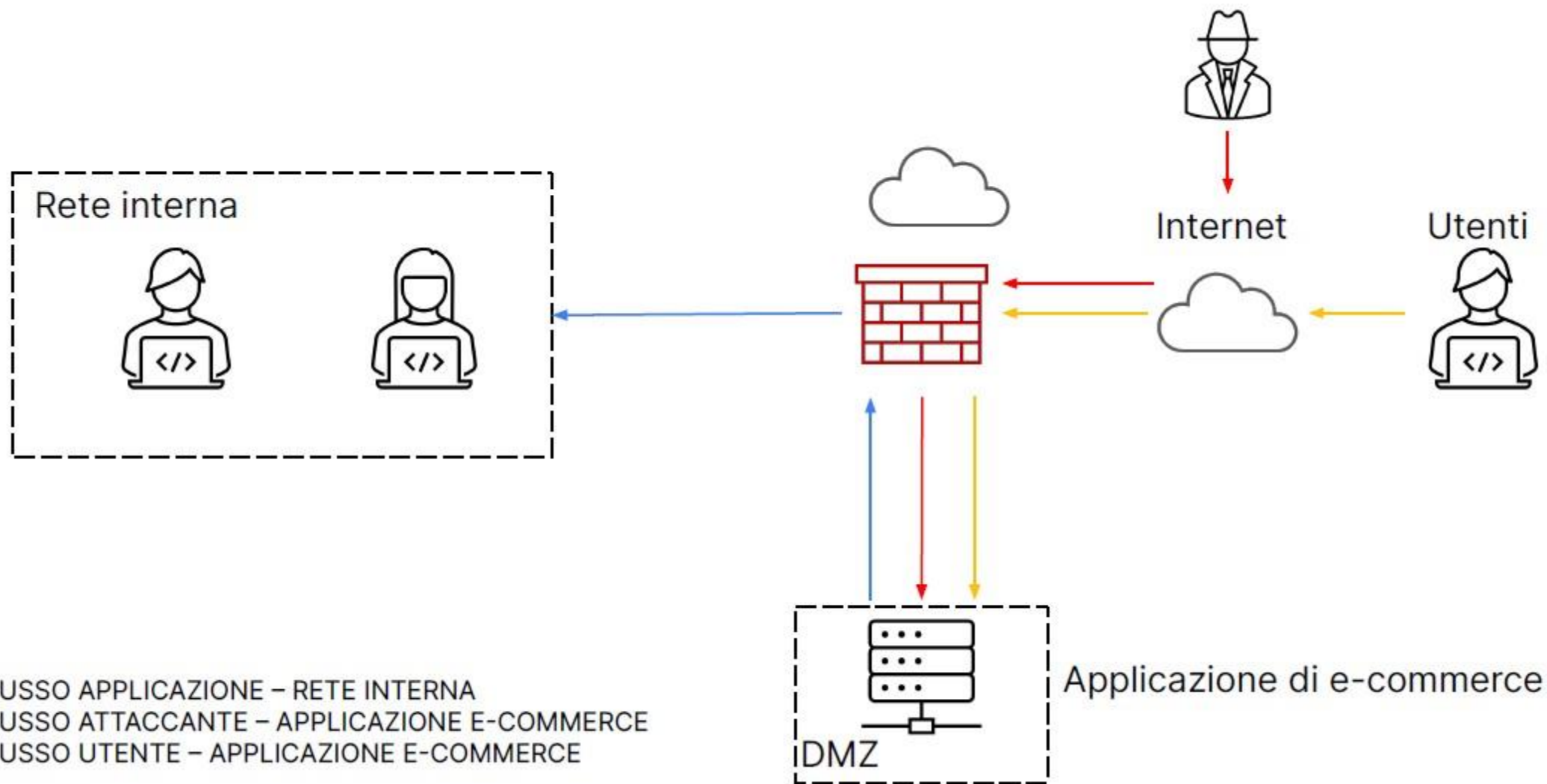


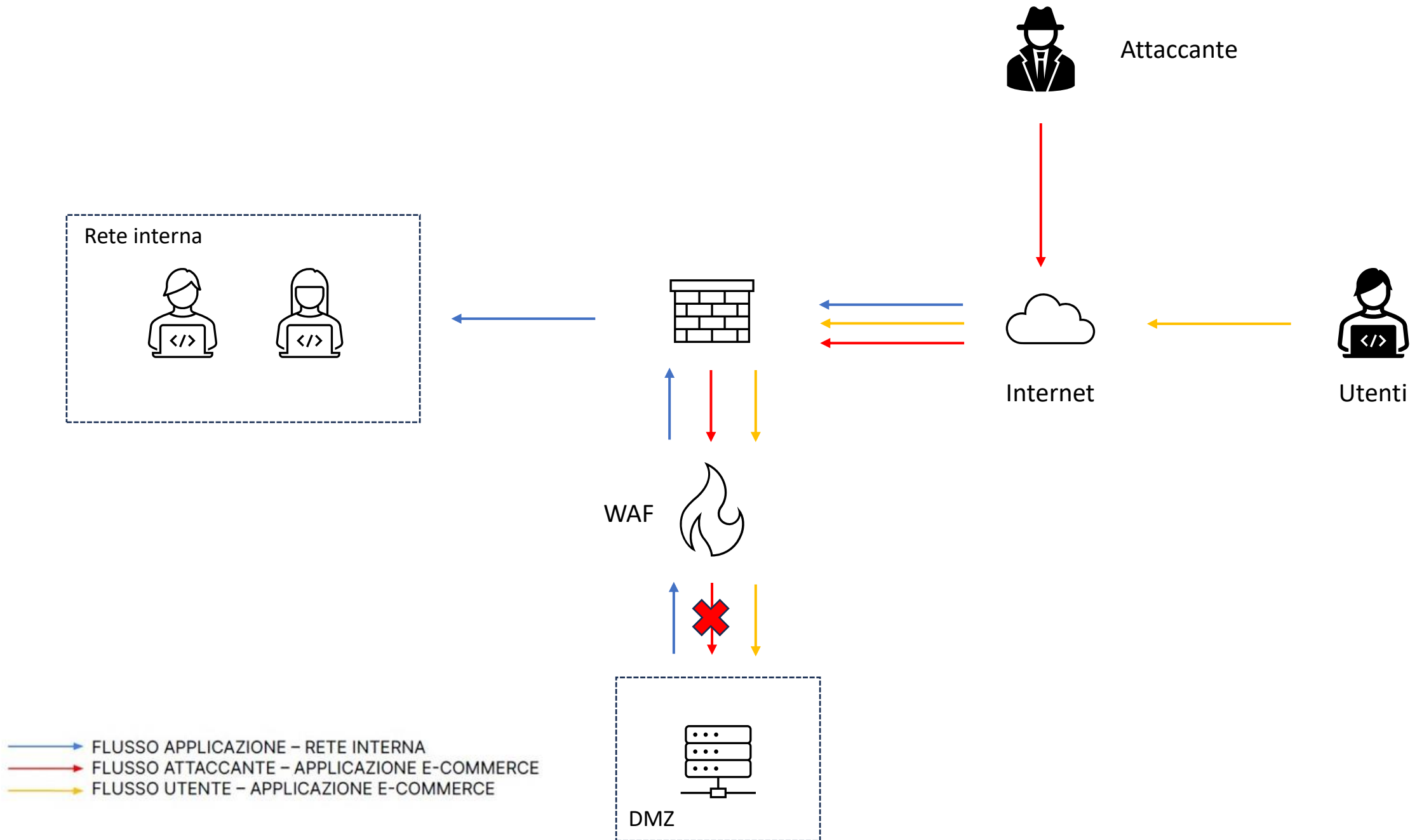
# ANALISI DEI LOG

EPICODE WEEK 9




## 1. AZIONI PREVENTIVE

Partendo dall'architettura di rete dell'immagine precedente, come azione preventiva per difendere l'e-commerce si potrebbe implementare un **WAF** (Web Application Firewall), una categoria di firewall dedicata proprio allo scopo di proteggere un sistema da attacchi *SQLi* e *XSS*. Nel caso specifico andrebbe aggiunto al normale firewall come ulteriore filtro agli accessi dagli utenti esterni sull'e-commerce:



## 2. ANALISI ATTACCO

Andiamo ad analizzare i link <https://tinyurl.com/linklosco1> e <https://tinyurl.com/linklosco2>. Tramite VirusTotal verifichiamo che gli url risultano sicuri.



https://tinyurl.com/linklosco1

0

/ 90

Community Score

No security vendors flagged this URL as malicious

https://tinyurl.com/linklosco1


tinyurl.com

Status

200

Last Analysis Date

2 hours ago



Reanalyze

Search

Graph

API

DETECTION

DETAILS

COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

ArcSight Threat Intelligence	<div>Suspicious</div>	Abusix	<div>Clean</div>
Acronis	<div>Clean</div>	ADMINUSLabs	<div>Clean</div>
AICC (MONITORAPP)	<div>Clean</div>	AlienVault	<div>Clean</div>
alphaMountain.ai	<div>Clean</div>	Antiy-AVL	<div>Clean</div>
Artists Against 419	<div>Clean</div>	Avira	<div>Clean</div>
benkow.cc	<div>Clean</div>	Bfore.Ai PreCrime	<div>Clean</div>
BitDefender	<div>Clean</div>	BlockList	<div>Clean</div>
Blueliv	<div>Clean</div>	Certego	<div>Clean</div>
Chong Lua Dao	<div>Clean</div>	CINS Army	<div>Clean</div>
CMC Threat Intelligence	<div>Clean</div>	CRDF	<div>Clean</div>
Cyble	<div>Clean</div>	CyRadar	<div>Clean</div>

Aprendoli si avvia Any.run, un sito specializzato in malware analysis basato su cloud. Qui viene mostrato il link di origine che fa riferimento a una repository github che mostra delle righe di codice in python. Apparentemente sembrerebbe un semplice programma per cambiare i DNS. Scaricando il codice viene salvato come file .ps1, ovvero un eseguibile powershell, la shell di windows.

The image is a composite of three screenshots from a Windows 7 desktop environment.

**Top Left Screenshot:** A Firefox browser window displaying a GitHub repository page for a PowerShell script. The script is titled "if ([Security.Principal.WindowsPrincipal][Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole] \"Administrator\") { Start-Process powershell.exe \"-NoProfile -ExecutionPolicy Bypass -File '\$PSCommandPath'\" -Verb RunAs; exit }". The script is a PowerShell script that checks if the user is an administrator and then starts a new PowerShell process with elevated privileges. The browser address bar shows the URL: <https://gist.github.com/chinmay-sh/037cd30cf125202a8b85ffcc0c2cf42/raw/7154ffd746be8626495a6e707388997...>

**Top Right Screenshot:** A Windows Task Manager window showing the "Processes" tab. It lists several running processes, including "firefox.exe" and "powershell.exe". The "powershell.exe" process is highlighted, showing its command line: `-file \"C:\Users\admin\Desktop\DNS_Changer.ps1\"`.

**Bottom Screenshot:** A network traffic analysis tool (Wireshark) displaying a list of network packets. The packets are filtered by "Filter by PID, name or url". The list shows several HTTP requests from "2513 ms" to "3520 ms", all with status "200: OK". The "Content" column shows various data types, including "text", "binary", and "der".

Nel download dalla lista processi non risulta ancora nulla di pericoloso. È nell'analisi del processo seguente all'avvio del suddetto codice che ci accorgiamo che il programma subdolamente ha cambiato le policy di esecuzione in amministratore. questo comportamento ovviamente è molto pericoloso, perché permette al codice di apportare modifiche al sistema a un livello privilegiato.

