**PROJECT: BUILDING A TYPICAL SECURITY ARCHITECTURE**

**Author: Sampath Ajit Chittella(2025)**

**OBJECTIVE:**

The purpose of this laboratory is to introduce students to different network security devices by having access to the network device and configuring the network devices IP addresses. Configuring the IP addresses of the network devices will expose students to some basic command lines and serve as a start to their introduction to different network security devices.

**NOTES:**

* Use the network topology in Fig 3 in page 3 to connect the devices, configure and assign IP addresses to interfaces of the network devices as provided along this guide.
* Use Fig. 1 options for the Palo Alto firewall image**:**

RAM (MB): **8192**

Console**: telnet**

Graphical user interface, text, application

Description automatically generated

**Fig.1**

* **Add public network to eve-ng (Fig. 2)**

1. Right-click on an empty part of the eve-ng window
2. Select network.
3. Change the **Name/Prefix** to **NAT**, select the **globe1.png** icon, and select **NAT** for the **type** as shown in the image below:

Graphical user interface

Description automatically generated

**Fig.2**

* **Add private network to eve-ng (Fig.2a)**

1. Follow steps i. and ii., just above.
2. Change the **Name/Prefix** to **Private**, select the **cloud.png** icon, and select **private** for the **type** as shown in the image below:

Graphical user interface

Description automatically generated  
**Fig.2a**

**TOPOLOGY**

Diagram

Description automatically generated **Fig. 3**

**TASK 1: EIU MAIN CAMPUS BASIC ROUTER CONFIGURATION**

***-On the* EIU Main Campus Gateway Router**

Router> ***enable***

Router# ***configure terminal***

Router(config)# ***hostname Campus-Gateway***

Campus-Gateway(config)# ***int g0/0***

Campus-Gateway(config-if)# ***ip address dhcp***

Campus-Gateway(config-if)# ***no shutdown***

Campus-Gateway(config)# ***exit***

Campus-Gateway(config)# ***int g0/1***

Campus-Gateway(config-if)# ***ip address 90.0.1.2 255.255.255.248***

Campus-Gateway(config-if)# ***no shutdown***

Campus-Gateway(config-if)# ***exit***

Campus-Gateway(config)# ***int g0/2***

Campus-Gateway(config-if)# ***ip address 192.168.10.100 255.255.255.0***

Campus-Gateway(config-if)# ***no shut***

Campus-Gateway(config-if)# ***exit***

Campus-Gateway(config)# ***exit***

Campus-Gateway# ***copy run start*** (Press Enter twice)

**INSTRUCTION: Use “show run” and “show ip interface brief” to re-check the parameters inputted in this task.**

**TASK 2: PALO ALTO INITIAL WEB ADMINISTRATION AND MANAGEMENT**

(**NOTE:** The following steps are applicable to **both Palo Alto Firewalls at both sites**)

1. **Set up a PC for the Configuration of the Two Palo Alto firewalls**

Select a Windows PC and connect it to the private network.

A picture containing diagram

Description automatically generated  
**Fig. 4**

1. **Set up the Palo Alto firewall**

Start the Palo Alto firewall and wait for a while for its booting process to complete

(**NOTE:** typical booting process of this Palo Alto image takes about **25 minutes**, you can keep connecting other parts of the network in the meantime).

**NOTE:** The Firewall logs in after several tries (even if we use the correct credentials), so if you’re not able to access, please wait a few minutes before you try again.

When the booting is completed, use **username/password** of **admin/admin** to access the CLI of the Palo Alto firewall, and use the following commands to assign its IP address:

admin@PA-VM> ***configure mode***

admin@PA-VM# ***set deviceconfig system type static***

admin@PA-VM# ***set deviceconfig system ip-address 192.168.1.x netmask 255.255.255.0***

admin@PA-VM# ***commit***

***(*NOTE: Use ip address in the range 192.168.1.1 to 192.168.1.254 for the Paloalto Firewalls, but do not use the same ip address for any two devices connected to the private network*)***

1. **Configure the Windows PC IP address**

You can assign any IP address ranging from **192.168.1.1 to 192.168.1.254/24**. Do not assign an IP address that is already in use by any of the Palo Alto Firewalls.

To verify the connection between the PC and the Palo Alto firewalls, open each Palo Alto firewall and ping the IP address as follows:

admin@PA-VM> ***ping host 192.168.1.x***

(**NOTE:** **Use *ctrl+c* to stop the reply packets**)

Click on the Click on Google Chrome **browser** icon and type [**https://192.168.1.x**](https://192.168.1.1) on the browser tab to open a Palo Alto configuration home page. (NOTE: Selectthe **Advanced…** then **Accept the Risk and Continue)**

Use **username/password** of **admin/Tech@lab** to login to the Palo Alto GUI.

Graphical user interface, application

Description automatically generated

**Fig.5**

Open a new tab on the browser and type **‘https://192.168.1.x’**, the ip address of the second Paloalto Firewall to access its home page**.**

1. **Create a role for an assistant administrator** which will allow access to all firewall functionality through the WEBUI except Monitor, Network, Privacy, and Device. Create an account using this role.

* Click **Device** → **Admin Roles**. (in the left pane)
* Click **Add** in the lower left of the panel and create a new admin role:
* Type **Policy Admins** in the **name** window

|  |  |
| --- | --- |
| **Web UI tab categories** | Click the following major categories to disable them:   * **Monitor** * **Network** * **Device** * **Privacy**   The remaining major categories should remain enabled. |

* Click **OK** to continue.

**TASK 3: CREATE A GENERAL ACCOUNT**

1. Click **Device** → **Administrators.**
2. Click **Add** in the lower left corner of the panel. Configure a new administrator account:

|  |  |
| --- | --- |
| **Name field** | Type **ip-admin** |
| **Password/Confirm** | Type  **paloalto** |
| **Administrator type** | Select **Role Based** |
| **Profile** | Select **Policy Admins** (scroll down menu) |
| **SSH & pass profile** | Leave it unchecked |

1. Click **OK**
2. To save your configuration, click the **Commit** link at the top‐right of the WEBUI. (Close to **Device** tab)
3. Click **OK** to the commit pop- up window and wait until the commit process completes, then click **Close**.

