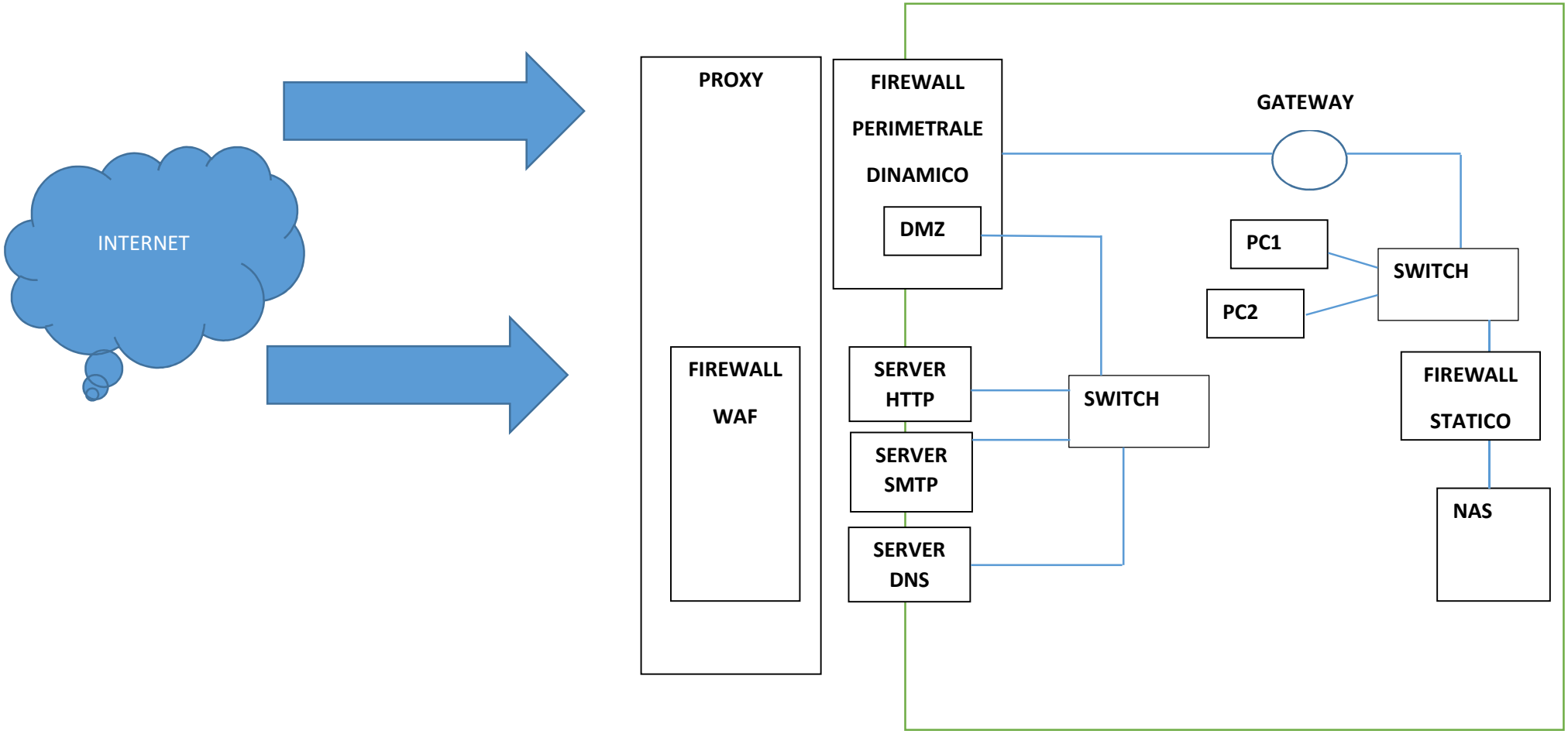
Compito di oggi: disegnare una rete con i seguenti componenti:

- 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.
- Spiegare le scelte.

Come da richiesta è stato messo un Firewall perimetrale dinamico per la protezione principale di tutto il perimetro dell'azienda, sapendo che il Firewall dinamico di default non permette l'accesso da una qualsiasi rete esterna verso l'interno. Per ovviare al problema dell'accessibilità dall'esterno verso l'interno è stata impostata una porta del Firewall perimetrale su DMZ (zona demilitarizzata) in modo da permettere l'accesso ai server web e a chiunque l'accesso per poter comunicare su internet (SERVER http) e tramite e-mail (SERVER SMTP); per proteggere e filtrare la DMZ è stato messo un firewall WAF che scansiona i contenuti a livello applicativo in modo da evitare eventuali minacce che potrebbero crearsi nella DMZ stessa.

A sua volta il WAF lavora all'interno di un Proxy per permettere a quest'ultimo di proteggere gli indirizzi IP della rete interna ed interfacciarli con quella esterna; sapendo che il Proxy nasconde l'indirizzo IP Pubblico, nel momento della richiesta verso la rete esterna, con un altro indirizzo IP Pubblico facendo navigare in anonimato e sicurezza.

All'interno della rete locale abbiamo inserito uno storage aziendale (NAS) protetto a sua volta da un Firewall Statico in modo che permetta un controllo selettivo configurato dall'interno e che consenta accessi solo per alcuni indirizzi IP selezionati (in questo caso pc della rete interna aziendale), sapendo che il firewall statico consente solo il passaggio di indirizzi IP selezionati come PERMIT nella propria tabella ACL.


INTERNET
PROXY
FIREWALL
WAF
FIREWALL
PERIMETRALE
DINAMICO
DMZ
SERVER
HTTP
SERVER
SMTP
SERVER
DNS
SWITCH
GATEWAY
PC1
PC2
SWITCH
FIREWALL
STATICO
NAS