Network Security Tools

- **ACL (Access Control List):** An Access Control List (ACL) is a set of rules that controls network traffic and restricts access to or from a network by allowing or denying traffic based on IP addresses and port numbers. ACLs are used to improve network security by filtering traffic and are commonly implemented in routers and firewalls.

```
access-list 100 deny ip 192.168.1.100 0.0.0.0 any
```

Network Security Tools

- **Intrusion Detection System (IDS)** is a security technology that monitors network traffic for suspicious activity and potential threats, alerting system administrators to potential breaches.
  - **Network Intrusion Detection System (NIDS)** is a security mechanism that monitors network traffic for suspicious activities and potential threats, alerting administrators about possible intrusions.
  - **Host-Based IDS** is a security tool that monitors and analyzes the activity and configuration of a single host to detect and respond to potential security threats or unauthorized access attempts.
- **Intrusion Prevention System (IPS)** is similar to an IDS but actively blocks or prevents identified threats from carrying out any potential harm to the network.

Devices and Procedures

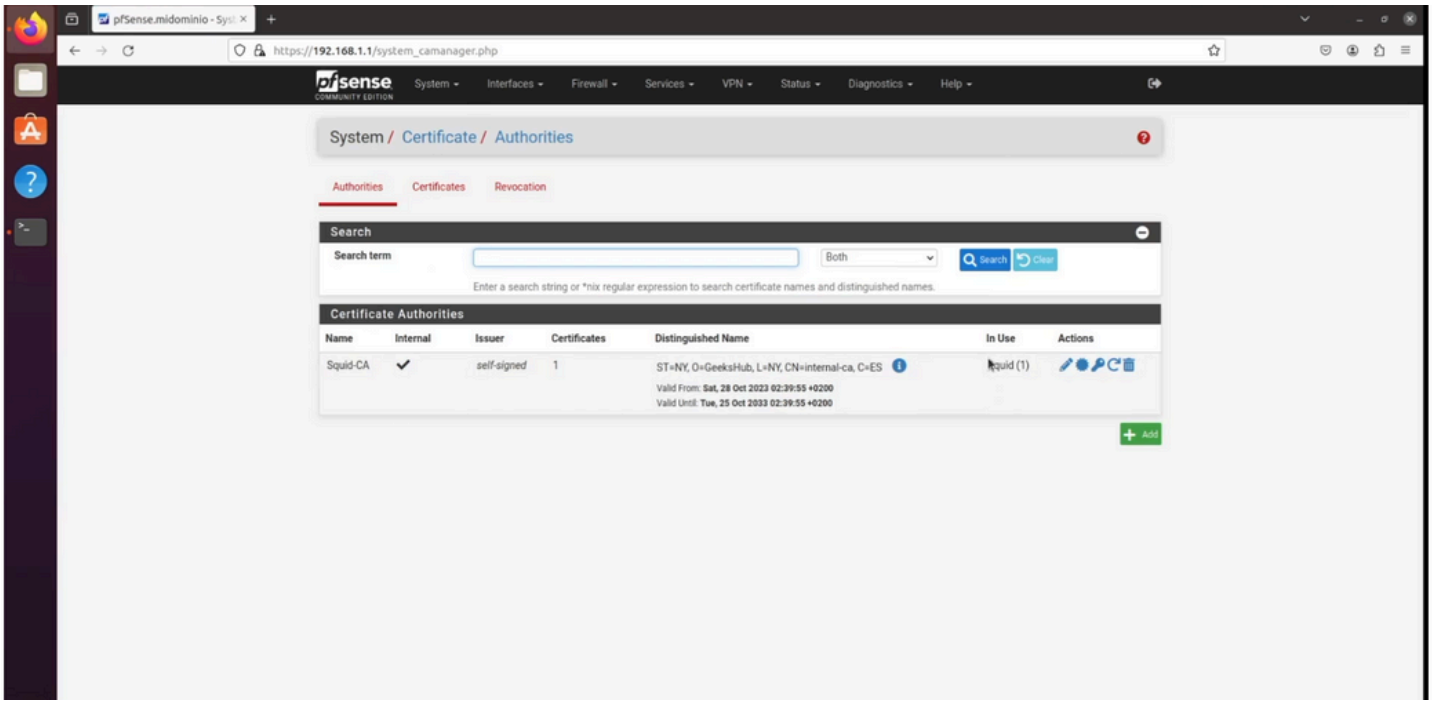
- **Proxy Server:** A proxy server is an intermediary between a user's device and the internet, which provides various functions such as web content caching, network traffic filtering, and anonymity by hiding IP addresses to enhance security and improve performance.

