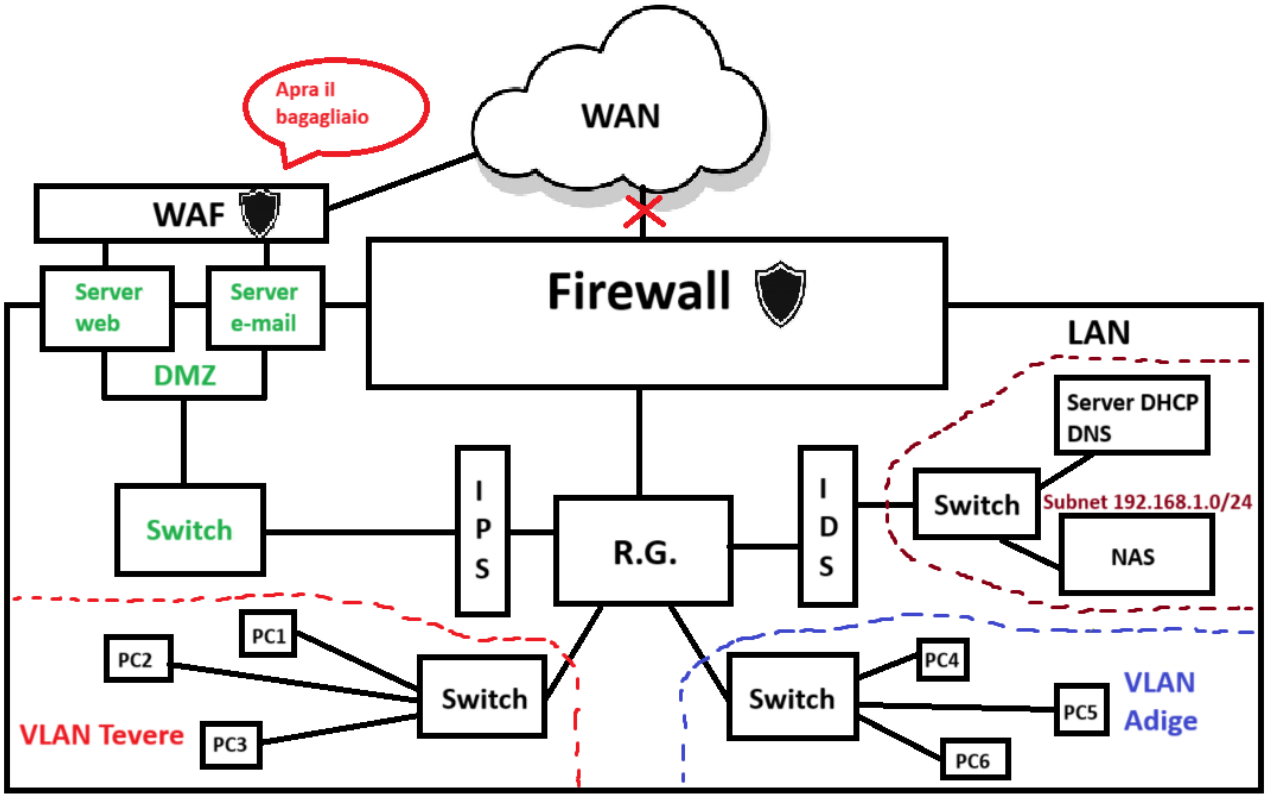

Abbiamo configurato una rete aziendale protetta da firewall.

Innanzitutto la rete è suddivisa all'interno in diverse sottoreti, precisamente abbiamo due VLAN (chiamate Tevere ed Adige) dedicate a uffici diversi dell'azienda, una sottorete dedicata alla sala server, in cui sono tenuti i dati sensibili, e infinine una DMZ che rappresenta la parte pubblica dell'azienda, affacciata su internet.

La rete LAN è protetta da un firewall statement, quindi dinamico; permette quindi solo dati in uscita, mentre in ingresso filtra solo quelli che arrivano in risposta ai dati in uscita (controllando l'indirizzo IP).

Abbiamo creato una DMZ per permettere il traffico in entrata sui server web e e-mail dell'azienda; questa DMZ è protetta da un diverso tipo di firewall chiamato WAF (Web Application Firewall), che filtra i pacchetti non guardando all'indirizzo IP, ma al payload degli stessi. Se il WAF riscontra un payload malevolo (lo possono riconoscere grazie a tabelle che riportano definizioni aggiornate di malware) blocca il pacchetto, altrimenti lo lascia passare.

All'interno della rete LAN abbiamo installato altri strumenti di sicurezza, l'IPS e l'IDS.
Abbiamo posto l'IPS (Intrusion Protection System) come ulteriore barriera tra la DMZ e il router/gateway che collega le altre reti/sottorenti interne, in modo da bloccare eventuali minacce che siano sfuggite al controllo del WAF prima che entrino effettivamente nella rete aziendale interna.

Infine abbiamo posto un'ultima linea di difesa a protezione dei server DHCP/DNS e del NAS (Network-Attached Storage), la parte più sensibile della rete. L'IDS (Intrusion Detection System) non blocca attivamente le minacce, si limita a segnalarle con un messaggio di alert.
Usiamo un IDS per venire incontro all'accessibilità, in quanto è probabile che gli utenti all'interno della rete abbiano bisogno di dati contenuti nei server e nel NAS per poter lavorare; se mettessimo

un IPS e questo risontrasse un falso positivo, l'utente che ha bisogno di un certo dato non potrebbe accedervi finché il responsabile della sicurezza informatica non sblocca la sua posizione e gli permette l'accesso. Si fa questo sacrificio alla sicurezza perché è molto più probabile che una minaccia arrivi dall'esterno, piuttosto che dall'interno.

In alternativa avremmo potuto installare un reverse proxy in entrata (comunque assistito da un firewall, in caso il proxy dovesse cadere) oppure un ulteriore server proxy interno, tra il firewall e il router gateway.