Ministerul Educației și Cercetării al Republicii Moldova

Universitatea Tehnică a Moldovei

Facultatea Electronică și Telecomunicații

Programul de masterat "Mentenanţă şi Managementul Reţelelor de Telecomunicaţii"

Admis la susţinere
Șef departament TSE:
conf.univ.dr. Sava L.

_____

„____”_____ 2021

ASIGURAREA TRANSPORTULUI DE DATE PENTRU REȚELELE CORPORATIVE ÎN BAZA TEHNOLOGIEI OPEN VPN.

Teză de master

Masterand: _____Ștîrbalov Dumitru

Conducător: _____ conf. univ., dr.,
Gujuman Lucia

Chişinău 2021

REZUMAT

Ștîrbalov Dumitru , masterandul grupei MMRT-201M

Tema: Asigurarea transportului de date pentru rețelele corporative în baza tehnologiei OPEN VPN.

Teza este constituită din introducere, trei capitol, concluzii și bibliografie.

Cuvinte cheie: Rețele virtuale private (VPN), Open VPN, SSH, Firewall, Internet, Proxy server .

Scopul lucrării este proiectarea rețelei corporative în bazat tehnologiei OpenVPN.

Pentru a atinge acest scop, este necesar să rezolvăm următoarele obiective:

1) Determinarea problemelor generale de securitate ale rețelei corporative.

2) Principiile organizării unei rețele VPN bazate pe diverse tehnologii, luând în considerare tipurile de rețele VPN și implementarea lor. Analiza soluțiilor existente pe piață pentru organizarea rețelelor VPN, avantajele și dezavantajele soluțiilor specifice.

3) Descrierea caracteristicilor tehnologiei selectate pentru organizarea unei rețele virtuale private OpenVPN.

4) Descrierea caracteristicilor și etapelor de construire a unei rețele VPN corporative pe un sistem asemănător Unix.

În lucrare au fost analizate principiile de lucru și metodele de construire a rețelelor private virtuale, care sunt clasificate în trei tipuri principale: VPN-uri cu acces la distanță, VPN-uri Intranet și VPN-uri Extranet. În funcție de mijloacele de construcție, se disting VPN-urile, construite pe baza de routere, firewall-uri, pe bază de software specializat.

În lucrare, au fost descrise caracteristicile tehnologiei OpenVPN și procesul de proiectare a unei rețele corporative pe baza acesteia. Partea practică a tezei a arătat că crearea unei rețele corporative bazată pe OpenVPN prin Internet este o sarcină destul de simplă.

În lucrare, au fost descrise soluții de evaluare a performanței canalelor și a metodelor de monitorizare a stării rețelei corporative în timp real pentru o anumită întreprindere privind starea serverelor și a echipamentelor de rețea, filtrarea traficului și monitorizarea activităților personalului.

.

SUMMARY

Ștîrbalov Dumitru, the master student of the group MMRT-201M
Theme: Ensuring data transport for corporate networks based on Open VPN technology.
Keywords Virtual Private Networks (VPN), Open VPN, SSH, Firewall, Internet, Proxy server.

The aim of the paper is to design the corporate network based on OpenVPN technology.
To achieve this goal, we need to address the following objectives:

1) Determining the general security issues of the corporate network.

2) The principles of organizing a VPN based on various technologies, taking into account the types of VPNs and how to implement them. We will analyze the existing solutions on the market for organizing VPNs, the advantages and disadvantages of specific solutions.

3) Description of the features of the selected technology for organizing an OpenVPN virtual private network.

4) Description of the features and stages of building a corporate VPN on a similar Unix system.

The paper analyzed the working principles and methods of building virtual private networks, which are classified into three main types: VPNs with remote access, VPNs Intranet and VPNs Extranet. Depending on the means of construction, VPNs are distinguished, built on the basis of routers, firewalls, on the basis of specialized software.

The paper described the features of OpenVPN technology and the process of designing a corporate network based on it. The practical part of the thesis showed that creating a corporate network based on OpenVPN over the Internet is a fairly simple task.

The paper described solutions for evaluating the performance of channels and methods for monitoring the state of the corporate network in real time for a particular enterprise regarding the status of servers and network equipment, traffic filtering and monitoring of staff activities.

CUPRINS

INTRODUCERE

În ultima perioadă , tot mai des fluxul documentelor și transferul informațiilor corporative se realizează în formă electronică. Pentru aceasta, există deja multe protocoale și metode de transmitere a datelor. Deci, de exemplu, fluxul de documente electronice al unei întreprinderi este realizat prin intermediul platformei 1C, care are multe configurații pentru orice nevoi de afaceri; trimiterea documentelor prin e-mail folosind protocoalele de e-mail POP, IMAP, SMTP; transfer de cantități mari de informații folosind protocolul FTP; organizarea unui site web corporativ folosind tehnologii web.

Tehnologiile informaționale ale secolului 21 oferă oportunități mari pentru îmbunătățirea funcționării întreprinderilor, înlocuirea forței de muncă umană cu forța de muncă la mașini, creșterea productivității muncii și reducerea costurilor. Se creează noi întreprinderi și se modernizează întreprinderile existente, dispersate geografic la nivel de oraș sau chiar de țară, întrucât acum mijloacele de comunicare sunt mult mai accesibile și mai ieftine.

