



CDM S.R.L.

PROGETTO S9L5

EPICODE - CS0124

Presented by:

Oliviero Camarota

Marco De Falco

Alessandro Marasca



INDICE

03

Traccia

04

Azioni preventive
XSS

05

Azioni preventive
SQLI

06 - 07

Impatti sul business
e prevenzioni

08

Response

09

Soluzione completa

10 - 11

Bonus

12

Il nostro Team

13

Ringraziamenti

TRACCIA

Con riferimento alla figura a lato, rispondere ai seguenti quesiti.

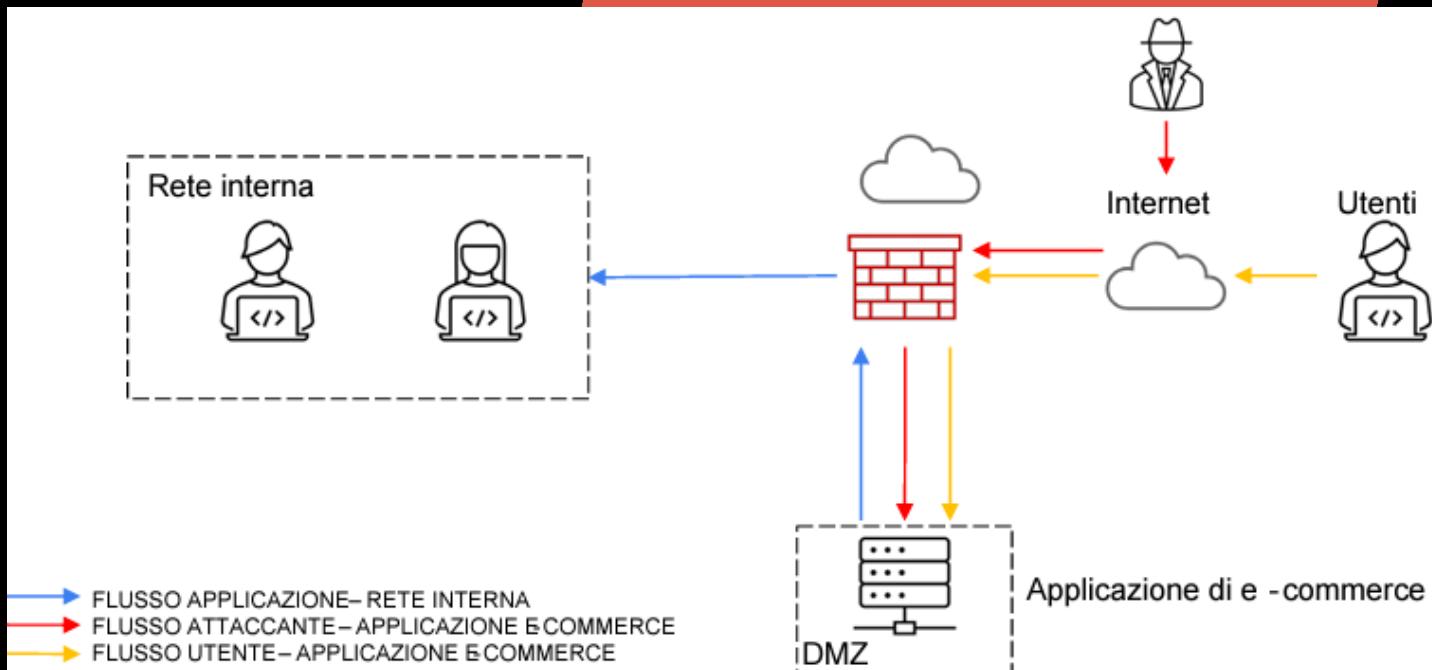
1. Azioni preventive: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni

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)



