Российская Академия Наук
Институт системного программирования

Security Architecture for the Internet Protocol

Архитектура безопасности для протокола IP

**RFC 4301 “Security Architecture for the Internet Protocol”
Перевод на русский язык.**

Москва 2007 г.

Список исполнителей

Исполнитель	Контактная информация	Примечания
Шнитман Виктор Зиновьевич, д.т.н., профессор	vzs@ispras.ru	Перевод.

История документа

№ версии	Дата	Примечания
1.0	01.12.2007	Перевод опубликован.

Аннотация.

В данном документе представлен перевод на русский язык основополагающего RFC 4301, регламентирующего архитектуру защиты данных IPsec на сетевом уровне стека протоколов TCP/IP.

Перевод выполнен в рамках проекта по гранту Российского фонда фундаментальных исследований № 07-07-00243 «Верификация функций безопасности протокола нового поколения IPsec v2».

Network Working Group
Request for Comments: 4301
Obsoletes: 2401
Category: Standards Track

S. Kent
K. Seo
BBN Technologies

December 2005

Security Architecture for the Internet Protocol

Архитектура безопасности для протокола IP

Статус данного меморандума

Данный документ определяет для сообщества Internet протокол, находящийся в процессе стандартизации, и требует обсуждения, а также предложений по улучшению. За информацией, касающейся состояния стандартизации и статуса данного протокола, обращайтесь, пожалуйста, к текущей версии документа "Официальные стандарты протоколов Internet" (STD 1). Распространение данного меморандума не ограничено.

Замечание относительно авторских прав

Аннотация

В данном документе описывается обновленная версия "Архитектуры безопасности для протокола IP", которая разработана для обеспечения сервисов безопасности трафику на уровне IP. Данный документ отменяет действие документа RFC 2401 (Ноябрь 1998).

Посвящение

Данный документ посвящается памяти Чарли Линна (Charlie Lynn), старейшего сотрудника BBN, который внес существенный вклад в документы IPsec.

Содержание

1. Введение

1.1. Краткое изложение содержания документа

Данный документ определяет базовую архитектуру систем, соответствующих IPsec. В нем описываются способы предоставления трафику на уровне IP множества сервисов безопасности как в среде IPv4 [Pos81a], так и в среде IPv6 [DH98]. В данном документе описываются требования к системам, которые реализуют IPsec, основные элементы таких систем, а также как эти элементы совмещаются друг с другом и со средой. В нем описываются также сервисы безопасности, предлагаемые протоколами IPsec, и как эти сервисы могут применяться в среде IP. В данном документе не рассматриваются все аспекты архитектуры IPsec. Дополнительные архитектурные детали для специализированных сред, например, использование IPsec в среде устройств трансляции сетевых адресов (NAT - Network Address Translation) и в среде с более полной поддержкой многоадресной IP-рассылки рассматриваются в других документах. Основные компоненты архитектуры безопасности IPsec обсуждаются в терминах их обязательной функциональности. Дополнительные документы RFC (см. ссылки на другие документы в подразд. 1.3) определяют протоколы, соответствующие нижеперечисленным пунктам (a), (c) и (d).

a. Протоколы безопасности – протокол аутентифицирующего заголовка (AH) и протокол инкапсулирующей защиты блока данных (ESP)
b. Контексты безопасности – что это такое и как они работают, как они управляются, связанная с ними обработка
c. Управление ключами – ручное и автоматическое (Протокол управления ключами в Internet – IKE)
d. Криптографические алгоритмы для аутентификации и шифрования

Данный документ не представляет архитектуру безопасности для Internet в целом; в нем рассматривается безопасность только на уровне IP, которая обеспечивается путем использования комбинации криптографических и протокольных механизмов безопасности.

Предпочтение отдается аббревиатуре "IPsec", которая используется в данном документе и во всех связанных с IPsec стандартах. Все другие соотношения прописных и строчных букв при написании слова IPsec (например, IPSEC, IPSec, ipsec) резко осуждаются. Однако любые соотношения прописных и строчных букв при написании "IPsec" должны пониматься как указание на протоколы IPsec.

Ключевые слова "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY" и " OPTIONAL ", которые появляются в данном документе, должны интерпретироваться так, как описано в RFC 2119 [Bra97].

1.2. Целевая аудитория

Целевой аудиторией для данного документа главным образом являются отдельные личности, которые занимаются реализацией этой технологии безопасности IP, или разрабатывают системы, использующие эту технологию. Пользователи, формально знакомые с этой технологией (конечные пользователи или системные администраторы), также являются частью целевой аудитории. В приложении A дается глоссарий, чтобы помочь заполнить пробелы в образовании или терминологии. В данном документе предполагается, что читатель знаком с протоколом IP, связанной с ним технологией построения сетей, а также с терминами и концепциями безопасности универсальных информационных систем.

1.3. Связанные документы

Как указывалось выше, детальное определение некоторых компонентов IPsec и их взаимосвязей дается в других документах. Эти документы включают RFC на следующие темы:

a. протоколы безопасности – документы RFC, описывающие протоколы аутентифицирующего заголовка (AH - Authentication Header) [Ken05b] и инкапсулирующей защиты блока данных (ESP - Encapsulating Security Payload) [Ken05a]
b. криптографические алгоритмы для обеспечения целостности и шифрования – один документ RFC, определяющий обязательные, применяемые по умолчанию алгоритмы, которые используются совместно с AH и ESP [Eas05], другой подобный документ RFC, определяющий обязательные алгоритмы для использования совместно с IKEv2 [Sch05], а также отдельные документы RFC для каждого криптографического алгоритма.
c. автоматическое управление ключами – документы RFC протокола управления ключами в Internet (IKEv2) [Kau05] и криптографических алгоритмов, которые используются во второй версии протокола управления ключами в Internet (IKEv2) [Sch05].

2. Цели проекта

2.1. Описание задач, целей, требований и проблем

IPsec разрабатывается с целью предоставления протоколам IPv4 и IPv6 высококачественных средств обеспечения безопасности, основанных на криптографии и обладающих свойством интероперабельности. Предлагаемый набор сервисов безопасности включает контроль доступа, целостность дейтаграмм, аутентификацию источника данных, обнаружение и отклонение повторно воспроизводимых сообщений (вид частичной целостности последовательности сообщений), конфиденциальность (с помощью шифрования) и ограниченную конфиденциальность потоков трафика. Эти сервисы предоставляются на уровне IP, предлагая стандартный метод защиты для всех протоколов, которые могут работать поверх IP (включая сам IP).

IPsec включает спецификацию минимальной функциональности межсетевых экранов, поскольку она является существенным аспектом организации контроля доступа на уровне IP. Реализации без каких-либо ограничений могут предоставлять более изощренные механизмы межсетевого экранирования и реализовывать обязательную для IPsec функциональность с помощью этих более изощренных механизмов. (Заметим, что в случае наложения реализацией IPsec дополнительных ограничений межсетевого экранирования на потоки трафика, интероперабельность может пострадать, но такие дополнительные ограничения не могут быть согласованы с помощью свойств селекторов трафика, определенных в данном документе, а также с помощью IKEv2). Функция межсетевого экранирования IPsec использует принудительно криптографически защищенные средства аутентификации и обеспечения целостности, предоставляемые всему трафику IPsec, что обеспечивает более полный контроль доступа по сравнению с использованием межсетевого экрана (не осведомленного о внутренних параметрах IPsec) и отдельных средств криптографической защиты.

Большинство сервисов безопасности предоставляются посредством двух протоколов обеспечения безопасности трафика, аутентифицирующего заголовка (AH) и инкапсулирующей защиты блока данных (ESP), а также посредством процедур и протоколов управления криптографическими ключами. Множество протоколов IPsec, применяемых в некотором контексте, а также способы их применения будут определяться пользователями или администраторами этого контекста. Задачей архитектуры IPsec является гарантия того, что соответствующие ей реализации будут включать сервисы и интерфейсы управления, необходимые для удовлетворения требований большого числа пользователей.

При правильной реализации и развертывании IPsec, он не может неблагоприятно влиять на пользователей, хосты и другие компоненты Internet, которые для защиты трафика IPsec не применяют. Протоколы безопасности IPsec (AH и ESP, и в меньшей степени IKE) разрабатываются так, чтобы не зависеть от

криптографических алгоритмов. Такая модульность допускает выбор различных наборов криптографических алгоритмов по обстановке, не оказывая влияния на другие части реализации. Например, различные сообщества пользователей могут выбирать, в случае необходимости, различные наборы криптографических алгоритмов (создавая группы с принудительно используемыми средствами криптографии).

Для упрощения интероперабельности в глобальной сети Internet в [Eas05] специфицируется набор используемых по умолчанию криптографических алгоритмов для работы совместно с AH и ESP, а в [Sch05] – набор обязательных для реализации алгоритмов для IKEv2. Документы [Eas05] и [Sch05] будут периодически обновляться, чтобы не отставать от достижений в области вычислений и криптологии. Благодаря специфицированию этих алгоритмов в документах, которые отделены от спецификаций AH, ESP и IKEv2, эти алгоритмы могут обновляться или заменяться, не оказывая влияния на процесс стандартизации остального набора документов IPsec. Использование этих криптографических алгоритмов совместно с протоколами защиты трафика и управления ключами IPsec подразумевает возможность развертывания разработчиками систем и приложений высококачественной криптографической технологии безопасности уровня IP.

2.2. Предупреждения и предположения

Семейство протоколов IPsec и связанные с ним криптографические алгоритмы разработаны для обеспечения высококачественной безопасности трафика в Internet. Однако безопасность, предоставляемая этими протоколами, в конечном счете, зависит от качества их реализации, которое выходит за рамки данного набора стандартов. Более того, безопасность вычислительной системы или сети зависит от многих факторов, в частности от правил работы с персоналом, процедурных ограничений, компрометирующих излучений и правил эксплуатации систем компьютерной безопасности. Таким образом, IPsec является только частью всеобъемлющей архитектуры безопасности системы.

Наконец, безопасность, предоставляемая благодаря использованию IPsec, критически зависит от многих аспектов операционной среды, в которой выполняется реализация IPsec. Например, дефекты в безопасности операционной системы, плохое качество источников случайных чисел, нестабильные протоколы управления и правила эксплуатации систем и т.д. могут свести на нет безопасность, предоставляемую IPsec. Как указывалось выше, ни один из этих параметров среды не входит в рамки данного стандарта, а также других стандартов IPsec.

3. Общее представление о системе

В данном разделе представлено высокоуровневое описание того, как работает IPsec, компонентов системы, а также того, как они взаимодействуют для обеспечения указанных выше сервисов безопасности. Цель данного описания заключается в том, чтобы позволить читателю представить общую "картину" процесса или системы, увидеть, как она вписывается в среду IP, и чтобы создать контекст для последующих разделов данного документа, которые более подробно описывают каждый компонент.

Реализация IPsec работает в хосте в качестве защитного шлюза или в качестве независимого устройства, предоставляющего защиту IP-трафику. (Защитный шлюз представляет собой промежуточную систему, реализующую IPsec, например, межсетевой экран или маршрутизатор с включенной функцией IPsec). Более подробно эти классы реализаций описаны ниже в подразд. 3.3. Защита, предлагаемая IPsec, базируется на требованиях, определяемых базой данных политики безопасности (SPD - Security Policy Database), устанавливаемой и поддерживаемой пользователем или системным администратором, либо приложением, работающим в рамках ограничений, устанавливаемых пользователем или системным администратором. В общем случае пакеты, которые сопоставляются с элементами SPD, отбираются на основе информации IP и заголовка следующего уровня (селекторы, пп. 4.4.1.1) для одного из трех выполняемых при обработке

действий. Каждый пакет, базируясь на соответствующих политиках SPD, определяемых селекторами, либо защищается (PROTECTed), используя сервисы безопасности IPsec, либо отбрасывается (DISCARDed), либо ему позволяется игнорировать (BYPASS) защиту IPsec.

3.1. Что делает IPsec

IPsec создает границу между защищенными и незащищенными интерфейсами для хоста или для сети (см. ниже рис. 1). Трафик, пересекающий границу, является объектом средств управления доступом, которые определяются пользователем или администратором, отвечающим за конфигурирование IPsec. Эти средства управления указывают, пересекут ли пакеты границу беспрепятственно, будут ли им предоставляться сервисы безопасности посредством AH или ESP, или они будут отбрасываться. Сервисы безопасности IPsec предлагаются на уровне IP путем выбора соответствующих протоколов безопасности, криптографических алгоритмов и криптографических ключей. IPsec может использоваться для защиты одного или нескольких "маршрутов" (a) между парой хостов, (b) между парой защитных шлюзов или (c) между защитным шлюзом и хостом. Реализация хоста, соответствующая данной спецификации, должна (MUST) поддерживать (a) и (c), а защитный шлюз, соответствующий данной спецификации, должен поддерживать все три вида коннективности, поскольку при определенных обстоятельствах защитный шлюз действует как хост.

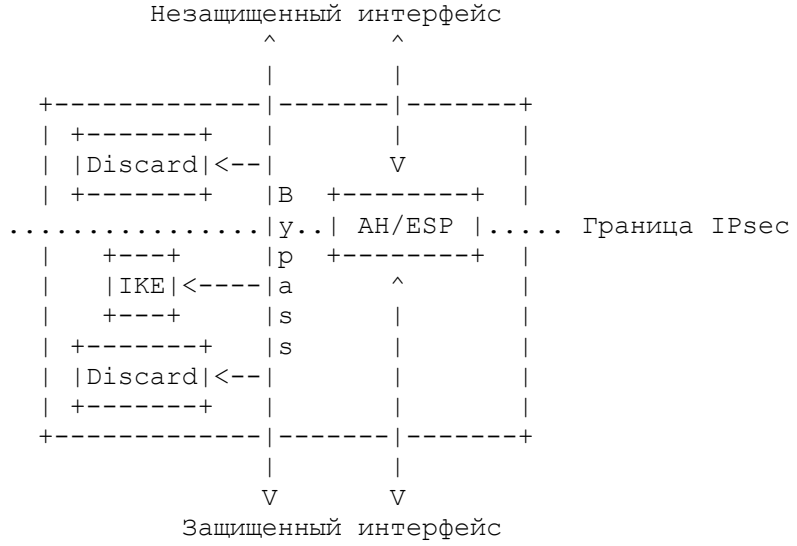

Рис. 1. Высокоуровневая модель обработки IPsec.

На этой диаграмме термин "незащищенный" (unprotected) относится к интерфейсу, который может быть также описан как "черный" (black) или "зашифрованный текст" (ciphertext). Термин "защищенный" (protected) относится к интерфейсу, который может быть также описан как "красный" (red) или "открытый текст" (plaintext). Указанный выше защищенный интерфейс может быть внутренним, например, в реализации IPsec для хоста защищенный интерфейс может быть связан с интерфейсом уровня сокетов, предоставляемым ОС. В данном документе термин "входящий" (inbound) относится к трафику, который поступает в реализацию IPsec через незащищенный интерфейс или порождается реализацией на незащищенной стороне границы и адресуется в направлении защищенного интерфейса. Термин "исходящий" (outbound) относится к трафику, который поступает в реализацию через защищенный интерфейс или порождается реализацией на защищенной стороне границы и адресуется в направлении незащищенного интерфейса. Реализация IPsec может поддерживать более одного интерфейса на любой стороне или обеих сторонах границы.

Обратите внимание на средства отбрасывания трафика на обеих сторонах границы IPsec, средство обхода (BYPASS), которое позволяет трафику пересекать границу

без криптографической защиты, и указатель на IKE в качестве функции управления ключами и безопасностью защищенной стороны.

В качестве опции IPsec поддерживает согласование IP-компрессии [SMPT01], частично оправданной наблюдением того факта, что когда в IPsec применяется шифрование, оно препятствует эффективной компрессии данных протоколами нижнего уровня.

3.2. Как работает IPsec

Для обеспечения сервисов безопасности трафика IPsec использует два протокола: протокол аутентифицирующего заголовка (AH - Authentication Header) и протокол инкапсулирующей защиты блока данных (ESP - Encapsulating Security Payload). Оба протокола более подробно описываются в соответствующих документах RFC [Ken05b, Ken05a]. Реализации IPsec должны (MUST) поддерживать ESP и могут (MAY) поддерживать AH. (Поддержка AH была переведена в более низкую категорию (MAY), поскольку опыт показал, что существует очень мало контекстов, в которых ESP не может обеспечить требуемые сервисы безопасности. Заметим, что ESP может использоваться для обеспечения только целостности без конфиденциальности, что в большинстве контекстов делает его сравнимым с AH).

- Протокол аутентифицирующего заголовка (AH) [Ken05b] предлагает целостность и аутентификацию источника данных, с факультативной возможностью (по усмотрению приемника) защиты от повторного воспроизведения.

- Протокол инкапсулирующей защиты блока данных (ESP) [Ken05a] предлагает тот же самый набор сервисов, а также конфиденциальность. Использование ESP для конфиденциальности без обеспечения целостности не рекомендуется (NOT RECOMMENDED). Когда ESP используется с включенной конфиденциальностью, предпринимаются меры предосторожности для обеспечения ограниченной конфиденциальности потоков трафика, т.е. меры для сокрытия длины пакетов, а также для упрощения эффективного формирования пакетов и отбрасывания фиктивных пакетов. Вероятно, такая возможность будет эффективной главным образом в контекстах VPN и наложенных сетей.

- Оба протокола, AH и ESP, предлагают контроль доступа, осуществляемый посредством распределения криптографических ключей и управления потоками трафика в соответствии с предписаниями базы данных политики безопасности (SPD - Security Policy Database, п. 4.4.1).

Эти протоколы могут применяться по отдельности или в комбинации друг с другом для обеспечения сервисов безопасности IPv4 и IPv6. Однако большинство требований безопасности могут быть удовлетворены при использовании одного протокола ESP. Каждый протокол поддерживает два режима использования: транспортный режим и туннельный режим. В транспортном режиме AH и ESP обеспечивают защиту главным образом для протоколов следующего уровня; в туннельном режиме AH и ESP применяются для туннелирования IP-пакетов. Различия между этими двумя режимами обсуждаются в подразд. 4.1.

IPsec позволяет пользователю (или системному администратору) контролировать степень детализации, с которой предлагаются сервисы безопасности. Например, можно создать один зашифрованный туннель для передачи всего трафика между двумя защитными шлюзами или можно создать отдельный зашифрованный туннель для каждого соединения TCP между каждой парой хостов, осуществляющих обмен информацией через эти защитные шлюзы. IPsec, благодаря парадигме управления SPD, включает средства для указания:

- Какой протокол безопасности (AH или ESP) применять, режим (транспортный или туннельный), опции сервисов безопасности, какие криптографические алгоритмы использовать, а также в каких комбинациях использовать специфицированные протоколы и сервисы.

- Степени детализации, с которой должна применяться защита.

Поскольку большинство сервисов безопасности, предоставляемых IPsec, требуют использования криптографических ключей, IPsec зависит от отдельного набора механизмов для установления этих ключей. Данный документ требует поддержки как ручного, так и автоматического распределения ключей. В нем для автоматического управления ключами специфицируется конкретный подход, базирующийся на открытых ключах (IKEv2 [Kau05]), но могут (MAY) использоваться и другие методы автоматического распределения ключей.

Примечание: Данный документ предоставляет поддержку нескольким функциям, поддержка которых доступна в IKEv2, но не в IKEv1, например, согласование контекста безопасности, представляющего диапазоны локальных и удаленных портов или согласование нескольких SA с одними и теми же селекторами. Поэтому данный документ предполагает использование IKEv2 или системы управления ключами и контекстами безопасности со сравнимыми свойствами.

3.3. Где может быть реализован IPsec

Имеется много способов реализации IPsec либо в хосте, либо в совокупности с маршрутизатором или межсетевым экраном для создания защитного шлюза, либо в качестве независимого устройства защиты.

a. IPsec может быть интегрирован в естественный IP-стек. Такой подход требует доступа к исходным кодам IP и применим как к хостам, так и к защитным шлюзам, хотя естественные реализации в хосте, как пояснено позже (п. 4.4.1, абзац 6; пп. 4.4.1.1, последний абзац), в наибольшей степени могут воспользоваться преимуществами такой стратегии.

b. В реализации типа "вставки в стек" (BITS - bump-in-the-stack), IPsec реализуется "ниже" существующей реализации стека протоколов IP, между драйвером родного IP и драйвером локальной сети. В этом контексте доступ к исходному коду IP-стека не требуется, что делает такой подход к реализации приемлемым для использования в унаследованных системах. Если выбирается такой подход, то обычно он применяется в хостах.

c. Использование специального процессора протокола безопасности, устанавливаемого на линии связи, является распространенной особенностью разработки систем, используемых военными, а также в некоторых коммерческих системах. Иногда его называют реализацией типа "вставки в линию" (BITW - bump-in-the-wire). При поддержке одного хоста такая реализация может быть почти аналогичной реализации BITS, но при поддержке маршрутизатора или межсетевого экрана она должна работать как защитный шлюз.

В данном документе часто идет речь в терминах использования IPsec хостом или защитным шлюзом безотносительно к тому, является ли реализация естественной, выполнена ли она в виде BITS или в виде BITW. Когда различия между этими возможными видами реализации оказываются существенными, в документе дается указание на конкретные подходы к реализации.

4. Контексты безопасности

Данный раздел определяет требования к управлению контекстами безопасности для всех реализаций IPv6, а также для тех реализаций IPv4, которые реализуют протокол AH, протокол ESP или оба протокола AH и ESP. Концепция "контекста безопасности" (SA - Security Association) для IPsec является главной. Как AH, так и ESP используют контексты безопасности, а главной функцией IKE является установление и поддержка контекстов безопасности. Все реализации AH или ESP должны (MUST) поддерживать концепцию SA так, как описано ниже. В оставшейся части данного раздела описаны различные аспекты управления контекстами безопасности путем определения параметров, требуемых для управления политиками SA, и методов управления SA.