Toate acestea au devenit posibile datorită computerizării și utilizării tehnologiilor de rețea la nivelul întreprinderii. Dar sunt lucruri care nu trebuie uitate: complexitatea implementării, performanța, securitatea, fiabilitatea sistemului. Principalele preocupări astăzi au devenit securitatea și viabilitatea sistemelor informatice.

Informațiile corporative transmise prin rețeaua deschisă de internet pot fi ușor interceptate folosind programe speciale de sniffer - răufăcători. Acestea includ informații critice conținute în documente confidențiale. În plus, login-urile și parolele de la corespondența corporativă sau alte servicii pot fi interceptate.

Confidențialitatea informațiilor transmise vine în prim-plan atunci când se creează o rețea corporativă.

Protecția informațiilor transmise prin canalele de comunicare folosind documente protejate cu parolă sau criptarea acestora nu asigură nivelul necesar de securitate, deoarece orice parolă poate fi spartă și este doar o chestiune de timp (totul depinde de complexitatea acesteia) și cu cu ajutorul criptoanalizei, poate fi detectată și cheia. Desigur, puteți folosi parole mari și complexe, chei moderne de criptare mari, dar toate acestea vor reduce performanța, transformând un mecanism simplu de operare a trimiterii într-unul care necesită mult timp.

Pentru a rezolva aceste contradicții, rețelele corporative folosesc diverse protocoale de rețea privată virtuală (Virtual Private Network). Cu ajutorul lor, sunt create canale virtuale de comunicare prin Internet. Acestea fac posibilă conectarea rețelelor locale cu diverse tehnologii și segmentele acestora într-o singură rețea corporativă. Dar cel mai important avantaj, de fapt, pentru care sunt

necesare, este criptarea întregului trafic care trece prin tunel la nivelul de legătură de date al modelului OSI. Criptarea protejează împotriva accesului la informațiile transmise, iar încapsularea nu permite unui atacator să afle destinatarul informațiilor transmise.

Toate acestea oferă oportunități excelente pentru construirea unei rețele securizate. Dar dacă ceva nu merge bine, programul sau hardware-ul serverelor, atunci canalul securizat nu mai funcționează. Starea rețelei de calculatoare trebuie monitorizată constant, astfel încât timpul de nefuncționare în cazul căderii unei secțiuni a rețelei să fie minim. Cu multe servere și servicii, nu este ușor să afli unde și ce s-a întâmplat. Instrumentele de monitorizare pot urmări acest lucru fără a trece prin fiecare server pe rând. Cu ajutorul unor tabele convenabile și notificări prin e-mail, acest lucru nu va fi dificil, iar administratorul va fi întotdeauna la curent cu starea rețelei, a serviciilor și a serverelor incluse în această rețea corporativă.

BIBLIOGRAFIE

1. ALANI, Mohammed M. *Guide to Cisco Routers Configuration.* SUA: Springer, 2017.234 p. ISBN 978-3-319-54630-8.
2. TASOS, D., JOE, M., Ioannis, T., VARVARIGOU, D. Berlin: Springer-Verlag, 2010. 155 p. ISBN 978-3-642-11733-6.
3. ADNAN, Ahmed Khan, HASSAN, Zahur. *Secure VPN solution in a converged net-work For Phoniro Systems, AB., an emerging SME*. Suedia: September 12, 2012. 345 p. ISBN 978-1-119-54630-7.
4. IOAN, GABRIEL LUCIAN „Calitatea serviciilor de telecomunicaţii", Bucureşti: Matrix Rom, 2016 – 593 pag.
5. *Cisco*: VPN and Endpoint Security Clients. Disponibil: https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/index.html.
6. Elsevier SciTech connects. *Defining-a-VPN, chapter 5 Defining-a-VPN*. Marea Britanie. 2013.
7. Disponibil: http://scitechconnect.elsevier.com/wp-content/uploads/2013/09/Defining-a-VPN.pdf.
8. ADNAN, Ahmed Khan, HASSAN, Zahur. *Secure VPN solution in a converged net-work For Phoniro Systems*, AB., an emerging SME. Suedia: September 12, 2012.
9. Cisco. IPSec VPN WAN Design Overview.USA. Disponibil: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/IPSec_Over.html.
10. SCARFONE, Karen, HOFFMAN, Paul. *Guidelines on Firewalls and Firewall Policy*.SUA: NIST; Septembrie, 2009.
11. BARON-COHEN, Simon. *How is the internet changing the way you think?* ;2015
12. Disponibil: https://edge.org/responses/how-is-the-internet-changing-the-way-you-think.
13. AceBit. Explanation of the FTP and SFTP protocols. Germany; 2014. Disponibil: URL: http://www.wise-ftp.com/know-how/ftp_and_sftp.htm
14. А.В. Соколов, В.Ф.Шаньгин. Защита информации в распределенных корпоративных сетях и системах. – М.:ДМК Пресс, 2002. – 656с.
15. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – 2001 г. 668 с.
16. Олег Колесников, Брайан Хетч. LINUX. Создание виртуальных частных сетей (VPN). - Издательство "КУДИЦ-ОБРАЗ" 2002 г. 464 с.