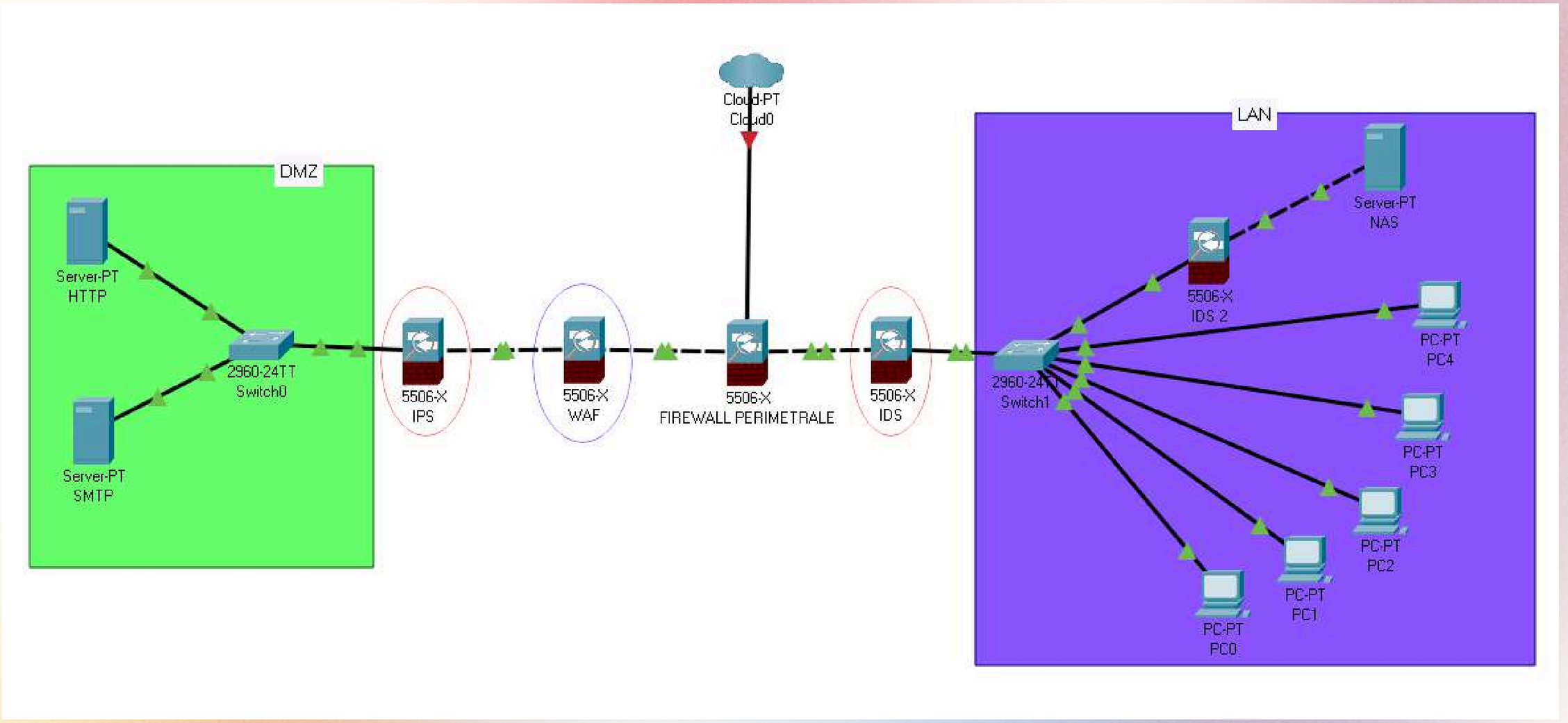
AMATO SARA
CYBER SECURITY SPECIALIST - EPICODE
18/10/2024

SEGMENTAZIONE DI UNA RETE

AMATO SARA
CYBER SECURITY SPECIALIST - EPICODE
18/10/2024



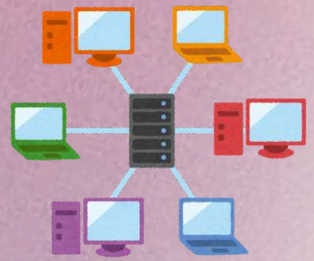
AMATO SARA
CYBER SECURITY SPECIALIST - EPICODE
18/10/2024

In questo progetto, viene rappresentata una rete segmentata che include una zona DMZ, un firewall perimetrale, un sistema di prevenzione delle intrusioni (IPS), un sistema di rilevamento delle intrusioni (IDS) e un Web Application Firewall (WAF). L'obiettivo è quello di garantire un'architettura di rete sicura ed efficace.

