FUNZIONALITÀ ASSOCIATE

Una funzione spesso associata al firewall è quella di **traduzione degli indirizzi di rete** (*NAT: Network Address Translation*), che può contribuire a rendere inaccessibili i calcolatori sulla rete interna mascherandone gli **indirizzi IP**.

Talvolta è associata anche la funzione di **rilevamento delle intrusioni** (**IDS**), un sistema basato su euristiche che analizza il traffico e tenta di riconoscere possibili attacchi alla sicurezza della rete, e può anche scatenare reazioni automatiche da parte del firewall (**Intrusion prevention system**).

Un'altra funzione molto diffusa nei firewall moderni è il supporto per le connessioni remote **VPN** (*Virtual Private Network*).

LIMITI E VULNERABILITÀ

Pur essendo spesso un componente vitale in una strategia di sicurezza informatica, il firewall resta un singolo elemento di tale strategia:

- la sua efficacia è legata strettamente all'**efficacia delle regole con cui è stato configurato**;
- la sua configurazione è un **compromesso** tra usabilità della rete, sicurezza e risorse disponibili per la manutenzione della configurazione stessa;
- una quota rilevante delle **minacce** alla sicurezza informatica proviene dalla **rete interna** (portatili, virus, connessioni abusive alla rete, reti wireless non adeguatamente protette, etc.).

Una delle vulnerabilità più conosciute di un firewall di fascia media è l'**HTTP tunneling**, che consente di "bypassare" le restrizioni Internet utilizzando comunicazioni **HTTP** solitamente concesse dai firewall. Altra tipica vulnerabilità è la **dll injection**, ovvero una tecnica utilizzata da molti **trojan**, che sovrascrive il codice maligno all'interno di librerie di sistema utilizzate da programmi considerati sicuri.

PERSONAL FIREWALL

Un **personal firewall**, o firewall personale, è un programma installato su un comune personal computer (**PC**) che controlla le comunicazioni in entrata e in uscita dal PC stesso, permettendo o vietando alcuni tipi di comunicazione in base a **regole o policy di sicurezza** preimpostate dall'utente in fase di configurazione.

Il personal firewall si differenzia dai firewall veri e propri (**perimetrali**) in quanto **non esiste** una distinzione tra l'hardware sul quale è in esecuzione il personal firewall stesso e le normali applicazioni dell'utente. Questo implica che il personal firewall protegge esclusivamente il PC sul quale è installato.

Rispetto ad un firewall perimetrale, il personal firewall è eseguito sullo stesso sistema operativo che dovrebbe proteggere, ed è quindi soggetto al rischio di venir **disabilitato da un malware** che prenda il controllo del calcolatore con diritti sufficienti. A suo favore, il personal firewall ha accesso ad un dato che un firewall perimetrale non può conoscere, ovvero può sapere quale applicazione ha generato un pacchetto o è in ascolto su una determinata porta di connessione, e può quindi basare le sue decisioni anche su queste informazioni.

Oggigiorno i sistemi operativi **Windows**, **MacOS** e **Linux**, per impostazione predefinita, integrano una soluzione firewall in grado di proteggere adeguatamente il sistema. Tuttavia nel caso di organizzazioni aziendali è preferibile installare soluzioni più avanzate volte a garantire un certo grado di protezione.

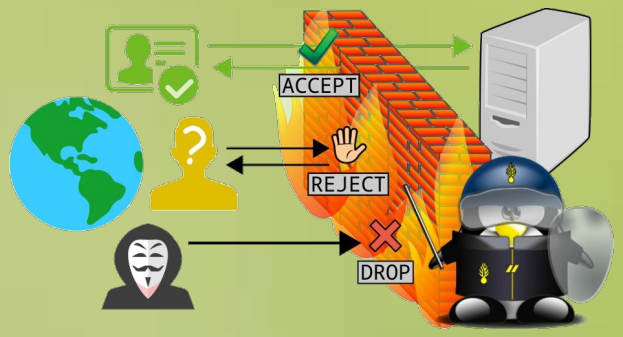
RIFERIMENTI

➢ https://www.c3t.it/projects/awareness/articoli&brochure/firewall/

POR FESR 2014-2020 obiettivo Crescita e Occupazione (CreO)

I FIREWALL

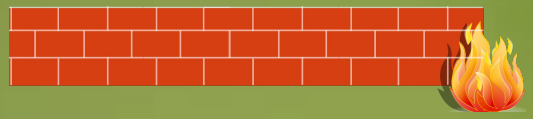
Scopri cosa sono i **firewall**, le loro funzionalità e perché sono importanti.



