Cisco Firepower Virtual for VMware Setup

After you install a Cisco Firepower System virtual appliance, you must complete a setup process that allows the new appliance to communicate on your trusted management network. You must also change the administrator password and accept the end user license agreement (EULA).

The setup process also allows you to perform many initial administrative-level tasks, such as setting the time, registering and licensing devices, and scheduling updates. The options you choose during setup and registration determine the default interfaces, inline sets, zones, and policies that the system creates and applies.

The purpose of these initial configurations and policies is to provide an out-of-the-box experience and to help you quickly set up your deployment, not to restrict your options. Regardless of how you initially configure a virtual appliance, you can change its configuration at any time using the Cisco Firepower Management Center. In other words, choosing a detection mode or access control policy during setup, for example, does not lock you into a specific device, zone, or policy configuration.

Regardless of how you deploy, begin by powering on the appliance to initialize it. After initialization completes, log in using the VMware console and complete the setup in one of the following ways, depending on the appliance type:

Cisco Firepower NGIPSv

Cisco Firepower NGIPSv virtual appliances do not have a web interface. If you deploy with the VI OVF template, you can perform the initial setup, including registering the appliance to a Firepower Management Center, using the deployment wizard. If you deploy with the ESXi OVF template, you must use the interactive command line interface (CLI) to perform the initial setup.

Cisco Firepower Management Center Virtual

If you deploy with the VI OVF template, you can perform the network configuration using the wizard in the deployment. If you choose not to use the setup wizard or you deploy with the ESXi OVF template, configure network settings using a script. After your network is configured, complete the setup process using a computer on your management network to browse to the Cisco Firepower Management Center's web interface.

Note: If you are deploying multiple appliances, set up your Firepower NGIPSv appliances first, then their managing Firepower Management Center. The initial setup process for a device allows you to preregister it to a Firepower Management Center; the setup process for a Firepower Management Center allows you to add and license preregistered managed devices.

Initializing a Virtual Appliance

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Any	Any	Admin

After you install a virtual appliance, initialization starts automatically when you power on the virtual appliance for the first time.

Caution: **Startup time depends on a number of factors, including server resource availability. It can take up to 40 minutes for the initialization to complete. Do not interrupt the initialization or you may have to delete the appliance and begin again.**

Use the following procedure to initialize a virtual appliance.

Procedure

1. Power on the appliance:
   - — In the VMware vCloud Director web portal, select the **vApp** from the display, then click **Start**.
   - — In the vSphere Client, right-click the name of your imported virtual appliance from the inventory list, then select **Power > Power On** from the context menu.
2. Monitor the initialization on the VMware console tab.

What to Do Next

If you used a VI OVF template and configured your Firepower System-required settings during deployment, no further configuration is required.

If you used an ESXi OVF template or you did not configure Firepower System-required settings when you deployed with the VI OVF template, continue with Setting Up a Firepower NGIPSv Device Using the CLI, page 16.

Setting Up a Firepower NGIPSv Device Using the CLI

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	NGIPSv	Any	Admin

Because Firepower NGIPSv devices do not have web interfaces, you must set up a virtual device using the CLI if you deployed with an ESXi OVF template. You can also use the CLI to configure Firepower System-required settings if you deployed with a VI OVF template and did not use the setup wizard during deployment.

Note: If you deployed with a VI OVF template and used the setup wizard, your virtual device is configured and no further action is required.

When you first log into a newly configured device, you must read and accept the EULA. Then, follow the setup prompts to change the administrator password, and configure the device’s network settings and detection mode.

When following the setup prompts, for multiple-choice questions, your options are listed in parentheses, such as `(y/n)`. Defaults are listed in square brackets, such as `[y]`. Press Enter to confirm a choice.

Note that the CLI prompts you for much of the same setup information that a physical device’s setup web page does. For more information, see the *Firepower 7000 and 8000 Series Installation Guide*.

Note: To change any of these settings for a virtual device after you complete the initial setup, you must use the CLI. For more information, see the Command Line Reference chapter in the *Firepower Management Center Configuration Guide*.

Understanding Device Network Settings

The Firepower System provides a dual stack implementation for both IPv4 and IPv6 management environments. You must set the IPv4 or IPv6 management IP address, netmask or prefix length, and default gateway. You can also specify up to three DNS servers, as well as the host name and domain for the device. Note that the host name is not reflected in the syslog until after you reboot the device.

Understanding Detection Modes

The detection mode you choose for a virtual device determines how the system initially configures the device’s interfaces, and whether those interfaces belong to an inline set or security zone. The detection mode is not a setting you can change later; it is simply an option you choose during setup that helps the system tailor the device’s initial configurations. In general, you should choose a detection mode based on how your device is deployed.

Passive

Choose this mode if your device is deployed passively, as an intrusion detection system (IDS). In a passive deployment, virtual devices can perform network-based file and malware detection, and Security Intelligence monitoring, as well as network discovery.

Inline

Choose this mode if your device is deployed inline, as an intrusion prevention system (IPS).

Note: Although general practice in IPS deployments is to fail open and allow non-matching traffic, inline sets on virtual devices lack bypass capability.

Access Control

Choose this mode if your device is deployed inline as part of an access control deployment, that is, if you want to perform application, user, and URL control. A device configured to perform access control usually fails closed and blocks non-matching traffic. Rules explicitly specify the traffic to pass.

In an access control deployment, you can also perform advanced malware protection, file control, Security Intelligence filtering, and network discovery.

Network Discovery

Choose this mode if your device is deployed passively, to perform host, application, and user discovery only.

The following table lists the interfaces, inline sets, and zones that the system creates depending on the detection mode you choose.

Table 1 Initial Configurations Based on Detection Mode

Detection Mode	Security Zones	Inline Sets	Interfaces
Inline	Internal and External	Default Inline Set	first pair added to Default Inline Set—one to the Internal and one to the External zone
Passive	Passive	none	first pair assigned to Passive zone
Access Control	none	none	none
Network Discovery	Passive	none	first pair assigned to Passive zone

Note that security zones are a Firepower Management Center-level configuration which the system does not create until you actually add the device to the Firepower Management Center. At that time, if the appropriate zone (Internal, External, or Passive) already exists on the Firepower Management Center, the system adds the listed interfaces to the existing zone. If the zone does not exist, the system creates it and adds the interfaces. For detailed information on interfaces, inline sets, and security zones, see the *Firepower Management Center Configuration Guide*.

Procedure

1. Open the VMware console.
2. Log into the virtual device at the VMware console using `admin` as the username and the new admin account password that you specified in the deployment setup wizard.

   If you did not change the password using the wizard or you are deploying with a ESXi OVF template, use `Admin123` as the password.

   The device immediately prompts you to read the EULA.
3. Read and accept the EULA.
4. Change the password for the `admin` account. This account has the Configuration CLI access level, and cannot be deleted.

Note: Cisco recommends that you use a strong password that is at least eight alphanumeric characters of mixed case and includes at least one numeric character. Avoid using words that appear in a dictionary.

5. Configure network settings for the device. First configure (or disable) IPv4 management settings, then IPv6. If you manually specify network settings, you must:

   — Enter IPv4 addresses, including the netmask, in dotted decimal form. For example, you could specify a netmask of `255.255.0.0`.

   — Enter IPv6 addresses in colon-separated hexadecimal form. For an IPv6 prefix, specify the number of bits; for example, a prefix length of `112`.

   The VMware console may display messages as your settings are implemented.

6. Specify the detection mode based on how you deployed the device.

   The VMware console may display messages as your settings are implemented. When finished, the device reminds you to register this device to a Cisco Firepower Management Center, and displays the CLI prompt.

What to Do Next

- Continue with the next section, Registering a Virtual Device to a Cisco Firepower Management Center, page 18 to use the CLI to register the device to the Cisco Firepower Management Center that will manage it. You must manage devices with a Cisco Firepower Management Center. If you do not register the device now, you must log in later and register it before you can add it to a Cisco Firepower Management Center.

Registering a Virtual Device to a Cisco Firepower Management Center

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	NGIPSv	Any	Admin CLI Configuration

Because virtual devices do not have web interfaces, you must use the CLI to register a virtual device to a Cisco Firepower Management Center, which can be physical or virtual. It is easiest to register a device to its Firepower Management Center during the initial setup process, because you are already logged into the device’s CLI.

To register a device, use the `configure manager add` command. A unique self-generated alphanumeric registration key is always required to register a device to a Firepower Management Center. This is a simple key that you specify, and it is not the same as a license key.

In most cases, you must provide the Firepower Management Center’s IP address along with the registration key, for example:

```
configure manager add XXX.XXX.XXX.XXX my_reg_key
```

where *XXX.XXX.XXX.XXX* is the IP address of the managing Firepower Management Center and *my_reg_key* is the registration key you entered for the virtual device.

Note: When using the vSphere Client to register a virtual device to a Firepower Management Center, you must use the IP address (not the hostname) of the managing Firepower Management Center.

However, if the device and the Firepower Management Center are separated by a Network Address Translation (NAT) device, enter a unique NAT ID along with the registration key, and specify `DONTRESOLVE` instead of the IP address, for example:

```
configure manager add DONTRESOLVE my_reg_key my_nat_id
```

where *my_reg_key* is the registration key you entered for the virtual device and *my_nat_id* is the NAT ID of the NAT device.

If the device, rather than the Firepower Management Center, is behind a NAT device, enter a unique NAT ID along with the registration key, and specify the host name or IP address of the Firepower Management Center. For example:

```
configure manager add [hostname | ip address] my_reg_key my_nat_id
```

where `my_reg_key` is the registration key you entered for the virtual device and `my_nat_id` is the NAT ID of the NAT device.

