Palo Alto Networks - Cybersecurity Foundation v1

Installation and Configuration Guide

Document Version: 2021-02-03

Contents

1   Introduction

This document provides detailed guidance on performing the installation and configuration of the *Palo Alto Networks - Fundamental Training* pod on the *NETLAB+ VE* system. This single pod design supports the individual *Cybersecurity Foundation*, *Cloud Security Fundamentals*, *Network Security Fundamentals*, and *Security Operations Fundamentals* labs-series.

1.1   Introducing the Palo Alto Networks - Fundamental Training Pod

The *Palo Alto Networks - Fundamental Training* pod is a 100% virtual machine pod consisting of four virtual machines. Linked together through virtual networking, these four virtual machines provide the environment for a student or a team to perform the *Palo Alto Networks - Cybersecurity Foundation v1* labs.
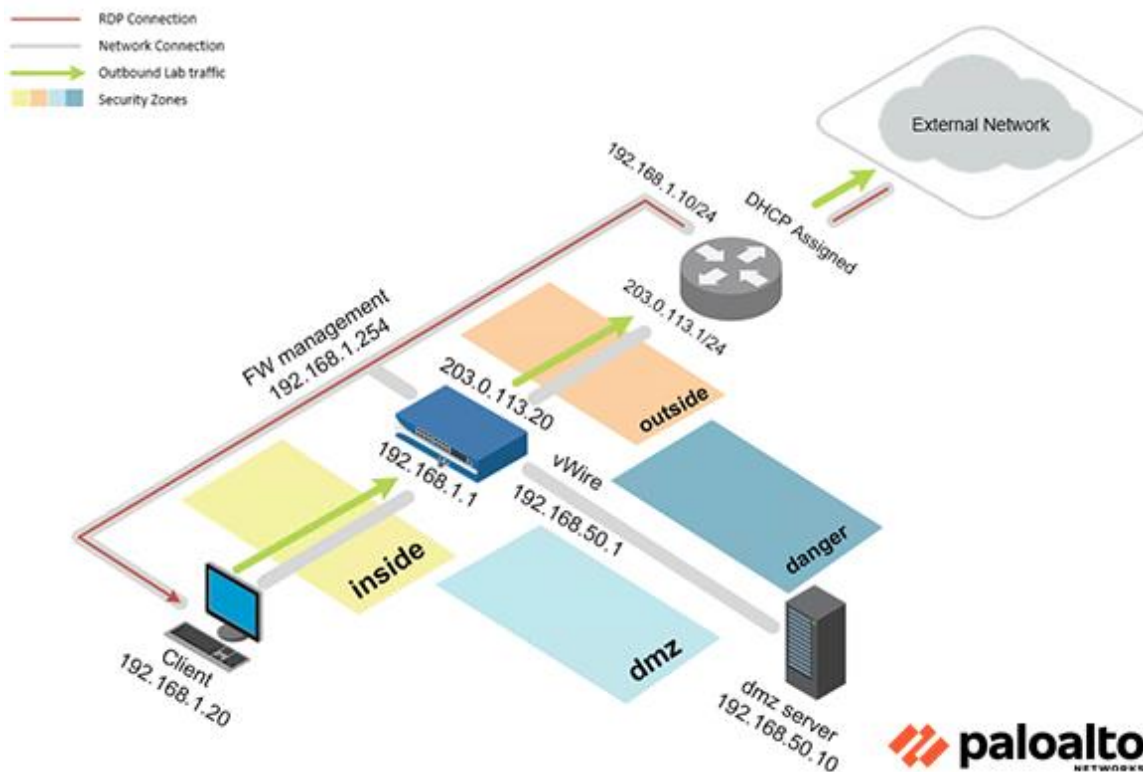
2 Planning

This guide provides specific information pertinent to delivering the *Palo Alto Networks - Fundamental Training* pod. The [NETLAB+ Remote PC Guide Series](#) provides the prerequisite guidance for setting up your VMware infrastructure, including:

- An introduction to virtualization using *NETLAB+*
- Detailed setup instructions for standing up *VMware vCenter* and *VMware ESXi*
- Virtual machine and virtual pod management concepts using *NETLAB+*

This document assumes that you have set up virtual machine infrastructure in accordance with the [NETLAB+ Remote PC Guide Series](#). The planning information below refers to specific sections in the *Remote PC Guide* when applicable.

2.1 Pod Creation Workflow

The following list is an overview of the pod setup process.

