Proxy

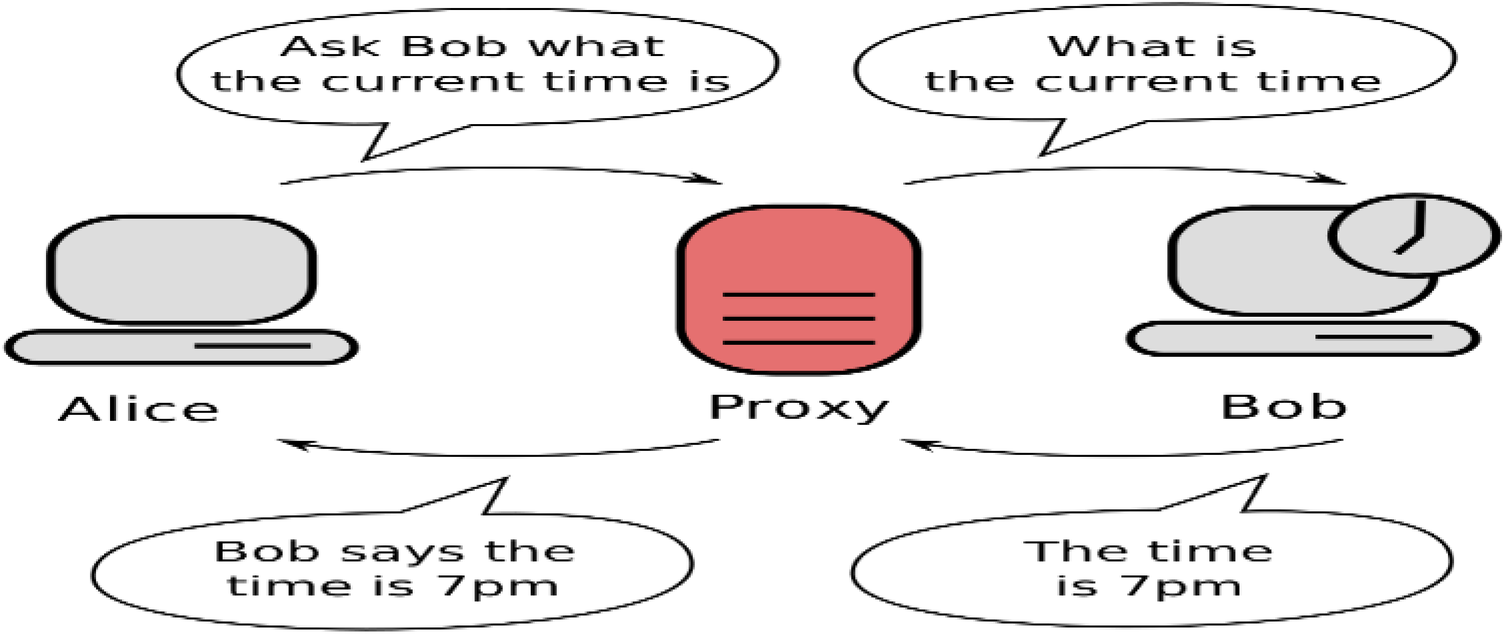
Cyber Security Foundation Course

AGENDA

- ➢ Definition
- ➢ Proxy types
- ➢ How Proxy Work
- ➢ Proxy Rules
- ➢ Proxy And SSL Interception
- ➢ Proxy Advantages

Proxy Definition

A server is layer 7 appliance, acts as a gateway between Endpoints and the internet, separating end users from the websites they browse. ... Proxy servers act as a firewall and web filter, control what allowed users to browse and what is not, and provide cache data to speed up common requests.



