pfSense Lab

1. Install pfSense in VMplayer or VirtualBox. Configure two interfaces of pfSense so that one of the interfaces is the WAN network, and the other interface is the LAN network.
2. Give a static IP address to the LAN interface and give a dynamic IP address to the WAN interface.
3. Make it so that you can access the pfSense web login only from the LAN network and not from the WAN network.
4. Login to pfSense and set up a username and password for the firewall.
5. Put two windows machines and two Ubuntu machines on the LAN side of the firewall.
6. Make sure all four machines can connect to the internet and get dynamic IP addresses from the university DHCP server.
7. Create 10 users for the pfSense so that people can log in.
8. Create two groups “admin” and “general-users” and add 5 users in each of the groups.
9. Make it so that you can access pfSense over the web only on port 2020.
10. Disable webConfigurator login autocomplete.
11. Enable DNS Rebinding Checks.
12. Enable SSH.
13. Find the serial speed of the console port.
14. Disable hardware large receive offload.
15. Disable hardware tcp segmentation offload.
16. Disable device polling.
17. Enable state killing on Gateway failure.
18. Clear invalid DF bits instead of dropping the packets.
19. Set the firewall maximum state to 30000000.
20. Block private and bogon networks on the WAN interface.
21. Deny 192.144.44.2 access to the internal network on all ports.
22. Allow 194.12.2.2.2 access to the internal network on port 2000.
23. Configure pfSense so that anyone with an internal IP address can access the internet.
24. Disallow any traffic to go out from the internal network to the internet on port 19
25. Turn on logging.
26. Enable logging of webConfigurator successful logins.
27. Configure openVPN for so that five users have access through the firewall.
28. Configure the DHCP server on pfSense and understand how it works. Then, assign an IP address to the computers in the internal network
29. Configure RDP access to pfSense.
30. Configure NAT.
31. Find the ARP table and see if it is populated. If so, note down the MAC address and the host name of the IP address in the table.
32. Select Korea as the top spammer country and deny any inbound connection coming in from Korea.
33. Deny inbound connection from Lesotho-ls
34. Deny inbound connection from Colombia-CO
35. Enable static ARP on the WAN side.
36. Set the lease time to 100000 seconds on the LAN side.
37. Make the last rule in WAN side deny all connections from all ports ( make sure to give a reason as to why this rule is added in the end in your presentation).
38. Deny one of the windows machine access to both of the Ubuntu machines.
39. Create VPN accounts for the five users in the admin group. Use openVPN on the client side to test these VPN accounts.
40. Create NAT rules for the Ubuntu machines.

Lab created by Rugved Jakka.