Ministerul Educaţiei și Cercetării

al Republicii Moldova   
Universitatea Tehnică a Moldovei

Faculatea Calculatoare, Infromatică și Microelectronică   
  
  
  
  
  
  
  
RAPORT

# LUCRARE DE LABORATOR NR. 5

# la Tehnologii ale securității informaționale

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

A efectuat:

st. gr. TI-211 Popa Cătălin

A verificat: Octavian Răducanu

UTM, Chișinău 2023

**Tema:**

Configurarea firewall software și VPN.

**Scopul lucrării:**

* **1. Firewall**
  + Configurarea windows firewall, configurarea firewall în linux
  + Tipuri de Firewall. Importanța
* **2. VPN (Virtual Private Network)**
  + Setarea unui VPN
  + Protocoale VPN (IPSec SSTP), Efectul de tunel
  + Tipuri de VPN. Aplicații
* **3. Tehnologiile IDS și IPS**
  + Configurarea unui IDS (Intrusion Detection System)
  + Configurarea unui IPS (Intrusion Prevention System)

**1. Firewall**

**Tipuri de Firewall. Importanța**

Există mai multe tipuri de firewall-uri, dar cele mai comune sunt:

Firewall hardware - este un dispozitiv dedicat care filtrează traficul de rețea și are capacitatea de a gestiona un volum mare de trafic. Este amplasat între rețeaua internă și internet și securizează rețeaua prin blocarea traficului nedorit.

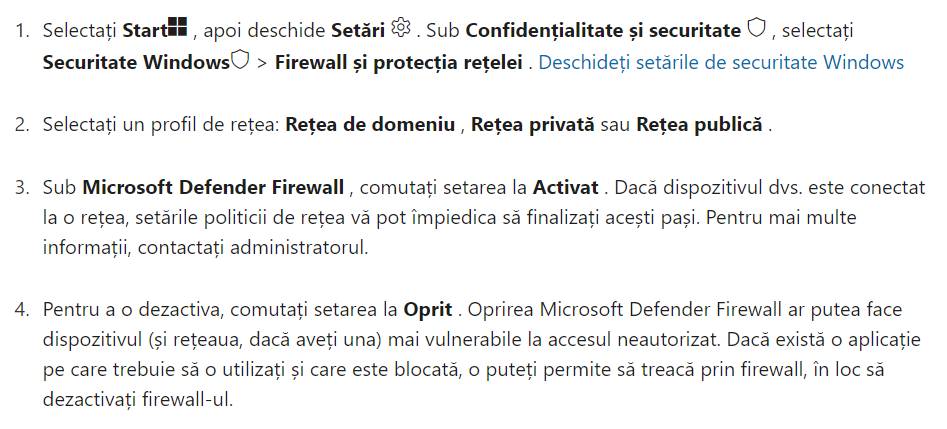
Firewall software - este un program instalat pe un sistem de operare care filtrează traficul de rețea. Este mai puțin costisitor decât un firewall hardware și poate fi configurat pentru a se potrivi nevoilor specifice ale unei rețele.

Firewall bazat pe cloud - este un serviciu de securitate bazat pe cloud care filtrează traficul de rețea și poate fi configurat pentru a se integra cu diferite tipuri de infrastructură de rețea.

Importanța firewall-ului constă în protejarea rețelei de atacuri externe, precum și a datelor și informațiilor sensibile care circulă prin rețea. Prin blocarea traficului nedorit, firewall-ul poate preveni accesul neautorizat la rețea și poate ajuta la prevenirea pierderii sau compromiterii datelor. Un firewall este, de asemenea, important pentru a proteja rețeaua împotriva virușilor și altor amenințări cibernetice care pot afecta performanța rețelei sau pot compromite securitatea datelor.

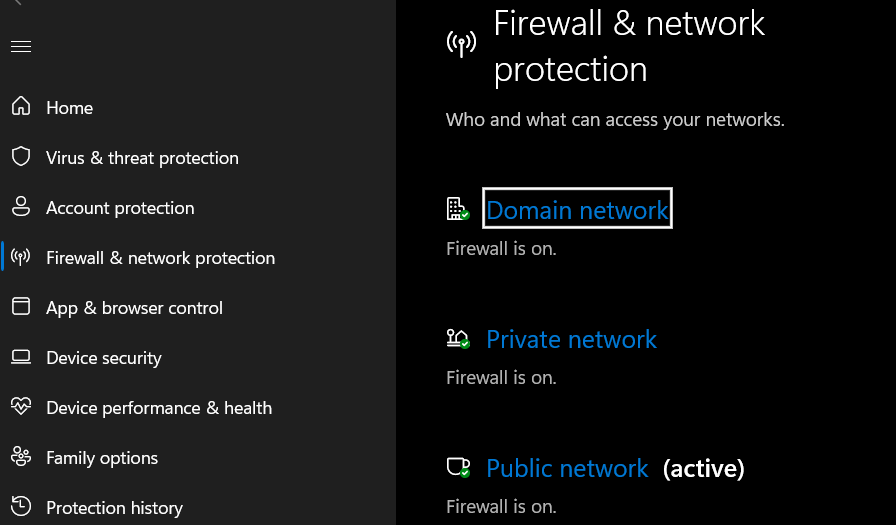
**Configurarea windows firewall, configurarea firewall în linux**

