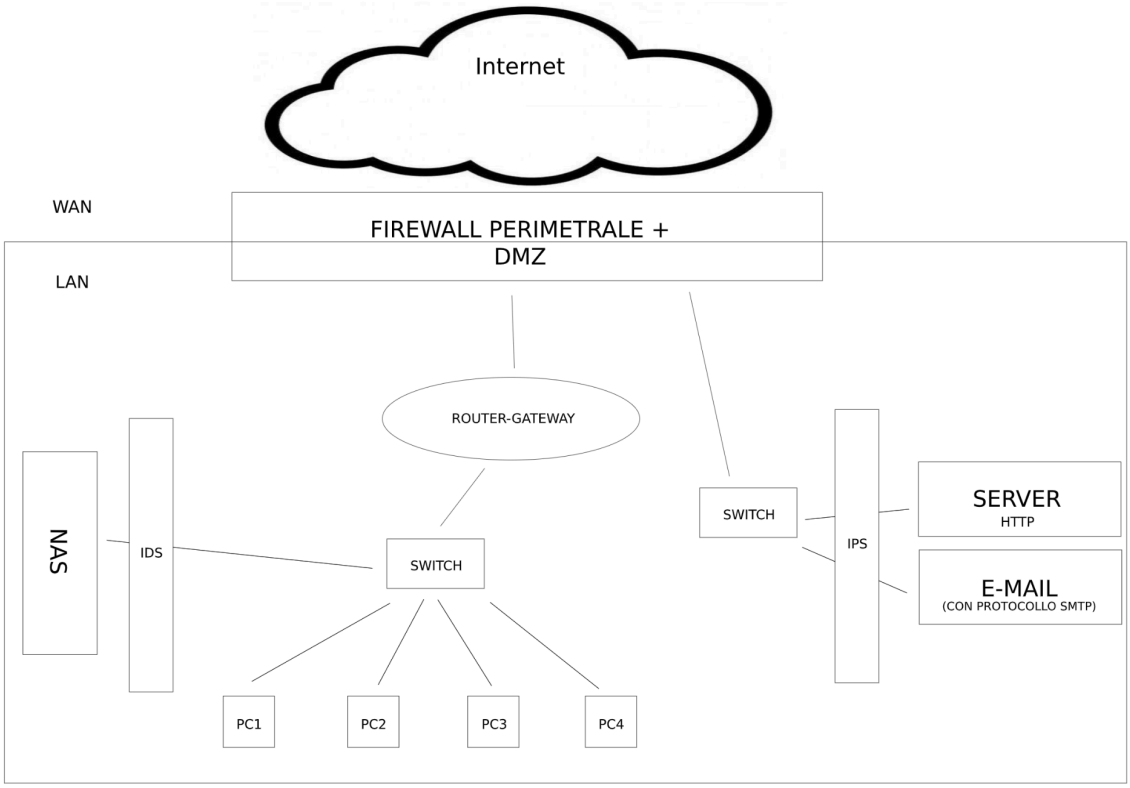
Illustrazione Rete Aziendale



Supponiamo di dover creare una rete aziendale, e consideriamo che la maggior parte degli attacchi e malware arrivino dall'esterno della nostra azienda e quindi da Internet:

Mettendo un Firewall Perimetrale con filtraggio dinamico (sempre a cavallo tra wan, rete internet, e lan, rete con distanza da 3 m fino a 2 km circa, il suo compito sarà quello di bloccare tutte le connessioni che hanno origine dall'esterno permettendo però a quelle interne di fuoriuscire, però cosi facendo nessuno riuscirebbe più a comunicare, quindi è stato creato il filtraggio a livello di applicazione (WAF). In questo sistema sono presenti delle aree "demilitarizzate", le DMZ , cioè aree in cui pacchetti possono arrivare senza compromettere il sistema per esempio come la posta elettronica. ciò va fatto tramite alcune configurazioni.

Un esempio è "owasp"(un organizzazione che si occupa della sicurezza web), che utilizza tabelle che sono sempre aggiornate e complete, il firewall capisce se un pacchetto è un malware spacchettandolo, leggendolo e confrontandolo con i criteri presenti già nella sua tabella interna e decidendo se i pacchetti corrispondono o meno,

quelli che corrispondono non potranno passare perchè saranno associati a pacchetti malevoli.
Quelli che non corrispondono invece potranno passare al dispositivo successivo, consideriamo anche che il firewall oltre che occuparsi della funzione appena descritta, ha le stesse funzionalità del router ma molto più performante, quindi avrà anche il compito di indirizzare i pacchetti verso l'indirizzo Ip ricercato.

Ipotizziamo che dopo aver superato il firewall, il pacchetto sia indirizzato alla posta elettronica, il pacchetto verrà indirizzato prima allo switch (dispositivo intelligente che si occupa di inviare i pacchetti al giusto indirizzo ip) , che controllerà tramite ping l'indirizzo corretto a cui dovrà arrivare, e una volta confermato invierà il pacchetto che però sarà filtrato dal firewall IPS.

il firewall IPS (Intrusion Prevention System) è un firewall avanzato e automatico il cui compito è quello di prevenire e bloccare eventuali intrusioni e malware, esiste anche un firewall simile, che è l' IDS che però ha il compito di denunciare e mandare un' allerta così da poter gestire il problema manualmente.
Inserire un IPS tra pc e NAS è sconsigliato perchè la maggior parte degli attacchi arriva principalmente dall'esterno ed è un sistema automatico e in caso di problematiche con falsi positivi potrebbe essere più complicato gestire la risoluzione.

Se il pacchetto supera anche il Firewall ICP allora potrà arrivare all'email e ci sarà comunicazione tramite un collegamento instaurato. L'email usa un protocollo SMTP (protocollo usato per inviare E-mail)

se invece vogliamo iniziare noi mandando dati, il nostro Web Server con HTTP (con dati in chiaro) avrà il compito di mandare una richiesta verso gli altri indirizzi che desideriamo raggiungere, tra queste richieste,le più comuni sono GET, POST, OPTION.
Con protocollo HTTP i dati non sono crittografati e sono in chiaro, quindi facilmente esposti ai programmi che sniffano come Burp Suite.

Ora ipotizziamo che ci sia un tentativo di intrusione o infezione malware indirizzato al Nas (network-attached storage, è un file centralizzato che consente di memorizzare e condividere file su una rete TCP/IP tramite wifi o cavo ethernet) proveniente dal NET, facciamo finta che riesca a superare il primo firewall perimetrale, procederà verso lo switch e andrà verso il NAS ma sarà automaticamente bloccato dal IDS (Intrusion Detection System), che manderà subito una notifica di allarme all'utente.
In caso però arrivasse un falso positivo e cioè un pacchetto che per esempio è una richiesta di accesso da un dispositivo effettivamente interno all'azienda e autorizzato, ma venisse comunque bloccato, si potrà velocemente dare l'accesso a quest'ultimo.

Diego Petronaci