**Ministerul Educaţiei și Cercetării al Republicii Moldova**

**Universitatea Tehnică a Moldovei**

**Facultatea Calculatoare, Informatică și Microelectronică**

**RAPORT**

Lucrarea de laborator nr.5

*la Tehnologii a Securitatii Informationale*

A efectuat:

st. gr. TI-216 Rosca Dorin

A verificat: Zalesciuc Maxim

Chişinău – 2023

**Lucrare de laborator nr. 5**

**Tema:**Configurarea firewall software si VPN.

**Scopul lucrării:** Gestionarea si Configurarea firewall software si VPN .

1. **FireWall:**

**Firewall-ul reprezintă o componentă esențială în domeniul securității cibernetice, oferind o barieră de protecție pentru sistemele și rețelele informatice împotriva amenințărilor și accesului neautorizat. Pe această pagină A4, ne vom concentra asupra configurării firewall-ului în sistemul de operare Windows și în sistemele de operare bazate pe Linux, vom explora diferitele tipuri de firewall-uri și vom evidenția importanța acestora.**

**Configurarea firewall-ului în sistemul de operare Windows presupune utilizarea instrumentului integrat numit Windows Firewall. Prin intermediul acestuia, se pot stabili reguli și politici de securitate pentru a controla traficul de rețea ce intră și iese din sistem. Configurarea implică setarea permisiunilor și restricțiilor pentru aplicații și servicii, astfel încât să se asigure o protecție adecvată a sistemului.**

**Procesul de configurare poate fi realizat prin intermediul panoului de control și al setărilor avansate ale Windows Firewall.**

**Pe de altă parte, configurarea firewall-ului în sistemele de operare bazate pe Linux poate fi efectuată prin diverse instrumente, iar unul dintre cele mai utilizate este iptables. Această unealtă permite administrarea regulilor de filtrare a pachetelor, precum și controlul traficului de rețea.**

**Configurarea în Linux implică specificarea regulilor de filtrare, adăugarea sau eliminarea acestora și asigurarea funcționării corecte a firewall-ului în cadrul sistemului de operare.**

**Există mai multe tipuri de firewall-uri, fiecare având caracteristici specifice și funcționalități adaptate diferitelor nevoi de securitate. Printre cele mai comune tipuri se numără firewall-urile de rețea, firewall-urile personale și firewall-urile de aplicații.**

**Firewall-urile de rețea sunt amplasate între o rețea privată și Internet și funcționează ca o poartă de acces securizată. Acestea analizează pachetele de date care trec prin ele și aplică politici de securitate, permițând doar traficul autorizat și blocând accesul neautorizat.**

**Firewall-urile personale sunt implementate pe dispozitive individuale, precum computere personale sau dispozitive mobile, și oferă protecție la nivel individual. Acestea monitorizează și controlează traficul de rețea către și dinspre dispozitiv, blocând potențiale amenințări cibernetice. Firewall-urile de aplicații, cunoscute și sub numele de firewall-uri de nivel aplicație, monitorizează traficul specific al aplicațiilor și furnizează o protecție adițională la nivelul aplicațiilor.**

**Ele permit controlul precis al traficului și aplică politici de securitate specifice pentru fiecare aplicație. Importanța firewall-ului în cadrul securității cibernetice nu poate fi neglijată.**

**Acesta reprezintă prima linie de apărare împotriva amenințărilor cibernetice, contribuind la prevenirea intruziunilor, a accesului neautorizat și a atacurilor asupra sistemelor și rețelelor.**

**Configurarea și administrarea corectă a firewall-ului sunt cruciale pentru asigurarea unui nivel adecvat de securitate și protecție a datelor și informațiilor sensibile. firewall-ul reprezintă un element esențial în protejarea sistemelor și rețelelor împotriva amenințărilor cibernetice.**

**Configurarea acestuia în sistemele de operare Windows și Linux, înțelegerea diferitelor tipuri de firewall-uri și recunoașterea importanței sale în cadrul securității cibernetice reprezintă pași critici pentru asigurarea unui mediu sigur și protejat digital.**

1. **VPN**

**VPN (Virtual Private Network) reprezintă o tehnologie esențială în domeniul securității cibernetice, furnizând o conexiune sigură și privată între utilizatori și rețelele lor.**

**Setarea unui VPN presupune configurarea parametrilor și protocolului de securitate pentru a stabili o conexiune criptată între client și server.**