Pentru a configura un firewall pe windows 11, mă voi folosi de Microsoft Defender Firewall. Astfel, mă voi conduce după pașii propuși de microsoft, reprezentați în figura 1.



**Figura 1.** Configurare firewall windows 11.

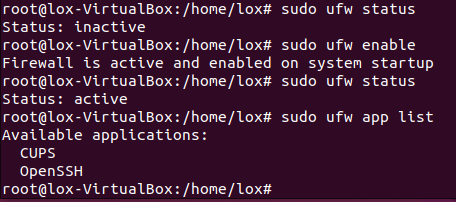
După activarea firewall-lui, ne vafișează protecția precum în figura 2. Observăm că firewall-ul este activ pentru toate rețelele și suntem în siguranță.



**Figura 2.** Windows Defender Firewall.

Pentru a configura un firewall pe linux, am folosit UFW (Firewall necomplicat), deoarece este ușor de utilizat și este instalat implicit în multe distribuții. Standart, în Ubuntu, UFW este dezactivat. Pentru a verifica starea acestuia, putem folosi comanda *sudo ufw status*.

Pentru a activa firewall-ul este nevoie de comanda *sudo ufw enable*, iar pentru dezactivare *sudo ufw disable*. Pașii respectivi sunt reprezentați în figura 3.



**Figura 3.** UFW Firewall.

De asemenea, putem verifica lista a aplicațiilor în care firewall-ul are reguli *sudo ufw app list*. Dacă dorim să păstrăm firewall-ul activat, dar să permitem accesul la computer de pe alte dispozitive din rețeaua locală, introducem *sudo ufw allow from 192.168.178.0/24*.

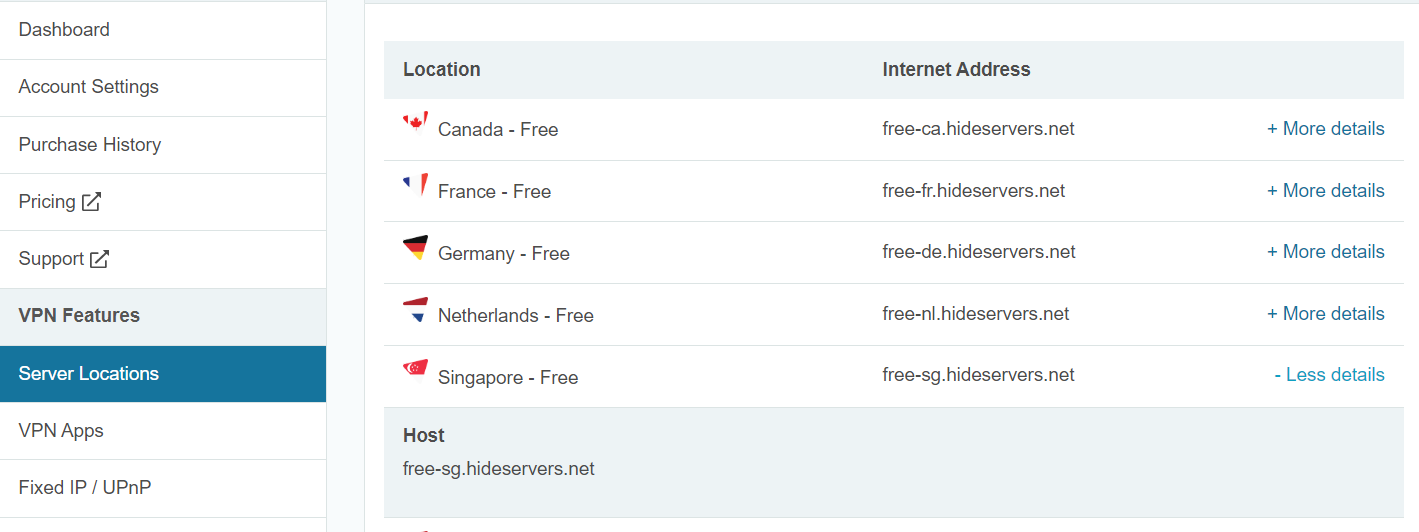
Pentru a șterge toate regulile personalizate și să revenim la configurarea inițială, vom folosi mai întâi *sudo ufw disable*, iar după *sudo ufw reset*, pentru a reseta.

