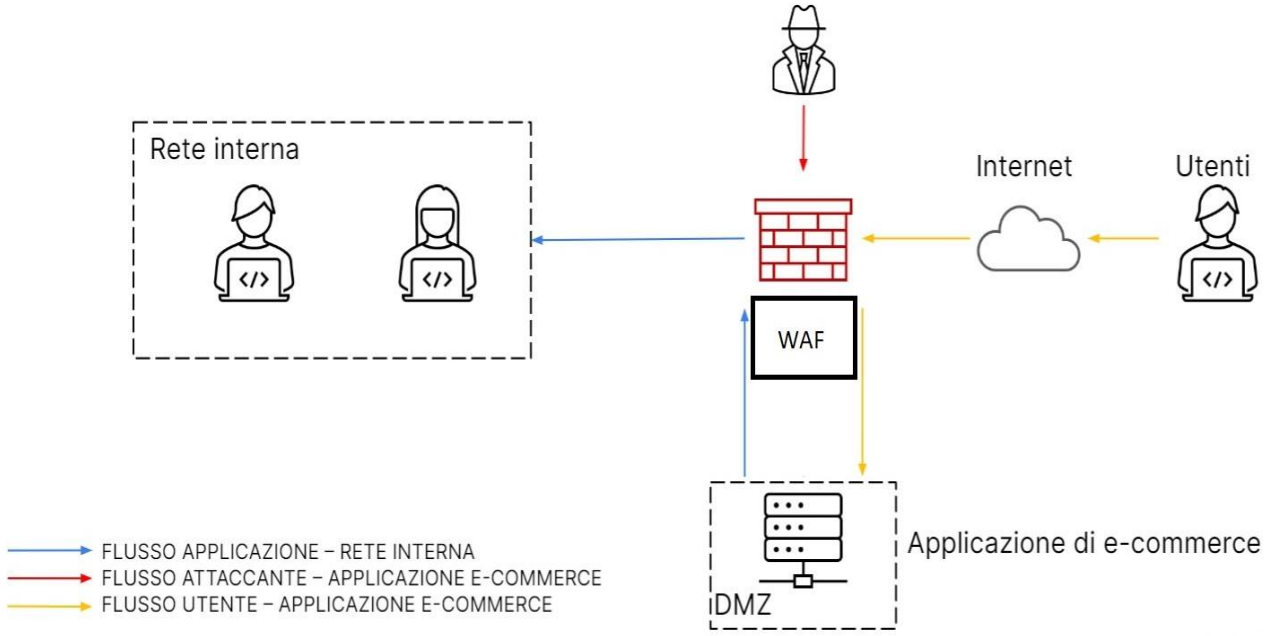
PROGETTO SETTIMANALE

E-commerce

L’esercizio di oggi ci chiede delle soluzioni per rendere più sicura la DMZ (demilitarized zone, non protetta dal firewall).
La soluzione più efficace è aggiungere un WAF prima della DMZ in modo da bloccare gli attacchi di XXS E SQLi.
Il WAF è una protezione che filtra, monitora e blocca il traffico HTTP verso un servizio web.
Come mostrato in figura.



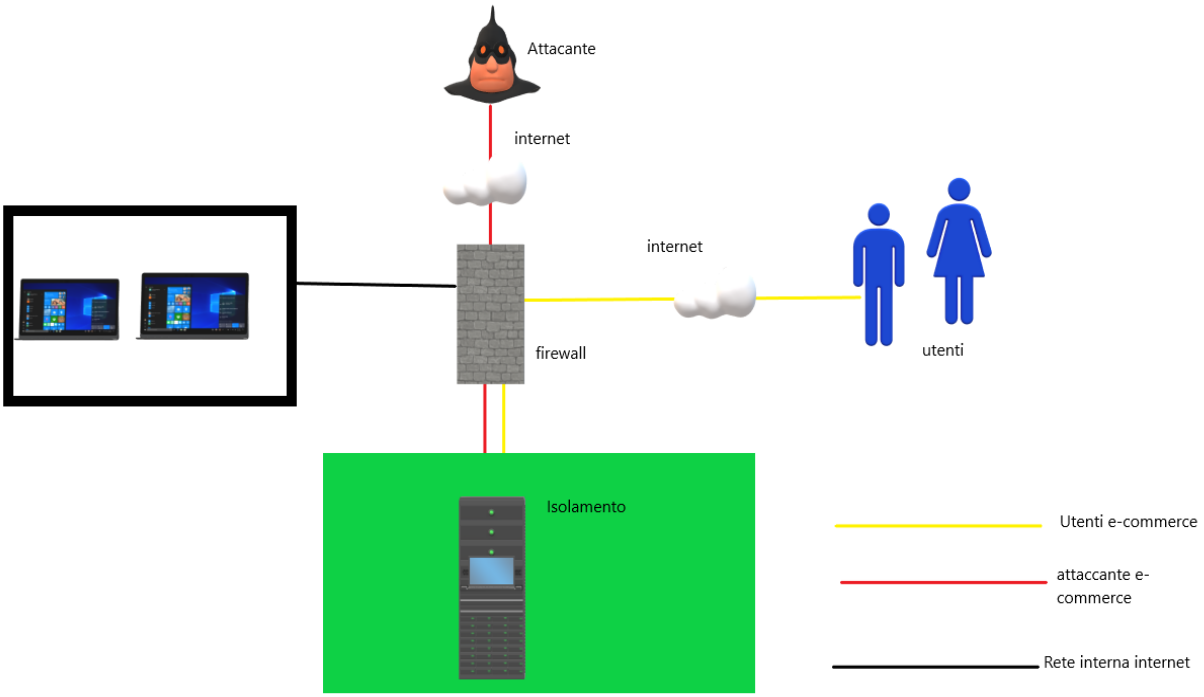
IMPATTI SUL BUSINESS

Considerando il fatto che l’azienda ha un introito di 1.500 euro per minuto e subendo un attacco Ddos il server web è in down per 10 minuti, possiamo applicare una semplice formula. Moltiplicare i

