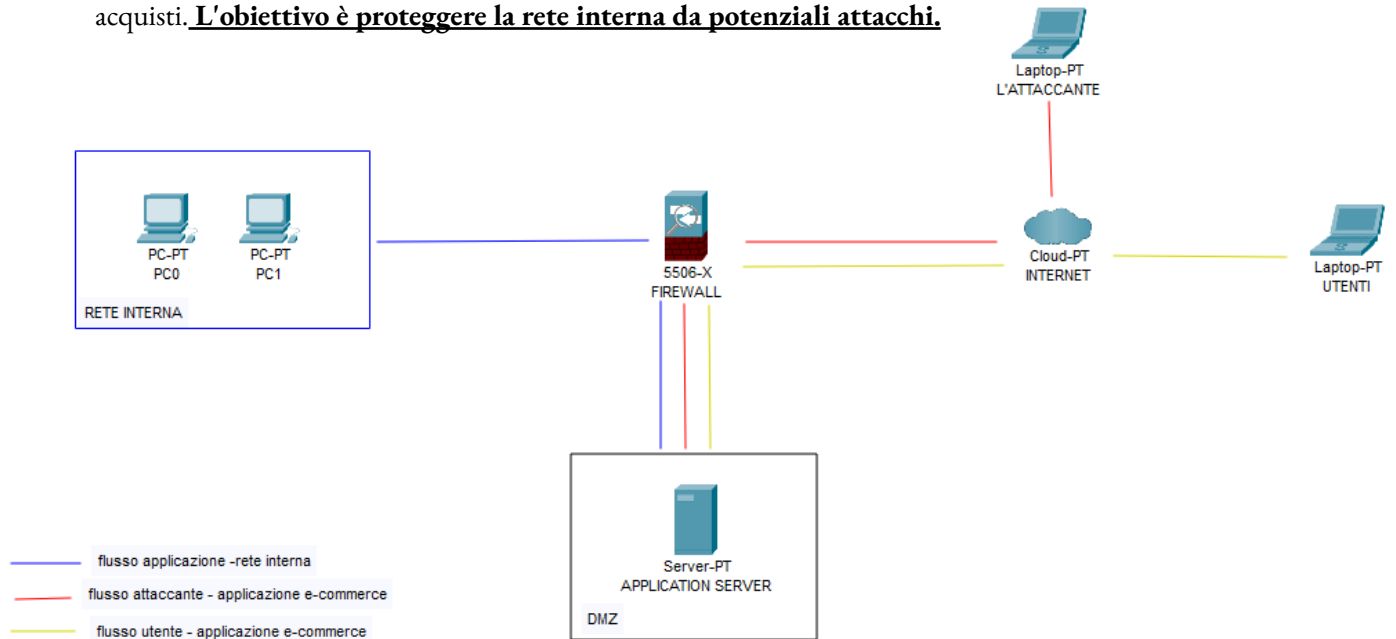


REPORT: Analisi dei log

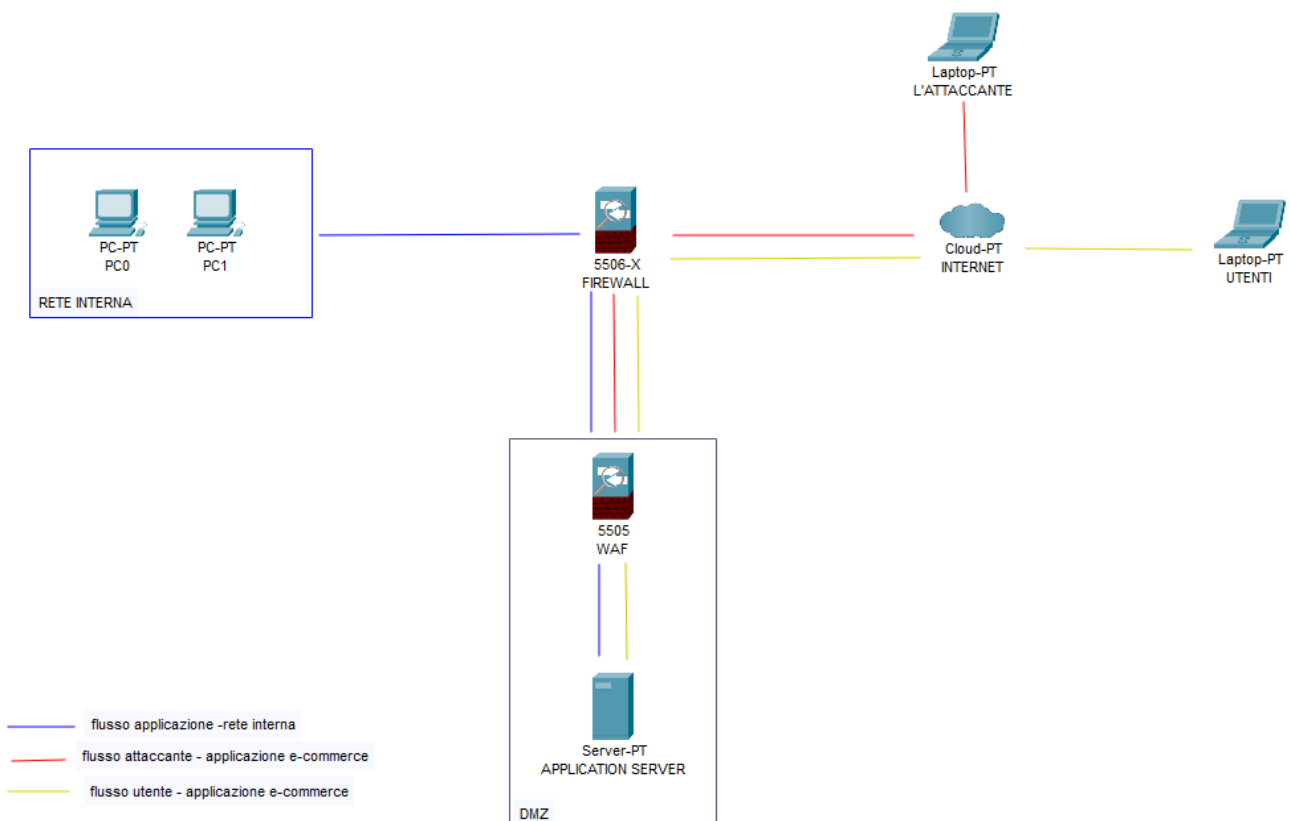
Eseguito da: **Anatoliy Prsyazhnyuk**, data: 30.06.2023

1. Azioni preventive:

L'ambiente di rete è stato modellato utilizzando **Cisco Packet Tracer**. È stato creato un'architettura composta da una **rete interna**, una **DMZ** contenente **un application server** e **un firewall** che funge da punto di ingresso verso **Internet**. Gli utenti si connettono a Internet attraverso il firewall per effettuare acquisti. **L'obiettivo è proteggere la rete interna da potenziali attacchi.**



Per mitigare i rischi di attacchi di **SQL Injection e XSS**, è stato implementato **un Web Application Firewall (WAF)** tra il firewall e l'application server. Il **WAF** agisce come un filtro aggiuntivo per rilevare e bloccare tentativi di attacco prima che raggiungano l'application server, impedendo all'attaccante di accedere alla **rete interna**.



REPORT: Analisi dei log

2. Analisi degli URL sospetti