**2. VPN (Virtual Private Network)**

**Setarea unui VPN**

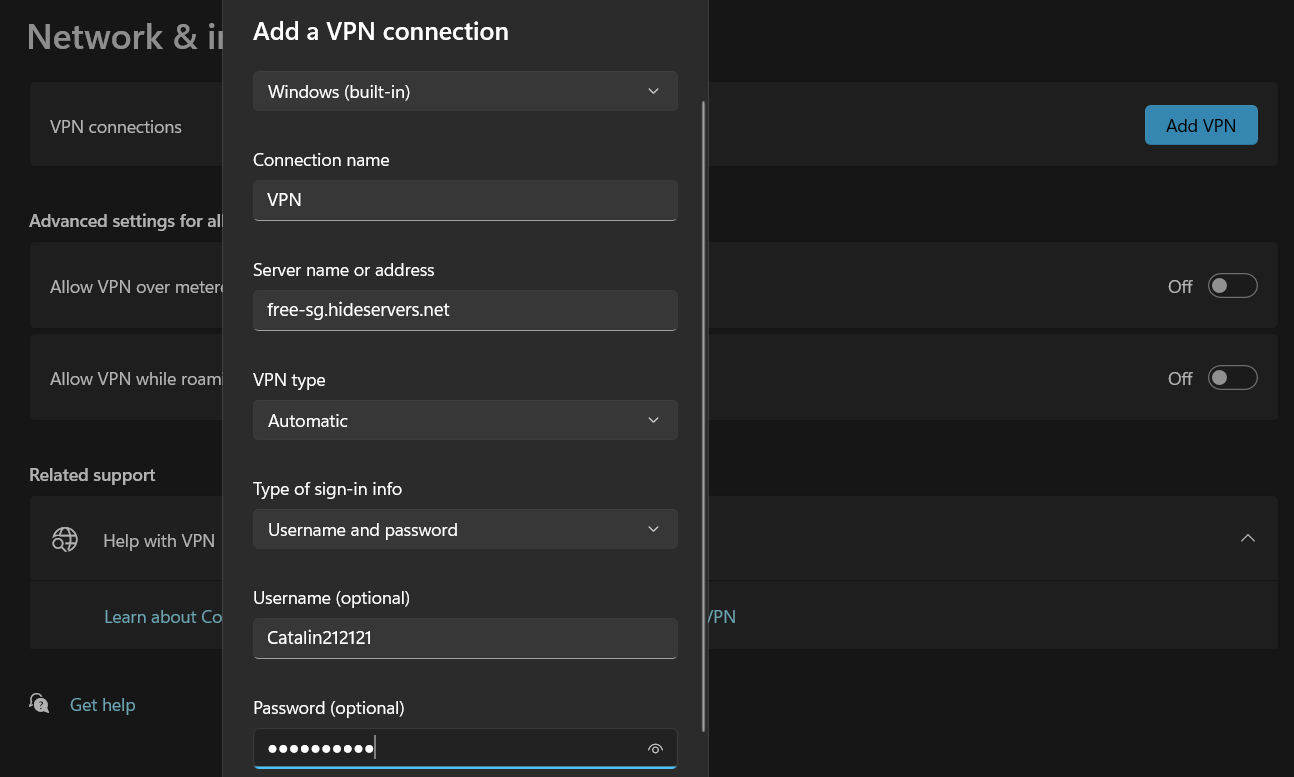
**Pentru setarea unui VPN pe sistemul Windows, am folosit serviciile oferite de compania Hide.me. Aceasta oferă servicii de rețea virtuală privată(VPN). Acest site este destinat exclusiv utilizatorilor Hide.me și oferă acces la funcții precum gestionarea contului, configurarea setărilor de securitate și descărcarea software-ului VPN. Cu serviciile Hide.me VPN, utilizatorii pot accesa conținut geo-restricționat, pot descărca fișiere de pe internet și pot naviga pe internet în mod securizat și anonim, fără a fi urmăriți sau înregistrați. Hide.me VPN oferă, de asemenea, o gamă largă de servere din diferite țări, ceea ce înseamnă că utilizatorii pot selecta serverul care se potrivește cel mai bine nevoilor lor specifice de navigare pe internet.**

Pentru a seta VPN-ul, este nevoie de a intra în setări la windows, după internet și securitate, alegem VPN și adăugăm adresa la VPN, pe care o luăm de la compania Hide.me. În figura 4, este reprezentat un exemplu de adresă de VPN.



