|  |  |
| --- | --- |
| Network Security Diploma in CSF  Year 3 (Apr 2021) Semester 5 | Week 2 |
| Practical |
| Firewall Interface 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.

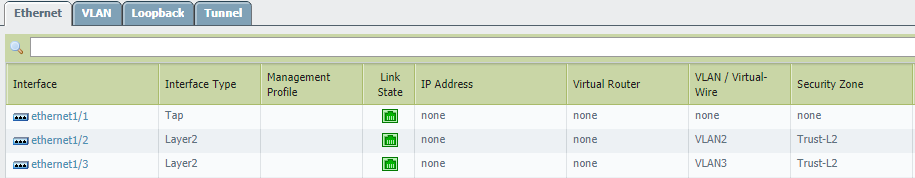
**Part A. Layer 2 Deployment (Inter-VLAN Routing)**

Make sure you have completed all the practical sections in Week 1. You can load your own config file to continue.

Required Information:

|  |  |
| --- | --- |
| Interfaces to use for Layer 2 interface | Ethernet1/2  Ethernet1/3 |
| Name for the Layer 2 zone | Trust-L2 |
| Name for the VLAN | VLAN2  VLAN3 |
| PC2 | IP: 2.2.2.2  Subnet Mask: 255.0.0.0  Default Gateway: 2.2.2.1 |
| PC3 | IP: 3.3.3.3  Subnet Mask: 255.0.0.0  Default Gateway: 3.3.3.1 |

1. Configure the interfaces of E1/2 and E1/3 as Layer 2 interfaces, assign them to the same Layer 2 zone named: Trust-L2, then assign E1/2 to VLAN2 and E1/3 to VLAN3.
2. Configure PC2 and PC3 IP addresses as indicated.
3. Ensure your Interface configurations are as similar to the below:



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

|  |
| --- |
|  |

[Now you have created two Layer 2 ports in the same security zone but different VLANs]

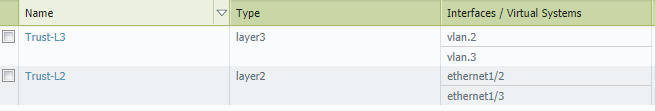
1. Test PC2 pings🡺PC3 and PC3 pings🡺PC2.
2. Explain the results you obtained.

|  |
| --- |
| The PCs are unable to ping each other because they are in two different VLANs  Although PC2 and PC3 are in the same security zone, they are in different VLANs with different network ID. With no routing, PC2 and PC3 cannot reach each other. |

1. Configuring the VLAN interfaces:
   1. Click **Network > Interfaces > VLAN**
   2. Click **Add**, create a new VLAN interface named **VLAN.2**.
   3. Click **Config > VLAN**, assign VLAN2 to this interface.
   4. Click **Config > Security Zone**, create a new security zone named **Trust-L3**.
   5. In **IPv4** tab, add static IP address **2.2.2.1/24**.
   6. Click **OK**.
   7. Click **Add** again, create a new VLAN interface named **VLAN.3**.
   8. Click **Config > VLAN**, assign VLAN3 to this interface.
   9. Click **Config > Security Zone**, choose **Trust-L3** that you just created.
   10. In **IPv4** tab, add static IP address **3.3.3.1/24**.
   11. Click **OK**.
2. Configure PC2 and PC3 with the following:

|  |  |
| --- | --- |
| PC2 | IP Address: 2.2.2.2  Subnet Mask: 255.0.0.0.0  Default Gateway: 2.2.2.1 |
| PC3 | IP Address: 3.3.3.3  Subnet Mask: 255.0.0.0.0  Default Gateway: 3.3.3.1 |

1. Verifying the Security Zones.
   1. Click **Network > Zones**.
   2. Make sure now you have both Trust-L2 zone and Trust-L3 zone similar to the below.



1. Reflection question: Are you able to put the two layer 2 interfaces E1/2 and E1/3 and the two VLAN interfaces VLAN.2 and VLAN.3 all into one security zone such as “Trust” zone?

|  |
| --- |
| No.  No. It is not possible.  Separate zones must be created for each type of interface (Layer 2 or Layer 3) E1/2 and E1/3 are layer 2 interfaces but VLAN 2 and VLAN 3 are layer 3 interfaces. So that only E1/2 and E1/3 can be assigned to any layer 2 zone while VLAN 2 and VLAN 3 can be assigned to any layer 3 zone. |

