



Securitate rețele

Rețele

3.1.1. Înțelegerea termenului de rețea și recunoașterea principalelor tipuri de rețele - local area network (LAN), wide area network (WAN), virtual private network (VPN)

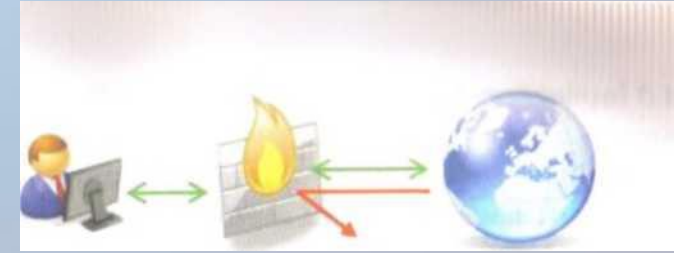
- Un grup de două sau mai multe computere conectate prin canale de comunicații, ce permit partajarea resurselor și informațiilor se numește rețea (network). Necesitatea de a partaja și transmite informații într-un mod foarte rapid a dus la crearea conceptului de rețea.
- Facilitățile oferite de o rețea sunt:
 - Facilitarea comunicațiilor - prin intermediul rețelei, oamenii pot comunica rapid și eficient prin email, mesagerie instantanee, telefon, video conferințe etc.
 - Partajare componente hardware - într-o rețea, fiecare computer poate accesa și utiliza resurse hardware cum ar fi imprimanta din rețea, discurile din rețea etc.
 - Partajare fișiere - în rețea, utilizatorii autorizați pot accesa date și informații stocate pe alte computere din rețea.
 - Partajare software - utilizatorii conectați la o rețea pot rula aplicații de pe alte computere.
- Metodele de conectare a calculatoarelor au evoluat și încă sunt în curs de dezvoltare, plecând de la cabluri metalice și ajungând în prezent la transmisia prin unde radio (wireless = fără fire).

- În funcție de aria de răspândire, rețele se împart în mai multe categorii cum ar fi:
 - **Local Area Network (LAN)** - rețea locală - O rețea ce conectează computere aflate în apropiere unele de altele, de obicei localizate în aceeași clădire.
 - **Metropolitan Area Network (MAN)** rețele metropolitane – o rețea de calculatoare în care două sau mai multe computere sau dispozitive sunt separate geografic, dar în același oraș.
 - **Wide Area NetWork (WAN)** - rețea de largă acoperire - O rețea de mare întindere geografică, de exemplu între două orașe, pe o țară, un continent sau chiar în întreaga lume.
 - **Virtual Private NetWork (VPN)** - rețea virtuală privată - O rețea care permite utilizatorilor să partajeze informații private între locații îndepărtate sau între o locație îndepărtată și rețeaua locală de la serviciu, prin intermediul rețelelor publice (Internet). Pentru asigurarea confidențialității datelor, rețeaua VPN utilizează metode de criptare la nivel de aplicații firewall și echipamente de rețea.

3.1.2. Înțelegerea rolului unui administrator de rețea în gestionarea autentificării și autorizării în cadrul unei rețele

- Un **administrator de rețea** este o persoană responsabilă de instalarea, configurarea, actualizarea, administrarea, monitorizarea și întreținerea rețelelor de calculatoare într-o organizație.
- De asemenea, administratorul de rețea folosește instrumente pentru gestionarea utilizatorilor și a drepturilor asociate, în ceea ce privește accesul la resursele rețelei. Astfel, accesarea serverelor, imprimantelor, documentelor, diferitelor servicii etc, se realizează pe baza proceselor de **autentificare și autorizare**:
 - **Autentificarea** permite validarea unui utilizator pe baza informațiilor de logare - nume de utilizator și parola aferentă. Aceste date sunt verificate într-o listă de utilizatori autorizați și dacă sunt corecte se permite accesul mai departe.
 - **Autorizarea** reprezintă un privilegiu (drept) acordat unui utilizator de către administratorul de rețea, pentru a accesa, procesa sau modifica date și resurse, în funcție de politicile de securitate ale companiei privind tehnologia informației.

3.1.3. Înțelegerea funcțiilor și limitărilor unui firewall



- **Firewall**-ul se referă la un program software sau un echipament hardware / software, destinate protejării unei rețele împotriva accesului neautorizat.
- Firewall-ul monitorizează porturile prin care se transmit date între calculului din rețeaua locală (considerată o rețea sigură și de încredere) și rețeaua publică (Internetul), considerată o rețea nesigură.
- **Porturile** reprezintă interfețe utilizate de aplicațiile software pentru a schimba date. Un port are două direcții - de intrare și de ieșire a datelor, iar numărul total al acestora este 65.535, ceea ce înseamnă tot atâtea posibilități de a compromite securitatea calculatorului.
- Cu toate că într-o sesiune obișnuită de lucru cu calculatorul sunt utilizate mult mai puține porturi, firewall-ul are un rol Important în protejarea calculatorului.
- Astfel, **firewall-ul ține evidența tuturor cererilor de date inițiate de utilizator/sistem de calcul, iar în momentul în care pachete de date vor să intre în sistem, li se permite accesul sau nu, în funcție de regulile stabilite.** Dacă este ceva solicitat (de exemplu, o pagină web), i se permite accesul; dacă nu este ceva solicitat, firewall-ul interpretează că este o tentativă de intruziune neautorizată în sistem și blochează accesul.

- În acest fel, un firewall poate ajuta la blocarea atacurilor cibernetice care ar putea prelua controlul asupra calculatorului și a unor amenințări malware, îndeosebi viermi informatici.
- Cu toate acestea, firewall-ul nu poate proteja sistemul de calcul de viruși, programe spion, adware și de vulnerabilitățile de securitate existente în sistemele de operare și aplicațiile neactualizate. Pentru aceste scopuri sunt necesare utilizarea unei soluții antivirus și actualizarea aplicațiilor software.
- De asemenea, un firewall poate bloca și traficul legitim de date și nu avertizează întotdeauna dacă sistemul de calcul este atacat. Mai există riscul compromiterii sistemului de calcul din interiorul rețelei locale, întrucât aceasta este considerată a fi sigură.

