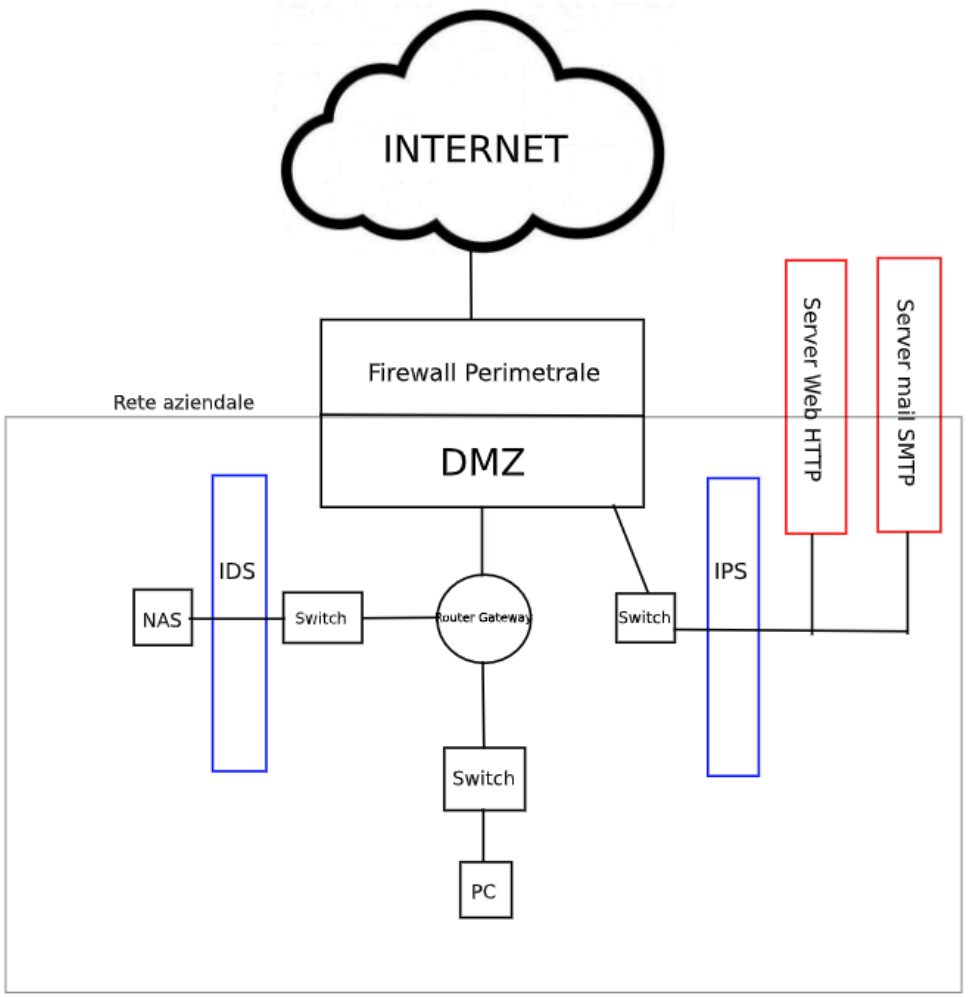
RAPPRESENTAZIONE DI UNA RETE

Traccia: Disegnare una rete con i seguenti componenti:

- Una zona di Internet (rappresentata da un cloud o un simbolo di Internet).
- Una zona DMZ con almeno un server web HTTP e un server di posta elettronica SMTP.
- Una rete interna con almeno un server o nas.
- Un firewall perimetrale posizionato tra le tre zone.
- Aggiungere IDS/IPS.
- Spiegare le scelte.

Di seguito sono andata a rappresentare, come da traccia, una bozza di rete aziendale semplice, per poi andare a spiegare le varie componenti cosa fanno e come funzionano:



Prendiamo ad esempio una semplice rete aziendale collegata ad Internet come quella stilizzata poco sopra.

La prima componente che incontreremo sarà il Firewall.
Il Firewall è un componente fondamentale nella rete ed la sua funzione è quella di implementare la sicurezza informatica, può essere un software o un dispositivo che ha la funzione di proteggere dalle minacce esterne, una sorta di “muro”, e regola il traffico di dati sia dall’esterno che dall’interno della rete e ne decreta la sicurezza o meno bloccando o lasciando passare i pacchetti in base a delle regole predefinite. Funziona in maniera simile ad un Router, ma è molto più potente. Nel caso preso in esame si tratta di un Firewall Perimetrale, ovvero un Firewall che funziona in WAN e in LAN.
Il pacchetti, dopo essere stati spacchettati ed analizzati dal Firewall, vengono spostati della DMZ (zona demilitarizzata), ovvero una zona di sicurezza che protegge la rete dall’esterno, dove i pacchetti potranno entrare senza compromettere la rete.
Nella traccia si chiede di inserire due server uno per la navigazione Web che utilizza il protocollo HTTP (porta 80) ed uno per l’invio delle mail che utilizza il protocollo SMTP (porta 587), i server sono dispositivi che offrono servizi ai client, in questo caso navigazione e mail.
I due server si collegano ad uno Switch (dispositivo utile al collegamento di due o più dispositivi tra loro), il quale si collega al Firewall, per avere una maggiore sicurezza.
Per implementare la sicurezza, andremo ad aggiungere l’IPS tra i Server e lo Switch, ovvero l’Intrusion Prevention System, ovvero un sistema che rileva, prevede, allerta e blocca eventuali minacce prima di farle passare attraverso la rete. Solitamente si sceglie di mettere il sistema IPS tra i server esterni ed il collegamento interno perchè le minacce maggiori provengono proprio dall’esterno, essendo l’IPS un sistema automatico, agisce direttamente sulle minacce bloccandole e non facendole passare all’interno della rete. Una volta decretato che il file sia effettivamente sicuro, passa attraverso il Firewall per un ulteriore accertamento per giungere al Router Gateway (dispositivo che smista i pacchetti tra le varie reti collegate) il quale poi si collegherà allo switch e/o ai dispositivi (in questo caso PC).
All’interno della rete aziendale troviamo anche il NAS, ovvero un dispositivo di archiviazione dati che, all’interno di una rete aziendale, serve per avere accessibilità semplice e veloce ai dati interni all’azienda stessa. Il NAS sarà collegato al Router Gateway attraverso uno Switch, ma a protezione del NAS, andremo a mettere il sistema IDS, ovvero Intrusion Detection System, il quale funziona in maniera analoga all’IPS, ma la differenza principale tra loro consiste nel fatto che l’IDS si limita ad inviare un alert, dopo aver spacchettato ed analizzato i pacchetti, ma non ne blocca l’accesso, cosa che invece fa l’IPS, che, come detto sopra, agisce autonomamente. La scelta di mettere l’IDS a difesa del NAS è dettata dalla necessità di rendere accessibili ai dipendenti dell’azienda i file presenti nel NAS, senza bloccare l’accesso in caso di minaccia, ma semplicemente inviando un alert di avvertimento.
I pacchetti così potranno passare al Router Gateway ed infine nel PC che ne ha fatto richiesta in maniera più sicura.