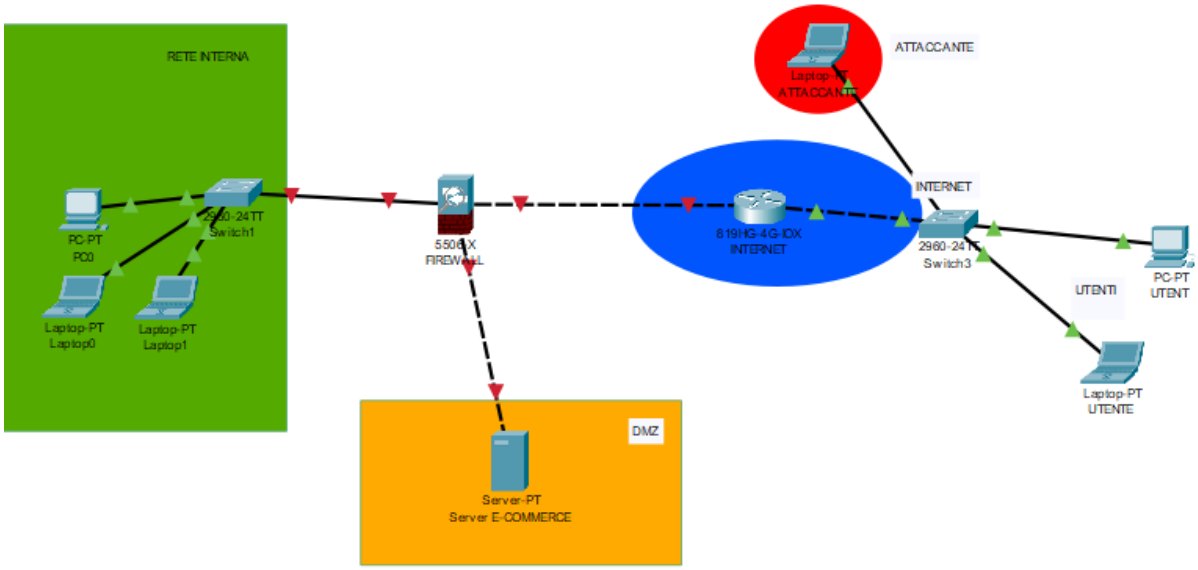
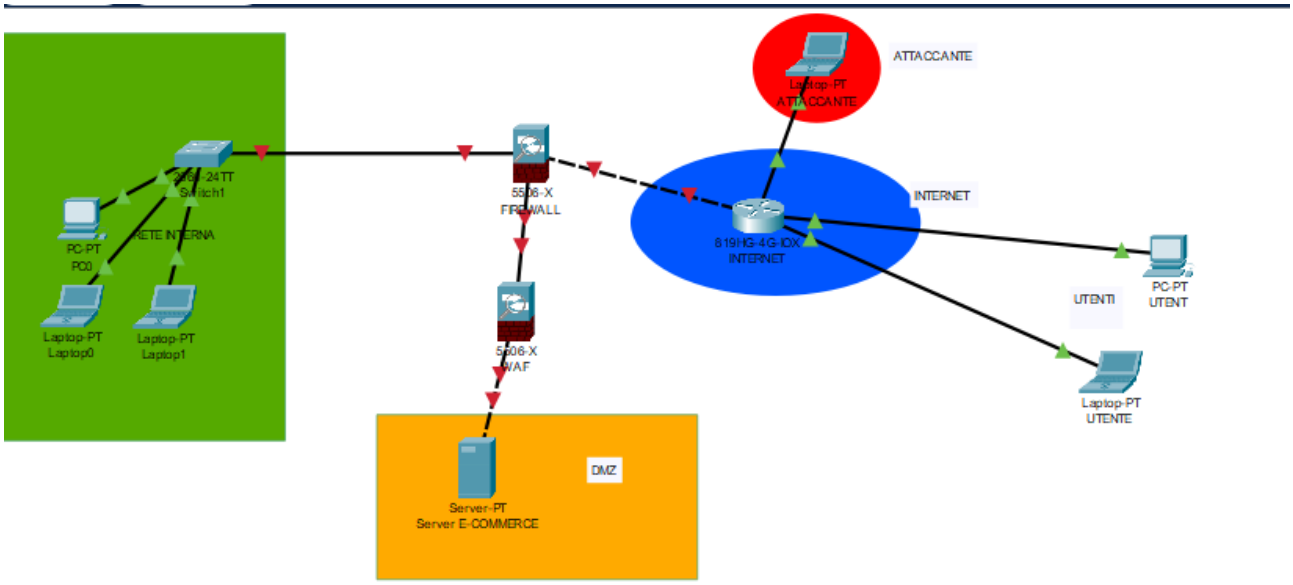
**ARCHITETTURA SISTEMA IN ESAME**




