Cisco Firepower Threat Defense Virtual Using Firepower Device Manager for KVM Deployment Quick Start Guide

Version 6.2.3 and greater

First Published: March 29, 2018

Last Updated: June 22, 2018

You can deploy the Firepower Threat Defense Virtual with Firepower Device Manager using the Kernel-based Virtual Machine (KVM) hypervisor.

About Deployment Using KVM

KVM is a full virtualization solution for Linux on x86 hardware containing virtualization extensions (such as Intel VT). It consists of a loadable kernel module, kvm.ko, that provides the core virtualization infrastructure and a processor specific module, such as kvm-intel.ko.

You can run multiple virtual machines running unmodified OS images using KVM. Each virtual machine has private virtualized hardware: a network card, disk, graphics adapter, and so forth.

The Firepower Threat Defense Virtual on KVM supports the following:

- Processors
  - Requires 4 vCPUs
- Memory
  - Requires 8GB RAM
- Networking
  - Requires two management interfaces and two data interfaces to boot

  Note: The Firepower Threat Defense Virtual default configuration puts the management interface and inside interface on the same subnet.
  - Supports virtio drivers

  - Supports a total of 10 interfaces
- Host storage per Virtual Machine
  - Firepower Threat Defense Virtual requires 50GB
  - Supports virtio block devices
- Console
  - Supports terminal server via telnet

Guidelines and Limitations

- The Firepower Threat Defense Virtual **must be powered up on firstboot with at least four interfaces**.
- The Firepower Threat Defense Virtual on KVM supports a total of 10 interfaces—1 management interface, 1 diagnostic interface, and a maximum of 8 network interfaces for data traffic. The interface-to-network assignments must be ordered as follows:
  - 1. Management interface (required)
  - 2. Diagnostic interface (required)
  - 3. Inside interface (required)
  - 4. Outside interface (required)
  - 5-10 Data interfaces (optional)
- If you deploy the Firepower Threat Defense Virtual in an OpenStack environment, you need to run with promiscuous mode and disable port security (i.e packet filtering). When doing so it is important to remember that port security cannot be disabled if a security group or allowed address pairs are assigned to an interface. Once port level security is disabled, all traffic (Ingress and Egress) will be allowed.
- Cloning a virtual machine is not supported.

Prerequisites for the Firepower Threat Defense Virtual, Firepower Device Manager, and KVM

- Download the Firepower Threat Defense Virtual qcow2 file from Cisco.com and put it on your Linux host:

  https://software.cisco.com/download/navigator.html

  Note: A Cisco.com login and Cisco service contract are required.
- You must install a new image (version 6.2.3 or greater) to get Firepower Device Manager support. You cannot upgrade an existing virtual machine from an older version and then switch to Firepower Device Manager.
- Firepower Device Manager (local manager) is enabled by default.

  Note: When you choose **Yes** for **Enable Local Manager**, the **Firewall Mode** is changed to **routed**. This is the only supported mode when using Firepower Device Manager.
- For the purpose of the sample deployment in this document, we are assuming you are using Ubuntu 14.04 LTS. Install the following packages on top of the Ubuntu 14.04 LTS host:
  - qemu-kvm
  - libvirt-bin
  - bridge-utils
  - virt-manager

  - virtinst
  - virsh tools
  - genisoimage
- Performance is affected by the host and its configuration. You can maximize the throughput of the Firepower Threat Defense Virtual on KVM by tuning your host. For generic host-tuning concepts, see Network Function Virtualization: Quality of Service in Broadband Remote Access Servers with Linux and Intel Architecture.
- Useful optimizations for Ubuntu 14.04 LTS include the following:
  - macvtap—High performance Linux bridge; you can use macvtap instead of a Linux bridge.

    Note: You must configure specific settings to use macvtap instead of the Linux bridge.
  - Transparent Huge Pages—Increases memory page size and is on by default in Ubuntu 14.04.
  - Hyperthread disabled—Reduces two vCPUs to one single core.
  - txqueuelength—Increases the default txqueuelength to 4000 packets and reduces drop rate.
  - pinning—Pins qemu and vhost processes to specific CPU cores; under certain conditions, pinning is a significant boost to performance.
- For information on optimizing a RHEL-based distribution, see Red Hat Enterprise Linux6 Virtualization Tuning and Optimization Guide.
- For KVM and Firepower System compatibility, see Cisco Firepower Threat Defense Virtual Compatibility.