Sono stati forniti due URL sospetti da analizzare: <https://tinyurl.com/linklosco1> e <https://tinyurl.com/linklosco2>. Per determinare la natura di questi link, sono state eseguite diverse scansioni utilizzando **VirusTotal**, **UrlVoid** e **HydraAnalysis**.

<https://tinyurl.com/linklosco1> e <https://tinyurl.com/linklosco2>

Visualizzando i link nella SandBox, nel primo link: viene scaricato un **DNS Changer**, con uno script per powershell che viene eseguito **senza** autorizzazioni amministrative.

Nel secondo link: visualizziamo che è un **RAT**, che è un tipo di malware che consente a un attaccante di accedere e controllare un computer o un sistema in remoto, senza il consenso dell'utente. Una volta che il RAT si installa nel sistema bersaglio, l'attaccante può ottenere accesso completo al computer, eseguire comandi, raccogliere informazioni personali, registrare attività dell'utente e persino assumere il controllo del sistema. Il **RAT** è spesso utilizzato per scopi dannosi come il furto di dati, lo spionaggio, il monitoraggio delle attività o l'esecuzione di azioni dannose sul sistema compromesso.

Entrambi i link forniscono un problema in comune:

VirusTotal: La scansione su VirusTotal ha indicato che il link è pulito e privo di malware.

