

PROGETTO S9, L5

MATTIA PASTORELLI



COMANDA:

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



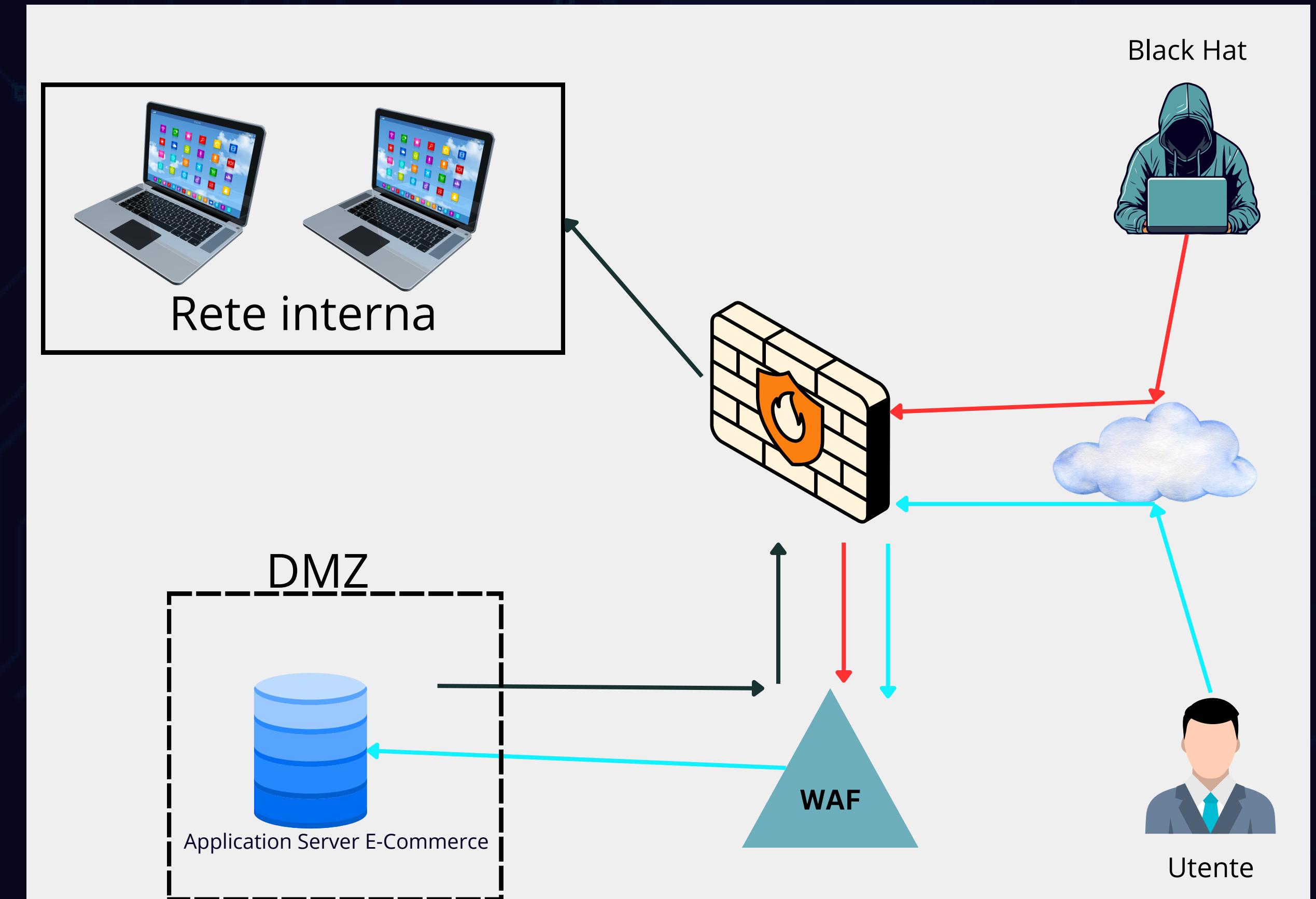
1. Azioni preventive : quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQL o pure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni
2. Impatti sul business : l'applicazione Web subisce un attacco 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)

QUESITO 1

Per prevenire la maggior parte degli attacchi SQLi e XXS, si procede con l'implementazione di un WAF (Web Application Firewall). Questa soluzione consente agli utenti di continuare a navigare su Internet, mentre gli attaccanti non possono eseguire i suddetti attacchi.