License Requirements

Your purchase of a Firepower Threat Defense device or Firepower Threat Defense Virtual automatically includes a Base license. All additional licenses (Threat, Malware, or URL Filtering) are optional. For more information about Firepower Threat Defense licensing, see the “Licensing the System” chapter of the *Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager*.

Prepare the Day 0 Configuration File

You can prepare a Day 0 configuration file before you launch the Firepower Threat Defense Virtual. This file is a text file that contains the initial configuration data that gets applied at the time a virtual machine is deployed. This initial configuration is placed into a text file named “day0-config” in a working directory you choose, and is manipulated into a day0.iso file that is mounted and read on first boot.

Note: The day0.iso file must be available during first boot.

If you deploy with a Day 0 configuration file, the process allows you to perform the entire initial setup for Firepower Threat Defense Virtual appliance. You can specify:

- EULA acceptance
- A host name for the system
- A new administrator password for the admin account
- The initial firewall mode
- Network settings that allow the appliance to communicate on your management network
- The managing Cisco Firepower Management Center

If you deploy without a Day 0 configuration file, you must configure Firepower System-required settings after launch; see Launch Without the Day 0 Configuration File, page 10 for more information.

Note: We are using Linux in this example, but there are similar utilities for Windows.

Procedure

1. Enter the CLI configuration for the Firepower Threat Defense Virtual in a text file called “day0-config”. Add network settings and information about the managing Firepower Management Center.

   Example:

   ```
   #Firepower Threat Defense on KVM
   {
       "EULA": "accept",
       "Hostname": "ftdv-kvm-production",
       "AdminPassword": "Admin123",
       "FirewallMode": "routed",
       "DNS1": "1.1.1.1",
       "DNS2": "1.1.1.2",
       "DNS3": "",
       "IPv4Mode": "manual",
       "IPv4Addr": "10.12.129.44",
       "IPv4Mask": "255.255.0.0",
       "IPv4Gw": "10.12.0.1",
       "IPv6Mode": "disabled",
       "IPv6Addr": "",
       "IPv6Mask": "",
       "IPv6Gw": "",
       "FmcIp": "",
       "FmcRegKey": "",
       "FmcNatId": "",
       "ManageLocally":"Yes"
   }
   ```

   Note: Enter **Yes** for **ManageLocally** in your Day 0 configuration file, and leave the Firepower Management Center fields (**FmcIp**, **FmcRegKey**, and **FmcNatId)** empty.

2. Generate the virtual CD-ROM by converting the text file to an ISO file:

   ```
   /usr/bin/genisoimage -r -o day0.iso day0-config
   ```

   or

   ```
   /usr/bin/mkisofs -r -o day0.iso day0-config
   ```

3. Repeat to create unique default configuration files for each Firepower Threat Defense Virtual you want to deploy.

What To Do Next

- If using virt-install, add the following line to the virt-install command:

  ```
  --disk path=/home/user/day0.iso,format=iso,device=cdrom \
  ```

- If using virt-manager, you can create a virtual CD-ROM using the virt-manager GUI; see Launch Using Virtual Machine Manager, page 6.

Launch the Firepower Threat Defense Virtual

Launch Using a Deployment Script

You can use a virt-install based deployment script to launch the Firepower Threat Defense Virtual.

Be aware that you can optimize performance by selecting the best guest caching mode for your environment. The cache mode in use will affect whether data loss occurs, and the cache mode can also affect disk performance.

Each KVM guest disk interface can have one of the following cache modes specified: *writethrough*, *writeback*, *none*, *directsync*, or *unsafe*. *writethrough* provides read caching. *writeback* provides read and write caching. *directsync* bypasses the host page cache. *unsafe* may cache all content and ignore flush requests from the guest.

Cache Mode Guidelines

- A *cache=writethrough* will help reduce file corruption on KVM guest machines when the host experiences abrupt losses of power. We recommend that you use *writethrough* mode.
- However, *cache=writethrough* can also affect disk performance due to more disk I/O writes than *cache=none*.
- If you remove the *cache* parameter on the *--disk* option, the default is *writethrough*.
- Not specifying a cache option may also significantly reduce the time required for the VM creation. This is due to the fact that some older RAID controllers have poor disk caching capability. Hence, disabling disk caching (*cache=none*) and thus defaulting to *writethrough*, helps ensure data integrity.

