MINISTERUL EDUCAȚIEI 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

_____

”_____” _____ 2023

SPORIREA SECURITĂȚII INFORMAȚIEI PRIN MIGRAREA ÎN REȚEAUA DE COMUNICAȚII A SERVICIULUI VAMAL NAȚIONAL LA ACCESUL DE TIPUL WAN

Teză de master

Masteranda: _____ Roșca Veronica

Conducător: _____ conf.univ.,dr. Tîrșu Valentina

Chişinău - 2023

ADNOTARE

Roșca Veronica, masteranda grupei MMRT-211M

Tema – Sporirea securității informației prin migrarea în rețeaua de comunicații a serviciului vamal național la accesul de tipul WAN.

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

Cuvinte-cheie: Rețea informațională de comunicații, serviciul vamal national, instrumente de Securitate a informației, metoda de acces WAN, tehnologia FTTx.

Scopul tezei constă în implementarea de noi instrumente de securitate cu utilizarea standardului IPsec pentru rețeaua informațională de comunicații a serviciului vamal national prin migrarea la noul tip de acces WAN în baza tehnologiei FTTx, care să corespundă cu politicele de securitate și planul de dezvoltare strategică ale serviciului vamal național.

În conformitate cu scopul tezei au fost determinate următoarele obiective:

1. Determinarea tehnologiei de acces pentru rețeaua informațională de comunicații a serviciului vamal national în contextual sporirei ratei de transfer a datelor și a utilizării de noi tehnici de Securitate cu asigurarea calității admisibile de transmisie a informației;
2. Asigurarea securității datelor informaționale in rețeaua de comunicații a serviciului vamal national prin selectarea protocolului din standardul IPsec;
3. Determinarea metodei de criptare pentru a optimiza timpul consumat la criptarea datelor în rețeaua de comunicații a serviciului vamal national prin selectarea lungimii cheii de criptare;
4. Asigurarea în rețeaua de comunicații a serviciului vamal national a gradului înalt de securitate a informației prin modernizarea și configurarea echipamentului de comutare.

În teză au fost determinate pentru rețeaua de comunicații a serviciului vamal național (SVN) infrastructura WAN, schemele de acces WAN prin Internet, schema de creare a tunelului VPN prin Internet cu elaborarea tabelului de rutare, a fost efectuată configurarea echipamentului de comutare, au fost selectate protocolul și metodele de criptare a datelor, efectuată multiplexarea conexiunilor punct-la-punct într-un singur port WAN, au fost determinate schema infrastructurii rețelei WAN a provaiderului, topologia rețelei SVN, schema de funcționare GRE (Generic Routing Encapsulation) over IPsec, a fost selectat echipamentul de comutare pentru crearea legăturilor VPN site-to-site, efectuată configurarea tunelelor VPN GRE over IPsec în rețeaua transport date a SVN, determinate asociațiile IPsec între routerul central și cele periferice, schema de tranziție la rețeaua cu acces WAN prin tehnologia FTTx .

ANNOTATION

Rosca Veronica, the master student of the group MMRT-211M

Theme – Increasing information security by migrating the communication network of the national customs service to WAN access.

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

Keywords: Information communication network, national customs service, information security tools, WAN access method, FTTx technology.

The aim of the thesis consists in the implementation of new security tools using the IPsec standard for the information communication network of the national customs service by migrating to the new type of WAN access based on FTTx technology, which corresponds to the security policies and the strategic development plan of the service national customs.

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

1. Determination of the access technology for the informational communication network of the national customs service in the context of increasing the data transfer rate and the use of new Security techniques with the assurance of the admissible quality of information transmission;
2. Ensuring the security of informational data in the communications network of the national customs service by selecting the protocol from the IPsec standard;
3. Determining the encryption method to optimize the time spent encrypting data in the communications network of the national customs service by selecting the length of the encryption key;
4. Ensuring a high degree of information security in the communications network of the national customs service by modernizing and configuring the switching equipment.

