MINISTERUL EDUCAŢIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei

Facultatea Calculatoare Informatică şi Microelectronică

Departamentul Ingineria Software și Automatică

Admis la susţinere
Şef departament:
FIODOROV Ion, conf. univ., dr.

_____

„__”_____ 2024

ANALIZA UNUI SISTEM DE ACCES PE GRUPURI DE UTILIZATORI ÎN CADRUL UNEI REȚELE DE COMUNICAȚII

Teză de master

Student: **BURDUJA Sergiu , gr. TIA-221M**

Conducător: **ȚURCANU Dinu, conf. univ. dr.**

Consultant: **COJOCARU Svetlana, asist. univ.**

Chişinău, 2024

АННОТАЦИЯ

Работа содержит 56 страниц: введение; глава 1: Анализ протоколов, используемых в сети поставщика услуг; глава 2: Разработка структуры и оптимизация сети поставщика услуг; глава 3: Проектирование и реализация сети поставщика услуг; заключение, библиография

Дипломный проект представляет собой комплексное исследование, направленное на оптимизацию сетевой инфраструктуры и усиление защиты от кибератак в сети провайдера услуг. Основная цель работы — изучение современных протоколов и методов оптимизации сетевых процессов с целью повышения эффективности и безопасности сети.

Работа начинается с анализа динамической маршрутизации и протокола переключения меток, включая исследование принципов сегментации сети и безопасности. Также рассматриваются аспекты виртуальных частных сетей и централизованного доступа пользователей по группам.

В проекте предлагаются решения для оптимизации сети провайдера, такие как внедрение технологии QinQ и оптимизация виртуального маршрутизационного протокола. Улучшение управления связями L2 и эффективизация протокола маршрутизатора-отражателя (IBGP) также рассматриваются как средства для достижения более стабильной и надежной сети.

Финальный раздел посвящен проектированию конфигурации сети и реализации централизованной системы доступа по группам пользователей. Исследование направлено на разработку эффективных методов управления и повышения безопасности сети.

Работа сопровождается вспомогательными материалами, включая таблицы и иллюстрации, что обеспечивает более глубокий анализ и обоснование предложенных решений. Список используемых источников демонстрирует основательный и обширный подход к исследованию.

ADNOTARE

Lucrarea constă din 56 de pagini: introducere; capitolul 1: Analiza protocoalelor utilizate în rețeaua furnizorului de servicii; capitolul 2: Dezvoltarea și optimizarea structurii rețelei furnizorului de servicii; capitolul 3: Proiectarea și implementarea rețelei furnizorului de servicii; concluzie, bibliografie.

Proiectul de diplomă este o investigație complexă, cu scopul de a optimiza infrastructura de rețea și de a consolida protecția împotriva atacurilor cibernetice în rețeaua furnizorului de servicii. Scopul principal al lucrării este de a studia protocoalele moderne și metodele de optimizare a proceselor de rețea pentru a îmbunătăți eficiența și securitatea rețelei.

Lucrarea începe cu analiza rutării dinamice și a protocolului de comutare a etichetelor, inclusiv investigarea principiilor de segmentare a rețelei și de securitate. De asemenea, sunt examinate aspectele legate de rețelele private virtuale și accesul centralizat al utilizatorilor pe grupuri.

În cadrul proiectului sunt propuse soluții pentru optimizarea rețelei furnizorului, cum ar fi implementarea tehnologiei QinQ și optimizarea protocolului de rutare virtuală. De asemenea, se examinează îmbunătățirea managementului legăturilor L2 și eficientizarea protocolului de rutare inter-BGP (IBGP) ca mijloace pentru a asigura o rețea mai stabilă și mai fiabilă.

Secțiunea finală este dedicată proiectării configurației rețelei și implementării unui sistem centralizat de acces pe grupuri de utilizatori. Investigarea vizează dezvoltarea de metode eficiente de gestionare și sporire a securității rețelei.

Lucrarea este însoțită de materiale auxiliare, inclusiv tabele și ilustrații, care asigură o analiză mai profundă și o justificare a soluțiilor propuse. Lista surselor utilizate demonstrează o abordare temeinică și extinsă a cercetării.

ANNOTATION

The paper consists of 56 pages: introduction; chapter 1: Analysis of protocols used in the service provider network; chapter 2: Development and optimization of the service provider network structure; chapter 3: Design and implementation of the service provider network; conclusion, bibliography.

The diploma project represents a comprehensive investigation aimed at optimizing the network infrastructure and strengthening protection against cyber attacks in the service provider network. The main goal of the work is to study modern protocols and methods for optimizing network processes to improve the efficiency and security of the network.

The work begins with an analysis of dynamic routing and label switching protocols, including an investigation of network segmentation and security principles. Also examined are aspects of virtual private networks and centralized user access by groups.

The project proposes solutions for optimizing the service provider network, such as implementing QinQ technology and optimizing the virtual routing protocol. Improving L2 link management and streamlining the Inter-BGP (IBGP) routing protocol are also considered means to achieve a more stable and reliable network.

The final section is dedicated to designing the network configuration and implementing a centralized user group access system. The research aims to develop effective network management methods and enhance network security.

The work is accompanied by supporting materials, including tables and illustrations, which provide a deeper analysis and justification of the proposed solutions. The list of sources used demonstrates a thorough and comprehensive approach to research.

