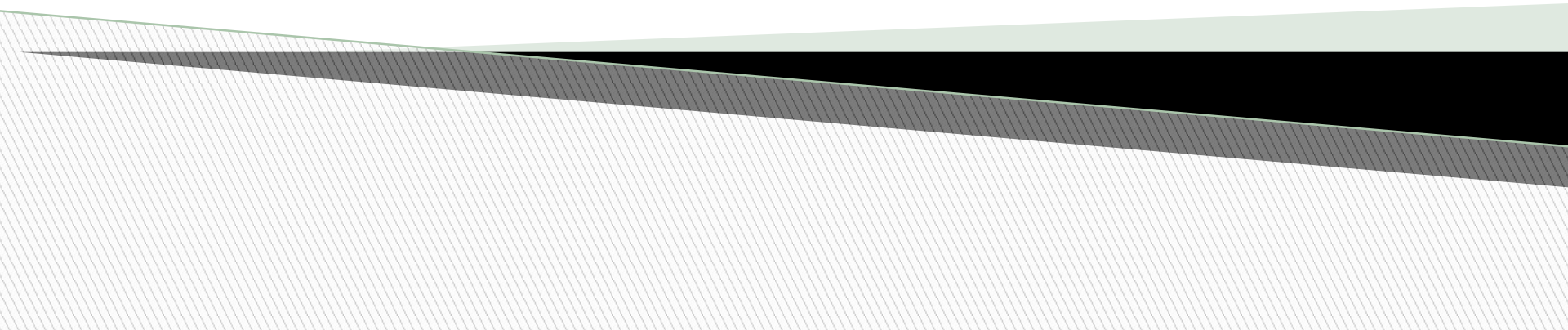


Аппаратное и программное обеспечение ЭВМ и сетей

Тема 6-37 *Сетевая безопасность. Сетевые экраны.
Прокси-серверы . Протоколы защищенного канала.
IPsec . Сети VPN на основе шифрования*



Сетевые экраны

Сетевой (межсетевой) экран — это комплекс программно-аппаратных средств, осуществляющий информационную защиту одной части компьютерной сети от другой путем анализа проходящего между ними трафика.

- Для сетевого экрана одна часть сети является внутренней, другая — внешней (рис. 6.44-1).
- Сетевой экран защищает внутреннюю сеть (например, локальную сеть предприятия или отдельный компьютер пользователя) от угроз, исходящих из внешней сети.

Брандмауэр — Изначально он обозначало перегородку в поезде, отделяющую область топки паровоза от пассажирского отделения.

Файервол (англ. - firewall) - противопожарная перегородка; хотя официально не принято, но применяется достаточно часто

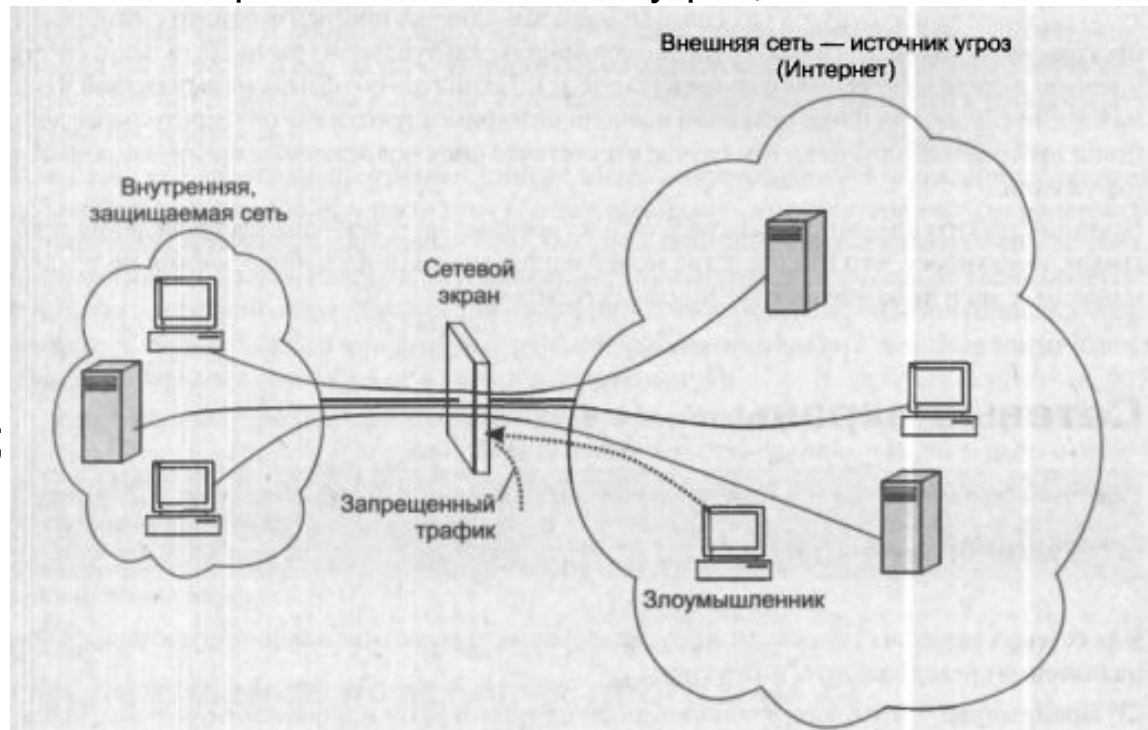


Рис. 6.44-1. Сетевой экран защищает внутреннюю сеть от угроз, исходящих из внешней сети

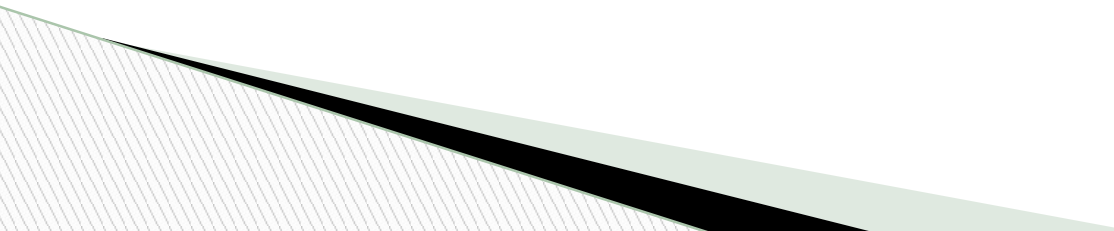
Сетевые экраны

▣ **Функции сетевого экрана:**

▣ *Базовые:*

- ▣ функция фильтрации — анализировать, контролировать и регулировать трафик;
- ▣ функция прокси-сервера — играть роль логического посредника между внутренними клиентами и внешними серверами;
- ▣ функция аудита — фиксировать все события, связанные с безопасностью.

▣ *Вспомогательные:*

- ▣ антивирусная защита;
 - ▣ шифрование трафика;
 - ▣ фильтрация сообщений по содержимому;
 - ▣ обнаружение сетевых атак;
 - ▣ функции VPN;
 - ▣ трансляция сетевых адресов.
- 

Сетевые экраны

Типы сетевых экранов (на основании уровней OSI)

- Сетевые экраны **сетевого уровня** — это экраны с фильтрацией пакетов (packet filtering firewall). Они фильтруют пакеты по IP-адресам и портам приложений на основании списков доступа — *простая фильтрация (stateless packet inspection)*.
- Сетевые экраны **сеансового уровня** отслеживают **состояние соединений**. Они фиксируют подозрительную активность, направленную на сканирование портов и сбор информации о сети и проверяют, **соответствует ли последовательность обмена сообщениями контролируемому протоколу** — *фильтрация с учетом контекста (statefull packet inspection)*. брандмауэры **сеансового** уровня могут защищать серверы внутренней сети от различных видов атак, использующих уязвимости протоколов, в частности от DoS-атак.
- Сетевые экраны **прикладного уровня** контролируют содержимое сообщений, которыми обмениваются приложения. К этому уровню относят прокси-серверы. Прокси-сервер перехватывает запросы клиентов к внешним серверам с тем, чтобы потом отправить их от своего имени. Этот тип сетевых экранов обеспечивает самый высокий уровень защиты.