The screenshot shows the VirusTotal interface for the URL <https://tinyurl.com/linklosco1>. At the top, a green circle with the number '0' indicates that no security vendors have flagged this URL as malicious. Below this, the URL is listed with a status of '200' and a last analysis date of '2 hours ago'. The 'DETECTION' tab is selected, showing a table of security vendors' analysis results. The table has four columns: Vendor, Detection, and two additional columns for other vendors. The results show that ArcSight Threat Intelligence and Abusix are 'Suspicious', while Acronis and ADMINUSLabs are 'Clean'. A banner at the top encourages joining the VT Community for additional insights and an API key.

Security vendors' analysis		Do you want to automate checks?	
ArcSight Threat Intelligence	Suspicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean

HTTP Response

Final URL

<https://app.any.run/tasks/8a2c185d-5a11-4aac-9286-43c641e1991a/>

Serving IP Address

172.67.1.225


Status Code

200

REPORT: Analisi dei log

UrlVoid: La scansione su UrlVoid ha confermato che il link è stato valutato come sicuro e non maligno.

Report Summary



Website Address	Tinyurl.com
Last Analysis	9 hours ago Rescan
Detections Counts	0/40
Domain Registration	2002-01-27 22 years ago
Domain Information	WHOIS Lookup DNS Records Ping
IP Address	172.67.1.225 Find Websites IPVoid Whois
Reverse DNS	Unknown
ASN	AS13335 CLOUDFLARENET
Server Location	 (US) United States
Latitude\Longitude	37.751 / -97.822 Google Map
City	Unknown
Region	Unknown

REPORT: Analisi dei log

HydraAnalysis: Durante la scansione su HydraAnalysis, è stato rilevato che il link è maligno e reindirizza a una pagina di **any.run**. In particolare, è stato identificato il file "mini-wallet.html" associato al link.

Analysis Overview

 Request Report Deletion

Submission name: hxxps://tinyurl.com/linklosco1
Size: 54B
Type:  url ⓘ
Mime: text/plain
Operating System: Windows 
Last Anti-Virus Scan: 06/30/2023 09:52:08 (UTC)
Last Sandbox Report: 06/30/2023 10:18:02 (UTC)

malicious

Threat Score: 100/100

 Link  Twitter  E-Mail

Files extracted during detonation


Name	Sha256	Verdict
mini-wallet.html	df47aac0fa71fbcecc16685ad4024965491e601880daf1fefa3735e769df661b	malicious
load-ec-i18n.bundle.js	4cac69d0545740f35cb9b1c4a473875a1f4064f087eb8ea19bafd98059a417e	no specific threat
miniwallet.bundle.js	78a7e765ffd6dff7af3b92b6234271fdOdddf5945f38e70d0e22324c1ec06eca	no specific threat
urlref_httpstinyurl.comlinklosco1	7e53c9a37b9548d5268fc41f49362ab5958f9fc8596758aa5f885ecd76b815b1	no specific threat
shopping_iframe_driver.js	456369ffe3542bb3ab1288484cfb909820a76f35e4d635a8638baf44ac6d3028	suspicious
edge_driver.js	4cb3db7a9fbaec8d6607d051b4b704d5a5689d4db6b19426f6b182c571308642	no specific threat

REPORT: Analisi dei log

Esamino precisamente i seguenti file: `mini-wallet.html`, `shopping_iframe_driver.js`, `notification_bundle.js`

Utilizzo le **SandBox di Falcon** per esaminare i vari file:

MALICIOUS


 **mini-wallet.html**


Analyzed on: 05/21/2023 20:25:11 (UTC)

Environment: Windows 10 64 bit


Threat Score: 80/100

Indicators: 3 12 44

Network: 



SUSPICIOUS

 **shopping_iframe_driver.js**

Analyzed on: 06/22/2023 01:50:32 (UTC)


Environment: Windows 10 64 bit

Threat Score: 45/100


AV Detection: Marked as clean

Indicators: 1 2 93

Network: (none)



SUSPICIOUS

 **notification_bundle.js**

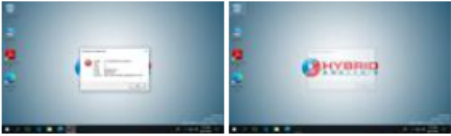
Analyzed on: 06/24/2023 08:07:26 (UTC)

Environment: Windows 10 64 bit

Threat Score: 35/100

Indicators: 0 2 103

Network: (none)



