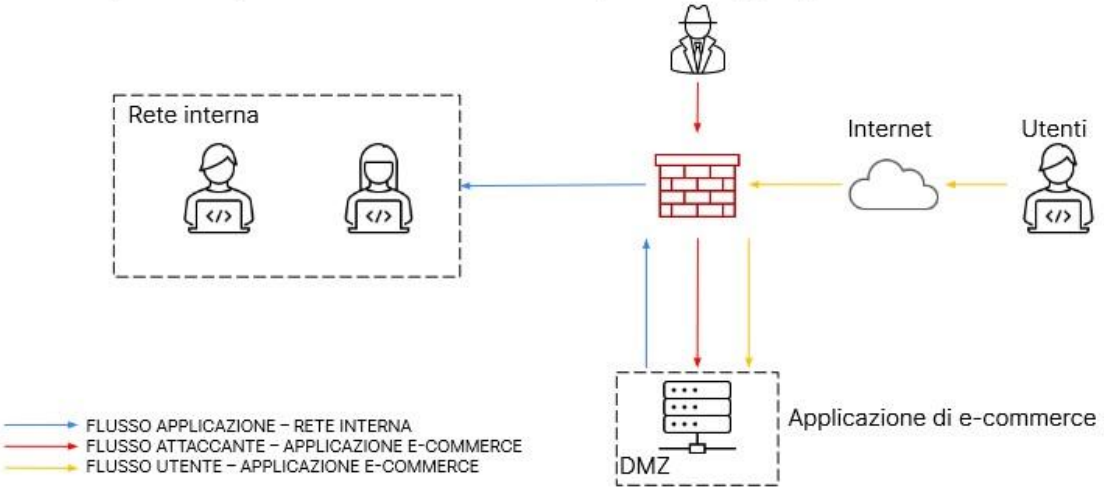
Analisi rete di e-commerce

Architettura di rete:
L'applicazione di e-commerce deve essere disponibile per gli utenti tramite internet per effettuare acquisti sulla piattaforma.

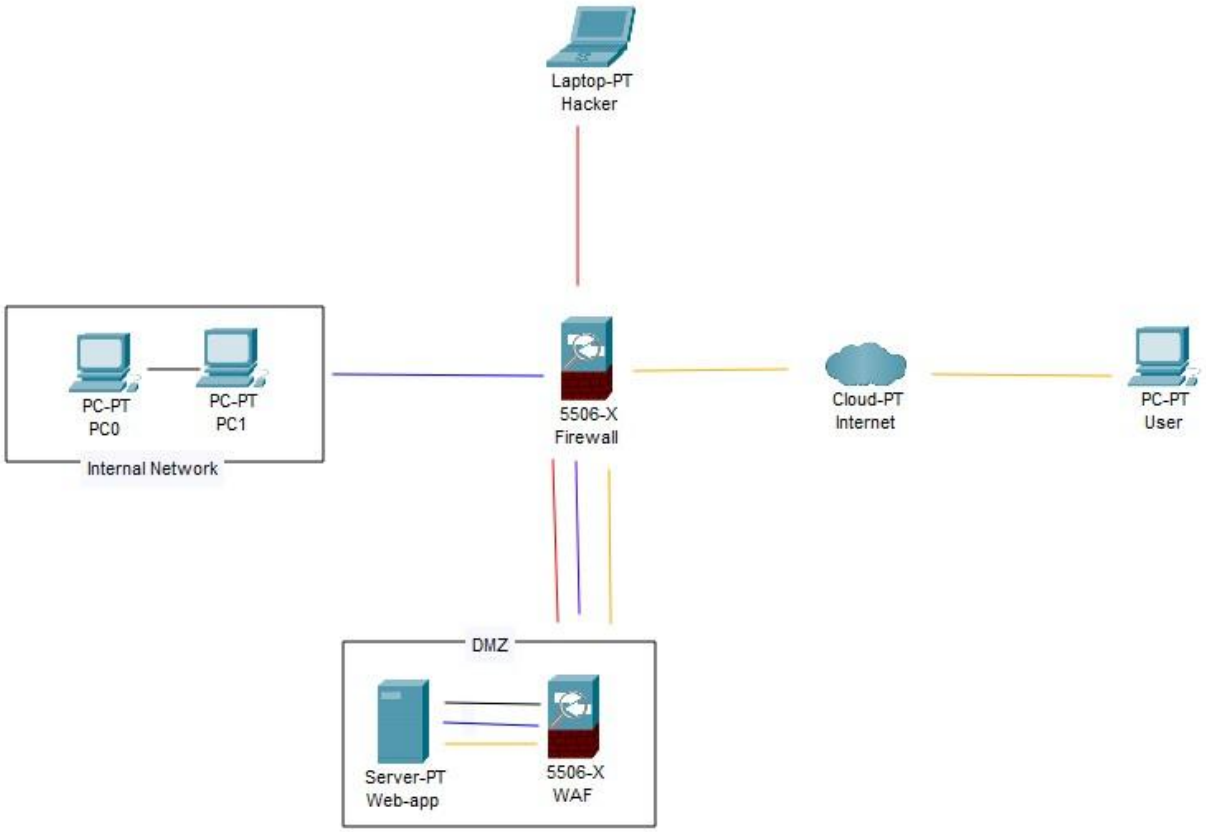
La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.