1. Obtain the master virtual machine images required for the master pod.
2. Deploy the master virtual machine images to your *VMware vCenter Appliance*.
   a. Deploy virtual machines using **Thin Provisioning** to reduce storage consumption.
   b. Make necessary adjustments to each virtual machine in the environment.
      i. Insert/Verify manual **MAC** addresses.
      ii. Change the default network to **SAFETY NET**.
      iii. Any other configuration changes mentioned in this guide.
3. Import the deployed virtual machines to the *NETLAB+* **Virtual Machine Inventory**.
4. Activate or license the required software on each virtual machine when prompted.
5. Take a snapshot of each virtual machine in the master pod labeled **GOLDEN_MASTER** after all configurations and licensing have taken effect. The *GOLDEN_MASTER* snapshot is used to clone virtual machine images for the user pods.
6. Use the *NETLAB+* **Pod Cloning** feature to create student pods from the master pod.
7. If multiple hosts are used in the *NETLAB+* environment, make a **Full Clone** of the master pod on the initial host (Host A) to the subsequent host (Host B) and so on using the *NETLAB+* **Pod Cloning** feature.

2.2   Pod Resource Requirements

The *Palo Alto Networks - Cybersecurity Foundation v1* course will consume 61.8 GB of storage per each master pod instance.

The following table provides details of the storage requirements for each of the virtual machines in the pod.

Virtual Machine	OVF/OVA	Initial Master Pod (Thin Provisioned)	Maximum Allocated Memory
Client	6.3 GB	18.6 GB	2 GB
DMZ	4.5 GB	16.1 GB	512 MB
Firewall	10.3 GB	24.9 GB	6 GB
VRouter	1 GB	2.2 GB	256 MB
Total	**22.1 GB**	**61.8 GB**	**8.77 GB**

2.3   ESXi Host Server Requirements

Please refer to the *NDG* website for specific *ESXi* host requirements to support virtual machine delivery: https://www.netdevgroup.com/products/requirements/

The deployment of the *Palo Alto Networks - Fundamental Training* pod requires VMware ESXi version of **6.0** or greater.

> Please Note   The number of **active** pods that can be used simultaneously depends on the *NETLAB+* product license and the number of *VMware ESXi* host servers meeting the hardware requirements specifications.

For current *ESXi* server requirements and active pod count, refer to the following URL:
http://www.netdevgroup.com/support/remote_pc.html#vm_host_server_specifications.

2.4   NETLAB+ Requirements

Installation of the *Palo Alto Networks - Fundamental Training* pod, as described in this guide, requires that you are running *NETLAB+ VE*.

Previous versions of *NETLAB+* do not support requirements for the *Palo Alto Networks - Cybersecurity Foundation v1* course on the physical host servers.

Please refer to the *NETLAB+ Remote PC Guide Series*.

2.5   NETLAB+ Virtual Machine Infrastructure Setup

The *NETLAB+ Virtual Machine Infrastructure* setup is described in the following sections of the *NETLAB+ Remote PC Guide Series*:

- *Registering a Virtual Datacenter in NETLAB+*
- *Adding ESXi hosts in NETLAB+*
- *Proactive Resource Awareness*

> It is important to configure *Proactive Resource Awareness* to maximize the number of active pods per physical *ESXi* host.

2.6   Software Requirements

For the purpose of software licensing, each virtual machine is treated as an individual machine, PC, or server. Please refer to the specific vendor license agreements (and educational discount programs, if applicable) to determine licensing requirements for your virtual machines' software, operating system, and applications.

The minimum virtual infrastructure software required for standing up this pod is in the following table.

Virtual Infrastructure Requirements	
Software	**Version**
vSphere ESXi	6.0
vCenter Server	6.0

Please refer to the *Software and Licenses* section regarding the software requirements for virtual machines in the pod.

2.7   Networking Requirements

To accommodate the movement of large *VMs*, *OVF/OVAs*, and *ISO* disk images from one host to another, gigabit Ethernet or better connectivity is recommended to interconnect your *NETLAB+*, *vCenter Server* system and *ESXi* host systems.

The two standard networking models recommended to interconnect your servers are described in detail in the *Networking Models* section of the *Remote PC Guide Series, Volume 1 - Introduction and Planning*.

2.7.1   Pod Internet Access

The pods for the *Palo Alto Networks - Cybersecurity Foundation v1* course each require Internet access. This access is required for licensing the Master pod, as well as the various lab objectives in the student pods.

This environment is designed to leverage one vSwitch per host that attaches to a network that has a DHCP server to assign IPv4 addresses that are routable to the Internet.

This lab environment is also designed to leverage the public DNS servers 8.8.8.8 and 4.2.2.2. This vSwitch must be able to access those servers, which may require adjustments in a firewall if applicable.

2.7.2   Completing the NETLAB+ Pod Internet Access and Use Agreement

> **STOP** You are required to complete the *NETLAB+ Pod Internet Access and Use Agreement* prior to obtaining access to the pod or content for this course.

Due to the security and legal implications regarding accessing the Internet from within the pod, we require that you agree to the terms contained within this online document prior to obtaining access to the pod or content for this course:
https://www.netdevgroup.com/content/paloalto/agreement

3   Software and Licenses

3.1   Obtaining Palo Alto Networks Software Licenses

To obtain licensing and access to the *Palo Alto Networks - Cybersecurity Foundation v1* labs, your institution must be a Palo Alto Networks Authorized Academy Center (AAC).

