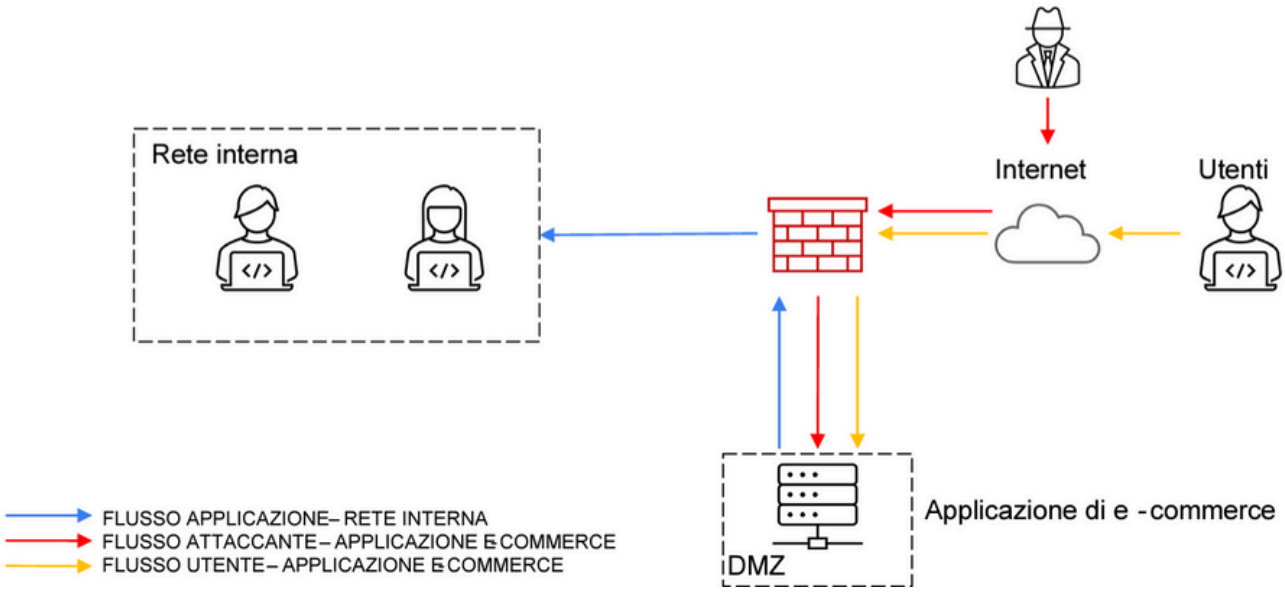
S9-L5 Analisi LOG

Emulo Francesco

Disegno rete di partenza:



Traccia numero 1

Per difendere la nostra applicazione da attacchi SQLi o XSS possiamo alterare la logica di rete inserendo un NGFW o un WAF che, sebbene simili in quanto a scopo (sicurezza applicativa), operano con approcci e specificità differenti.
Analizziamo nel dettaglio i due casi e come la loro implementazione possa difenderci.

Sia i ***NGFW*** che i ***WAF*** offrono protezioni vitali contro XSS e SQLi, ma lo fanno con approcci differenti.

