Сравнительный анализ протоколов построения виртуальных частных сетей.

Выполнил: Студент группы ИТСб-141
Етерсков Иван Александрович
Научный руководитель: Ст.преп.кафедры ТКС Тюхтяев Д. А.

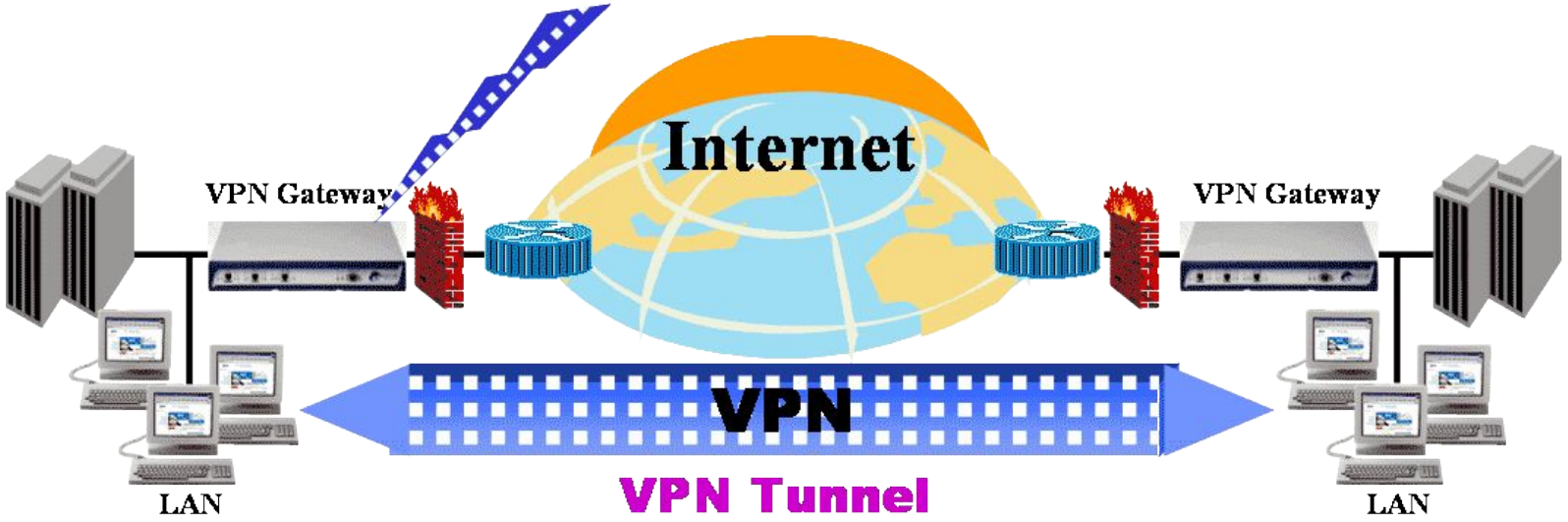
Цель работы:

- Произвести сравнительный анализ наиболее распространённых протоколов, используемых для построения VPN соединений

