



Report di una tipica rappresentazione di rete aziendale:

**Cloud-PX Internet:** Tutto inizia dal Cloud-PX Internet, che rappresenta il punto di accesso alla rete internet pubblica con l'indirizzo di rete 192.168.0.0/24.

**Firewall Perimetrale 5506-X:** Le connessioni in ingresso dal Cloud-PX Internet passano attraverso un firewall di tipo 5506-X. Il firewall funge da barriera tra la rete esterna (internet) e la rete interna, permettendo o negando il traffico basato su un insieme di regole di sicurezza definite.

**Router-PT-Empty Router2:** Dopo aver attraversato il firewall, il traffico raggiunge il Router-PT-Empty Router2. Questo router potrebbe essere configurato per indirizzare il traffico a diverse parti della rete interna. Non sono forniti dettagli sulle sue regole o configurazione nell'immagine.

**DMZ/192.168.2.0/24 (area demilitarizzata):** Una parte del traffico viene indirizzata alla DMZ, che è una sotto-rete isolata che contiene servizi esposti all'internet pubblico, ma separata dalla rete LAN interna. Qui, l'indirizzo di rete è 192.168.2.0/24.

- All'interno della DMZ, c'è un Intrusion Prevention System (IPS) rappresentato come un blocco verde, connesso a uno switch (2960-24TT Switch1). L'IPS monitora e analizza il traffico e può eseguire azioni preventive contro le attività sospette per proteggere i server nella DMZ.
- Due server si trovano nella DMZ:
  - Server-PT HTTP: Un server configurato per ospitare un sito web o un'applicazione web, accessibile tramite il protocollo HTTP.

- **Server-PT SMTP:** Un server configurato per la gestione della posta elettronica, utilizzando il protocollo SMTP (Simple Mail Transfer Protocol).

**LAN/Intranet 192.168.1.0/24 (rete locale):** Altra parte del traffico è indirizzata verso la rete interna dell'organizzazione, nota come LAN o intranet, con l'indirizzo di rete 192.168.1.0/24.

- All'interno della LAN, il traffico attraversa un altro dispositivo di sicurezza: l'**Intrusion Detection System (IDS)**, indicato con un cerchio rosso. A differenza dell'IPS, l'IDS di solito rileva e segnala attività sospette ma non interviene attivamente.
- C'è un singolo dispositivo utente indicato come **PC-PT PC0**, presumibilmente un computer personale o di lavoro, e un **Server-PT NAS** che rappresenta probabilmente un dispositivo di archiviazione di rete (**Network-Attached Storage**).

L'architettura della rete illustrata è una configurazione standard per molte aziende, che utilizza un firewall per la protezione perimetrale, una DMZ per i servizi esposti e un IDS/IPS per il monitoraggio e la prevenzione delle intrusioni.