

RICCARDO LEPORE

Security OPERATION



Contenuti

- 01** AZIONI PREVENTIVE
- 02** IMPATTI SUL BUSINESS
- 03** RESPONSE
- 04** SOLUTION



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?

01

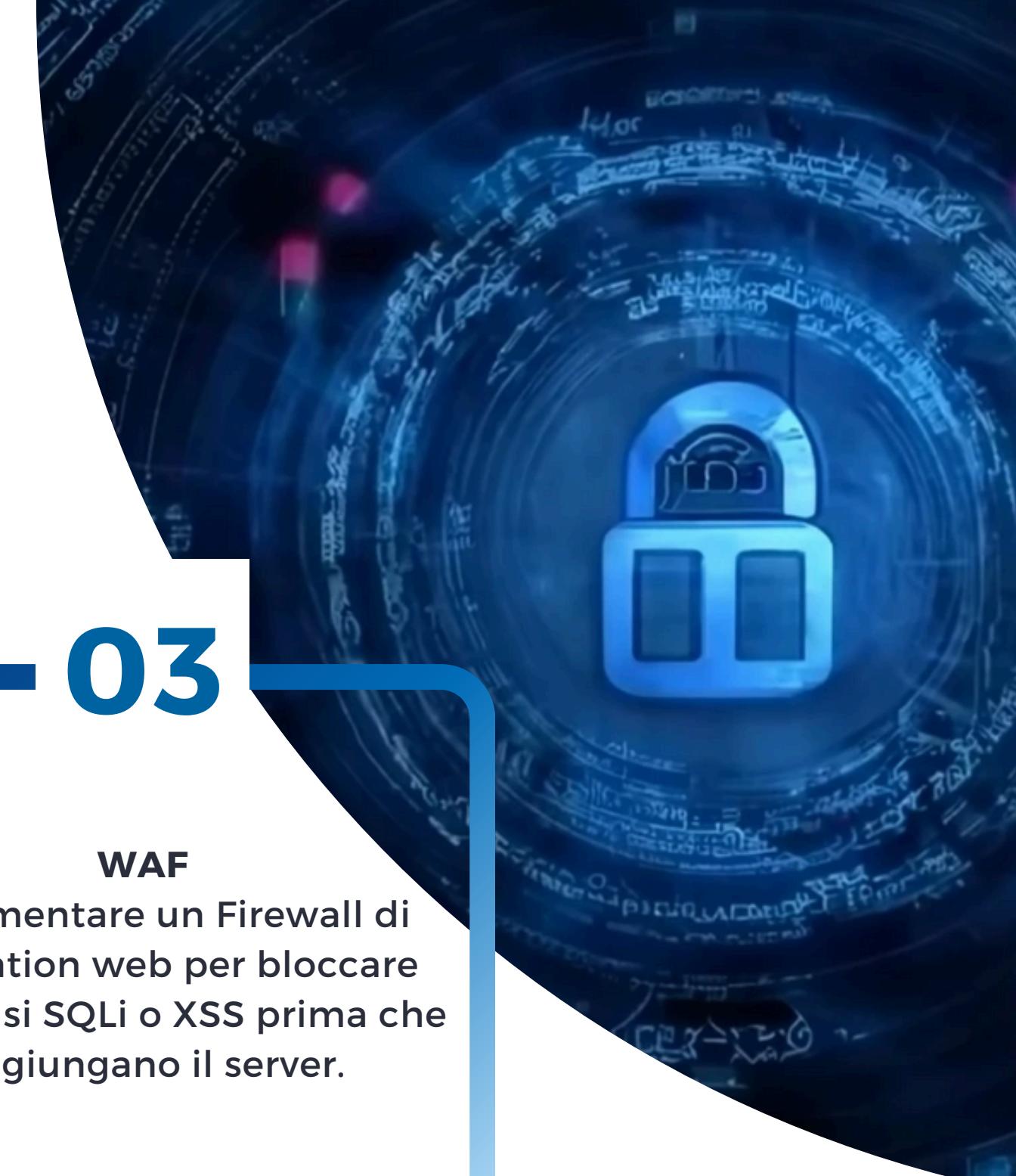
PARAMETERIZED QUERIES
Implementare query specifiche per impedire che l'input dell'utente venga interpretato come parte di una query SQL. Questa tecnica garantisce che i valori passati come input vengano trattati come dati e non come comandi SQL.

02

SANIFICAZIONE INPUT
Implementare policy di sanificazione degli input degli utenti per evitare che un utente malevolo provi a sfruttare dei caratteri speciali per inserire delle query malevoli.

03

WAF
Implementare un Firewall di application web per bloccare attacchi si SQLi o XSS prima che raggiungano il server.



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?

04

CSP

Implementare delle Content Security Policy in modo da limitare i contenuti esterni e per prevenire l'inserimento di codice malevolo.

