PROXY SERVERS

COMPUTER NETWORKS (LAB)

April 27TH, 2023

—

CS-373L

—

Ma’am Fatima Shahzadi

COMPUTER NETWORKS

PRESENTERS

SYED AOON ABBAS
(2020-CS-535)

KHAVEELA NADEEM
(2020-CS-504)

SAWERA BIBI
(2020-CS-512)

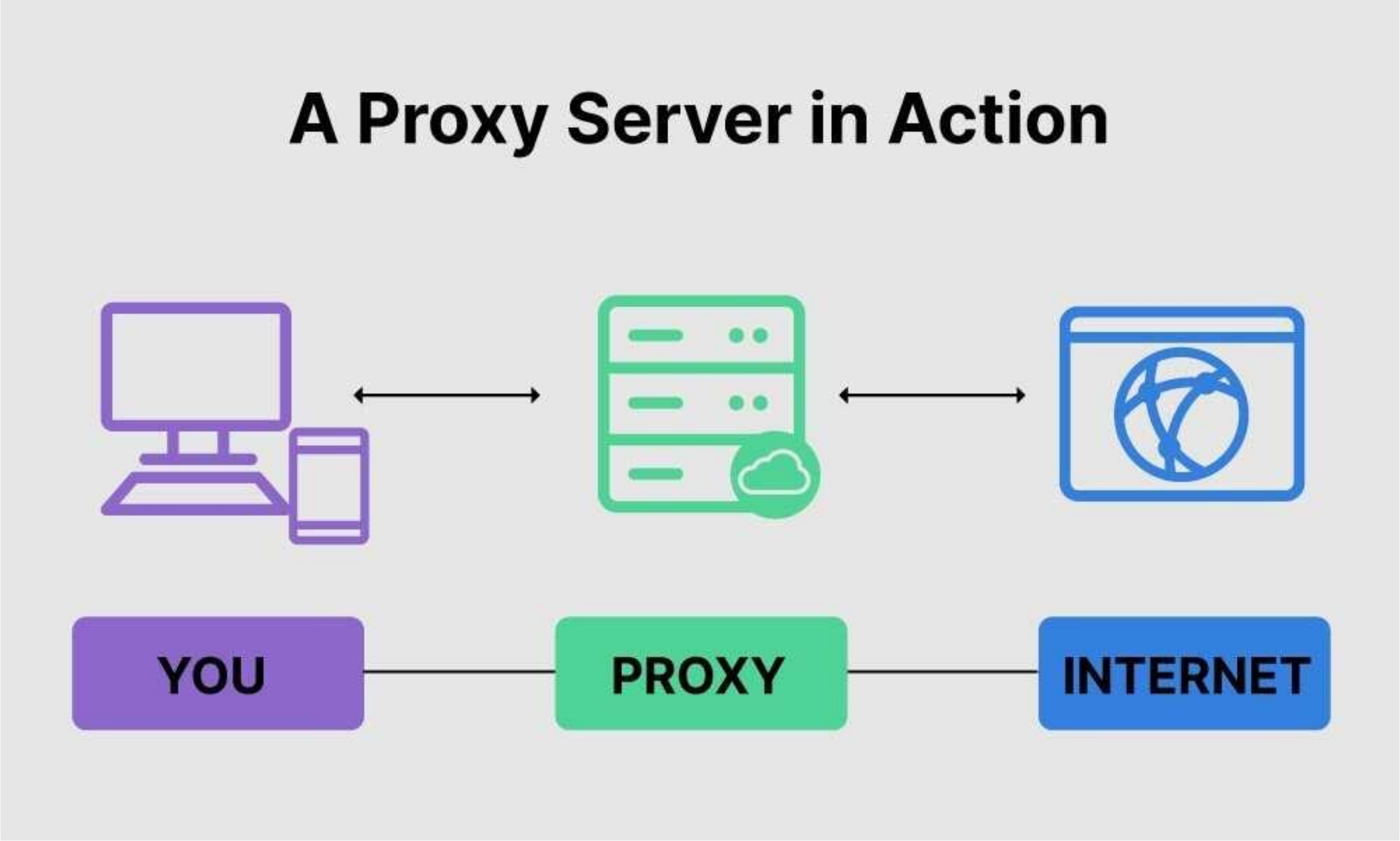
USWAH RIAZ
(2020-CS-520)

Table of contents

Introduction

A proxy server is a system or router that provides a gateway between users and the internet. Therefore, it helps prevent cyber attackers from entering a private network. It is a server, referred to as an “intermediary” because it goes between end-users and the web pages they visit online.

