

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.

Авторские права

Copyright (C) The Internet Society (2005).

Аннотация

Данная спецификация определяет метод инкапсуляции и декапсуляции пакетов ESP¹ в пакеты UDP для передачи через трансляторы NAT². Определённая здесь инкапсуляция ESP может использоваться как с протоколом IPv4, так и с IPv6. По согласованию инкапсуляция применяется при обмене ключами IKE³.

Оглавление

1. Введение.....	1
2. Формат пакетов.....	2
2.1. Формат заголовка при инкапсуляции ESP в UDP.....	2
2.2. Формат заголовка IKE для порта 4500.....	2
2.3. Формат пакетов NAT-Keeralive.....	2
3. Процедуры инкапсуляции и декапсуляции.....	3
3.1. Дополнительные процедуры.....	3
3.1.1. Процедура декапсуляции NAT в туннельном режиме.....	3
3.1.2. Процедура декапсуляции NAT в транспортном режиме.....	3
3.2. Инкапсуляция ESP в транспортном режиме.....	3
3.3. Декапсуляция ESP в транспортном режиме.....	3
3.4. Инкапсуляция ESP в туннельном режиме.....	4
3.5. Декапсуляция ESP в туннельном режиме.....	4
4. Процедура NAT Кеералив.....	4
5. Вопросы безопасности.....	4
5.1. Конфликт туннельного режима.....	4
5.2. Конфликт транспортного режима.....	4
6. Взаимодействие с IAB.....	5
7. Благодарности.....	5
8. Литература.....	6
8.1. Нормативные документы.....	6
8.2. Дополнительная литература.....	6
Приложение А. Разъяснения для случая множества клиентов за NAT.....	6
Адреса авторов.....	7
Полное заявление авторских прав.....	7

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 кеералив), упрощает настройку (только один порт на межсетевом экране) и реализацию.

¹Encapsulating Security Payload - инкапсулированное защищённое содержимое.

²Network Address Translator - транслятор сетевых адресов.

³Internet Key Exchange - обмен ключами в Internet.

Выбор транспортного или туннельного режима следует выполнять с учётом потребностей клиента (см. [RFC3715], раздел 3, «Удалённые пользователи»). Клиенты L2TP/IPsec **должны** поддерживать режимы, определённые 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

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|           Source Port           |           Destination Port           |
+-----+-----+-----+-----+-----+-----+-----+-----+
|           Length                 |           Checksum                   |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                               Заголовок ESP [RFC2406]                               |
~                                                                           ~
|                                                                           |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

Заголовок UDP соответствует стандарту [RFC0768] с учётом 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

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|           Source Port           |           Destination Port           |
+-----+-----+-----+-----+-----+-----+-----+-----+
|           Length                 |           Checksum                   |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                               Non-ESP Marker                               |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                               Заголовок ESP [RFC2406]                               |
~                                                                           ~
|                                                                           |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

Заголовок UDP соответствует стандарту [RFC0768] и применяется, как описано в [RFC3947]. Этот документ не задаёт 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

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|           Source Port           |           Destination Port           |
+-----+-----+-----+-----+-----+-----+-----+-----+
|           Length                 |           Checksum                   |
+-----+-----+-----+-----+-----+-----+-----+-----+
|           0xFF                   |                                     |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

Заголовок UDP соответствует стандарту [RFC0768] с учётом 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, "Mode supsupport и «Удалённые пользователи») внутренний заголовок IP может содержать адреса, не подходящие для текущей сети. Эта процедура определяет, как такие адреса преобразуются в подходящие для текущей сети.

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 партнёров, проверяется соответствие IP-адреса во внутреннем заголовке этому пространству.
2. Если удалённому партнёру 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 заголовков IP будут меняться в процессе передачи. Приведённая 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 перерасчёт 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 перерасчёт 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 расчёта 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 создаётся отправителем и проверяется получателем; значение поля контрольной суммы защищено протоколом IPsec).

