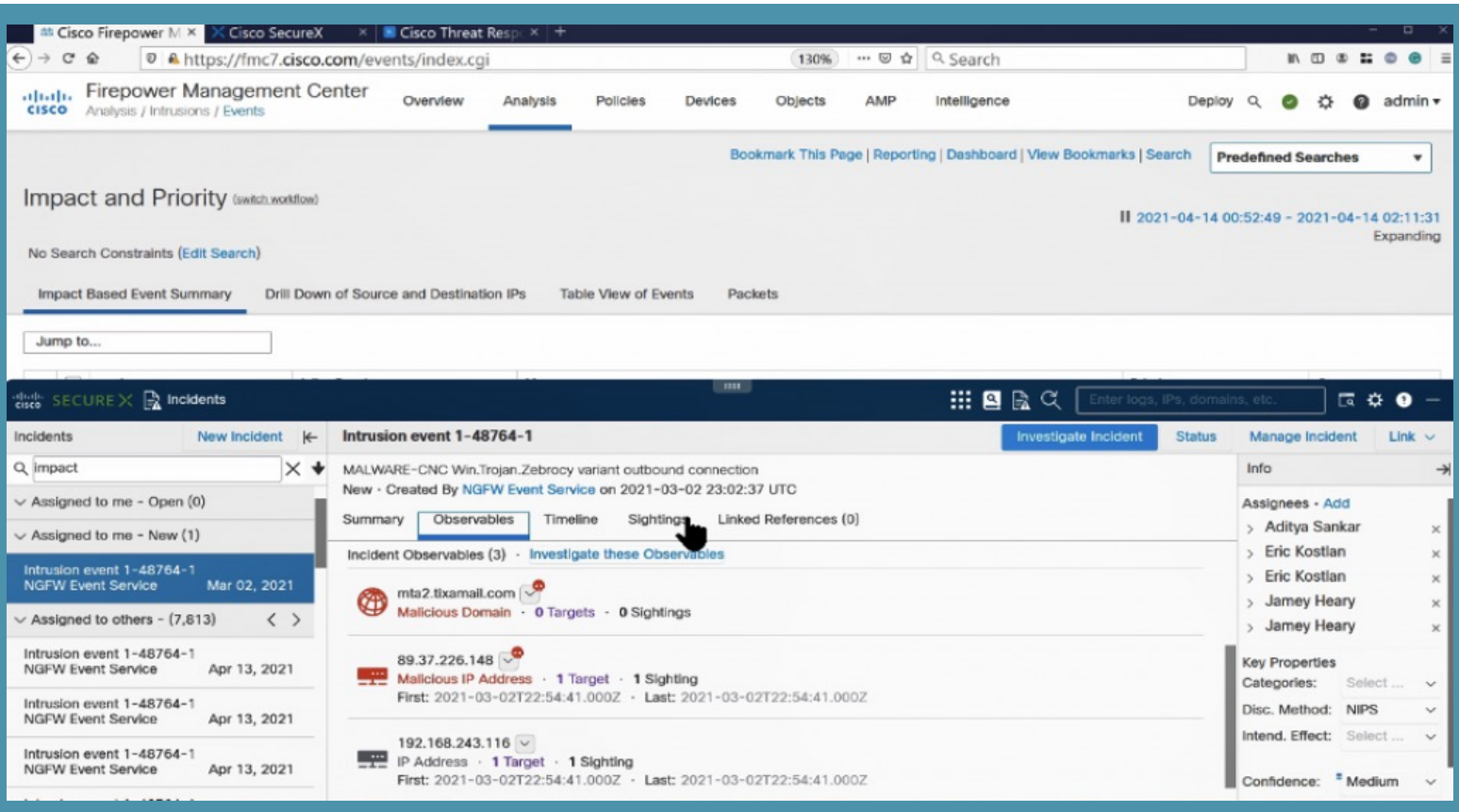
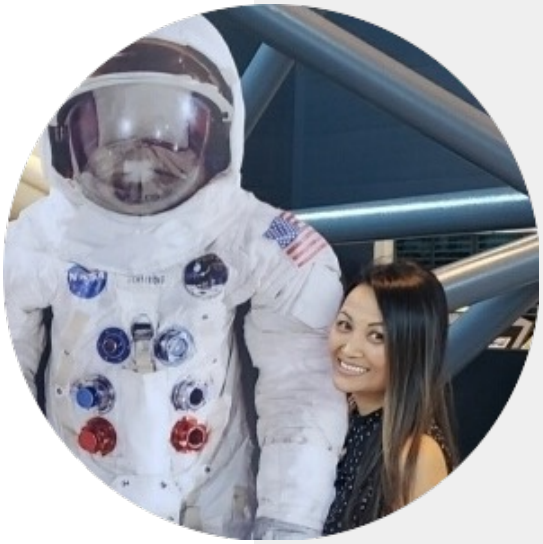
accendnetworks®

Cisco Secure Firewall Threat Defense and Management Center Deployment Guide

All-in-One Guide for Initial virtual deployment of Cisco Secure Firewall Threat Defense and Management Center Using VMware



About the Author



Paula Wong

CEO and Founder, CCIE#13062, Speaker, Trainer, Senior Security Architect/Engineer, C-7#1086962

An IT veteran with over 27+ years, worked previously for Cisco Security TAC, Cisco Advanced Services, Webex, Salesforce, Expedia/Hotwire, and other fortune 500 companies.

@accendnetworks @paulawong

Table of Contents

1

Chapter One

Introduction

Chapter One

Introduction

This Ebook will cover the initial configuration steps needed for deploying the virtual appliance using VMware for following:

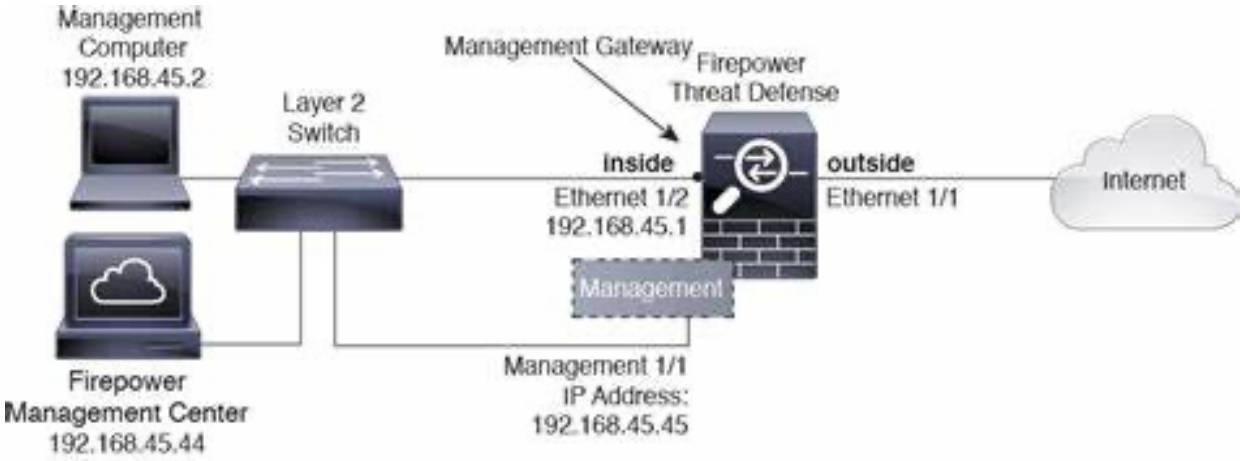
- **Cisco Secure Threat Defense**
- **Cisco Secure Firewall Management Center**

We will then cover the initial steps to get the threat defense added to management center by providing the following:

- **Initial configuration for threat defense via CLI**
- **Registering your threat defense in the management center**

At the end, you will have a functional and working Cisco Secure Threat Defense and Firewall Management Center.

**The exact order may not be the same as above.*



Deploy the Threat Defense Virtual on VMware

We will focus on just deploying the 64-bit threat defense virtual device Version 7.0 and later for VMware vSphere vCenter and ESXi hosting environments.

You can deploy the threat defense virtual to any x86 device that is capable of running VMware ESXi. You should be familiar with VMware and vSphere, including vSphere networking, ESXi host setup and configuration, and virtual machine guest deployment prior to deploying this.

Feature	Description	Support	Comment
vMotion	Used for live migration of VMs	Yes	Use shared storage. See vMotion Support
Suspend and resume	The VM is suspended, then resumed.	Yes	
VMware vSphere Standalone Windows Client	Used to deploy VMs	Yes	
VMware vSphere Web Client	Used to deploy VMs	Yes	

Threat Defense Virtual Appliance Resource Requirements

Settings	Value
Performance Tiers	**Version 7.0 and later** Throughput levels and VPN connection limits deployment requirements: • FTDv5 4vCPU/8GB (100Mbps) • FTDv100 4vCPU/8GB (1Gbps) • FTDv20 4vCPU/8GB (3Gps) • FTDv30 8vCPU/12GB (5GPs) • FTDv50 12vCPU/24GB (10GPs) • FTDv100 16vCPU/32GB (16Gbps) See "Licensing" chapter in Cisco Secure Firewall Management Center Admin Guide for more guidelines on licensing. **Note** To change the vCPU/memory values, the threat defense virtual device must first be power off.
Storage	Based on Disk Format selection • Thin Provision disk size is 48.24GB