Сетевые экраны

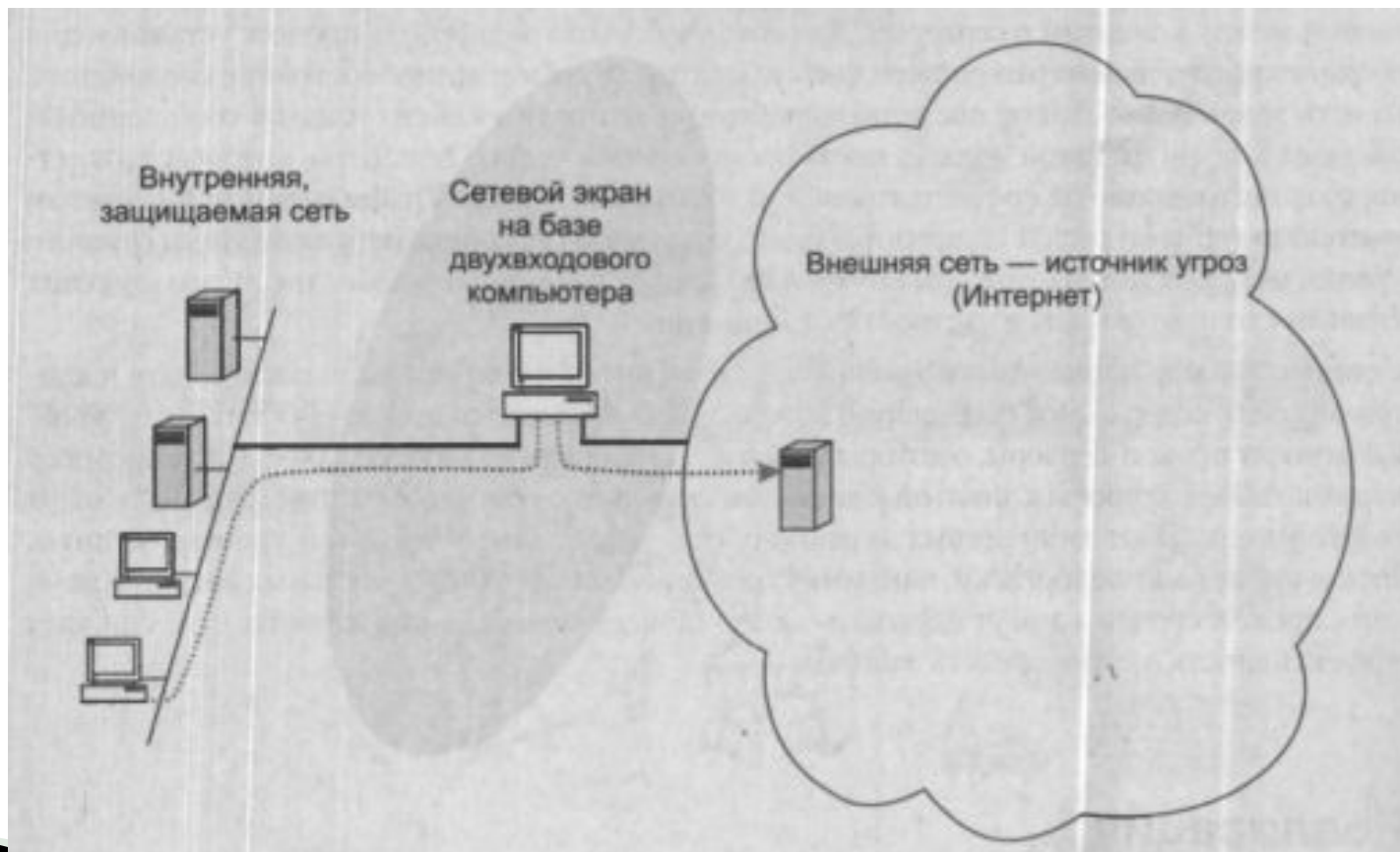
Реализация

- В качестве аппаратной составляющей сетевого экрана может выступать 1 или несколько маршрутизаторов, компьютеров, комбинация маршрутизаторов и компьютеров или специализированное устройство. Разнообразна и программная составляющая, имеющая гибкую структуру и включающая в себя различные модули.
- Только в случае качественной настройки аппаратуры и программных модулей сетевой экран может стать краеугольным камнем системы защиты сети предприятия.

Сетевые экраны

Архитектура

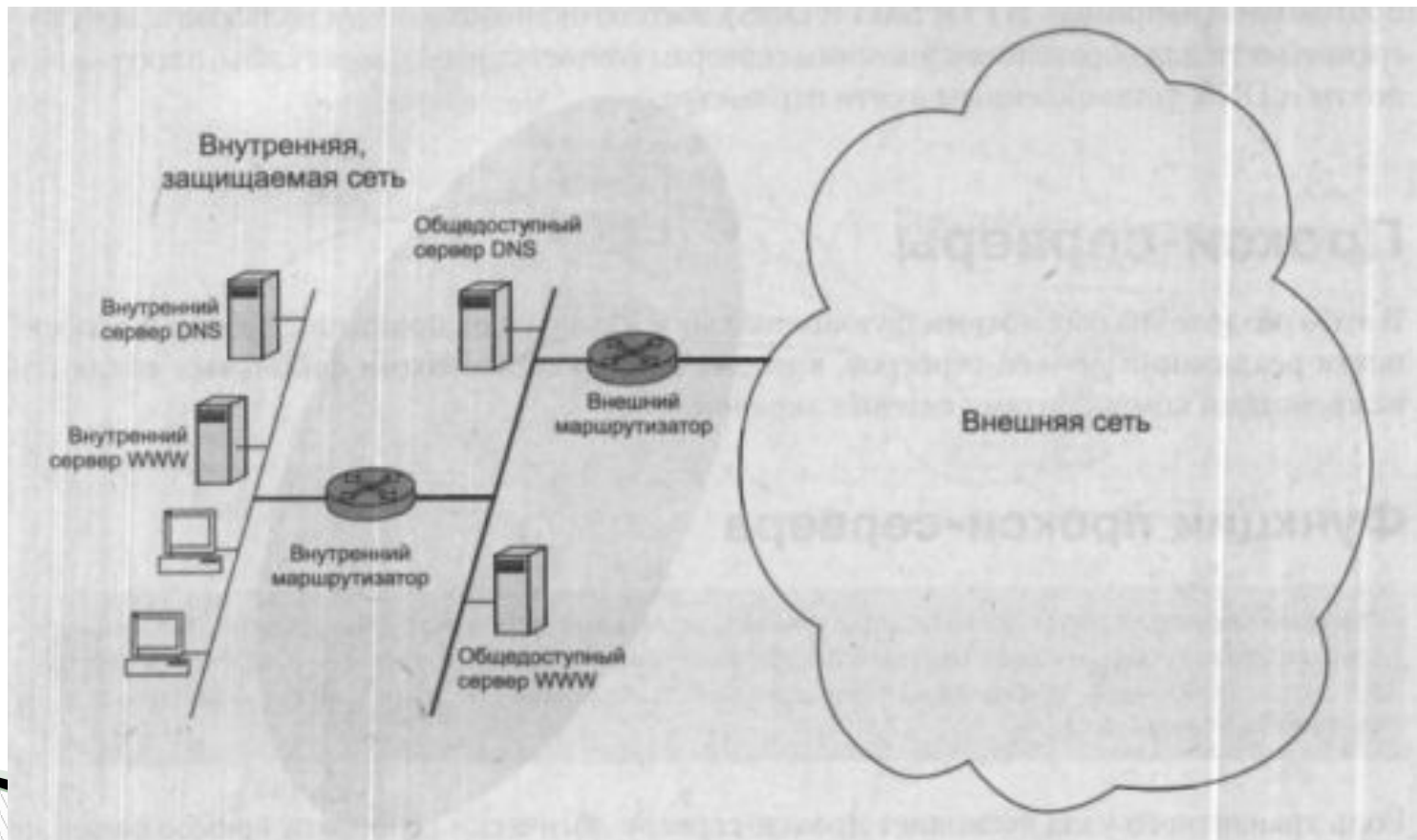
- Простейшая архитектура сети с сетевым экраном: все функции сетевого экрана реализуются одним программно-аппаратным устройством (маршрутизатором, компьютером — рис. 6.44-3). Ее недостаток — полная зависимость системы защиты от работоспособности одного звена.



