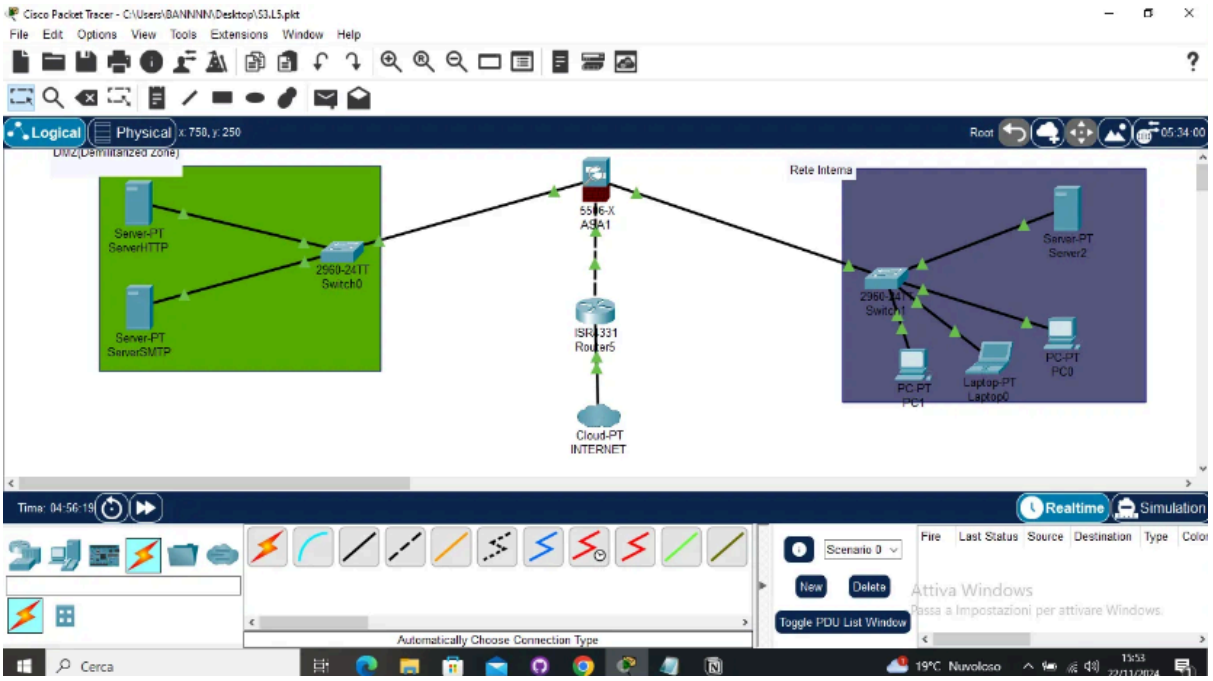

Questa rete è strutturata seguendo un concetto di segmentazione, ossia un concetto di separazione logica delle reti, che ha come obbiettivo quello di aumentare la sicurezza e migliorarne la gestione.

Applicando il concetto di segmentazione, una rete verrà frammentata in base ad aree della rete che necessitano di misure di sicurezza aggiuntive e altre aree della stessa rete che non necessitano di misure di sicurezza elevate, questa tecnica aiuta a limitare l'accesso e minimizzare il rischio di diffusione di attacchi o problemi da una zona all'altra. Tuttavia non implementando misure di sicurezza come firewall o dispositivi che filtrano il traffico, questa segmentazione da sola non offre una protezione effettiva.

Per applicare il metodo di segmentazione della rete su questo caso, la rete è stata suddivisa in 3 parti, una parte dedicata all'accesso ad internet, quest'area è isolata da tutto il resto poichè un accesso da internet direttamente alla rete aziendale potrebbe causare grossi problemi per quanto riguarda sviluppo di attacchi via web alla rete aziendale. La seconda area della segmentazione è la DMZ(Demilitarized Zone) è una parte della rete aziendale dedicata a servizi che offre un'azienda su internet, in questa zona si collocano solo ed esclusivamente server che devono essere accessibili da internet per poter offrire servizi come ad esempio un sito web o un servizio di posta elettronica. Nella DMZ per proteggere la rete interna si espongono solo i servizi strettamente necessari, isolando i server che forniscono i servizi, questo aumenta notevolmente le possibilità di non compromettere la rete aziendale se un server pubblico viene compromesso. Il traffico all'interno della DMZ è limitato dal firewall, prevenendo movimenti laterali in caso uno di questi server venga compromesso.

Infine la terza area è la rete interna dell'azienda, la quale ospita risorse critiche per l'azienda come server di backup serve NAS e altre applicazioni aziendali o dati sensibili. I dispositivi interni devono essere protetti in modo stretto per evitare che attacchi provenienti dall'esterno

(attraverso internet o dalla DMZ) possano comprometterli. Solo i dipendenti autorizzati e i servizi interni devono poter accedere a queste risorse, solitamente questi dispositivi sono separati sia fisicamente sia virtualmente da internet e dalla DMZ.

Come già detto in precedenza però questa tecnica di segmentazione non ha valore se non si utilizzano Firewall per impostare regole e filtri per l'instradamento del traffico e per poter isolare le reti. Il Firewall è cruciale per impedire attacchi diretti verso la rete interna e per poter applicare le politiche di accesso restrittive, filtri su come il traffico deve essere instradato e l'isolamento delle varie aree di una rete.

Un 'ulteriore misura di sicurezza potrebbe essere quella di frammentare la rete attraverso le VLAN, implementando ulteriormente l'isolamento delle reti e migliorando anche la gestione della rete, poichè la segmentazione è un concetto teorico che senza nessun tipo di firewall o altre misure di sicurezza rimane solo una misura di sicurezza a livello concettuale, mentre le VLAN sono delle segmentazioni della rete vera e propria implementate attraverso gli switch, che separano sia fisicamente che logicamente i dispositivi in diverse sotto reti. In questa maniera nel caso ci fosse un malfunzionamento del nostro Firewall, comunque la nostra rete rimarrebbe segmentata e isolata in parte.