Proxy Log Analysis Questions

By: Ryan Stewart

Proxy Log Analysis

The Proxy acts as a bridge between the endpoint and the internet, commonly used by organizations for purposes like enhancing internet speed, centralized control, and improving security levels.

- Transparent Proxy: The target server can see the real source IP address.
- Anonymous Proxy: The target server cannot see the real source IP address; it sees the IP address of the proxy as the source IP address.

Examples of well-known proxy solutions in the market include Cisco Umbrella, Forcepoint Web Security Gateway, Check Point URL Filtering, and Fortinet Secure Web Gateway.

Proxy Working Structure

The proxy working structure controls the access of systems (server, client, etc.) to services such as HTTP, HTTPS, FTP based on determined policies, and enacts actions such as block or pass. While these policies may vary, they typically query the URL/domain to be accessed from the category database. If the category is deemed risky, a block action is applied; otherwise, a pass action is applied. Some systems may have an implicit deny applied to all networks other than those needed for access.

Sample Proxy Log

```
date=2022-05-21
time=16:15:44
type="utm"
subtype="webfilter"
eventtype="urlfilter"
level="warning"
srcip=192.168.209.142
srcport=34280
srcintfrole="lan"
dstip=54.20.21.189
dstport=443
dstintfrole="wan"
service="HTTPS"
hostname="android.prod.cloud.netflix.com"
profile="Wifi-Guest"
action="blocked"
url="https://android.prod.cloud.netflix.com/"
sentbyte=517
rcvdbyte=0
direction="outgoing"
urlsource="Local URLfilter Block"
msg="URL was blocked because it is in the URL filter list"
```

When we review the above log:

Upon reviewing the log, it is evident that the request to access "https://android.prod.cloud.netflix.com/" from the system with the IP address 192.168.209.142 in the "Wifi_Guest" group has been blocked due to the policy applied to the relevant profile. The block action is applied because the URL is in the "Local URLfilter Block" list.

Log Details

- **date**: Date information
- **time**: Time information
- **type**: Log type
- **subtype**: Log sub-type (values like forward, vpn, webfilter, virus, ips, system, etc.)
- **eventtype**: Event type belonging to the sub-type
- **level**: Incident severity level
- **srcip**: Source IP address
- **srcport**: Source port information
- **srcintfrole**: Source interface information
- **dstip**: Destination IP address
- **dstport**: Destination port information
- **dstintfrole**: Destination interface information
- **service**: Service information
- **hostname**: Requested domain
- **profile**: Source profile
- **action**: Action information
- **url**: URL address requested
- **sentbyte**: Size of data sent in bytes
- **rcvdbyte**: Size of data received in bytes
- **direction**: Direction of the traffic
- **urlsource**: URL sources
- **msg**: Message information

Importance of Proxy Logs

Proxy logs are crucial for SOC analysts to check which domain/URL a system is requesting from internal systems and whether it successfully established a connection. They are also vital in determining if the domain/URL falls into a risky category and whether any successful connections were established before.

- Suspicious activities detectable through proxy logs:
    - Connections to/from suspicious URLs
    - Infected system detection
    - Detection of tunneling activities

Example Forcepoint Web Security Gateway Log:

```
Jun 17 10:47:00 10.10.18.11
CEF:0|Forcepoint|Security|8.5.4|194|Transaction blocked|7| act=blocked
app=https dvc=10.10.18.11 dst=104.26.11.18
dhost=sentry-proxy.cargox.cc dpt=443 src=10.80.18.50 spt=61603
suser=Test_User requestMethod=POST
requestClientApplication=Mozilla/5.0 (Windows NT 10.0; Win64; x64)
cs1Label=Policy cs1=Block_Risk_Category_Policy(Servers)
request=https://sentry-proxy.cargox.cc/api/3/envelope/?sentry_key\=e25
06000e29247eba06eee9df3f011e0&sentry_version\=7
```

In this example, the "Test_User" user sent a POST request to "https://sentry-proxy.cargox.cc/" using the Mozilla browser, resulting in a block action. The target address was determined by the "Block_Risk_Category_Policy(Servers)" policy.

The domain category to be accessed in this log is expressed by the category number 194, which, after review, is found to belong to suspicious domains in the form of "194:Extended Protection Suspicious Content."

