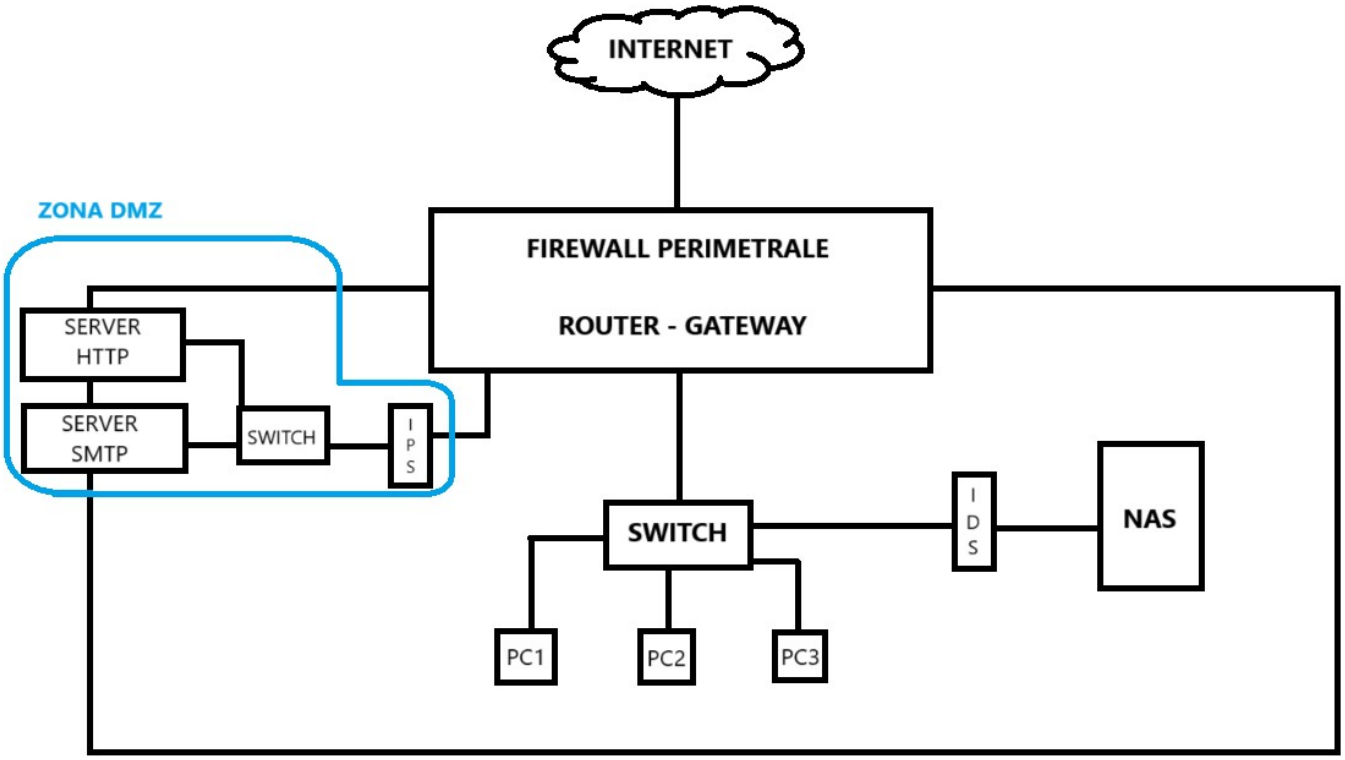
Esercitazione S3/L5



In questa esercitazione ho simulato una rete aziendale con diversi componenti.
La rete presenta 1 firewall/router-gateway perimetrale a protezione di tutta la rete, 1 switch che collega un Nas e degli host (in figura ne ho rappresentati 3, in un azienda sono ovviamente di più), 1 IDS e una zona DMZ dove ci sono 2 server, 1 HTTP e 1 SMTP, (entrambi collegati con un secondo switch) e 1 IPS a protezione ulteriore della zona.
Vediamo nel dettaglio i componenti e i vari collegamenti.
Come primo componente che si collega alla WAN (Wide area network) troviamo il firewall.
Il firewall è un componente fondamentale per la protezione di una rete o di un dispositivo e può essere sia software che hardware. La differenza è solo nell'efficenza del firewall visto che gli hardware progettati appositamente per questo compito sono molto performanti.
In base al numero delle connessioni che ha una azienda, si installano firewall hardware più o meno performanti.
I firewall si differenziano tra: perimetrali che si trovano tra WAN e LAN(Local area network) e non perimetrali che si trovano solo in LAN.
Il firewall installato in questa rete è un firewall perimetrale a filtraggio dinamico.
Il funzionamento del filtraggio dinamico consiste nel bloccare tutte le connessioni dall'esterno all'interno della rete. Per poter comunicare con l'esterno il firewall ha una sua tabella,chiamata ACL(Access control list), e quando dall'interno ci si collega verso l'esterno viene registrato l'IP di destinazione in questa ACL e viene permesso lo scambio di pacchetti.
Una volta terminata la connessione, la tabella, essendo una memoria volatile, verrà cancellata dell'IP con il quale ci si è scambiati momentaneamente dei pacchetti per ripristinare la sicurezza della rete. Grazie a questa ACL, se qualcuno prova ad entrare nella rete e l'IP non è registrato in tabella, il firewall bloccherà automaticamente il tentativo di connessione.

In questo caso l’azienda presenta 2 server, 1 web server HTTP e 1 server di posta elettronica SMTP.
Questi server ovviamente devono essere accessibili dall’esterno e andrebbero in conflitto con il funzionamento del firewall che renderebbe inaccessibile il raggiungimento dei server. Per ovviare a questa problematica ho creato una zona DMZ (zona demilitarizzata), è una zona appositamente creata con porte aperte e protocolli sbloccati per far in modo che dall’esterno possano essere raggiunti i 2 server. Per mantenere la protezione della rete interna, ho installato un IPS (Intruder prevention system) che analizza i pacchetti in entrata e blocca potenziali pacchetti malevoli grazie ad una sua tabella o alle impostazioni che verranno salvate. Tutta la zona viene poi collegata al firewall.
Come si può notare dal disegno non è presente il router-gateway come componente aggiuntivo. Il firewall presente in questa simulazione, infatti, mi svolge anche la funzione di router-gateway per permettermi il collegamento ad internet.
Il resto della rete interna, quindi gli host e il nas, sono collegati tramite switch che a sua volta è collegato al firewall. Il NAS(network attached storage), essendo un componente molto importante è protetto ulteriormente dall’ IDS (Intruder detection system). L’IDS si differenzia dall’IPS (installato nella DMZ) unicamente per l’azione che svolge quando rileva un potenziale pacchetto malevolo. L’IDS infatti quando analizza il pacchetto e rivela potenziali criticità non blocca nessun pacchetto ma manda un alert all’host che prova ad accedere, in questo caso, al NAS. Non viene utilizzato in situazioni di questo tipo l’IPS perché soffre di falsi positivi e potrebbe bloccare anche chi è autorizzato ad accedere al NAS, rendendo il lavoro più lento e macchinoso.
Si può notare quindi da questa simulazione l’importanza di un firewall e le accortezze che si devono utilizzare per mantenere la sicurezza di una rete.