

Firewall

The firewall is a simple computer with `pfSense` installed on it.

`pfSense` is a `FreeBSD` based software that is often used to power firewalls. This means that there are some hardware requirements involved:

⚠ Warning!

- the device must be powered by an **AMD64 CPU** (because ARM CPUs are not widely supported) and its network interfaces mustn't use **Realtek chipsets** (Intel chipset are recommended because of compatibility issues).
- we need at least three network interfaces (**WAN**, **LAN** and **OPT1**).

In our case, the hardware doesn't matter because it is installed on a VM.

Description

The firewall has several uses in this architecture:

- **Packets filtering**: restrict access outwards and inwards using rules applying on specific ports and protocols.
- **DHCP (Dynamic Host Configuration Protocol)**: network management protocol used on Internet Protocol (IP) networks for automatically assigning IP addresses and other communication parameters to devices connected to the network using a client-server architecture.
- **DNS (Domain Name System)**: hierarchical and distributed name service that provides a naming system for computers, services, and other resources on the Internet or other Internet Protocol (IP) networks.
- **Router**: acts as a bridge between different networks (here, between the sub-LANs and the WAN).
- **NAT (Network Address Translation)**: method of mapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device (here, rules for HTTP and HTTPS requests for the web server).
- **VPN (Virtual Private Network)**: creates a secure connection on a public network.

- **Monitoring and reports:** provides tools to monitor the traffic on the network and to generate detailed reports.
- **Bandwidth management:** controls and limits the bandwidth.

Network interfaces

LAN (Local Area Network) & OPT1

The LAN (and OPT1) interface is connected to our internal private networks. It is responsible for the communication between devices on those private networks.

- **IP Addresses:** LAN 10.0.0.1, OPT1 10.0.0.9
- **Description:** Gives access to internet to all devices connected to that interface and applies security rules to protect the local networks.

WAN (Wide Area Network)

The WAN interface is connected to internet. It receives a public IP address from the ISP (Internet Service Provider). **On our VM, we configured this interface in NAT, so that it receives an IP address from the host, without having problems with the network configurations at YNOV.**

- **IP Address:** Attributed by DHCP (VM's host)
- **Description:** Manages the inward and outward traffic, applying the security rules to protect from outside threats.





































DMZ (Demilitarized Zone)

The DMZ interface is used to host services reachable from internet, isolating it from the local network (LAN) for security purposes.

























- **IP Address:** 10.0.1.1
- **Description:** Hosts our webserver which documentation is publicly reachable and applies security rules to limit access to specific services.

Filtering Rules





































LAN

| Rules (Drag to Change Order) | | | | | | | | | | | |
|------------------------------|---------------|--------------|-----------------------|------|---------------|-------------|---------|-------|----------|--|---|
| <input type="checkbox"/> | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
| <input type="checkbox"/> | ✓ 0/6.29 MiB | IPv4 TCP | Linux_ Workstation_IP | * | LAN address | 443 (HTTPS) | * | none | | Allow access to pfSense's webconfigurator. |       |
| <input type="checkbox"/> | ✓ 1/309 KiB | IPv4 TCP/UDP | LAN subnets | * | LAN subnets | Usual_Ports | * | none | | Allow internal traffic. |       |
| <input type="checkbox"/> | ✓ 0/18 KiB | IPv4 TCP/UDP | Linux_ Workstation_IP | * | WebServer_DMZ | 22 (SSH) | * | none | | Allow SSH connection from Admin client (Linux Workstation) to Webserver DMZ. |       |
| <input type="checkbox"/> | ✓ 0/1.00 MiB | IPv4 TCP | LAN subnets | * | WebServer_DMZ | WebPorts | * | none | | Allow HTTP(S) access to Webserver from LAN. |       |
| <input type="checkbox"/> | ✓ 5/60.96 MiB | IPv4 * | LAN subnets | * | ! 10.0.0.0/4 | * | * | none | | Permit all outwards traffic from LAN to public network. |       |
| <input type="checkbox"/> | ✓ 0/1.22 MiB | IPv4 TCP/UDP | LAN subnets | * | Jetbrains | 443 (HTTPS) | * | none | | Static files requests for documentation website to JetBrains server. |       |




















































OPT1

| Rules (Drag to Change Order) | | | | | | | | | | | |
|------------------------------|--------------|--------------|------------------|------|---------------|----------|---------|-------|----------|--|---|
| <input type="checkbox"/> | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
| <input type="checkbox"/> | ✓ 0/22 KiB | IPv4 TCP | OPT1 subnets | * | OPT1 address | 53 (DNS) | * | none | | Allow DNS requests from OPT1 subnets to OPT1 address. |       |
| <input type="checkbox"/> | ✓ 0/8 KiB | IPv4 TCP | OPT1 subnets | * | WebServer_DMZ | WebPorts | * | none | | Allow HTTP(S) access to Webserver from OPT1. |       |
| <input type="checkbox"/> | ✓ 0/1.07 MiB | IPv4 TCP/UDP | Backup_Server_IP | * | WebServer_DMZ | 22 (SSH) | * | none | | Allow SSH connection from Backup Server OPT1 to Webserver DMZ. |       |
| <input type="checkbox"/> | ✓ 0/0 B | IPv4 TCP/UDP | OPT1 subnets | * | ! 10.0.0.0/4 | * | * | none | | Allow traffic from OPT1 subnets to public network (ENABLE ONLY WHEN UPDATING BACKUP SERVER). |       |