Procedure

1. Log into the virtual device as a user with CLI Configuration (Administrator) privileges:
   - If you are performing the initial setup from the VMware console, you are already logged in as the `admin` user, which has the required access level.
   - Otherwise, log into the device using the VMware console, or, if you have already configured network settings for the device, SSH to the device's management IP address or host name.
2. At the prompt, register the device to a Cisco Firepower Management Center using the `configure manager add` command, which has the following syntax:

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} reg_key
[nat_id]
```

   where:
   - `{`*hostname* `|` *IPv4_address* `|` *IPv6_address* `| DONTRESOLVE}` specifies the IP address of the Firepower Management Center. If the Firepower Management Center is not directly addressable, use `DONTRESOLVE`.
   - *reg_key* is the unique alphanumeric registration key required to register a device to the Firepower Management Center.
   - *nat_id* is an optional alphanumeric string used during the registration process between the Cisco Firepower Management Center and the device. It is required if the hostname is set to `DONTRESOLVE`.
3. Log out of the appliance.

What to Do Next

- Log into its web interface and use the Device Management (**Devices > Device Management**) page to add the device if you have already set up the Firepower Management Center. For more information, see the Managing Devices chapter in the *Firepower Management Center Configuration Guide*.
- See the *Cisco Firepower Management Center Virtual Quick Start Guide for VMware* for a virtual Firepower Management Center, or see the *Cisco Firepower Management Center Installation Guide* for a physical Firepower Management Center if you have not already set up the Firepower Management Center.

Enabling VMware Tools

VMware Tools is a suite of utilities installed in the operating system of a virtual machine to enhance the performance of the virtual machine and to make possible many of the ease-of-use features of VMware products. The system supports the following plugins on all virtual appliances:

- guestInfo
- powerOps
- timeSync
- vmbackup

For more information on the supported plugins and full functionality of VMware Tools, see the VMware website (http://www.vmware.com/).

After you setup your virtual appliance, you can enable VMware Tools on your virtual appliances on your managed device using the command line interface (CLI).

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	NGIPSv	Any	Admin

You can log into the virtual device and enter one or more of the following commands:

- `show vmware-tools` displays whether VMware Tools are running on the system.
- `configure vmware-tools enable` </code> enables VMware Tools on the virtual device.
- `configure vmware-tools disable` disables VMware Tools on the virtual device.

To enable VMware Tools on a virtual device:

1. At the console, log into the virtual device and, at the CLI prompt, enter the appropriate command to enable or disable VMware Tools, or display whether VMware Tools is enabled, and press **Enter**.

Next Steps

After you complete the initial setup process for a virtual appliance and verify its success, Cisco recommends that you complete various administrative tasks that make your deployment easier to manage. You should also complete any tasks you skipped during the initial setup, such as device registration and licensing. For detailed information on any of the tasks described in the following sections, as well as information on how you can begin to configure your deployment, see the *Firepower Management Center Configuration Guide*.

Individual User Accounts

After you complete the initial setup, the only user on the system is the `admin` user, which has the Administrator role and access. Users with that role have full menu and configuration access to the system, including via the shell or CLI. Cisco recommends that you limit the use of the `admin` account (and the Administrator role) for security and auditing reasons.

Creating a separate account for each person who will use the system allows your organization not only to audit actions and changes made by each user, but also to limit each person’s associated user access role or roles. This is especially important on the Cisco Firepower Management Center, where you perform most of your configuration and analysis tasks. For example, an analyst needs access to event data to analyze the security of your network, but may not require access to administrative functions for the deployment.

The system includes ten predefined user roles designed for a variety of administrators and analysts. You can also create custom user roles with specialized access privileges.

Health and System Policies

By default, all appliances have an initial system policy applied. The system policy governs settings that are likely to be similar for multiple appliances in a deployment, such as mail relay host preferences and time synchronization settings. Cisco recommends that you use the Firepower Management Center to apply the same system policy to itself and all the devices it manages.

By default, the Firepower Management Center also has a health policy applied. A health policy, as part of the health monitoring feature, provides the criteria for the system continuously monitoring the performance of the appliances in your deployment. Cisco recommends that you use the Firepower Management Center to apply a health policy to all the devices it manages.

Software and Database Updates

You should update the system software on your appliances before you begin any deployment. Cisco recommends that all the appliances in your deployment run the most recent version of the Firepower System. If you are using them in your deployment, you should also install the latest intrusion rule updates, VDB, and GeoDB.

Caution: Before you update any part of the Firepower System, you must read the release notes or advisory text that accompanies the update. The release notes provide important information, including supported platforms, compatibility, prerequisites, warnings, and specific installation and uninstallation instructions.