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/>

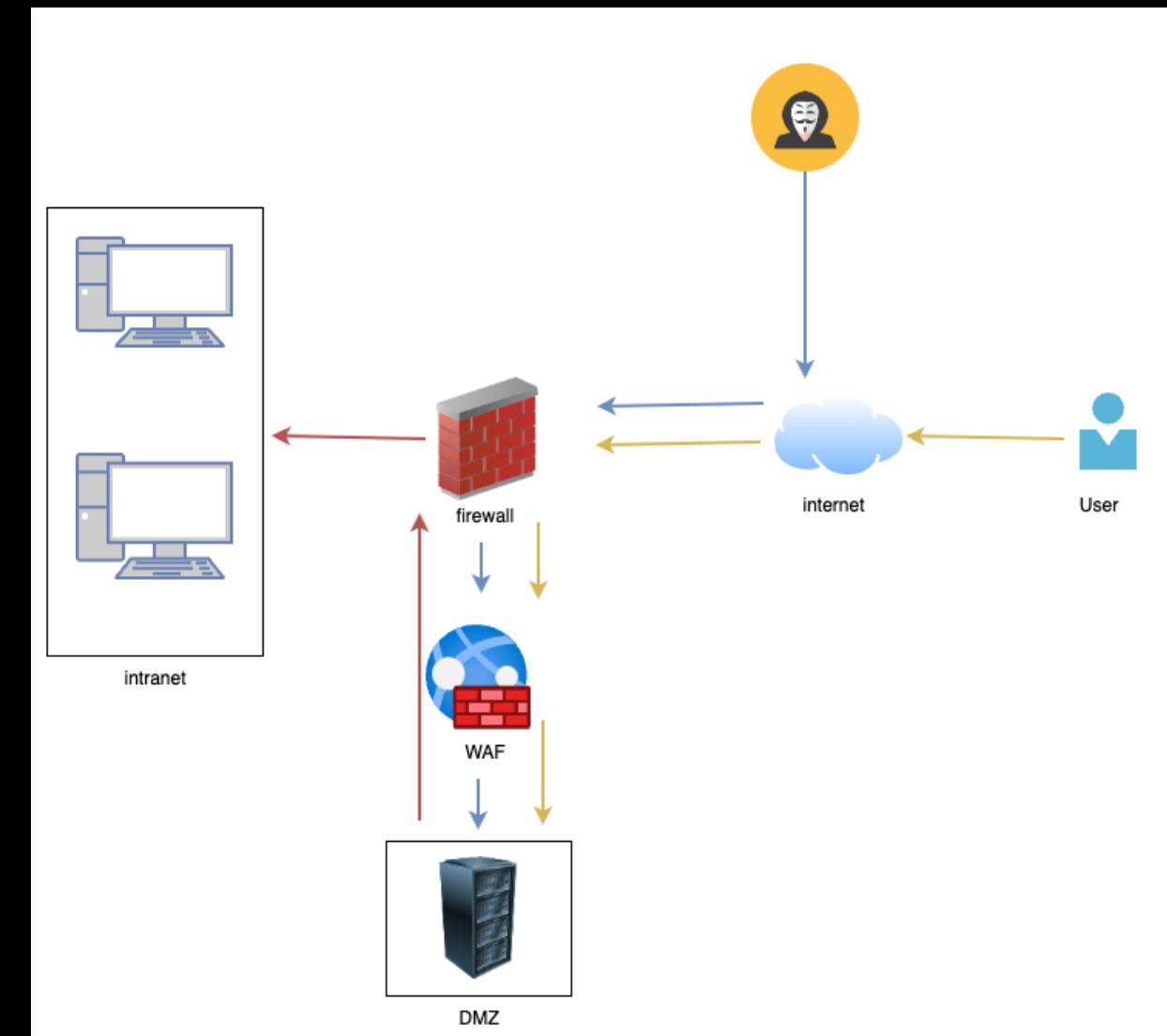
<https://app.any.run/tasks/60b9570f-175b-4b03-816b-a38cc2b0255e/>

AZIONI PREVENTIVE XSS

Un attacco **XSS** (Cross-Site Scripting) è una vulnerabilità web che consente a un attaccante di iniettare **script dannosi** (solitamente JavaScript) nelle pagine web visualizzate da altri utenti: questo consente all'attaccante di eseguire azioni malevoli sul browser degli utenti che visualizzano la pagina compromessa, come il furto di cookie di sessione, il reindirizzamento a pagine fraudolente o l'inserimento di contenuti dannosi.

