Network Working Group
Request for Comments: 3948
Category: Standards Track

A. Huttunen
F-Secure Corporation
B. Swander
Microsoft
V. Volpe
Cisco Systems
L. DiBurro
Nortel Networks
M. Stenberg
January 2005

Инкапсуляция пакетов IPsec ESP в UDP

UDP Encapsulation of IPsec ESP Packets

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.

Тезисы

Данная спецификация определяет метод инкапсуляцию и декапсуляцию пакетов ESP[1] в пакеты UDP для передачи через трансляторы NAT[2]. Определенная здесь инкапсуляция ESP может использоваться как с протоколом IPv4, так и с IPv6. По согласования инкапсуляция применяется при обмене ключами IKE[3].

Оглавление

1. Введение

Эта спецификация протокола определяет методы инкапсуляции и декапсуляции пакетов ESP в пакеты UDP для прохождения через трансляторы сетевых адресов (NAT) (см. [RFC3715], параграф 2.2, п. i). Номера портов UDP используются те же самые, что применяются для трафика IKE, как определено в [RFC3947].

Использование общих номеров портов для IKE и инкапсулированного в UDP трафика ESP обусловлено тем, что это обеспечивает более эффективное масштабирование (одно отображение в NAT и не требуется передача отдельных сообщений IKE keepalive), упрощает настройку (только один порт на межсетевом экране) и реализацию.

[1]Encapsulating Security Payload — инкапсулированное защищенное содержимое.
[2]Network Address Translator — транслятор сетевых адресов.
[3]Internet Key Exchange — обмен ключами в Internet.

Выбор транспортного или туннельного режима следует выполнять с учетом потребностей клиента (см. [RFC3715], раздел 3, «Удаленные пользователи»). Клиенты L2TP/IPsec **должны** поддерживать режимы, определенные в [RFC3193]. Клиенты IPsec в туннельном режиме **должны** поддерживать туннельный режим.

Реализациям IKE, поддерживающим этот протокол, **недопустимо** использовать поле ESP SPI со значением 0 для пакетов ESP. Это позволяет различать пакеты IKE и ESP.

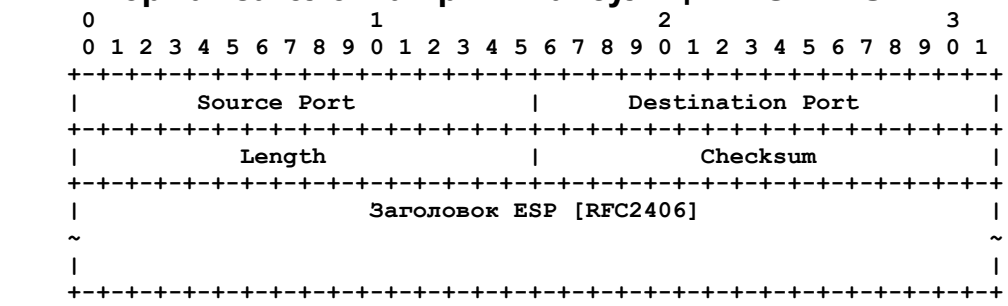
Как определено в этом документе, инкапсуляция пакетов ESP в UDP описывается в терминах заголовков IPv4. Нет никаких технических ограничений на использование заголовков IPv6 в качестве внешних и/или внутренних.

Поскольку защита внешних адресов IP в IPsec AH принципиально не совместима с NAT, спецификация протокола просто не включает IPsec AH. Данный протокол предполагает использование IKE (IKEv1 [RFC2401] или IKEv2 [IKEv2]) для согласования IPsec SA. Установка ключей вручную не поддерживается.

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].

