W20D4

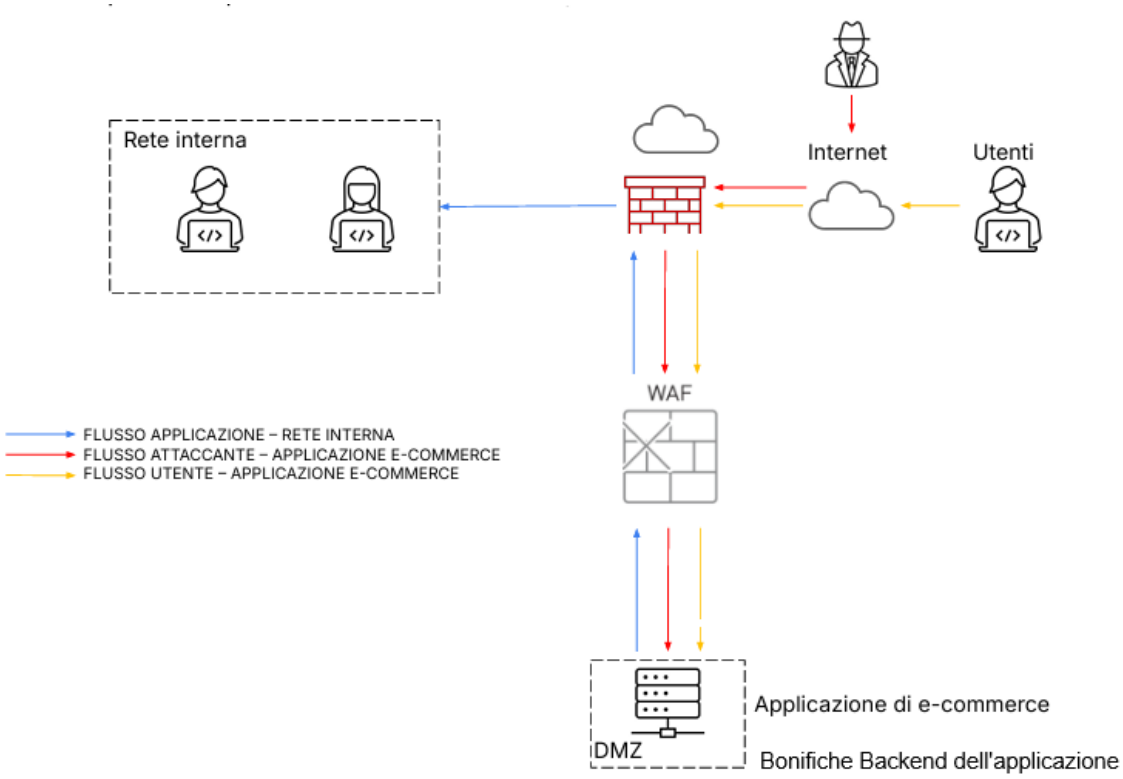
Sommario

Scenario 1 Azioni preventive

Azioni preventive:

1. Sanitizzazione dell'input nel back end dell'applicazione in modo che eventuali codici malevoli non vengano considerati, si può usare funzione htmlspecialchars() per pagine in PHP
2. Assegnazione del cookie HttpOnly
3. Implementazione di una CSP (Content Security Policy) per limitare le risorse che il Browser può mettere a disposizione in caso di attacco

4. Aggiunta di un WAF (Web Application Firewall) davanti alla web application. Questa andrà a filtrare le richieste verso la nostra Web app



Scenario 2 Impatti sul business

Possiamo andare a calcolare le perdite del Business andando a moltiplicare il tempo in cui l'applicazione è fuori servizio (10 min) per la spesa media al minuto (1500€/min)