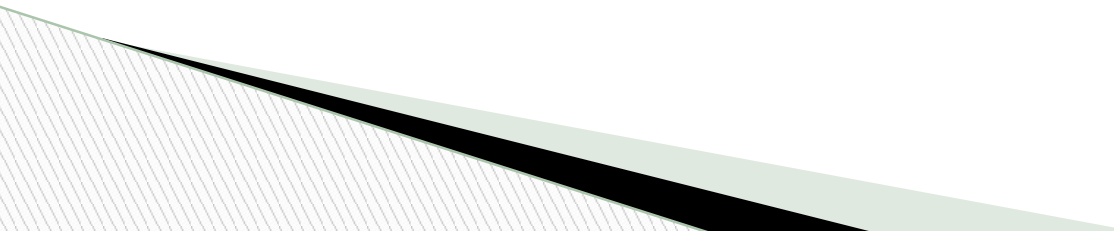
- Рис. 6.44-3. Сетевой экран на базе двухходового компьютера

Сетевые экраны

- Более надежные схемы сетевых экранов включают несколько элементов. В сети, показанной на рис. 6.44-4, между внутренней и внешней сетями размещают сеть периметра, или сеть демилитаризованной зоны (DMZ).
- В ней обычно располагаются компьютеры, предоставляющие общедоступные сервисы (почтовый сервер, внешний сервер DNS и др.) и прокси-серверы.



Сетевые экраны

- Если злоумышленник «взламывает» внешний, то он получит доступ только к трафику общедоступных серверов, который не является секретным.
 - Основная работа по обеспечению безопасности сети возлагается на внутренний маршрутизатор, который должен отбрасывать все пакеты, следующие во внутреннюю сеть из сети периметра, исключая пакеты нескольких протоколов (например, HTTP, SMTP, DNS).
- 

Прокси-серверы

- **Прокси-сервер** — это особый тип приложения, выполняющий функции посредника между **клиентскими и серверными частями** распределенных сетевых приложений.
- Роль транзитного узла позволяет ему логически разорвать соединение между клиентом и сервером с целью контроля сообщений.
- Прокси-сервер может быть установлен на платформе, где работают все остальные модули сетевого экрана (рис. 6.44-5, а), либо на другом узле внутренней сети или сети периметра (рис. 6.44-5, б).

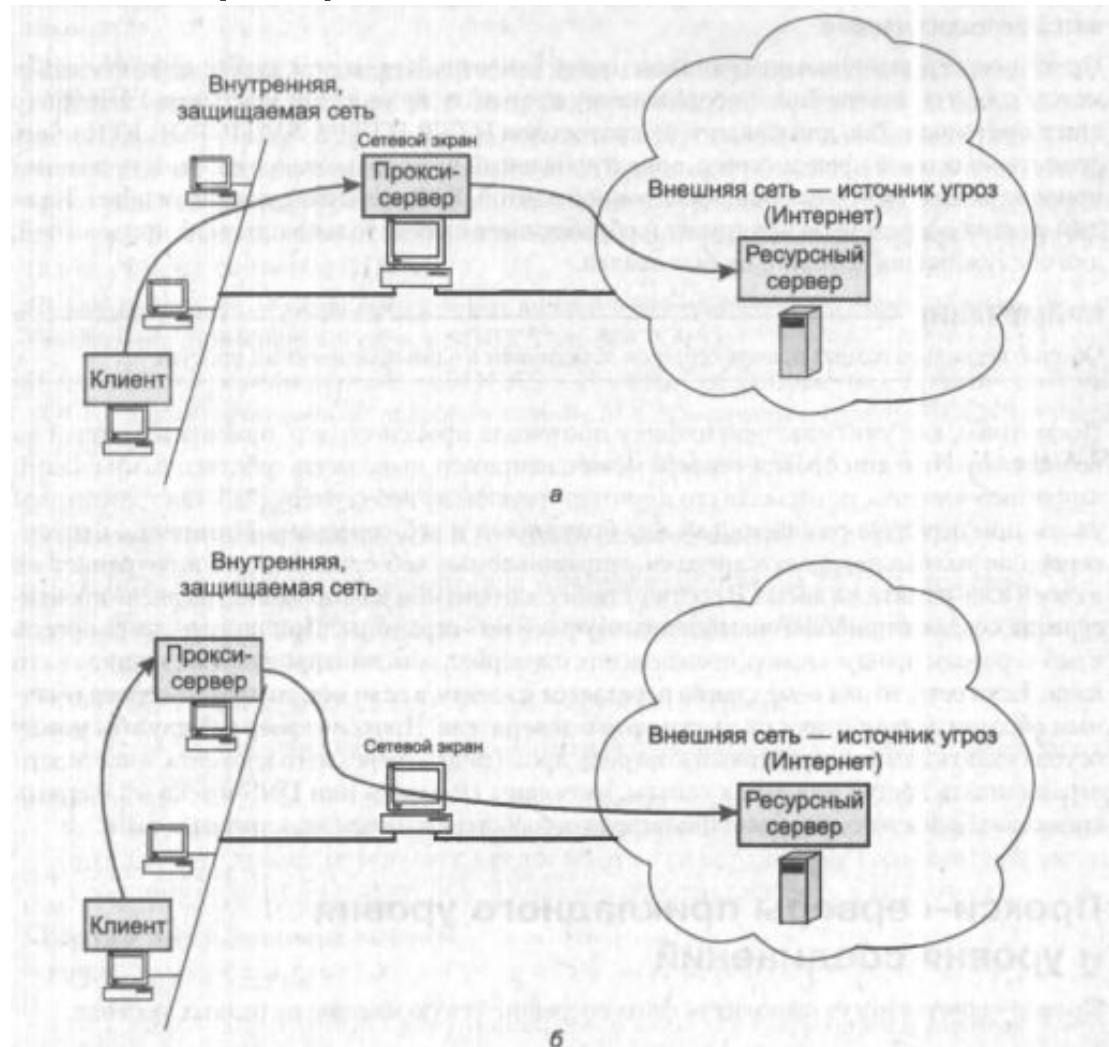


Рис. 6.44-5. Варианты расположения прокси-серверов : а — на сетевом экране, б — на узле внутренней сети

Прокси-серверы

□ **Принцип работы прокси-сервера:**

- 1) Когда клиенту необходимо получить ресурс от какого-либо сервера, он посылает запрос прокси-серверу.
- 2) Прокси-сервер анализирует запрос и решает: он должен быть отброшен, передан без изменения серверу либо модифицирован перед передачей.
- 3) Если запрос удовлетворяет условиям прохождения во внешнюю сеть, прокси-сервер выполняет соединение с сервером от своего имени.
- Для каждого из протоколов HTTP, HTTPS, SMTP/POP, FTP, telnet существует особый прокси-сервер, ориентированный на использование соответствующими приложениями.
- Обычно несколько разных прокси-серверов объединяют в один программный продукт.

□ **Типы прокси-серверов:**

- ***Прокси-сервер прикладного уровня*** «вклинивается» во взаимодействие клиента и сервера по одному из прикладных протоколов.
- ***Прокси-сервер уровня соединений*** контролирует TCP-соединение, работая на транспортном уровне, Например прокси-сервер может изменять запрос клиента, используя функцию трансляции сетевых адресов, он может подменять в пакете запроса IP-адреса и/или номера TCP- и UDP-портов отправителя.