Successivamente, verrà effettuata la correzione degli eventuali errori di programmazione.

- ← Flusso rete attaccante
- ← Flusso rete utente
- ← Flusso rete interna



QUESITO 2

Evento	Tempo	Perdita al minuto	Perdita totale
DDoS	10min	1500,00 €	15000

All'interno di un'azienda, è consigliabile identificare preventivamente le minacce che potrebbero minacciare seriamente le attività aziendali. Questo può essere realizzato tramite un piano specifico chiamato Business Continuity Plan.

Per creare un solido BCP, è essenziale disporre di un report sull'aspetto economico-finanziario legato agli eventuali impatti degli attacchi subiti(Di natura informatica o ambientale), denominato Business Impact Analysis.

Grazie a un sistema di calcolo con finalità di previsione, è possibile stimare in modo approssimativo i danni economici derivanti dall'evento dannoso che potrebbe verificarsi.

QUESITO 3

La richiesta è relativa alla presenza di un malware nell'applicazione web.

Ci è stato chiesto di dare priorità alla gestione del malware per evitare la sua diffusione all'interno della rete interna.

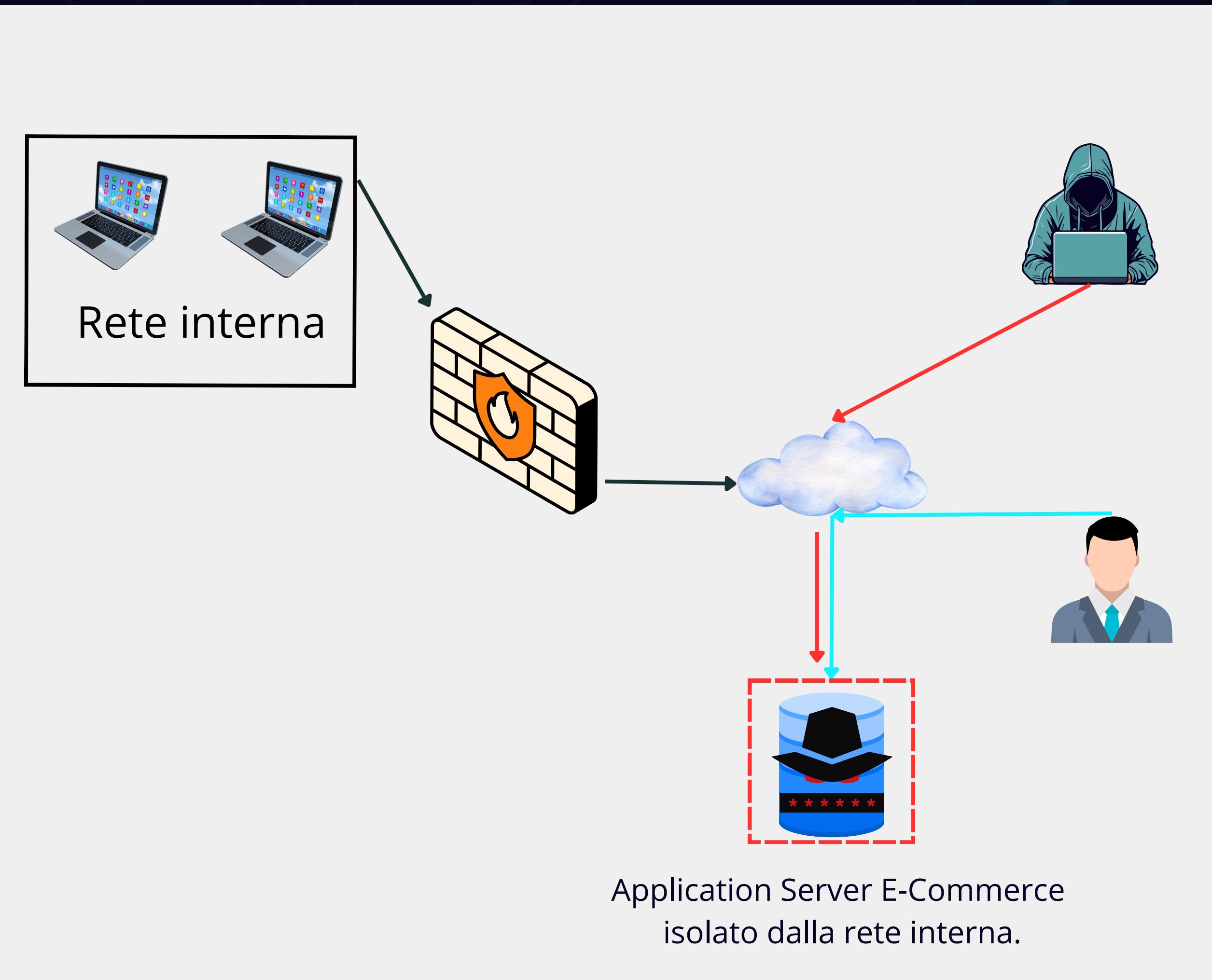
Una possibile soluzione potrebbe essere quella di spostare il server dell'e-commerce su una connessione esterna, separata dalla nostra rete.

