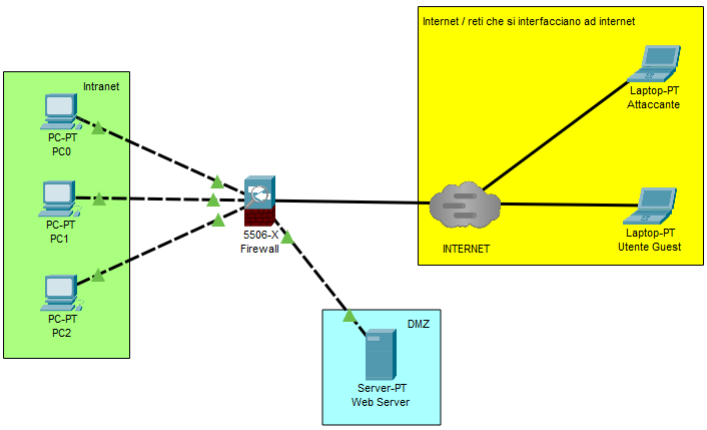
Prova pratica

PREVENZIONE, ATTACCO & RINFORZO

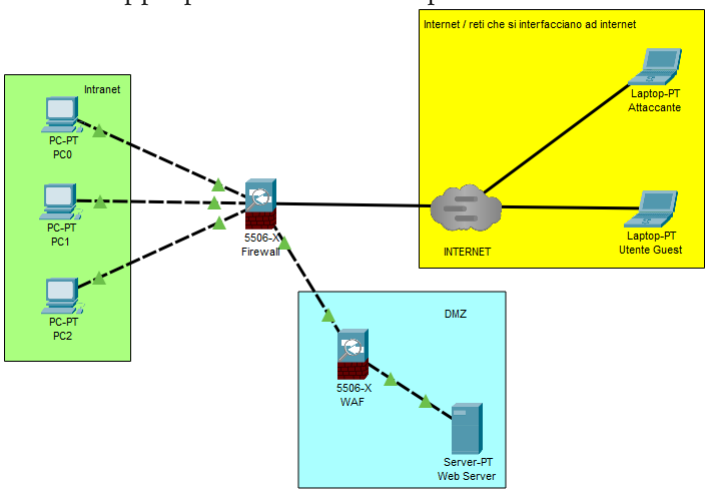
03-24-2023

PUNTO 1

Per difendere la nostra web application situata nella DMZ dall'eventuale azione da parte di utenti malintenzionati aggiungiamo alla rete un Web Application Firewall che filtra ed analizza il traffico, permettendoci di definire e gestire regole per evitare minacce provenienti dall'esterno, inoltre fornisce anche sistemi di registro dei log che possono facilitare il lavoro di ricerca post attacco fornendo utili informazioni agli operatori tecnici.
Il WAF non è l'unico modo per proteggere il nostro sito da attacchi di tipo SQLi e XSS appunto basterebbe controllare ed eventualmente sanificare l'input utente con controlli appropriati a livello di script.



Rete di partenza



Rete con WAF

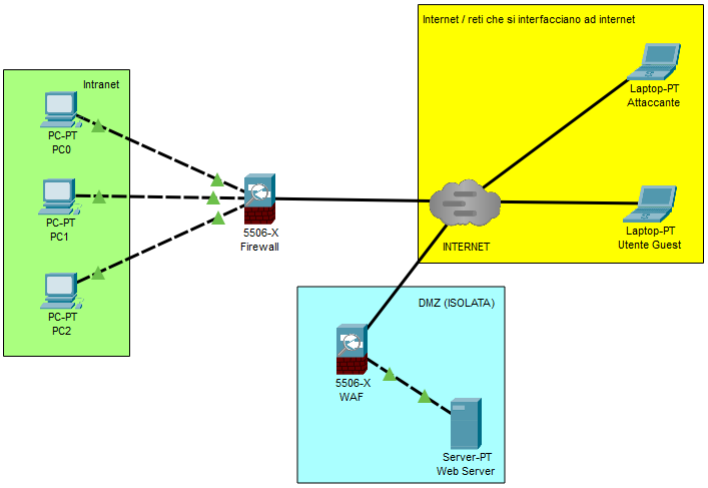
PUNTO 2

Se la nostra web application subisce un attacco di tipo DDoS dall'esterno che abbatte il sito per 10 minuti, tenendo di conto il fatto che per ogni minuto la media di acquisti è di 1.500 euro, si può incorrere in gravi danni a livello economico, superiori ai circa 15.000 che son stati persi durante l'azione malevola, infatti il sito potrebbe non essere più ritenuto affidabile da parte di alcuni clienti portandoli ad andare dalla concorrenza con una conseguente perdita di denaro esponenziale nel tempo, un attacco del genere è attuabile solo se l'azienda in questione non ha attuato sufficienti misure di prevenzione ad esempio l'utilizzo di un WAF specifico o l'appoggio a servizi di terzi come Cloudflare che garantisce il 99% di uptime del server.

