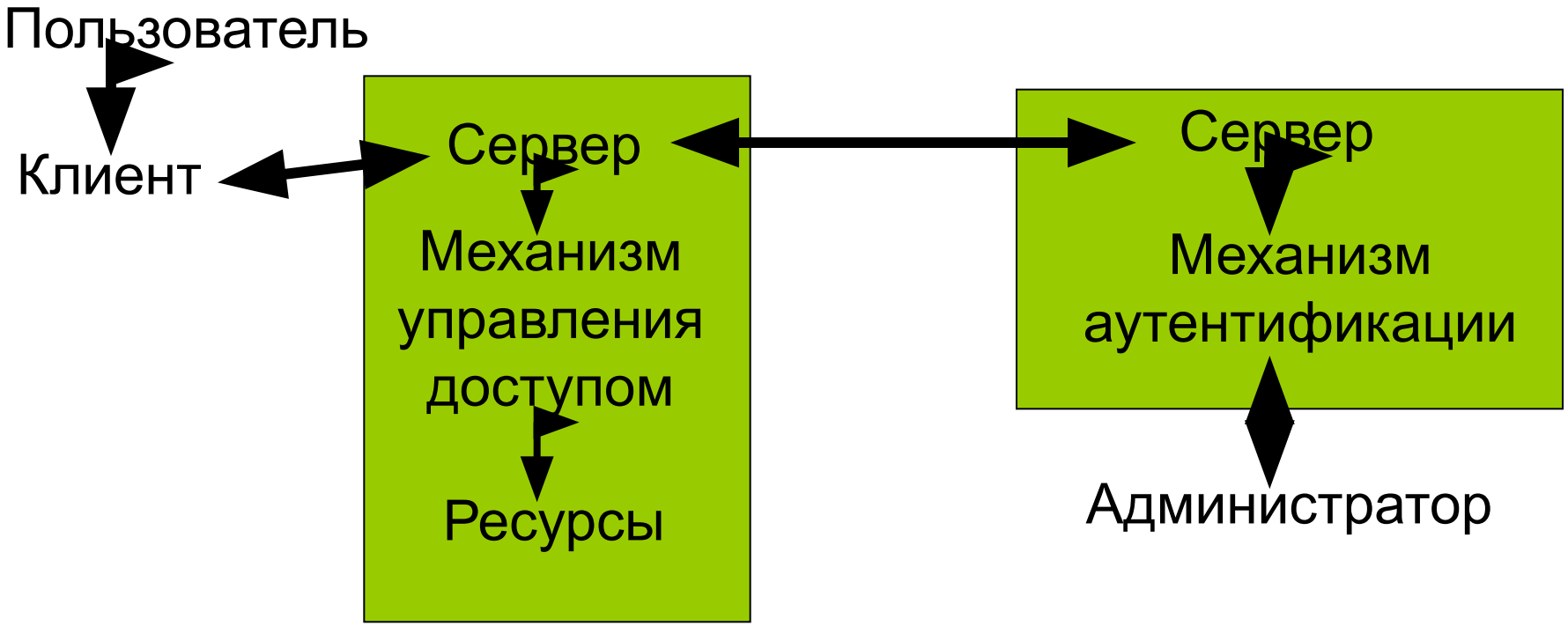
Лекция 7. Аутентификация при удаленном доступе

1. Непрямая аутентификация пи удаленном доступе.
2. Виртуальные частные сети и способы их построения.
3. Средства защиты информации в глобальных компьютерных сетях.

Непрямая аутентификация

Решение проблемы масштабируемости КС.

Механизм аутентификации реализован на отдельном сервере, а все другие серверы связываются с сервером аутентификации.



Непрямая аутентификация

Используются более сложные протоколы (RADIUS, Kerberos), выполнение которых начинается после попытки входа на какой-либо сервер пользователя с удаленной клиентской PC.

Дополнительная угроза – подделка ответов сервера аутентификации или сервера обслуживания.

Для повышения отказоустойчивости поддерживается автоматическая репликация базы учетных записей для распределения нагрузки между несколькими серверами аутентификации (могут появляться проблемы при объединении КС разных организаций).