1. Discuss about what is a VLAN interface? Why do we need to create VLAN interfaces for each VLAN?

|  |
| --- |
| A VLAN Interface is a virtual interface that is attached to the physical network port or bond that your VLAN is configured on.  The VLAN Interface is used to automatically tag traffic that is routed through it with the appropriate VLAN ID.  To configure connectivity on the Firewall between the VLANs, a VLAN interface must be created. This is not a physical interface. It is a construct used to add a Layer 3-type interface to a Layer 2 VLAN.  VLAN interfaces operate at Layer 3, not Layer 2. As such, the VLAN interface will have a different zone than the physical Layer 2 interfaces.  A VLAN interface must be created and assigned to the same VLAN as the Layer 2 interfaces that require connectivity. |

1. Configuring a virtual router:
   1. Click **Network > Virtual Routers**.
   2. Click **Add** to add a new virtual router named **VR-VLAN**.
   3. In **General** tab, add Interfaces **VLAN.2** and **VLAN.3**.
   4. Click **OK**.
2. Test PC2 pings🡺PC3 and PC3 pings🡺PC2.
3. Explain the results you obtained.

|  |
| --- |
| The two PCs are able to ping each other as a virtual router has been added that facilitates the traffic between the two PCs in the two different VLANs. |

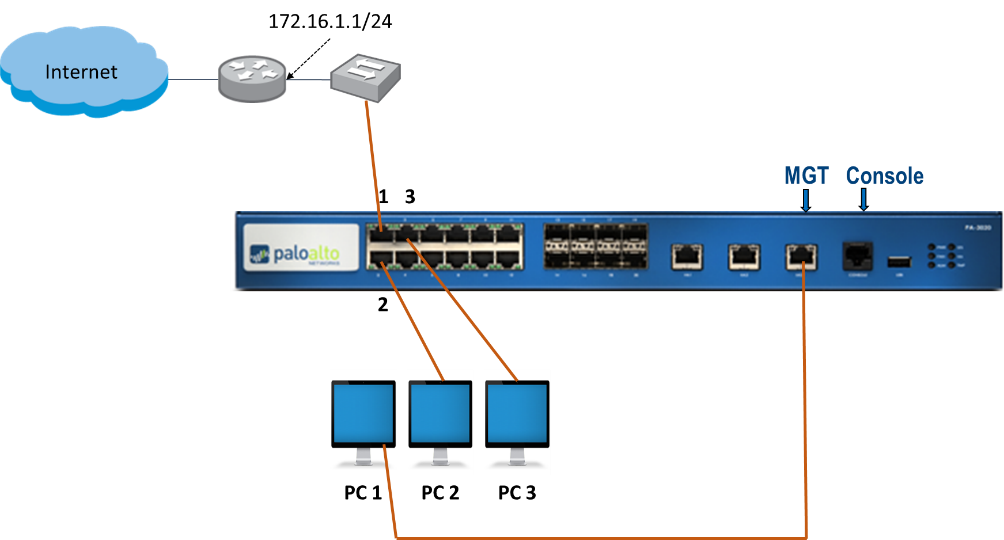
1. Draw a simple network diagram to illustrate the current network connections.

|  |
| --- |
|  |

**Part B. Virtual Wire Deployment**

Recap that the interface Ethernet1/1 of the firewall is connected to a router with the default gateway IP address of 172.16.1.1.

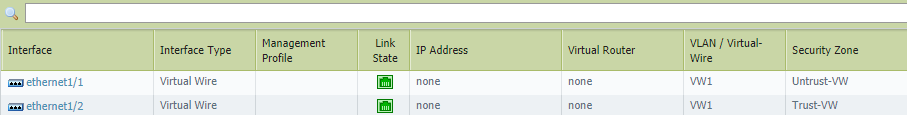
The below steps will create a virtual wire between E1/1 and E1/2.



1. Reflection: Under what situation would you deploy Virtual Wire configuration?

|  |
| --- |
| To transparently insert the firewall between 2 ports where no routing or switching is required. |

1. Configuring the Virtual Wire Interface :
   1. Click **Network > Interfaces > Ethernet**
   2. Click **Ethernet1/1,** select **Interface Type** as Virtual Wire.
   3. Click **Config > Virtual Wire**, add a new virtual wire named **VW1**.
   4. Click **Config > Security Zone,** add a new zone named **Untrust-VW.**
   5. Click **OK**.
   6. Click **Ethernet1/2,** change **Interface Type** to Virtual Wire.
   7. Click **Config > Virtual Wire**, select the virtual wire named **VW1**.
   8. Click **Config > Security Zone,** add a new zone named **Trust-VW**.
   9. Click **OK**.
2. Click **Network > Interfaces > Ethernet**. Make sure you have the similar configurations.