You can find information about the Palo Alto Networks AAC at the following link: https://www.paloaltonetworks.com/services/education/academy

Once your membership in the Palo Alto Networks AAC is approved, you can request licenses for use with your pods from your Palo Alto Networks Academy representative or by emailing *academy@paloaltonetworks.com*.

3.2   Downloading OVF Files

The virtual machines are made available as *Open Virtualization Format* (*OVF*) or *Open Virtualization Archive* (*OVA*) files. These files are available for download from *CSSIA*.

To request access to the preconfigured virtual machine templates from *CSSIA*:

1. Go to *the CSSIA Resources* page: https://www.cssia.org/cssiaresources/
2. Select **CSSIA VM Image Sharing Agreement**.
3. Complete and submit your access request by following the instructions on the request form.
4. *CSSIA* will provide, via email, password-protected download links. Access to the download links is provided only to customers who are current with their NETLAB+ support contract and are participants in the appropriate partner programs (*i.e., Cisco Networking Academy, VMware IT Academy, Red Hat Academy, and/or Palo Alto Networks*).
5. Once all virtual machines have been downloaded, they can be deployed following the steps in the appropriate pod installation guide. Each virtual machine is deployed individually.

4 Master Pod Configuration

4.1 Deploying Virtual Machine OVF/OVA Files

Deploy on your host server the pod virtual machine *OVF/OVA* files you have downloaded.

1. Navigate to your **vSphere Client** using your management workstation, ensure that your downloaded *OVA/OVF* files are accessible on this machine, and then connect to your **vCenter Server**.
2. From the *vSphere Client* interface, navigate to **Hosts and Clusters**.
3. Right-click on the target **ESXi Host Server** and select **Deploy OVF Template**.
4. In the *Deploy OVF Template* window, on the *Select source* step, select the **Local File** radio button and click **Browse**.
5. Locate and select one of the VMs for the pod, click **Open**.

> **Please Note**
>
> Only one VM can be selected using this wizard. The process will have to be repeated for the remaining VMs.

6. Verify that the VM information populates next to the *Browse* button and click **Next**.
7. On the *Review details* step, make sure to fill the checkbox for **Accept extra configuration options** (*if present*) and click **Next**.
8. On the *Select name and folder* step, change the name of the virtual machine to something that is easy to manage. You can use the names provided in the list below as names for the virtual machines if you do not have a set naming convention. Select the appropriate **datacenter** and click **Next**.

VM Name	VM OS	Virtual Machine Deployment Name
Client	Linux	PAN_FTv1_Master.Client
DMZ	Linux	PAN_FTv1_Master.DMZ
Firewall	Linux	PAN_FTv1_Master.Firewall
VRouter	Linux	PAN_FTv1_Master.VRouter

9. On the *Select Storage* step, choose the appropriate storage device and make sure that **Thin Provision** is selected. Click **Next**.
10. In the *Setup networks* section, select **SAFETY NET** as the destination and click **Next.**

> **STOP**
>
> If *SAFETY NET* is not available, refer to the *Create a Safe Staging Network* section in the *Remote PC Guide Series – Volume 2*.

11. In the *Ready to complete* section, make sure **Power on after deployment** is **unchecked** and confirm the settings. Click **Finish**.

12. *vCenter* will begin deploying the virtual machine. This may take some time depending on the speed of your connection, HDDs, etc. Repeat the previous steps for each remaining virtual machine in the master pod.

13. The Firewall VM requires an extra step. First, deploy the VM from the OVA using the name *PAN_FTv1_FW_Init* while following the instructions in the previous steps. Then, clone *PAN_FTv1_FW_Init*, naming it *PAN_FTv1_Master.Firewall* or whichever naming convention you chose for the previous VMs. Next, delete *PAN_FTv1_FW_Init*. This extra cloning procedure is to help remove existing licensing with the PAN Firewall, if any. You only need to perform this step with the Firewall VM.

4.1.1 Modify Virtual Machines

Once the virtual machines are imported onto the host, verify the configurations. The following steps will guide you through the process.

1. In the *vSphere Client* interface, right-click on the imported virtual machine and select **Edit Settings**.

2. For all the virtual machines, manually assign the *MAC* addresses for each *NIC*. The table below identifies the *MAC* addresses per *NIC*.

Virtual Machine	NIC	MAC
Client	1	00:50:56:8a:0d:49
DMZ	1	00:50:56:8a:92:db
	2	00:50:56:8a:c6:2b
Firewall	1	00:50:56:8a:7c:78
	2	00:50:56:8a:91:be
	3	00:50:56:8a:91:c4
	4	00:50:56:8a:54:c7
	5	00:50:56:8a:84:17
	6	00:50:56:8a:b3:fc
VRouter	1	*(automatic)*
	2	00:50:56:8a:c8:55
	3	00:50:56:8a:a6:88

3. Repeat the previous steps for each of the remaining virtual machines in the master pod.

4. For the *vRouter* virtual machine, change *Network adapter 1* to the network that has DHCP Internet access available, as well as making sure that the *MAC* is set to **Automatic**, see *Pod Internet Access*.

