6. TEHNOLOGII ALE SECURITĂȚII CIBERNETICE

Preliminarii

Tehnologiile cele mai des utilizate pentru a asigura securitatea cibernetică sunt: firewall-urile, sistemele de detectare și prevenire a intruziunilor, filtrele de conținut, rețelele virtuale private și alte tehnologii de securitate utilizate pe scară largă. Toate cele enumerate vor fi studiate în această temă cu scopul de a evalua și a gestiona controalele tehnice utilizate de programele InfoSec. Pentru configurarea și mentenanța acestor tehnologii este nevoie de mai multă expertiză, de aceea nevoia de educație și formare pe această dimensiune este mare.

Scopul:

- *studierea tehnologiilor de securitate utilizate de către organizații pentru a-și proteja rețelele de comunicații electronice și informațiile de acces neautorizat.*

Obiectivele educaționale:

- *studierea și identificarea tehnologiilor software și hardware de securitate;*
- *înțelegerea algoritmului de funcționare a tehnologiilor de securitate;*
- *clasificarea tehnologiilor de securitate cibernetice.*

Finalitățile de referință:

- *capacitatea de a deosebi diferite tipuri de tehnologii ale securității cibernetice;*
- *înțelegerea principiilor de funcționare a tehnologiilor de securitate hardware/software;*
- *configurarea de bază a tehnologiilor de securitate cibernetică.*

Modalitățile de evaluare

Evaluarea masteranzilor se va efectua în baza testelor formative realizate pe parcursul semestrului de studiu, care vor conține întrebări de tip grilă, întrebări deschise și studii de caz. De asemenea, masteranzii vor îndeplini sarcini practice individuale sau de grup și vor prezenta oral o temă relevantă domeniului de securitate cibernetică. La finele semestrului masteranzii vor susține un examen care va acoperi toate temele din acest suport de curs.

6.1. Firewall

Un firewall poate fi un dispozitiv sau program care controlează traficul de intrare și ieșire din rețeaua organizației, de asemenea fiind responsabil de direcționarea corectă a traficului de date în rețea, ca de exemplu calea corectă către un server de email sau web.

6.1.1. Tipuri de firewall

Firewall-ul analizează absolut toate pachetele din rețea pentru a permite sau restricționa accesul acestora. Firewall-urile pot fi clasificate în următoarele categorii descrise în continuare.

Firewall de filtrare a pachetelor

Firewall-ul analizează antetele pachetelor de date care intră în rețeaua organizației și determină acceptarea sau neacceptare acestui tip de trafic [22]. Antetele pachetelor conțin: adresa sursă și adresa destinație, tipul serviciului solicitat etc. după cum se observă în figura 6.1.