In questo modo, sia gli utenti che gli attaccanti potrebbero ancora accedere al server, ma quest'ultimo non avrebbe più accesso alla rete interna.

← Flusso rete attaccante —

← Flusso rete utente —

← Flusso rete interna —



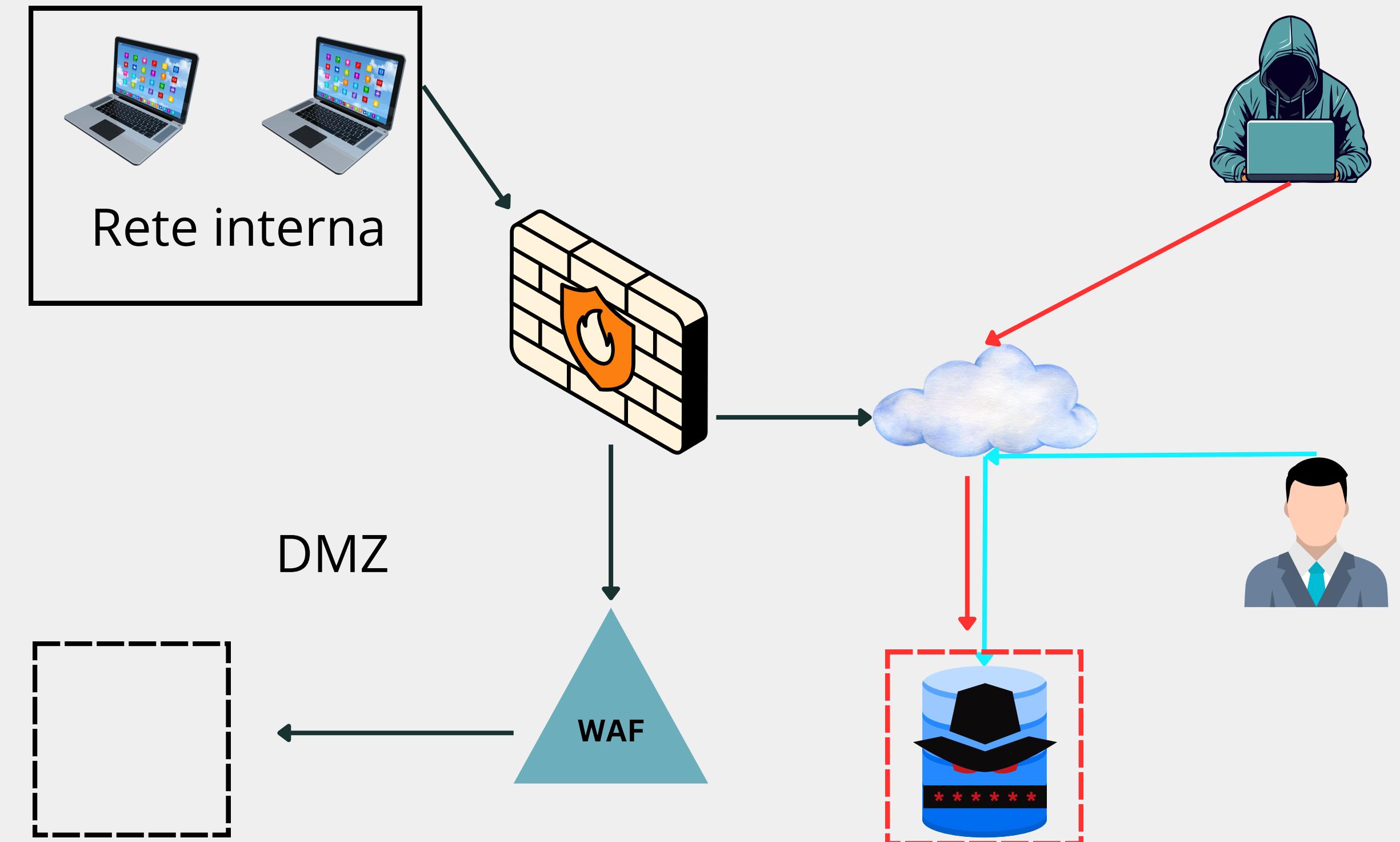
QUESITO 4

Unione del Quesito 1 e Quesito 3

← Flusso rete attaccante —

← Flusso rete utente —

← Flusso rete interna —

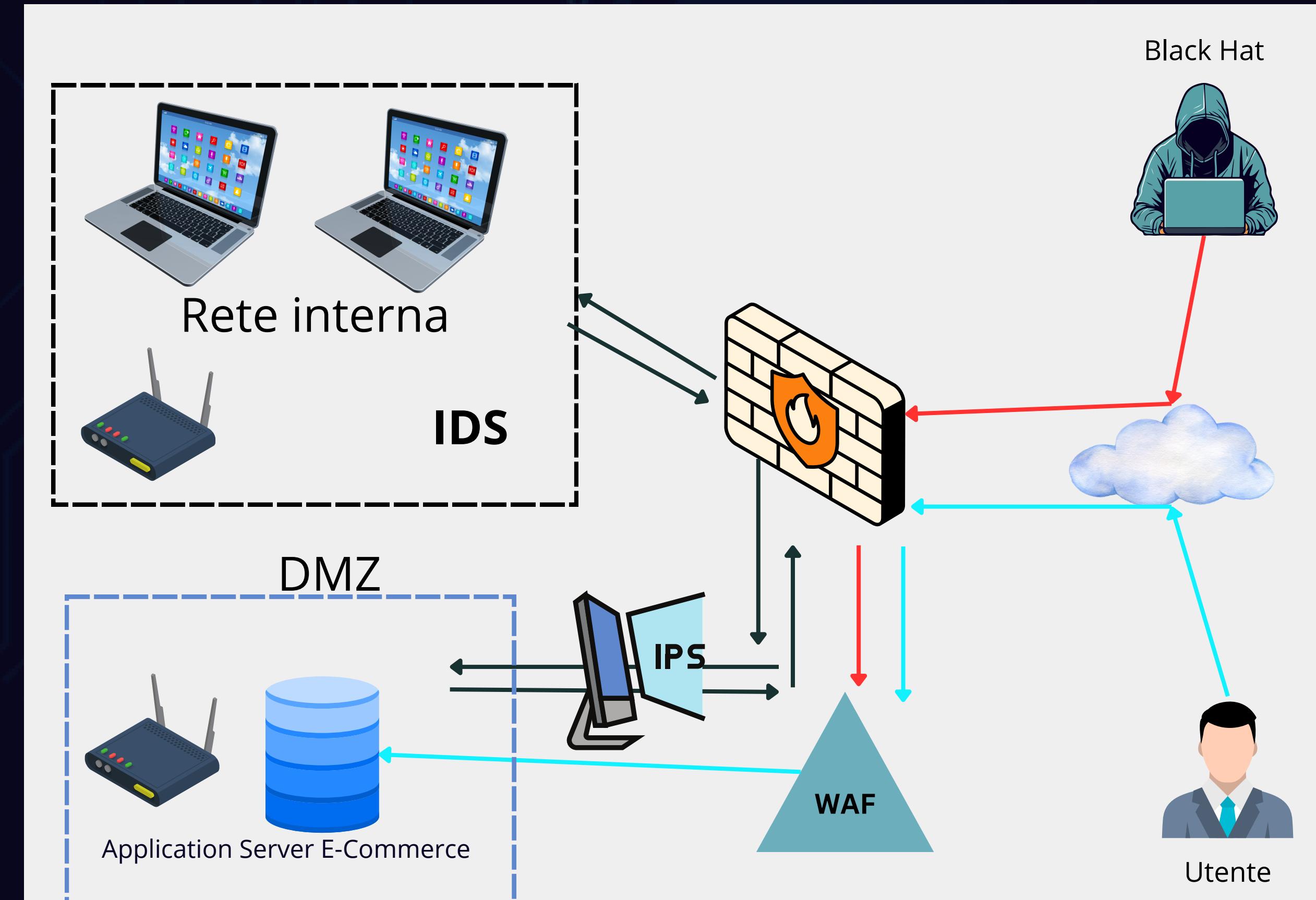


Application Server E-Commerce
isolato dalla rete interna.