When a computer connects to the internet, it uses an IP address. This is similar to your home’s street address, telling incoming data where to go and marking outgoing data with a return address for other devices to authenticate. A proxy server is essentially a computer on the internet that has an IP address of its own.

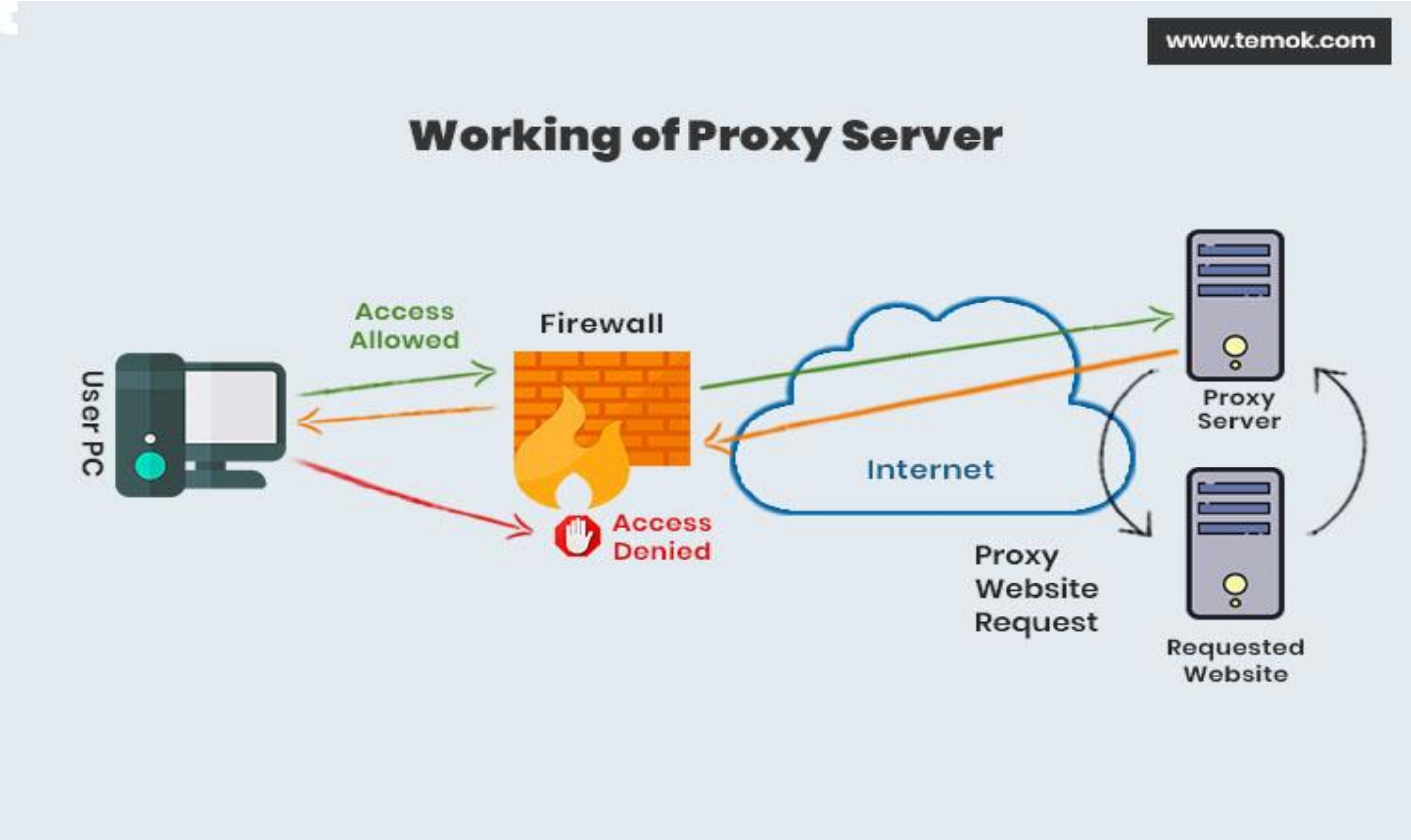


Proxy servers provide varying levels of functionality, security, and privacy depending on your use case, needs, or company policy. In a proxy server, internet traffic flows through the proxy server on its way to the address you requested. The request then comes back through that same proxy server and then the proxy server forwards the data received from the website to you.

