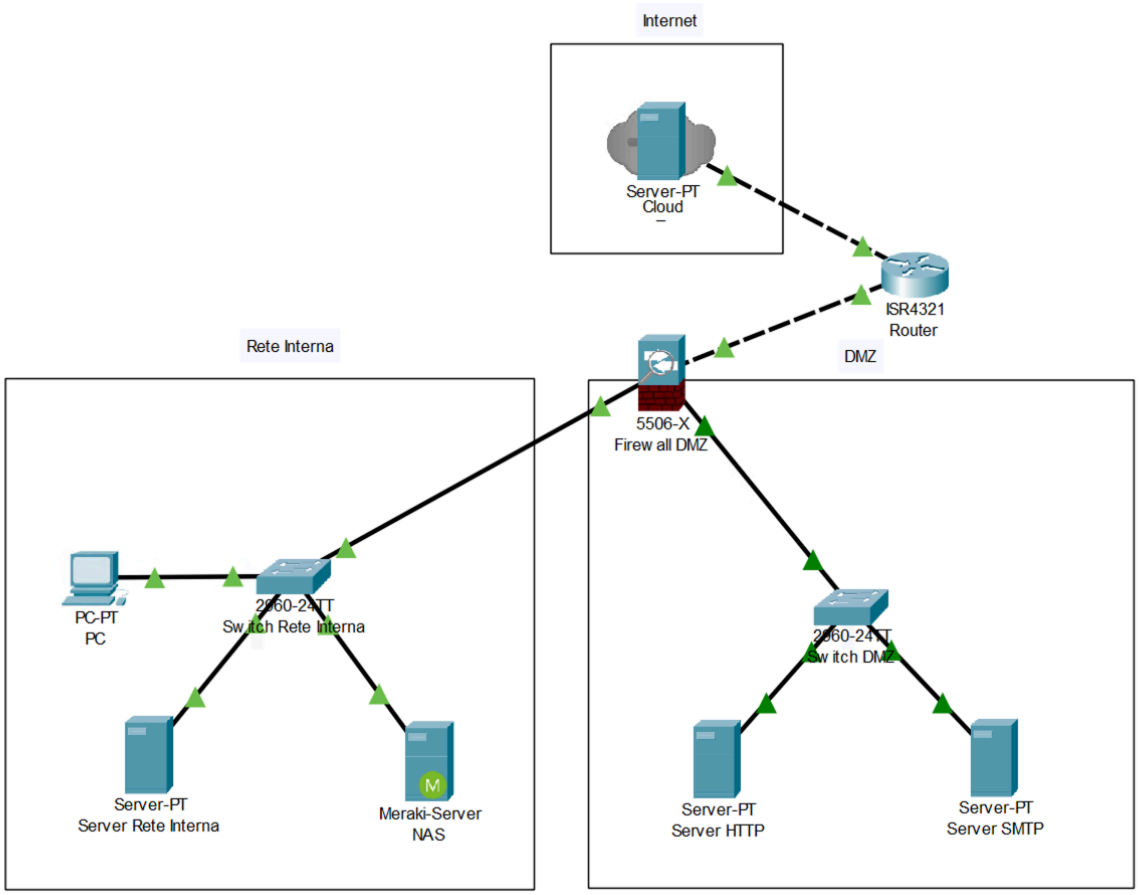
EPICODE-CS0124
S2/L1 - Pratica

Flaviano Sedici

Compito

- 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.
- Spiegare le scelte

Architettura selezionata:



Nell'architettura selezionata si è scelto di inserire, al fine di non eccedere con complessità e costi, **un router e un firewall**.

Router in Entrata

Il router è stato configurato, per le comunicazioni in ingresso provenienti da Internet, con un protocollo di **NAT (Network address translation)** in modo che sia possibile, tramite un IP pubblico, raggiungere gli IP della rete interna assegnati ai server HTTP e SMTP che risiedono nella DMZ.

Quindi ad esempio nel caso si tenti di accedere al servizio HTTP l'instradamento avverrà sull'IP di rete DMZ del server HTTP, in alternativa se si volesse accedere ai servizi SMTP, l'instradamento avverrà verso l'IP del server SMTP. Per tutte le altre comunicazioni verranno instradate secondo quanto descritto di seguito.

Router in Uscita

Per le comunicazioni in uscita, ossia provenienti dalla rete interna e dirette verso l'esterno, il router non devia o blocca alcun passaggio di dati, instradandoli verso Internet per entrambe le reti.

Firewall Policy in Entrata (IP Provenienza, IP Destinazione, Porta, Action)

Il firewall è stato configurato per le comunicazioni in ingresso (provenienti da Internet) in modo da accettare solamente le comunicazioni instradate dal router verso gli IP dei server SMTP e HTTP (DMZ).

Tutti gli altri instradamenti o le richieste di comunicare con IP della rete Interna, saranno configurati sul firewall in modo che il firewall le scarti (DROP).

Si è pensato alla configurazione **DROP al posto del DENY** per dare meno informazioni possibili ad eventuali attaccanti sulla natura della eventuale mancata comunicazione.

Le uniche porte che saranno aperte per la DMZ saranno la **80 (HTTP) e le 25, 110, 143 per consentire di far offrire il servizio di SMTP, POP3 e IMAP** al server di posta elettronica.

Non sono state incluse le porte per i servizi che richiedono SSL in quanto nell'assegnazione del compito non sono previsti (HTTP e SMTP e non HTTPS e SMTPS).

Firewall Policy in Uscita (IP Provenienza, IP Destinazione, Porta, Action)

Per le comunicazioni in uscita (verso internet) il firewall è stato impostato in modo da consentire la comunicazione della DMZ solamente sulle suddette porte.

La rete interna potrà accedere ad Internet sulle principali porte standard (posta, internet, etc.) dedicate ai servizi utili in azienda o che l'azienda stessa ritiene opportuni.

Per le comunicazioni in uscita dalla rete interna sarà applicato anche un **Filtraggio di Stato** (Stateful filtering) in modo da consentire le comunicazioni in entrata solo se espressamente richiesto dagli host della rete interna magari tramite delle sessioni three-way handshake (altrimenti avendo bloccato le comunicazioni in entrata si verrebbe a creare il caso in cui un host interno effettua una richiesta ad un server su internet senza poter riceve risposta).

Per le comunicazioni interne, ossia tra la rete interna e la DMZ, il firewall sarà configurato con una tabella di DENY in modo da impedire le comunicazioni tra le due reti e nello stesso tempo offrire agli utenti finali un messaggio di errore per evitare di reiterare la richiesta di accesso diretto.

Ovviamente gli utenti della rete interna, pur non potendo accedere direttamente ai server nella DMZ, possono accedere ai loro servizi esposti tramite la rete Internet.

Suddivisione dei due segmenti aziendali

La suddivisione dei due segmenti, per una maggior sicurezza, può essere effettuata eventualmente tramite la configurazione di due VLAN, ma nel caso specifico non si ritiene sia necessario utilizzando degli IP statici e configurando correttamente le Firewall Policies.

Rete Interna

Gli host nella rete interna avranno quindi accesso al server e al NAS nella loro stessa rete, ad Internet ma non accesso diretto alla DMZ. Saranno comunque isolati da contatti diretti provenienti da Internet.

DMZ

I server in questo segmento avranno accesso solo ad internet tramite le porte designate. L'accesso sarà di natura bidirezionale sulle suddette porte.