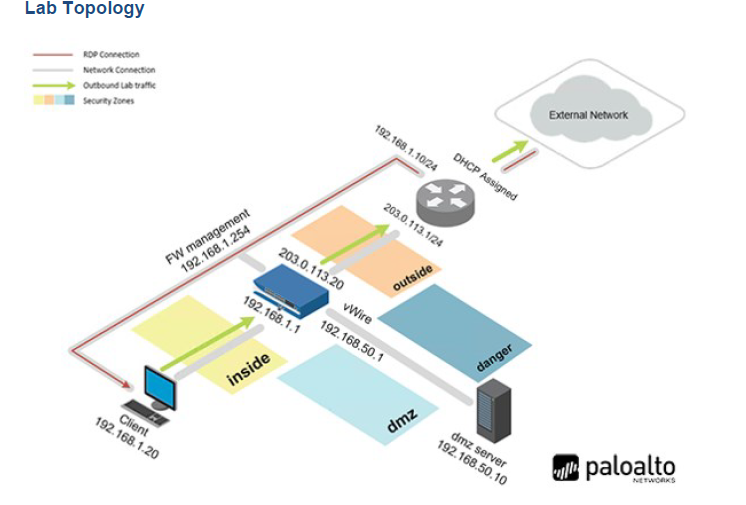
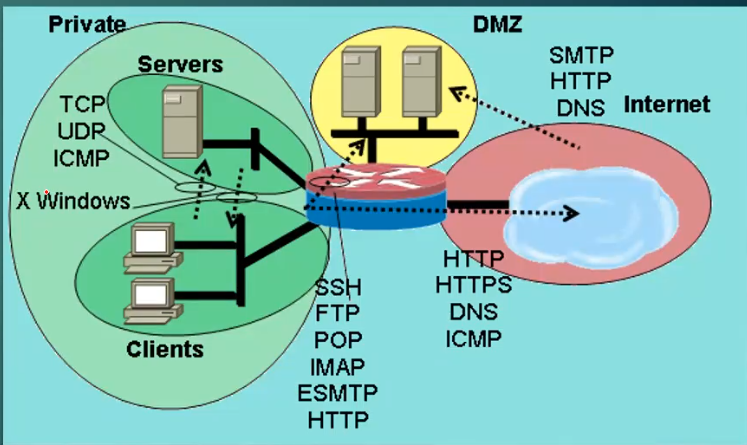
<https://github.com/msu-cnm/cyberteam/blob/main/tools/scripts/unix/first_hour.sh>

<https://github.com/msu-cnm/cyberteam/blob/main/tools/checklists/linux/common.md>

<https://github.com/msu-cnm/cyberteam/blob/main/tools/checklists/linux/advanced.md>