05

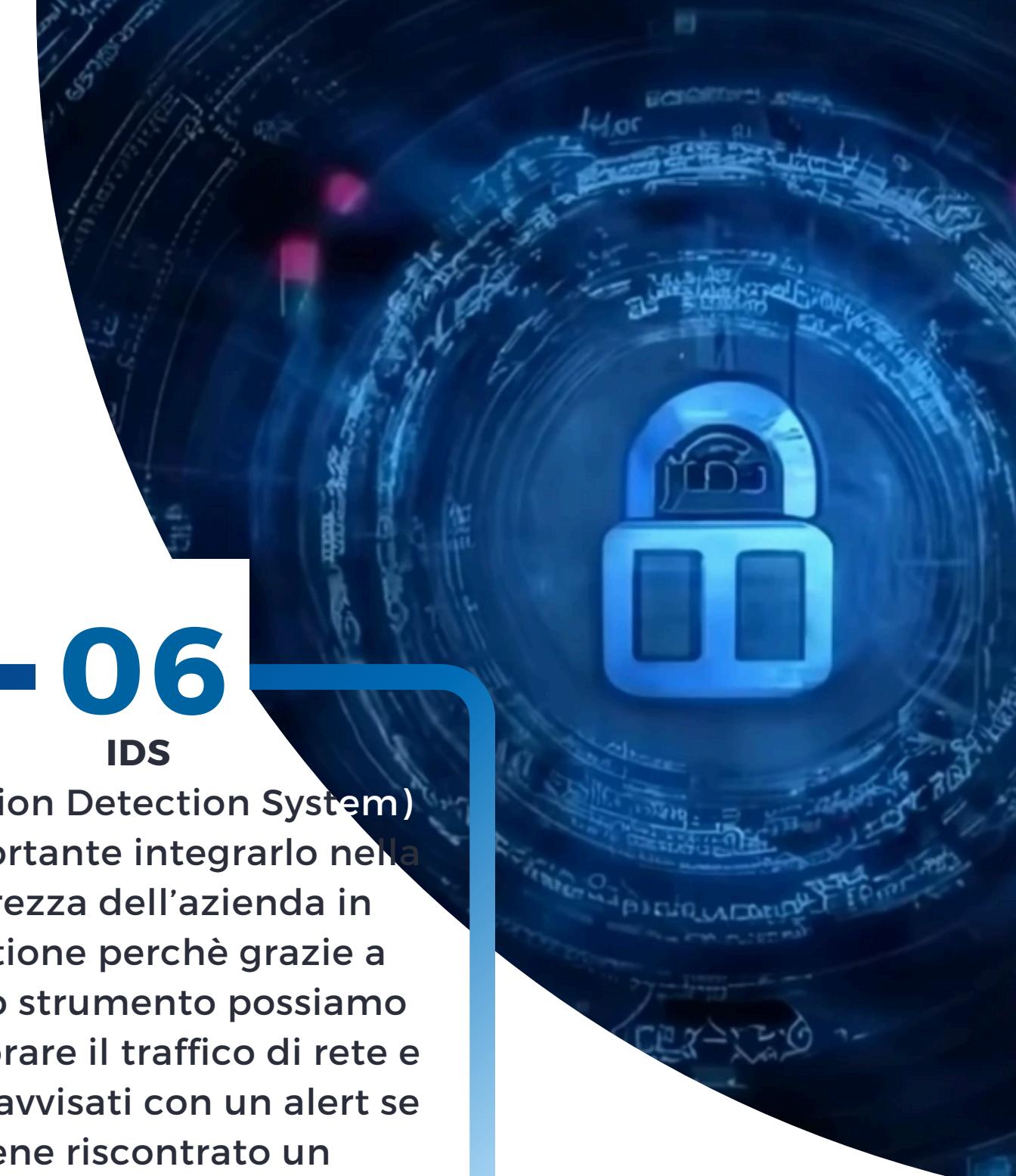
ESCAPING

Implementare questa tecnica è utile per far sì che ogni carattere inserito dall'utente venga interpretato come tale e non come del codice HTML O SQL.

06

IDS

(Intrusion Detection System)
E' importante integrarlo nella sicurezza dell'azienda in questione perchè grazie a questo strumento possiamo monitorare il traffico di rete e essere avvisati con un alert se viene riscontrato un comportamento anomalo.



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?

07

IPS (PRO-EDITION)
(Intrusion Prevention System)
E' una soluzione ottima perchè monitora in tempo reale il flusso di rete cercando di rilevare comportamenti anomali ancora prima che possano fare danno all'azienda target.

08

RATE LIMITING (PRO EDITION)
Si possono integrare dei limiti sulla quantità di richieste che un singolo indirizzo IP può fare in un certo intervallo di tempo per prevenire l'esaurimento delle risorse soprattutto se sappiamo che se un server dovesse essere attaccato i rimanenti dovrebbero dividersi più carico di lavoro

09

NAC (PRO-EDITION)
Introdurre un NAC è di fondamentale importanza per gestire e controllare gli accessi all'interno della rete interna assicurandoci che solo i dispositivi autorizzati posano avere accesso alla rete interna o agli asset da proteggere.



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?

10

CLOUD

Implementare una soluzione cloud a livello di sicurezza e gestione delle memorie è ottimale per proteggere i dati da attacchi esterni in quanto offre tantissimi strumenti di monitoring e prevenzione delle minacce e in più per i fattori scalabilità disponibilità delle risorse

11

BACKUP

Fare dei backup ricorrenti è un strategia necessaria per permettere all'azienda di ripristinare i sistemi in caso di incidente.



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.

