SETTIMANA 2 LEZIONE 1

In questo esercizio, ho disegnato e costruito una rete con un firewall perimetrale, un firewall si può presentare sotto forma di hardware o software (quello hardware è utilizzato da aziende che fanno il loro lavoro in modo professionale, contiene tante CPU, memorie ram… e riesce a sopportare meglio l’enorme quantità di dati contenuta nei pacchetti) il firewall è stato creato per difendere le reti. In questa immagine ho utilizzato un firewall dinamico che però ha un problema quello di accettare le connessioni dall’interno verso l’esterno ma non viceversa, quindi ho messo i server web in una zona chiamata “DMZ” zona demilitarizzata, questa è raggiungibile dall’esterno però non ha barriere di difesa avendo tutti quanti l’accesso. Per ovviare al problema ho utilizzato un “WAF” web application firewall, questo legge l’indirizzo IP del mittente e apre e analizza i pacchetti si ricevono andando ad analizzarne il contenuto, se questo è malevolo viene bloccato altrimenti viene accettato. Nella rete possiamo vedere che è stata utilizzata la tecnologia di sicurezza IDS/IPS, utilizzati come seconda barriera in caso ci fosse un malfunzionamento di qualsiasi tipo del firewall, per proteggere il NAS che è un dispositivo di raccolta e archiviazione di dati (di tutti i tipi compresi quelli sensibili) ho utilizzato una tecnologia di sicurezza chiamata IPS, avvisa e blocca gli indirizzi IP che ritiene inviino pacchetti contenenti file malevoli, dall’altro lato ho utilizzato lDS questa a differenza dell’IPS manda solo un segnale di avvertimento senza bloccare gli IP. (la tecnica IPS ha un problema potrebbe rilevare falsi positivi e quindi non permettere agli impiegati di un’azienda ad esempio di accedere alle informazioni contenute nel NAS).

(ACL access control list, prende i pacchetti, controlla gli IP, in una tabella con altri indirizzi IP salvati, li controlla e se combaciano permette di accedere.)

