

## Obiettivi

1. Progettare una rete con diverse zone di rete, tra cui una DMZ e una rete interna.
2. Configurare un firewall perimetrale per controllare il traffico tra le zone di rete.
3. Assicurare l'accesso sicuro ai servizi esposti nella DMZ dall'esterno e dalla rete interna.

## Progettazione della Rete

La rete è stata progettata per includere diverse zone di rete:

- Una zona di Internet rappresentata da un'icona "Cloud".
- Una DMZ con almeno un server web (HTTP) e un server di posta elettronica (SMTP).
- Una rete interna con dispositivi finali come PC, NAS e Server.

## Configurazione del Firewall

1. Definizione delle Regole del Firewall: Sono state create le regole del firewall per controllare il flusso del traffico tra le diverse zone di rete. Le regole includono il permesso o il blocco del traffico in base al protocollo, alla porta e all'indirizzo IP di origine e destinazione.
2. Applicazione delle Regole: Le regole del firewall vengono applicate sul dispositivo che separa le diverse zone di rete, come un router o un firewall dedicato, per controllare il traffico in ingresso e in uscita.
3. Test e Verifica: Dopo la configurazione del firewall, vengono effettuati test per verificare che il traffico fosse controllato in modo appropriato e che l'accesso ai servizi esposti nella DMZ fosse sicuro e autorizzato.

## Conclusioni

La configurazione di un firewall è essenziale per garantire la sicurezza e il controllo del traffico nelle reti moderne. Utilizzando Packet Tracer, è stato possibile rappresentare modo efficace e realistico, fornendo una protezione dei servizi esposti nella DMZ e alla rete interna. La corretta definizione e applicazione delle regole del firewall permettono di controllare il flusso del traffico in modo appropriato, garantendo l'accesso sicuro ai servizi.

