

Esercizio W20D4 - Security Operation (Benchmark M5)

RICHIESTA

Per l'esercizio di fine modulo W20D4, è richiesto all'utente di rispondere ad alcuni quesiti relativi all'architettura di rete proposta. Nello specifico, è richiesto all'utente di approntare azioni preventive per evitare attacchi SQLi o XSS all'applicazione, di illustrare gli impatti sul business di un attacco DDos, di mettere in campo le giuste operazioni di contrasto al propagarsi di un'infezione da malware e di modificare l'architettura di rete - ipotizzando di avere a disposizione un budget fra i 20.000 e i 30.000 euro - per aumentarne la sicurezza

~~~

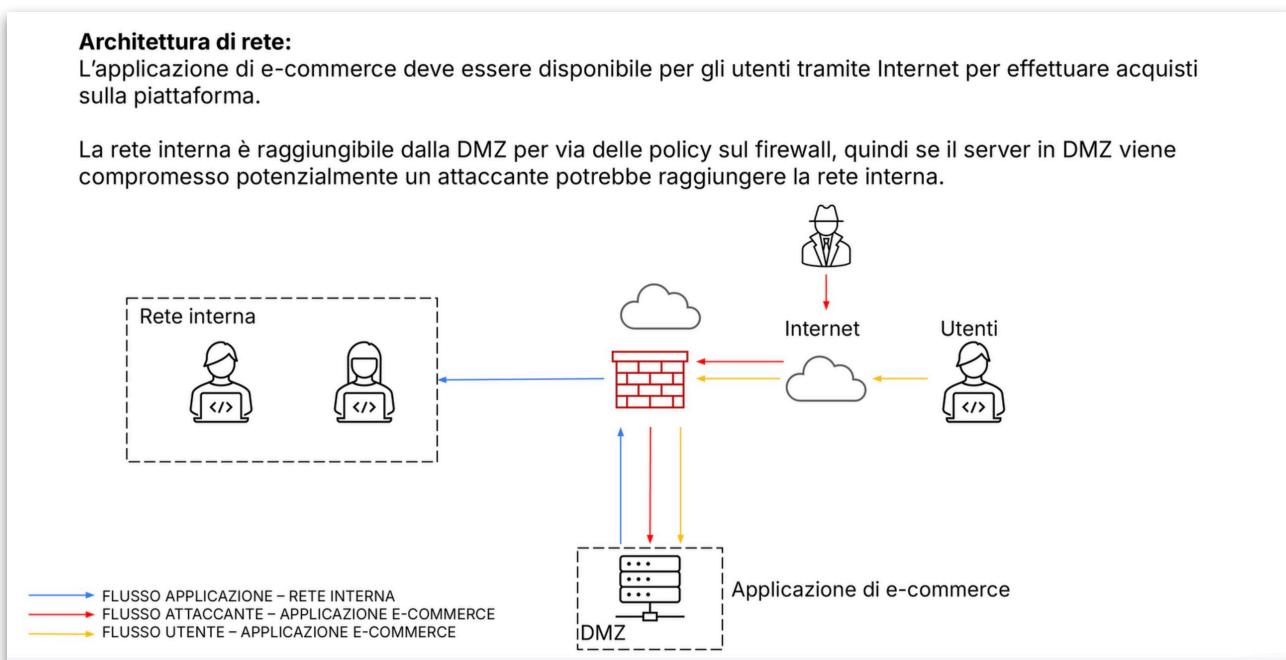
## ARCHITETTURA DI RETE

Nella seguente immagine, l'architettura di rete oggetto dell'esercizio:

### **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.



~~~

AZIONI PREVENTIVE CONTRO EVENTUALI ATTACCHI SQLI e XSS

Nello scenario proposto, l'azienda in questione gestisce un e-commerce di una certa rilevanza. Questo vuol dire che la sicurezza, sia dei clienti che dell'azienda stessa, ha un'importanza enorme. Le misure preventive chiave da implementare per difendere l'applicazione dalle minacce più comuni si dividono in due macrocategorie: quelle più generali per la sicurezza complessiva, e quelle più specifiche per gli attacchi SQLi e XSS.

