

Сравнительный анализ протоколов построения виртуальных частных сетей.

Выполнил: Студент группы ИТСб-141

Етерсков Иван Александрович

Научный руководитель: Ст.преп.кафедры
ТКС Тюхтяев Д. А.

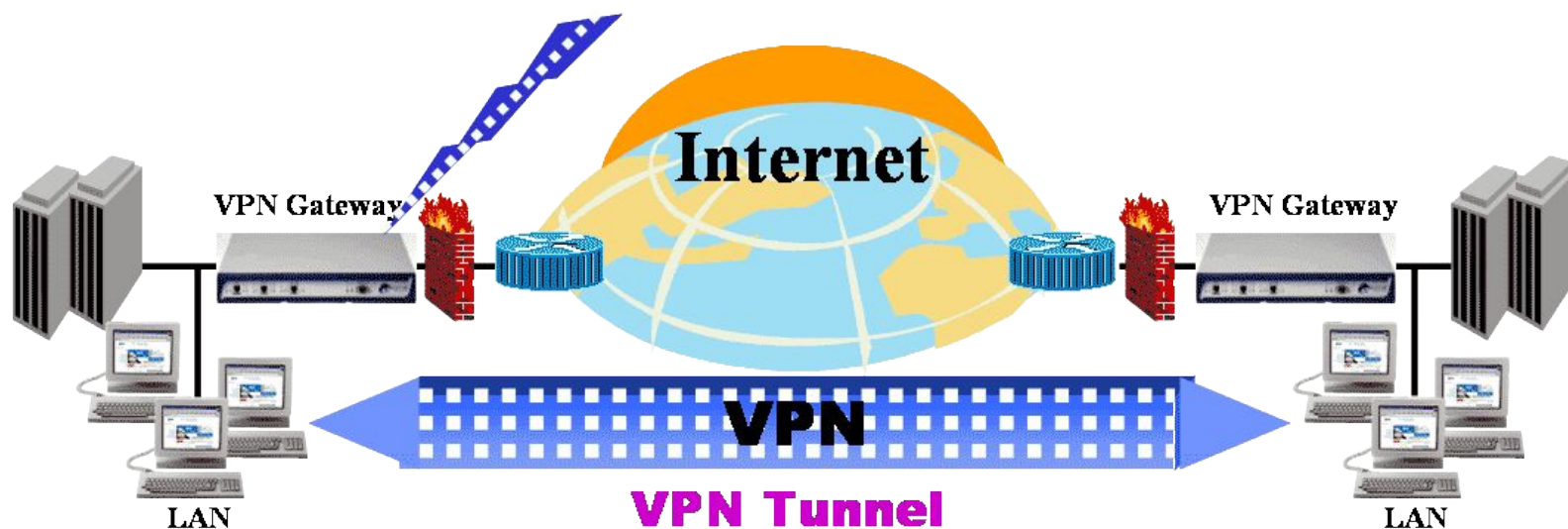
Цель работы:

- 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 распространённых протоколов для построения VPN;
- Сравнить наиболее распространённые 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 в интернете



