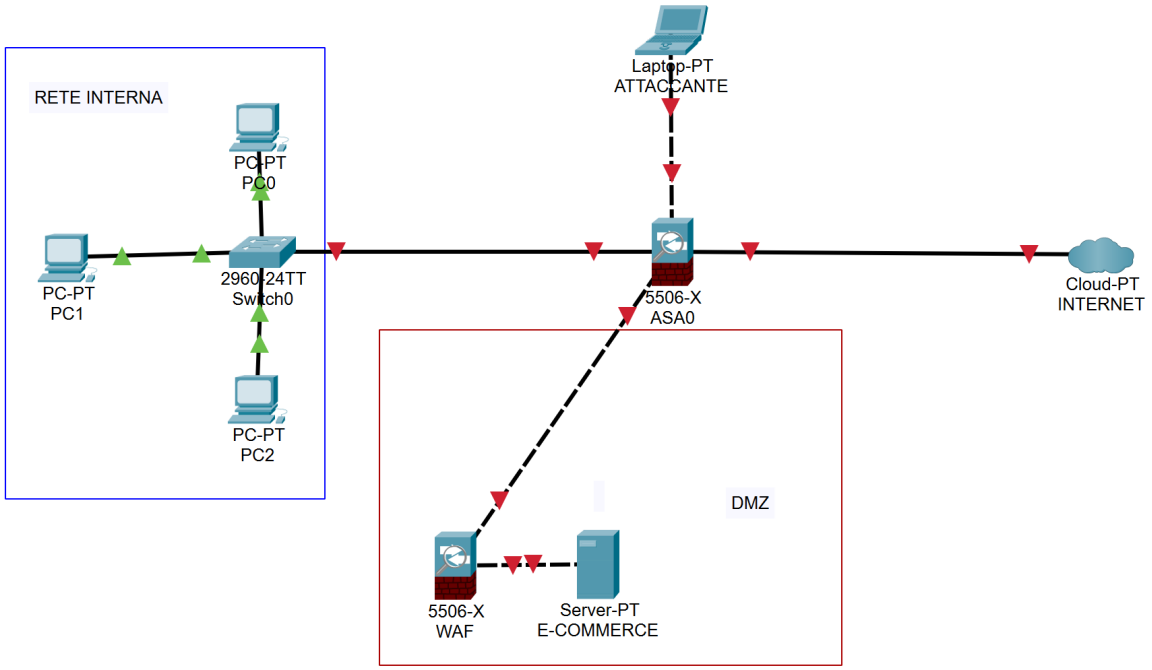
1)Azioni preventive su XSS e SQL injection

Ricordiamo che entrambi questi tipi di attacchi sfruttano un normale dato di input di una web app per eseguire un programma in back o front end. Entrambi possono causare gravi danni e spesso sono difficili da individuare e questo li rende ancora più pericolosi.
La prima contromisura che possiamo eseguire è la sanitizzazione dell'input.
Per fare ciò possiamo sfruttare le numerose librerie che troviamo online come per esempio:
PHP AntiXSS: https://code.google.com/p/php-antixss/
SQLi avoider: https://code.google.com/c/sql/inj-avoid/
Tuttavia ciò potrebbe non essere sufficiente contro un utente esperto che potrebbe trovare vulnerabilità nelle librerie stesse. Per impedire connessioni che sfruttano tale tipo di vulnerabilità andiamo a installare un WAF (Web Application Firewall) sul server dell' E-COMMERCE così da svolgere la funzione di Intrusion Detection System.



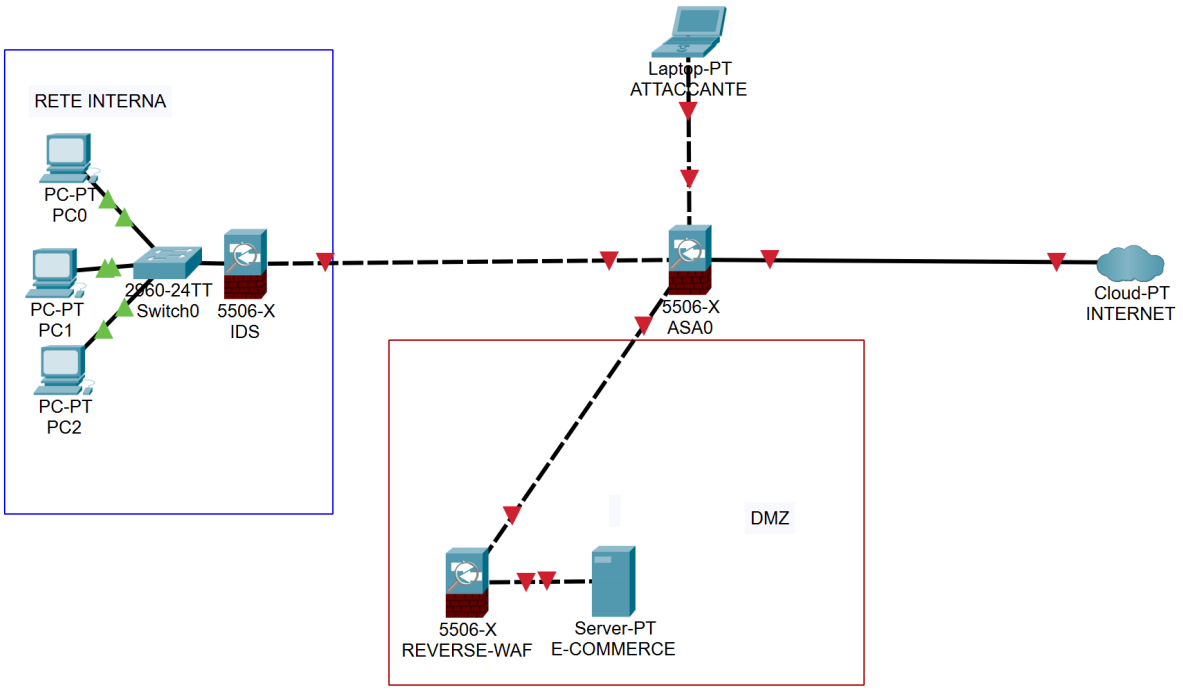
2)Impatti sul business

Supponiamo ora che il nostro server abbia subito un ddos e quindi sia temporaneamente (**10 minuti**) irraggiungibile.
Si stima che in media la nostra attività frutta un introito di **1500 €/min.**
Calcoliamo l'impatto economico dell'attacco: $10 * \cancel{min} * 1500 * \frac{€}{\cancel{min}} = 15000€$
Tuttavia l'attacco potrebbe generare costi aggiuntivi di ripristino del sistema che in questo caso non considereremo.

3) Response

Sfortunatamente la nostra web-app è stata infettata da un malware generico.
Dato che non sappiamo molto sul malware dobbiamo presupporre che possa essere di tipo worm e che quindi possa trasmettersi ad altri utenti. Inoltre la traccia specifica che non c'è interesse nel terminare la comunicazione tra attaccante e server.
Per impedire la trasmissione e tenere sotto controllo il traffico dati in uscita dal server andiamo installare su di esso un reverse-waf e per maggior sicurezza implementiamo il

firewall della rete interna per svolgere la funzione IDS. Utilizzando le giuste regole e permessi possiamo quindi mantenere la connessione tra attaccante e server/malware impedendo che questo si duplichi.



4)Soluzione completa