Per ciò che riguarda le misure preventive generali abbiamo:

- La corretta **configurazione del web-server** per ridurre la superficie di attacco

- La corretta **configurazione dei cookie**, con specifici parametri che aumentano di molto la sicurezza

Per ciò che invece riguarda gli attacchi SQLi e XSS in particolare, abbiamo:

- La **validazione e sanificazione degli input**, in modo che ogni dato inserito dall'utente (e quindi anche da un eventuale attaccante) venga controllato e ripulito
- La **codifica sicura dell'output (Escaping)**, in modo che qualsiasi carattere speciale inserito dall'utente, e potenzialmente pericoloso, venga trattato dal sistema come semplice testo e non come codice eseguibile dal browser dell'utente
- L'utilizzo di **Query Parametrizzate (Prepared Statements)**, in modo che le interrogazioni al database non possano essere manipolate dall'attaccante

In questa fase non è ancora necessario apportare modifiche all'infrastruttura fisica della rete per aumentare la sicurezza dell'e-commerce.

~~~

## **IMPATTI SUL BUSINESS IN CASO DI ATTACCO DDOS E AZIONI PREVENTIVE**

Nell'analizzare i danni arrecati al business da un attacco DDos - nel caso specifico un attacco DDos che rende il sito irraggiungibile per 10 minuti - c'è da tener conto di due diverse tipologie di impatto.

**L'impatto diretto** è immediatamente calcolabile: per un sito che genera ricavi di 1.500 euro al minuto, 10 minuti di irraggiungibilità rappresentano un **danno da 15.000 euro** ( $1.500 \times 10$ ).

L'impatto diretto è però, come detto, solo una parte del danno. Molto più insidiosi sono gli **impatti indiretti** dell'attacco DDos. Seppur non quantificabili in termini numerici, conseguenze come **perdita di fiducia dei clienti**, danni alla reputazione, perdita di produttività interna e costi da recupero dell'immagine possono rivelarsi fatali per l'azienda. È opinione comune che l'impatto indiretto di un attacco DDos sia molto più grave rispetto all'impatto diretto.

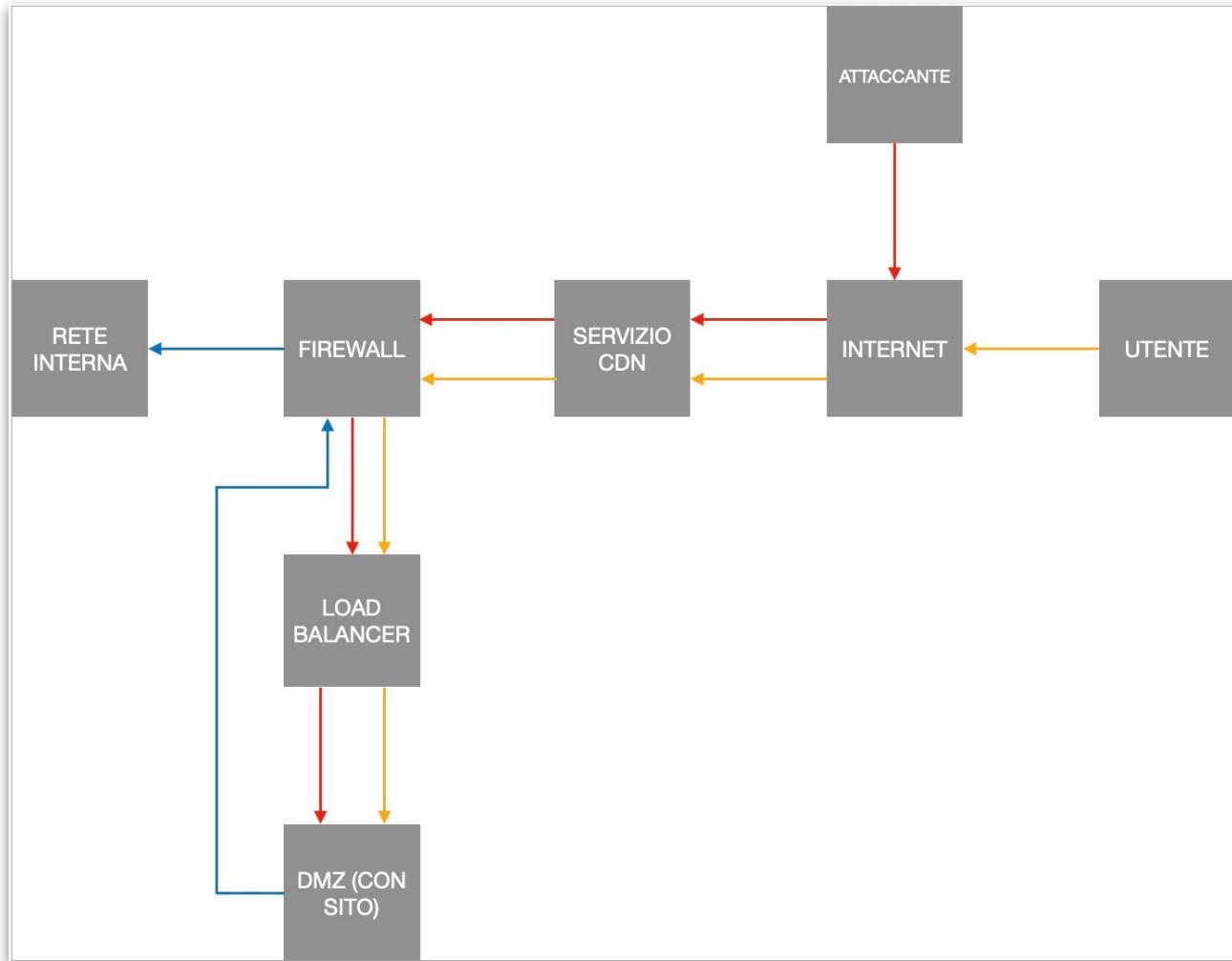
Nel discutere invece delle azioni preventive che è possibile applicare in merito agli attacchi DDos, è essenziale sottolineare un punto: **non è possibile garantire una protezione al 100% contro un attacco DDoS**. Le operazioni e le modifiche all'architettura di rete che illustrerò nei paragrafi successivi riducono drasticamente la probabilità di successo di un attacco, e ne mitigano l'impatto, ma è impossibile eliminare completamente il rischio. L'obiettivo di un esperto della sicurezza è quello di **ridurre il rischio a un livello accettabile** attraverso un'adeguata gestione e configurazione della rete.