La rete è suddivisa in tre zone principali:

Internet: rappresentata da un cloud, è la zona esterna alla rete, dove si trovano gli utenti e i servizi accessibili pubblicamente.

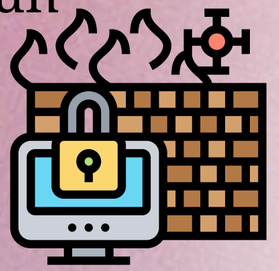
DMZ (Demilitarized Zone): contiene i server web (HTTP) e di posta elettronica (SMTP), accessibili dall'esterno per fornire servizi agli utenti.



Rete Interna: comprende i PC e il NAS (Network Attached Storage) che forniscono servizi interni.

AMATO SARA
CYBER SECURITY SPECIALIST - EPICODE
18/10/2024

- Il **firewall**, che possiamo definire il cuore di questa segmentazione di rete, è uno dei componenti fondamentali nella sicurezza informatica. Si tratta di un dispositivo o di un software progettato per proteggere una rete informatica o un sistema da minacce esterne, regolando il traffico di rete in entrata e in uscita.



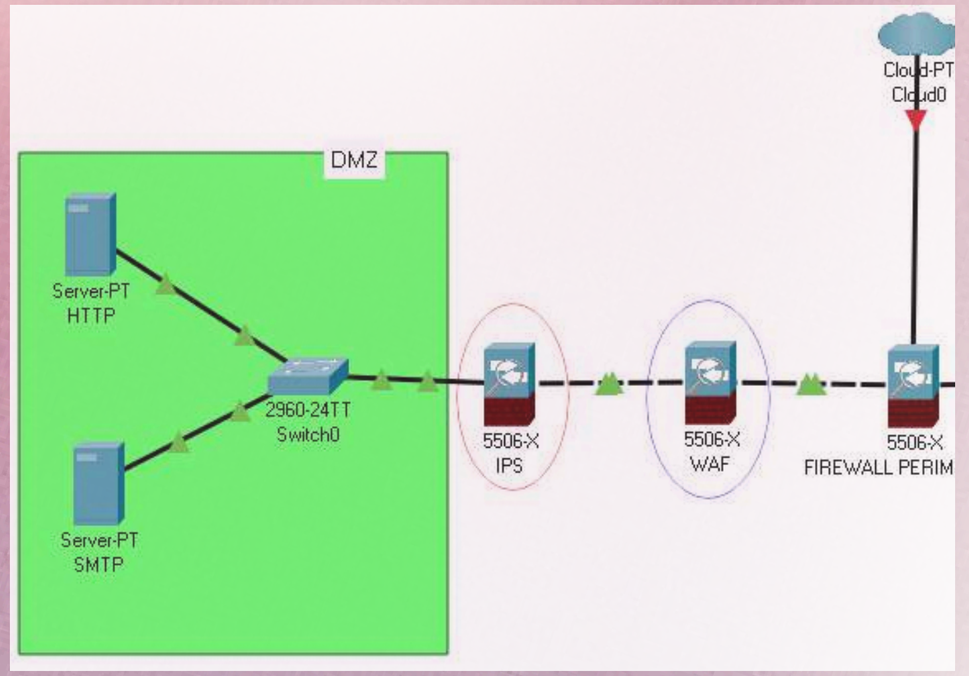
- Il **WAF**, Web Application Firewall, è specializzato nella protezione delle applicazioni web, bloccando attacchi e altre minacce specifiche per le applicazioni web, monitorando e filtrando il traffico HTTP/HTTPS tra l'applicazione web e l'utente finale.
- L'**IPS,** Intrusion Prevention System, monitora il traffico di rete in tempo reale e agisce per bloccare attività sospette o malevoli. È progettato per prevenire attacchi prima che possano causare danni.