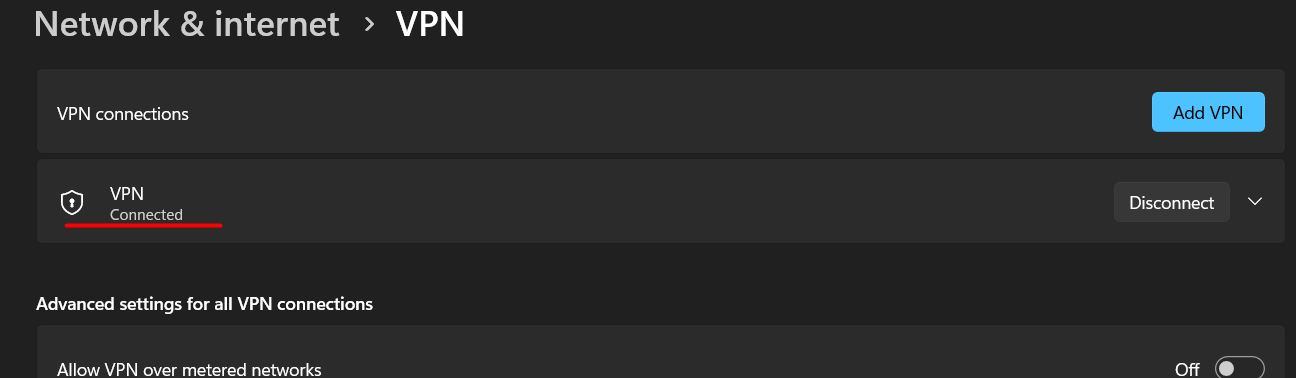
**Figura 4.** Configurare VPN windows.

Copiem hostul, după care al introducem în căsuța cu numele Server Address, cum este reprezentat în figura 5. Numele la cont și porola, este aceeași cu care ne-am conectat pe siteul Hide.me. Acestea sunt necesare pentru a acorda accesul la VPN, doar utilizatorilor autentificați.



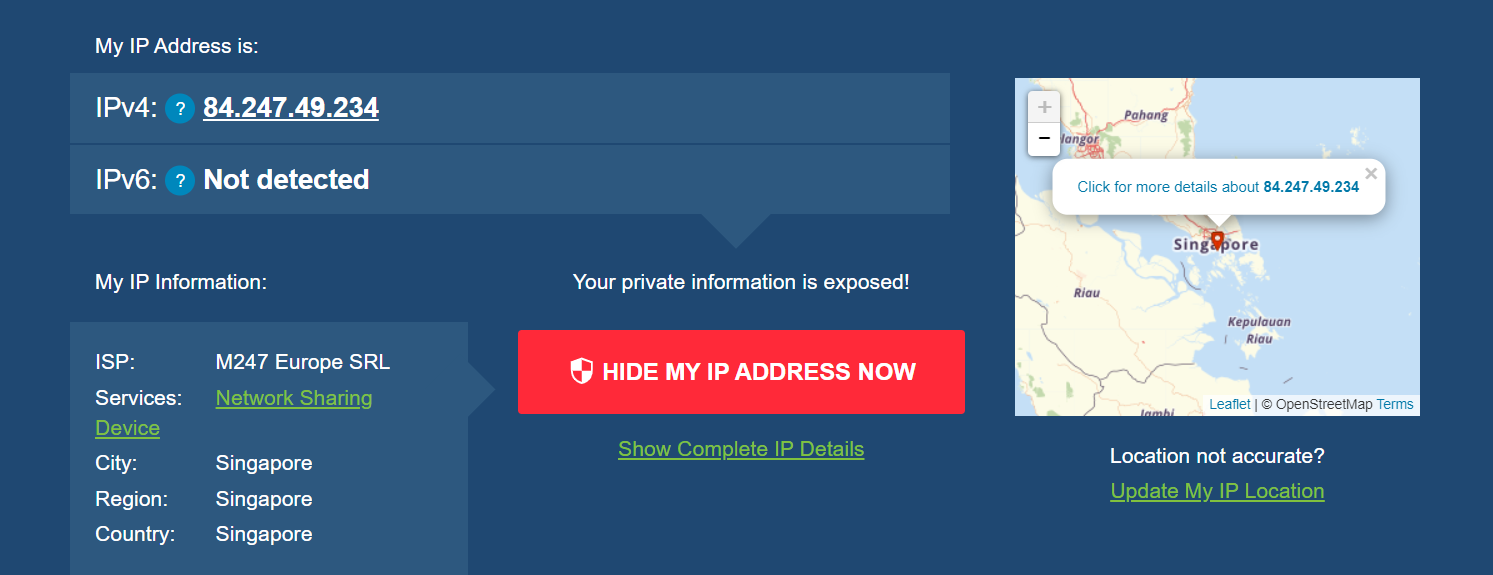
**Figura 5**. VPN Windows 11.

