PROGETTO
S9 L5

Davide Andreozzi

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 da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato?
   Modificate la figura in modo da evidenziare le implementazioni

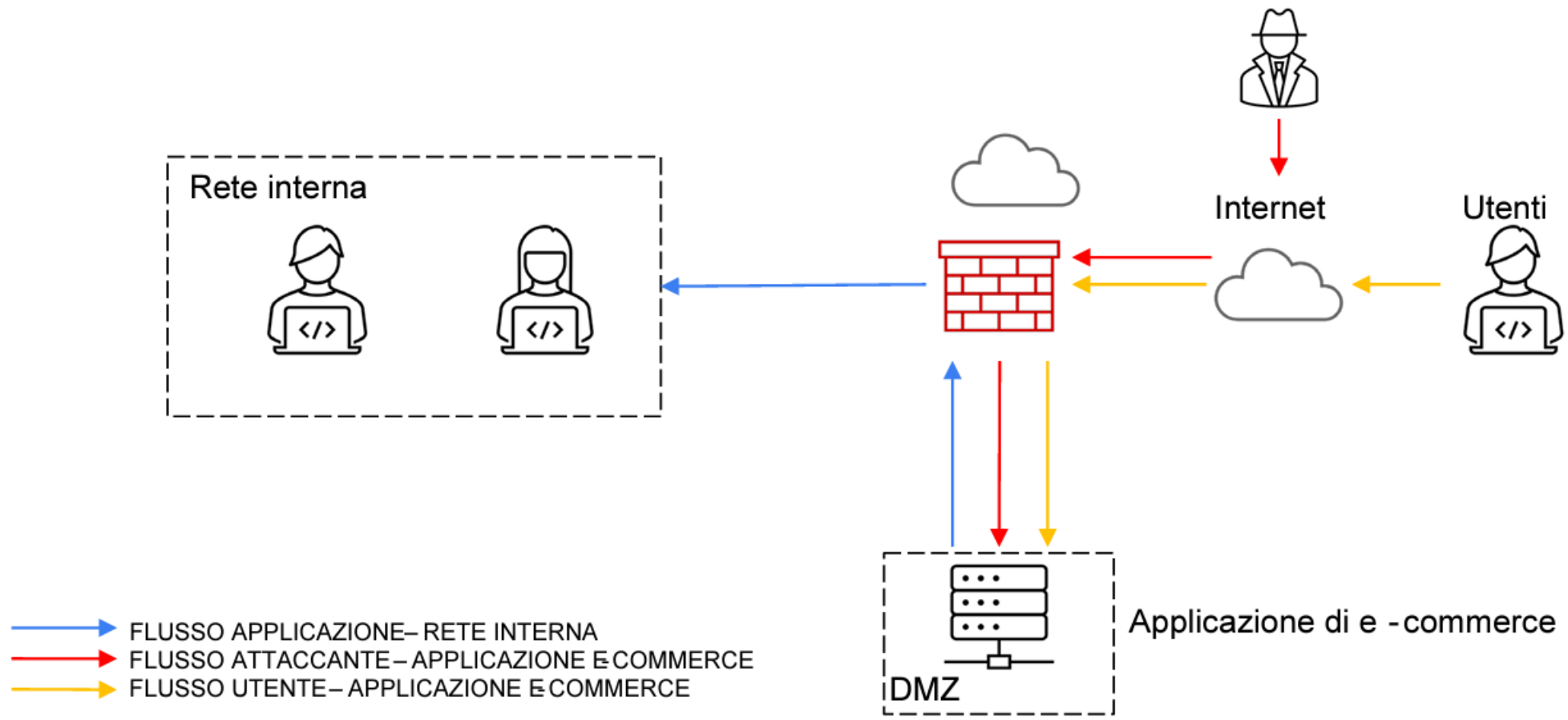
2. **Impatti sul business** : l'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per **10 minuti** .
   Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media **ogni minuto gli utenti spendono 1.500 €** 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 vostre 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 .