The screenshot displays a Windows 7 desktop environment. In the foreground, a PowerShell window titled 'Administrator: Windows PowerShell' is open, showing a script that prompts the user to change DNS server settings. The script lists options: 1. AdGuard DNS, 2. AdGuard Family Protection DNS, 3. Reset DNS to default, 4. Exit. The user has selected option 1. A file explorer window is also open, showing the contents of the 'Desktop' folder, which includes files like 'islandsent.rtf', 'laprocessing.jpg', 'listenup.rtf', 'lyricsdate.png', 'minutespan.jpg', 'partshall.jpg', and 'sellerdrive.rtf'. A network traffic analysis tool (Wireshark) is running in the background, displaying a list of HTTP requests. The requests are filtered by PID, name, or URL. The table below shows the captured traffic:

Time	Source	Destination	Method	Status	Process	Content
2513 ms	GET	200: OK	3384	firefox.exe	http://detectportal.firefox.com/success.txt	8 b + text
3359 ms	POST	200: OK	3384	firefox.exe	http://ocsp.digicert.com/	83 b + binary
3394 ms	POST	200: OK	3384	firefox.exe	http://r3.o.lencr.org/	503 b + der
3409 ms	GET	200: OK	3384	firefox.exe	http://detectportal.firefox.com/success.txt?pv4	8 b + text
3411 ms	POST	200: OK	3384	firefox.exe	http://ocsp.digicert.com/	83 b + binary
3520 ms	POST	200: OK	3384	firefox.exe	http://r3.o.lencr.org/	503 b + der

On the right side of the screenshot, a 'Suspicious activity' panel is visible. It shows a list of processes with their PIDs, names, and execution policies. The processes listed are:

- 1648 firefox.exe -contentproc --channel="3384.13.327271405\1549222807" -childID 2 -isForBrowser -prefsHandle 3764 -prefM...
- 1160 firefox.exe -contentproc --channel="3384.20.307103037\2146044254" -childID 3 -isForBrowser -prefsHandle 2100 -prefM...
- 3260 firefox.exe -contentproc --channel="3384.21.336355644\1791217740" -childID 4 -isForBrowser -prefsHandle 3336 -prefM...
- 2404 firefox.exe -contentproc --channel="3384.34.549990267\825554380" -childID 5 -isForBrowser -prefsHandle 2708 -prefM...
- 2272 powershell.exe -file "C:\Users\admin\Desktop\DNS\_Changer.ps1"
- 3300 powershell.exe -NoProfile -ExecutionPolicy Bypass -File "C:\Users\admin\Desktop\DNS\_Changer.ps1"

The panel also shows a 'Danger' warning with the message: 'Bypass execution policy to execute commands'. Below this, a 'Warning' section lists three items: 'Query Registry (1)', 'Reads the Internet Settings', and 'Using PowerShell to operate with local accounts'.



Apprendo invece il secondo link, questo ci riporta ad any.run dove possiamo analizzare un altro url sospetto. Questo collegamento riporta a un file doc google che però apparentemente non è raggiungibile. Dall'analisi del traffico si evince che svariate connessioni sono andate a buon fine e diverse richieste tcp sono state completate, e google in effetti si accorge del traffico anomalo e richiede una verifica dell'utente. Infine dalla pagina viene scaricato un file tar, un archivio.

The screenshot displays a web browser window with the URL `docs.google.com/uc?export=download&id=1Q3gFN2hrmBADTOBymgTAG_apwTYT6OYs`. The page shows an error: "This site can't be reached" with the message "docs.google.com took too long to respond." and the error code "ERR\_CONNECTION\_TIMED\_OUT". Below the error, there are links to "Reload" and "Details".