## 1) AZIONI PREVENTIVE A DIFESA DELL'APPLICAZIONE WEB DA ATTACCHI SQLi / XSS:




- <u>Implementazione WAF (Web Application Firewall):</u>
  firewall dedito a proteggere le comunicazioni in entrata nella Web application
- <u>Implementazione autentificazione a due fattori:</u>
  meccanismi di autentificazione per gli utenti che siano forti come appunto l'autenticazione a due fattori (2FA).

- Utilizzo di Utilizzare query SQL parametrizzate:
  l'applicazione dovrebbe utilizzare query che utilizzano variabili anziché costanti nella stringa di query
- Validazione/sanificazione input utente:
  tutti i dati inseriti dall'utente devono essere validati, filtrati e sanificati, in modo da evitare l'inserimento di dati malevoli.
- Utilizzo di token CSRF:
  i token CSRF (Cross-Site Request Forgery) servono per evitare che un attaccante possa sfruttare la sessione di un utente per eseguire azioni malevole.
- Monitoraggio dei Log dei Firewall e dei Log Applicativi:
  ovvero monitorare eventi relativi al traffico che attraversa i firewall ed monitorare tutte le informazioni registrate per l'applicazione web ( accesso al database, modifiche a determinate table)
- Aggiornare costantemente la web application :
  aggiornare tutte le componenti del sistema con le ultime patch sul mercato;

## 2) IMPATTO SUL BUSINESS A SEGUITO DI UN ATTACCO DDoS

Nel caso studio, l'applicazione Web subisce un attacco di tipo DDos ((Distributed Denial of Service) , cioè un attacco che tenta di rendere non disponibile un'applicazione web o una risorsa di rete sovraccaricandoli con traffico dannoso inviato contemporaneamente da sorgenti multiple , per un totale di 10 minuti. Considero che in media ogni minuto gli utenti spendono euro 1500 sulla piattaforma e-commerce.

- Calcolo l'impatto sul business:

Impatto totale = 10 minuti * 1.500 €/minuto = **15.000 €**

- Azioni preventive:
  - Segmentazione di rete :
    assegnando diversi livelli di sicurezza alla retE dividendola ad esempio creando una zona DMZ o una INTERNET NETWORK;
  - Avere dei sistemi ottimizzati:
    ovvero senza servizi inutili, assegnazione controllata dei diritti, elevato livello di autenticazione, i patch sono aggiornati, i cookies SYN sono attivati
  - Effettuare backup dei sistemi almeno 2 volte al giorno

- Remediation :

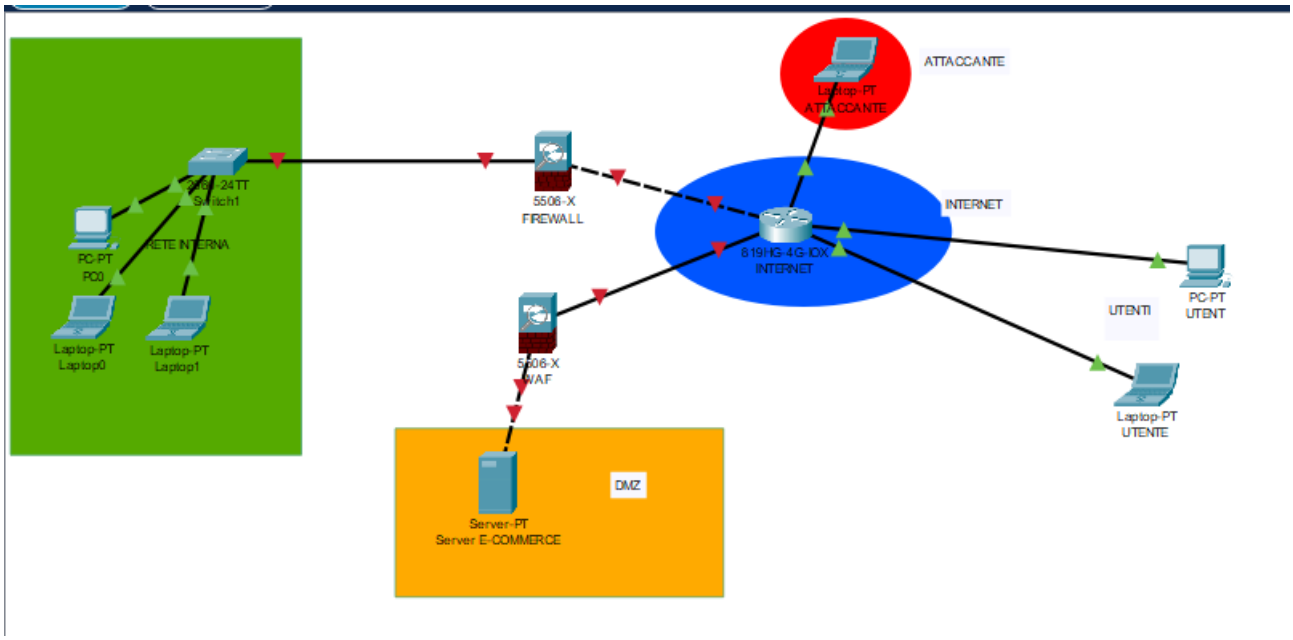
Creazione di un Failover Cluster:

includere due o più server replicati ; ciò permette operatività del sistema anche in caso di un errore, poiché nel momento in cui il server e-commerce venisse infettato/dossato il secondo server2  prenderebbe in automatico il suo posto.

## 3) RESPONSE NEL CASO IN CUI L'APPPLICAZIONE WEB VIENE INFETTATA DA UN MALWARE

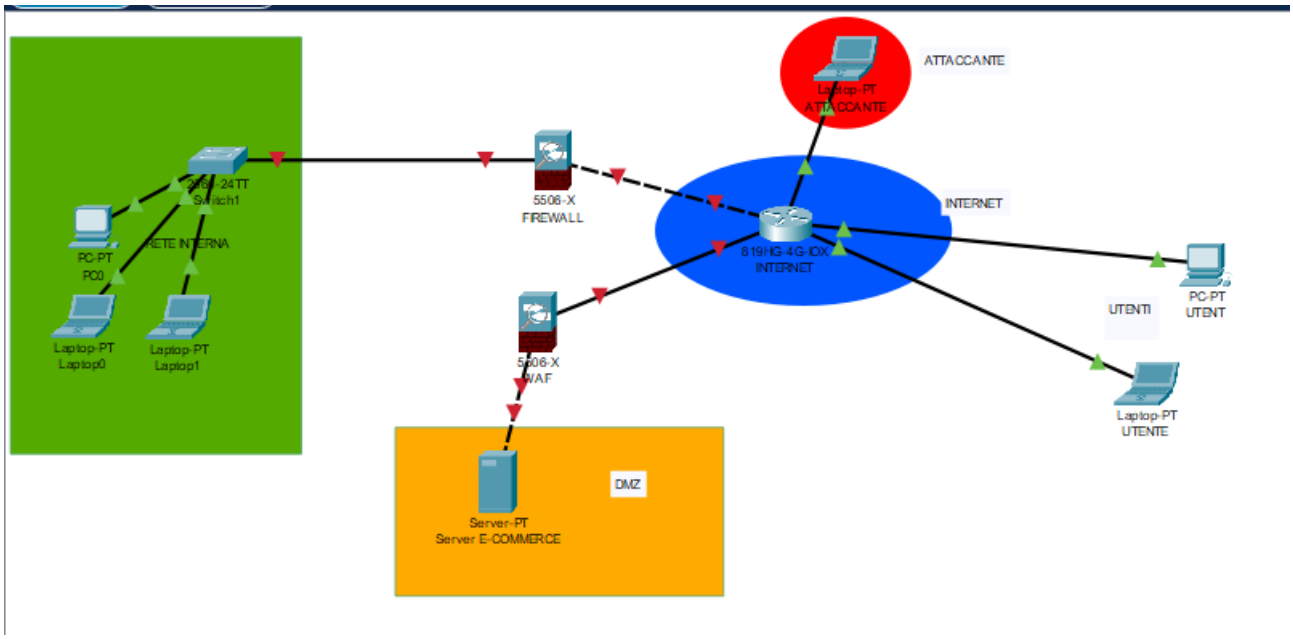
- Per evitare che il malware si propaghi nella rete interna :
  - isolare il prima possibile la macchina/sistema infetto;
  - analisi del codice del malware per capire cosa fa e quindi quali danni possa aver causato;
  - rimuovere il malware
  - ripulire e ripristinare il sistema:

  eliminare tutte le attività e i processi che restano dell'attacco ( ex rimuovere backdoor, ripulire il disco ecc); ripristinare la configurazione pre attacco da backup.



