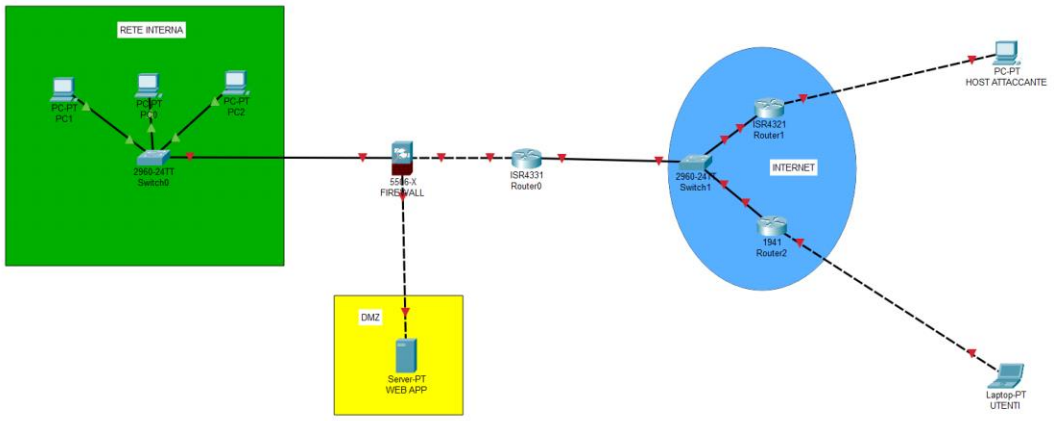



TRACCIA 1

Questa è la nostra architettura di rete dove possiamo vedere che la rete interna è raggiungibile dalla DMZ quindi se il server in DMZ viene compromesso un attaccante potrebbe raggiungere la rete interna.

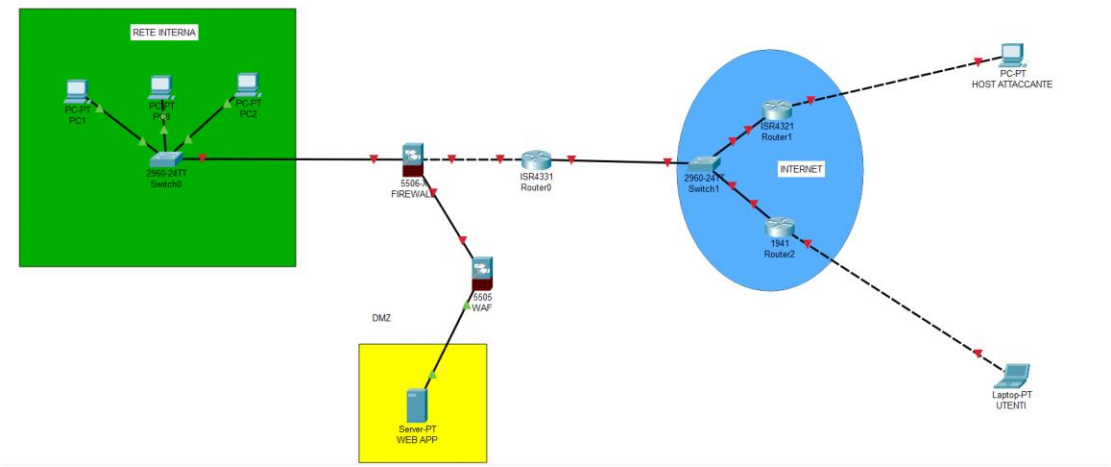
Per poter difendere le web applications da attacchi di tipo XSS ed SQLi,si possono implementare diverse azioni preventive come:

-Validazione dei dati in input: tutti i dati inseriti dall'utente devono essere validati, filtrati e sanificati, in modo da evitare l'inserimento di dati malevoli.

-Una difesa importante è fornita dai WAF (Web Application Firewall). Si tratta di un sistema di difesa da posizionare davanti all'applicazione web.I WAF sono dei firewall che lavorano al livello 7 (applicativo) della pila ISO/OSI.Fondamentalmente ispezionano il traffico HTTP in entrata, assegnano un punteggio di pericolosità alla richiesta e, superato il livello di attenzione previsto, la bloccano.

