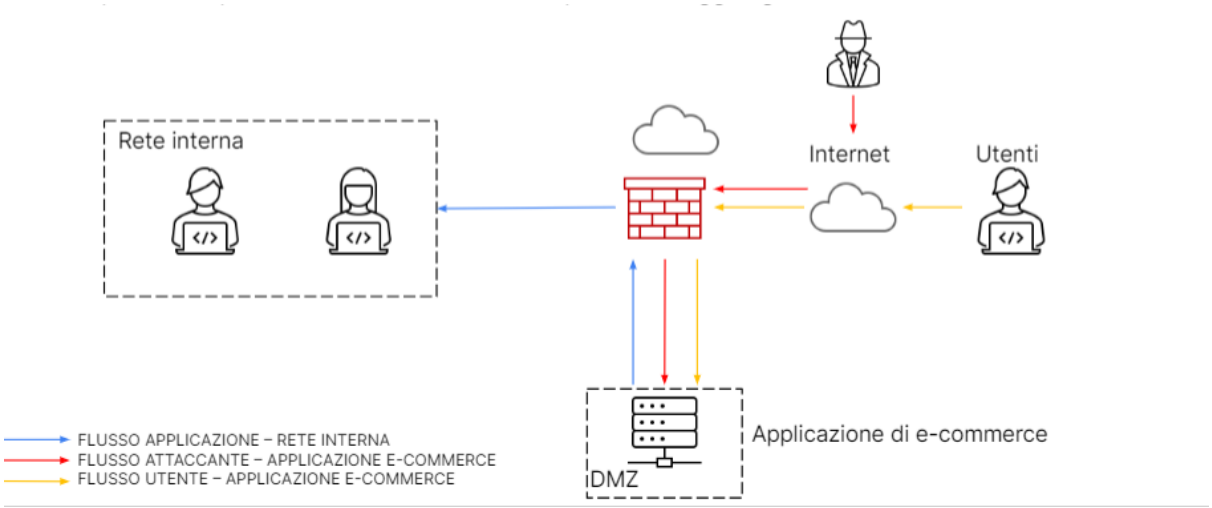
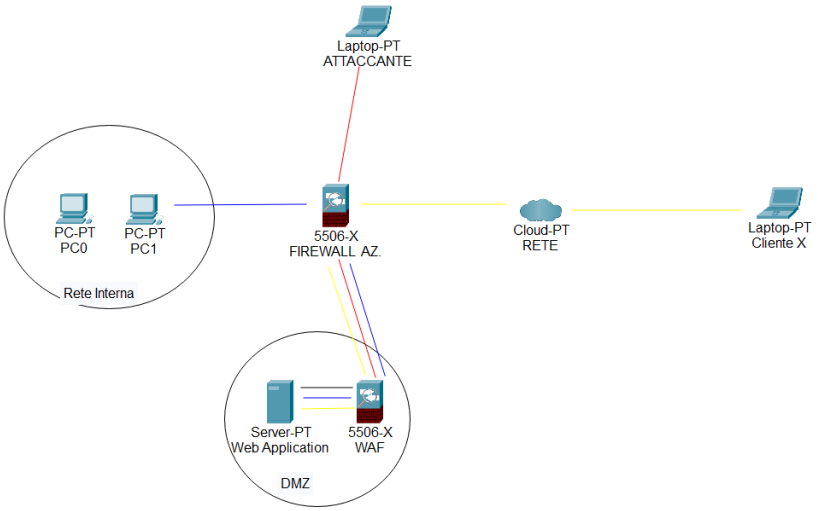
Analisi di una rete di e-commerce

Nel caso odierno saremo impegnati nell'attività di messa in sicurezza della rete dell'azienda cliente anche in maniera preventiva, attualmente la rete si presenta configurata come in figura sottoriportata.



Secondo quanto richiesto dall'azienda cliente, la stessa in primo luogo vorrebbe che la rete venga modificata in modo che si implementi una protezione aggiuntiva all'applicazione web che vada a proteggere quindi il server da eventuali attacchi di tipo SQLi e XSS.
Per effettuare questo tipo di implementazione ci serviremo di un firewall aggiuntivo definito WAF (web application firewall) da inserire nella demilitarized zone come possiamo notare nel progetto eseguito con l'aiuto di Packet Tracer.



