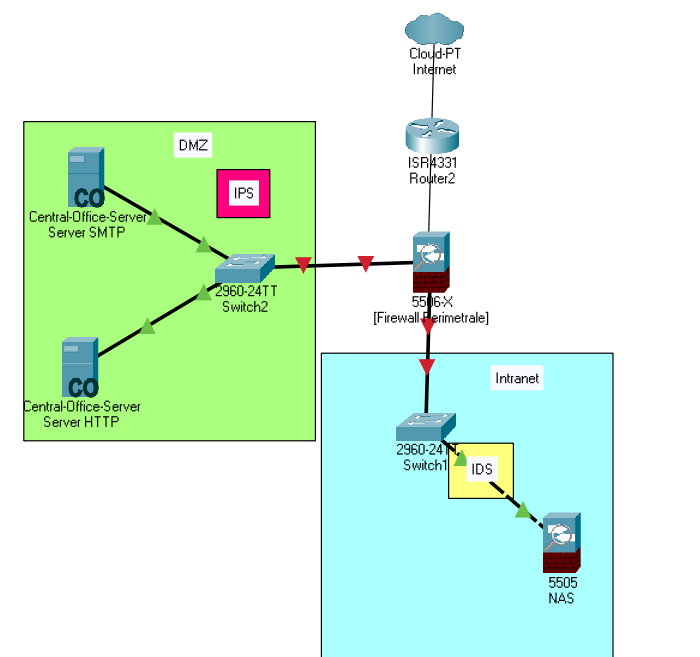
S2/L1  
  
Dopo aver configurato il router che sarà affiancato da un firewall perimetrale andremo a suddividere i nostri spazi. Essi saranno divisi in due aree, nella prima la DMZ comprende due server web rispettivamente un server SMTP ed un server HTTP. Essi sono sottoposti a vari sistemi di sicurezza, uno tra questi è IPS che cerca di identificare i malware che potrebbero presentarsi nella nostra DMZ.  
Invece nella seconda abbiamo una “intranet” ovvero una rete interna in contatto direttamente con la “NAS”. L’abbiamo posizionata dopo la DMZ perché trattando questi dati come sensibili avranno una sicurezza maggiore data da una “IDS” affiancata ad un esperto di sicurezza informatica che andrà a valutare la minaccia personalmente  
 **DMZ:** “Delimitary station zone” Abbiamo una zona di accesso dinamico che non ferma gli indirizzi IP sconosciuti e permette agli esterni di comunicare con i nostri server  
**Server** **SMTP**: Server di posta eletronica  
**Server** **HTTP**: Server web  
**IPS**: è un sistema di rilevamento di potenziali minacce , esso procede alla notifica ed al blocco della condivisione dati  
**IDS:** Esso è un sistema di rilevamento di potenziali minacce e le notifica all’operatore **NAS:** Network Access strorage esso deve essere collegato tramite LAN e protegge i dati sensibili