***IMPORTANT NOTE: Every time you make a change in a PALO ALTO firewall, if you do not “Commit” the change will not take effect. Please beware of this fact throughout this guide, even if it is not mentioned in every change***.

The web page will appear as shown below (Fig. 6):

Graphical user interface, text, application, email

Description automatically generated  
**Fig. 6**

**TASK 4: CONFIGURE THE MAIN CAMPUS PALO ALTO INTERFACES**

1. Click on **Network** tab.
2. From the left-hand pane, configure the **management interface.**

* Click on **Interface Mgmt.**
* Click on **Add** button (At the bottom left of the dialogue box).
* Name: **Ping-Only**
* Check **Ping** box.
* Click **OK.**

1. Click on **Interfaces** at the left-hand pane. Click on **Ethernet1/1** to configure it.

* Change **Interface Type** to **Layer3** using the drop-down menu.
* Click on **IPV4** tab, click on **Add** on the opened window (ensure the **Static** type category is selected).
* Enter the IP address **90.0.1.1/29.** Click any open space.
* Click **Advanced** tab, select “**ping-only”** for management profile, then click **OK**, **OK.**

1. Configure **Ethernet1/2** with IP address **10.144.1.2/29** following the steps for Ethernet1/1 above.
2. Configure **Ethernet1/3** with IP address **172.16.1.1/24** following the steps for Ethernet1/1 above.
3. Click on **Zones,** click **Add**, use the following parameters:

* Name: **Trust**
* Type: **Layer3**
* Interface: Click **Add,** select **ethernet1/2**
* Click **OK**

1. Add the **Untrust** Zone with the following details:

* Name: **Untrust**
* Type: **Layer3**
* Interface: Click **Add**, select **ethernet1/1**
* Click **OK**

1. Add the **DMZ** Zone with the following details:

* Name: **DMZ**
* Type: **Layer3**
* Interface: Click **Add,** select **ethernet1/3**
* Click **OK**

1. Click on The **NETWORK** tab, then on **Virtual Routers**

* Click on **default**.
* Click **Add**, and then add the three Palo Alto interfaces **Ethernet1/1, Ethernet1 /2** and **Ethernet 1/3** and click **OK** when done.

**INSTRUCTION: \*\* Please commit your configurations before proceeding.**

You should see figures 7,8, and 9 below at this point, if you don’t, please call the attention of your instructor.

Graphical user interface, application

Description automatically generated  
**Fig. 7**

Graphical user interface, table

Description automatically generatedGraphical user interface, application

Description automatically generated

**Fig. 8**

Table

Description automatically generated**Fig. 9**

**FIGURE 3 REPRODUCED FOR YOUR CONVENIENCE**

Diagram

Description automatically generated

**TASK 5:**

**CONFIGURE THE CISCO ASA**

Ciscoasa>

Ciscoasa> ***enable*** (Press Enter twice)

Ciscoasa# ***configure terminal***

Ciscoasa(config)# ***hostname ASA-FW-IPS***

ASA-FW-IPS(config)#

ASA-FW-IPS(config)# ***int gig0/1***

ASA-FW-IPS(config-if)# ***nameif Outside***

ASA-FW-IPS(config-if)# ***ip address 10.144.1.1 255.255.255.248***

ASA-FW-IPS(config-if)# ***no shutdown***

ASA-FW-IPS(config-if)# ***exit***

ASA-FW-IPS(config)# ***int gig0/3***

ASA-FW-IPS(config-if)# ***nameif Inside***

ASA-FW-IPS(config-if)# ***ip address 172.16.32.2 255.255.255.248***

ASA-FW-IPS(config-if)# ***no shutdown***

ASA-FW-IPS(config-if)# ***exit***

**INSTRUCTION: Use “show run” to re-check the parameters inputted in this task.**

**TASK 6: CONFIGURE THE INTERNAL ROUTER**

Internal-Router> ***enable***

Internal-Router# ***conf t***

Internal-Router(config)# ***int g0/0***

Internal-Router(config-if)# ***ip address 172.16.32.1 255.255.255.248***

Internal-Router(config-if)# ***no shutdown***

Internal-Router(config-if)# ***exit***

Internal-Router(config)# ***int g0/1***

Internal-Router(config-if)# ***ip address 10.234.100.1 255.255.255.0***

Internal-Router(config-if)# ***no shutdown***

Internal-Router(config-if)# ***end***

Internal-Route# ***copy run start*** (Press **Enter** twice)

**INSTRUCTION: Use “show run” and “show ip interface brief” to re-check the parameters inputted in this task.**

**TEST:**

At this point, Check some basic connectivity between the devices with ping command:

1. Log on to **Internal-Router**, ping 172.16.32.2 (ASA G0/3 interface)
2. Log on to **ASA-FW-IPS**, ping 172.16.32.1 (Internal-Router G0/0 interface)
3. Log on to **ASA-FW-IPS**, ping 10.144.1.1 (Palo Alto eth1/2 interface)

* All these pings should be successful, otherwise call the attention of your Instructor/GA
* Check that the E1/2 Palo Alto port is now green (Provided the Palo Alto firewall at EIU main campus is configured already)

**TASK 7: CONFIGURE THE CHAMPAGNE REMOTE SITE** Champagne\_GatewayRouter> **e*nable***

Champagne\_GatewayRouter# ***conf t***

Champagne\_GatewayRouter(config)# ***int g0/0***

Champagne\_GatewayRouter(config-if)# ***ip address dhcp*** Champagne\_GatewayRouter(config-if)# ***no shutdown*** Champagne\_GatewayRouter(config-if)# ***exit***

Champagne\_GatewayRouter(config)# ***int g0/1***

Champagne\_GatewayRouter(config-if)# ***ip address 80.0.1.2 255.255.255.248***

Champagne\_GatewayRouter(config-if)# ***no shutdown*** Champagne\_GatewayRouter(config-if)# ***exit***

