

Шифронаборы для IPsec

Cryptographic Suites for IPsec

Статус документа

В этом документе описан предлагаемый стандарт протокола для сообщества Internet; документ служит приглашением к дискуссии в целях развития протокола. Информацию о текущем состоянии стандартизации протокола можно найти в документе Internet Official Protocol Standards (STD 1). Данный документ может распространяться свободно.

Авторские права

Copyright (C) The Internet Society (2005).

Тезисы

Протоколы IPsec, IKE¹ и IKEv2 основаны на алгоритмах защиты, обеспечивающих сохранение тайны и аутентификацию между инициатором и отвечающей стороной. Существует множество таких алгоритмов и две системы IPsec не смогут взаимодействовать между собой, если они не будут использовать одинаковые алгоритмы. Данный документ определяет дополнительные наборы алгоритмов и атрибуты, которые могут использоваться для упрощения администрирования IPsec при работе в ручном режиме обмена ключами² с IKEv1 или IKEv2.

1. Введение

Этот документ используется совместно с IPsec [RFC2401³] и двумя протоколами обмена ключами IKE [RFC2409] и IKEv2 [IKEv2]. Подобно многим другим протоколам защиты, IPsec, IKE и IKEv2 позволяют пользователям выбрать используемый криптографический алгоритм в соответствии со своими потребностями.

Опыт разработки IPsec с ручным обменом ключами и IKE показывает, что для типовых систем существует множество вариантов выбора и это затрудняет решение задачи обеспечения интероперабельности без предварительного соглашения. По этой причине рабочая группа IPsec согласилась с тем, что следует выбрать небольшое число именованных наборов, подходящих для типовых ситуаций. Эти наборы могут быть представлены в интерфейсе администратора систем IPsec. Такие наборы, часто называемые UI suite⁴, являются необязательными и не запрещают разработчикам предоставлять возможность выбора отдельных алгоритмов защиты.

Хотя перечисленные здесь наборы UI не являются обязательными для реализации, этот документ внесен как предложенный стандарт, поскольку разработчики называют конкретные наборы перечисленными здесь именами для подтверждения соответствия наборам, перечисленным в этом документе. Эти наборы следует рассматривать не как расширения IPsec, IKE и IKEv2, а как административные методы описания набора конфигураций.

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

2. Наборы UI

В этой главе перечислены необязательные наборы, которые могут представляться системным администраторам для упрощения задачи выбора среди множества опций в системах IPsec. Эти наборы не перекрывают всех опций, которые требуется выбрать администратору. Наборы представляют собой лишь подмножества таких опций.

Отметим, что эти наборы UI представляют собой лишь значения для некоторых опций IPsec. Использование наборов UI не вносит каких-либо изменений в протоколы IPsec, IKE и IKEv2. В частности, должна использоваться подструктура преобразования в IKE и IKEv2 для задания значения каждой указанной опции независимо от использования наборов UI.

Используя наборы UI реализациям **следует** также обеспечивать интерфейс управления для задания значений отдельных криптографических опций. Таким образом, маловероятно, чтобы наборы UI давали полное решение для создания политики безопасности большинства пользователей IPsec и, следовательно, весьма желательно также наличие интерфейса с более полным набором опций.

Реализациям IPsec, использующим наборы UI, **следует** применять для наборов имена, приведенные в этом документе. Реализациям IPsec **не следует** использовать для описанных здесь наборов имена, отличающиеся от приведенных ниже, и **недопустимо** использовать приведенные в этом документе имена для наборов, не соответствующих этому документу. Эти требования важны из соображений обеспечения интероперабельности.

¹Internet Key Exchange - обмен ключами в Internet.

²В оригинале - manual keying mode. Прим. перев.

³Этот документ устарел и заменен RFC 4301. Прим. перев.

⁴User interface suite - набор пользовательских интерфейсов.

Отметим, что перечисленные здесь наборы предназначены для использования IPsec в виртуальных частных сетях (VPN¹). Для иных приложений IPsec могут быть определены свои наборы с другими именами.

Дополнительные наборы могут определяться в RFC. Имена, используемые для идентификации наборов UI, регистрируются в IANA.

2.1. Набор VPN-A

Этот набор соответствует наиболее распространенным на момент подготовки документа системам VPN, использующим IKEv1.

IPsec:

Протокол	ESP ² [RFC2406]
Шифрование ESP	TripleDES в режиме CBC [RFC2451]
Целостность ESP	HMAC-SHA1-96 [RFC2404]

ИКЕ и IKEv2:

Шифрование	TripleDES в режиме CBC [RFC2451]
Псевдослучайная функция	HMAC-SHA1 [RFC2104]
Целостность	HMAC-SHA1-96 [RFC2404]
Группа Diffie-Hellman	1024-bit Modular Exponential (MODP) [RFC2409]

Функции Rekeying of Phase 2 (для IKE) или CREATE_CHILD_SA (для IKEv2) **должны** поддерживаться обеими частями этого набора. Инициатор обмена **может** включать новый ключ Diffie-Hellman. Если ключ включен, он **должен** представлять собой 1024-битовую группу MODP. Если инициатор обмена включает ключ Diffie-Hellman, отвечающая сторона **должна** включить ключ Diffie-Hellman и этот ключ **должен** быть 1024-битовой группой MODP.

