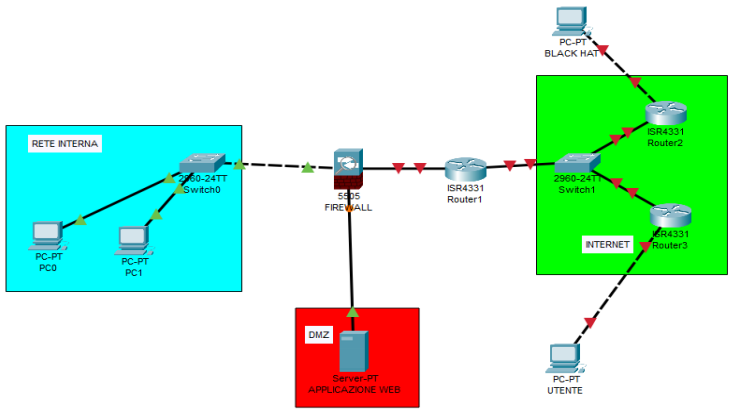
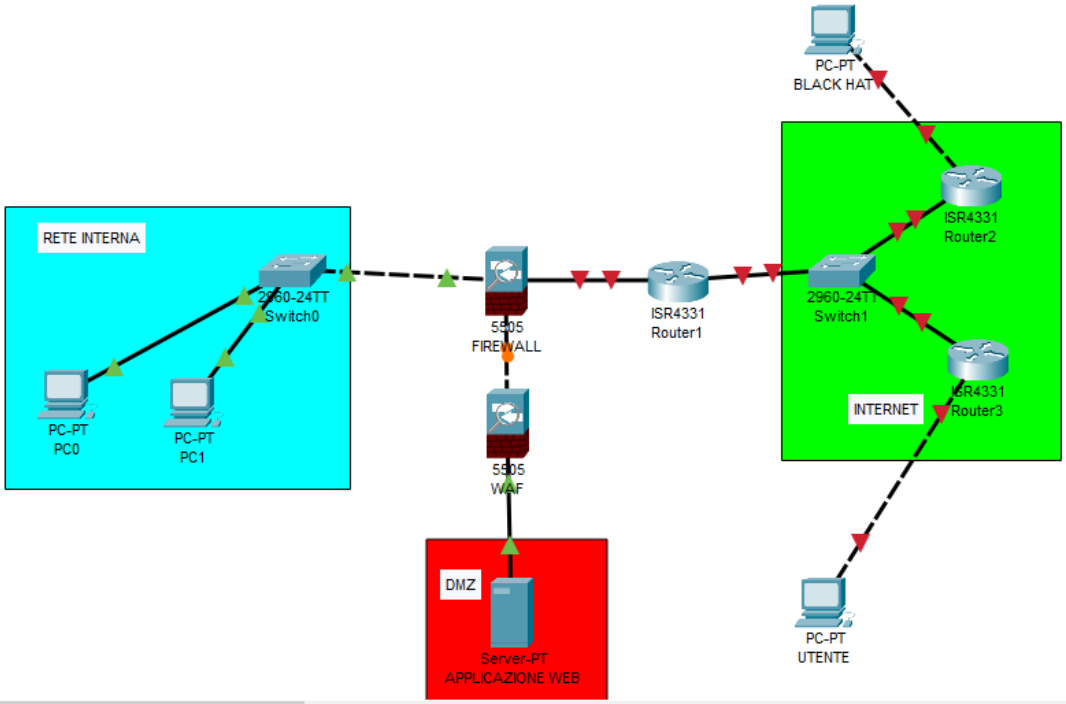
QUI VEDIAMO L’APPLICAZIONE WEB CONNESSA AL FIREWALL CON ACCESSO ALLA RETE INTERNA



TRACCIA NUMERO 1
, L’applicazione viene compromessa e andiamo a evitare l’accesso alla rete interna attraverso un waf .I Web Application Firewall (WAF) consentono di proteggere le applicazioni Web da attacchi dannosi e traffico Internet indesiderato, inclusi bot, injection e denial of service (DoS) a livello di applicazione. WAF consentirà di definire e gestire le regole per evitare minacce a Internet, tra cui indirizzi IP, intestazioni HTTP, corpo HTTP, stringhe URI, scripting tra siti (XSS), inserimento SQL e altre vulnerabilità definite da OWASP. Il firewall dell'applicazione Web viene distribuito per proteggere le applicazioni Web e raccogliere i log di accesso per la conformità e l'analisi.
Per difendere l’applicativo Web da attacchi SQLi e XSS si consiglia di implementare le seguenti azioni:

1. Controllo dei dati di input in modo che tutti i dati che vengono inseriti dall’utente vengano controllati in modo che siano validi, filtrati e sanificati prima che possano essere inseriti in modo da evitare inserimenti di dati malevoli.
2. Usare un WAF cioè un Web Aplication Firewall per proteggere il sito di e-commerce.
3. Utilizzare i parametri preparati per la query di SQL invece che concatenare i valori direttamente nella query cosicché si possa prevenire gli attacchi di tipo SQLi.
4. 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 NUMERO 2

Gli utenti spendono in media 1500 euro al minuto e l’applicazione risulta irraggiungibile per 10 minuti , quindi applicando una semplice formula , ci risulta che l’azienda perda 15 mila euro.

