**Ministerul Educației și Cercetării al Republicii Moldova**

**Universitatea Tehnică a Moldovei**

**Facultatea Calculatoare, Informatică și Microelectronică**

**RAPORT**

Lucrarea de laborator nr.5

*la Tehnologii ale Securității Informaționale*

Tema: Configurare firewall software și VPN

A efectuat:

st. gr. TI-216 Ștefan Vlașițchi

A verificat:

asist. univ. M. Zalesciuc

Chișinău - 2023

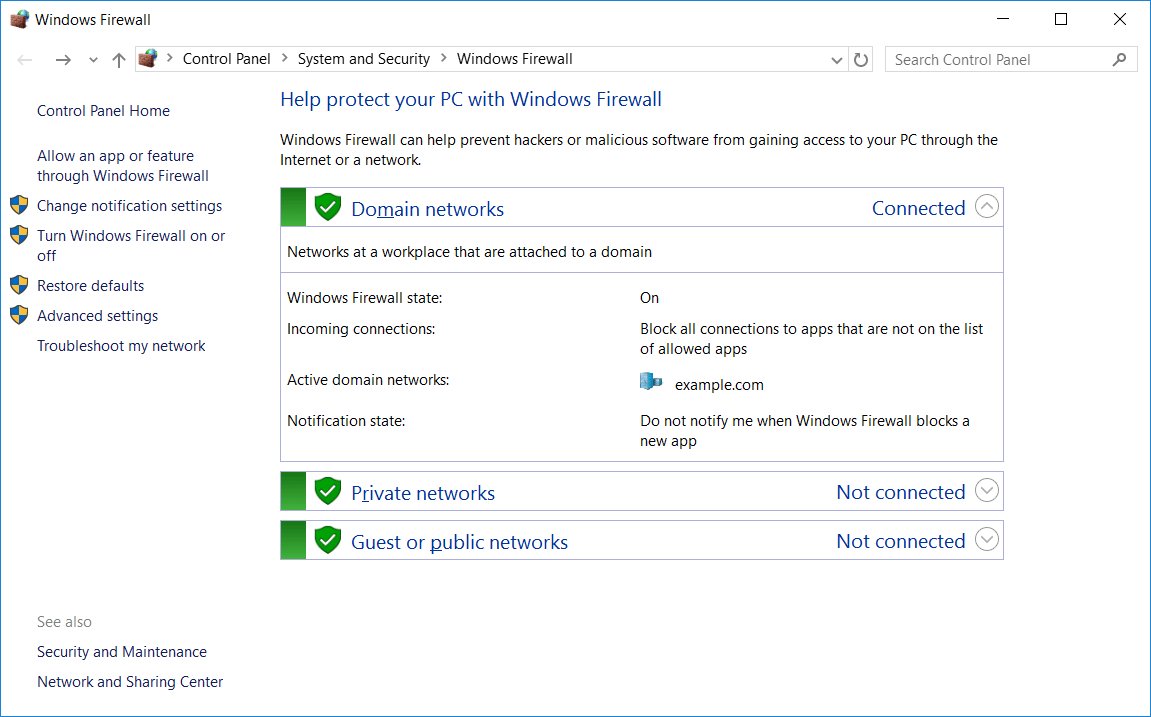
**Lucrare de laborator nr 5**

**Scopul lucrarii:**

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)

**Continutul lucrarii:**

Setările de bază ale firewall-ului Windows pot fi modificate prin intermediul Control Panel > System and Security > Windows Firewall, așa cum se arată mai jos. Această interfață poate fi accesată și prin PowerShell sau Command Prompt prin introducerea "firewall.cpl".