REPORT: Analisi dei log

Mini-wallet.html:

Ricaviamo queste informazioni:

Malicious Indicators

Anti-Detection/Stealthiness

Creates a process in suspended mode (likely for process injection)

details "ie_to_edge_stub.exe" called "CreateProcessW" with parameter ""%PROGRAMFILES%(x86)\Microsoft\Edge\Application\msedge.exe" --from-ie-to-edge=3 --ie-frame-hwnd=11003e" - (UID: 00000000-00004056)
source API Call
relevance 10/10
ATT&CK ID T1055 (Show technique in the MITRE ATT&CK™ matrix)

General

Calls an API typically used to execute an application

details "ie_to_edge_stub.exe" called "ShellExecuteW" with parameter %PROGRAMFILES%(x86)\Microsoft\Edge\Application\msedge.exe (UID: 00000000-00004056)
source API Call
relevance 10/10
ATT&CK ID T1106 (Show technique in the MITRE ATT&CK™ matrix)

Installation/Persistence

Writes data to a remote process

details "ie_to_edge_stub.exe" wrote 4024 bytes to a remote process "%PROGRAMFILES%(x86)\Microsoft\Edge\Application\msedge.exe" (Handle: 992)
"ie_to_edge_stub.exe" wrote 8 bytes to a remote process "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" (Handle: 992)
source API Call
relevance 6/10
ATT&CK ID T1055 (Show technique in the MITRE ATT&CK™ matrix)

Anti-Detection/Stealthiness: Questo indica che l'azione analizzata è stata progettata per eludere la rilevazione e agire in modo furtivo per evitare di essere rilevata.

Creates a process in suspended mode (likely for process injection): Questa indicazione suggerisce che un processo è stato creato in modalità sospesa, il che potrebbe essere un segno di un tentativo di iniezione di processo. L'iniezione di processo è una tecnica utilizzata da alcune minacce informatiche per inserire il proprio codice maligno all'interno di un processo legittimo e sfruttarne i privilegi.

Calls an API typically used to execute an application: Questa indicazione indica che è stata effettuata una chiamata a un'API che viene comunemente utilizzata per eseguire un'applicazione. Questo potrebbe suggerire che un'applicazione o un processo è stato avviato utilizzando questa chiamata.

Writes data to a remote process: Questa indicazione indica che un processo ha scritto dati all'interno di un processo remoto. Questo tipo di comportamento potrebbe essere utilizzato per inserire codice maligno o effettuare modifiche all'interno di un processo legittimo.

REPORT: Analisi dei log

Durante l'analisi del file "**mini-wallet.html**" sono state individuate **numerose** indicazioni di potenziali **minacce/file sospetti**.

Name	Sha256	Verdict
shopping.html	4a07676f7b8f79d9db68e385485daa5912cbc46cbf1bcc003f2caacfd1132e35	no specific threat
tokenized-card.html	1f7b07ba65350f4884a5241f58ebdd7035d3abbf01972f9108e6b1519a103656	no specific threat
bnpl_driver.js	b7aef5068ff4fab58e377effaa6119c21378c3730dc2ec8f4b4bcd18556787b9	suspicious
edge_confirmation_page_validator.js	9fef3ea4924e153bf01ef1daf1d3ca5415dff8405a4062eb49f5f6cd68f7c585	suspicious
wallet-drawer.html	c7c7217f0cb8894939bd7c3fd008bf8d396286e213eb8cbe6bd2dd50679fb18	no specific threat
wallet-drawer.bundle.js	4b140276f5d8a035571d0e327a032d3ba3021eb316303c3b37d47d2419892a5c	no specific threat
notification.bundle.js	e826fa8eb17a8afd9aaa673d8df2bc740e6f8f075b90c57c76052958a05baa81	suspicious
edge_tracking_page_validator.js	026192e464362a68b057c1c3161b2d593edc5d0562b9831262e581217e744288	suspicious
vendor.bundle.js	6646d414355d5d41f5f58fb62b4f38abb731b4318b9c34c7ae03f7e88db9cb64	no specific threat
runtime.bundle.js	31c9ac555f384e1fbcf07912acdeb5e67ca824ead7feaaa05357be0d942e80a7	suspicious
tokenized-card.bundle.js	bb14ae4f3573ad57a6c5bc90009310e55bd6b9686f5142320a317cf7c5799bb3a	no specific threat
wallet.bundle.js	29e014b4b5601768041edc39516b87d578f1d459aced77bb6dd34635579db2b7	no specific threat

è probabile che il file abbia lo scopo di eseguire azioni dannose sul sistema o sul browser dell'utente, potenzialmente coinvolto in attività come il **furto di informazioni personali o finanziarie o il phishing**.

