Ministrerul Educației și Cercetării a Republicii Moldova

Universitatea Tehnică a Moldovei

Facultatea Calculatoare Informatică și Microelectronică

# RAPORT

la lucrarea de laborator nr. 5

la Tehnologii ale Securității Informaționale

**Tema:** **”** **Configurare firewall software și VPN”**

      A efectuat:                                       st. TI-213, Caraman Eliza

A verificat:                                      Rodica Bulai

Chişinău 2023

**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)

**Firewall-ul** este un sistem de securitate care ajută la protejarea rețelei și a dispozitivelor conectate la ea împotriva atacurilor cibernetice. Acesta analizează traficul de date care intră și iese din rețea și blochează sau permite accesul în funcție de regulile de securitate predefinite.

Configurarea Windows Firewall:

* Windows Firewall este inclus în sistemul de operare Windows și este activat în mod implicit. Pentru a configura Windows Firewall, urmați acești pași:
* Deschideți "Windows Defender Firewall" din "Control Panel" sau din "Settings".
* Selectați "Allow an app or feature through Windows Defender Firewall".
* Selectați aplicațiile sau caracteristicile pe care doriți să le permiteți sau să le blocați.
* Puteți, de asemenea, să creați reguli personalizate pentru aplicațiile dvs. prin selectarea opțiunii "Advanced Settings" din meniul lateral.

Configurarea Firewall în Linux:

Există mai multe opțiuni pentru configurarea firewall-ului în Linux, dar cea mai comună este utilizarea iptables. Iptables este o interfață de linie de comandă pentru firewall-ul Linux și poate fi configurat pentru a bloca sau permite traficul de rețea în funcție de regulile predefinite.

Iată câțiva pași de bază pentru configurarea iptables în Linux:

* Verificați starea actuală a iptables cu comanda "sudo iptables -L".
* Creați o nouă regulă pentru a permite sau bloca traficul cu comanda "sudo iptables -A INPUT -s [adresa IP] -j [ACCEPT / DROP]".
* Salvați configurarea cu comanda "sudo iptables-save".
* Verificați din nou starea firewall-ului cu comanda "sudo iptables -L".

**Tipuri de Firewall:**

Există mai multe tipuri de firewall-uri, printre care:

* Firewall-uri de rețea: Acestea sunt instalate între rețelele separate pentru a controla traficul de date între ele.
* Firewall-uri de host: Acestea sunt instalate pe un singur dispozitiv pentru a controla traficul de date către și dinspre acel dispozitiv.
* Firewall-uri personale: Acestea sunt destinate utilizării individuale și sunt instalate pe computerul personal pentru a proteja împotriva atacurilor cibernetice.

**Importanța Firewall-urilor:**

Firewall-urile sunt importante pentru protejarea rețelei și a dispozitivelor conectate la ea împotriva atacurilor cibernetice, cum ar fi hacking-ul, malware-ul și phishing-ul. Ele ajută la blocarea traficului de date nedorit sau periculos, astfel încât să nu ajungă la dispozitivele conectate la rețea. Prin urmare, este important să configurați și să utilizați un firewall pe toate dispozitivele conectate la rețea pentru a asigura securitatea rețelei și a datelor.

Graphical user interface, text, application

Description automatically generated

*Figura 1 – Fereastra de acces Firewall*

**VPN sau Virtual Private Network** este o tehnologie care oferă o conexiune securizată între două sau mai multe dispozitive prin intermediul internetului. Aceasta ajută la protejarea datelor și a identității utilizatorilor împotriva interceptării și atacurilor cibernetice.

Setarea unui VPN:

Iată câțiva pași de bază pentru setarea unui VPN:

* Alegeți un furnizor de servicii VPN și creați un cont.
* Descărcați și instalați aplicația VPN pe dispozitivul dvs.
* Conectați-vă la serverul VPN și introduceți credențialele de autentificare.
* Puteți selecta un server dintr-o listă de servere disponibile și alegeți protocoalele de securitate dorite.

Protocoale VPN (IPSec SSTP), Efectul de tunel:

Există mai multe protocoale VPN disponibile, cum ar fi:

* IPSec (Internet Protocol Security): Este un protocol de securitate care oferă autentificare, confidențialitate și integritate pentru datele transmise prin intermediul rețelei. Acesta creează un canal criptat între două dispozitive care utilizează VPN.
* SSTP (Secure Socket Tunneling Protocol): Este un protocol VPN dezvoltat de Microsoft. Acesta utilizează SSL/TLS pentru a cripta traficul de date și este utilizat în special pe sistemele de operare Windows.

