



Universitatea Tehnică a Moldovei

**Analiza și proiectarea rețelei optime de comunicații
securizate pentru prestatorul de servicii internet (la
nivelul rețelei corporative)**

Student:

Plămădeală Virginia

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 optime de comunicații securizate pentru
prestatorul de servicii internet (la nivelul rețelei corporative)**

Teză de master

Student: _____ **Plămădeală Virginia**

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

Chișinău, 2020

REZUMAT

Plămădeală Virginia

Tema: Analiza și proiectarea rețelei optimale de comunicații securizate pentru prestatorul de servicii internet (la nivelul rețelei corporative)

Structura lucrării: Introducere; Capitolul 1: Analiza nivelele ierarhice de proiectare a unei rețele; Capitolul 2: Elaborarea structurii și optimizarea rețelei corporative; Capitolul 3: Proiectarea și implementarea rețelei corporative; Concluzii, Bibliografia; Anexa 1.

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

Scopul lucrării: Analiza și proiectarea rețelei optimale de comunicații securizate la nivelul rețelei corporative.

Obiectivele: Analiza protocoalelor și tehnologiilor necesare pentru a avea posibilitate de a asigura omiterii dependenței de producător; Elaborarea și proiectarea infrastructurii rețelei optimale cu posibilitate de extindere; Implementarea și analiza disponibilității serviciilor prestate la nivel de campus; Analiza și implementarea sistemelor de monitorizare a echipamentele de rețea.

Metodele aplicate: Conform setului de practici ITIL (Information Technology Infrastructure Library) s-a aplicat concepțiile metodelor nivelelor ierarhice al rețelei de echipamente, care este format din nivelul de acces, distribuție și core. Prin aplicarea tehnologiilor VLAN, Stackwise, IPS și NGFW, protocoalele LACP, RPVST+, NAT, DHCP și Isec. Implementând aplicațiile The Dude și Cacti pentru monitorizarea rețelei.

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. Proiectarea și optimizarea rețelei s-a efectuat în baza cerințelor. Pentru Disponibilitatea rețelei s-a folosit tehnologia High Availability (HA) ce n-ea oferit evitarea pierderilor serviciilor prin reducerea sau gestionarea eșecurilor și minimizarea timpului de nefuncționare planificată și cazul unui eșec. Pentru scalabilitatea rețelei s-a folosit echipamentele modulare care au posibilitate de a fi actualizate fără a stopa serviciile. În cerințele de securitatea rețelei s-a implementat sistemul de prevenire a intruziunilor (IPS). Pentru a obține o rețea convergentă pentru a presta a mai multor servicii de transport de date prin aceeași infrastructură s-a folosit tehnologia VLAN în combinație cu utilizarea protocolului din familia spanning-tree RPVST+ . Accesul la resursele Internet au fost oferite prin implementarea mecanismului NAT ce translează mai multe IP adrese private (RFC 1918) în una sau mai multe IP publica (globale).

S-a implementat sisteme de monitorizare de tip activ și pasiv, pentru a avea mecanisme de reacție care informează imediat administratorul.

SUMMARY

Plămădeală Virginia

Theme: Analysis and design of the optimal secure communications network for the internet service provider (at the level of the corporate network).

Structure: Introduction; Chapter 1: Analysis of hierarchical levels of network design; Chapter 2: Elaboration of the structure and optimization of the corporate network; Chapter 3: Design and implementation of the corporate network; Conclusions, Bibliography; Annex 1.

Cuvintele-Cheie: communications network, design, security, optimization.

The purpose of the works: Analysis and design of the optimal secure communications network at the level of the corporate network.

The objectives: Analysis of the necessary protocols and technologies in order to be able to ensure the omission of the manufacturer's dependence; Elaboration and design of the optimal network infrastructure with the possibility of extension; Implementation and analysis of the availability of services provided at campus level; Analysis and implementation of network equipment monitoring systems.

Applied methods: According to the ITIL (Information Technology Infrastructure Library) set of practices, the concepts of the methods of the hierarchical levels of the equipment network were applied, which consists of the level of access, distribution and core. By applying VLAN, Stackwise, IPS and NGFW technologies, LACP, RPVST +, NAT, DHCP and Ipsec protocols. Implementing The Dude and Cacti applications for network monitoring.