How Does a Proxy Server Operate?

Each device connected to the internet requires a unique Internet Protocol (IP) Address, similar to a physical street address. This address allows the internet to route data to the correct device. A proxy server is a type of computer on the internet that has its own IP address and is known to your computer. When you make a request to access a web page, the request is first sent to the proxy server. The proxy server then acts on your behalf by making the web request, gathering the response from the web server, and sending you the web page data to display in your browser.

The proxy server has the ability to modify the data you send and still deliver the expected information. It can change your IP address so that the web server doesn't know your exact location. Additionally, it can encrypt your data to keep it secure while in transit. Finally, the proxy server can block access to specific web pages based on IP addresses. A proxy server has its own IP address, it acts as a go-between for a computer and the internet. Your computer knows this address, and when you send a request on the internet, it is routed to the proxy, which then gets the response from the web server and forwards the data from the page to your computer's browser, like Chrome, Safari, Firefox, or Microsoft Edge.



Need of Proxy Servers

There are several reasons organizations and individuals use a proxy server.

- **To control internet usage of employees and children:**

Organizations and parents set up proxy servers to control and monitor how their employees or kids use the internet. Most organizations don’t want you looking at specific websites on company time, and they can configure the proxy server to deny access to specific sites, instead of redirecting you with a nice note asking you to refrain from looking at said sites on the company network. They can also monitor and log all web requests, so even though they might not block the site, they know how much time you spend cyber-loafing.

- **Bandwidth savings and improved speeds:**

Organizations can also get better overall network performance with a good proxy server. Proxy servers can cache (save a copy of the website locally) popular websites – so when you ask for www.varonis.com, the proxy server will check to see if it has the most recent copy of the site, and then send you the saved copy. What this means is that when hundreds of people hit www.varonis.com at the same time from the same proxy server, the proxy server only sends one request to varonis.com. This saves bandwidth for the company and improves the network performance.

- **Privacy benefits:**

Individuals and organizations alike use proxy servers to browse the internet more privately. Some proxy servers will change the IP address and other identifying information the web request contains. This means the destination server doesn’t know who actually made the original request, which helps keeps your personal information and browsing habits more private.

- **Improved security:**

Proxy servers provide security benefits on top of the privacy benefits. You can configure your proxy server to encrypt your web requests to keep prying eyes from reading your transactions. You can also prevent known malware sites from any access through the proxy server. Additionally, organizations can couple their proxy server with a Virtual Private Network (VPN), so remote users always access the internet through the company proxy. A VPN is a direct connection to the company network that companies provide to external or remote users. By using a VPN, the company can control and verify that their users have access to the resources (email, internal data) they need, while also providing a secure connection for the user to protect the company data.

- **Get access to blocked resources:**

Proxy servers allow users to circumvent content restrictions imposed by companies or governments. Is the local sports ball team's game blacked out online? Log into a proxy server on the other side of the country and watch from there. The proxy server makes it look like you are in California, but you actually live somewhere else. Several governments around the world closely monitor and restrict access to the internet, and proxy servers offer their citizens access to an uncensored internet.

Types Of Proxy Servers

Not all proxy servers work the same way. It's important to understand exactly what functionality we want to get from the proxy server and ensure that the proxy server meets your use case.

- **Transparent Proxy**

A transparent proxy tells websites that it is a proxy server and it will still pass along your IP address, identifying you to the webserver. Businesses, public libraries, and schools often use transparent proxies for content filtering: they're easy to set up both client and server-side.

- **Anonymous Proxy**

An anonymous proxy will identify itself as a proxy, but it won't pass your IP address to the website – this helps prevent identity theft and keep your browsing habits private. They can also prevent a website from serving you targeted marketing content based on your location. For example, if CNN.com knows you live in Raleigh, NC, they will show you news stories they feel are relevant to Raleigh, NC. Browsing anonymously will prevent a website from using some ad targeting techniques, but is not a 100% guarantee.

- **Distorting proxy**

A distorting proxy server passes along a *false* IP address for you while identifying itself as a proxy. This serves similar purposes as the anonymous proxy, but by passing a false IP address, you can *appear* to be from a different location to get around content restrictions.