Shopping_iframe_driver.js:

Malicious Indicators

Network Related

Making HTTPS connections using insecure TLS/SSL version

details

Connection was made using TLSv1.1 [tls.handshake.version: 0x00000302]

source

Network Traffic

relevance

10/10

ATT&CK ID

T1573 (Show technique in the MITRE ATT&CK™ matrix)

Suspicious Indicators

General

Executes a JavaScript file

details

Process "WScript.exe" with commandline ""C:\\shopping_iframe_driver.js"" (Show Process)

source

Monitored Target

relevance

10/10

ATT&CK ID

T1059.007 (Show technique in the MITRE ATT&CK™ matrix)

Unusual Characteristics

Found decoded Javascript strings

details

"executing"

source

File/Memory

relevance

10/10

REPORT: Analisi dei log

È stato rilevato che il file **effettua connessioni HTTPS** utilizzando **una versione non sicura di TLS/SSL (TLSv1.1)**. Ciò potrebbe esporre i dati scambiati durante la connessione a rischi di sicurezza. Inoltre, il file esegue un altro file JavaScript e contiene stringhe decodificate insolite, tra cui la stringa **"executing"**.

Questi indizi suggeriscono che il file potrebbe essere coinvolto in attività malevole o costituire una minaccia per la sicurezza del sistema. **Le tecniche di attacco MITRE ATT&CK™ Matrix menzionate indicano che le azioni del file possono essere correlate a schemi di attacco noti.**

Notification.bundle.js:

Suspicious Indicators

General

Executes a JavaScript file

details Process "WScript.exe" with commandline ""C:\notification.bundle.js"" (Show Process)
source Monitored Target
relevance 10/10
ATT&CK ID T1059.007 (Show technique in the MITRE ATT&CK™ matrix)

Spyware/Information Retrieval

Found an instant messenger related domain

details "Skype" (Indicator: "skype.com"; File: "urlref_httpsaka.msEdgeSaveCardFAQ")
source File/Memory
relevance 10/10

Dettagli dell'esecuzione del file JavaScript:

Questo indicatore è ritenuto altamente rilevante (10/10) in termini di potenziale minaccia.

Il file JavaScript viene eseguito tramite il processo **"WScript.exe"**.

La riga di comando specifica il percorso del file JavaScript eseguito (**"C:\notification.bundle.js"**).

Queste informazioni indicano che il file in questione esegue un altro file JavaScript utilizzando il processo **"WScript.exe"**.

Spyware/Information Retrieval:

Anche questo indicatore è ritenuto altamente rilevante (10/10) in termini di potenziale minaccia.

Viene rilevato un dominio correlato a un instant messenger, specificamente "skype.com".

Il riferimento al dominio viene trovato nel file **"urlref_httpsaka.msEdgeSaveCardFAQ"**.

Queste informazioni indicano che il file contiene un riferimento a un dominio correlato a Skype, un servizio di messaggistica istantanea. **Questo può suggerire che il file potrebbe essere coinvolto in attività di spyware o recupero di informazioni.**