-Aggiornamenti costanti sul software per mantenere l applicazione web e le sue componenti sempre aggiornate in modo tale da evitare possibili sfruttamenti delle vulnerabilità note

- Utilizzare i token CSRF o Cross-Site Request Forgery che vengono utilizzati per evitare che un’attaccante possa sfruttare le sessioni degli utenti per eseguire attacchi.




TRACCIA 2

Se l applicazione web subisce un attacco di tipo DDoS che la rende irraggiungibile dall esterno per 10 minuti,considerando che in media ogni minuto gli utenti spendono 1500€ l impatto del business sarà dato dal seguente calcolo;

10 * 1500 =15000€

Eventuali azioni preventive per questo tipo di attacco possono essere:

-Arginare il traffico in arrivo da protocolli non essenziali e da indirizzi IP non validi applicando dei filtri a livello di router e firewall.

-Sinkholing:In caso di attacco, questa tecnica prevede di deviare tutto il traffico verso un vicolo cieco, in modo da preservare la stabilità e la piena funzionalità delle risorse informatiche. Ha il punto debole di rendere inaccessibile la risorsa, deviando sia il traffico lecito sia il traffico illecito, ma quanto meno salva l'infrastruttura informatica da danni irreparabili

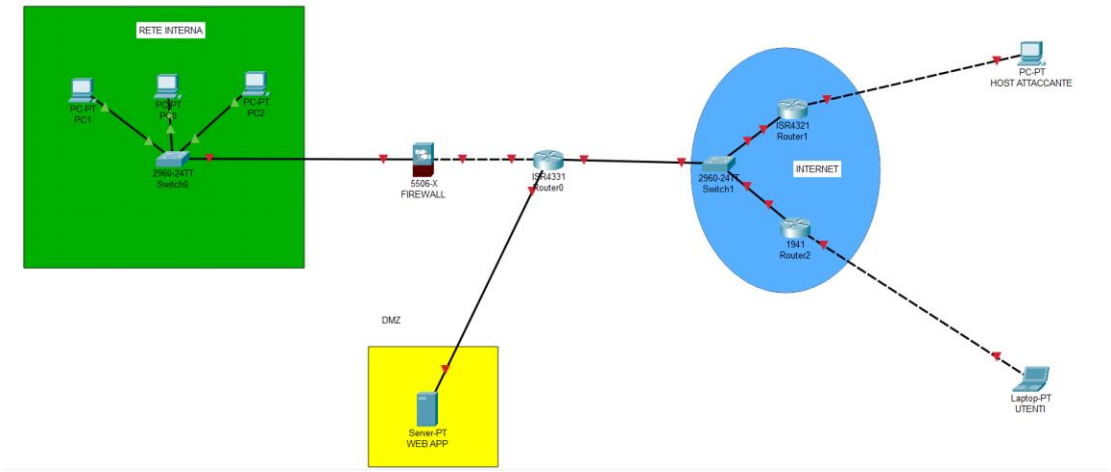
-Ridondanza: la maggior parte delle grandi aziende impiega una quantità sovrastimata di risorse hardware e di larghezza di banda, in modo da poter gestire i picchi di traffico e limitare i danni in caso di attacco DDoS.

-Formare il personale sulla sicurezza informatica e sulle procedure da seguire in caso di attacco informatico.

-Installare Intrusion Detection System (IDS) che possono rilevare e segnalare attività sospette.