- **High Anonymity proxy**

High Anonymity proxy servers periodically change the IP address they present to the web server, making it very difficult to keep track of what traffic belongs to who. High anonymity proxies, like the TOR Network is the most private and secure way to read the internet.

- **Data Center Proxy**

proxies are not affiliated with an internet service provider (ISP) but are provided by another corporation through a data center. The proxy server exists in a physical data center, and the user’s requests are routed through that server. Data center proxies are a good choice for people who need quick response times and an inexpensive solution. They are therefore a good choice for people who need to gather intelligence on a person or organization very quickly. They carry the benefit of giving users the power to swiftly and inexpensively harvest data. On the other hand, they do not offer the highest level of anonymity, which may put users’ information or identity at risk.

- **Residential Proxy**

A residential proxy gives you an IP address that belongs to a specific, physical device. All requests are then channeled through that device. Residential proxies are well-suited for users who need to verify the ads that go on their website, so you can block cookies, suspicious or unwanted ads from competitors or bad actors. Residential proxies are more trustworthy than other proxy options. However, they often cost more money to use, so users should carefully analyze whether the benefits are worth the extra investment.

- **Public Proxy**

A public proxy is accessible by anyone free of charge. It works by giving users access to its IP address, hiding their identity as they visit sites.

Public proxies are best suited for users for whom cost is a major concern and security and speed are not. Although they are free and easily accessible, they are often slow because they get bogged down with free users. When you use a public proxy, you also run an increased risk of having your information accessed by others on the internet.

- **Shared Proxy**

Shared proxies are used by more than one user at once. They give you access to an IP address that may be shared by other people, and then you can surf the internet while appearing to browse from a location of your choice. Shared proxies are a solid option for people who do not have a lot of money to spend and do not necessarily need a fast connection. The main advantage of a shared proxy is its low cost. Because they are shared by others, you may get blamed for someone else’s bad decisions, which could get you banned from a site.

- **SSL Proxy**

A secure sockets layer (SSL) proxy provides decryption between the client and the server. As the data is encrypted in both directions, the proxy hides its existence from both the client and the server. These proxies are best suited for organizations that need enhanced protection against threats that the SSL protocol reveals and stops. Because Google prefers servers that use SSL, an SSL proxy, when used in connection with a website, may help its search engine ranking. On the downside, content encrypted on an SSL proxy cannot be cached, so when visiting websites multiple times, you may experience slower performance than you would otherwise.

Proxy Servers and Network Security

Proxies provide a valuable layer of security for your computer. They can be set up as web filters firewalls, protecting your computer from internet threats like Malwares. This extra security is also valuable when coupled with a secure web gateway or other email security products. This way, you can filter traffic according to its level of safety or how much traffic your network—or individual computers—can handle.

Organizations and Companies use Proxy Servers to achieve the following benchmarks or milestones:

1. Improve security
2. Secure employees’ internet activity from people trying to snoop on them
3. Balance internet traffic to prevent crashes
4. Control the websites employees and staff access in the office
5. Save bandwidth by caching files or compressing incoming traffic

IP Addresses & Network Topologies

Proxy servers can use a variety of IP addresses, depending on how they are configured and the specific type of proxy server being used. Here are some common types of IP addresses used in proxy servers:

1. **Public IP addresses:**

These are the IP addresses used by the proxy server to communicate with the internet. When you use a proxy server, your requests are routed through the proxy server's public IP address, which may be visible to the websites you visit.

2. **Private IP addresses:**

These are the IP addresses used within the local network of the proxy server. Private IP addresses are not visible to the internet and are used for internal communication within the network.

3. **Static IP addresses:**

These are IP addresses that do not change and are assigned to the proxy server permanently. Static IP addresses are commonly used for proxy servers that require a consistent and reliable connection.

4. **Dynamic IP addresses:**

These are IP addresses that can change over time and are assigned to the proxy server by a DHCP server. Dynamic IP addresses are commonly used for proxy servers that do not require a permanent connection.

5. **Shared IP addresses:**

These are IP addresses that are shared among multiple proxy servers. Shared IP addresses can be used to hide the identity of individual proxy servers and provide a higher level of anonymity for users.