4.1. Определение и область действия

Контекст безопасности (SA) представляет собой симплексное "соединение", которое предоставляет сервисы безопасности трафику, который по нему передается. Сервисы безопасности предоставляются некоторому контексту безопасности путем использования либо протокола AH, либо протокола ESP, но не обоих протоколов. Если к потоку трафика применяется защита обоих протоколов AH и ESP, то должны создаваться и координироваться два контекста безопасности для осуществления защиты путем итеративного применения этих протоколов безопасности. Чтобы защитить типичный двунаправленный обмен информацией между двумя системами, включающими IPsec, требуется пара SA (по одному в каждом направлении). В знак признания этого общего требования по применению протокол IKE явно создает пары SA.

Для SA, используемого для передачи индивидуального (unicast) трафика, одного индекса параметров безопасности (SPI - Security Parameters Index, см. приложение A, спецификации AH [Ken05b] и ESP [Ken05a]) достаточно, чтобы определить SA. Однако, в качестве частного решения для идентификации SA, реализация может отдать предпочтение использованию SPI в совокупности с типом протокола IPsec (AH или ESP). Если реализация IPsec поддерживает передачу группового (multicast) трафика, то она должна (MUST) поддерживать групповые контексты безопасности (multicast SAs), используя представленный ниже алгоритм для отображения входящих IPsec-дейтаграмм на контексты безопасности. Реализации, поддерживающие только индивидуальный трафик, не нуждаются в реализации этого алгоритма демультиплексирования.

Во многих архитектурах передачи группового (multicast) трафика (или anycast-трафика), например в [RFC3740], центральный контроллер группы или сервер ключей (Group Controller/Key Server) в одностороннем порядке присваивает SPI групповому контексту безопасности (GSA - Group Security Association). Это присваивание SPI не согласуется с подсистемами управлением ключами (например, IKE), которые размещаются в отдельных оконечных системах, образующих группу, или не координируется ими. Следовательно, имеется вероятность того, что GSA и индивидуальный (unicast) SA будут одновременно использовать один и тот же SPI. Реализация IPsec, допускающая передачу группового трафика, должна (MUST) правильно демультиплексировать входящий трафик даже в контексте коллизий SPI.

Каждый элемент в базе данных контекстов безопасности (SAD - SA Database) (п. 4.4.2) должен указывать, используются ли при поиске SA кроме SPI IP-адрес места назначения, или IP-адреса источника и места назначения. Для групповых (multicast) SA поле протокола для поиска SA не применяется. Для каждого входящего пакета, защищенного IPsec, реализация должна выполнять поиск в SAD таким образом, чтобы в результате он находил элемент, который совпадает с "наиболее длинным" идентификатором SA. В этом контексте, если два или большее число элементов SAD совпадают по значению SPI, то элемент, который совпадает также по адресу места назначения или по адресам источника и места назначения (что указано в элементе SAD) обеспечивает "наиболее длинное" совпадение. Это предполагает следующий логический порядок поиска в SAD:

1. Поиск в SAD на совпадение комбинации SPI, адреса места назначения и адреса источника. Если элемент SAD подходит, то обработать входящий пакет в соответствии с этим подходящим элементом SAD. В противном случае перейти к шагу 2.

2. Поиск в SAD на совпадение комбинации SPI и адреса места назначения. Если элемент SAD подходит, то обработать входящий пакет в соответствии с этим подходящим элементом SAD. В противном случае перейти к шагу 3.

3. Поиск в SAD на совпадение только по SPI, если получатель принял решение поддерживать одно пространство SPI для протоколов AH и ESP, или в противном случае на совпадение комбинации SPI и протокола. Если элемент SAD подходит, то обработать входящий пакет в соответствии с этим подходящим элементом SAD. В противном случае отбросить пакет и записать в журнал событие, подлежащее аудиту.

На практике реализация может отдать предпочтение любому методу ускорения этого поиска (или не применять никаких методов ускорения), хотя ее наблюдаемое извне поведение должно (MUST) быть функционально эквивалентно поиску в SAD в указанном выше порядке. Например, программная реализация может осуществлять индексирование хэш-таблицы с помощью SPI. Элементы SAD в каждом связанном списке хэш-таблицы участков памяти, адресуемых как единое целое, могли бы быть отсортированы так, чтобы элементы SAD с наиболее длинными идентификаторами SA в этом списке находились в его начале. Элементы SAD, имеющие самые короткие идентификаторы SA, могли бы быть отсортированы так, чтобы в этом списке они находились в конце. Аппаратная реализация могла бы в действительности выполнять поиск наиболее длинного совпадения, используя особенности обычно доступной адресуемой по содержимому памяти с тремя элементами (TCAM0 - Ternary Content-Addressable Memory).

Указание требования соответствия адреса источника и места назначения для отображения входящего IPsec-трафика на SA должно (MUST) устанавливаться либо в виде побочного эффекта ручного конфигурирования SA, либо посредством согласования с помощью протокола управления SA, например, IKE или GDOI [RFC3547]. Обычно группы с конкретным источником группового трафика (SSM - Source-Specific Multicast) [HC03] используют трехэлементный идентификатор SA, состоящий из SPI, группового адреса места назначения и адреса источника. Контекст безопасности группы с произвольным источником группового трафика (Any-Source Multicast) требует в качестве идентификатора только SPI и группового адреса места назначения.

Если по одному и тому же SA посылаются различные классы трафика (различаемые битами DSCP - Differentiated Services CodePoint [NiBlBaBL98], [Gro02]), и если получатель применяет факультативную функцию защиты от повторного воспроизведения, доступную как в AH, так и в ESP, то из-за механизма отсечения, используемого этой функцией, это может приводить к неуместному отбрасыванию низкоприоритетных пакетов. Поэтому, чтобы качество обслуживания (QoS - Quality of Service) поддерживать соответствующим образом, отправитель должен (SHOULD) направлять трафик различных классов, но с одними и теми же значениями селекторов, на разные SA. Чтобы это разрешить, реализация IPsec должна (MUST) разрешать установление и поддержание нескольких SA между заданными отправителем и получателем с одними и теми же селекторами. Распределение трафика между этими параллельными SA для поддержки QoS определяется локально отправителем и с помощью IKE не согласуется. Получатель должен (MUST) без предубеждения обрабатывать пакеты из различных SA. Эти требования применяются как к SA транспортного режима, так и к SA туннельного режима. В случае SA туннельного режима значения битов DSCP в вопросе появляются во внутреннем IP-заголовке. В транспортном режиме значение DSCP может поменяться по дороге, но это не должно приводить к проблемам обработки IPsec, поскольку это значение не применяется для выбора SA и не должно (MUST NOT) проверяться как часть подтверждения правильности SA или пакета. Однако, если в SA происходит существенное переупорядочивание пакетов, например в результате произошедших по дороге изменений значений DSCP, то это может привести к отбрасыванию пакетов приемником из-за применения механизма предотвращения повторного воспроизведения пакетов.

ОБСУЖДЕНИЕ: Хотя поля DSCP [NiBlBaBL98, Gro02] и явного уведомления о перегрузке (ECN - Explicit Congestion Notification) [RaFlBl01] не являются "селекторами", поскольку именно этот термин используется в данной архитектуре, отправителю необходим механизм для направления пакетов с заданными значениями (множеством значений) DSCP по соответствующему SA. Такой механизм может быть назван "классификатором" (classifier).

Как указано выше, определены два типа SA: транспортного режима и туннельного режима. IKE создает пары SA, поэтому для упрощения мы решили потребовать, чтобы оба контекста безопасности (SA) в паре были одного и того же типа, либо транспортного, либо туннельного.

SA транспортного режима представляет собой контекст безопасности, который обычно применяется между парой хостов для обеспечения сквозных сервисов безопасности. Когда желательно обеспечить безопасность между двумя промежуточными системами, находящимися на пути пакетов (в отличие от сквозного использования IPsec), между защитными шлюзами или между защитным шлюзом и хостом может (MAY) использоваться транспортный режим. В случае, когда между защитными шлюзами или между защитным шлюзом и хостом используется транспортный режим, такой транспортный режим может применяться для поддержки туннелирования в IP через контексты безопасности транспортного режима (например, IP-in-IP [Per96], туннелирования GRE [FaLiHaMeTr00] или динамической маршрутизации [ToEgWa04]). Более точно, использование транспортного режима промежуточной системой (например, защитным шлюзом) разрешается, только если он применяется для пакетов, адрес источника которых (для исходящих пакетов) или адрес места назначения которых (для входящих пакетов) совпадает с адресом, принадлежащим самой промежуточной системе. В этом контексте функции контроля доступа, являющиеся важной частью IPsec, существенно ограничены, поскольку они не могут применяться к сквозным заголовкам пакетов, которые проходят по используемому таким способом SA транспортного режима. Таким образом, перед применением в конкретном контексте этот способ использования транспортного режима должен тщательно оцениваться.

В IPv4 заголовок протокола безопасности в транспортном режиме появляется непосредственно после IP-заголовка и любых опций и перед любым протоколом следующего уровня (например, TCP или UDP). В IPv6 заголовок протокола безопасности появляется после основного IP-заголовка и выбранных заголовков расширения, но может появляться до и после опций места назначения; он должен (MUST) появляться до протоколов следующего уровня (например, TCP, UDP, SCTP). В случае ESP, SA транспортного режима обеспечивает сервисы безопасности только для этих протоколов следующего уровня, а не для IP-заголовка или какого-либо заголовка расширения, предшествующего заголовку ESP. В случае AH, защита распространяется также на выбранные части предшествующего ему IP-заголовка, выбранные части заголовков расширения, а также выбранные опции (содержащиеся в заголовке IPv4, в заголовке расширения Hop-by-Hop IPv6 или в заголовках расширения места назначения IPv6). Более подробную информацию о покрытии, осуществляемом AH, см. в спецификации AH [Ken05b].

SA туннельного режима по существу представляет собой контекст безопасности, используемый для IP-туннеля с контролем доступа, который применяется к заголовкам трафика, находящегося внутри туннеля. Два хоста могут (MAY) установить между собой SA туннельного режима. Кроме указанных ниже двух исключений, каждый раз, когда любым из концов SA является защитный шлюз, этот SA должен (MUST) быть контекстом безопасности туннельного режима. Таким образом, SA между двумя защитными шлюзами, как и SA между хостом и защитным шлюзом, обычно представляют собой SA туннельного режима. Имеются следующие два исключения.

- Когда трафик предназначен для защитного шлюза, например, команд SNMP, защитный шлюз работает как хост, и использование транспортного режима разрешается. В этом случае SA заканчивается в (управляющей) функции хоста в защитном шлюзе и, таким образом, заслуживает другой обработки.

- Как отмечено выше, шлюзы безопасности могут (MAY) поддерживать SA транспортного режима для обеспечения безопасности IP-трафика между двумя промежуточными системами, находящимися на пути пакетов, например, между хостом и защитным шлюзом или между двумя защитными шлюзами.

Использование туннельного режима для контекста безопасности, связанного с защитным шлюзом, мотивируется несколькими моментами, вызывающими беспокойство. Например, если существует несколько путей к одному и тому же месту назначения, находящемуся за защитным шлюзом (например, через различные защитные шлюзы), важно, чтобы пакет IPsec посылался на защитный шлюз, с которым был согласован SA. Подобным образом, для пакета, который по пути мог быть фрагментирован, все пакеты фрагментов должны быть доставлены одному и тому же экземпляру IPsec для реассемблирования до криптографической

обработки. Кроме того, когда фрагмент обрабатывается IPsec и передается, а затем по пути фрагментируется, то необходимо, чтобы существовали внутренний и внешний заголовки, чтобы сохранить данные о состоянии фрагментации для пре- и пост-IPsec форматов пакетов. Поэтому когда один из концов SA представляет собой защитный шлюз, существует несколько причин применения туннельного режима. (Использование туннеля IP-in-IP в совокупности с транспортным режимом также может решить эти проблемы фрагментации. Однако такая конфигурация ограничивает возможность IPsec осуществлять для трафика политики контроля доступа).

Примечание: AH и ESP не могут применяться в транспортном режиме к пакетам IPv4, которые представляют собой фрагменты. В этих случаях может применяться только туннельный режим. Для IPv6 в принципе существует возможность передавать фрагмент открытого текста по SA транспортного режима; однако для упрощения данное ограничение применяется также и к пакетам IPv6. Более подробную информацию об обработке фрагментов открытого текста на защищенной стороне границы IPsec см. в разд. 7.

Для SA туннельного режима имеется "внешний" IP-заголовок, который определяет источник и место назначения IPsec-обработки, а также "внутренний" IP-заголовок, который определяет (очевидно) первоначальные источник и место назначения пакета. Заголовок протокола безопасности появляется после внешнего IP-заголовка и перед внутренним IP-заголовком. Если AH применяется в туннельном режиме, то (как указано выше) защита предоставляется частям внешнего IP-заголовка, а также всему туннелируемому пакету (т.е. защищается весь внутренний IP-заголовок, а также протоколы следующего уровня). Если применяется ESP, то защита предоставляется только туннелируемому пакету, но не внешнему заголовку.

В итоге:

a) Реализация IPsec в хосте должна (MUST) поддерживать как транспортный, так и туннельный режим. Это справедливо для реализаций в хосте в виде BITS, BITW и в естественном виде.

b) Защитный шлюз должен (MUST) поддерживать туннельный режим и может (MAY) поддерживать транспортный режим. Если он поддерживает транспортный режим, то последний должен использоваться только когда защитный шлюз работает как хост, например, для управления сетью или для обеспечения безопасности между двумя промежуточными системами, находящимися на пути пакетов.

4.2. Функциональность SA

Набор сервисов безопасности, предлагаемых контекстом безопасности, зависит от выбранного протокола безопасности, режима SA, оконечных точек SA и от выбора дополнительных сервисов в рамках протокола.

Например, как AH, так и ESP предлагают сервисы обеспечения целостности и аутентификации, но покрытие отличается для каждого протокола и отличается между транспортным и туннельным режимами. Если по пути между отправителем и получателем должна защищаться целостность опции IPv4 или заголовка расширения IPv6, то AH может предоставить такой сервис, за исключением случаев, когда IP-заголовок и заголовок расширения могут меняться непредсказуемым для отправителя способом. Однако в некоторых контекстах тот же самый уровень безопасности может быть достигнут путем применения ESP к туннелю, передающему пакет.

Предоставляемая степень детализации контроля доступа обуславливается выбором селекторов, которые определяют каждый SA. Более того, средства аутентификации, применяемые партнерами IPsec, например, во время создания IKE SA (по сравнению с дочерним SA), также влияют на степень детализации предоставляемого контроля доступа.

Если выбрана конфиденциальность, то ESP SA (туннельного режима) между двумя защитными шлюзами может предложить частичную конфиденциальность потоков трафика. Использование туннельного режима позволяет зашифровать внутренние IP-заголовки, скрывая идентификаторы (первоначальных) источника и места назначения трафика. Более того, чтобы скрыть размер пакетов, может быть также осуществлено дополнение блока данных заполнителем ESP, что позволяет еще больше скрыть внешние характеристики трафика. Подобные сервисы конфиденциальности потоков трафика могут быть предложены в коммутируемом (dialup) контексте, когда мобильному пользователю присваивается динамический IP-адрес, и он устанавливает ESP SA (туннельного режима) с корпоративным межсетевым экраном (работающим в качестве защитного шлюза). Заметим, что контексты безопасности с высокой степенью детализации, как правило, оказываются более уязвимыми к анализу трафика по сравнению с контекстами безопасности, имеющими низкую степень детализации, которые передают трафик от многих абонентов.

Примечание: Реализация, соответствующая данной спецификации, не должна (MUST NOT) позволять создавать ESP SA, в котором применяется как нулевое шифрование, так и отсутствует алгоритм обеспечения целостности. Попытка согласовать такой SA является событием, которое должно подвергаться аудиту как инициатором, так и ответчиком. Элемент журнала аудита для такого события должен (SHOULD) включать текущие дату и время, локальный IP-адрес IKE и удаленный IP-адрес IKE. Инициатор должен (SHOULD) записать соответствующий элемент SPD.

4.3. Комбинирование контекстов безопасности

Данный документ не требует поддержки вложенных контекстов безопасности или того, что RFC 2401 называет "связкой контекстов безопасности" (SA bundles). Эти функции могут быть осуществлены путем соответствующего конфигурирования как SPD, так и локальных функций пересылки (для входящего и исходящего трафика), но эта возможность находится за рамками модуля IPsec и, следовательно, области действия данной спецификации. В результате управление вложенными или связанными контекстами безопасности оказывается потенциально более сложным и менее обеспеченным, чем в модели, предполагаемой в RFC 2401. Реализация, которая обеспечивает поддержку вложенных SA, должна (SHOULD) предоставлять интерфейс управления, который позволяет пользователю или администратору выразить требование вложенности и затем создать соответствующие элементы SPD и элементы таблицы пересылки, чтобы осуществить требуемую обработку. (См. в приложении E пример того, как конфигурировать вложенные SA).

4.4. Основные базы данных IPsec

Многие детали, связанные с обработкой IP-трафика в реализации IPsec, в значительной степени являются локальным вопросом, а не предметом стандартизации. Однако некоторые внешние аспекты обработки должны быть стандартизованы, чтобы гарантировать интероперабельность и чтобы обеспечить минимальную возможность управления, что существенно для продуктивного использования IPsec. Для поддержки этих задач обеспечения интероперабельности и функциональности в данном подразделе описывается общая модель обработки IP-трафика, связанная с функциональностью IPsec. Описанная ниже модель является формальной; реализации не должны придерживаться деталей этой модели в том виде, в котором они представлены, но внешнее поведение реализаций для обеспечения соответствия настоящей спецификации должно (MUST) быть аналогичным наблюдаемым извне характеристикам этой модели.

В этой модели имеются три формальные базы данных: база данных политики безопасности (SPD - Security Policy Database), база данных контекстов безопасности (SAD - Security Association Database) и база данных авторизации партнеров (PAD - Peer Authorization Database). Первая база данных устанавливает политики, которые определяют распределение всего входящего или исходящего IP-трафика хоста или защитного шлюза (п. 4.4.1). Вторая база данных содержит параметры, которые ассоциируются с каждым установленным

(снабженным ключами) SA (п. 4.4.2). Третья база данных, база данных авторизации партнеров, обеспечивает связь между протоколом управления SA, подобным IKE, и SPD (п. 4.4.3).

Несколько отдельных контекстов IPsec

Если реализация IPsec работает в качестве защитного шлюза для нескольких абонентов, то она может (MAY) реализовывать несколько отдельных контекстов IPsec. Каждый контекст может (MAY) иметь и может (MAY) использовать полностью независимые идентификаторы, политики, контексты безопасности управления ключами и/или IPsec SA. Это в значительной степени является локальным вопросом реализации. Однако средство для привязки входящих предложений (SA) к локальным контекстам требуется. С этой целью, в случае поддержки используемым протоколом управления ключами, идентификаторы контекстов могут (MAY) передаваться от инициатора к ответчику в сигнальных сообщениях с таким результатом, что IPsec SA создаются с привязкой к конкретному контексту. Например, защитный шлюз, который предоставляет VPN-сервис нескольким потребителям, будет способным ассоциировать трафик каждого потребителя с правильной сетью VPN.

Выбор пересылки или выбор безопасности

Чтобы обеспечить широкий ряд контекстов, в которых может применяться IPsec, описанная здесь модель IPsec включает ясное разделение между выбором пересылки (маршрутизации) и выбором безопасности. Пересылка может быть тривиальной в том случае, когда имеется только два интерфейса. Либо она может быть сложной, например, если имеется несколько защищенных или незащищенных интерфейсов или если контекст, в котором реализуется IPsec, применяет сложную функцию пересылки. IPsec предполагает только, что исходящий и входящий трафик, который прошел обработку IPsec, пересылается способом, согласованным с контекстом, в котором реализуется IPsec. Поддержка вложенных SA является необязательной возможностью; если такая возможность необходима, то она требует координации между таблицами пересылки и элементами SPD, чтобы пакет мог пересечь границу IPsec более одного раза.

"Локальный" или "удаленный"

В данном документе термины "локальный" и "удаленный" используются для выражения правил политики по отношению к IP-адресам и портам. Термин "локальный" указывает на объект, защищаемый реализацией IPsec, например, адрес/порт "источника" исходящих пакетов или адрес/порт "места назначения" входящих пакетов. Термин "удаленный" указывает на объект партнера или объекты партнера. Термины "источник" и "место назначения" используются для полей заголовка пакета.

"Не начальный" фрагмент или "начальный" фрагмент

В данном документе выражение "не начальные" фрагменты используется для обозначения фрагментов, которые не содержат всех значений селекторов, которые могут потребоваться для контроля доступа (например, они могут не содержать протокола следующего уровня, порты источника и места назначения, тип/код сообщения ICMP, тип заголовка мобильности). А выражение "начальный" фрагмент используется для обозначения фрагмента, содержащего все значения селекторов, которые необходимы для контроля доступа. Однако следует заметить, что для протокола IPv6, фрагмент которого содержит протокол следующего уровня и порты (или тип/код сообщения ICMP, или тип заголовка мобильности), все будет зависеть от вида и числа имеющихся заголовков расширения. В этом контексте "начальный" фрагмент может оказаться не первым.