Palo Alto Firewall 11



* Change Admin Password
  + Select Device>Administrators>admin
    - Type old password then new password
* 2.2 Configure the **DNS and NTP Servers**
  + In the web interface, select Device > Setup > Services. Click the Services gear icon to open the Services window
    - In the Services window, verify that the Update Server is set to updates.paloaltonetworks.com. Set the **Primary DNS** Server to 8.8.8.8 and the Secondary DNS Server to 192.168.50.53.
    - Select the **NTP** tab. Set the Primary NTP Server to 0.pool.ntp.org and the Secondary NTP Server to 1.pool.ntp.org. Click OK.
* 2.3 Configure **General Settings**
  + select Device > Setup > Management. Click the Services gear icon to open the General Settings window.
    - In the General Settings window, verify the **Hostname** is firewall-a. For the **Domain**, enter lab.local. For the **Login Banner**, enter Authorized Access Only. Choose the **Time Zone** of your location
* 2.4 Modify the **Management Interface**
  + o Device > Setup > Interfaces and click on interface name Management.
    - In the Management Interface Settings window, verify 192.168.1.254 for the IP Address, 255.255.255.0 for the Netmask, and 192.168.1.1 for the Default Gateway. At the bottom of the **Permitted IP Addresses** area, click Add.
      * In the **Permitted IP Addresses**, type (MGT Computer IP)/24 for the IP Address and MGT access from this host only for the Description. Click OK.
* **2.5 Check for New PAN-OS Software**
  + In the PA-VM web interface, navigate to Device > Software. If needed, use the scroll bar to find Software.
* 
* **Connecting the Firewall to Production Networks with Security Zones**
  + C**reate Layer 3 Network Interfaces**
    - select **Network > Interfaces > Ethernet**.
    - **ethernet1/1** to configure the interface
      * Comment (Internet Connection, Users Network, Extranet Servers , etc.)
      * Interface Type (Layer 3)
      * Virtual Router (None)
      * Select **IPV4** tab
        + Set **Type** to *Static*
        + Add IP address (203.0.1.13.20/24)
        + Select OK
    - Repeat for other interfaces as necessary
  + **Create a Virtual Router**
    - In the web interface, select **Network > Virtual Routers**.
    - Click default to open the default router.
    - In the Virtual Router - *default* window, rename the default router to VR-1. Click Add to add the following interfaces: ethernet1/1, ethernet1/2, and ethernet1/3.
    - In the Virtual Router - *default* window, click the link on the side for Static Routes. Under the tab for IPv4, click Add at the bottom of the window.
    - In the Virtual Router – Static Route - IPv4 window, for Name, enter Firewall Default Gateway, for Destination, enter 0.0.0.0/0, for Interface, select ethernet1/1, for the Next Hop address, enter 203.0.113.1 (Internet IP). Leave the remaining settings unchanged. Click OK.
  + **Segment Your Production Network Using Security Zones**
    - In the web interface, select **Network > Zones**.
    - Click **Add** to create a new zone**.**
    - In the *Zone* window, enter **Internet, Users\_net, or Extranet** for the *Name*, for *Type*, select **Layer3**. Under the *Interfaces* section, click **Add**. Select Ethernet 1/1, 2, or 3 and leave all other settings unchanged. Click OK**.**
    - Commit
* **2.2 Create a Security Policy Rule**