WAN

| Rules (Drag to Change Order) | | | | | | | | | | | |
|------------------------------|---------------|--------------|-----------------------|------|---------------|-------------|---------|-------|----------|--|---|
| <input type="checkbox"/> | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
| <input type="checkbox"/> | ✓ 0/6.29 MiB | IPv4 TCP | Linux_ Workstation_IP | * | LAN address | 443 (HTTPS) | * | none | | Allow access to pfSense's webconfigurator. |       |
| <input type="checkbox"/> | ✓ 1/309 KiB | IPv4 TCP/UDP | LAN subnets | * | LAN subnets | Usual_Ports | * | none | | Allow internal traffic. |       |
| <input type="checkbox"/> | ✓ 0/18 KiB | IPv4 TCP/UDP | Linux_ Workstation_IP | * | WebServer_DMZ | 22 (SSH) | * | none | | Allow SSH connection from Admin client (Linux Workstation) to Webserver DMZ. |       |
| <input type="checkbox"/> | ✓ 0/1.00 MiB | IPv4 TCP | LAN subnets | * | WebServer_DMZ | WebPorts | * | none | | Allow HTTP(S) access to Webserver from LAN. |       |
| <input type="checkbox"/> | ✓ 5/60.96 MiB | IPv4 * | LAN subnets | * | ! 10.0.0.0/4 | * | * | none | | Permit all outwards traffic from LAN to public network. |       |
| <input type="checkbox"/> | ✓ 0/1.22 MiB | IPv4 TCP/UDP | LAN subnets | * | Jetbrains | 443 (HTTPS) | * | none | | Static files requests for documentation website to JetBrains server. |       |

DMZ

| Rules (Drag to Change Order) | | | | | | | | | | | |
|------------------------------|------------|---------------|--------------------------|------|-------------------|-----------------|---------|-------|----------|--|---|
| <input type="checkbox"/> | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
| <input type="checkbox"/> | ✓ 0/0 B | IPv4 TCP | Backup_Server_ IP | * | WebServer_ DMZ | 22 (SSH) | * | none | | Allow access to Webserver from Backup Server over SSH. |       |
| <input type="checkbox"/> | ✓ 0/0 B | IPv4 TCP | Linux_ Workstation_IP | * | WebServer_ DMZ | 22 (SSH) | * | none | | Allow access to Webserver from Linux Client (administrator) over SSH. |       |
| <input type="checkbox"/> | ✓ 0/0 B | IPv4 TCP | * | * | WebServer_ DMZ | WebPorts | * | none | | Allow access to the Webserver's website over HTTP(S). |       |
| <input type="checkbox"/> | ✗ 0/0 B | IPv4 * | DMZ subnets | * | OPT1 subnets | * | * | none | | Block traffic from DMZ to OPT1 subnets. |      |
| <input type="checkbox"/> | ✗ 0/756 B | IPv4 * | DMZ subnets | * | LAN subnets | * | * | none | | Block traffic from DMZ to LAN subnets. |      |
| <input type="checkbox"/> | ✓ 0/46 KiB | IPv4 TCP | WebServer_ DMZ | * | DMZ address | 53 (DNS) | * | none | | Allow DNS requests from Webserver to DMZ address. |       |
| <input type="checkbox"/> | ✓ 0/504 B | IPv4 ICMP any | WebServer_ DMZ | * | DMZ address | * | * | none | | Allow ping from Webserver to DMZ address. |       |
| <input type="checkbox"/> | ✓ 0/0 B | IPv4 TCP/UDP | WebServer_ DMZ | * | ! 10.0.0.0/4 | Usual_ Ports | * | none | | Permit outward traffic from Webserver to public network (ENABLE ONLY WHEN UPDATING WEBSERVER). |       |
| <input type="checkbox"/> | ✓ 0/0 B | IPv4 ICMP any | WebServer_ DMZ | * | ! 10.0.0.0/4 | * | * | none | | Allow ping from Webserver to public network (FOR TESTING PURPOSES ONLY). |       |

Conclusion

The **pfSense** firewall plays a crucial role in the security of our network infrastructure controlling all traffic between its interfaces (WAN, LAN, OPT1, DMZ) applying security rules that we chose and just presented.

This documentation provides a complete overview of the configurations of pfSense and its filtering rules.

Revision #1
Created 9 August 2024 09:02:55 by Admin
Updated 9 August 2024 09:07:30 by Admin