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. The design and optimization of the network was performed based on the requirements. For Network Availability, High Availability (HA) technology was used, which did not offer the avoidance of service losses by reducing or managing failures and minimizing the planned downtime and the case of a failure. For the scalability of the network, modular equipment was used, which has the possibility to be updated without stopping the services. The network security system (IPS) has been implemented in the network security requirements. To obtain a converged network to provide multiple data transport services through the same infrastructure, VLAN technology was used in combination with the use of the RPVST + spanning-tree family protocol. Access to Internet resources was provided by implementing the NAT mechanism that translates multiple private IP addresses (RFC 1918) into one or more public (global) IPs.

Active and passive monitoring systems have been implemented, in order to have reaction mechanisms that immediately inform the administrator.

CUPRINS

INTRODUCERE	8
1. ANALIZA NIVELELE IERARHICE DE PROIECTARE A UNEI REȚELE	8
1.1 Analiza nivelului Acces.....	9
1.1.1 Analiza securității al primului nivel ierarhic	13
1.2 Analiza nivelului de Distribuție ale rețelei ierarhice de comunicații.....	15
1.2.1 Studiarea tehnologia de interconectare a mai multor switch-uri.....	16
1.2.2 Cercetarea tehnologiei router virtual	17
1.3 Analiza nivelului Core al modelului ierarhic în rețelele de corporative.....	18
1.3.1 Protocolul de atribuire dinamică a IP.....	18
1.3.2 Sistemul de securitate (Firewall)	19
1.3.3 Suita de protocoale IPsec pentru rețele private virtuale.....	20
1.4 Investigarea sistemelor de monitorizare și principiul de funcționare	22
1.4.1 Monitorizarea activă	23
1.4.2 Monitorizarea pasivă	25
2 ELABORAREA STRUCTURII ȘI OPTIMIZAREA REȚELEI CORPORATIVE	27
2.1 Elaborarea structurii rețelei corporative.	27
2.2 Optimizarea sistemul de securitate.	28
2.2 Optimizarea procesului de funcționare a protocolului de gestionare a legăturii L2	31
3. PROIECTAREA ȘI IMPLEMENTAREA REȚELEI CORPORATIVE	33
3.1 Proiectarea configurării pe echipamente	33
3.2 Implementarea sistemele de monitorizare a echipamentele de rețea.....	41
3.2.1 Sistema de monitorizare activă The Dude.	41
3.2.2 Sistema de monitorizare pasivă Cacti	44
CONCLUZII	47
BIBLIOGRAFIA	49
Anexa 1	51

INTRODUCERE

O dată cu extinderea domeniilor de aplicare și numărul utilizatorilor ce doresc să facă schimb de date sau să prelucreze informații comune, a fost implementate nivelele ierarhice care permit segmentarea, izolarea și securizarea stațiilor de lucru la nivele diferite ale stivei OSI. Proiectarea, întreținere și administrare rețelelor de comunicații este mai eficientă prin folosirea acestui model de rețea stratificat. Modelul ierarhic în topologie este divizat în trei categorii de bază: Acces, Distribution și Core. Stratificarea rețelei ne permite aplicarea și utilizarea a diferitor protocoale ale stivei OSI pentru crea o rețea bine calculată care ne-ar permite creșterea acesteia pe viitor. Pentru aceasta este necesar de a optimiza lacunele care se omit.

Din aceste considerente **scopul tezei de master este: Analiza și proiectarea rețelei corporative optime de comunicații securizate pentru prestatorul de servicii internet.**

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

1. Analiza protocoalelor și tehnologiilor necesare pentru a avea posibilitate de a asigura omiterii dependenței de producător.
2. Elaborarea și proiectarea infrastructurii rețelei optime pentru a avea posibilitate de a o extinde.
 - a. Alegerea mecanismelor și protocoalelor pentru a crea o rețea redundată și scalabilă.
 - b. Utilizarea protocoalelor de securizare a rețelei
3. Implementarea și analiza disponibilității serviciilor prestate la nivel de campus, cum ar fi:
 - a. Acces la resursele Internet.
 - b. Transport date pentru telefonie digitală, sistemul de acces control, sistemul anti incendiar, sistemul de monitorizare video.
 - c. Acces utilizatorilor la resursele interne al companiei (sistemele operaționale).
4. Analiza și implementarea sistemelor de monitorizare a echipamentele de rețea.

La baza efectuării acestei lucrări va fi o rețea tipică, în baza cărei 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. Ca o notă bună va fi cercetarea și implementarea unui sistem de monitorizare decent pentru a avea o accesibilitate mai prezentabilă la informație statutului rețelei și posibilitatea de raportare.