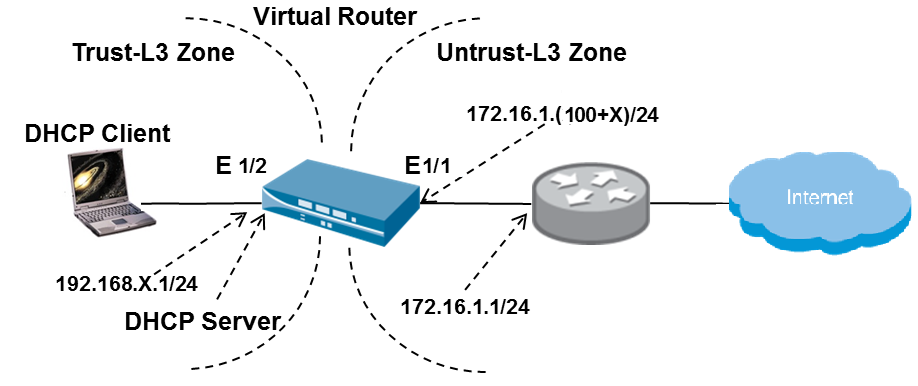
1. Discussion: What are the ways to test and ensure your virtual wire configuration is successful?

|  |
| --- |
| Virtual wire just binds two physical interfaces together since E1/1 is connected to the  router with internet access, E1/2 should have the same connectivity.  Configure PC2 to obtain IP address automatically and after a short while, PC2 should be able to obtain an IP address and can access internal (with a proper security policy  in place) |

1. Click **Network > Virtual Wires**, delete the virtual wire you created. This is to ensure the virtual wire will not conflict with the layer 3 configuration later.

**Part C: Layer 3 Configuration**

**Scenario:**



Reflection: Under what situation would you deploy Layer 3 configuration?

|  |
| --- |
| Layer 3 Mode: To deploy in a Layer 3 environment where routing and NAT are required. E.g. Use firewall to interconnect different networks. |

**Required Information**

|  |  |
| --- | --- |
| Interface Management Profile Names | allow\_all  allow\_ping |
| Internal-facing IP Address | 192.168.X.1/24 |
| Internal-facing interface | Ethernet1/2 |
| External-facing IP Address | 172.16.1.(100+X)/24 (X is your firewall number e.g. 172.16.1.115/24 for FW 15) |
| External-facing interface | Ethernet1/1 |
| DHCP Server: Gateway | 192.168.X.1 |
| DHCP Server: DNS Server | 153.20.62.122 |
| DHCP Server: IP address range | 192.168.X.50 - 192.168.X.60 |
| Virtual Router Name | Student-VR |
| Virtual Router: Default route destination | 0.0.0.0/0 |
| Virtual Router: Next Hop IP | 172.16.1.1 |

**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.X.1/24 |
| **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 172.16.1.(100+X)/24 |
| **Advanced**  **> Other Info** tab |  |
| Management Profile | Select **allow\_ping** |

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

1. Click **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.X.1 |
| Primary DNS | Enter 153.20.62.122 |
| IP Pools | Click **Add** then enter 192.168.X.50-192.168.X.60 |

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

**(d) Create a Virtual Router**

1. Click **Network > Virtual Routers**.
2. Click **Add** to define a new virtual router:

|  |  |
| --- | --- |
| **General** tab |  |
| Name | Enter Student-VR |
| Interfaces | Click **Add** then select **ethernet1/1**  Click **Add** again and select **ethernet1/2** |
| **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 172.16.1.1 |

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 PC2 to ping E1/1 IP address 172.16.1.(100+X), explain the result you obtained.

|  |
| --- |
| PC2 is not able to ping E1/1 yet although there is management profile and a  virtual router configured, inter-zone traffic is still denied by default. |

**(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 PC2 to ping E1/1 IP address 172.16.1.(100+X), explain the result you obtained. Can you also find the log in the Monitor tab?

|  |
| --- |
| The Ping is successful  There is one Security policy created to allow traffic from Trust-L3 Security Zone to Untrust-L3 Security Zone.  Traffic Log is also generated in the Monitor tab. |

1. Test whether PC2 can access internet.

|  |
| --- |
|  |

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

The details of the Network Address Translation will be learnt in Week 3.

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 **172.16.1.(100+X)/24** |

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 PC2 is able to access internet.

**Part D: Challenge**

Change another team member to configure the firewall, and follow the above similar settings to make PC3 be able to access internet. Show your results to your tutor.