Champagne\_GatewayRouter(config)# ***int g0/2***

Champagne\_GatewayRouter(config-if)# ***ip address 192.168.10.101 255.255.255.0***

Champagne\_GatewayRouter(config-if)# ***no shutdown***

Champagne\_GatewayRouter(config-if)# ***exit***

Champagne\_GatewayRouter(config)# ***exit***

Champagne\_GatewayRouter#

**INSTRUCTION: Use “show run” and “show ip interface brief” to re-check the parameters inputted in this task.**

**TASK 8: CONFIGURE CHAMPAGNE REMOTE SITE PALO ALTO FIREWALL**

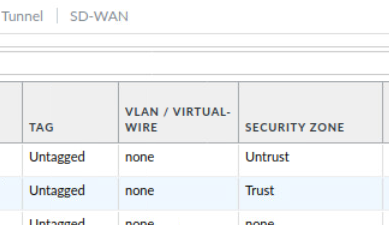
Follow the same procedures above for EIU Main Campus Palo Alto to configure champagne Palo alto using the details on the topology. Note the IP address and the zones of each of the interface to configure below:

* Ethernet1/1 ➔ 80.0.1.1/29
* Ethernet1/2 ➔ 10.234.200.1/24
* Zones: Untrust ➔ ethernet1/1
* Zones: Trust ➔ ethernet1/2
* Interface Mgmt: **Ping-Only,** check **Ping** box.
* Default virtual routers: add e1/1 and e1/2.

**INSTRUCTION: \*\* Please commit your configurations before proceeding**.

Check if your Champagne Palo Alto looks like the following figures:

Table

Description automatically generated  
**Fig. 10**

Table

Description automatically generated

**Fig. 11**

**TEST:**

At this point, check some basic connectivity between the devices with **ping** command:

* Log on to Champagne\_GatewayRouter and ping 80.0.1.1 (Palo Alto eth1/1 interface)

This ping should be successful, otherwise call the attention of your Instructor/GA

**TASK 9: CONFIGURE DHCP SERVERS ON BOTH SITES**

**For EIU Main Campus Site:**

1. Log on to **Internal Router** and configure DHCP Server as follows: Internal\_Router(config)# ***ip dhcp excluded-address 10.234.100.1*** Internal\_Router(config)# ***ip dhcp pool CAMPUSPOOL***

Internal\_Router(dhcp-config)# ***network 10.234.100.0 /24***

Internal\_Router(dhcp-config)# ***dns-server 8.8.8.8 4.2.2.2***

Internal\_Router(dhcp-config)# ***default-router 10.234.100.1***

**INSTRUCTION: Use “show run” and “show ip interface brief” to re-check the parameters inputted in this task.**

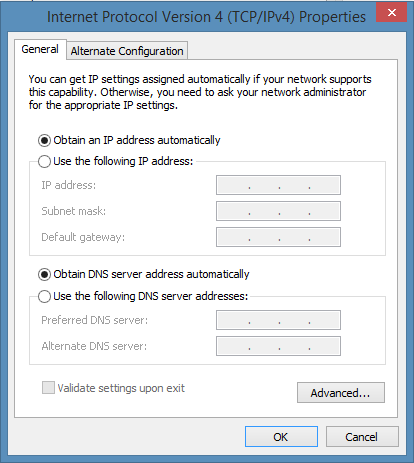
1. Connect the LAN Hosts as shown on the topology. Set the IP configuration to dynamic:

* For the **Virtual PC (VPCS),** type “**ip dhcp**” command

Type “**show ip”** command to check the IP address obtained from the dhcp server.

* For the Windows PC, take the following steps:

**Start Menu>Control Panel>**[**Network**](https://askleo.com/glossary/network/) **and Sharing center>Change adapter settings>** click on the LAN that shows up **>>> >>>Properties > Internet** [**Protocol**](https://askleo.com/glossary/protocol/) **(TCP/IPv4) > Properties**



**Fig. 12**

Click on “**Obtain an IP address automatically**” and **“Obtain DNS server address automatically”** to dynamically assign IP address to the PC, then Click **OK** once you are done.

Open the command prompt and type the command “i**pconfig /all”** to check the IP address.

Inform the GA if the hosts did not receive IP address.

1. From the Hosts, ping the default gateway IP address. This must be successful, otherwise report to the GA.

**For the Champagne Remote Site:**

Log on to the **Palo Alto firewall.**

1. Click on **Network** tab.
2. On the left-hand pane, click on **DHCP**.
3. On the DHCP Server window, click **Add,** on the Interface option, click on the drop-down menu, select **ethernet1/2.**
4. Click on the **Timeout** radio button and leave it to 1 day.
5. Under the **options** tab:
   * For **Gateway,** enter **10.234.200.1**
   * For **Primary DNS,** enter **8.8.8.8**
   * For **Secondary DNS**, enter **4.2.2.2**
6. Under the Lease tab, for **IP Pool section**, click **Add** and enter **10.234.200.2- 10.234.200.100**

**INSTRUCTION: \*\* Please commit your configurations before proceeding**.

**TESTING CONNECTIVITIES**

From all the LAN Hosts, ping the default gateways – this should be successful. IMPORTANT: DISABLE ALL OTHER INTERFACES (Except the one used), and the Windows firewall defender of the Windows PCs. Set the PCs to obtain IP address and DNS configurations automatically. But note that the LAN Hosts have no internet connection as they cannot go online. Test if the PCs can go online from both sites.

**TASK 10: VPN CONFIGURATION on MAIN CAMPUS ROUTER**

The aim of this task is to connect the two sites over the public network. As of now, both sites cannot communicate LAN-TO-LAN. This is expected because the two sites are still isolated.