Прокси-серверы

«Проксификация» приложений

- Не каждое приложение должно или имеет возможность работать через прокси-сервер.
- Список приложений (точнее их клиентских частей) определяется администратором.
- Приложения должны быть оснащены средствами, позволяющими перенаправить запросы к внешним серверам на соответствующий прокси-сервер.
- Задача администраторов — приобретение таких приложений и их конфигурирование. В частности, нужно сообщить клиенту адрес узла сети с установленным прокси-сервером и номер порта.
- Еще один подход — встраивание поддержки прокси-сервера в операционную систему.
- Прокси-сервер перехватывает запросы клиентов к внешним серверам с тем, чтобы потом отправить их от своего имени. Этот тип сетевых экранов обеспечивает самый высокий уровень защиты

Системы обнаружения вторжений

Система обнаружения вторжений (Intrusion Detection System , IDS) — это программное или аппаратное средство , предназначенное для предупреждения, выявления и протоколирования некоторых типов сетевых атак.

- Система обнаружения вторжений используется в ситуациях, когда сетевой экран оказывается проницаемым для злоумышленника (атака идет из взломанной сети, попытка легального пользователя скопировать файл с паролями и т.д.), может обнаружить только система со встроенными агентами во многих точках сети, следящая за трафиком и за обращениями к критически важным ресурсам и имеющая информацию о перечне подозрительных действий (сигнатур атак) пользователей. Она не дублирует действия межсетевого экрана, а дополняет их, производя, кроме того, автоматический анализ всех журналов событий, имеющихся у сетевых устройств и средств защиты, чтобы попытаться найти следы атаки, если ее не удалось зафиксировать в реальном времени.

Протоколы защищенного канала. IPsec

- Технология защищенного канала обеспечивает защиту трафика между двумя точками в открытой транспортной сети (например, в Интернете).

- Функции защищенного канала:
 - взаимная аутентификация абонентов;
 - защита сообщений от несанкционированного доступа;
 - подтверждение целостности сообщений.

- В зависимости от места расположения программного обеспечения защищенного канала различают две схемы его образования:
 - ❖ защищенный канал организован полностью между конечными узлами (рис. 6.44-б, а);
 - ❖ схема с оборудованием поставщика услуг, расположенным между частной и публичной сетями (рис. 6.44-б, б).

Протоколы защищенного канала. IPsec

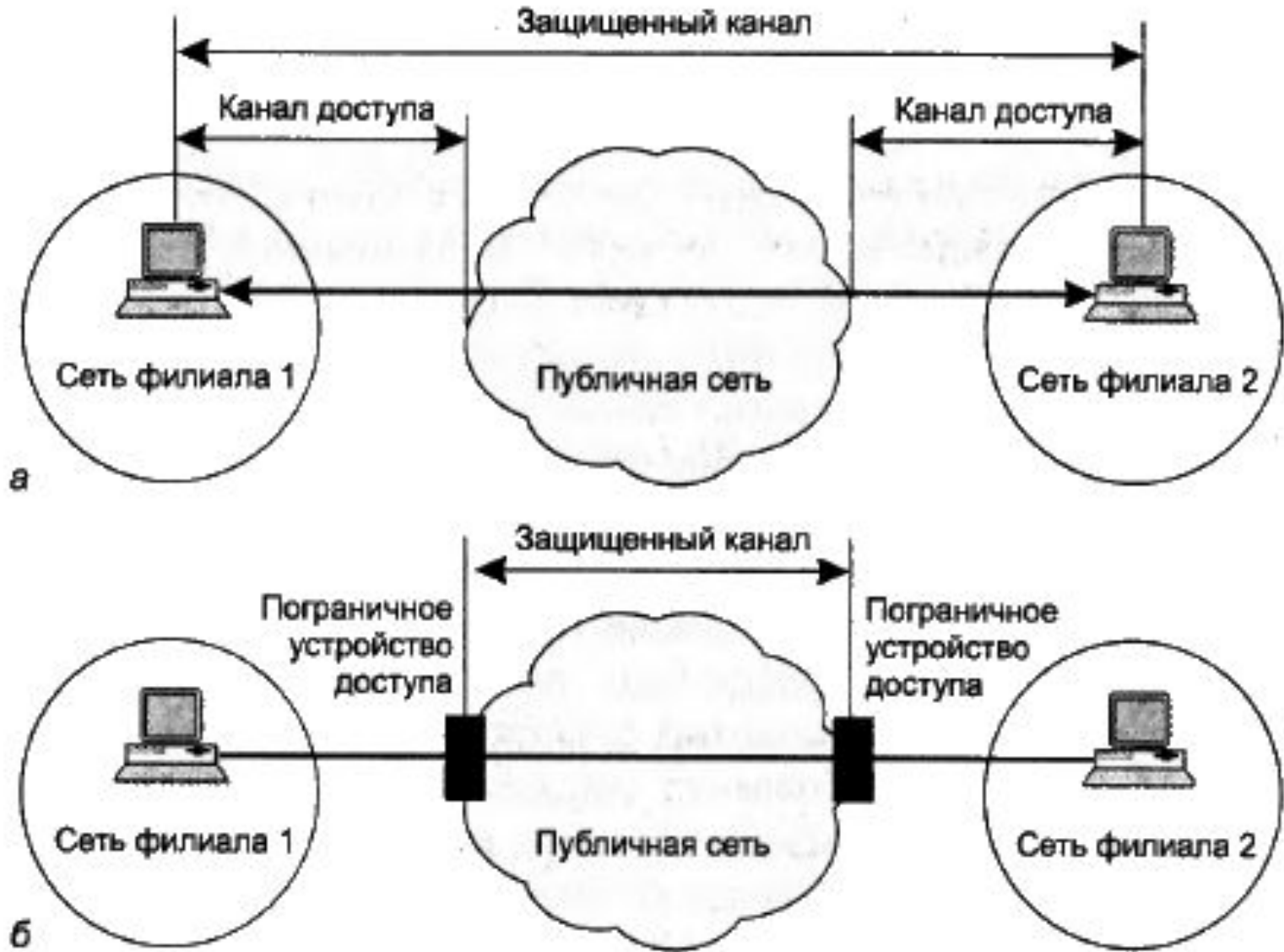


Рис. 6.44-б. Два подхода к образованию защищенного канала

Протоколы защищенного канала. IPsec

Иерархия технологий защищенного канала

- Защищенный канал можно построить с помощью системных средств, реализованных на разных уровнях модели OSI (рис. 6.44-7).

Прикладной	HTTP/S, S/MIME	Непрозрачны для приложений, не зависят от транспортной инфраструктуры
Презентационный	SSL	
Сеансовый		
Транспортный		
Сетевой	IPSec, SKIP	Прозрачны для приложений, зависят от транспортной инфраструктуры
Канальный	PPTP	
Физический		

- Рис. 6.44-7. Протоколы, формирующие защищенный канал на разных уровнях модели OSI

Протоколы защищенного канала. IPsec

- ▣ Популярный протокол SSL (Secure Socket Layer — слой защищенных сокетов) использует следующие технологии безопасности:
 - взаимная аутентификация приложений путем обмена сертификатами (стандарт X.509);
 - контроль целостности данных с использованием дайджестов;
 - секретность путем симметричной шифрации.

Протоколы защищенного канала. IPsec

- ▣ Протокол IPsec прозрачен для приложений и может работать практически во всех сетях, так как использует любую технологию канального уровня (PPP, Ethernet, ATM и т. д.).

