INCIDENT RESPONSE

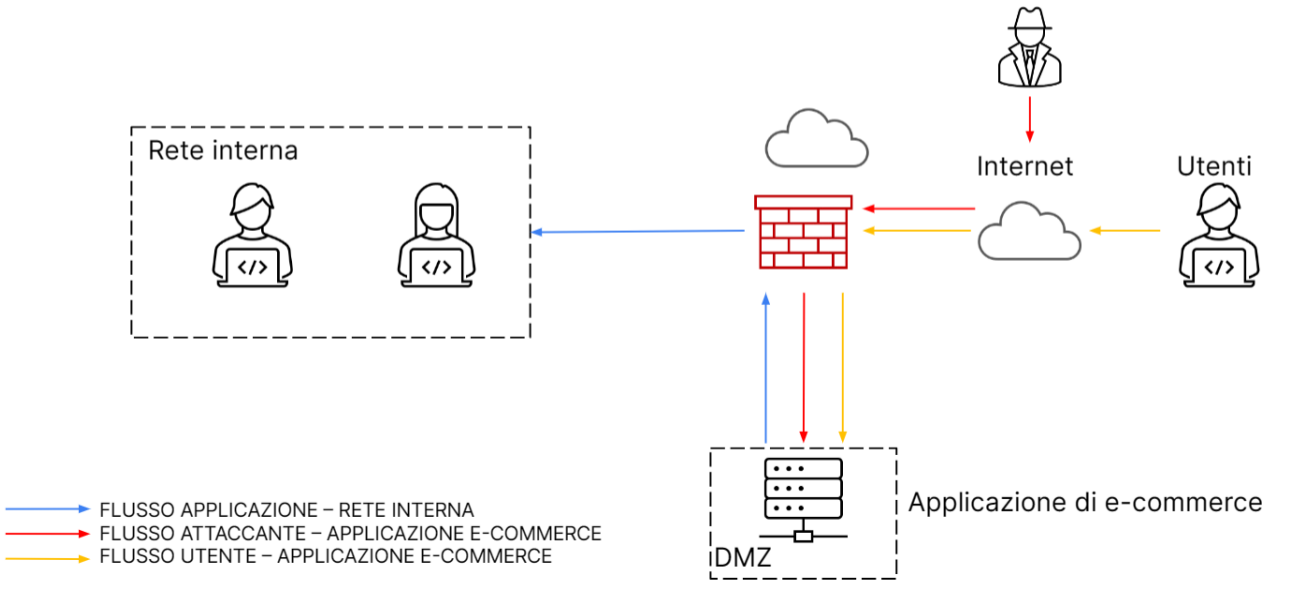
Malware Analysis - Intro e analisi statica basica

PROGETTO

TRACCIA:
Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti

1. **Azioni preventive**: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web Modificate la figura in modo da evidenziare le implementazioni
2. **Impatti sul business**: l'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per 10 minuti. Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media ogni minuto gli utenti spendono 1.500 euro sulla piattaforma di e-commerce. Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica
3. **Response**: l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostra rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide 2 con la soluzione proposta
4. **Soluzione completa**: unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)
5. **Modifica 'più aggressiva' dell'infrastruttura** (se necessario/facoltativo magari integrando la soluzione al punto 2)

ARCHITETTURA DI RETE:
L'applicazione di e-commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma. La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.



1. Azioni preventive

Quali azioni preventive si potrebbero implementare per difendere l'applicazione Web. Modificate la figura in modo da evidenziare le implementazioni

I) Utilizzare la Web Application Firewall

Ogni azienda che gestisce un server o il proprio sito aziendale, si trova di fronte allo stesso problema: i computer che forniscono servizi web devono essere disponibili via Internet. Allo stesso tempo, i dipendenti della LAN (Local Area Network) hanno bisogno di un accesso rapido a queste risorse. Operare all'interno della stessa rete non è una soluzione, in quanto è molto rischioso. I server DNS, web, mail o proxy che richiedono l'accesso alle reti pubbliche offrono agli hacker ampie opportunità di lanciare un attacco. Se uno di questi, è collegato direttamente alla LAN, c'è il rischio che un server danneggiato possa infliggere danni all'intero server aziendale.

DMZ, talvolta indicata anche come 'rete perimetrale', offre una soluzione a questo dilemma esternalizzando i server vulnerabili.

