Ծանոթացում Firewall-ին:

Firewall-ը ցանցային անվտանգության սարք կամ ծրագրային հավելված է, որը նախատեսված է վերահսկելու և վերահսկելու մուտքային և ելքային ցանցային տրաֆիկը՝ հիմնված կանխորոշված անվտանգության կանոնների վրա: Այն գործում է որպես խոչընդոտ վստահելի ներքին ցանցի և անվստահելի արտաքին ցանցերի միջև, ինչպիսին է ինտերնետը, կանխելու չարտոնված մուտքը՝ միաժամանակ թույլ տալով օրինական հաղորդակցության անցումը:

Firewall-ի հիմնական նպատակն է բարձրացնել ցանցի անվտանգությունը՝ կարգավորելով մուտքային և ելքային տրաֆիկը: Այն օգտագործվում է մասնավոր ցանցեր կամ դրանցից չարտոնված մուտքը կանխելու համար և կարող է իրականացվել ցանցային տարբեր միջավայրերում, ներառյալ տնային ցանցերը, կորպորատիվ ցանցերը և տվյալների կենտրոնները:

Թվային firewalls-ը ծրագրային ապահովման վրա հիմնված լուծումներ են, որոնք տեղադրված են սերվերների, երթուղիչների կամ համակարգիչների վրա՝ ծրագրային մակարդակով երթեւեկությունը վերահսկելու համար: Ֆիզիկական firewalls-ը, մյուս կողմից, ապարատային սարքեր են, որոնք սովորաբար տեղադրված են տեղական ցանցի և արտաքին ցանցի միջև՝ ապարատային մակարդակով տրաֆիկը զտելու և կառավարելու համար:

Firewall-ներն ունեն մի քանի հիմնական կարողություններ և գործառույթներ.

1. Փաթեթների զտում (Packet Filtering). տվյալների փաթեթների ուսումնասիրություն և դրանք թույլ տալ կամ արգելափակել՝ հիմնվելով նախապես սահմանված կանոնների վրա:

2. Ակտիվ կապերի վիճակի մոնիտորինգ և միայն օրինական տրաֆիկի թույլատրում:

3. Proxying. Գործելով որպես միջնորդ ներքին և արտաքին ցանցերի միջև ցանցի հասցեները թաքցնելու և անվտանգությունը բարձրացնելու համար:

4. Ցանցային հասցեների թարգմանություն (NAT). Փաթեթների վերնագրերում ցանցի հասցեի տեղեկատվությունը փոփոխել՝ տարբեր ցանցերի միջև հաղորդակցությունը հնարավոր դարձնելու համար:

Web Application Firewall-ը (WAF) մասնագիտացված firewall է, որը նախատեսված է պաշտպանելու վեբ հավելվածները՝ զտելով և վերահսկելով HTTP տրաֆիկը վեբ հավելվածի և ինտերնետի միջև: Այն գործում է OSI մոդելի կիրառական (Application) շերտում (շերտ 7) և օգնում է պաշտպանվել վեբ վրա հիմնված սովորական հարձակումներից, ինչպիսիք են SQL ներարկումը (Injection), միջկայքի սկրիպտավորումը (XSS – Cross Site Scripting) և ծառայության հերքումը բաշխված (DDoS - Distributed Denial of Service) հարձակումներից:

Firewall-ները կարող են պաշտպանել տարբեր տեսակի ցանցային հարձակումներից, ներառյալ, բայց չսահմանափակվելով հետևյալով.

- Denial of Service (DoS) Attacks
- Distributed Denial of Service (DDoS) Attacks
- Malware Infections
- Port Scanning
- Packet Spoofing
- Man-in-the-Middle (MitM) Attacks
- Unauthorized Access Attempts

Firewall-ները սովորաբար գործում են՝ օգտագործելով երեք հիմնական շղթաներ.

- Ներածման շղթա (Input). վերահսկում է մուտքային տրաֆիկը, որը նախատեսված է հենց firewall-ի համար:

- Արդյունքների շղթա (Output/Outgoing). վերահսկում է ելքային տրաֆիկը, որը ծագում է հենց firewall-ից:

- Փոխանցման շղթա (Forward). վերահսկում է ցանցի մի հատվածից մյուսը firewall-ով անցնող տրաֆիկը:

Յուրաքանչյուր շղթա կիրառում է հատուկ կանոններ՝ որոշելու՝ թույլատրել կամ արգելափակել երթևեկությունը՝ հիմնվելով իր աղբյուրի, նպատակակետի, արձանագրության և այլ հատկանիշների վրա: