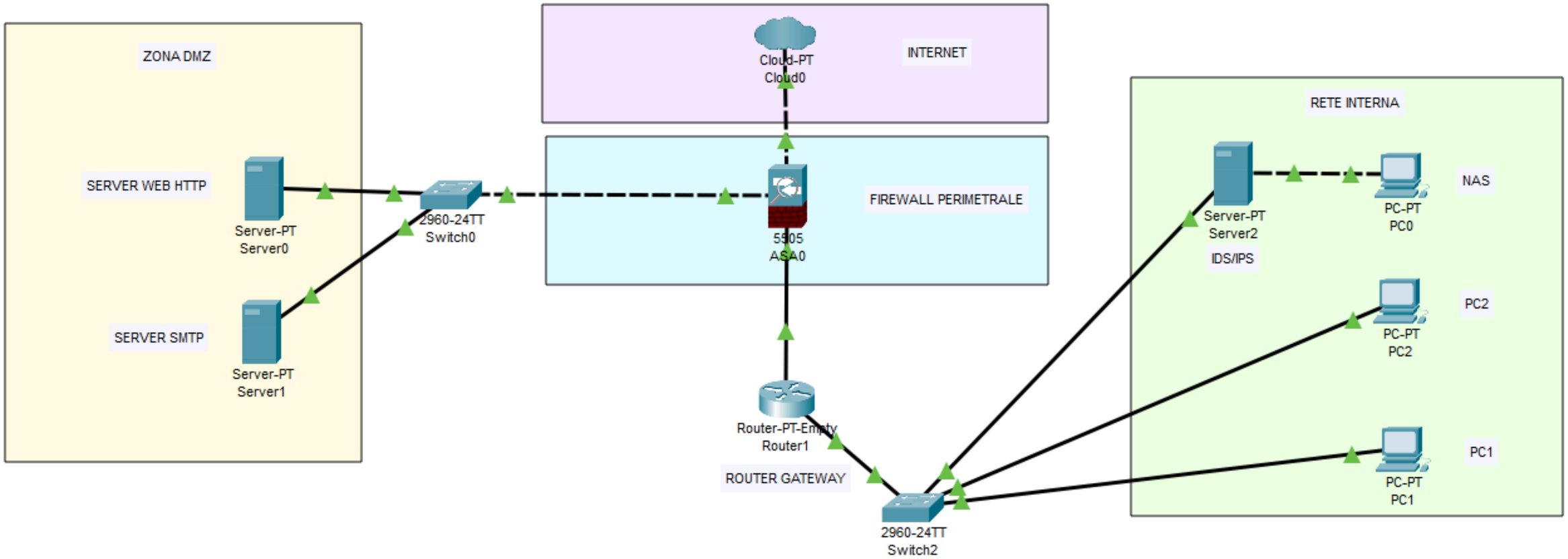
Federico
Cuccu

Analisi di una rete connessa a internet difesa da Firewall perimetrale

Pratica S3/L5

Rete


ZONA DMZ
SERVER WEB HTTP
Server-PT
Server0
SERVER SMTP
Server-PT
Server1
2960-24TT
Switch0
Cloud-PT
Cloud0
INTERNET
FIREWALL PERIMETRALE
5505
ASA0
Router-PT-Empty
Router1
ROUTER GATEWAY
2960-24TT
Switch2
RETE INTERNA
Server-PT
Server2
IDS/IPS
PC-PT
PC0
NAS
PC-PT
PC2
PC2
PC-PT
PC1
PC1

Spiegazione della rete

Questo è un esempio di rete aziendale, **connessa ad internet**, che ha la necessità di fornire un servizio pubblico e di conservare al sicuro i suoi dati.

Il firewall perimetrale di tipo hardware si occuperà, tramite il **filtraggio dinamico**, di proteggere la rete interna da tutte le connessioni che provengono dall'esterno, bloccandole. Permetterà invece le connessioni che hanno origine dall'interno verso l'esterno.

Affinché i due servizi siano raggiungibili (server web HTTP, che ospita ad esempio il sito web, e il server SMTP, per l'invio e la ricezione delle email) siano raggiungibili dall'esterno, abbiamo creato una **zona demilitarizzata (DMZ)**. Bisogna fare attenzione perché la zona DMZ permette tutte le connessioni in entrata e in uscita.

L'ideale sarebbe avere anche un firewall a **filtraggio per contenuto (WAF)**, dedicato alla protezione della zona demilitarizzata, in grado di ispezionare il traffico in entrata verificando il contenuto dei pacchetti e confrontandoli con la tabella ACL e il server esterno OWASP dove sono presenti tutte le definizioni anti-malware.

Spiegazione della rete

Nella rete interna troviamo il NAS (Network Attached Storage), che si occupa della **conservazione e del backup di tutti i dati aziendali**.

Questo sarà ulteriormente filtrato da un **server IDS/IPS** che lancerà l'allarme nel caso in cui un pacchetto sospetto sia arrivato fino a questo punto della rete, bypassando il firewall perimetrale.

Si potrebbe utilizzare l'IDS nel caso in cui non si vogliano avere problemi causati dai possibili **falsi positivi**, di cui l'IPS soffre.

Dato che l'IPS, oltre a lanciare l'allarme, **blocca il potenziale pacchetto malevolo**, potrebbe bloccare il lavoro ad uno o più dipendenti dell'azienda per errore.

L'IDS garantisce una migliore velocità e accessibilità, a discapito di un po' di sicurezza in più.