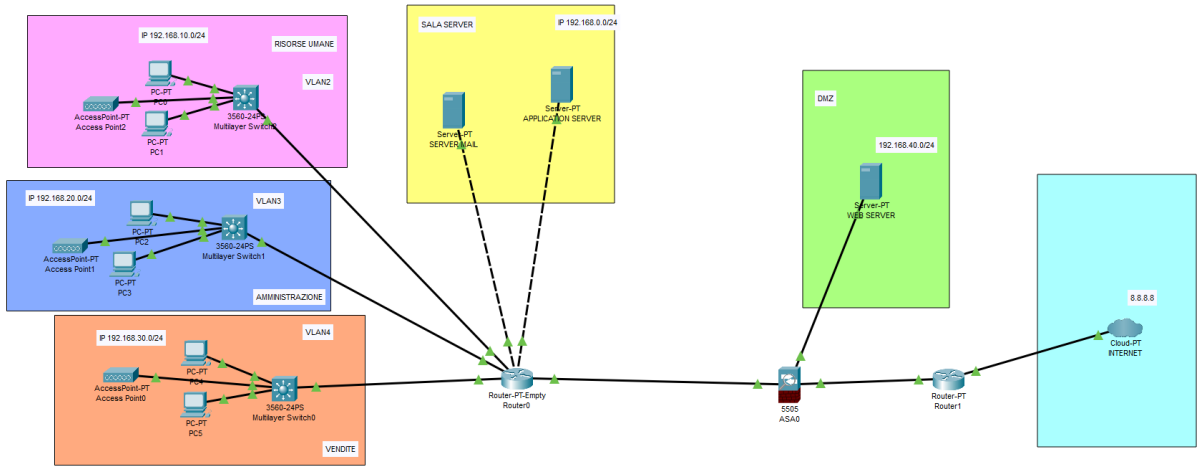
THETA NETWORK PROJECT



RETE	VLAN	IP	DEFAULT GATEWAY
Risorse umane	10	192.168.10.0	192.168.10.1
Amministrazione	20	192.168.20.0	192.168.20.1
Vendite	30	192.168.30.0	192.168.30.1
Sala Server	...	192.168.0.0	192.168.0.1
DMZ	...	192.168.40.0	192.168.40.1

Nel progetto di rete per la compagnia Theta ogni dipartimento ha una Vlan dedicata, ogni rete consente il collegamento di vari dispostivi (pc, serve, stampanti ed altro), ed ogni dispositivo viene dotato di indirizzo statico; inoltre ho aggiunto degli access-point per consentire l'accesso a wifi protetto da password.

La DMZ è l'area di rete tra la rete interna e la rete esterna(internet). Il traffico in questa zona è meno controllato rispetto alla zona di rete interna, ed è infatti un'area usata per inserire i vari server che devono essere accessibili dagli utenti esterni. Nel nostro progetto di rete all'interno della DMZ troviamo il Web server della compagnia Theta che espone vari servizi.

Per creare la nostra DMZ useremo il firewall fornito da CISCO che lavora con le Vlan, ne ha due di default: *inside* e *outside*. *Inside* sarà la nostra rete interna, e outside rappresenterà internet. La Vlan inside, la nostra rete interna avrà livello di sicurezza 100, in quanto a questa rete non devono poter accedere host esterni.
La vlan outside, idealmente considerato internet, ha livello di sicurezza pari a 0, non è di nostra competenza essendo area esterna all'azienda. La DMZ deve essere configurata in modo che non possa comunicare con la rete interna, per questo sul firewall imposteremo #no forward interface vlan *inside* (la nostra rete interna). Andrebbero anche configurati gli ACL per poter regolare il traffico in entrata ed in uscita.
In questo modo il server DMZ può raggiungere l'esterno, mentre la rete esterna non può raggiungere il server interno.

Il firewall perimetrale quindi ci permette di mitigare e regolamentare il traffico da e verso internet; è il nostro primo livello di protezione.

Nella rete interna di Theta troviamo la Sala server in cui possiamo vedere l'Application server che espone sulla rete aziendale interna un applicativo e-commerce accessibile solo dagli impiegati della compagnia, dunque non accessibile da utenti esterni.

Il firewall perimetrale quindi andrebbe posizionato tra la rete interna e la rete esterna perché appunto serve a proteggere la rete interna dalle eventuali minacce provenienti dall'esterno/internet, per questo è anche importante che non comunichi direttamente con la DMZ. Con il filtraggio statico il firewall viene configurato proprio per consentire la ricezione o meno di un pacchetto andando a verificare se l'indirizzo IP di origine e destinazione è consentito, se la porta di destinazione è autorizzata e se il protocollo usato è permesso. Nella DMZ vogliamo in questo caso consentire l'accesso alla porta 80 (HTTP) per la trasmissione di pagine web su internet.