Business Impact = 1500 X 10 =15000€

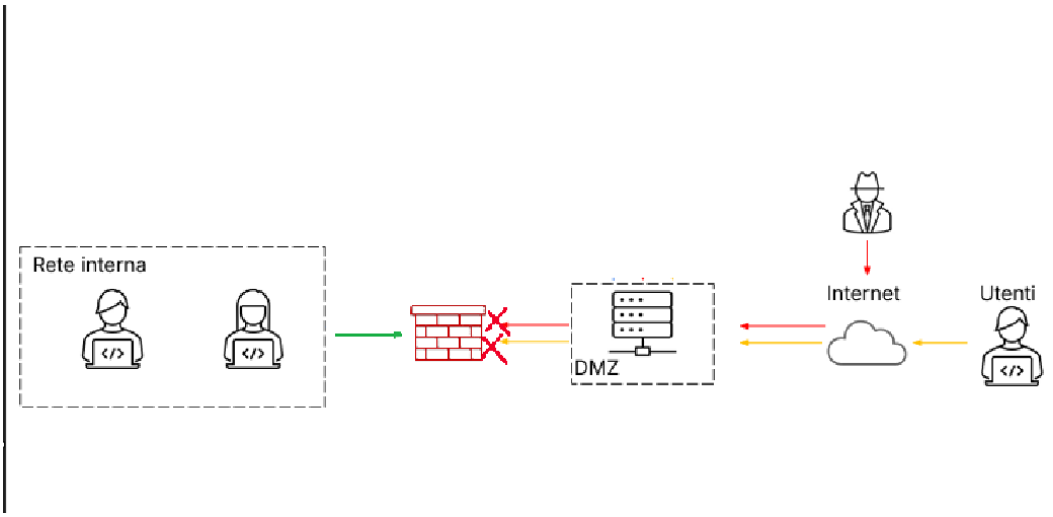
La prevenzione di attacchi Dos è piuttosto complessa e passa per più soluzioni contemporaneamente

- Implementazione di Firewall di applicazione avanzati
- limitare il numero di richieste che un client può inviare a un sistema (rate limiting)
- IDS/IPS cha vadano a bloccare traffico anomalo in tempo reale
- Implementazione di un SOC che possa andare ad analizzare il traffico in tempo reale

Inoltre a livello infrastrutturale si può pensare di implementare una ridondanza di server affinché distribuiscano il carico su più nodi.

Scenario 3 Response

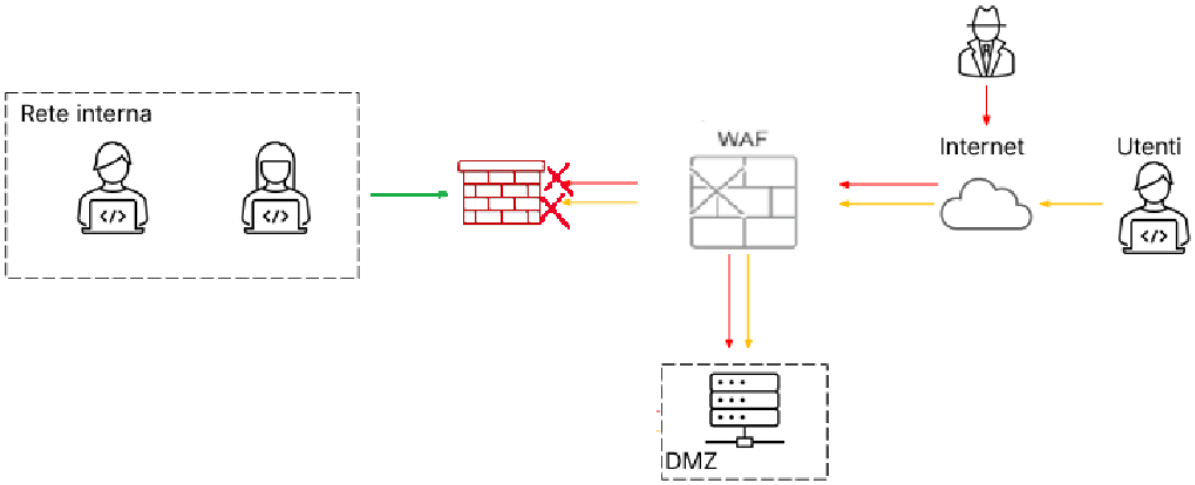
La Dmz viene complente isolata ponendola al di fuori del firewall che andrà a bloccare tutte le connessioni in ingresso verso la rete interna