Протокол RADIUS

- Remote Authentication Dial In User Service.
- Сервер доступа (NAS, Network Access Server) выступает в качестве агента RADIUS. Агент отвечает за передачу сведений о пользователе заданным серверам RADIUS и дальнейшие действия в зависимости от возвращенной сервером информации.
- Серверы RADIUS отвечают за прием запросов агента, идентификацию и аутентификацию пользователей и возврат агенту всех конфигурационных параметров, требуемых для предоставления пользователю соответствующих услуг.

Протокол RADIUS

- Аутентификация транзакций между агентом и сервером RADIUS осуществляется с использованием разделяемого ключа K_R (ключа RADIUS), который никогда не передается через сеть. В дополнение к этому пользовательские пароли между агентами и серверами RADIUS передаются в зашифрованном виде во избежание перехвата паролей при их передаче через незащищенные сети.

Протокол RADIUS

1. Клиент C->Агент A: ID, P.
2. A: генерация случайного N, вычисление сеансового ключа $K=H(K_R,N)$, шифрование пароля пользователя $EP=K \oplus P$.
3. A->Сервер аутентификации S: N, ID, EP.
4. S: вычисление сеансового ключа $K=H(K_R,N)$, расшифрование пароля пользователя $P=EP \oplus K$, извлечение из регистрационной базы данных пароля пользователя и сравнение его с P, генерация ответа R – «доступ разрешен» или «в доступе отказано», вычисление аутентификатора ответа $RA= H(R,N,K_R)$.
5. S->A: R, RA.
6. A: вычисление $H(R,N,K_R)$ и сравнение его с RA, при совпадении проверка R (авторизация пользователя или отказ ему в доступе).