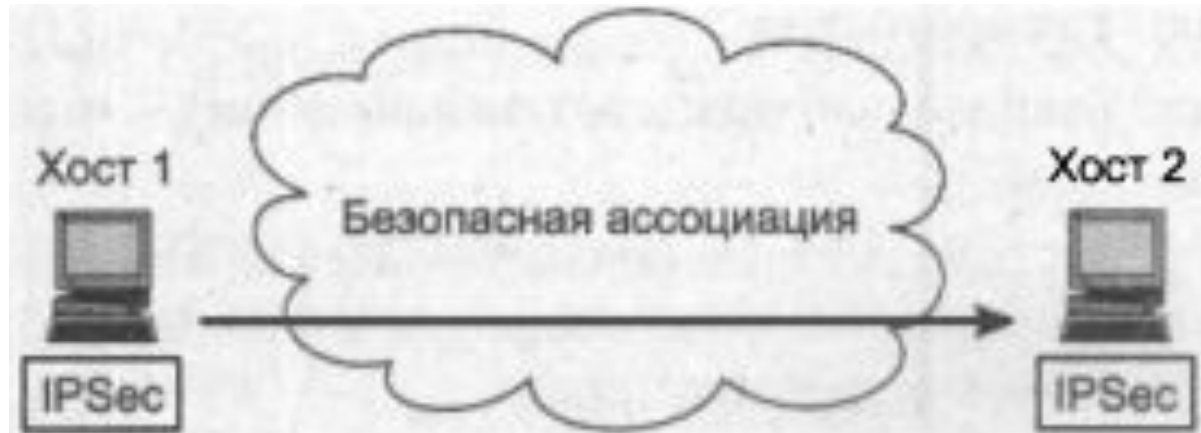
- ▣ Ядро IPsec составляют три протокола:
 - **AH** (Authentication Header — заголовок аутентификации) — гарантирует целостность и аутентичность данных;
 - **ESP** (Encapsulating Security Payload — инкапсуляция зашифрованных данных) — шифрует передаваемые данные;
 - **IKE** (Internet Key Exchange — обмен ключами Интернета) — решает задачу автоматического предоставления конечным точкам секретных ключей.

- Каждый из этих протоколов может использоваться как самостоятельно, так и одновременно с другим.

Протоколы защищенного канала. IPsec

Безопасная ассоциация

- Чтобы протоколы AH и ESP могли выполнять работу по защите данных, протокол IKE устанавливает между двумя конечными точками логическое соединение (рис. 6.44-9), которое в стандартах IPsec носит название безопасной ассоциации (Security Association, SA).



□ Рис. 6.44-9. Безопасная ассоциация

- SA представляет собой однонаправленное (симплексное) логическое соединение. Если требуется обеспечить двусторонний обмен, необходимо установить две безопасные ассоциации.

Протоколы защищенного канала. IPsec

□ Установление безопасной ассоциации:

- 1) Взаимная аутентификация сторон.
- 2) Определение протокола (AH или ESP) и его функций (например, только аутентификацию, обеспечивать конфиденциальность).

□ Способы установления безопасной ассоциации:

- **Ручной способ** — администратор конфигурирует конечные узлы так, чтобы они поддерживали согласованные параметры ассоциации.
- **Автоматическая процедура** — протоколы IKE, работающие по разные стороны канала, выбирают параметры в ходе переговорного процесса.

□ Протоколы AH и ESP могут защищать данные в двух режимах:

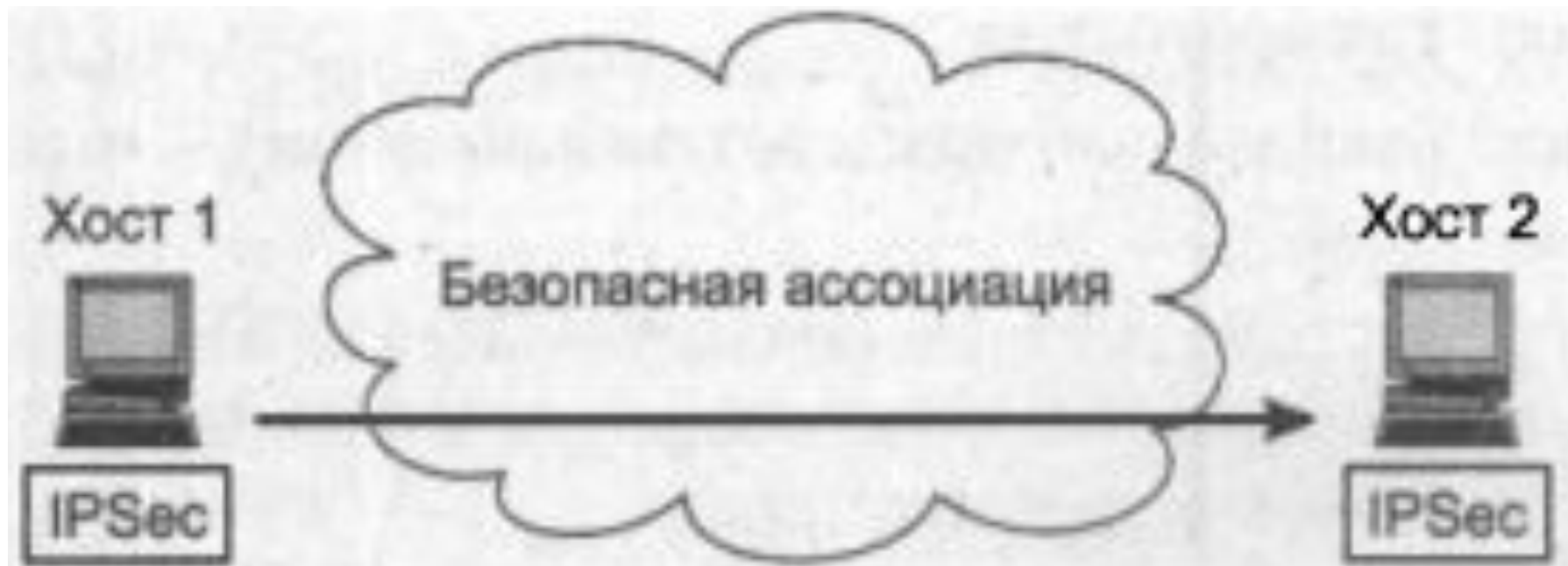
- В *транспортном* — передача IP-пакета выполняется с помощью его оригинального заголовка.
- В *туннельном* — исходный пакет помещается в новый IP-пакет, и передача данных выполняется на основании заголовка нового IP-пакета.

□ Схемы применения протокола IPSec:

- хост-хост;
- шлюз-шлюз;
- хост-шлюз

Протоколы защищенного канала. IPsec

- ▣ **В схеме хост-хост** безопасная ассоциация устанавливается между двумя конечными узлами сети (см. рис. 6.44-9).



- ▣ Рис. 6.44-9. Безопасная ассоциация хост-хост

▣

Протоколы защищенного канала. IPsec

- В схеме **шлюз-шлюз** защищенный канал устанавливается между двумя промежуточными узлами, так называемыми шлюзами безопасности (рис. 6.44-11).