**Această configurare implică adăugarea informațiilor de autentificare, stabilirea protocolului de tunelare și a setărilor de criptare. Utilizarea unei interfețe de administrare sau a unei aplicații dedicate facilitează procesul de configurare, oferind utilizatorului opțiuni intuitive de personalizare.**

**Protocoalele VPN, precum IPSec (Internet Protocol Security) și SSTP (Secure Socket Tunneling Protocol), sunt utilizate pentru a stabili și gestiona conexiunea VPN. IPSec oferă un cadru de securitate flexibil și puternic, asigurând autentificare, integritatea datelor și confidențialitatea prin criptarea traficului. SSTP utilizează protocoalele SSL/TLS (Secure Sockets Layer/Transport Layer Security) pentru a stabili conexiuni VPN sigure prin intermediul unui singur port.**

**Efectul de tunel în VPN permite încapsularea datelor într-un pachet criptat și protejat, care este transmis prin intermediul unei rețele publice sau nesigure. Acest pachet criptat traversează tunelul securizat între client și server, asigurând confidențialitatea și integritatea datelor în tranzit. Există diverse tipuri de VPN utilizate în funcție de necesitățile specifice ale utilizatorilor și organizațiilor. VPN-urile de acces remote permit utilizatorilor să se conecteze de la distanță la rețelele lor interne, asigurând o conexiune sigură prin intermediul internetului public.**

**VPN-urile de site-to-site conectează două sau mai multe rețele geografic separate, oferind o rețea privată virtuală între ele. VPN-urile mobile sunt concepute pentru a furniza securitate și confidențialitate utilizatorilor de dispozitive mobile, permițându-le să se conecteze în siguranță la rețele publice nesigure.**

**Aplicațiile VPN sunt instrumente software utilizate pentru a facilita setarea și utilizarea VPN-urilor. Acestea oferă interfețe intuitive și funcționalități avansate pentru gestionarea conexiunilor VPN, configurarea setărilor de securitate și monitorizarea traficului de rețea.**

**Aplicațiile VPN pot fi utilizate pe diverse platforme, inclusiv computere, telefoane mobile și routere. VPN-ul reprezintă o soluție esențială în asigurarea securității cibernetice, furnizând conexiuni sigure și private între utilizatori și rețelele lor.**

**Configurarea unui VPN, utilizarea protocoalelor VPN precum IPSec și SSTP, înțelegerea efectului de tunel și a diferitelor tipuri de VPN, precum și utilizarea aplicațiilor dedicate, contribuie la crearea unui mediu de comunicare sigur și confidențial în cadrul rețelelor informatice.**

1. **Tehnologii IDS si IPS**

**Tehnologiile IDS (Intrusion Detection System) și IPS (Intrusion Prevention System) reprezintă instrumente esențiale în domeniul securității cibernetice, furnizând protecție activă împotriva intruziunilor și atacurilor asupra sistemelor și rețelelor informatice.**

**Configurarea unui IDS presupune implementarea și personalizarea unui sistem care detectează și monitorizează activitățile suspecte sau neautorizate în rețele și sisteme. Acest proces implică identificarea și selectarea senzorilor potriviți, configurarea setărilor de analiză a traficului de rețea și a bazelor de date de semnături, precum și definirea regulilor și politicii de detectare a intruziunilor.**

**Utilizarea unei interfețe de administrare facilitează procesul de configurare și permite administratorului să monitorizeze activitatea și să ia măsuri adecvate în cazul unei intruziuni.**

**Pe de altă parte, configurarea unui IPS implică implementarea unui sistem care nu numai detectează, ci și previne activitățile neautorizate și atacurile cibernetice. Acesta poate fi configurat pentru a bloca automat traficul sau a notifica administratorul în cazul unei amenințări iminente.**

**Configurarea unui IPS presupune definirea politicii de prevenire a intruziunilor, configurarea regulilor și semnăturilor de securitate și stabilirea nivelului de intervenție. Astfel, sistemul va putea detecta și bloca automat activitățile suspecte sau periculoase, asigurând protecție în timp real.**

**IDS și IPS sunt tehnologii cruciale în cadrul securității cibernetice, deoarece permit detectarea și prevenirea intruziunilor, minimizând riscul de compromitere a sistemelor și rețelelor. Aceste tehnologii monitorizează și analizează traficul de rețea, identificând semnăturile și comportamentele specifice ale atacurilor cibernetice și trăsăturile neautorizate.**