3. Response:

REPORT: Analisi dei log

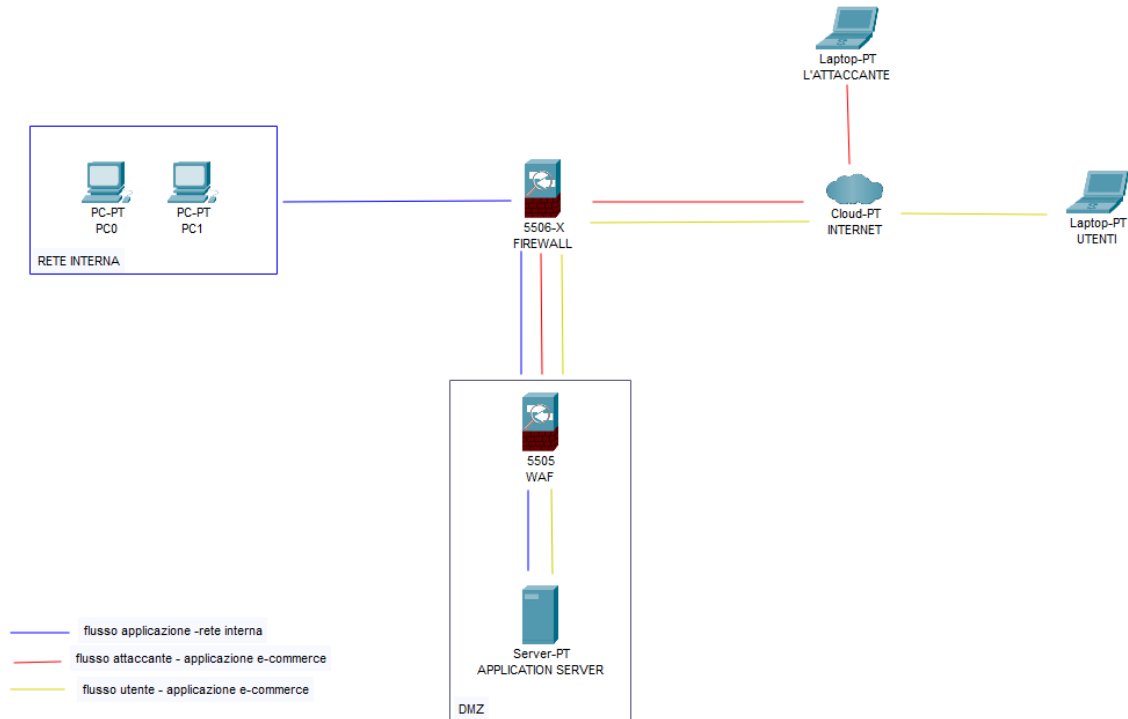
In questa fase è importante isolare l'Application Server infettato dal malware, eliminare tutte le attività, le componenti, i processi che sono rimasti dall'avvenuto incidente all'interno della rete o sui sistemi. Bisogna anche rimuovere eventuali backdoor installate dal malware, ripulire i dischi e chiavette USB compromesse.

Dopo la rimozione, si passa al recupero dei dati e delle informazioni perse, l'applicazione delle patch dove disponibili per eventuali sistemi obsoleti, revisione delle politiche dei firewall, IPS e IDS oppure l'aggiornamento delle firme degli antivirus.

4. Soluzione completa: Reconstruction

La reconstruction, è il processo di ripristino e riparazione di un sistema o di un'applicazione dopo un attacco o un'incidente di sicurezza. Nel contesto dell'application server infetto, la reconstruction si riferisce all'insieme di passaggi e azioni necessari per riportare il server in uno stato sicuro e funzionante **dopo aver rimosso il malware e effettuato il backup dei file recuperabili**. Ciò implica il ripristino del sistema operativo, la reinstallazione delle applicazioni, la configurazione delle impostazioni di sicurezza, il ripristino dei dati critici e la verifica del corretto funzionamento del server. **La reconstruction è un processo importante per ripristinare l'integrità, la disponibilità e la sicurezza del server e delle applicazioni collegate.**