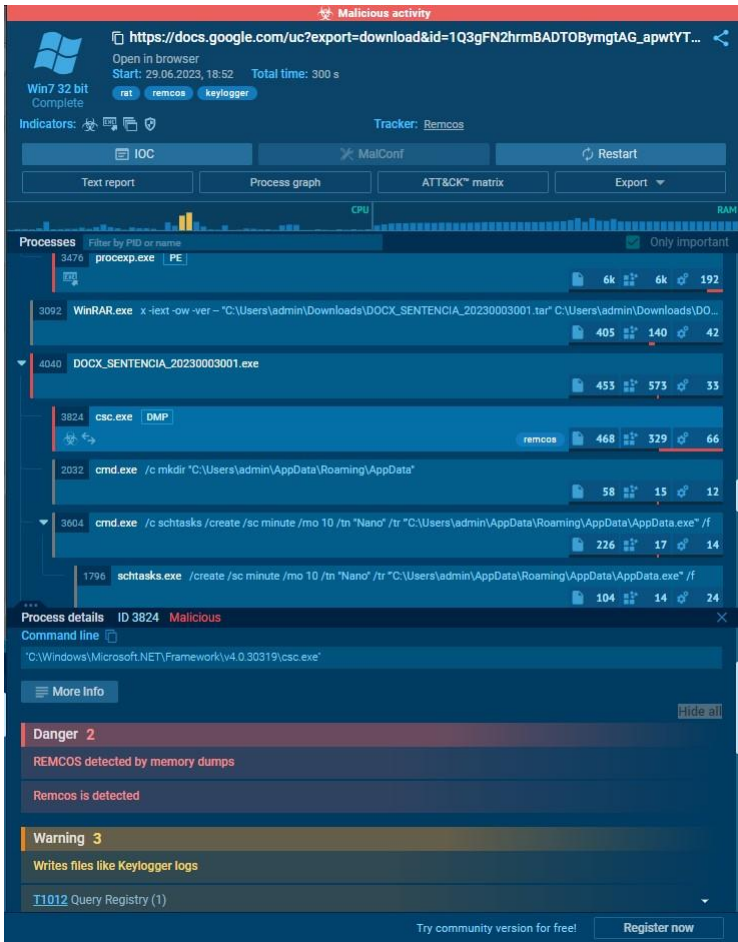
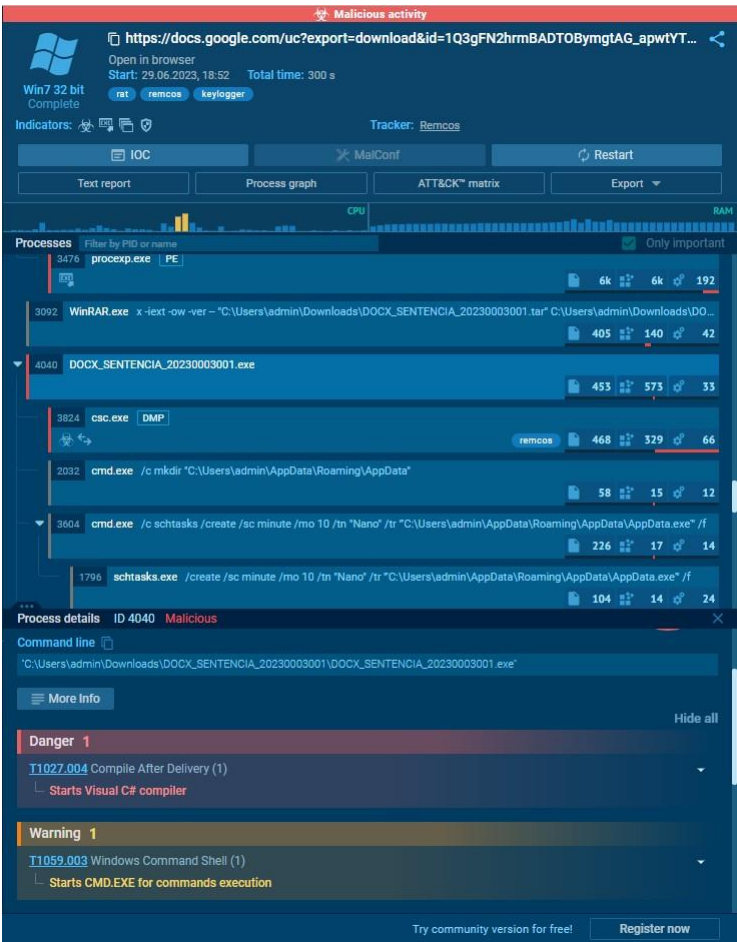
Below the browser window, the Sysinternals Suite interface is visible. It shows a list of network requests and connections. The "Connections" tab is active, displaying a table of network activity:

Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic
1482 ms	UDP	✓	2624	svchost.exe	?	239.255.255.250	1900	-	-	↑ 1.04 Kb ↓ -
1489 ms	UDP	✓	4	System	?	192.168.100.255	137	-	-	↑ 2.09 Kb ↓ -
1491 ms	UDP	✓	3140	chrome.exe	?	239.255.255.250	1900	-	-	↑ 696 b ↓ -
1492 ms	UDP	✓	1076	svchost.exe	?	224.0.0.252	5355	-	-	↑ 44 b ↓ -
2497 ms	TCP	✓	3440	chrome.exe	?	142.250.186.77	443	accounts.google.com	GOOGLE	No Data
2499 ms	UDP	✓	4	System	?	192.168.100.255	138	-	-	↑ 2.24 Kb ↓ -
2582 ms	TCP	✓	3440	chrome.exe	?	172.217.18.14	443	clients2.google.com	GOOGLE	↑ 1.02 Kb ↓ 8.71 Kb
2608 ms	TCP	✓	3440	chrome.exe	?	216.58.212.142	443	docs.google.com	GOOGLE	No Data
2668 ms	TCP	✓	3440	chrome.exe	?	216.58.212.142	443	docs.google.com	GOOGLE	No Data
3488 ms	TCP	✓	3440	chrome.exe	?	142.250.186.77	443	accounts.google.com	GOOGLE	↑ 1.06 Kb ↓ 6.42 Kb

The Sysinternals Suite interface also shows a "Processes" tab with a list of running processes. The "chrome.exe" process is highlighted, showing its PID (3140) and various system parameters. The "Process details" section for "chrome.exe" is expanded, showing the command line and other information.

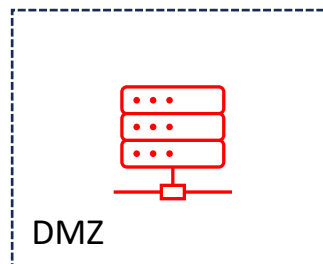
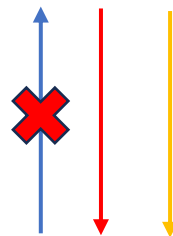
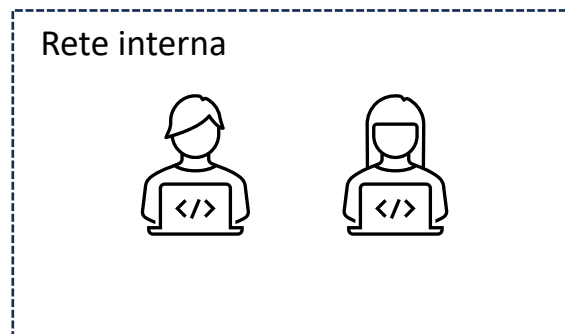


Aprendo l'archivio viene estratto un file eseguibile .exe spacciato per un documento adobe. Il file una volta aperto si rivela un malware, contiene infatti un eseguibile del compilatore in C# e apre la shell di comando per l'esecuzione di REMCOS, un remote access trojan per prendere il controllo remoto del pc. Un semplice finto documento google ha dato accesso al sistema a una persona malintenzionata.



### 3. RESPONSE

L'applicazione web è stata infettata. Il malware non deve propagarsi e dobbiamo impedire di divulgare informazioni sensibili su internet. Per fare ciò dobbiamo procedere all'**isolamento** dell'asset infetto, quindi si isola il sistema compromesso, staccandolo dalla rete principale con delle adeguate regole sul firewall, ma mantenendo una connessione ad internet protetta come in figura:



Internet

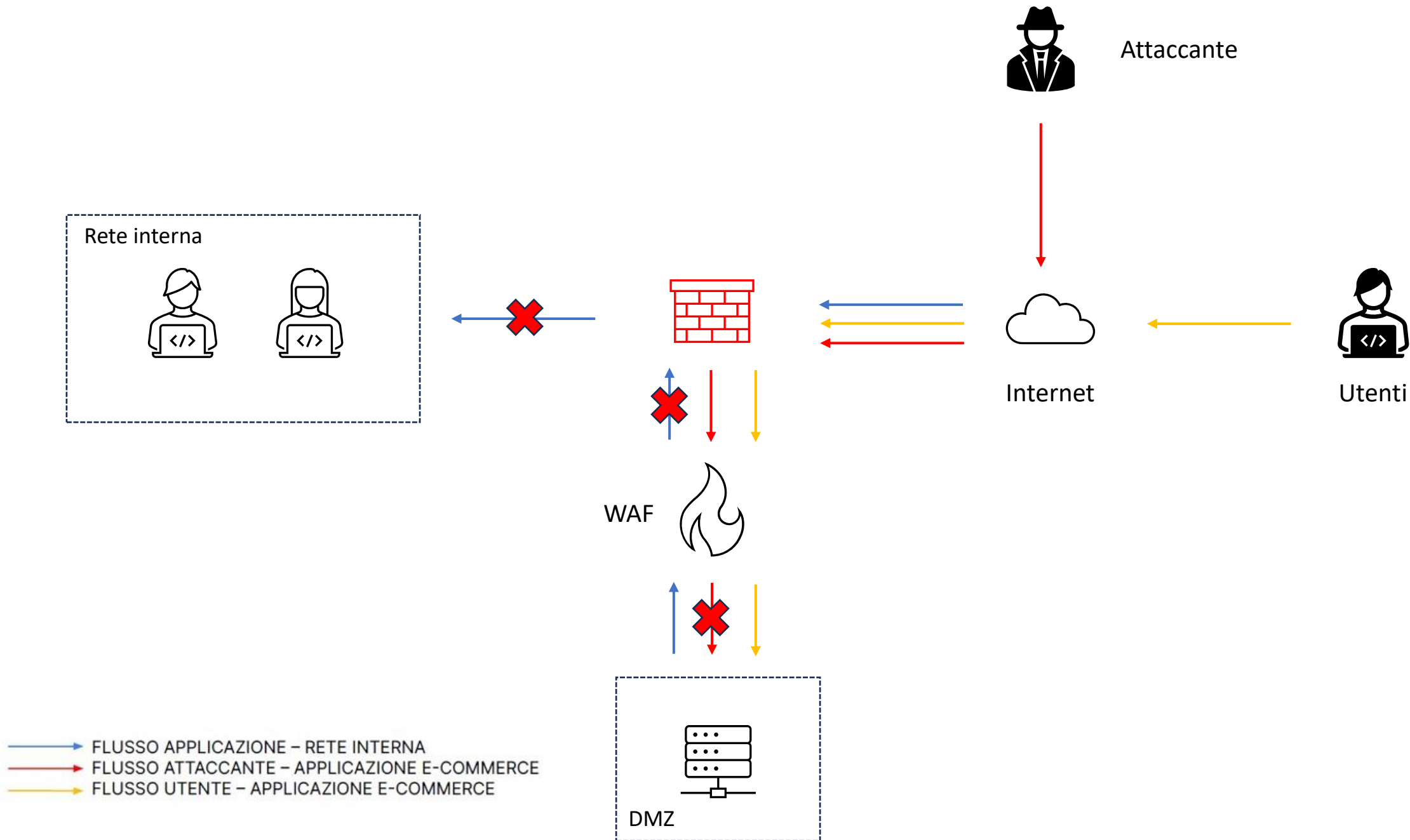


Utenti

- FLUSSO APPLICAZIONE - RETE INTERNA
- FLUSSO ATTACCANTE - APPLICAZIONE E-COMMERCE
- FLUSSO UTENTE - APPLICAZIONE E-COMMERCE

