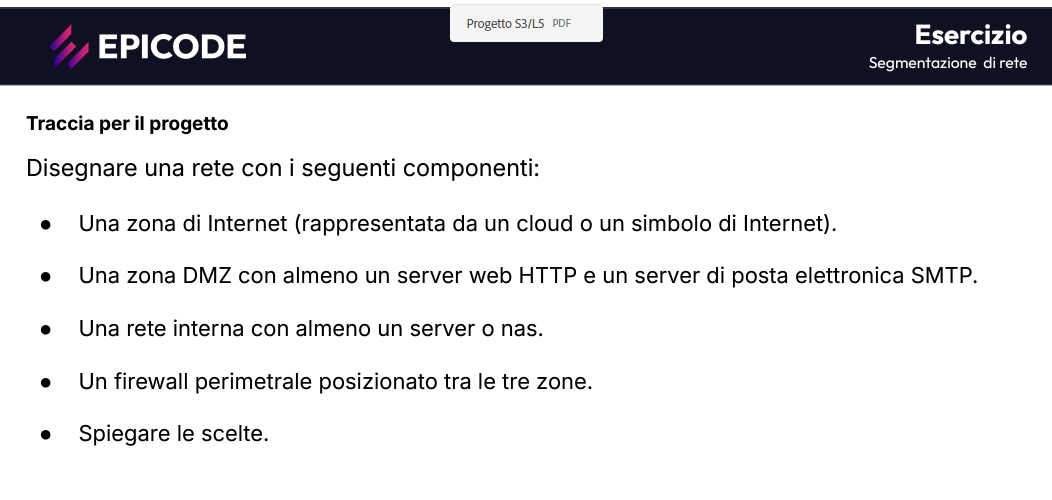
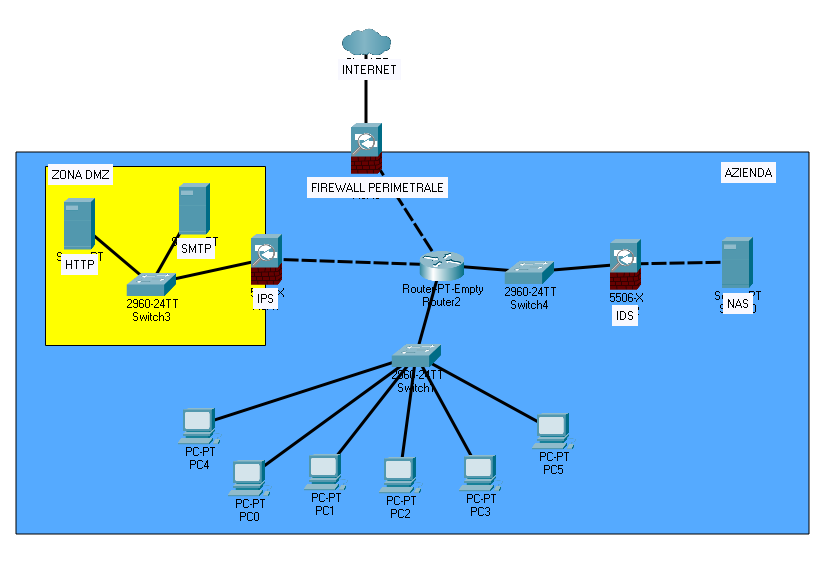
Progetto S3L5 Luca Calvigioni



Disegno il progetto di rete in base alla traccia del progetto:



Spiegazione:

La nuvola rappresenta Internet ovvero l’area WAN, utilizziamo un firewall perimetrale in modo che una parte si occupi della WAN e l’altra della LAN

Il firewall in questione è a livello hardware, questo può agire anche da router gateway ma molto più performante a livello hardware perchè il suo compito è di gestire migliaia di connessione, ispeziona i pacchetti contemporaneamente.

Il Firewall è dotato di diversi tipi di filtraggio quello più utilizzato oggi è il filtraggio dinamico che permette le connessioni che vanno dall’interno verso l’esterno ma non viceversa.

Grazie alla tabella acl di cui è dotato il firewall legge gli indirizzi ip e in base al tipo di IP pubblico / privato saprà se un ip proviene dall’esterno (IP pubblico) o dall’interno (IP privato) tutti gli indirizzi ip della tabella acl vengono salvati nella memoria cache (memoria volatile) del firewall.

La zona DMZ (demilitarizzata) è la zona scoperta del firewall, dove metto tutti i servizi che voglio siano raggiunti da tutto il mondo, come richiesto, dalla traccia ho messo il server SMTP (email) e HTTP (pagina web) anche perchè senno non esisterebbe comunicazione con nessuno senza DMZ perchè il firewall bloccherebbe tutte le comunicazioni che vengono dall’esterno.

Anche se i server si trovano nella zona DMZ sono comunque protetti dal firewall attraverso il filtraggio per contenuto (WAF) il compito del WAF legge il codice del pacchetto in entrata e determina, se un pacchetto è malevolo lo distruggerà, altrimenti lo lascerà passare facendo un confronto con una sua tabella interna usata come dizionario dei malware o siti esterni come OWASP, quest’ultimo più sicuro perchè sempre aggiornato.

I sistemi di sicurezza informatica IPS e IDS rispettivamente:

* IDS = Intrusion Detection System con l’arrivo di un pacchetto in entrata una volta esaminato lo confronta con le sue regole, scritte da noi e se risultasse malevolo manderà un alert e sarà gestita in maniera manuale.
* IPS = Intrusion Prevention System funziona come l’IDS ma questo oltre a dare l’alert, bloccherà il pacchetto.

Il sistema IPS soffre di falsi positivi ovvero che anche file non malevoli vengono classificati come tali, se all’interno di una LAN avessi un IPS prima di un NAS e mi rilevasse come un falso positivo, io dipendente di un’azienda non ho possibilità di accedere al NAS quindi non avrei possibilità di accedere ai file dell’azienda e non avrei modo di poter lavorare.

Per questo come possiamo vedere dal disegno in alto prima del NAS posizionerò un IDS che comunque rende sicuro l’accesso al NAS e in caso di problemi invierà soltanto un alert ma avrò comunque l’accesso, l’IPS invece lo posiziono sul lato web, dato che è la parte meno sicura perchè tutti possono accedere ai server e gestirà tutto in maniera automatica.