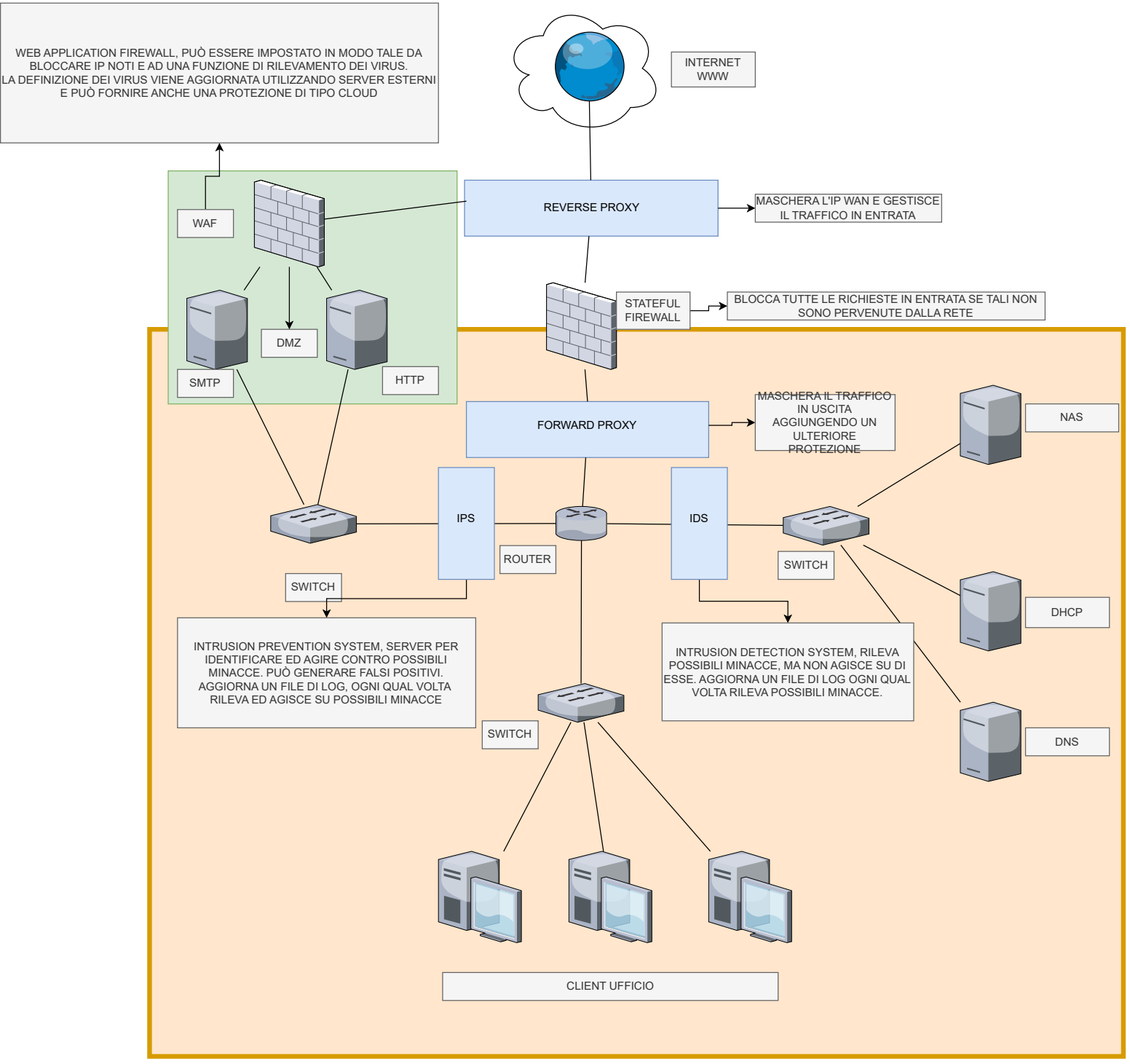

SPIEGAZIONE

HO POSTO **DUE PROXY** IN MODO CHE IL TRAFFICO IN USCITA DALLA RETE LOCALE VENGA MASCHERATO DAL FORWARD E QUELLO IN ENTRATA VENGA GESTITO DAL REVERSE, IN MODO DA PROTEGGERE IN MODO ULTERIORE LA RETE INTERNA ED EFFETTUARE LOAD BALACING.

LO **STATEFUL FIREWALL,** È UN FIREWALL CHE GESTISCE IL TRAFFICO IN MODO DINAMICO E BLOCCA TUTTE LE RICHIESTE IN INGRESSO, A MENO CHE, TALI RICHIESTE NON SIANO EFFETTUATE DALLA RETE INTERNA.

HO POSTO UN **WEB APPLICATION FIREWALL** PER PROTEGGERE LA DMZ(DEMILITARIZED ZONE, ZONA CHE PERMETTERE DI ESPORRE DEGLI HOST VERSO LA RETE INTERNET, SENZA ESPORRE L'INTERA RETE LOCALE)
IL WAF, COME IL FIREWALL, GESTISCE LE RICHIESTE IN ENTRATA, SOLO CHE, LE ACCETTA TUTTE, A MENO CHE, GLI IP DA CUI PROVENGONO, NON SIANO PRESENTI NELLA BLACKLIST OPPURE TENTATIVI DI INFEZIONE.

HO PREFERITO PORRE UN **IPS** TRA DMZ E RETE INTERNA, IN MODO DA EVITARE ATTACCHI MALEVOLI, POICHÈ OLTRE A INDIVIDUARLI, AGISCE SU DI ESSI.

PER LA PARTE DI RETE DOV'È PRESENTE IL NAS, HO PREFERITO PORRE UN SISTEMA **IDS**, CHE NON CREA LATENZA, MA MI PERMETTE COMUNQUE DI RILEVARE ATTIVITÀ SOSPETTE E QUINDI DI INFORMARE L'AMMINISTRATORE DELLA RETE.
UN ALTRO MOTIVO È ANCHE, IL VOLER EVITARE CHE, RICHIESTE LEGITTIME, VENGANO SCARTATE E QUINDI RENDEREBBE IL NAS IRRAGGIUNGIBILE.