MINISTERUL EDUCAȚIEI, CULTURII ȘI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei

Facultatea Electronică și Telecomunicații

Departamentul Telecomunicații și Sisteme Electronice

Programul de master ”Mentenanța și Managementul Rețelelor de Telecomunicații”

Admisă la susţinere
Șefa Departament TSE, conf.univ.,dr. Sava Lilia

_____

”_____” _____ 2020

TESTAREA FUNCȚIONALITĂȚII REȚELEI DE COMUNICAȚII PRIVATE PRIN APLICAREA IPSecVPN

Teză de master

Masteranda: _____ Cerlat Cristina

Conducător: _____ conf.univ.,dr. Nistiriuc Pavel

Chişinău - 2020

ADNOTARE

Cerlat Cristina, masteranda grupei MMRT-191M

Tema - Testarea funcționalității rețelei de comunicații private prin aplicarea IPSecVPN.

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

Cuvinte-cheie: Rețeaua virtuală privată VPN, securitatea transportului de date, protocolul IPSec.

Rețeaua de comunicații a unei companii private pentru care se implementează tehnologia VPN este constituită din sediul central, două filiale și doi parteneri de afaceri. Pentru realizarea securității schimbului de date dintre parteneri, filiale și sediul central al companiei, se propune de a utiliza protocolul IPsec peste tunelul GRE (Generic Routing Encapsulation).

Scopul tezei este asigurarea securității transferului de date pentru rețeaua de comunicații a companiei private în baza aplicației IPSecVPN (Internet Protocol Security Virtual Private Network).

În conformitate cu scopul tezei au fost determinate următoarele obiective:

1. Configurarea routerelor rețelei de de comunicații a companiei private pentru organizarea Virtual Local Area Network VLAN - rilor;
2. Determinarea politicii de securitate informațională Internet Key Exchange IKE pentru rețeaua de comunicații a companiei private;
3. Planificarea politicii de securitate informațională prin selectarea setului de transformări a protocolului IPSec pentru rețeaua de comunicații a companiei private;
4. Crearea rețelei virtuale private VPN (Virtual Private Network) distante și tunelului GRE (Generic Routing Encapsulation) cu utilizarea protocolului IPSec în cadrul rețelei de comunicații a companiei private.

În teză au fost configurate routerele rețelei de comunicații pentru crearea VLAN-urilor, elaborate transformările suportate de protocolul IPSec (Internet Protocol Security), a fost configurată lista de acces privind criptarea pachetelor, au fost realizate conexiunea VPN prin intermediul tunelului GRE peste IPSec și serverul de autentificare AAA (Authentication; Authorization and Accounting).

ANNOTATION

Cerlat Cristina, the master student of the group MMRT-191M

Theme -Testing the functionality of the private communications network by applying IPSecVPN.

The thesis consists of introduction, three chapters, conclusions and bibliography.

Keywords: VPN private network, data transport security, IPSec protocol.

The communications network of a private company for which VPN technology is implemented consists of headquarters, two subsidiaries and two business partners. To ensure the security of data exchange between partners, subsidiaries and the company's headquarters, it is proposed to use the IPSec protocol over the GRE (Generic Routing Encapsulation) tunnel.

The purpose of the thesis is to ensure the security of data transfer for the private company`s communications network based on the Internet Protocol Security Virtual Private Network IPSecVPN application.

In accordance with the purpose of the thesis, the following objectives were determined:

1. Configuring the routers of the private company's communications network for organizing the Virtual Local Area Network VLAN;

2. Determining the Internet Security Exchange IKE information security policy for the private company's communications network;

3. Planning the information security policy by selecting the set of transformations of the IPSec protocol for the communications network of the private company;

4. Creation of the remote VPN (Virtual Private Network) and the GRE (Generic Routing Encapsulation) tunnel using the IPSec protocol within the private company's communications network.

In the thesis were configured the communication network routers for creating VLANs, elaborated the transformations supported by the IPSec protocol (Internet Protocol Security), configured the access list on packet encryption, made the VPN connection through the GRE tunnel over IPSec and the server AAA (Authentication; Authorization and Accounting).

CUPRINS

INTRODUCERE

Dezvoltarea actuală a societăţii contemporane conduce treptat spre o societate informaţională în care mijloacele de comunicare şi de transfer al informaţiilor devin de o importanţă majoră. Sporirea cerinţelor de comunicare şi a necesităților de noi servicii de telecomunicaţii, precum şi posibilităţile oferite de tehnologiile moderne au condus la dezvoltarea unor reţele şi sisteme care permit transmisiunea informaţiei multimedia spre un terminal ce poate fi amplasat oriunde pe glob. Astfel, într-o societate informațională securitatea cibernetică a informației reprezintă un obiectiv foarte important pentru fiecare calculator conectat la Internet. Cu atât mai mult, este necesară securitatea informațională pentru o rețea de comunicații privată, deoarece într-o asemenea rețea zilnic are loc schimbul de informații cu caracter privat, care dacă ar fi interceptate de personae cu acces neautorizat ar putea aduce prejudicii considerabile pentru compania privată. Evident, că în cazul în care avem de-a face cu o asemenea rețea de calculatoare asigurarea securității informaționale reprezintă o întrebare foarte importantă.

