключей ответчиком, когда номера используемых портов известны заранее и никаких дополнительных изменений не требуется. Отсчёт таймера keepalive начинается после перехода на новый номер порта и сообщения keepalive не передаются в порт 500.

5. Ускоренный режим

После фазы 1 обе стороны знают о наличии между ними транслятора NAT. Окончательное решение об использовании NAT-Traversal относится к ускоренному режиму (Quick Mode). Применение NAT-Traversal согласуется в элементах данных SA ускоренного режиме. В Quick Mode обе стороны могут также передавать исходные адреса своих пакетов IPsec (в транспортном режиме) на другую сторону и каждая из сторон может скорректировать поле контрольной суммы TCP/IP после преобразования NAT.

5.1. Согласование инкапсуляции для NAT-Traversal

Согласование работы через NAT (NAT-Traversal) добавляет два новых режима инкапсуляции, приведённых ниже.

```
UDP-Encapsulated-Tunnel          3
UDP-Encapsulated-Transport       4
```

Обычно не имеет смысла предлагать сразу обычный туннельный или транспортный режим и режимы UDP-Encapsulated. Инкапсуляция в UDP требуется для обеспечения передачи трафика, не относящегося к протоколам UDP/TCP, через трансляторы NAT (см. [RFC3715], параграф 2.2, п. i).

Если между хостами имеется транслятор NAT, обычная туннельная или транспортная инкапсуляция может не работать. В таких случаях **следует** использовать инкапсуляцию в UDP. Если между хостами нет устройств NAT, не возникает причины для неоправданного расхода полосы, связанного с дополнительной инкапсуляцией пакетов в UDP. В таких случаях применять инкапсуляцию в UDP **не следует**.

Инициаторам **не следует** включать в свои предложения одновременно обычный туннельный или транспортный режим и режим UDP-Encapsulated-Tunnel или UDP-Encapsulated-Transport.

5.2. Передача исходных адресов отправителя и получателя

Для обновления контрольных сумм TCP оба партнёра должны знать использованные партнёром при создании пакета адреса IP (см. [RFC3715], параграф 2.1, п. b). Для инициатора исходным адресом будет его адрес IP, а исходным адресом ответчика будет воспринятый IP-адрес партнёра. Для ответчика исходным адресом инициатора будет воспринятый адрес партнёра, а исходным адресом ответчика - его собственный адрес IP.

Исходные адреса передаются с использованием элемента данных NAT-OA (NAT Original Address).

Первым является элемент Initiator NAT-OA, вторым - Responder NAT-OA.

Пример 1

```
        Инициатор <---------> NAT <---------> Ответчик
                    ^                 ^           ^
                  Iaddr             NatPub      Raddr
```

Инициатор, находящийся за NAT обменивается данными с публично доступным ответчиком. Адреса IP ответчика и инициатора обозначим Iaddr и Raddr, публичный адрес транслятора NAT - NatPub.

```
Инициатор
                  NAT-OAi = Iaddr
                  NAT-OAr = Raddr
Ответчик
                  NAT-OAi = NATPub
                  NAT-OAr = Raddr
```

Пример 2

```
        Инициатор <------> NAT1 <---------> NAT2 <-------> Ответчик
                  ^              ^           ^               ^
                Iaddr         Nat1Pub     Nat2Pub          Raddr
```

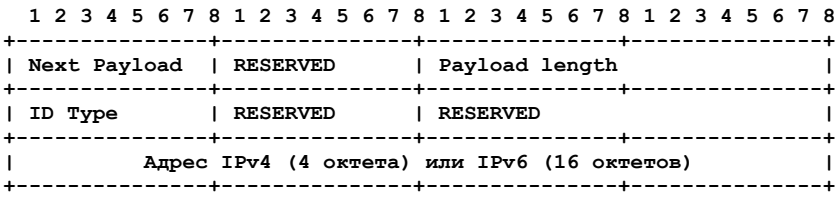
Здесь NAT2 «публикует» адрес Nat2Pub для ответчика и пересылает весь направленный по этому адресу трафик ответчику.

```
Инициатор
                  NAT-OAi = Iaddr
                  NAT-OAr = Nat2Pub
Ответчик
                  NAT-OAi = Nat1Pub
                  NAT-OAr = Raddr
```

В транспортном режиме обе стороны **должны** передавать на другую сторону исходные адреса инициатора и ответчика. В туннельном режиме обеим сторонам **не следует** передавать исходные адреса на другую сторону.

