Ministerul Educaţiei al Republicii Moldova

Universitatea Tehnică a Moldovei

Facultatea Inginerie și Management în Electronică și Telecomunicații

Programul de masterat "Mentenanța și managementul rețelelor de telecomunicații"

Admis la susţinere

şef catedră:

conf.univ.dr. Nistiriuc Pavel

_____

„__"_____ 2016

ANALIZA METODELOR DE SECURITATE A TRANSPORTULUI DE DATE ÎN REȚELE DE COMUNICAȚII PE BAZA TEHNOLOGIEI DE ACCES FTTX

Teză de master

Masterand: _____Bînzari Ch.

Conducător: ___conf.univ.dr. Sava L.

Chişinău 2016

R E Z U M A T

Capitolul introductiv al tezei prezintă problemele legate de asigurarea calităţii transmisiei datelor securizate în rețelele LAN și WAN, cu accent pe protocoale ce asigură securitatea informațională care pot fi utilizate în infrastucturile IT contemporane. Au fost descrise detaliat procedurile de securizare ale standardului IPsec pentru fiecare protocol din componența acestuia ESP și AH, reprezentînd tehnicile și metodele de criptare și autentificare a acestora. Fiecare protocol de securitate trebuie să corespundă următoarelor cerințe de încredere a unui mediu securizat: confidențialitatea, integritatea, autentificarea și non-repudierea datelor cu caracter secret. S-au ilustrat metodele de protejare a datelor contra atacurilor informaționale în mediile nesigure de transmisiuni de date.

Capitolul 2 „Studiul și colectarea datelor primare ale rețelei transport date proiectată în baza serviciului CrossNet” prezintă starea actuală a rețelei WAN studiată. Este realizată o evaluare a riscurilor și lacunelor de securitate în rețeaua existentă care nu oferă calitatea necesară a datelor transmise prin rețelele de comunicații proiectate anterior. Au fost redate în detalii dezavantajele utilizării metodelor de acces WAN prin crossnet și Internet, astfel s-a demonstrat că utilizarea noilor instrumente de securitate pentru circuitele digitale punt-la-punct oferite de tehnologia crossnet nu au efectul scontat fără a migra la o nouă metodă de acces WAN prin FTTx, care oferă o rată de transfer a circuitelor de comunicații de 2Mbps.

În capitolul 3 este prezentată o analiză detaliată a noilor intrumente de securitate alese, ce vor fi folosite în procesul de securizare a datelor informaționale prin noul tip de acces WAN prin FTTx. În acest context s-a demonstrat că metoda optimă de securizare a datelor ce corespunde politicilor și cerințelor de securitate a sistemului informațional integrat este intrumentul GRE over IPsec, ce folosește protocolul ESP cu algoritmul de criptare AES-128 bit și algoritmul de autentificare a originii datelor SHA-1 HMAC. În alegerea prototipului s-a ținut cont și de condițiile tehnice existente și de cele prestate de prestatorul transport date, având un efect economic de implementare mai puțin costisitor. Rezultatele obținute au fost indicate prin configurarea echipamentelor de comutare și printout-rile oferite de acestea.

S U M M A R Y

The introductory chapter of the thesis is devoted to a presentation of the problems linked to quality assurance of data security transmission in LAN and WAN networks, making an accent on the used protocols that provide information security in the present IT infrastructures. There was described in details the security procedures of the IPsec standard, for each IPsec's protocols ESP and AH was shown the methods and techniques of encryption and data authentication. Each security protocol must matches the following requirements to ensure a secure environment: confidentiality, integrity, authentication and non-repudiation of data secret character.

The second chapter "Study and collection of primary data of network data transport based on CrossNet Services" presents the current state of the studied WAN network. An evaluation of the risks and gaps is performed for current network that doesn't provide the necessary quality of data transmission through old designed communication networks. It was described in details the disadvantages of using CrossNet and internet of WAN access methods, so it was demonstrated that the using of security tools for digital point-to-point circuits provided by CrossNet technology doesn't have the desired effect without migrating to a new method WAN access through FTTx, which offers 2Mbps of data rate for communication channels.

The third chapter introduces a detailed analysis of selected new security tools that will be used in data security information by the new type of WAN access via FTTx. In this context it has been shown that the method corresponding data security policies and security requirements are integrated information system GRE over IPsec the instrument that uses the ESP protocol with encryption algorithm AES-128 bit and data origin authentication algorithm SHA-1 HMAC. Taken into account in selecting prototype and technical conditions and the bit-provided data provider with economic effect of implementing less expensive. Desired results obtained were indicated by setting switching equipment and printouts provided.

C U P R I N S

INTRODUCERE…….……..……....…….....8

1. TEHNICI ŞI INSTRUMENTARII PENTRU SECURIZAREA INFORMAȚIONALĂ A REȚELEI.....10

1.1. Dispozitive utilizate ca instrument de protecție a rețelei.....10

1.2. Protocoale și standarde de securitate: IPsec, ESP, AH.....16

2. STUDIUL ȘI COLECTAREA DATELOR PRIMARE ALE REȚELEI TRANSPORT DATE PROIECTATĂ ÎN BAZA SERVICIULUI CROSSNET …….....27

2.1. Organizarea accesului la rețeaua informațională peste Internet.....27

2.2. Organizarea accesului la rețeaua informațională în baza serviciului CrossNet.....33

2.3. Comparația metodelor de acces utilizate în rețea.....35

3. STUDIUL ŞI POSIBILITATEA IMPLEMENTĂRII METODELOR DE SECURIZARE A REŢELELELOR TRANSPORT DE DATE UTILIZÎND TEHNOLOGIA DE ACCES FTTX.....46

3.1. Organizarea accesului la rețea în baza tehnologiei FTTx.....47

3.2. Identificarea și alegerea eficientă a protocoalelor de securitate în cadrul rețelei.....48

3.3. Caracteristica implementării tunelelor GRE în baza IPsec ESP.....57

3.4. Configurarea și testare transportării datelor în baza tunelelor VPN în rețea.....63

CONCLUZII.....75

BIBLIOGRAFIE.....77