Il 99,99% dei bersagli degli attacchi DDoS è composto da grandi aziende. I motivi per cui alcuni servizi web vengono presi di mira sono vari: ricatto, attivismo, concorrenza sleale… Fatto sta che gli attacchi DDoS sono quasi esclusivamente un problema delle grandi compagnie che prestano servizi o vendono prodotti online.

Queste aziende hanno diversi modi per proteggersi dagli attacchi DDoS, tra cui i principali sono:

- Firewall
- Rilevamento delle intrusioni: i sistemi IDS rilevano le connessioni anomale e avvisano il team di cybersicurezza
- 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.

Queste funzionalità sono molto utili, ma non consentono di risolvere completamente il problema: l’efficacia di un attacco DDoS può essere ridotta da queste misure di sicurezza, ma rimane direttamente proporzionale all’estensione della botnet utilizzata. Di conseguenza, l’unico modo per evitare questi attacchi sarebbe impedire la diffusione dei malware che creano le botnet.

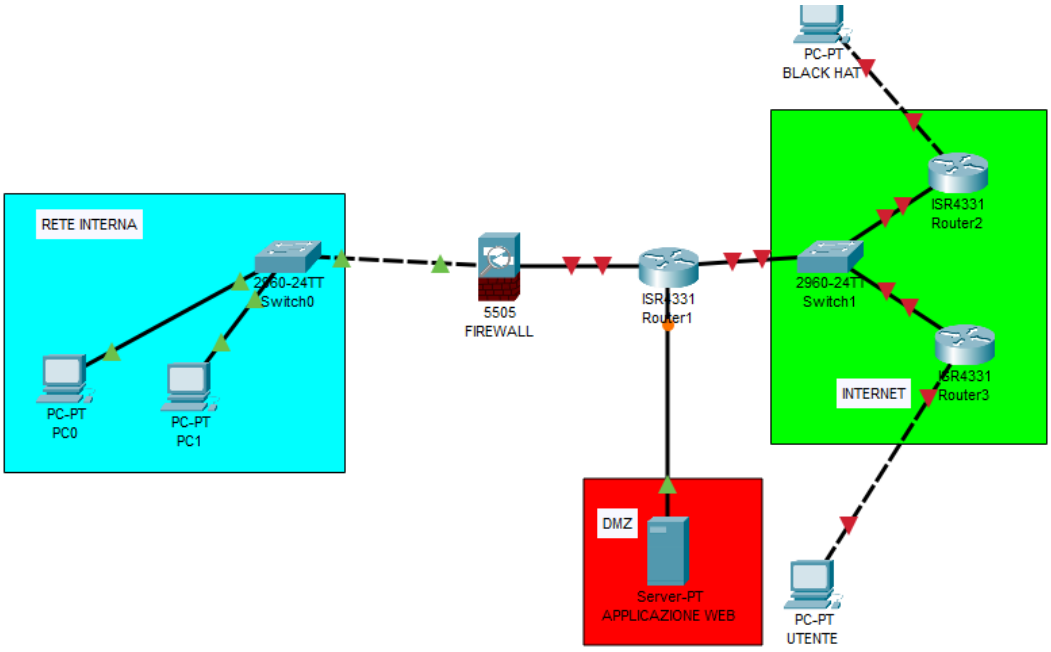
Come soluzione definitiva possiamo avere un server app di riserva da attivare nel caso in cui il nostro server principale vada in down.

TRACCIA NUMERO 3
Per evitare il propagarsi del malware sulla rete interna, abbiamo isolato l'applicazione fuori dal firewall, facendola passare prima dal router, abbiamo dovuto aprire la porta del router manualmente
L'Incident Response Plan è un processo strutturato e ripetibile utile alle organizzazioni a prevedere, prioritizzare e rispondere in maniera tempestiva ed efficace agli incidenti di cybersecurity grazie alla predisposizione di standard, policy, procedure e team adeguati.

