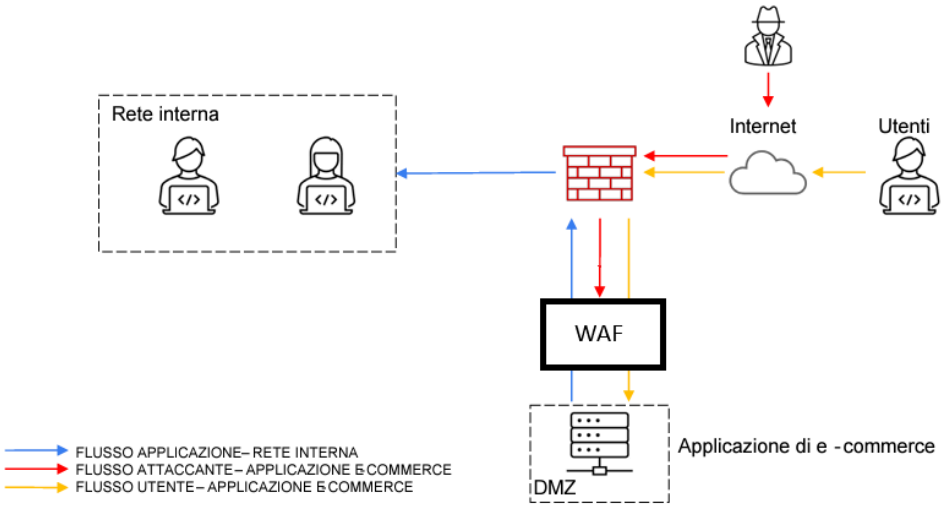
1. Posizioniamo un Web Application Firewall (WAF) tra Internet e l'applicazione web che si desidera proteggere. Il WAF agisce come un filtro per il traffico HTTP/HTTPS in entrata e in uscita, analizzando le richieste e le risposte web per individuare e bloccare attacchi informatici come SQL injection (SQLi), cross-site scripting (XSS), e altre vulnerabilità delle applicazioni web.

Il posizionamento del WAF permette di proteggere l'applicazione web dagli attacchi prima che raggiungano l'infrastruttura interna. In questo modo, il WAF può filtrare il traffico malevolo prima che possa danneggiare l'applicazione o raggiungere i server interni.

Inoltre, posizionare il WAF in questa posizione consente anche di applicare politiche di sicurezza specifiche e personalizzate per proteggere l'applicazione web dagli attacchi esterni, senza interferire con il traffico interno tra gli utenti e l'applicazione.



2. Calcoliamo l'impatto finanziario dovuto alla non raggiungibilità del servizio per 10 minuti a causa di un attacco DDoS:

Impatto Finanziario = (Minuti di non raggiungibilità) x (Spesa media degli utenti per minuto)

Minuti di non raggiungibilità = 10 minuti
Spesa media degli utenti per minuto = 1.500 €
Calcolo dell'impatto finanziario:
Impatto Finanziario = 10 minuti x 1.500 €/minuto = 15.000 €

Quindi, l'impatto finanziario dovuto alla non raggiungibilità del servizio per 10 minuti è di 15.000 €.

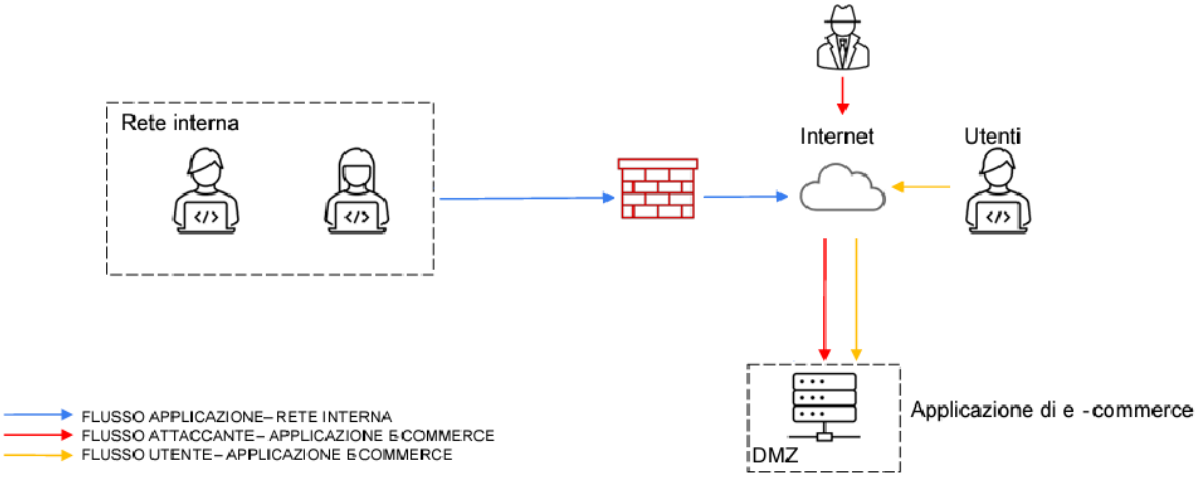
Per mitigare gli effetti di un attacco DDoS e proteggere l'applicazione web, è possibile adottare le seguenti azioni preventive:

- Configurazione per distribuire il carico di traffico e mitigare gli effetti di un attacco DDoS. Cioè distribuire il traffico su più server distribuiti, garantendo che l'applicazione rimanga disponibile anche durante un attacco DDoS.

- Monitoraggio del traffico di rete: Utilizzare strumenti di monitoraggio del traffico di rete per rilevare e rispondere tempestivamente agli attacchi DDoS, identificando i pattern di traffico dannoso e applicando misure di mitigazione appropriate.

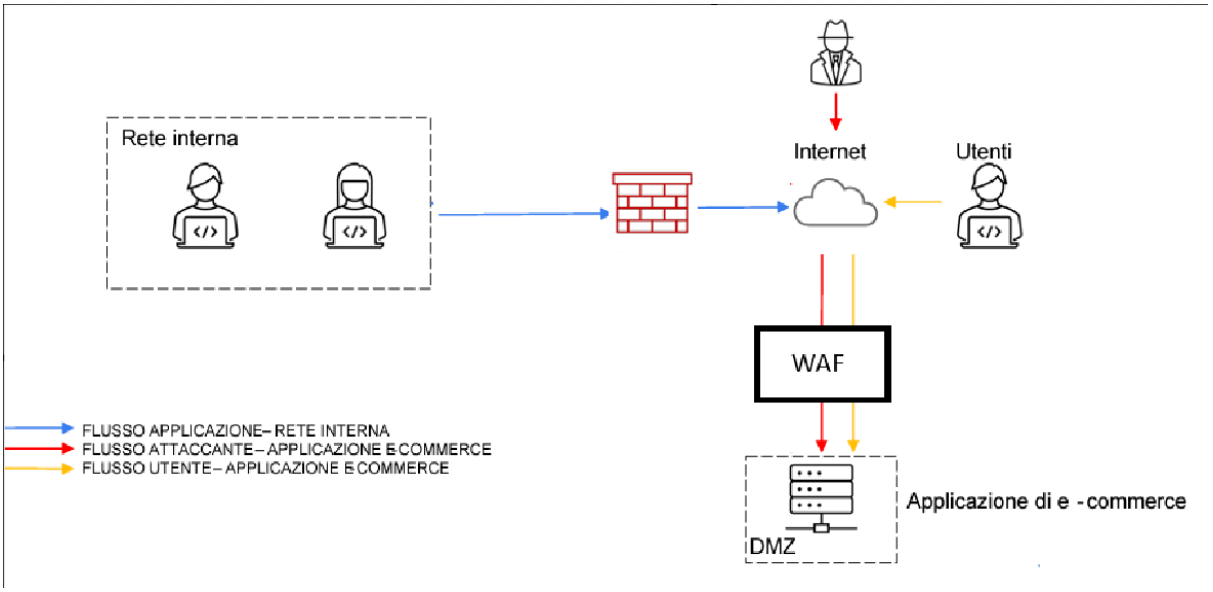
Implementando queste azioni preventive, è possibile ridurre l'impatto degli attacchi DDoS sull'applicazione web e proteggere l'attività commerciale dai danni finanziari causati dalla non raggiungibilità del servizio.

3. La DMZ viene isolata dal resto della rete. Cioè che il traffico tra la DMZ e la rete interna si interrompe, impedendo al sistema infetto nella DMZ di comunicare con altri dispositivi nella rete interna. Tuttavia, l'accesso dell'attaccante al sistema infetto viene mantenuto.



