

S3-E5

Progetto Disegno di rete



Overview

- Consegna
- Progetto rete
- LAN
- LAN-WAN
- Firewall
- WAN
- Considerazioni

02
03
04
05
06
08
09



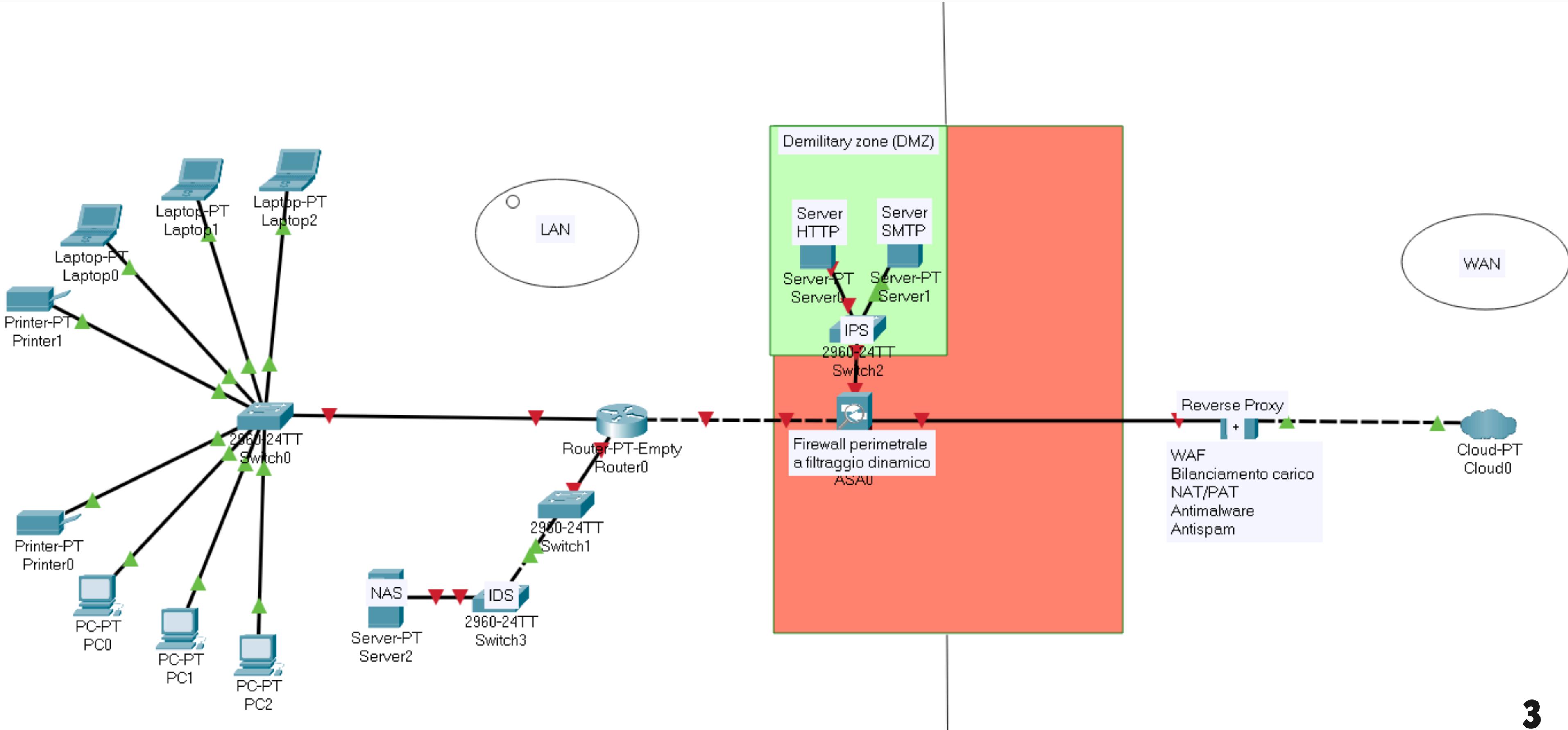
Consegna

Disegnare una rete con i seguenti componenti:

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



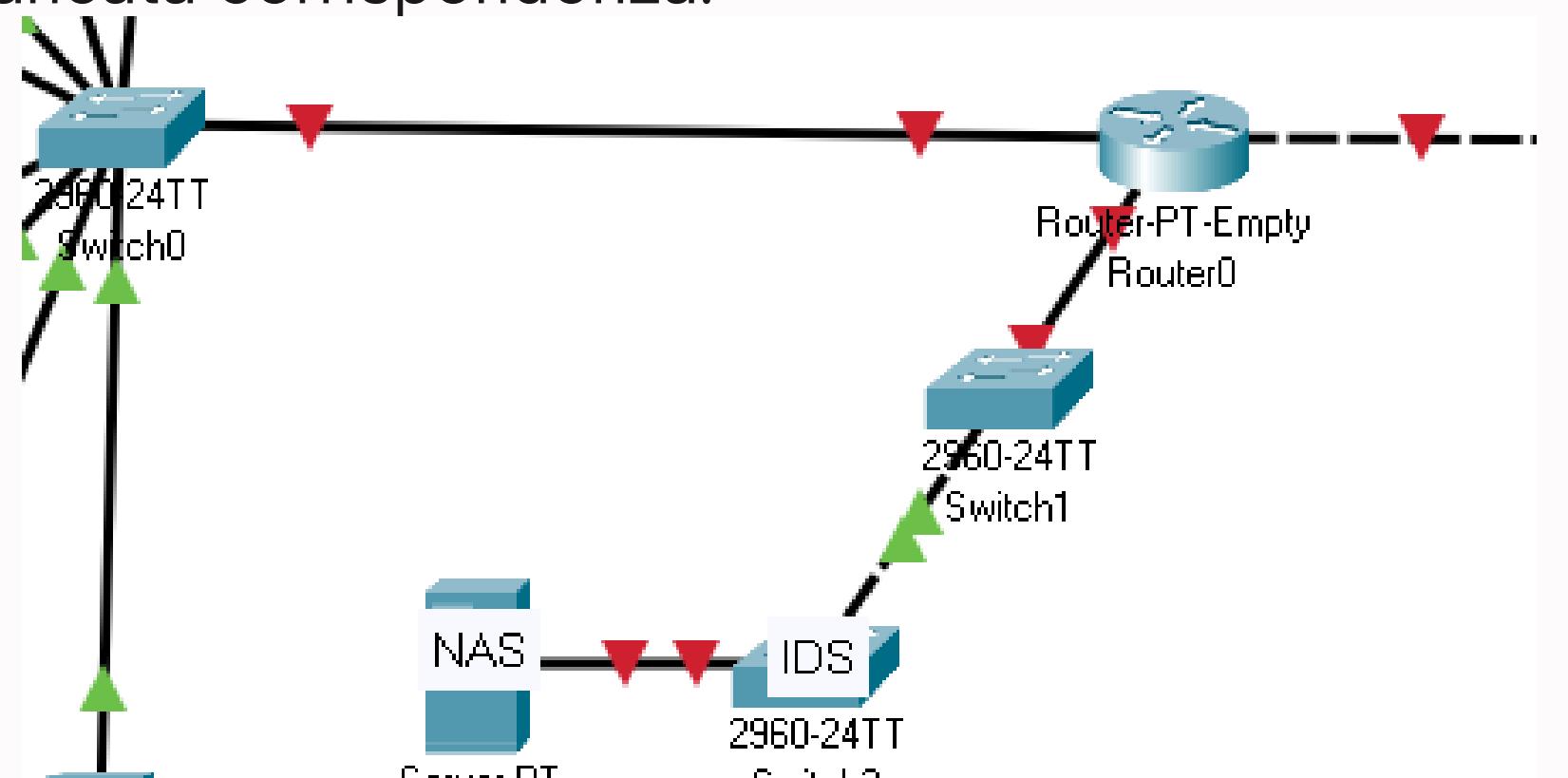
Progetto di Rete



LAN

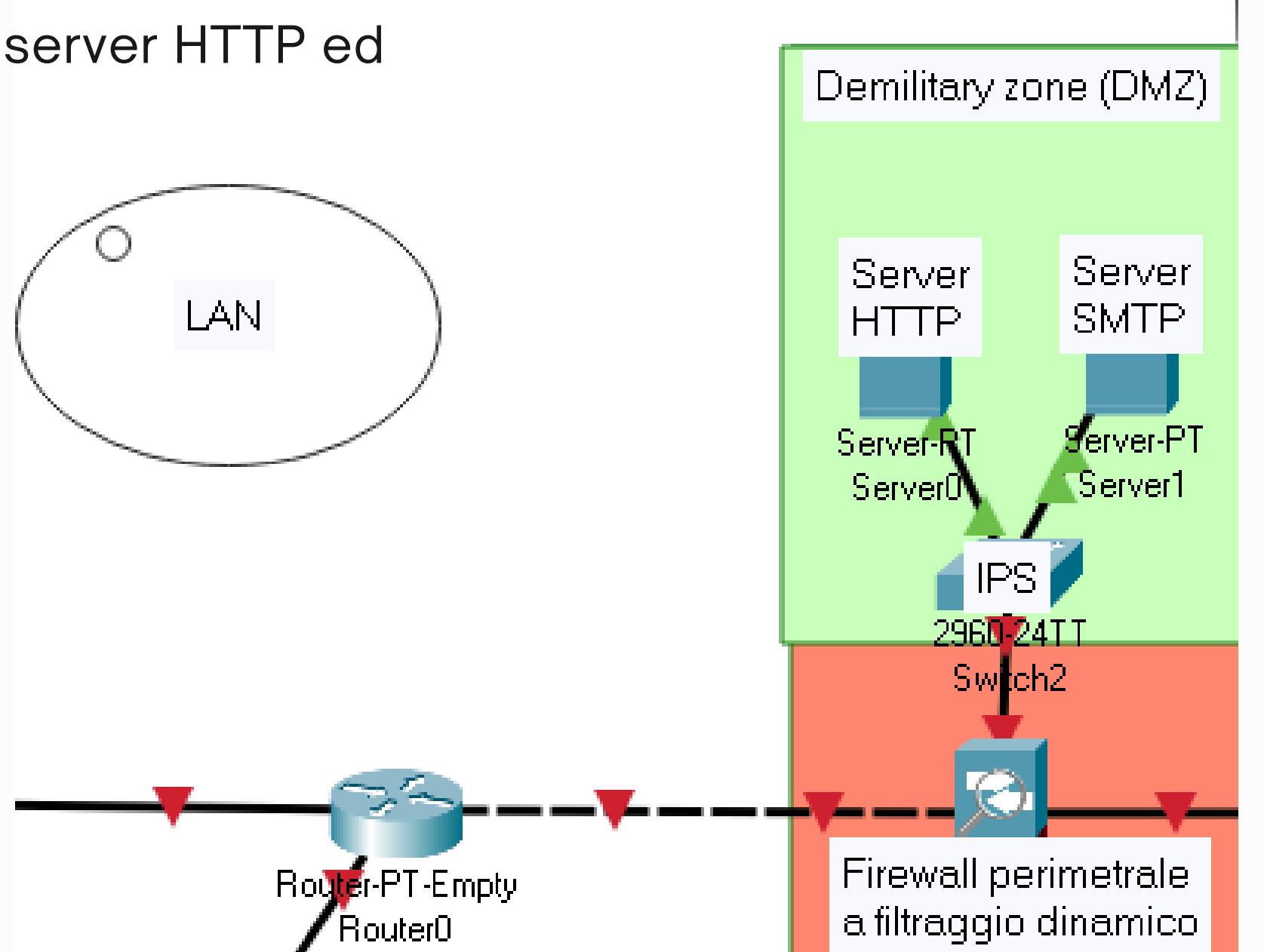
Per osservare al meglio questo progetto di rete è conveniente ripartire la rete, partendo dalla rete LAN: notiamo una classica rete composta da un singolo router gateway che metterà in comunicazione due bretelle, quella superiore che andrà ad allacciarsi ad uno switch collegato a 8 Host. Nel braccio inferiore invece il percorso prevede l'arrivo iniziale ad uno Switch, passando successivamente per un dispositivo, nella quale troviamo un IDS, per giungere infine ad un NAS.