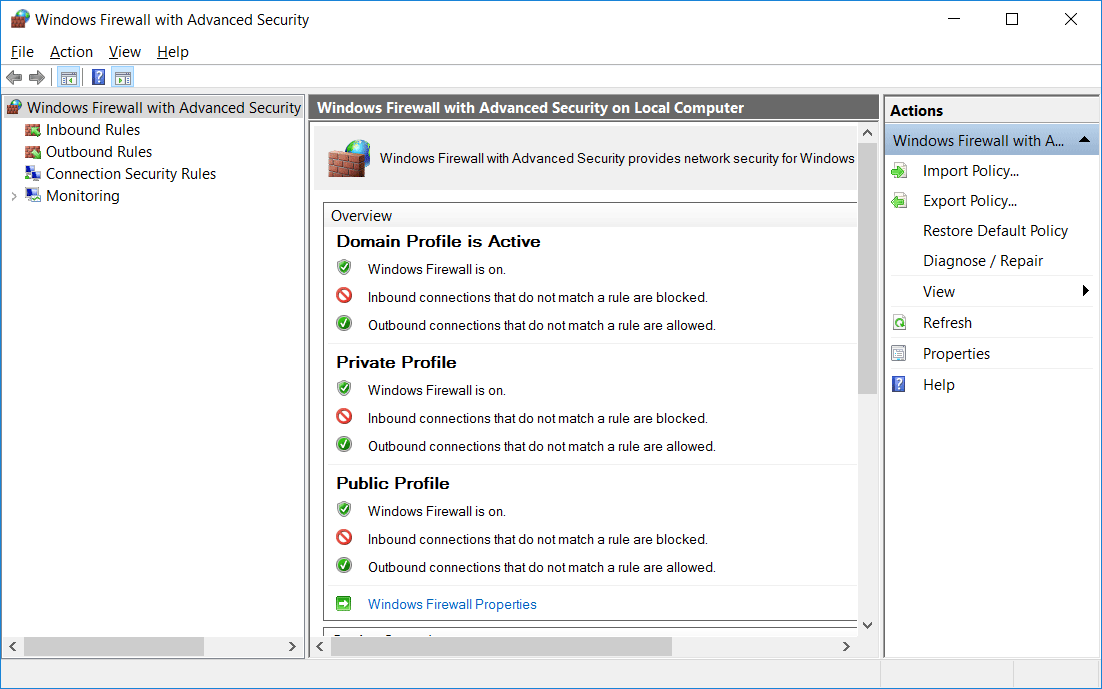
****

**Figura 1.** Firewall Control Panel

De aici putem vizualiza grafic starea firewall-ului pentru profilurile de domeniu, privat și public. Aceste profile diferite sunt utilizate în funcție de conexiunea de rețea curentă. De exemplu, dacă sunteți conectat la un domeniu Active Directory, regulile aplicate în profilul de domeniu vor fi utilizate, în timp ce dacă sunteți conectat la o rețea wireless publică, setările din profilul public vor fi utilizate.

Sarcinile care pot fi finalizate aici sunt afișate în meniul din stânga, dar nu vom intra în detalii aici deoarece ne vom ocupa mai ales de setările avansate. Pentru a accesa setările avansate, puteți selecta linkul de setări avansate din acest meniu din stânga din cadrul Windows Firewall.

După cum s-a menționat mai sus, putem deschide Windows Firewall cu Advanced Security făcând clic pe butonul de setări avansate din Windows Firewall. Putem de asemenea rula comanda 'wf.msc' în PowerShell sau Command Prompt pentru a deschide interfața de securitate avansată direct. Imaginea de mai jos arată interfața de securitate avansată după deschidere.