L'integrazione del Web Application Firewall ha molti vantaggi grazie ad una protezione proattiva che protegge le applicazioni web da attacchi automatizzati, DDoS, Brute Force, SQL injection, XSS . La protezione proattiva aiuta a identificare e mitigare gli attacchi prima di essere eseguiti realmente sulle vostre applicazioni web riducendo notevolmente i rischi da vulnerabilità e possibili data breach.

Analisi di una rete di e-commerce

In secondo luogo ci sono stati segnalati due link malevoli e adesso andremo a farne un'analisi dettagliata degli stessi.

Nel primo link fornitoci dall'azienda grazie all'utilizzo di any.run (un potente strumento che ci permette il rilevamento, il monitoraggio e la ricerca di minacce informatiche in tempo reale) analizziamo il comportamento del link malevolo e scopriamo che si tratta di uno script PowerShell che consente di modificare le impostazioni del server DNS. Questo quindi significa che se un dipendente anche solo per errore clicchi su quel link malevolo potrebbe permettere ad un potenziale attaccante la pratica del ***DNS hijacking*** che può essere di più varianti, tra le quali troviamo :

- ***Router Hijack*** dove i malintenzionati attaccano i dispositivi, sfruttando proprio le credenziali d'accesso al sistema predefinite e manomettere le impostazioni del DNS.
- ***Local Hijack***, dove attaccano direttamente il pc dell'utente installando un malware capace di accedere alle impostazioni DNS del dispositivo e inserire il proprio server DNS.
- Attacchi DNS man in the middle (***MITM***), dove vengono intercettate le comunicazioni tra utente e server DNS per cambiare l'indirizzo IP di destinazione verso pagine web dannose.
- ***Rogue Hijack*** dove non si colpisce direttamente il dispositivo ma un name server.

Nel secondo link invece fornitoci dall'azienda analizzando il comportamento nella sanbox di any.run arriviamo alla conclusione che si tratti di ***keylogger*** della categoria r***emcos RAT*** che permette l'installazione di una backdoor da parte di un attaccante con il quale lo stesso riesce a percepire:

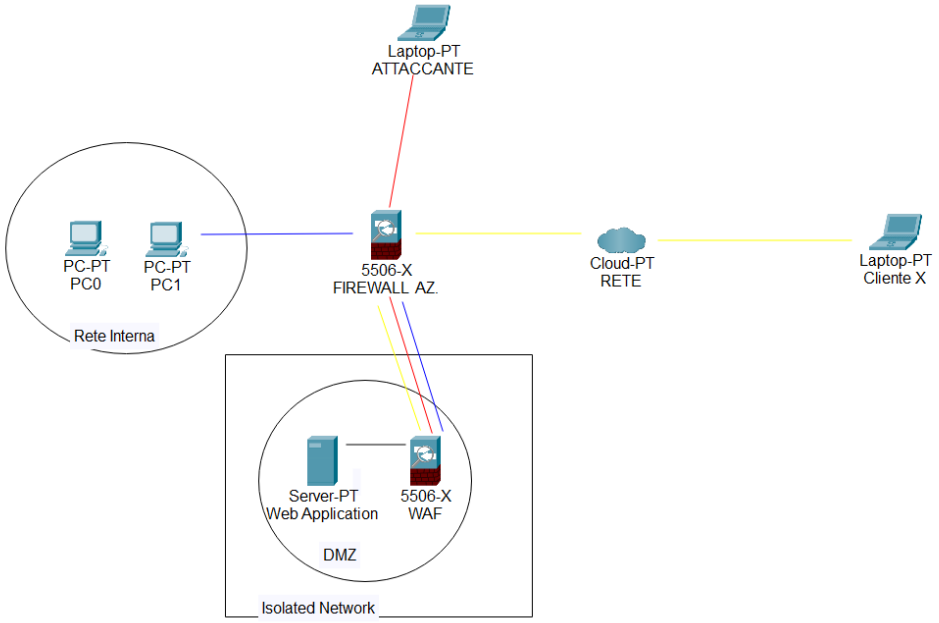
- informazioni sul computer (versione del sistema operativo, nome del computer, tipo di sistema, nome del prodotto, adattatore principale)
- informazioni utente (accesso utente, profilo utente, nome utente, dominio utente)
- informazioni sul processore (numero di revisione del processore, livello del processore, identificatore del processore, architettura del processore)