Procedure

1. Create a virt-install script called “virt_install_ftdv.sh”.

   The name of the Firepower Threat Defense Virtual VM must be unique across all other virtual machines (VMs) on this KVM host.

   Note: The Firepower Threat Defense Virtual on KVM supports a total of 10 interfaces—1 management interface, 1 diagnostic interface, and a maximum of 8 network interfaces for data traffic. The virtual NIC must be Virtio. The interface-to-network assignments must be ordered as follows:

   - 1. Management interface (required)
   - 2. Diagnostic interface (required)
   - 3. Data interface (required)
   - 4. Data interface (required)
   - 5-10 Data interfaces (optional)

```
virt-install \
   --connect=qemu:///system \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --name=ftdv \
   --arch=x86_64 \
   --cpu host \
   --vcpus=4 \
   --ram=8192 \
   --os-type=linux \
   --os-variant=virtio26 \
```

```
--virt-type=kvm \
--import \
--watchdog i6300esb,action=reset \
--disk path=<ftd_filename>.qcow2,format=qcow2,device=disk,bus=virtio,
  cache=writethrough \
--disk path==<day0_filename>.iso,format=iso,device=cdrom \
--console pty,target_type=serial \
--serial tcp,host=127.0.0.1:<port>,mode=bind,protocol=telnet \
--force
```

2. Run the virt_install script:

```
/usr/bin/virt_install_ftdv.sh

Starting install...
Creating domain...
```

A window appears displaying the console of the VM. You can see that the VM is booting. It takes a few minutes for the VM to boot. Once the VM stops booting, you can issue CLI commands from the console screen.

What to Do Next

- Configure the device using Firepower Device Manage; see How to Configure the Device in Firepower Device Manager, page 11.

Launch Using Virtual Machine Manager

Use virt-manager, also known as Virtual Machine Manager, to launch the Firepower Threat Defense Virtual. virt-manager is a graphical tool for creating and managing guest virtual machines.

1. Start virt-manager (**Applications > System Tools > Virtual Machine Manager**).

   You may be asked to select the hypervisor and/or enter your root password.
2. Click the button in the top left corner to open the **New VM** wizard.
3. Enter the virtual machine details:
   a. Specify a **Name**.
   b. For the operating system, select **Import existing disk image**.

      This method allows you to import a disk image (containing a pre-installed, bootable operating system) to it.
   c. Click **Forward** to continue.
4. Load the disk image:
   a. Click **Browse...** to select the image file.
   b. Choose *Linux* for the **OS type**.
   c. Choose *Generic 2.6.25 or later kernel with virtio* for the **Version**.
   d. Click **Forward** to continue.
5. Configure the memory and CPU options:
   a. Set **Memory (RAM)** to *8192*.
   b. Set **CPUs** to *4*.
   c. Click **Forward** to continue.

6. Check the **Customize configuration before install** box first before you click **Finish**.

   Doing so opens another wizard that allows you to add, remove, and configure the virtual machine's hardware settings.

7. Modify the CPU configuration:

   From the left panel, select **Processor**, then select **Configuration > Copy host CPU configuration**.

   This applies the physical host's CPU model and configuration to your virtual machine.

8. Configure the Virtual Disk:
   a. From the left panel, select **Disk 1**.
   b. Select **Advanced options**.
   c. Set the **Disk bus** to *Virtio*.
   d. Set the **Storage format** to *qcow2*.
9. Configure a serial console:
   a. From the left panel, select **Console**.
   b. Select **Remove** to remove the default console.
   c. Click **Add Hardware** to add a serial device.
   d. For **Device Type**, select *TCP net console (tcp)*.
   e. For Mode, select Server mode (bind).
   f. For **Host**, enter the IP address and **Port** number.
   g. Check the **Use Telnet** box.
   h. Configure device parameters.
10. Configure a watchdog device to automatically trigger some action when the KVM guest hangs or crashes:
    a. Click **Add Hardware** to add a watchdog device.
    b. For **Model**, select *default*.
    c. For **Action**, select *Forcefully reset the guest*.
11. Configure at least 4 virtual network interfaces:
    a. Click **Add Hardware** to add an interface.
    b. For **Source device**, select *macvtap*.
    c. For **Device model**, select *virtio*.
    d. For **Source mode**, select *Bridge*.