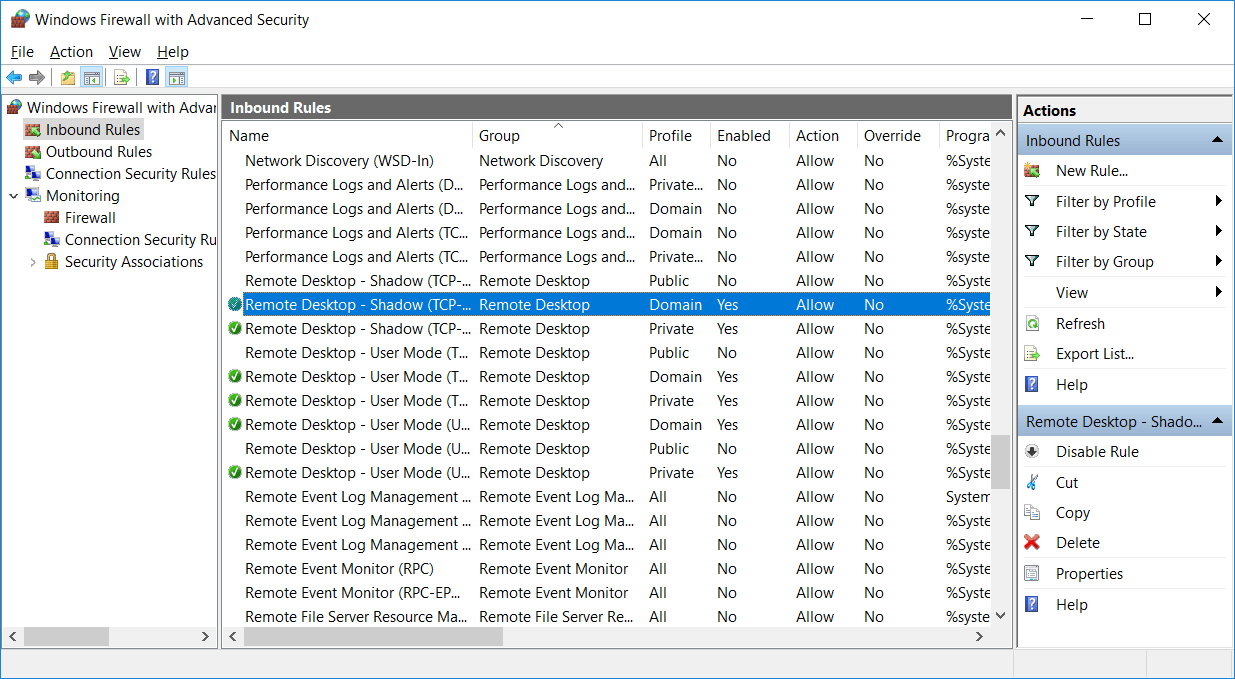


**Figura 2.** Firewall Control Panel-Advanced Settings

În această fereastră, putem vedea o prezentare generală a profilurilor de domeniu, privat și public, care în mod implicit ar trebui să fie activate și să blocheze traficul de intrare și să permită traficul de ieșire.

Din meniul din stânga, putem selecta regulile pentru traficul de intrare sau de ieșire. Deoarece toate conexiile de ieșire sunt permise în mod implicit, ne vom concentra aici pe regulile pentru traficul de intrare. De asemenea, pot fi configurate reguli de securitate pentru conexiunile IPSec, iar monitorizarea poate fi utilizată pentru a înregistra diferite evenimente ale firewall-ului.

Sub regulile de intrare și de ieșire, putem vizualiza regulile existente și cele care sunt activate în prezent. Aceste reguli sunt disponibile în mod implicit, regulile cu o pictogramă verde de bifare în stânga sunt activate și vor permite traficul, în timp ce regulile fără pictogramă sunt dezactivate.

**Figura 3.** Firewall Control Panel-Inbound Rules

O regulă dezactivată poate fi activată prin simpla selectare cu clic dreapta și selectarea opțiunii activare. La fel, putem selecta cu clic dreapta o regulă activată și să o schimbăm în dezactivată. De asemenea, putem vizualiza proprietățile regulii, selectând cu clic dreapta și selectând proprietățile. Acest lucru ne va permite să vedem ce face de fapt regula, inclusiv porturile care sunt permise prin firewall către programe specifice, vom vedea acest lucru în detaliu în continuare când vom crea propria regulă.

Pentru a configura firewall-ul in linux se foloseste aplicatia firewalld. Firewalld este un firewall open source, bazat pe gazdă, care încearcă să prevină accesul neautorizat la computer. Un firewall este de obicei o cerință minimă pentru orice echipă de securitate a informațiilor din orice organizație modernă, dar este și o idee bună pentru utilizarea generală a computerului. Firewalld poate restricționa accesul la servicii, porturi și rețele. Puteți bloca anumite subrețele și adrese IP.