## 4) PROPOSTA SOLUZIONE COMPLETA

- Di seguito viene mostrato in figura l'asset di rete base completo a seguito delle implementazioni precedenti atti a difendere il sito da :
    - Attacchi XSS ed SQLi;
    - Attacchi DDoS
    - Attacco in cui viene iniettato un malware sul server;

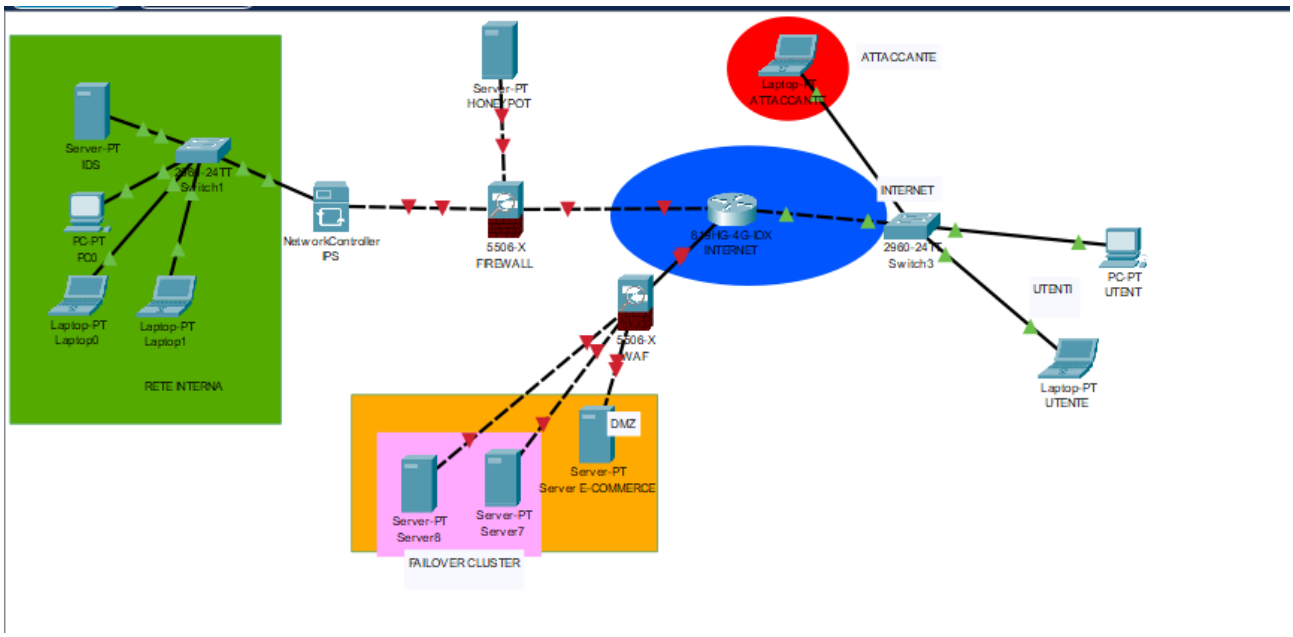



## 5) SOLUZIONE AGGRESSIVA:

Di seguito una proposta che implementa e migliora la sicurezza con maggiore sicurezza che però richiede un **budget maggiore;**

- è stato aggiunto un sistema IDS che rileva intrusioni all'interno di una rete;
- è stato aggiunto un sistema IPS nella rete interna che permette non solo di rilevare intrusioni anomale ma anche di attivare immediatamente delle misure di sicurezza adeguate;
- è stato aggiunto un sistema FAILOVER CLUSTER a livello della Web application;
- È stato aggiunto un sistema HONEYPOT a livello del firewall usato come "trappola" o "esca" a fini di protezione contro attacchi malevoli.

.


Server-PT
IDS
2960-24TT
Switch1
PC-PT
PC0
Laptop-PT
Laptop0
Laptop-PT
Laptop1
RETE INTERNA
NetworkController
IPS
Server-PT
HONEYPOT
5506-X
FIREWALL
ATTACCANTE
Laptop-PT
ATTACCANTE
INTERNET
2960-24TT
Switch3
PC-PT
UTENT
UTENTI
Laptop-PT
UTENTE
5506-X
WAF
DMZ
Server-PT
Server E-COMMERCE
Server-PT
Server8
Server-PT
Server7
FAILOVER CLUSTER