4.4.1. База данных политик безопасности (SPD - Security Policy Database)

Контекст безопасности (SA) представляет собой управляющую логическую структуру, используемую для осуществления политики безопасности по отношению к трафику, пересекающему границу IPsec. Таким образом, существенным элементом обработки SA является лежащая в основе база данных политик безопасности (SPD - Security Policy Database), которая определяет, какие сервисы и каким способом должны предлагаться для IP-дейтаграмм. Вид базы данных и ее интерфейс находятся за рамками данной спецификации. Однако в данном подразделе специфицирована минимальная функциональность управления, которая должна быть обеспечена для того, чтобы позволить пользователю или системному администратору управлять решением о том, должен ли применяться и как применять IPsec к трафику, передаваемому или принимаемому хостом, или передающемуся через защитный шлюз. В процессе обработки всего трафика (входящего и исходящего), включая трафик, не защищенный IPsec, который пересекает границу IPsec, должны выполняться обращения к SPD, или к соответствующим кэшам. Это включает и трафик управления IPsec, например, трафик IKE. Реализация IPsec должна (MUST) иметь по крайней мере одну SPD, и она может (MAY) поддерживать несколько SPD, если это соответствует контексту, в котором работает реализация IPsec. Отсутствуют требования по поддержке SPD для каждого интерфейса, как это было специфицировано в RFC 2401. Однако в случае поддержки реализацией нескольких SPD, она должна (MUST) содержать в себе явную функцию выбора SPD, которая вызывается для выбора соответствующей SPD для обработки исходящего трафика. Входными данными этой функции являются исходящий пакет и какие-либо локальные метаданные, которые требуются для осуществления функции выбора SPD (например, интерфейс, через который прибыл пакет). Выходными данными этой функции является идентификатор SPD (SPD-ID).

SPD представляет собой упорядоченную базу данных, согласованную с использованием списков контроля доступа (ACL) или пакетных фильтров в межсетевых экранах, маршрутизатарах и т.д. Требование упорядочивания возникает из-за того, что ее элементы будут часто перекрываться вследствие наличия (не тривиальных) диапазонов, каковыми являются значения селекторов. Таким образом, пользователь или администратор должен (MUST) быть способным упорядочить элементы для выражения требуемой политики контроля доступа. Вследствие разрешенного использования для значений селекторов групповых символов, а также из-за того, что различные типы селекторов не связаны иерархически, отсутствует способ установления общего, канонического порядка элементов SPD.

Альтернативы обработки: DISCARD (отбросить), BYPASS (обойти), PROTECT (защитить)

SPD должна отличать трафик, которому предоставляется IPsec-защита, от трафика, которому позволено обойти IPsec. Это относится к защите IPsec, которая должна применяться отправителем, и к защите IPsec, которая должна существовать в получателе. Для любой исходящей или входящей дейтаграммы возможны три альтернативы обработки с помощью IPsec: DISCARD (отбросить), BYPASS (обойти) IPsec, или PROTECT (защитить). Первая возможность относится к трафику, которому не позволено пересекать границу IPsec (в указанном направлении). Вторая возможность относится к трафику, которому позволено пересекать границу IPsec без защиты IPsec. Третья возможность относится к трафику, которому предоставляется защита IPsec, и для такого трафика SPD должна определять протоколы безопасности, которые должны применяться, их режим, опции сервисов безопасности, а также криптографические алгоритмы, которые должны использоваться.

SPD-S, SPD-I, SPD-O

Логически SPD делится на три части. Часть SPD-S (secure traffic - защищаемый трафик) содержит элементы для всего трафика, который является предметом защиты IPsec. Часть SPD-O (outbound - исходящий) содержит элементы для всего исходящего трафика, который должен игнорироваться (идти в обход) или отбрасываться. Часть SPD-I (inbound - входящий) применяется к входящему трафику, который будет игнорироваться (пускаться в обход) или отбрасываться. Для упрощения кэширования ко всем этим трем частям может

быть применен процесс декорреляции (с исключением, отмеченным выше для естественных реализаций хоста). Если реализация IPsec поддерживает только одну SPD, то эта SPD содержит все три части. Если поддерживается несколько SPD, то некоторые из них могут быть частичными (неполными), например, для контроля входящего идущего в обход трафика некоторые SPD могут содержать только элементы SPD-I для каждого входного интерфейса. Для такого трафика расщепление на несколько SPD позволяет осуществлять проверку в SPD-I без обращений к SPD-S. Поскольку SPD-I на самом деле является частью SPD, то если пакет, поиск которого осуществляется в SPD-I, не совпадает с некоторым ее элементом, то такой пакет должен (MUST) быть отброшен. Заметим, что для исходящего трафика в случае отсутствия совпадения при поиске в SPD-S, необходимо проверить SPD-O для того чтобы увидеть, должен ли этот трафик пускаться в обход. Подобным образом, если сначала проверяется SPD-O, и совпадения не найдено, то должна быть проверена SPD-S. В упорядоченной SPD, к которой не применялся процесс декорреляции, элементы SPD-S, SPD-I и SPD-O чередуются. Таким образом, в SPD осуществляется один поиск.

Элементы SPD

Каждый элемент SPD определяет передачу пакета в виде действий BYPASS, DISCARD или PROTECT. Поиск элемента производится по ключу, в качестве которого используется список из одного или нескольких селекторов. SPD содержит упорядоченный список таких элементов. Типы требуемых селекторов определяются в пп. 4.4.1.1. Эти селекторы используются для определения степени детализации контекстов безопасности, которые создаются в ответ на исходящий пакет или в ответ на предложение от партнера. Подробная структура элемента SPD описывается в пп. 4.4.1.2. Каждая SPD должна (SHOULD) иметь формальный последний элемент, который совпадает с чем угодно, что во всем остальном не совпадало, и отбрасывает его. ???

SPD должна (MUST) разрешать пользователю или администратору определять элементы политики следующим образом:

- SPD-I: Для входящего трафика, который должен быть пущен в обход (игнорироваться) или отбрасываться, элемент состоит из значений селекторов, применяемых к трафику, который должен быть пущен в обход (игнорироваться) или отбрасываться.

- SPD-O: Для исходящего трафика, который должен быть пущен в обход (игнорироваться) или отбрасываться, элемент состоит из значений селекторов, применяемых к трафику, который должен быть пущен в обход (игнорироваться) или отбрасываться.

- SPD-S: Для трафика, который должен защищаться с помощью IPsec, элемент состоит из значений селекторов, которые применяются к трафику, подлежащему защите с помощью AH или ESP, средств управления тем, как создавать контексты безопасности на основе этих селекторов, а также параметров, необходимых для осуществления этой защиты (например, алгоритмов, режимов и т.п.). Заметим, что элемент SPD-S содержит также такую информацию, как флаг "заполнить из пакета" (PFP - populate from packet) (см. ниже абзацы о том, "Как получить значения для элемента SAD") и биты, указывающие, используются ли при поиске SA, в дополнение к SPI, локальные и удаленные IP-адреса (см. спецификации AH [Ken05b] или ESP [Ken05a]).

Представление направления в элементе SPD

В соответствии с соглашениями IKE для трафика, защищаемого IPsec, с целью представления направления в элементе SPD локальный и удаленный адрес и порты переставляются местами. В общем случае для протоколов, с которыми имеет дело IPsec, необходимо наличие симметричных контекстов безопасности с переставленными локальными/удаленными IP-адресами. Однако для ICMP такое требование двунаправленной авторизации часто отсутствует. Тем не менее,

ради единообразия и упрощения элементы SPD для ICMP определяются тем же самым способом, что и для других протоколов. Заметим также, что в пакетах ICMP, заголовка мобильности и не начальных фрагментов отсутствуют поля портов. ICMP имеет тип и код сообщения, а заголовок мобильности имеет тип заголовка мобильности. Таким образом, элементы SPD имеют средства для выражения возможностей управления доступом, соответствующие этим протоколам, вместо обычных средств управления полем порта. Для игнорируемого (идущего по обходному пути) или для отбрасываемого трафика поддерживаются отдельные входящие или исходящие элементы, например, для того, чтобы в случае необходимости разрешить однонаправленные потоки.

Значения OPAQUE (непрозрачный) и ANY (любой)

Для каждого селектора в элементе SPD кроме значений литеральных констант, которые определяют совпадение, имеется два специальных значения: ANY и OPAQUE. Значение ANY представляет собой групповой символ, который совпадает с любым значением в соответствующем поле пакета, а также соответствует пакетам, в которых данное поле не присутствует или не определено. Значение OPAQUE указывает на то, что соответствующее поле селектора для опроса не доступно, поскольку оно может отсутствовать во фрагменте, не существует для заданного протокола следующего уровня или поскольку предшествующее применение IPsec могло зашифровать это значение. Значение ANY включает в себя значение OPAQUE. Таким образом, значение OPAQUE должно использоваться только когда существует необходимость различать случай любого дозволенного для поля значения, от случая отсутствия или недоступности поля (например, вследствие шифрования).

Как получить значения для элемента SAD

Для каждого селектора в элементе SPD этот элемент определяет, как получить соответствующие значения для нового элемента базы данных SA (SAD, см. п. 4.4.2) из значений, имеющихся в SPD и в пакете. Задача заключается в том, чтобы позволить создать элемент SAD и элемент кэша SPD, базируясь на конкретных значениях селекторов из пакета, или из совпадающего элемента SPD. Для исходящего трафика существуют элементы кэша SPD-S и элементы кэша SPD-O. Для входящего трафика, не защищенного IPsec, существуют элементы кэша SPD-I и имеется SAD, которая представляет собой кэш для входящего трафика, защищенного IPsec (см. рис. 3 в подразд. 5.2). Если для некоторого элемента определяется обработка IPsec, то для одного или нескольких селекторов в элементе SPD (локальный IP-адрес; удаленный IP-адрес; протокол следующего уровня; и, в зависимости от протокола следующего уровня, локальный порт и удаленный порт, или тип/код ICMP, или тип заголовка мобильности) может быть объявлен флаг "заполнить из пакета" (PFP). Если флаг объявлен для заданного селектора X, то он указывает на то, что создаваемый SA должен взять свое значение (значения) для X из значения (значений) в пакете. В противном случае, SA должен брать свое значение (значения) для X из значения (значений) в элементе SPD. Примечание: В случае отсутствия объявления PFP, значения селекторов, согласованные протоколом управления ключами (например, протоколом IKEv2), могут быть подмножеством значений в элементе SPD в зависимости от политики SPD, применяемой партнером. Кроме того, вопрос использования одного флага, например, для порта источника, типа/кода ICMP и типа заголовка мобильности, или использования для каждого из них отдельного флага, является локальным вопросом.

Следующий пример иллюстрирует использование флага PFP в контексте защитного шлюза или реализации BITS/BITW. Рассмотрим элемент SPD, в котором разрешенным значением для удаленного адреса является диапазон IPv4-адресов: с 192.168.2.1 по 192.168.2.10. Предположим, что исходящий пакет поступает с адресом места назначения 192.168.2.3 и в текущий момент времени отсутствует SA для передачи этого пакета. Значение, используемое для SA, создаваемого чтобы передать этот пакет, может принимать одно из показанных ниже двух значений в зависимости от того, что говорит элемент SPD для этого селектора относительно источника значения селектора:

Значение флага PFP для селектора удаленного адреса	Пример нового значения селектора адреса места назначения в SAD
a. PFP TRUE	192.168.2.3 (один хост)
b. PFP FALSE	192.168.2.1 to 192.168.2.10 (диапазон хостов)

Заметим, что если бы указанный выше элемент SPD для удаленного адреса имел значение ANY, то для случая (b) значение селектора в SAD должно было бы быть равно ANY, но в случае (a) будет равно проиллюстрированному значению. Таким образом, флаг PFP может использоваться для запрещения разделения некоторого SA даже пакетами, которые соответствуют одному и тому же элементу SPD.

Интерфейс управления

Для каждой реализации IPsec должен (MUST) существовать интерфейс управления, который позволяет пользователю или системному администратору управлять SPD. Интерфейс должен позволять пользователю (или администратору) определять обработку защиты, которая должна применяться к каждому пакету, который пересекает границу IPsec. (Как указывалось выше, в естественной реализации IPsec хоста, использующей интерфейс сокетов, нет необходимости осуществлять поиск в SPD для каждого пакета). Интерфейс управления для SPD должен (MUST) позволять создавать элементы, согласованные с селекторами, определенными в пп. 4.4.1.1, и должен (MUST) поддерживать (общее) упорядочивание этих элементов, которое видно через этот интерфейс. Селекторы элементов SPD аналогичны спискам контроля доступа (ACL – Access Control List) или пакетным фильтрам, которые, как правило, создаются в бесконтекстном межсетевом экране или осуществляющем фильтрацию пакетов маршрутизаторе и которые в настоящее время управляются таким способом.

В хост-системах приложениям может (MAY) быть позволено создавать элементы SPD. (Средства передачи таких запросов реализации IPsec выходят за рамки данного стандарта). Однако системный администратор должен (MUST) иметь возможность указать, может или не может пользователь или приложение не принимать во внимание (аннулировать) (установленные по умолчанию) политики системы. Вид интерфейса управления в данном документе не специфицируется, и он может отличаться между хостами и защитными шлюзами, а в рамках хостов этот интерфейс может отличаться для реализаций, базирующихся на сокетах, от реализаций BITS. Тем не менее данный документ специфицирует стандартный набор элементов SPD, которые должны (MUST) поддерживать все реализации IPsec.

Декорреляция

Описанная в данном документе модель обработки предполагает возможность декорреляции пересекающихся элементов SPD, чтобы обеспечить кэширование, которое позволяет реализовать более эффективную обработку исходящего трафика в защитных шлюзах и реализациях BITS/BITW. Декорреляция [CoSa04] является только средством увеличения производительности и упрощения описания обработки. Данный документ RFC не требует, чтобы соответствующие ему реализации использовали декорреляцию. Например, естественные реализации в хостах обычно используют кэширование неявно, поскольку они привязывают контексты безопасности к интерфейсам сокетов, и, таким образом, для этих реализаций отсутствует требование их способности декоррелировать элементы SPD.

Примечание: Если иное не уточняется, использование термина "SPD" относится к основной части информации о политиках, находящейся как в упорядоченном состоянии, так и в декоррелированном (неупорядоченном) состоянии. В приложении B представлен алгоритм, который может использоваться для декорреляции элементов SPD, но может использоваться любой алгоритм,

который дает эквивалентный результат. Заметим, что когда элемент SPD декоррелируется, все получающиеся элементы должны (MUST) быть связаны друг с другом так, чтобы все члены группы, полученной из одного элемента SPD (существовавшего до осуществления декорреляции), могли быть помещены в кэши и в SAD одновременно. Например, предположим, что мы начинаем с элемента A (из упорядоченной SPD), который в процессе декорреляции порождает элементы A1, A2 и A3. Когда вслед за этим приходит пакет, который совпадает, скажем, с A2, и инициирует создание SA, то протокол управления SA (например, IKEv2) согласует A. И все три декореллированных элемента A1, A2, и A3 помещаются в соответствующий кэш SPD-S и привязываются к этому SA. Смысл этого заключается в том, что использование декореллированной SPD не должно создавать больше контекстов безопасности, чем могло появиться при использовании не декоррелированной SPD.

Если применяется декоррелированная SPD, то имеются три дополнительных возможности для того, что инициатор посылает партнеру с помощью протокола управления контекстами безопасности (например, IKE). При посылке полного набора связанных декоррелированных элементов, которые были выбраны из SPD, партнеру дается наиболее полная информация, позволяющая осуществить выбор на его конце соответствующего элемента SPD, особенно когда партнер также декоррелировал свою SPD. Однако в случае связывания большого количества декоррелированных элементов, это может приводить к большим размерам пакетов для согласования SA, а, следовательно, к проблемам фрагментации для протокола управления SA.

В качестве альтернативы может быть сохранен и передан протоколу управления SA оригинальный элемент из (коррелированной) SPD. Передача коррелированного элемента SPD протоколу управления SA превращает использование декоррелированной SPD в локальный вопрос, не видимый партнерами, и позволяет избежать возможных проблем с фрагментацией, хотя и предоставляет ответчику менее точную информацию для сопоставления с его SPD.

Промежуточный подход заключается в посылке некоторого подмножества полного набора связанных декоррелированных элементов SPD. Этот подход позволяет избежать указанных выше проблем фрагментации, к тому же предоставляет более хорошую информацию по сравнению с оригинальным коррелирующим элементом. Основной недостаток этого подхода заключается в том, что он может приводить впоследствии к созданию дополнительных контекстов безопасности, поскольку партнеру посылается только некоторое подмножество полного набора связанных декоррелированных элементов. Разработчики реализаций могут свободно применять любой из указанных выше подходов.

Ответчик использует предложения селекторов трафика, которые он получает с помощью протокола управления SA, для выбора соответствующего элемента в своей SPD. Смысл сопоставления заключается в том, чтобы выбрать элемент SPD и создать SA, который бы наиболее близко соответствовал цели инициатора, так чтобы трафик, проходящий по результирующему SA, был бы приемлем для обоих концов соединения. Если ответчик применяет декореллированную SPD, он должен (SHOULD) использовать для сопоставления декоррелированные элементы SPD, поскольку в общем случае это будет приводить к созданию контекстов безопасности, которые наиболее вероятно соответствуют целям обоих партнеров. Если ответчик имеет коррелированную SPD, то он должен (SHOULD) сопоставить предложения с коррелирующими элементами. Для IKEv2 использование декоррелированной SPD предоставляет ответчику наилучшую возможность породить «минимально успешный» ответ.

Во всех случаях, когда доступна декоррелированная SPD, декоррелированные элементы используются для заполнения кэша SPD-S. Если SPD не декоррелирована, то кэширование не допускается и для проверки того, что входящий трафик, прибывающий по некоторому SA, согласуется с политикой контроля доступа, выраженной в SPD, должен (MUST) осуществляться упорядоченный поиск в SPD.

Обработка изменений в SPD во время работы системы

Если изменение в SPD производится во время работы системы, то должна (SHOULD) быть выполнена проверка влияния этого изменения на существующие в этот момент контексты безопасности. Реализация должна (SHOULD) проверить влияние изменения SPD на существующие SA и должна (SHOULD) предоставить пользователю или администратору механизм для конфигурирования предпринимаемых действий, например, для удаления затронутого SA, разрешения затронутому SA продолжать работу без изменений и т.д.

4.4.1.1. Селекторы

Контекст безопасности (SA) может быть иметь тонкую или грубую степень детализации в зависимости от селекторов, которые используются для определения множества трафика для этого SA. Например, весь трафик между двумя хостами может передаваться через один SA, и ему может предоставляться единообразный набор сервисов безопасности. В качестве альтернативы трафик между парой хостов, в зависимости от используемого приложения (что определяется протоколом более высокого уровня и связанными с ним полями, например, портами) может быть распределен по нескольким SA с разными сервисами безопасности, предлагаемыми разными SA. Подобным образом, весь трафик между парой защитных шлюзов может передаваться по одному SA, либо для каждой пары хостов, осуществляющих обмен информацией, может быть назначено по одному SA. Для упрощения управления степенью детализации SA всеми реализациями IPsec должны (MUST) поддерживаться следующие параметры селекторов. Заметим, что как локальные, так и удаленные адреса должны быть либо IPv4-, либо IPv6-адресами, но не смесью адресов этих типов. Кроме того, заметим, что селекторы локальных/удаленных портов (а также тип и код сообщений ICMP и тип заголовка мобильности) могут быть помечены признаком OPAQUE (непрозрачный), чтобы приспособиться к ситуациям, когда эти поля не доступны из-за фрагментации пакетов.

- Remote IP Address (es) - Удаленный IP-адрес (адреса) (IPv4 или IPv6): это список диапазонов IP-адресов (типа unicast, broadcast (только для IPv4)). Такая структура допускает выражение одного IP-адреса (с помощью тривиального диапазона), или списка адресов (каждый из которых представляется тривиальным диапазоном), или диапазона адресов (включая наименьшее и наибольшее значения), а также наиболее общую форму списка диапазонов адресов. Диапазоны адресов используются для поддержки нескольких удаленных систем, имеющих один и тот же SA, например, находящихся за защитным шлюзом.

- Local IP Address (es) - Локальный IP-адрес (адреса) (IPv4 или IPv6): это список диапазонов IP-адресов (типа unicast, broadcast (только для IPv4)). Такая структура допускает выражение одного IP-адреса (с помощью тривиального диапазона), или списка адресов (каждый из которых представляется тривиальным диапазоном), или диапазона адресов (включая наименьшее и наибольшее значения), а также наиболее общую форму списка диапазонов адресов. Диапазоны адресов используются для поддержки нескольких систем-источников, имеющих один и тот же SA, например, находящихся за защитным шлюзом. Признак "локальный" указывает на адрес (адреса), который защищается данной реализацией (или элементом политики).

  Примечание: SPD не включает поддержку элементов для групповых (multicast) адресов. Для поддержки групповых (multicast) SA реализация должна использовать SPD группы (GSPD – Group SPD), как определено в [RFC3740]. Элементы GSPD требуют другой структуры, например, нельзя использовать симметричный отношения, ассоциированные со значениями локального и удаленного адреса для однонаправленных (unicast) SA, в групповом контексте. Более точно, исходящий трафик, направляемый на групповой (multicast) адрес по некоторому SA не будет приниматься по парному входящему SA с групповым адресом в качестве источника.

- Next Layer Protocol - Протокол следующего уровня: Берется из полей IPv4 "Protocol" или IPv6 "Next Header". Это персональный номер протокола, значение ANY, или значение OPAQUE (только для IPv6). Параметр "Next Layer Protocol " определяет все, что поступает после любого из имеющихся заголовков расширения IP. Для упрощения определения местоположения "протокола следующего уровня" должен (SHOULD) существовать механизм конфигурирования для указания пропуска заголовков расширения IPv6. По умолчанию такое конфигурирование пропуска заголовков расширения IPv6 должно (SHOULD) включать следующие протоколы: 0 (Hop-by-hop options), 43 (Routing Header), 44 (Fragmentation Header) и 60 (Destination Options). Примечание: Этот используемый по умолчанию список не (NOT) включает протоколы 51 (AH) или 50 (ESP). С точки зрения поиска селекторов, IPsec рассматривает AH и ESP как протоколы следующего уровня.