La modifica principale per rendere la rete più resiliente agli attacchi DDoS è l'integrazione di un **servizio di protezione DDoS basato su CDN**. Questo servizio "intercetta" il traffico prima che raggiunga l'e-commerce, lo "pulisce" separando le richieste legittime da quelle generate dal servizio DDos, e fa arrivare a destinazione solo le richieste legittime.

Nel caso in esame, al firewall della nostra azienda e poi all'applicazione di e-commerce arriva dunque solo traffico legittimo, riducendo così drasticamente le probabilità che un attacco DDoS raggiunga e sovraccarichi le risorse aziendali. Tra i principali fornitori di servizi di protezione DDoS basati su CDN, degni di nota sono **Cloudflare**, Akamai, AWS Shield Advanced, Google Cloud Armor e Azure DDoS Protection.

Altro strumento molto importante per rendere la rete più sicura è l'utilizzo di un **Bilanciatore di Carico (Load Balancer)**. È un dispositivo (hardware o software) che si occupa di distribuire il traffico in ingresso nei vari server di rete. Nello specifico, il Load Balancer suddivide il traffico in ingresso tramite un algoritmo, in modo da inviare la richiesta sempre al server meno carico. Questo aumenta sia la sicurezza che la scalabilità dell'applicazione, consentendo alla stessa di gestire un elevato numero di richieste simultanee. Da non trascurare poi il fatto che in questo modo l'applicazione resta sempre disponibile, anche in caso di guasto a uno dei server. In questo caso il Load Balancer andrebbe infatti a "dirottare" il traffico su di un altro server.

L'integrazione del servizio di protezione DDoS basato su CDN e del Bilanciatore di Carico modifica la nostra architettura di rete in questo modo:



L'ultimo aspetto da considerare è che **il traffico relativo alla rete interna non passa attraverso il Load Balancer**. Come illustrato, il Load Balancer ha infatti il compito di distribuire il traffico in ingresso tra più server di un'applicazione, per bilanciare il carico e garantire alta disponibilità, ma a meno di configurazioni particolari non gestisce il traffico in uscita.