Per potersi difendere da attacchi di tipo XSS è possibile applicare le seguenti **azioni preventive**:

- O1** **Escape HTML:** per convertire caratteri utilizzati spesso negli script (come <, >, ", & ...) nelle loro corrispettive entità HTML per evitare l'esecuzione di script malevoli.
- O2** **Utilizzo di protocolli HTTPS:** per far viaggiare i cookie su canali cifrati.
- O3** **Applicazioni di Policy di Sicurezza** tramite Firewall che gestisce il traffico di rete
- O4** **Aggiornamenti frequenti:** per poter godere delle patch più fornite ed essere più preparati ad eventuali attacchi
- O5** **Sanitizzazione degli input** per rendere più difficile l'inserimento di script malevoli.



AZIONI PREVENTIVE SQLI

La **SQL Injection** è un'altra vulnerabilità comune che si verifica quando un'applicazione web non convalida i dati inseriti dall'utente prima di utilizzarli in una query SQL.

Gli attaccanti possono sfruttare questa vulnerabilità per eseguire comandi SQL non autorizzati e ottenere accesso non autorizzato al database sottostante. Ciò può consentire loro di recuperare, modificare o eliminare dati sensibili, o addirittura compromettere l'intero sistema. Le azioni preventive che possiamo attuare sono:

- 01** **Least Privilege Principle:** assegnare solamente i privilegi strettamente necessari al personale che ha accesso ai database
- 02** **Implementazione di un WAF (Web Application Firewall):** che permette di rendere più sicura i servizi web filtrando le richieste HTTP causa degli attacchi SQL
- 03** **Aggiornamenti frequenti:** per poter godere delle patch più fornite ed essere più preparati ad eventuali attacchi
- 04** **Sanitizzazione degli input** per rendere più difficile l'inserimento di script malevoli



IMPATTI SUL BUSINESS E PREVENZIONE

L'applicazione web è stata soggetta a un attacco **DDoS** proveniente dall'esterno, il quale ha comportato l'inaccessibilità dell'applicazione per un periodo di dieci minuti. In virtù del fatto che su questa piattaforma gli utenti mediamente spendono 1500 euro al minuto, l'attacco ha generato un impatto finanziario per l'azienda pari a **15000 euro** ($1500 \text{ euro} \times 10 \text{ min} = 15000 \text{ euro}$).

È pertanto opportuno valutare anche il danno reputazionale arrecato all'immagine aziendale a causa dell'interruzione del servizio, il quale risulta più complesso da quantificare in termini monetari. Tuttavia, qualitativamente, è

plausibile ipotizzare una diminuzione della clientela: nel caso in cui i consumatori non riescano ad accedere al servizio, potrebbero optare per rivolgersi ad altre aziende operanti nel settore dell'**e-commerce**.

L'ATTACCO DDOS

Un attacco **DDoS (Distributed Denial of Service)** è un tipo di attacco informatico in cui un gran numero di dispositivi connessi a Internet, noti come "**botnet**", inviano simultaneamente una grande quantità di richieste di servizio a un determinato sistema, come un server web. L'obiettivo principale di un attacco DDoS è quello di **sovrafficare** il sistema bersaglio con un traffico illegittimo, rendendolo incapace di servire le richieste legittime degli utenti, e quindi rendendo il servizio non disponibile. Nel caso che stiamo analizzando, l'attacco ha comportato il crashing dell'applicazione per dieci minuti, come possiamo quindi prevenire questi tipi di attacco? Nella prossima slide mostriamo alcune azioni preventive da poter attuare

AZIONE PREVENTIVE

Servirsi di un firewall robusto: Configurare e mantenere aggiornato un firewall che possa filtrare il traffico dannoso, bloccando le richieste provenienti da indirizzi IP sospetti o che superano una certa frequenza.