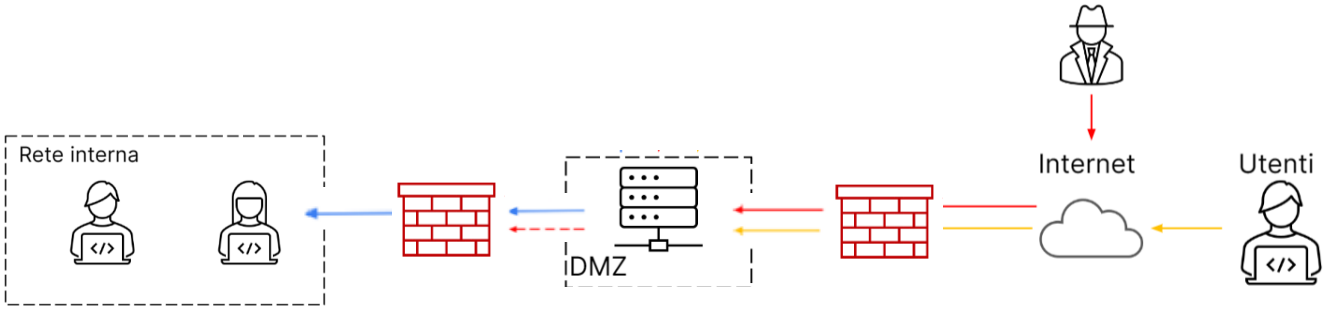
Tra le azioni preventive che si potrebbero implementare per difendere l'applicazione Web da attacchi SQLi e XSS, vi è sicuramente quella di implementare delle misure di sicurezza con l'aggiunta di un Web Application Firewall (WAF), dei dispositivi di sicurezza dedicati a proteggere le applicazioni da attacchi quali SQL injection e XSS. I WAF a differenza dei firewall tradizionali, che si focalizzano principalmente sul traffico a livello di rete, i WAF si focalizzano per lo più sul traffico a livello applicativo.

Il WAF infatti, è una difesa di livello 7 del protocollo (nel modello OSI) e non è progettato per difendersi da tutti i tipi di attacchi. Questo metodo di mitigazione degli attacchi fa solitamente parte di una serie di strumenti che insieme creano una difesa olistica contro una serie di vettori di attacco.
Mentre un server proxy protegge l'identità di un computer client utilizzando un intermediario, un WAF è un tipo di proxy inverso, che protegge il server esposto, facendo in modo che i client passino attraverso il WAF prima di raggiungere il server.

Un WAF opera attraverso un set di regole spesso denominate criteri che hanno lo scopo di proteggere dalle vulnerabilità nell'applicazione filtrando il traffico dannoso.

II) Usare una struttura differente di rete

Un altra azione è quella di implementare due firewall in una diversa struttura di rete: per poter proteggere in modo affidabile le reti aziendali dagli attacchi provenienti dalle reti pubbliche (WAN). Questa configurazione può utilizzare componenti hardware autonomi o software firewall installati su un router. Il firewall esterno protegge la DMZ dalle reti pubbliche, mentre il firewall interno si sposta tra la DMZ e la rete aziendale.
E sebbene le DMZ si trovino fisicamente all'interno della stessa azienda, non sono direttamente collegate a nessuno dei dispositivi della rete locale.



III) Implementare un gateway sicuro

Nel caso in cui un hacker ottenga l'accesso a un file server nella DMZ, potrebbe essere in grado di accedere e scaricare dati sensibili e file dei partner commerciali che vi sono stati inseriti. Anche i file crittografati possono essere a rischio per gli aggressori di alto livello se le chiavi o le password vengono compromesse. Esiste anche una forte probabilità che le credenziali utente, i certificati o qualsiasi altra cosa necessaria per l'autenticazione possano essere mantenuti nella DMZ, aumentando la vulnerabilità.