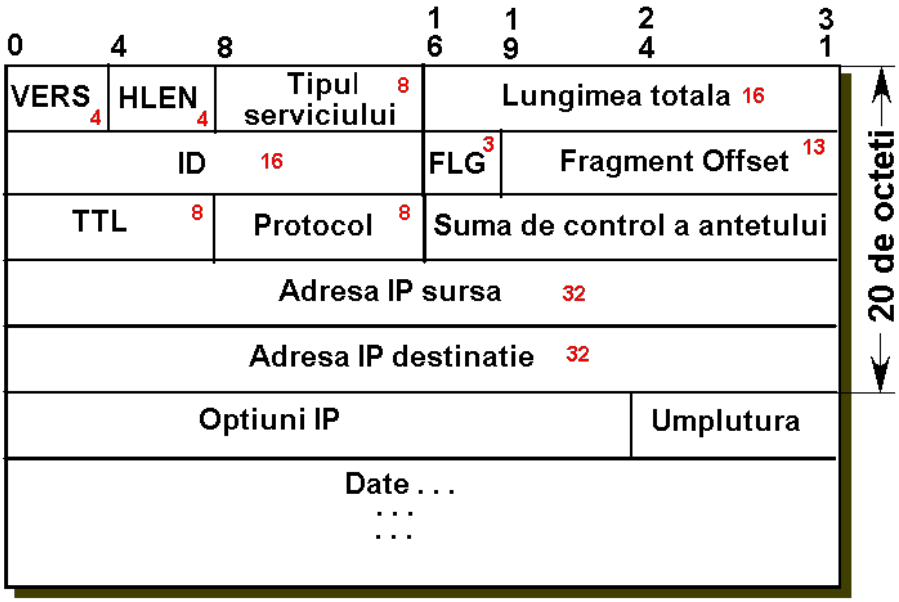

Fig. 6.1. Header-ul pachetelor de date

Firewall-urile de filtrare a pachetelor scanează pachetele de date din rețea și monitorizează respectarea regulilor date de firewall sau încălcarea acestor reguli. Firewall-urile de filtrare inspectează pachetele la stratul de rețea, Layer 3, al modelului Open Systems Interconnect (OSI), care reprezintă cele șapte straturi ale proceselor de rețea. Dacă dispozitivul găsește un pachet ce corespunde unei restricții, acesta oprește pachetul. Restricțiile cel mai frecvent implementate pe firewall-urile de filtrare a pachetelor se bazează pe o combinație a următoarelor:

- adresă IP sursă și destinație;
- direcție (inbound sau outbound);
- protocol pentru firewall-uri capabile să examineze nivelul de protocol IP;
- protocolul de control al transmisiei (TCP) sau protocolul de datagramă utilizator (UDP) și cererile de port destinație pentru firewall capabile să examineze stratul TCP/UPD.

Firewall-urile de filtrare a pachetelor se clasifică suplimentar în ***firewall de filtrare statică a pachetelor, firewall de filtrare dinamică a pachetelor și firewall SPI (stateful packet inspection)***.

Anterior, firewall-urile de filtrare a pachetelor funcționau doar în mod static, adică în baza anumitor reguli prestabilite. Actualmente acesta acționează în mod dinamic, modificându-și regulile în dependență de condiții. De exemplu, dacă firewall-ul detectează un trafic neobișnuit, care vine dintr-o sursă sau din mai multe surse, ca în cazul atacurilor DoS, firewall-ul static maximum putea notifica administratorul, pe când cel dinamic va ignora acest trafic pentru o anumită perioadă de timp.

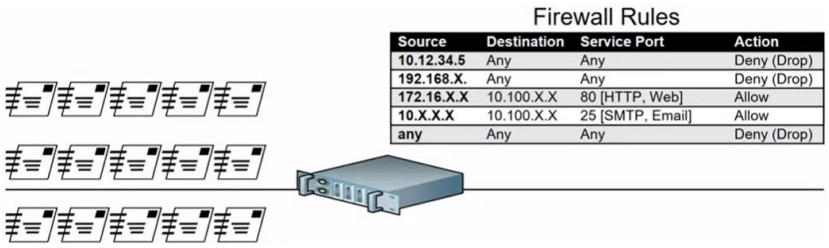

Fig. 6.2. Starea dinamică a firewall-ului

Suplimentar, firewall-urile SPI urmăresc toate modificările și înregistrează datele în tabelul de stare, date precum adresa sursă și portul logic, adresa destinatarului și portul destinatar, timpul și protocolul de transport utilizat, TCP sau UDP, la fel ca în exemplul reflectat în figura 6.2.

Application layer proxy firewall

Acest tip de firewall funcționează ca un proxy server, ca un server intermediar între un server web de exemplu și rețeaua externă. În acest caz, când se primește o solicitare, firewall-ul va solicita web serverului informația, iar dispozitivul din afară o va accesa din proxy și nu direct de pe web server. Va fi creată așa-numita zonă demilitarizată (DMZ) în care vor fi configurate serverul web, de email, de fișiere, astfel încât utilizatorii externi să aibă acces doar la acea zonă a rețelei corporative(figura 6.3).

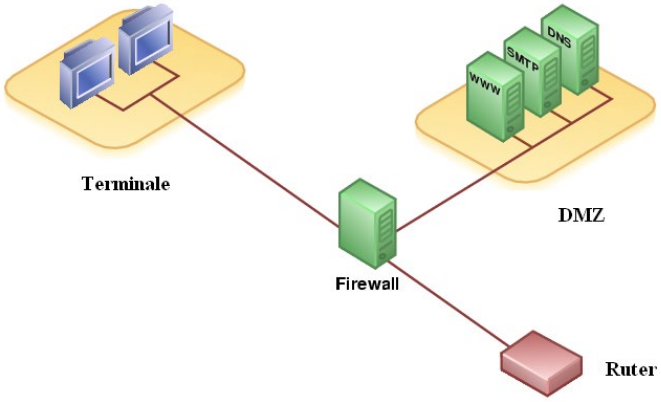

Fig. 6.3. Zonă demilitarizată

De asemenea, acționând ca și proxy servere, aceste firewall-uri salvează în memoria cache cele mai accesate date de pe serverele interne și le oferă ca răspuns la cererile utilizatorilor externi fără a mai fi nevoie să direcționeze traficul spre serverele solicitate.