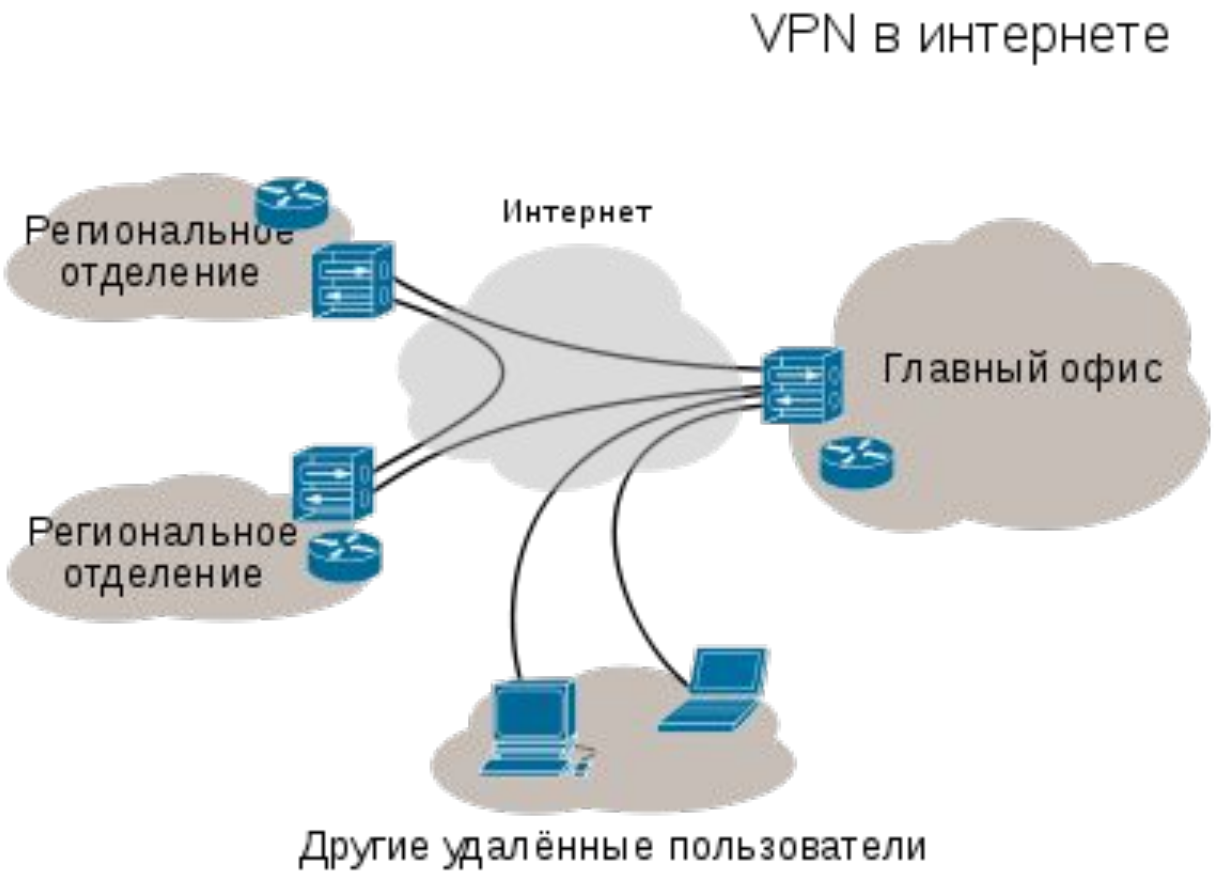
Задачи курсовой работы:

- Произвести обзор наиболее распространённых протоколов для построения VPN;
- Произвести анализ наиболее распространенных протоколов для построения VPN;
- Сравнить наиболее распространенные протоколы для построения VPN

VPN (Virtual Private Network — виртуальная частная сеть) — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет).