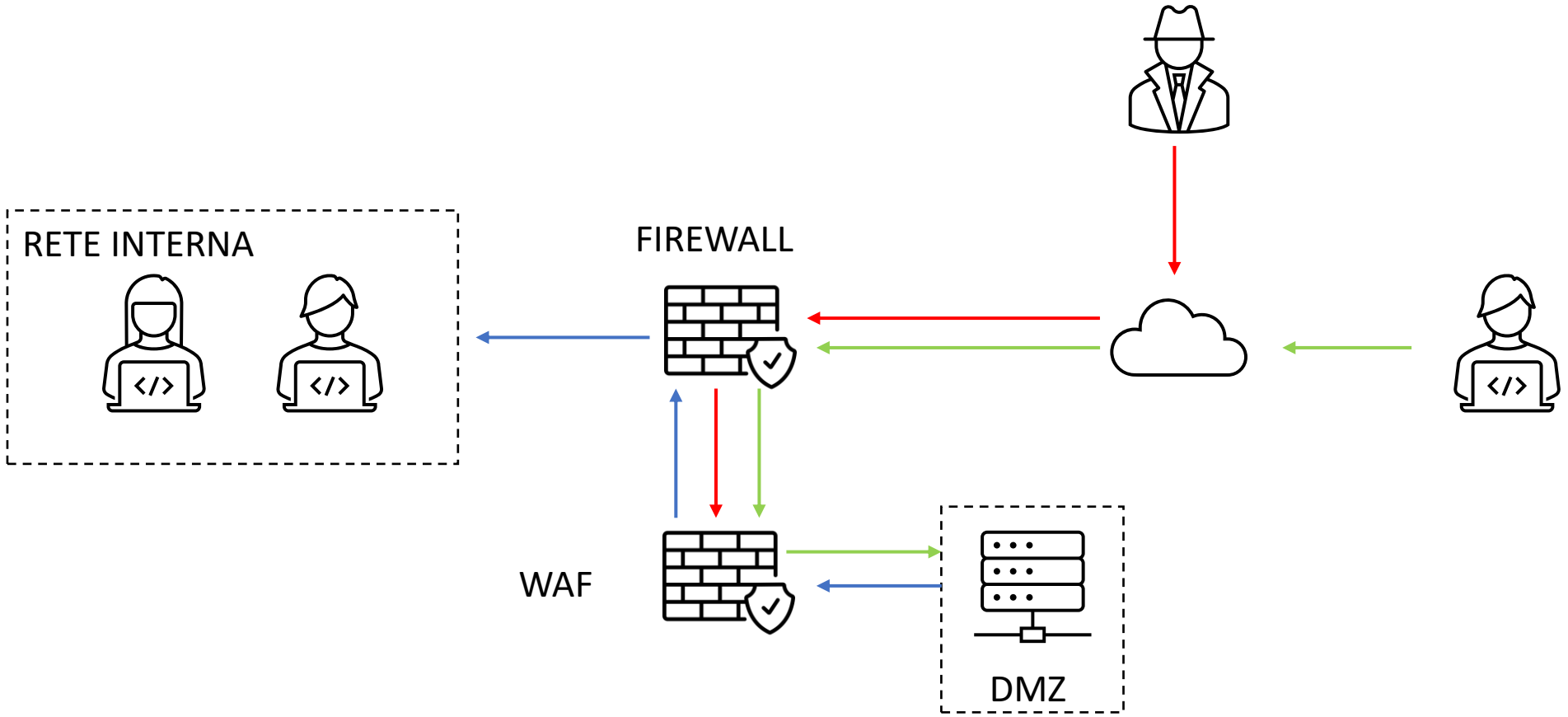
4. **Soluzione completa** : unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)

5. **Modifica «più aggressiva» dell'infrastruttura:** integrando eventuali altri elementi di sicurezza **(se necessario/facoltativo magari integrando la soluzione al punto 2)**

Traccia – Architettura di rete



Azioni preventive – Aggiunta di un WAF



Azioni preventive – Aggiunta di un WAF

E’ stato aggiunto nella figura precedente un Web Application Firewall che ci aiuterà a proteggere la rete da attacchi di tipo SQLi o XSS.