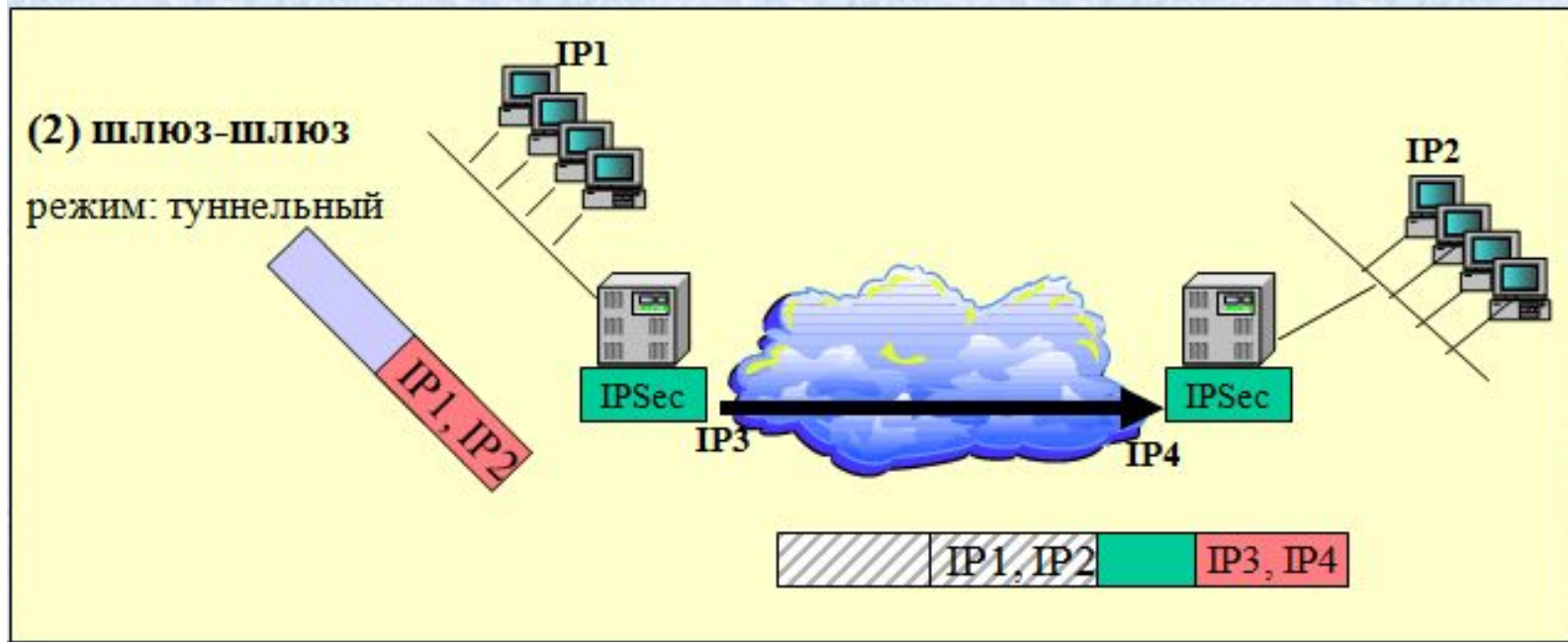
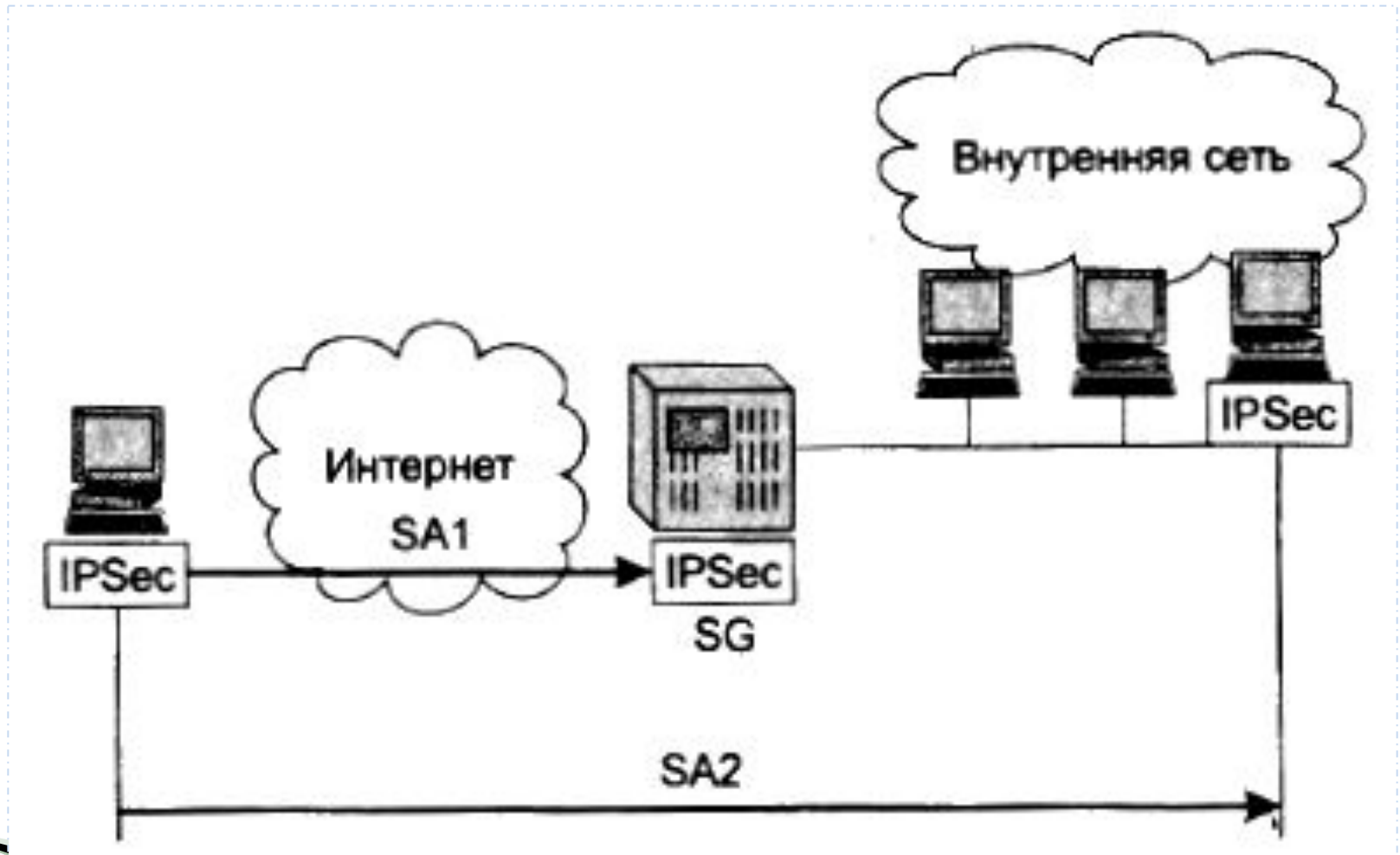


Рис. 6.44-11. Схема установления SA шлюз-шлюз

Протоколы защищенного канала. IPsec

- ▣ **В схеме хост-шлюз** защищенный канал прокладывается между удаленным хостом и шлюзом, защищающим трафик для всех хостов, входящих во внутреннюю сеть предприятия (рис. 6.44-12).

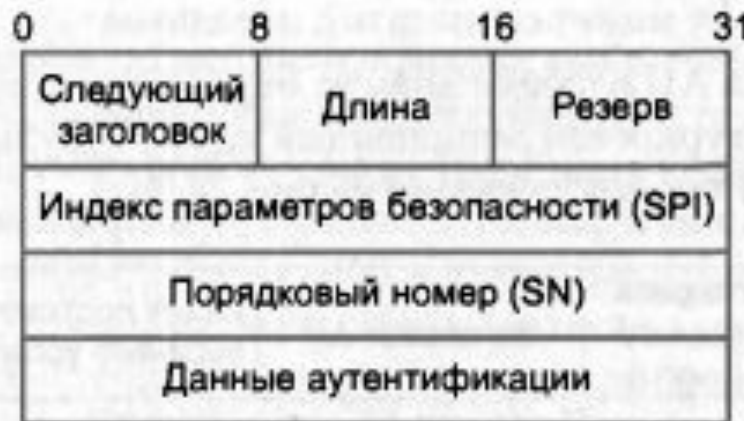


▣ Рис. 6.44-12. Схема защищенного канала хост-шлюз

Протоколы защищенного канала. IPsec

▣ *Протокол AH*

- ▣ Протокол AH позволяет приемной стороне убедиться, что:
 - пакет отправлен стороной, с которой установлена безопасная ассоциация;
 - содержимое не было искажено в процессе передачи по сети;
 - пакет не является дубликатом уже полученного пакета.
- Для выполнения этих функций протокол AH использует специальный заголовок (рис. 6.44-13) в пакете IP протокола.