Inserire un sistema di rilevamento degli intrusioni (IDS) e di prevenzione degli intrusioni (IPS): Implementare sistemi di rilevamento e prevenzione delle intrusioni per identificare e mitigare gli attacchi DDoS in corso.

Applicare servizi di mitigazione del DDoS: Utilizzare servizi di mitigazione del DDoS forniti da fornitori specializzati che possono filtrare e instradare il traffico dannoso prima che raggiunga il server, proteggendo così l'infrastruttura di rete.

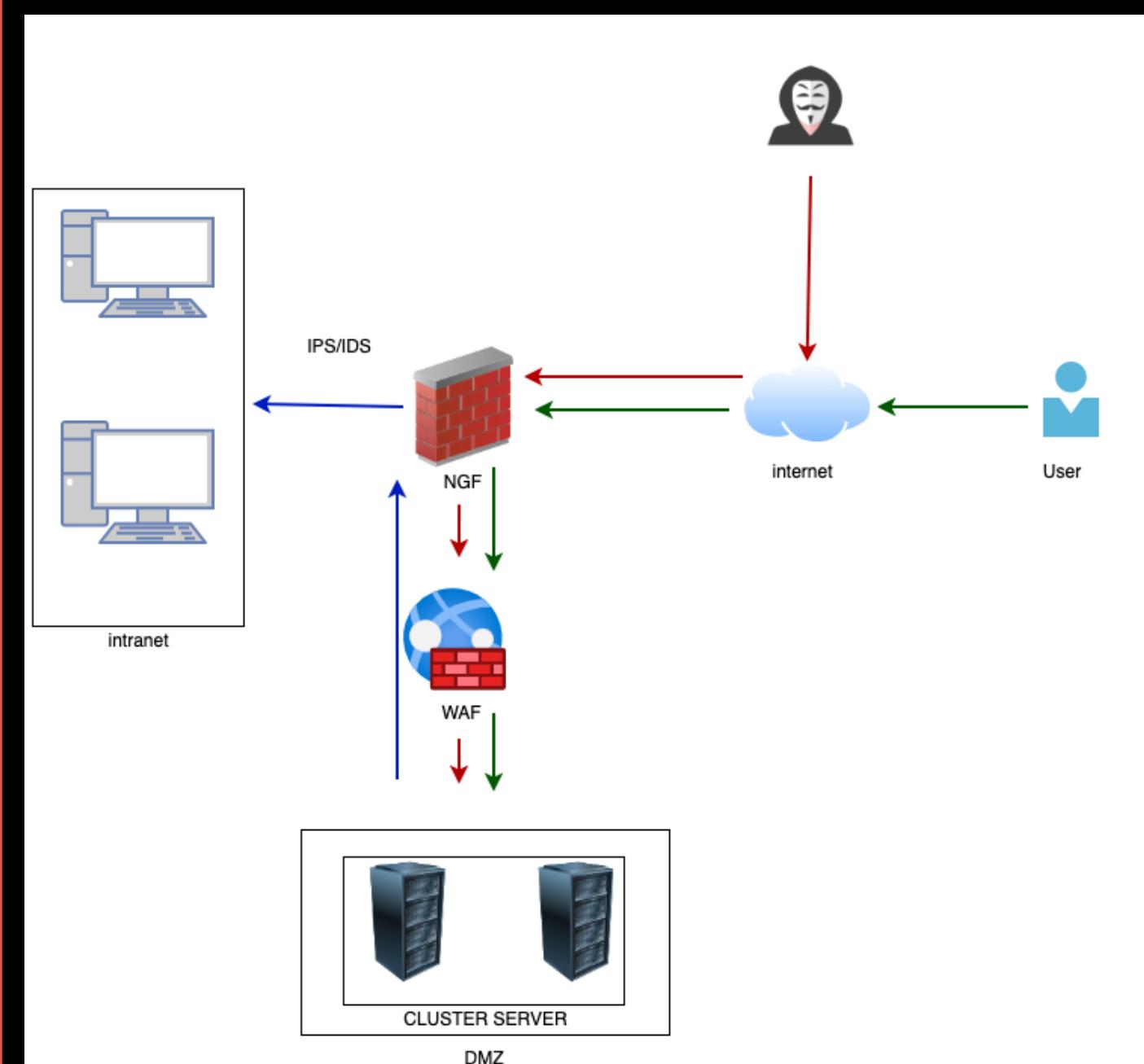
Bilanciare del carico: Distribuire il traffico su più server utilizzando servizi di bilanciamento del carico, in modo che un singolo server non diventi un punto di fallimento durante un attacco DDoS.

