Universitatea Tehnică a Moldovei

Analiza și proiectarea rețelei optimale de comunicații securizate pentru prestatorul de servicii internet (segmentul transport de date a clienților)

Student: **Iepure Marin**

Conducător: **dr. conf. univ. Țurcanu Tatiana**

Chișinău, 2020

MINISTERUL EDUCAȚIEI, CULTURII ȘI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei

Facultatea Electronică și Telecomunicații

Departamentul Telecomunicații și Sisteme electronice

Admis la susținere

Șef departament: Sava Lilia, conf. univ,. dr.,

_____

"___" _____2020

Analiza și proiectarea rețelei optimale de comunicații securizate pentru prestatorul de servicii internet (segmentul transport de date a clienților)

Teză de master

Student: **_____** **Iepure Marin**

Conducător: **_____** **dr. conf. univ. Țurcan Tatiana**

Chișinău, 2020

REZUMAT

Iepure Marin

Tema: Analiza si proiectarea rețelei optimale de comunicații securizate pentru prestatorul de servicii internet (segmentul transport de date a clienților)

Structura lucrării: Introducere; Capitolul 1: Analiza protocoalelor utilizate în rețeaua prestatorului de servicii; Capitolul 2: Elaborarea structurii și optimizarea rețelei prestatorului de serviciu; Capitolul 3: Proiectarea și implementarea rețelei prestatorului de serviciu; Concluzii, Bibliografia; Anexa1.

Cuvintele-Cheie: rețelei de comunicații, proiectarea, securitatea, optimizarea.

Scopul lucrării: Analiza și proiectarea rețelei optimale de comunicații securizate pe segmentul transport de date a clienților.

Obiectivele: Analiza protocoalelor utilizate în rețelele echipamentelor IT și tehnologiilor necesare pentru a avea posibilitate de asigura omiterii dependenței de producător; Proiectarea infrastructurii rețelei optimale cu o posibilitate de extindere; Utilizarea protocoalelor de securizare a rețelei pe nivelele 2 și 3 ale stivei OSI; Implementarea și analiza disponibilității serviciilor prestate; Implementarea sistemelor împotriva atacurilor cibernetice de tip DDoS; Implementarea sistemului centralizat de oferire a accesului pe grupuri de utilizatori.

Metodele aplicate: Conform protocolului standardizat EGP (exterior gateway protocol) s-a aplicat protocoalele BGP, OSPF, MPLS, LDP și RPVST+, tehnologiile VLAN, EtherChannel, L2VPN, L3VPN,QinQ, VRF și IPS, cât și aplicația TACACSGUI pentru a gestiona controlul utilizatorilor care accesează echipamentele de rețea.

Rezultatele obținute: Analizând toate protocoalele Open Source s-a depistat că este posibilitate de a interconecta echipamente de producători diferiți ce ne oferă o flexibilitate pentru proiectarea și optimizarea rețelei. Pentru a efectuarea proiectarea infrastructurii rețelei s-a dus cont de echipamente modulare care suportă tehnologia Stackwise ce permite extinderea rețelei. Pentru securizarea rețelei și izolarea traficului la nivelul de acces au fost aplicate diferite mecanisme de protejare, cum ar fi: limitarea numărului de MAC pe porturi, limitarea traficului excesiv de tip broadcast/multicast, BPDU GUARD, dezactivarea recepționarea și transmiterii mesajelor de către CDP, LLDP sau alte protocoale de descoperire a vecinelor. Pentru a asigura transportul de date L2 și a omiterea dependenței de numărul de Vlan-uri a fost implementat tehnologia QinQ sau/și L2VPN. Pentru transportul de date IP a fost utilizat L3VPN, din acest motiv clienții au posibilitate de a dezvălui infrastructurile proprii. Protejarea rețeaua împotriva atacurilor DDoS a fost posibila prin aplicarea tehnologiei IPS. Implementarea sistemului centralizat de oferire a accesului pe grupuri de utilizatori a fost posibilă prin instalarea a aplicației TACACSGUIE.

SUMMARY

Iepure Marin

Theme: Analysis and design of the optimal secure communications network for the internet service provider (customer data transport segment).

Structure: Introduction; Chapter 1: Analysis of the protocols used in the service provider's network; Chapter 2: Development of the structure and optimization of the service provider's network; Chapter 3: Design and implementation of the service provider's network; Conclusions, Bibliography; Annex1.

Key words: communications networks, design, security, optimization.

The purpose of the works.: Analysis and design of the optimal secure communications network on the customer data transport segment.

