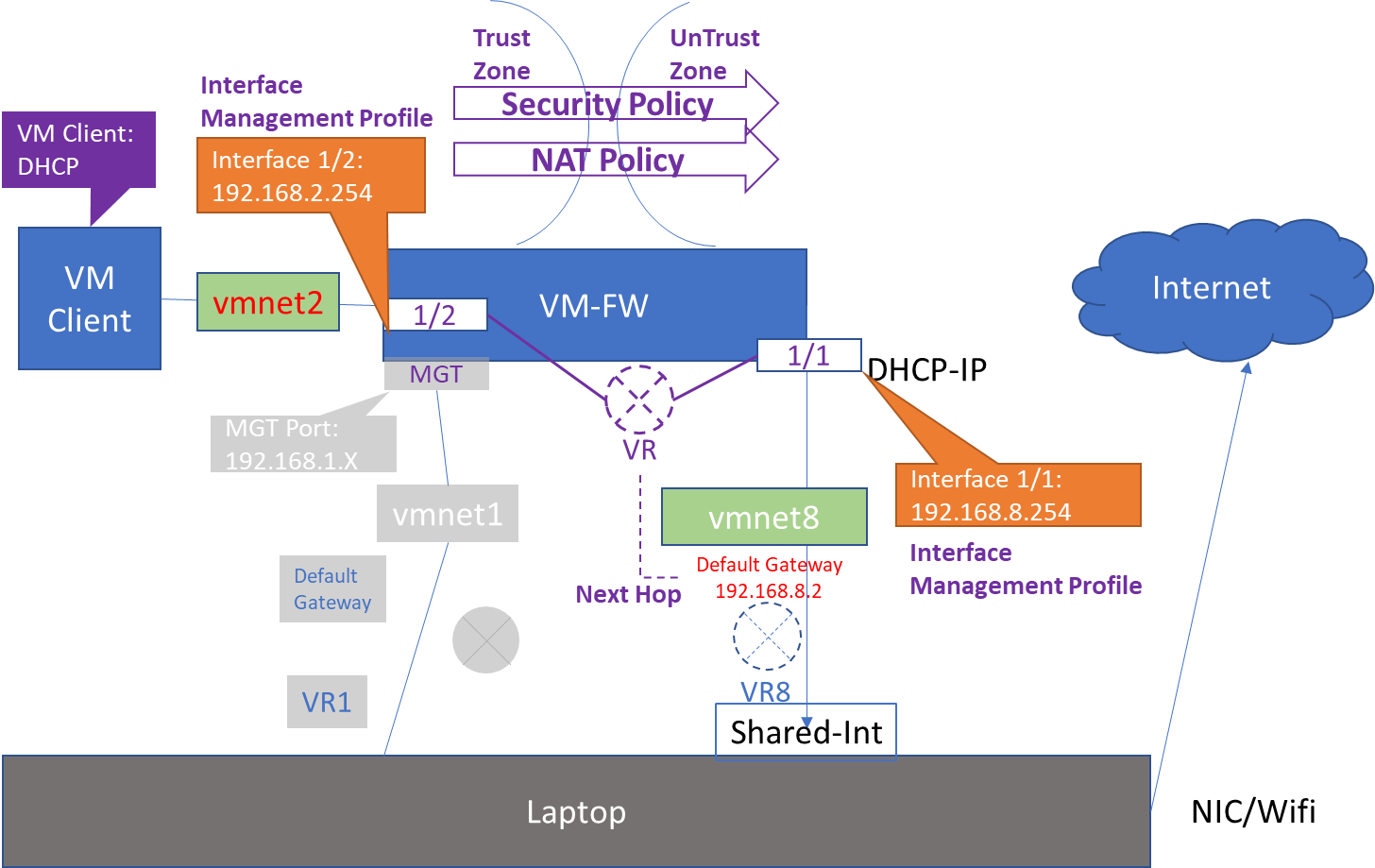
|  |  |
| --- | --- |
| Network Security Diploma in CSF  Year 3 (Apr 2021) Semester 5 | Week 3 |
| Practical |
| Firewall Layer 3 Configuration | |

**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. Layer 3 Configuration**

**Scenario:**



**Required Information**

|  |  |
| --- | --- |
| Interface Management Profile Names | allow\_all  allow\_ping |
| Internal-facing IP Address | Assigned by Ethernet1/2 |
| Internal-facing interface | Ethernet1/2 |
| External-facing IP Address | Ethernet1/1 Address |
| External-facing interface | Ethernet1/1 |
| DHCP Server: Gateway | Ethernet1/2 Address |
| DHCP Server: DNS Server | (Find out from Your VMnet8) |
| DHCP Server: IP address range | 192.168.Y.50 - 192.168.Y.60 |
| Virtual Router Name | Default |
| Virtual Router: Default route destination | 0.0.0.0/0 |
| Virtual Router: Next Hop IP | VMnet8 Default Gateway |

**Configuring Firewall to meet the Requirements in the Scenario**

**(a) Create Interface Management Profiles**

1. Click **Network > Network Profiles > Interface Mgmt.**
2. Click **Add** and create an interface management profile:

|  |  |
| --- | --- |
| Name | Enter allow\_all |
| Permitted Services | Select all check boxes |
| Permitted IP Addresses | Do not add any addresses |

Click **OK** to close the interface management profile creation window.