Media Access Control Layer Firewalls

Un firewall este proiectat să funcționeze la substratul de control al accesului media al stratului legătură de date al rețelei (Layer 2). Deși nu este la fel de bine cunoscut sau menționat pe scară largă precum firewall-urile descrise în secțiunile anterioare, firewall-urile stratului de control al accesului media ia decizii de filtrare pe baza adresei fizice a terminalului, reprezentată de controlul accesului media (MAC) sau de adresa de rețea a cardului de interfață (NIC), care operează la nivelul de legătură de date al modelului OSI sau stratul de acces rețea al modelului TCP/IP. Astfel, firewall-urile stratului de control al accesului media leagă adresele anumitor calculatoare-gazdă la intrările ACL, care identifică tipurile specifice de pachete ce pot fi trimise către fiecare gazdă și blochează tot restul traficului. Acestea sunt denumite și firewall-uri layer MAC, însă poate apărea confuzia cu controalele de acces obligatorii (MAC).

Pentru a clarifica lucrurile cu privire la tipul de firewall și nivelul OSI sau TCP/IP la care acționează poate fi analizată fig. 6.4.

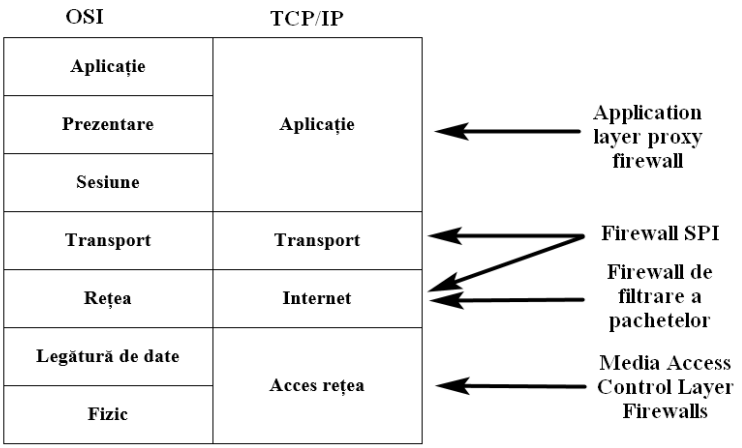

Fig. 6.4. Tipul de firewall și modele de rețea

Firewall hibrid

Firewall-urile hibride combină elementele altor tipuri de firewall-uri, adică elementele de filtrare de pachete, proxy la nivel de aplicație și firewall-uri la nivel de control al accesului media.

Un sistem de firewall hibrid poate consta de fapt din două dispozitive firewall separate; fiecare este un sistem de firewall separat, dar sunt conectate astfel încât să funcționeze în tandem. Primul tip de firewall hibrid este cunoscut sub numele de Unified Threat Management (UTM). UTM funcționează ca un dispozitiv all-in-one [3], cu diverse funcționalități, numit și firewall de generație viitoare, după cum se arată în figura 6.5. Aceste dispozitive sunt clasificate în funcție de capacitatea lor de a efectua munca unui firewall SPI, a unui sistem de detectare și prevenire a intruziunilor în rețea, a filtrului de conținut, a filtrului de spam și de malware. Sistemele UTM profită de creșterea capacității de memorie și capacitatea procesorului și poate reduce complexitatea asociată cu implementarea, configurarea și integrarea mai multor dispozitive de rețea.