The objectives: Analysis of the protocols used in the networks of IT equipment and technologies necessary to have the possibility to ensure the omission of the manufacturer's dependence; Designing the optimal network infrastructure to be able to expand it; Use of network security protocols on levels 2 and 3 of the OSI stack; Implementation and analysis of the availability of services provided; Implementation of systems against DDoS cyber-attacks; Implementing the centralized system for providing access to user groups.

Applied methods: According to the standardized EGP protocol (external gateway protocol), the BGP, OSPF, MPLS, LDP and RPVST + protocols, VLAN, EtherChannel, L2VPN, L3VPN, QinQ, VRF and IPS technologies were applied, as well as the TACACSGUI application to manage the control of users accessing the equipment. network.

The results obtained are as follows: Analyzing all Open Source protocols, it was found that it is possible to interconnect equipment from different manufacturers that gives us flexibility for network design and optimization. In order to carry out the design of the network infrastructure, modular equipment was taken into account that supports the Stackwise technology that allows the extension of the network**.** Various protection mechanisms have been applied to secure the network and isolate traffic at the access level, such as: limiting the number of MACs on ports, limiting excessive broadcast / multicast traffic, BPDU GUARD, disabling the reception and transmission of messages by CDP, LLDP or other neighbor discovery protocols. In order to ensure the transport of L2 data and to avoid the dependence on the number of VLans, the QinQ and / or L2VPN technology was implemented. L3VPN was used for IP data transport, for this reason customers have the opportunity to disclose their own infrastructure. Protecting the network against DDoS attacks was made possible by applying IPS technology. The implementation of the centralized

system for providing access to user groups was possible by installing the application TACACSGUIE.

CUPRINS

INTRODUCERE

Odată cu dezvoltarea rețelelor de calculatoare a apărut necesitatea de a le interconecta la distanțe mari. În timp ce numărul companiilor Mari și Mici crește o sarcină de bază a unui prestator de servicii internet are scopul de a avea o infrastructură care ar asigura toate necesitățile clienților. Ca până la fine să asigure calitatea și varietatea serviciilor prestate, rețeaua companiei trebuie să fie dotată cu echipament actualizat la zi și platformele trebuie să dispună de sisteme de operare care ar putea să ruleze protocoalele necesare.

Din aceste considerente **scopul tezei de master este: Analiza și proiectarea rețelei optimale de comunicații securizate pe segmentul transport de date a clienților**.

Pentru a atingerea scopului trebuie de rezolvat următoarele **obiectivele:**

1. Analiza protocoalelor utilizate în rețelele echipamentelor IT și tehnologiilor necesare pentru a avea posibilitate de asigura omiterii dependenței de producător.
2. Proiectarea infrastructurii rețelei optimale pentru a avea posibilitate de a o extinde.
3. Utilizarea protocoalelor de securizare a rețelei pe nivelele 2 și 3 ale stivei OSI.
4. Implementarea și analiza disponibilității serviciilor prestate clienților, cum ar fi:
   a. Acces la resursele Internet.
   b. Asigurarea canalului de legătură și acces la serviciile de schimb informațional protejat între departamente pentru clienți (Intranet).
   c. Asigurarea canalului de legătură securizat la nivel de IP.
   d. Asigurarea transportului de date pe nivelul de MAC.
5. Implementarea sistemelor împotriva atacurilor cibernetice de tip DDoS.
6. Implementarea sistemului centralizat de oferire a accesului pe grupuri de utilizatori.

În baza configurărilor esențiale vom studia vulnerabilitățile existente, pentru a omite lacunele de securitate în rețea. La baza efectuării acestei lucrări va fi o rețea tipică, în baza căreia vom aplica cele mai bune practici de organizare a unei rețele de echipamente și vom cerceta posibilele vulnerabilități pentru a putea securiza rețeaua. Vom atrage atenție și la protocoalele utilizate și scenariul lor specific de configurare pe diferite echipamentele a diferitor producători.

Noțiunea de securitatea este un aspect foarte important într-o organizație și extrem de important în o rețea se prestator de servicii internet, din acest motiv ne vom axa pe metodele de securitate pentru fiecare nivel ierarhic. Totodată analiza și aplicarea a metodelor ce ne permite utilizarea sistemului centralizat de oferire a permisiunilor diferitor grupuri de utilizatori care sunt responsabili de gestionarea echipamentelor de rețea.

