Buid Week - 1

RETE COMPLESSA

La struttura della rete si divide in quattro parti:

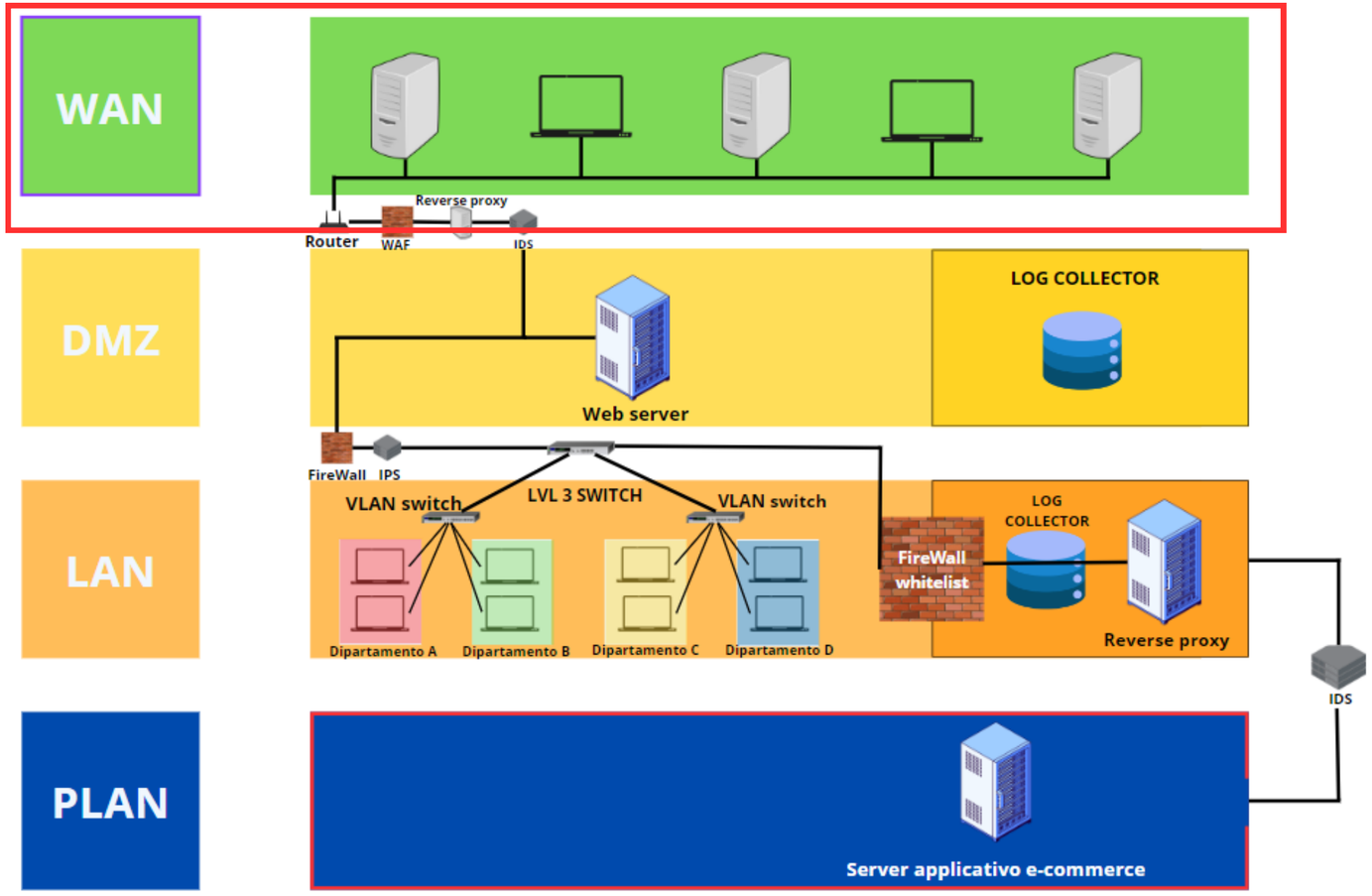
- WAN = Rappresenta la rete pubblica da cui proviene il traffico, costituito dalle richieste dei clienti.