    Note: The Firepower Threat Defense Virtual on KVM supports a total of 10 interfaces—1 management interface, 1 diagnostic interface, and a maximum of 8 network interfaces for data traffic. The interface-to-network assignments must be ordered as follows:

    – 1. Management interface (required)
    – 2. Diagnostic interface (required)

- 3. Inside interface (required)
- 4. Outside interface (required)
- 5-10 Data interfaces (optional)

12. If deploying using a Day 0 configuration file, create a virtual CD-ROM for the ISO:
    a. Click **Add Hardware**.
    b. Select **Storage**.
    c. Click **Select managed or other existing storage** and browse to the location of the ISO file.
    d. For **Device type**, select *IDE CDROM*.
13. After configuring the virtual machine's hardware, click **Apply**.
14. Click **Begin installation** for virt-manager to create the virtual machine with your specified hardware settings.

What to Do Next

- Configure the device using Firepower Device Manage; see How to Configure the Device in Firepower Device Manager, page 11.

Launch Using OpenStack

You can deploy the Firepower Threat Defense Virtual in an OpenStack environment. OpenStack is a set of software tools for building and managing cloud computing platforms for public and private clouds, and is tightly integrated with the KVM hypervisor.

Note: If you deploy the Firepower Threat Defense Virtual in an OpenStack environment, you need to run with promiscuous mode and disable port security (i.e packet filtering). When doing so it is important to remember that port security cannot be disabled if a security group or allowed address pairs are assigned to an interface. Once port level security is disabled, all traffic (Ingress and Egress) will be allowed.

About the Day 0 Configuration File on OpenStack

OpenStack supports providing configuration data via a special configuration drive (config-drive) that is attached to the instance when it boots. To deploy a Firepower Threat Defense Virtual instance with Day 0 configuration using the nova boot command, include the following line:

```
--config-drive true --file day0-config=/home/user/day0-config \
```

When the *--config-drive* command is enabled, the file *=/home/user/day0-config*, as found on the Linux filesystem where the nova client is invoked, is passed to the virtual machine on a virtual CDROM.

Note: While the VM may see this file with the name *day0-config*, OpenStack typically stores the file contents as /openstack/content/xxxx where xxxx is an assigned four-digit number (e.g. /openstack/content/0000). This may vary by OpenStack distribution.

Launch Using the Command Line

Use the **nova boot** command to create and boot a Firepower Threat Defense Virtual instance.

Procedure

1. Boot a Firepower Threat Defense Virtual instance using image, flavor, interface and Day 0 configuration information.

The Firepower Threat Defense Virtual can support up to 10 network interfaces. This example uses four interfaces.

Note: The Firepower Threat Defense Virtual requires a minimum of four interfaces to launch: two management interfaces and two traffic interfaces.

```
local@maas:~$ nova boot \
  --image=6883ee2e-62b1-4ad7-b4c6-cd62ee73d1aa \
  --flavor=a6541d78-0bb3-4dc3-97c2-7b87f886b1ba \
  --nic net-id=5bf6b1a9-c871-41d3-82a3-2ecee26840b1 \
  --nic net-id=ae638375-d0d1-4f1e-a93d-6e621e5fabd2 \
  --nic net-id=e9cedefd-178e-41a8-9c47-4e1feaa48477
  --nic net-id=f8b8dd2d-c8cc-452e-98f3-9542dddc7965 \
  --config-drive true --file day0-config=/home/local/day0-config \
```

Launch Using the OpenStack Dashboard

Horizon is an OpenStack Dashboard, which provides a web-based user interface to OpenStack services including Nova, Swift, Keystone, and so forth.

Before You Begin

- Download the Firepower Threat Defense Virtual qcow2 file from Cisco.com and put it on your local MAAS server:

  https://software.cisco.com/download/navigator.html

  Note: A Cisco.com login and Cisco service contract are required.

Procedure

1. On the Log In page, enter your user name and password, and click **Sign In**.

   The visible tabs and functions in the dashboard depend on the access permissions, or roles, of the user you are logged in as.

2. Select **Admin > System Panel > Flavor** from the menu.

   Virtual hardware templates are called *flavors* in OpenStack, and define sizes for RAM, disk, number of cores, and so on. This procedure creates a flavor for your Firepower deployments.