In the thesis, the WAN infrastructure, the WAN access schemes over the Internet, the scheme for creating the VPN tunnel over the Internet with the elaboration of the routing table were determined for the communication network of the national customs service (SVN), the configuration of the switching equipment was carried out, were the data encryption protocol and methods were selected, multiplexing of point-to-point connections in a single WAN port was performed, the provider's WAN network infrastructure scheme, SVN network topology, GRE (Generic Routing Encapsulation) over IPsec operation scheme were determined, the switching equipment for the creation of site-to-site VPN links was selected, the configuration of GRE over IPsec VPN tunnels in the data transport network of SVN was performed, the IPsec associations between the central and peripheral routers were determined, the transition scheme to the network with WAN access through the technology FTTx.

CUPRINS

INTRODUCERE

În contextual actual al societății informaționale colectarea, transmisia și prelucrarea datelor prin intermediul rețelelor de comunicații/calculatoare tind să ajungă principalul mijloc de comunicare între oameni amplasați oriunde pe mapamond. Sporirea cerinţelor de securizare a informației în rețelele de comunicaţii, precum şi posibilităţile oferite de tehnologiile moderne au contribuit la dezvoltarea rețelelor de comunicații securizate care permit transmisia a orice tip de informaţie cu caracter secret printr-un mediu fizic nesigur de comunicaţii.

Calitatea serviciilor prestate de serviciul vamal national (SVN) în mare măsură depinde de gradul de dezvoltare a infrastructurii rețelei informaționale de comunicații utilizată de SVN. La momentul proiectării reţelelei de comunicaţii în cadrul SVN (anul 2003), nu- au fost luate în considerare dezvoltarea și performanțele tehnologiilor moderne şi sporirea permanentă a resurselor informaţionale pentru serverelor centrului de date. Astfel, în timp a apărut necesitatea de a optimiza și reconfigura rețeaua de comunicații a SVN pentru a spori viteza, securitatea și calitatea de transmisie a datelor, ce a condus la selectarea unui nou tip de acces WAN cu utilizarea tehnologiei FTTx.

Scopul prezentei teze constă în implementarea de noi instrumente de securitate cu utilizarea standardului IPsec pentru rețeaua informațională de comunicații a SVN prin migrarea la noul tip de acces WAN în baza tehnologiei FTTx, care să corespundă cu politicele de securitate și planul de dezvoltare strategică ale SVN.

În conformitate cu scopul tezei au fost determinate următoarele obiective:

1. Determinarea tehnologiei de acces pentru rețeaua informațională de comunicații a serviciului vamal national în contextual sporirei ratei de transfer a datelor și a utilizării de noi tehnici de securitate cu asigurarea calității admisibile de transmisie a informației;
2. Asigurarea securității datelor informaționale in rețeaua de comunicații a serviciului vamal national prin selectarea protocolului din standardul IPsec;
3. Determinarea metodei de criptare pentru a optimiza timpul consumat la criptarea datelor în rețeaua de comunicații a serviciului vamal national prin selectarea lungimii cheii de criptare;
4. Asigurarea în rețeaua de comunicații a serviciului vamal national a gradului înalt de securitate a informației prin modernizarea și configurarea echipamentului de comutare.

CONCLUZII

În rezultatul implementării intrumentelor de securitate pentru rețeaua de comunicații a serviciului vamal national în baza standardului IPsec și migrării la noul tip de acces WAN în baza tehnologiei FTTx, pot fi effectuate următoarele concluzii:

1. Utilizarea metodei de acces WAN prin FTTx în rețeaua de comunicații a SVN, permite să sporim rata de transfer a datelor ce oferă posibilitatea de a implementa instrumentele de securitate avansate, precum standardul IPsec în baza protocolului ESP cu asigurarea calității necesare de transmisie a datelor;
2. S-a stabilit, că pentru rețeaua de comunicații a SVN cu acces WAN prin FTTx sarcina generată de sursă și rata datelor transmise după procesarea lor în IPsec-ESP nu se modifică, pentru canalele cu capacitatea de 2 Mbps, indifirent de algoritmul de criptare selectat DES, 3DES și AES;
3. S-a constatat, că timpul consumat pentru criptarea pachetelor depinde de metoda de criptare/lungimea cheii de criptare și s-a stabilit, că algoritmul AES este cel mai performant în comparație cu algoritmele de criptare DES și 3DES, deoarece ne permite să reducem timpul consumat pentru criptarea pachetelor de date și să asigurăm confidențialitatea datelor;
4. A fost demonstrat, că pentru rețeaua de comunicații a SVN cu acces WAN prin FTTx, algoritmul în combinația ESP-AES posedă cel mai performant nivel de securitate, începând cu dimensiunea cheii AES de 128 biți;
5. Pentru rețeaua de comunicații a SVN cu acces WAN prin FTTx, a fost propusă soluția de multiplexare a tuturor canalelor punct-la-punct dintre echipamentul central de comutare și cele periferice utilizând instrumentul GRE;
6. În baza rezultatelor obținute, se propune de a crea legăturile VPN în rețeaua de comunicații a SVN cu acces WAN prin FTTx, utilizând instrumentele de securitate GRE a standardului IPsec cu selectarea protocolului ESP în combinație cu algoritmul de criptare AES-128 biți (și mai mult) și combinația algoritmilor de integritate a datelor SHA-1 – HMAC pentru a asigura nivele înalte de securite și de calitate la transmisia datelor;
7. Pentru a îmbunătăți eficiența de funcționare a rețelei de comunicații a SVN cu acces WAN prin FTTx a fost propus de a substitui routerul central c3640 cu un router mai performant, după cum este routerul c7200, iar pentru routerele periferice c2801 s-a propus de a efectua upgrade-ul imaginei IOS.

BIBLIOGRAFIE

1. Implementing Secure Converged Wide Area Networks, Student Guide for Cisco System, Vol.1, 2006.
2. TISOVSKY, A., KLUCIK S., Method for Calculation the Packet-Size Dependent Throughput of a Computationally Intensive IPsec, Process", Elektrorevue, ISSN 1213-1539, Noiembrie 2010, Art. Nr. 98.
3. ADAM TISOVSKY, IVAN BARONAK, Performance Analysis of IPsec Gateway, Elektrorevue, ISSN 1213-1539, Aprilie 2012, art. Nr. 1.
4. DIAA SALAMA ABD ELMINAAM, HATEM MOHAMED ABDUAL KADER, Evaluating The Performance of Symmetric Encryption Algorithms, în : International Journal of Network Security, Vol.10, Nr.3, P.216–222, Mai 2010.
5. Ludmila Peca, Dinu Ţurcanu. Computer networks: Practical examples solved to be introduced in computer networks. ISBN 978-9975-45-812-2. Chișinău, Publisher ,,Tehnica-UTM", 2022.
6. M. KAEO, Methodology for Benchmarking IPsec Devices, IETF Draft, 2009.
7. KHALED SALAH, Integrated performance evaluating criterion for selecting between interrupt coalescing and normal interruption, International Journal of High Performance Computing and Networking, Vol. nr. 3, December 2005.
8. M. ZEC, M. MIKUC, M. ŽAGAR, Estimating the Impact of Interupt Coalescing Delays on Steady State TCP Throughput, a 10-a conferinţă SoftCom, 2002.
9. Dinu Ţurcanu, Natalia Spinu, Serghei Popovici, Tatiana Țurcanu. Cybersecurity of the Republic of Moldova: a retrospective for the period 2015-2020. Journal of Social Sciences, Vol. IV, no. 1 (2021), pp. 74 – 83.
10. S. Z. S. IDRUS, and S. A. ALJUNID, Performance analysis of encryption algorithms text length size on web browsers, Jurnalul Internaţional de ştiinţe ale computerelor şi a securităţii reţelelor, Vol. 8, nr.1, Ianuarie 2008.
11. Politica de securitate a informaţiei în cadrul seviciului vamal. http://customs.gov.md/files/Politica%20securit%20inf%20final.pdf
12. Programul de dezvoltare strategică al serviciului vamal http://customs.gov.md/files/raport/PDS%202012-2014%20web.pdf
13. Cisco 2800 Series Integrated Services Routers Data Sheet. http://www.cisco.com/en/US/prod/collateral/routers/ps5854/ps5882/product_data_sheet0900aecd8016fa68_ps5854_Products_Data_Sheet.html.
14. VPN Performance of Cisco Routers and Switches. http://www.ccsleeds.co.uk/kb/routers/cisco-vpn-throughput-comparison-doc.pdf.