- DMZ = La DMZ (Demilitarized Zone) costituisce una zona di rete intermedia tra la rete interna aziendale e la rete esterna WAN. Nel nostro caso, viene impiegata per ospitare i servizi web accessibili dall'esterno senza compromettere la sicurezza interna.

- LAN = La LAN (Local Area Network) è una rete informatica locale che connette gran parte dei dispositivi aziendali, accessibile esclusivamente ai dipendenti di Theta.

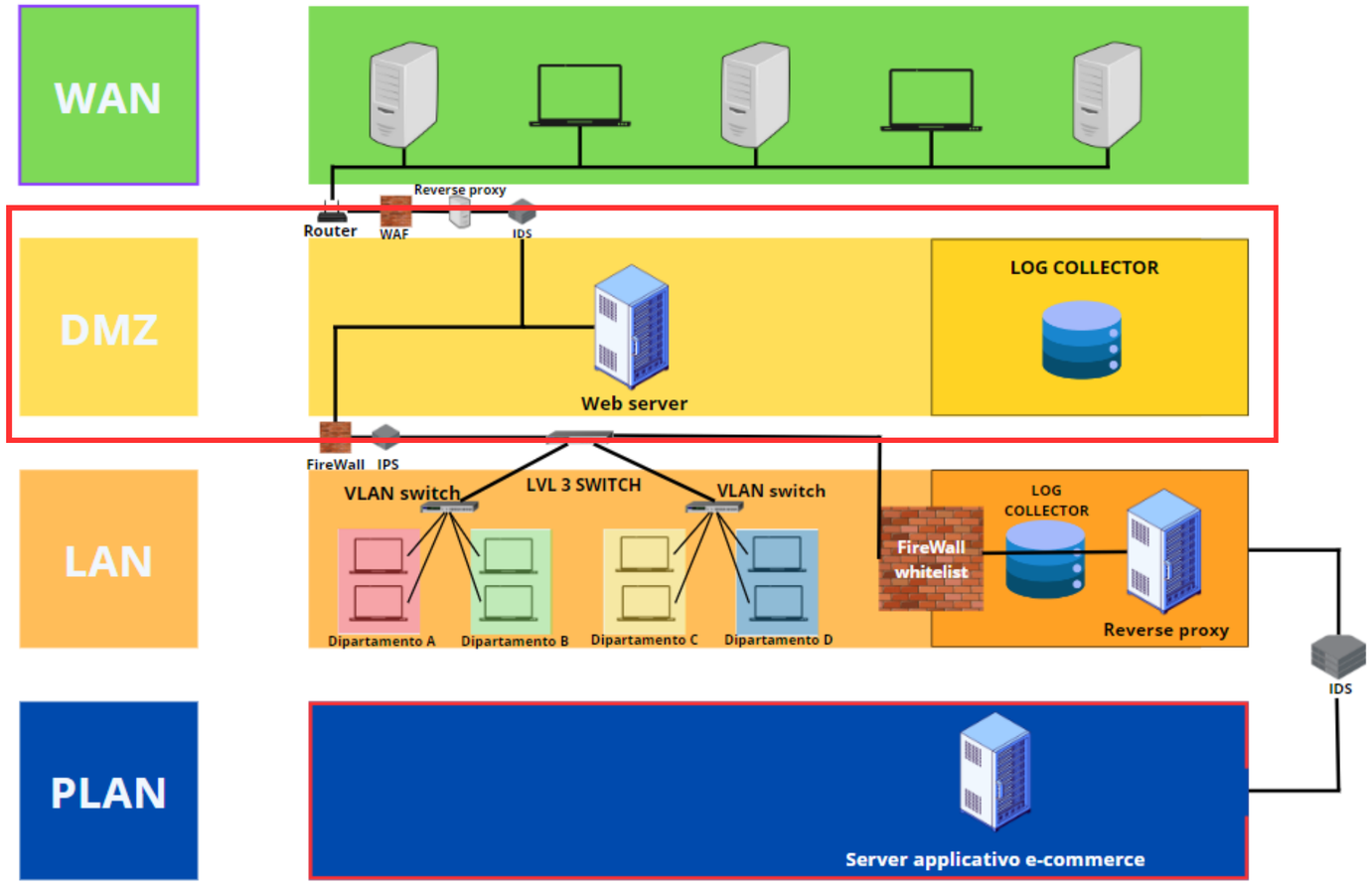
- PLAN = La PLAN è la rete più protetta ed esclusiva di questo schema. Privata di accesso a Internet, può comunicare solamente con un server reverse proxy, che rappresenta il punto di accesso per i dipendenti.

