Lab 04: Firewall and NAT

Network Infrastructure Security (CSP)  
 2024-2025

© Henk Brouckxon, Chris Roets, Nico Declerck

# Introduction

## Lab concept

During this lab, we will ...

## Learning goals

* Zone-based firewall configuration
* Firewall rules for LAN and DMZ networks
* NAT
* Port forwarding to make services available to the outside world

## Practicalities and prerequisites

You will need the following:

* A laptop/desktop 😊
* Your personal NIS environment, configured as required at the end of lab 3, e.g. with the following:
  + 3 VLANs (**workstations**, **management** and **DMZ**), each with its own subnet
  + inter-VLAN routing enabled in such a way that all hosts can communicate with each other and have working internet access (through WAN)
  + correctly configured DNS overrides in the DNS server (firewall -> services -> unbound DNS)

# Firewall rules – inspecting the initial configuration

1. Log in to the web configuration interface of the firewall host, and make a backup of its initial configuration (System -> Configuration -> Backups -> Download configuration).

A screen shot of a computer

Description automatically generated

1. investigate the firewall rules for the different interfaces. Also look at the ‘floating’ rules
   1. what are floating rules?

This rules can apply to more than one interface for example. It is like a matching rules, that It works for if only something complies with its description.

* 1. One of the rules has a description “anti-lockout rule”. What is this rule used for?

This is a rule that allows administrators not to get locked automatically whenever they mess something up.

* 1. What is the result of the current rules? What connections are (not) allowed?

A screenshot of a computer

Description automatically generated

For the VLANs, we allow all type of traffic. For other types of floating rules we really have not much, like allow anything from firewall to others, disables sshlockout, disabled all traffic ipv4/6 for port 0

# Firewall configuration part 1 – testing a simple rule

1. Perform an NMAP scan of the complete **DMZ** network from the workstation-01 host. What services can you see?

A computer screen shot of a black screen

Description automatically generated

http services look to be up and running, the default gateway is probably the firewall.

1. Open the web configuration interface of the **firewall**, and create a new firewall rule for the **workstations** interface (Firewall -> Rules -> workstations). This rule should **block** all incoming IPv4 and IPv6 connections at the **workstations** interface, that are aimed at **TCP port 22** on **any host** in the **DMZ** network. Make sure that the firewall logs the connection attempts that trigger this rule[[1]](#footnote-2).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Action | TCP/IP version | protocol | source | Source port(s) | destination | Destination port(s) |
| block | IPv4+6 | TCP | \* | \* | DMZ net | 22 |

IN ORDER TO NOT GET LOCKED OUT AND DISABLE DEFAULT ALL ALLOWING RULES:

Create a new rule

A screenshot of a computer

Description automatically generated

The idea is to create a new rule, that will allow to connect from the outer network, or from the inside.

Then I tried to perform the scan, and I had no results. That is because the “all allowing” rule got disabled, hence I had no way to see the processes. Now I added a rule for WorkstationVLAN, towards DMZVLAN, that allows all type of traffic.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

The order of rules matters, as first it will allow everything, then it will block ssh, and go up by rules.

1. Again perform an NMAP scan of the complete **DMZ** network from the workstation-01 host. What services can you see now? If necessary, modify the firewall rule until you reach the expected result (i.e. that the service on port 22 is no longer available). Keep in mind that the order of the rules is also important!!

A screenshot of a computer

Description automatically generated

I finally see them working.

1. Now modify the firewall rule to **reject** the connections, instead of **blocking** them.

In the rule, change from Block -> Reject

1. Again perform an NMAP scan of the complete **DMZ** network from the **workstation-01** host. Can you see a difference compared to the previous scans?

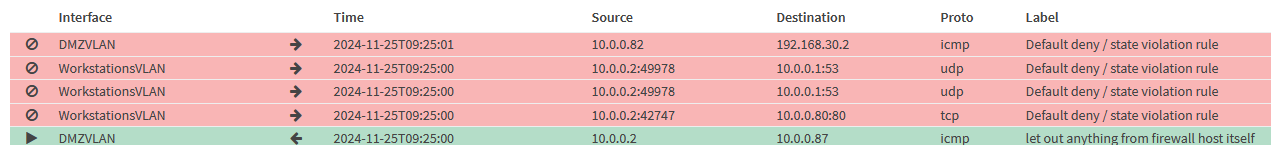
A computer screen shot of a black screen

Description automatically generated

The services do not even appear in there.

