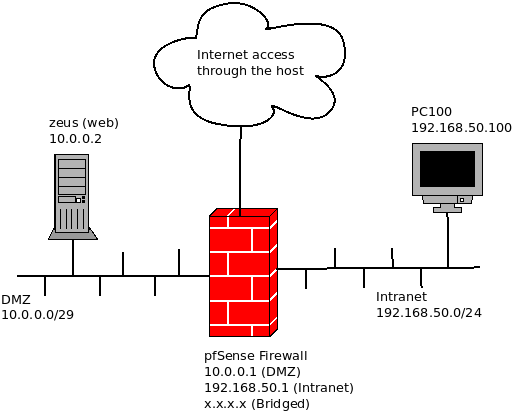
Laud Mills

Prepare the network as per the design below:

You will need to create a new virtual machine for pfSense. The client and server are already available to import from the file pfSense\_lab.ova. The password for both the user herzing and root is Herzing2021.

Please make sure the first interface in the firewall is set as bridged, the second as internal (network name: intranet) and the third internal as well (network name: dmz). Once the pfSense ISO file is linked to the optical drive, the installer will be launched. Remember to remove the ISO file from the optical drive when done. After the installation is finished, pfSense must be initially set up using the non-graphical menu options 1 (assign interfaces) and 2 (assign IP addresses).

Reference tutorial: https://docs.netgate.com/pfsense/en/latest/install/install-pfsense.html

After the initial set up, you can continue the configuration from the client. Open the URL [http://192.168.50.1](http://192.168.50.1/) in the browser. The default credentials are admin / pfsense.

Please note most changes in the firewall require clicking on “Save” and/or on “Apply changes”. This will not be specified on the tasks but it must be done anyway.

Perform the tasks **providing screenshots** and respond to the questions below:

1. Capture the interfaces summary as shown above the firewall’s text menu.

A computer screen shot of a computer

AI-generated content may be incorrect.

1. What is the default domain and primary DNS server? Set the domain to herzing.lab and the DNS servers to 208.67.222.222 (primary) and 208.67.220.220 (secondary). Do not allow the configuration to be overridden by disabling the checkbox.

The default domain is home.arpa but has no primary DNS Server

A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.

1. You can leave the WAN interface in DHCP mode, but make sure you are aware of the IP assigned by your home router or device that is assigning IP addresses in your host’s network. Disable the check “Block RFC1918 Private Networks”, for you will need to test the firewall from your host machine, which has a private IP address. In a real case scenario, you would not disable this option for security reasons. What is the use of the “Block bogon networks” option that is checked at the bottom?

The Block Bogon Networks, blocks unwanted traffic from invalid or reserved IP address ranges, helping to secure the network from a range of potential threats.

1. Set the password to the one used for root and herzing user. Reusing the password would not be recommended in a real scenario. Why? What other security measure regarding the password would you recommend?

Because default passwords are well documented and known and prone to easy access to systems and its resultant compromise. It is therefore a good practice to quickly change default passwords with between 12 to 16 character password with combination of Alphabets, Numbers including capitalization and lower cases with special characters blended to avoid easy guess. There is also the need to avoid dictionary words and names that are easy to guess.

A screenshot of a computer

AI-generated content may be incorrect.

1. Once finished, the system information is shown. What are the full system name and the user? What kind of digits compose the Netgate Device ID?

Full system name:pfSense.herzing.lab

User [admin@192.168.50.100](mailto:admin@192.168.50.100) (Local Database)

Netgate Device ID is composed of alphanumeric characters.

A screenshot of a computer

AI-generated content may be incorrect.

1. Click on the menu and go to Firewall → Rules. Explain the existing rules on the WAN interface.

Currently there are no rules on the WAN interface, hence all incoming connections in the WAN interface will be blocked until an explicit rule to allow is added.

1. Also, explain the existing rules on the LAN interface.

The LAN interface has HTTP traffic allowed and two rules for anything IPV4 and IPV6.

1. Why is it necessary to have two “Add” buttons? What is the difference?

One adds rule to the top of the list and the other adds rules to the bottom of the list and since firewall rules are executed in sequence of their appearance, it matters the position of a rule amid other rules. For instance, and allow rule mostly must come after deny in many circumstances.

1. What interfaces might a floating rule apply to?

The Floating rule can apply to multiple interfaces (WAN, LAN and OPT interfaces)

1. On the menu, go to Firewall → Aliases. Create one to reference the server “zeus” as “webserver”. What information did you provide?