4.2   NETLAB+ Virtual Machine Inventory Setup

This section will guide you in adding your templates to the *Virtual Machine Inventory* of your *NETLAB+ VE* system.

1. Log in to your *NETLAB+ VE* system using the administrator account.

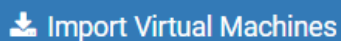2. Select the **Virtual Machine Infrastructure** icon.

Virtual Machine Infrastructure

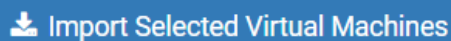3. Click the **Virtual Machine Inventory** icon.

Virtual Machine Inventory

Import, clone, and manage the inventory of virtual machines to be used with NETLAB+.

4. Click the **Import Virtual Machines** button located at the bottom of the list.

⬇ Import Virtual Machines

5. Select the appropriate datacenter from the list where your master VMs reside.
6. Select the checkbox next to the virtual machines you had just deployed and click **Import Selected Virtual Machines**.

⬇ Import Selected Virtual Machines

7. When the *Configure VMs* window loads, you can set your virtual machine parameters.

   a. Check the dropdown box for the correct operating system for each imported virtual machine.
   b. Change *Role* to **Master** for each VM.
   c. Add any comments for each virtual machine in the last column.

   > It is advised to leave the *Version* and *Build* numbers for reference when requesting *NDG* support.

   d. Verify your settings and click **Import (X) Virtual Machines** (notice the number in parenthesis is dynamic, depending on the amount of VMs selected).

   ⬇ Import (4) Virtual Machines

e. Verify all *Import Statuses* report back with **OK** and then click on the **Dismiss** button.
f. Verify that your virtual machines show up in the inventory.

For additional information, please refer to the NETLAB+ VE Administrator Guide.

4.3   Building the Master Palo Alto Networks - Fundamental Training Pod

This section will assist you in adding the *Palo Alto Networks - Fundamental Training* pod to your *NETLAB+* system.

4.3.1   Enabling Lab Content in Course Manager

Please refer to the *Course Manager* section *of the* NETLAB+ VE Administrator Guide on how to enable content. Please install the **Palo Alto Networks Cybersecurity Foundation - v1.0** course.

4.3.2   Create the Master Pod

1. Log into **NETLAB+ VE** with the *administrator* account.
2. Select the **Pods** icon.

3. Create a new pod by scrolling to the bottom and clicking the **Create New Pod** button.

4. Then, click on the **PAN Fundamental Training** pod design from the list of installed pod types.

PAN Fundamental Training
The Palo Alto Networks - Fundamental Training pod provides candidates to conduct labs from the Cybersecurity Foundation, Cloud Security Fundamentals, Network Security Fundamentals, and Security Operations Fundamentals training series.
2021 Copyright (C) Network Development Group, Inc.
https://www.netdevgroup.com/support/tech_support.html

5. On the *New Pod* window, input a value into the **Pod ID** and **Pod Name** fields. Click **Next**.

> The *Pod ID* determines the order in which the pods will appear in the scheduler. It is best practice to use a block of sequential ID numbers for the *Pod Id* that allows for the number of pods you are going to install.
>
> The *Pod Name* identifies the pod and is unique per pod. Here we used the name of the lab set or course in a shortened form along with a host identifier (H120), the type and number of the pod (M1000).

6. To finalize the wizard, click **OK**.

For additional information, please refer to the *NETLAB+ VE Administrator Guide*.

4.3.3 Attach Virtual Machines to the Master Pod

Update the master pod to associate the virtual machines with the newly created pod.

1. Select the **PAN Fundamental Training** master pod from the pod list.

2. Click on the **Action** dropdown next to the virtual machine you are about to assign and select **Attach VM**.

Remote PC ④					
PC Name	VM	Operating System	VM Role	Runtime Host	Action
🖥 Client	ABSENT				▾
🗄 Firewall	ABSENT				👁 View
🗄 DMZ	ABSENT				⚙ Settings
🗄 VRouter	ABSENT				⊕ Attach VM
					⊖ Remove VM From...
					📷 Snapshots

3. Select the corresponding virtual machine from the inventory list.

Virtual Machine Name ▲	Operating System ⇕	Role ⇕
🖳 PAN_FTv1_Master.Client	Linux	Master
🖳 PAN_FTv1_Master.DMZ	Linux	Master
🖳 PAN_FTv1_Master.Firewall	Linux	Master
🖳 PAN_FTv1_Master.VRouter	Linux	Master

4. Click **OK** to confirm the VM attachment and repeat the previous steps for the remaining virtual machines.

4.3.4   Create Snapshots for the Master Virtual Machines

In order to proceed with pod cloning, snapshots must be created on each of the pod's virtual machines.