3. Enter the required information in the **Flavor Info** window:
   a. **Name**—Enter a descriptive name that easily identifies the instance. For example, *FTD-FMC-4vCPU-8GB*.
   b. **VCPUs**—Set VCPUs to 4.
   c. **RAM MB**—Set RAM to 8192.
4. Select **Create Flavor**.
5. Select **Admin > System Panel > Images** from the menu.
6. Enter the required information in the **Create An Image** window:
   a. **Name**—Enter a name that easily identifies the image. For example, *FTD-Version-Build*.
   b. **Description**—(Optional) Enter a description for this image file.
   c. **Browse**—Select the Firepower Threat Defense Virtual qcow2 file previously downloaded from Cisco.com.
   d. **Format**—Select *QCOW2-QEMU Emulator* as the format type.

e. Check the **Public** box.

7. Select **Create Image**.

   View the newly created Image.

8. Select **Project > Compute > Instances** from the menu.
9. Click **Launch Instance**.
10. Enter the required information in the **Launch Instance > Details** tab:

    a. **Instance Name**—Enter a name that easily identifies the instance. For example, *FTD-Version-Build*.

    b. **Flavor**—Select the flavor created earlier in Step 3. Enter a description for this image file.

    c. **Instance Boot Source**—Select *Boot from image*.

    d. **Image Name**—Select the image created earlier in Step 6.

11. From the **Launch Instance > Networking** tab, select a management network and data networks for the Firepower Threat Defense Virtual instance.

    Note: The Firepower Threat Defense Virtual requires a minimum of four interfaces to launch: two management interfaces and two traffic interfaces.

12. Click **Launch**.

    The instance starts on a compute node in the cloud. View the newly created instance from the **Instances** window.

13. Select the Firepower Threat Defense Virtual instance.
14. Select the **Console** tab.
15. Log into the virtual appliance at the console.

What to Do Next

- Configure the device using Firepower Device Manage; see How to Configure the Device in Firepower Device Manager, page 11.

Launch Without the Day 0 Configuration File

Because Firepower Threat Defense Virtual appliances do not have web interfaces, you must set up a virtual device using the CLI if you deployed without a Day 0 configuration file.

When you first log into a newly deployed 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 firewall 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: To change any of these settings for a virtual device after you complete the initial setup, you must use the CLI;

Procedure

1. Open a console to the Firepower Threat Defense Virtual.
2. At the **firepower login** prompt, log in with the default credentials of *username* **admin** and the *password* **Admin123**.
3. When the Firepower Threat Defense system boots, a setup wizard prompts you for the following information required to configure the system:

- Accept EULA
- New admin password
- IPv4 or IPv6 configuration
- IPv4 or IPv6 DHCP settings
- Management port IPv4 address and subnet mask, or IPv6 address and prefix
- System name
- Default gateway
- DNS setup
- HTTP proxy
- Management mode (local management required)

4. Review the Setup wizard settings. Defaults or previously entered values appear in brackets. To accept previously entered values, press **Enter**.
5. Complete the system configuration as prompted.
6. Verify the setup was successful when the console returns to the firepower **#** prompt.
7. Close the CLI:

   ```
   > exit
   ```

What to Do Next

- Configure the device using Firepower Device Manage; see How to Configure the Device in Firepower Device Manager, page 11.

How to Configure the Device in Firepower Device Manager

After you complete the setup wizard, you should have a functioning device with a few basic policies in place:

- Security zones for the inside and outside interfaces.
- An access rule trusting all inside to outside traffic.
- A interface NAT rule that translates all inside to outside traffic to unique ports on the IP address of the outside interface.
- A DHCP server running on the inside interface or bridge group.

The following steps provide an overview of additional features you might want to configure. Please click the help button (**?**) on a page to get detailed information about each step.

Procedure

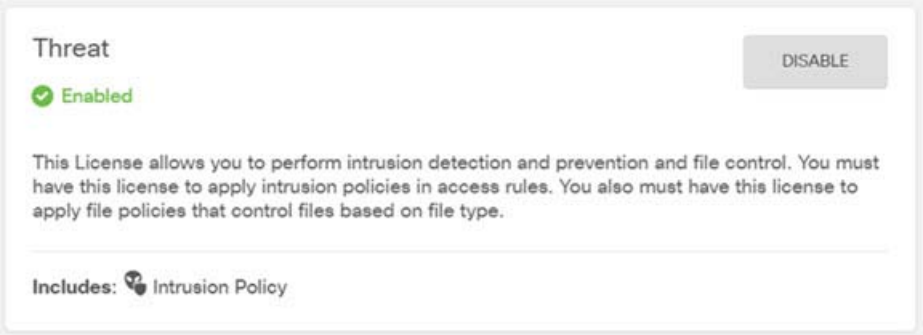
1. Choose **Device**, then click **View Configuration** in the **Smart License** group.

