|  |  |
| --- | --- |
| Network Security Diploma in CSF  Year 3 (Apr 2021) Semester 5 | Week 1 |
| Practical |
| Palo Alto Firewall Basic Configuration | |

**Objectives:**

1. To learn about Initial Configuration, GUI and CLI of Palo Alto Firewall: PA-3000 Series.
2. To configure interface types for various deployment options and security zones on the Palo Alto Firewall.

**Part A. Lab Network Diagram**

Figure A-1 shows the network diagram of the lab. Eight Palo Alto Firewalls are mounted in one rack located in the server room. All the firewalls are connected to a router with the interface IP address 172.16.1.1/24. The router is then connected to NPNet to have internet connection.

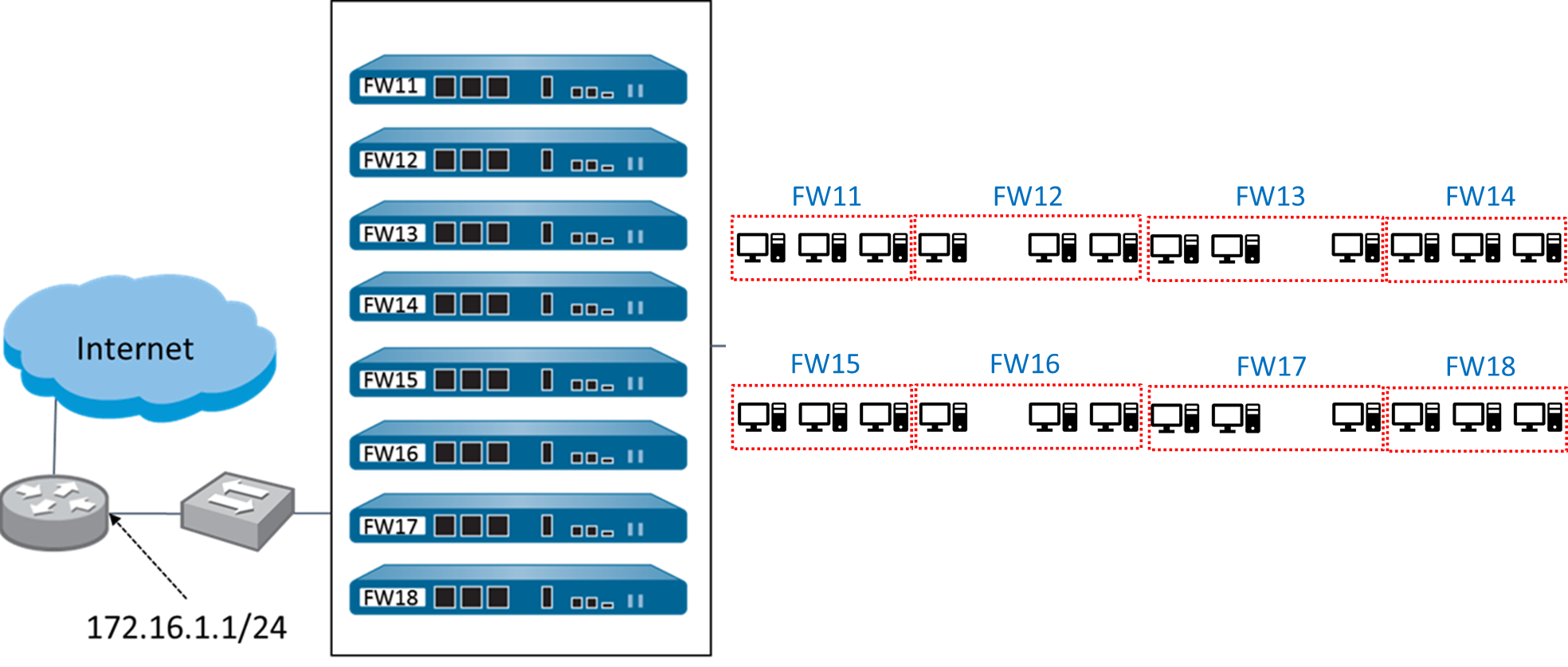


Figure A-1

Figure A-2 shows the computers grouping of the lab. Every three computers are connected to one firewall. Students are advised to work in teams to configure and manage their respective firewall.

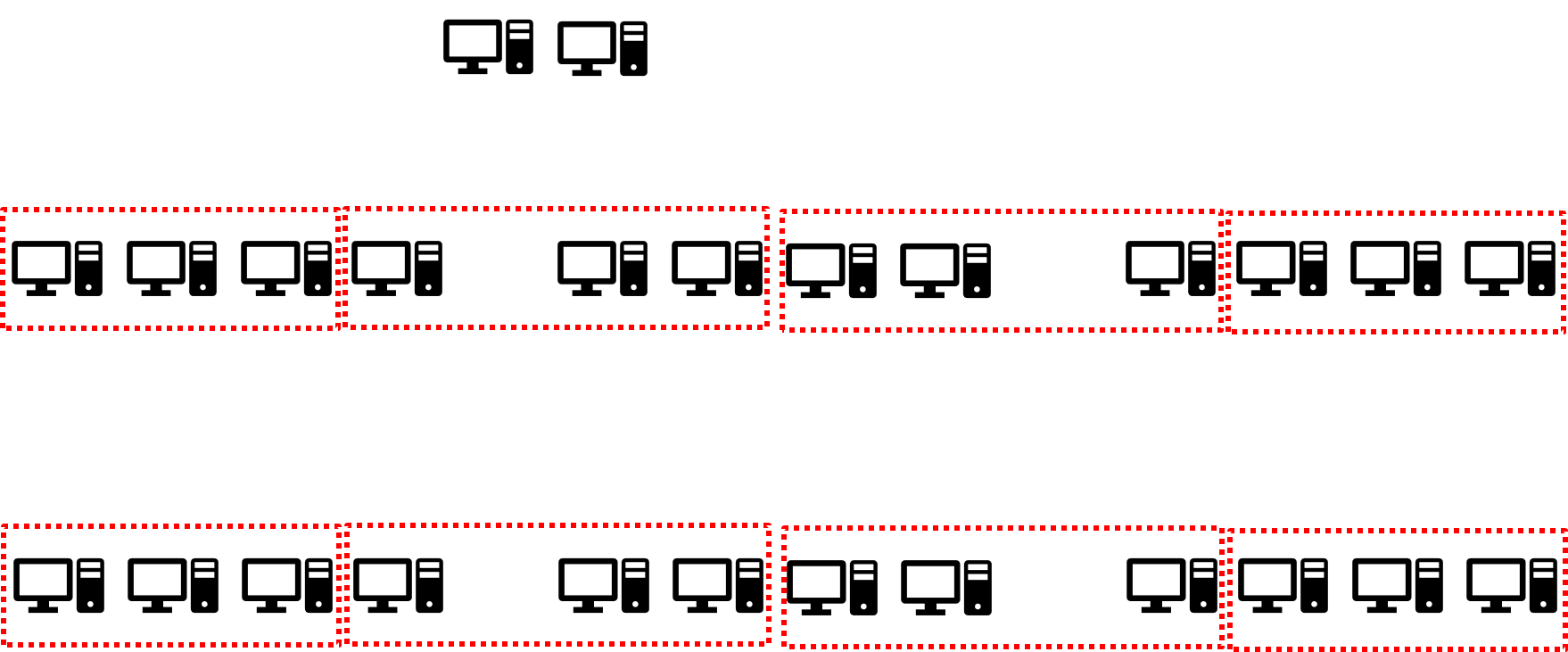


Figure A-2

Figure A-3 shows the detailed connection of one group of computers. As a summary:

|  |  |
| --- | --- |
| **Firewall Port:** | **Connected to:** |
| Port 1 | Internet |
| Port 2 | PC2 |
| Port 3 | PC3 |
| MGT Port | PC1 |

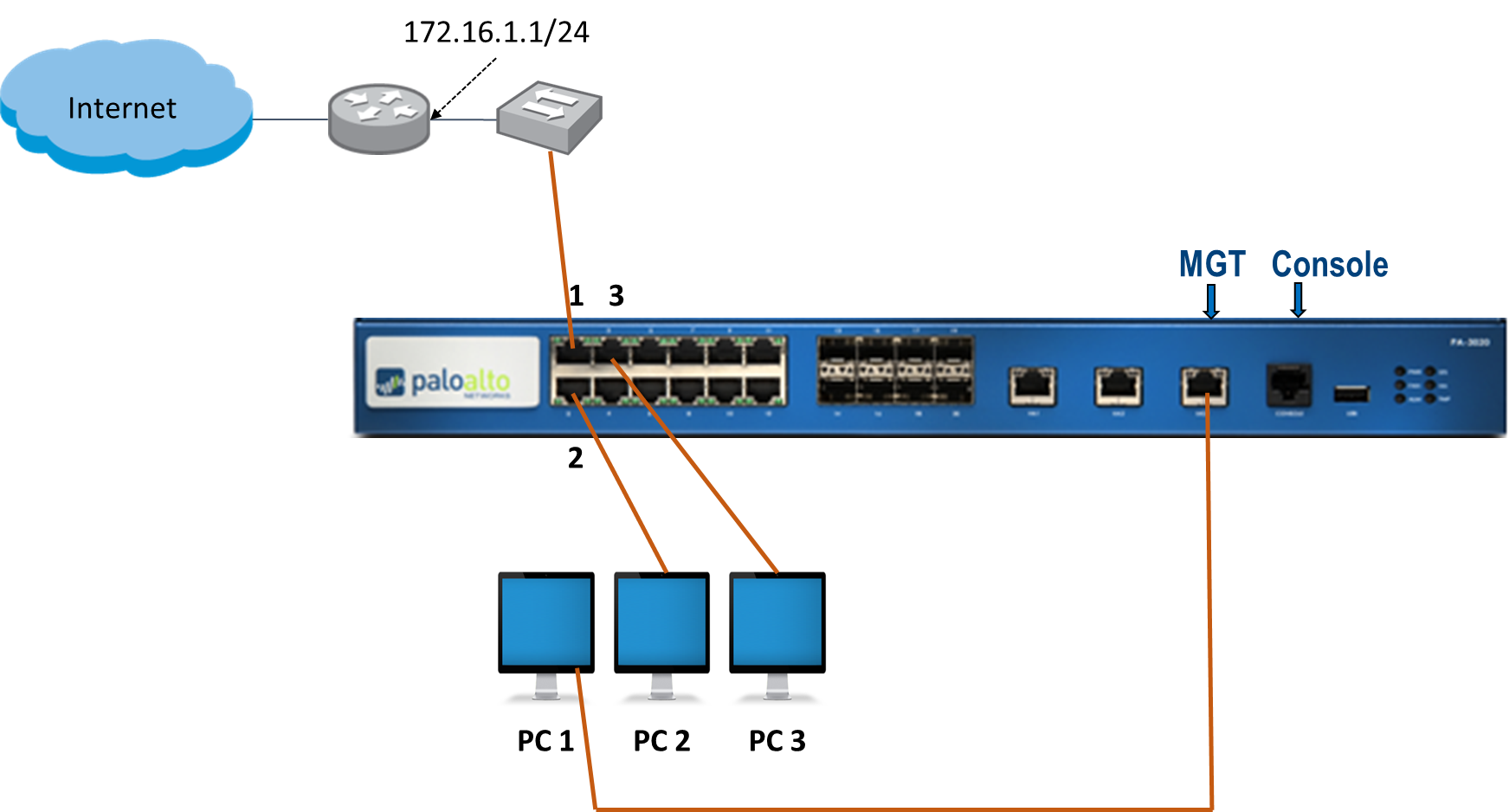


Figure A-3

Reflection Questions.

1. State which PC your team should use to configure and manage the firewall. Also suggest a proper IP address to be configured for this PC.

|  |
| --- |
| PC1 is connected to MGT interface, which is used for direct connection to the management plane of the firewall.  Since the MGT interface has an ip address of 192.168.1.1. PC1 should be configured with an ip address of the same network |

1. The MGT interface is also called as “out-of-band” network management interface. Briefly explain the meaning of “out-of-band”.

|  |
| --- |
| The MGT interface is also called as "out-of-band" network management interface. Briefly explain the meaning of 'out-of-band". Pato Alto Networks firewalls are built with a dedicated out-of-band network management interface labeled MGT. This interface passes only management traffic for the firewall and cannot be configured as a standard traffic interface. The 12 physical interfaces are normal, in-band traffic interfaces. |

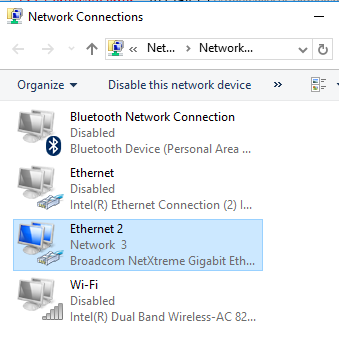
1. Suggest one possible usage of PC2 or PC3.

|  |
| --- |
| Suggest one possible usage of PC2 or PC3. PC2 and PC3 are connected to the in-band traffic interfaces, they can have normal traffic to and from the firewall. They can be used for testing the functions and configurations of the firewall. |

**Part B. Module 1 – Administration and Management**

**Configuring the MGT Interface – GUI**

1. Ensure PC1 is using Ethernet2 connection (Broadcom NIC). Disable all the unwanted network connections.



1. Set PC1 with a proper IP Address.
2. Launch the browser (Chrome preferred) and enter **https://192.168.1.1**.

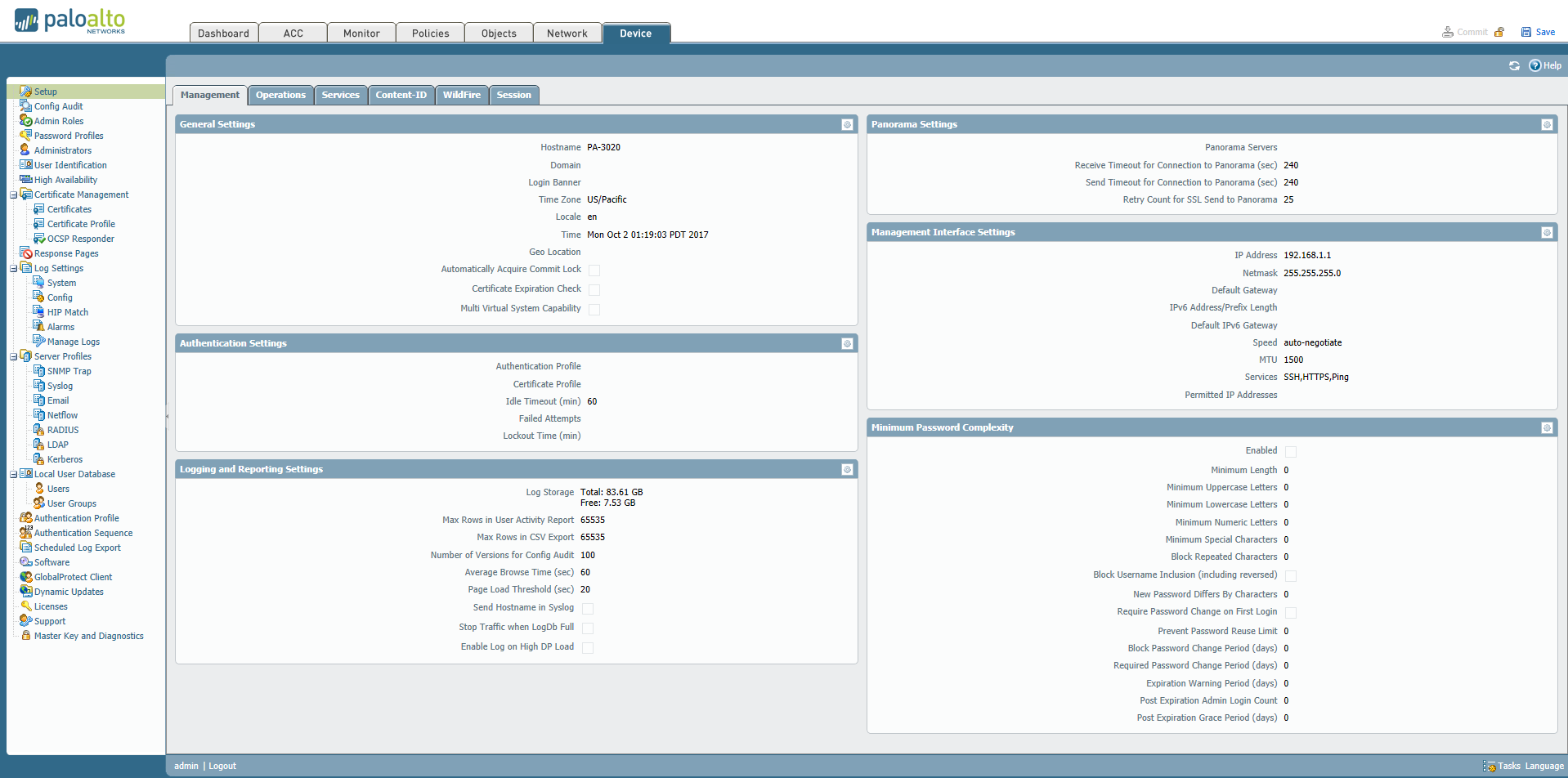
Ignore the security warnings and click proceed. The login page of the PA-3020 management console appears.

(Always use **HTTPS** connection when you are entering the firewall’s management UI)

1. Type **admin** in both the **Name** and **Password** fields.
2. Click **Login**.
3. Go to **Device > Setup > Operations**, select “Import named configuration snapshot” and then browse the config file named Reset-Config.xml. You can download this file from MeL and transfer the file to PC1 using thumbdrive.
4. After import, select “Load named configuration snapshot”.
5. Note that the Reset-Config.xml is the firewall configuration file with all the initial factory settings, you can import and load this file every time you want reset your configurations.
6. Click **Commit**.
7. Discussion: What is the function of **Commit**?

|  |
| --- |
| The running configuration is the actual configuration controlling the operation of the firewall. It is maintained in a file on the firewall named running-config,xml.  In-progress edits are made to the candidate configuration. Eg, settings changes, policies changes and etc.  When you click Commit at the top of the WebUI, the candidate configuration overwrites the current running configuration, which activates all configuration changes. |

1. Go to **Device > Setup > Management**, ensure the Management Interface Settings has the IP address of 192.168.1.1 with a netmask of 255.255.255.0.
2. Configure the General Settings with the correct Time Zone and Time.
3. Click **Commit**.



1. Explore the **Network** tab, **Policies** tab and **Monitor** tab, and briefly state the functions of each tab.

|  |
| --- |
| Explore the Network tab, Policies tab and Monitor tab, and briefly state the functions of each tab. Network tab is to configure all the networking related settings of the firewall, for example, firewall interface settings, zones, VLANs, DHCP, virtual routers and also VPN tunnel.  Policies tab is to configure security policies (firewall rules) and NAT policies. This is the main part to control and regulate the traffic in and out of the firewall.  Monitor tab contains the displays the logs for the Palo Alto Networks firewall. Log entries are added to the traffic database at end of session by default. All other logs are updated when a policy match occurs while processing network traffic. The log in the Monitor tab show a summary of the event in the GUI. |

**Part C. Module 2 – Interface Configuration**

**Choosing a Deployment Option**

1. There are 2 deployment options learnt in this week:
   1. Tap Mode
   2. Layer 2 Mode

Under what situation would you deploy each of these options?

|  |
| --- |
| Tap Mode: To connect to a core switch's mirrored port to identify applications r -- running on the network. In this mode, the Orewall cannot block traffic.  Layer 2 Mode: To deploy in an environment where switching is required (not limited to 2 ports). |

**Layer 2 Deployment (VLAN Implementation)**

Required Information:

|  |  |
| --- | --- |
| Interfaces to use for Layer 2 interface | Ethernet1/2  Ethernet1/3 |
| Name for the Layer 2 zone | Layer2-VLAN2 |
| Name for the VLAN | VLAN2 |

1. Configuring the interfaces:
   1. Click **Network > Interfaces**
   2. Click **ethernet 1/2**, choose **Layer2**  as Interface Type.
   3. Click **Config > VLAN**, choose to set a new VLAN.
   4. Set the VLAN name as VLAN2, and then click **OK**.
   5. Click **Config > Security Zone**, choose to set a new zone.
   6. Set the zone name as **Layer2-VLAN2**, and then click **OK**.
   7. Click **ethernet 1/3**, choose **Layer2**  as Interface Type.
   8. Click **Config > VLAN**, choose the VLAN2 you just created.
   9. Click **Config > Security Zone**, choose the **Layer2-VLAN2** zone you just created.
2. Verifying the Security Zones.
   1. Click **Network > Zones**.
   2. Click the **Layer2-VLAN** zone you just created.
   3. Make sure the Interfaces contains **ethernet 1/2** and **ethernet 1/3**.
3. Verifying the VLANs:
   1. Click **Network > VLANs**.
   2. Make sure the Interfaces contains **ethernet 1/2** and **ethernet 1/3**.
4. Click **Commit**.

[Now You have created a VLAN with two Layer 2 ports in the same security zone]

1. Ensure PC2 and PC3 are also using the Ethernet2 connection (Broadcom NIC) and set proper IP addresses for both PC.
2. Discussion: What are the IP addresses you set for PC2 and PC3? Are they able to ping each other? What is the function of the firewall in this scenario?

|  |
| --- |
| PC2: 192.168.1.3  PC3: 192.168.1.4  Ensure IP addresses of PC2 and PC3 are in the same network range. They can ping each other. (If necessary, turn off the Windows firewall)  The firewall is doing switching between its port 2 and port 3. |

1. Draw a simple network diagram to illustrate the current network connections.

|  |
| --- |
|  |

1. Re-configuring the Security Zones.
   1. Click **Network > Interfaces**.
   2. Click **ethernet 1/3**.
   3. Click **Config > Security Zone**, choose to set a new zone.
   4. Set the zone name as **Layer2-VLAN3**, and then click **OK**.
   5. Click **Commit**.

[Now you have created a VLAN with two Layer 2 ports in different security zones]

1. Draw a simple network diagram to illustrate the current network connections.

|  |
| --- |
|  |

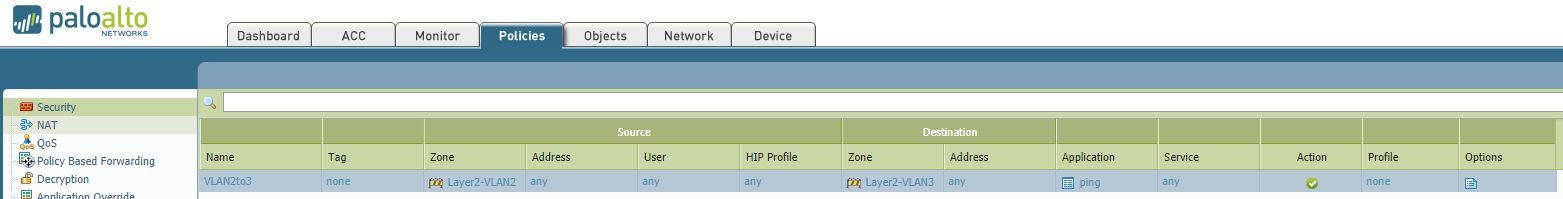
1. Without changing the IP addresses of PC2 and PC3, test whether they can still ping each other. Briefly explain your results.

|  |
| --- |
| PC2 and PC3 are not able to ping each other.  PAN implicit rule: traffic between two zone (inter-zone) is denied |

1. Create a Security policy to allow flow of traffic from **Layer2-VLAN2** to **Layer2-VLAN3**.
   1. Click **Policies > Security**. Click **Add**.

|  |  |
| --- | --- |
| **General** tab |  |
| Name | **VLAN2to3** |
| **Source** tab |  |
| Source Zone | Click **Add** and select **Layer2-VLAN2** |
| Source Address | Keep default: check box is set to **Any** |
| **Destination** tab |  |
| Destination Zone | Click **Add** and select **Layer2-VLAN3** |
| Destination Address | Keep default: check box is set to **Any** |
| **Application** tab |  |
| Applications | Choose **Ping** |
| **Action** tab |  |
| Action Setting | Keep default: radio button is set to **allow** |

* 1. Ensure your security policy looks like below:



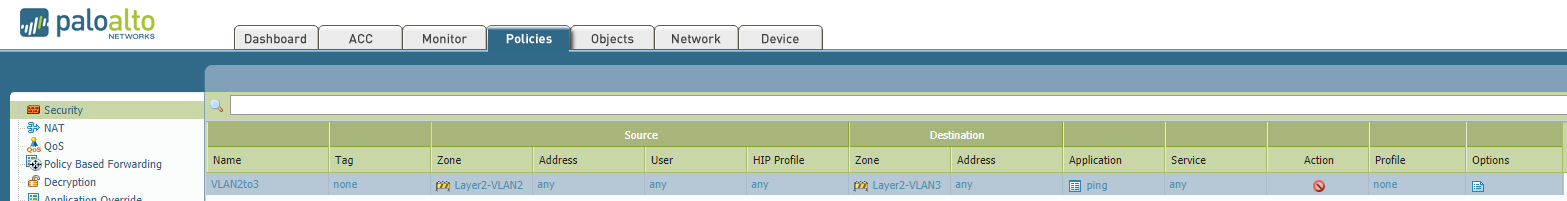
* 1. Click **Commit**.
  2. Test PC2 pings🡺PC3 and PC3 pings🡺PC2.
  3. Explain the results you obtained.

|  |
| --- |
| PC2 is able to ping PC3 as there is a security policy created to allow traffic from the security zone which PC2 is into the security zone which PC3 is in.  PC3 is not able to ping PC2 because there is no security policy allowed this ping. |

1. Go to Monitor tab and observe the traffic log. Do you have a log entry showing that PC2 pings🡺PC3 is allowed? Do you have a log entry showing that PC3 pings🡺PC2 is denied?

|  |
| --- |
| There is log entry showing PC2 pings -> PC3 is allowed.  However, there is no log entry showing PC3 pings -> PC2 is denied. The reason is that, this ping is denied by the implicit rule 'traffic between two zones (inter-zone) is denied." Implicit rules do not generate traffic log entries. |

1. Modify the security policy by changing the action from “Allow” to “Deny”. Commit the changes and then test PC2 pings🡺PC3. What can you observe from the traffic log?

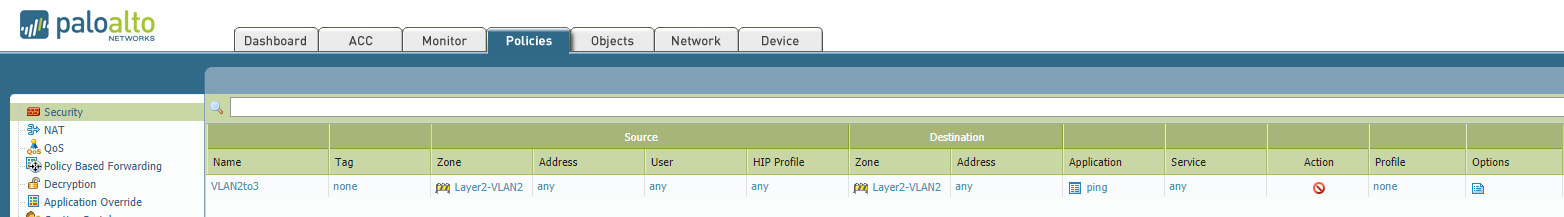


|  |
| --- |
| There is one traffic log entry showing PC2 pings ->PC3 is denied. Explicit rule will always generate traffic log entries. |

1. Revert the configurations for **ethernet 1/3** byputting it into Layer2-VLAN2 zone again. Ensure PC2 and PC3 can ping each other which you have already tested in step 6 above. Reflect on why they can ping each other.

|  |
| --- |
| Beside that PC2 and PC3 are in the same network range and the same VLAN, they are also in the same security zone. PAN firewall implicit rule: traffic within a single zone (intra-zone) is allowed. |

1. Modify the security policy by changing the destination zone to be the same as the source zone: **Layer2-VLAN2**.



1. Test PC2 pings🡺PC3. What is the result obtained and what is the reason behind?

|  |
| --- |
| Although the implicit rule allows infra zone traffic, but there is an explicit rule created deny the intra zone traffic. An explicit rule at the end of the user-defined policies will be processed before the implicit rule, and that is why the infra-zone traffic is denied. |

**Part D. Save the Configuration**

1. Go to **Device > Setup > Operations**, select “Save named configuration snapshot”. You can assign a name to your config file and name it as <name>.xml.
2. Select “Export named configuration snapshot” and then choose the location where you want to export this config file to the PC.
3. You can keep your own config file so that next practical session you can import and load your own config again.