AMATO SARA
CYBER SECURITY SPECIALIST - EPICODE
18/10/2024

- La **DMZ**, Demilitarized Zone, è una rete a sicurezza intermedia progettata per ospitare risorse pubbliche, come server web e di posta, che devono essere accessibili sia dall'esterno che dall'interno della rete.
- Il server **HTTP** è responsabile di ospitare siti web e applicazioni web accessibili dagli utenti esterni.
- Il server **SMTP** gestisce l'invio e la ricezione di e-mail. È progettato per essere accessibile sia da utenti esterni che interni.
- L'**IDS**, Intrusion Detection System, monitora il traffico di rete alla ricerca di attività sospette e invia avvisi agli amministratori di rete. Non blocca direttamente il traffico, ma permette di rilevare le intrusioni.
- Il **NAS**, Network-Attached Storage, è un dispositivo di archiviazione che consente l'accesso centralizzato ai file e ai dati da parte degli utenti interni alla rete.

AMATO SARA
CYBER SECURITY SPECIALIST - EPICODE
18/10/2024

Per la creazione di questa rete segmentata, ho iniziato collegando il firewall alle diverse zone della rete: il cloud (che rappresenta Internet), la DMZ (zona demilitarizzata) e la rete interna (LAN). Questo firewall perimetrale funge da prima linea di difesa, regolando l'accesso e proteggendo la rete interna da possibili minacce esterne.
Nella parte sinistra della rete, subito dopo il firewall, è stato posizionato il WAF (Web Application Firewall). Il suo compito è intercettare e analizzare il traffico web per rilevare eventuali attacchi mirati alle applicazioni web, come attacchi SQL injection o cross-site scripting, prima che possano compromettere i server HTTP e SMTP situati nella DMZ. Il WAF agisce come un filtro specializzato che protegge i server dalle vulnerabilità specifiche delle applicazioni web.
Dopo il WAF, ho collocato l'IPS (Intrusion Prevention System), strategicamente posizionato per aumentare ulteriormente la sicurezza della rete. L'IPS monitora il traffico alla ricerca di comportamenti sospetti o anomali e agisce immediatamente per bloccare qualsiasi minaccia rilevata. Questo componente è fondamentale per identificare e prevenire attacchi più generici e sofisticati che potrebbero eludere il WAF.
L'IPS è quindi collegato alla DMZ, una zona di sicurezza separata che ospita i server accessibili dall'esterno, come il server web (HTTP) e il server di posta elettronica (SMTP). La DMZ è progettata per isolare questi server dal resto della rete interna, in modo che, in caso di compromissione, l'attaccante non possa accedere direttamente ai dati sensibili o ai dispositivi della LAN.



AMATO SARA
CYBER SECURITY SPECIALIST - EPICODE
18/10/2024

Analizzando la parte destra della rete, possiamo osservare che il firewall è collegato direttamente a un IDS (Intrusion Detection System). L'IDS svolge un ruolo fondamentale nel rilevare attività sospette o comportamenti anomali nella rete e invia avvisi di allerta in caso di potenziali minacce. La sua posizione strategica, subito dopo il firewall, consente di monitorare attentamente tutto il traffico che entra nella rete interna (LAN), riducendo il rischio di eventuali intrusioni che possano compromettere i dati sensibili e le risorse cruciali presenti in questa parte della rete.
Proseguendo con l'analisi della rete interna, si nota il collegamento tra gli host e uno switch, che funge da punto centrale per la connessione di tutti i dispositivi della LAN, facilitando la comunicazione interna. In aggiunta, è stato inserito un ulteriore IDS posizionato direttamente davanti al NAS (Network Attached Storage), un dispositivo di archiviazione progettato per centralizzare e proteggere i dati aziendali. Questo secondo IDS offre un ulteriore livello di sicurezza, monitorando specificamente l'accesso ai dati memorizzati e proteggendo il NAS da possibili intrusioni o attività sospette che potrebbero compromettere le informazioni archiviate.