A rischio è anche il software di condivisione dei file stesso, in particolare quando è possibile accedervi dall'interno della DMZ. Ad esempio, supponiamo che un utente malintenzionato ottenga l'accesso al tuo territorio creando un account utente "backdoor" in un server SFTP tramite la sua console di amministrazione. Questo account utente potrebbe apparentemente apparire come "legittimo" e consentire all'hacker l'opportunità di rubare file di dati sensibili. I log di controllo possono anche essere manipolati se sono archiviati nella DMZ, consentendo all'utente malintenzionato di cancellare qualsiasi traccia in cui si trovasse

Con un gateway sicuro DMZ, i problemi di sicurezza vengono risolti consentendo a un'organizzazione di spostare la condivisione di file e altri servizi pubblici dalla DMZ alla rete privata senza dover aprire alcuna porta in entrata. Questo approccio mantiene i file di dati al sicuro nella rete privata poiché non è più necessario eseguire la gestione temporanea nella rete perimetrale.

I servizi di condivisione di file possono essere mantenuti sicuri e protetti all'interno della rete privata, senza esporre i dati alla DMZ.

2. Impatti sul business:

L'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per 10 minuti. Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media ogni minuto gli utenti spendono 1.500 euro sulla piattaforma di e-commerce. Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica

SVOLGIMENTO:
Considerando che l'applicazione rimane irraggiungibile per 10 minuti, e considerando che gli utenti spendono mediamente 1.500 euro al minuto sulla piattaforma e-commerce, allora:

€1.500 x 10(minuti) = €15.000

Nello specifico, a valle dell'identificazione dei rischi e delle probabilità che essi si verifichino, possiamo utilizzare i parametri del Business Impact Analysis (BIA), in particolare da un punto di vista quantitativo:

ASSET VALUE

AV = €1.500 x 1.440min = €2.160.000

rendita al minuto x minuti totali in 24h = Valore dell'asset

EXPOSURE FACTOR

EF = 10min/1.440min = 0.00694444%

minuti totali di irraggiungibilità del sito / minuti totali in 24h = Percentuale di esposizione

---

SINGLE LOSS EXPECTANCY

SLE = €2.160.000 x 0.00694444% = €14.999,99 ⇒ €15.000 (arrotondato)

Valore dell'asset x Percentuale di esposizione = Perdita subita al verificarsi dell'evento

In questo caso il livello di criticità è media, in quanto la compagnia non riesce ad erogare alcuni dei servizi critici o parte di essi ad un sottoinsieme limitato di utenti. La compagnia si aspetta quindi, un impatto economico piuttosto notevole, pari a 15.000 euro.

Pertanto, le azioni preventive che potremmo applicare a questa problematica potrebbero essere:

- Implementazione di un Firewall che funga da barriera di scansione del traffico tra le reti.
- Implementazione di tool UEBA (User and Entity Behavior Analytics), vale a dire software sviluppati per profilare il comportamento degli utenti al fine di identificare eventuali attività sospette..
- Segmentazione della rete e dei sistemi in sottoreti con controlli e protocolli di sicurezza che consentirebbero di facilitare l'identificazione di attività sospette all'interno della rete e dei sistemi;
- Strumenti di cattura del traffico continuativa (ad esempio tramite Wireshark o altri software) dove il team CSIRT, una volta identificato l'incidente di sicurezza, potrà rimuovere tali minacce basate sul Web, bloccando il traffico anomalo;
- Distribuire il traffico su un'ampia rete di server: affidarsi a più server distribuiti rende difficile per un hacker attaccare tutti i server contemporaneamente. Se un utente malintenzionato lancia un DDoS riuscito su un singolo dispositivo hosting, gli altri server rimangono inalterati e assumono traffico aggiuntivo finché il sistema preso di mira, non torna online. Quando parliamo di server infatti, possiamo introdurre il concetto di ridondanza (applicato a tutti gli asset critici) che trova la sua applicazione nella cosiddetta «failover cluster», dove con 'cluster' si intende un gruppo di computer (chiamati anche nodi del cluster) che svolgono principalmente lo stesso ruolo e che sono anche sincronizzati tra loro. Dunque secondo questa logica, il failover cluster permette l'operatività dell'intero sistema anche a fronte di un errore su uno dei due server: quando il server smette di funzionare, il secondo server lo sostituisce come server attivo tramite un processo chiamato per l'appunto 'failover'
- Maggiore sicurezza sugli endpoint che garantisce che gli endpoint di rete (desktop, laptop, dispositivi mobili, ecc.) non diventino un punto di ingresso per attività dannose.
- Utilizzare siti web HTTPS: con protocolli di crittografia più sicuri.

3. Response:

L'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostra rete, mentre non siete interessati a rimuovere l'accesso da parte l'accesso da parte dell'attaccante alla macchina infettata.