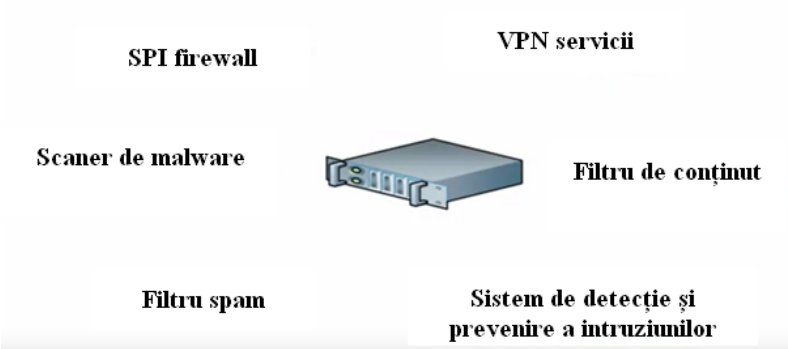

Fig. 6.5. UTM

Alt tip de firewall hibrid este firewall-ul de generație următoare (NextGen sau NGFW). Similar dispozitivelor UTM, firewall-urile NextGen combină funcțiile tradiționale de firewall cu alte funcții de securitate ale rețelei, cum ar fi inspecția profundă a pachetelor, IDPS și capacitatea pentru a decripta traficul criptat. Funcțiile sunt atât de asemănătoare cu cele ale dispozitivelor UTM, încât diferența de multe ori poate consta doar în descrierea vânzătorului.

6.1.2. Arhitectura firewall-urilor

Valoarea unui firewall vine din capacitatea sa de a filtra traficul nedorit sau periculos ce intră în perimetrul rețelei unei organizații. O provocare pentru valoarea firewall-urilor o

reprezintă modalitatea de utilizare a rețelelor prin tehnologiile cloud pe care le implementează, dispozitivele personalului care se conectează la rețelele organizațiilor și care pot provoca vulnerabilități suplimentare. Astfel, dispozitivele firewall pot fi configurate pentru mai multe arhitecturi ale conexiunilor la rețea. Aceste abordări se exclud uneori reciproc, dar uneori pot fi combinate. Configurația care funcționează cel mai bine pentru o anumită organizație depinde de trei factori: *obiectivele rețelei, capacitatea organizației de a dezvolta și implementa arhitecturile și bugetul disponibil pentru această funcție*. Deși există sute de variații posibile, trei implementări arhitecturale ale firewall-urilor sunt deosebit de comune: *gazde cu un singur bastion, firewall-uri de gazdă ecranate* și *firewall-uri de subrețea ecranate.*

Gazde cu un singur bastion (Bastion host model)

Este arhitectura cel mai des utilizată și de obicei reprezintă ținta atacatorilor cibernetici.

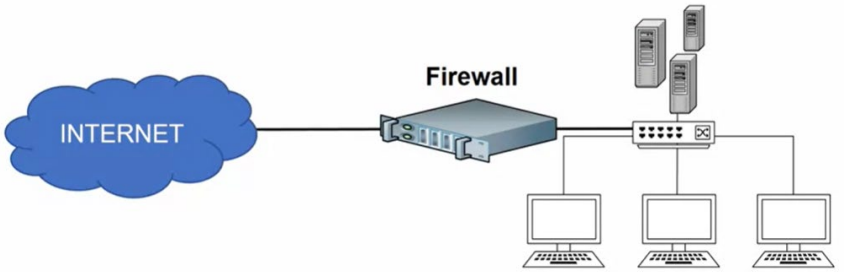

Fig. 6.6. Gazde cu un singur bastion

În această arhitectură există un singur firewall care oferă protecție în spatele routerului organizației [4]. După cum se observă în figura 6.6, arhitectura gazdă cu un singur bastion poate fi implementată ca un router de filtrare a pachetelor sau ar putea fi un firewall în spatele unui router care este configurat pentru filtrarea pachetelor. Orice sistem router sau firewall care este expus la rețeaua publică poate fi denumit *gazdă cu un singur bastion*, uneori denumită gazdă sacrificială, deoarece stă singură la perimetrul rețelei. Această arhitectură este definită pur și simplu prin prezența unui singur dispozitiv de protecție a perimetrului rețelei fiind obișnuită în mediile rezidențiale SOHO. Organizațiile mai mari caută de obicei să implementeze arhitecturi cu o apărare mai aprofundată, cu dispozitive de securitate suplimentare concepute pentru a oferi o strategie de apărare mai robustă.

