

Il compito di oggi prevede di disegnare una rete con i seguenti componenti:

* Una zona internet, o rete WAN (wide area network), un tipo di rete informatica che copre un'ampia area geografica e collega dispositivi e risorse in posizioni distanti tra loro;
* Una zona DMZ (Demilitarized Zone): un'area separata e isolata che si trova tra una rete interna sicura e una rete esterna non sicura. Essa funge da zona tampone tra queste due reti con diversi livelli di sicurezza; qui vengono posizionati server e servizi che devono essere accessibili sia dalla rete interna che da Internet, come server web o server di posta elettronica. Questi sono esposti alla rete esterna, ma sono isolati dalla rete interna, riducendo così il rischio di un accesso non autorizzato o di attacchi informatici diretti alla rete principale. In questo caso, è presente un firewall di tipo perimetrale, cioè posto a cavallo tra la LAN (rete privata) e la WAN (internet). Si tratta di una difesa che protegge da attacchi malware, phishing, ransomware etc...e operando con metodologia dinamica, consente il passaggio di dati solo verso l’esterno, ecco perchè si necessita di un sistema DMZ;
* Una NAS: dispositivo di archiviazione dati collegato a una rete che fornisce accesso a file e dati a diversi utenti e sistemi all'interno di quella rete. Esso è progettato per essere condiviso attraverso una rete, consentendo a più utenti di accedere e condividere dati simultaneamente;
* WAF: la cui funzione principale è di monitorare, filtrare e bloccare il traffico Http malevolo tra un'applicazione web e Internet. Per fare ciò dispone di una tabella di riferimento, già di default all’interno del WAF, o si rifà a database OWASP, un’organizzazione che si occupa di informare e bloccare tutto ciò che attacca il web.
* IPS/IDS: sistemi di difesa software simili. Si differenziano perché l’IDS opera in modo passivo inviando un allert al client di un possibile arrivo di dati malware ma senza bloccarlo, mentre l’IPS opera attivamente bloccandolo oltre ad inviare un allert. Andiamo quindi a collocare l’IDS in corrispondenza del NAS in modo che tutti riescano ad accedervi senza essere bloccati, mentre andremo a inserire l’IPS in corrispondenza dei due server, luogo in cui vi è più probabilità di ricevere un attacco.