1. Check in the logs of the firewall if you can see the blocked/rejected connection attempts.

Tried to check the live view, too lazy to filter, hence this looks like:



But it does work.

1. Remove the firewall rule.

A screenshot of a computer

Description automatically generated

I disabled it for now.

# Firewall configuration part 2 – firewall policy

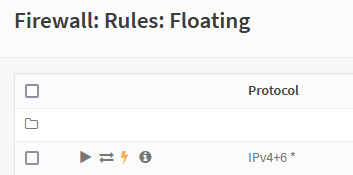
1. Design a set of firewall rules for the different zones, based on the following policies:

* None of the internal networks (**workstations**, **management** and **DMZ**) should be directly accessible from the **WAN** network

I swear to all the Computer Science gods, I already restarted this first step a very big amount of times.

What I did, is that I removed all the rules that I had. I also found out that I can not ping my firewall from my workstations, but can do it from other machines.

Next thing, I disabled the floating rule allowing everything, all the traffic.



For EVERY SINGLE INTERFACE, I created another set of rules, that allows all the type of traffic, BOTH ways.

Like here

A screenshot of a computer

Description automatically generated

Then, I will disable from WAN to every other VLAN.

A screenshot of a computer

Description automatically generated

* Devices in the internal networks (**workstations, management and DMZ)** should have almost unrestricted access to the internet (through the **WAN** interface), but should only be allowed to use our own internal DNS server (which is running on the firewall device).

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

This started working only after a couple of minutes, and I do not know why it is so slow. This does not make any sense to be this slow even in such an environment.

* Devices in the **workstations** network should have access to all the websites that are hosted in the **DMZ** network. They should also be able to access server-01 through ssh .

A screenshot of a computer

Description automatically generated

A screenshot of a computer

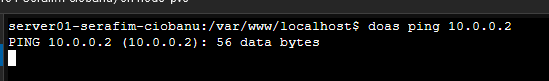
Description automatically generated

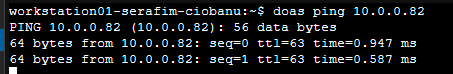
* Devices in the **management** network should have full access to the other internal networks (**workstations, DMZ**).

A screenshot of a computer

Description automatically generated

* Devices in the **DMZ** network should not have access to the other internal networks (**workstations, management**).





A screenshot of a computer

Description automatically generated

Workstations interface

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Action | TCP/IP version | protocol | source | Source port(s) | destination | Destination port(s) |
| Block | IPv4+6 | TCP/UDP | WorkstationsVLAN | \* | ! This Firewall | 53 (DNS) |
| Allow | IPv4+6 | TCP/UDP | WorkstationsVLAN | \* | This Firewall | 53 (DNS) |
| Allow | IPv4+6 | TCP | WorkstationsVLAN | \* | DMZVLAN | 80-443 |
| Allow | IPv4 | TCP | WorkstationsVLAN | \* | 10.0.0.82/29 | 22 (SSH) |

Don’t know what is up with this but whatever, I can get access to first one at least.

A screenshot of a browser

Description automatically generated

A screenshot of a computer

Description automatically generated

Management interface

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Action | TCP/IP version | protocol | source | Source port(s) | destination | Destination port(s) |
| Block | IPv4+6 | TCP/UDP | ManagementVLAN | \* | ! This Firewall | 53 (DNS) |
| Allow | IPv4+6 | TCP/UDP | ManagementVLAN | \* | This Firewall | 53 (DNS) |
| Allow | IPv4+6 | \* | ManagementVLAN | \* | DMZVLAN | \* |
| Allow | IPv4+6 | \* | ManagementVLAN | \* | WorkstationsVLAN | \* |

DMZ interface

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Action | TCP/IP version | protocol | source | Source port(s) | destination | Destination port(s) |
| Block | IPv4+6 | TCP/UDP | DMZVLAN | \* | ! This Firewall | 53 (DNS) |
| Allow | IPv4+6 | TCP/UDP | DMZVLAN | \* | This Firewall | 53 (DNS) |
| Block | IPv4+6 | \* | DMZVLAN | \* | WorkstationsVLAN | \* |
| Block | IPv4+6 | \* | DMZVLAN | \* | ManagementVLAN | \* |