  Несколько дополнительных селекторов зависят от значения Next Layer Protocol:

  * Если протокол следующего уровня использует два порта (например, TCP, UDP, SCTP, ...), то имеются селекторы для локального и удаленного портов. Каждый из этих селекторов содержит список диапазонов значений. Заметим, что локальные и удаленные порты могут быть не доступны в случае приема фрагментированного пакета или если поля портов защищены с помощью IPsec (зашифрованы), таким образом также должно (MUST) поддерживаться значение OPAQUE. Примечание: В не начальном фрагменте значения портов не будут доступны. Если селектор порта определяет значение, отличное от ANY или OPAQUE, то оно не может сопоставляться с пакетами, которые являются не начальными фрагментами. Если SA требует значения порта, отличного от ANY или OPAQUE, то прибывающий не имеющий портов фрагмент должен (MUST) отбрасываться. (См. разд. 7 Обработка фрагментов).

  * Если протоколом следующего уровня является Mobility Header (заголовок мобильности), то для типа сообщения заголовка мобильности IPv6 (MH type) имеется селектор [Mobip]. Это 8-битовое значение, которое определяет конкретное сообщение мобильности. Заметим, что в случае получения фрагментированного пакета поле MH type может быть недоступным. (См. разд. 7, Обработка фрагментов). Для IKE тип сообщения заголовка мобильности IPv6 (MH type) помещается в наиболее значимые восемь бит 16-битового селектора локального "порта".

  * Если значением параметра Next Layer Protocol является ICMP, то имеется 16-битовый селектор для полей type (тип) и code (код) сообщений ICMP. Тип сообщения представляет собой одиночное 8-битовое значение, которое определяет либо тип сообщения ICMP, либо значение ANY. Код ICMP представляет собой одиночное 8-битовое значение, которое определяет конкретный подтип сообщения ICMP. Для IKE тип сообщения помещается в наиболее значимые 8 бит 16-битового селектора, а код помещается в менее значимые 8 бит. Этот 16-битовый селектор может содержать либо один тип и диапазон кодов, либо один тип и код ANY, либо тип ANY и код ANY. Имея элемент политики с диапазоном типов (от T-start до T-end), диапазоном кодов (от C-start до C-end) и пакет ICMP с типом t и кодом c, реализация должна (MUST) его проверить на соответствие с помощью выражения

    (T-start*256) + C-start <= (t*256) + c <= (T-end*256) + C-end

    Заметим, что тип и код сообщения ICMP могут быть недоступными в случае получения фрагментированного пакета. (См. разд. 7. Обработка фрагментов).

- Name (имя): Это не селектор, подобный другим, указанным выше селекторам. Оно не берется из пакета. Имя может использоваться в

качестве символического идентификатора для локального или удаленного адреса IPsec. Поименованные элементы SPD используются двумя способами:

1. Поименованный элемент SPD используется ответчиком (не инициатором) для поддержки контроля доступа, когда IP-адрес из пакета не будет соответствовать селектору Remote IP Address, например, для "мобильных пользователей" (road warriors). Имя, используемое для сопоставления с этим полем, передается в процессе согласования IKE в блоке данных ID. В этом контексте IP-адрес источника (Source IP address) инициатора (из внутреннего IP-заголовка в туннельном режиме) связывается с удаленным IP-адресом (Remote IP Address) в элементе SAD, созданным при согласовании IKE. Когда элемент SPD выбирается таким образом, этот адрес аннулирует значение удаленного IP-адреса в SPD. Все реализации IPsec должны (MUST) поддерживать такое использование имен.

2. Поименованный элемент SPD может использоваться инициатором для указания пользователя, для которого будет создан IPsec SA (или для которого трафик может идти в обход). Поле Source IP address инициатора (из внутреннего IP-заголовка в туннельном режиме) используется для замены следующих параметров, когда и где бы их не пришлось их создавать:

   - локального адреса в элементе кэша SPD
   - локального адреса в исходящем элементе SAD
   - удаленного адреса во входящем элементе SAD

   Поддержка такого использования для естественных многопользовательских реализаций хостов является факультативной возможностью и не применима для других реализаций. Заметим, что это имя используется только локально; оно не передается протоколом управления ключами.

Элемент SPD может содержать как имя (или список имен), так и значения локального и удаленного IP-адресов. Идентификаторы, применяемые в именованных элементах SPD, могут быть одного из следующих четырех типов:

a. строка полностью определенного имени пользователя электронной почты (email), например, mozart@foo.example.com
   (она соответствует ID_RFC822_ADDR в IKEv2)

b. полностью определенное имя DNS, например, foo.example.com
   (оно соответствует ID_FQDN в IKEv2)

c. различительное имя X.500, например,
   C = US, SP = MA,
   O = BBN Technologies, CN = Stephen T. Kent
   (после декодирования оно соответствует ID_DER_ASN1_DN в IKEv2)

d. строка байтов
   (она соответствует Key_ID в IKEv2)

Контекст реализации IPsec определяет то, как используются селекторы. Например, в естественной реализации хоста обычно используется интерфейс сокетов. Когда устанавливается новое соединение, можно обратиться к SPD и привязать SA к сокету. Таким образом, трафик, посылаемый через такой сокет, не требует дополнительного поиска в кэше SPD (SPD-O и SPD-S). В отличие от этого реализация BITS, BITW или защитного шлюза требует рассмотрения каждого пакета и выполнения поиска в кэше SPD-O/SPD-S на основе селекторов.

4.4.1.2. Структура элемента SPD

Данный подпункт содержит прозаическое описание элемента SPD. Кроме того, в Приложении C представлен пример определения элемента SPD на языке ASN.1.

Чтобы гарантировать, что политика, требуемая элементами SPD, может быть согласована с помощью IKE, в данном тексте SPD описывается таким способом, который прямо отображается на блоки данных IKE. К сожалению, семантика версии IKEv2, опубликованной одновременно с настоящим документом [Kau05], точно не совпадает с семантикой, определенной для SPD. Более точно, IKEv2 не разрешает согласование одиночного SA, который привязывает несколько пар локальных и удаленных адресов и портов к одному SA. Вместо этого, когда для одного SA согласуются несколько локальных и удаленных адресов и портов, IKEv2 рассматривает их не как пары, а как (неупорядоченные) наборы локальных и удаленных значений, которые могут объединяться в пары произвольным образом. До тех пор пока IKE не обеспечит средство, которое передает семантику, выраженную в SPD с помощью наборов селекторов (как описано ниже), пользователи не должны (MUST NOT) включать несколько наборов селекторов в один элемент SPD, за исключением ситуации, когда цель контроля доступа соответствует семантике «смеси и соответствия», принятой в IKE.

Графический пользовательский интерфейс (GUI) управления может предложить пользователю другие виды элемента данных и отображения, например, опцию использования адресных префиксов, а также диапазонов и символических имен для протоколов, портов и т.д. (Не путайте использование символических имен в интерфейсе управления с селектором SPD "Name" (имя)). Заметим что определения Remote/Local (удаленный/локальный) применяются только к IP-адресам и портам, но не к типу/коду сообщения ICMP или типу заголовка мобильности. Кроме того, если для данного типа селектора применяется зарезервированное значение символического селектора OPAQUE или ANY, то в списке для этого селектора может появиться только такое значение, и для этого селектора оно должно появляться в списке только один раз. Заметим, что значения ANY и OPAQUE являются соглашениями локального синтаксиса – IKEv2 согласует эти значения с помощью указанных ниже диапазонов:

```
ANY:     start = 0         end = <max>
OPAQUE:  start = <max>     end = 0
```

SPD представляет собой упорядоченный список элементов, каждый из которых содержит следующие поля:

- Name (имя) - список идентификаторов (ID). Этот квази-селектор является факультативным. Виды идентификаторов, которые должны (MUST) поддерживаться, описываются выше в пп. 4.4.1.1 в абзаце "Name".

- PFP flags (флаги PFP) – по одному на каждый селектор трафика. Заданный флаг, например, для протокола следующего уровня, применяется к соответствующему селектору во всех "наборах селекторов" (selector sets) (см. ниже), содержащихся в элементе SPD. При создании SA каждый флаг для соответствующего селектора трафика указывает, нужно ли брать селектор из соответствующего поля в пакете, который инициировал создание SA, или из значения (значений) в соответствующем элементе SPD (см. п. 4.4.1 "Как получать значения для элемента SAD). Вопрос об использовании одного общего флага, например, для порта источника, типа/кода сообщения ICMP или типа заголовка MH, или отдельного флага для каждого из указанных полей, является локальным вопросом. Имеются флаги PFP для:

  - локального адреса (Local Address)
  - удаленного адреса (Remote Address)
  - протокола следующего уровня (Next Layer Protocol)
  - локального порта (Local Port), или типа/кода сообщения ICMP (ICMP message type/code) или типа заголовка мобильности (Mobility Header type) (в зависимости от протокола следующего уровня)

- удаленного порта (Remote Port), или типа/кода сообщения ICMP (ICMP message type/code) или типа заголовка мобильности (Mobility Header type) (в зависимости от протокола следующего уровня)

o От одного до N наборов селекторов, которые соответствуют "условию" применения конкретного действия IPsec. Каждый набор селекторов содержит:

  - локальный адрес (Local Address)
  - удаленный адрес (Remote Address)
  - протокол следующего уровня (Next Layer Protocol)
  - локальный порт (Local Port), или тип/код сообщения ICMP (ICMP message type/code) или тип заголовка мобильности (Mobility Header type) (в зависимости от протокола следующего уровня)
  - удаленный порт (Remote Port), или тип/код сообщения ICMP (ICMP message type/code) или тип заголовка мобильности (Mobility Header type) (в зависимости от протокола следующего уровня)

  Примечание: Селектор "следующий протокол" (next protocol) в элементе набора селекторов представляет собой одиночное значение (в отличие от локальных и удаленных адресов). Это соответствует тому, как IKEv2 согласует значения селекторов трафика (TS) для SA. Это имеет смысл также потому, что может возникнуть необходимость связать с разными протоколами различные номера портов. С одним SA можно связать несколько протоколов (и портов) путем определения для такого SA нескольких наборов селекторов.

o Информация для обработки (processing info) – какое действие требуется выполнить – защитить (PROTECT), пустить в обход (BYPASS), или отбросить (DISCARD). Для всех наборов селекторов выполняется только одно действие, а не отдельное действие для каждого набора. Если в качестве требуемой обработки указывается защита (PROTECT), то элемент содержит следующую информацию:

  - режим IPsec (IPsec mode) – туннельный или транспортный

  - (в случае туннельного режима) локальный адрес туннеля (local tunnel address) – Для немобильного хоста, если имеется только один интерфейс, это просто; а если имеется несколько интерфейсов, то он должен конфигурироваться статически. Для мобильного хоста управление заданием локального адреса осуществляется внешними по отношению к IPsec средствами.

  - (в случае туннельного режима) удаленный адрес туннеля (remote tunnel address)– Для его определения не существует стандартного способа. См. п. 4.5.3. "Определение местоположения защитного шлюза".

  - расширенный порядковый номер (extended sequence number) – Использует ли данный SA расширенные порядковые номера?

  - контекстная проверка фрагментов (stateful fragment Checking) – Использует ли данный SA контекстную (с сохранением состояния) проверку фрагментов (более подробно см. в разд. 7).

  - обойти бит DF (T/F) – применим к контекстам безопасности туннельного режима

  - обойти DSCP (T/F) или отобразить на незащищенные значения (массив) DSCP, если необходимо ограничить обход значений DSCP – применим к контекстам безопасности туннельного режима

  - протокол IPsec - AH или ESP

- алгоритмы – какие из них использовать для AH, какие из них использовать для ESP, какие из них использовать для комбинированного режима, упорядоченные в порядке убывания приоритета

Что касается обработки существующих в текущий момент времени контекстов безопасности при внесении изменений в SPD, то вопрос о том, какую информацию поддерживать, является локальным.

4.4.1.3. Дополнительно о полях, связанных с протоколами следующего уровня

С полями заголовка протокола следующего уровня часто связываются дополнительные селекторы. Конкретный протокол следующего уровня может иметь ноль, один или два селектора. Могут существовать ситуации, в которых отсутствуют как локальные, так и удаленные селекторы для полей, которые зависят от протокола следующего уровня. Заголовок мобильности (Mobility Header) IPv6 имеет только тип сообщения заголовка мобильности. AH и ESP не имеют никаких дополнительных селекторных полей. Система может быть готова послать тип и код сообщения ICMP, которые она не хочет получать. В приведенных ниже описаниях термин "port" (порт) используется для обозначения поля, которое зависит от протокола следующего уровня.

A. Если протокол следующего уровня не имеет селекторов "port", то селекторы локального и удаленного портов ("port") в соответствующем элементе SPD устанавливаются в значение OPAQUE, например,

```
Селектор локального порта
  next layer protocol = AH
  "port" selector     = OPAQUE

Селектор удаленного порта
  next layer protocol = AH
  "port" selector     = OPAQUE
```

B. Даже если протокол следующего уровня имеет только один селектор, например, Mobility Header type, то селекторы локального и удаленного портов используются для указания того, хочет ли система посылать и/или принимать трафик с определенными значениями поля "port". Например, если по некоторому SA допускается посылать и принимать заголовки мобильности определенного типа, то соответствующий элемент SPD будет установлен следующим образом:

```
Селектор локального порта
  next layer protocol = Mobility Header
  "port" selector     = Mobility Header message type

Селектор удаленного порта
  next layer protocol = Mobility Header
  "port" selector     = Mobility Header message type
```

Если по некоторому SA заголовки мобильности определенного типа разрешается посылать, но не (NOT) принимать, то соответствующий элемент SPD будет установлен следующим образом:

```
Селектор локального порта
  next layer protocol = Mobility Header
  "port" selector     = Mobility Header message type

Селектор удаленного порта
  next layer protocol = Mobility Header
  "port" selector     = OPAQUE
```

Если по некоторому SA заголовки мобильности определенного типа разрешается принимать, но не (NOT) посылать, то соответствующий элемент SPD будет установлен следующим образом:

```
Селектор локального порта
  next layer protocol = Mobility Header
  "port" selector     = OPAQUE

Селектор удаленного порта
  next layer protocol = Mobility Header
  "port" selector     = Mobility Header message type
```

C. Если система готова посылать трафик с конкретным значением поля "port", но не принимать (NOT receive) трафик с этим видом значения порта, то селекторы трафика системы в соответствующем элементе SPD устанавливаются следующим образом:

```
Селектор локального порта
  next layer protocol = ICMP
  "port" selector     = <конкретные тип и код сообщения ICMP>

Селектор удаленного порта
  next layer protocol = ICMP
  "port" selector     = OPAQUE
```

D. Для указания того, что система готова принимать трафик с конкретным значением поля "port", но не посылать этот вид трафика, селекторы трафика системы в соответствующем элементе SPD устанавливаются следующим образом:

```
Селектор локального порта
  next layer protocol = ICMP
  "port" selector     = OPAQUE

Селектор удаленного порта
  next layer protocol = ICMP
  "port" selector     = <конкретные тип и код сообщения ICMP>
```

Например, если защитный шлюз готов разрешить находящимся за ним системам посылать сообщения traceroute ICMP, но не готов позволить внешним системам выполнять traceroute ICMP к находящимся за ним системам, то селекторы трафика защитного шлюза в соответствующем элементе SPD устанавливаются следующим образом:

```
Селектор локального порта
  next layer protocol = 1 (ICMPv4)
  "port" selector     = 30 (traceroute)

Селектор удаленного порта
  next layer protocol = 1 (ICMPv4)
  "port" selector     = OPAQUE
```

4.4.2. База данных контекстов безопасности

В каждой реализации IPsec имеется номинальная база контекстов безопасности (SAD - Security Association Database), в которой каждый элемент определяет параметры, связанные с одним контекстом безопасности (SA). Каждый SA имеет элемент в SAD. Для обработки исходящего трафика каждый элемент SAD указывается элементами в части SPD-S кэша SPD. Для обработки входящего трафика для индивидуальных (unicast) SA для поиска SA используется либо только SPI, либо SPI может использоваться совместно с типом протокола IPsec. Если реализация IPsec поддерживает групповой (multicast) трафик, то для поиска SA используется SPI плюс адрес места назначения, либо SPI плюс адрес места назначения и адрес источника. (Детали алгоритма, который должен (MUST) использоваться для отображения входящих IPsec-дейтаграмм на контексты безопасности см. в подразд. 4.1). С каждым элементом SAD связываются

следующие параметры. Все они должны присутствовать, если не указывается иное, например, алгоритм аутентификации AH. Данное описание не претендует на роль базы данных управляющей информации (MIB), а представляет собой лишь спецификацию минимального числа элементов данных, которые требуются для поддержки SA в реализации IPsec.

Для каждого селектора, определенного в пп. 4.4.1.1, элемент для входящего SA в SAD в начале должен (MUST) быть заполнен значением или значениями, согласованными во время создания SA. (Руководство по последствиям изменений в SPD для существующих в настоящее время SA см. в п. 4.4.1, абзац об обработке изменений в SPD при работе системы). Для приемника эти значения используются для проверки того, что поля заголовка входящего пакета (после обработки IPsec) соответствуют значениям селекторов, согласованным для этого SA. Таким образом, SAD работает в качестве кэша для проверки селекторов входящего трафика, поступающего по этому SA. Для приемника это является частью проверки того, что пакет, поступающий по данному SA, не противоречит политике для этого SA. (Правила для сообщений ICMP см. в разд. 6). Как описано в пп. 4.4.1.1 "Селекторы", эти поля могут представляться в виде конкретных значений, диапазонов, значения ANY или значения OPAQUE. Заметим также, что имеется несколько ситуаций, в которых SAD может иметь элементы для контекстов безопасности, которые не имеют соответствующих элементов в SPD. Поскольку данный документ не обязывает выполнять селективную очистку SAD при изменении SPD, то элементы SAD могут оставаться, когда очищающие их элементы SPD изменяются или удаляются. Кроме того, если создается вручную управляемый SA, то для этого SA может появиться элемент SAD, который не соответствует ни одному элементу SPD.

Примечание: SAD может поддерживать групповые (multicast) SA, если они конфигурируются вручную. Исходящий групповой SA имеет ту же самую структуру, что и индивидуальный (unicast) SA. Адресом источника является адрес отправителя, а адресом места назначения – адрес мультикастовой группы. Входящий групповой SA должен конфигурироваться адресами источников каждого из партнеров, авторизованных на передачу по данному групповому SA. Значение SPI для группового SA предоставляется контроллером мультикастовой группы, а не приемником, как это делается для индивидуального SA. Поскольку от элемента SAD может требоваться размещение нескольких индивидуальных IP-адресов источников, которые были частью некоторого элемента SPD (для индивидуальных SA), требуемая возможность для входящих групповых SA в реализации IPsec уже существует. Однако, поскольку SPD не предоставляет средств для размещения групповых (multicast) элементов, то в данном документе автоматический способ создания элемента SAD для группового входящего SA не специфицируется. Для обеспечения входящего группового трафика могут создаваться только вручную конфигурируемые элементы SAD.

Руководство по реализации: В данном документе не специфицируется, каким образом элемент SPD-S указывает на соответствующий элемент SAD, поскольку это является деталью, зависящей от реализации. Однако известно, что некоторые реализации (базирующиеся на опыте RFC 2401) в этом смысле имеют проблемы. В частности, не достаточно просто хранить в кэше SPD просто пару (удаленный IP-адрес туннельного заголовка, удаленный SPI), поскольку эта пара не всегда уникально идентифицирует отдельный элемент SAD. Например, два хоста, находящиеся за одним и тем же устройством NAT, могут выбрать одно и то же значение SPI. Такая ситуация может возникнуть также, если хосту присваивается IP-адрес (например, с помощью DHCP), который ранее использовался каким-то другим хостом, а SA, ассоциированные со старым хостом, еще не были уничтожены посредством механизмов определения мертвого (неработоспособного) партнера. Это может привести к посылке пакетов по неправильному SA или, если управление ключами гарантирует уникальность пары, к отказу в создании SA, которые в иных отношениях были правильными. Таким образом, разработчики реализаций должны реализовывать связи между кэшем SPD и SAD таким способом, который не порождает таких проблем.

4.4.2.1. Элементы данных в SAD

В SAD должны (MUST) быть следующие элементы данных:

- Индекс параметров безопасности (SPI - Security Parameter Index): 32-битовое значение, выбираемое принимающим концом SA для уникальной идентификации SA. В элементе SAD для исходящего SA, SPI используется для создания заголовка пакета AH или ESP. В элементе SAD для входящего SA, SPI используется для отображения трафика на соответствующий SA (см. текст об индивидуальном/групповом (unicast/multicast) трафике в подразд. 4.1).

- Счетчик порядковых номеров (Sequence Number Counter): 64-битовый счетчик, который используется для формирования поля Sequence Number в заголовках AH или ESP. По умолчанию предполагаются 64-битовые порядковые номера, но 32-битовые порядковые номера также поддерживаются, если были согласованы.

- Переполнение счетчика порядковых номеров (Sequence Counter Overflow): флаг, указывающий, должно ли переполнение счетчика порядковых номеров генерировать подлежащее аудиту событие и предотвращать передачу по SA дополнительных пакетов, или что перебор разрешен. Элемент журнала аудита для этого события должен (SHOULD) включать значение SPI, текущие дату/время, локальный адрес, удаленный адрес и селекторы из соответствующего элемента SAD.