După salvarea datelor, verificăm conectare. După cum observăm în figura 6, conectarea este cu succes.



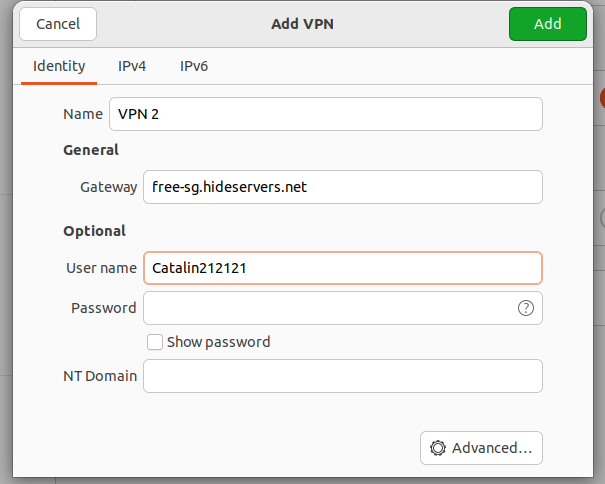
**Figura 6.** Conectare cu succes.

De asemenea, am efectuat verificare la locația IP. Cum observăm în figura 7, locația este în Singapur. Respectiv, configurarea este cu succes.



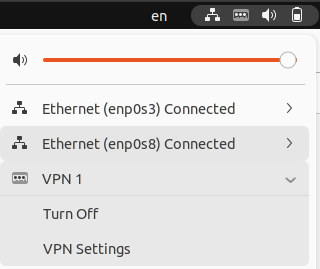
**Figura 7.** Verificare VPN.

Pentru a configura un VPN pe Linuxx Ubuntu, este nevoie de a intra în serări, network și alegem adăugare VPN. În continuare este nevoie de a introduce Gateway-ul, numele de utilizator și parola, cum este reprezentat în figura 8.



**Figura 8.** Configurare VPN Ubuntu.

După conectarea VPN-lui, se va fișa ca în figura 9. Respectiv putem dezactiva VPN-ul sau redacta setările.



**Figura 9.** Afișare VPN.

**Protocoale VPN (IPSec SSTP)**

Protocoalele VPN sunt utilizate pentru a crea conexiuni sigure între dispozitivele aflate în rețele diferite, prin intermediul internetului sau a altor rețele publice. Aceste protocoale permit transferul datelor într-un mod sigur, folosind criptarea informațiilor transmise între dispozitive. Două dintre cele mai utilizate protocoale VPN sunt IPSec și SSTP.

IPSec (Internet Protocol Security) este un protocol standard de securitate pentru comunicațiile de rețea. Acesta este utilizat pentru a asigura autentificarea și criptarea datelor în timpul transmiterii lor între dispozitive. IPSec poate fi utilizat în două moduri: modul de transport și modul de tunel. În modul de transport, numai datele sunt criptate, în timp ce în modul de tunel, întreaga conexiune între dispozitive este criptată.

SSTP (Secure Socket Tunneling Protocol) este un protocol de tunelare VPN dezvoltat de Microsoft. Acesta utilizează SSL (Secure Sockets Layer) pentru a cripta datele transmise între dispozitive. SSTP este un protocol sigur și fiabil, care poate fi utilizat cu succes în rețelele VPN.

Ambele protocoale oferă niveluri ridicate de securitate și criptare, ceea ce le face ideale pentru utilizarea în rețelele VPN. În timp ce IPSec este utilizat în mod obișnuit pentru conexiuni VPN site-to-site, SSTP este mai frecvent utilizat în conexiuni VPN de tip client-to-site, în care un utilizator se conectează la o rețea de la distanță.

**Efectul de tunel**

Efectul de tunel (sau tunelarea) este un concept cheie în tehnologia VPN (Virtual Private Network). Acesta se referă la faptul că o conexiune VPN creează o "tunel" prin intermediul căruia datele pot fi transmise în siguranță între două sau mai multe puncte de pe internet.