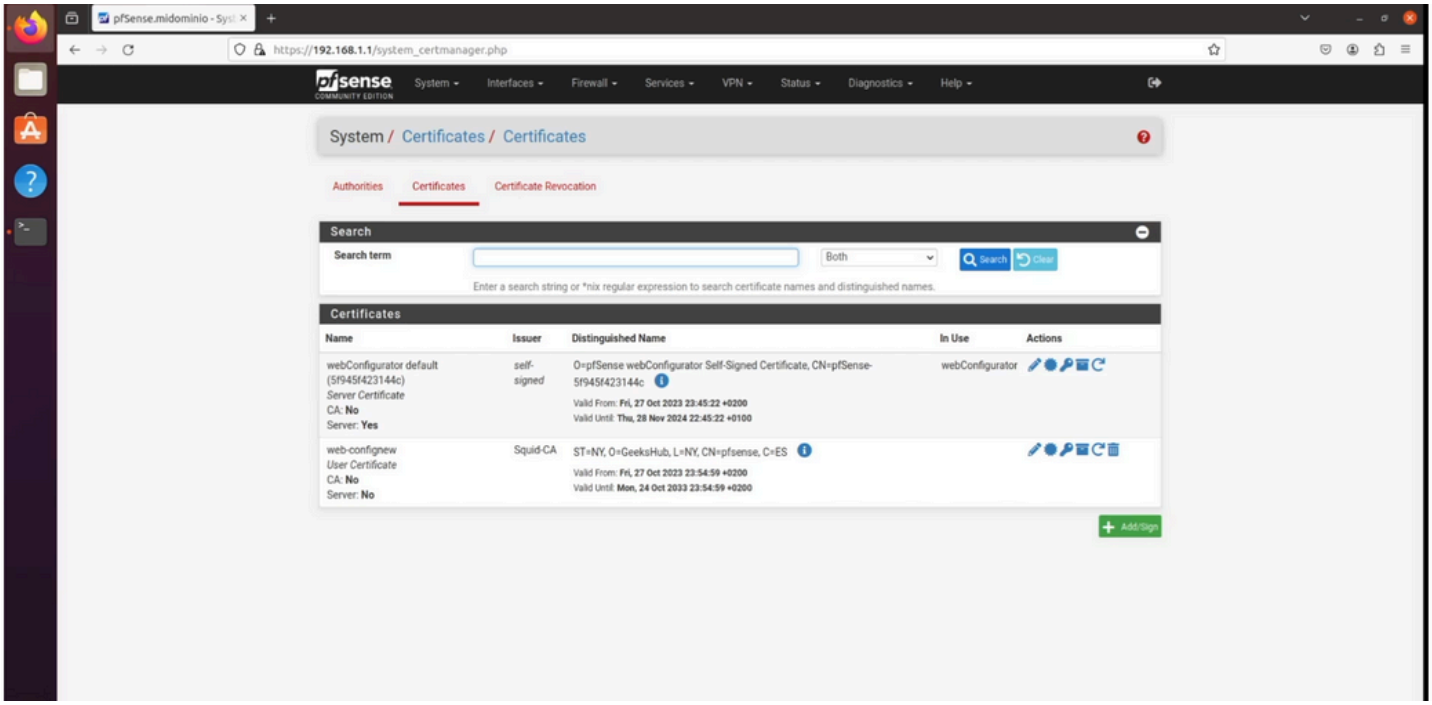
- **Reverse Proxy:** A reverse proxy is a type of server that sits in front of web servers and forwards client (e.g., web browser) requests to those web servers. It provides functions such as load balancing, authentication, decryption, and caching to improve security, performance, and scalability of web applications.

Devices and Procedures

- **SSH** (Secure Shell)

Picture source: own creation


pfSense.midominio - Syst
https://192.168.1.1/system_camanager.php
System / Certificate / Authorities
Authorities
Certificates
Revocation
Search
Search term
Both
Search
Clear
Enter a search string or *nix regular expression to search certificate names and distinguished names.
Certificate Authorities
Name
Internal
Issuer
Certificates
Distinguished Name
In Use
Actions
Squid-CA
self-signed
1
ST=NY, O=GeeksHub, L=NY, CN=internal-ca, C=ES
Valid From: Sat, 28 Oct 2023 02:39:55 +0200
Valid Until: Tue, 25 Oct 2033 02:39:55 +0200
squid (1)
Add


pfSense.midominio - Syst
https://192.168.1.1/system_certmanager.php
System / Certificates / Certificates
Authorities
Certificates
Certificate Revocation
Search
Search term
Both
Search
Clear
Enter a search string or *nix regular expression to search certificate names and distinguished names.
Certificates
Name
Issuer
Distinguished Name
In Use
Actions
webConfigurator default (5f945f423144c)
Server Certificate
CA: No
Server: Yes
self-signed
O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-5f945f423144c
Valid From: Fri, 27 Oct 2023 23:45:22 +0200
Valid Until: Thu, 28 Nov 2024 22:45:22 +0100
webConfigurator
web-confignew
User Certificate
CA: No
Server: No
Squid-CA
ST=NY, O=GeeksHub, L=NY, CN=pfsense, C=ES
Valid From: Fri, 27 Oct 2023 23:54:59 +0200
Valid Until: Mon, 24 Oct 2033 23:54:59 +0200
Add/Sign

DNS Security

- **DNS (Domain Name System) Security**

DNS is crucial for internet operation, translating domain names to IP addresses, and its security is vital to prevent cyber attacks and ensure reliable internet access.

Some DNS Attacks:

- **DDoS**
- **DNS Spoofing**
- **DNS Hijacking**

DNS Security

DNS Hardening

- Having a local DNS backup.
- Using IPAM or IP Address Management to gain a comprehensive view of the infrastructure.
- Performing updates on DNS servers.
- Implementing RRL or Response Rate Limiting to restrict the number of responses.
- Deploying DNSSEC or DNS Security Extensions, which allow adding validation to responses.
- Using RPZ or Response Policy Zones to control requests.