Limitare le connessioni: Impostare limiti sul numero di connessioni consentite da un singolo indirizzo IP o da un singolo utente per evitare che un attaccante saturi il sistema con un numero eccessivo di richieste.

Monitorare il traffico: Utilizzare strumenti di monitoraggio del traffico per rilevare anomalie nel flusso di dati e identificare potenziali attacchi DDoS in corso.

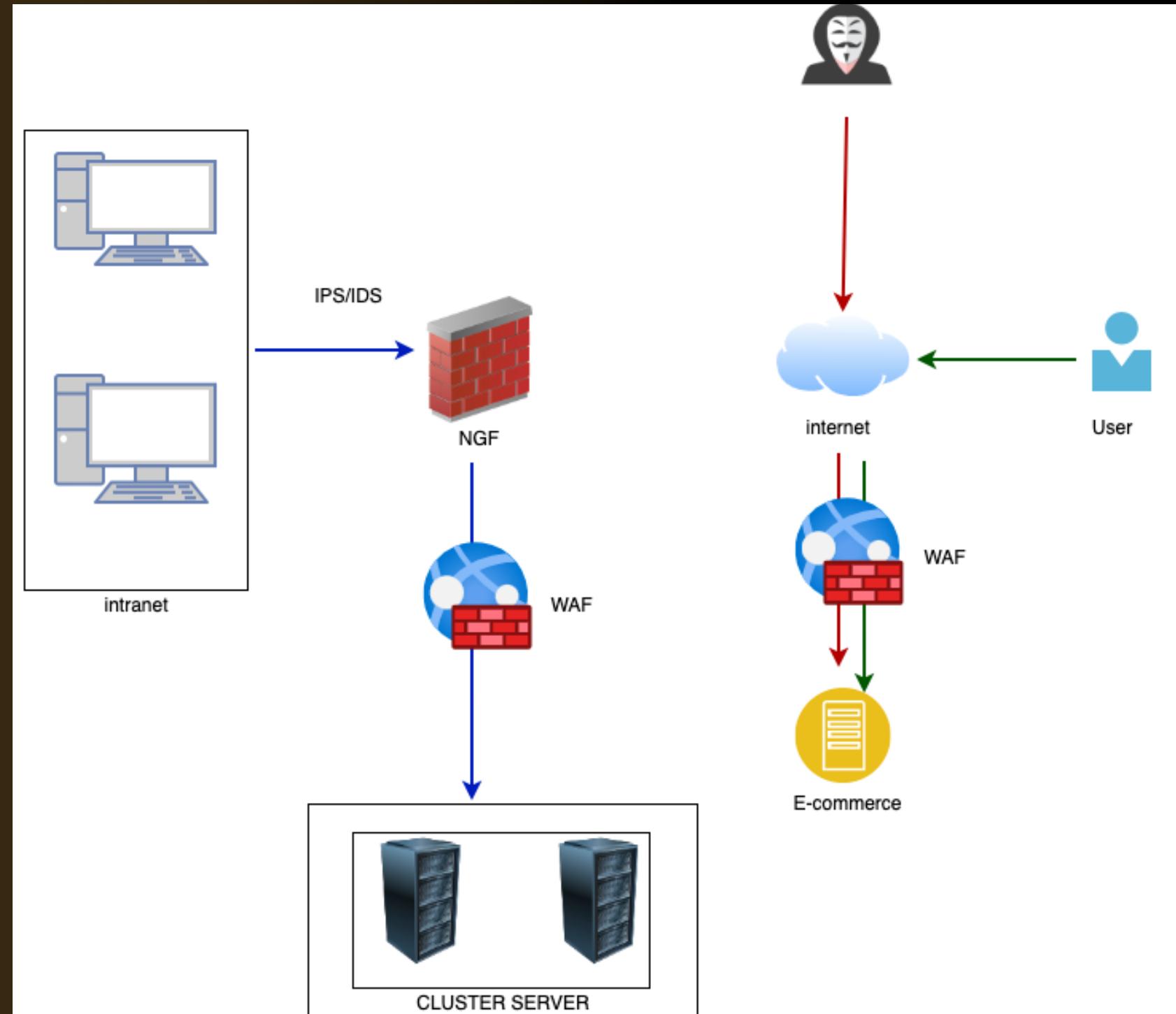
Pianificare le risposte agli incidenti: Avere un piano d'azione ben definito per rispondere rapidamente agli attacchi DDoS, inclusa la comunicazione con i fornitori di servizi Internet (ISP) e l'implementazione di contromisure appropriate.