> ⚠ Verify that all VMs are still powered off before taking snapshots.

1. Make sure to view the **PAN Fundamental Training** master pod you just assigned machines to. In the pod view, click on the dropdown menu option underneath the *Action* column for a specific VM and select **Snapshots**.

	PC Name	VM	Operating System	VM Role	Runtime Host	Action
🐧	Client	PAN_FTv1_Master.Client	Linux	MASTER		▼
🐧	Firewall	PAN_FTv1_Master.Firewall	Linux	MASTER		👁 View
						⚙ Settings
🐧	DMZ	PAN_FTv1_Master.DMZ	Linux	MASTER		⊕ Attach VM
						⊖ Remove VM From...
🐧	VRouter	PAN_FTv1_Master.VRouter	Linux	MASTER		📷 Snapshots

Remote PC 4

2. In the *Snapshot Manager* window, click on the **Take** button. This will take a snapshot of the current state of the virtual machine.
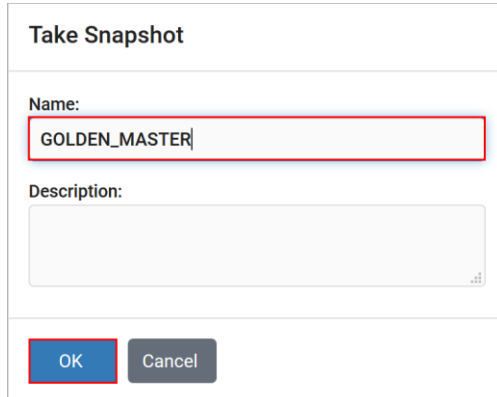
Snapshot Manager

- 🖥 [_____]
  - 🔘 You Are Here!

Name:

Description:

[📷 Take] [📷 Delete All]   [🔘 Go To] [📝 Edit] [📷 Delete]

[⊕ Dismiss]

⚠️ Any changes made after this will require a new snapshot or those changes will not reflect in the reset state of the pod or its clones.

3. In the *Take Snapshot* window, type `GOLDEN_MASTER` into the *Name* text field, or you may choose another naming convention as long as it is consistent for easy management. Click **OK**.

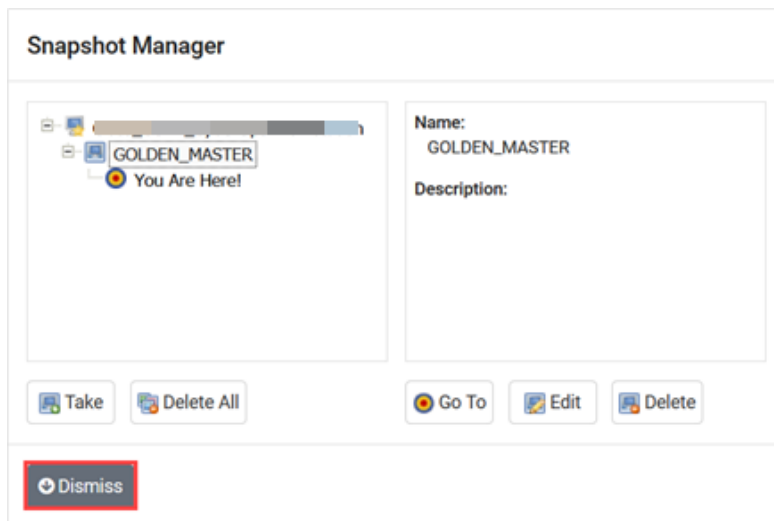> ⚠️ It is recommended to use *GOLDEN_MASTER* as the snapshot name when working with normalized pod types.

4. In the *Snapshot Manager* window, notice the snapshot is created. Click the **Dismiss** button.

> ⚠️ At this point it is good to verify that you have only one snapshot on the virtual machine. Multiple snapshots increase the likelihood of having problems, especially if the snapshots are named the same. Also, the more snapshots a virtual machine has, the slower the performance and the more drive space is used.

5. Repeat the previous steps for the remaining virtual machines.

4.3.5 Set the Revert to Snapshot

1. Make sure to view the **PAN Fundamental Training** master pod you just created snapshots for. In the pod view, click on the dropdown menu option underneath the *Action* column and select **Settings**.

2. In the virtual machine's *Settings* window, click on the *Revert to Snapshot* dropdown and select **GOLDEN_MASTER** and then click the **Submit** button.

> This sets the snapshot on the virtual machine that will get reverted to each time the pod is scheduled.

3. Click **OK** to confirm.

4. Return to the pod view page and repeat the previous steps for the remaining virtual machines.

4.3.6 Bring the Master Pod online

1. In the pod view, click the drop arrow under *State* and select **Online**.
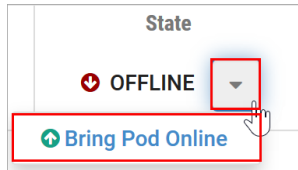
4.4 Make changes to the Master Pod

Some pods have software that needs to be altered on the host machine before it can be used properly. This normally happens when software requires licenses to function.