S9-L5

Analisi LOG

Traccia numero 1

Emulo Francesco

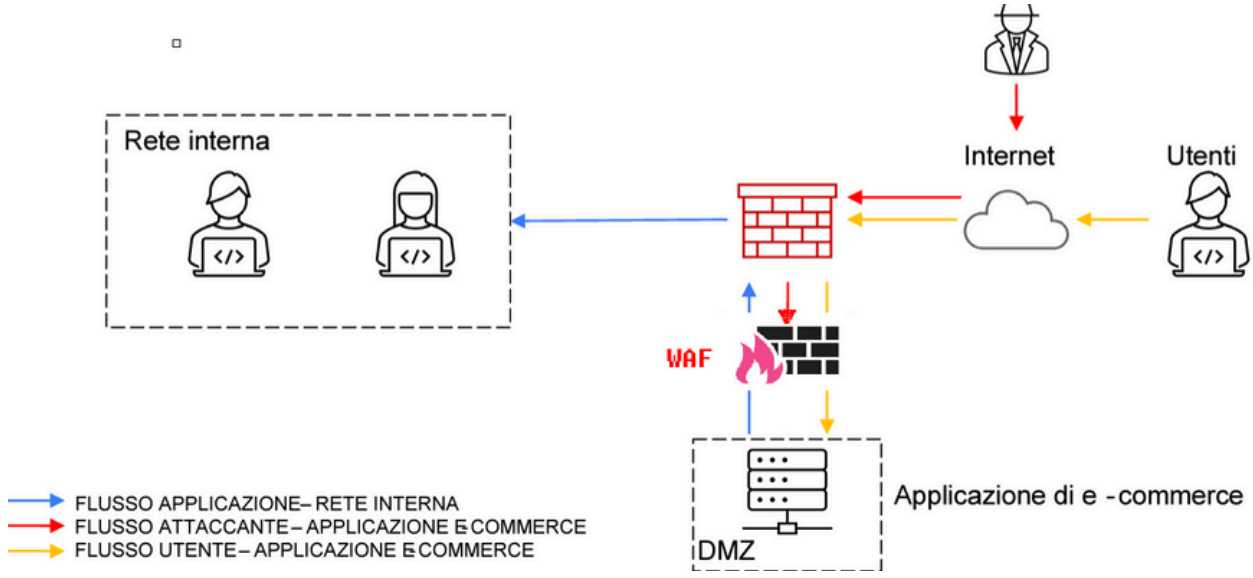
Web Application Firewall

La prima differenza sostanziale fra questi due firewall riguarda i ***Layer*** del modello ISO/OSI sul quale operano.
Chiarito questo, vediamo le tecniche di protezione che adattano.

- ***WAF***, operano al **Layer 7** (Livello applicativo), responsabile della gestione delle applicazione e dei servizi di rete (compresi HTTP, HTTPS, FTP).
- Questi firewall analizzano e filtrano il contenuto delle query e delle risposte web andando a proteggere l'applicazione dagli attacchi sopra citati (SQLi ed XSS)

.

  - Filtraggio rule-based, tramite un insieme di regole dettagliate riescono ad ispezionare il traffico web bloccando input dannosi;
  - Utilizzo di Pattern e Firme di minacce, contengono dei database aggiornati regolarmente nei quali vengono incluse le firme di nuove vulnerabilità utili a migliorare la capacità di rilevamento di XSS ed SQLi;
  - Protezione da vettori di attacco specifici, i WAF possono difendere l'applicazione da attacchi basati sull'utilizzo di caratteri speciali volti a manipolare query SQL o XSS tramite url.



S9-L5 Analisi LOG Traccia numero 1

Emulo Francesco

Next Generation Firewall

- ***NGFW***, questi firewall, invece, operano su **più strati** del modello ISO/OSI, come:
  - **Layer 3** (livello di rete), a questo layer analizzano e filtrano i pacchetti basandosi sull'IP (instradano il traffico ed applicano regole IP-based);
  - **Layer 4** (livello di trasporto), a questo layer ispezionano informazioni relative i protocolli di trasporto TCP ed UDP filtrando in base ai numeri di porta e sessione;
  - **Layer 7** (livello di applicazione), come i WAF possono ispezionare il contenuto del traffico a livello applicativo utilizzando funzionalità come il DPI (Deep Packet Ispection) ed altri, vediamoli:

    - ***Ispezione livello applicativo***, gli NGFW possono identificare e bloccare potenziali attacchi identificando script malevoli XSS o query SQL non autorizzate mediante l'analisi del payload delle richieste;
    - ***Firme e Pattern di minacce***, medesimo meccanismo dei WAF (sopra trattato);
    - ***Rilevamento di anomalie***, la loro notifica permette di identificare comportamenti sospetti o non convenzionali a livello del traffico di rete (indice di possibilit entativi di exploit).
    - ***IPS***, i NGFW integrano la funzionalità di Intrusion Prevention System (utile per meglio delineare lo schema di rete logico dell'immagine della traccia 4);
    - ***DPI***, tecnica avanzata che consente di esaminare il contenuto dei pacchetti di dati in modo dettagliato (blocca payload malevoli nel traffico, ed il traffico criptato, permettendo l'identificazione di Trojan ed altri malware prima che raggiungano il target)

S9-L5

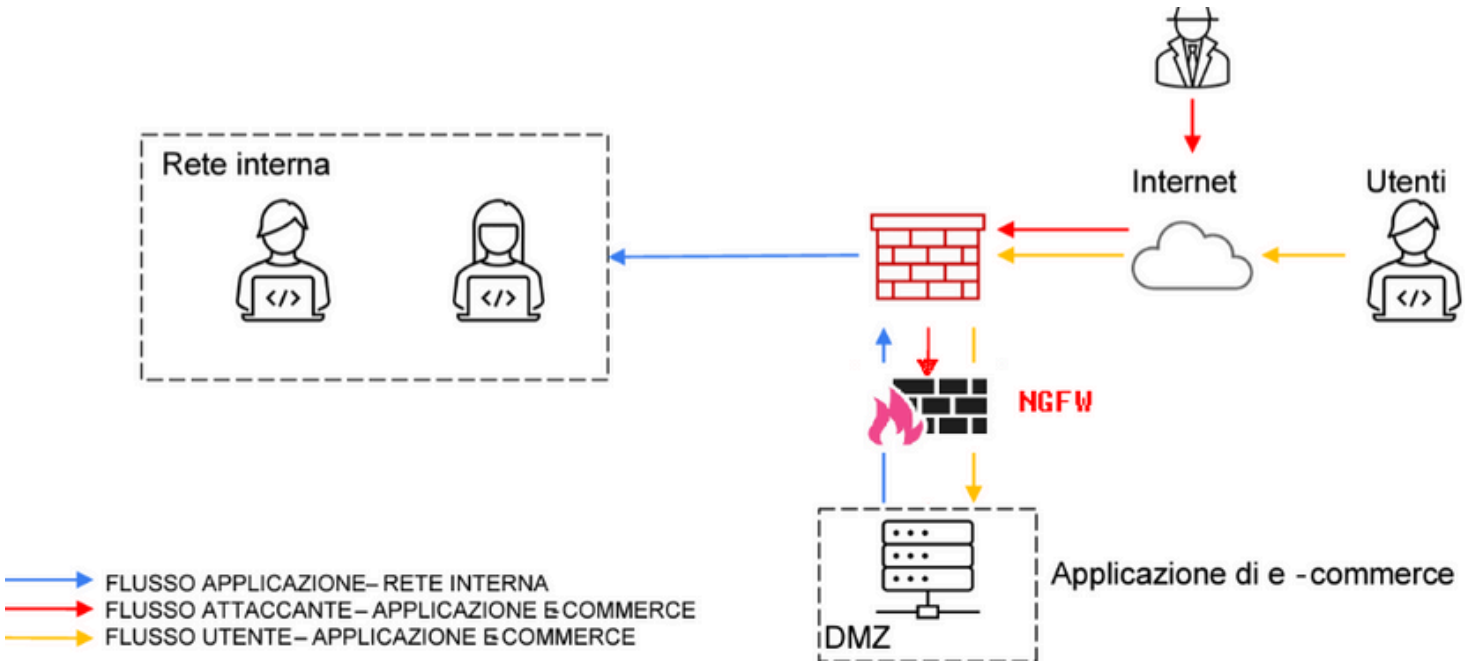
Analisi LOG

Traccia numero 1

Emulo Francesco

Next Generation Firewall

Schema di rete



Emulo Francesco

Traccia numero 2

Iniziamo calcolando **l'impatto sul business** dovuto alla non raggiungibilità del servizio.
Se l'interruzione del servizio ha una durata di 10 minuti, ed in media ogni minuto gli utenti spendono 1.2k$ sulla piattaforma e-commerce, il calcolo per individuare la **perdita complessiva** è:

Tempo di disservizio (in minuti) x Perdita economica (al minuto) = Perdita complessiva

10 x 1200 = 12k$

Questa perdita appena calcolata è la ***perdita diretta***; tuttavia questo non è l'unico danno che l'azienda in questione riporta essa, infatti, subirà anche una ***perdita indiretta*** a livello reputazionale e di mistrust:

- **Danno reputazionale**, la non raggiungibilità del sito può comportare una trustless da parte dei clienti verso l'azienda, evento a cui fa seguito un'eventuale riduzione delle vendite future;
- **Perdita di clienti**, l'insoddisfazione potrebbe comportare il passaggio di parte della clientela alla concorrenza.

Emulo Francesco

Traccia numero 2

Analizziamo, quindi, come ridurre la possibilità di incombere in attacchi DDos e, quando inevitabili, come contenere le perdite.

- Implementazione di **soluzioni** di rete verso **DDos**

  - **Soluzioni di Rete**
    - ***NGFW***, l'implementazione di un NGFW aiuta a rilevare e mitigare questa tipologia di attacco bloccando il traffico in base a regole predefinite e firme d'attacco;
    - ***IPS***, analizzando il traffico in tempo reale può rilevare attacchi DDos e bloccare i pacchetti sospetti prima che giungano al target;
    - ***CDN***, le Content Delivery Network distribuiscono il contenuto su una rete di server siti in diverse località geografiche (distribuzione del carico di lavoro);
    - ***Limitazioni di rete***, impostare un massimo di traffico generabile da un singolo IP può aiutare a prevenire tale tipologia di attacco.

  - **Altre** soluzioni
    - ***Monitoraggio***, un monitoraggio attivo volto a rilevare anomalie nel traffico di rete può incrementare la proattività di risposta.
    - ***Ridondanza***, implementare la ridondanza può aiutarci a mantenere la disponibilità dei servizi anche in caso di attacchi DDoS
    - ***Pianificazione della Business Continuity plan***.

Emulo Francesco

Traccia numero 3

In questo caso veniamo a conoscenza del fatto che la nostra **web-app** sia stata **infettata** da un malware.

Le **tipologie di malware** che statisticamente compaiono con maggiore frequenza in queste circostanze sono:

- ***Trojan***, ovvero programmi malevoli che si fingono software legittimi. Questi trojan sono spesso il mezzo tramite il quale un'attaccante si garantisce un accesso non autorizzato al sistema (seguito dall'installazione di una backdoor utile a bypassare, in un secondo momento, le normali procedure di autenticazione);

- ***Virus***, sono tipologie di malware che si replicano attaccandosi a file o programmi. Quando il file viene eseguito, il virus si attiva e comporta danni (come la corruzione di dati e la cancellazione di file);

- ***Worms***, simili ai virus, questi possono auto-replicarsi senza necessitare di un file host. I worms diffondono rapidamente attraverso rete ed applicazioni web a dispositivi collegati, causando interruzioni e perdite di dati.