Элементы данных NAT-OA передаются в первом и втором пакетах ускоренного режим (Quick Mode). Инициатор **должен** передавать эти элементы, если он предлагает любой из режимов UDP-Encapsulated[1], а ответчик **должен** передавать такой элемент только при выборе режима UDP-Encapsulated-Transport. Возможна передача инициатором элемента NAT-OA при одновременной поддержке транспортного и туннельного режима UDP-Encapsulated. В такой ситуации ответчик, выбравший туннельный режим UDP-Encapsulated, не возвращает элемента данных NAT-OA.

Формат пакета NAT-OA показан на рисунке.



Идентификатор типа для элементов данных NAT-OA имеет значение 21.

Поле ID Type определено в [RFC2407]. Разрешены только типы ID_IPV4_ADDR и ID_IPV6_ADDR. Два резервных поля после ID Type должны иметь нулевые значения.

Ниже приведён пример Quick Mode с использованием элементов данных NAT-OA.

```
Инициатор                              Ответчик
------------                           ------------
HDR*, HASH(1), SA, Ni, [, KE]
    [, IDci, IDcr ]
    [, NAT-OAi, NAT-OAr] -->

                                       <-- HDR*, HASH(2), SA, Nr, [, KE]
                                                 [, IDci, IDcr ] [, NAT-OAi, NAT-OAr]
HDR*, HASH(3)              -->
```

6. Уведомления INITIAL-CONTACT

Адрес отправителя и номер порта[2] в уведомлении INITIAL-CONTACT для расположенного за транслятором NAT хоста не имеют смысла (NAT заменит их), поэтому адреса IP и номера портов **недопустимо** использовать для идентификации удаляемой IKE/IPsec SA (см. [RFC3715], параграф 2.1, п. c). Взамен **следует** использовать элемент данных ID, переданный другой стороной. Т. е. при получении INITIAL-CONTACT от другой стороны, принимающему **следует** удалить все связи SA, ассоциированные с этим элементом ID.

7. Восстановление после утраты отображения NAT

В некоторых случаях транслятор NAT может удалять отображения, которые ещё используются (например, при слишком редких сообщениях keepalive или в результате перезагрузки устройства NAT). В таких случаях стороне, не расположенной за транслятором NAT **следует** использовать последний корректный пакет IKE или IPsec, инкапсулированный в UDP, от другой стороны для определения адреса IP и номера порта, которые следует использовать. Хосту, расположенному за динамическим NAT, **недопустимо** делать это (такое поведение открывает возможность для DoS-атаки), поскольку адрес и номер порта другой стороны не изменились (она не находится за NAT).

Любой аутентифицированный IKE пакет ESP или IKE может служить для обнаружения смена адреса и номера порта, но сообщения keepalive не подходят для этого, поскольку они не аутентифицируются.

8. Вопросы безопасности

В тех случаях, когда предлагаются те или изменения фундаментальных частей протокола защиты, проверка влияния изменений на безопасность не может быть опущена. Поэтому ниже приводятся некоторые соображения о последствиях и оценки эффективности предложений.

[1] В оригинале ошибочно сказано UDP-Encapsulated-Transport. См. https://www.rfc-editor.org/errata_search.php?eid=4936. *Прим. перев.*
[2] В оригинале ошибочно сказано port address. См. https://www.rfc-editor.org/errata_search.php?eid=4937. *Прим. перев.*

- Пробы IKE раскрывают поддержку NAT-Traversal для любого, кто может отслеживать трафик, однако раскрытие поддержки работы через трансляторы NAT не создаёт новых уязвимостей.