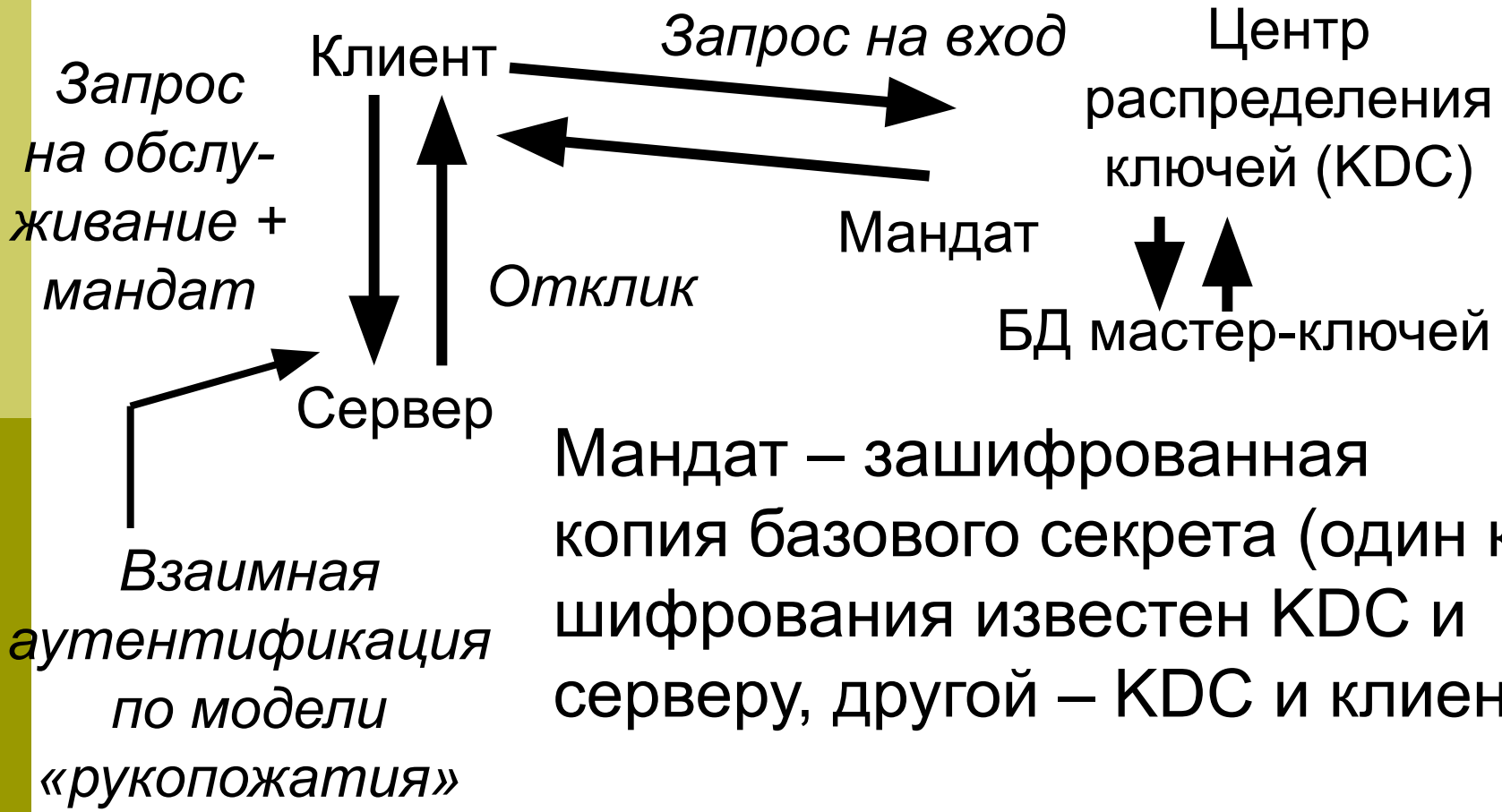
Протокол RADIUS

Случайное значение *N* предназначено для вычисления уникального сеансового ключа шифрования пароля (защиты от перехвата и повтора сообщения шага 3). Аутентификатор ответа *RA* предназначен для связывания ответа сервера и запроса агента (защиты от подмены сообщения шага 5).

Протокол RADIUS

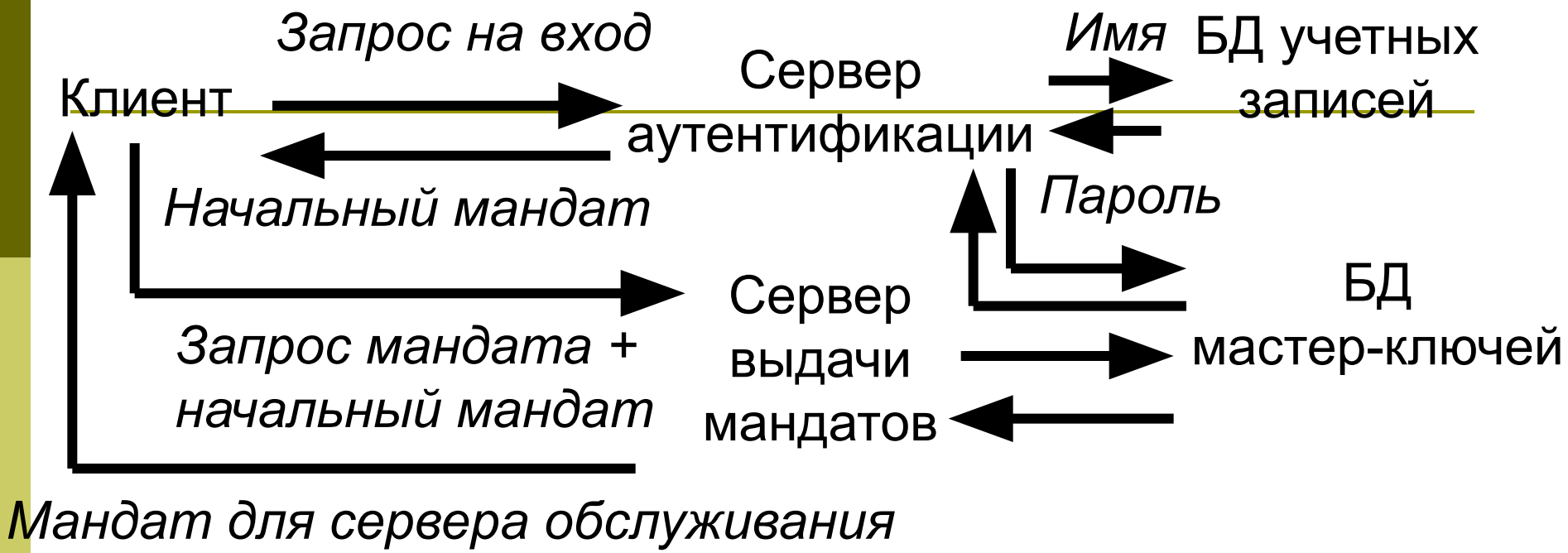
Недостаток – при любом обращении пользователя к серверу удаленного доступа (агенту RADIUS) требуется проведение аутентификации пользователя с помощью сервера RADIUS, что увеличивает сетевой трафик и усложняет масштабирование компьютерной сети.