FASE DI CONTENIMENTO:

La prima azione da fare per contenere gli impatti, è isolare il sistema, rispetto al resto della rete, per impedire al malware di propagarsi su altri nodi. Questa soluzione:

- permette comunque all'attaccante di avere accesso alla Web Application
- permette all'azienda non solo di poter analizzare il malware ma conseguentemente anche di procedere con la fase di rimozione e recupero.

L'isolamento consiste nella disconnessione del sistema infetto dalle rete, in modo da restringere ulteriormente l'accesso alla rete interna da parte dell'attaccante. In questo modo:

- blocchiamo l'accesso alla DMZ
- continuiamo a garantire la continuità del servizio e-commerce.

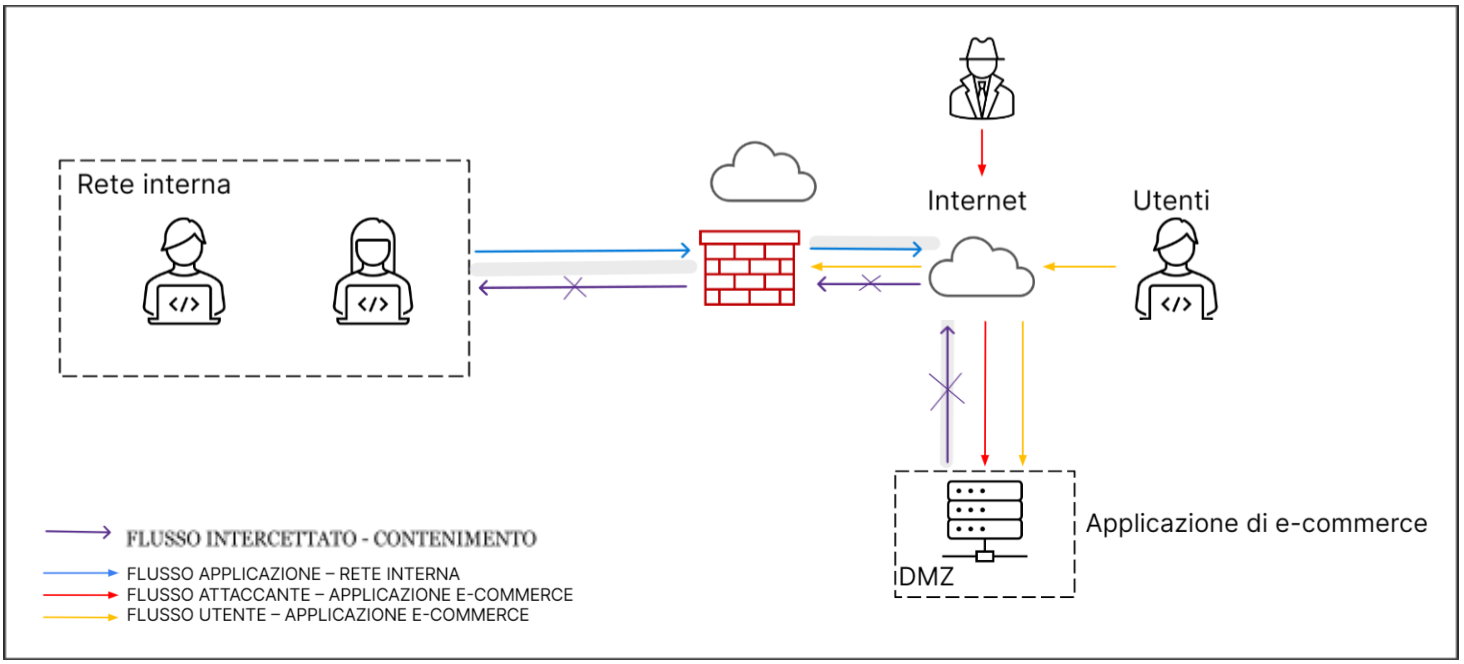
FASE DI RIMOZIONE

Pertanto, il team CSIRT, a seguito delle attività di contenimento, passerà alla fase di rimozione dell'incidente con l'obbiettivo di eliminare tutte le attività, componenti, processi che restano dell'incidente all'interno della rete o sui sistemi.