VPN - туннель



VPN Сеть предприятия

Классификация VPN протоколов

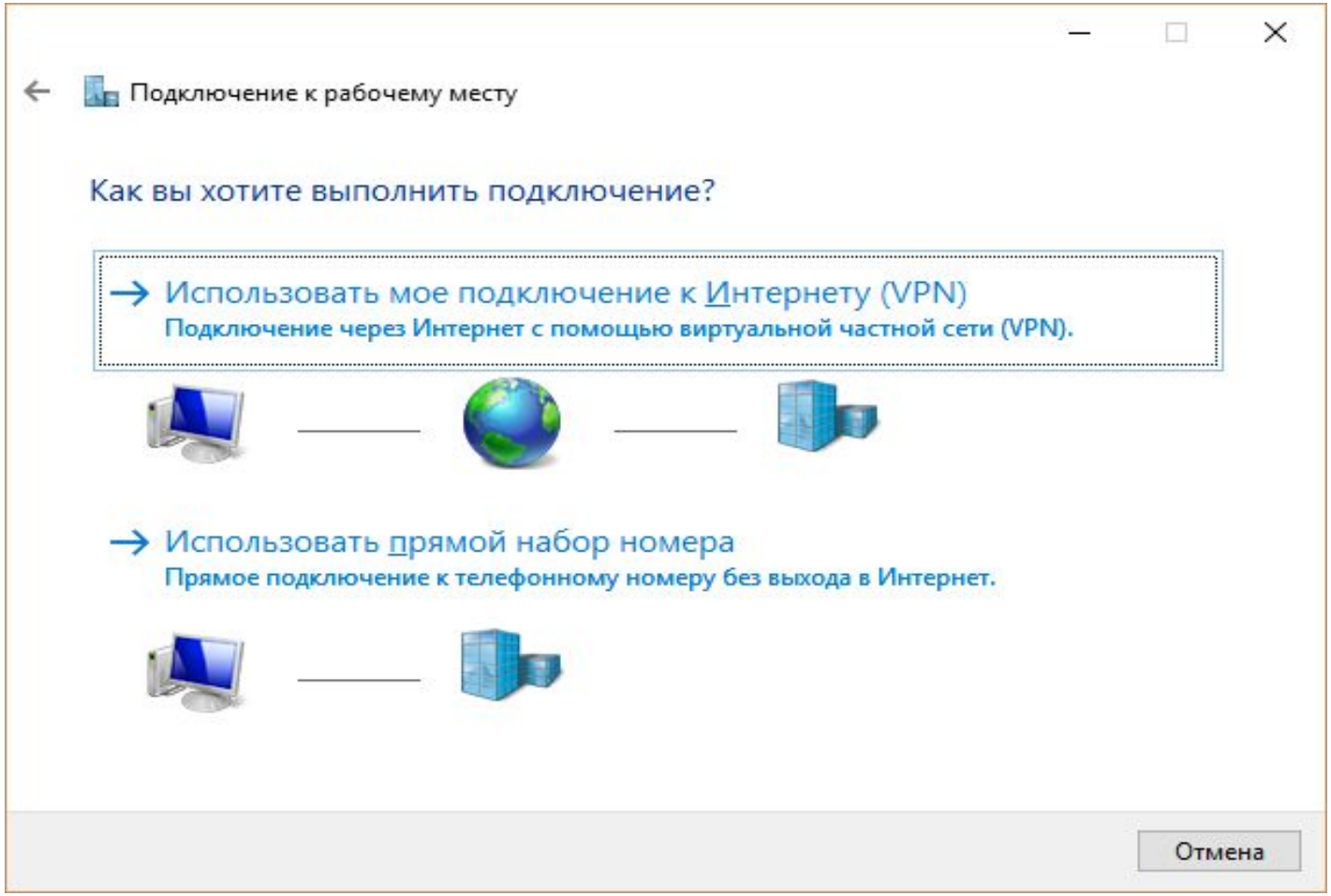
- В современных условиях развития IT-технологий преимущества использования VPN неоспоримы. VPN сеть позволяет защитить информацию во время ее передачи по незащищенной Всемирной сети Интернет. Существует несколько способов классификации VPN- решений. Ниже рассмотрены те, которые чаще всего используются на практике.

- По рабочему уровню модели OSI
- По архитектуре технического решения
- По способу технической реализации
- По типу и уровню протокола