Per calcolare l'impatto economico di un'interruzione del servizio, come in questo caso di attacco DDoS, si utilizza la formula del CoD (Cost of Downtime). Questa formula viene utilizzata quando viene stilato il Business continuity plan.

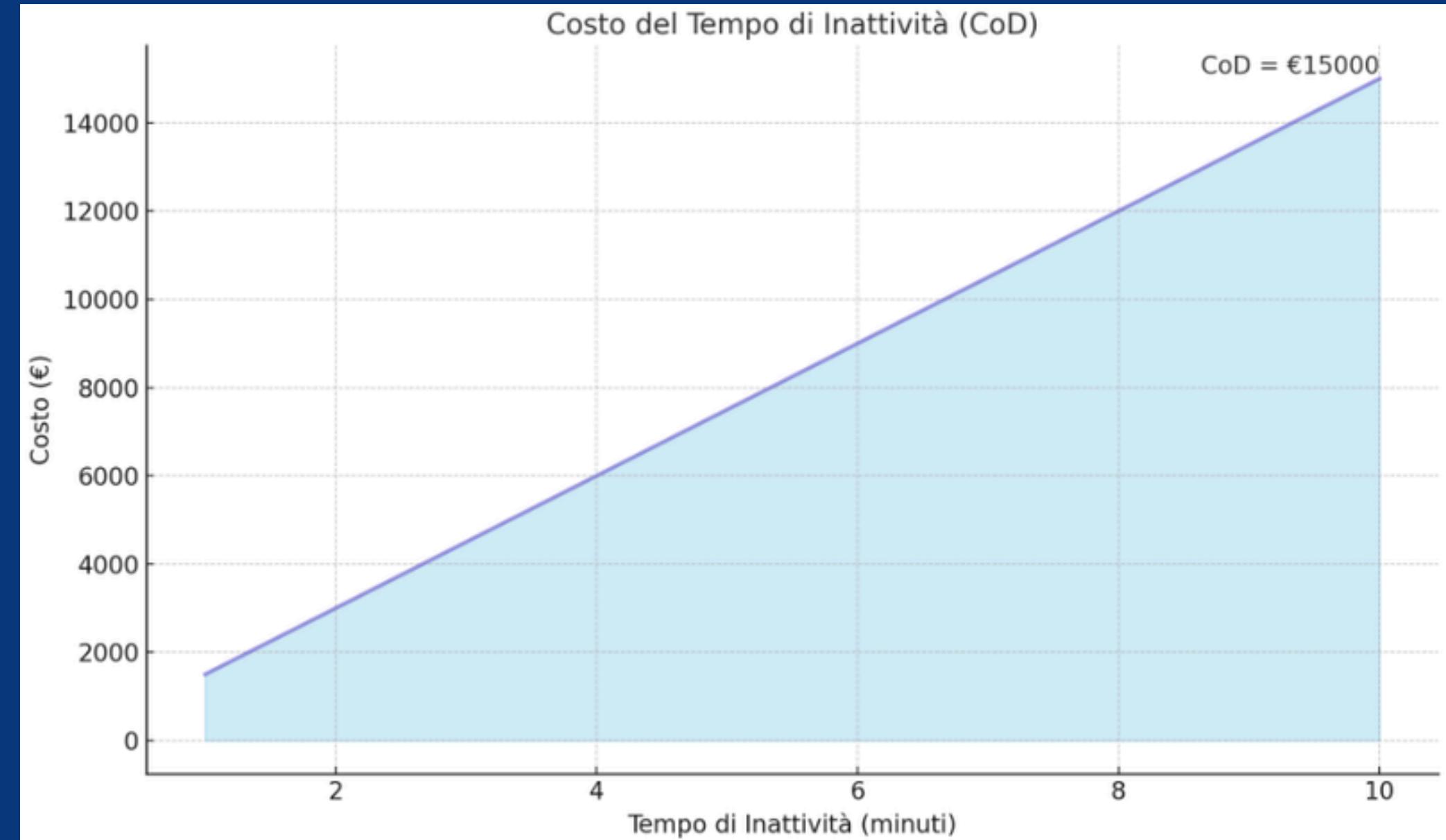
$$\text{CoD} = (\text{GpM} \times \text{TdI}) + \text{AC}$$