Proxy Types

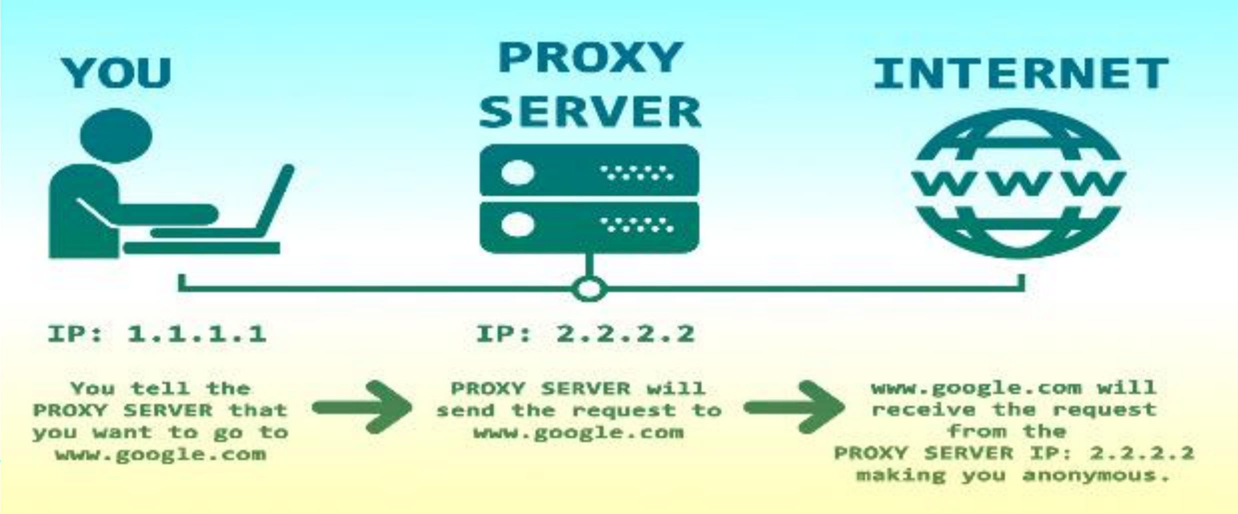
- **Forward Proxy:** sits in front of clients and is used to get data to groups of users within an internal network. When a request is sent, the proxy server examines it to decide whether it should proceed with making a connection “Forinet”

- **Anonymous Proxy:** making internet activity untraceable. It works by accessing the internet on behalf of the user while hiding their identity and computer information.

- **Reverse Proxy: also known as WAF (Covered Later)**

How Proxy Work

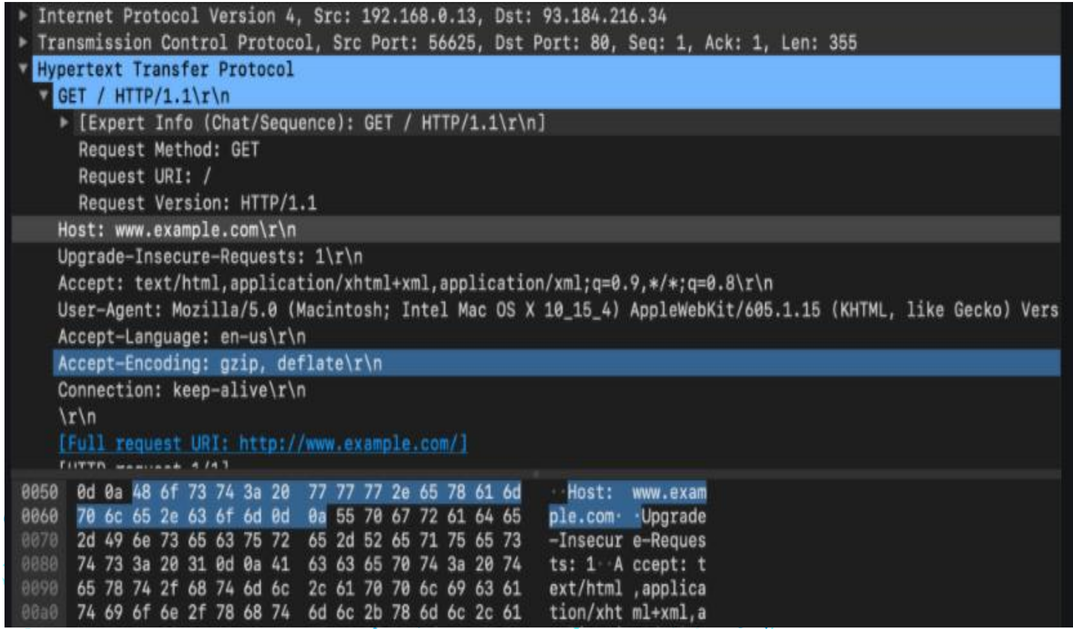
1. The Endpoint is configured to send all web requests to the Proxy for handling.
2. Endpoint request to access a Website.
3. A Proxy receives the request, first, the proxy will check if the request is allowed or not. (Take a decision)
4. If allowed, the proxy will send the request to the web server on behalf of the user.
5. The webserver responds to the Proxy. (send the requested Web page and recourses).
6. The Proxy forwards the response to the Endpoint