~~~

RESPONSE: APP INFETTATA DA UN MALWARE

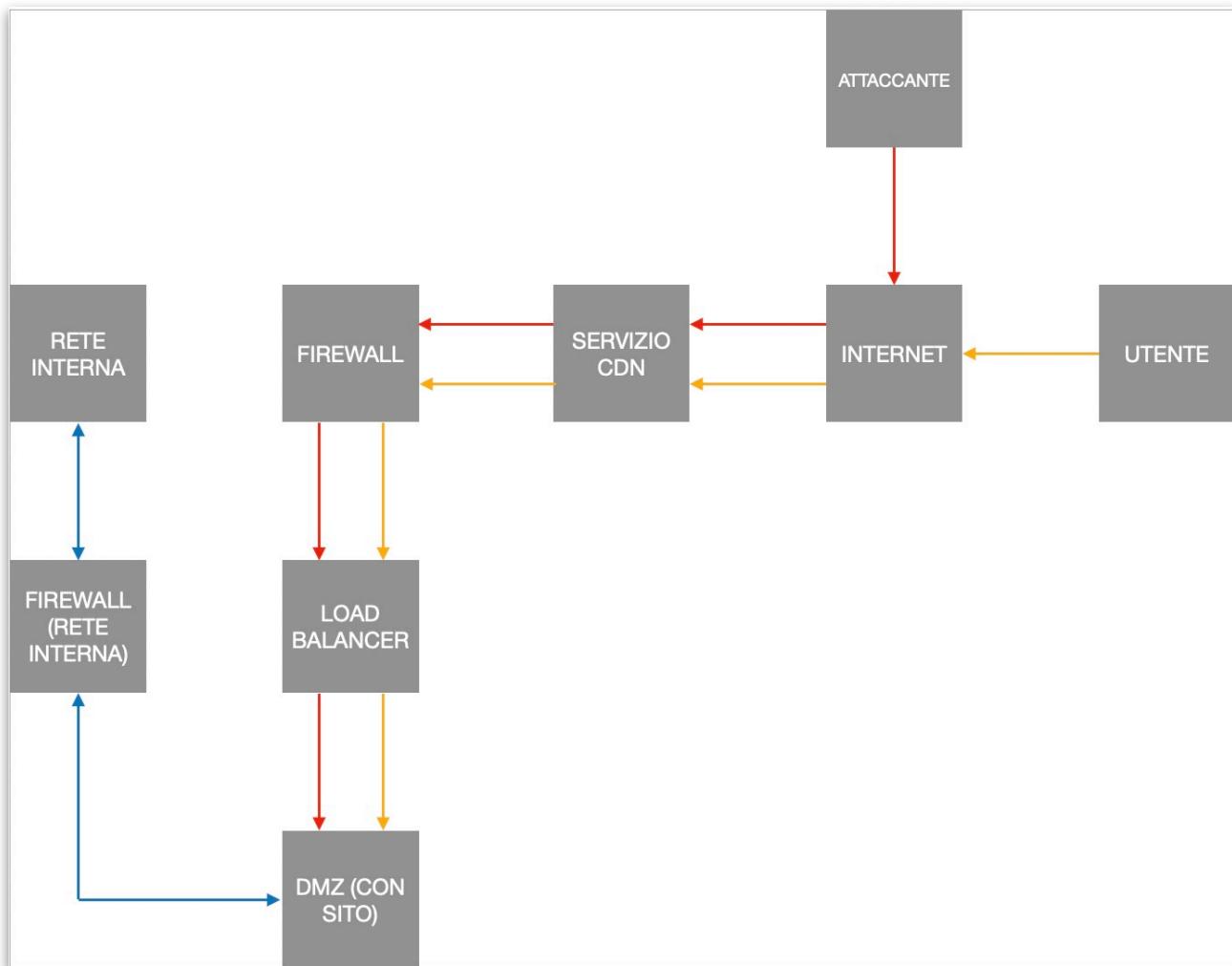
In un'architettura ad alta complessità e in un sistema che gestisce dati sensibili, avere un singolo firewall che gestisce l'intero flusso di rete è **una pratica non ideale**. È facile capire il perché: se il firewall viene compromesso o configurato male, l'intera rete sarà vulnerabile (**Single Point of Failure**).