CoD = Costo del Tempo di Inattività

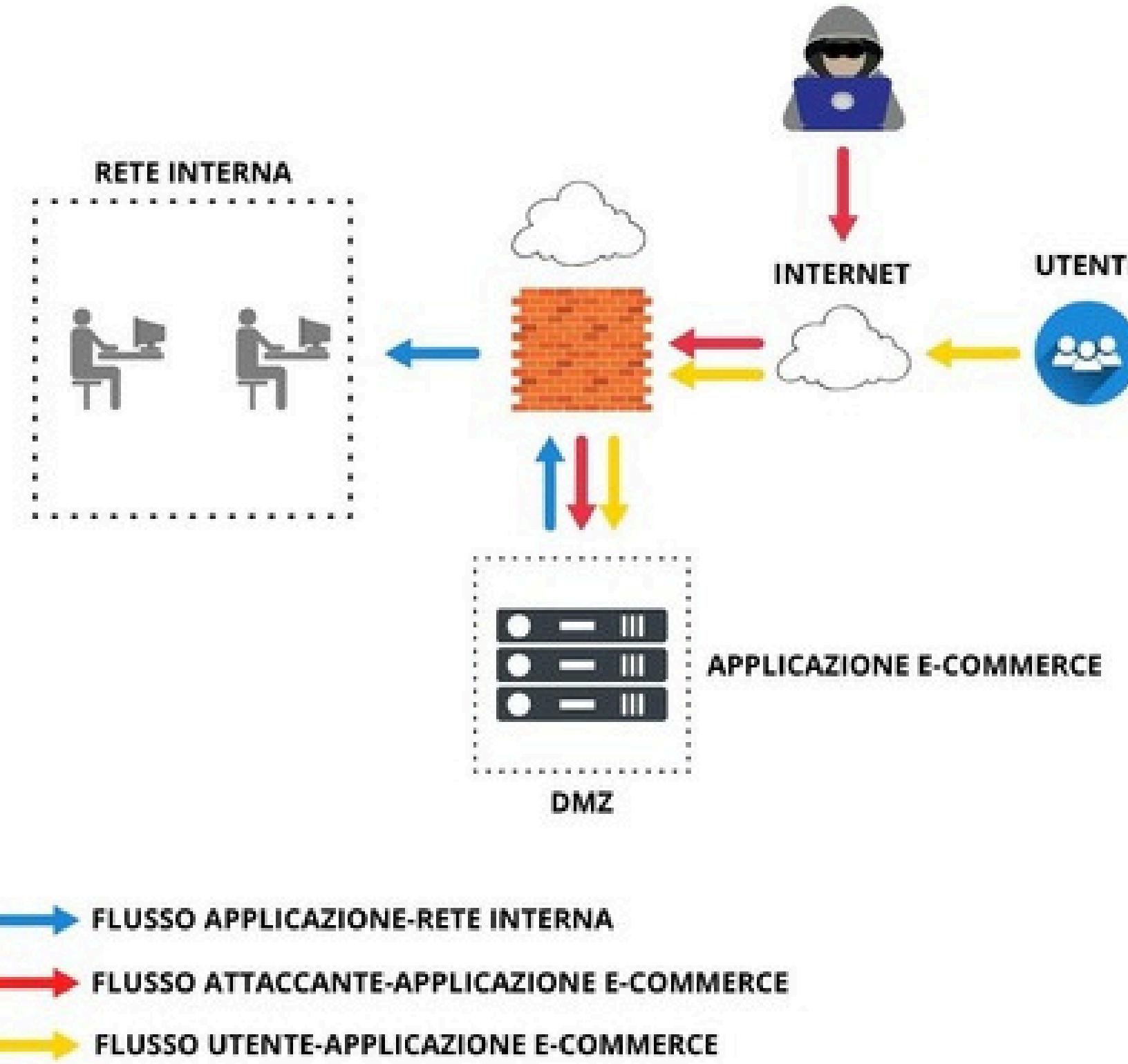
GpM = Guadagno per Minuto

TdI = Tempo di Inattività (in minuti)