2. Формат пакетов

2.1. Формат заголовка при инкапсуляции ESP в UDP

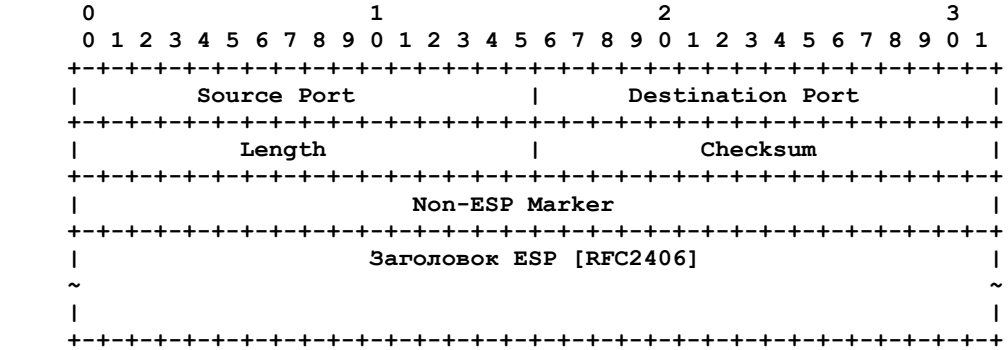


Заголовок UDP соответствует стандарту [RFC0768] с учетом перечисленных ниже ограничений:

- поля Source Port и Destination Port **должны** совпадать с аналогичными полями трафика IKE;
- в поле IPv4 UDP Checksum **следует** указывать значение 0;
- получателям **недопустимо** зависеть от нулевого значения в поле контрольной суммы UDP.

В поле SPI заголовка ESP **недопустимо** устанавливать значение 0.

2.2. Формат заголовка IKE для порта 4500



Заголовок UDP соответствует стандарту [RFC0768] и применяется, как описано в [RFC3947]. Этот документ не задает новых требований к обработке контрольных сумм для пакетов IKE.

Поле Non-ESP Marker представляет собой 4 байта с нулевыми значениями, служащими для выравнивания с полем SPI в пакетах ESP.

2.3. Формат пакетов NAT-Keepalive

Заголовок UDP соответствует стандарту [RFC0768] с учетом перечисленных ниже ограничений:

- поля Source Port и Destination Port **должны** совпадать с аналогичными полями трафика UDP-ESP, как указано в параграфе 2.1;
- в поле IPv4 UDP Checksum **следует** указывать значение 0;

- получателям **недопустимо** зависеть от нулевого значения в поле контрольной суммы UDP.

Отправитель **должен** использовать 1-октетный элемент данных со значением 0xFF. Получателям **следует** игнорировать принятые пакеты NAT-keepalive.

3. Процедуры инкапсуляции и декапсуляции

3.1. Дополнительные процедуры

3.1.1. Процедура декапсуляции NAT в туннельном режиме

При использовании для передачи пакетов туннельного режима (см. [RFC3715], раздел 3, criteria "Mode support" и «Удаленные пользователи»), the inner IP header can contain addresses that are not suitable for the current network. This procedure defines how these addresses are to be converted to suitable addresses for the current network.

В зависимости от локальной политики **должно** выполняться одно из перечисленных ниже условий.

1. Если в политике определено приемлемое пространство IP-адресов отправителей для инкапсулированных пакетов от партнеров, проверяется соответствие IP-адреса во внутреннем заголовке этому пространству.
2. Если удаленному партнеру присвоен адрес, проверяется соответствие адреса отправителя во внутреннем заголовке присвоенному адресу IP.
3. Для пакета выполняется трансляция NAT, делающая его подходящим для пересылки в локальную сеть.

3.1.2. Процедура декапсуляции NAT в транспортном режиме

При использовании для передачи пакетов транспортного режима контрольные суммы в заголовках TCP и UDP будут не корректны, поскольку отдельные части заголоков IP будут меняться в процессе передачи. Приведенная здесь процедура определяет корректировку контрольных сумм (см. [RFC3715], параграф 2.1, п. b).

В зависимости от локальной политики **должно** выполняться одно из перечисленных ниже условий.

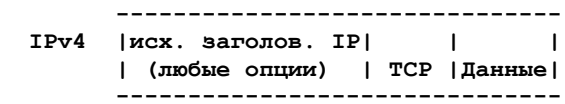
1. Если после заголовка ESP следует заголовок TCP/UDP и реальные адреса отправителя и получателя были определены в соответствии с [RFC3947], выполняется перерасчет контрольной суммы TCP/UDP:
   - из контрольной суммы в пакете вычитается IP-адрес отправителя, указанный в заголовке пакета;
   - к результату прибавляется реальный IP-адрес отправителя полученный от IKE (из NAT-OA);
   - вычитается IP-адрес получателя, указанный в заголовке пакета;
   - прибавляется реальный IP-адрес получателя полученный от IKE (из NAT-OA).