Overall, the specific IP addresses used in proxy servers can vary depending on the configuration and requirements of the proxy server, as well as the specific use case.

Similarly, in terms of Network Topologies, proxy servers are configured with different topologies as per the need of the network and the organization needs. Proxy servers can be based on a variety of network topologies, depending on the specific needs of the network and the purpose of the proxy server.

Proxy Servers OR VPN?

VPN (Virtual Private Network) and proxy servers are both used to provide privacy and security when accessing the internet, but they work in different ways.

A VPN provides a secure and encrypted connection between your computer and the internet, by creating a private network over a public network, such as the internet. When you use a VPN, all your internet traffic is routed through the VPN server, which encrypts your data and hides your IP address from prying eyes, providing you with online privacy and security.

On the other hand, a proxy server acts as a gateway between you and the internet. When you use a proxy server, your internet traffic is first routed through the proxy server, which makes requests to websites on your behalf, and then forwards the response back to you. This makes it appear as if your requests are coming from the proxy server, rather than your computer, and can also provide you with some level of privacy and security, as your IP address is hidden from the website you are visiting.

Conclusion:

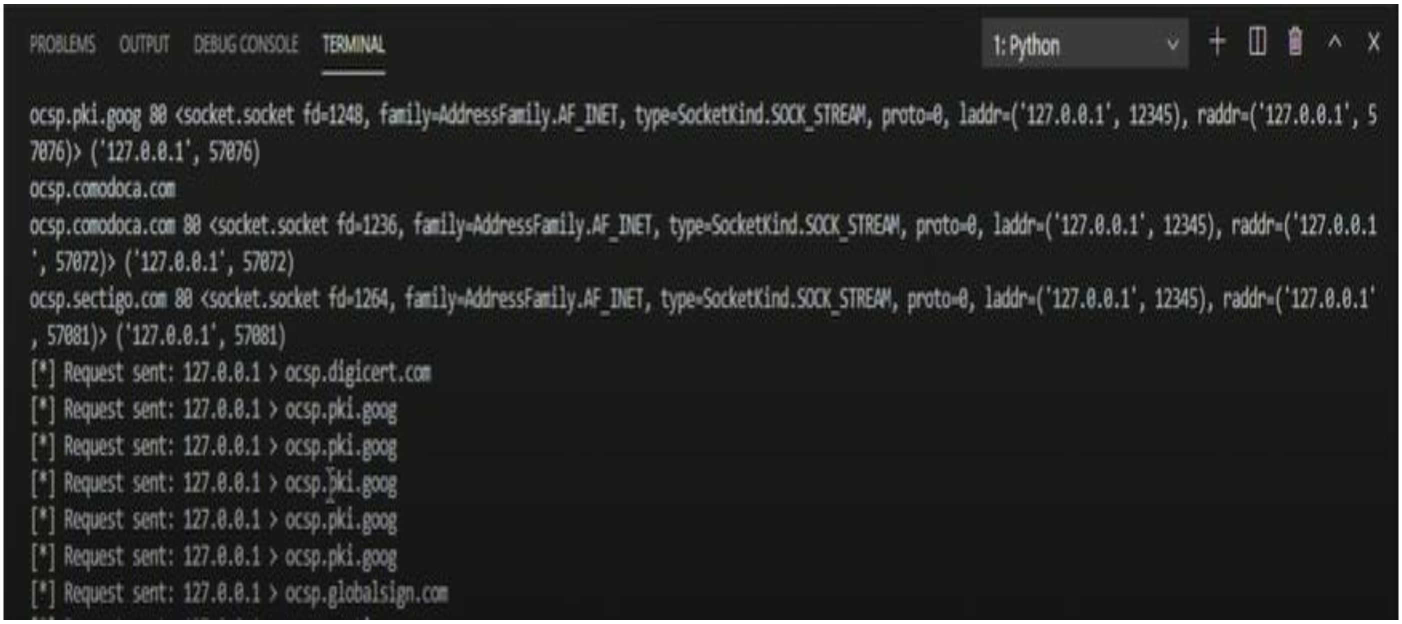
While both VPN and proxy servers provide privacy and security, VPNs are generally considered to be more secure, as they provide end-to-end encryption of all your internet traffic, whereas proxy servers only encrypt traffic between your computer and the proxy server. Additionally, VPNs also provide more reliable and consistent privacy and security, as all traffic is always routed through the VPN server, whereas with proxy servers, some traffic may bypass the proxy server altogether.