Управление сетевыми ресурсами внутри одной организации (протокол Kerberos)



Мандат – зашифрованная копия базового секрета (один ключ шифрования известен KDC и серверу, другой – KDC и клиенту)

Получение мандата



Пользователь вводит свой пароль только для расшифровки начального билета, после чего он уже не должен находиться на его рабочей станции. Для защиты от повтора в мандатах используются метки времени, имена пользователей (серверов) и сетевые адреса компьютеров.

Виртуальные частные сети

Типовые угрозы безопасности открытых сетей передачи данных (типа Интернета):

- Анализ сетевого трафика.
- Подмена субъекта или объекта соединения.
- Внедрение ложного объекта (угроза «человек посередине»).
- Отказ в обслуживании.

Виртуальные частные сети (Virtual Private Network, VPN)

Технология предназначена для защиты от перечисленных выше угроз и включает в себя следующие этапы:

1. Согласование параметров защищенной связи (криптографических алгоритмов и ключей).
2. Шифрование исходного IP-пакета.
3. Инкапсуляция его в блок данных нового IP-пакета.
4. Добавление заголовка к новому IP-пакету.

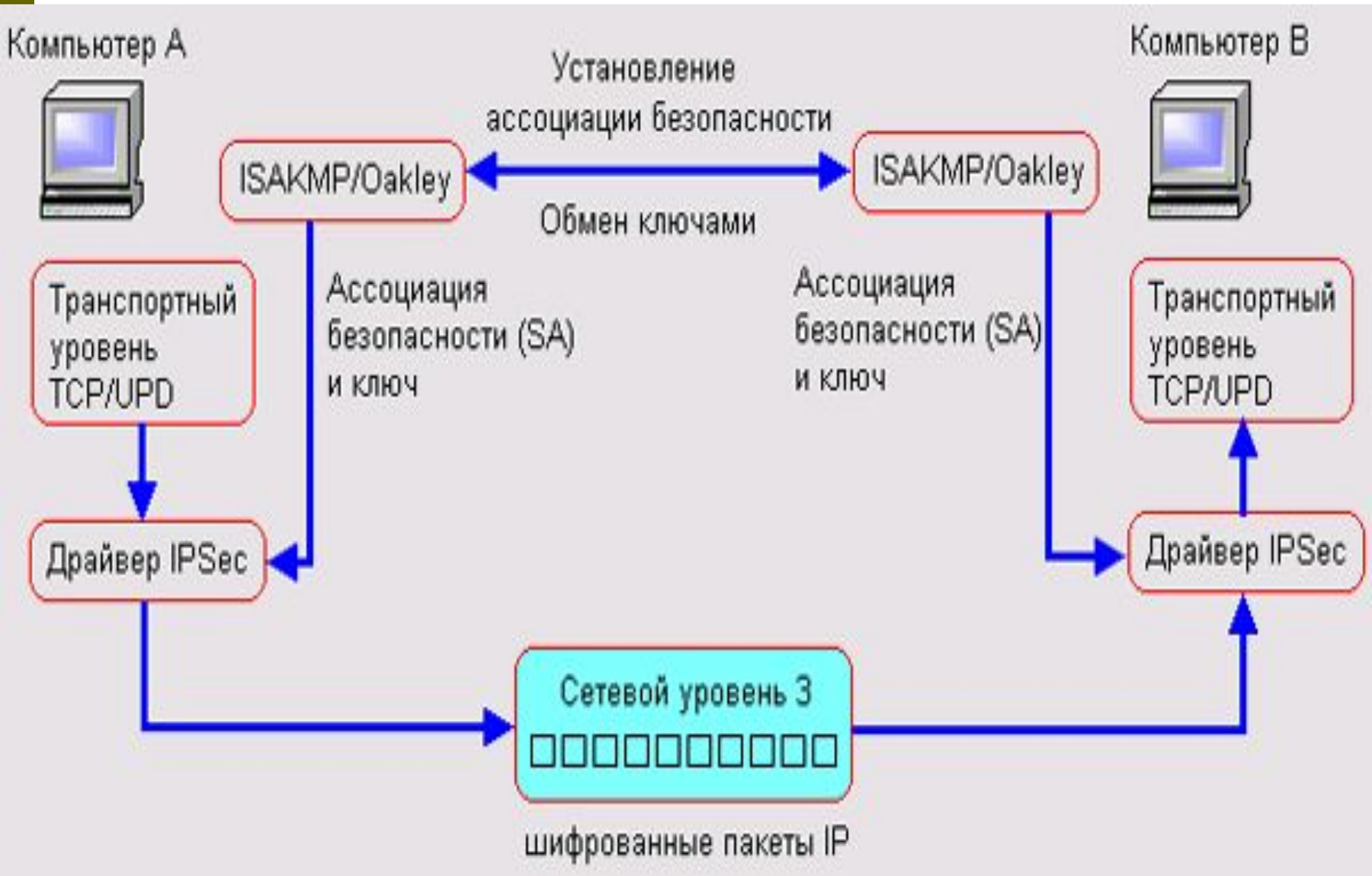
Способы построения VPN

- Програм-мные.
- Програм-мно-аппарат-ные.

- На канальном уровне модели OSI (протоколы L2TP, PPTP, L2F) – обеспечивается независимость от протоколов сетевого уровня, но сложность конфигурирования при соединении двух ЛВС.
- На сетевом уровне (IPSec, SKIP) – хорошая масштабируемость.
- На сеансовом уровне (SSL, TLS, SOCKS) – независимое управление передачей данных в обоих направлениях, возможность сочетания с VPN других типов.

Протокол IPSec

Протокол IPSec



Протокол IPSec

- Протокол аутентифицирующего заголовка (AH) предназначен для защиты от атак, связанных с несанкционированным изменением содержимого пакета, в том числе от подмены адреса отправителя сетевого уровня.
- Протокол инкапсуляции зашифрованных данных (ESP) предназначен для обеспечения конфиденциальности данных. Необязательная опция аутентификации в этом протоколе может обеспечить контроль целостности зашифрованных данных.

Протокол ESP

- Обеспечивает шифрование данных исходного IP-пакета с использованием симметричного алгоритма и заранее согласованного ключа.
- Дополнительно может включаться опция аутентификации, обеспечивающая вычисление контрольного хеш-значения от данных IP-пакета и другого заранее согласованного ключа.

