NASA Homework #4

Student Name: 林楷恩
Student ID: b07902075

Network Administration

pfSense

1.
   - **Create VLAN**: In `Interfaces->Assignments->VLANs`, add `VLAN 5` and `VLAN 99`, with parent interface set to the LAN interface.
   - **Create interfaces**: In `Interfaces->Assignments->Interface Assignments`, add two interfaces:
     (a) **OPT1(VLAN 5)**: select `Enable interface`, set `Static IPv4` with address `192.168.5.254/24`
     (b) **OPT2(VLAN 99)**: select `Enable interface`, set `Static IPv4` with address `192.168.99.254/24`
   - **Setup DHCP servers**: In `Services->DHCP Server`:
     (a) **OPT1(VLAN 5)**:
       – Select `Enable DHCP server`
       – Set `General Options->Range` to `192.168.5.1`∼`192.168.5.253`
       – Add `8.8.8.8` and `8.8.4.4` in `Server->DNS servers`
       – As for the `Gateway`, the default setting is using the IP on this interface of the firewall as the gateway, so I don't need to configure it.
     (b) **OPT2(VLAN 99)**: Almost the same as **OPT1**, except `Range` is `192.168.99.1`∼`192.168.99.253`
   - **Initiate Firewall Rules(preparation for other problems**: In `Firewall->Rules`:
     (a) **OPT1(VLAN 5)**, because of problem 6, the default rule will be "Accept All":
       – Action: Pass
       – Protocol: Any
       – Source, Destination: Any
     (b) **OPT2(VLAN 99)**, because of problem 3, the default rule will be "Block All":
       – Action: Block
       – Protocol: Any
       – Source, Destination: Any
2.
   - Enable SSH management: In `System->Advanced->Secure Shell` select `Enable Secure Shell`
   - Create aliases to make things simple: In `Firewall->Aliases->Ports` add a port alias called **ManagementPort**, which containing port **22(ssh), 80(http), 443(https)**
   - Create rules to control access: In `Firewall->Rules`:
     (a) **OPT1(VLAN 5)**
       – Action: Reject
       – Protocol: TCP
       – Destination: This firewall(self)
       – Destination Port Range: **ManagementPort**
     (b) **OPT2(VLAN 99)**, because of problem 3, I don't need to restrict this rule to specific ports
       – Action: Pass
       – Protocol: Any
       – Destination: This firewall(self)
     (c) **LAN**, I need to disable webConfigurator anti-lockout rule in `System->Advanced` first
       – Action: Reject
       – Protocol: TCP

  - Destination: This firewall(self)
  - Destination Port Range: **ManagementPort**

(d) **WAN**, only block SSH:
  - Action: Reject
  - Protocol: TCP
  - Destination: This firewall(self)
  - Destination Port Range: From 22 to 22

3. • In `Firewall->Rules->OPT2`, add rules to allow specified traffic:

(a) `linux1.csie.org`:
  - Action: Pass
  - Protocol: Any
  - Destination: Single host or alias, `140.112.30.32`

(b) *pfSense*:
  - Action: Pass
  - Protocol: Any
  - Destination: This firewall(self)

(c) Hosts in VLAN 5:
  - Action: Pass
  - Protocol: Any
  - Destination: Network, `192.168.5.0/24`

4. • In `Firewall->Rules->OPT1`, add rule to block traffic to VLAN 99:
  - Action: Block
  - Protocol: Any
  - Destination: Network, `192.168.99.0/24`

5. • In `Firewall->Schedules`, add a schedule:
  - Schedule Name: *meow*
  - Add two time:
    (a) November 23, 2019, 14:00∼17:00
    (b) November 24, 2019, 14:00∼17:00

• In `Firewall->Rules->OPT1`, add a rule:
  - Action: Block
  - Protocol: UDP
  - Source, Destination: Any
  - Advanced Options->Schedule: *meow*

6. Because I have set `OPT1`'s default rules to "Pass Any", so it will not be restricted by any others except the rules I set above.

7. Since there isn't any NAT configuration, everything behaves properly, and there are no needs to change anything. Proof:

```
localhost:~# nc -lvp 9999
listening on [::]:9999 ...
connect to [::ffff:192.168.5.1]:9999 from [::ffff:192.168.99.2]:43997 ([::ffff:192.168.99.2]:43997)
```

*** References**

- https://docs.netgate.com/pfsense/en/latest/