- Окно противодействия атакам повторного воспроизведения (Anti-Replay Window): 64-битовый счетчик и битовая карта (или ее эквивалент), используемые для определения того, что входящий пакет AH или ESP является повторно воспроизведенным.

  Примечание: Если противодействие атакам повторного воспроизведения было заблокировано приемником SA, например, в случае вручную управляемого SA, то окно противодействия атакам повторного воспроизведения для данного SA игнорируется. По умолчанию используются 64-битовые порядковые номера, однако этот размер счетчика приспособлен также для 32-битовых порядковых номеров.

- Алгоритм аутентификации AH, ключ и т.д. Он требуется только, если поддерживается AH.

- Алгоритм шифрования ESP, ключ, режим, IV и т.д. Если используется алгоритм комбинированного режима, то эти поля применяться не будут.

- Алгоритм целостности ESP, ключи и т.д. Если сервис обеспечения целостности не выбирается, то эти поля применяться не будут. Если используется алгоритм комбинированного режима, то эти поля применяться не будут.

- Алгоритмы комбинированного режима ESP, ключ (ключи) и т.д. Эти данные используются, когда с ESP используется алгоритм комбинированного режима (шифрования и обеспечения целостности). Если алгоритм комбинированного режима не используется, то эти поля не применяются.

- Время жизни данного SA: интервал времени, после истечения которого SA должен быть заменен новым SA (и новым SPI) или завершен, а также указание на то, какое из этих действий должно произойти. Оно может быть выражено временем или количеством байтов, или одновременным использованием обоих типов, причем преимуществом обладает первое исчерпанное время жизни. Реализация, соответствующая данной спецификации, должна (MUST) поддерживать оба типа времени жизни и должна (MUST) поддерживать одновременное использование обоих типов времени жизни. Если применяется время, и если для установления SA протокол IKE применяет сертификаты X509, то время жизни SA должно быть ограничено периодом достоверности сертификатов и значением даты следующего выпуска (NextIssueDate) списков аннулированных сертификатов

(CRL), которые использовались в обмене IKE для данного SA. Как инициатор, так и ответчик несут ответственность за ограничение времени жизни SA таким способом. Примечание: Детали обработки обновлений ключей при истечении времени жизни контекстов безопасности являются локальным вопросом. Однако разумный подход заключается в том, что:

(a) Если используется количество байтов, то реализация должна (SHOULD) подсчитывать количество байтов, к которым применяется криптографический алгоритм IPsec. Для ESP это алгоритм шифрования (включая нулевое шифрование), а для AH это алгоритм аутентификации. Этот подсчет включает байты заполнения и т.д. Заметим, что реализации должны (MUST) быть способными справляться с ситуациями, когда счетчики на разных концах SA выходят из синхронизации, например, из-за потери пакетов или из-за того, что реализации на разных концах SA неодинаково выполняют некоторые вещи.

(b) Должны поддерживаться (SHOULD) два вида времени жизни – мягкое время жизни, которое оповещает реализацию о необходимости инициации такого действия, как планирование смены SA; и жесткое время жизни, когда текущий SA завершается и ликвидируется.

(c) Если в течение времени жизни SA пакет не был доставлен целиком, то такой пакет должен (SHOULD) быть отброшен.

- Режим протокола IPsec: туннельный или транспортный. Указывает, какой режим AH или ESP применяется к трафику по данному SA.

- Флаг контекстной проверки фрагментов. Указывает, применяется ли к данному SA контекстная проверка фрагментов (осуществляемая с сохранением состояния).

- Обход бита DF (T/F) – применим для контекстов безопасности туннельного режима, когда и внутренний и внешний заголовки соответствуют протоколу IPv4.

- Значения DSCP – множество значений DSCP, которые разрешаются для пакетов, передающихся по данному SA. Если не определяется никаких значений, то специфическая для DSCP фильтрация не применяется. Если определяются одно или большее количество значений, то они используются для выбора одного из нескольких SA, которые соответствуют селекторам трафика исходящего пакета. Заметим, что эти значения не проверяются для входящего трафика, поступающего по этому SA.

- Обход DSCP (T/F) или отображение на незащищенные значения DSCP (массив), в случае необходимости ограничить обход значений DSCP – применим для контекстов безопасности туннельного режима. Этот признак отображает значения DSCP из внутреннего заголовка на значения во внешнем заголовке, например, чтобы иметь дело с сигнализацией секретного канала.

- MTU пути (Path MTU): любое наблюдаемое значение MTU пути и переменные старения.

- IP-адреса источника и места назначения туннельного заголовка – оба адреса должны быть либо адресами IPv4, либо адресами IPv6. Версия предполагает тип IP-заголовка, который должен использоваться. Используются, только когда режим протокола IPsec является туннельным.

4.4.2.2. Связь между SPD, флагом PFP, пакетом и SAD

Для каждого селектора следующие таблицы показывают связь между значением в SPD, флагом PFP, значением в инициирующем пакете и результирующим значением в SAD. Заметим, что административный интерфейс для IPsec может использовать различные синтаксические опции, чтобы упростить

администратору ввод правил. Например, хотя в IKEv2 пересылается список диапазонов, для пользователя ввод одного IP-адреса или адресного префикса IP может оказаться более ясным и вызывающим меньше ошибок.

Селектор	Элемент SPD	PFP	Значение в инициирующем пакете	Получающийся элемент SAD
loc addr	список диапазонов	0	IP addr "S"	список диапазонов
	ANY	0	IP addr "S"	ANY
	список диапазонов	1	IP addr "S"	"S"
	ANY	1	IP addr "S"	"S"
rem addr	список диапазонов	0	IP addr "D"	список диапазонов
	ANY	0	IP addr "D"	ANY
	список диапазонов	1	IP addr "D"	"D"
	ANY	1	IP addr "D"	"D"
protocol	список протоколов*	0	prot. "P"	список протоколов*
	ANY**	0	prot. "P"	ANY
	OPAQUE****	0	prot. "P"	OPAQUE
	список протоколов*	0	не доступно	отбросить пакет
	ANY**	0	не доступно	ANY
	OPAQUE****	0	не доступно	OPAQUE
	список протоколов*	1	prot. "P"	"P"
	ANY**	1	prot. "P"	"P"
	OPAQUE****	1	prot. "P"	***
	список протоколов*	1	не доступно	отбросить пакет
	ANY**	1	не доступно	отбросить пакет
	OPAQUE****	1	не доступно	***

Если протокол таков, что имеет два порта, то будут существовать селекторы, как для локального, так и для удаленного порта.

Селектор	Элемент SPD	PFP	Значение в инициирующем пакете	Получающийся элемент SAD
loc port	список диапазонов		0 src port "s"	list of ranges
	ANY	0	src port "s"	ANY
	OPAQUE	0	src port "s"	OPAQUE
	list of ranges	0	not avail.	discard packet
	ANY	0	not avail.	ANY
	OPAQUE	0	not avail.	OPAQUE
	list of ranges	1	src port "s"	"s"
	ANY	1	src port "s"	"s"
	OPAQUE	1	src port "s"	***
	list of ranges	1	not avail.	discard packet
	ANY	1	not avail.	discard packet
	OPAQUE	1	not avail.	***
rem port	list of ranges	0	dst port "d"	list of ranges
	ANY	0	dst port "d"	ANY
	OPAQUE	0	dst port "d"	OPAQUE
	list of ranges	0	not avail	discard packet

	ANY	0	not avail	ANY
	OPAQUE	0	not avail.	OPAQUE
	list of ranges	1	dst port "d"	"d"
	ANY	1	dst port "d"	"d"
	OPAQUE	1	dst port "d"	***
	list of ranges	1	not avail.	discard packet
	ANY	1	not avail.	discard packet
	OPAQUE	1	not avail.	***

Если протоколом является заголовок мобильности, то будет существовать селектор для типа заголовка мобильности (MH type).

Selector	SPD Entry	PFP	Value in Triggering Packet	Resulting SAD Entry
mh type	list of ranges	0	mh type "T"	list of ranges
	ANY	0	mh type "T"	ANY
	OPAQUE	0	mh type "T"	OPAQUE
	list of ranges	0	not avail.	discard packet
	ANY	0	not avail.	ANY
	OPAQUE	0	not avail.	OPAQUE
	list of ranges	1	mh type "T"	"T"
	ANY	1	mh type "T"	"T"
	OPAQUE	1	mh type "T"	***
	list of ranges	1	not avail.	discard packet
	ANY	1	not avail.	discard packet
	OPAQUE	1	not avail.	***

Если протоколом является ICMP, то будет существовать 16-битовый селектор для типа ICMP и кода ICMP. Заметим, что тип и код связаны друг с другом, то есть коды применяются с конкретным типом. Этот 16-битовый селектор может содержать один тип и диапазон кодов, один тип и код ANY, тип ANY и код ANY.

Selector	SPD Entry	PFP	Value in Triggering Packet	Resulting SAD Entry
ICMP type and code	a single type & range of codes	0	type "t" & code "c"	single type & range of codes
	a single type & ANY code	0	type "t" & code "c"	single type & ANY code
	ANY type & ANY code	0	type "t" & code "c"	ANY type & ANY code
	OPAQUE	0	type "t" & code "c"	OPAQUE
	a single type & range of codes	0	not avail.	discard packet
	a single type & ANY code	0	not avail.	discard packet
	ANY type & ANY code	0	not avail.	ANY type & ANY code
	OPAQUE	0	not avail.	OPAQUE
	a single type &	1	type "t" &	"t" and "c"

range of codes		code "c"	
a single type &	1	type "t" &	"t" and "c"
ANY code		code "c"	
ANY type &	1	type "t" &	"t" and "c"
ANY code		code "c"	
OPAQUE	1	type "t" &	***
		code "c"	
a single type &	1	not avail.	discard packet
range of codes			
a single type &	1	not avail.	discard packet
ANY code			
ANY type &	1	not avail.	discard packet
ANY code			
OPAQUE	1	not avail.	***

Если используется селектор имени:

Selector	SPD Entry	PFP	Value in Triggering Packet	Resulting SAD Entry
name	list of system-dependent user or sys. names	N/A	packet from user or system	N/A

* "List of protocols" is the information, not the way that the SPD or SAD or IKv2 have to represent this information.
** 0 (zero) is used by IKE to indicate ANY for protocol.
*** Use of PFP=1 with an OPAQUE value is an error and SHOULD be prohibited by an IPsec implementation.
**** The protocol field cannot be OPAQUE in IPv4. This table entry applies only to IPv6.

* "Список протоколов" (List of protocols) – это информация, а не способ, которым SPD, SAD или IKv2 должны представлять эту информацию.
** 0 (ноль) используется IKE для указания для протокола значения ANY.
*** Использование PFP=1 со значением OPAQUE является ошибкой и должно (SHOULD) быть запрещено реализацией IPsec.
**** Поле протокола в IPv4 не может иметь значение OPAQUE. Этот элемент таблицы применим только к IPv6.

4.4.3. База данных авторизации партнера (PAD)

База данных авторизации партнера (PAD - Peer Authorization Database) обеспечивает связь между протоколом управления SA, подобным IKE, и SPD. Она реализует несколько критически важных функций:

- Идентифицирует партнеров или группы партнеров, которые авторизованы для обмена информацией с данным объектом IPsec
- Определяет протокол и метод, используемые для аутентификации каждого партнера
- Предоставляет аутентификационные данные для каждого партнера
- Ограничивает типы и значения идентификаторов, которые могут объявляться партнером относительно создания дочернего SA, чтобы гарантировать, что партнер не объявляет идентификаторы для поиска в SPD, которые он не авторизован представлять при создании дочерних SA
- Информация о местоположении шлюза партнера, например, IP-адрес (адреса) или имена DNS, может (MAY) быть включена для партнеров, о которых известно, что они находятся «за» защитным шлюзом.

PAD предоставляет эти функции для партнера IKE, когда партнер действует в качестве инициатора или в качестве ответчика.

Для выполнения этих функций PAD содержит элемент для каждого партнера или группы партнеров, с которыми объект IPsec будет осуществлять обмен информацией. Элемент именует индивидуального партнера (пользователя, оконечную систему или защитный шлюз) или определяет группу партнеров (используя идентификатор, соответствующий определенным ниже правилам). Элемент определяет протокол аутентификации (например, IKEv1, IKEv2, KINK), используемый метод (например, сертификаты или заранее распределенные секреты) и аутентификационные данные (например, заранее распределенный секретили доверительный якорь, относительно которого сертификат партнера будет подтверждаться). Для аутентификации, основанной на сертификатах, элемент может также обеспечивать информацию для содействия проверке состояния аннулирования партнера, например, указатель на хранилище списков аннулированных сертификатов (CRL), или имя сервера протокола оперативного статуса сертификатов (OCSP – Online Certificate Status Protocol), связанного с партнером, или указатель на доверительный якорь, связанный с партнером.

В каждом элементе определяется также, будет ли использоваться для поиска в SPD в качестве символического имени блок данных IKE ID, или будет ли использоваться для поиска в SPD при открывании дочерних SA удаленный IP-адрес, предоставляемый блоках данных селекторов трафика.

Заметим, что информация PAD может (MAY) использоваться для поддержки создания между двумя партнерами за раз нескольких SA туннельного режима, например, двух туннелей для защиты одних и тех же адресов/хостов, но с различными оконечными точками туннелей.

4.4.3.1. Идентификаторы элементов PAD и правила сопоставления

PAD представляет собой упорядоченную базу данных, в которой порядок определяется администратором (или пользователем в случае однопользовательской оконечной системы). Обычно один и тот же администратор будет ответственным как за PAD, так и за SPD, поскольку обе базы данных должны быть скоординированными. Требование упорядочивания возникает по тем же причинам, что и в SPD, то есть из-за того, что использование элементов со «звездными именами» (star name) допускает пересечение в множестве идентификаторов IKE, которое соответствует конкретному элементу.

Для элементов в PAD поддерживаются шесть типов идентификаторов, согласующихся с типами символических имен и IP-адресами, используемыми для идентификации элементов SPD. Идентификатор (ID) для каждого элемента действует в качестве индекса для PAD, то есть он представляет собой значение, которое используется для выбора элемента. Все эти типы идентификаторов могут использоваться для сопоставления с типами блоков данных IKE ID. Этими шестью типами идентификаторов являются:

- Имя DNS (конкретное, либо частичное)
- Различительное имя (полное, либо ограниченное поддеревом)
- Адрес электронной почты RFC 822 (полный или частично квалифицированный)
- Адрес IPv4 (диапазон)
- Адрес IPv6 (диапазон)
- Key ID - Идентификатор ключа (только в точности совпадающий)

Первые три типа могут осуществлять совпадение по поддереву, а также полное совпадение. Имя DNS может быть полностью квалифицированным, и тем самым в точности совпадать с одним именем, например, foo.example.com. В качестве альтернативы, будучи частично квалифицированным, имя может охватывать группу партнеров, например, строка «.example.com.» может быть использована для сопоставления с любым именем DNS, которая заканчивается этими двумя компонентами доменного имени.

Подобным образом, различительное имя может определять полное различительное имя для сравнения с ровно одним элементом, например, CN = Stephen, O = BBN Technologies, SP= MA, C = US. В качестве альтернативы элемент может охватывать группу партнеров путем определения поддерева, например, элемент вида «C = US, SP= MA» может использоваться для сопоставления со всеми различительными именами, которые содержат эти два атрибута в качестве двух верхних относительных различительных имен (RDN).

Для адресов электронной почты RFC 822 имеется такая же возможность. Полный адрес, например, foo@example.com соответствует одному элементу, но имя поддерева, например «@example.com» может использоваться для сопоставления со всеми элементами, имена которых заканчиваются двумя компонентами доменного имени, расположенными справа от знака @.

Специальный синтаксис, используемый реализацией для осуществления сравнения поддеревьев для различительных имен, доменных имен и адресов электронной почты RFC 822, является локальным вопросом. Но, как минимум, сравнение поддеревьев описанного выше вида должно (MUST) поддерживаться. (Сравнение с подстроками в различительном имени, имени DNS или адресе RFC 822 может (MAY) поддерживаться, но не требуется).

Для адресов IPv4 и IPv6 должен (MUST) поддерживаться тот же самый синтаксис диапазонов адресов, что и для элементов SPD. Это позволяет определять индивидуальный адрес (посредством тривиального диапазона), адресный префикс (путем выбора диапазона, который придерживается стиля префиксов бесклассовой междоменной маршрутизации (CIDR – Classless Inter-Domain Routing)), или произвольный диапазон адресов.

Поле Key ID в IKE определяется как строка октетов. Для этого типа имени должен (MUST) поддерживаться только синтаксис точного совпадения (поскольку для этого типа идентификатора подробно разработанная структура отсутствует). Для этого типа идентификатора могут (MAY) поддерживаться дополнительные функции сравнения.

4.4.3.2. Данные аутентификации партнера IKE

В PAD указывается номенклатура идентификаторов, которые партнер IPv4 или IPv6 авторизуется представлять, когда с ним согласуются (дочерние) SA. Эти идентификаторы могут представлять собой список диапазонов адресов IPv4 или IPv6, или набор символических имен. Версия IP идентификаторов не обязательно должна быть той же самой, что и версия IP партнера, их представляющего. Фундаментальное требование, связанное с PAD, заключается в том, что селекторы трафика, передаваемые протоколом управления контекстом безопасности для сравнения с SPD, должны (MUST) быть проверены как авторизованные по отношению к аутентифицированному партнеру протокола управления SA. (См. также п. 4.5.3, который вводит требования к PAD по поддержке определения местоположения защитных шлюзов).

PAD определяет также, как аутентифицировать каждого партнера, например, с помощью общего секрета или с помощью сертификата. Если используется общий секрет, то этот секрет хранится здесь. Если должен использоваться сертификат, то для подтверждения сертификата через PAD доступен доверительный якорь. PAD может (MAY) включать также данные для поддержки проверки статуса отмены сертификата, если эта информация иным образом не доступна из доверительного якоря или из сертификата партнера. Поскольку PAD может быть встроена в реализацию протокола управления контекстами безопасности, в данном документе она широко не обсуждается.

4.5. SA и управление ключами

Все реализации IPsec должны (MUST) поддерживать как ручное, так и автоматическое управление SA и криптографическими ключами. Протоколы IPsec, AH и ESP, почти совершенно не зависят от связанных с ними методов управления SA, хотя применяемые методы влияют на некоторые сервисы безопасности, обеспечиваемые этими протоколами. Например, факультативный сервис предотвращения повторного воспроизведения пакетов, доступный для AH и ESP, требует автоматического управления SA. Более того, степень детализации распределения ключей, применяемая с IPsec, определяет предоставляемую степень детализации аутентификации. Вообще, аутентификация первоисточника данных в AH и ESP ограничена той степенью, с которой секреты, используемые с алгоритмами обеспечения целостности (или с протоколом управления ключами, который создает такие секреты), разделяются между несколькими возможными источниками.

В нижеследующем тексте описываются минимальные требования для обоих типов управления SA.

4.5.1. Ручные методы

Простейшей формой управления является ручное управление, при котором человек вручную конфигурирует каждую систему ключевым материалом и данными управления SA, соответствующими необходимой защите обмена информацией с другими системами. Ручные методы являются практичными в небольших статических средах, но они хорошо не масштабируются. Например, некоторая компания может создать виртуальную частную сеть (VPN - Virtual Private Network), используя IPsec в защитных шлюзах на нескольких сайтах. Если количество сайтов не велико, и поскольку все сайты попадают в границы одного административного домена, это могло бы быть реальным контекстом для методов ручного управления. В этом случае защитный шлюз мог бы выборочно защищать трафик к другим сайтам и от них в рамках организации, используя вручную конфигурируемый ключ, не защищая при этом трафик, предназначенный для других мест назначения. Такой метод может также подойти, если требуется защитить только специально выбранные обмены информацией. Подобный аргумент можно применить для использования IPsec полностью в рамках некоторой организации для небольшого числа хостов и/или защитных шлюзов. Методы ручного управления часто применяют статически конфигурируемые, симметричные ключи, хотя существуют также и другие дополнительные возможности.

4.5.2. Автоматическое управление SA и ключами

Широкое развертывание и использование IPsec требует стандартного для Internet, масштабируемого, автоматического протокола управления SA. Такая поддержка требуется для облегчения использования свойств AH и ESP по противодействию повторному воспроизведению пакетов, а также для обеспечения создания SA по запросу, например, для установки ключей, ориентированной на пользователя и сеансы связи. (Заметим, что понятие "переустановки" SA (rekeying) в действительности предполагает создание нового SA с новым SPI, процесс, который в общем случае предполагает использование автоматического протокола управления контекстами безопасности и ключами).

По умолчанию автоматическим протоколом управления ключами, выбранным для использования с IPsec является IKEv2 [Kau04]. Данный документ предполагает доступность определенных функций протокола управления ключами, которые не поддерживаются IKEv1. Другие автоматические протоколы управления SA могут (MAY) применяться.

Когда применяется автоматический протокол управления контекстами безопасности и ключами, выходные данные этого протокола используются для генерации нескольких ключей для одного SA. Это происходит также потому, что для каждого из двух SA, создаваемых IKE, используются разные ключи. Если применяется как обеспечение целостности, так и обеспечение конфиденциальности, то требуется как минимум четыре ключа. Кроме того, некоторые криптографические алгоритмы могут требовать нескольких ключей, например, 3DES.