VPN Сеть предприятия

Классификация VPN протоколов

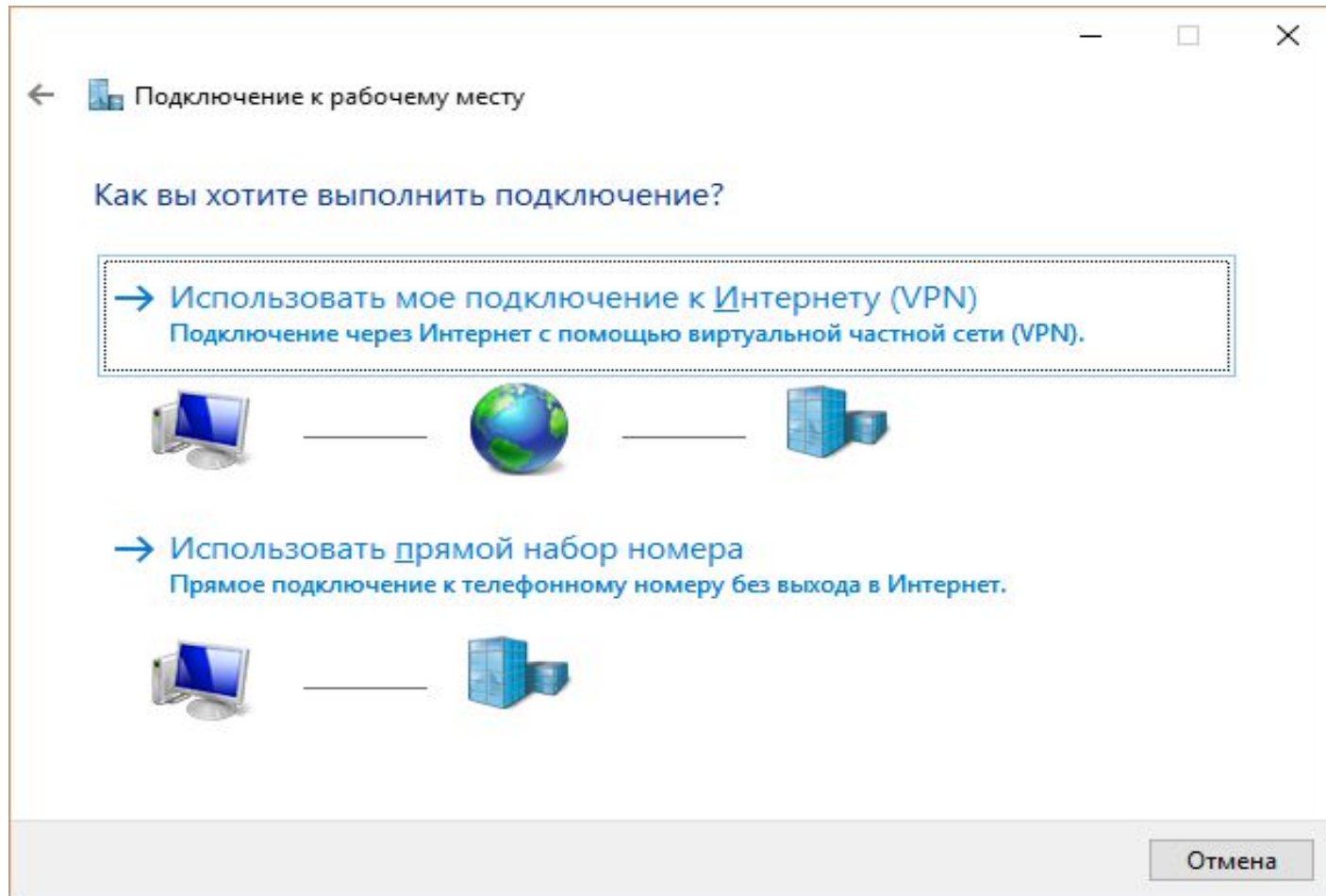
- В современных условиях развития IT-технологий преимущества использования VPN неоспоримы. VPN сеть позволяет защитить информацию во время ее передачи по незащищенной Всемирной сети Интернет. Существует несколько способов классификации VPN- решений. Ниже рассмотрены те, которые чаще всего используются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

localhost (This server) - SoftEther VPN Server Manager

Manage VPN Server "localhost"

Virtual Hub Name	Status	Type	Users	Groups	Sessions	MAC Tables	IP Tables
VPN	Offline	Standalone	1	0	0	0	0

< >

Manage Virtual Hub Online Offline View Status Create a Virtual Hub Properties Delete

Management of Listeners:
Listener List (TCP/IP port):

Port Number	Status
TCP 443	Listening
TCP 992	Listening
TCP 1194	Listening
TCP 5555	Listening

Create Delete Start Stop

VPN Server and Network Information and Settings:

- Encryption and Network
- View Server Status
- About this VPN Server
- Clustering Configuration
- Clustering Status
- Show List of TCP/IP Connections
- Edit Config

Local Bridge Setting Layer 3 Switch Setting IPsec / L2TP Setting OpenVPN / MS-SSTP Setting

Dynamic DNS Setting VPN Azure Setting VPN Gate Setting Refresh Exit

Current DDNS Hostname: vpn154013389.softether.net

OpenVPN



Пропускная способность

Измерения пропускной способности	Название протокола туннелиро вания	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 распространённых протоколов для построения VPN;
- Сравнили наиболее распространённые протоколы для построения VPN