Building and Configuring a Basic Multi-Subnet Network and Firewall

Part 2

Continuing from part 1

Initial Functionality Testing

*Pinged the server via both its IP address and its URL from each of the two clients:*

Text

Description automatically generated

Text

Description automatically generated

Basic Firewall Rules

------------------------------------------------------------------------------------------------------------------------------

***The pfSense webconfigurator (webpage) can only be accessed from the LAN interface.***

------------------------------------------------------------------------------------------------------------------------------

*In order to establish basic network connectivity, you started with “ALLOW ALL” (or PASS ALL) rules in pfSense for the LAN net and OPT1 net. Now you must remedy this significant security issue prior to permitting other users on the network. You must remove the “ALLOW ALL” rules and create appropriate rules for specific protocols to allow the functionality specified by corporate policy. It is not up to you to decide what should be allowed – it is your duty to implement the policy.*

The following are the firewall ***policies*** that must be implemented. Remember that it is the security architect’s duty to create *rules that enforce the policy* **in the most restrictive way possible!** Another way of saying that is that the policy must pass the least number of packets possible while meeting the policy objective. If it’s not done in the most restrictive way possible, it will not survive a vulnerability test.

**Policy 1:**

*- The IT department (LANnet) will have access to all systems in the server subnet (WANnet) via VNC (port 5900) & SSH (port 22) only. That is, only ports 5900 and 22 should be allowed as the destination port from the LANnet to the WANnet.*

*- Note that that LANnet has access to ports 443 and 80 by default, as the “anti-lockout rule”. This rule can not be removed to prevent the case where you accidentally “lock yourself out”.*

*- Remember, after you specified all the “allow” rules, the last rule in the Firewall should always be “reject any”, which essentially denies all the other possibilities that has not been explicitly allowed.*

1. Created pfSense firewall rules that implement policy 1.

Down Below is a screenshot for the rules of the LAN net

Graphical user interface, text, application

Description automatically generated

**Policy 2:**

*- Corporate clients (OPT1net) will have access to the server via HTTP (port 80), HTTPS (port 443) and FTP (port 21) only. That is, only ports 80, 443, and 21 should be allowed as the destination port from OPT1net to WANnet.*

*- Don’t forget to add a “reject any” rule at the end.*

2. Created pfSense firewall rules that implement Policy 2. Graphical user interface, application, Word

Description automatically generated

1. Demonstrated that the rules I created for Policy 1 actually work. On the Admin Client,

This screenshot shows nn active VNC connection to the server (VNC session window in Remmina).

A screenshot of a computer

Description automatically generated with medium confidence

Next screenshot shows a successful SSH session log in to the server (5.5.5.5) using a terminal

Text

Description automatically generated

Next screenshot shows An attempt to access the web server from a web browser

A screenshot of a computer

Description automatically generated

1. Demonstrated that the rules I created for Policy 2 on the OPT1 ACL actually work. From the Cooperate Client.

The server’s default web page (index.html with my first name and last name in it)

Graphical user interface, text, application

Description automatically generated

A successful FTP connection screen

* 1. Text

     Description automatically generated