If there are changes that need to be made to the master pod prior to link cloning, either student pods or full cloning other master pods on other hosts, you will need to follow this set of instructions to ready your master pod.

For the *Palo Alto Networks - Fundamental Training* master pod, you will need to license the *Palo Alto Networks Firewall* machine. This process consists of:

- Scheduling the master pod
- Licensing the *Firewall*
- Shutting down the *Firewall*
- Resetting the network interface cards to *SAFETY NET*
- Taking a new *GOLDEN_MASTER* snapshot for the *Firewall*
- Ending the reservation

4.4.1 Virtual Machine Credentials

For your reference, the following table provides a list of the credentials for the systems in the pod:

Machine	User name	Password
Client	lab-user	Train1ng$
Firewall	admin	Train1ng$

4.4.2   Create Class and Schedule the Master Pod

Create a class as identified in the *Add Classes* section of the *NETLAB+ VE Instructor Guide* followed by adding the appropriate content to the selected class, and then schedule the *Master Pod* to license the *Firewall* virtual machine.

> ⚠️ When scheduling the *Master Pod*, it is important to schedule the pod for enough time to complete the following steps. Failure to complete the steps prior to taking the final snapshot could mean redeploying necessary virtual machines.

4.4.3   License the Firewall

1. Launch the **Client** virtual machine to access the graphical login screen.
2. Click within the splash screen to bring up the login screen. Log in as `lab-user` using the password `Train1ng$`.
3. Launch the **Chrome** browser and connect to `https://192.168.1.254`.
4. If a security warning appears, click **Advanced** and proceed by clicking on **Proceed to 192.168.1.254 (unsafe)**.
5. Log in to the *Palo Alto Networks* firewall as `admin` with the password as `Train1ng$`.
6. In the *Palo Alto Networks* firewall web interface, select **Device > Setup > Operations**.
7. Click **Load named configuration snapshot**:
8. Click the dropdown list next to the *Name* text box and select **pan-nsf-lab-06.xml**. Click **OK**.
9. Click **Close**.
10. Click the **Commit** link at the top-right of the web interface.
11. Click **Commit** and wait until the commit process is complete.
12. Once completed successfully, click **Close** to continue.
13. Scroll down in the window on the left-hand side. Click on **Licenses**.
14. Click on **Activate feature using authorization code**.
15. Enter the Authorization Code and click **OK**.
16. Click **OK** on the Warning window.

4.4.4   Shut Down the Firewall

1. In the *Palo Alto Networks* firewall web interface, make sure the **Device** tab is selected at the top and click **Setup** on the left side.
2. Click on **Shutdown Device** under *Device Operations*.
3. Click **Yes** on the *Shutdown Device* window.
4. Close the web browser.

4.4.5 Reset the NIC to SAFETY NET

1. Outside the *NETLAB+* web interface, navigate to your **vSphere Client** using your management workstation, and then connect to your **vCenter Server**.
2. From the *vSphere Client* dashboard, select **Hosts and Clusters**.
3. Select your host under the **NETLAB** datacenter.
4. Locate the **Firewall** virtual machine, right-click it, and select **Edit Settings**.
5. Change all six network adapters to be connected to **SAFETY NET**.
6. Click **OK** to confirm settings.

4.4.6 Create Snapshot on the Changed Master Virtual Machines

1. Right-click on the **Firewall** virtual machine and select **Snapshots-> Manage Snapshots**.
2. Click **Delete** to delete the current snapshot. Remember the name of this snapshot, as the new snapshot will need to have the exact same name.
3. Click **OK** on the *Confirm Delete* window.
4. Click **Done** on the *Manage Snapshots* window.
5. Right-click on the **Firewall** virtual machine and select **Snapshots-> Take Snapshot**.
6. In the *Take Snapshot* window, type `GOLDEN_MASTER` or whatever prior snapshot name the virtual machine had. Click **OK** to take the snapshot.

4.4.7 End Reservation

You may now end the reservation of the master pod.

5   Pod Cloning

This section will help you create multiple student pods. The following sections describe the *NETLAB+* pod cloning feature used to create student pods on one or two host systems.

5.1   Linked Clones and Full Clones

NETLAB+ can create *linked clones* or *full clones*.

A **linked clone** (or linked virtual machine) is a virtual machine that shares virtual disks with the parent (or master) virtual machine in an ongoing manner. This conserves disk space and allows multiple virtual machines to use the same software installation. Linked clones can be created very quickly because most of the disk is shared with the parent VM.

A **full clone** is an independent copy of a virtual machine that shares nothing with the parent virtual machine after the cloning operation. Ongoing operation of a full clone is entirely separate from the parent virtual machine.