Questa é la rete attuale dell'ecommerce al quale presenta diverse vulnerabilitá.

Risposta 1:
Difendi da SQLi e XSS.

Per prevenire attacchi SQLi e XSS è possibile aggiungere un WAF (Web Application Firewall) e dei controlli dell'input utente sulla web-app, qui sotto lo schema. Qui é possibile vedere l'implementazione del WAF.

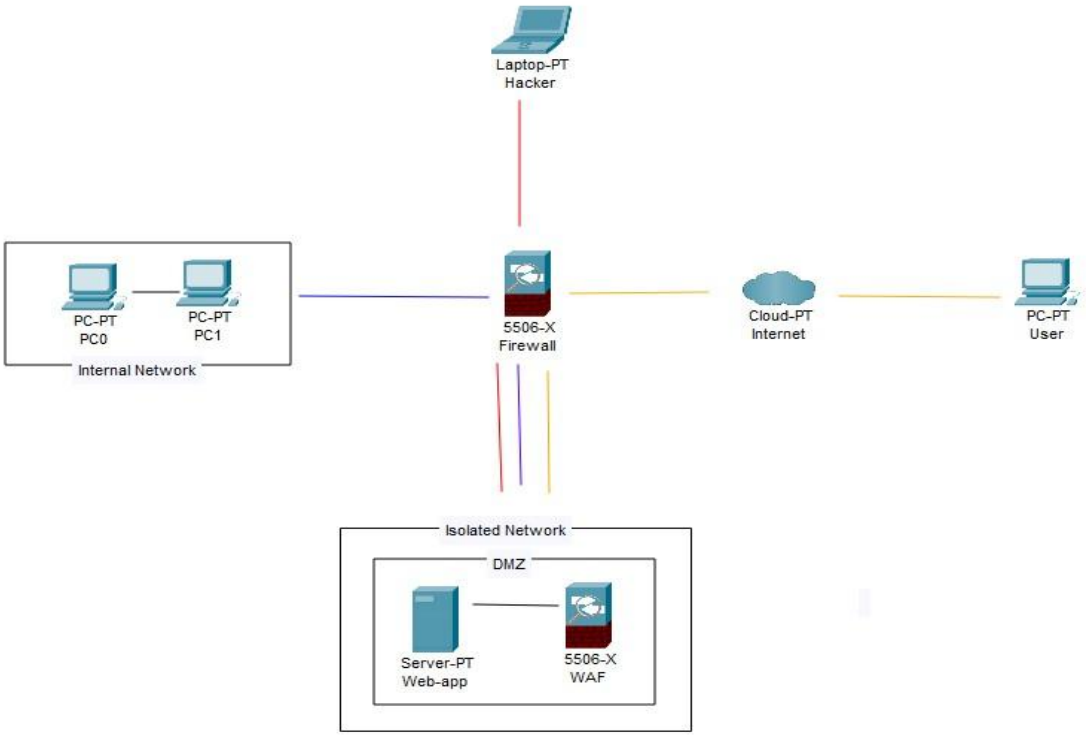


Risposta 2:
Impatto sul business, service down per 10 minuti, soldi spesi nella piattaforma ogni minuto = 1.500$