Code Demo

```
import socket,sys,_thread,traceback, ssl


def main():
    global listen_port, buffer_size, max_conn
    try:
        listen_port = int(input("Enter a listening port: "))
    except KeyboardInterrupt:
        sys.exit (0)

    max_conn = 10000
    buffer_size = 10000
    try:
        s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
        s.bind(("", listen_port))
        s.listen(max_conn)
        print("[*] Intializing socket. Done.")
        print("[*] Socket binded successfully...")
        print("[*] Server started successfully [{}]".format(listen_port))
    except Exception as e:
        print(e)
        sys.exit(2)

    while True:
        try:
            conn,addr = s.accept()
            data = conn. recv(buffer_size)
            _thread.start_new_thread(conn_string,(conn, data, addr))
        except KeyboardInterrupt:
            s.close()
            print("\n[*] Shutting down...")
            sys.exit(1)
    s.close()

def conn_string(conn, data, addr):
    try:
        print(addr)
        first_line = data.decode('latin-1').split("\n")[0]
        print(first_line)
        url = first_line.split(" ")[1]

        http_pos = url.find("://")
        if http_pos == -1:
            temp = url
        else:
            temp = url[(http_pos + 3):]

        port_pos = temp.find(":")
        webserver_pos = temp.find("/")
        if webserver_pos == -1:
            webserver_pos = len(temp)
        webserver = ""
        port = -1
        if port_pos == -1 or webserver_pos < port_pos:
            port = 80
            webserver = temp[:webserver_pos]
        else:
            port = int(temp[(port_pos + 1):][:webserver_pos - port_pos -1])
            webserver = temp[:port_pos]

        print(webserver)
        proxy_server(webserver,port,conn,data,addr)
    except Exception as e:
        print(e)
        traceback.print_exc()
```

```python
def proxy_server(webserver, port, conn, data, addr):
    print("{} {} {} {}".format(webserver, port, conn, addr))
    try:
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.connect((webserver, port))
        s.send(data)
        while 1:
            reply = s.recv(buffer_size)

            if len(reply) > 0:
                conn.sendall(reply)
                print("[*] Request sent: {} > {}".format(addr[0],webserver))
            else:
                break

        s.close()
        conn.close()

    except Exception as e:
        print(e)
        traceback.print_exc()
        s.close()
        conn.close()
        sys.exit(1)

if __name__ == "__main__":
    main()
```

Output:



```
ocsp.pki.goog 80 <socket.socket fd=1248, family=AddressFamily.AF_INET, type=SocketKind.SOCK_STREAM, proto=0, laddr=('127.0.0.1', 12345), raddr=('127.0.0.1', 5
7076)> ('127.0.0.1', 57076)
ocsp.comodoca.com
ocsp.comodoca.com 80 <socket.socket fd=1236, family=AddressFamily.AF_INET, type=SocketKind.SOCK_STREAM, proto=0, laddr=('127.0.0.1', 12345), raddr=('127.0.0.1
', 57072)> ('127.0.0.1', 57072)
ocsp.sectigo.com 80 <socket.socket fd=1264, family=AddressFamily.AF_INET, type=SocketKind.SOCK_STREAM, proto=0, laddr=('127.0.0.1', 12345), raddr=('127.0.0.1'
, 57081)> ('127.0.0.1', 57081)
[*] Request sent: 127.0.0.1 > ocsp.digicert.com
[*] Request sent: 127.0.0.1 > ocsp.pki.goog
[*] Request sent: 127.0.0.1 > ocsp.pki.goog
[*] Request sent: 127.0.0.1 > ocsp.pki.goog
[*] Request sent: 127.0.0.1 > ocsp.pki.goog
[*] Request sent: 127.0.0.1 > ocsp.pki.goog
[*] Request sent: 127.0.0.1 > ocsp.globalsign.com
```

References

- https://www.fortinet.com/resources/cyberglossary/proxy-server
- https://www.varonis.com/blog/what-is-a-proxy-server
- https://en.wikipedia.org/wiki/Proxy_server
- https://www.slidegeeks.com/business/product/firewall-and-proxy-server-configuration-ppt-powerpoint-presentation-file-smartart-pdf
- https://www.academia.edu/35373770/Presentation_on_Proxy_Server