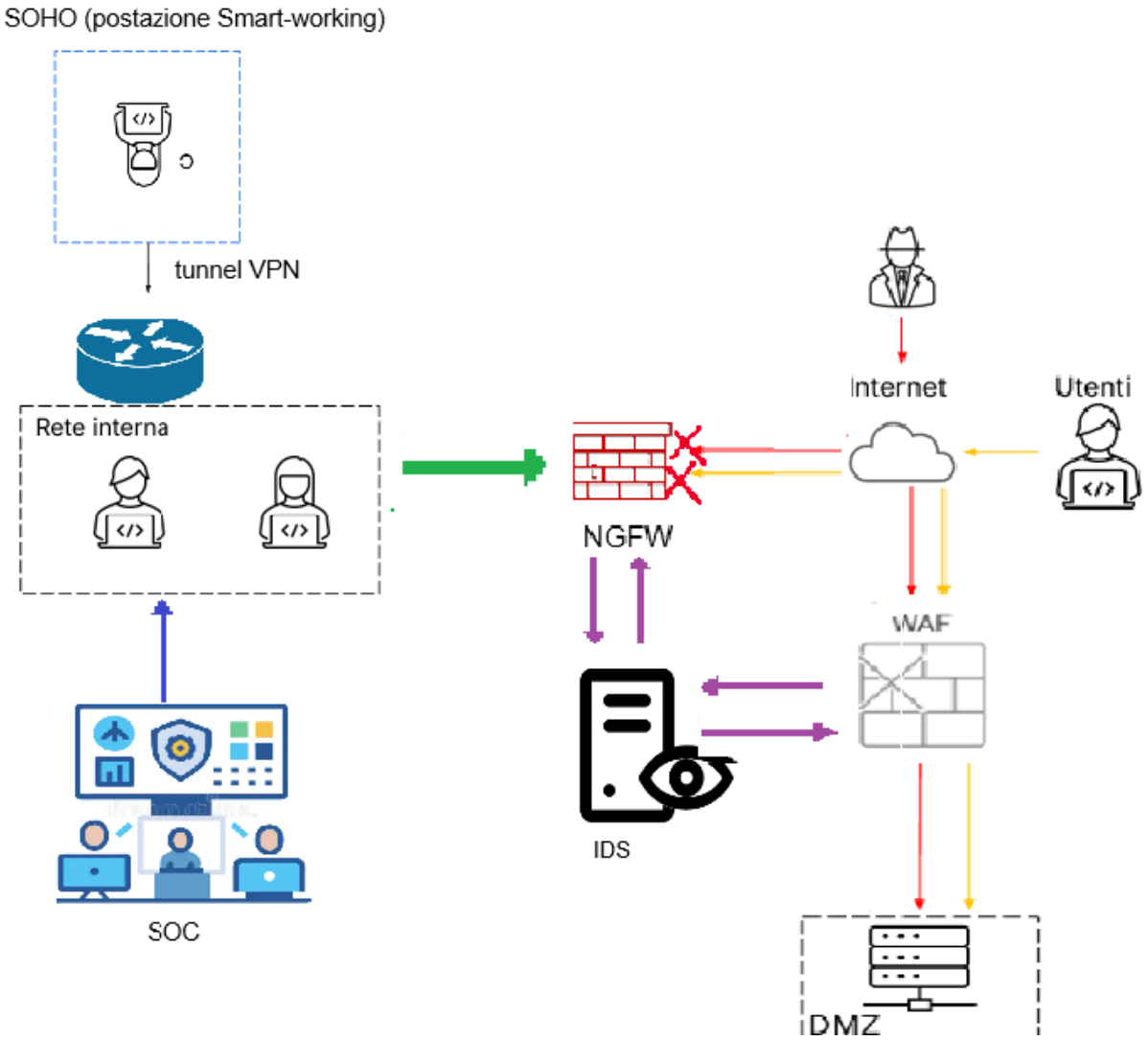
Faccio presente che questa topologia serve ad isolare la rete interna senza aggiunger nessun hardware

Scenario 4 Soluzione completa

Andiamo ad unire le due topologie proposte in modo da avere una rete interna ben protetta e una web-app difesa da un Waf server (firewall dedicato)



Scenario 5 modifica più aggressiva



Nella nuova topologia abbiamo segmentato ulteriormente la rete interna dalla DMZ, che sono ancora in contattato attraverso un IDS. Abbiamo un unico Firewall Next generation che va a filtrare tutto il traffico dalla rete interna verso internet e verso la Web- app. Inoltre, abbiamo la possibilità di accedere alla rete interna tramite una Vpn per i dipendenti che lavorano in smart working. Il Soc esterno è opzionale anche se fortemente raccomandato, il costo del budget però considerato non tenendone conto.

Componente	Fascia di prezzo stimata (USD)
IDS	7 000 – 15 000
NGFW	1 500 – 5 000
WAF	10 000 – 30 000 (media); fino a 120 000+ (enterprise)
Cisco 1100	1 000 – 2 000

Totale tra i 20000$ e i 50000$, andando a contenere i costi scegliendo hardware non eccessivamente entreprise riusciamo a contenere i costi sotto il Budget dei 30 K.

Upgrade consigliati

I seguenti Upgrade sono in ordine rispetto effort/costo

1. Soc esterno già aggiunto in topologia andrà a migliorare di molto la sicurezza dell'azienda monitorando in tempo reale H24 ogni possibile minaccia
2. Sostituzione del IDS con un IPS migliora la risposta della rete a eventuali minacce
3. WAF di maggiore qualità permetterà una maggiore resilienza della web app ad eventuali minacce