FASE DI RECUPERO

Nella fase di recupero (che include recupero dati, informazioni perse, revisione delle politiche firewall, IPS e IDS oppure l'aggiornamento delle firme antivirus) vi è l'obbiettivo di evitare che lo stesso attacco possa capitare nuovamente. Infatti in caso di compromissione di sistemi, server e host, dovrebbero considerarsi inaffidabili e quindi conseguentemente ripuliti a fondo prima di essere nuovamente riutilizzati. A tal proposito si utilizzano le tecniche di «reconstruction» o «rebuildingr»

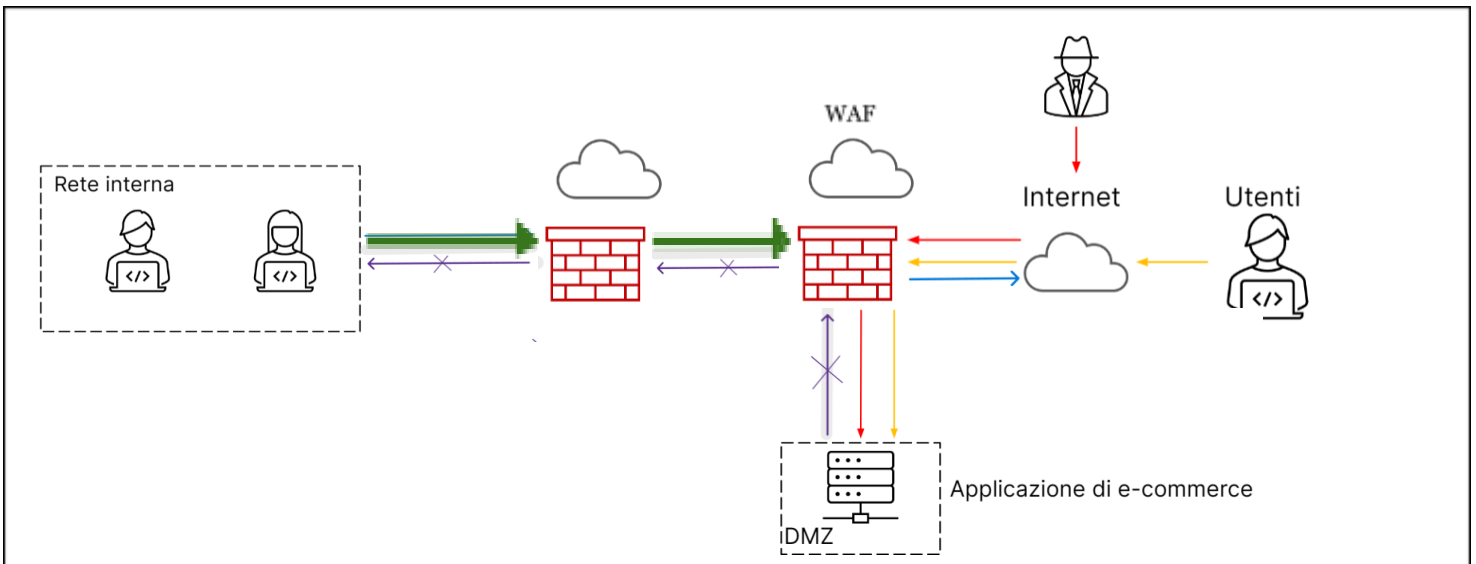
- ➔ reconstruction: si intendono tutte quelle attività mirate a recuperare quelle parti ancora affidabili di un sistema compromesso;
- ➔ rebuilding: riguardano le attività che mirano a ricostruire **interamente** un sistema impattato considerato **non più affidabile**