La decisione di isolare la DMZ infetta su Internet è una misura critica per limitare la propagazione del malware e proteggere la rete interna. Isolare la DMZ infetta significa separarla completamente dal resto della rete, impedendo qualsiasi comunicazione con altri segmenti di rete. Questa azione serve a prevenire che il malware si diffonda ulteriormente all'interno della rete e possa compromettere altri sistemi critici.

4.



Abbiamo discusso dell'implementazione di un WAF per proteggere l'applicazione web da attacchi esterni. Questa misura preventiva mira a filtrare il traffico in arrivo e a bloccare potenziali minacce prima che possano raggiungere l'applicazione. Poi è stato proposto di isolare la DMZ infetta su Internet per limitare la propagazione del malware e proteggere la rete interna dall'attaccante. Unendo queste due azioni, possiamo ipotizzare un approccio integrato per affrontare la minaccia in corso. In particolare, potremmo:

- Implementare il WAF per proteggere l'applicazione web e filtrare il traffico in arrivo.
- Isolare la DMZ infetta su Internet per impedire all'attaccante di accedere alla rete interna e limitare la diffusione del malware.

In questo modo, stiamo combinando le misure preventive (WAF) con le azioni di risposta agli incidenti (isolamento) per garantire una protezione completa dell'ambiente aziendale. Questa integrazione aiuta a mitigare il rischio di compromissione della sicurezza e a mantenere la continuità operativa dell'azienda.

5. Implementiamo alcune soluzioni aggiuntive per migliorare la sicurezza della rete:

- Servizio di monitoraggio avanzato: Investire in un servizio di monitoraggio avanzato per rilevare e rispondere tempestivamente agli attacchi, integrando sistemi di rilevamento delle minacce e di analisi del comportamento anomalo. Ad esempio un ottima soluzione potrebbe essere l'implementazione di IPS e IDS

- Software anti-malware avanzato: Acquistare e implementare un software anti-malware avanzato per proteggere l'intera rete, incluso il traffico in arrivo e in uscita, e fornire una difesa contro le minacce informatiche. Ad esempio WAF e EDR

- Formazione sulla sicurezza: Condurre sessioni di formazione sulla sicurezza per educare il personale sulla consapevolezza delle minacce e delle migliori pratiche di sicurezza informatica, riducendo così il rischio di compromissioni causate da errori umani. Ad esempio cosa fare e assolutamente cosa non fare in caso di problemi

riguardanti la rete o problemi con dispositivi, e inoltre sessioni per la sicurezza riguardo il phishing, ecc

- Aggiornamento delle politiche di sicurezza: Rivedere e aggiornare le politiche di sicurezza della rete per garantire che siano allineate alle migliori pratiche e alle nuove minacce emergenti.

Queste misure aggiuntive possono contribuire a rafforzare la sicurezza della rete e a mitigare i rischi di futuri attacchi informatici, fornendo una protezione più completa e sofisticata.

BONUS

- Performance Booster:

Questo programma presenta una seria minaccia poiché consente agli attaccanti di creare un utente nascosto con privilegi di PowerShell, potenzialmente compromettendo la sicurezza dei nostri dispositivi e dell'azienda. Per evitare che situazioni simili si verifichino in futuro, è fondamentale seguire alcuni passaggi precauzionali. Prima di tutto, è importante non scaricare o installare software non autorizzato, specialmente senza il consenso dell'azienda. In secondo luogo, anche se ci viene dato il permesso di scaricare software, dobbiamo verificare attentamente la sua provenienza e assicurarci di ottenere solo versioni aggiornate da fonti attendibili.

- Microsoft Edge:

Un'altra minaccia emersa riguarda una vulnerabilità in una specifica versione di Microsoft Edge, che potrebbe consentire a un attaccante di accedere al nostro sistema. Per prevenire futuri attacchi simili, è consigliabile eseguire l'aggiornamento a una versione più recente del browser o, se possibile, disabilitare direttamente il programma. Inoltre, è essenziale mantenere sempre una stretta vigilanza sulle potenziali vulnerabilità dei software utilizzati e adottare al più presto l'applicazione di patch di sicurezza.

Possiamo concludere dicendo che con una combinazione di consapevolezza, attenzione e prontezza d'azione, possiamo ridurre significativamente il rischio di subire attacchi informatici e proteggere l'integrità dei nostri sistemi e dei nostri dati aziendali.