Система управления ключами (Key Management System) может представить отдельную битовую строку для каждого ключа, или может сформировать одну битовую строку, из которой извлекаются все ключи. Если предоставляется одна битовая строка, то необходимо соблюдать осторожность, чтобы гарантировать, что части системы, которые отображают эту битовую строку на требуемые ключи, выполняли это одинаковым способом на обоих концах SA. Чтобы гарантировать, что реализации IPsec на каждом из концов SA будут использовать те же самые биты для одних и тех же ключей, и независимо от того, какая часть системы делит битовую строку на отдельные ключи, ключи шифрования должны (MUST) браться из первых (самых левых, наиболее значимых) бит, а ключи обеспечения целостности должны (MUST) браться из оставшихся бит. Количество бит для каждого ключа определяется в соответствующем документе RFC спецификации криптографического алгоритма. В случае нескольких ключей шифрования или нескольких ключей обеспечения целостности спецификация криптографического алгоритма должна определять порядок, в котором они должны выбираться из одной битовой строки, подготовленной для криптографического алгоритма.

4.5.3. Определение местоположения защитного шлюза

В данном пункте обсуждаются вопросы, связанные с тем, как хост узнает относительно существования соответствующих защитных шлюзов, и когда хост связался с этими защитными шлюзами, откуда он знает, что они представляют собой правильные защитные шлюзы. Детали того, где хранится требуемая информация, является локальным вопросом, но база данных авторизации партнеров (PAD), описанная в подразд. 4.4, является наиболее вероятным кандидатом. (Примечание: S* указывает систему, которая выполняет IPsec, например, ниже системы SH1 и SG2).

Рассмотрим ситуацию, в которой удаленный хост (SH1) использует Internet для получения доступа к серверу или другой машине (H2) и имеется защитный шлюз (SG2), например, межсетевой экран, через который должен проходить трафик H1. Примером такой ситуации может служить мобильный хост (road warrior), соединяющийся через Internet с межсетевым экраном (SG2) своей родной организации. В этой ситуации возникает несколько вопросов:

1. Откуда SH1 знает/узнает относительно существования защитного шлюза SG2?

2. Каким образом он аутентифицирует SG2, и когда он аутентифицировал SG2, каким образом он подтверждает, что SG2 был авторизован для представления H2?

3. Каким образом SG2 аутентифицирует SH1 и проверяет, что SH1 авторизован для связи с H2?

4. Откуда SH1 знает/узнает о любых дополнительных шлюзах, которые предоставляют альтернативные пути к H2?

Для решения этих проблем хост или защитный шлюз, поддерживающие IPsec, должны (MUST) иметь административный интерфейс, который позволяет пользователю/администратору конфигурировать адрес одного или нескольких защитных шлюзов для диапазонов адресов мест назначения, которые требуют его использования. Это включает возможность конфигурирования информации для определения местоположения и аутентификации одного или нескольких защитных шлюзов и проверки авторизации этих защитных шлюзов на предмет представления хоста места назначения. (Функция авторизации предполагается в PAD). Данный документ не рассматривает вопрос о том, как автоматизировать поиск/проверку защитных шлюзов. Рабочая группа IPSP (IP Security Policy) является возможным будущим источником руководящих материалов. Одной из ее задач является выпуск чернового варианта проекта (Internet Draft) на тему "Security Gateway Discovery, Policy Exchange and Negotiation Protocol".

4.6. Контексты безопасности (SA) и групповой трафик (Multicast)

Ориентация контекстов безопасности на приемника трафика предполагает, что в случае индивидуального (unicast) трафика система назначения выберет значение SPI. Когда система назначения выбирает значение SPI, отсутствует потенциальная возможность вручную сконфигурированным контекстам безопасности конфликтовать с контекстами безопасности, конфигурируемыми автоматически (например, посредством протокола управления ключами), или контекстам безопасности из нескольких источников конфликтовать друг с другом. Для группового (multicast) трафика существует несколько систем назначения, связанных с одним SA. Таким образом, некоторая система или человек должны координировать все мультикастовые группы для выбора SPI или нескольких SPI по поручению каждой мультикастовой группы и затем сообщить IPsec-информацию группы всем легитимным членам этой мультикастовой группы с помощью механизмов, которые в данном документе не определены.

Когда применяется алгоритм шифрования или обеспечения целостности с симметричным ключом, несколько отправителей трафика в мультикастовую группу должны (SHOULD) использовать один контекст безопасности (а поэтому и SPI) для всего трафика, направляемого этой группе. В этих обстоятельствах получатель вообще не будет иметь возможность аутентифицировать, какая система послала групповой трафик. Спецификации других, более общих подходов к групповому трафику отложены на усмотрение рабочей группы IETF Multicast Security.

5. Обработка IP-трафика

Как упоминалось в п. 4.4.1, "База данных политики безопасности" (SPD - Security Policy Database), к SPD (или к связанным с ней кэшам) должны (MUST) выполняться обращения во время обработки всего трафика, который пересекает границу IPsec, включая трафик управления IPsec. Если в SPD не найдено никакой политики, которая соответствует пакету (для входящего или для исходящего трафика), то этот пакет должен (MUST) быть отброшен. Чтобы упростить обработку и обеспечить очень быстрый поиск SA (для реализаций SG/BITS/BITW), данный документ вводит понятие кэша SPD для всего исходящего трафика (SPD-O и SPD-S), а также кэша для входящего, не защищенного IPsec трафика (SPD-I). (Как упоминалось ранее, SAD действует в качестве кэша для проверки селекторов входящего, защищенного IPsec трафика, поступающего по контекстам безопасности). Номинально имеется один кэш на каждую SPD. Для целей данной спецификации предполагается, что каждый кэшированный элемент будет отображаться ровно на один контекст безопасности (SA). Однако заметим, что возникают исключения, когда используются несколько SA для передачи трафика с различными приоритетами (например, как указывается отдельными значениями DSCP), но с одними и теми же селекторами.

Поскольку элементы SPD могут перекрываться, в общем случае нельзя безопасно кэшировать эти элементы. Простое кэширование может привести к совпадению с каким-то элементом кэша, в то время как упорядоченный поиск в SPD может привести к совпадению с другим элементом. Однако, если элементы SPD сначала декоррелируются, то элементы, полученные в результате этого процесса, могут безопасно кэшироваться. Каждый кэшированный элемент будет указывать, что совпадающий трафик должен быть передан в обход или отбрасываться, соответственно. (Примечание: Первоначальный элемент SPD может привести к нескольким контекстам безопасности (SA), например, из-за PFP). Если иное не отмечается, все приведенные ниже указания на "SPD", или "кэш SPD", или "кэш", относятся к декоррелированным SPD (SPD-I, SPD-O, SPD-S) или к кэшу SPD, содержащему элементы из декоррелированной SPD.

Примечание: В реализации IPsec хоста, основанной на сокетах, обращения к SPD будут происходить каждый раз, когда открывается новый сокет, чтобы определить, какая обработка IPsec, если таковая необходима, будет применяться к трафику, который будет проходить через этот сокет. Это предоставляет неявный механизм кэширования, и части данного выше обсуждения, которые касаются кэширования, в таких реализациях могут игнорироваться.

Примечание: Предполагается, что все начинается с коррелированной SPD, поскольку она отражает то, как пользователи и администраторы приучены

управлять этого рода списками контроля доступа или правилами фильтрации межсетевых экранов. Затем применяется алгоритм декоррелирования, чтобы построить список готовых для кэширования элементов SPD. Декоррелирование не видимо на интерфейсе управления.

Для входящего IPsec-трафика элемент SAD, выбранный по SPI, служит в качестве кэша для селекторов, которые должны сопоставляться с поступающими IPsec-пакетами после того, как будет выполнена обработка AH или ESP.

5.1. Обработка исходящего IP-трафика (с защищенного интерфейса на незащищенный интерфейс)

Сначала рассмотрим путь трафика, поступающего на вход реализации через защищенный интерфейс и выходящего через незащищенный интерфейс.

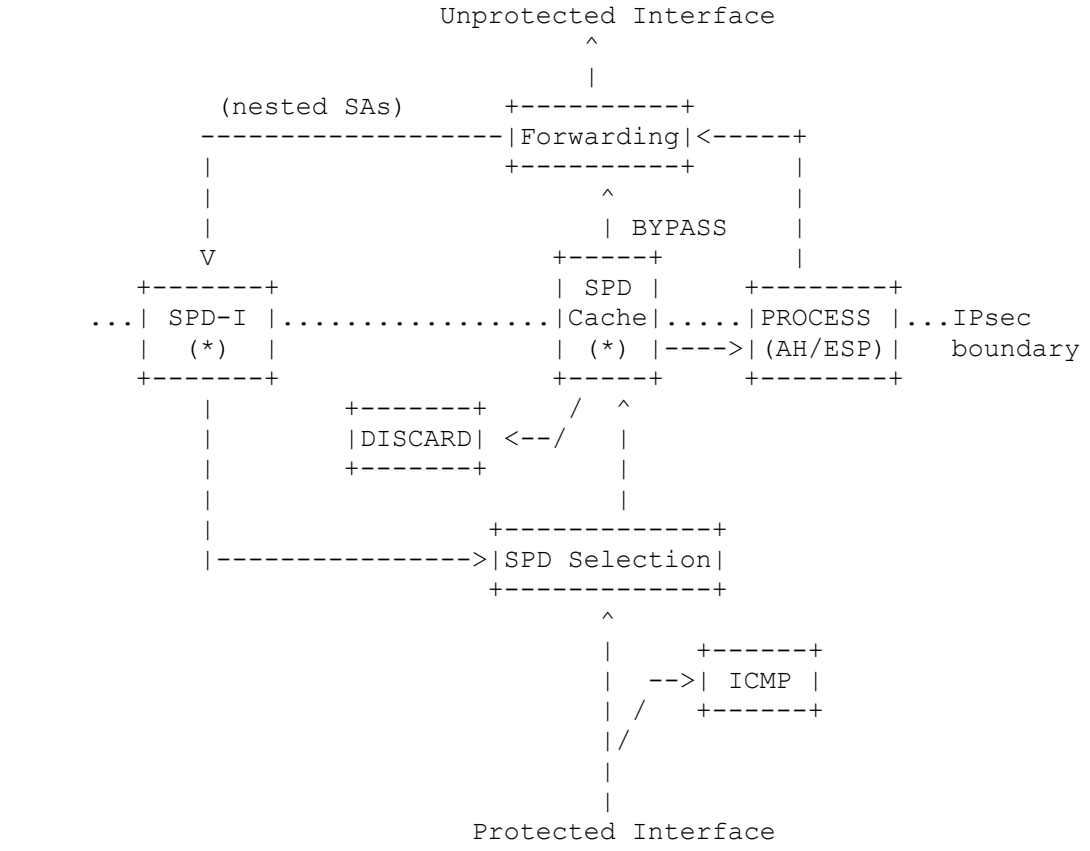

Рис. 2. Модель обработки исходящего трафика
(*) = Здесь показаны кэши SPD. Если происходит промах в кэше, то проверяется SPD. Отсутствует требование того, чтобы реализация буферизовала пакет в случае промаха в кэше.

При обработке исходящих пакетов IPsec должен (MUST) выполнять следующие шаги:

1. Когда пакет поступает с (защищенного) интерфейса абонента, вызвать функцию выбора SPD, чтобы получить SPD-ID, необходимый для выбора соответствующей SPD. (Если реализация использует только одну SPD, то этот шаг является холостым).

2. Сравнить заголовки пакета с кэшем для SPD, определенной идентификатором SPD-ID на шаге 1. Заметим, что этот кэш содержит элементы из SPD-O и SPD-S.

3a. Если имеется совпадение, то обработать пакет так, как определено совпадающим элементом кэша, т.е. пустить в обход (BYPASS), отбросить (DISCARD), или защитить (PROTECT) с помощью AH или ESP. Если применяется обработка IPsec, то существует связь (указатель) от

элемента кэша SPD к соответствующему элементу SAD (определяющему режим, криптографические алгоритмы, ключи, SPI, PMTU, и т.д.). Обработка IPsec, как было ранее определено, выполняется для туннельного или транспортного режимов и для AH или ESP, как специфицировано в соответствующих им RFC [Ken04b и Ken04a]. Заметим, что значение PMTU SA, плюс значение флага контекстной проверки фрагментов (и бита DF в IP-заголовке исходящего пакета) определяют, может ли (должен ли) пакет фрагментироваться до или после IPsec-обработки, или должен ли он отбрасываться и посылаться сообщение ICMP PMTU.

3b. Если в кэше совпадение не найдено, выполнить поиск в SPD (в частях SPD-S и SPD-O), определяемых SPD-ID. Если элемент SPD требует передачи в обход (BYPASS) или отбрасывания (DISCARD), то создать один или несколько новых элементов исходящего кэша SPD. (Может быть создано более одного элемента кэша, поскольку декоррелированный элемент SPD может быть связан с другими такими элементами, которые были созданы в результате побочного эффекта процесса декорреляции). Если элемент SPD требует защиты (PROTECT), т.е. создания SA, то для создания SA вызывается механизм управления ключами (например, IKEv2). Если создание SA происходит успешно, то создается новый элемент исходящего кэша (SPD-S) вместе с исходящими и входящими элементами SAD, в противном случае пакет отбрасывается. (Пакет, который инициирует поиск в SPD, может (MAY) реализацией либо обрабатываться, либо он может (MAY) реализацией обрабатываться на фоне вновь создаваемого элемента кэша, если последний создается). Поскольку контексты безопасности создаются парами, то создается также и элемент SAD для соответствующего входящего SA для использования при проверке входящего трафика, доставляемого через этот SA, и он содержит значения селекторов, взятые из элемента SPD (и пакета, если какой-либо флаг PFP имел значение "true"), который использовался для создания входящего SA.

4. Пакет передается функции исходящей пересылки (работающей вне реализации IPsec) для выбора интерфейса, на который будет направлен пакет. Эта функция может стать причиной того, что пакет должен будет передаваться назад через границу IPsec для дополнительной обработки IPsec, например, при поддержке вложенных SA. Если это случится, должен (MUST) существовать элемент в базе данных SPD-I, который разрешает входящий обходной путь пакета, в противном случае пакет будет отброшен. Если необходимо, т.е. если существует более одной SPD-I, то заворачиваемый назад трафик может (MAY) быть помечен, как пришедший с этого внутреннего интерфейса. В случае необходимости это позволит использовать различные SPD-I для "реального" внешнего трафика и завернутого трафика.

Примечание: За исключением транспортного режима IPv4 и IPv6, реализация SG, BITS, или BITW может (MAY) фрагментировать пакты до применения IPsec. (Это применимо только для IPv4. Для IPv6-пакетов только первоисточнику позволено их фрагментировать). Устройство должно (SHOULD) иметь конфигурационную установку для отмены этого. Результирующие фрагменты сравниваются с SPD обычным образом. Таким образом, фрагменты, не содержащие номеров портов (или тип и код сообщений ICMP, или тип заголовка мобильности), будут соответствовать правилам, имеющим значения селекторов портов (или типов и кодов сообщений ICMP, или типов MH) равные OPAQUE или ANY. (См. более подробно в разд. 7).

Примечание: Что касается определения и установки PMTU SA, то система IPsec должна (MUST) следовать шагам, описанным в подразд. 8.2.

5.1.1. Обработка исходящего пакета, который должен быть отброшен

Если система IPsec получает исходящий пакет, и определяет, что он должен быть отброшен, то она должна (SHOULD) быть способной формировать и посылать сообщение ICMP для указания отправителю исходящего пакета того, что он был отброшен. Как специфицировано ниже, тип и код сообщения ICMP будет зависеть

от причины отбрасывания пакета. Сама причина должна (SHOULD) быть записана в журнал аудита. Элемент журнала аудита для этого события должен (SHOULD) содержать причину, текущие дату и время, а также значения селекторов из пакета.

a. Селекторы пакета совпадают с элементом SPD, требующим отбрасывания пакета.

IPv4 Type = 3 (destination unreachable) Code = 13 (Communication Administratively Prohibited)

IPv6 Type = 1 (destination unreachable) Code = 1 (Communication with destination administratively prohibited)

b1. Система IPsec успешно достигла удаленного партнера, но не смогла согласовать контекст безопасности (SA), требуемый элементом SPD, который совпадает с пакетом, например, из-за того, что удаленному партнеру административно запрещен обмен информацией с инициатором, или партнер-инициатор не смог себя аутентифицировать у удаленного партнера, или удаленный партнер не смог себя аутентифицировать у партнера-инициатора, или SPD у удаленного партнера не имела подходящего элемента и т.п.

IPv4 Type = 3 (destination unreachable) Code = 13 (Communication Administratively Prohibited)

IPv6 Type = 1 (destination unreachable) Code = 1 (Communication with destination administratively prohibited)

b2. Система IPsec не смогла установить контекст безопасности, требуемый элементом SPD, который совпадает с пакетом, из-за того, что с партнером IPsec на другом конце обмена не смогла связаться.

IPv4 Type = 3 (destination unreachable) Code = 1 (host unreachable)

IPv6 Type = 1 (destination unreachable) Code = 3 (address unreachable)

Заметим, что злоумышленник, находящийся за защитным шлюзом, может посылать пакеты с подделанным адресом источника W.X.Y.Z на элемент SPD, который вынуждает его посылать сообщения ICMP на адрес W.X.Y.Z. Это создает возможность проведения атак на доступность хостов, находящихся за защитным шлюзом. Чтобы с ними иметь дело, защитный шлюз должен (SHOULD) включать средство управления, позволяющее администратору конфигурировать реализацию IPsec так, чтобы в этих случаях посылать или не посылать сообщения ICMP, и если выбирается такое средство, то ограничивать скорость передачи таких ICMP-ответов.

5.1.2. Создание заголовка для туннельного режима

В данном разделе описывается обработка внутреннего и внешнего IP-заголовков, заголовков расширения и опций для AH- и ESP-туннелей в отношении к обработке исходящего трафика. Он включает информацию о том, как создавать инкапсулирующий (внешний) IP-заголовок, как обрабатывать поля во внутреннем IP-заголовке, а также информацию о том, какие другие действия должны быть выполнены для исходящего трафика туннельного режима. Описанная здесь общая обработка основана на модели RFC 2003, "IP Encapsulation with IP" [Per96]:

- Поля Source Address и Destination Address внешнего IP-заголовка указывают "оконечные точки" туннеля (инкапсулятор и декапсулятор). Поля Source Address и Destination Address внутреннего IP-заголовка указывают

истинных отправителя и получателя дейтаграммы, соответственно (с точки зрения этого туннеля). (Более подробно об инкапсуляции IP-адреса источника см. примечание 3 после таблицы в разделе 5.1.2.1).

- Внутренний IP-заголовок не меняется, за исключением полей TTL (или Hop Limit) и DS/ECN, как указано ниже. Во всем остальном внутренний IP-заголовок остается неизменным во время его доставки до точки выхода из туннеля.

- Во время доставки инкапсулированной дейтаграммы через туннель не происходит никаких изменений IP-опций и заголовков расширения.

Примечание: Туннельный режим IPsec отличается от туннелирования IP-in-IP (RFC 2003) в нескольких аспектах:

- IPsec предлагает администратору безопасности определенные средства управления секретными каналами (о которых обычно не заботятся при туннелировании), а также для гарантии того, что приемник проверит должное состояние полученного пакета: применение контроля доступа. Реализация IPsec может (MAY) конфигурироваться относительно того, как она обрабатывает для передаваемых пакетов внешнее поле DS для туннельного режима. Для исходящего трафика одна из конфигурационных установок для внешнего поля DS будет работать, как описано в следующих разделах, касающихся обработки заголовков IPv4 и IPv6 для туннелей IPsec. Другая установка позволит отображать внешнее поле DS на фиксированное значение, которое может (MAY) конфигурироваться для каждого контекста безопасности (SA). (В действительности это значение может быть зафиксировано для всего трафика, исходящего из устройства, но детализация с точностью до каждого SA также позволяет это сделать). Эта опция конфигурирования позволяет локальному администратору принять решение о том, превосходит ли секретный канал, предоставляемый копированием этих бит, преимущество копирования.

- IPsec описывает, как обрабатывать ECN или DS.

- IPsec позволяет иметь версию IP инкапсулирующего заголовка, отличную от версии IP внутреннего заголовка.

Таблицы в следующих подразделах показывают обработку для различных полей заголовка/опций (термин "созданное" означает, что значение во внешнем поле создается независимо от значения во внутреннем поле).

5.1.2.1. IPv4 -- создание заголовка для туннельного режима

	<-- How Outer Hdr Relates to Inner Hdr -->	
	Outer Hdr at	Inner Hdr at
IPv4	Encapsulator	Decapsulator
Header fields:	---	---
version	4 (1)	no change
header length	constructed	no change
DS Field	copied from inner hdr (5)	no change
ECN Field	copied from inner hdr	constructed (6)
total length	constructed	no change
ID	constructed	no change
flags (DF,MF)	constructed, DF (4)	no change
fragment offset	constructed	no change
TTL	constructed (2)	decrement (2)
protocol	AH, ESP	no change
checksum	constructed	constructed (2)(6)
src address	constructed (3)	no change
dest address	constructed (3)	no change
Options	never copied	no change

1. Значение версии IP в инкапсулирующем заголовке может отличаться от значения версии во внутреннем заголовке.

2. Поле TTL во внутреннем заголовке декрементируется инкапсулятором до пересылки и декапсулятором, если он пересылает пакет. (Контрольная сумма IPv4 при изменении TTL изменяется).

   Примечание: Декрементирование значения TTL является стандартной частью пересылки пакета. Таким образом, пакет, исходящий из того же узла, что и инкапсулятор, не имеет инкрементированного значения TTL, поскольку узел-отправитель скорее создает пакет, а не пересылает его.

3. Локальный и удаленный адреса зависят от SA, используемого для определения удаленного адреса, который, в свою очередь, определяет, какой локальный адрес (сетевой интерфейс) используется для пересылки пакета.

