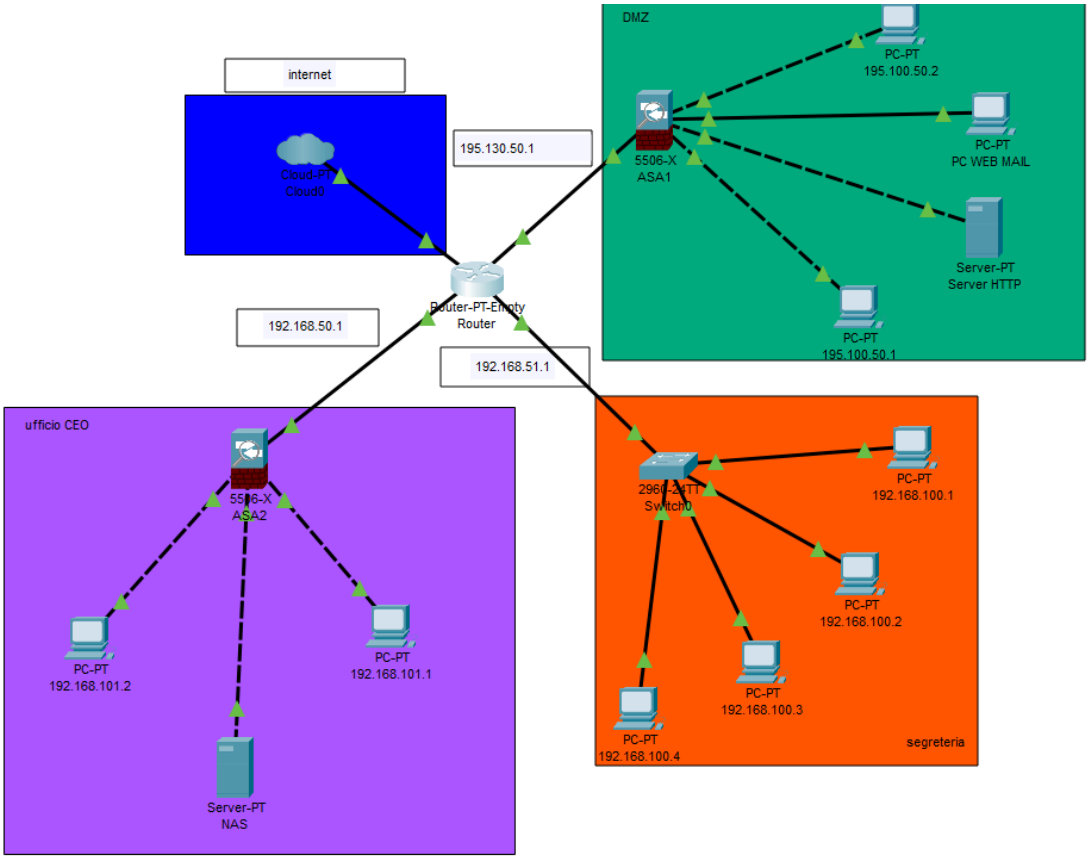
Relazione sulla Configurazione della Rete



Ho progettato una rete per garantire la massima sicurezza e una gestione efficiente del traffico. La rete è composta da tre sezioni principali: Internet, una zona DMZ e una rete interna, tutte protette da un firewall perimetrale.

Per rappresentare **Internet**, ho utilizzato un cloud che simula la connessione esterna. Questo cloud è collegato a un router perimetrale, che gestisce il traffico tra Internet, la DMZ e la rete interna.

La zona DMZ funge da "zona cuscinetto" e ospita i server accessibili pubblicamente: un server web e un server di posta elettronica. Questi server sono isolati per garantire che eventuali attacchi non possano propagarsi alla rete interna. Ho utilizzato un firewall ASA 5506-X per proteggere la DMZ e controllare rigorosamente il traffico.

La rete interna contiene le risorse aziendali più sensibili, come i PC dell'ufficio del CEO e un NAS per l'archiviazione dei dati. Ho segmentato ulteriormente questa rete: l'ufficio del CEO utilizza indirizzi IP specifici, così come la segreteria, collegata tramite uno switch. Un altro firewall ASA

5506-X protegge questa sezione, assicurando che solo il traffico autorizzato possa entrare o uscire.

Il **firewall perimetrale** (router) collega tutte le sezioni e gestisce il traffico con configurazioni IP specifiche per ogni interfaccia.

In sintesi, questa configurazione garantisce che i server pubblici siano isolati e protetti, mentre le risorse interne rimangono sicure e ben gestite. La segmentazione della rete e l'uso di firewall avanzati forniscono un solido livello di sicurezza per l'intera infrastruttura.