5.2   Creating User Pods

The following section describes how to create user pods on the same *VMware Host* system that holds your master pod's virtual machines. In this scenario, we will create linked virtual machines using the *NETLAB+* pod cloning utility.

1. Log in to **NETLAB+ VE** with the *administrator* account.
2. Select the **Pods** icon.

3. Click on your master pod.
4. Make sure the pod is offline by selecting **Take Pod Offline**.
5. Click the **Clone Pod** button to create a new pod-based on the settings and snapshots of this pod.
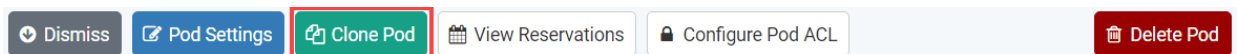
6. Input a new ID value into the **New Pod ID** field. It is advised to keep the pods in numerical order. If the pod IDs are not in numerical order, they will not show up in the scheduler in numerical order. Click **Next**.

7. Enter a name for the cloned pod into the **New Pod Name** field. For example, **PAN_FTv1_H120_S1001**. Click **Next**.

> The *Pod Name* identifies the pod and is unique per pod. Here we used the name of the lab set or course in a shortened form along with a host identifier (H120), the type and number of the pod (S1001).
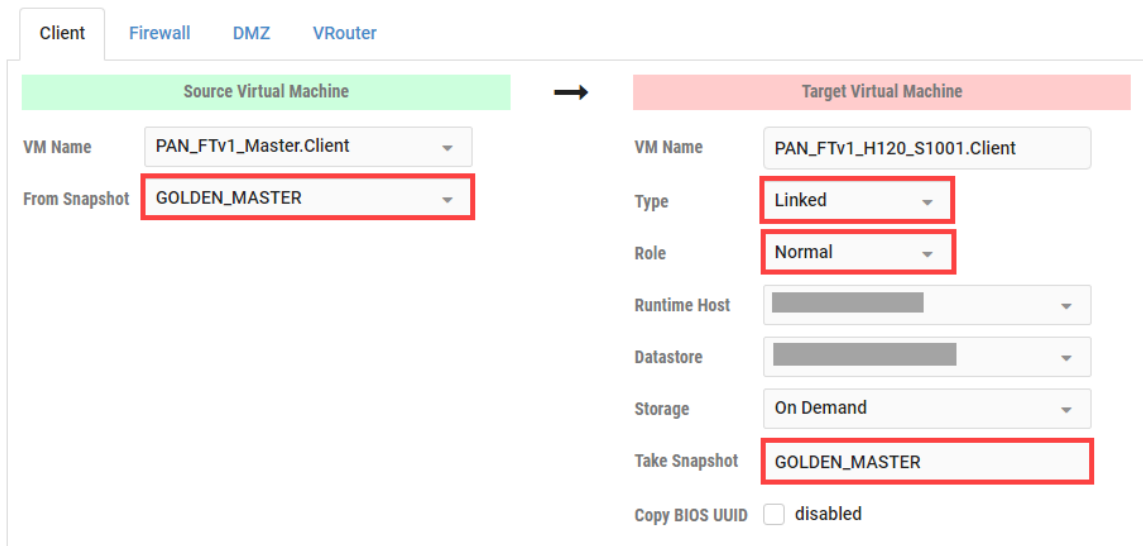
8. When the action has finished processing, you are presented with a settings screen. Notice each VM has its own tab. Go through each tab and verify the following:

Source Virtual Machine:
   a. *From Snapshot* should be set to the **GOLDEN_MASTER** snapshot you created previously.

Target Virtual Machine:
   a. For *Type*, verify that **Linked** is selected.
   b. For *Role*, verify that the **Normal** role is selected.
   c. For *Take Snapshot*, verify that **GOLDEN_MASTER** is inputted.

9. When you are done changing settings, click **Clone Pod**. This should complete within a minute as we are creating linked virtual machines.
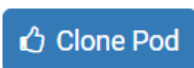
10. When the pod clone process is finished, click **OK**.
11. If you want to dedicate this pod to a particular class, team, or student, use the *Pod ACLs* feature. For details, see the [NETLAB+ VE Instructor Guide](#).

12. Click the **Online** Button on the *Pod Management* page to make the pod available.

Activity	ACL State	State
IDLE	🔓 DISABLED	⏻ OFFLINE ▾
		⊕ Bring Pod Online
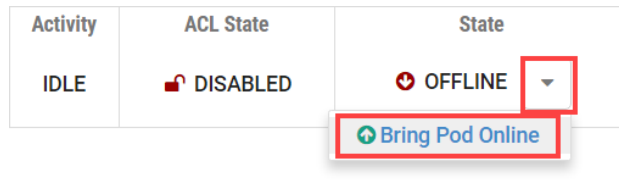
The user pod can now be reserved. When the reservation becomes active, *NETLAB+* will automatically configure virtual machines and virtual networking for your new pod.