**Configure the VPN on the Campus Gateway Router**

**Create tunnel interface.**

Campus-Gateway(config)# ***interface tunnel 12***

Campus-Gateway(config-if)# ***ip add 10.0.0.1 255.255.255.0***

Campus-Gateway(config-if)# ***tunnel source g0/2***

Campus-Gateway(config-if)# ***tunnel destination 192.168.10.101***

**VPN Phase I**

Campus-Gateway(config)# ***crypto isakmp policy 10***

Campus-Gateway(config-isakmp)# ***auth pre-share***

Campus-Gateway(config-isakmp)# ***encryption aes***

Campus-Gateway(config-isakmp)# ***hash sha***

Campus-Gateway(config-isakmp)# ***group 5***

Campus\_Gateway(config-isakmp)# ***exit***

Campus-Gateway(config)# ***crypto isakmp key CapstonE#1! address 192.168.10.101***

**INSTRUCTION: Use “show run” to re-check the parameters inputted in this task.**

**VPN Phase II**

Campus-Gateway(config)# ***crypto ipsec transform-set EIUVPN esp-aes esp-sha-hmac***

Campus-Gateway(cfg-crypto-trans)# **exit**

**Create the ipsec profile to link Phase II**

Campus-Gateway(config)# ***crypto ipsec profile VPNPROFILE***

Campus-Gateway(ipsec-profile)# ***set transform-set EIUVPN***

Campus-Gateway(ipsec-profile)# ***exit***

**Apply the profile to the appropriate interface.**

Campus-Gateway(config)# ***int tunnel 12***

Campus-Gateway(config-if)# ***tunnel mode ipsec ipv4***

Campus-Gateway(config-if)# ***tunnel protection ipsec profile VPNPROFILE***

Campus-Gateway(config-if)# ***exit***

**INSTRUCTION: Use “show run” to re-check the parameters inputted in this task.**

**TASK 11: RUN OSPF ON THE MAIN CAMPUS ROUTER**

Campus-Gateway(config)# ***router ospf 1***

Campus-Gateway(config-router)# ***network 10.0.0.0 0.0.0.255 area 0***

Campus-Gateway(config-router)# ***network 192.168.10.0 0.0.0.255 area 0***

Campus-Gateway(config-router)# ***network 90.0.1.0 0.0.0.7 area 0.0.0.1***

Campus-Gateway(config-router)# ***default-information originate***

Campus-Gateway(config-router)# ***exit***

**INSTRUCTION: Use “show run” to re-check the parameters inputted in this task.**

**TASK 12: VPN CONFIGURATION ON THE CHAMPAGNE REMOTE SITE ROUTER**

**Create tunnel interface**

Champagne\_GatewayRouter(config)# ***interface tunnel 21***

Champagne\_GatewayRouter(config-if)# ***ip add 10.0.0.2 255.255.255.0*** Champagne\_GatewayRouter(config-if)# ***tunnel source g0/2***

Champagne\_GatewayRouter(config-if)# ***tunnel destination 192.168.10.100***

**VPN Phase I**

Champagne\_GatewayRouter(config)# ***crypto isakmp policy 10*** Champagne\_GatewayRouter(config-isakmp)# ***auth pre-share*** Champagne\_GatewayRouter(config-isakmp)# ***encryption aes*** Champagne\_GatewayRouter(config-isakmp)# ***hash sha***

Champagne\_GatewayRouter(config-isakmp)# ***group 5***

Champagne\_GatewayRouter(config-isakmp)# ***exit***

Champagne\_GatewayRouter(config)# ***crypto isakmp key CapstonE#1! address 192.168.10.100***

**VPN Phase II**

Champagne\_GatewayRouter(config)# ***crypto ipsec transform-set EIUVPN esp-aes esp-sha-hmac***

Champagne\_GatewayRouter(cfg-crypto-trans)# ***exit***

**Create the ipsec profile to link Phase II**

Champagne\_GatewayRouter(config)# ***crypto ipsec profile VPNPROFILE*** Champagne\_GatewayRouter(ipsec-profile)# ***set transform-set EIUVPN*** Champagne\_GatewayRouter(ipsec-profile)# ***exit***

**Apply the profile to the appropriate interface.**

Champagne\_GatewayRouter(config)# ***int tunnel 21***

Champagne\_GatewayRouter(config-if)# ***tunnel mode ipsec ipv4***

Champagne\_GatewayRouter(config-if)# ***tunnel protection ipsec profile VPNPROFILE***

Champagne\_GatewayRouter(config-if)# ***exit***

**Run OSPF on the Router**

Champagne\_GatewayRouter(config)# ***router ospf 1***

Champagne\_GatewayRouter(config-router)# ***network 10.0.0.0 0.0.0.255 area 0***

Champagne\_GatewayRouter(config-router)# ***network 192.168.10.0 0.0.0.255 area 0***

Champagne\_GatewayRouter(config-router)# ***network 80.0.1.0 0.0.0.7 area 0.0.0.2***

Champagne\_GatewayRouter(config-router)# ***default-information originate*** Champagne\_GatewayRouter(config-router)# ***exit***

**INSTRUCTION: Use “show run” to re-check the parameters inputted in this task.**

**TEST**

Ping the tunnel interface on both routers, this should be successful, otherwise call the attention of your GA. On both Routers, issue the following show commands: (From privileged mode), type:

**show crypto isakmp sa**

**show crypto ipsec sa**

Now, we will configure Routing Configurations on the other Devices for a complete LAN-TO-LAN connectivity.

**TASK 13: CONFIGURE OSPF ON CISCO ASA**

ASA-FW-IPS(config)# ***router ospf 1***

ASA-FW-IPS(config-router)# ***network 172.16.32.0 255.255.255.248 area 0.0.0.1***

ASA-FW-IPS(config-router)# ***network 10.144.1.0 255.255.255.0 area 0.0.0.1***

ASA-FW-IPS(config-router)# ***exit***

**NOTE:**

By default, the echo-reply ICMP is not allowed from a lower security to a higher security interface.

**Enabling ICMP inspection in the policy-map global\_policy:**

1. Firstly, check if class-map called **“inspection-default”** is preconfigured on the firewall:

ASA-FW-IPS(config)# ***sh run class-map***

If yes, proceed to step 3 below, otherwise proceed to step 2 to create it.