Aggiornamenti regolari del software e del firmware: Mantenere aggiornato il software e il firmware dei server e dei dispositivi di rete per proteggerli da vulnerabilità note che potrebbero essere sfruttate dagli aggressori.



Per proteggere la nostra rete ci siamo serviti di un cluster di server. Un cluster di server può distribuire il carico del traffico in arrivo tra i vari server nel cluster. Quando arriva un attacco DDoS, il carico viene distribuito tra i server nel cluster, impedendo che un singolo server sia sopraffatto dal traffico dannoso.

Abbiamo anche implementato una policy firewall che limita il numero di connessioni da parte di un'indirizzo IP/ utente, in modo tale da evitare che un'attaccante saturi il sistema con un numero eccessivo di richieste.



RESPONSE

La priorità è che il malware **non si espanda sulla rete**, ma che si possa comunque monitorare l'andamento dell'attacco per adottare una risposta più appropriata.

Si può adottare una strategia d'**isolamento** della macchina infettata: la macchina sarà direttamente collegata ad internet, raggiungibile dall'attaccante ma non connessa alla rete interna.

In questo modo non avviene più comunicazione tra la **Web App** e la rete interna, ma l'attaccante può comunque accedere ad internet tramite la macchina infetta.

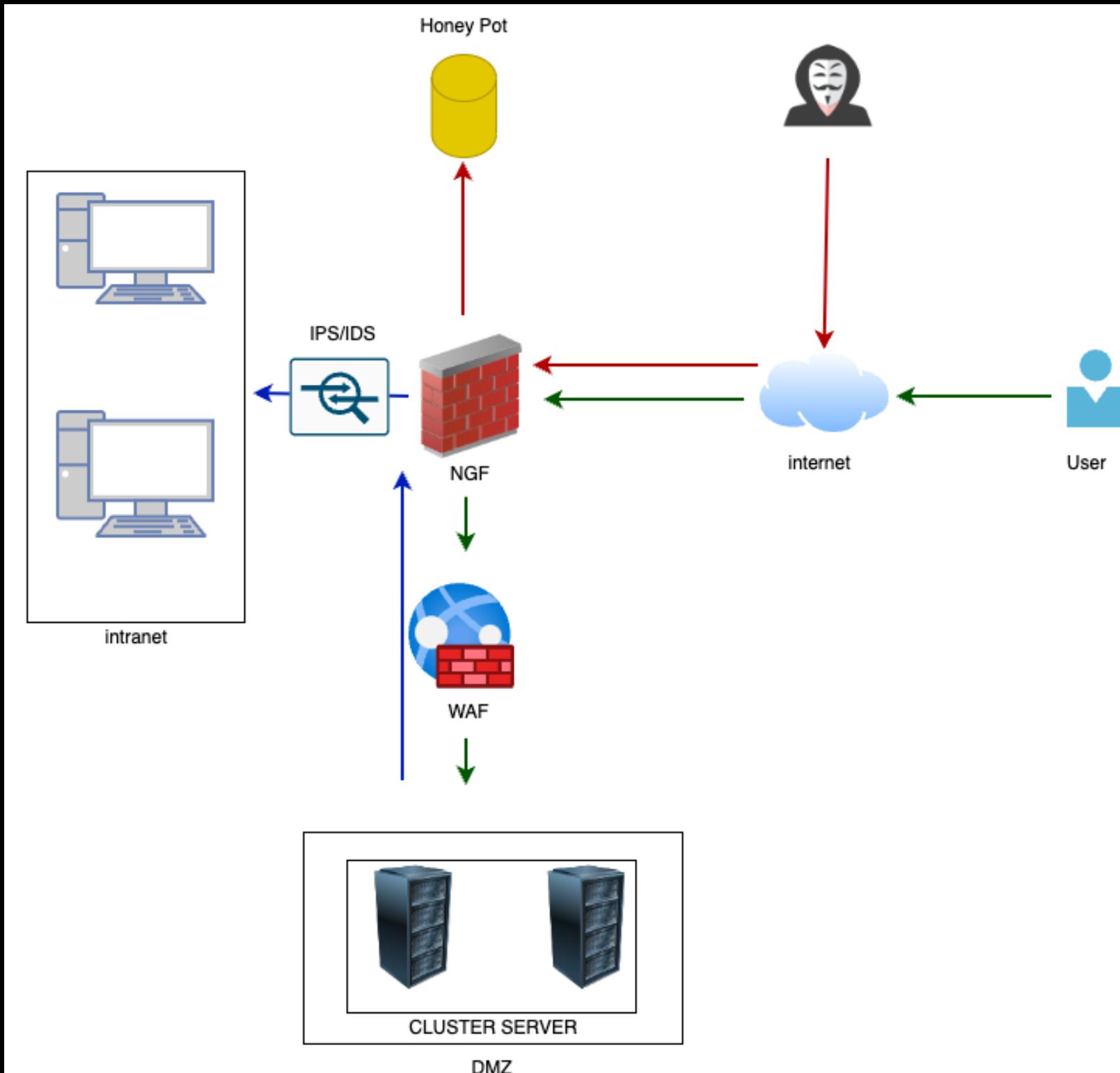
Nel caso si volesse evitare questa eventualità si può procedere con la tecnica della rimozione (che prevede qualunque tipo di accesso ad internet).