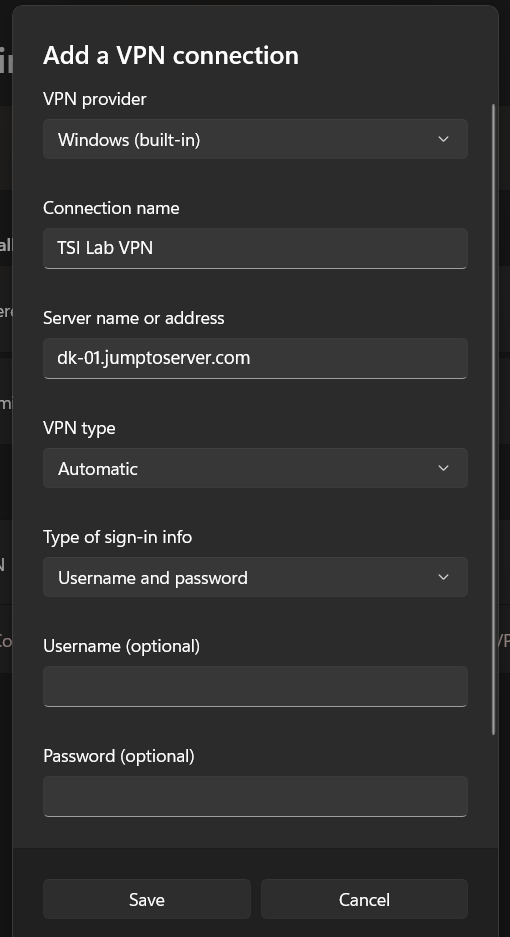
**Prin configurarea adecvată a unui IDS și IPS, se poate reduce timpul de răspuns la incidente și se poate proteja infrastructura de atacuri avansate și sofisticate. Importanța tehnologiilor IDS și IPS constă în capacitatea lor de a detecta și preveni amenințările cibernetice, asigurând integritatea, confidențialitatea și disponibilitatea sistemelor și rețelelor.**

**Configurarea corespunzătoare a unui IDS și a unui IPS asigură o protecție proactivă împotriva atacurilor și intruziunilor, contribuind la menținerea unui mediu cibernetic sigur și protejat, tehnologiile IDS și IPS reprezintă un element crucial în asigurarea securității cibernetice, oferind capacitatea de a detecta și preveni intruziunile și atacurile cibernetice.**

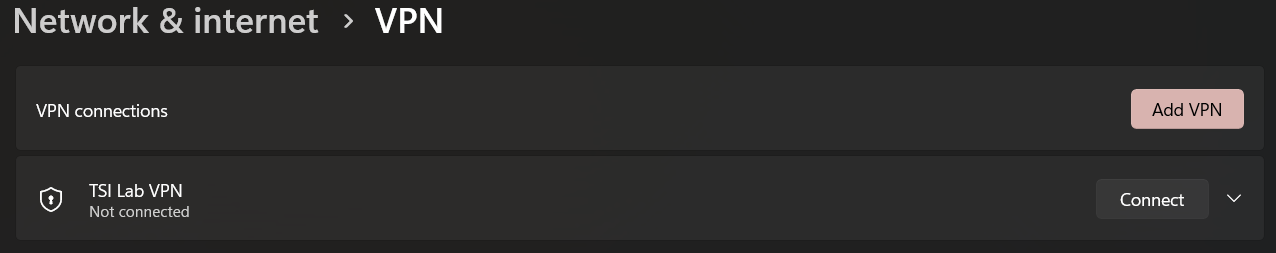
**Configurarea unui IDS și a unui IPS implică stabilirea setărilor de analiză, definirea politicii de securitate și configurarea semnăturilor și regulilor. Prin utilizarea acestor tehnologii și prin implementarea unor politici de securitate solide, se poate asigura un nivel adecvat de protecție a sistemelor și rețelelor împotriva amenințărilor cibernetice.**