1. Click **Add** and create another interface management profile:

|  |  |
| --- | --- |
| Name | Enter allow\_ping |
| Permitted Services | Select only the **Ping** check box |
| Permitted IP Addresses | Do not add any addresses |

Click **OK** to close the interface management profile creation window.

1. Click the **Commit** link at the top-right of the GUI. Click **OK** again and wait until the commit process completes before continuing.

**(b) Configure Ethernet Interfaces with Layer 3 Information**

1. Click **Network > Interfaces > Ethernet**.
2. Click the interface name **ethernet1/2**. Configure the interface:

|  |  |
| --- | --- |
| Interface Type | Select **Layer3** |
| **Config** tab |  |
| Virtual Router | Keep the default setting (**none**) |
| Security Zone | Select **Trust-L3 (Create it if not exist)** |
| **IPv4** tab |  |
| Type | Keep the default setting (**Static**) |
| IP | Click **Add** then enter 192.168.Y.254/24 |
| **Advanced**  **> Other Info** tab |  |
| Management Profile | Select **allow\_all** |

Click **OK** to close the interface configuration window.

1. Click the interface name **ethernet1/1**. Configure the interface:

|  |  |
| --- | --- |
| Interface Type | Select **Layer3** |
| **Config** tab |  |
| Virtual Router | Keep the default setting (**none**) |
| Security Zone | Select **Untrust-L3 (Create it if not exist)** |
| **IPv4** tab |  |
| Type | Keep the default setting (**Static**) |
| IP | Click **Add** then enter 192.168.X.254/24 |
| **Advanced**  **> Other Info** tab |  |
| Management Profile | Select **allow\_ping** |

Click **OK** to close the interface configuration window.

1. Click the **Commit.**

**(c) Configure DHCP**

1. Click **Network > DHCP > DHCP Server**
2. Click **Add** to define a new DHCP Server:

|  |  |
| --- | --- |
| Interface Name | Select **ethernet1/2** |
| Gateway | Enter 192.168.Y.254 |
| Primary DNS | Enter 192.168.8.2 (Check your own VMnet8 DNS) |
| IP Pools | Click **Add** then enter 192.168.Y.50-192.168.Y.60 |

Click **OK** to close the DHCP Server configuration window.

**(d) Create a Virtual Router**

1. Click **Network > Virtual Routers**.
2. Open your default virtual router:

|  |  |
| --- | --- |
| **General** tab |  |
| **Static Route> IPv4** tab | Click **Add**  and create an entry with the following values: |
| Name | Enter default |
| Destination | Enter 0.0.0.0/0 |
| Next Hop | Select **IP Address** |
| Next Hop IP Address | Enter 192.168.8.2 (Check your own VMnet8 Default Gateway) |

Click **OK** to add the static route then click **OK** again to close the virtual router configuration window.

1. Click the **Commit**
2. Now you have created two layer 3 interfaces E1/1 and E1/2 with the above configurations, these are the minimum requirement for configuring a layer 3 interface.
3. Test from VM Client to ping E1/2 IP address, explain the result you obtained.

|  |
| --- |
|  |

1. Test from VM Client to ping E1/1 IP address, explain the result you obtained.

|  |
| --- |
|  |

**(e) Create a Security Policy**

1. Create a Security policy to allow flow of traffic from **Trust-L3** Security Zoneto **Untrust-L3** Security Zone.
   1. Click **Policies > Security**. Click **Add**.

|  |  |
| --- | --- |
| **General** tab |  |
| Name | **Trust-L3 to Untrust-L3** |
| **Source** tab |  |
| Source Zone | Click **Add** and select **Trust-L3** |
| Source Address | Keep default: check box is set to **Any** |
| **Destination** tab |  |
| Destination Zone | Click **Add** and select **Untrust-L3** |
| Destination Address | Keep default: check box is set to **Any** |
| **Action** tab |  |
| Action Setting | Keep default: radio button is set to **allow** |

* 1. Click **Commit**.

1. Now test from VM Client to ping E1/1 IP address, explain the result you obtained. Can you also find the log in the Monitor tab?

|  |
| --- |
|  |

1. Test whether VM Client can access internet.

|  |
| --- |
|  |

**(f) Create a Source NAT Policy**

1. Click **Policies > NAT**.
2. Click **Add** to define a new source NAT policy:

|  |  |
| --- | --- |
| **General** tab |  |
| Name | Enter Student Source NAT |
| **Original Packet** tab |  |
| Source Zone | Click **Add** and select **Trust-L3** |
| Destination Zone | Select **Untrust-L3** |
| Destination Interface | Select **ethernet1/1** |
| **Translated Packet > Source Address Translation** tab |  |
| Translation Type | Select **Dynamic IP and Port** |
| Address Type | Select **Interface Address** |
| Interface | Select **ethernet1/1** |
| Translated Address | Select the IP address of E1/1 from the dropdown list |

Click **OK** to close the NAT policy configuration window.

1. Click the **Commit** link at the top-right of the GUI. Click **OK** again and wait until the commit process completes before continuing.
2. Verify that now VM Client is able to access internet.