WAN



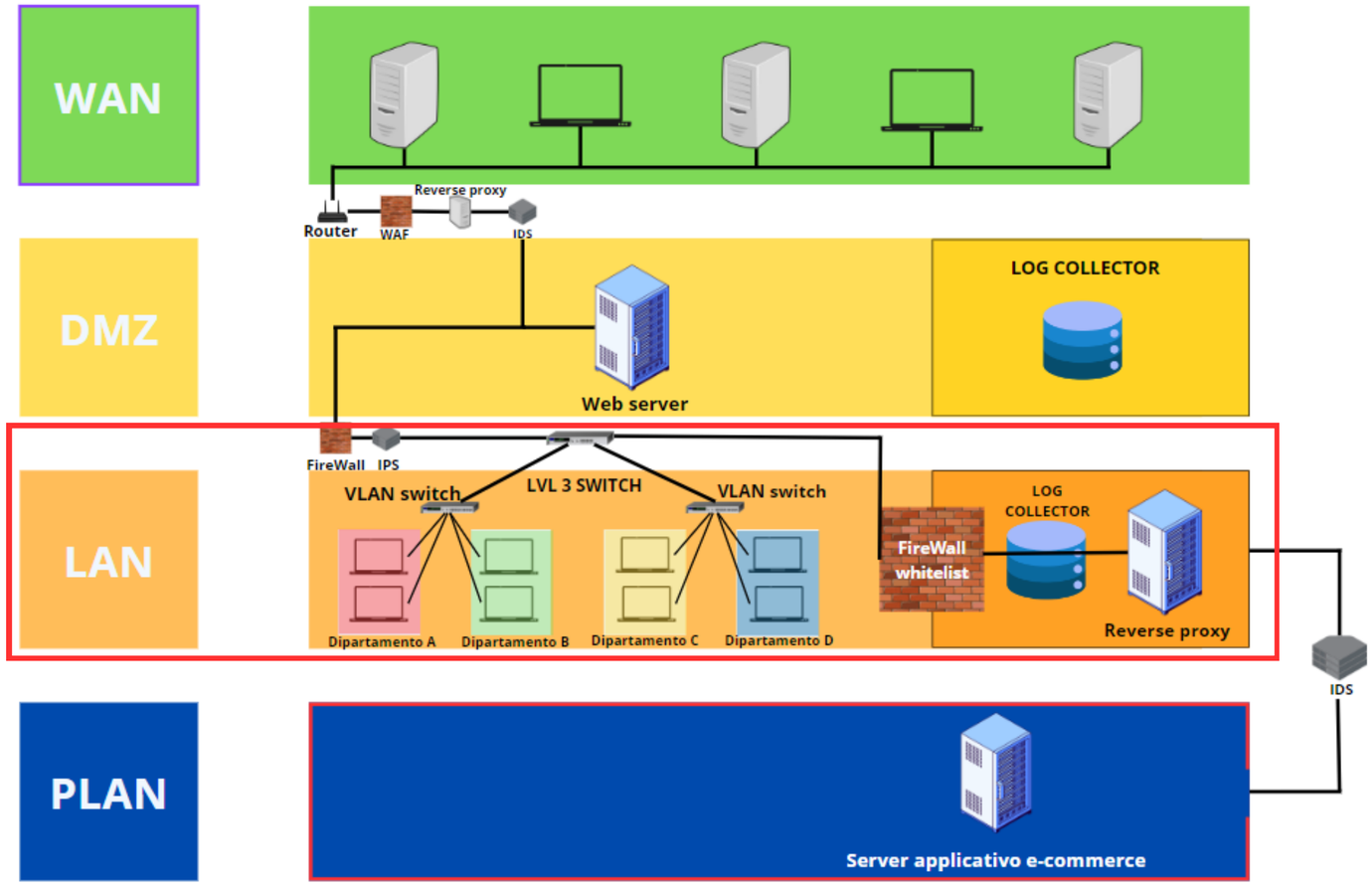
Una rete WAN (Wide Area Network) costituisce un sistema di connessioni che collega dispositivi su vaste aree geografiche. Le WAN facilitano la connessione di sedi distanti, consentendo la condivisione di dati, risorse e servizi. Organizzazioni aziendali, istituti educativi e fornitori di servizi di telecomunicazioni sfruttano le reti WAN per integrare operazioni in diverse località. In questo contesto, la rete WAN offre agli utenti la possibilità di connettersi al server HTTP e, di conseguenza, alla pagina web.

