

E-commerce

Per rendere più sicura la DMZ [demilitarized zone] si è pensato di adottare la seguente soluzione: Aggiungere un WAF in corrispondenza della DMZ in modo da bloccare eventuali attacchi XSS e/o SQLi, essendo il WAF un particolare tipo di Firewall in grado monitorare e bloccare il traffico HTTP verso il web.

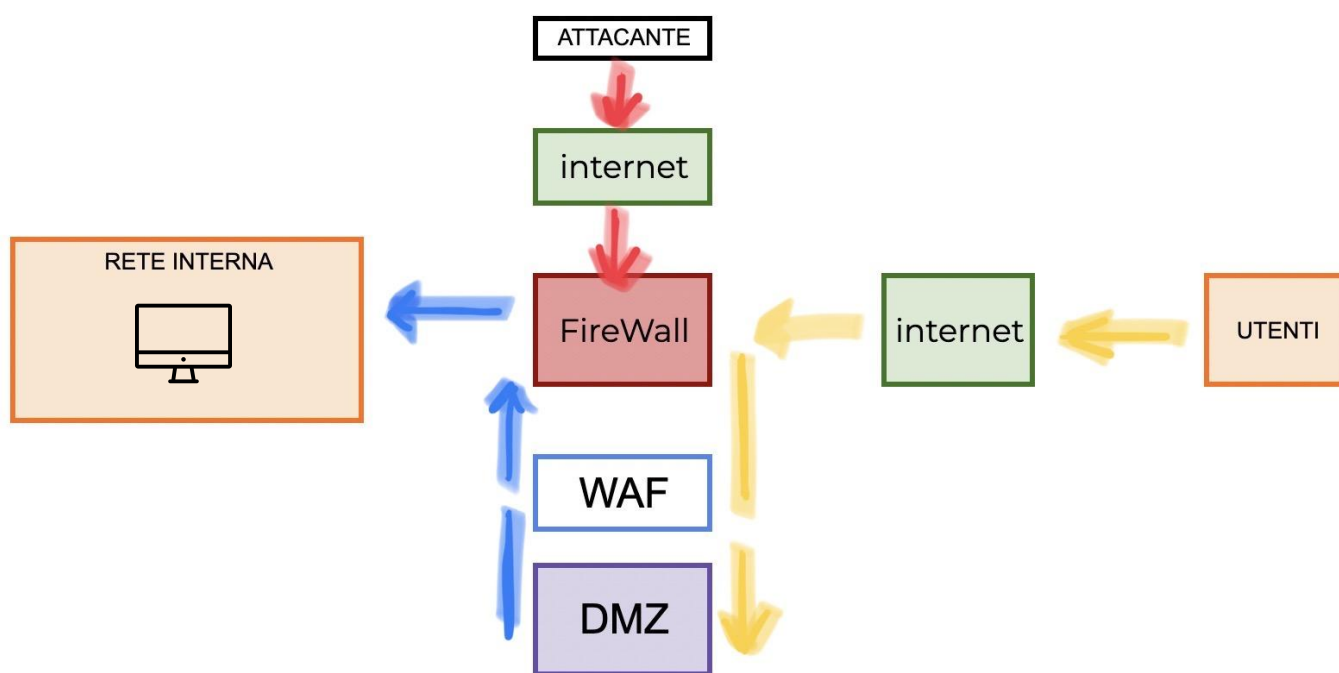
Impatti sul business

Preso in considerazione che l'azienda ha un ricavo di 1.500\$ per minuto nell'ipotesi di un attacco Ddos il server andrà in down per circa 10 minuti, il che ci porta a concludere che l'azienda perderà 15.000\$ durante questo attacco.

Response

Per la risoluzione di questo attacco malware si consiglia di adottare “L'isolamento” tecnica la quale andrà ad isolare il malware senza negare l'accesso all'attaccante così anche da poterci permettere di studiare le sue strategie d'azione

Soluzione Grafica



Soluzione più aggressiva

Per migliorare ulteriormente l'infrastruttura della rete si potrebbe pensare di aggiungere un honeypot sempre subito dopo il WAF