   Примечание: Для группового (multicast) трафика адрес места назначения или адреса источника и места назначения могут потребоваться для демультиплексирования. В этом случае важно гарантировать согласованное состояние времени жизни SA путем обеспечения того, что адрес источника, возникающий в инкапсулирующем туннельном заголовке, был бы тем же самым, что и адрес, который был согласован в процессе установления SA. Имеется одно исключение к этому общему правилу, а именно, реализация IPsec мобильного узла в процессе перемещения будет обновлять свой адрес источника.

4. Конфигурация определяет, должен ли DF копироваться из внутреннего заголовка (только IPv4), обнуляться или устанавливаться.

5. Если пакет поступит непосредственно в домен, для которого значение DSCP во внешнем заголовке не соответствует, это значение должно (MUST) быть отображено на значение, соответствующее этому домену [RFC 2474]. Дополнительную информацию см. в RFC 2475[BBCDWW98].

6. Если поле ECN во внутреннем заголовке устанавливается в значение ECT(0) или ECT(1), а поле ECN во внешнем заголовке устанавливается в значение CE, то установить поле ECN во внутреннем заголовке в значение CE, в противном случае не проводить никаких изменений поля ECN во внутреннем заголовке. (Контрольная сумма IPv4 при изменении поля ECN изменяется).

Примечание: IPsec не копирует опции из внутреннего заголовка во внешний заголовок и не создает опций во внешнем заголовке. Однако код post-IPsec может (MAY) вставлять/создавать опции для внешнего заголовка.

5.1.2.2. IPv6 – Создание заголовка для туннельного режима

См. примечания 1-6, указываемые (номером сноски) в предыдущем разделе 5.1.2.1.

	<-- How Outer Hdr Relates	Inner Hdr --->
	Outer Hdr at	Inner Hdr at
IPv6	Encapsulator	Decapsulator
Header fields:	----------	----------
version	6 (1)	no change
DS Field	copied from inner hdr (5)	no change
ECN Field	copied from inner hdr	constructed (6)
flow label	copied or configured (8)	no change
payload length	constructed	no change
next header	AH,ESP,routing hdr	no change
hop limit	constructed (2)	decrement (2)
src address	constructed (3)	no change
dest address	constructed (3)	no change
Extension headers	never copied (7)	no change

7. IPsec не копирует заголовки расширения из внутреннего пакета во внешние заголовки, а также не создает заголовков расширения во внешнем заголовке. Однако код post-IPsec может (MAY) вставлять/создавать заголовки расширения для внешнего заголовка.

8. См. [RaCoCaDe04]. Копирование является приемлемым только для оконечных систем, но не для защитных шлюзов. Если защитный шлюз (SG) скопировал метки потоков из внутреннего заголовка во внешний заголовок, то могут произойти коллизии.

5.2. Обработка входящего IP-трафика (с незащищенного на защищенный интерфейс)

Входящая обработка несколько отличается от исходящей обработки из-за использования индексов параметров безопасности (SPI) для отображения защищенного IPsec трафика на контексты безопасности (SA). Входной SPD-кэш (SPD-I) применяется только к трафику, который идет в обход или отбрасывается. Если поступающий пакет оказывается IPsec-фрагментом с незащищенного интерфейса, то реассемблирование выполняется до обработки IPsec. Смысл любого кэша SPD заключается в том, что пакет, который не совпадает ни с одним его элементом, передается затем на рассмотрение соответствующей SPD. Каждая SPD должна (SHOULD) иметь формальный последний элемент, который обнаруживает все что угодно, что в других отношениях не совпало, и отбрасывает его. Это гарантирует, что трафик, незащищенный IPsec, который поступает и не совпадает ни с одним элементом SPD-I, будет отброшен.

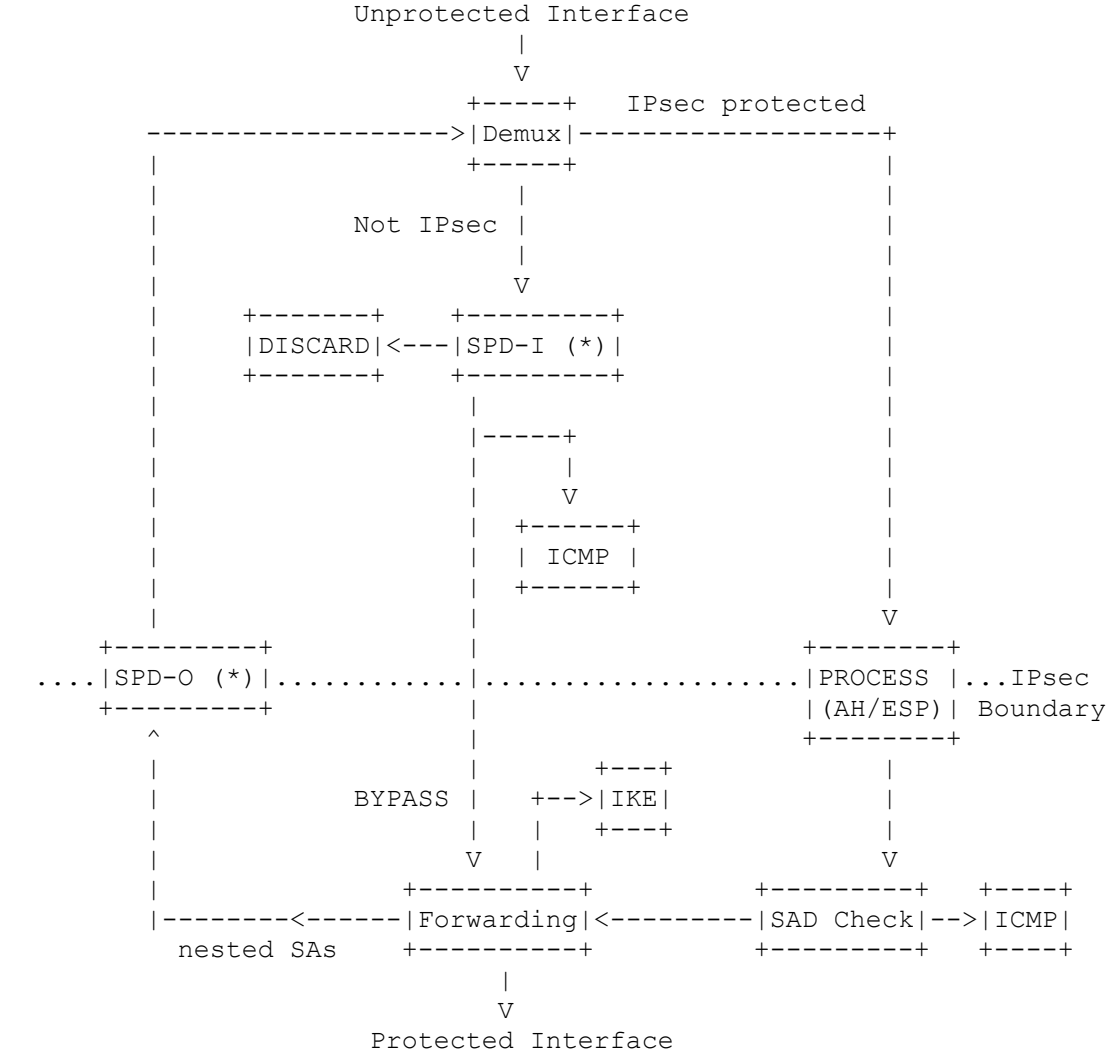

Figure 3. Inbound Traffic Processing Model
(*) = The caches are shown here. If there is

a cache miss, then the SPD is checked.
There is no requirement that an
implementation buffer the packet if
there is a cache miss.

Рис. 3. Модель обработки входящего трафика
(*) = Здесь показываются кэши. Если имеется промах в кэше, то проверяется SPD. Отсутствует требование того, чтобы реализация буферизовала пакет при наличии промаха в кэше.

До выполнения обработки AH или ESP любые IP-фрагменты, которые поступают через незащищенный интерфейс, реассемблируются (IP). Каждая входящая IP-дейтаграмма, к которой будет применяться IPsec-обработка, идентифицируется наличием значений AH или ESP в поле IP Next Protocol (или AH или ESP в качестве протокола следующего уровня в контексте IPv6).

IPsec должен (MUST) выполнять следующие шаги:

1. Когда поступает пакет, он может быть помечен идентификатором (ID) интерфейса (физического или виртуального), через который он поступает, если это необходимо для поддержки нескольких SPD и связанных с ними кэшей SPD-I. (Идентификатор интерфейса отображается на соответствующий SPD-ID).

2. Пакт проверяется и демультиплексируется на одну из двух категорий:

   - Если пакет выглядит как защищенный IPsec и адресован данному устройству, то делается попытка отобразить его на некоторый SA через SAD. Заметим, что устройство может иметь несколько IP-адресов, которые могут использоваться при поиске в SAD, например, в случае таких протоколов, как SCTP.

   - Трафик, не адресованный данному устройству, или адресованный данному устройству и не являющийся AH или ESP, направляется для поиска в SPD-I. (Это предполагает, что IKE-трафик должен (MUST) иметь явный элемент BYPASS в SPD). Если применяется несколько SPD, то метка, присвоенная пакету на шаге 1 используется для выбора соответствующей SPD-I (и кэша) для выполнения поиска. Поиск в SPD-I определяет, какое действие выполнять (DISCARD или BYPASS).

3a. Если пакет адресуется устройству IPsec и в качестве протокола указывается AH или ESP, то пакет осуществляет поиск в SAD. Для индивидуального (unicast) трафика использовать только SPI (или SPI и протокол). Для группового (multicast) трафика использовать только SPI и адрес места назначения, или SPI и адреса источника и места назначения, как определено в разделе 4.1. В любом случае (индивидуального или группового трафика) при отсутствии совпадения отбросить трафик. Это проверяемое событие. Элемент журнала аудита для этого события должен (SHOULD) включать текущие дату/время, SPI, источник и место назначения пакета, протокол IPsec и любые другие значения селекторов пакета, которые доступны. Если пакет найден в SAD, обработать его соответствующим образом (см. шаг 4).

3b. Если пакет не адресован этому устройству или адресован этому устройству и не является AH или ESP, то осуществить поиск заголовка пакета в (соответствующем) кэше SPD-I. Если имеется совпадение и пакет должен быть отброшен или пущен в обход, то сделать это. Если отсутствует совпадение с элементом кэша, то выполнить поиск пакета в соответствующей SPD-I и по ситуации создать элемент кэша. (В ответ на получение пакета, который требует защиты IPsec, не создаются контексты безопасности (SA); этим способом могут создаваться только элементы кэша BYPASS или DISCARD). Если совпадение отсутствует, отбросить трафик. Это проверяемое событие. Элемент журнала аудита для этого события должен (SHOULD) включать текущие дату/время, SPI при доступности, протокол

IPsec при доступности, источник и место назначения пакета и любые другие значения селекторов пакета, которые доступны.

3c. Предполагается, что обработка сообщений ICMP происходит на незащищенной стороне границы IPsec. Незащищенные сообщения ICMP проверяются, и для определения того, принять или отклонить эти сообщения, применяется локальная политика и, в случае их принятия, какие действия предпринять в качестве результата. Например, если получено сообщение ICMP unreachable, то реализация должна решить, действовать ли в соответствии с ним, отбросить его, или действовать в соответствии с ним с ограничениями. (См. раздел 6).

4. Применить обработку AH или ESP, как определено, используя элемент SAD, выбранный на шаге 3a выше. Затем сопоставить пакет с входящими селекторами, указанными элементом SAD, для проверки того, что принятый пакет соответствует SA, через который он был получен.

   Если система IPsec получает входящий пакет по SA, и поля заголовка пакета не согласуются с селекторами для SA, она должна (MUST) отбросить пакет. Это проверяемое событие. Элемент журнала аудита для этого события должен (SHOULD) включать текущие дату/время, SPI, протокол (протоколы) IPsec, источник и место назначения пакета, а также значения селекторов из соответствующего элемента SAD. Система должна (SHOULD) также быть способной формировать и посылать отправителю (партнеру IPsec) уведомление IKE INVALID_SELECTORS для указания того, что принятый пакет был отброшен из-за ошибки при прохождении проверок селекторов.

   Для минимизации воздействия DoS-атак, или неправильного конфигурирования партнера система IPsec должна (SHOULD) включать средство управления, чтобы позволить администратору конфигурировать реализацию IPsec для посылки или не посылки этого уведомления IKE, и если такое средство выбирается, то ограничивать скорость передачи таких уведомлений.

   После того, как трафик был пущен в обход или обработан IPsec, он передается для управления функции входящей пересылки. Эта функция может стать причиной того, что этот пакет необходимо будет послать (в качестве исходящего) через границу IPsec для дополнительной входящей IPsec-обработки, например, при поддержке вложенных SA. Если это так, то, как и для всего (ALL) исходящего трафика, который должен быть пущен в обход, необходимо (MUST) сравнить пакет с элементом SPD-O. В конечном счете, пакет должен быть переслан для управления хосту или процессу назначения.

6. Обработка ICMP

В данном разделе описана IPsec-обработка ICMP-трафика. Имеются два вида ICMP-трафика: сообщения об ошибках (например, type = destination unreachable) и сообщения не об ошибках (например, type = echo). Данная секция занимается исключительно сообщениями об ошибках. Возможность использования ICMP-сообщений не об ошибках (которые сами по себе не относятся к реализации IPsec) должна (MUST) явно учитываться для использования элементов SPD.

Обсуждаемое в данном разделе применимо к ICMPv6, а также к ICMPv4. Кроме того, в качестве инструмента диагностики неисправностей должен предоставляться механизм, позволяющий администратору записывать в журнал сообщения об ошибках ICMP (отобранные сообщения, все сообщения или никаких сообщений).

6.1. Обработка сообщений ICMP, направляемых реализации IPsec

6.1.1. Сообщения об ошибках ICMP, полученные на незащищенной стороне границы

На рис. 3 в разделе 5.2 показан отдельный модуль обработки ICMP на незащищенной стороне границы IPsec для обработки сообщений ICMP (об ошибках или других), которые адресованы устройству IPsec и которые не защищены посредством AH или ESP. Сообщения ICMP такого сорта не аутентифицированы, и их обработка может привести к отказу в обслуживании или к его деградации. Это наводит на мысль о том, что в общем случае желательно такие сообщения игнорировать. Однако многие сообщения ICMP будут приниматься хостами или защитными шлюзами от неаутентифицированных источников, например, от маршрутизаторов в общедоступной сети Internet. Игнорирование таких сообщений ICMP может приводить к деградации сервиса, например, из-за ошибки при обработке сообщения PMTU или сообщений переадресации. Таким образом, имеется также мотивация в пользу приема и исполнения неаутентифицированных сообщений ICMP.

Чтобы обеспечить оба конца этого спектра возможностей, совместимая IPsec-реализация должна (MUST) позволять локальному администратору конфигурировать реализацию IPsec на предмет приема или отклонения неаутентифицированного IPsec-трафика. Это управление должно (MUST) осуществляться с точностью до типа сообщения ICMP и может (MAY) осуществляться с точностью до типа и кода ICMP. Дополнительно, реализация должна (SHOULD) включать в свой состав механизмы и параметры для работы с таким трафиком. Например, могла бы существовать возможность установления минимального PMTU для трафика (по каждому месту назначения), предотвращающая установку тривиального размера PMTU при приеме неаутентифицированных сообщений ICMP.

Если сообщение ICMP PMTU проходит указанную выше проверку, и система конфигурируется для его приема, то имеются две возможности. Если реализация применяет фрагментацию на стороне границы с зашифрованным текстом, то принятая информация PMTU передается модулю пересылки (находящемуся за пределами реализации IPsec), который ее использует для управления фрагментацией исходящих пакетов. Если реализация конфигурируется для осуществления фрагментации на стороне открытого текста, то информация PMTU передается стороне с открытым текстом и обрабатывается так, как описано в разделе 8.2.

6.1.2. Сообщения об ошибках ICMP, полученные на защищенной стороне границы

Эти сообщения ICMP не аутентифицируются, но они действительно приходят от источников на защищенной стороне границы IPsec. Таким образом, эти сообщения вообще рассматриваются как более "надежные", чем их двойники, поступающие из источников на незащищенной стороне границы. Здесь главное беспокойство системы безопасности заключается в том, что скомпрометированный хост или маршрутизатор может выпускать ложные сообщения об ошибках ICMP, которые могут деградировать сервис для других устройств, находящихся "за" защитным шлюзом, или которые даже могут приводить к нарушениям конфиденциальности. Например, если защитным шлюзом было потреблено подложное сообщение ICMP redirect, то оно может стать причиной того, что таблица пересылки на защищенной стороне границы будет модифицирована так, чтобы доставлять трафик на неправильное место назначения "за" шлюзом. Таким образом, разработчики реализации должны (MUST) обеспечить средства, позволяющие локальным администраторам ограничивать обработку сообщений ICMP об ошибках, полученных на защищенной стороне границы и направленных реализации IPsec. Эти средства аналогичны средствам, которые применяются на незащищенной стороне и описаны в разделе 6.1.1.

6.2. Обработка защищенных транзитных сообщений ICMP об ошибках

Когда сообщение ICMP об ошибке передается через SA устройству, находящемуся "за" реализацией IPsec, то с точки зрения контроля доступа проверки требуют как блок данных, так и заголовок сообщения ICMP. Если одно из этих сообщений пересылается хосту, находящемуся за защитным шлюзом, то принимающая реализация IP хоста будет принимать решения, базируясь на блоке данных, т.е. заголовке пакета, который по смыслу инициировал ответ об ошибке. Таким

образом, реализация IPsec должна (MUST) иметь возможность конфигурироваться для проверки того, что эта заголовочная информация блока данных является согласованной с SA, через который она поступила. (Это означает, что заголовок блока данных с расположенными в обратном порядке полями адресов источника, места назначения и портов, совпадает с селекторами трафика для SA). Если такого рода проверка не выполняется, то, например, любой абонент, с которым принимающая система IPsec (A) имеет активный SA, может послать сообщение с незаконным (мертвым) местом назначения, которое указывает на любой хост/сеть с которым A в настоящее время осуществляет обмен информацией, и, таким образом, осуществлять весьма эффективную DoS-атаку, затрагивающую обмены информацией с другими партнерами A. Обычной обработки трафика приемником IPsec для защиты от таких атак оказывается не достаточно. Однако такие проверки могут потребоваться не всем контекстам, так что необходимо также разрешить локальному администратору конфигурировать реализацию и не (NOT) выполнять такие проверки.

Чтобы обеспечить обе политики, принимаются следующие соглашения. Если администратор хочет позволить передачу по SA сообщений ICMP об ошибках без инспекции блоков данных, то конфигурировать элемент SPD, который явно позволяет передачу такого трафика. Если администратор хочет, чтобы для обеспечения согласованности реализация IPsec осуществляла проверку блоков данных сообщений ICMP об ошибках, то не создавать никаких элементов SPD, которые осуществляют передачу такого трафика, основываясь на заголовке пакета ICMP. Это соглашение служит причиной следующего описания обработки.

Отправители и приемники IPsec должны (MUST) поддерживать следующую обработку для сообщений ICMP об ошибках, которые посылаются и принимаются через SA.

Если существует SA, который обеспечивает исходящее сообщение ICMP об ошибке, то сообщение отображается на SA и после получения в нем проверяются только заголовки IP и ICMP, также, как это происходит с другим трафиком. Если не существует SA, который совпадает с селекторами трафика, связанными с сообщением ICMP об ошибке, то осуществляется поиск в SPD, чтобы определить, может ли быть создан такой SA. Если так, то создается SA, и сообщение ICMP об ошибке передается через этот SA. После получения это сообщение в приемнике является объектом обычных проверок селекторов трафика. Такая обработка представляет собой в точности то, что произошло бы в общем случае с трафиком, и, таким образом, не представляет собой какой-либо специальной обработки для сообщений ICMP об ошибках.

Если не существует никакого SA, который передавал бы данное исходящее сообщение ICMP, и если ни один элемент SPD не позволяет передавать это исходящее сообщение ICMP об ошибке, то реализация IPsec должна (MUST) отобразить это сообщение на SA, который будет передавать ответный трафик, связанный с пакетом, который инициировал сообщение ICMP об ошибке. Это требует того, чтобы реализация IPsec обнаруживала исходящие сообщения ICMP об ошибках, которые отображаются на несуществующий в настоящее время SA или элемент SPD, и обрабатывать его специально с точки зрения создания SA и осуществления поиска. Реализация извлекает заголовок для пакета, который инициировал ошибку (из блока данных сообщения ICMP), переставляет местами поля IP-адресов источника и места назначения, извлекает поле протокола и переставляет местами поля портов (если они доступны). Затем она использует эту извлеченную информацию для определения местоположения соответствующего активного SA и передает сообщение об ошибке через этот SA. Если такого SA не существует, никаких SA не будет создано, и это представляет собой событие, подлежащее ревизии.

Если реализация IPsec принимает входящее сообщение ICMP об ошибке по какому-либо SA, и заголовки IP и ICMP сообщения не совпадают с селекторами трафика для этого SA, то приемник должен (MUST) обрабатывать принятое сообщение специальным образом. А именно, приемник должен извлечь заголовок инициирующего пакета из блока данных ICMP, поменять местами поля так, как было описано выше, для определения, является ли пакет согласованным с селекторами SA, по которому было получено сообщение ICMP об ошибке. Если эта

проверка пакета заканчивается неудачей, то реализация IPsec не должна (MUST NOT) пересылать это сообщение ICMP на место назначения. Это представляет собой событие, подлежащее ревизии.