Efectul de tunel se referă la crearea unui canal securizat între două dispozitive care utilizează VPN. Acest canal criptat protejează datele transmise între dispozitive și împiedică interceptarea sau modificarea lor.

Tipuri de VPN, Aplicații:

Există mai multe tipuri de VPN disponibile, inclusiv:

* VPN de acces: Acesta permite utilizatorilor să acceseze rețelele private de la distanță. Aceasta este utilizată frecvent de angajați pentru a se conecta la rețelele de la locul de muncă.
* VPN de site-to-site: Acesta conectează două sau mai multe rețele private între ele prin intermediul internetului.
* VPN de rețea privată virtuală: Acesta permite utilizatorilor să se conecteze la o rețea privată prin intermediul internetului, ceea ce le permite să acceseze resursele și datele rețelei fără a fi fizic conectați la aceasta.

VPN-urile sunt utilizate frecvent în aplicații care necesită securitate și confidențialitate, cum ar fi:

* Accesarea rețelelor de la distanță în scopuri de lucru.
* Accesarea conținutului restricționat geografic, cum ar fi site-uri web sau servicii de streaming.
* Utilizarea de aplicații de mesagerie sau de partajare a fișierelor în mod securizat.
* Conectarea la rețele private din afara locației fizice a utilizatorului, cum ar fi sucursale sau centre de date.

Graphical user interface, application

Description automatically generated

*Figura 2 – Setarea unui tunel VPN din sitemului de operare Windows 11*

IDS (Intrusion Detection System) și IPS (Intrusion Prevention System) sunt tehnologii utilizate pentru a detecta și preveni atacurile cibernetice asupra unei rețele sau sistem informatic. IDS detectează atacurile cibernetice, în timp ce IPS previne atacurile și poate bloca traficul neautorizat.

Configurarea unui IDS:

Pentru a configura un IDS, urmați acești pași:

* Selectați un IDS software sau hardware care să se potrivească cu nevoile dvs.
* Instalați și configurați IDS pe rețeaua sau sistemul dvs. informatic.
* Configurați regulile de detecție a atacurilor. Acestea includ setarea alarmelor pentru anumite evenimente sau blocarea traficului neautorizat.
* Configurați alarmele și alertele pentru a vă informa când apare un atac cibernetic.
* Monitorizați IDS pentru a vă asigura că funcționează corect.

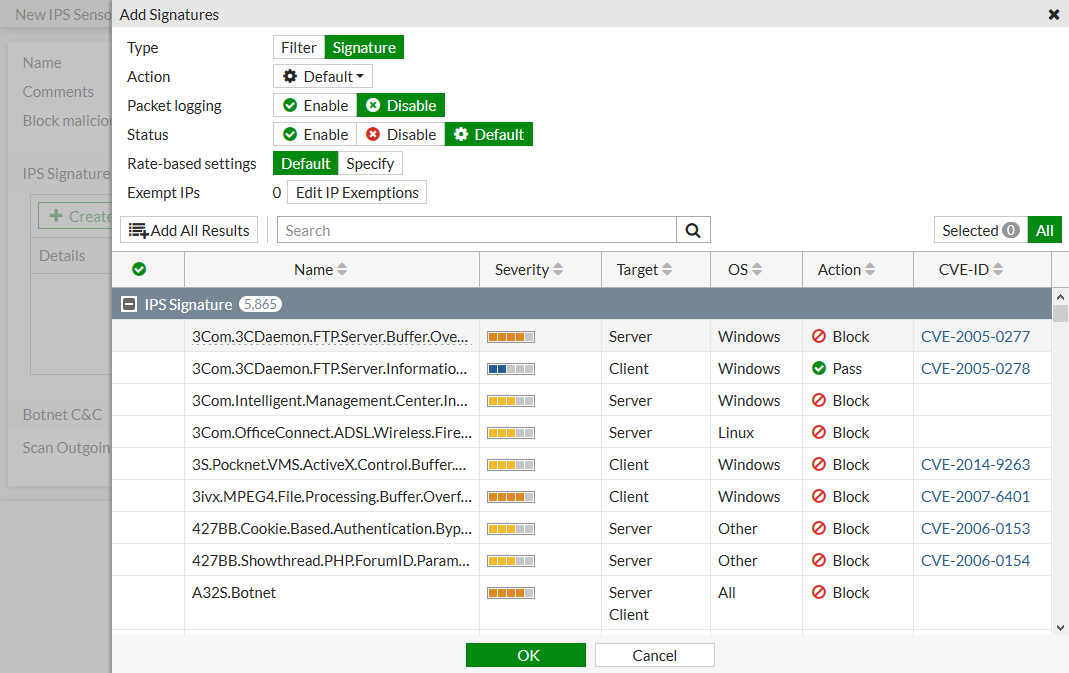
Configurarea unui IPS:

Pentru a configura un IPS, urmați acești pași:

* Selectați un IPS software sau hardware care să se potrivească cu nevoile dvs.
* Instalați și configurați IPS pe rețeaua sau sistemul dvs. informatic.
* Configurați regulile de prevenire a atacurilor. Acestea includ blocarea traficului neautorizat sau aplicarea altor măsuri de securitate, cum ar fi criptarea datelor.
* Configurați IPS pentru a vă informa când apare un atac cibernetic și pentru a bloca traficul neautorizat.
* Monitorizați IPS pentru a vă asigura că funcționează corect.

***Pentru a configura adresele IP în aplicația FortiGate, urmați acești pași:***

1. Accesați interfața web a dispozitivului FortiGate.
2. Conectați-vă la interfața CLI (Command Line Interface) folosind un client SSH.
3. Selectați opțiunea "Network" din meniul principal și apoi "Interfaces".
4. Selectați interfața de rețea pe care doriți să o configurați și faceți clic pe butonul "Edit".
5. În pagina de configurare a interfeței, faceți clic pe butonul "IPv4" sau "IPv6", în funcție de tipul de adresă IP pe care doriți să o configurați.
6. Introduceți adresa IP dorită, precum și subnet mask și gateway-ul corespunzător.
7. Dacă doriți să utilizați DNS-uri personalizate, introduceți adresele DNS corespunzătoare.
8. Faceți clic pe butonul "OK" pentru a salva configurația.
9. Repetați acești pași pentru fiecare interfață de rețea pe care doriți să o configurați.
10. După ce ați finalizat configurarea, faceți clic pe butonul "Apply" pentru a aplica noile setări.
11. Verificați configurația pentru a vă asigura că adresele IP au fost configurate corect. Pentru aceasta, puteți utiliza comanda "show interface" în CLI sau puteți verifica informațiile de configurare în interfața web.
12. Dacă doriți să configurați adrese IP suplimentare pe aceeași interfață, puteți face acest lucru prin accesarea paginii de configurare a interfeței și apoi selectând opțiunea "Add" în secțiunea "IPv4" sau "IPv6".
13. După ce ați terminat de configurat adresele IP, ar trebui să verificați și să configurați setările de securitate corespunzătoare pentru a proteja rețeaua dvs.
14. Dacă întâmpinați probleme în timpul procesului de configurare, puteți accesa documentația FortiGate sau puteți solicita asistență tehnică de la Fortinet sau de la partenerul Fortinet local.



*Figura 3 – Secventa de configurare a IPS*

**Concluzie:**

În urma lucrării de laborator la tema VPN și IPS, am învățat că utilizarea unei conexiuni VPN este esențială în protejarea datelor și a rețelelor într-un mediu online, mai ales în ceea ce privește accesul la resurse de la distanță. De asemenea, am înțeles importanța implementării unui sistem IPS pentru a detecta și preveni atacurile cibernetice.

Această experiență de învățare ne-a permis să dezvoltăm abilitățile practice în implementarea acestor tehnologii, cum ar fi configurarea unui sistem IPS folosind software-ul FortiGate și analizarea log-urilor generate de sistem pentru a identifica și preveni potențialele amenințări cibernetice.

Este important să ne dezvoltăm astfel de abilități într-un mediu cibernetic din ce în ce mai complex, deoarece acestea sunt esențiale pentru protejarea datelor și a rețelelor în fața amenințărilor cibernetice. În concluzie, lucrarea de laborator la tema VPN și IPS a fost o experiență utilă și informativă, care ne-a permis să înțelegem importanța acestor tehnologii și să ne dezvoltăm abilitățile practice în implementarea lor.