REPORT: Analisi dei log

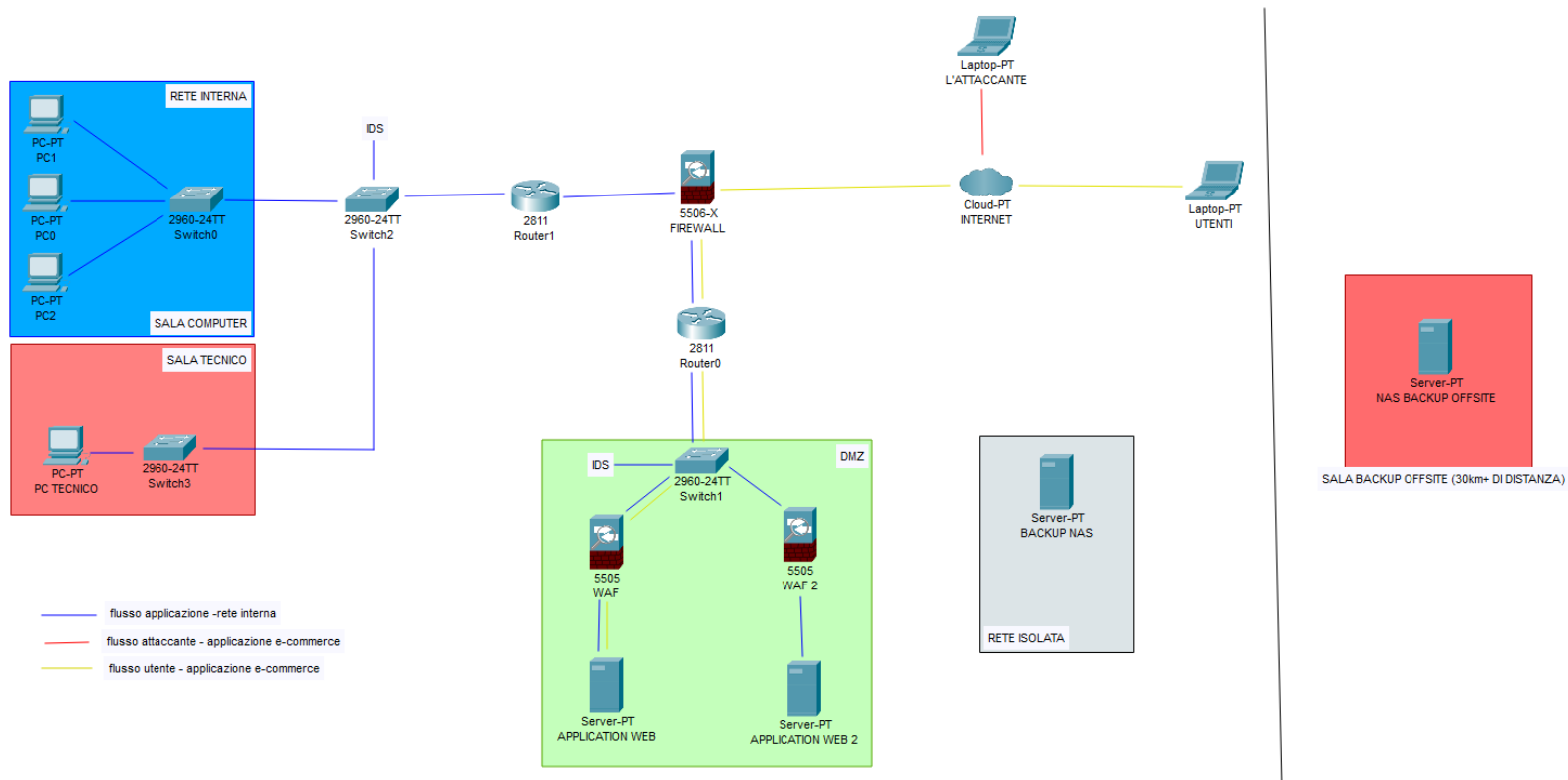


I passaggi di ricostruzione comprendono:

- Ripristino del sistema operativo e installazione delle applicazioni necessarie.
- Configurazione delle impostazioni di sicurezza, inclusi firewall, politiche di accesso e soluzioni antivirus/antimalware.
- Ripristino dei dati critici utilizzando il backup verificato.
- Esecuzione di test e verifiche per assicurarsi del corretto funzionamento del server e delle applicazioni.
- Implementazione di un sistema di monitoraggio continuo per individuare eventuali comportamenti anomali.
- Fornitura di formazione sulla sicurezza informatica agli utenti e al personale IT.
- Aggiornamento regolare del server, backup dei dati e mantenimento delle misure di sicurezza.
- Monitoraggio costante del server e manutenzione per rilevare e affrontare eventuali vulnerabilità.

REPORT: Analisi dei log

5. Modifica “Più aggressiva” dell’infrastruttura:



Ho completato l'infrastruttura di rete della nostra azienda implementando un nuovo server **Application Web**. Ho collegato il server tramite uno switch e ho assicurato una protezione aggiuntiva utilizzando i **Web Application Firewalls (WAF)** per filtrare il traffico. Inoltre, ho configurato i router per creare reti separate al fine di migliorare la sicurezza e garantire un'efficace gestione del traffico di rete. Ho dedicato una sala tecnica per ospitare l'hardware di rete e ho implementato sistemi di rilevamento delle intrusioni (**IDS**) per monitorare e mitigare potenziali minacce. Infine, ho istituito **due NAS Backup**, uno all'interno dell'azienda, isolato dal resto della rete, e l'altro in un sito esterno, distante più di 30 km, **per garantire la ridondanza e la protezione dei dati in caso di emergenze**.