1. **Create access-list and link it to the class map.**

ASA-FW-IPS(config)# ***access-list 150 permit icmp any any***

ASA-FW-IPS(config)# ***class-map inspection\_default***

ASA-FW-IPS(config-cmap)# ***match access-list 150***

ASA-FW-IPS(config-cmap)# ***exit***

1. **Create a policy map for icmp inspection**

ASA-FW-IPS(config)# ***policy-map global\_policy***

ASA-FW-IPS(config-pmap)# ***class inspection\_default***

ASA-FW-IPS(config-pmap-c)# ***inspect icmp***

ASA-FW-IPS(config-pmap-c)# ***exit***

**TASK 14:CONFIGURE THE INTERNAL ROUTER**

**Configure OSPF on the router**

Internal\_Router(config)# ***router ospf 1***

Internal\_Router(config-router)# ***network 10.234.100.0 0.0.0.255 area 0.0.0.1***

Internal\_Router(config-router)# ***network 172.16.32.0 0.0.0.7 area 0.0.0.1*** Internal\_Router(config-router)# ***router-id 172.16.32.1***

Internal\_Router(config-router)# ***exit***

Internal\_Router(config)# ***exit***

**TASK 15: CONFIGURE PALO ALTO FIREWALLS ON BOTH SITES**

**(A).** For EIU Main Campus Site Palo Alto

Log on to the Palo Alto firewall and follow below steps:

1. Click on **Network** tab.
2. Click **Virtual Routers** on the left-hand pane.
3. Click on **default** router configuration.
4. On the Interfaces section displayed on the **Virtual Router** window, click **Add.**
5. Check: Select all three ethernet interfaces i.e. **ethernet1/1, ethernet1/2 and ethernet1/3** (**click on each square at the left of each one**).
6. Then click on **OSPF.**
7. On the OSPF Routing section, tick **Enable** and uncheck **Reject Default Route.**
8. Enter **90.0.1.1** as **Router ID**
9. Click **Add** under **Areas** tab.
10. For **Area ID** type **0.0.0.1**
11. Click the **Interface** tab, then click **ADD;** then using the drop-down menu, select the interfaces **ethernet1/1, ethernet1/2,** and **ethernet1/3** one after the other. Click OK each time to add the interfaces to the dynamic routing. Click OK when done.
12. Click on **Policies** tab.
13. Click on **Security** at the left-hand pane, and click **Add.**
14. Under **General** tab, type **ACCESS-POLICY** as **Name.**
15. Under **Source** tab, click **Add** under **Source Zone,** select **Trust.**
16. Under **Destination** tab, click Add under **Destination Zone,** select **Untrust.**
17. Ensure **Action setting** under **Actions** tab is set to **Allow.**
18. Click **OK**.

**INSTRUCTION: \*\* Please commit your configurations before proceeding**.

**(B).** For the Champagne Remote Site Palo Alto

Log on to the Palo Alto firewall and follow below steps:

1. Click on **Network** tab.
2. Click **Virtual Routers** on the left-hand pane.
3. Click on **default** router configuration.
4. CHECK: On the **Interfaces** section displayed on the **Virtual Router** window, click **Add.**
5. Select the ethernet interfaces one after the other i.e. **ethernet1/1, ethernet1/2**
6. Then click on **OSPF.**
7. On the OSPF Routing section, tick **Enable** and uncheck **Reject Default Route.**
8. Enter **80.0.1.1** as **Router ID.**
9. Click **Add** under **Areas** tab.
10. For **Area ID** type **0.0.0.2**
11. Click the **Interface** tab, then click **ADD;** then using the drop-down menu, select the interfaces **ethernet1/1,** and **ethernet1/2** one after the other. Click **OK** each time to add the interfaces to the dynamic routing. Click **OK** when done.
12. Click on **Policies** tab.
13. Click on **Security** at the left-hand pane, and click **Add.**
14. Under **General** tab, enter **ACCESS-POLICY** as **Name.**
15. Under **Source** tab, click **Add** under **Source Zone**, select **Trust.**
16. Under **Destination** tab, click **Add** under **Destination Zone,** select **Untrust**.
17. Ensure **Action setting** under **Action** tab is set to **Allow.**
18. Click **OK.**

**INSTRUCTION: \*\* Please commit your configurations before proceeding**.

**TEST**

On the Internal Router, EIU Main Router and Champagne Router, From the privileged mode, issue the commands below:

**Show ip route ospf** – Can you see any OSPF routes in the routing table?

**TASK 16: NAT AND ACCESSING THE INTERNET**

The purpose of this task is to configure Network Address Translation (NAT) necessary for internet accessibility. NAT can allow multiple private IP addresses to access the internet with a single shared public IP address. We will also be introduced to static NAT, by statically NATing the private IP address of the web server to our public IP address to enable online access to the webserver from the internet.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Before you configure NAT, test if you can access the webserver:

From the two sites, open the web-browser of any of the host and type: <http://172.16.1.2>

This should not be successful, I bet you know why!!

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Solution Guide**

1. On the **EIU Main Campus Gateway Router**, Create Access-list for the permitted traffic.

Campus-Gateway> ***enable***

Campus-Gateway# ***conf t***

Campus-Gateway(config)# ***access-list 105 permit ip any any***

The access-list is permitting all traffic from the internal network to any network on the internet.

1. Configure a default route to the ISP

Campus-Gateway(config)# ***ip route 0.0.0.0 0.0.0.0 172.29.129.254***

1. Configure NAT

Campus-Gateway(config-if)# ***int g0/0***

Campus-Gateway(config-if)# ***ip nat outside***

Campus-Gateway(config-if)# ***exit***

Campus-Gateway(config)# ***int g0/1***

Campus-Gateway(config-if)# ***ip nat inside***

Campus-Gateway(config-if)# ***exit***

Campus-Gateway(config)# ***ip nat inside source list 105 interface g0/0 overload***

**INSTRUCTION: Use “show run” to re-check the parameters inputted in this task.**

**NAT Overloading** or **Port Address Translation (PAT)** is a modified form of dynamic **NAT** where the number of inside local addresses is greater than the number of inside global addresses. Mostly, there is just a single inside global IP address providing Internet access to all inside hosts.