After this log analysis, it is discovered that the action is **blocked.** However, further investigation is necessary, as the request was made by a server, possibly infected, attempting to access a different proxy address to hide its actual destination. In such cases, a more in-depth analysis and examination of the process making the request are warranted. **EDR/XDR log sources should be explored for the continuation of this review.**

# Quiz Questions

Question 1: Proxy is only used for accessing the internet via the web. -False

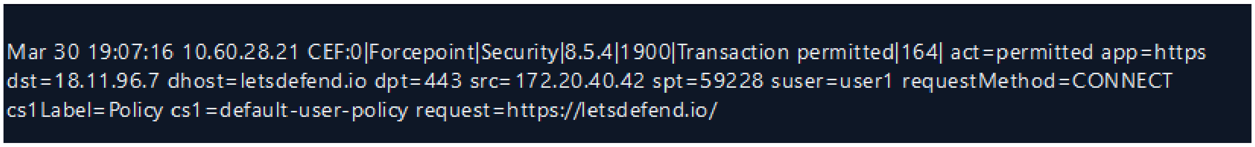
Question 2: Through which logs do we verify the response from the requested target in the proxy log above? (assuming that there are Firewall, AV, DLP, IPS/IDS, EDR, WAF devices in the environment.)

A) From the antivirus logs

B) From Email Gateway logs

C) From Firewall logs

D) From DLP logs



```
Mar 30 19:07:16 10.60.28.21 CEF:0|Forcepoint|Security|8.5.4|1900|Transaction permitted|164| act=permitted app=https
dst=18.11.96.7 dhost=letsdefend.io dpt=443 src=172.20.40.42 spt=59228 suser=user1 requestMethod=CONNECT
cs1Label=Policy cs1=default-user-policy request=https://letsdefend.io/
```

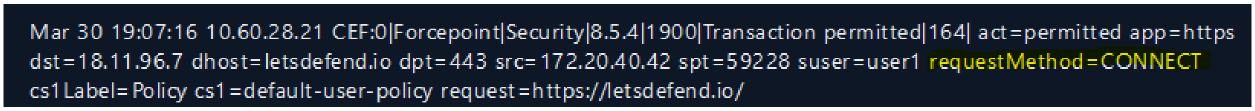
Question 3: According to the Proxy log above, which of the following is not true?

A) SSL/TLS used.

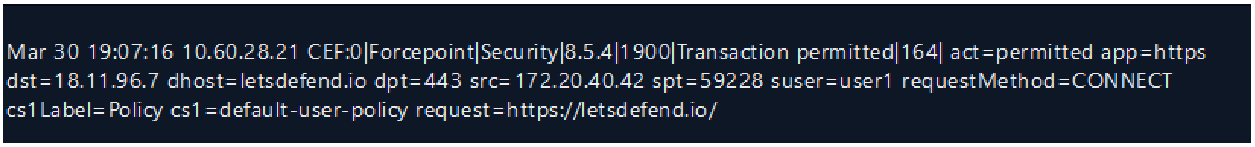
B) User1 made the query.

C) The proxy device has blocked this request.

D) The domain accessed works on the server with the address "18.11.96.7".



```
Mar 30 19:07:16 10.60.28.21 CEF:0|Forcepoint|Security|8.5.4|1900|Transaction permitted|164| act=permitted app=https
dst=18.11.96.7 dhost=letsdefend.io dpt=443 src=172.20.40.42 spt=59228 suser=user1 requestMethod=CONNECT
cs1Label=Policy cs1=default-user-policy request=https://letsdefend.io/
```



```
Mar 30 19:07:16 10.60.28.21 CEF:0|Forcepoint|Security|8.5.4|1900|Transaction permitted|164| act=permitted app=https
dst=18.11.96.7 dhost=letsdefend.io dpt=443 src=172.20.40.42 spt=59228 suser=user1 requestMethod=CONNECT
cs1Label=Policy cs1=default-user-policy request=https://letsdefend.io/
```

Question 4: When the above proxy log record turns into an alert, which action below is not required?

A) Checking domain reputation

B) Dynamic analysis of the accessed address

C) Controlling which different systems accessed the requested domain

D) Obtaining information by contacting the user who made the request

E) Blocking access to the domain

F) Check of Windows Application Events of the requesting system