**Sarcina:**

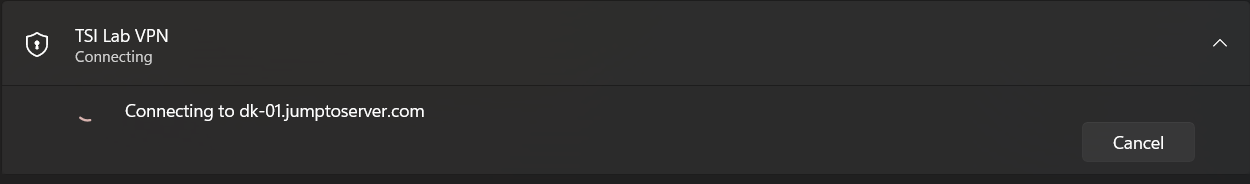
Adauga VPN Conectiunea

****

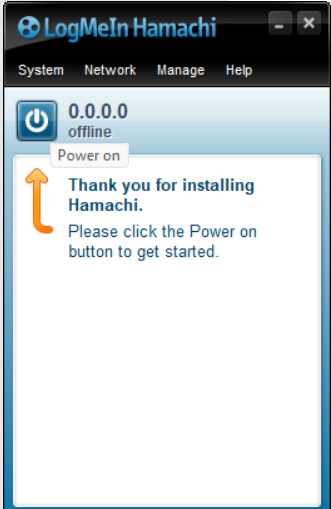
**Fig1.Crearea Conectiune**

****

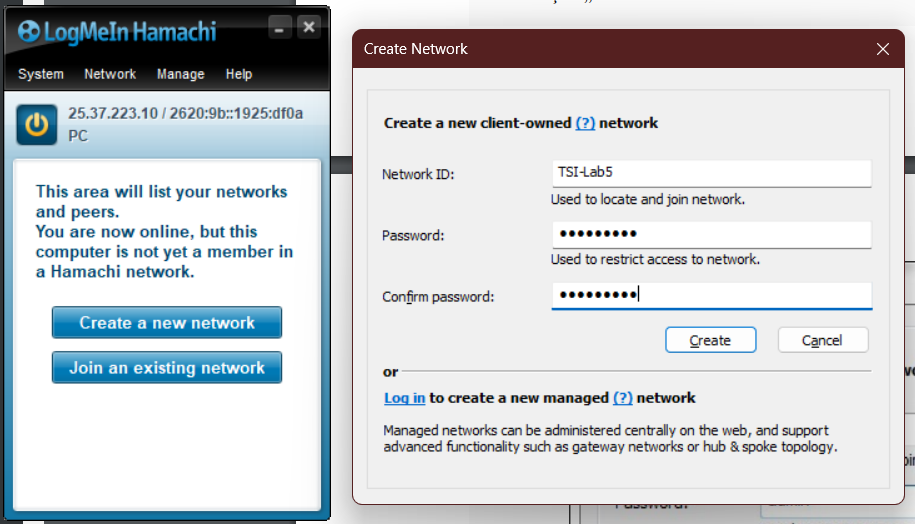
**Fig2.Adaugare Conectiune**

****

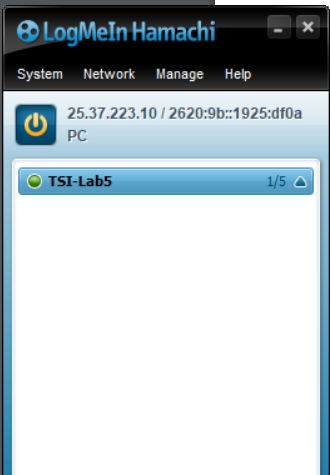
**Fig3.Conectare**

**Aplicarea Instrumentelor VPN Utilizand Hamachi LogMeIn** ****

**Fig4.Deschiderea Aplicatiei**

****

**Fig5.Creaza NetWork**

****

**Fig6.Rezultat**

**Concluzie:**

Lucrarea de laborator nr. 5 s-a concentrat pe configurarea firewall-ului software și VPN-ului, două elemente esențiale în asigurarea securității cibernetice. Configurarea firewall-ului în sistemele Windows și Linux, înțelegerea diferitelor tipuri de firewall-uri și importanța lor în securitatea cibernetica reprezintă pași critici pentru protejarea sistemelor și rețelelor împotriva amenințărilor cibernetice. Setarea unui VPN, utilizarea protocoalelor VPN și a aplicațiilor dedicate contribuie la crearea unui mediu de comunicare sigur și confidențial. De asemenea, tehnologiile IDS și IPS au fost abordate, evidențiindu-se importanța lor în detectarea și prevenirea intruziunilor și atacurilor cibernetice, asigurând un nivel adecvat de protecție pentru sistemele și rețelele informatice. Configurarea corespunzătoare a acestor tehnologii și implementarea unor politici de securitate solide sunt cruciale pentru asigurarea unui mediu cibernetic sigur și protejat."