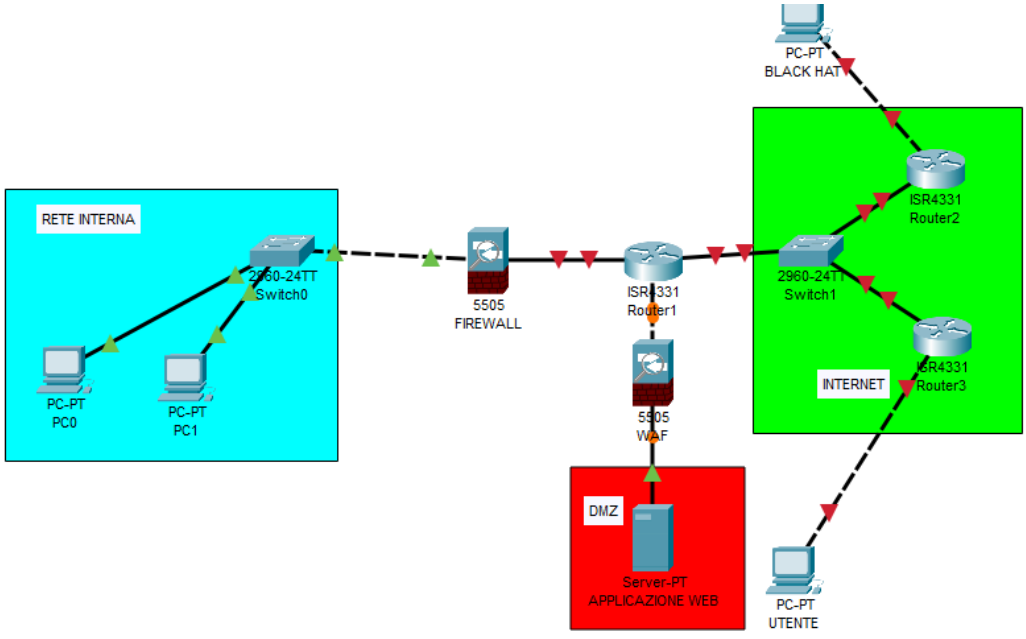
L'Incident Response è la capacità operativa dell'Incident Management di minimizzare l'impatto delle violazioni e ripristinare nel più breve tempo possibile le regolari operazioni.

L'IRP prevede diverse fasi che permettono di prevenire o ridurre i danni causati da un incidente di sicurezza informatica grazie ad una anticipata e programmata verifica della capacità dell'organizzazione a rispondere a problemi di sicurezza stabilendo la messa in atto di tool e know-how necessari a prevenire la violazione.

Possiamo procedere poi a rimuovere l'applicazione infetta utilizzando uno dei metodi tra cui clear purge o destroy

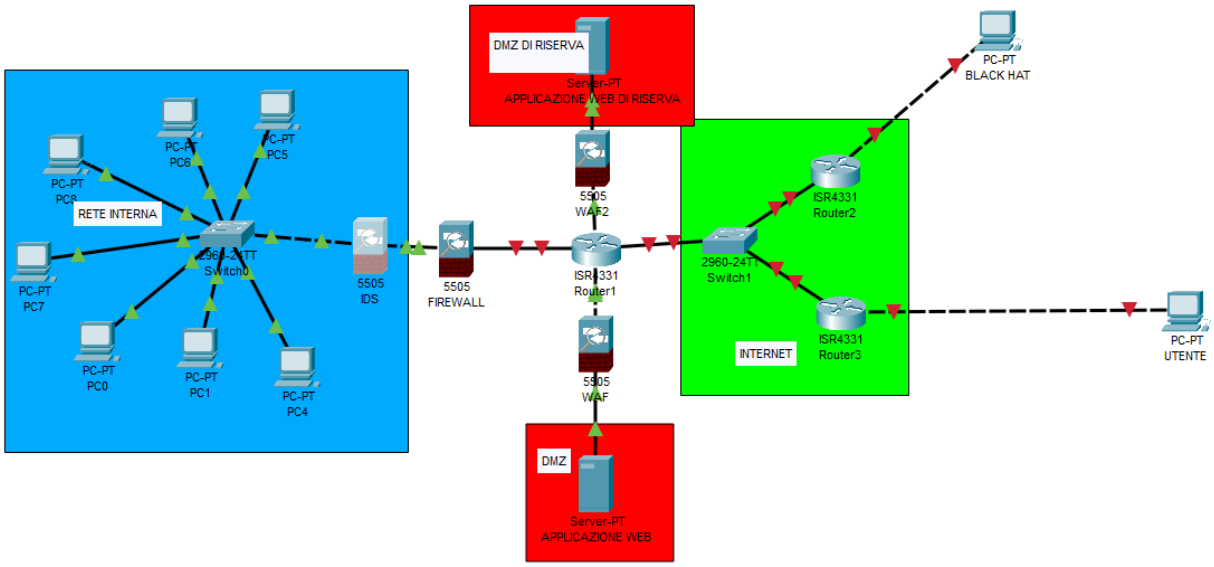


TRACCIA 4
Qui abbiamo unito le soluzioni 1 e 2 , mettendo sia il waf che isolando l'applicazione web fuori



TRACCIA NUMERO 5

PER FARE UNA RETE PIU' AVANZATA, ABBIAMO AGGIUNTO UN IPS TRA IL FIREWALL E LO SWITCH DELLA RETE INTERNA, PIU ABBIAMO AGGIUNTO UN SERVER DI RISERVA NEL CASO IN CUI IL PRIMO SERVER FOSSE ANDATO DOWN



I sistemi di Intrusion Detection System (IDS) sono sicuramente tra gli strumenti di sicurezza informatica più utilizzati e apprezzati per proteggere i perimetri cyber delle aziende. Si tratta di strumenti atti ad eseguire un monitoraggio continuo della sicurezza, allo scopo di identificare – in anticipo – tutti gli attacchi alle reti informatiche e ai computer.

Un sistema di rilevamento delle intrusioni basato sulla rete (NIDS) **viene utilizzato per monitorare e analizzare il traffico di rete per proteggere un sistema dalle minacce basate sulla rete**.