Bibliografia

1. Raymond, Lacoste, Kevin, Wallace: *CCNP Routing and Switching TSHOOT 300-135 Official Cert Guid.* SUA: Indianapolis, 2015 172-205p. ISBN-978-1-58720-561-3

2. Aruba Networks: What is AAA, © 2018, [citat 24.09.2020]. Disponibil: https://www.arubanetworks.com/techdocs/ClearPass/6.7/Aruba_DeployGd_HTML/Default.htm#802.1X%20Authentication/About_AAA.htm

3.Wikipedia: FreeRadius, © 26 mart 2020, [citat 19.09.2020]. Disponibil: https://en.wikipedia.org/wiki/FreeRADIUS

4. Habra: Графический интерфейс к демону tacacs- TacacsGUI, © 23 mai 2016, [citat 15.09.2020]. Disponibil: https://habr.com/ru/post/301468/

5. **Wikipedia: Border Gateway Protocol**, © 27 noiembrie 2020, [citat 05.10.2020]. Disponibil: https://en.wikipedia.org/wiki/Border_Gateway_Protocol

6. GeeksforGeeks: Open Shortest path first (OSPF) Protocol fundamentals, © 09 august 2019, [citat 06.10.2020]. Disponibil: https://www.geeksforgeeks.org/open-shortest-path-first-ospf-protocol-fundamentals/

7. GeeksforGeeks: Open Shortest path first (OSPF) Protocol States, © 14 mai 2020, [citat 06.10.2020]. Disponibil: https://www.geeksforgeeks.org/open-shortest-path-first-ospf-protocol-states

8. Juniper Networks: MPLS Overview. © 29 septembrie 2020, [citat 17.10.2020]. Disponibil: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/mpls-overview.html

9. Juniper Networks: MPLS Overview, © 22 decembrie 2019, [citat 17.10.2020].

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

10. Juniper Networks: LDP Overview, © 29 septembrie 2020, [citat 17.10.2020]. Disponibil: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/ldp-overview.html#id-label-operations

11. Cisco: L2VPN and Ethernet Services Configuration Guide for Cisco ASR 9000 Series Routers, IOS XR Release 6.2.x © 11 septembrie 2020, [citat 20.10.2020]. Disponibil: 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

12. Techhub: MPLS L3VPN overview, ©2016, [citat 20.10.2020]. Disponibil: https://techhub.hpe.com/eginfolib/networking/docs/switches/3600v2/5998-7619r_l3-ip-rtng_cg/content/442284574.htm

13. Juniper Networks: Layer 3 VPNs User Guide for Routing Devices © 05 decembrie 2019, [citat 20.10.2020].

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

14.Juniper Networks: Overview of Port Security, ©24 septembrie 2020, [citat 21.10.2020].

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

15. Huawei: This is NE40E V800R010C10SPC500 Configuration Guide - LAN Access and MAN Access, Overview of QinQ, © 01 martie 2019, [citat 21.10.2020]. Disponibil: https://support.huawei.com/enterprise/en/doc/EDOC1100055021/76ac1ea4/overview-of-qinq

16. Cisco: Virtual Route Forwarding Design Guide, © 12 noiembrie 2008, [citat 25.10.2020]. Disponibil:https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/vrf/design/guide/vrfDesignGuide.html

17. Diane, Teare, Bob, Vachon, Rick, Graziani: *CCNP Route 300-101 Official Cert Guide.* SUA: Indianapolis. 2015 385-387p. ISBN: 978-1-58720-456-2

18. Juniper Networks: BGP Route Reflectors, © 29 septembrie 2020, [citat 26.10.2020]. Disponibil: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/bgp-rr.html ¶

19. GeeksforGeeks: Port Security in Compuer Network, © 09 august 2019, [citat 21.10.2020]. Disponibil: https://www.geeksforgeeks.org/port-security-in-computer-network/

20. Akadia Global Comopetence in Today's Information Tehnology :What is a firewall proxy server?, ©2020, [citat 16.10.2020].

Disponibil: https://akadia.com/services/firewall_proxy_server.html

21- Huawei: This is NE40E V800R010C10SPC500 Configuration Guide - LAN Access and MAN Access, Summary of QinQ Configuration Tasks, © 01 martie 2019, [citat 21.10.2020]. Disponibil: https://support.huawei.com/enterprise/en/doc/EDOC1100055021/efa54f1e/summary-of-qinq-configuration-tasks

22- Nokia: Manual: Unicast Routing Protocols Guide 20.0.R1>3.OSPF, ©2020 [citat 21.11.2020]. Disponibil:https://infocenter.nokia.com/public/7750SR202R1A/index.jsp?topic=%2Fcom.sr.unicast%2Fhtml%2Fospf_config.html

23. TacacsGui: Manual Installation. Section Content, ©2020, [citat 25.11.2020]. Disponibil: https://tacacsgui.com/documentation/installation/manual/