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

3.2. Инкапсуляция ESP в транспортном режиме

До применения ESP/UDP

```

-----
IPv4 |исх. заголов. IP|   |   |
    | (любые опции) | TCP |Данные|
-----

```

После применения ESP/UDP

```

-----
IPv4 |исх. заголов. IP|Загол|Загол|   |   |   ESP | ESP|
    | (любые опции) | UDP | ESP | TCP |Данные| Trailer |Auth|
-----
                                |<----- зашифровано ----->|
                                |<--- аутентифицировано ---->|

```

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

```

-----
IPv4 |исх. заголов. IP|   |   |
     | (любые опции) | TCP |Данные|
-----

```

После применения ESP/UDP

```

-----
IPv4 |нов. загол| UDP | ESP |исх. заголов. IP|   |   | ESP | ESP|
     | (опции) | Hdr | Hdr | (любые опции) | TCP |Данные| Trailer |Auth|
-----
                                |<----- зашифровано ----->|
                                |<----- аутентифицировано ----->|

```

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 Keeralive

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

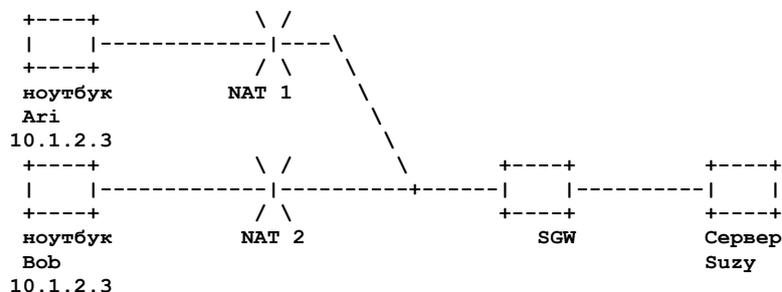
Узел **может** передать пакет NAT-keeralive, если между партнёрами имеется одна или множество связей SA (phase I или phase II) или такие связи были не более N ранее. Значение N задаётся в локальной конфигурации, по умолчанию используется 5 минут.

Узлу **следует** передать пакет NAT-keeralive, если нужно детектировать этот узел в соответствии с [RFC3947], а партнёру не передавалось других пакетов в течение M секунд. Значение M задается 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 удалённые пользователи будут согласовывать на SGW¹ (защитный шлюз) пересекающиеся параметры, которые могут воздействовать на работу в туннельном режиме (см. [RFC3715], параграф 2.1, п. е).



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 неопределённости.

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 А.

5.2. Конфликт транспортного режима

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

¹Security gateway.

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](#), November 1998.
- [RFC2406] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", [RFC 2406](#), November 1998.
- [RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", [RFC 2409](#), 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 Progress¹, October 2004.

Приложение А. 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-T². Приведённый 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 NAT (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).

Разработчики могут также выбрать ограничение совместимости 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 совместимости для транспортного режима ESP.

Tr4) Реализовать в протоколе вышележащего уровня осведомлённость 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 иницированием 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 QM³.

¹Работа опубликована в [4306](#), который затем заменён [RFC 5996](#) и [RFC 7296](#). Прим. перев.

²NAT Traversal - работа через NAT. Прим. перев.

³Ускоренного режима. Прим. перев.

Ниже перечислены варианты ограниченной совместимости для транспортного режима ESP.

Tn4) Совпадает с Tr4.

Адреса авторов

Ari Huttunen

F-Secure Corporation
Tammasaarencatu 7
HELSINKI FIN-00181
FI
E-Mail: Ari.Huttunen@F-Secure.com

Brian Swander

Microsoft
One Microsoft Way
Redmond, WA 98052
US
E-Mail: briansw@microsoft.com

Victor Volpe

Cisco Systems
124 Grove Street
Suite 205
Franklin, MA 02038
US
E-Mail: vvolpe@cisco.com

Larry DiBurro

Nortel Networks
80 Central Street
Boxborough, MA 01719
US
E-Mail: ldiburro@nortelnetworks.com

Markus Stenberg

FI
E-Mail: markus.stenberg@iki.fi

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 ВСП 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 ВСП 78 и ВСП 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.