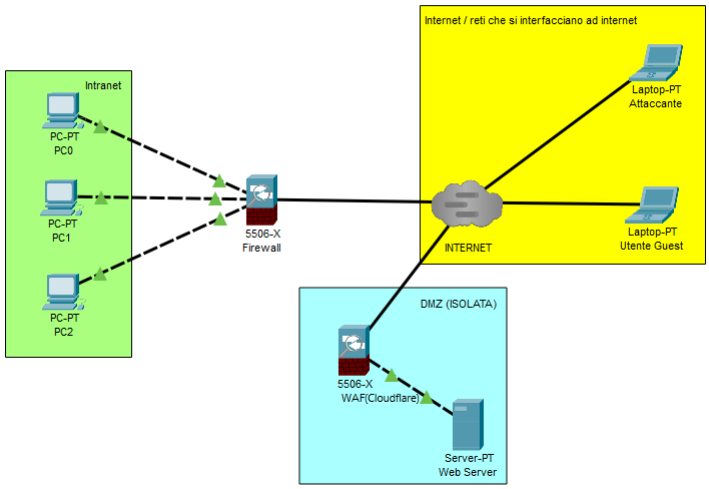
Immagine nel punto 4

PUNTO 3

Se il nostro sito viene infettato da un malware possiamo fare il modo che non si propaghi nella nostra rete privata escludendolo direttamente dalla rete interna ma non da internet, dato che tenendolo in una rete isolata abbiamo la possibilità di indagare ed eventualmente scovare il colpevole o semplicemente studiare il metodo d'attacco per far si che non si ripresenti una cosa simile in futuro.
Una soluzione meno sicura ma che non implica un secondo contratto con il provider sarebbe di aggiungere regole al firewall creando una sottorete in cui verrà ospitato solo il server infetto.



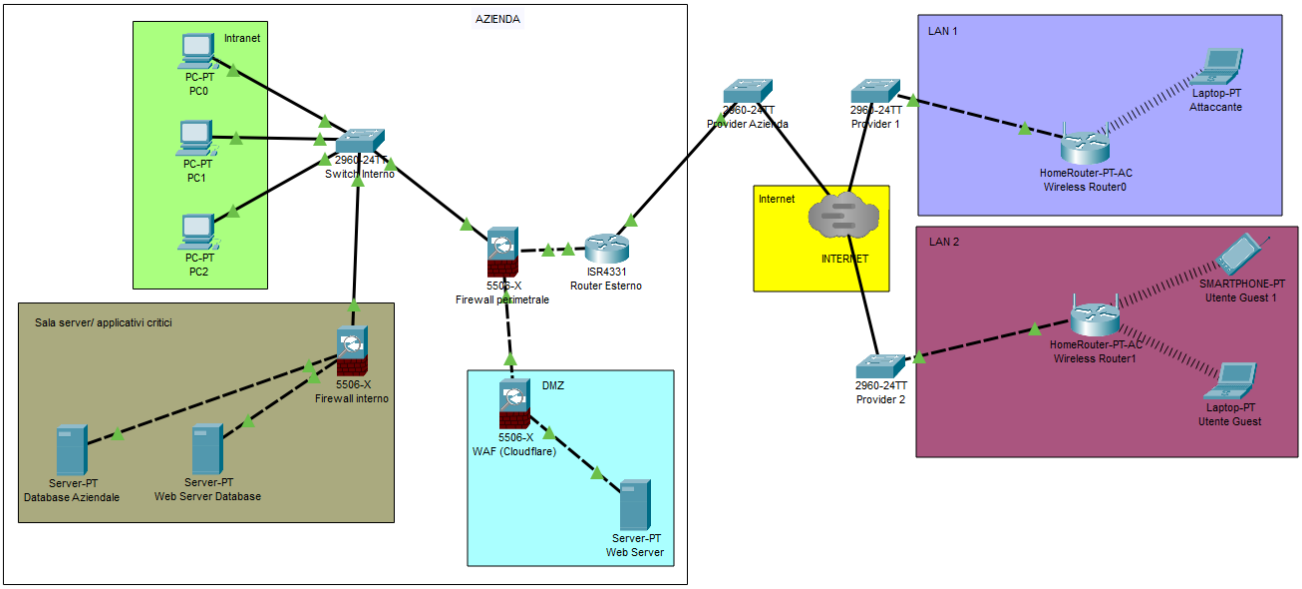
PUNTO 4



L'immagine sopra è pressoche uguale all'immagine di figura 3, con la differenza che in questo caso abbiamo la protezione aggiuntiva di Cloudflare che ci permette di avere uno strato solido di protezione in più ad un costo irrisorio per un azienda.

PUNTO 5

Sotto vediamo invece una rete aziendale più "reale" con vari sistemi di prevenzione e segmentazione che assicurano un corretto svolgimento del lavoro evitando il più possibile le azioni di malintenzionati, ma pur sempre rimanendo in uno schema economico e accessibile anche ad un'azienda medio piccola, se il budget fosse maggiore si potrebbe pensare all'implementazione di sistemi IDS, IPS, honeypot e server di backup, inutile dire che tutto questo risulterebbe inutile senza una corretta configurazione dei singoli componenti.



PedrazziAndrea