Difesa perimetrale: Proxy e DMZ

Collegando un router tra una LAN e Internet il traffico viene instradato sia verso l'esterno ma anche verso l'interno della rete, esponendola a rischi di vario tipo come per esempio gli accessi indesiderati da host esterni aventi lo scopo di acquisire i dati dagli archivi o compromettere i servizi oppure l'installazione di software in grado di provocare anomalie di funzionamento in uno o più nodi della rete, quindi e necessario interporre tra la LAN e Internet un meccanismo che consenta di controllare il traffico della rete. A questo componente è stato dato il nome di firewall (muro tagliafuoco). Un firewall è un sistema hardware-software dedicato alla difesa perimetrale di una rete che agisce filtrando il traffico dei pacchetti in entrata o in uscita dalla rete.

Vi sono vari tipi di firewall che possono agire in diversi livelli, a seconda della protezione desiderata. Un esempio è l'application proxy.

Il proxy permette di filtrare il traffico di una singola applicazione, quindi è in grado di bloccare i contenuti indesiderati ed è in grado di bloccare dei pacchetti in cui contengono certi nomi di siti.

Il proxy è un programma che viene eseguito sul gateway e si simula client quando comunica con il server e si simula server quando comunica con il client, offrendo molti vantaggi come per esempio una protezione vasta perché non vi è nessuna connessione diretta tra i client e il server e quindi tutti i pacchetti, prima di arrivare a destinazione, passano dal proxy e vengono ispezionati permettendo un controllo completo dei pacchetti sia in entrata che in uscita di una LAN. Nel caso di crash del proxy la LAN rimane isolata e inaccessibile dall'esterno rimanendo protetta. Offre dei log dettagliati all'utente per controllare gli accessi e i movimenti degli host collegati alla rete. E' in grado di gestire connessioni separate che appartengono alla stessa applicazione. E' semplice da configuare. Offre l'autenticazione dell'utente e il filtraggio dei contenuti. Ha una cache interna per le pagine web che permette di liberare il traffico inutile della rete in caso di richiesta di una stessa pagina.

Gli svantaggi di un proxy sono che è poco trasparente, e quindi richiede che ogni computer della LAN interna sia configurato per utilizzare il proxy, per ogni applicazione è richiesto un proxy, e la gestione della connessione attraverso il proxy richiede molto lavoro per la CPU e quindi si avrebbero più costi per aver un hardware sufficiente per lavorare con il proxy.

Un altro esempio di firewall è la DMZ o zona demilitarizzata che consiste in un segmento isolato di LAN (una "sottorete") raggiungibile sia da reti interne sia esterne, ma caratterizzata dal fatto che gli host attestati sulla DMZ hanno possibilità limitate di connessione verso host specifici della rete interna.

Tale configurazione viene normalmente utilizzata per permettere ai server posizionati sulla DMZ di fornire servizi all'esterno senza compromettere la sicurezza della rete aziendale interna, nel caso una di tali macchine sia sottoposta ad un attacco informatico. La principale difesa contro gli attacchi a una rete consiste sulla corretta organizzazione topologica di essa. La DMZ necessita di un IP statico e permette di esporre al WWW un solo indirizzo IP al quale vengono inoltrare tutte le richieste di connessioni. Vi sono tre possibili architetture di DMZ: dentro un ramo del firewall, tra due firewall e sopra il firewall interno.