TRACCIA

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

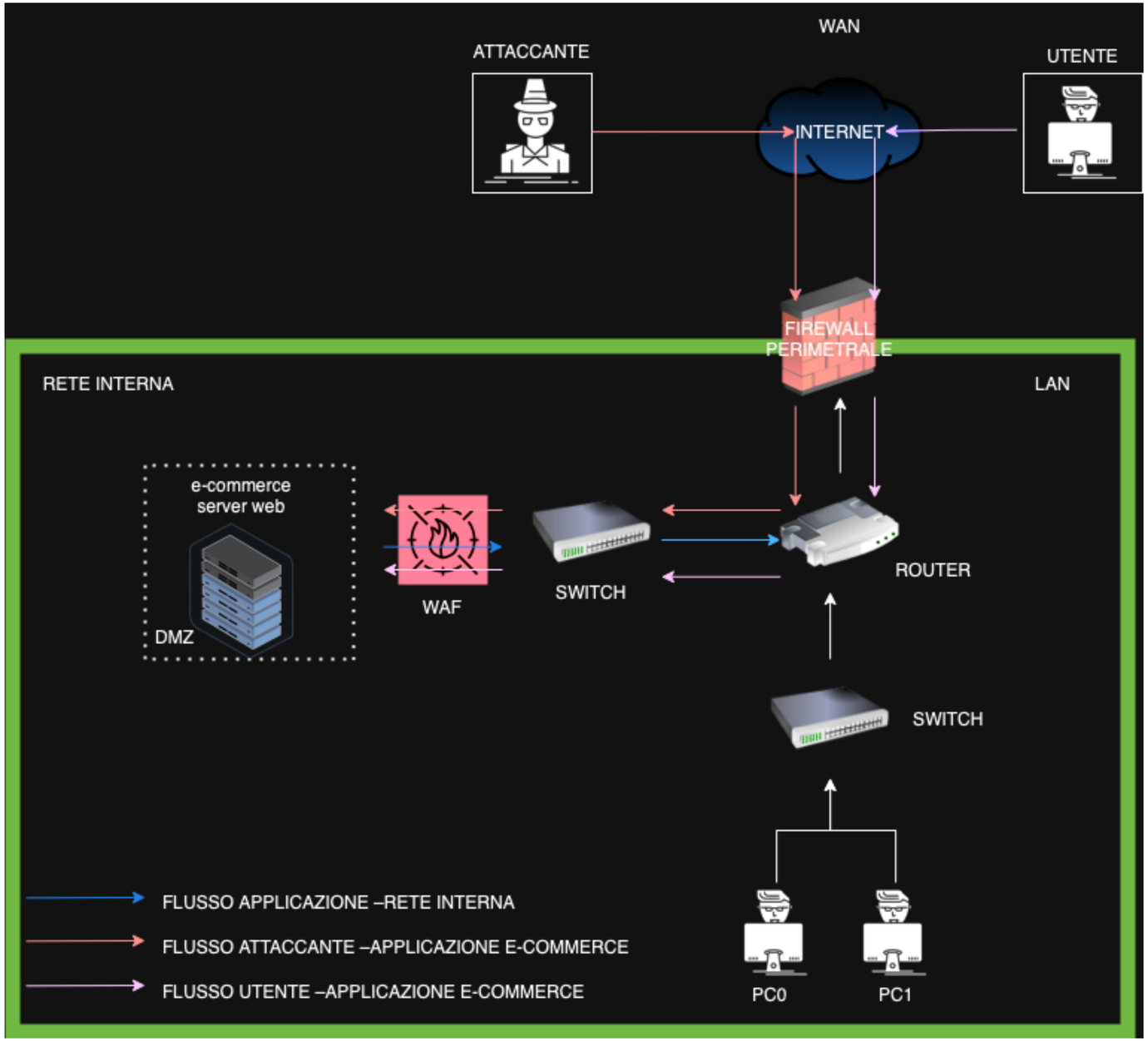
1.Azioni preventive : quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni

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)

Azioni preventive



Per proteggerci da attacchi di tipo SQLI oppure XSS, converrebbe agire modificando il codice sorgente dell nostro applicativo, andando ad implementare un sistema di “sanificazione” dell’input.Questo però potrebbe richiedere mesi di lavoro da parte del programmatore, andiamo perciò ad utilizzare un ***WAF.*** (Senza però escludere la possibilità di modificare anche il codice sorgente per andare a rafforzare l’applicazione)

Web Application Firewall cos’è ?

Funziona come uno scudo per le applicazioni web. Vediamo ora come potrebbe proteggerci da attacchi di tipo SQLI e XSS.