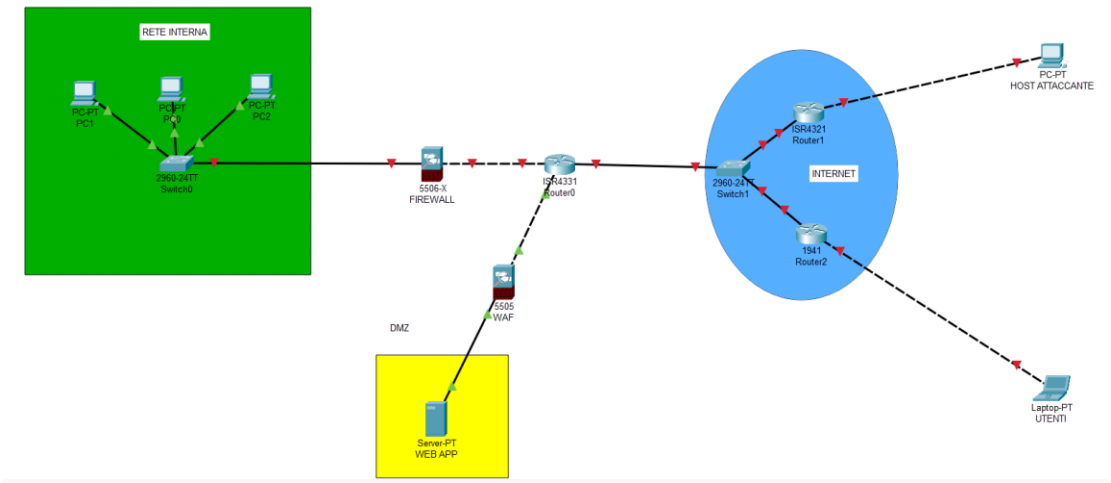
TRACCIA 3

Response:

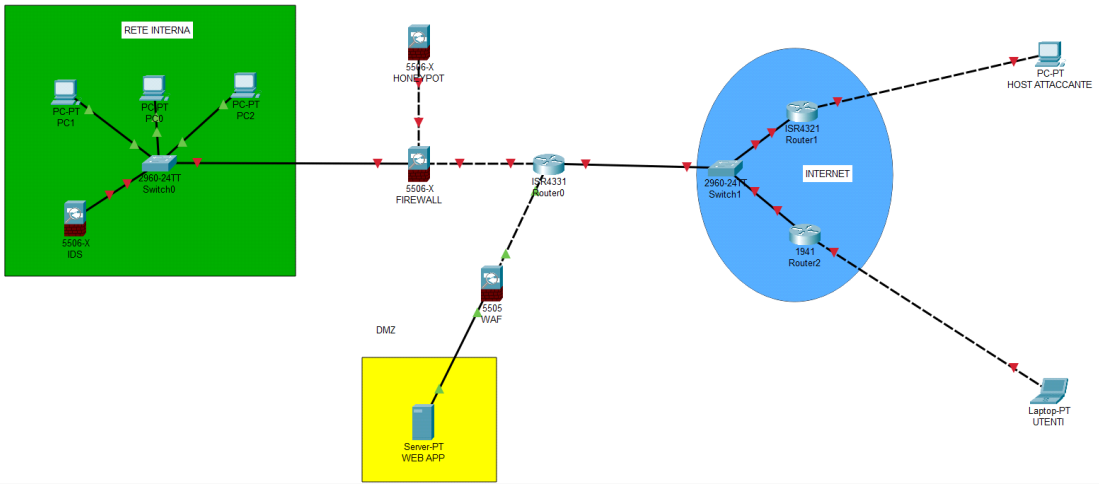



Per evitare il propagarsi del malware sulla rete interna, abbiamo isolato l'applicazione fuori dal firewall, facendola passare prima dal router.Una volta isolata la macchina infetta si dovrebbe procedere all analisi del malware per capire com è entrato e che danni ha arreccato.Passare poi alla sua rimozione ed infine pulire la macchina infettata ripristinando la sua configurazione precedente.

TRACCIA 4




TRACCIA 5


RETE INTERNA
PC-PT
PC1
PC-PT
PC0
PC-PT
PC2
2960-24TT
Switch0
5506-X
IDS
5506-X
HONEYPOT
5506-X
FIREWALL
ISR4331
Router0
5505
WAF
DMZ
Server-PT
WEB APP
2960-24TT
Switch1
ISR4321
Router1
INTERNET
1941
Router2
PC-PT
HOST ATTACCANTE
Laptop-PT
UTENTI