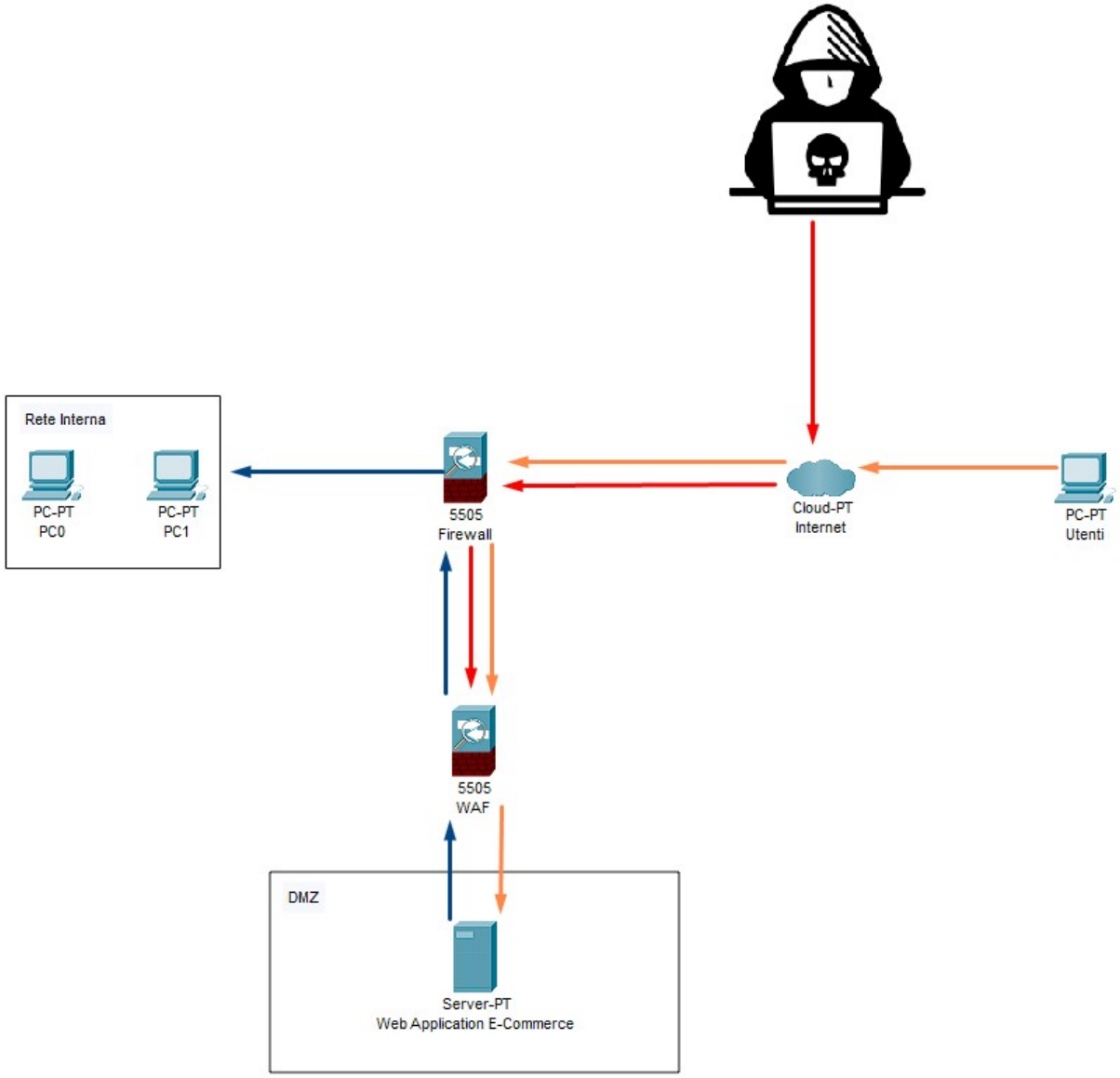
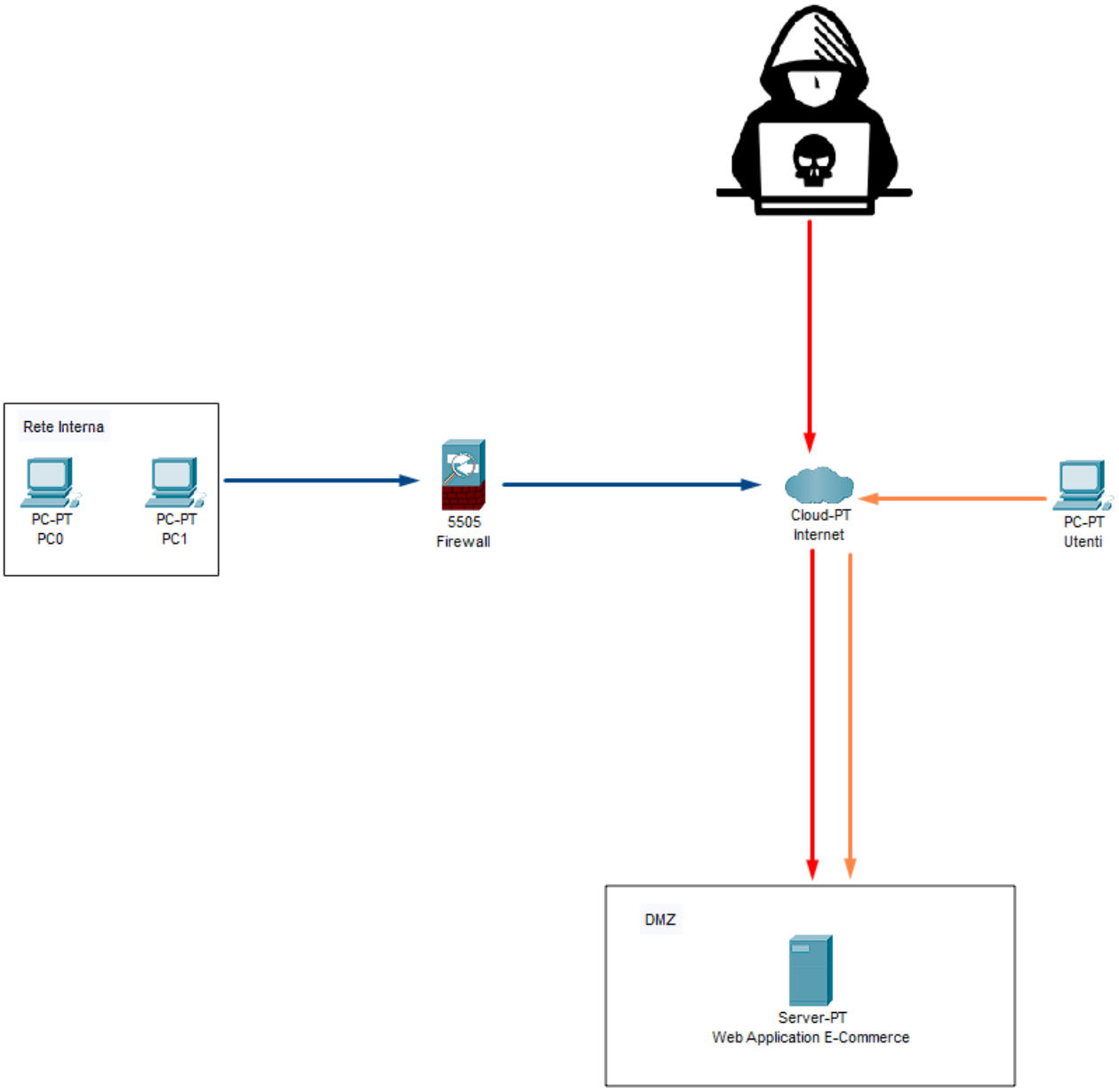
Alaimo Alessandro
23/12/2022

Report Weekend 9

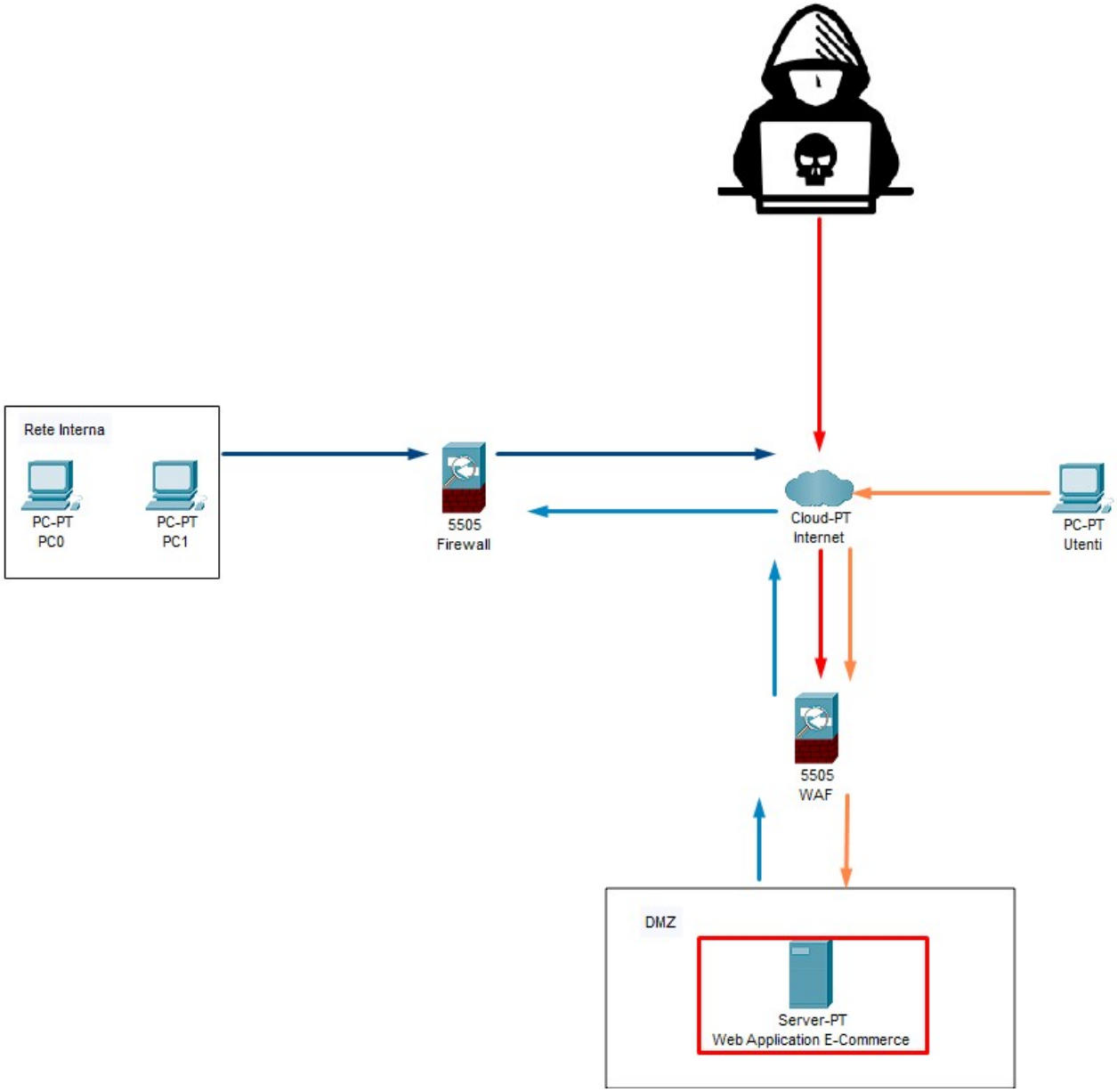
Data la casistica dell'esercizio dato, il nostro compito è quello di rimediare e attutire i danni dell'attaco di un hacker, calcolandone anche la perdita per il DDoS effettuato. Prima di tutto, partiamo dalle azioni preventive da implementare per evitare attacchi di tipo SQLi e XSS, aggiungendo un WAF come riportato di seguito:



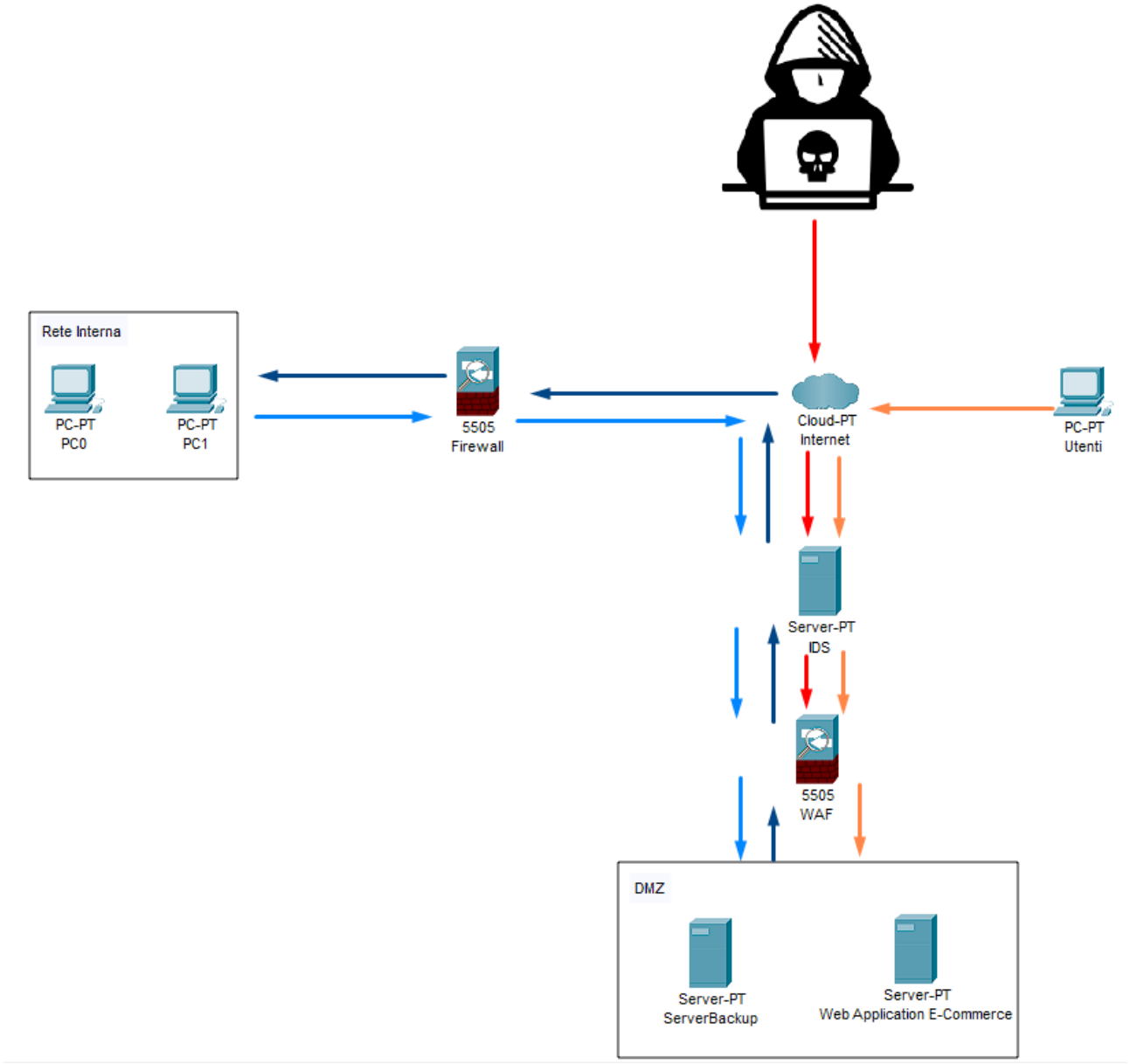
Dopodiché ci viene richiesto di calcolare la perdita di guadagno da 10 minuti di inattività, avendo come media un guadagno di €1500,00. Il calcolo da effettuare sarà di fatto 10*1500= €15.000,00 di perdita data dal DDoS. Ora andiamo a prendere in analisi il caso in cui il **Server** viene infettato da un Malware. Andiamo ad adottare un approccio di isolamento del **Server** oltre ad alzare una policy al **Firewall** nel quale verrà specificato che il **Server** non potrà comunicare con la rete interna, lasciandola libera di connettersi ad **Internet** come riportato di seguito:



Ora ritornando alla prima casistica, andiamo ad effettuare una remediation per essa, andando ad alzare una policy al **Firewall** in modo tale che il **Server Infetto** non comunichi con la **Rete Interna,** andando anche ad implementare un **WAF**:



Infine, nel caso vi è disponibile il capitale, andiamo a fare una modifica sostanziosa alla rete. Essa vedrà implementata un **IDS** per il controllo del traffico, il **WAF** ed un **Server di Backup,** nel quale andremo ad effettuare un **Full Backup** del **Server Principale** ogni Lunedì mentre nel mezzo della settimana andrà ad effettuare dei **Differential Backup,** che funzionerà al posto del **Server Principale** in caso esso non potrà erogare servizi:


Rete Interna
PC-PT
PC0
PC-PT
PC1
5505
Firewall
Cloud-PT
Internet
PC-PT
Utenti
Server-PT
IDS
5505
WAF
DMZ
Server-PT
ServerBackup
Server-PT
Web Application E-Commerce