Режимы протокола IPSec

- Транспортный режим используется для шифрования поля данных IP пакета, содержащего протоколы транспортного уровня (TCP, UDP, ICMP), которое, в свою очередь, содержит информацию прикладных служб.
- Туннельный режим предполагает шифрование всего пакета, включая заголовок сетевого уровня. Туннельный режим применяется в случае необходимости скрытия информационного обмена организации с внешним миром. При этом, адресные поля заголовка сетевого уровня пакета, использующего туннельный режим, заполняются межсетевым экраном организации и не содержат информации о конкретном отправителе пакета.

Пример VPN на основе программно-аппаратных средств

Модель (возможности) нарушителя

- знает топологию всей сети;
- знает IP-адреса хостов защищаемых подсетей (ЛВС организации);
- имеет образцы программного и аппаратного обеспечения установленных в подсетях рабочих станций и серверов;
- владеет сведениями о внедренных в стандартное программное обеспечение рабочих станций и серверов закладках, случайно или намеренно оставленной отладочной информации, ключах шифрования и т.п.;
- не знает сеансовых и базовых ключей шифрования, используемых специализированными криптомаршрутизаторами;
- не имеет возможности осуществить локальный несанкционированный доступ к информации.

Характеристики криптомаршрутизатора

- физическое разделение внешних (с сетью Интернет) и внутренних (с хостами обслуживаемой подсети) интерфейсов (например, с помощью двух разных сетевых карт);
- возможность шифрования всех исходящих (в другие ЛВС организации) и расшифрования всех входящих (из этих ЛВС) пакетов данных.

Криптомаршрутизатор

Алгоритм работы криптомаршрутизатора CR_1

1. По таблице маршрутов ищется адрес криптомаршрутизатора, который обслуживает подсеть, содержащую получателя пакета ($AD(CR_2)$).
2. Определяется интерфейс, через который доступна подсеть, содержащая CR_2.
3. Шифруется весь пакет от А (вместе с его заголовком) на сеансовом ключе связи CR_1 и CR_2, извлеченном из таблицы маршрутов.
4. К полученным данным добавляется заголовок, содержащий $AD(CR_1)$ в качестве адреса отправителя и $AD(CR_2)$ в качестве адреса получателя нового пакета.
5. Сформированный пакет отправляется через сеть Интернет.