DMZ



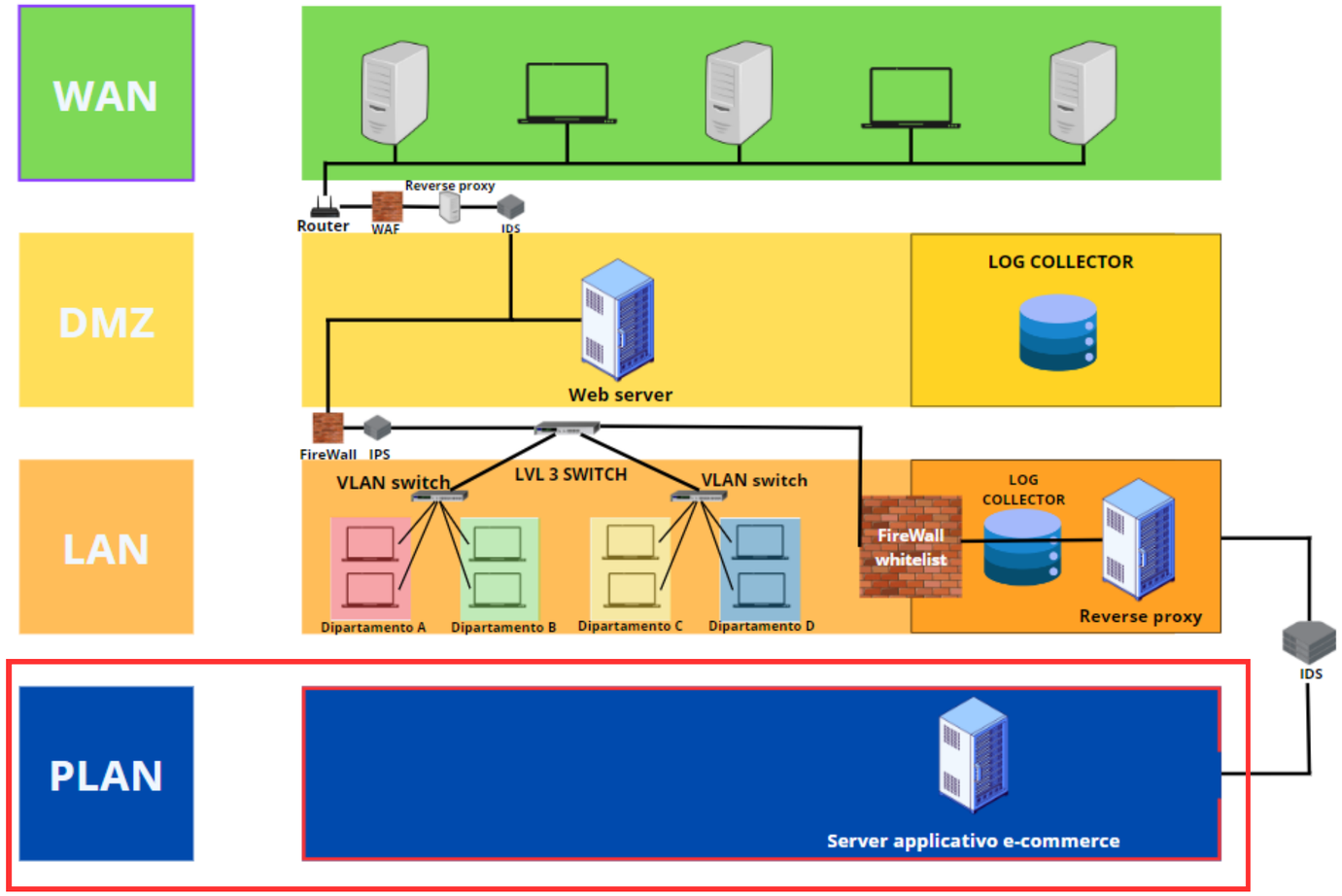
Una DMZ è una rete separata esterna, ottimale per gestire il traffico del server web senza compromettere la sicurezza interna. In questa zona isolata, si implementano misure di sicurezza come WAF, reverse proxy server e IDS per proteggere dai rischi esterni. Questi strumenti lavorano sinergicamente per garantire la sicurezza del server web e prevenire l'accesso non autorizzato alla rete interna. La DMZ funge da barriera protettiva, instradando il traffico esterno attraverso dispositivi di sicurezza dedicati anziché attraverso il firewall interno. Questo approccio contribuisce a preservare la sicurezza complessiva del sistema, mantenendo separate le reti interne ed esterne e mitigando potenziali minacce esterne.