Motivaţia de bază pentru construirea unei rețele de comunicații private VPN (Virtual Private Network) este reducerea costurilor privind organizarea comunicaţiilor, deoarece este cu mult mai ieftin să se utilizeze o singură legătură fizică comună pentru deservirea mai multor clienţi din reţea, decât să se utilizeze legături separate pentru fiecare client din rețeaua de comunicații privată. Plus la aceasta, un VPN este o soluție care pote asigura nivelul de securitate prescris pentru a putea păstra și schimba informațiile într-un mod sigur. Mesajele din traficul VPN pot fi transmise prin intermediul infrastructurii unei rețele publice de date, precum este Internetul, utilizând protocoalele standard, sau prin intermediul unei rețele private a furnizorului de servicii Internet. VPN-ul este o soluție eficientă din punctul de vedere al costurilor, pentru ca diferite organizații să poată asigura accesul la rețeaua internă pentru angajații și colaboratorii aflați la distanță, şi pentru a permite confidențialitatea datelor schimbate între punctele de lucru aflate la distanță.

Reţelele virtuale private reprezintă un mod de a conecta locaţii aflate la distanţă (filiale, utilizatori mobili, clienţi, furnizori, etc.) într-o unică reţea virtuală, cu asigurarea mecanismelor de securitate informațională.

În teză se propune de a analiza o rețea VPN care să deservească o companie privată cu un sediu central, două filiale și doi parteneri de afaceri amplasați în diverse regiuni geografice. Zilnic, filialele trebuie să schimbe informații, atât cu sediul central, cât și între ele. Pentru a realiza scenariul nominalizat, există două variante: prima variantă, se creează un Intranet cu toate locaţiile în baza unei conexiuni permanente (linii inchiriate) între sediul central şi celelalte locaţii și a doua variantă se utilizează o soluţie de tip VPN. Prima variantă este costisitoare și astfel se optează pentru o soluție VPN.

Soluţia optimă pentru cazul analizat va reprezenta o aplicaţie VPN în baza protocolului IPSec de tipul “Site-to-Site”.

Scopul tezei este asigurarea securității transferului de date pentru rețeaua de comunicații a companiei private în baza aplicației IPSecVPN (Internet Protocol Security Virtual Private Network).

În conformitate cu scopul tezei au fost determinate următoarele obiective:

1. Configurarea routerelor rețelei de comunicații a companiei private pentru organizarea Virtual Local Area Network VLAN - rilor ;
2. Determinarea politicii de securitate informațională Internet Key Exchange IKE pentru rețeaua de comunicații a companiei private;
3. Planificarea politicii de securitate informațională prin selectarea setului de transformări a protocolului IPSec (Internet Protocol Security) pentru rețeaua de comunicații a companiei private;
4. Crearea rețelei virtuale private VPN (Virtual Private Network) distante cu utilizarea tunelului GRE (Generic Routing Encapsulation) și protocolului IPSec în cadrul rețelei de comunicații a companiei private.

BIBLIOGRAFIE

1. FANINACCI D., MORENO V. LISP Network, The: Evolution to the Next-Generation of Data Networks. Cisco Press. 2019.

2. CITTADINI L., BATTISTA G. MPLS Virtual Private Networks. Cisco Press. 2013.

3. SNADER J.C. VPNS ILLUSTRATED: TUNNELS, VPNS, AND IPSEC - Cisco Press, 2010.

4. LEWIS MARK , Comparing, Designing, and Deploying VPNs - Cisco Press, 2010.

5. HUCABY D., MCQUERRY S. Cisco Router Configuration Handbook. Cisco Press. 2010.

6. DORASWAMY N., HARKINS D. IPsec. The New Security Standard for the Internet, Intranets and Virtual Private Networks- 2008.

7. CANGEA O. Transmisia și criptarea datelor. – București: MatrixRom, 2008.

8. RĂDULESCU T., COANDĂ H.G. QoS în reţelele IP multimedia. - Cluj-Napoca , Editura Albastră , 2007.

9. STANDARDUL RFC 4301 Security Arhitecture for the Internet Protocol. 2005.

10. THOMAS T. Primii paşi în securitatea reţelelor. - Bucureşti, Editura „Corint", 2005.

11. THOMAS T. Understanding Internet Protocol Security. - Electrical and Computer Engineering Departament, 2006.

12. WOOD R. Next-Generation Network Services. - Cisco Press, 2005.

13. NAGANAND D. IPSec – The New Security Standard for the Internet; Intranets, and Virtual Private Networks. Pretince Hall. 2003.

14. ЗАПЕЧНИКОВ С. В., МИЛОСЛАВСКАЯ Н. Г., ТОЛСТОЙ А. И.Основы построения виртуальных частных сетей. - Москва: Горячая Линия – Телеком, 2003.

15. TANENBAUM A.S. Rețele de calculatoare. – București: Byblos, 2003.

16. MASON, ANDREW G. Cisco Secure Virtual Private Networks. Cisco Pres. 2002.

17. KILMER W. Rețele de calculatoare și internet pentru oamenii de afaceri. – București: Editura Teora, 2002.

18.http://www.cisco.com/en/US/docs/security/pix/pix61/configuration/guide. ipsecint.html

19. http://www.slideshare.net/Sandra4211/cisco-presentation-guide.

20. http://www.scribd.com/doc/45328408/4-5-0-IPsec

21. http://www.amazon.com/Ipsec-Security-Standard-Intranet Networks.Dp. 0130118982