S9-L5

Emulo Francesco

Analisi LOG

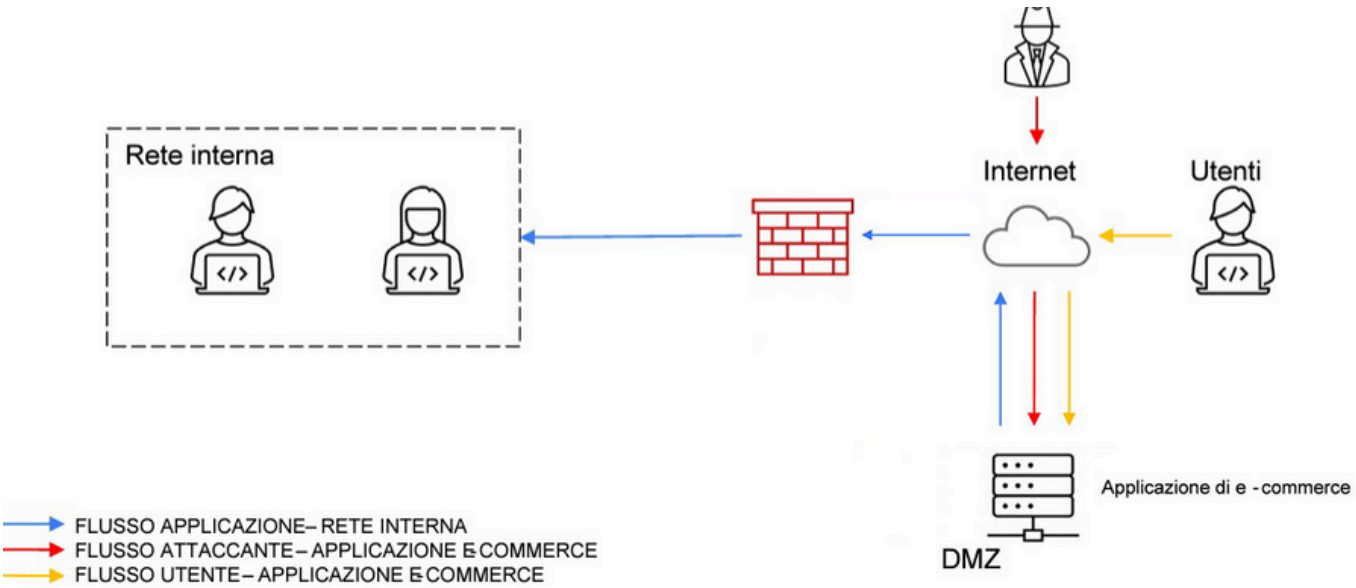
Traccia numero 3

Possibili risoluzioni

La traccia ci chiede di non rimuovere l'accesso dell'attaccante alla macchina infettata e di mettere in sicurezza la nostra rete. Queste condizioni ci fanno comprendere come la soluzione di ***rimozione*** non sia contemplata.

Concentriamoci, quindi, sul comprendere pro e contro dell'**isolamento** e della **quarantena**.

Analizziamo il **disegno di rete** realizzato, argomenteremo tali scelte nella slide successiva:



Emulo Francesco

Traccia numero 3

Quarantena

- ***Quarantena***, con questa tecnica andiamo a mettere in una subnet differente la macchian infettata, tuttavia questa soluzione, sebbene rapida, non è sicura quanto l'isolamento (sebbene il suo fine sia quello di isolare la minaccia per evitare che diffonda ulteriormente a tutta la restante rete): l'attaccante, se esperto, potrebbe bypassare la quarantena e compromettere le altre parti dell'infrastruttura di rete (come l'intranet), sebbene in subnet differenti. La tecnica più utile a tale fine è il Pivoting.

    - **Pivoting**, tecnica utile ad accedere a reti diverse o segmenti di rete utilizzando un host compromesso. Le principali tipologie di Pivoting sono:

        - ***Proxy Pivoting***, il sistema compromesso viene sfruttato come proxy per reindirizzare il traffico verso altre macchine o segmenti di rete (altrimenti inaccessibili), come l'intranet. Come tool viene utilizzato SSH tunneling principalmente;
        - ***VPN Pivoting***, l'attaccante configura una VPN sul target compromesso utile a far sembrare che tutto il traffico proveniente dal suo dispositivo arrivi, in realtà, dal sistema compromesso. L'host, nel caso della quarantena, ha accesso diretto alla subnet interna, motivo per il quale, in questo caso, tale impostazione di rete è sconsigliato.