1. Verificați configurația firewalld

Înainte de a începe, confirmați că firewalld rulează:

**$** sudo firewall-cmd --state

Ieșirea fie rulează, fie nu rulează. Pentru a porni firewall-ul dacă nu rulează, utilizați systemctl:

**$** sudo systemctl --enable --now firewalld

1. Vizualizare zone

Pentru a vizualiza toate zonele dintr-un sistem, utilizați --get-zonesopțiunea:

**$** sudo firewall-cmd --get-zones

Pentru a afișa zona implicită, utilizați --get-default-zone:

**$** sudo firewall-cmd --get-default-zone

În mod implicit, dacă firewalld este activat și rulează și în zona publică, tot traficul de intrare este respins, cu excepția SSH și DHCP.

1. Permiteți un port

Pentru a permite traficul de la orice IP printr-un anumit port, utilizați opțiunea --add-portîmpreună cu numărul portului și protocolul:

**$** sudo firewall-cmd --add-port=80/tcp

Această regulă intră în vigoare imediat, dar durează doar până la următoarea repornire. Adăugați --permanentsteagul pentru a-l face persistent:

**$** sudo firewall-cmd --add-port=80/tcp –permanent

1. Reîncărcați firewalld

Prefer să-mi reîncarc firewall-ul după ce am făcut modificări. Pentru a reîncărca firewalld și toate regulile permanente:

**$** sudo firewall-cmd --reload

1. Adăugați un serviciu

Există servicii predefinite pe care le puteți permite prin firewall. Pentru a vedea toate serviciile predefinite disponibile pe sistemul dvs.:

**$** sudo firewall-cmd --get-services

De exemplu, pentru a adăuga permanent serviciul HTTP la firewall, introduceți:

**$** sudo firewall-cmd --add-service=http --permanent

**$** sudo firewall-cmd --reload

Tipurile de firewall includ:

1. Firewall-uri de rețea: Acestea sunt amplasate între rețeaua internă și cea externă și monitorizează și controlează traficul de rețea. Ele pot fi hardware sau software și pot aplica politici de securitate pe baza adreselor IP, porturilor și protocoalelor.
2. Firewall-uri de aplicație: Acestea analizează traficul la nivel de aplicație și aplică politici de securitate pentru a preveni atacuri și acces neautorizat la aplicații. Ele pot monitoriza conținutul datelor și pot identifica atacuri precum SQL injection sau cross-site scripting.
3. Firewall-uri de bază de date: Acestea protejează bazele de date împotriva accesului neautorizat și a atacurilor. Ele pot restricționa accesul la baza de date în funcție de utilizatori, roluri și privilegii.

Importanța firewall-urilor constă în protejarea rețelelor și a sistemelor informatice împotriva amenințărilor și atacurilor cibernetice. Ele acționează ca o barieră între rețeaua internă și rețeaua externă (de exemplu, Internetul) și controlează fluxul de trafic, permițând doar conexiunile și comunicările autorizate să treacă prin ele. Acestea pot detecta și bloca atacurile cibernetice, cum ar fi scanarea porturilor, atacurile de tipul Denial of Service (DoS) sau tentativa de acces neautorizat la sistem. De asemenea, firewall-urile pot ajuta la implementarea politicii de securitate a unei organizații, restricționând accesul la anumite resurse și asigurând confidențialitatea și integritatea datelor.