QUESITO 5

La soluzione finale più completa consiste nell'implementare il nostro sistema di sicurezza utilizzando:

- VLAN = Aumenta la sicurezza suddividendo le reti in subnet, creando due reti completamente separate. Anche se comunicano in questo caso, è possibile interrompere la comunicazione al bisogno.
- IPS/IDS = Un IPS che rileva e blocca istantaneamente attività sospette dal nostro server applicativo verso la rete, intervenendo immediatamente bloccando o limitando il flusso di rete. L'IDS opera all'interno della rete interna, segnalando gli accessi ai sistemi sensibili (Nas).



BONUS 1

Possiamo notare un malware installato dal proprietario del computer, sotto la falsa motivazione di migliorare le prestazioni del sistema. In realtà, il vero obiettivo di questo malware è assumere il controllo amministrativo del dispositivo tramite Power Shell per rubare informazioni personali, eseguire azioni non autorizzate e avere il controllo completo del computer.

Soluzione per contrastare questo malware:

- Effettuare una scansione approfondita del sistema con un programma anti-malware.
- Se individuato, mettere in quarantena il malware e eliminarlo definitivamente.
- Se il computer è compromesso in modo significativo, è consigliabile formattare completamente il sistema.

Behavior activities

Add for printing ▾

MALICIOUS

Changes powershell execution policy (Unrestricted)

- cmd.exe (PID: 668)

Drops the executable file immediately after the start

- PERFORMANCE_BOOSTER_v3.6.exe (PID: 2088)

SUSPICIOUS

Starts CMD.EXE for commands execution

- PERFORMANCE_BOOSTER_v3.6.exe (PID: 2088)

Using PowerShell to operate with local accounts

- powershell.exe (PID: 3332)

Starts POWERSHELL.EXE for commands execution

- cmd.exe (PID: 668)

Executing commands from a ".bat" file

- PERFORMANCE_BOOSTER_v3.6.exe (PID: 2088)

Checks for the .NET to be installed

- regedit.exe (PID: 2824)

Reads the Internet Settings

- powershell.exe (PID: 3332)

Reads Microsoft Outlook installation path

- regedit.exe (PID: 2824)

Searches for installed software

- regedit.exe (PID: 2824)

Runs PING.EXE to delay simulation

- cmd.exe (PID: 668)

Reads the history of recent RDP connections

- regedit.exe (PID: 2824)

Uses ATTRIB.EXE to modify file attributes

- cmd.exe (PID: 668)

INFO

Reads the machine GUID from the registry

- regedit.exe (PID: 2824)

Reads Microsoft Office registry keys

- regedit.exe (PID: 2824)

Checks transactions between databases Windows and Oracle

- regedit.exe (PID: 2824)

Create files in a temporary directory

- PERFORMANCE_BOOSTER_v3.6.exe (PID: 2088)

Checks supported languages

- PERFORMANCE_BOOSTER_v3.6.exe (PID: 2088)

- mode.com (PID: 2380)

Manual execution by a user

- notepad.exe (PID: 3372)

- wmpnscfg.exe (PID: 3828)

Reads Windows Product ID

- regedit.exe (PID: 2824)

BONUS 2

In questo caso, è evidente la presenza di un Malware che si maschera da aggiornamento di Windows Edge. La differenza principale rispetto al malware precedente è che in questo caso viene installato erroneamente dall'utente tramite una notifica push.

Il funzionamento del malware è descritto nel report:

- Può essere attivato a distanza all'avvio del computer della vittima.
- Disabilita il sistema SEHOP, fondamentale per gestire gli errori su dispositivi Windows e garantire che l'applicazione non vada in crash. Disattivandolo, l'attaccante può sfruttare le vulnerabilità delle eccezioni SEH per eseguire codice dannoso e compromettere il sistema.
- Sfruttando il sistema Windows, può operare in background e accedere a tutte le funzionalità del dispositivo.
- È in grado di inviare e ricevere file, nonché creare directory temporanee.