Protezione da SQL Injection (SQLi):

Filtraggio delle query SQL sospette.
Validazione dei parametri nelle richieste.
Uso di firme per riconoscere pattern noti di attacchi SQLi.

Protezione da Cross-Site Scripting (XSS):

Validazione rigorosa dell'input utente.
Filtraggio dei contenuti per rilevare e bloccare script dannosi.
Implementazione di header di sicurezza come **Content-Security-Policy (CSP)**.

Impatti sul business

Se la nostra applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per 10 minuti, per andare a calcolare l'impatto finanziario ci avvaliamo della seguente formula.

Calcolo dell'Impatto Finanziario:

- Impatto = (Tempo di Indisponibilità) x (Valore Monetario per Minuto Utente)
- Impatto = 10 minuti x 1.500 €/minuto

TOTALE = 15 000 EURO.

MITIGAZIONE :

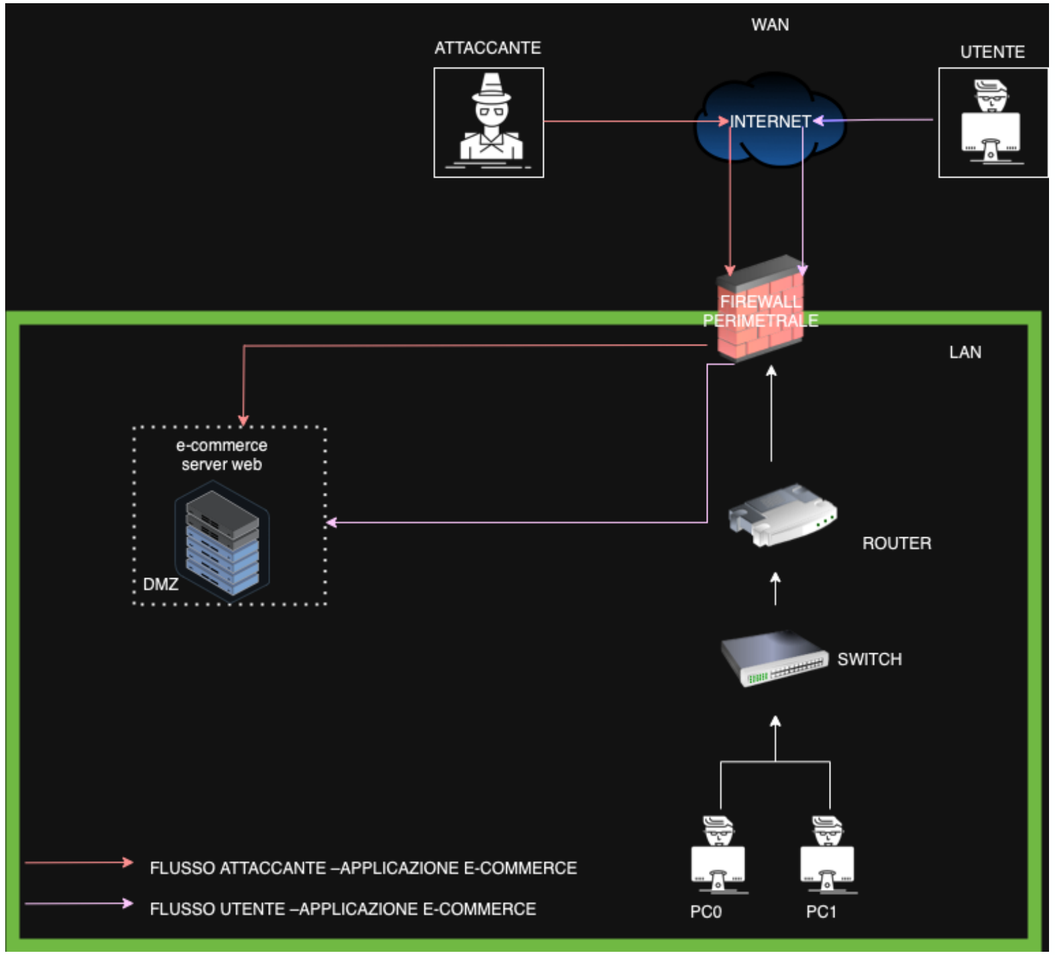
In primis devo avere un piano di risposta agli incidenti ben definito per agire prontamente quando si verificano questi attacchi, incluso anche un monitoraggio frequente del mio sistema, per anticipare attività compromettenti.

Disabilitazione delle richieste PING.

Utilizzo di provider online che forniscono sistemi di prevenzione da questi tipi di attacco (cloudflare.com).

Configurazione del Firewall per andare a bloccare gli IP sospetti.