Алгоритм работы криптомаршрутизатора CR_2

1. Из таблицы маршрутов извлекается сеансовый ключ связи CR_1 и CR_2.
2. Выполняется расшифрование данных полученного пакета.
3. Если после расшифрования структура «вложенного» пакета некорректна или адрес его получателя не соответствует обслуживаемой CR_2 подсети (не совпадает с AD(X)), то полученный пакет уничтожается;
4. Расшифрованный пакет, содержащий AD(A) в поле отправителя и AD(X) в поле получателя, передается X через внутренний интерфейс ЛВС.

Защита информации в глобальных сетях

- Межсетевые экраны (брандмауэры, firewalls).
- Сканеры уязвимостей (vulnerability assessment).
- Системы обнаружения атак (Intrusion Detect Systems, IDS).
- Системы контроля содержания (анализа трафика, MIME-sweeper for Web).

Межсетевые экраны

Реализуют набор правил, которые определяют условия прохождения пакетов данных из одной части распределенной компьютерной системы (открытой) в другую (защищенную). Обычно межсетевые экраны (МСЭ) устанавливаются между сетью Интернет и локальной вычислительной сетью организации, но могут устанавливаться и на каждый хост локальной сети (персональные МСЭ).

Межсетевые экраны

В зависимости от уровня взаимодействия объектов сети основными разновидностями МСЭ являются:

- фильтрующие (экранирующие) маршрутизаторы,
- шлюзы сеансового уровня (экранирующие транспорты),
- шлюзы прикладного уровня,
- МСЭ экспертного уровня, работающие на разных уровнях модели OSI.

Фильтрующие маршрутизаторы

Достоинства:

- простота их создания, установки и конфигурирования,
- прозрачность для приложений пользователей КС и минимальное влияние на их производительность,
- невысокая стоимость.

Недостатки :

- отсутствие аутентификации на уровне пользователей КС;
- уязвимость для подмены IP-адреса в заголовке пакета;
- незащищенность от угроз нарушения конфиденциальности и целостности передаваемой информации;
- сильная зависимость эффективности набора правил фильтрации от уровня знаний администратора МСЭ конкретных протоколов;
- открытость IP-адресов компьютеров защищенной части сети.

Шлюзы сеансового уровня

Основные функции:

- контроль виртуального соединения между рабочей станцией защищенной части сети и хостом ее незащищенной части;
- трансляция IP-адресов компьютеров защищенной части сети (технология Network Address Translation, NAT).

Шлюзы сеансового уровня

К достоинствам относятся также их простота и надежность программной реализации.

К недостаткам – отсутствие возможности проверять содержимое передаваемой информации, что позволяет нарушителю пытаться передать пакеты с вредоносным программным кодом через подобный МСЭ и обратиться затем напрямую к одному из серверов (например, Web-серверу) атакуемой КС.

Шлюзы прикладного уровня

Не только исключают прямое взаимодействие между авторизованным клиентом из защищенной части сети и хостом из ее открытой части, но и фильтрует все входящие и исходящие пакеты данных на прикладном уровне (т.е. на основе анализа содержания передаваемых данных).

Шлюзы прикладного уровня

К основным функциям относятся:

- идентификация и аутентификация пользователя КС при попытке установить соединение;
- проверка целостности передаваемых данных;
- разграничение доступа к ресурсам защищенной и открытой частей распределенной КС;
- фильтрация и преобразование передаваемых сообщений (обнаружение вредоносного программного кода, шифрование и расшифрование и т.п.);
- регистрация событий в специальном журнале;
- кэширование запрашиваемых извне данных, размещенных на компьютерах внутренней сети (для повышения производительности КС).

Шлюзы прикладного уровня

Достоинства:

- наиболее высокая степень защиты КС от удаленных атак,
- скрытость структуры защищенной части сети для остальных хостов,
- надежная аутентификация и регистрация проходящих сообщений,
- возможность реализации дополнительных проверок.

Недостатки:

- более высокая стоимость,
- сложность разработки, установки и конфигурирования,
- снижение производительности КС,
- «непрозрачность» для приложений пользователей КС.

Общие недостатки МСЭ

В принципе не могут предотвратить многих видов атак (например, угрозы несанкционированного доступа к информации с использованием ложного сервера службы доменных имен сети Интернет, угрозы анализа сетевого трафика, угрозы отказа в обслуживании).