Atunci când se stabilește o conexiune VPN, datele sunt încapsulate (împachetate) într-un pachet special, denumit "pachet VPN", care este criptat și apoi trimis prin intermediul tunelului creat prin intermediul rețelei publice de internet. În acest fel, datele pot fi transmise în siguranță între cele două puncte, fără a fi interceptate sau accesate de către terți.

Efectul de tunel este esențial pentru securitatea VPN-ului, deoarece criptarea și encapsularea datelor le protejează împotriva interceptării sau a accesării neautorizate în timp ce traversează rețeaua publică de internet. Acest efect de tunel este creat prin utilizarea protocoalelor speciale de VPN, cum ar fi IPSec sau SSTP, care sunt proiectate pentru a asigura securitatea și confidențialitatea datelor în timpul transferului.

Prin urmare, efectul de tunelare este unul dintre cele mai importante aspecte ale tehnologiei VPN și permite utilizatorilor să se conecteze în siguranță la rețelele private de la distanță, astfel încât să poată accesa resursele rețelei într-un mod securizat și privat, indiferent de locația fizică.

**Tipuri de VPN. Aplicații**

Există mai multe tipuri de VPN, fiecare fiind potrivit pentru situații diferite. Câteva dintre cele mai comune tipuri de VPN sunt:

* VPN de acces la distanță: Acest tip de VPN permite utilizatorilor să se conecteze la rețele de la distanță, utilizând o conexiune securizată. VPN de acces la distanță este util pentru a permite angajaților să se conecteze la rețelele corporative de la distanță sau pentru a oferi acces sigur la rețelele pentru clienți și parteneri.
* VPN site-to-site: Acest tip de VPN conectează două sau mai multe rețele într-o rețea securizată. VPN site-to-site este util în situațiile în care trebuie să fie conectate mai multe locații geografice sau filiale.
* VPN de intrare în rețea: Acest tip de VPN se concentrează pe securizarea traficului de intrare în rețeaua companiei. VPN de intrare în rețea poate fi utilizat pentru a proteja împotriva atacurilor DDoS și pentru a monitoriza și limita traficul de la utilizatorii externi.
* VPN de ieșire din rețea: Acest tip de VPN se concentrează pe securizarea traficului de ieșire din rețeaua companiei. VPN de ieșire din rețea poate fi utilizat pentru a proteja împotriva atacurilor cibernetice, pentru a bloca accesul la site-uri web nedorite și pentru a monitoriza și limita traficul către site-urile și serviciile online.

Aplicațiile VPN sunt foarte variate și includ:

* Accesul la rețele de la distanță: Angajații pot accesa rețelele de la distanță, astfel încât să poată lucra în siguranță și eficient de oriunde se află.
* Protejarea informațiilor confidențiale: VPN-ul criptează datele transmise între dispozitive, protejând astfel informațiile confidențiale de accesul neautorizat.
* Accesul la site-uri și servicii restricționate: VPN-ul poate fi utilizat pentru a accesa site-uri și servicii care sunt restricționate în anumite țări sau regiuni.
* Protejarea vieții private online: VPN-ul protejează adresa IP și alte informații personale, ajutând utilizatorii să navigheze pe internet în mod anonim și în siguranță.

**3. Tehnologiile IDS și IPS**

**Configurarea unui IDS (Intrusion Detection System)**

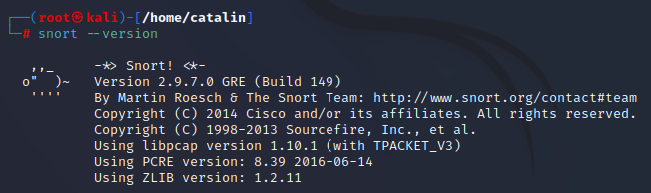
**Snort este un sistem de detectare a intruziunilor (IDS - Intrusion Detection System) open-source, dezvoltat inițial de către Martin Roesch. Scopul acestuia este de a monitoriza traficul rețelei și de a identifica activitățile suspecte sau neautorizate.**

**Snort poate detecta o varietate de atacuri, inclusiv: scanarea porturilor, încercările brute-force de autentificare, atacuri de tip DoS (Denial of Service), atacuri de tip buffer overflow, exploit-uri, malware și multe altele. De asemenea, Snort poate fi configurat să detecteze și să prevină anumite tipuri de atacuri prin adăugarea de reguli specifice.**

