

I singoli host sono protetti da un Firewall (evidenziato in azzurro) installato negli stessi dispositivi, invece la rete è protetta da un Firewall perimetrale dinamico (evidenziato in arancione). Una piccola sezione di questo firewall, la DMZ (evidenziata in giallo) permette a qualunque utente di internet di accedere alla sezione di rete dove sono presenti “server 1” e “server 2”. Per non permettere ad utenti esterni di entrare nel resto della rete, viene installato un software che filtra in base ai contenuti in arrivo chiamato WAF che tramite il confronto tra tabelle esterne ed il pacchetto inviato deciderà se far passare o meno il file. Dopo il confronto del file, se malevolo, l’IPS (evidenziato in rosso) banna e invia un’allert per segnalare il tentato attacco. D’altra parte esiste anche l’IDS (evidenziato in blu) che è un software che non banna a priori il mittente del pacchetto perché questo è studiato per essere installato in parti delle reti in cui vengono salvati dati sensibili, quindi per evitare fenomeni di falsi positivi e bloccare dati potenzialmente molto importanti, viene solo inviato un’allert.