Failure). Inoltre, gestire tutte le policy su un unico dispositivo può rivelarsi molto complesso, e questo aumenta la possibilità di errori. La best practice impone quindi l'utilizzo di **almeno due firewall**.

Nel caso specifico, ho lasciato inalterato il firewall perimetrale esterno (quello che regola la comunicazione tra Internet e la DMZ), ma ho implementato un **nuovo firewall interno** tra la rete interna e la DMZ. In questo modo, il traffico della rete interna non passa più dal firewall esterno.

Con questa modifica si crea una sorta di "zona cuscinetto" che, in combinazione con regole di sicurezza ferree, rende molto più difficile per un attaccante muoversi dalla DMZ compromessa alla Rete Interna. Punto fondamentale, come già anticipato, quello del rispetto **Principio del Minimo Privilegio**: le policy sul nuovo firewall interno devono essere estremamente restrittive, andando a bloccare tutte le comunicazioni che non riguardano servizi specifici nella Rete Interna.

L'integrazione di un nuovo firewall interno modifica l'architettura di rete in questo modo:



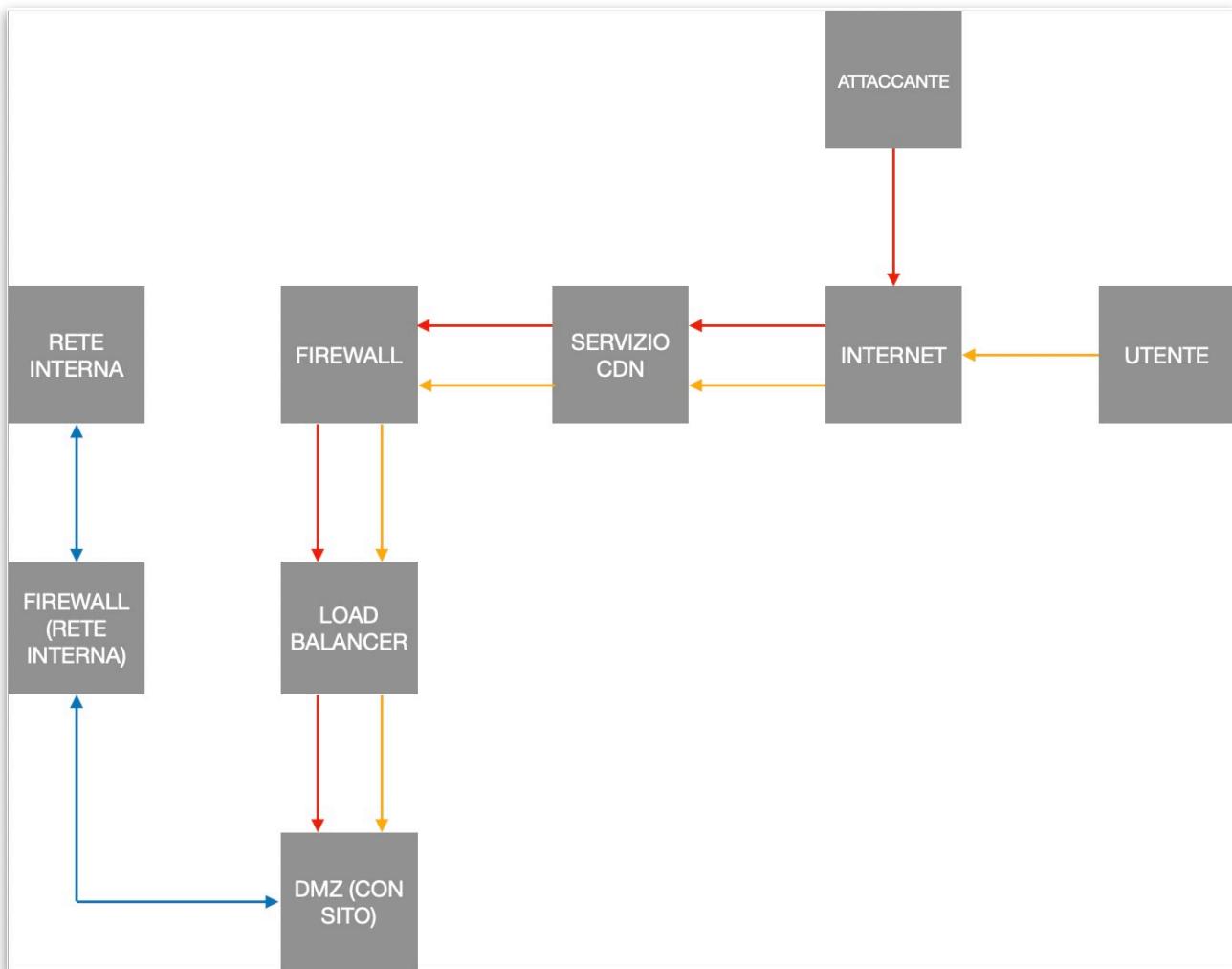
L'architettura di rete appena illustrata rappresenta anche la **configurazione più sicura possibile** all'interno dei parametri stabiliti dall'esercizio. È infatti garantita una protezione a monte (con il servizio di protezione DDoS basato su CDN), disponibilità e scalabilità dei server e protezione in profondità con un'essenziale zona di isolamento tra la DMZ e la Rete Interna.