Gazda cu un singur bastion este de obicei implementată ca gazdă dual-homed, deoarece conține două interfețe de rețea: una care este conectată la rețeaua externă și una care este conectată la rețeaua internă. Tot traficul trebuie să treacă prin dispozitiv pentru a se deplasa între cele două rețele. Acestei arhitecturi îi lipsește apărarea în profunzime și complexitatea ACL utilizate pentru filtrarea pachetelor ce pot crește și degrada performanța rețelei. Un atacator care se infiltrează în gazda cu un singur bastion poate descoperi configuraţia reţelelor interne și eventual furniza surselor externe informații interne.

Firewall de gazdă ecranat (Screened Host Model)

O arhitectură gazdă ecranată combină filtrarea pachetelor pe router cu un firewall separat, dedicat, cum ar fi un server proxy de aplicație, care preia informații în numele altor utilizatori de sistem și adesea memorează în cache copii ale paginilor Web și alte informații necesare pe unitățile sale interne pentru a accelera accesul [4]. Această abordare permite routerului să pre-screeneze pachetele pentru a minimiza traficul de rețea și încărcarea în interior a *proxy serverului.*

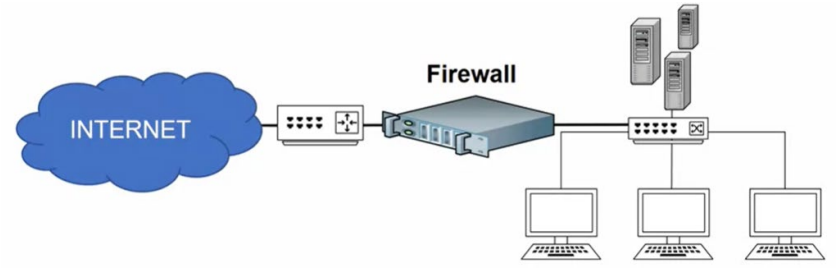

Fig. 6.7. Firewall de gazdă ecranat

Avantajul acestei arhitecturi (figura 6.7) constă în faptul că atacul extern trebuie să compromită două sisteme separate înainte ca atacatorul să poată accesa datele interne. În acest fel, gazda bastion protejează datele mai bine decât în cazul existenței unui singur router.

Firewall de subrețea ecranat (Screened subnet model)

Arhitectura dominantă astăzi este subrețeaua ecranată utilizată cu un DMZ. DMZ poate fi un port dedicat pe firewall-ul dispozitiv, care conectează o singură gazdă bastion sau poate fi conectat la o subrețea ecranată, așa cum se arată în figura 6.8. Până de curând, serverele care furnizau servicii printr-o rețea publică erau plasate în mod obișnuit în DMZ. Exemplele includ servere web, servere de protocol de transfer de fișiere (FTP) și anumite servere de baze de date.

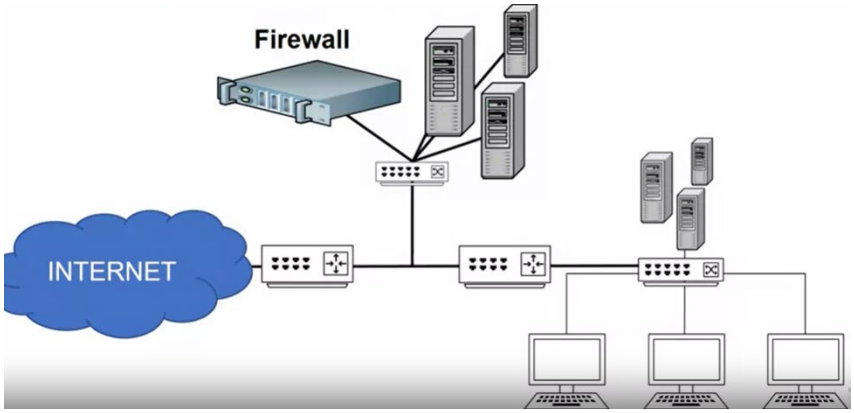

Fig. 6.8. Firewall de subrețea ecranat

O arhitectură comună este un firewall de subrețea care constă din două sau mai multe gazde bastion interne în spatele unui router de filtrare a pachetelor, fiecare gazdă protejând o anumită parte din rețeaua internă.