#### 4. SOLUZIONE COMPLETA

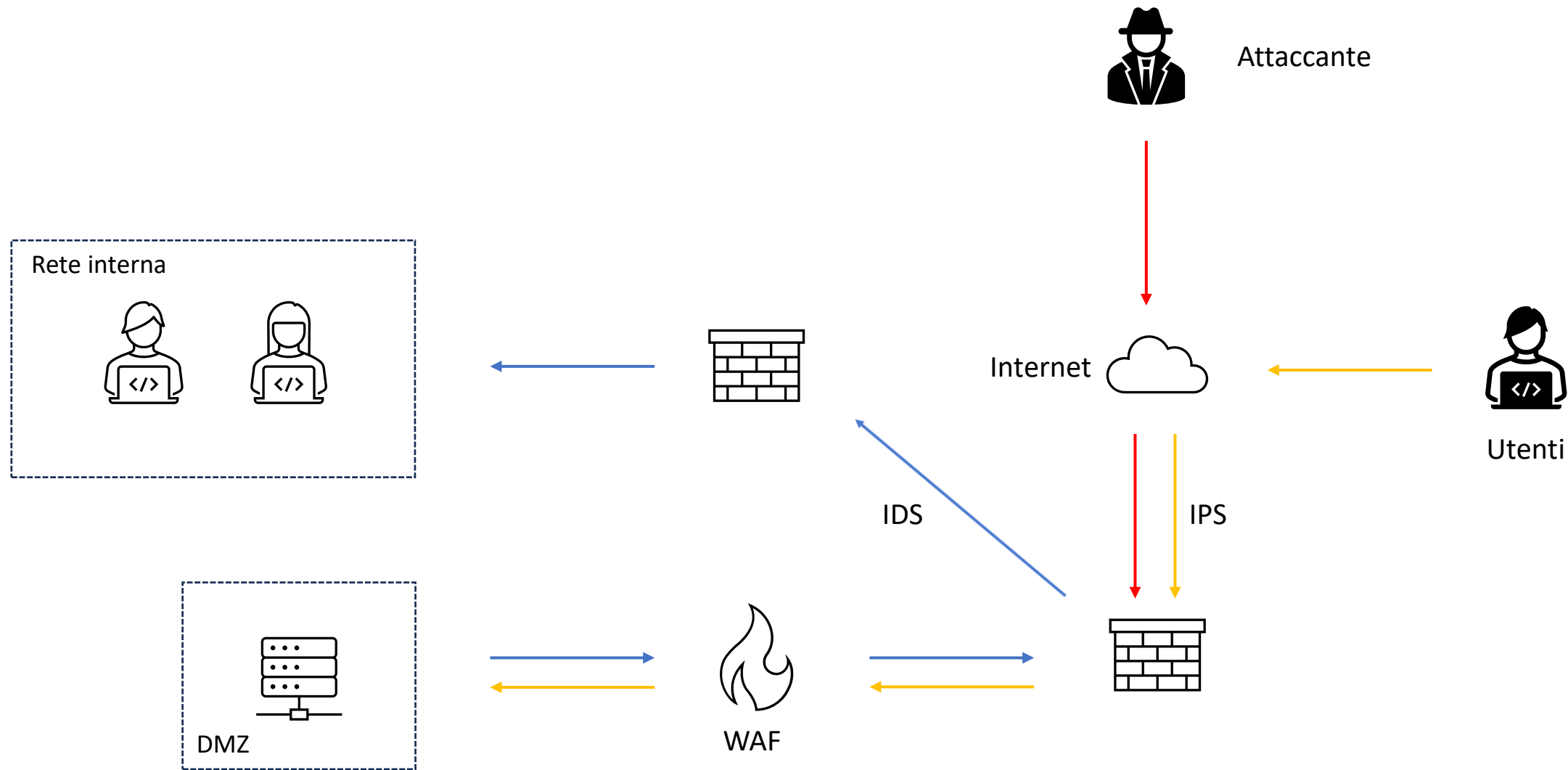
Una soluzione che unisca la sicurezza della protezione verso attacchi SQLi e XSS e permetta l'isolamento preventivo del sistema potrebbe essere la seguente:



## 5. MODIFICA AGGRESSIVA DELL'INFRASTRUTTURA

A seguito delle azioni di prevenzione e delle azioni di remediation a valle dell'attacco, il sistema della figura precedente sembrerebbe essere stato messo in sicurezza, ma possiamo migliorare e aumentare ancora la qualità della difesa, integrando altri elementi e migliorando quelli attuali per ottimizzare la rete. Una soluzione adatta potrebbe essere la seguente, che aggiunge un firewall perimetrale aumentando la segmentazione della rete, nonché un IPS e un IDS per la prevenzione e il rilevamento delle intrusioni:





- FLUSSO APPLICAZIONE - RETE INTERNA
- FLUSSO ATTACCANTE - APPLICAZIONE E-COMMERCE
- FLUSSO UTENTE - APPLICAZIONE E-COMMERCE