Configure Static NAT for internet users to be able to access the web server using EIU Main Gateway router public facing interface IP address.

1. On the Champagne Remote site Router.Create Access-list for the permitted traffic.

Champagne\_GatewayRouter> ***enable***

Champagne\_GatewayRouter# ***conf t***

Champagne\_GatewayRouter(config)# ***access-list 105 permit ip any any***

**NOTE:** The access-list is permitting all traffic from the internal network to any network on the internet.

1. Configure a default route to the ISP.

Champagne\_GatewayRouter(config)# ***ip route 0.0.0.0 0.0.0.0 172.29.129.254***

1. Configure NAT

Champagne\_GatewayRouter(config-if)# ***int g0/0***

Champagne\_GatewayRouter(config-if)# ***ip nat outside*** Champagne\_GatewayRouter(config-if)# ***exit***

Champagne\_GatewayRouter (config)# ***int g0/1***

Champagne\_GatewayRouter(config-if)# ***ip nat inside*** Champagne\_GatewayRouter(config-if)# ***exit***

Champagne\_GatewayRouter (config)# ***ip nat inside source list 105 interface g0/0 overload***

**INSTRUCTION: Use “show run” to re-check the parameters inputted in this task.**

**TEST**

Test to see that ALL LAN Hosts can browse to internet now. If Unsuccessful, call the attention of your GA.

**At this stage, no one can connect to the web server. To make this happen, follow below guides on Main Campus Router and Palo alto.**

**Diagram

Description automatically generated**

**Fig. 13**

1. **For the EIU Main Campus:**

First, check what is the IP address assigned through DHCP to the Campus-Gateway G0/0 interface.

Campus-Gateway# ***show ip interface brief***

The IP address should be in the 172.29.129.0/24 network (Provided by DHCP through the Internet).

After verifying, type the following command:

Campus-Gateway(config)# ***ip nat inside source static tcp 90.0.1.1 80 172.29.129.x 80 extendable***

**INSTRUCTION: Replace the x in “172.29.129.x” for the corresponding number assigned through DHCP by the internet.**

Here the router is configured to NAT to the Palo Alto Outside interface (90.0.1.1) which is then configured to do static NATing to the web server which is 172.16.1.2.

Configure the static NAT on Palo Alto to the web server (Only on the EIU Main Campus Network).

Graphical user interface

Description automatically generated

Graphical user interface, table

Description automatically generated with medium confidence

**Fig. 14**

1. On the **Palo Alto at Main Campus**, follow the steps below to configure NAT.
2. Click the **Policies** tab, Choose **NAT** On the left pane.
3. Click **Add,** under **General** tab, type **WEBSERVER-NAT.**
4. **NAT Type** should be set to **IPV4.**
5. Click **Original Packet** tab.
6. Under **Source Zone,** click Add, then select **DMZ.**
7. Under **Destination Zone,** use the drop-down menu to select **Untrust,** for **Destination Interface** select **ethernet1/1,** for Service, select **service-http.**
8. Under **Source Address,** click **Add,** click **Address** (in blue), on the new dialogue box, enter **WebServer.** Type **172.16.1.2/32** in space provided in front of **IP Netmask** and click **OK.**
9. Click on **Translated Packet,** under **Source Address Translation,** select **Static IP** as **Translation Type.**
10. Type **90.0.1.1/32** as **Translated Address.**
11. Click on **Yes** for **Bi-directional.**
12. Click **OK.**
13. Configure the **Security Policy** to allow both external and Internal access to the web server
14. Under the **Policies** tab.
15. Click on **Security** on the left-hand pane.
16. Click **Add.**
17. Under **General** tab, type **DMZ-Policy** as Name
18. Click **Source** tab and click **Add.**
19. Under **Source Zone**, click **Add,** and select both **Trust** and **Untrust Zones.**
20. Click on **Destination** tab, under **Destination Zone,** click **Add,** select **DMZ.**
21. Click **Service/URL Category**, under **Service** **click Add** and select **service-http.**
22. Under **Actions** tab, ensure **Allow** is selected.
23. Click **OK.**
24. Click **Commit** at the top right corner of the Palo Alto and follow the prompts..

Graphical user interface, application

Description automatically generatedTable

Description automatically generated

**Fig. 15**

(If you do not see exactly what is depicted in figure 15, please call the attention of your instructor)

**TASK 17: ACCESSING THE WEBSERVER**

**Access the Web Server:**

1. Press Ctrl + Alt + Shift on the keyboard.
2. Change the Input Method to On-Screen Keyboard.

Graphical user interface, application

Description automatically generated

1. Using the On-Screen Keyboard, press Ctrl + Alt + Del.
2. Press Ctrl + Alt + Shift again to change the Input Method back to none.
3. When prompted for the password, type **Test123** to access.

**Setup the Web Server**

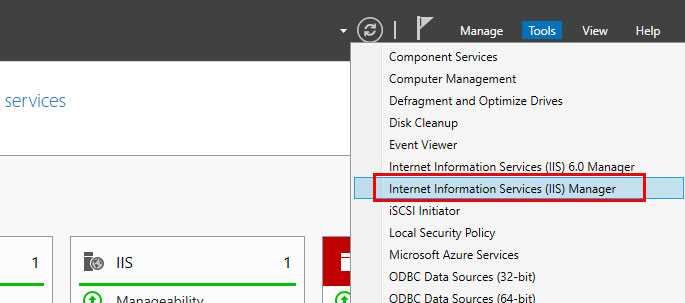
**INSTRUCTION:** Configure the IP address of the web server as 172.16.1.2/24. Configure the default gateway as 172.16.1.1 (Palo Alto eth1/3 interface).