Pentru a instala Snort, am folosit comanda *sudo apt install snort*, dar mai întâi am folosit cheile specifice publice:

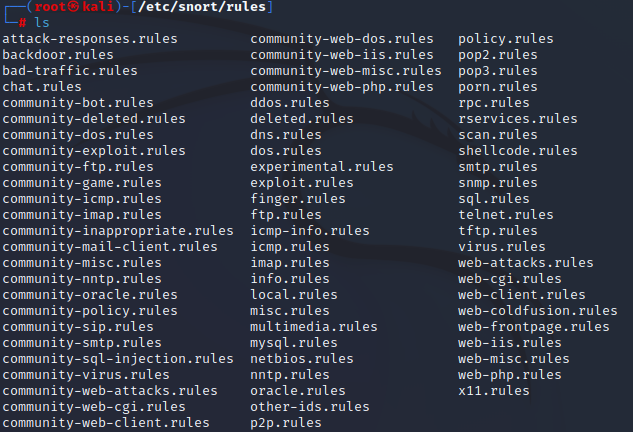
* sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 3B4FE6ACC0B21F32
* sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 871920D1991BC93C

După instalare putem verifica versiunea la Snort, observăm în figura 10.

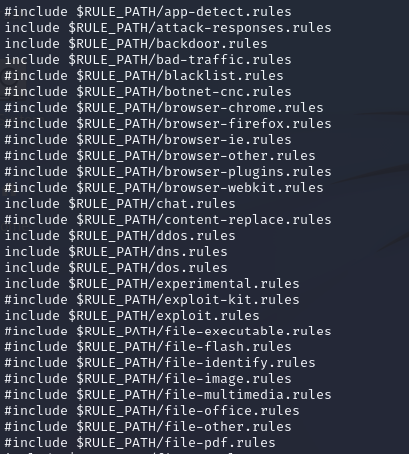


**Figura 10.** Snort versiune.

Regulile necesare au fost setate automat, iar pentru a le vizualiza este nevoie de a naviga în directoriu */etc/snort/rules* și folosim comanda *ls*. Regulele le observăm în figura 11. De asemenea, putem verifica regulile și prin navigarea în directoriu */etc/snort/snort.conf*, afișarea este în figura 12.



**Figura 11.** Regulile Snort.



**Figura 12.** Fișierul snort.conf.

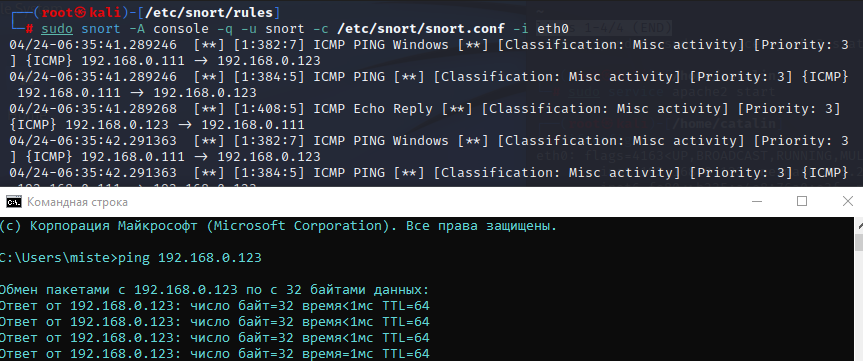
În fișierul snort.conf sunt foarte multe reguli, dar, din motiv că nu încap în imagine, am reprezentat doar câteva în figura 12.

Pentru a da start la Snort, am folosit comanda precum este reprezentat în figura 13.



**Figura 13.** Activare Snort.

Respectciv, dacă o sa facem ping pe calculator, vom avea o afișsare precum în figura 14, ceea ce ne demonstrează că Snort a detectat operațiunea.



**Figura 14**. Verificare funcționare.

**Configurarea unui IPS (Intrusion Prevention System)**

Suricata este un sistem de prevenire a intruziunilor (IPS - Intrusion Prevention System) open-source, dezvoltat de către comunitatea de securitate informatică pentru a identifica și preveni atacurile cibernetice în timp real. Suricata poate monitoriza traficul de rețea și poate detecta atacurile, cum ar fi scanările de porturi, exploatarea vulnerabilităților cunoscute și atacurile de tipul "buffer overflow". Datorită capacității sale de a detecta atacuri bazate pe semnături, dar și prin analiza comportamentală și prin identificarea de anomalii, Suricata poate preveni cu succes atacurile asupra rețelelor și sistemelor. Suricata este un IPS flexibil și scalabil, ceea ce îl face potrivit atât pentru utilizatorii casnici, cât și pentru întreprinderile mari și complexe. Suricata este disponibil sub licența GNU GPL și poate fi descărcat și utilizat gratuit.

