Лекция 4.3. Построение защищённых каналов связи

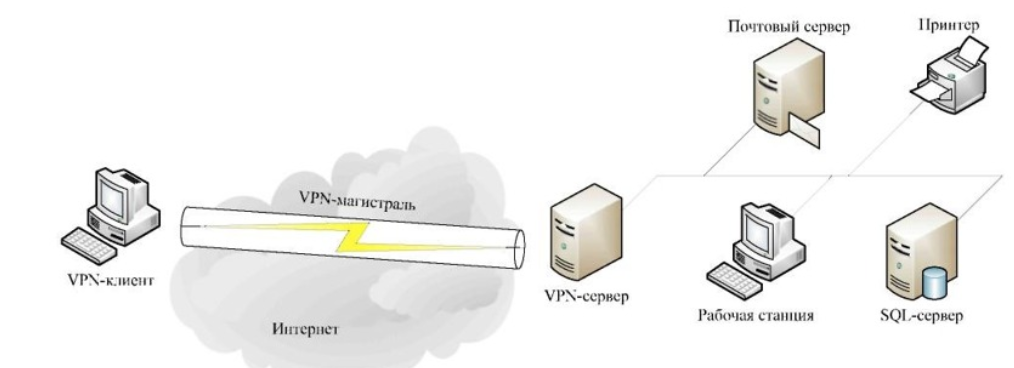
В данной лекции рассмотрены следующие вопросы:  
1. Удалённый доступ.  
2. Виды коммутируемых линий.  
3. Основные понятия и виды виртуальных частных сетей.  
4. Классификация сетей VPN Основные варианты архитектуры VPN.

Глава 1. Построение защищённых каналов связи

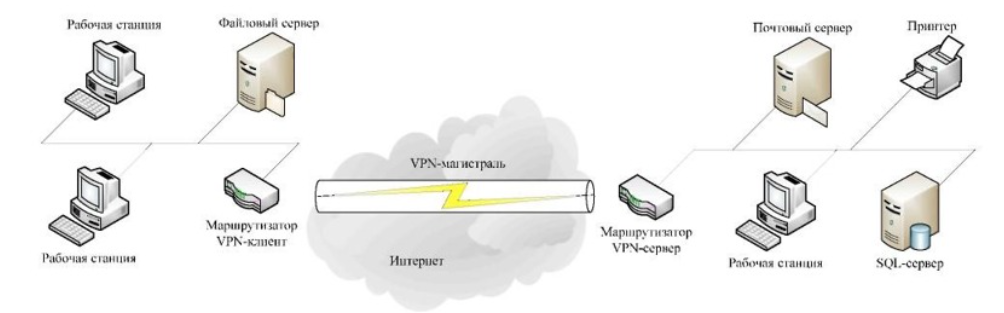
Удалённый доступ. Виды коммутируемых линий  
Компьютерная сеть многих организаций не ограничивается локальной сетью, размещённой в одном или нескольких близко расположенных зданиях. Пользователи могут находиться на большом удалении от основного офиса, например, если филиал находится в другом городе или если сотрудник организации уезжает в командировку в другую страну с ноутбуком.  
Возможность использования удалёнными пользователями ресурсов локальной сети называется удалённым доступом (remote access). Различают два основных вида удалённого доступа:  
1. Соединение по коммутируемой линии (dial-up connection).  
2. Соединение с использованием виртуальных частных сетей (Virtual Private Networks, VPN).  
Виды коммутируемых линий  
Соединения по коммутируемым линиям могут осуществляться с использованием следующих средств связи.  
1. Телефонные сети — наиболее распространённый и дешёвый вариант, хотя и самый медленный (максимальная скорость передачи данных 56,6 кбит/с). Предполагает установку модемов на клиенте и сервере.  
2. Сети ISDN (Integrated Services Digital Network) — цифровая сеть с комплексными услугами) обеспечивают скорость передачи данных 128 кбит/с, но их использование дороже, чем использование обычных телефонных сетей.  
3. ATM поверх ADSL — передача трафика АТМ (Asynchronous Transfer Mode — асинхронный режим передачи) посредством линий ADSL (Asymmetric Digital Subscriber Line — асимметричная цифровая абонентская линия).  
Соединение посредством коммутируемых линий долгое время оставалось единственным решением проблемы связи локальных сетей с удалёнными пользователями. Однако данное решение является довольно дорогим и недостаточно безопасным.  
В последние годы стоимость использования каналов связи Интернета стала уменьшаться и скорость стала ниже, чем цена использования коммутируемых линий. Однако при установлении соединения через Интернет серьёзной проблемой является обеспечение безопасности, так как сеть является открытой, и злоумышленники могут перехватывать пакеты с конфиденциальной информацией. Решением этой проблемы стала технология виртуальных частных сетей.  
Виртуальные частные сети (Virtual Private Network, VPN) — это защищённое соединение двух узлов через открытые сети. При этом организуется виртуальный канал, обеспечивающий безопасную передачу информации, а узлы, связанные VPN, могут работать так, как будто соединены напрямую.  
Компьютер, инициирующий VPN-соединение, называется VPN-клиентом. Компьютер, с которым устанавливается соединение, называется VPN-сервером.  
VPN-магистраль — это последовательность каналов связи открытой сети, через которые проходят пакеты виртуальной частной сети.  
Существует два типа VPN-соединений:  
1. Соединение с удалёнными пользователями (Remote Access VPN Connection).  
2. Соединение маршрутизаторов (Router-to-Router VPN Connection).

