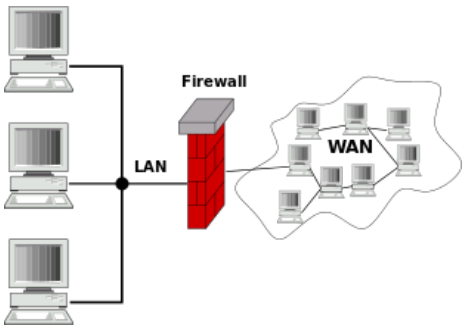
Il firewall

Definizione

Un **firewall** (in italiano “muro di fuoco”) è un **componente hardware e/o software di difesa perimetrale di una rete**, originariamente passivo, che può anche svolgere funzioni di collegamento tra due o più segmenti di rete, o tra una rete e un computer locale, fornendo dunque una **protezione in termini di sicurezza informatica della rete stessa e proteggendo il computer da malware o altri pericoli di internet.**



Evoluzione e tipi di firewall

1. La prima generazione fu quella dei **packet filter firewall** o **stateless firewall**, il cui primo esemplare venne sviluppato nel 1988 dalla Digital Equipment Corporation. Il loro funzionamento consisteva nel **filtrare il traffico secondo un insieme di regole basate su alcune informazioni presenti nell'header dei pacchetti**. Questi semplici filtri, usati spesso all'interno dei router e degli switch, potevano essere facilmente aggirati.
2. La seconda generazione di firewall introdusse, rispetto alla prima, la possibilità di salvare e monitorare lo stato di una connessione. Il primo **stateful firewall** (chiamato anche circuit-level gateway) venne sviluppato tra il 1989 e il 1990 dagli AT&T Bell Laboratories. Un firewall di questo tipo **consentiva la formulazione di regole in grado di bloccare pacchetti fasulli, cioè non appartenenti ad alcuna connessione attiva**, ma non garantiva la protezione da attacchi che sfruttavano vulnerabilità nei livelli superiori del modello OSI. Inoltre erano sensibili anche ad attacchi di tipo DoS che puntavano a riempire la tabella dello stato delle connessioni.
3. Un ulteriore tipo di firewall è il **proxy**, il quale **non controlla solo l’header del pacchetto in entrata ma anche tutto il body**. Sebbene aumenti il livello della sicurezza, un application firewall è specifico per ogni applicazione e costituisce un collo di bottiglia per le performance della rete.
4. L’ultimo tipo di firewall è il **next-generation firewall**, il quale **riunisce diverse tecnologie**. Fra queste ci sono le tecnologie di filtraggio dei firewall presentati in precedenza ovvero il filtraggio stateless, la stateful inspection, l'analisi dei pacchetti a livello applicativo (deep-packet introspection). Alcune delle altre caratteristiche tipiche di un next-generation firewall sono: il rilevamento e la prevenzione delle intrusioni (sistemi IDS e IPS), la definizione di policy specifiche per ogni applicazione,

l'integrazione dell'identità dell'utente, l'acquisizione di dati di supporto per la sicurezza da fonti esterne, la qualità di servizio.

Video consigliato

Approfondimento sul proxy:
https://www.youtube.com/watch?v=jX3Q-8FK7d4&list=PL3itjooulgzMy2oWg9wu-rz4f0mvP3Q65&index=18