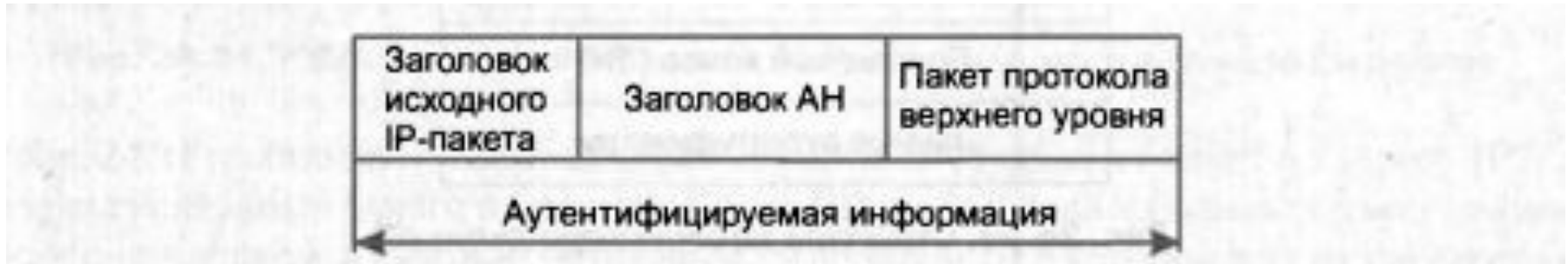
- Рис. 6.44-13. Структура заголовка протокола AH

Протоколы защищенного канала. IPsec

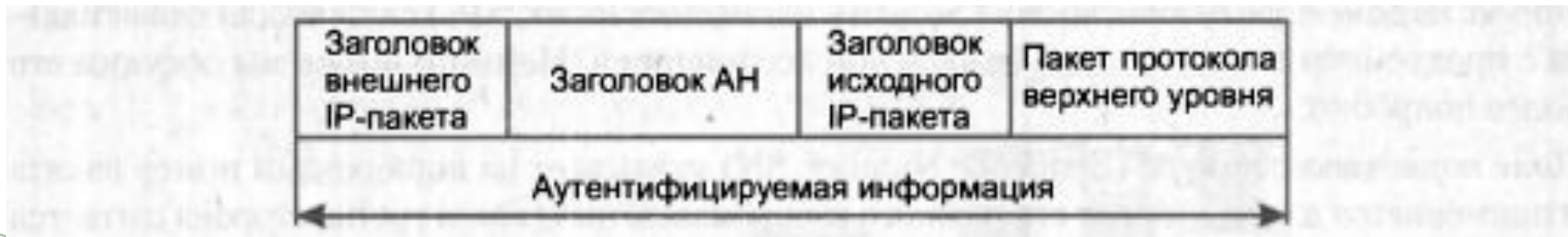
- ▣ В поле **следующего заголовка** (next header) указывается код протокола более высокого уровня.
- ▣ В **поле длины полезной нагрузки** (payload length) содержится длина заголовка АН.
- ▣ **Индекс параметров безопасности** (Security Parameters Index, SPI) соответствует индексу безопасной ассоциации.
- ▣ **Поле порядкового номера** (Sequence Number, SN) указывает на порядковый номер пакета, который отправляющая сторона последовательно увеличивает в каждом новом пакете.
- ▣ **Поле данных** аутентификации (authentication data) содержит значение проверки целостности (Integrity Check Value, ICV) пакета.

Протоколы защищенного канала. IPsec

- Местоположение заголовка АН в пакете зависит от того, в каком режиме — транспортном или туннельном — сконфигурирован защищенный канал:



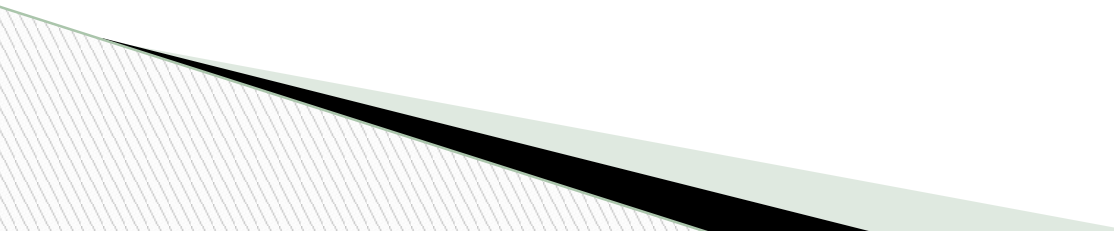
- Рис. 6.44-14. Структура IP-пакета, обработанного протоколом АН в транспортном режиме



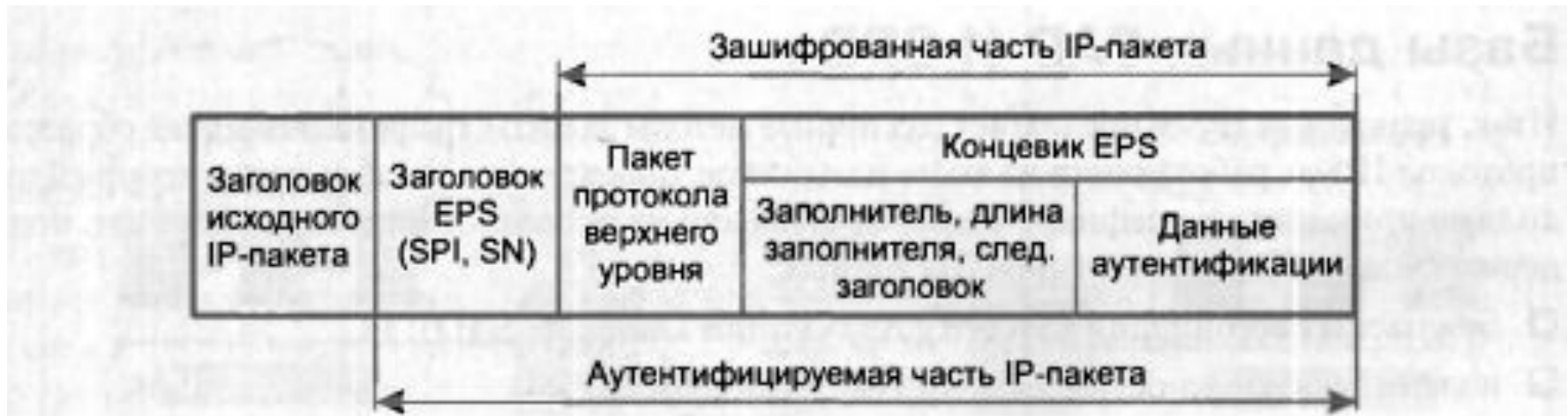
- Рис. 6.44-15. Структура IP-пакета, обработанного протоколом АН в туннельном режиме

Протоколы защищенного канала. IPsec

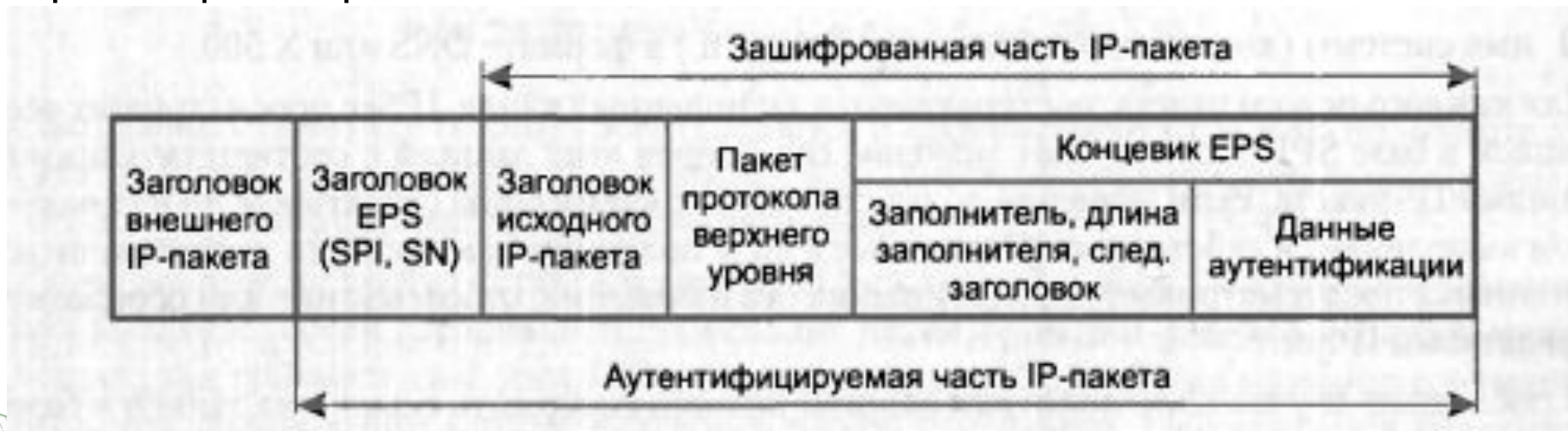
Протокол ESP

- Протокол ESP решает две задачи:
 - 1) Обеспечение аутентификации и целостности данных.
 - 2) Защита передаваемых данных путем их шифрования.
-
- Заголовок ESP делится на две части:
 - 1) Собственно заголовок ESP образуется двумя полями (SPI и SN).
 - 2) Служебные поля, называемые концевиком ESP, — следующий заголовок, данные аутентификации, заполнитель и длина заполнителя.
- 