SOLUZIONE COMPLETA

Le implementazioni apportate alla rete sono:

Un Honey pot: un dispositivo, un'applicazione o un sistema informatico progettato per simulare risorse di sistema vulnerabili o interessanti per gli hacker, allo scopo di attirarli e monitorare o analizzare i loro comportamenti

IPS/IDS: sono 2 sistemi di monitoraggio della rete che hanno lo scopo di rilevare attacchi (IDS) e attuare contromisure per prevenirli (IPS) bloccando il traffico dannoso indirizzato verso la rete interna.



BONUS 1

PERFORMANCE_BOOSTER_V3.6.EXE

Grazie all'analisi effettuata dal ANYRUN , abbiamo potuto constatare che il file PERFORMANCE_BOOSTER_V3.6.exe è un malware. Il file finge di poter migliorare le prestazioni del sistema Windows 7, ma in realtà esegue un comando sulla CLI che permette di avviare dei file eseguibili dannosi, nascondendo la sua presenza. In questo modo il file potrebbe avere gravi conseguenze sul client perchè, agendo in incognito, avrebbe accesso ai dati sensibili e potrebbe mettersi in ascolto tra due o più dispositivi collegati fra loro creando ulteriori danni (MITM). Applicando le prassi del nostro Recovery Plan, il modo migliore per contrastare il malware è quello di disinstallare il file e avviare una scasione specifica antivirus. Successivamente andremmo a controllare i log per risalire alla sorgente da dove è stato scaricato il file. Grazie a Virus Total abbiamo potuto constatare che si tratta di un Trojan che contiene un ransomware.



