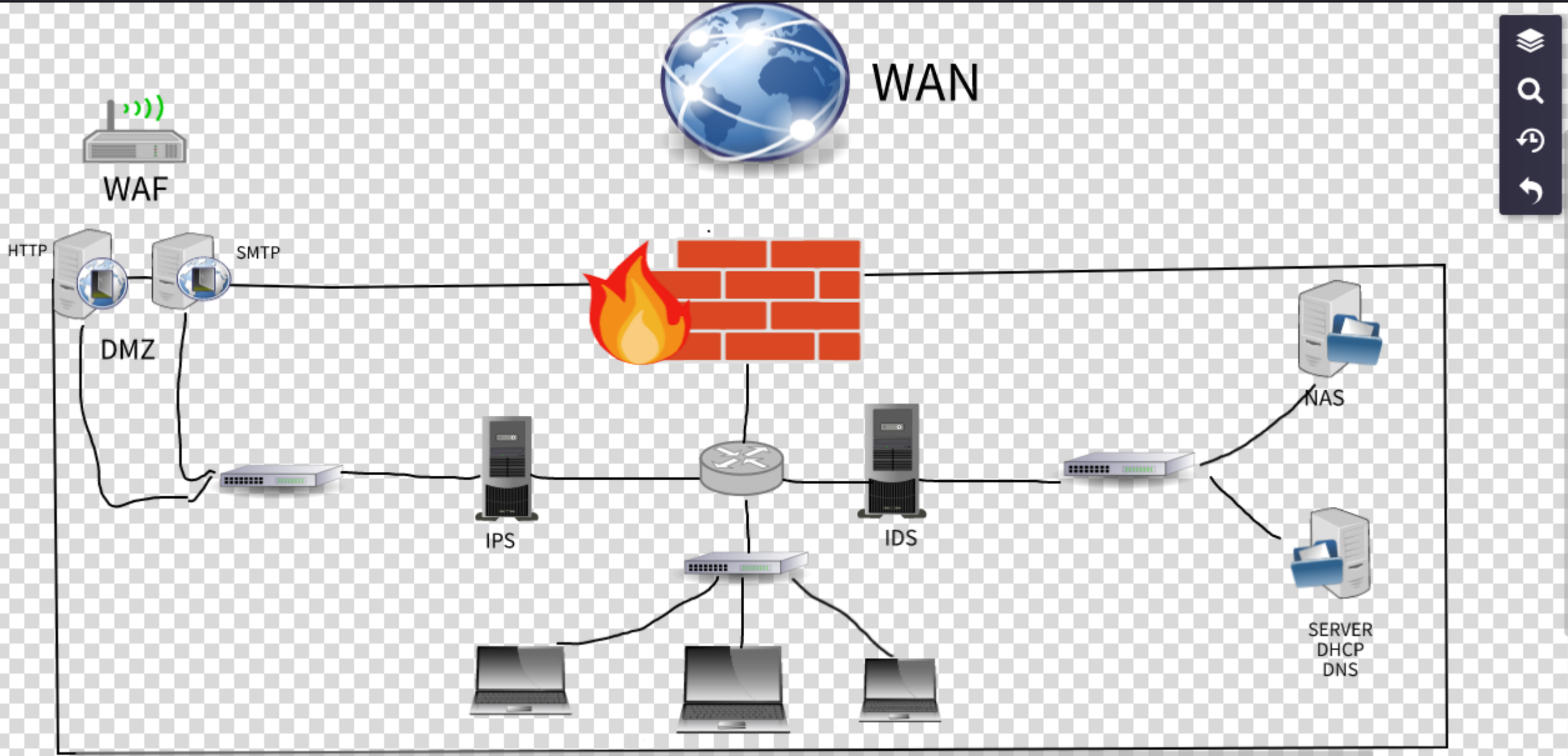
WAN
WAF
HTTP
SMTP
DMZ
IPS
IDS
NAS
SERVER
DHCP
DNS

il diesegno caricato nell'immagine precedente raffigura la configurazione di una rete aziendale, di sotto andremo a elenzare i vari dispositivi e verrà spiegata la loro funzionalità.

come vediamo raffigurato cio che comprende il riquadro rappresenta una azienda e i vari dispositivi presenti all'inteno di essa se pariamo dall'alto nella zona perimetrale troveremo il firewall:

FIREWALL è un firewall perimetrale dinamico (firewall statefull) si trova sul perimetro dell'azienda e il suo scopo è quello di far connettere dispositivi dall'INTERNO verso l'esterno, una volta creato un collegamneto i due dispositivi potranno scambiarsi pacchetti.inoltre puo bloccare automaticamente l'accesso da un indirizzo IP sospetto o consentire l'accesso solo a utenti autenticati.

WAF(web application firewall) è progettato specificamente per proteggere le applicazioni web da minacce e attacchi online. come vediamo nell'immagine è un server esterno alla rete aziendale che permette il filtraggio di pacchetti indirizzato verso le web application (nel nostro caso HTTP e SMTP). Esso a doifferenza del firewall tradizionale riesce a leggere il codice dei messaggi in arrivo (es. email) e vedere se è registarto nella sua tabella di virus o maleware, se cosi fosse è in grado di bloccare il traffico da quell'indirizzo ip.

DNZ (zona demilitarizzata) questa è la zona piu vulnerabile dell'azienda, in quanto è lunico punto d'accesso più "vulnerabile" perche sono presenti i server web e di posta elettronica, che scambiano ripetutamnete pacchetti con il mondo esterno. (se non ci fosse la WAF vista in precedenza i black hat potrebbero inviare codice malevolo attraverso questo punto della rete)

IPS (intrusion prevention system) è uno strumento progettato per identificare e prevenire attacchi informatici e intrusioni non autorizzate all'interno di una rete. le sue due funzioni principali sono: RILEVAMENTO delle intrusioni e BLOCCO delle intrusioni.
il dispositivo ha una tabella al suo interno dove sono registarti e registra anomalie nel traffico di rete, ogni volta cio avviene manda un allert al l'esperto di sicurezza che lavora nell'azienda, inoltre BLOCCA automaticamente quell'indirizzo ip sospetto.
l'IPS come vediamo nell'immagine è posizionato tra il router e lo switch collegato alla DMZ, perche possa impedire l'acesso a qualsiasi indirizzo ip che in qualche modo riesca a oltrepassare il WAF (quindi esterno all'azienda), e bloccarlo (sarà lesperto di sicurezza che verrà avvisato dai vari allert a valutare se si tratti di un falso positivo o meno nel frattempo lo teniamo bloccato per motivi di sicurezza)

IDS(intreusion detection system) anchesso uno strumento di sicurezza progettato per identificare intrusioni non autorizzate, ma a differenza dell'ips esso non blocca automaticamnete l'IP non desiderato, ma manda solamente un allert all'esperto di sicurezza.
l'IDS è stato configurato nel lato destro dell'immagine dove abbiamo il NAS e il server DHCP quindi dove abbiamo informazioni molto importanti dell'azienda.
è stato scelto un IDS per evitare che falsi positiv all'interno dell'azienda vengano bloccati inutilente, a differenza dell'IPS crea molta meno latenza ed è situato in un posto dell'azienda molto sicuro a differenza dell'IPS che si trova nella zona del DMZ accessibile dal mondo esterno.
in questo caso abbiamp deciso far premiare la velocita in quanto a termini di sicurezza dato che quella zona ha l'accesso protetto dal firewall perimetrale prima di passare dall'IDS