Immagine che contiene testo, diagramma, mappa, schermata

Descrizione generata automaticamente

Firewall Dinamico: Tipo di Firewall Perimetrale (come quello Statico) posto a cavallo tra Lan e Wan. Blocca tutte le connessioni automaticamente se queste hanno origine dall’esterno verso l’interno (out 🡪 in : block), mentre permette tutte quelle che provengono dall’interno verso l’esterno (in 🡪 out : permit). Dotato sia di tabella (white list) di Ip con permesso per avviare connessioni (impostata dall’host) che di una memoria interna dinamica che si resetta ogni volta che termina la connessione con Ip del server. Prende il posto di quello Statico principalmente per due motivi : con la venuta del web 2.0, diventò impossibile scrivere a mano sulla ACL (tabella accessi) tutti gli IP con il permesso di entrare nella rete, in più era molto facile poterlo camuffare (“sbuff”) oltrepassando così il Firewall.

Sorge però un problema: dato che le connessioni out 🡪 in venivano bloccate in automatico, il mio server web ed il mio server di posta elettronica, ad esempio, non potevano essere raggiunti da nessuno. Quindi si trovò un modo per renderli accessibili tramite una porta posta sul Firewall Dinamico, la DMZ (Delimitary Zone), la quale però, permettendo completo accesso ai web server, li esponeva ad un rischio importante. Siccome un firewall dinamico non poteva essere usato date le problematiche viste prima, ecco che venne introdotto lo WAF.

WAF: tipo di Firewall che filtra “per contenuto” i PDU provenienti dalla zona di internet. Una volta spacchettato il PDU, confronta il codice del payload con la sua tabella e, a seconda se ci sono corrispondenze o meno, bloccherà o lascerà passare il PDU. Altro modo, anche più efficace, è quello di appoggiarsi allo OWASP, comunità open source per la sicurezza delle applicazioni web. Lo WAF posso “incorporarlo” all’interno di un server reverse proxy, ad ulteriore protezione dei miei server web

Server Reverse Proxy : Un tipo di Proxy che funziona come una sorta di tela bianca, un setaccio per tutto ciò che proviene dalla zona di Internet (WAN) ai server di rete interna, server web (HTTP) e server di posta (SMTP) in questo caso, proteggendoli attraverso vari tipi di servizio che posso annettere come WAF, NAT/PAT, ANTIMALWARE, Bilanciamento del Carico, ecc.

Infine si possono utilizzare anche altri software, installabili nei nostri dispositivi, per rilevare e bloccare minacce contro la nostra rete. Stiamo parlando dei sistemi di rilevamento e di prevenzione delle intrusioni (rispettivamente IDS e IPS). Entrambi possono essere utilizzati anche a livello perimetrale, ma è in LAN che danno il meglio di sé. L’IDS tramite messaggio di “alert” avverte l’amministratore di eventuali accessi non autorizzati, mentre l’IPS, oltre a ciò, può anche bloccare di default la minaccia.

Come possiamo vedere in figura, l’IDS viene meglio impiegato a difesa dei miei dati sensibili, posti all’interno del NAS (Network Access Storage) garantendomi una migliore accessibilità. Se invece utilizzassimo l’IPS, c’è il rischio che mi blocchi lo sharing dei file all’interno della rete. Quest’ultimo viene meglio impiegato a protezione dei miei server web.