2.2. Набор VPN-B

Этот набор соответствует системам VPN, которые будут наиболее массово применяться в ближайшие несколько лет после публикации этого документа.

IPsec:

Протокол	ESP [RFC2406]
Шифрование ESP	AES со 128-битовыми ключами в режиме CBC [AES-CBC]
Целостность ESP	AES-XCBC-MAC-96 [AES-XCBC-MAC]

ИКЕ и IKEv2:

Шифрование	AES со 128-битовыми ключами в режиме CBC [AES-CBC]
Псевдослучайная функция	AES-XCBC-PRF-128 [AES-XCBC-PRF-128]
Целостность	AES-XCBC-MAC-96 [AES-XCBC-MAC]
Группа Diffie-Hellman	2048-bit MODP [RFC3526]

Функции Rekeying of Phase 2 (для IKE) или CREATE_CHILD_SA (для IKEv2) **должны** поддерживаться обеими частями этого набора. Инициатор обмена **может** включать новый ключ Diffie-Hellman. Если ключ включен, он **должен** представлять собой 2048-битовую группу MODP. Если инициатор обмена включает ключ Diffie-Hellman, отвечающая сторона **должна** включить ключ Diffie-Hellman и этот ключ **должен** быть 2048-битовой группой MODP.

2.3. Время жизни для IKEv1

IKEv1 имеет два параметра защиты, которые отсутствуют в IKEv2, а именно - время жизни ассоциаций SA³ для фазы 1 и фазы 2. Системы, использующие IKEv1 с наборами VPN-A или VPN-B, **должны** задавать для времени жизни SA значение 86400 секунд (1 сутки) для фазы 1 и 28800 секунд (8 часов) для фазы 2.

3. Благодарности

Большая часть текста этого документа и идеи заимствованы из ранних версий документа IKEv2 под редакцией Charlie Kaufman. Остальной текст и идеи были включены другими членами рабочей группы IPsec.

4. Вопросы безопасности

Этот документ наследует все связанные с безопасностью аспекты документов IPsec, IKE и IKEv2.

Некоторые из указанных в наборах опций защиты в будущем могут быть сочтены существенно более слабыми, нежели считалось во время создания этого документа.

¹Virtual private network.

²Encapsulating Security Payload.

³Security association.

5. Согласование с IANA

Агентство IANA создало и поддерживает реестр "Cryptographic Suites for IKEv1, IKEv2, and IPsec". Этот реестр состоит из текстовых строк и номеров RFC, в которых описаны соответствующие преобразования. Новые записи добавляются в реестр лишь после публикации RFC и одобрения экспертов, назначенных IESG.

Начальными значениями реестра являются:

Идентификатор	Документ
VPN-A	RFC 4308
VPN-B	RFC 4308

6. Нормативные документы

- [AES-CBC] Frankel, S., Glenn, R., and S. Kelly, "The AES-CBC Cipher Algorithm and Its Use with IPsec", RFC 3602, September 2003.
- [AES-XCBC-MAC] Frankel, S. and H. Herbert, "The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec", RFC 3566, September 2003.
- [AES-XCBC-PRF-128] Hoffman, P., "The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)", RFC 3664, January 2004.
- [IKEv2] Kaufman, C., Ed., "Internet Key Exchange (IKEv2) Protocol", [RFC 4306](#), December 2005.
- [RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", [RFC 2104](#), February 1997.
- [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 2401¹, November 1998.
- [RFC2404] Madson, C. and R. Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH", RFC 2404, November 1998.
- [RFC2406] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406², November 1998.
- [RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409³, November 1998.
- [RFC2451] Pereira, R. and R. Adams, "The ESP CBC-Mode Cipher Algorithms", RFC 2451, November 1998.
- [RFC3526] Kivinen, T. and M. Kojo, "More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)", RFC 3526, May 2003.

Адрес автора

Paul Hoffman

VPN Consortium

127 Segre Place

Santa Cruz, CA 95060

USA

E-Mail: paul.hoffman@vpnc.org

Перевод на русский язык

Николай Малых

nmalykh@protocols.ru

Полное заявление авторских прав

Copyright (C) The Internet Society (2005).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

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

¹Этот документ устарел и заменен [RFC 4301](#). Прим. перев.

²Этот документ устарел и заменен [RFC 4303](#) и [RFC 4305](#). Прим. перев.

³Этот документ устарел и заменен [RFC 4306](#), который, в свою очередь, заменен RFC 5996. Прим. перев.

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 procedures with respect to rights in RFC 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 обеспечено Internet Society.