RESPONSE

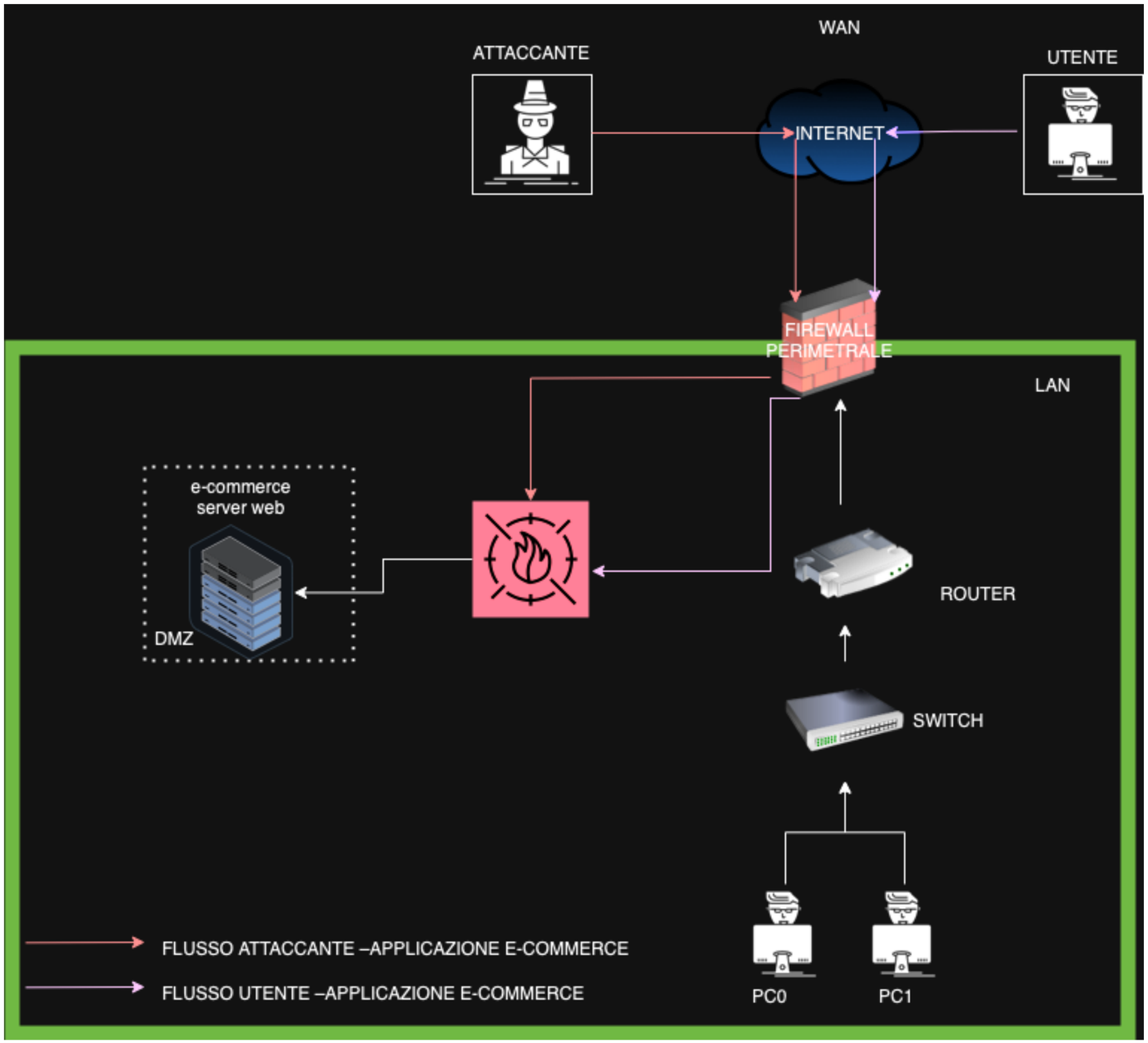


L'applicazione web è stata infettata da un malware, e la priorità è prevenire la propagazione del malware sulla rete interna.

Soluzione Proposta:

- **Isolamento Fisico:**
  Disconnettere fisicamente il server web infetto dallo switch che lo collega al router interno, riducendo il rischio di propagazione del malware sulla rete interna.
- **Configurazione del Firewall Perimetrale:**
  Configurare il firewall perimetrale per consentire solo il traffico strettamente necessario al server web infetto. Limitare le porte e i protocolli aperti al minimo indispensabile.

Soluzione completa



La soluzione completa prevede l'unione delle due soluzioni, proposte in precedenza. Server web isolato dalla rete interna e **WAF** per protezione da attacchi di tipo **SQLI** e **XSS**.

COSTI :

1 SWITCH : 1500 EURO
1 ROUTER : 1500 euro
1 server web : 2000 euro
2 firewall : 2000 euro