- Значение механизмов аутентификации на основе адресов IP сразу же исчезает при появлении трансляторов NAT. Это совсем не обязательно считать недостатком (для любой реальной защиты следует использовать отличные от адресов IP способы аутентификации). Это означает, что аутентификация с заранее распространёнными ключами (pre-shared key) не может применяться в основном режиме (Main Mode) без использования групповых (group-shared) ключей для находящихся за NAT хостов. Использование групповых ключей связано с огромным риском, поскольку оно позволяет любому члену группы аутентифицировать себя у любой другой стороны, заявив себя в качестве «кого-то из группы». Т. е., обычный пользователь может выдать себя за шлюз VPN и действовать, как «человек посередине» (man in the middle), читая/изменяя весь трафик, идущий другим членам группы или от них. Использование групповых ключей **не рекомендуется**.

- Поскольку внутреннее адресное пространство имеет размер лишь 32 бита и обычно занято достаточно неплотно, для злоумышленника может оказаться возможным определение внутреннего адреса, используемого за транслятором NAT, путём проверки всех возможных адресов IP на предмет соответствия хэш-значению. Номера портов обычно фиксированы (500), а значения cookie можно извлечь из пакетов. Это ограничивает число рассчитываемых хэш-значений до 232. Если требуется угадать адрес из приватных блоков IP, число рассчитываемых значений снижается до $2^{24} + 2 * (2^{16})$[1].

- Элементы данных NAT-D и Vendor ID не аутентифицируются ни в основном (Main Mode), ни в агрессивном (Aggressive Mode) режиме. Это означает, что атакующий может удалить, изменить или вставить такой элемент. Удаляя или добавляя элементы, атакующий может организовывать атаку на отказ служб (DoS[2]). Изменяя пакеты NAT-D, атакующий может вынудить обе стороны использовать режимы UDP-Encapsulated вместо прямой организации туннеля или транспортного соединения, что приведёт к неоправданному расходу полосы.

- Передача исходного адреса отправителя в ускоренном режиме раскрывает другой стороне внутренний адрес IP за транслятором NAT. Однако в этом случае другая сторона уже аутентифицирована (подтвердила свою подлинность) и передача исходного адреса отправителя нужна только в транспортном режиме.

- Обновление адресов и портов при инкапсуляции IKE SA/ESP в UDP для каждого приемлемого аутентифицированного пакета может вызывать отказ служб (DoS), если атакующий имеет возможность прослушивать весь трафик в сети, менять порядок пакетов и вставлять новые пакеты перед пакетом, который он уже видел. Иными словами, атакующий может взять аутентифицированный пакет от хоста, находящегося за NAT, поменять порты UDP отправителя/получателя или адрес IP и передать с нарушением порядка этот пакет перед реальным пакетом. Хост, не находящийся за NAT, обновит у себя отображение IP-адреса и порта, а потом будет передавать последующий трафик по обманным адресу и порту. Эта проблема решается сразу же, как только атакующий прекращает изменение пакетов - первый же пакет от реального хоста восстановит нормальную ситуацию. В реализациях **следует** поддерживать аудит событий при каждом изменении отображений и не разрешать такие изменения слишком часто.

9. Взаимодействие с IANA

Этот документ включает два новых «магических значения», выделенные в имеющемся реестре IANA для IPsec и изменены названия для зарегистрированного ранее порта 4500. Документ также определяет два новых элемента данных для IKE.

В реестр Internet Security Association and Key Management Protocol (ISAKMP) Identifiers добавлены указанные в таблице идентификаторы режимов инкапсуляции.

Имя	Значение	Документ
UDP-Encapsulated-Tunnel	3	[RFC3947]
UDP-Encapsulated-Transport	4	[RFC3947]

В реестр номеров портов внесены изменения, указанные в таблице.

