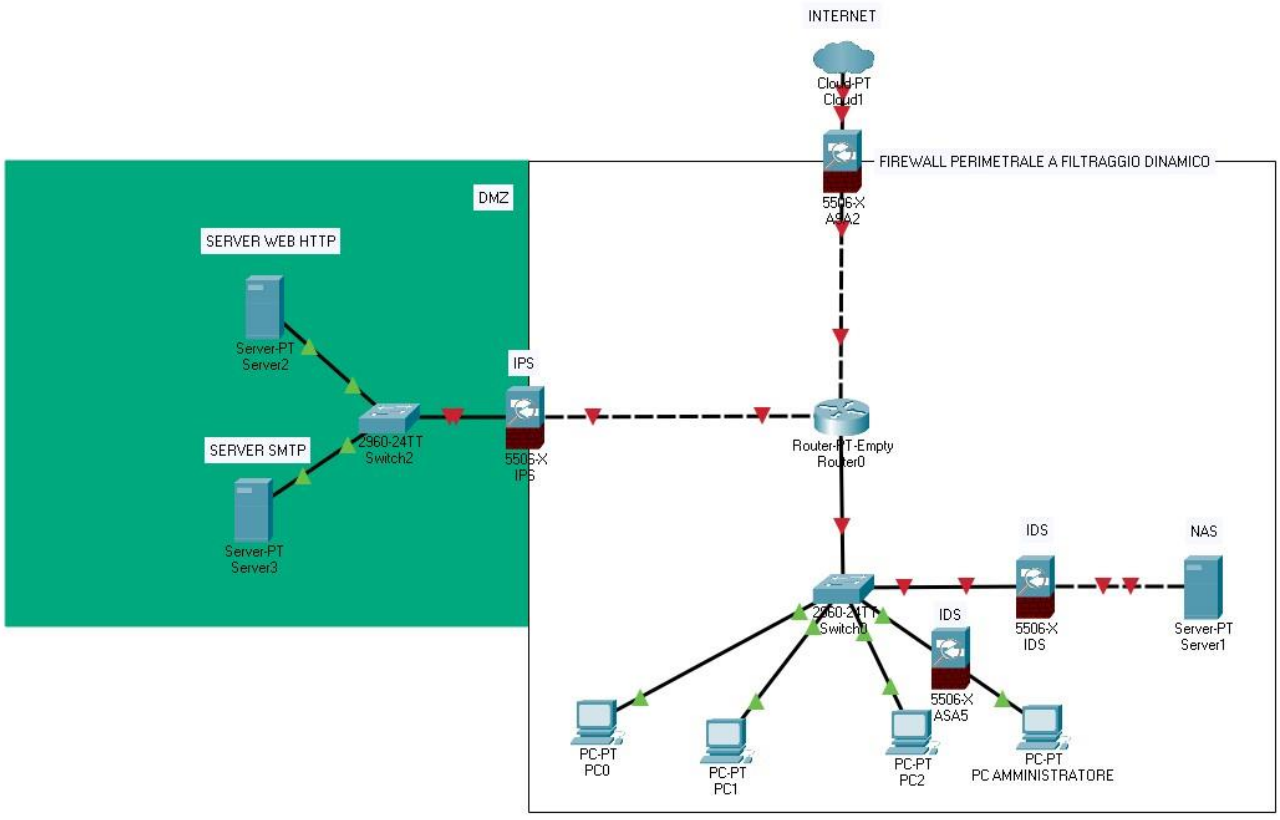
Esercizio S3 L5 ***Daniele Paolone***

Disegnare una rete con i seguenti componenti:

- Una zona di Internet (rappresentata da un cloud o un simbolo di Internet).
- Una zona DMZ con almeno un server web HTTP e un server di posta elettronica SMTP.
- Una rete interna con almeno un server o nas.
- Un firewall perimetrale posizionato tra le tre zone.
- Inserire IDS/IPS.
- Spiegare le scelte.