ULTERIORI MODIFICHE ALLA RETE E DETTAGLIO COSTI

La parte facoltativa dell'esercizio chiede all'allievo di effettuare eventuali altre modifiche alla rete e calare la teoria nella pratica, ipotizzando di creare una corretta architettura di rete disponendo di un budget compreso fra i 20.000 e i 30.000 euro.

Per la risoluzione di questa parte dell'esercizio, ho considerato sia le spese relative all'hardware che quelle relative al software. Mi preme sottolineare il fatto che lo stanziamento di tale budget è **insufficiente alle necessità di un'azienda** in così rapido sviluppo, e che l'aumento degli stanziamenti consentirebbe di aumentare in maniera importante la resilienza della rete.

Come evidenziato in precedenza, l'ultima versione dell'architettura di rete rappresenta la migliore soluzione possibile, dal punto di vista concettuale e strutturale, per le esigenze dell'azienda. Assicura infatti protezione a monte, disponibilità e scalabilità dei servizi e l'essenziale isolamento tra la Rete Interna e l'esterno. Questa è l'architettura di rete attuale:



Ho suddiviso l'allocazione del budget in spese per l'acquisto di hardware e spese relative al software. Per ciò che riguarda l'aspetto hardware, è necessario l'acquisto di 2 Firewall di Nuova Generazione (NGFW) e di 3 Switch.

I Firewall di Nuova Generazione (NGFW) rappresentano un'evoluzione dei vecchi Firewall. Integrano all'interno funzionalità di Intrusion Prevention System (IPS)/Intrusion Detection System (IDS), che rilevano e bloccano attivamente tentativi di intrusione ed exploit noti, Antivirus e Antimalware, Web Filtering e controllo delle Applicazioni. **L'investimento in due NGFW è**

cruciale per la robustezza e la segmentazione della rete. Guardando al nostro budget, sono tre le soluzioni disponibili. Per tutte le soluzioni sono compresi tre anni di sottoscrizione ai software di sicurezza associati:

- FortiGate 100F (prezzo stimato per due unità tra i 12.000 e i 18.000 euro)
- Sophos XG 210/310 (prezzo stimato per due unità tra i 14.000 e i 26.000 euro)
- Palo Alto PA-440 (prezzo stimato per due unità tra i 18.000 e i 30.000 euro)

L'acquisto di tre Switch è una scelta strategica per garantire la segmentazione, la sicurezza e la scalabilità delle diverse zone della rete. Uno sarà dedicato alla DMZ, un secondo alla Rete Interna e il terzo metterà in comunicazione i due Firewall. Per quel che riguarda gli Switch, ho selezionato due soluzioni. Entrambe non prevedono sottoscrizione a software proprietari:

- Ubiquiti UniFi Switches (prezzo stimato per tre unità tra i 1.000 e i 2.000 euro)
- Cisco Catalyst 2960-L Series (prezzo stimato per unità tra i 1.500 e i 2.500 euro)

Entrambi i brand proposti sono riconosciuti per l'affidabilità, e le soluzioni offrono le funzionalità di base necessarie per la creazione dell'architettura.