Имя	Номер/имя	Описание	Документ
ipsec-nat-t	4500/tcp	IPsec NAT-Traversal	[RFC3947]
ipsec-nat-t	4500/udp	IPsec NAT-Traversal	[RFC3947]

В реестр Next Payload Types добавлены новые типы элементов данных IKE:

```
NAT-D          20          NAT Discovery Payload
NAT-OA         21          NAT Original Address Payload
```

10. Взаимодействие с IAB

Вопросы UNSAF [RFC3424] решаются требованиями совместимости IPsec-NAT, описанными в [RFC3715].

11. Благодарности

Спасибо Markus Stenberg, Larry DiBurro и William Dixon за активное участие в подготовке этого документа.

Спасибо Tatu Ylonen, Santeri Paavolainen и Joern Sierwald, которые подготовили документы, послужившие основой для данного документа.

12. Литература

12.1. Нормативные документы

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

[1] Суммарный размер выделенных для приватных сетей блоков адресов IP (RFC 1918). *Прим. перев.*
[2] Denial of Service.

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

[RFC3948] Huttunen, A., Swander, B., Volpe, V., DiBurro, L., and M. Stenberg, "UDP Encapsulation of IPsec Packets", RFC 3948, January 2005.

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

12.2. Дополнительная литература

[RFC3715] Aboba, B. and W. Dixon, "IPsec-Network Address Translation (NAT) Compatibility Requirements", RFC 3715, March 2004.

[RFC3424] Daigle, L. and IAB, "IAB Considerations for Unilateral Self-Address Fixing (UNSAF) Across Network Address Translation", RFC 3424, November 2002.

Адреса авторов

Tero Kivinen
SafeNet, Inc.
Fredrikinkatu 47
FIN-00100 HELSINKI
Finland
EMail: kivinen@safenet-inc.com

Brian Swander
Microsoft
One Microsoft Way
Redmond, WA 98052
USA
EMail: briansw@microsoft.com

Ari Huttunen
F-Secure Corporation
Tammasaarenkatu 7,
FIN-00181 HELSINKI
Finland
EMail: Ari.Huttunen@F-Secure.com

Victor Volpe
Cisco Systems
124 Grove Street
Suite 205
Franklin, MA 02038
USA
EMail: vvolpe@cisco.com

Перевод на русский язык

Николай Малых
nmalykh@protokols.ru

Полное заявление авторских прав

Copyright (C) The Internet Society (2005).

К этому документу применимы права, лицензии и ограничения, указанные в BCP 78, и, за исключением указанного там, авторы сохраняют свои права.

Этот документ и содержащаяся в нем информация представлены **"как есть"** и **автор, организация, которую он/она представляет или которая выступает спонсором (если таковой имеется), Internet Society и IETF отказываются от каких-либо гарантий (явных или подразумеваемых), включая (но не ограничиваясь) любые гарантии того, что использование представленной здесь информации не будет нарушать чьих-либо прав, и любые предполагаемые гарантии коммерческого использования или применимости для тех или иных задач**.

Интеллектуальная собственность

IETF не принимает какой-либо позиции в отношении действительности или объема каких-либо прав интеллектуальной собственности (Intellectual Property Rights или IPR) или иных прав, которые, как может быть заявлено, относятся к реализации или использованию описанной в этом документе технологии, или степени, в которой любая лицензия, по которой права могут или не могут быть доступны, не заявляется также применение каких-либо усилий для определения таких прав. Сведения о процедурах IETF в отношении прав в документах RFC можно найти в BCP 78 и BCP 79.

Копии раскрытия IPR, предоставленные секретариату IETF, и любые гарантии доступности лицензий, а также результаты попыток получить общую лицензию или право на использование таких прав собственности разработчиками или пользователями этой спецификации, можно получить из сетевого репозитория IETF IPR по ссылке http://www.ietf.org/ipr.

IETF предлагает любой заинтересованной стороне обратить внимание на авторские права, патенты или использование патентов, а также иные права собственности, которые могут потребоваться для реализации этого стандарта. Информацию следует направлять в IETF по адресу ietf-ipr@ietf.org.

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.