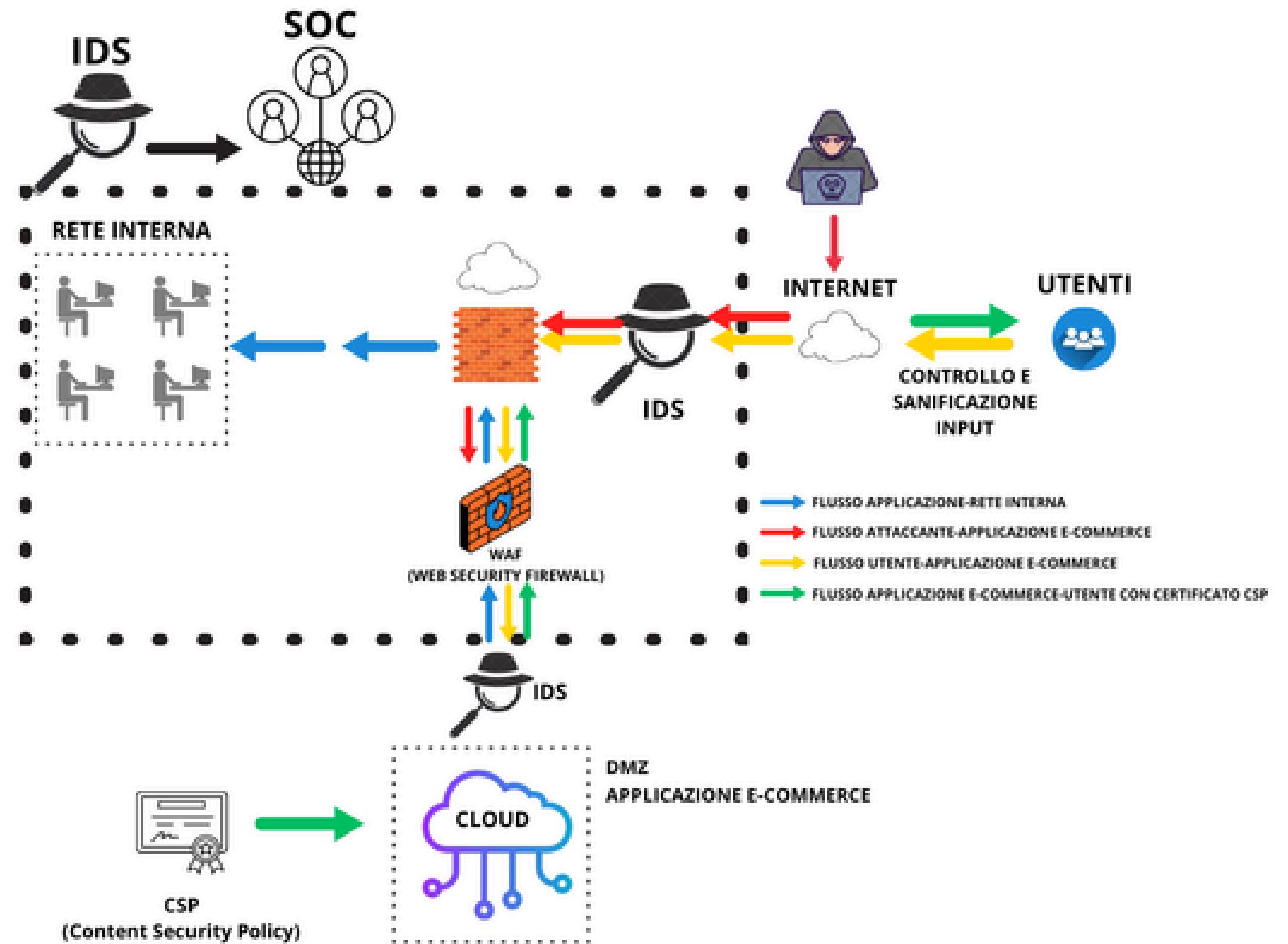
$$\text{CoD} = (1500 \text{ euro} \times 10 \text{ minuti}) = \\ \mathbf{15.000 \text{ euro}}$$