Quello che invece accade ad un sistema compromesso e come si comporta lo stesso è riassumibile in questi punti:

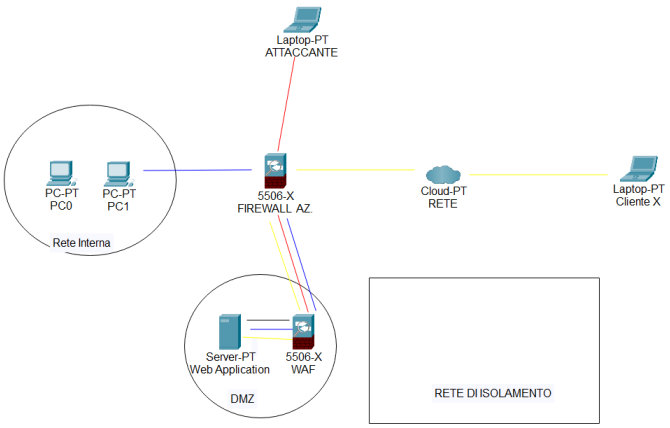
- Bypassa i prodotti antivirus
- Mantiene la persistenza sulla macchina attaccata
- Viene eseguito come processo legittimo di Windows
- Ottiene i privilegi di amministratore e disabilita il controllo dell'account utente (UAC)
- Ruba informazioni aziendali
- Compromette la sicurezza del sistema, con funzionalità backdoor in grado di eseguire comandi dannosi
- Viola la privacy dell'utente: raccoglie le credenziali dell'utente, registra i tasti premuti e ruba le informazioni dell'utente.

Analisi di una rete di e-commerce

Per quanto riguarda la response richiesta relativa all'applicazione web infetta da un malware la soluzione migliore rimane l'isolamento della stessa per avere contenimento e il non verificarsi della propagazione del malware .
Andremo quindi a disconnettere dalla rete interna la web application per evitare quindi la propagazione nella rete interna ma mantenere l'accesso ad internet.
Sotto vediamo una figura delle modifiche che andremo ad effettuare.



Nella quarta richiesta da parte dell'azienda la soluzione mirata sia alla prevenzione che alla response sarebbe quella di integrare sia il WAF che una zona già predisposta per l'isolamento in caso di attacco malware ed uno schema della rete con queste modifiche viene proposto qui di seguito con un design di rete appropriato.



Analisi di una rete di e-commerce

Come soluzione finale e quindi più aggressiva e definitiva per l'azienda proporrei questo design di rete che vede implementati e migliorati molti aspetti della stessa che andremo ad analizzare di seguito sotto.
Per prima cosa consiglio l'implementazione di un IDS (intrusion dectection system) e non un IPS (intrusion prevention system) per evitare problemi di rete e di latenza per l'utilizzo dello stesso ma allo stesso tempo rilevare eventuali intrusioni nella rete.

In secondo luogo ho aggiunto un server di backup per memorie NAS (network attached storage) per eseguire il backup delle web app ma anche dei vari pc degli utenti aziendali e quindi permettere in maniera condivisa lo storage dei vari backup sulla rete. A questo server si ha accesso solo da rete interna.

Verrebbe inoltre aggiunto un server di backup per la web app in una dmz secondaria che abbiamo anche definito di isolamento nel caso in cui il server primario venga attaccato e avere quindi un rimpiazzo pronto per evitare danno economico all'ecommerce.

Miglioria che integrerei è l'installazione di un UPS che rende sempre accessibile anche in caso di perdita di corrente l'utilizzo della web app e di tutti gli altri dispositivi.

Per finire aggiungerei un honeypot web app che va a simulare il funzionamento della web app di ecommerce e quindi permette di confondere l'attaccante.
Questa verrà resa particolarmente appetibile costruendoci attorno vulnerabilità di sicurezza. Ad esempio, avrà porte che rispondono a una scansione, o una password debole. Le porte vulnerabili potrebbero venire lasciate aperte per attirare gli hacker nell'ambiente honeypot, invece che nella più sicura rete aziendale.