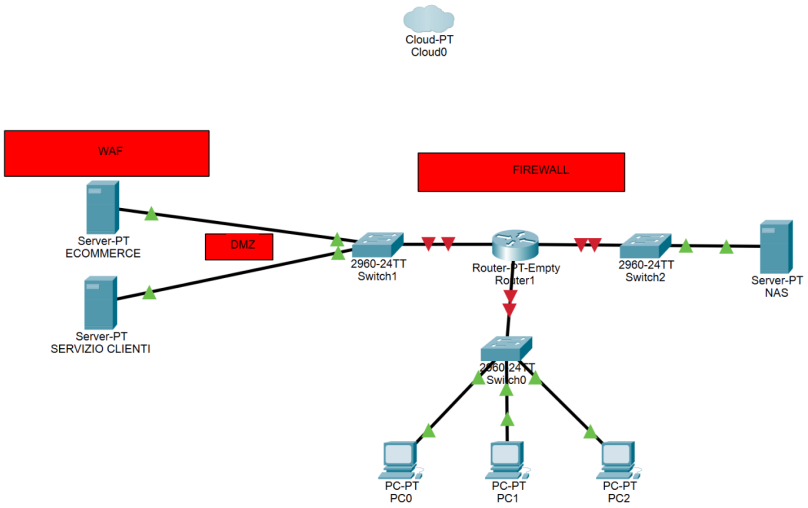
RETE CON FIREWALL



Nel seguente esercizio ho creato un'ipotetica rete di un'azienda con i dispositivi di sicurezza informatica annessi per quest'ultima.
La rete è suddivisa dapprima nella parte WAN e LAN, questa ulteriormente divisa in un'area solo aziendale in cui non ci deve essere nessun utente esterno che può entrarvi (comprensiva anche dell'area NAS che è quella che vorremmo proteggere meglio) e un'area riservata alla comunicazione con l'utenza, quest'ultima chiamata DMZ.

A protezione della LAN ci sono due tipologie di Firewall, che hanno caratteristiche diverse e scopi diversi, per cui vanno ad essere inserite entrambe e coesistere.

Il Firewall dinamico è messo "a protezione" della parte della rete non accessibile per il pubblico, infatti la caratteristica del Firewall dinamico è quella che possono comunicare con l'interno solo indirizzi IP che sono originariamente stati interpellati da un indirizzo IP interno. Esempio semplice è la navigazione in internet, in cui è un dispositivo interno che va a passare per il firewall dall'interno, si interfaccia col sito di destinazione e gli permette di rispondere all'IP interno e di bypassare il firewall. Questo "permesso" finisce col terminare della sessione, infatti la lista di indirizzi IP permessi è una memoria volatile che scompare alla chiusura della sessione.

Se ci fosse solo questo firewall però l'utenza non potrebbe mai accedere al sito della nostra azienda per cui si è resa necessaria una partizione della rete e la creazione di una parte accessibile a tutti gli indirizzi IP.
Per proteggere però questa parte di server e non permettere da lì l'ingresso nella rete è stato inserito un WAF.

Questo software va a fare una difesa non basata sugli indirizzi IP degli utenti, ma riesce a vedere il contenuto del pacchetto e quindi respingere eventuali pacchetti contenenti malware (questo supportato da aziende terze che si occupano di stilare database di malware conosciuti).

Eventualmente in tale rete possono essere inseriti dispositivi di alert quali IDS e IPS. la differenza sostanziale è che l'IDS è un dispositivo di difesa passivo che da un alert qualora ci sia una minaccia, ma l'eventuale rimozione di questa è compito dello specialista, questo è inserito tra la DMZ e la rete privata poiché passibile di falsi positivi si richiede che uno specialist valuti la minaccia eventuale prima di rimuoverla, mentre l'IPS una volta rilevata una minaccia va a rimuoverla in automatico senza possibilità di analisi.