О преимуществах использования IPsec и IKEv2 в современных VPN/FW-решениях

Валерий Смыслов
Архитектор системы, ОАО «ЭЛВИС-ПЛЮС»

Сергей Нейгер
Менеджер по маркетинговым коммуникациям, ОАО «ЭЛВИС-ПЛЮС»

В последние несколько лет аналитики и эксперты рынка ИБ (как отечественные, так и зарубежные) отмечают рост количества [1] и разнообразия [2] кибер-угроз. В этой связи ускоренными темпами развиваются и инструменты противодействия этим угрозам. Одним из таких инструментов являются межсетевые экраны и VPN/FW-решения.

В данной статье рассмотрены задачи, которые решают современные VPN/FW-продукты и преимущества, которые получают разработчики и пользователи от перехода VPN/FW-продуктов на протокол IKEv2.

Что такое «современный межсетевой экран»?

Межсетевой экран или сетевой экран — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами[3].

Однако это определение относится к межсетевым экранам в классическом их понимании. Все современные решения (и российские, и зарубежные) помимо задач межсетевого экранирования выполняют и функции построения VPN-сетей.

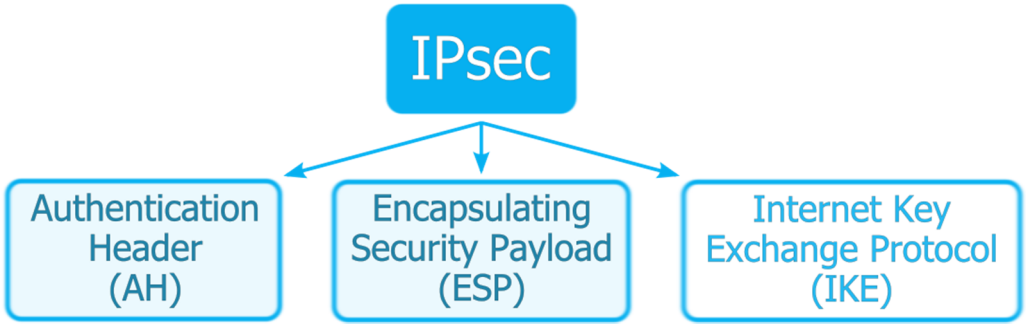
Задачи, решаемые современным VPN/FW-продуктом:

- ☑ Организация доверенных и защищённых каналов связи в рамках единой, территориально распределённой информационной системы.
- ☑ Сегментирование информационных систем.
- ☑ Защита корпоративной информационной системы от внешних угроз.
- ☑ Организация защищённого доступа удалённых (мобильных) пользователей к корпоративным ресурсам.
- ☑ Обеспечение надёжности и отказоустойчивости защищаемой информационной системы.

[1] Лаборатория Касперского, «Предварительные киберитоги и прогнозы 2011-2012».
[2] Wade Baker, Alexander Hutton, C. David Hylender и др., «2011 Data Breach Investigations Report».
[3] ru.wikipedia.org/wiki/Межсетевой_экран

Положение IKE в семействе IPsec

Прежде чем говорить о преимуществах IKEv2 над IKEv1, необходимо разобраться в том, какое место занимает этот протокол в семействе протоколов, с помощью которых реализуется технология VPN.



IPsec — это набор протоколов (protocol suite), созданный The Internet Engineering Task Force (IETF) для обеспечения безопасности в IPv4 и IPv6. IPsec стал стандартом реализации VPN-решений во всём мире, и его используют ведущие зарубежные и отечественные разработчики, работающие на российском рынке обеспечения информационной безопасности. IPsec имеет три протокола (англ. «sub protocols»):

- ☑ Authentication Header (Аутентификационный заголовок). Обеспечивает аутентификацию источника и контроль целостности пакета.
- ☑ Encapsulating Security Payload (Шифрование данных). Обеспечивает конфиденциальность и, опционально, аутентификацию источника и контроль целостности пакета.
- ☑ Internet Key Exchange Protocol (Протокол согласования ключей). Обеспечивает аутентифицированное согласование ключей.

AH и ESP — протоколы непосредственной защиты данных. Роль IKE совсем другая — он не занимается непосредственно защитой данных пользователя, но обеспечивает AH и ESP аутентифицированными ключами. Именно поэтому на схеме они выделены разными цветами.