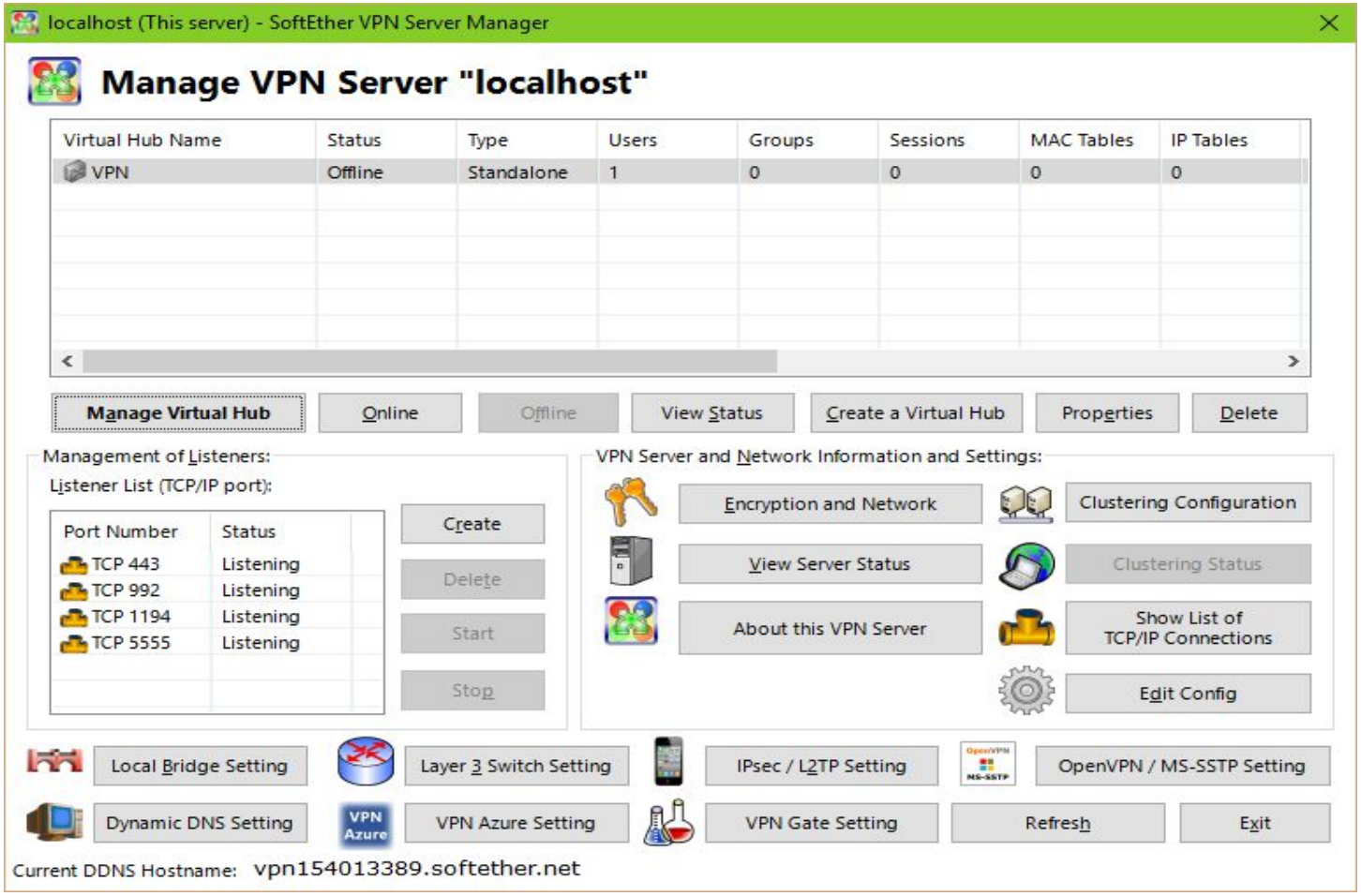
Протоколы VPN

- PPTP (Point-to-Point Tunneling Protocol) — туннельный протокол типа точка-точка, позволяющий компьютеру устанавливать защищённое соединение с сервером за счёт создания специального туннеля в стандартной, незащищённой сети.
- L2TP/IPSec (англ. Layer 2 Tunneling Protocol — протокол туннелирования второго уровня) — в компьютерных сетях туннельный протокол, использующийся для поддержки виртуальных частных сетей.
- OpenVPN — свободная реализация технологии виртуальной частной сети (VPN) с открытым исходным кодом для создания зашифрованных каналов типа точка-точка или сервер-клиенты между компьютерами. Она позволяет устанавливать соединения между компьютерами, находящимися за NAT и сетевым экраном, без необходимости изменения их настроек.