Costo del disservizio = 15.000$

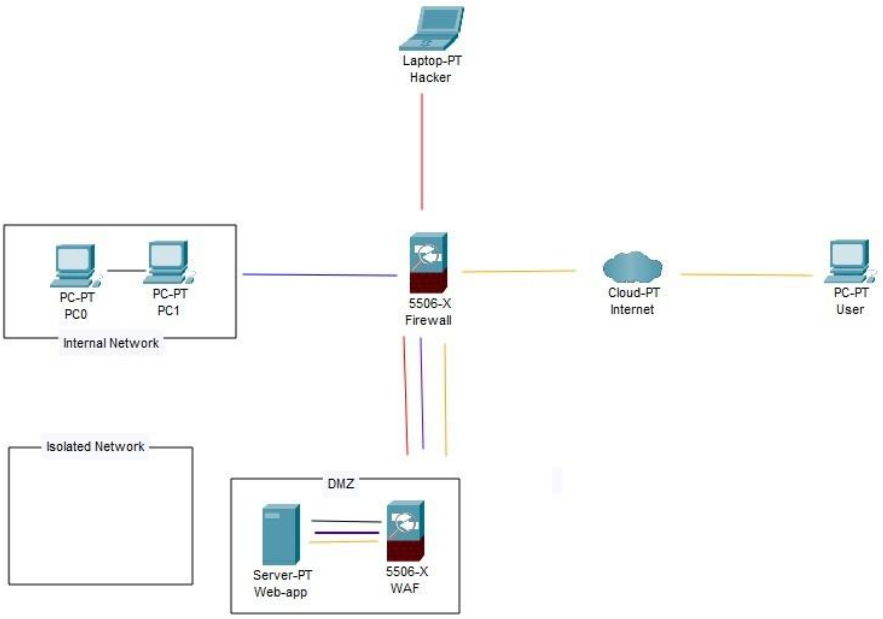
Risposta 3:
La Web-app è infettata da un malware, evitare che si propaghi in tutta la rete.

Qui sotto l'immagine con l'isolamento per evitare che si propaghi, la web-app non è più accessibile da nessuno e non si puó propagare.



Risposta 4:
Unione delle precedenti soluzioni.

Aggiunta la rete isolata per eventuali eventi:



Risposta 5:
Modifica all'intera infrastruttura, contando anche i costi sull'impatto del business.

Aggiunte:
- IDS (Intrusion detection system), non ho scelto l'IPS perché può aggiungere latenza nell'utilizzo della Web-App. Puó essere aggiunto dal firewall oppure online sono a circa 200$

- NAS per fare backup della web-app e non solo. Per questo business circa 1000$ per raid 6

- Server di backup per la Web-App in caso di disservizio in modo tale da causare un disservizio minimo in caso di eventi. Prezzo da calcolare in base alla web-app.

- Piú reti per la diversificazione in piú per la NAS è possibile accedere sono nella rete locale ed a determinati IP in modo tale da avere + layer di sicurezza.

- Per la configurazione della Web-App utilizzerei DOCKER perché quando si avvia un nuovo servizio è containerizzato quindi anche in caso di ransomware è possibile avere un layer in piú di sicurezza ed inoltre in caso di disservizio si puó prendere il backup di docker ed avviarlo nel server secondario e ció ha due pro:

1. Si puó avviare all'istante il servizio
2. Non ci sono problemi di mis-configuration o di configurazione in generale.

- UPS per mantenere sempre ON la web-app circa 800$

Quindi in caso di disservizio sarà possibile spostare la web-app infetta in una rete isolata e avviare all'istante il server di scorta con il backup di docker della web-app.

Si possono quindi limitare i problemi con circa 2000$ da contare in piú il server di backup.