На сегодня единственной официальной версией протокола согласования ключей является IKEv2. Предыдущая версия (IKEv1) была принята ещё в конце 1998 года. К сожалению, многие недостатки в первой версии протокола были обусловлены спешкой, в которой он разрабатывался. IKEv1 создавался группой разработчиков, в которой различались персональные взгляды на проблему и столкнулись политические амбиции компаний-работодателей этих разработчиков [4]. Поэтому протокол получился компромиссным: необходимо было учесть различные интересы этих групп. Для России у IKEv1 оказался ещё один серьёзный недостаток — в нём были чётко определены режимы шифрования, что создавало проблемы с использованием отечественного криптоалгоритма ГОСТ-28147-89 и сертификацией VPN/FW-решений на его основе[5]. Эти факторы привели к тому, что протокол стал слишком сложным для практического применения (проблема usability). Но поскольку альтернативы на тот момент не было, вендоры были вынуждены реализовывать IKEv1 в своих

[4] С. Рябко, В. Смыслов. «Безопасность IP: таинство творения».
[5] Это связано с тем, что режим Cipher Block Chaining (CBC) для ГОСТа формально не определён.

продуктах. Однако необходимость изменений в протоколе согласования ключей была очевидна всем разработчикам VPN-решений, поэтому работы в этом направлении не прекращались и, как результат, вторая версия увидела свет в конце 2005 года.

IKEv2 стал более зрелым и структурированным решением, по сравнению с IKEv1. Появилось более чёткое разделение элементов протокола, отвечающих за различные функции.

Преимущества IKEv2

I. Допускается более гибкое использование криптографических алгоритмов.

Это значительно расширяет возможности практического применения IKEv2. Разработчик (или интегратор) VPN/FW-решений может предложить заказчику использование того криптоалгоритма, который ему подходит.

II. Лучшая защита от DoS-атак.

Перед тем как однозначно аутентифицировать стороны VPN-соединения, VPN-агенты должны осуществить достаточно большое количество сетевых взаимодействий и вычислительных операций (в т. ч. и вычисление ключа по алгоритму Диффи-Хеллмана[6] (англ. Diffie-Hellman, DH)). При увеличении числа VPN-соединений, количество таких взаимодействий растёт экспоненциально[7], если используется IKEv1, и линейно[8], если используется IKEv2. Таким образом, IKEv1 существенно хуже защищён от DoS-атак, чем IKEv2. В настоящее время в связи с ростом числа и размеров ботнетов и снижением стоимости проведения DoS-атак это преимущество является ключевым.

III. Повышение эффективности использования ресурсов.

Повышение эффективности использования вычислительных ресурсов VPN-агентов достигается также и за счет использования т.н. «криптографических cookies[9]», которые позволяют проверить легитимность VPN-агента со значительно меньшими вычислительными затратами.

[6] RFC 2631. E. Rescorla. Diffie–Hellman Key Agreement Method.
[7] H. Soussi, M. Hussain, H. Afifi, D. Seret. «IKEv1 and IKEv2: A Quantitative Analyses».
[8] Там же.
[9] Изобретатель — Фил Карн (Phil Karn). Фактически эти cookies появились в предшественнике IKEv1 — протоколе Photuris, затем были использованы в IKEv1, но в процессе адаптирования подверглись профанации, в результате которой их сущность как механизма weak stateless address verification потерялась (в частности потерялась «statelessness», то есть отсутствие стейта на отвечающей стороне). В IKEv2 их использование было пересмотрено, так что изначально заложенные в них качества были возвращены.

Уменьшение количества необходимых сетевых взаимодействий снижает нагрузку на каналы передачи данных и всю сетевую инфраструктуру в целом.

IV. Исправлены замеченные криптографические ошибки.

Протокол стал более защищённым с точки зрения криптографии.

V. Существенно повышена надёжность работы протокола в условиях, когда велика вероятность потери сетевых пакетов.

Все операции теперь требуют подтверждения от другой стороны VPN-соединения.

VI. Расширения (дополнения к стандарту).

Вторая версия протокола предусматривает возможность подключения к ядру IKEv2 расширений, реализующих различный дополнительный функционал. В настоящий момент основными расширениями являются:

- ☑ RFC4555, IKEv2 Mobility and Multihoming Protocol (MOBIKE).
- ☑ RFC6311, Protocol Support for High Availability of IKEv2/IPsec.
- ☑ RFC5685, Redirect Mechanism for the Internet Key Exchange Protocol Version 2 (IKEv2).
- ☑ RFC5723, Internet Key Exchange Protocol Version 2 (IKEv2) Session Resumption.
- ☑ RFC6290, A Quick Crash Detection Method for the Internet Key Exchange Protocol (IKE).

VII. Улучшенная usability.

Поскольку спецификации протокола IKEv2 создавались в гораздо более спокойном режиме, без жёстких временных ограничений и «политических» противоречий между группами разработчиков, то протокол стал более структурированным, описание различного функционала сделано более логичным и подробным, произошло «вычищение» спецификаций.