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. Wikipedia: LLDP, © 21 noiembrie 2016, [citat 22.09.2020]. Disponibil: https://ru.wikipedia.org/wiki/LLDP#cite_note-1
3. Diane, Teare, Bob, Vachon, Rick, Graziani: *CCNP Route 300-101 Official Cert Guide.* SUA: Indianapolis. 2015 385-387p. ISBN: 978-1-58720-456-2.
4. Cisco: Cisco Catalyst 3850 Series Switches: Install and Upgrade Guides [imagine], © 7 august 2020, [citat 25.09.2020]. Disponibil: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/hardware/installation/guide/b_c3850_hig/b_c3850_hig_chapter_010.html
5. **Первый сервисный провайдер: Наш блок.** The Dude. Часть 1. Теория, © 2017, [citat 24.09.2020]. Disponibil: <https://1spla.ru/blog/the-dude-chast-1-teoriya/>
6. Comparitech: LAN Monitor: 12 Best LAN Monitoring Software Tools for 2020, © 2020, [citat 20.09.2020]. Disponibil: <https://www.comparitech.com/net-admin/lan-monitoring>
7. DNSstuff: Reviews, Opinions, Tools. Top Free Network Monitoring Tools. © 1 noiembrie 2019, [citat 17.09.2020]. Disponibil: <https://www.dnsstuff.com/free-network-monitoring-software>
8. DNSstuff: Reviews, Opinions, Tools. Top Free Network Monitoring Tools. © 1 noiembrie 2019, [citat 17.09.2020]. Disponibil: <https://www.dnsstuff.com/free-network-monitoring-software>
9. Cisco: Cisco Catalyst 3850 Series Switches: Install and Upgrade Guides [imagine], © 7 august 2020, [citat 25.09.2020].
Disponibil: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/hardware/installation/guide/b_c3850_hig/b_c3850_hig_chapter_010.html
10. GeeksforGeeks: Introduction of Firewall in Computer Network, © 21 noiembrie 2019, [citat 05.10.2020]. Disponibil: <https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network>
11. Wikipedia: IPsec, © 11 noiembrie 2019, [citat 10.10.2020]. Disponibil: <https://ro.wikipedia.org/wiki/IPsec>

12. [GeoSolutions: Introduction to Clustering and High Availability, ©2020, \[citat 15.10.2020\]. Disponibil: https://docs.geoserver.geo-solutions.it/edu/en/clustering/clustering/introduction.html](https://docs.geoserver.geo-solutions.it/edu/en/clustering/clustering/introduction.html)
13. GeeksforGeeks: Intrusion Prevention System (IPS), © 09 aprilie 2019, [citat 16.10.2020]. Disponibil: <https://www.geeksforgeeks.org/intrusion-prevention-system-ips/>
14. Akadia Global Competence 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
15. Cisco: What is a Next-Generation Firewall? © 2020 [citat 16.10.2020]. Disponibil: <https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html>
16. GeeksforGeeks: Introduction of Firewall in Computer Network, © 21 noiembrie 2019, [citat 05.10.2020]. Disponibil: <https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network>
17. GeeksforGeeks: Port Security in Computer Network, © 09 august 2019, [citat 21.10.2020]. Disponibil: <https://www.geeksforgeeks.org/port-security-in-computer-network/>
18. Juniper: Overview of Port Security, © 24 septembrie 2020, [citat 20.10.2020]. Disponibil: https://www.juniper.net/documentation/en_US/junos/topics/example/overview-port-security.html
19. [DNSstuff: Reviews, Opinions, Tools. Top Free Network Monitoring Tools \[imagine\]. © 1 noiembrie 2019, \[citat 17.09.2020\]. Disponibil: https://www.dnsstuff.com/free-network-monitoring-software](https://www.dnsstuff.com/free-network-monitoring-software)
20. [Packt: Using Cacti for the first time, © 2020, \[citat 14.11.2020\]. Disponibil: https://subscription.packtpub.com/book/networking_and_servers/9781788299183/1/ch01/v1/sec13/using-cacti-for-the-first-time](https://subscription.packtpub.com/book/networking_and_servers/9781788299183/1/ch01/v1/sec13/using-cacti-for-the-first-time)
- 21- Packt: Installing Cacti on a Windows system, © 2020 [citat 14.11.2020]. Disponibil: https://subscription.packtpub.com/book/networking_and_servers/9781788299183/1/ch01/v1/sec11/installing-cacti-on-a-windows-system
- 22- Mikrotik: Manual: The Dude v6/ Install, ©18.09.2018 [citat 14.11.2020]. Disponibil: https://wiki.mikrotik.com/wiki/Manual:The_Dude_v6/Installation