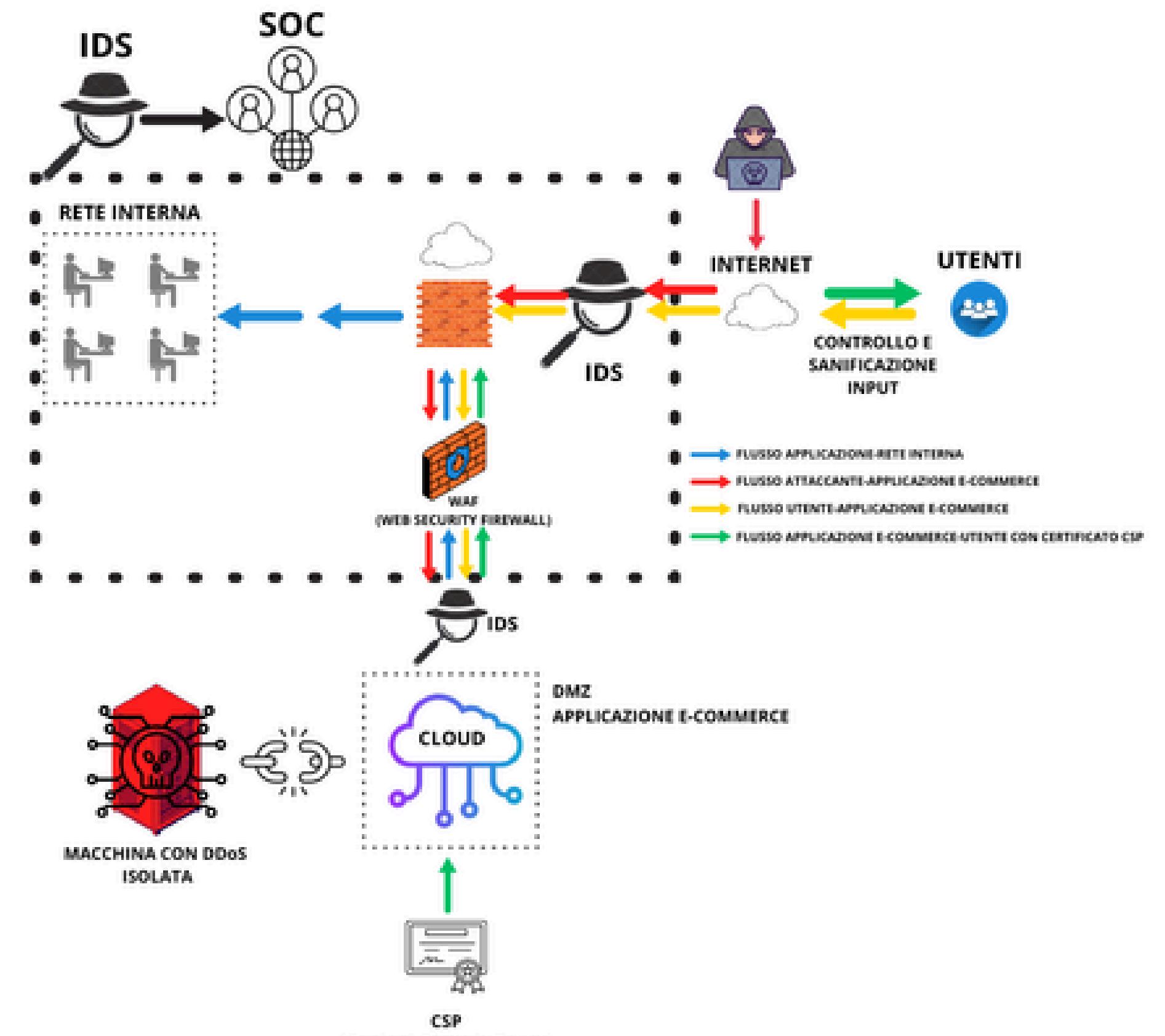
SITUAZIONE INIZIALE



AZIONI PREVENTIVE RETE STANDARD-EDITION



RESPONSE RETE STANDARD-EDITION

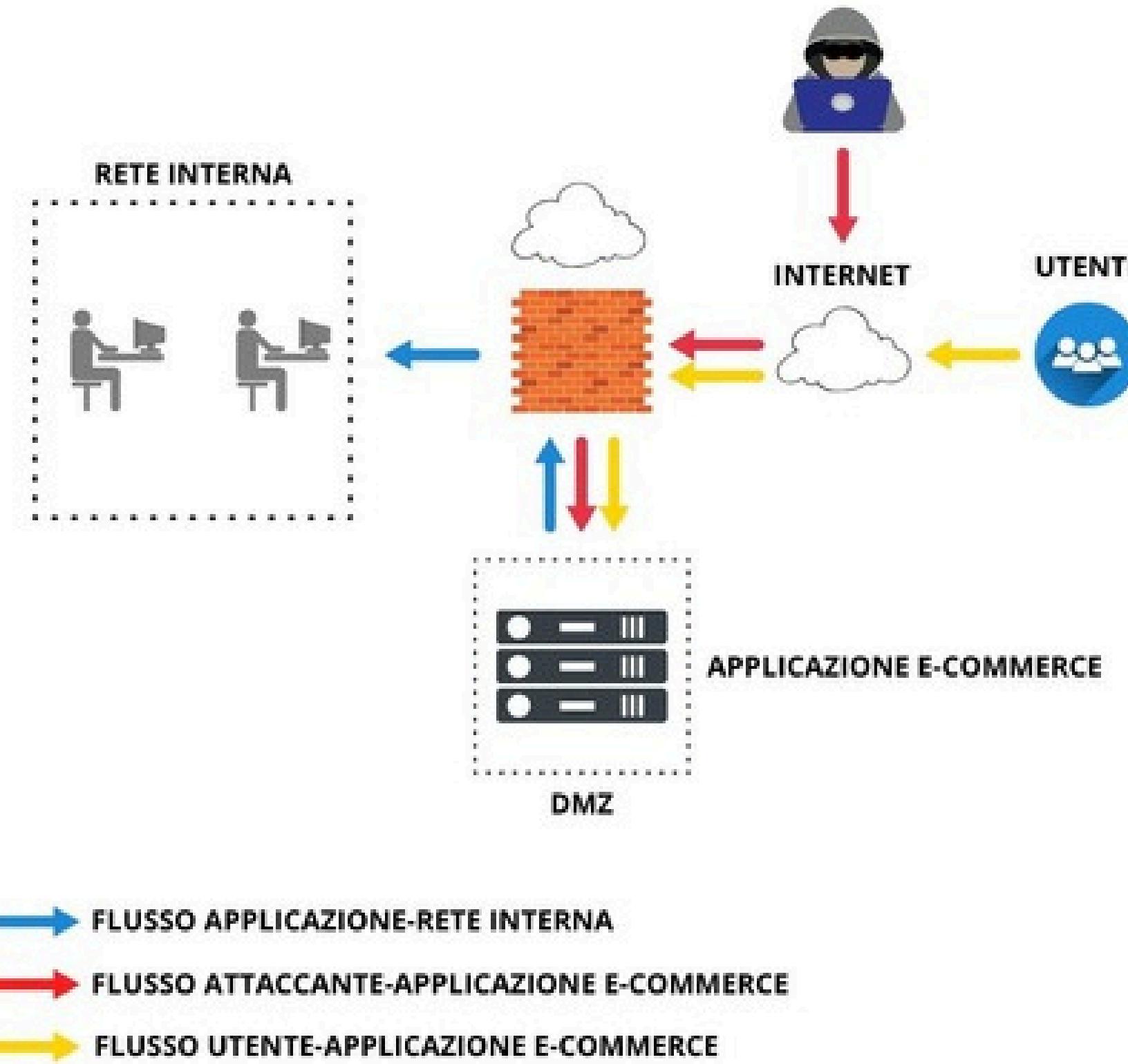




RETE PRO EDITION

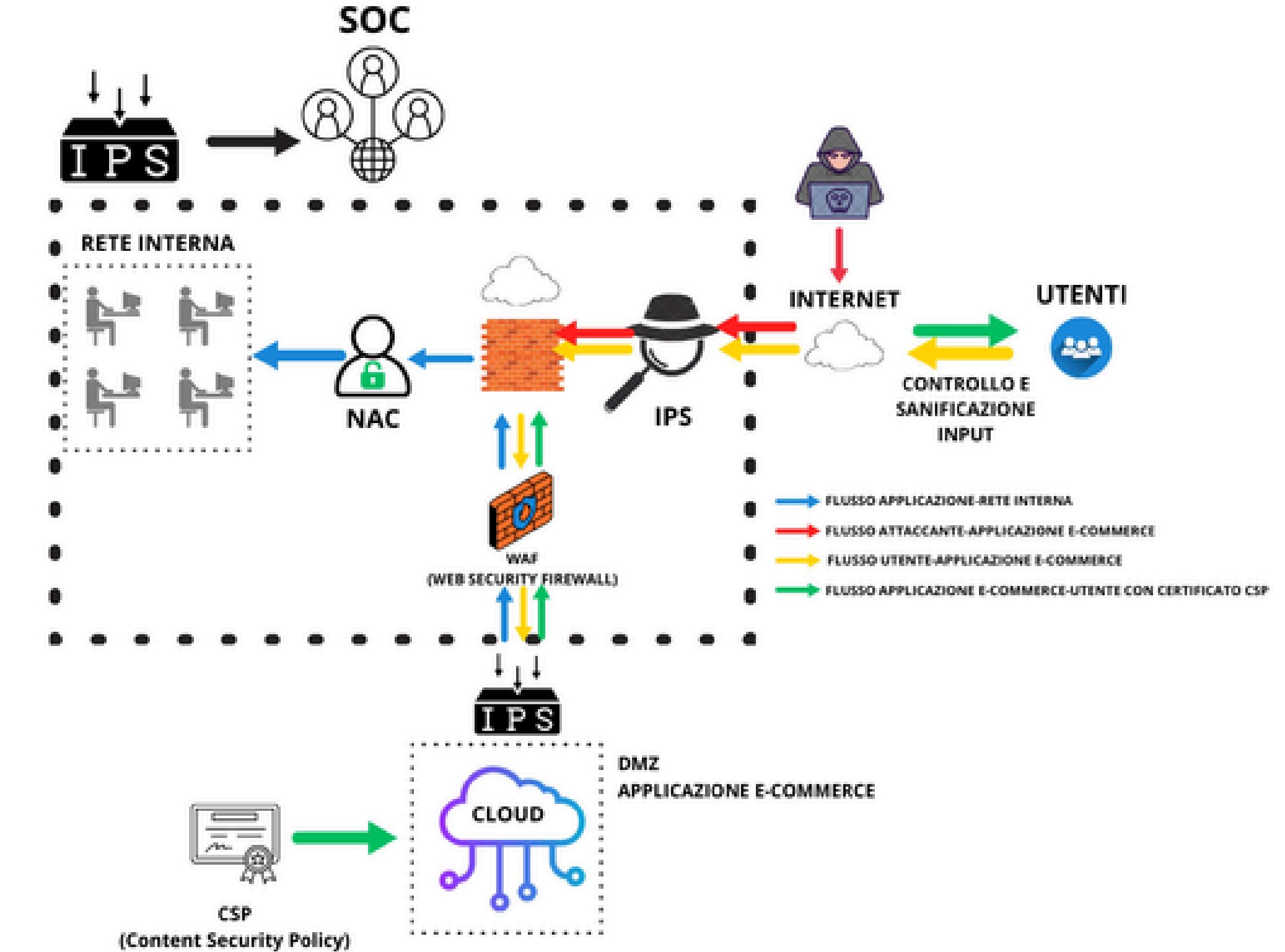
The logo consists of the word "RETE" in white capital letters to the left of a yellow rounded square button. The button has a dark blue border and contains the word "PRO" in large, bold, dark blue capital letters. To the right of the button is the word "EDITION" in white capital letters. The background is a dark blue circle with a light blue and white curved graphic element on the left side.