   Примечание. Если полученный и реальный адреса (например, для получателя) совпадают, соответствующую пару операций выполнять не требуется.
2. Если после заголовка ESP следует заголовок TCP/UDP, выполняется перерасчет контрольной суммы TCP/UDP.
3. Если после заголовка ESP следует заголовок UDP, устанавливается нулевое значение для поля контрольной суммы UDP. Если после заголовка ESP следует заголовок TCP и имеется опция для отключения расчета контрольной суммы TCP, **можно** воспользоваться этой опцией. Это **следует** применять только для транспортного режима при обеспеченной защите целостности пакетов, в туннельном режиме контрольная сумма TCP должна проверяться (это не является нарушением духа параграфа 4.2.2.7 в [RFC1122], поскольку контрольная сумма создается отправителем и проверяется получателем; значение поля контрольной суммы защищено протоколом IPsec).

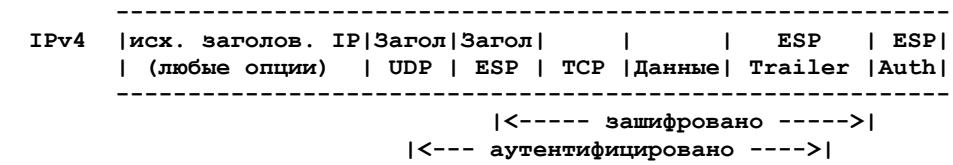
В дополнение к этому реализация **может** фиксировать все вложенные протоколы, работа которых нарушеается транслятором NAT (см. [RFC3715], параграф 2.1, п. g).

3.2. Инкапсуляция ESP в транспортном режиме

До применения ESP/UDP



После применения ESP/UDP



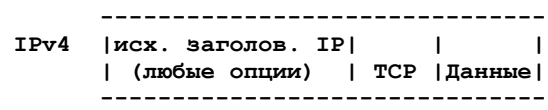
1. Применяется обычная процедура инкапсуляции ESP.
2. В нужное место помещается корректно отформатированный заголовок UDP.
3. Поля Total Length, Protocol и Header Checksum (для IPv4) в заголовке IP редактируются в соответствии с результирующим пакетом IP.

3.3. Декапсуляция ESP в транспортном режиме

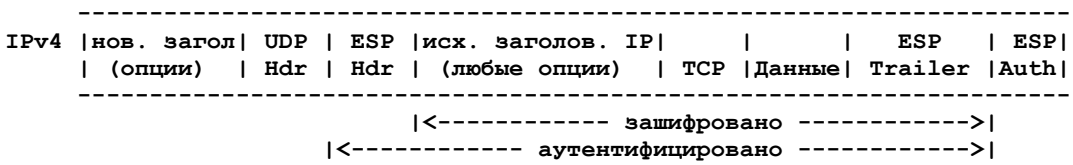
1. Заголовок UDP удаляется из пакета.
2. Поля Total Length, Protocol и Header Checksum (для IPv4) в заголовке IP редактируются в соответствии с результирующим пакетом IP.
3. Применяется обычная процедура декапсуляции ESP.
4. Выполняется процедура декапсуляции NAT для транспортного режима.

3.4. Инкапсуляция ESP в туннельном режиме

До применения ESP/UDP



После применения ESP/UDP



1. Применяется обычная процедура инкапсуляции ESP.
2. В нужное место помещается корректно отформатированный заголовок UDP.
3. Поля Total Length, Protocol и Header Checksum (для IPv4) в заголовке IP редактируются в соответствии с результирующим пакетом IP.

3.5. Декапсуляция ESP в туннельном режиме

1. Заголовок UDP удаляется из пакета.
2. Поля Total Length, Protocol и Header Checksum (для IPv4) в заголовке IP редактируются в соответствии с результирующим пакетом IP.
3. Применяется обычная процедура декапсуляции ESP.
4. Выполняется процедура декапсуляции NAT для туннельного режима.

4. Процедура NAT Keepalive

Единственной целью отправки пакетов NAT-keepalive является обеспечение сохранности отображений NAT в течение всего срока действия соединения между партнерами (см. [RFC3715], параграф 2.2, п. j). Прием сообщения NAT-keepalive **недопустимо** использовать в качестве подтверждения жизнеспособности соединения.