Il WAF va a filtrare e mitigare infatti questo tipo di attacchi attraverso il filtraggio, la validazione degli input, il monitoraggio e il riconoscimento di attacchi già noti.

E’ importante notare che un WAF non è una soluzione completa per la sicurezza delle applicazioni web e dovrebbe essere utilizzato insieme ad altre misure di sicurezza, ad esempio:

- Segmentazione della rete
- Aggiornamenti e Patching
- IPS/IDS

Impatti sul Business – Calcolo SLE

Per calcolare il danno al business possiamo utilizzare il concetto di SLE (Single Loss Expectancy), che rappresenta la perdita economica attesa in caso di accadimento di un singolo evento.

AV (Asset Value)= Sarà il valore dell'asset, in questo caso il valore dell'asset sarà il guadagno in un'minuto che è pari a € 1.500

EF (Exposure Factor)= E' la percentuale di esposizione dell'asset «perso» a causa del verificarsi di un evento, in questo caso essendo il server offline possiamo affermare che la % è del 100%. Quindi:

SLE= 1.500 * 10(minuti) = 15.000 €

<u>In base ai dati possiamo calcolare una impatto economico sul business di € 15.000</u>

Impatti sul Business – Azioni preventive

Considerando il danno possiamo fare una riflessione sulle azioni preventive che possono essere adoperate per evitare questo tipo di problema

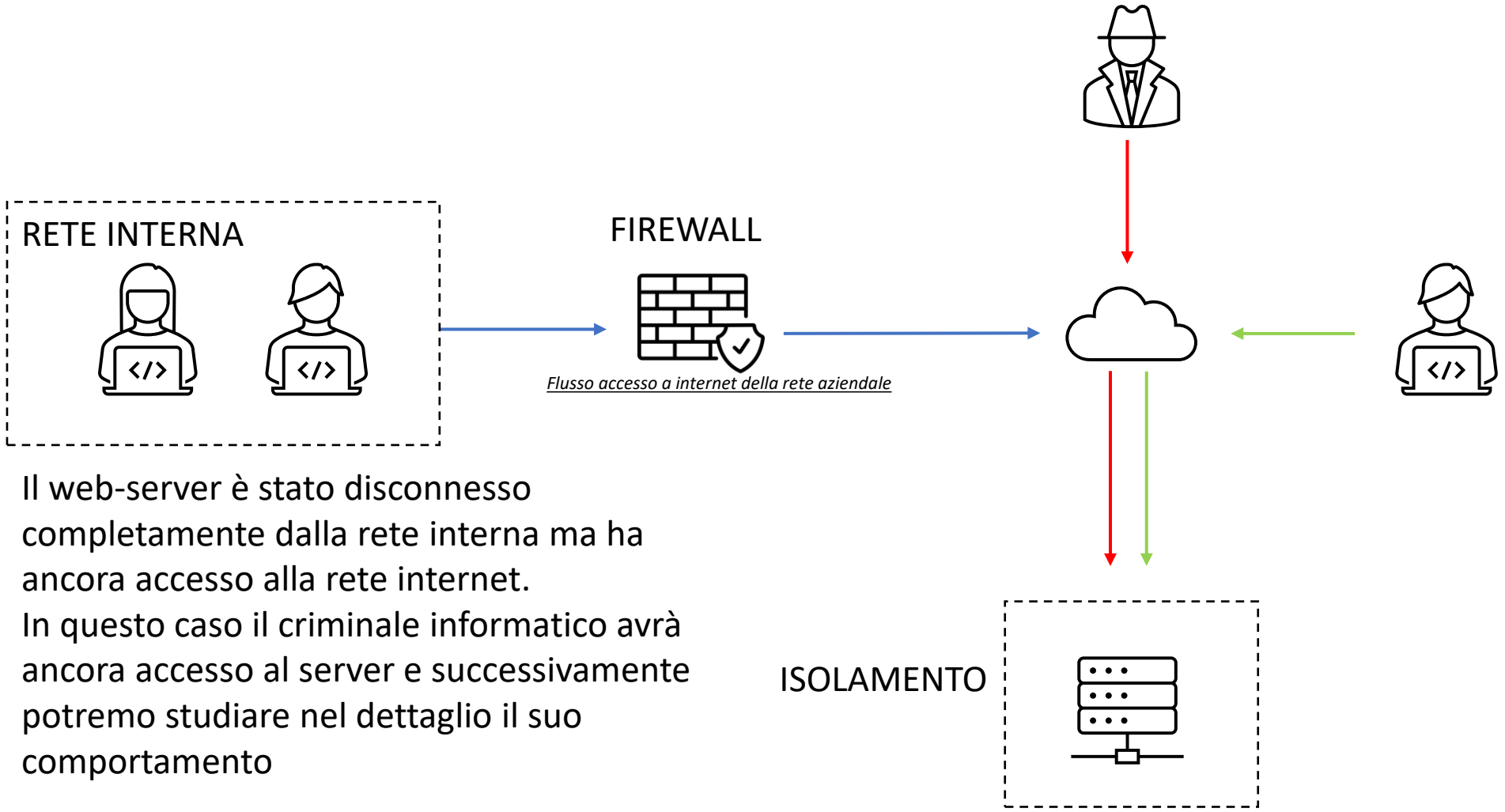
1. Adozione del «**Failover Cluster**»