> The *GOLDEN_MASTER* snapshot is the starting point for all pods. We recommend that you reserve the 1st pod and conduct some labs to make sure the snapshot images work correctly. If there are defects, make corrections to the images to the master pod and retake the *GOLDEN_MASTER* snapshot before creating additional pods.

5.3   Copying Your Master Pod to the Second Host

For this task, we will use the pod cloning utility to copy our master pod to the second host.

1. Log in to *NETLAB+* with the administrator account.
2. Select the **Pods** icon.

Pods

3. Click on the master pod.
4. Make sure the pod is offline by selecting **Take Pod Offline**.
5. Click the **Clone** button to create a new pod-based on the settings of this pod.
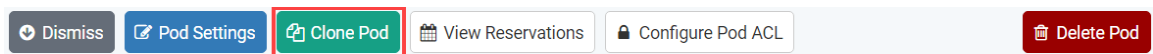
⊘ Dismiss	✎ Pod Settings	⎘ Clone Pod	🗓 View Reservations	🔒 Configure Pod ACL	🗑 Delete Pod

6. Input a new ID value into the **New Pod ID** field. It is advised to keep the pods in numerical order. If the pod IDs are not in numerical order, they will not show up in the scheduler in numerical order. Click **Next**.

7. Enter a name for the cloned pod into the **New Pod Name** field. For example, **PAN_FTv1_H130_M1000**. Click **Next**.

> The **Pod Name** identifies the pod and is unique per pod. Here we used the name of the lab set or course in a shortened form along with a host identifier (H130), the type and number of the pod (M1000).
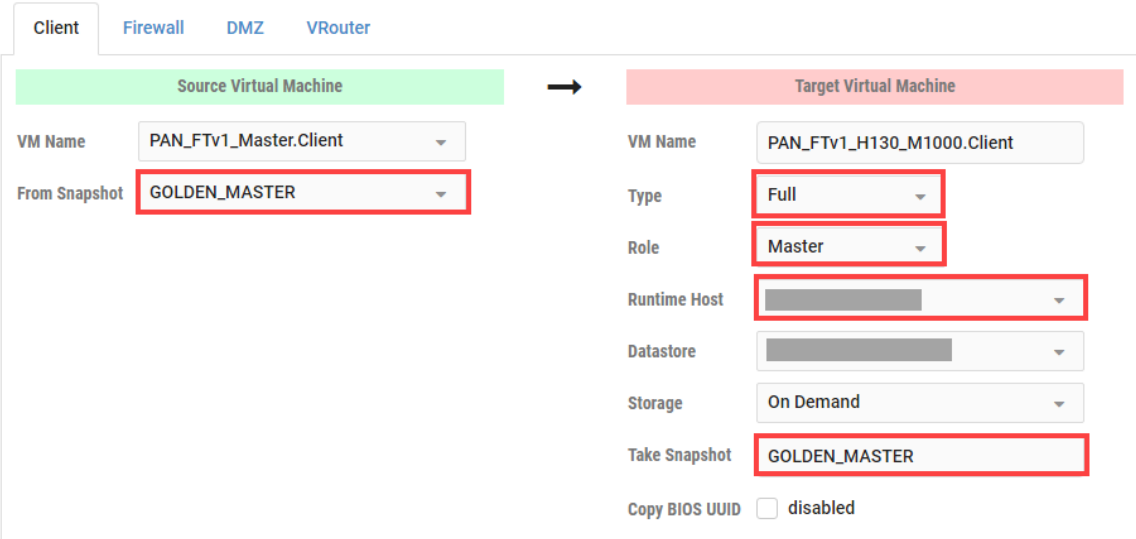
8. When the action has finished processing, you are presented with a settings screen. Notice each VM has its own tab. Go through each tab and verify the following:

Source Virtual Machine:
   a. *From Snapshot* should be set to the **GOLDEN_MASTER** snapshot you created previously.

Target Virtual Machine:
   a. For *Type*, verify that **Full** is selected.
   b. For *Role*, verify that the **Master** role is selected.
   c. For *Take Snapshot*, verify that **GOLDEN_MASTER** is inputted.
   d. For *Runtime Host*, select the second host system (which should be different than the system you are cloning from).

9. When you are done changing settings, click **Clone Pod**. This may take up to 30 minutes as full copies are being made. You may navigate away from the cloning progress screen, and then later return to the pod to check progress.
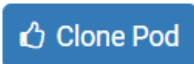
👍 Clone Pod

10. When the pod clone process is finished, click **OK**.

11. It is likely that you will need to reactivate the licensing on any VMs in the Master pod on the second (third, etc.) host. Please test the master pod prior to cloning student pods.

5.4   Creating User Pods on the Second Host

To create user pods on the second host, repeat the steps to create user pods on the first host (see *Creating User Pods)*, substituting the second master pod (created in the previous section) as the cloning source.

5.5   Assigning Pods to Students, Teams, or Classes

Please refer to the *NETLAB+ VE Instructor Guide* for details on using the *Pod ACLs* feature.