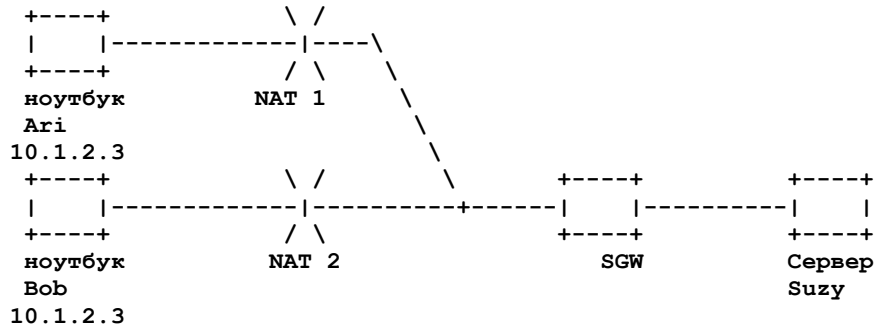
Узел **может** передать пакет NAT-keepalive, если между партнерами имеется одна или множество связей SA (phase I или phase II) или такие связи были не более N ранее. Значение N задается в локальной конфигурации, по умолчанию используется 5 минут.

Узлу **следует** передать пакет NAT-keepalive, если нужно детектировать этот узел в соответствии с [RFC3947], а партнеру не передавалось других пакетов в течение M секунд. Значение M адается в локальной конфигурации, по умолчанию используется 20 секунд.

5. Вопросы безопасности

5.1. Конфликт туннельного режима

Разработчикам следует принимать во внимание возможность возникновения ситуаций, когда удаленные пользователи будут согласовывать на SGW[1] (защитный шлюз) пересекающиеся параметры, которые могут воздействовать на работу в туннельном режиме (см. [RFC3715], параграф 2.1, п. e).



Поскольку SGW будет видеть две SA, ведущие в 10.1.2.3, ему непонятно, в которую направлять пакеты от сервера Suzy. Разработчики **должны** обеспечить способ снятия такой неопределенности.

[1]Security gateway.

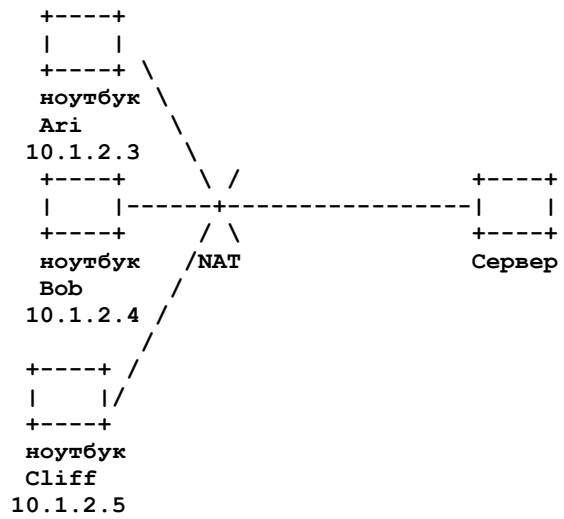
Рекомендуется на устройстве SGW присваивать уникальные в локальном масштабе адреса IP компьютерам Ari и Bob (используя протокол типа DHCP over IPsec) или использовать NAT для смены адресов отправителя в пакетах от Ari и Bob на уникальные в местном масштабе адреса IP до отправки их пакетов в направлении сервера Suzy. Это описано в параграфе «Масштабирование» раздела 3 в [RFC3715].

См. также Приложение A.

5.2. Конфликт транспортного режима

Похожая проблема возникает в транспортном режиме, когда 2 клиента (Ari и Bob), расположенные за одним транслятором NAT, организуют защищенные соединения с одним сервером (см. [RFC3715], параграф 2.1, п. e).

Клиент Cliff хочет подключиться к тому же серверу без использования защиты.



Транспортные связи SA с сервером будут иметь вид

для Ari: Server -> NAT, <дескриптор трафика 1>, инкапсуляция UDP <4500, Y>

для Bob: Server -> NAT, <дескриптор трафика 2>, инкапсуляция UDP <4500, Z>

Трафик Cliff передается в открытом виде без организации SA.