6.2. Filtre de conținut

Pe lângă firewall-uri, un filtru de conținut este un alt utilitar care poate ajuta la protejarea sistemelor unei organizații contra utilizării greșite și probleme neintenționate de refuzare a serviciului [8]. Un filtru de conținut este un software filtru din punct de vedere tehnic, nu un firewall, care permite administratorilor să restricționeze accesul la conținutul unei rețele. Este în esență un set de scripturi sau programe care restricționează accesul utilizatorilor la anumite protocoale de rețea și locații din internet sau care restricționează utilizatorii să primească informații generale sau exemple specifice de conținut de pe Internet. În cele mai comune modele de implementare, filtrul de conținut are două componente: ***evaluarea și filtrarea***. Evaluarea reprezintă un set de reguli precum cele pentru firewall pentru site-urile Web și este utilizată în filtrele de conținut rezidențial. Evaluarea poate fi complexă, cu setări multiple de control al accesului pentru diferite niveluri ale organizației, sau aceasta poate fi simplă, cu o schemă de bază de autorizare/refuzare precum cea a unui firewall. Filtrarea este o

metodă utilizată pentru a restricționa cererile de acces specifice la resursele identificate, care pot fi site-uri Web, servere sau alte resurse configurate de administratorul filtrului de conținut.

Avantajul implementării filtrelor de conținut este asigurarea că angajații nu sunt distrași de materiale ce nu țin de atribuțiile de serviciu și nu pierd timpul și resursele organizației navigând pe Internet.

6.3. Rețele private virtuale (VPN)

Deseori este necesar ca angajații care lucrează de acasă, sau organizațiile care sunt dispersate geografic să acceseze datele corporative. Pentru a o face în siguranță, sunt utilizate rețele virtuale private, care asigură conexiunea securizată prin rețelele neprotejate. VPN-urile utilizează criptarea pentru a securiza comunicațiile sigure (despre criptare mai multe informații se vor găsi în temele următoare). VPN este o rețea privată de date care folosește infrastructura de telecomunicații publică pentru a crea un mijloc de comunicare privată prin utilizarea protocolului de tunelare combinat cu proceduri de securitate [23]. VPN sunt de obicei folosite pentru a extinde conexiunile sigure ale rețelei interne din cadrul unei organizații cu locații îndepărtate. Pot fi distinse trei tehnologii VPN:

- *VPN-uri de încredere;*
- *VPN-uri securizate;*
- *VPN-uri hibride*.

Un ***VPN de încredere***, cunoscut și ca VPN moștenit, utilizează circuite închiriate de la un furnizor de servicii de telecomunicații și efectuează comutarea de pachete prin aceste circuite închiriate. Organizația trebuie să aibă încredere în furnizorul de servicii, care oferă asigurări contractuale că nimeni altcineva nu are voie să folosească circuitele și că circuitele sunt întreținute și protejate corespunzător.

VPN-urile securizate utilizează protocoale de securitate precum IPSec pentru a cripta traficul transmis prin rețele publice nesecurizate precum Internetul. Un ***VPN hibrid*** le combină pe cele două. Deoarece VPN asigură conexiuni sigure și de încredere în timp ce se bazează pe rețele publice, trebuie să realizeze următoarele, indiferent de tehnologiile și protocoalele specifice utilizate:

- *Încapsularea datelor* de intrare și de ieșire, în care protocolul nativ al clientului este încorporat în cadrele unui protocol care poate fi direcționat către rețeaua publică și să fie utilizabil de mediul de rețea-server.
- *Criptarea datelor de intrare și de ieșire* pentru a menține confidențialitatea conținutului datelor în timp ce sunt în tranzit prin rețeaua publică, dar utilizabil de către calculatoarele client și server și/sau rețelele locale de la ambele capete ale conexiunii VPN.
- *Autentificarea calculatorului la distanță* și, probabil, a utilizatorului la distanță. Autentificarea și autorizarea ulterioară a utilizatorului pentru a efectua acțiuni specifice se bazează pe identificarea precisă și fiabilă a sistemului și utilizatorului de la distanță.

VPN pot fi ***persistente*** sau ***temporare*** și se clasifică astfel:

- ***VPN mod tunel***, care criptează pachetele de date, apoi le transmite (figura 6.9).