Enable IIS and the required IIS components:

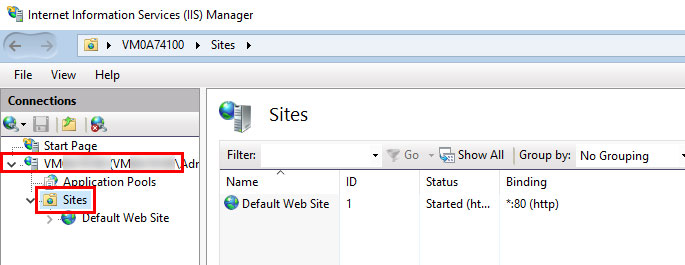
1. Open **Server Manager** and click **Manage** > **Add Roles and Features**. Click **Next.**
2. Select **Role-based or feature-based installation** and click **Next.**
3. Select the appropriate server. The **local server** is selected by default. **Click Next.**
4. Enable **Web Server (IIS)** and click **Next.**
5. **No additional features are necessary** to install the Web Adaptor, so click Next.
6. On the **Web Server Role (IIS) dialog box**, click **Next.**
7. On the Select role services dialog box, leave everything as default and click Next.
8. Verify that your settings are correct and click Install.
9. When the installation completes, click **Close** to exit the wizard.

**Add a website:**

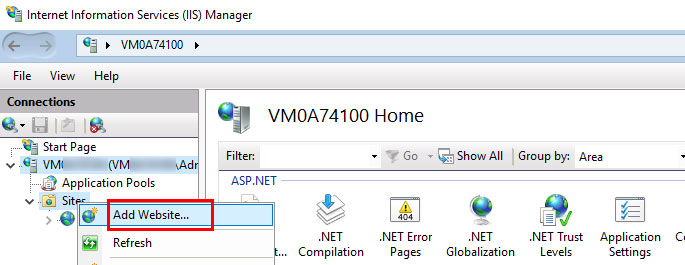
1. Create a folder named **“Web”** on **Local Disk (C:)**
2. On the **Server Manager Dashboard**, click **Tools** > **Internet Information Services (IIS) Manager.**



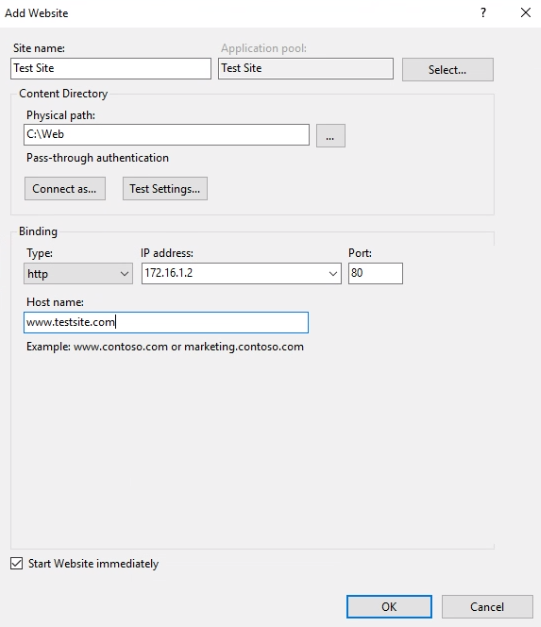
1. In the **Connections pane,** click to expand the server entry, then right-click **Sites.**



1. Click **Add Website...**



1. Fill out the following information:

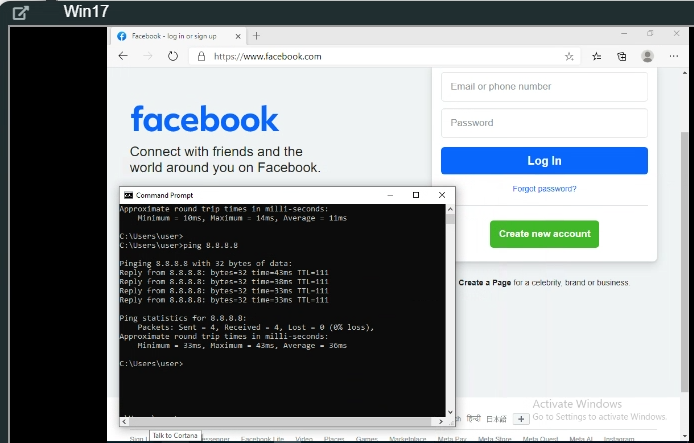


1. The website will be added, and you will be able to view the website's files in a browser.

**FINAL TEST**

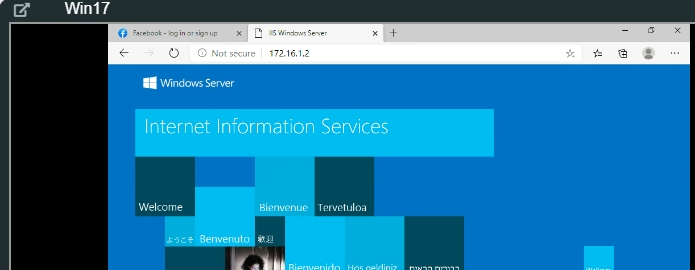
1. Keeping **only** the devices on the EIU Main Campus on, test the connection of the LAN hosts to the internet. You can do this by pinging any known domain name like google.com, yahoo.com or by launching a web browser on the Windows PC on LAN and visiting any registered website.

**Is this successful?**

**Ans: Yes.**

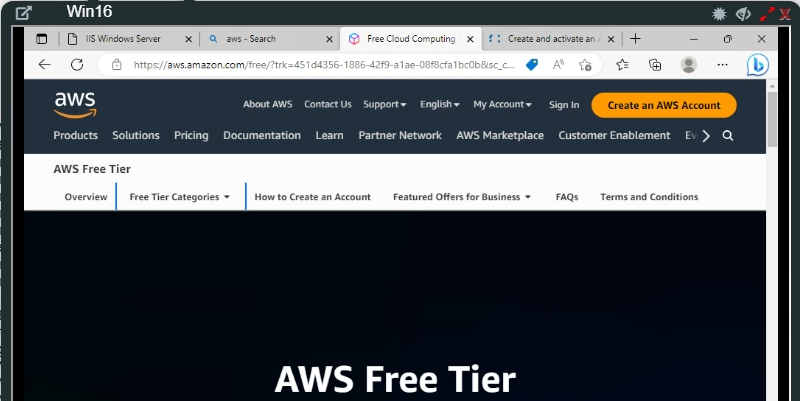
1. Keeping **only** the devices on the EIU Main Campus on, test the connection of the LAN hosts to the Webserver. Open your web browser on the Windows PC and type: http://172.16.1.2 and press enter.