Дескрипторы трафика содержат информацию о протоколах и номерах портов. Для инкапсуляции в UDP используется порт 4500 и описанный в параграфе 2.1 формат. Y и Z — динамические номера портов, выделяемые транслятором NAT на этапе согласования IKE. Таким образом, трафик IKE от ноутбука Ari будет иметь вид UDP <4500,4500> и придет на сервер в виде UDP <Y,4500>, где Y указывает динамически выделенный транслятором порт.

Если дескрипторы трафика 1 и 2 перекрываются, обычного просмотра базы может быть не достаточно для определения связи SA, которая служит для передачи трафика. Реализации **должны** обрабатывать эту ситуации, запрещая конфликты соединений или с помощью иных мер.

Предположим, что Cliff хочет подключиться к тому же серверу без применения защиты трафика. Организовать такое соединение непросто, поскольку на сервере уже имеется правило (от сервера на внешний адрес устройства NAT) для защиты по дескриптору трафика. Если дескрипторы трафика совсем не перекрываются, такое соединение становится возможным.

Ниже приведен пример правил для сервера

для Ari: Server -> NAT, только UDP, защита

для Bob: Server -> NAT, только TCP, защита

для Cliff: Server -> NAT, только ICMP, без защиты

Отметим, что эти правила позволяет Ari и Bob отправлять серверу пакеты ICMP без защиты.

Сервер видит всех расположенных за транслятором NAT клиентов с одним адресом IP, поэтому установка разных правил для одного и того же дескриптора трафика не возможно в принципе.

Ниже приведен пример сомнительной политики на сервере для описываемого случая.

Server -> NAT, TCP, защита (Ari и Bob)

Server -> NAT, TCP, без защиты (Cliff)

Сервер не сможет реализовать такую политику, поскольку Bob может предать свой трафик в открытом виде и сервер не сможет отличить его от трафика Cliff. Таким образом, становится невозможным обеспечить гарантию защиты некоторым клиентам, расположенным за NAT, одновременно предоставляя другим клиентам за тем же транслятором работать без защиты. Если политика сервера позволяет, он может просто обеспечить некий (best effort - по возможности) уровень защиты, обеспечивая ее расположенным за NAT клиентам, которые инициировали защиту, и передавая в открытом виде отклики на незащищенные запросы.

Для обеспечения гарантированной защиты описанный выше проблемный вариант **недопустимо** разрешать на серверах. Если устраивает защита уровня best effort (по возможности), такой вариант **можно** использовать.

См. также Приложение A.

6. Согласование с IAB

Вопросы UNSAF [RFC3424] решаются документом с требованиями по совместимости IPsec-NAT [RFC3715].

7. Благодарности

Спасибо Tero Kivinen и William Dixon за активное участие в подготовке этого документа.

Спасибо Joern Sierwald, Tamir Zegman, Tatu Ylonen и Santeri Paavolainen за их вклад в ранние документы по работе через трансляторы NAT.

8. Литература

8.1. Нормативные документы

[RFC0768] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.

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

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

[RFC2406] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406[2], November 1998.

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409[3], November 1998.

[RFC3947] Kivinen, T., "Negotiation of NAT-Traversal in the IKE", RFC 3947, January 2005.

8.2. Дополнительная литература

[RFC1122] Braden, R., "Requirements for Internet Hosts - Communication Layers", STD 3, RFC 1122, October 1989.

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

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

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

[IKEv2] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", Work in Progress[4], October 2004.

Приложение A. Разъяснения для случая множества клиентов за NAT

В этом приложении даны разъяснения, касающиеся возможных решений проблем в случаях, когда множество находящихся за одним транслятором NAT узлов одновременно подключаются к одному адресу IP.

В разделах 5.1 и 5.2 отмечено, что вы **должны** избегать таких проблем. Поскольку эти проблемы возникают и решаются не на уровне протокола, а на уровне локальной реализации, механизмы решения не относятся к самому протоколу. По этой причине они вынесены в данное приложение.

Выбор варианта будет очевидно зависеть от сценария использования (поддержки) IPsec NAT-T[5]. Приведенный здесь список не является исчерпывающим и могут существовать другие решения. Сначала будут описаны базовые решения, пригодные для всех протоколов вышележащего уровня.

При использовании ESP в транспортном режиме имеется несколько основных вариантов, перечисленных ниже.