   The Firepower Threat Defense Virtual default configuration puts the management interface and inside interface on the same subnet. You must have Internet connectivity on the management interface in order to use Smart Licensing and to obtain updates to system databases.

   Click **Enable** for each of the optional licenses you want to use: Threat, Malware, URL. If you registered the device during setup, you can also enable the RA VPN license desired. Read the explanation of each license if you are unsure of whether you need it.

If you have not registered, you can do so from this page. Click **Request Register** and follow the instructions. Please register before the evaluation license expires.

For example, an enabled Threat license should look like the following:



2. The Firepower Threat Defense Virtual default configuration is designed so that you can connect both the Management0/0 and GigabitEthernet0/1 (inside) to the same network on the virtual switch. Choose **Device**, then click **View Configuration** in the **Interfaces** group to configure additional interfaces.

   The default management address uses the inside IP address as the gateway. Thus, the management interface routes through the inside interface, then through the outside interface, to get to the Internet.

   Note: You also have the option of attaching Management0/0 to a different subnet than the one used for the inside interface, as long as you use a network that has access to the Internet. Ensure that you configure the management interface IP address and gateway appropriately for the network.

   Note that the management interface IP configuration is defined on **Device > System Settings > Management Interface**. It is not the same as the IP address for the Management0/0 (diagnostic) interface listed on **Device > Interfaces > View Configuration**.

   Click the edit icon ( )for each interface to define the IP address and other settings. Click **Save** when you are finished.

3. If you configured new interfaces, choose **Objects**, then select **Security Zones** from the table of contents.

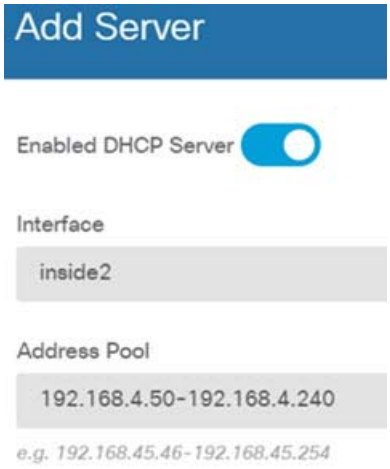
   Edit or create new zones as appropriate. Each interface must belong to a zone, because you configure policies based on security zones, not interfaces. You cannot put the interfaces in zones when configuring them, so you must always edit the zone objects after creating new interfaces or changing the purpose of existing interfaces.

   The following example shows how to create a new dmz-zone for the dmz interface.

4. If you want internal clients to use DHCP to obtain an IP address from the device, choose **Device** > **System Settings** > **DHCP Server**, then select the **DHCP Servers** tab.

   There is already a DHCP server configured for the inside interface, but you can edit the address pool or even delete it. If you configured other inside interfaces, it is very typical to set up a DHCP server on those interfaces. Click + to configure the server and address pool for each inside interface.

   You can also fine-tune the WINS and DNS list supplied to clients on the **Configuration** tab. The following example shows how to set up a DHCP server on the inside2 interface with the address pool 192.168.4.50-192.168.4.240.



5. Choose **Device**, then click **View Configuration** (or **Create First Static Route**) in the **Routing** group and configure a default route.

   The default route normally points to the upstream or ISP router that resides off the outside interface. A default IPv4 route is for any-ipv4 (0.0.0.0/0), whereas a default IPv6 route is for any-ipv6 (::0/0). Create routes for each IP version you use. If you use DHCP to obtain an address for the outside interface, you might already have the default routes that you need.

   Note: The routes you define on this page are for the data interfaces only. They do not impact the management interface. Set the management gateway on **Device** > **System Settings** > **Management Interface**.

The following example shows a default route for IPv4. In this example, isp-gateway is a network object that identifies the IP address of the ISP gateway (you must obtain the address from your ISP). You can create this object by clicking **Create New Network** at the bottom of the **Gateway** drop-down list.