Emulo Francesco

Traccia numero 3

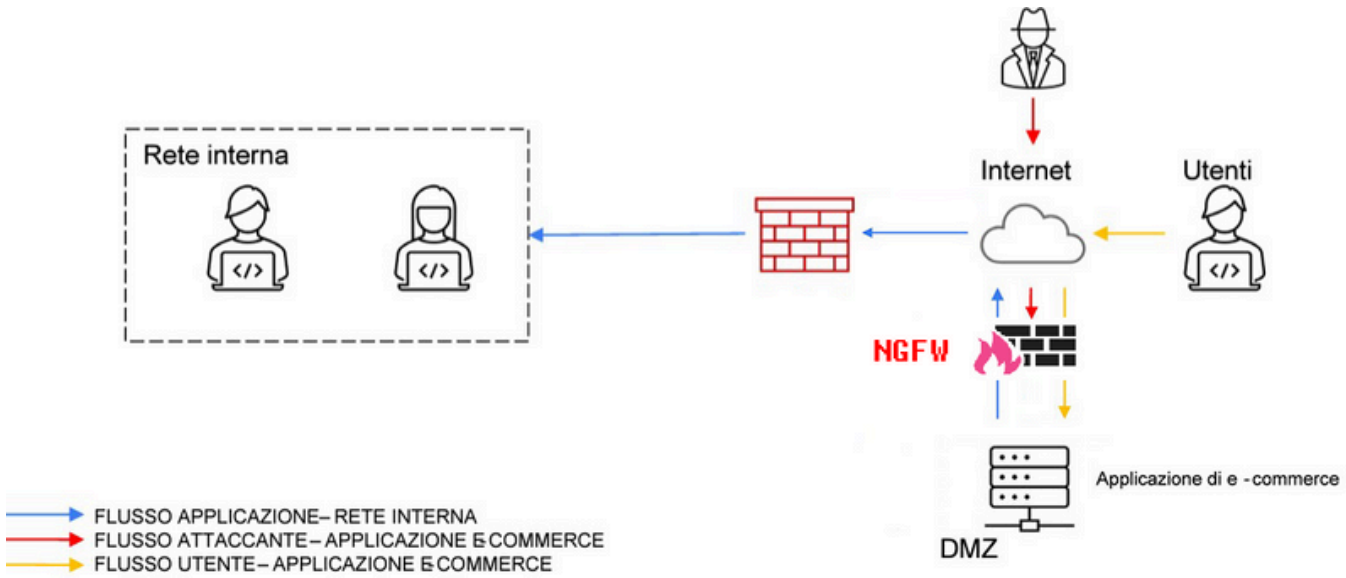
Isolamento

Isolamento, questa tecnica è quella migliore in questo caso dato che può restringere l'accesso dell'attaccante alla rete interna e mantiene il sistema infetto ancora accessibile dall'attaccante via internet (come richiesto dalla traccia).

Emulo Francesco

Traccia numero 4

Unendo le soluzioni uno (facciamo l'esempio del NGFW in modo da prevenire i malware e bloccare l'attaccante) e tre, quello che otteniamo è l'isolamento della macchina infetta ed una protezione verso una vasta gamma di attacchi (guarda le caratteristiche che ci hanno portato a scegliere questo device di rete nella traccia numero uno).



Emulo Francesco

Traccia numero 5

Honeypot

Considerando come schema di rete definitivo quello della task 4, possiamo aggiungere, per una modifica ancora più aggressiva dell'infrastruttura, un ***honeypot*** nella DMZ.
Un honeypot è una trappola digitale progettata per attirare e studiare attività malevole, permettendo agli amministratori di rete di monitorare e analizzare i tentativi di attacco.

Posizionando l'honeypot in questo segmento, si può monitorare e analizzare il traffico proveniente da potenziali attaccanti che tentano di accedere alle risorse pubblicamente esposte.
L'honeypot può essere configurato per simulare vulnerabilità comuni nelle applicazioni web (**bassa interazione**), attirando così i tentativi di intrusione; o può essere configurato per ricreare un ambiente copleto che può registrate attività avanzate e sofisticate da parte degli attaccanti (**alta interazione**).