**Is this successful?**

**Ans: Yes**

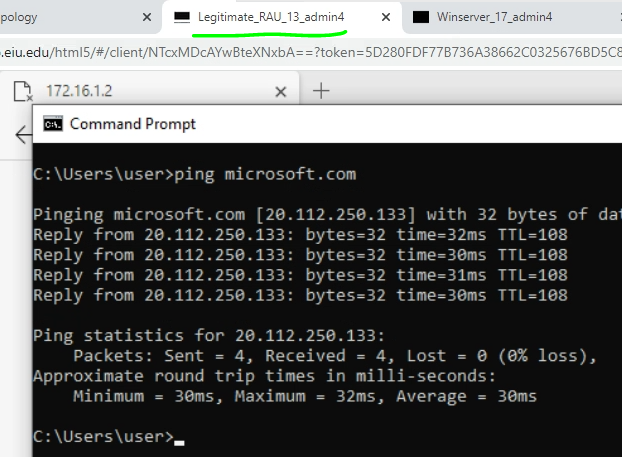
1. Keeping only the devices on the Champagne Satellite Campus on, test the connection of the LAN host to the internet. You can do this by pinging any known domain name like google.com, yahoo.com (from the command prompt) or by launching a web browser on the Windows PC on LAN and visiting any registered website.

**Is this successful?**

**Ans: Yes**

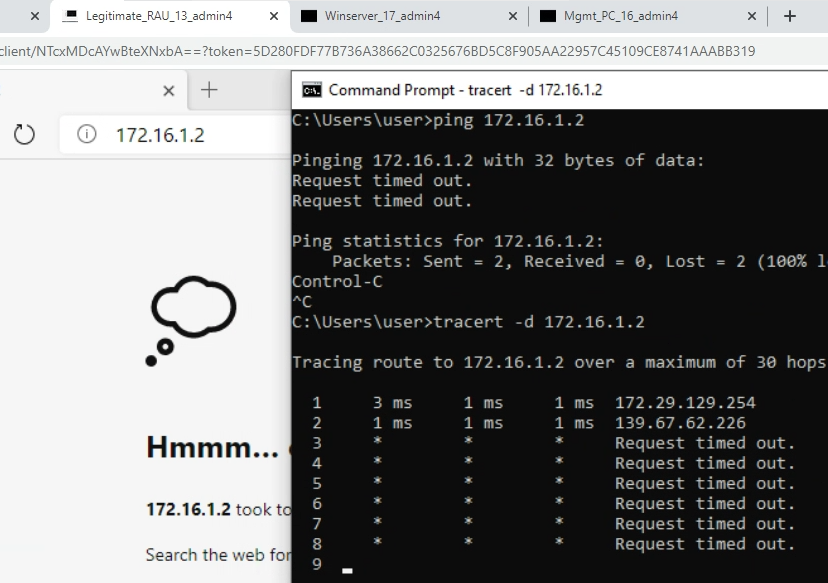
1. Keeping only the Legitimate Remote Access User and the devices on the EIU Main Campus on except the Windows PC on the main campus LAN, test the connection of the Legitimate RAU to the internet.

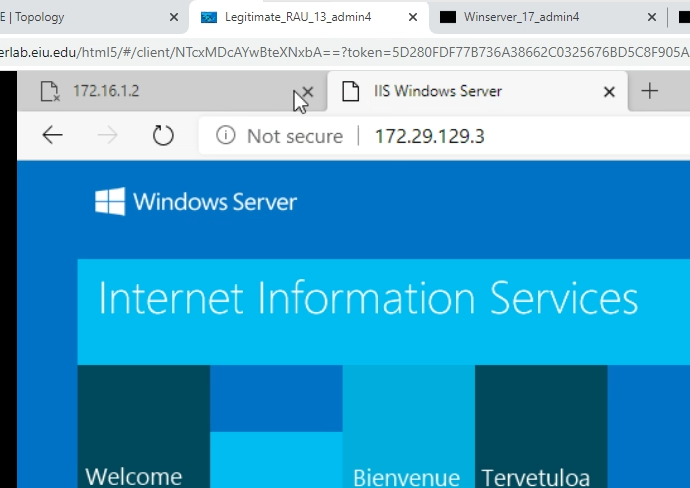
**Is this successful?**

**Ans: Yes**

1. Keeping only the Legitimate Remote Access User and the devices on the EIU Main Campus on except the Windows PC on the main campus LAN, test the connection of the Legitimate RAU to the Windows server (type <http://172.16.1.2>) on the web browser.

**Is this successful?**

**Ans: No, 172.16.1.2 is not known on the internet. Rather 172.29.129.3 is known and works.**



1. Keeping the devices on the Main Campus and the Satellite Campus on except the Windows PC on the Main Campus, test the connection between the LAN host on the Satellite Campus and the Webserver. Type <http://172.16.1.2> on the web browser.

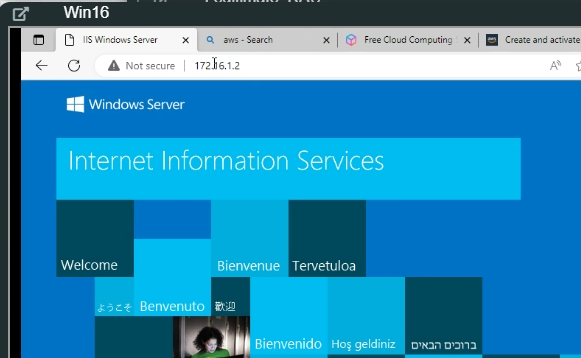
**Is this successful?  
Ans: Yes**

Fig 3: reproduced for your convenience.

Diagram

Description automatically generated