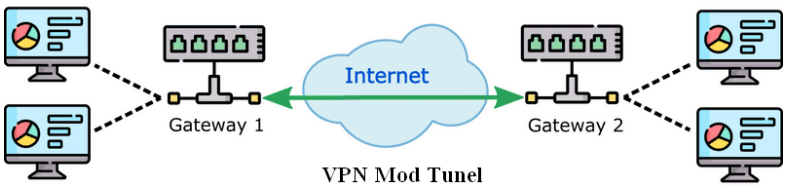

Fig. 6.9. VPN mod tunel

Modul tunel stabilește două servere de tunel perimetral pentru a cripta tot traficul care va traversa o rețea nesecurizată. În modul tunel, întregul pachet adresat clientului este criptat și adăugat ca porțiune de date a unui pachet adresat de la un server de tunel la altul. Serverul de primire decriptează pachetul și îl trimite la adresa finală. Avantajul principal al acestui model este că un pachet interceptat nu dezvăluie nimic despre adevărata destinație din sistem.

- ***VPN mod transport***. În modul de transport (figura 6.10) datele dintr-un pachet IP sunt criptate, dar informațiile din antet nu. Acest lucru permite utilizatorului să stabilească o legătură securizată direct cu gazda de la distanță, criptând doar conținutul de date al pachetului. Dezavantajul acestui lucru este că cei care interceptează pachetele pot încă identifica sistemul de destinație. Dacă atacatorii cunosc destinația, ei pot să compromită unul dintre nodurile finale și să obțină informațiile despre pachet. Pe de altă parte, modul de transport elimină necesitatea de servere speciale și software de tunel și permite utilizatorilor finali să transmită trafic de oriunde, ceea ce este util în special pentru angajații care călătoresc sau lucrează de la distanță.

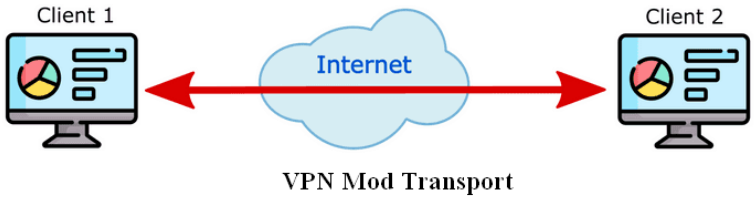

Fig. 6.10. VPN mod transport

6.4. Sisteme de detecție și prevenire a intruziunilor

Sistemele de detecție și prevenire a intruziunilor funcționează ca sisteme de alarmă antiincendiară, doar că pe dimensiunea de asigurare a securității cibernetice.

Fig. 6.11. IDPS (imagine reprezentativă) [3]

Multe IDS permit administratorilor să configureze sistemele pentru a-i notifica direct despre probleme prin e-mail sau cu notificări pe telefon.

Configurațiile care permit IDS să ofere nivelurile personalizate de detectare și răspuns sunt destul de complexe. O extensie actuală a tehnologiei IDS este încorporarea tehnologiei de prevenire a intruziunilor, care poate preveni o intruziune cu succes prin intermediul unui răspuns activ, după exemplul sistemelor antiincendiare reflectate în figura 6.11. Deoarece rareori se găsește o astfel de tehnologie care să nu aibă și capacități de detectare și prevenire, termenul IDS a fost extins la sisteme de detectare și prevenire (IDPS) care este utilizat în mod obișnuit.

IDPS se clasifică astfel:

- *IDPS bazate pe gazdă* – rezidă într-un server sau calculator anume și monitorizează doar activitatea de pe acel dispozitiv. Periodic verifică fișierele de pe calculator, inclusiv le verifică hash-ul pentru a se convinge de integritatea acestora și notifică administratorul în caz că hash-ul a fost modificat, putând pune în carantină fișierele suspecte.
- *IDPS bazate pe rețea* – monitorizează traficul din rețea și poate bloca traficul suspect.
- *IDPS bazate pe semnături* – se bazează pe semnăturile sau cunoștințele deținute și compară comunicațiile suspicioase cu bazele de date, acționează similar cu antivirusul, detectând în baza semnăturilor deținute și pune în carantină sau șterge traficul suspicios.
- *IDPS bazate pe anomalii* – reacționează doar la anomaliile din sistem, ca de exemplu un atac de tip DoS, blocând tentativele.