   E’ una soluzione di Ridondanza, il failover cluster include due o più server che fanno «lo stesso lavoro», se il server per un’eventuale motivo smette di funzionare il secondo server si sostituisce al primo in modo che il servizio possa continuare senza problemi.
   In sostanza il failover cluster è un sistema automatico per garantire che il servizio resti attivo andando a «promuovere» il secondo dispositivo a nodo primario.

2. Configurazione di servizi **Cloud**

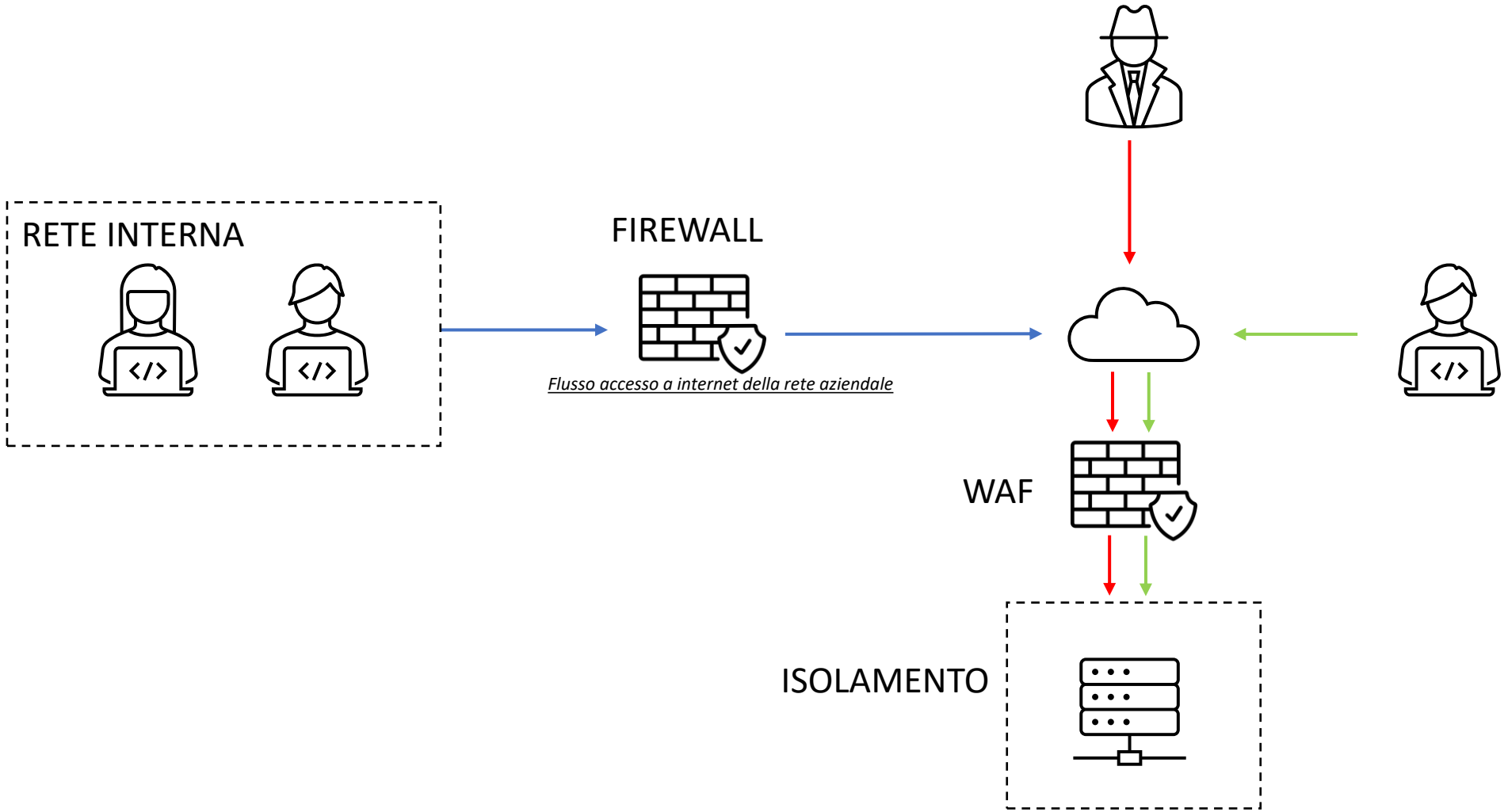
   Usare una soluzione tipo «cloudflare» che è utile contro attacchi DDoS. In questo caso il traffico Web dei clienti viene instradato attraverso la loro rete, che può identificare e bloccare le minacce prima che raggiungano il server di destinazione.