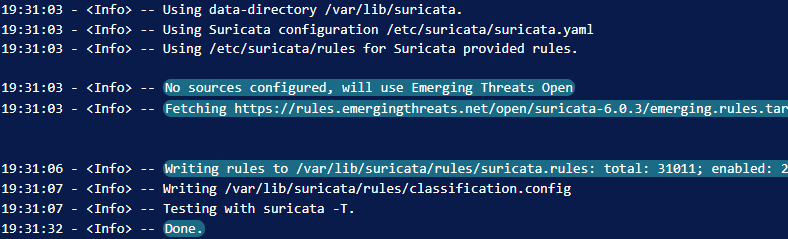
Pentru a începe instalarea Suricata, va trebui să adăugăm informațiile din depozitul software al Open Information Security Foundation (OISF) la sistemul dumneavoastră Ubuntu. Putem folosi comanda *add-apt-repository* pentru a face acest lucru.



**Figura 15.** Adăugare repositoriu.

După care, putem rula comanda de instalare Suricata, *sudo apt install suricata*.

Pentru a actualiza setul de reguli Suricata, am folosit un instrument numit *suricata-update*. Acesta poate prelua seturi de reguli de la furnizori externi. În afișare ar trebui să avem ca îm figura 16.



**Figura 16.** Actualizare reguli.

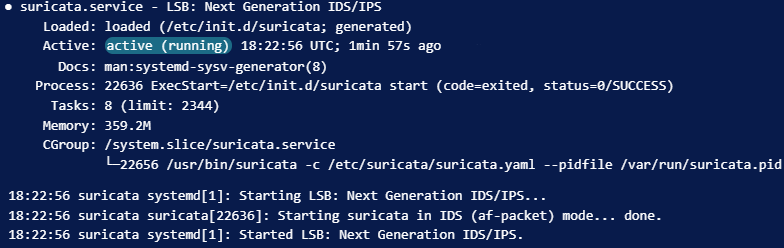
În pasul următor vom activa deja Suricata, folosind comanda

* **$ sudo systemctl start suricata.service**

Iar pentru a verifica statutul Suricata am folosit comanda

* **$ sudo systemctl status suricata.service**

În figura 17, este reprezentat cum arată statutul la Suricata.



**Figura 17.** Status Suricata.

Pentru a verifica funcționalitatea, voi rula comanda:

* **$ curl** [**http://testmynids.org/uid/index.html**](http://testmynids.org/uid/index.html)

În acest pas, am testat regula ET open cu numărul 2100498 folosind comanda curl. Astefl, rulând comanda, vom genera o solicitare HTTP, care va returna un răspuns care se potrivește cu regula de alertă a lui Suricata.



**Figura 18.** Generarea solicitării.

Acest exemplu de date de răspuns este conceput pentru a declanșa o alertă, pretizând că returnează rezultatul unei comenzi de genul id care are putea rula pe un sistem la distanță compromis printr-un shell web.

Acum putem verifica jurnalele Suricata pentru o alertă corespunzătoare. Există două jurnale care sunt activate cu configurația implicită Suricata. Primul este în */var/log/suricata/fast.log*.

Astfel, folosim comanda **$ grep 2100498 /var/log/suricata/fast.log,** pentru a verifica o intrare în jurnal. Respectiv se va afișa un astfel de răspuns, ca în figura 19.

01/05/2023-18:35:57.247239 [\*\*] [1:2100498:7] GPL ATTACK\_RESPONSE id check returned root [\*\*] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.56.1:80 -> 203.0.113.1:36364

**Figura 19.** Vizualizare fișier fast.log.

**Concluzie**

În concluzie, securitatea cibernetică este o preocupare majoră în lumea digitală în care trăim, iar Firewall-ul, VPN-ul, IDS și IPS sunt instrumente esențiale pentru protejarea rețelelor noastre împotriva atacurilor și amenințărilor cibernetice. Firewall-ul este primul nivel de apărare împotriva intruziunilor și este esențial să fie configurat corespunzător pentru a asigura protecția rețelei noastre. VPN-ul oferă o modalitate sigură de a accesa rețelele într-un mod securizat și privat, iar IDS și IPS ajută la detectarea și prevenirea atacurilor cibernetice. Configurarea acestor instrumente de securitate este crucială și trebuie să fie făcută cu atenție pentru a asigura o protecție adecvată împotriva amenințărilor cibernetice.