Come affrontare la situazione:

- Attraverso una scansione dettagliata del sistema è possibile individuare il potenziale malware.
- Poiché il processo si maschera tra i processi di Windows, è consigliabile controllare la presenza di servizi sconosciuti o che consumano più memoria del normale. In tal caso, è possibile terminare il processo e/o eliminare il file che lo ha avviato.

MALICIOUS

Drops the executable file immediately after the start

- MicrosoftEdgeSetup.exe (PID: 3360)
- MicrosoftEdgeUpdateSetup.exe (PID: 2476)

SUSPICIOUS

Process drops legitimate windows executable

- iexplore.exe (PID: 3564)
- iexplore.exe (PID: 1632)
- MicrosoftEdgeSetup.exe (PID: 3360)
- MicrosoftEdgeUpdateSetup.exe (PID: 2476)
- MicrosoftEdgeUpdate.exe (PID: 4040)

Executable content was dropped or overwritten

- MicrosoftEdgeSetup.exe (PID: 3360)
- MicrosoftEdgeUpdateSetup.exe (PID: 2476)

Starts a Microsoft application from unusual location

- MicrosoftEdgeUpdate.exe (PID: 3728)
- MicrosoftEdgeUpdateSetup.exe (PID: 2476)
- MicrosoftEdgeUpdate.exe (PID: 4040)

Disables SEHOP

- MicrosoftEdgeUpdate.exe (PID: 4040)

Starts itself from another location

- MicrosoftEdgeUpdate.exe (PID: 4040)

Creates/Modifies COM task schedule object

- MicrosoftEdgeUpdate.exe (PID: 4012)

Creates a software uninstall entry

- MicrosoftEdgeUpdate.exe (PID: 4040)

Reads the Internet Settings

- MicrosoftEdgeUpdate.exe (PID: 3408)

Reads settings of System Certificates

- MicrosoftEdgeUpdate.exe (PID: 3408)

Checks Windows Trust Settings

- MicrosoftEdgeUpdate.exe (PID: 3408)

Executes as Windows Service

- MicrosoftEdgeUpdate.exe (PID: 3796)

Reads security settings of Internet Explorer

- MicrosoftEdgeUpdate.exe (PID: 3408)

INFO

Executable content was dropped or overwritten

- iexplore.exe (PID: 3564)
- iexplore.exe (PID: 1632)

Drops the executable file immediately after the start

- iexplore.exe (PID: 3564)
- iexplore.exe (PID: 1632)

Application launched itself

- iexplore.exe (PID: 1632)

The process uses the downloaded file

- iexplore.exe (PID: 1632)
- MicrosoftEdgeSetup.exe (PID: 3360)

Checks supported languages

- MicrosoftEdgeSetup.exe (PID: 3360)
- MicrosoftEdgeUpdate.exe (PID: 3728)
- MicrosoftEdgeUpdateSetup.exe (PID: 2476)
- MicrosoftEdgeUpdate.exe (PID: 4012)
- MicrosoftEdgeUpdate.exe (PID: 4040)
- MicrosoftEdgeUpdate.exe (PID: 2436)
- MicrosoftEdgeUpdate.exe (PID: 2812)
- MicrosoftEdgeUpdate.exe (PID: 3408)
- MicrosoftEdgeUpdate.exe (PID: 3796)

Create files in a temporary directory

- MicrosoftEdgeSetup.exe (PID: 3360)
- MicrosoftEdgeUpdate.exe (PID: 3728)
- MicrosoftEdgeUpdate.exe (PID: 3408)

Reads the computer name

- MicrosoftEdgeUpdate.exe (PID: 3728)
- MicrosoftEdgeUpdate.exe (PID: 4040)
- MicrosoftEdgeUpdate.exe (PID: 4012)
- MicrosoftEdgeUpdate.exe (PID: 2436)
- MicrosoftEdgeUpdate.exe (PID: 3408)
- MicrosoftEdgeUpdate.exe (PID: 2812)
- MicrosoftEdgeUpdate.exe (PID: 3796)

Reads the machine GUID from the registry

- MicrosoftEdgeUpdate.exe (PID: 3728)