L'**IDS** - (Intrusion detection system) è un software la cui funzione è quella di spacchettare i dati, confrontare i dati con una tabella, ed eventualmente inviare un allert in caso di mancata corrispondenza.



LAN-WAN

Proseguendo lungo la rete LAN il router Gateway si va a collegare ad un Firewall perimetrale a filtraggio dinamico. Siamo entrati così in una zona che si pone a cavallo tra la rete locale e la WAN. Qui si apre un ulteriore collegamento tra routergateway su cui opera il firewall, e un dispositivo IPS da cui si arriverà a due server fondamentali per una azienda operante online, un server HTTP ed un server SMTP.



Firewall

Il firewall è una componente Software e/o Hardware la cui funzione è quella di svolgere una gestione e difesa di rete. Distinguiamo due tipologie di Firewall, in base alla posizione in cui è impiegato:

Perimetrale: Posto nella zona di mezzo fra LAN e WAN

Non perimetrale: 1.Di Network, se posto a difesa di un braccio di rete.
2. Host, se protegge direttamente un Host.

Inizialmente, negli anni 90', questa componente attuava un filtraggio "Statico".

All'interno del firewall era presente una tabella (ACL) in cui manualmente erano inseriti gli indirizzi IP con annessi consensi o blocchi. Al tentativo di una connessione l'IP in arrivo veniva confrontato in maniera unidirezionale (dall'alto al basso) con la tabella ACL. In caso di mancato Match, di default, veniva bloccato l'accesso.

Questo filtraggio divenne obsoleto con la diffusione degli indirizzi IP da cui ne conseguiva un interminabile lavoro nell'aggiunta manuale di tali indirizzi nella ACL , oltretutto risultò estremamente vulnerabile ai fenomeni di "Spoofing"(camuffamento IP)



Firewall

Dagli anni 2000 subentrò il “filtraggio dinamico”:

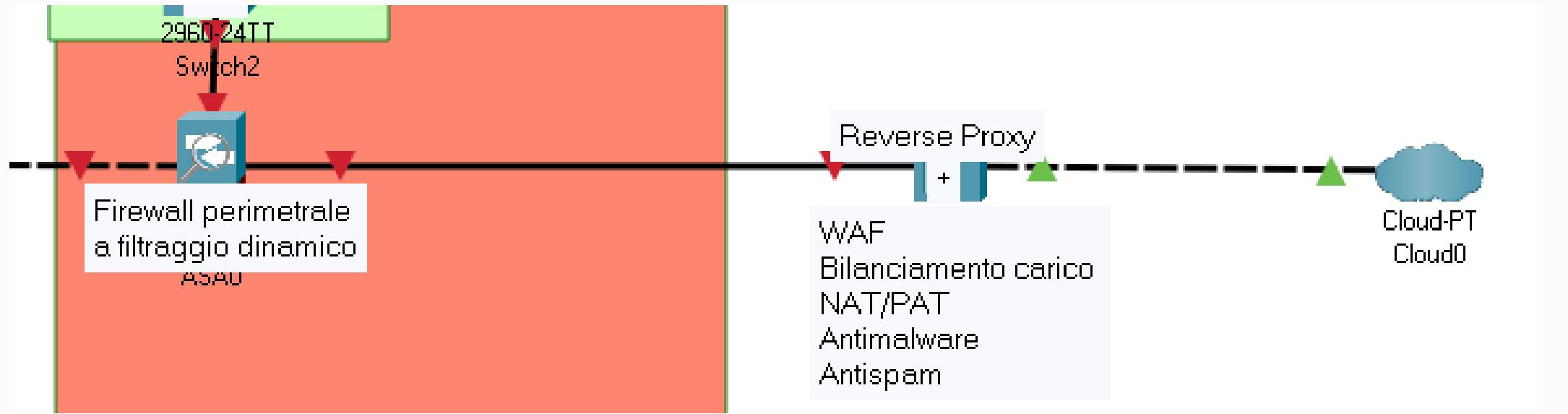
Per sventare il problema Spoofing, questo filtraggio prevede la chiusura di qualsiasi connessione dall'esterno verso l'interno della rete LAN. Al contrario permettendo quelle dall'interno all'esterno. Il procedimento, durante un tentativo di connessione, prevede la registrazione dell'indirizzo IP destinatario nella tabella ACL. Quando l'IP destinatario tenterà a sua volta di inviare dati all'host mittente, i dati passeranno poichè l'IP di provenienza risulterà presente nella ACL. Al termine della connessione la tabella ACL eliminerà la presenza dell'IP esterno, e ne impedirà un tentativo di collegamento non richiesto dall'interno della rete LAN.

Al contrario, al fine di permettere ai dispositivi che vogliono essere raggiunti, di ricevere un flusso di dati, è nata la DMZ-zona demilitarizzata (nella nostra rete è su sfondo verde). La DMZ permette di isolare i server pubblici dal resto della rete interna, e renderli visibili e raggiungibili da tutti.

Nella rete presa in esame i due server web sono posti appunto nella DMZ, anticipati però da un IPS. Questo svolge le medesime funzioni dell'IDS, con l'aggiunta di bloccare il pacchetto non riconosciuto.



WAN



Osservando l'arrivo alla zona WAN, troviamo un collegamento dal firewall a un reverse proxy, giungendo infine al cloud.

Un server proxy ha la funzione di mettere in collegamento due indirizzi IP, privati o pubblici che siano, e camuffarne l'indirizzo IP. Distinguiamo due proxy:

-**Forward proxy**, direzionato da Utente verso WAN

-**Reverse proxy**, dalla WAN alla rete locale.

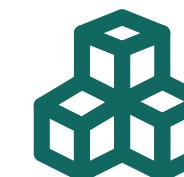
Fondamentale è la possibilità di implementare il proxy con altri servizi come WAF, bilanciamento carico, NAT/PAT, antimalware, antispam.

Il WAF è estremamente utile, letteralmente Web Application Firewall, protegge a tutti e 7 i livelli della scala ISO/OSI. Nello specifico ogni pacchetto che passa attraverso questo servizio viene spaccettato e confrontato con la sua tabella (fornita di dizionari antimalware) e qualora ci fosse riscontro, bloccherebbe il pacchetto malevolo.



Considerazioni

L'impiego tra un software IDS o IPS è legato alla necessità. Fondamentale è la possibilità di un falso negativo nell'esaminazione dei pacchetti da parte dell'IPS. Questo errore, visto il conseguente blocco del dato, porterebbe a forti rallentamenti all'interno di un'azienda. Mentre un IDS segnalerebbe con allert il mancato match con la tabella, e rimetterebbe alla decisione umana il provvedimento.



Sicurezza

Alla base di una rete è fondamentale il concetto di ripartizione, maggiori sono le compartimentazioni più sicura è la rete.



Produttività

La corretta scelta delle implementazioni nella rete, garantisce una rete più efficiente e quindi più produttiva.



Aggiornamento

Imprescindibile è la necessità di mantenersi aggiornati sulle novità in ambito di difesa e attacco. Le difese antiquate sono più vulnerabili.