Response – Isolamento del web-server

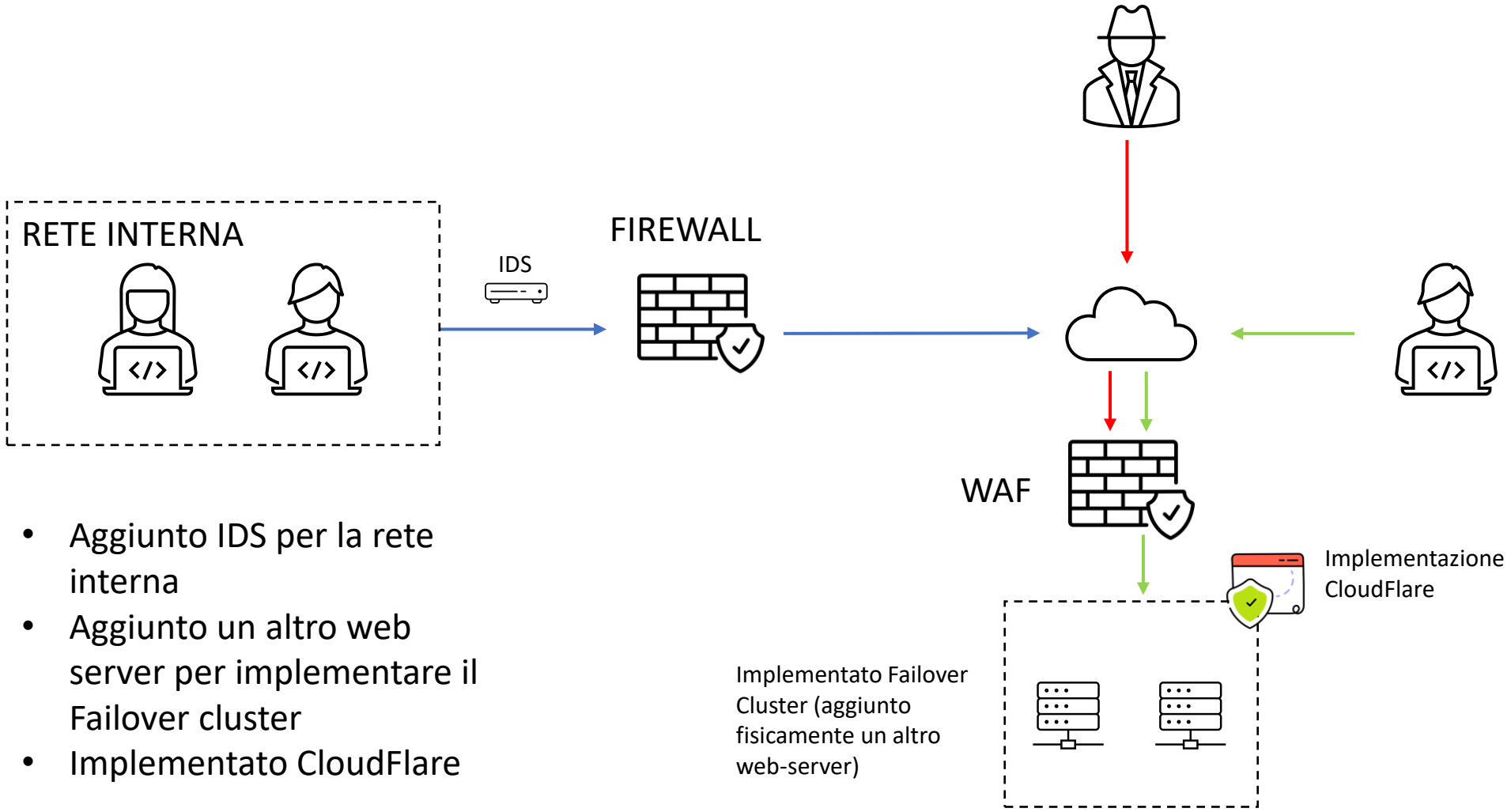


Il web-server è stato disconnesso completamente dalla rete interna ma ha ancora accesso alla rete internet.
In questo caso il criminale informatico avrà ancora accesso al server e successivamente potremo studiare nel dettaglio il suo comportamento

Soluzione completa – Unione soluzione 1+3



Soluzione aggressiva



- Aggiunto IDS per la rete interna
- Aggiunto un altro web server per implementare il Failover cluster
- Implementato CloudFlare

Bonus

Analizzare le seguenti segnalazioni caricate su anyrun e fare un piccolo report di ciò che si scopre relativo alla segnalazione dell'eventuale attacco spiegando ad utenti e dirigenti la tipologia di attacco e come evitare questi attacchi in futuro:

https://app.any.run/tasks/8e6ad6d9-4d54-48e8-ad95-bfb67d47f1d7/

https://app.any.run/tasks/60b9570f-175b-4b03-816b-a38cc2b0255e/

Bonus

Gli attacchi rilevati sono casi di malware.

Questo tipo di attacco coinvolge il download e l'esecuzione di software dannoso sui sistemi informatici dell'azienda. Una volta infettati da malware, dei potenziali attaccanti possono leggere configurazioni di sistema, sfruttare vulnerabilità di particolari app per ottenere privilegi particolari, ottenere accesso completo al sistema tramite "privilege escalation".

I malware possono essere distribuiti attraverso vari strumenti, come allegati mail, siti web compromessi o download di file.

Spesso possono sembrare dei programmi legittimi e/o comunque che vadano a compiere azioni legittime, ad esempio il miglioramento delle prestazioni di un dispositivo come il caso visto su anyrun, il programma una volta avviato ha accesso ai registri di sistema, può andare a modificarli, ottenere accessi da amministratore e leggere i dati sul dispositivo.

Bonus – Come proteggersi?

1. Aggiornamenti del Software: Mantenere sempre aggiornati i software e sistemi operativi. Gli aggiornamenti spesso includono patch di sicurezza
2. Formazione del Personale sul Phishing: Il phishing è una delle tecniche più comuni utilizzate per distribuire malware.
3. Politiche per l'Accesso a Siti Autorizzati: politiche di accesso che vadano a limitare l'accesso a siti web autorizzati.
4. Gestione dei Privilegi: Limitate i privilegi di accesso dei dipendenti solo alle risorse e alle funzionalità necessarie per svolgere il proprio lavoro.
5. Backup Regolari: Effettuare backup regolari dei dati e conservarli in un luogo sicuro e isolato dalla rete aziendale.