Proxy servers and HTTP tunneling

Dominik Stipić

01-09-2023

1 Introduction

The proxy servers are servers who intemediate communication between client and target server. The target server is the server whose resources the client wants to retrieve. We usually distinguish between the forward and reverse proxies. Proxies can be used to create a secure tunnel between two networks by encapsulating the traffic withing a secure protocol. A tunneling is a way to encapsulate one network protocol within another network protocol. A tunneling is often used to avoid firewall protection or to establish secure connection between two networks. The purpose of this article is to briefly explain how this two concepts are related and how each of them is used in practice.

2 Proxy Servers

Most enterprises today, maintain their private network where some information resources are protected and have high security status. They usually protect these resources with the firewall and by having proxy servers that prevent direct access to these resource servers. Every attempt to connect to the private network must go through the proxy server. This security policy puts constraints on outside legitimate users who would like to access company resources. In this article section, I would like to explain different ways in which proxy servers could be used and what are their benefits and potential flows.

Proxy servers introduce privacy and security because they prevent potentialy maliciuos access to the company resources. In general, The physical location of the proxy server can be anywhere between the client and the server. In figure 2 we can see a simple network architecture that could be used to expose company resources to the outside world. This type of network architecture is called network with **reverse proxy**. A reverse proxy is used for regulating the traffic that enters into some closed private network system. All the traffic that enters the company network goes through reverse proxy and thus protects the services or resources because the client cannot access them directly. This is important because direct exposure of the company servers to the unknown internet traffi could infect the servers. Network configuration where the proxy

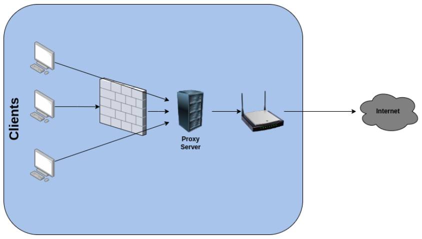

Figure 1: Image shows the network architecture and elements which are used for protecting and exposing private network to the internet. Firewall is used for traffic filtering and prevents outside clients from accessing protected resources. The proxy server is used as the gateway to the outside world and enhances the security, privacy and network performance.

is used for regulating traffic from clients to internet is called **forward proxy** configuration.

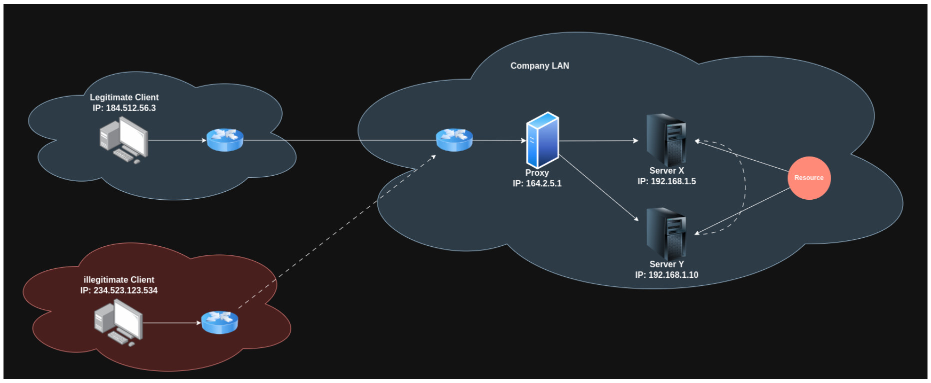

Figure 2: **Example network**. A company controls the information resource whose symbol is a pink circle. This resource resides on server X and server Y. Those servers aren't exposed to the outside world directly. The outside client cannot reach the resource directly. He needs to use a proxy server in order to retrieve resources. Entities inside the LAN network can talk with each other freely. The network colored with red color is illegitimate client who cannot access the company resources. Proxy servers are the gateway between internal and external networks and thus they are put in front of the firewall

Furthermore, in the figure 2, the proxy server can act as a *load-balacer*. It can split the incoming traffic and deliver the requests to the server X or Y. We can summarize the functionality of the reverse proxy as follows:

- **Security**. Servers aren't exposed directly to the client requests, all the traffic goes through proxy servers. We want to protect it from malicious client requests

- **Privacy**. The server's location, protocol, and other technical information are hidden from the user.
- **Load-Balancing**. A proxy server can prevent the explotation of some servers and distribute traffic to other servers who can share the same resource.
- **Caching**. Frequent content that passes through a proxy server can be cached and speed up the delivery.
- **Observability or monitoring**. If all traffic passes through a proxy server, then this fact could be used to save and analyze the traffic that passes through the proxy.