Passando al software, più volte nel documento ho evidenziato come la protezione da attacchi DDoS sia la prima e più critica linea di difesa per garantire la disponibilità del servizio. Altrettanto importante è che il vendor fornisca, incluso nel prezzo, **il servizio di Web Application Firewall (WAF) integrato**. Fra le tante soluzioni, e in considerazione del budget allocato, la soluzione principale è:

- Cloudflare Business Plan (prezzo stimato per un anno di sottoscrizione tra i 2.400 e i 3.200 euro)

Altro punto fondamentale per la sicurezza dell'azienda è l'integrazione di un **Endpoint Detection and Response (EDR)**. È una soluzione di sicurezza che monitora continuamente i terminali, rilevando e investigando su eventuali minacce. Gli agenti EDR saranno installati su tutti i server critici all'interno della rete. Fra le varie proposte, ho selezionato tre soluzioni:

- SentinelOne (prezzo stimato per licenza triennale e 5-10 server tra i 1.500 e i 3.000 euro)
- CrowdStrike Falcon (prezzo stimato per licenza triennale e 5-10 server tra i 2.000 e i 4.000 euro)
- Microsoft Defender for Endpoint (prezzo stimato per licenza triennale e 5-10 server tra i 1.800 e i 3.500 euro)

Tutte e tre le soluzioni EDR proposte sono valide, e la scelta specifica dipende da fattori come l'eventuale integrazione con altri strumenti già in uso, la preferenza per un'interfaccia utente.

A concludere, c'è il **Bilanciatore di Carico (Load Balancer)**. Come visto in precedenza, si occupa di distribuire in modo intelligente il traffico di rete in entrata tra più server che ospitano la stessa applicazione. Questo previene che un singolo server venga sovraccaricato, garantendo una performance ottimale per tutti gli utenti. Stante le stringenti limitazioni sul budget, ho selezionato esclusivamente Load Balancer software, ma in commercio esistono Load Balancer hardware, più prestanti. Le soluzioni individuate sono:

- NGINX Plus (prezzo stimato per licenza annuale tra i 2.000 e i 4.000 euro)
- HAProxy (soluzione Open Source, non ha costi)

ULTERIORI CONSIDERAZIONI SUL BUDGET

Come evidenziato nel capitolo precedente, l'architettura di rete proposta è stata accuratamente progettata per massimizzare il livello di sicurezza e resilienza per l'applicazione e-commerce, rimanendo però all'interno del budget allocato di €20.000 - €30.000. Ritengo questo budget non sufficiente alle necessità di un'azienda in rapido sviluppo.

In particolare, l'allocazione di un budget più ampio avrebbe consentito l'acquisto di un Sistema di Gestione Eventi e Informazioni di Sicurezza (**SIEM**). Questo software raccoglie, normalizza e correla i log e gli eventi di sicurezza da tutti i dispositivi e servizi della rete, fornendo una panoramica centralizzata su tutti gli aspetti della sicurezza e identificando in tempo reale pattern di attacco complessi.

Applicando una stima per un'azienda di medie dimensioni, ho identificato alcune valide soluzioni che andrebbero a rafforzare la sicurezza della rete:

- Splunk Enterprise Security (prezzo stimato dai 50.000 ai 200.000 euro l'anno)
- Microsoft Sentinel (prezzo stimato dai 18.000 ai 60.000 euro l'anno)
- IBM QRadar (prezzo stimato dai 40.000 ai 150.000 euro l'anno)

Altri campi di intervento in presenza di un budget più elevato riguardano l'acquisto di un Load Balancer hardware (in sostituzione di quello software incluso attualmente), un'Appliance WAF Dedicata (in sostituzione di quella inclusa nel servizio di protezione da DDoS) e l'acquisto di licenze per scanner di vulnerabilità automatici.