CHE COS'È UN FIREWALL

Secondo la definizione di **Cisco**, una delle imprese leader nel settore delle reti informatiche, un **firewall** è "*un dispositivo per la sicurezza della rete che permette di monitorare il traffico in entrata e in uscita utilizzando una serie predefinita di regole di sicurezza per consentire o bloccare gli eventi*". Per dispositivo si intende un elemento hardware o un'applicazione software.

In inglese, la parola firewall significa "**muro tagliafuoco**", ovvero una parete costruita all'interno di un edificio per limitare la propagazione di eventuali incendi. I firewall informatici svolgono una funzione simile: controllano il traffico di dati in entrambe le direzioni per impedire l'entrata o l'uscita di connessioni pericolose per il sistema.



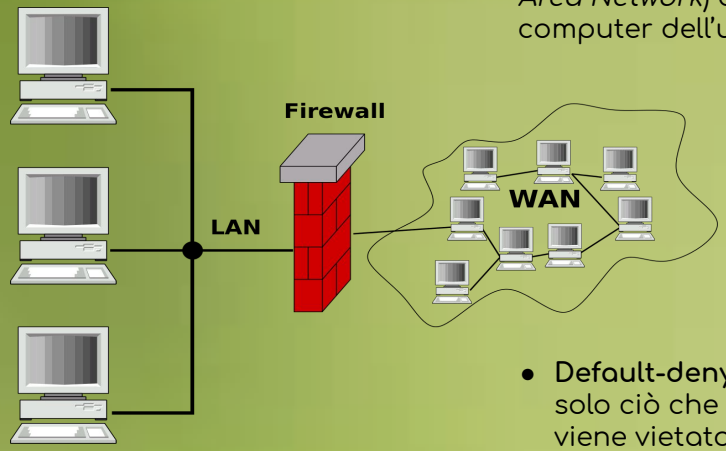
TIPI FIREWALL

1. Firewall con filtro di pacchetti

Analizzano i dati contenuti nelle "etichette" dei pacchetti trasmessi, li confrontano con le regole di filtro impostate e decidono se bloccare o lasciar passare la connessione. Questa tipologia di firewall è affidabile ma limitata, in quanto esposta a diverse minacce moderne come lo **spoofing dell'IP**, ovvero la sostituzione di un indirizzo IP che verrebbe bloccato con uno legittimo.

2. Firewall con analisi dello stato della connessione

Non analizzano solo i pacchetti di dati, ma anche lo stato della connessione, le porte utilizzate sui computer e i protocolli di trasmissione.



3. Firewall a livello di applicazioni

Dedicati a una singola applicazione, funzionano come intermediari nella comunicazione di dati tra questa e la rete esterna. Questi firewall svolgono un'analisi molto più approfondita e possono bloccare le connessioni in tempo reale. Si tratta di soluzioni di livello aziendale, utili quando il grado di sicurezza richiesto è molto alto e si hanno a disposizione dispositivi potenti, che non risentono del rallentamento causato dall'attività del firewall.

4. Firewall di nuova generazione

Dispongono di funzionalità di prevenzione di intrusioni e monitoraggio delle applicazioni. Si tratta di software per aziende o persone con necessità particolari, che richiedono la supervisione da parte di personale esperto. Possono essere paragonati a un sistema antifurto di un edificio.

COME FUNZIONA UN FIREWALL

Dal punto di vista del funzionamento, un firewall è una specie di **filtro che controlla il traffico di dati e blocca le trasmissioni pericolose o indesiderate in base a una serie di regole** specifiche. La maggior parte dei firewall dispone di norme standard a cui l'utente finale può aggiungere altre personalizzate, in base alle proprie necessità.
Esistono vari tipi di firewall, ognuno dei quali analizza determinate caratteristiche delle trasmissioni di dati.

Il firewall **si interpone** tra la rete esterna (*WAN: Wide Area Network*), che comprende Internet, e la rete interna (*LAN: Local Area Network*) dell'azienda, di casa o semplicemente il computer dell'utente finale. Da un punto di vista teorico, la rete interna è considerata conosciuta, sicura, attendibile e protetta, mentre quella esterna è la presunta fonte di potenziali minacce, in quanto nel complesso è sconosciuta, insicura e non attendibile.

La maggior parte dei firewall utilizza uno di questi due criteri generali di applicazione delle regole:

- **Default-deny**: per impostazione predefinita viene permesso solo ciò che viene autorizzato esplicitamente, mentre il resto viene vietato.
- **Default-allow**: per impostazione predefinita viene bloccato solo ciò che viene vietato esplicitamente, mentre il resto viene permesso.

Il primo criterio è quello più utilizzato perché garantisce maggiore sicurezza e una maggiore precisione nella definizione delle regole. Tuttavia, il secondo criterio consente una configurazione più semplice e rapida delle regole.