Definizioni:
CLI: Command Line Interface, anche conosciuto come prompt dei comandi, è un'interfaccia testuale. Consente agli utenti di interagire direttamente con il sistema operativo attraverso comandi testuali, eseguendo varie operazioni come la gestione dei file, l'automazione dei compiti ripetitivi, la navigazione tra cartelle e la risoluzione dei problemi

LOG: Sono dei file di testo che registrano eventi rilevanti nei sistemi informatici. Servono per monitorare attività, analizzare problemi, garantire sicurezza e ottimizzare le prestazioni., Contengono dettagli come data e ora, tipo di evento e sono spesso usati per diagnosticare errori o comportamenti anomali.

| | | | |
|--------------------|----------------------------------|---------------------|---|
| BitDefenderTheta | ⚠ Gen:NN.Zexaf.36308.uu1@ae9A1Fk | ClamAV | ⚠ Win.Ransomware.Crypren-9864892-0 |
| Cylance | ⚠ Unsafe | Elastic | ⚠ Malicious (moderate Confidence) |
| Google | ⚠ Detected | Malwarebytes | ⚠ Malware.Heuristic.1008 |
| MaxSecure | ⚠ Trojan.Malware.300983.susgen | McAfee | ⚠ RDN/Generic.dx |
| McAfee-GW-Edition | ⚠ RDN/Generic.dx | Microsoft | ⚠ PUAdvertising:Win32/LoadMoney |
| Palo Alto Networks | ⚠ Generic.ml | Rising | ⚠ Trojan.Generic@AI.96 (RDML:Jewgxwy2...) |
| Sophos | ⚠ Generic ML PUA (PUA) | Symantec | ⚠ ML.Attribute.HighConfidence |
| TrendMicro | ⚠ Malicious moderate risk score | Acronis (Static ML) | ⚠ Undetected |

BONUS 2

[HTTPS://DRV.MS/U/S!AT7EQ7H8KX6-NQMIRTCUZ3AQSPOE](https://drv.ms/u/s!At7eQ7h8kx6-nQM1RTCuZ3aQspOE)



Questo malware si spaccia come un'aggiornamento per il browser Windows. Una volta inviata una richiesta GET, la macchina comincia a scaricare file dannosi all'interno del sistema camuffandosi come un file di sistema. Questo malware va a modificare le impostazioni di rete tramite un server remoto, creando una serie di danni che gravano sulla produttività del dispositivo e rendendo ostica qualunque tipo di operazione online. Dalle ricerche fatte tramite Any Run sembra essere un Loader, nello specifico un hijackloader: questo malware modulare funge da veicolo per la distribuzione di diversi tipi di software dannoso su sistemi compromessi. Ha acquisito importanza durante l'estate del 2023 e da allora è stato utilizzato in molteplici attacchi contro organizzazioni di vari settori, comprese le imprese del settore alberghiero. Il miglior modo per contrastare questo tipo di malware è quello di installare un Web Application Firewall, così da rilevare più facilmente i file malevoli di questo tipo. Nel caso il malware abbia già infettato la macchina, andrebbe eseguita una scansione antivirus specifica.

A screenshot of a Windows taskbar. On the left, there's a system tray icon for a 32-bit Windows 7 Professional edition from February 2024 at 23:12. Next to it is a green checkmark icon. Following that is a standard Internet Explorer icon. To the right of the browser icon is a red rectangular box containing the text "Malicious activity". Below this box is a URL: "https://1drv.ms/u/s!At7eQ7h8kx6-nQM1RTCuZ3aQspOE". Underneath the URL, there are two buttons: "Open in browser" and "hijackloader". Further down, there are two more buttons: "loader" and another "hijackloader". At the bottom of the taskbar, there are several small icons representing different system functions like power, volume, and network.

IL TEAM

Oliviero
Camarota

Marco
De Falco

Alessandro
Marasca



CDM S.R.L.

GRAZIE