WAN interface

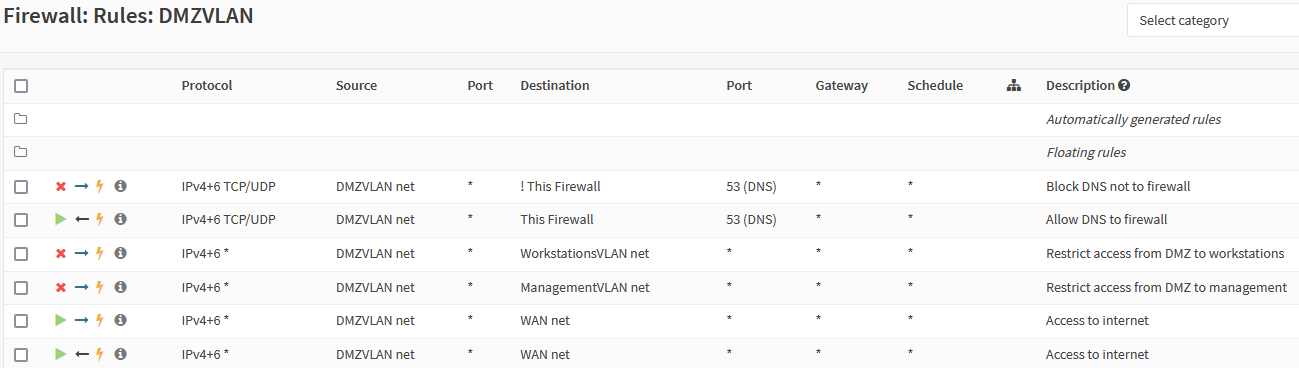
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Action | TCP/IP version | protocol | source | Source port(s) | destination | Destination port(s) |
| Block | IPv4+6 | \* | WAN | \* | WorkstationsVLAN | \* |
| Block | IPv4+6 | \* | WAN | \* | DMZVLAN | \* |
| Block | IPv4+6 | \* | WAN | \* | ManagementVLAN | \* |
| Allow | IPv4+6 | \* | \* | \* | \* | \* |

A screenshot of a computer

Description automatically generated

1. Apply the designed rules in your environment, and verify/test them.

OVERVIEW:



A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

FLOATING RULE NOT DISABLED.

1. Make a screenshot of the firewall rules table for the **workstations** interface in the firewall’s configuration website. To prove that you performed this on your own environment, add your first name to the description of the rule that to allows access to server-01 through ssh**. Submit this screenshot on Leho.**

**A screenshot of a computer

Description automatically generated**

# Making services available to the outside world: port forwarding

Because the NIS company wants to run its own website(s) on-premises, we want to make the websites that are hosted on **server-01** and **server-02** available to the outside world. Unfortunately, NIS doesn’t yet have access to IPv6 (which would provide each host with its own GUA address which can be made internet-accessible ), and only has the WAN IPv4 address of the router which is accessible from the outside world. Therefore, we decide to use port forwarding to make the websites accessible through this IPv4 address. The websites are only available through HTTP (a HTTPS version would be more secure, but is not yet available)

1. Use NAT port forwarding in the OPNsense firewall to make the HTTP websites of server-01 and server-02 available to the outside world:

* The HTTP website of server-01 should be available on http:// <WAN IP>:8081
* The HTTP website of server-02 should be available on http:// <WAN IP>:8082

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. to test the port forwarding by connecting to the WAN IP address (and corresponding ports) from your laptop’s web browser[[2]](#footnote-3).

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Firewall > Settings > Advanced

* + - * Enable automatic NAT for Reflection
      * ~ Enable Disable reply-to on WAN rule

# Bibliography

|  |  |
| --- | --- |
| [1] | "OPNsense manual: Firewall rules," [Online]. Available: https://docs.opnsense.org/manual/firewall.html. |

1. You may need to also remove an existing firewall rule [↑](#footnote-ref-2)
2. The website on the server-01 requires you to explicitly go to its html page http://<IP>/index.html [↑](#footnote-ref-3)