Глава 2. Построение защищённых каналов связи

Соединение с удалёнными пользователями осуществляется в том случае, если одиночный клиент подключается к локальной сети организации через VPN:



Соединение маршрутизаторов устанавливается между двумя локальными сетями, если узлы обоих сетей нуждаются в доступе к ресурсам друг друга. При этом один из маршрутизаторов играет роль VPN-сервера, а другой — VPN-клиента:



VPN-соединение возможно не только через Интернет, но и в рамках локальной сети.  
Классификация сетей VPN  
Существуют разные признаки классификации VPN. Наиболее часто используются:

«рабочий» уровень модели OSI;

архитектура технического решения VPN;

способ технической реализации VPN.

Классификация VPN по «рабочему» уровню модели OSI  
Для технологий безопасной передачи данных по общедоступной (незащищённой) сети применяют защищённый канал (secure channel), т. е. защита данных обеспечивается между двумя узлами сети (хостами или шлюзами) вдоль некоторого виртуального пути, проложенного в сети с коммутацией пакетов.  
По признаку «рабочего» уровня модели OSI различают следующие группы VPN:  
1. VPN канального уровня.  
2. VPN сетевого уровня.  
3. VPN сеансового уровня.  
Классификация VPN по архитектуре технического решения  
По архитектуре технического решения принято выделять три основных вида виртуальных частных сетей:  
1. Внутрикорпоративные VPN (Intranet VPN).  
2. VPN с удалённым доступом (Remote Access VPN).  
3. Межкорпоративные VPN (Extranet VPN).  
Классификация VPN по способу технической реализации  
Конфигурация и характеристики виртуальной частной сети во многом определяются типом применяемых VPN-устройств.  
По способу технической реализации различают VPN на основе:

маршрутизаторов;

межсетевых экранов;

программных решений;

специализированных аппаратных средств со встроенными шифропроцессорами.

1. Получение доступа к компьютеру, сети или файлам из удалённого места с использованием сетевых технологий называется:
   1. Дистанционный доступ
   2. Удаленный доступ
   3. Нет верного ответа
2. Процесс передачи данных по сети путём установления временного канала связи.
   1. Комьюнити
   2. Коммуникация
   3. Коммутация
3. При каком методе коммутации доступ к линии связи предоставляется на определённый временной интервал, называемый временным слотом?
   1. Линия связи с коммутацией пакетов
   2. Виртуальная частная сеть
   3. Линия связи с коммутацией временного слота
4. При каком методе коммутации данные разделяются на пакеты и передаются через сеть независимо друг от друга?
   1. Линия связи с коммутацией пакетов
   2. Линия связи с коммутацией пакетов
   3. Виртуальная частная сеть
5. Выберите все составляющие, которые являются базой для создания безопасного и зашифрованного канала связи через общественные сети:
   1. Шифрование
   2. Аутентификация
   3. Туннелирование
   4. Декодирование
6. Как называется механизм, который создаёт виртуальный «туннель» между отправителем и получателем данных в рамках общедоступной сети?
   1. Шифрование
   2. Аутентификация
   3. Туннелирование
7. Процесс преобразования данных в непонятный для посторонних вид:
   1. Шифрование
   2. Аутентификация
   3. Туннелирование
8. Процесс проверки подлинности и идентификации пользователей или устройств, имеющих доступ к VPN:
   1. Шифрование
   2. Аутентификация
   3. Туннелирование
9. Выберите все виды виртуальных частных сетей:
   1. Клиент к сети
   2. Удаленный доступ
   3. Сайт к сайту
   4. Коммуникационный доступ
10. Эта архитектура VPN предполагает наличие центрального сервера, к которому подключаются клиенты для получения доступа к ресурсам сети:
    1. Оба ответа верны
    2. Клиент-сервер
    3. Межсетевой экран