YOU
PROXY SERVER
INTERNET
WWW
IP: 1.1.1.1
IP: 2.2.2.2
You tell the PROXY SERVER that you want to go to www.google.com
PROXY SERVER will send the request to www.google.com
www.google.com will receive the request from the PROXY SERVER IP: 2.2.2.2 making you anonymous.

Proxy Rules

As previously shown, the proxy is a layer 7 appliance, hence the proxy can take a decisions based on the Layer 7 (Application Level). We can make control the access on the following:

- IP Addressee Example.. (10.10.10.10)
- User-Agent Example.. (Chrome, WIN7)
- URL. Example.. (https://www.youtube.com/playlist?list=PLdUDP-atVHBpsvwINVbfbPAasnQnuCxGk)
- Web Domain . Example.. (google.com)
- Username . Example.. (mostafa.yahia)
- Web category . Example.. (Spam, pornography)



```
▸ Internet Protocol Version 4, Src: 192.168.0.13, Dst: 93.184.216.34
▸ Transmission Control Protocol, Src Port: 56625, Dst Port: 80, Seq: 1, Ack: 1, Len: 355
▾ Hypertext Transfer Protocol
  ▾ GET / HTTP/1.1\r\n
    ▸ [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
    Host: www.example.com\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_4) AppleWebKit/605.1.15 (KHTML, like Gecko) Vers
    Accept-Language: en-us\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://www.example.com/]
    [HTTP request 1/1]

0050  0d 0a 48 6f 73 74 3a 20  77 77 77 2e 65 78 61 6d   ··Host:  www.exam
0060  70 6c 65 2e 63 6f 6d 0d  0a 55 70 67 72 61 64 65   ple.com· ·Upgrade
0070  2d 49 6e 73 65 63 75 72  65 2d 52 65 71 75 65 73   -Insecur e-Reques
0080  74 73 3a 20 31 0d 0a 41  63 63 65 70 74 3a 20 74   ts: 1··A ccept: t
0090  65 78 74 2f 68 74 6d 6c  2c 61 70 70 6c 69 63 61   ext/html ,applica
00a0  74 69 6f 6e 2f 78 68 74  6d 6c 2b 78 6d 6c 2c 61   tion/xht ml+xml,a
```

Proxy And SSL Interception

1. Endpoint establish a HTTPS connection to google.com.
2. The Proxy send his SSL Digital Certificate instead of google.com Certificate.
3. the Proxy Send the HTTPS connection to google.com.
4. Google.com send his SSL Digital Certificate to proxy

Hence the Connection between endpoint and Proxy will be Encrypted by using the Proxy Digital Certificate and the connection between the Proxy and Google.com will be Encrypted by using the Google.com Digital Certificate.

Advantages of the PROXY

- Enforce the Policy.
- Layer 7 Control.(Block Domains, URL, Categories, …)
- Very Useful logging Capability (See The SOC Investigation: 1- Suspicious outbound Traffic from local to remote (Proxy Log Analysis)

Thanks!

Any questions?