

MINISTERUL EDUCAȚIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Calculatoare Informatică și Microelectronică
Departamentul Ingineria Software și Automatică

Admis la susținere
Șef de departament:
Fiodorov I. dr., conf. univ.

„_____” _____ **2021**

Analiza și compararea protocoalelor VPN pentru construirea unei rețele corporative

Teza de master

Student: _____ **Cusnir Vladislav, TI-201M**

Conducător: _____ **Chirev Pavel, lect.univ, dr.**

Consultant: _____ **Cojocarul Svetlana, lect. univ.**

Chișinău, 2022

Аннотация

В данной работе проводилось исследование существующих на сегодняшний день протоколов VPN, их теоретическое сравнение, а также был приведен пример настройки протокола который был выделен в качестве более оптимального решения.

Были проанализированы существующие протоколы, такие как open-source, так и платные решения. В конечном итоге был выбран протокол который имеет больше положительных сторон и приведен пример настройки данного протокола.

Rezumat

În această lucrare a fost realizat un studiu al protocoalelor VPN existente în prezent, compararea lor teoretică și, de asemenea, a fost dat un exemplu de înființare a unui protocol, care a fost evidențiat ca o soluție mai optimă.

Au fost analizate protocoalele existente, cum ar fi soluțiile open-source și plătite. În final s-a ales un protocol care are mai multe aspecte pozitive și este dat un exemplu de înființare a acestui protocol.

Abstract

In this work, a study of the currently existing VPN protocols was carried out, their theoretical comparison, and also an example of setting up a protocol was given, which was highlighted as a more optimal solution.

Existing protocols such as open-source and paid solutions were analyzed. In the end, a protocol was chosen that has more positive aspects and an example of setting up this protocol is given.

Содержание

ВВЕДЕНИЕ	9
1 ИЗУЧЕНИЕ ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ СЕТИ	10
1.1 Угрозы информационной безопасности.....	10
1.2 Анализ методов обеспечения безопасности корпоративной сети.....	10
1.2.1 Межсетевые экраны	10
1.2.2 Система обнаружения атак.....	12
1.2.3 Виртуальная частная сеть.....	13
2 АНАЛИЗ СПОСОБА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ СЕТИ С ПОМОЩЬЮ ПРОТОКОЛОВ VPN	14
2.1 Исследование принципов работы VPN	14
2.2 Виды VPN в интернете	16
2.2.1 VPN удаленного доступа.....	16
2.2.2 Интранет VPN.....	17
2.2.3 Экстранет VPN	18
2.3 Технология VPN.....	19
2.3.1 Сеть VPN основанная на протоколе IPSec	20
2.3.2 Сеть VPN основанная на протоколе SSL.....	21
2.4 Обоснование использования протоколов VPN для обеспечения безопасности корпоративной сети.....	24
2.5 Средства построения сетей VPN	24
2.6 Обзор существующих программных решений VPN.....	26
2.6.1 ПК Застава.....	26
2.6.2 Шлюза безопасности ViPNet Coordinator	27
2.6.3 КриптоПро IPSec	29
2.6.4 Сеть VPN на основе Cisco System	29
3 OPENVPN КАК ЛУЧШЕЕ РЕШЕНИЕ ДЛЯ КОРПОРАТИВНЫХ VPN СЕТЕЙ.....	30
3.1 Выбор технологии и содержание главы.....	30
3.2 Описание технологии OpenVPN	30
3.3 Состав программы OpenVPN	34
3.4 Пример настройки OpenVPN	35

3.4.1 Создание сертификатов	35
3.4.2 Пример настройки серверов и клиентов	38
3.4.3 Отзыв сертификата клиентов	48
ЗАКЛЮЧЕНИЕ.....	50
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	51

Введение

В наше время, корпоративная информация очень часто передается в электронном виде, как правило для этого используются электронные почты. Благодаря тому, что данная информация передается через открытую сеть, есть риск перехвата данных злоумышленниками и в последствии чего использование этих данных в корыстных целях. Информация, которая передается компаниями для работ и прочих потребностей можно отнести к информации, которая может содержать персональные и корпоративные данные.

Безопасность корпоративной сети прежде всего актуально для компаний с многоуровневой структурой, к примеру, государственные компании и банки. Так как при обмене данными или передачей данных в другие компании или с внешним миром, данные могут быть выкрадены, при помощи вредоносных программ.

Самую большую опасность представляют вредоносные программы по типу троянских коней, червей, спама, фишинг-атак, подмены страниц интернет ресурсов и социальной инженерии.

Таким образом, главной задачей для любой информационной системы является:

- обеспечение конфиденциальной информации;
- целостность информации, и ее защищённость от несанкционированного уничтожения или изменения.

Целью работы являются анализ и сравнение VPN протоколов для обеспечения безопасности для компаний и корпораций. Выбрана данная работа для выявления оптимального и лучшего решения построения сетей с целью предотвратить проблемы с кражей лично информации и атак на бизнес-компаниями. Для достижения поставленной цели будут рассмотрены следующие разделы.

- изучение области обеспечения безопасности корпоративной сети;
- анализ методов обеспечения безопасности корпоративной сети;
- анализ способа обеспечения безопасности корпоративной сети с помощью протоколов VPN;
- обоснование использования протоколов VPN для обеспечения безопасности корпоративной сети.

Список использованных источников

1. DJERRY LOW: Виртуальная частная сеть (VPN). [цитирован 07.10.21] – Режим доступа: <https://www.webhostingsecretrevealed.net/ru/the-a-to-z-vpn-guide/>
2. SMART-SOFT: Межсетевые экраны – виды и особенности. [цитирован 07.10.21] – Режим доступа: <https://www.smart-soft.ru/blog/mezhsetevye-ekrany-vidy/>
3. JOEL TIMOTHY: IPSEC против SSL: какой протокол VPN лучше для вас. [цитирован 08.10.21] – Режим доступа: <https://vpn.inform.click/ipsec-protiv-ssl-kakoi-protokol-vpn-luchshe-dlya-vas/>
4. NIKOLAY TERESHCHENKO: SSL VPN – шаг вперед в технологии VPN сетей. [цитирован 10.10.21] – Режим доступа: <https://www.anti-malware.ru/node/449>
5. SERGIY UVAROV: Что такое OpenVPN. [цитирован 01.11.21] – Режим доступа: <https://openmaniak.com/ru/openvpn.php>
6. ORACLE-PATCHES: Руководство по IPTables: как это работает. [цитирован 02.11.21] – Режим доступа: <https://oracle-patches.com/os/руководство-по-iptables-как-это-работает-понятное-объяснение-с-примерами>
7. OPENVPN: Официальная документация OpenVPN. [цитирован 05.11.21] – Режим доступа: <https://openvpn.net/community-resources/>
8. ALEXANDRE FROLOV: Руководство по установке и настройке OpenVPN. [цитирован 06.12.21] – Режим доступа: <https://habr.com/ru/post/233971/>
9. PETE ZABORSZKY: PPTP vs L2TP vs OpenVPN vs SSTP. [цитирован 06.12.21] – Режим доступа: <https://habr.com/ru/post/191874/>
10. LOSST: Маршрутизация в Linux. [цитирован 07.12.21] – Режим доступа: <https://losst.ru/marshrutizatsiya-v-linux>