Di seguito vi è una rappresentazione della rete con i componenti richiesti dall' esercizio:



La rete aziendale è composta da rete interna e DMZ. Nella rete interna si trovano:

- 4 host (di cui una macchina con diritti amministratore)
- Un NAS

Nella DMZ si trovano due server:

- Il server web dove è hostato il sito aziendale
- Il server per ricevere le email dall' esterno

Per quanto riguarda la rete interna, essa è protetta, a livello perimetrale, da un firewall a filtraggio dinamico che si trova tra la WAN e il router-gateway. Il firewall monitora le attività, il traffico di rete, sia in uscita che in entrata, e rileva se ci sono intrusioni. Come in questo caso, è posizionato all' ingresso di una rete ed è capace di filtrare il traffico per bloccare pacchetti malevoli in entrata. Nello specifico, nell' esercizio viene impiegato un firewall con filtraggio stateful (dinamico), cioè un filtraggio che blocca tutte le connessioni che hanno origine dall' esterno. Sono permesse solo le connessioni create da un host interno verso l'esterno e mai il contrario. Per via di questa peculiarità, è in grado di riconoscere le connessioni già stabilite e di consentire automaticamente il traffico associato a quelle connessione.
Addentrandoci nella rete interna, troviamo un altro dispositivo di sicurezza: l'IDS. Qui ne sono stati impiegati due e sono stati messi a protezione, uno del NAS e l'altro della macchina con diritti di amministratore. Questo perché i due dispositivi sono molto importanti. Il NAS è un dispositivo che può ospitare diverse unità di memoria per conservare e condividere i dati in una rete dove sono collegati più macchine che possono accedervi. Ovviamente questo dispositivo in un'azienda conserverà vari tipi di dati, vitali per l'azienda stessa, dai meno confidenziali ai più confidenziali e con accessi a diversi livelli di autorizzazione.
La macchina con diritti di amministratore, oltre ad avere accesso completo al contenuto del NAS, ha anche accesso a tutti i dispositivi di rete, monitora la rete e gli altri host. In aziende grandi queste funzioni possono essere divise in più macchine, ad esempio, macchina che monitora la rete dove ha accesso l'IT manager; e la macchina con accesso a tutte le informazioni conservate nel NAS dove ha accesso l'amministratore dell'azienda.
Come specificato, data l'importanza di questi due dispositivi, a loro protezione vengono messi gli IDS. L' IDS (Intrusion Detection system) è un filtro in grado di monitorare il traffico e rilevare le intrusioni. La sua funzione è quella di notificare se un pacchetto malevolo è entrato nella rete, in questo caso nel NAS o nella macchina con diritti di amministratore. L' IDS però svolge solo la funzione di notifica non blocca la connessione come il firewall. Per questo motivo non è posizionato a livello perimetrale, ma bensì in prossimità punti strategici della rete.

Quanto enunciato finora riguardava la rete interna, ora si vedrà l'altra parte della rete, la DMZ. Essa (abbreviazione di zona demilitarizzata) è una sezione della rete non protetta da firewall, dove vengono posizionati i server pubblici, accessibili dall' esterno, cioè tramite internet.
I server posizionati in questa zona sono:

- Il server web del sito aziendale che utilizza porta HTTP 80 e porta HTTPS 443
- Il server per ricevere email dai clienti e fornitori che utilizza porta SMPT 25

Grazie a questa sezione di rete così strutturata, l'azienda può fornire servizi all' esterno attraverso il suo sito web e rimanere in contatto tramite la ricezione di email. Ma per far si che non vengano messi a rischio da traffico non attendibile i gli host e i server all' interno della LAN, viene impiegato un IPS tra la DMZ e il router-gateway.
L' IPS (Intrusion Detection System), svolge la stessa funzione dell'IDS, cioè notificare intrusioni dall' esterno di pacchetti malevoli, ma in aggiunta, ha un'altra funzione: queste intrusioni vengono bloccate. Infatti l'IPS è in grado a bloccare il traffico in entrata (dalla DMZ in questo caso) se considerato dannoso.