IKEv2 в решениях зарубежных и российских разработчиков

Крупнейшие зарубежные разработчики VPN/FW-решений поддерживают семейство протоколов IPsec. Из представленных на российском рынке продуктов можно выделить решения Cisco Systems, Check Point Software Technologies, StoneSoft, Huawei. Предприятия малого и среднего бизнеса успешно используют продукты D-Link и ZyXEL.

Однако у продуктов зарубежной разработки есть достаточно серьёзные проблемы с их сертификацией в ФСБ России, которая является регулятором в сфере разработки и производства средств криптографической защиты информации. Поэтому практически весь рынок сертифицированных СКЗИ принадлежит VPN/FW-решениям отечественных разработчиков.

К сожалению, среди всех российских компаний о своих планах по разработке программного обеспечения открыто заявляет лишь ОАО «ЭЛВИС-ПЛЮС». Следующая версия VPN/FW-решения «ЗАСТАВА» будет полностью поддерживать протокол IKEv2. В настоящий момент это **единственный** отечественный продукт с заявленной поддержкой IKEv2.

Все остальные российские решения построены либо на предыдущей версии протокола (а значит им присущи многие описанные выше недостатки IKEv1), либо на своих проприетарных протоколах, что значительно ограничивает совместимость таких решений с продуктами других производителей.

Вопрос совместимости вообще является одним из самых сложных в построении защищённых корпоративных информационных систем: различные сегменты ИС могут быть построены на оборудовании и программных решениях различных вендоров. Поэтому **использование общепринятых стандартов и протоколов** в разработке VPN/FW-решений — это шаг навстречу заказчику и конечному пользователю, который будет эксплуатировать информационную систему. Такой подход снижает издержки заказчика на поддержку и администрирование своей информационной системы.

Ярким примером такого подхода к разработке является линейка продуктов «ЗАСТАВА» компании ЭЛВИС-ПЛЮС. Она состоит из трёх основных продуктов: ЗАСТАВА-Клиент, ЗАСТАВА-Офис и ЗАСТАВА-Управление.

Персональный межсетевой экран и VPN-агент «ЗАСТАВА-Клиент» обеспечивает полный набор функций сетевой защиты для **отдельных рабочих станций и мобильных пользователей** — например, при работе из Интернет, включая режим выделения мобильному пользователю внутреннего локального адреса для удаленного VPN-доступа в защищённую корпоративную сеть.

Межсетевой экран и VPN-агент «ЗАСТАВА-Офис» реализует **функции прикладного проксирования популярных сетевых сервисов и протоколов** (Telnet, FTP, SMTP, HTTP, SOCKS), а также маскирование топологии защищаемой сети в режиме VPN-туннелирования либо с использованием встроенного централизованно управляемого NAT-сервера.

«ЗАСТАВА-Управление» обеспечивает централизованное, гибкое и динамическое управление всей совокупностью агентов «ЗАСТАВА-Офис» и «ЗАСТАВА-Клиент» на основе бизнес-логики и бизнес-ролей. Это позволяет координировать корпоративную политику сетевой безопасности с бизнес-процессами и организационной структурой защищаемой информационной системы.

Благодаря использованию международных стандартов и протоколов, «ЗАСТАВА-Управление» работает не только с агентами «ЗАСТАВА-Офис» и «ЗАСТАВА-Клиент», но и обеспечивает управление конфигурациями VPN/FW-продуктов сетевой защиты лидеров зарубежного рынка информационной безопасности: Cisco IOS Router, МЭ Cisco PIX Firewall, шлюзов Check Point VPN-1/FireWall-1 Gateway, а также встроенных в ОС Microsoft 2000/XP/2003 агентов IPsec Agent.

Компания ЭЛВИС-ПЛЮС идёт в ногу со временем и предлагает своим клиентам сертифицированные решения, построенные на базе современных международных стандартов.

Игорь Шитов, Менеджер по продукту «ЗАСТАВА»: «Компания ЭЛВИС-ПЛЮС идёт в ногу со временем и предлагает своим клиентам сертифицированные решения, построенные на базе современных международных стандартов. IKEv2 будет реализован в следующей версии

продуктов «ЗАСТАВА 6.0». Данная технология сделает наш продукт уникальным на рынке отечественных сетевых решений. Технический релиз мы планируем уже в конце 2012 года, сразу после которого наши заказчики и партнёры смогут протестировать новую линейку продуктов».

Более подробную информацию о разработках компании и VPN/FW «ЗАСТАВА» можно получить на сайтах www.elvis.ru и www.zastava.ru.