Протоколы защищенного канала. IPsec



- Рис. 6.44-16. Структура IP-пакета, обработанного протоколом ESP в транспортном режиме



- Рис. 6.44-17. Структура IP-пакета, обработанного протоколом ESP в туннельном режиме

Протоколы защищенного канала. IPsec

Базы данных SAD И SPD

- ▣ Протокол IPsec определяет способ использования защиты в каждом узле с помощью:
 - Баз данных безопасных ассоциаций (Security Associations Database, SAD). Две стороны принимают ряд соглашений, регламентирующих процесс передачи потока данных между ними, фиксирующихся в виде набора параметров, которые хранятся на конечных узлах в виде SAD.
 - Баз данных политики безопасности (Security Policy Database, SPD). SPD определяет соответствие между IP-пакетами и установленными для них правилами обработки. Записи SPD состоят из полей селектора пакета и полей политики защиты.

Селектор включает следующий набор признаков:

 - IP-адреса источника и приемника;
 - порты источника и приемника;
 - тип протокола транспортного уровня;
 - имя пользователя;
 - имя системы (хоста, шлюза безопасности и т. п.).

Протоколы защищенного канала. IPsec

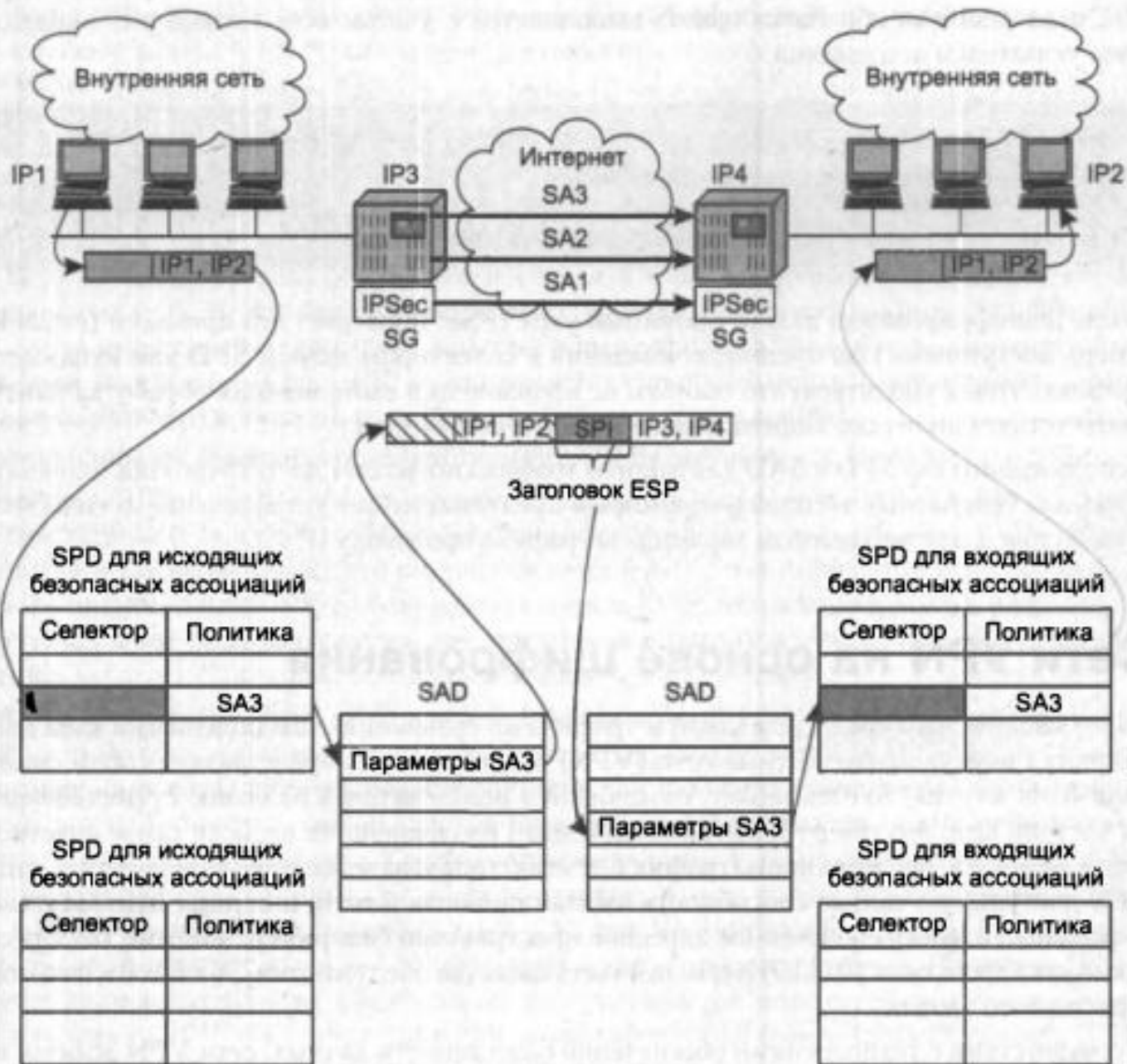


Рис. 6.44-18. Использование баз данных SPD и SAD

Сети VPN на основе шифрования

- Более масштабным средством защиты трафика являются виртуальные частные сети (VPN). Подобная сеть представляет собой «сеть в сети» (иллюзию частной сети внутри публичной с защищенностью трафика от атак пользователей публичной сети).

- Сети VPN делятся на два класса:
 - сети VPN на основе разграничения трафика;
 - сети VPN на основе шифрования.

- В VPN техника защищенных каналов связывает не двух пользователей, а произвольное количество клиентских сетей.

- VPN на основе шифрования включают:
 - **Шифрование**;
 - **Аутентификацию**;
 - **Туннелирование** (возможность передавать зашифрованные пакеты по открытой публичной сети).

Сети VPN на основе шифрования

- Наиболее широко используются сети VPN на основе протоколов IPSec и SSL.
- IPSec обеспечивает высокую степень гибкости.
- Режим инкапсуляции IPSec позволяет изолировать адресные пространства клиента и поставщика услуг за счет применения внешнего и внутреннего IP-адресов.
- Конфигурирование на основе IPSec довольно трудоемко, поскольку при полносвязной топологии их количество пропорционально $N \times (N - 1)$, где N — число соединений.
- Наиболее популярным приложением, использующим защищенные каналы SSL, является веб-браузер. В этом случае защищенные каналы SSL задействует протокол HTTP, и в этом режиме работы его часто называют протоколом HTTPS.
- VPN на основе SSL функционирует на основе веб-портала, развернутого в локальной сети.
- Отсутствие специального клиентского программного обеспечения — значительное преимущество VPN на основе SSL.

Список использованных источников

- В.Г. Олифер, Н.А. Олифер Компьютерные сети, 3-е издание, 2009г.