СОДЕРЖАНИЕ

СОКРАЩЕНИЯ

ISP- Internet Service Provider

IP- Internet Protocol

OSI- Open Systems Interconnection

MAC -Media Access Control

DDoS - Distributed Denial of Service

BGP- Border Gateway Protocol

AS- Autonomous System

OSPF- Open Shortest Path First

TCP- Transmission Control Protocol

iBGP - Internal Border Gateway Protocol

eBGP- External Border Gateway Protocol

MPBGP- Multi-Protocol BGP

AFI- Address Family Identifier

SAFI- Subsequent Address Family Identifier

DR -Designated Router

BDR- Backup Designated Router

MPLS- Multiprotocol Label Switching

LDP- Label Distribution Protocol

VLAN- Virtual Local Area Network):

STP- Spanning Tree Protocol

LACP- Link Aggregation Control Protocol

AAA- Authentication, Authorization, and Accounting

VRF- Virtual Routing and Forwarding

ВВЕДЕНИЕ

Тема **анализ системы доступа по группам пользователей в рамках сети связи** имеет высокую важность по следующим причинам:

Управление доступом и безопасность

Централизованная система доступа обеспечивает аутентификацию и авторизацию пользователей перед предоставлением доступа к сетевым ресурсам, что важно для защиты сети от несанкционированного доступа и вредоносных атак.

Можно реализовать механизмы контроля доступа на основе политик, определяющих права и привилегии для различных групп пользователей в зависимости от их ролей и функций в сети.

Оптимизация управления ресурсами

Централизованная система управления доступом позволяет более эффективно распределять и управлять сетевыми ресурсами, включая управление пропускной способностью, каналами связи, IP-адресами и другими ресурсами.

Путем назначения доступа к ресурсам на основе групп пользователей провайдер может лучше управлять нагрузкой на сеть, избегать перегрузок и оптимизировать использование имеющихся ресурсов.

Удобство администрирования и мониторинг

Централизованная система управления обеспечивает единую точку входа для администраторов, что облегчает управление правами доступа, а также мониторинг и анализ активности пользователей;

Инструменты аудита и журналирования позволяют провайдеру отслеживать действия пользователей, выявлять аномалии и реагировать на потенциальные угрозы безопасности.

Соблюдение нормативных требований

Во многих странах мира, таких как США, страны ЕС, Канада, Япония и другие, существуют законодательные и нормативные требования к обеспечению безопасности и конфиденциальности данных в сети, и централизованная система доступа может помочь провайдерам соответствовать этим требованиям, предоставляя контроль и прозрачность в использовании данных.

Все эти аспекты делают централизованную систему доступа по группам пользователей важным инструментом для обеспечения безопасности, эффективности и соблюдения законодательства в сетях интернет-провайдеров.

БИБЛИОГРАФИЯ

1- Raymond Lacoste, Kevin Wallace: *CCNP Routing and Switching TSHOOT 300-135 Official*

2- https://www.arubanetworks.com/techdocs/ClearPass/6.7/Aruba_DeployGd_HTML/Content/802.1X%20Authentication/About_AAA.htm

3- https://habr.com/ru/post/301468/

4- https://en.wikipedia.org/wiki/Border_Gateway_Protocol

5- https://www.geeksforgeeks.org/open-shortest-path-first-ospf-protocol-fundamentals/

6- https://www.geeksforgeeks.org/open-shortest-path-first-ospf-protocol-states/

7- https://www.juniper.net/documentation/en_US/junos/topics/topic-map/mpls-overview.html

8- https://www.juniper.net/documentation/en_US/junos/topics/concept/mpls-security-overview.html

9- https://www.juniper.net/documentation/en_US/junos/topics/topic-map/ldp-overview.html#id-label-operations

10- https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r6-2/lxvpn/configuration/guide/b-l2vpn-cg-asr9000-62x/b-l2vpn-cg-asr9000-62x_chapter_0101.html

11- https://techhub.hpe.com/eginfolib/networking/docs/switches/3600v2/5998-7619r_l3-ip-rtng_cg/content/442284574.htm

12- https://www.juniper.net/documentation/en_US/junos/topics/topic-map/l3-vpns-overview.html

13- https://www.juniper.net/documentation/en_US/junos/topics/example/overview-port-security.html#id-port-security-features

14- https://support.huawei.com/enterprise/en/doc/EDOC1100055021/76ac1ea4/overview-of-qinq

15- https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/vrf/design/guide/vrfDesignGuide.html

16- Implementing Cisco IP Routing Foundation Learning Guide, Diane Teare, Bob Vachon, Rick Graziani, 2015 p597

17- https://www.juniper.net/documentation/en_US/junos/topics/topic-map/bgp-rr.html

18- https://www.geeksforgeeks.org/port-security-in-computer-network/

19- https://www.akadia.com/services/firewall_proxy_server.html

20- https://support.huawei.com/enterprise/en/doc/EDOC1100055021/efa54f1e/summary-of-qinq-configuration-tasks

21- https://infocenter.nokia.com/public/7750SR202R1A/index.jsp?topic=%2Fcom.sr.unicast%2Fhtml%2Fospf_config.html

22- https://tacacsgui.com/documentation/installation/manual/