SITUAZIONE INIZIALE



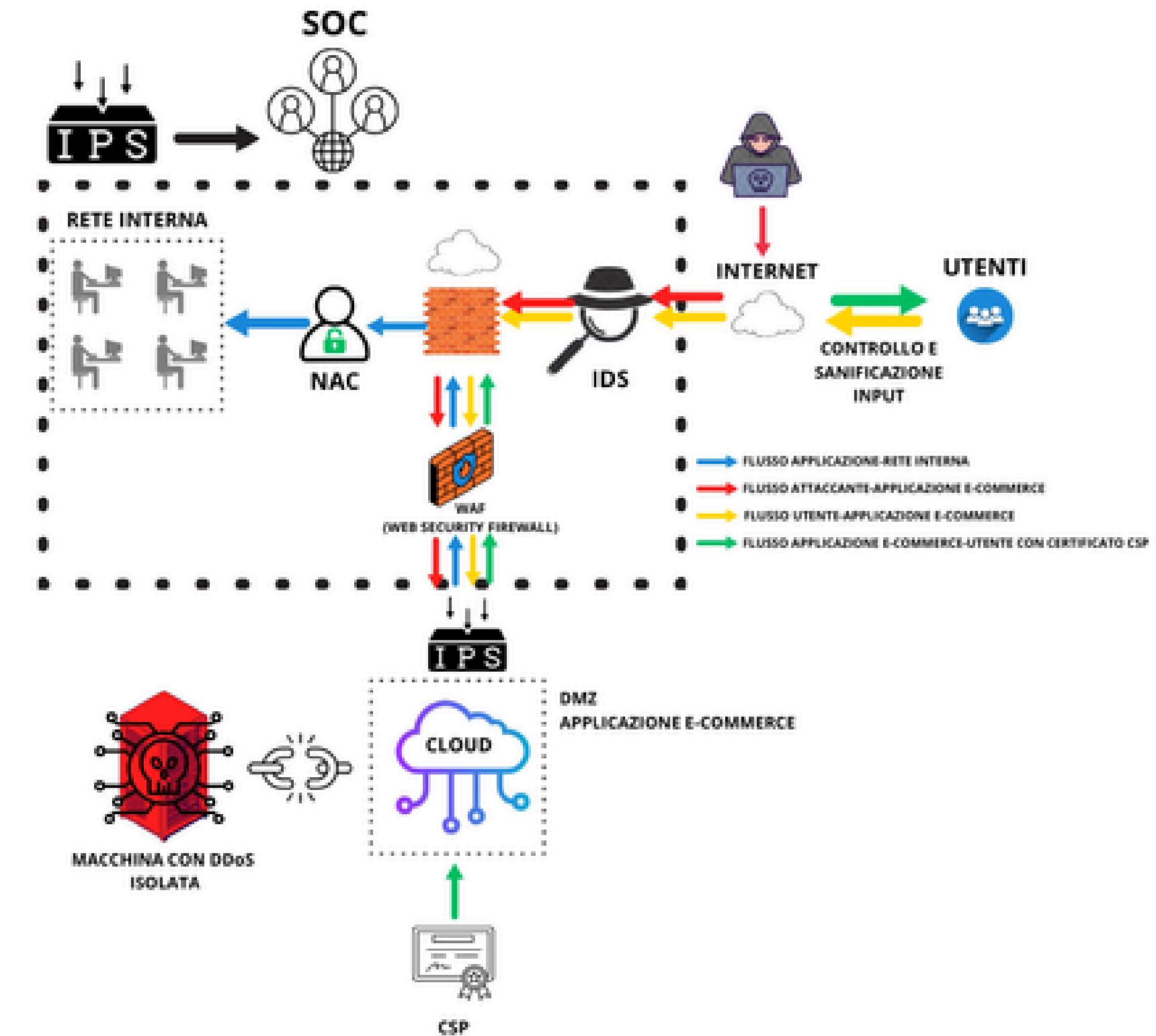
AZIONI PREVENTIVE

PRO EDITION



RESPONSE

PRO EDITION



RESPONSE

Una strategia per rispondere o addirittura prevenire la perdita di denaro dovuta all'attacco DDoS sarebbe quella di utilizzare un CLOUD ovvero un server virtualizzato che offre diversi servizi configurabili (a seconda dell'azienda) al suo interno.

Uno dei più utili ai fini della nostra esercitazione è quello della segmentazione delle risorse in quanto se una macchina dovesse essere attaccata da un malware sarebbe immediatamente isolata (può essere messa su una VPC) e il business non dovrebbe interrompersi a causa dell'attacco. Questo è fondamentale ai fini della business continuity poichè permette all'azienda di abbattere le perdite. Un'altra azione preventiva che offrono i servizi di cloud è quello dei BACKUP. Fondamentali per ripristinare i sistemi in una fase antecedente all'attacco.

RESPONSE

Altri strumenti che ho implementato nella figura sono:

- IDS(Standard edition) un sistema che monitora in tempo reale il traffico di rete in modo che se viene rilevato qualcosa di anomalo lancia un alert.
- IPS (Pro-edition) un sistema che monitora il traffico di rete e svolge in autonomia delle funzioni preventive per bloccare azioni malevole.

- WAF: Un Firewall fatto apposta per applicazioni web che filtri il traffico in entrata per evitare che possano essere fatti attacchi al target.
- CSP: delle policy per limitare l'utente in modo che non possa inserire codice malevolo come XSS e SQLi
- NAC: è un altro strumento che ho implementato che controlla gli accessi per evitare che utenti non autorizzati possano accedere alla rete interna aziendale.

MODIFICA

LE IMPLEMENTAZIONI DELLA RICHIESTA OVVERO INTEGRARE LA SOLUZIONE AGLI IMPATTI SUL BUSINESS E' STATA INTEGRATA NELLE IMMAGINI IN QUANTO INTEGRANDO UN CLOUD IL TDI VIENE AZZERATO O COMUNQUE DIMINUITO DI MOLTO POICHÉ' IL CLOUD OFFRE MOLTI VANTAGGI TRA QUI QUELLO DELLA SEGMENTAZIONE DELLE RISORSE; GRAZIE A STRUMENTI DI PREVENZIONE COME L'IDS SIAMO IN GRADO DI INDIVIDUARE E ISOLARE LA MACCHINA INFETTA (AD ESEMPIO IN UNA VPC VIRTUAL PRIVATE CLOUD) COSÌ IN FUTURO SI POTRA' ACCEDERE ALLA MACCHINA PER MONITORARE CIO' CHE È SUCCESSO ED EVITARE LA PROPAGAZIONE DEL DDoS E PREVENIRE UNO SCENARIO SIMILE IN FUTURO.



RICCARDO LEPORE

FINE PRESENTAZIONE



Mail

riccardo.lepore1997@gmail.com



Website

riccardo_lepore_cybersecurity_analyst.com



linkedin

[RICCARDO LEPORE](#)