4. Soluzione completa:

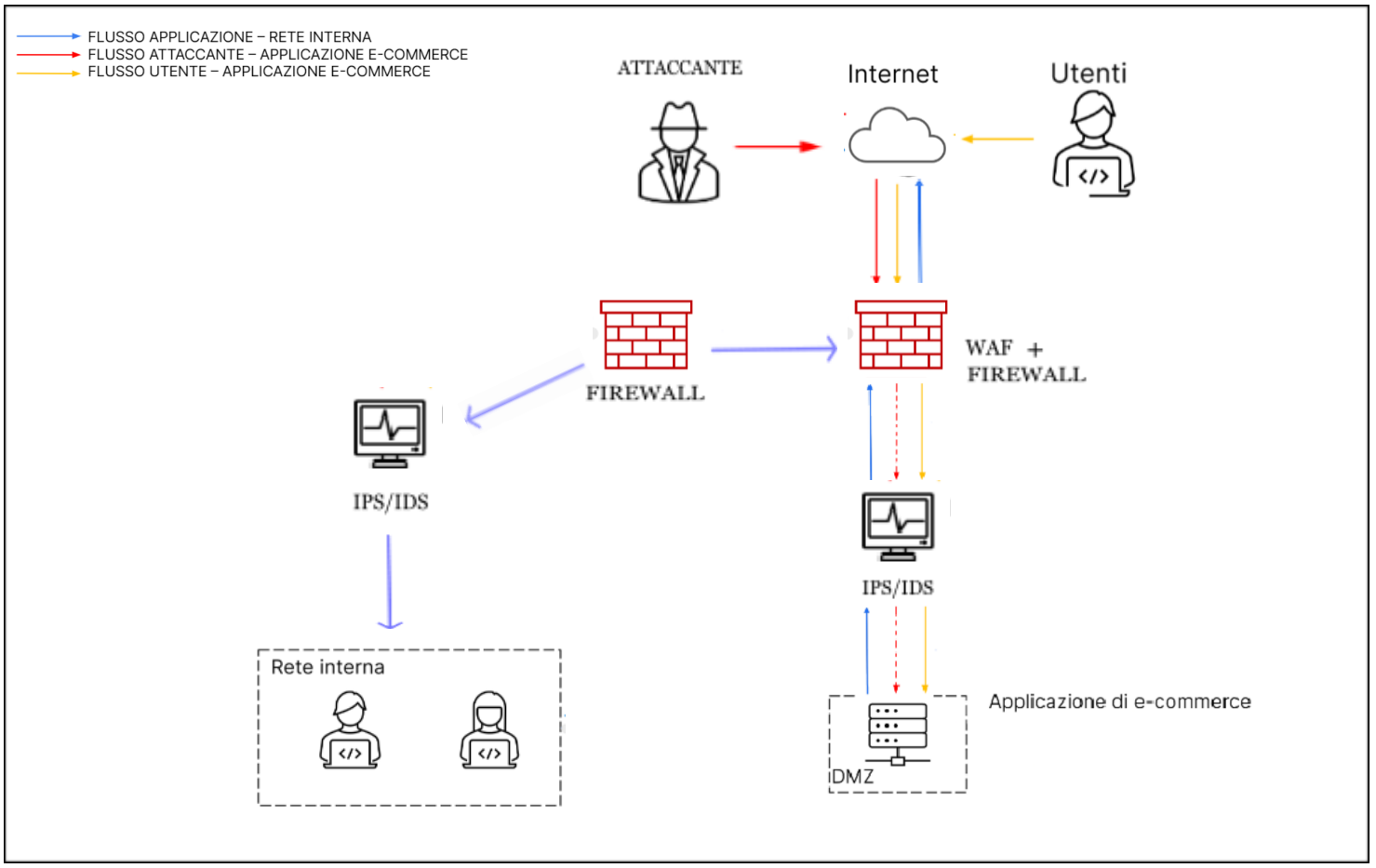
Unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)

Di seguito verrà quindi illustrata una soluzione completa unendo l'azione preventiva e quella di response



Il server DMZ viene isolato dalla rete interna perché infettato dal malware, quindi inserendo un WAF, riusciremo a proteggere la Web Application da eventuali attacchi SQLi e XSS che in questo caso, non andrebbero ad impattare la rete interna.

5. Modifica ‘più aggressiva’ dell’infrastruttura



IPS/IDS i sistemi di prevenzione e rilevamento delle intrusioni servono a individuare preventivamente potenziali attacchi alle reti e alle macchine.

La nostra struttura di rete è stata riorganizzata in modo tale da proteggere la rete interna da eventuali attacchi alla DMZ. La separazione dei servizi critici dalla rete interna infatti, permetterebbe ai sistemi di prevenzione e rilevamento delle intrusioni (IPS/IDS) a individuare preventivamente potenziali attacchi alle reti e alle macchine. Mentre il sistema di rilevamento si occupa solo del monitoraggio di specifiche eventi di sicurezza in tempo reale alla ricerca di ‘anomalie sospette”, il sistema di prevenzione, supporta anche le azioni automatiche per fermare la potenziale intrusione.