6. Choose **Policies** and configure the security policies for the network.

   The device setup wizard enables traffic flow between the inside-zone and outside-zone, and interface NAT for all interfaces when going to the outside interface. Even if you configure new interfaces, if you add them to the inside-zone object, the access control rule automatically applies to them.

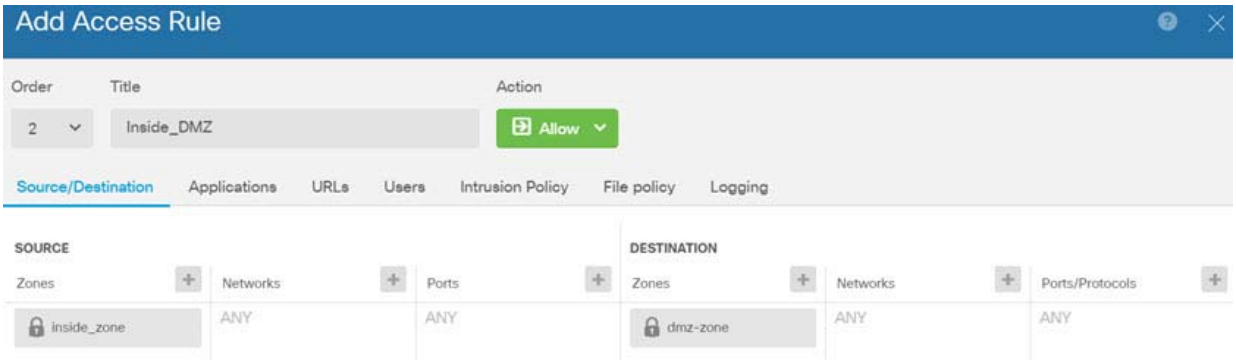
   However, if you have multiple inside interfaces, you need an access control rule to allow traffic flow from inside-zone to inside-zone. If you add other security zones, you need rules to allow traffic to and from those zones. These would be your minimum changes.

   In addition, you can configure other policies to provide additional services, and fine-tune NAT and access rules to get the results that your organization requires. You can configure the following policies:

   - **SSL Decryption**—If you want to inspect encrypted connections (such as HTTPS) for intrusions, malware, and so forth, you must decrypt the connections. Use the SSL decryption policy to determine which connections need to be decrypted. The system re-encrypts the connection after inspecting it.
   - **Identity**—If you want to correlate network activity to individual users, or control network access based on user or user group membership, use the identity policy to determine the user associated with a given source IP address.
   - **Security Intelligence**—Use the Security Intelligence policy to quickly drop connections from or to blacklisted IP addresses or URLs. By blacklisting known bad sites, you do not need to account for them in your access control policy. Cisco provides regularly updated feeds of known bad addresses and URLs so that the Security Intelligence blacklist updates dynamically. Using feeds, you do not need to edit the policy to add or remove items in the blacklist.
   - **NAT** (Network Address Translation)—Use the NAT policy to convert internal IP addresses to externally routeable addresses.

- **Access Control**—Use the access control policy to determine which connections are allowed on the network. You can filter by security zone, IP address, protocol, port, application, URL, user or user group. You also apply intrusion and file (malware) policies using access control rules. Use this policy to implement URL filtering.
- **Intrusion**—Use the intrusion policies to inspect for known threats. Although you apply intrusion policies using access control rules, you can edit the intrusion policies to selectively enable or disable specific intrusion rules.

The following example shows how to allow traffic between the inside-zone and dmz-zone in the access control policy. In this example, no options are set on any of the other tabs except for **Logging**, where **At End of Connection** is selected.



7. Choose **Device**, then click **View Configuration** in the **Updates** group and configure the update schedules for the system databases.

   If you are using intrusion policies, set up regular updates for the Rules and VDB databases. If you use Security Intelligence feeds, set an update schedule for them. If you use geolocation in any security policies as matching criteria, set an update schedule for that database.

8. Click the **Deploy** button in the menu, then click the Deploy Now button( ), to deploy your changes to the device.

   Changes are not active on the device until you deploy them.

What to Do Next

- For complete information about managing the Firepower Threat Defense Virtual using the Firepower Device Manager, see the *Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager*, or the Firepower Device Manager online help.