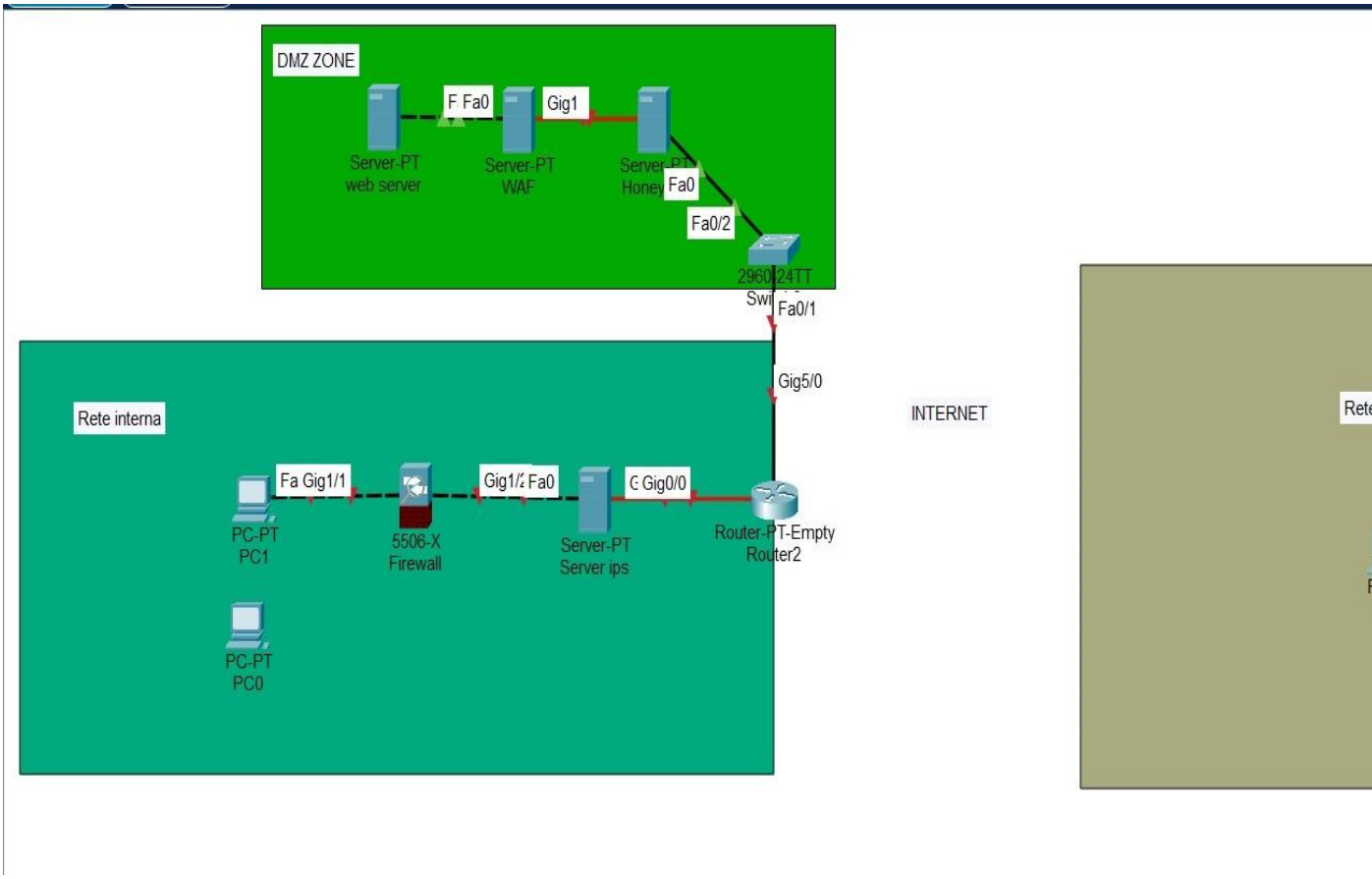
minuti di stop per i soldi fatti al minuto dal E-commerce.
10*1500= 15.000 EURO Che sono i soldi persi durante questo attacco.

Incident response

Nella response siamo già stati attaccati da un malware nella zona DMZ dell’azienda.
La soluzione che possiamo adottare è quella dell' ‘isolamento’ quindi isoliamo la DMZ, cambiando la policy del firewall e bloccando il traffico in entrata dalla DMZ alla rete interna così da non compromettere l’intera rete.
Come in figura:



Soluzione aggressiva.



Se potessimo adottare una soluzione più aggressiva per quanto riguarda la rete interna prima del firewall metterei un IPS (Che prevede e rivela le minacce di sicurezza).
Mentre per quanto riguarda la DMZ oltre al WAF ho messo anche un Honeypot, una vera e proprio esca per un attaccante una macchina che fa finta di contenere informazione preziose. Ovviamente la mettiamo nella DMZ per farsi che sia più facilmente raggiungibile dall'attaccante.
Altra soluzione non applicata era mettere nella DMZ un reverse proxy sempre per filtrare attacchi o richieste non volute.