L'installazione dell'honeypot può **distogliere il focus** degli attaccanti dai sistemi critici ed aiutarci a raccogliere informazioni su di loro o sui metodi da loro attuati.

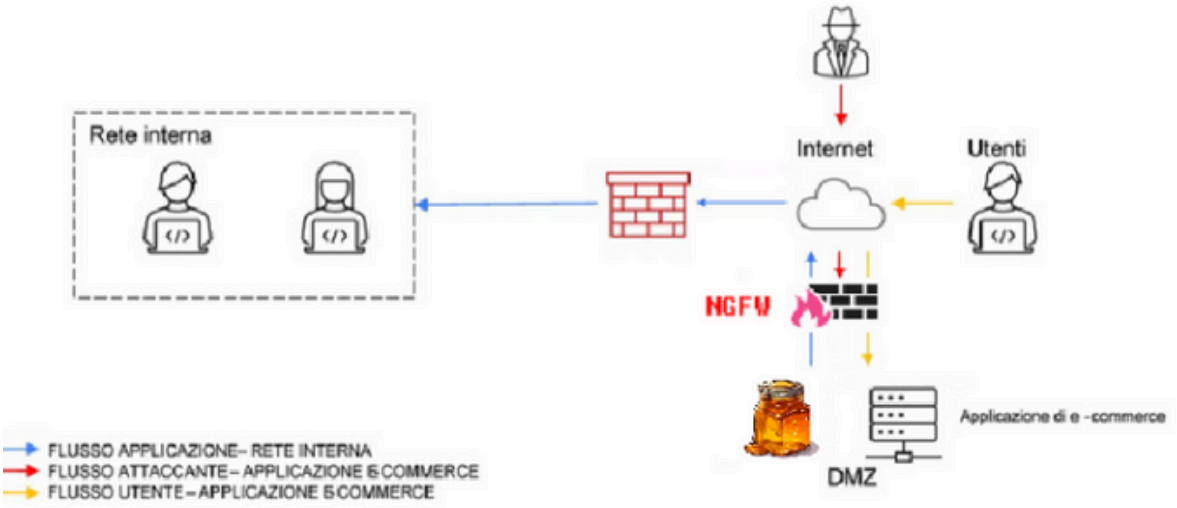
Circa i **prezzi**, questi variano molto. Si passa, infatti da cifre di 2-5k$ a licenza per Honeypot ad alta interazione (come quello di KFSensor), fino a 10k per soluzioni complete di analisi dettagliata degli attacchi e reportistica avanzata (caso di HoneyDB by Binary Defense).

NB: L'honeypot lo possiamo inserire sotto il NGFW affianco alla DMZ (posizione strategica).

S9-L5 Analisi LOG

Traccia numero 5

Emulo Francesco



Traccia numero 5

NGFW e ridondanza

Circa il NGFW, invece, considerando un budget di 5-10k, possiamo selezionare un **NGFW di livello avanzato** (utilizzato nelle medie e grandi imprese).

I principali NGFW che rientrano in questo budge sono il “**Palo Alto Networks PA-850**” ed il “**Cisco FortiGate 100F**”.

Entrambe le soluzioni sono progettate per gestire reti complesse con requisiti di sicurezza rigorosi e forniscono funzionalità avanzate come l’**ispezione del traffico crittografato**, la **prevenzione delle intrusioni**, il **controllo delle applicazioni** etc. Avere due firewall garantisce ridondanza, il secondo deve essere configurato in modalità ***failover (standby)*** in modo da intervenire se il primo fallisce senza interrompere il traffico di rete.

Server di ridondanza

Nella zona DMZ possiamo configurare altri server per l’applicazione e-commerce in modo da effettuare un bilanciamento del carico per gestire meglio il traffico tra i server.