Setarea unui VPN (Virtual Private Network) implică următoarele etape:

1. Alegerea unui furnizor de servicii VPN: Există numeroși furnizori de servicii VPN disponibili. Este important să alegi unul de încredere, care să ofere o conexiune sigură și stabilă.
2. Descărcarea și instalarea aplicației VPN: Majoritatea furnizorilor de VPN oferă aplicații dedicate pentru diferite dispozitive și sisteme de operare. Descarcă și instalează aplicația potrivită pe dispozitivul tău.
3. Crearea unui cont: După instalare, va trebui să creezi un cont la furnizorul de VPN. Aceasta poate implica furnizarea unei adrese de e-mail și a unei parole sau utilizarea altor metode de autentificare.
4. Conectarea la un server VPN: După autentificare, vei avea opțiunea de a selecta un server VPN la care să te conectezi. Furnizorii de VPN oferă de obicei o listă de servere din diferite țări și locații geografice. Poți alege un server dintr-o anumită țară pentru a obține o adresă IP din acea țară și pentru a-ți ascunde adresa IP reală.
5. Configurarea preferințelor de securitate: Aplicațiile VPN oferă de obicei opțiuni suplimentare de configurare a nivelului de securitate. Acestea pot include utilizarea protocoalelor VPN specifice, criptarea traficului sau setări de tip kill switch pentru a întrerupe conexiunea în cazul în care VPN-ul cade.
6. Conectarea la VPN: După configurare, poți conecta VPN-ul prin intermediul aplicației. Acest lucru va crea o conexiune criptată între dispozitivul tău și serverul VPN.
7. Testarea conexiunii VPN: Pentru a te asigura că VPN-ul funcționează corect, poți testa conexiunea prin verificarea adresei IP și a traficului tău pe internet. Există site-uri web specializate care îți pot afișa adresa IP actuală și locația, permițându-ți să verifici dacă VPN-ul funcționează corect.

Este important să menționez că procedura de setare a unui VPN poate varia în funcție de furnizorul de servicii VPN și de aplicația pe care o utilizezi. În general, însă, aceste etape ar trebui să te ajute să configurezi un VPN de bază pe dispozitivul tău.

Două protocoale VPN comune sunt IPSec (Internet Protocol Security) și SSTP (Secure Socket Tunneling Protocol).

IPSec este un set de protocoale și algoritmi utilizat pentru a crea și a gestiona conexiuni VPN securizate. Acesta oferă autentificare, confidențialitate și integritate a datelor prin criptarea traficului IP. IPSec poate fi utilizat în două moduri principale: modul de tunel și modul de transport. În modul de tunel, pachetele de date sunt criptate și plasate într-un nou pachet IP, ceea ce creează un tunel virtual între punctele finale ale VPN-ului. Acest tunel protejează traficul împotriva interceptării și modificării de către terți.

SSTP este un protocol VPN dezvoltat de Microsoft și este utilizat în special pe sistemele de operare Windows. SSTP utilizează SSL/TLS (Secure Sockets Layer/Transport Layer Security) pentru a stabili o conexiune criptată între client și server. Acest protocol poate trece prin firewalls care blochează alte protocoale VPN, deoarece utilizează portul TCP 443, care este adesea deschis pentru conexiuni HTTPS.

Efectul de tunel în cadrul unui VPN se referă la împachetarea și criptarea datelor originale într-un nou pachet de date, care este trimis prin intermediul unei conexiuni securizate între client și server. Aceasta înseamnă că traficul și informațiile transmise prin VPN sunt protejate împotriva interceptării și modificării de către terți, deoarece acestea sunt criptate în timpul tranzitului prin tunelul securizat. Astfel, efectul de tunel într-un VPN asigură confidențialitatea și securitatea datelor, permițând utilizatorilor să comunice într-un mod sigur prin intermediul rețelelor nesigure, cum ar fi Internetul public.

Există mai multe tipuri de VPN, fiecare având utilizări și caracteristici specifice. Iată câteva dintre cele mai comune tipuri de VPN și aplicațiile lor:

1. VPN pentru acces la distanță (Remote Access VPN): Acest tip de VPN permite utilizatorilor să se conecteze în siguranță la rețelele organizației lor de la distanță. Este util pentru angajații care lucrează de acasă sau sunt în deplasare și doresc să acceseze resursele și datele din rețeaua internă a companiei într-un mod securizat.
2. VPN de site-to-site: Acest tip de VPN leagă două sau mai multe rețele locale (site-uri) și permite comunicarea securizată între ele prin intermediul Internetului. Este utilizat de obicei de către organizații cu filiale multiple sau birouri regionale pentru a crea o rețea privată virtuală între acestea.
3. VPN pentru securitate în rețele publice (Public Wi-Fi VPN): Acest tip de VPN este destinat utilizatorilor care doresc să se conecteze în siguranță la rețelele publice Wi-Fi, care pot fi nesigure și expuse la riscuri de securitate. VPN-ul criptează traficul lor și îi protejează împotriva interceptării și atacurilor cibernetice.
4. VPN pentru circumvenirea restricțiilor geografice (Geographic Restriction Bypass VPN): Acest tip de VPN permite utilizatorilor să acceseze conținut online care este restricționat geografic. Prin conectarea la un server VPN dintr-o țară specifică, utilizatorii pot obține o adresă IP din acea țară și pot accesa conținutul restricționat în mod normal în acel loc.
5. VPN pentru confidențialitate online (Privacy VPN): Acest tip de VPN oferă utilizatorilor confidențialitate și anonimitate online prin criptarea traficului lor și ascunderea adresei IP reale. Este util pentru protejarea vieții private, evitarea monitorizării și a colectării de date de către terțe părți și pentru deblocarea conținutului restricționat geografic.

Acestea sunt doar câteva exemple de tipuri de VPN și aplicațiile lor. În funcție de nevoile și scopurile individuale, există și alte variante de VPN care pot fi utilizate pentru diverse scenarii și cerințe de securitate și conectivitate.

Configurarea unui IDS (Intrusion Detection System) implică următoarele etape:

1. Planificarea și analiza cerințelor: Începe prin a determina obiectivele și cerințele tale specifice în ceea ce privește IDS-ul. Ce tipuri de atacuri sau activități dorești să detectezi? Ce resurse de rețea și sisteme dorești să monitorizezi? Aceste informații te vor ajuta să configurezi IDS-ul în mod corespunzător.
2. Selecția și implementarea IDS-ului potrivit: Există diferite soluții IDS disponibile, atât open-source, cât și comerciale. Alege un IDS care se potrivește nevoilor și infrastructurii tale. Instalează și configurează IDS-ul pe un sistem dedicat sau pe un server existent.
3. Definirea politicilor de detectare: IDS-ul are nevoie de politici de detectare pentru a identifica activitățile suspecte sau atacurile. Configurează reguli și filtre specifice pentru a monitoriza și a detecta semnalele de alarmă. Acestea pot fi bazate pe semnături cunoscute ale atacurilor, comportament anormal al traficului sau alte criterii.
4. Configurarea surselor de date: IDS-ul trebuie să monitorizeze fluxul de trafic sau evenimentele relevante pentru detectarea intruziunilor. Configură sursele de date, cum ar fi logurile de sistem, logurile de firewall sau traficul de rețea, astfel încât IDS-ul să poată analiza aceste informații.
5. Configurarea alertelor și notificărilor: Setează opțiuni de alertare pentru IDS, astfel încât să primești notificări în timp real sau să genereze înregistrări de evenimente pentru activitățile suspecte detectate. Aceasta îți permite să răspunzi rapid la eventualele incidente de securitate.
6. Testarea și ajustarea IDS-ului: După configurare, testează IDS-ul pentru a te asigura că funcționează corespunzător și detectează intruziunile dorite. Monitorizează alertele și analizează evenimentele pentru a identifica eventualele probleme sau ajustări necesare.
7. Monitorizarea și întreținerea continuă: IDS-ul trebuie să fie monitorizat și actualizat în mod regulat pentru a se asigura că este la zi cu noile amenințări și atacuri. Efectuează verificări periodice, actualizează semnăturile și regulile de detecție și asigură-te că IDS-ul funcționează în mod continuu.
8. Este important să menționez că configurarea unui IDS poate fi o sarcină complexă și pot apărea diferențe în funcție de soluțiile IDS utilizate. Dacă nu ai experiență sau cunoștințe tehnice adecvate, poate fi util să apelezi la profesioniști în securitate cibernetică pentru a te ajuta în configurarea și implementarea IDS-ului în mod corespunză