Allow network traffic from on security zone to another security zone

* + In the web interface, select **Policies > Security**. Click **Add**.
  + In the *Security Policy Rule* window, on the *General* tab. Type **Users\_to\_Extranet** for the N*ame*. For *Description*, enter **Allows hosts in Users\_Net zone to access servers in Extranet zone**.
  + Select the **Source** tab. Under the *Source Zone* section, click **Add,** and select **Users\_Net**.
  + Select the **Destination** tab. Under the *Destination Zone* section, click **Add,** and select **Extranet**.
  + Select the Application tab. Verify Any is selected for Applications.
  + Select the **Service/URL Category** tab. Verify **Application Default** is selected for *Service,* and **Any** is selected for *URL Category. Select the Actions tab.* Do not make any changes in this section but notice that the Action is set to Allow by default. Click OK.
  + Verify the Users\_to\_Extranet security policy rule appears in the Security policies window.
  + Commit
* **Create Security Rules for Internet Access**
  + In the *PA-VM firewall* web interface, navigate to **Policies > Security**. Click **Add** at the bottom of the window.
  + In the *Security Policy Rule* window, on the *General* tab. Type **Users\_to\_Internet** for the *Name*. For *Description*, enter **Allows hosts in Users\_Net zone to access Internet zone**.
  + Select the **Source** tab. Under the *Source Zone* section, click **Add,** and select **Users\_Net**.
  + Select the **Destination** tab. Under the *Destination Zone* section, click **Add,** and select **Internet**.
  + Select the **Application** tab. Verify **Any** is selected for *Applications*.
  + Select the **Service/URL Category** tab. Verify **Application Default** is selected for *Service,* and **Any** is selected for *URL Category.* 
    - The application-default setting instructs the firewall to allow an application such as web-browsing as long as that application is using the predefined service (or destination port). For an application like web-browsing, the application default service is TCP 80; for an application such as SSL, the application default service is TCP 443.
  + *Select the* ***Actions*** *tab. Do not make any changes in this section but notice that the Action is set to* ***Allow*** *by default****.*** *Click* ***OK****.*
* ***Modify Existing Security Policies***
  + Select **Objects > Security Profiles > Antivirus**. Place a check in the box next to the **default** entry**.**
  + At the bottom of the window, click the Clone button.
  + In the Clone window that appears, leave the settings unchanged. Click OK.
  + A new entry called **default-1** will appear in the Antivirus list. Click the entry for **default-1** to edit it.
  + In the *Antivirus Profile* window, for the *Name*, enter **Corp-AV**. For *Description*, enter **Standard antivirus profile for all security policy rules**. Click **OK**.
  + Leave the *Palo Alto Networks Firewall* open and continue to the next task.
* **Create A Corporate Vulnerability Security Profile**
  + Select **Objects > Security Profiles > Vulnerability Protection**. Place a check in the box beside **strict.** Click **Clone.**
  + In the *Clone* window, click **OK**.
  + Click the entry for **strict-1** to open it.
  + In the *Vulnerability Protection Profile* window, change the name to **Corp-Vuln**. For *Description*, enter **Standard vulnerability profile for all security policy rules**. Click **OK**.
  + Leave the *Palo Alto Networks Firewall* open and continue to the next task.
* **Create A Corporate File Blocking Profile**
  + Select **Objects > Security Profiles > File Blocking**. Place a check beside the entry for **strict file blocking**. Click **Clone**.
  + In the *Clone* window, click **OK**.
  + Click the entry for **strict file blocking-1** to open it.
  + Change the *Name* to **Corp-FileBlock**. For *Description*, enter **Standard file blocking profile for all security policy rules**. Click **OK**.
  + Leave the *Palo Alto Networks Firewall* open and continue to the next task.
* **Create Data Filtering Profiles**
  + Select **Objects > Custom Objects > Data Patterns**. Click **Add**.
  + In the *Data Patterns* window, for *Name*, enter **US-SSNs**. For *Description*, enter **US Social Security Numbers.** Change the *Pattern Type* to **Predefined Pattern**. Click **Add** and scroll down the available list and select **Social Security Numbers**. Click **Add** again and select **Social Security Numbers (without dash separator)**. Click **OK**.
  + Select **Objects > Security Profiles > Data Filtering**. Click **Add**.
  + In the *Data Filtering Profiles* window, for *Name*, enter **Corp-DataFilter**. For *Description*, enter **Standard data filtering profile for all security rules.** Click **Add** and select the **US-SSNs** data pattern that you defined. Click in the **Alert Threshold** field and change the value to **1.** Click in the **Block Threshold** field and change the value to **3.** Change the **Log Severity** to **critical.** Click **OK.**
  + Leave the *Palo Alto Networks Firewall* open and continue to the next task.
* **Create a Corporate Anti Spyware Profile** 
  + Select **Objects > Security Profiles > Anti-Spyware**. Select the check box next to the **strict** Anti-Spyware Profile. Click **Clone**.
  + In the *Clone* window, click **OK**.
  + Click the entry for **strict-1** to open it.
  + In the *Data Filtering Profiles* window, for *Name*, enter **Corp-AS**. For *Description*, enter **Standard anti-spyware profile for all security policy rules.** Click **OK.**
  + Leave the *Palo Alto Networks Firewall* open and continue to the next task.
* **Create a Security Profile Group**
  + Select **Objects > Security Profile Groups.** Click **Add.**
  + **In the *Security Profile Group* window, enter Corp-Profiles-Group for the name. For each of the available Profiles, use the drop-down list to select the Corp-\* entry you have created. Click OK.**
  + You will have to add it to each individual Security policy
    - Policies->Security
      * Change the profile setting under the actions tab to use the corp-profiles-group to all applicable rules
* **Create a Wildfire Analysis Profile**
  + In the web interface, select **Objects > Security Profiles > WildFire Analysis**. Click **Add**.
  + Configure name and description
* Click **Add** and configure the following. Click **OK** to close the *WildFire Analysis Profile* window.

|  |  |
| --- | --- |
| **Parameter** | **Value** |
| **Name** | **All\_Files** |
| **Applications** | **any** |
| **File Types** | **any** |
| **Direction** | **both** |
| **Analysis** | **public-cloud** |

* **Modify Security Profile Group**
  + Select **Objects > Security Profile Groups**. Click and edit the **Corp-Profiles-Group**.
  + Use the drop-down list for **Wildfire Analysis Profile** to select **Corp-WF**. Set the other **Profiles** to **None**. Click **OK**.
  + Leave the *Palo Alto Networks Firewall* open and continue to the next task.
* **Update WildFire Settings** 
  + Select Device > Setup > WildFire. Click the gear icon to edit the General Settings.
  + In the *General Settings* window, check the boxes for **Report Benign Files** and **Report Grayware Files**. Leave the remaining settings unchanged and click **OK**.
  + Navigate to **Policies > Security** and click **Allow-PANW-Apps**.