Tr1) Реализация встроенного NAT (трансляция сетевых адресов) выше декапсуляции IPsec.

Tr2) Реализация встроенного NAPT (трансляция сетевых адресов и портов) выше декапсуляции IPsec.

Tr3) Инициатор может отказаться от запроса транспортного режима при обнаружении NAT и запросить взамен организацию туннельной SA. Это может произойти после отказа поддержки транспортного режима отвечающим или изначально по желанию инициатора. Решение этого вопроса не сложнее вопроса выбора туннельного или транспортного режима без NAT. Если по тем или иным соображениям ответчик предпочитает или требует использовать туннельный режим для работы через NAT, он должен отвергнуть предложение организации транспортной SA в ускоренном режиме.

При использовании ESP в туннельном режиме имеется несколько основных вариантов, перечисленных ниже.

Tn1) Совпадает с Tr1.

Tn2) Совпадает с Tr2.

Tn3) Этот вариант возможен, если инициатору может быть выделен адрес через его туннельную связь SA от сервера DHCP на отвечающей стороне. Инициатор может сразу запросить адрес через DHCP-IPsec, независимо от его предположений о наличии или отсутствии NAT. Он может заново инициировать согласование IKE в ускоренном режиме для DHCP через туннельную SA после того, как ответчик отвергнет ускоренное предложение о создании транспортной SA. Это происходит при передаче элемента данных NAT-OA или в результате обнаружения через NAT-D размещения инициатора за транслятором NAT и требования локальной политики (конфигурации, воспринимать соединения через NAT только при выделении адресов через DHCP-IPsec.

---

[1] Этот документ признан устаревшим и заменен RFC 4301. *Прим. перев.*
[2] Этот документ признан устаревшим и заменен RFC 4303, RFC 4305. *Прим. перев.*
[3] Этот документ признан устаревшим и заменен RFC 4306, а затем RFC 5996 и RFC 7296. *Прим. перев.*
[4] Работа завершена и опубликована в RFC 4306, который затем заменен RFC 5996 и RFC 7296. *Прим. перев.*
[5] NAT Traversal — работа через NAT. *Прим. перев.*

Разработчики могут также выбрать ограничение интероперабельности для своей реализации. Разработчикам следует указывать, какие протоколы и приложения смогут работать в таком ограниченном варианте. Отметим, что для вариантов Tr4 и Tn4 не предполагается возможность работы с трафиком TCP (см. ниже).

Ниже перечислены варианты ограниченной интероперабельности для транспортного режима ESP.

Tr4) Реализовать в протоколе вышележащего уровня осведомленность о необходимости отказа от использования во входящих и исходящих IPsec SA адреса IP и номера порта отправителя в качестве идентификатора сессии (например, идентификаторы сессий L2TP отображаются на пары IPsec SA без использования порта UDP или IP-адреса отправителя).

Tr5) Реализовать интеграция приложения с инициированием IKE так, чтобы можно было организовать привязку к другому порту отправителя, если ускоренное предложение IKE SA будет отвергнуто ответчиком; после этого может быть заново предложен новый селектор QM[1].

Ниже перечислены варианты ограниченной интероперабельности для транспортного режима ESP.

Tn4) Совпадает с Tr4.

Адреса авторов

Ari Huttunen

F-Secure Corporation

Tammasaarenkatu 7

HELSINKI FIN-00181

FI

EMail: Ari.Huttunen@F-Secure.com

Brian Swander

Microsoft

One Microsoft Way

Redmond, WA 98052

US

EMail: briansw@microsoft.com

Victor Volpe

Cisco Systems

124 Grove Street

Suite 205

Franklin, MA 02038

US

EMail: vvolpe@cisco.com

Larry DiBurro

Nortel Networks

80 Central Street

Boxborough, MA 01719

US

EMail: ldiburro@nortelnetworks.com

Markus Stenberg

FI

EMail: markus.stenberg@iki.fi

Перевод на русский язык

Николай Малых

nmalykh@gmail.com

[1]Ускоренного режима. *Прим. перев.*

Полное заявление авторских прав

Интеллектуальная собственность

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the IETF's procedures with respect to rights in IETF Documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Подтверждение

Финансирование функций RFC Editor обеспеченоInternet Society.