Name, Description, Type, IP address or the Fully Qualified Domain Name (FQDN)

A screenshot of a computer

AI-generated content may be incorrect.

1. Create a new alias named “webports” that include both ports TCP 80 and 443. Describe the provided information. What category was the alias put on?

Information provided are: Name, Description, Type and Ports. It was put on Ports Cartegory.

A screenshot of a computer

AI-generated content may be incorrect.

1. Now add a firewall rule to allow the communication from the internal network to “zeus” on port TCP 25. Use some of the alias you created. What source did you specify? What destination? What did you choose from the port range list? Why?

I specified LAN net as source and Single Host or Alias as Destination – webserver

A screenshot of a computer

AI-generated content may be incorrect.

1. Copy the previous rule but changing the port to 80 and 443. Use the corresponding alias. How did you copy it? What position did the new rule take (top or below another rule)? What did you use as Destination Port Range?

I clicked on the duplicate button the rule is directly below the previous one it was copied from. Destination Ports other – custom webports (80:443)

A screenshot of a computer

AI-generated content may be incorrect.

1. Just after this two rules, add another one to block all traffic from the internal network to any host in the DMZ on any port. What information did you provide in the first, second and third sections? Note: remember to apply the changes or the rules will not be active.

Action is to BLOCK Source:LAN net and Destination: OPT1 net which is the DMZ

A screenshot of a computer

AI-generated content may be incorrect.

1. What would happen if the three rules were in different order (block first and allow second)?

When the Block rule is placed first without specific details as to what to block, it takes precedence over all other subsequent rules and all including good traffic will be blocked.

1. You can make sure the port 25 rule is working by executing “telnet 10.0.0.2 25” from a shell in the client. After a while, you should get a response from Exim, the mail server. If the rule didn’t work, you would simply wait a long time after “Trying 10.0.0.2…” What message did you get from Exim? You can type “quit” and press ENTER to get the shell prompt again.

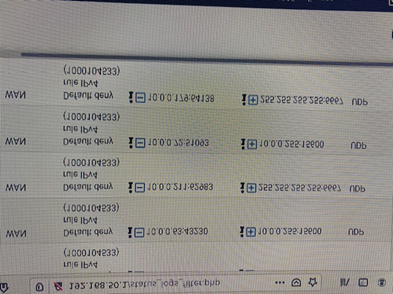
220 Zeus ESMTP Exim 4.94.2

A computer screen shot of a computer

AI-generated content may be incorrect.

1. Try executing “telnet 10.0.0.2 8080” from a shell in the client. Leave it trying. Meanwhile, on the firewall dashboard go to Status → System Logs → Firewall. Is there any information regarding port 8080 at the bottom of the normal view? What kind of traffic is being blocked? What are the three last numbers of the rule?

UDP traffic is being blocked and the last three numbers of the rule is 533.



1. Go to Firewall → Rules and, in the LAN tab, activate the logging for the rule you created to block all traffic to the DMZ by editing the rule and scrolling to the “Extra Options” section. Try again “telnet 10.0.0.2 8080” from a shell and check now the firewall log. What type of rule and number is available regarding port 8080? What the buttons “-” and “+” are for?

UDP and the number is 103. The - and + buttons are use to delete and add rules respectively.

A computer screen with a number of words

AI-generated content may be incorrect.

1. You probably have seen blocked DNS traffic. To allow it, create a single rule that applies to both the DMZ and internal network for outbound traffic on port UDP 53. What kind of rule did you create? Describe the information provided for Interface, Direction, Protocol, Source, Destination and Port Range.

I created an Alias for DMZ and LAN(DNSServer) and used it for a single Floating Rule.

Interfaces:LAN and OPT1 Direction: out Protocol: UDP Source: DNSServer Destination Any (UDP 53)

A screenshot of a computer

AI-generated content may be incorrect.

1. Clear the log and check that no new entries appear. How did you clear it?

Go to Status, then firewall then setting. That takes you to the General Logging Option, scroll down to Reset Log Files. Then reset which means clear.

1. Maintenance of a firewall is paramount. What menu and option would allow you to check if the system is updated?

You click on system on the menu tab then click on update. That shows you the latest version.

1. What menu entry would you use to backup the firewall? What format the output file is in? Could you restore only some areas, for instance the firewall rules?

Diagnostics then click on backup and restore. It is in an XML format. Yes you can different parts of the packages ie RRD Data, Encryption, extra data etc.