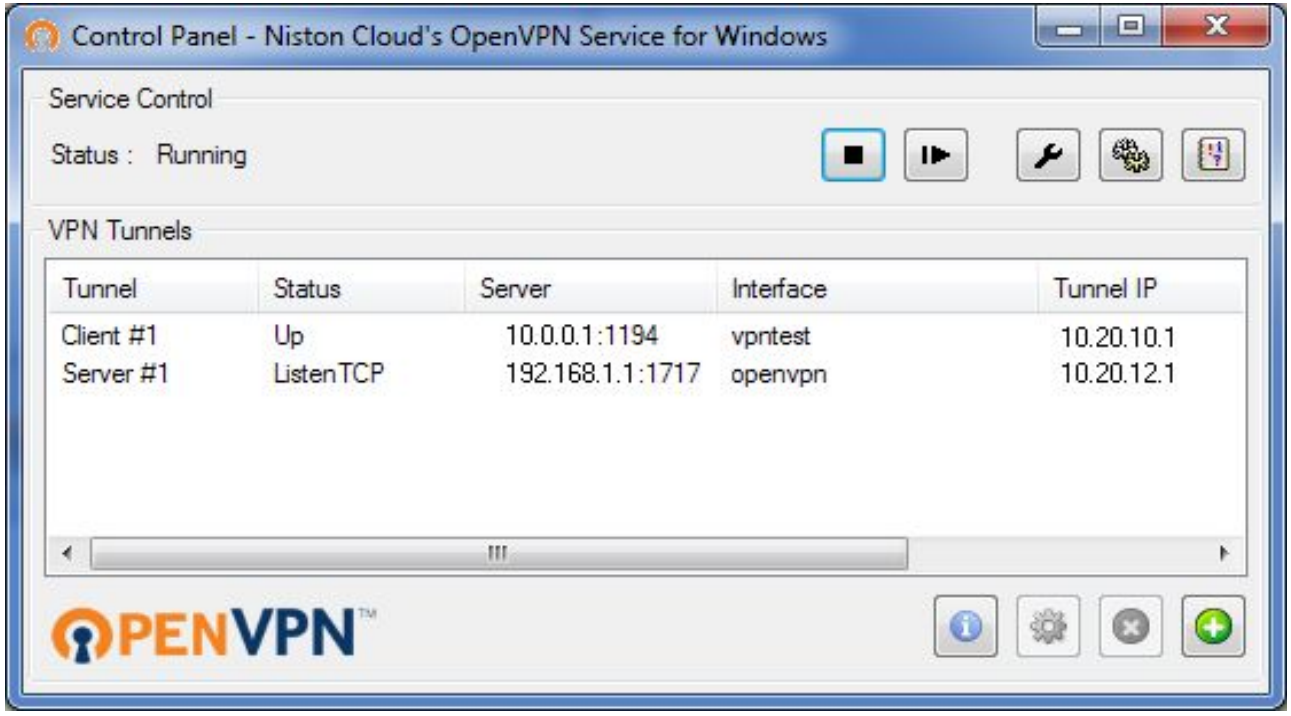
Встроенное программное обеспечение Windows



SoftEther VPN Project



OpenVPN


Control Panel - Niston Cloud's OpenVPN Service for Windows
Service Control
Status : Running
VPN Tunnels
Tunnel
Status
Server
Interface
Tunnel IP
Client #1
Up
10.0.0.1:1194
vpntest
10.20.10.1
Server #1
ListenTCP
192.168.1.1:1717
openvpn
10.20.12.1
OPENVPN™

Пропускная способность

Название протокола туннелирования Измерения пропускной способности	PPTP	L2TP/IPSec	OpenVPN
1 измерение	28,23	95,01	61,96
2 измерение	31,56	95,11	83,02
3 измерение	28,97	95,22	84,00
4 измерение	28,35	95,04	89,87
5 измерение	26,99	95,18	87,02
Среднее значение	28,821	95,112	81,174

Заключение

В курсовой работе произвели сравнительный анализ наиболее распространённых протоколов, используемых для построения VPN соединений

Были выполнены поставленные задачи по курсовой работе:

- Произвели обзор наиболее распространённых протоколов для построения VPN;
- Произвели анализ наиболее распространенных протоколов для построения VPN;
- Сравнили наиболее распространенные протоколы для построения VPN