3 Tunneling

The most common form of HTTP tunneling is the standardized HTTP CONNECT method. When the client sends a CONNECT request to the proxy server, he commands the proxy server to establish the TCP connection to the background server. After the connection between the proxy and resource server is established, any data sent to the proxy will automatically be blindly forwarded, unmodified, and unprocessed to the remote host. This type of tunneling is often used to bypass firewalls or access resources that are not normally accessible from the outside. We said that traffic is *blindly* forwarded because the proxy doesn't decrypts the forwarded data. Here is an example of the HTTP request which client sends to the proxy server by whom it requests the proxy server to establish a TCP connection with the remote server *example.com.*

```
|************************************|
|CONNECT www.example.com:80 HTTP/1.1 |
|Proxy-Connection: Keep-Alive        |
|************************************|
```

Proxy responds with *OK* message when he establishes the connection with a remote server. Without the CONNECT method, the client would send the Proxy HTTP GET method to the server: —**********************************—
—GET example.com:80 HTTP/1.1 — —**********************************—
Thus indicating that he would like his request is forwarded to the target server. When the proxy receives the request he decrypts the data and creates the new request to the target server. The big shortcoming of this approach is that the proxy can read all the data that is intended for the target server. Because of this HTTP CONNECT tunneling process is engineered in order to prevent the decryption of traffic between the client and proxy server. In comparison with HTTPS proxy forwarding, the CONNECT method establishes end-to-end SSL/TLS sessions between the client machine and target server. The proxy is only used for forwarding requests and he processes messages only till the TCP layer. On the image 3 we can see how HTTPS tunneling works. In standard HTTP

proxying the proxy server would exchange the certificate and session key with the client and because of, that he would be able to decipher the messages.

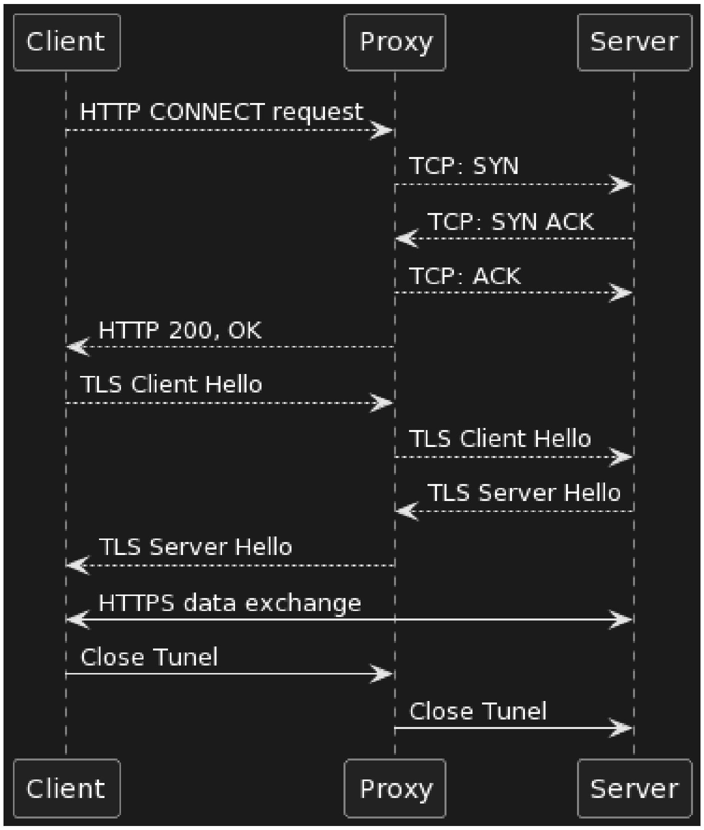

Figure 3: **Communication graph for HTTP CONNECT**. After the client initiates the HTTP CONNECT request, the proxy does a 3-way TCP handshake with the server in order to establish the TCP connection. Next, the client wants to establish the SSL/TLS session with the server, and in this process, the proxy only forwards the protocol flags. When the secure SSL connection is established, the data exchange between the client and the server can begin. In the end, the client closes the connection

Tunneling could also be used to avoid firewall traffic filtering and retrieving the protected resources. Because the firewall filters the traffic and prevents exposure of the resources to unauthorized users, users can retrieve protected content through proxy server and tunneling methodology.