LAN



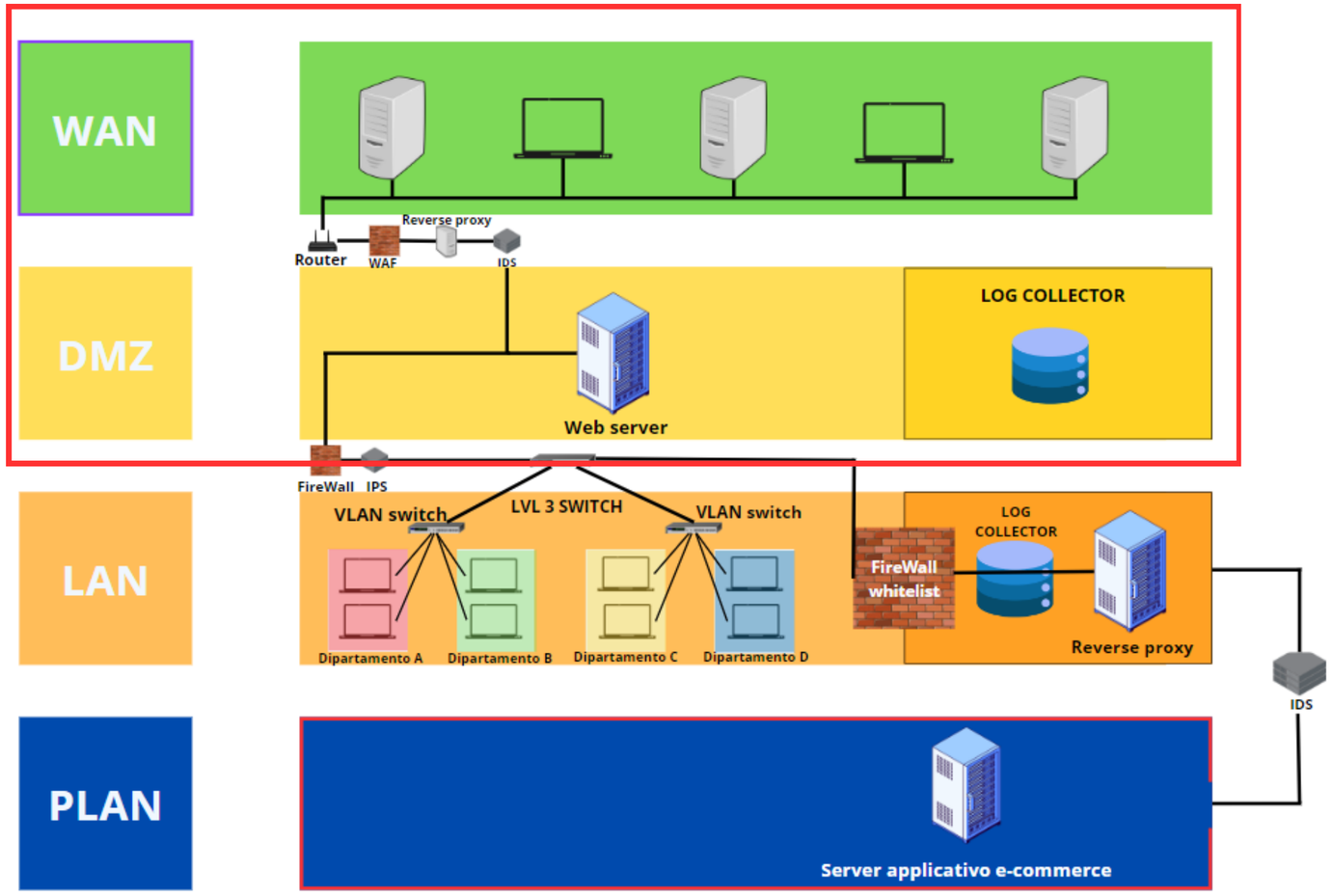
La rete LAN (Local Area Network) costituisce la maggior parte dei nostri dispositivi aziendali, come computer e stampanti. Questi dispositivi sono distribuiti in diverse WLAN che segregano la comunicazione in modo che i dispositivi non possano visualizzare il traffico delle altre WLAN senza una ragione di comunicazione specifica. Ogni dispositivo è connesso a uno switch VLAN, e ogni VLAN switch è collegato allo switch principale di livello 3, che consente il routing dalla rete interna verso l'esterno e facilita il routing e la comunicazione tra diverse VLAN senza compromettere i vantaggi di sicurezza.