Configurarea unui IPS (Intrusion Prevention System) implică următoarele etape:

1. Planificarea și analiza cerințelor: Identifică obiectivele și cerințele specifice pentru IPS. Ce tipuri de atacuri sau activități dorești să previi? Ce resurse și sisteme dorești să protejezi? Aceste informații vor ghida configurarea IPS-ului.
2. Selecția și implementarea IPS-ului potrivit: Alege un IPS care corespunde nevoilor și infrastructurii tale. Există opțiuni comerciale și open-source disponibile. Instalează și configurează IPS-ul pe un sistem dedicat sau pe un dispozitiv de rețea compatibil.
3. Configurarea politicilor de securitate: Definirea politicilor de securitate este esențială pentru a decide cum IPS-ul va acționa în ceea ce privește traficul de rețea. Configurează reguli și politici specifice pentru a bloca, respinge sau redirecționa traficul suspect sau potențial dăunător. Aceste politici pot fi bazate pe semnături de atac, caracteristici comportamentale sau alți factori relevanți.
4. Configurarea surselor de date și de monitorizare: IPS-ul trebuie să monitorizeze traficul de rețea sau alte evenimente pentru a detecta și preveni atacurile. Configurează sursele de date, cum ar fi logurile de sistem, logurile de firewall sau traficul de rețea, astfel încât IPS-ul să poată analiza și acționa în consecință.
5. Configurarea alertelor și notificărilor: Setează opțiuni de alertă pentru IPS pentru a fi notificat în timp real sau pentru a genera înregistrări de evenimente pentru activitățile suspecte. Acest lucru te va ajuta să răspunzi rapid la eventualele incidente de securitate.
6. Testarea și ajustarea IPS-ului: După configurare, testează IPS-ul pentru a verifica funcționalitatea și eficacitatea sa. Monitorizează alertele și analizează evenimentele pentru a identifica eventuale probleme sau ajustări necesare în politicile și setările IPS-ului.
7. Monitorizarea și întreținerea continuă: IPS-ul trebuie monitorizat și actualizat în mod regulat pentru a se asigura că este la zi cu noile amenințări și tactici de atac. Efectuează verificări periodice, actualizează semnăturile și politicile de securitate și asigură-te că IPS-ul funcționează în mod continuu.

**Concluzie**

Configurarea unui firewall software și a unui VPN sunt aspecte cruciale pentru protejarea rețelelor și a datelor în mediul digital. Un firewall software, configurat corespunzător, asigură securitatea prin monitorizarea și controlul traficului de rețea, blocarea accesului neautorizat și protejarea împotriva atacurilor cibernetice. Aceasta include configurarea regulilor și politiciilor de filtrare a pachetelor, gestiunea porturilor și protocolor, și actualizarea constantă a semnăturilor de atac pentru a detecta și bloca noile amenințări.

Pe de altă parte, configurarea unui VPN permite utilizatorilor să creeze conexiuni securizate în mediul online. VPN-ul criptează traficul și asigură confidențialitatea datelor prin crearea unui tunel virtual între punctele finale. Acest lucru este esențial pentru protejarea informațiilor sensibile și pentru a permite accesul sigur la rețelele interne de la distanță.

Atât firewall-ul software, cât și VPN-ul sunt instrumente importante în arsenalul de securitate cibernetică. O configurare corectă și adaptată nevoilor specifice ale organizației sau utilizatorului final este esențială pentru a asigura o protecție adecvată împotriva amenințărilor cibernetice și a atacurilor. În plus, monitorizarea și actualizarea constantă a acestor soluții sunt cruciale pentru a menține securitatea în fața evoluțiilor tehnologice și a noilor vulnerabilități care pot apărea. Prin implementarea și configurarea corespunzătoare a unui firewall software și a unui VPN, utilizatorii și organizațiile pot beneficia de o securitate îmbunătățită și de o protecție eficientă a datelor.