Răspunsurile IDPS sunt diverse – de la punerea în carantină a pachetelor de date suspicioase până la ștergerea acestora. De asemenea, una dintre capabilități este înregistrarea electronică a comportamentului observat (log file), dezavantajul constă în faptul că administratorul este cel care trebuie să revizuiască log-urile și să ia măsuri; IDPS pot actualmente să fie configurate astfel, încât să transmită mesaje prin email, telefon, după preferințele administratorului. Alertele emise false de către IDPS se clasifică astfel:

- *False pozitive* atunci când IDPS consideră în baza analizei că este un atac în progres, dar de fapt nu este;
- *False negative* când de fapt este un atac, însă IDPS consideră că nu este.

Pentru a minimiza aceste alerte poate fi stabilit un anumit nivel la care va reacționa IDPS, ca de exemplu dacă primește un număr mic de pachete suspicioase, generează doar log-uri, dacă volumul crește substanțial, atunci alertează administratorul și blochează activitatea.

IDPS pot fi atât dispozitive, cât și aplicații instalate pe anumite dispozitive, când organizația are multiple IDPS instalate pe mai multe dispozitive sau aflate în mai multe rețele. Așadar, se obișnuiește a instala un IDPS pe o stație de management, o aplicație care cumulează informația de la celelalte IDPS, după cum este arătat în figura 6.12.

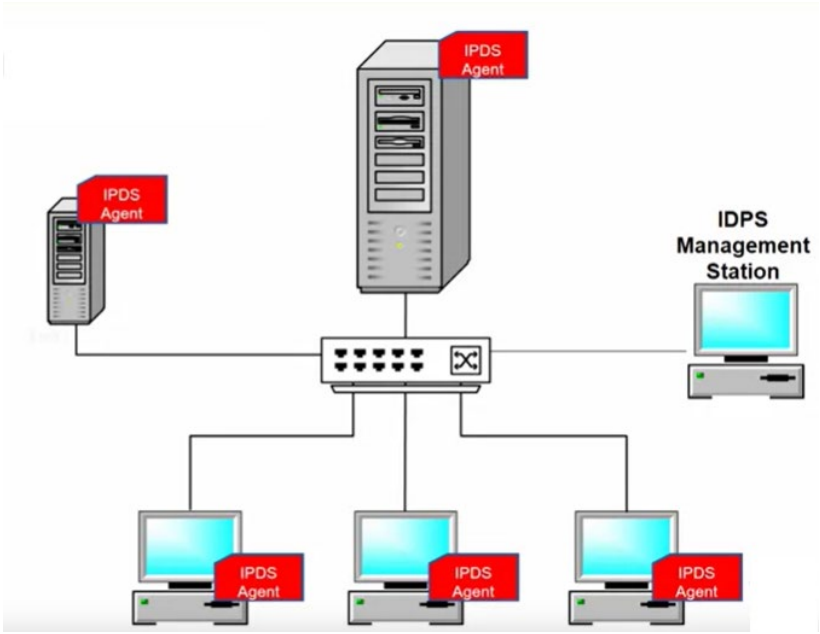

Fig. 6.12. Stație de management IDPS

Tehnologiile de securitate cibernetică sunt parte esențială și indispensabilă pentru orice program de securitate cibernetică, iar capacitatea de a le configura corespunzător este esențială pentru protecția domeniului cibernetic în orice organizație.

Întrebări și subiecte pentru aprofundarea cunoștințelor

1. Ce este un DMZ? Este acesta într-adevăr un nume adecvat pentru tehnologie, având în vedere funcția pe care o îndeplinește acest tip de subrețea?
2. Descrieți în baza unei organizații specifice importanța configurării zonelor demilitarizate.
3. Descrieți modul în care diferitele tipuri de firewall-uri interacționează cu traficul de rețea la diferite niveluri ale modelului OSI.
4. Care sunt tipurile de firewall implementate la scară largă în organizații?
5. Care este principiul prin care utilizatorilor li se permite accesul limitat la sistemul informatic doar pentru a-și îndeplini atribuțiile de afaceri?
6. Descrieți principiul de funcționare a filtrelor de conținut.
7. Expuneți importanța utilizării rețelelor virtuale private în organizații.
8. Analizați și expuneți diferențele esențiale dintre rețelele virtuale private tunel versus transport.
9. Ce li se atribuie în controlul accesului obligatoriu fiecărui subiect și obiect?
10. Clasificați și descrieți prin exemple concrete tipurile controalelor de securitate în dependență de momentul și cauza pentru care au fost aplicate.