PLAN



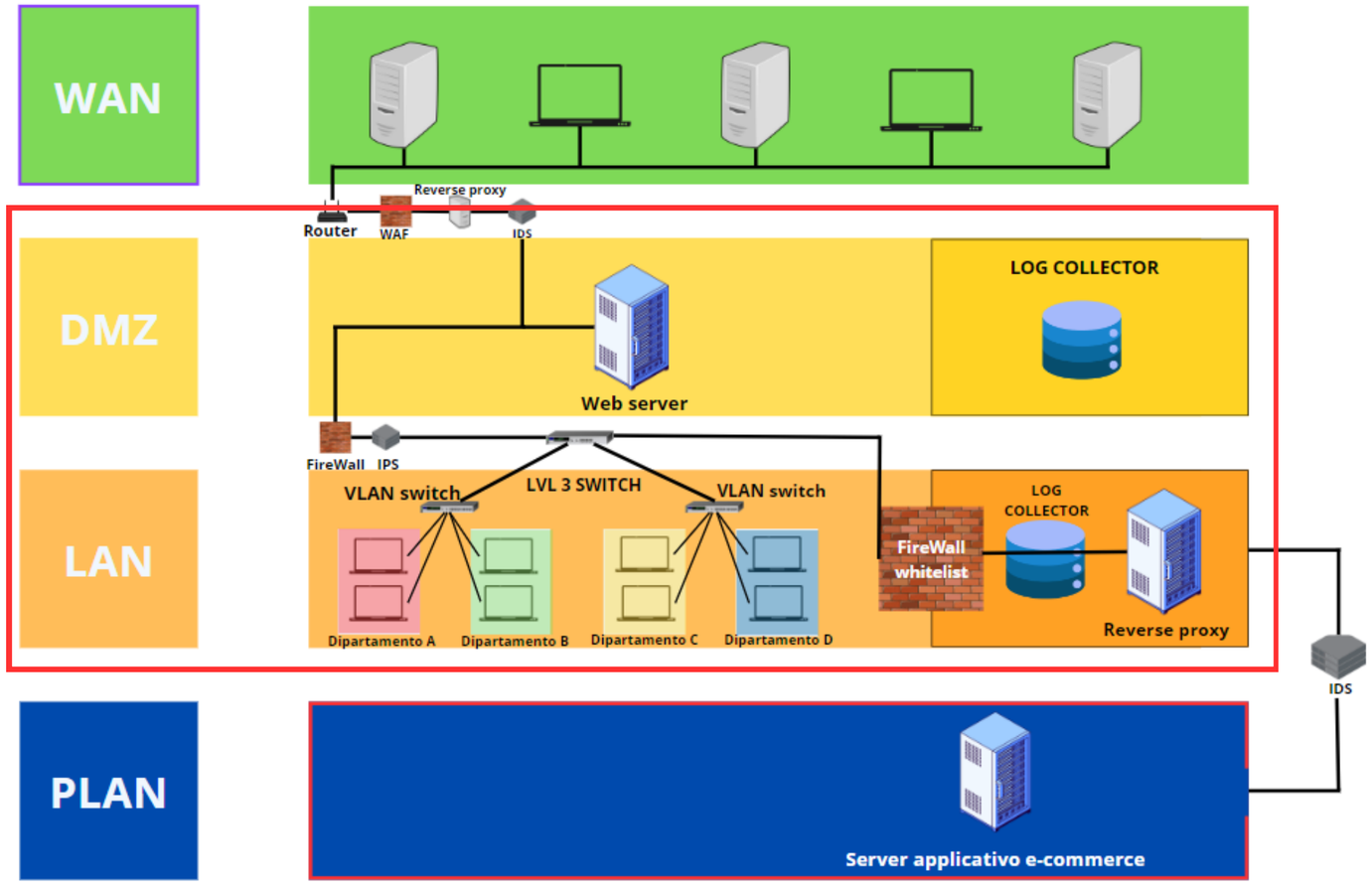
Una rete isolata senza accesso a Internet, definita come "blindata", comunica esclusivamente tramite un server proxy. Il server proxy funge da intermediario, gestendo richieste e risposte tra la rete isolata e la LAN aziendale. Tale configurazione fornisce sicurezza, limitando l'esposizione diretta dalla zona restritta alla LAN. Gli utenti aziendali possono accedere alle risorse del server applicativo solo attraverso il server proxy.