7. Обработка фрагментов (на защищенной стороне границы IPsec)

В предыдущих разделах данного документа описываются механизмы для (a) фрагментирования исходящего пакета после применения обработки IPsec и его реассемблирования в приемнике до обработки IPsec, а также для (b) обработки входящих фрагментов, принятых с незащищенной стороны границы IPsec. В данном разделе описывается, как реализация должна выполнять обработку фрагментов исходящего открытого текста на защищенной стороне границы IPsec. (Логическое обоснование обработки фрагментов см. в приложении D). В частности, он затрагивает:

- Отображение исходящего не начального фрагмента на правильный SA (или нахождение правильного элемента SPD)
- Проверку того, что принятый не начальный фрагмент авторизуется для SA, через который он был получен
- Отображение исходящих и входящих не начальных фрагментов на правильный элемент SPD-O/SPD-I или соответствующий элемент кэша для отбрасываемого (BYPASS) или идущего в обход (BYPASS) трафика

Примечание: В разделе 4.1 контексты безопасности (SA) транспортного режима были определены так, чтобы не передавать фрагменты (IPv4 или IPv6). Заметим также, что в разделе 4.4.1 были определены два специальных значения, ANY и OPAQUE, и что ANY включает OPAQUE. Термин "не тривиальный" (non-trivial) используется для обозначения того, что селектор имеет значение, отличное от OPAQUE или ANY.

Примечание: Термин "не начальный фрагмент" (non-initial fragment) используется здесь для указания фрагмента, который не содержит все значения селекторов, которые могут потребоваться для контроля доступа. Как рассматривалось в разделе 4.4.1, в зависимости от протокола следующего уровня (Next Layer Protocol) в дополнение к портам (Ports) в не начальных фрагментах могут отсутствовать тип/код (type/code) сообщения ICMP или тип (type) заголовка мобильности (Mobility Header). Кроме того, для IPv6, в зависимости от вида и числа присутствующих заголовков расширения, даже первый фрагмент может не содержать (NOT) протокол следующего уровня или порты (или тип/код сообщения ICMP или тип заголовка мобильности). Если не начальный фрагмент содержит порт (или тип и код ICMP, или тип заголовка мобильности), но не содержит протокол следующего уровня, то за исключением случая, когда имеется элемент SPD для соответствующих локального/удаленного адресов с значением ANY для протокола следующего уровня и порта (или типа и кода ICMP, или типа заголовка мобильности), фрагмент не будет содержать всю информацию о селекторах, необходимую для контроля доступа.

Чтобы справиться с указанными выше проблемами, здесь были определены три подхода:

- SA туннельного режима, которые передают начальный и не начальные фрагменты (см. раздел 7.1)
- Отдельные SA туннельного режима для не начальных фрагментов (см. раздел 7.2)
- Контекстная (с сохранением состояния) проверка фрагментов (см. раздел 7.3)

7.1. SA туннельного режима, по которым передаются начальные и не начальные фрагменты

Все реализации должны (MUST) поддерживать SA туннельного режима, которые конфигурируются для передачи трафика безотносительно к значениям поля порт (или полей тип/код ICMP, или поля тип заголовка мобильности). Если по SA будет передаваться трафик для специфицированных протоколов, то набор селекторов для SA должен (MUST) определять поля портов (или тип/код ICMP, или тип заголовка мобильности) как имеющих значение ANY. По SA, определенному таким способом, будет передаваться весь трафик, включая начальные и не начальные фрагменты для указанных локального/удаленного адресов и специфицированного протокола (специфицированных протоколов) следующего уровня. Если по SA будет передаваться трафик безотносительно к значению конкретного протокола (т.е. в качестве значения селектора протокола (следующего уровня) специфицировано значение ANY), то значения полей портов не определяются и должны (MUST) также устанавливаться в значение ANY. (Как отмечалось в разделе 4.4.1, значение ANY включает значение OPAQUE, а также все конкретные значения).

7.2. Отдельные SA туннельного режима для не начальных фрагментов

Реализация может (MAY) поддерживать SA туннельного режима, по которым передаются только не начальные фрагменты, отделенные от нефрагментированных пакетов и начальных фрагментов. Для SA, по которому будут передаваться такие фрагменты, для спецификации селекторов поля порта (или типа/кода ICMP, или типа заголовка мобильности) будет использоваться значение OPAQUE. Когда применяются SA этого типа, приемники должны (MUST) выполнять минимальную проверку смещения (не начальных) фрагментов IPv4, чтобы защититься от атак перекрывающихся фрагментов. Поскольку такие проверки не могут выполняться над не начальными фрагментами IPv6, пользователи и администраторы уведомляются о том, что передача таких фрагментов может оказаться опасной, а реализаторы могут принять решение не (NOT) поддерживать такие SA для IPv6-трафика. Кроме того, по SA такого сорта будут передаваться все не начальные фрагменты, которые совпадают со специфицированными парой адресов локальный/удаленный и значением протокола, т.е. фрагменты, передаваемые по этому SA, относятся к пакетам, которые при отсутствии фрагментации могли бы пройти по отдельным SA с различной степенью безопасности. Поэтому пользователям и администраторам дается совет, защищать такой трафик с помощью ESP (с обеспечением целостности) и использовать между обоими партнерами "самые стойкие" алгоритмы обеспечения целостности и шифрования. (Определение "самых стойких" алгоритмов требует наложения упорядочивания доступных алгоритмов, локальное определение оставляется на усмотрение инициатора SA).

Конкретные значения селекторов портов (или типа/кода ICMP, или типа заголовка мобильности) будут использоваться для определения контекстов безопасности (SA) для передачи начальных фрагментов и нефрагментированных пакетов. Такой подход может использоваться, если пользователь или администратор хочет создать один или несколько SA туннельного режима между одними и теми же локальными/удаленными адресами, которые различаются на основе полей портов (или типа/кода ICMP, или типа заголовка мобильности). Эти SA должны (MUST) иметь нетривиальные значения селекторов протоколов, иначе должен (MUST) использоваться указанный выше подход № 1.

Примечание: Вообще говоря, для подхода, описанного в этом разделе, необходим только один SA между двумя реализациями для передачи всех не начальных фрагментов. Однако если делается выбор в пользу нескольких SA между двумя реализациями для установления различий в QoS (качестве обслуживания), то можно захотеть иметь также несколько SA для передачи фрагментов без портов, по одному для каждого поддерживаемого класса QoS. Поскольку поддержка QoS через отдельные SA является локальным вопросом, не определяемым данным документом, решение иметь несколько SA для передачи не начальных фрагментов, также должно быть локальным.

7.3. Контекстная проверка фрагментов

Реализация может (MAY) поддерживать некоторую форму контекстной проверки фрагментов для SA туннельного режима с нетривиальными значениями полей портов

(или типа/кода ICMP, или типа заголовка мобильности) (не ANY и не OPAQUE). Реализации, которые будут передавать не начальные фрагменты по SA туннельного режима, который использует нетривиальные селекторы портов (или типа/кода ICMP, или типа заголовка мобильности) должны (MUST) уведомлять об этом партнера с помощью блока данных IKE NOTIFY NON_FIRST_FRAGMENTS_ALSO.

Партнер должен (MUST) отвергнуть это предложение, если он не будет принимать не начальные фрагменты в этом контексте. Если реализация не согласовала успешно передачу не начальных фрагментов для такого SA, она не должна (MUST NOT) посылать такие фрагменты через этот SA. Данный стандарт не специфицирует, как партнеры будут иметь дело с такими фрагментами, например, с помощью реассемблирования или других средств, как на стороне отправителя, так и на стороне приемника. Однако приемник должен (MUST) отбрасывать не начальные фрагменты, которые поступают по некоторому SA с нетривиальными значениями селекторов портов (или типа/кода ICMP, или типа заголовка мобильности), за исключением случая, когда такая функция была согласована. Кроме того, приемник должен (MUST) отбрасывать не начальные фрагменты, которые не согласуются с политикой безопасности, применяемой ко всему пакету. Отбрасывание таких пакетов является проверяемым событием. Заметим, что в сетевых конфигурациях, в которых фрагменты пакета могут посылаться или приниматься через различные защитные шлюзы или через реализации BITW, использовать контекстные стратегии для отслеживания фрагментов может не удаться.

7.4. Трафик, пускаемый в обход / отбрасываемый трафик

Все реализации должны (MUST) поддерживать отбрасывание (DISCARDing) фрагментов, используя обычные механизмы классификации пакетов по SPD. Все реализации должны (MUST) поддерживать контекстную (с сохранением состояния) проверку фрагментов, чтобы обеспечить пропускание в обход (BYPASS)трафика, для которого определяется нетривиальный диапазон портов. Беспокойство заключается в том, что пропускание в обход (BYPASS) не начальных фрагментов открытого текста, поступающих в реализацию IPsec, может подорвать безопасность, предоставляемую защищенному IPsec трафику, направляемому на то же самое место назначения. Например, рассмотрим реализацию IPsec, сконфигурированную с элементом SPD, который требует IPsec-защиты трафика между конкретной парой адресов источника/места назначения, а также для конкретного протокола и порта назначения, например, TCP-трафик на порт 23 (Telnet). Предположим, что эта реализация позволяет также пускать в обход (BYPASS) трафик с теми же самыми адресной парой и протоколом, но для другого порта назначения, например, для порта 119 (NNTP). Злоумышленник может послать не начальный фрагмент (с подделанным адресом источника), который, в случае его пропускания в обход, может перекрыться (наложиться) с IPsec-защищенным трафиком из того же самого источника и тем самым нарушить целостность IPsec-защищенного трафика. Требование контекстной проверки фрагментов для элементов BYPASS с нетривиальными диапазонами портов предотвращает атаки такого сорта.

8. Обработка Path MTU/DF

Применение AH или ESP к исходящему пакету увеличивает размер пакета и, таким образом, может вызвать превышение пакетом PMTU для того SA, через который пакет будет отправлен. Реализация IPsec может также получить незащищенное сообщение ICMP PMTU и, если она примет решение действовать в соответствии с ним, результат будет влиять на обработку исходящего трафика. В данном разделе описывается обработка, требуемая от реализации IPsec, чтобы решить эти две проблемы PMTU.

8.1. Бит DF

Все реализации IPsec должны (MUST) поддерживать опцию копирования бита DF из исходящего пакета в заголовок туннельного режима, который они порождают, когда трафик передается через SA туннельного режима. Это означает, что должна

(MUST) существовать возможность конфигурирования реализационной обработки для каждого SA (установить, сбросить, копировать из внутреннего заголовка).

8.2. Определение Path MTU (PMTU)

В данном разделе обсуждается обработка IPsec для незащищенных сообщений определения Path MTU. Здесь обозначение ICMP PMTU используется для указания сообщений ICMP, предназначенных для:

IPv4 (RFC 792 [Pos81b]):
- Type = 3 (Destination Unreachable – Место назначения недостижимо)
- Code = 4 (Fragmentation needed and DF set – Требуется фрагментация и установлен флаг DF)
- MTU следующего интервала (Next-Hop MTU) в младших 16 битах второго слова заголовка ICMP (помеченных как неиспользуемые ("unused") в RFC 792) при старших 16 битах установленных в ноль)

IPv6 (RFC 2463 [CD98]):
- Type = 2 (Packet Too Big – Пакет слишком велик)
- Code = 0 (Fragmentation needed –Требуется фрагментация)
- MTU следующего интервала (Next-Hop MTU) в 32 битах поля MTU Сообщения ICMPv6

8.2.1. Распространение PMTU

Когда реализация IPsec получает неаутентифицированное сообщение PMTU и она сконфигурирована для обработки (в отличие от игнорирования) таких сообщений, она отображает это сообщение на SA, которому оно соответствует. Это отображение осуществляется путем извлечения заголовочной информации из блока данных сообщения PMTU и применения процедуры, описанной в разделе 5.2. PMTU, определяемый этим сообщением, используется для обновления поля PMTU в SAD, учитывая размер заголовка AH или ESP, который будет применяться, криптографические синхронизационные данные и накладные расходы, определяемые дополнительным IP-заголовком в случае SA туннельного режима.

В естественной реализации хоста возможно поддерживать данные PMTU с той же степенью детализации, что и для незащищенных обменов информацией, так что потеря функциональности отсутствует. Передача информации о PMTU является внутренней для хоста. Для всех других возможных реализаций IPsec данные PMTU должны распространяться с помощью синхронизованного ICMP PMTU. В этих случаях реализация IPsec должна (SHOULD) дождаться исходящего трафика, который должен отображаться на элемент SAD. Когда такой трафик поступает, в случае если трафик превысит обновленное значение PMTU, такой трафик должен обрабатываться следующим образом:

Случай 1: Первоначальный пакет (открытого текста) является пакетом IPv4 и имеет установленный бит DF. Реализация должна (SHOULD) отбросить этот пакет и послать сообщение PMTU ICMP.

Случай 2: Первоначальный пакет (открытого текста) является пакетом IPv4 и имеет сброшенный бит DF. Реализация должна (SHOULD) фрагментировать пакет (до или после шифрования в соответствии со своей конфигурацией) и затем пересылать фрагменты. Она не должна (SHOULD NOT) посылать сообщения PMTU ICMP.

Случай 3: Первоначальный пакет (открытого текста) является пакетом IPv6. Реализация должна (SHOULD) отбросить этот пакет и послать сообщение PMTU ICMP.

8.2.2. Старение PMTU

Во всех реализациях IPsec PMTU, связанный с некоторым SA, должен (MUST) «стареть» и требуется некоторый механизм периодического обновления PMTU,

главным образом для определения того, не является ли PMTU меньшим, чем требуется текущим состоянием сети. Заданный PMTU должен оставаться без изменений достаточно долго так, чтобы пакет дошел от источника SA к партнеру, и чтобы удалось распространить сообщение об ошибке ICMP в случае, если текущее значение PMTU слишком велико.

Реализации должны (SHOULD) использовать подход, описанный в документе Path MTU Discovery (RFC 1191 [MD90], Section 6.3), который советует периодически переустанавливать PMTU в значение канального MTU первого интервала и затем дает возможность обычным процессам определения PMTU обновлять PMTU по мере необходимости. Этот период должен быть (SHOULD) конфигурируемым.

9. Выполнение ревизии

От реализаций IPsec не требуется поддержка проведения ревизий. В целом, степень детализации проведения ревизий является локальным вопросом. Однако несколько событий, подлежащих ревизии, определены в данном документе, и для каждого такого события определен минимальный набор информации, который должен (SHOULD) включаться в ревизионный журнал. Требование передачи приемником какого-либо сообщения подразумеваемому передатчику в ответ на обнаружение подлежащего ревизии события отсутствует из-за потенциальной возможности вызвать отказ в обслуживании посредством подобного действия.

10. Требования соответствия

Все реализации IPv4 должны (MUST) выполнять все требования данного документа. Все реализации IPv6 должны (MUST) выполнять все требования данного документа.

11. Анализ безопасности

Безопасность является главным предметом данного документа; поэтому анализ безопасности пронизывает данную спецификацию.

Если реализация IPsec конфигурируется для передачи ICMP-сообщений об ошибках через контексты безопасности (SA), базируясь на значениях заголовка ICMP без проверки заголовочной информации из блока данных сообщения ICMP, то могут возникнуть серьезные уязвимости. Рассмотрим сценарий, в котором несколько сайтов (A, B, и C) соединены друг с другом через защищенные ESP туннели: A-B, A-C и B-C. Предположим также, что селекторы трафика для каждого туннеля определяют значение ANY для полей протоколов и портов, а также диапазоны IP-адресов источников/мест назначения, которые охватывают диапазон адресов для систем, находящихся за защитными шлюзами, обслуживающими каждый сайт. Это позволит хосту на сайте B послать сообщение ICMP destination dead любому хосту на сайте A, которое объявляет все хосты в сети на сайте C недостижимыми. Это очень эффективная DoS-атака, которую удалось бы избежать, если бы ICMP-сообщения об ошибках подвергались проверке того, что обеспечивает IPsec в случае соответствующего конфигурирования SPD, как описано в разделе 6.2.

12. Соображения для IANA

Данный документ не содержит действий для IANA.

13. Отличия от RFC 2401

Данный документ по архитектуре существенно отличается от RFC 2401 в деталях и по организации, но фундаментальные понятия остались неизмененными.

- Была подвергнута ревизии модель обработки, чтобы охватить новые сценарии, улучшить работу и упростить реализацию. Это включает разделение между выбором пересылки (маршрутизации) и SPD, несколько изменений в SPD, а также добавление выходного кэша SPD и входного кэша SPD для трафика идущего в обход и отбрасываемого трафика. Кроме того, имеется новая база данных авторизации партнеров (PAD - Peer

Authorization Database). Она обеспечивает связь между протоколом управления SA, типа IKE, и SPD.

- Больше не выдвигается требование поддержки вложенных SA или «связок SA». Вместо этого данная функциональность может быть достигнута путем конфигурирования SPD и таблицы маршрутизации. Пример конфигурирования добавлен в Приложение E.

- Элементы SPD были переопределены для обеспечения большей гибкости. Каждый элемент SPD теперь включает от 1 до N наборов селекторов, где каждый набор селекторов включает один протокол, а «список диапазонов» теперь может определяться для локального IP-адреса, удаленного IP-адреса, и любые поля (если таковые имеются) связываются с протоколом следующего уровня (локальный порт, удаленный порт, тип и код ICMP-сообщения и тип заголовка мобильности). Индивидуальное значение селектора представляется с помощью тривиального диапазона, а значение ANY представляется с помощью диапазона, который покрывает все значения селектора. Пример описания на языке ASN.1 включен в Приложение C.

- Поля TOS (IPv4) и Traffic Class (IPv6) заменены на DSCP и ECN. Раздел, касающийся туннелей, был обновлен, чтобы объяснить, как обрабатывать биты DSCP и ECN.

- Для SA туннельного режима реализации SG, BITS, или BITW теперь позволено фрагментировать пакеты до применения IPsec. Это применяется только к IPv4. Для пакетов IPv6 только первоисточнику позволено их фрагментировать.

- Если желательна безопасность между двумя промежуточными системами, находящимися на пути пакетов, или между промежуточной системой и оконечной системой, то теперь между защитными шлюзами и между защитным шлюзом и хостом может использоваться транспортный режим.

- Данный документ разъясняет, что для всего трафика, который пересекает границу IPsec, включая трафик управления IPsec, необходимо консультироваться с SPD или связанными с ней кэшами.

- Данный документ определяет, как работать в случае защитного шлюза с несколькими абонентами, требующими отдельных контекстов IPsec.

- Добавлено определение зарезервированных SPI.

- Добавлен текст, разъясняющий, почему должны проверяться ВСЕ IP-пакеты – IPsec включает минимальную функциональность межсетевого экрана для поддержки контроля доступа на уровне IP.

- Обновлен раздел, касающийся туннелей, для разъяснения того, как обрабатывать поле IP options и заголовки расширения IPv6 при создании внешнего заголовка.

- Обновлено отображение SA для входящего трафика, чтобы оно было согласовано с изменениями, сделанными в AH и ESP для поддержки контекстов безопасности (SA) типа unicast, anycast и multicast.

- Добавлено руководство, касающееся того, как работать со скрытым каналом, созданным в туннельном режиме путем копирования значения DSCP во внешний заголовок.

- Поддержка AH как в IPv4, так и в IPv6 больше не требуется.

- Обновлена обработка PMTU. Ликвидировано приложение, касавшееся PMTU/DF/Fragmentation.

- Добавлен текст, говорящий «Дальнейшим источником руководящих материалов является рабочая группа IPSP (IP Security Policy). Одной из ее задач является создание чернового проекта (Internet Draft) протокола определения защитных шлюзов, обмена политиками и согласования ("Security Gateway Discovery, Policy Exchange and Negotiation Protocol)".

- Добавлены три подхода к обработке фрагментов открытого текста на защищенной стороне границы IPsec. В приложении D представлено их логическое обоснование.

- Добавлен исправленный текст, описывающий, как получить значения селекторов (из элемента SPD или из пакета, и т.д.)

- Добавлена новая таблица, описывающая взаимосвязь между значениями селекторов в элементе SPD, флагом PFP и результирующими значениями селекторов в соответствующем элементе SAD.

- Добавлено Приложение B, описывающее декорреляцию.

- Добавлен текст, описывающий как обрабатывать исходящий пакет, который должен быть отброшен.

- Добавлен текст, описывающий как обрабатывать входящий отбрасываемый пакет, т.е. пакет, который не соответствует SA, по которому он поступил.

- Добавлен заголовок мобильности IPV6 в качестве возможного протокола следующего уровня. Добавлен тип сообщения заголовка мобильности IPv6 в качестве селектора.

- Добавлены тип и код сообщения ICMP в качестве селекторов.

- Для упрощения ликвидирован селектор типа "data sensitivity level".

- Обновлен текст, описывающий обработку ICMP-сообщений об ошибках. Ликвидировано Приложение по категоризации ICMP-сообщений.

- Обновлен и разъяснен текст, касающийся имен селекторов.

- Более подробно объяснено понятие протокола следующего уровня и добавлен список подразумеваемых протоколов, которые нужно пропустить при поиске протокола следующего уровня.

- Поправлен текст, чтобы сказать, что данный документ предполагает использование IKEv2 или протокола управления SA со сравнимыми свойствами.

- Добавлен текст, разъясняющий алгоритм отображения входных IPsec-дейтаграмм на контексты безопасности (SA) при наличии SA типа multicast.

- Ликвидировано приложение "Sequence Space Window Code Example".

- Для правил политики по отношению к IP-адресам и портам используются термины «локальный» (Local) и «удаленный» (Remote) (заменяя источник и место назначения). Термин «локальный» указывает на объект, подлежащий защите реализацией IPsec, т.е. адрес/порт «источника» исходящих пакетов или адрес/порт «места назначения» входящих пакетов. Термин «удаленный» указывает на объект партнера или объекты партнера. Термины «источник» и «место назначения» все еще используются для полей заголовков пакетов.