WAN - DMZ



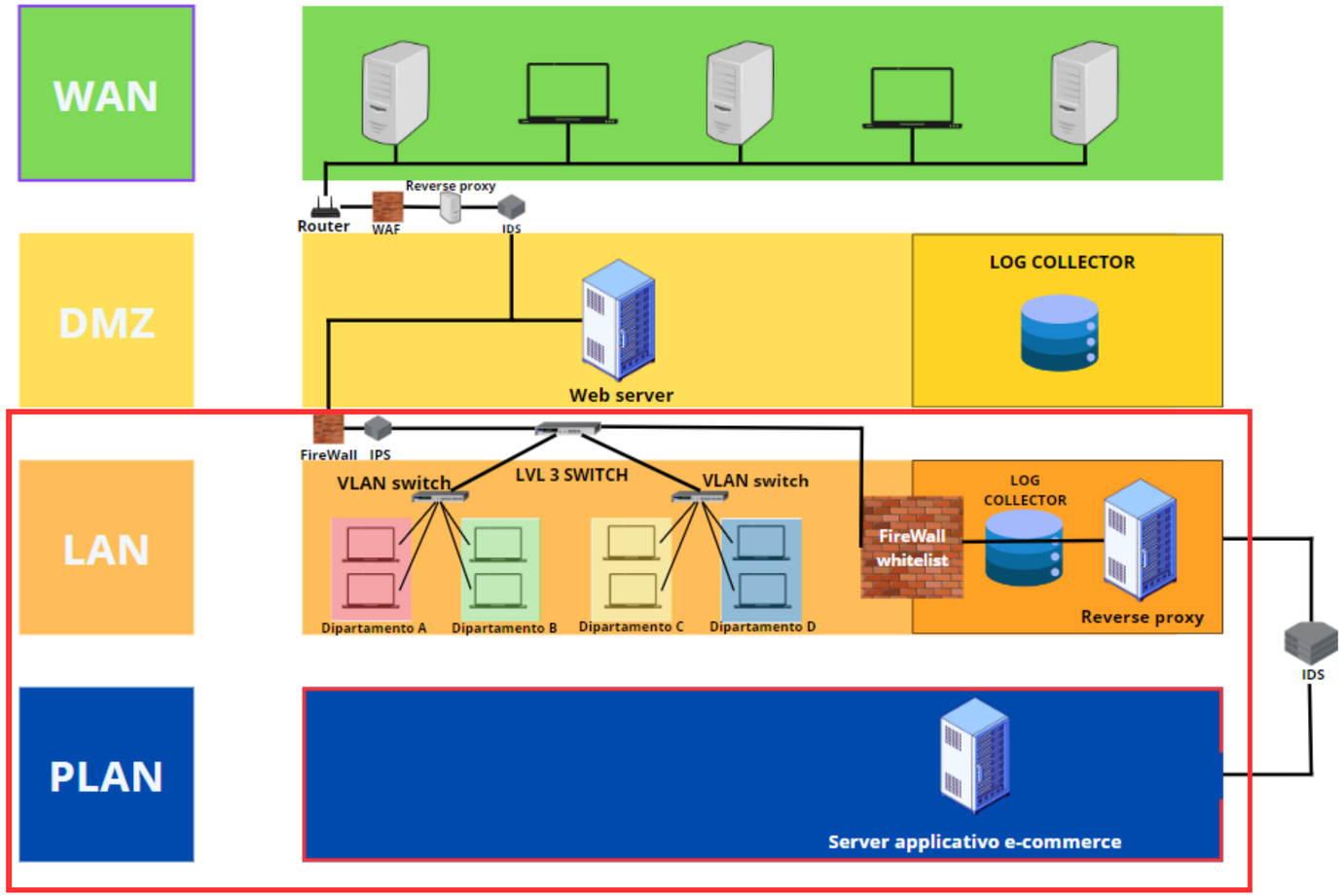
Per abilitare la comunicazione tra la rete WAN e la DMZ, è cruciale impiegare un router avanzato. Dietro questo dispositivo, vengono implementati meccanismi di sicurezza come firewall, reverse proxy e sistemi di rilevamento delle intrusioni (IDS). Il WAF (Web Application Firewall) riveste un ruolo essenziale, filtrando e monitorando le richieste e le risposte dei servizi per prevenire attacchi come DoS, XSS ed SQL al proxy server. Il reverse proxy agisce come intermediario tra la rete esterna e il vero server Web, mentre l'IDS monitora il traffico per individuare comportamenti sospetti. Questa configurazione protegge il server Web da minacce esterne, garantendo che il traffico raggiunga solo il reverse proxy server. Nel caso superasse questa barriera, l'IDS e il log collector forniranno avvisi tempestivi.

DMZ - LAN



Per consentire la comunicazione tra la DMZ e la rete LAN interna, è essenziale implementare un firewall e un sistema di prevenzione delle intrusioni (IPS). Questi dispositivi devono attentamente filtrare il traffico in entrata e in uscita, garantendo che solo le comunicazioni autorizzate attraversino la barriera tra le due reti. Il firewall stabilisce regole per controllare il flusso dei dati, permettendo solo il traffico specificato. L'IPS monitora il traffico per identificare e prevenire intrusioni. Successivamente, il traffico sicuro può essere instradato attraverso uno switch di livello 3 che collega la DMZ alla rete LAN, agevolando la comunicazione tra le due reti in modo sicuro e controllato.

LAN - PLAN



Per agevolare la comunicazione tra la rete aziendale LAN e la PLAN, senza accesso a Internet, si può adottare il seguente approccio: implementare un firewall con whitelist e un reverse proxy per fornire agli utenti le informazioni necessarie senza richiederle direttamente al server applicativo.

Successivamente, i dati sicuri sono sottoposti a un IDS che analizza la presenza di eventuali tentativi maliziosi di infiltrarsi nella PLAN. Questa configurazione offre un controllo granulare sulla sicurezza, con il firewall e il reverse proxy che filtrano l'accesso dalla LAN alla PLAN.

LOG COLLECTOR

Un log collector è un elemento di un sistema di gestione dei log che raccoglie, elabora e archivia i dati di registro provenienti da varie fonti all'interno di una rete. I log contengono dettagli su eventi, attività e problematiche verificatesi nei dispositivi di rete e nei sistemi informatici. Il log collector è progettato per centralizzare questi dati da diverse fonti, quali firewall, server e dispositivi di rete, archiviandoli in modo centralizzato. Questa centralizzazione agevola un monitoraggio più efficace, la tracciabilità delle attività, la sicurezza informatica e la risoluzione dei problemi, contribuendo a mantenere la sicurezza e l'integrità del sistema.