Deploy the Threat Defense Virtual on Vmware (contd)

Threat Defense Virtual Appliance Resource Requirements

Settings	Value
vNICs	The threat defense virtual supports the following virtual network adapters: • **VMXNET3** • **IXGBE** • **E1000** **Important:** For versions earlier than 6.4, the e1000 was the default interface for threat defense on VMware. Starting with release 6.4, threat defense virtual on VMware defaults to vmxnet3 interfaces. If your virtual device is currently using e1000 interfaces, it is **strongly recommended** that you use vmxnet3. See Configure VMXNET3 interfaces for more information. • IXGBE-VF

There are other interface settings, deployment guidelines and detailed steps for deploying the OVF file can be found below:

Cisco Secure Firewall Threat Defense Virtual Getting Started Guide, Version 7.2 and Earlier

Note: See the section on completing the setup using the CLI by opening the VMware console and at **the firepower login**, enter the default username **admin** and **Admin123** and go through the wizard to do the following:

- Accept EULA
- New admin password
- IPv4 configuration
- IPv4 DHCP settings
- Management for IPv4 address and subnet mask
- System name
- Default gateway
- DNS setup
- HTTP proxy
- Management mode (local management uses the device manager). You want to answer No for Enable Local Manager so that it can be managed via the Management Center.

Initial Configuration for the Threat Defense

Now you can start to configure the Threat Defense via the CLI so that it can be added to Management Center. Below are the steps needed:

Procedure

Step 1 Connect to the threat defense CLI, either from the console port or using SSH to the Management interface, which obtains an IP address from a DHCP server by default. If you intend to change the network settings, we recommend using the console port so you do not get disconnected.

The console port connects to the FXOS CLI. The SSH session connects directly to the threat defense CLI.

Step 2 Log in with the username **admin** and the password **Admin123**.

Example:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin.
You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Initial Configuration for the Threat Defense (contd)

Step 3. If you connected to FXOS on the console port, connect to the threat defense CLI.

connect ftd

Example:

```
firepower# connect ftd >
```

Step 4. You are then asked to accept the EuLA, and enter the network configuration information such IPv4 address, if you want to manage the Threat Defense via locally or via the Management Center, Answer No to use the Management Center:

Initial Configuration for the Threat Defense (contd)

Example:

You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]
Please enter 'YES' or press <ENTER> to AGREE to the EULA:
System initialization in progress. Please stand by.
You must change the password for 'admin' to continue.
Enter new password: ********
Confirm new password: ********
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: **10.10.10.15**
Enter an IPv4 netmask for the management interface [255.255.255.0]: **255.255.255.192**
Enter the IPv4 default gateway for the management interface [data-interfaces]: **10.10.10.1**
Enter a fully qualified hostname for this system [firepower]: **ftd-1.cisco.com**
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'
Manage the device locally? (yes/no) [yes]: **no**

Initial Configuration for the Threat Defense (contd)

Manage the device locally? (yes/no) [yes]: **no**
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ..

Update policy deployment information
- add device configuration
- add network discovery
- add system policy

You can register the sensor to a Firepower Management Center and use the Firepower Management Center to manage it. Note that registering the sensor to a Firepower Management Center disables on-sensor Firepower Services management capabilities.

When registering the sensor to a Firepower Management Center, a unique alphanumeric registration key is always required. In most cases, to register a sensor to a Firepower Management Center, you must provide the hostname or the IP address along with the registration key. 'configure manager add [hostname | ip address] [registration key]'

However, if the sensor and the Firepower Management Center are separated by a NAT device, you must enter a unique NAT ID, along with the unique registration key. 'configure manager add DONTRESOLVE [registration key] [NAT ID]'

Later, using the web interface on the Firepower Management Center, you must use the same registration key and, if necessary, the same NAT ID when you add this sensor to the Firepower Management Center.

Initial Configuration for the Threat Defense (contd)

Step 5

Identify the management center that will manage this threat defense.
configure manager
add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *reg_key* [*nat_id*]

Example:

- **configure manager add MC.example.com 123456**

Manager successfully configured.

Initial Configuration for the Threat Defense (contd)

If the management center is behind a NAT device, enter a unique NAT ID along with the registration key, and specify DONTRESOLVE instead of the hostname, for example:

Example:

- **configure manager add DONTRESOLVE regk3y78 natid90**

Manager successfully configured.

If the threat defense is behind a NAT device, enter a unique NAT ID along with the management center IP address or hostname, for example:

Example:

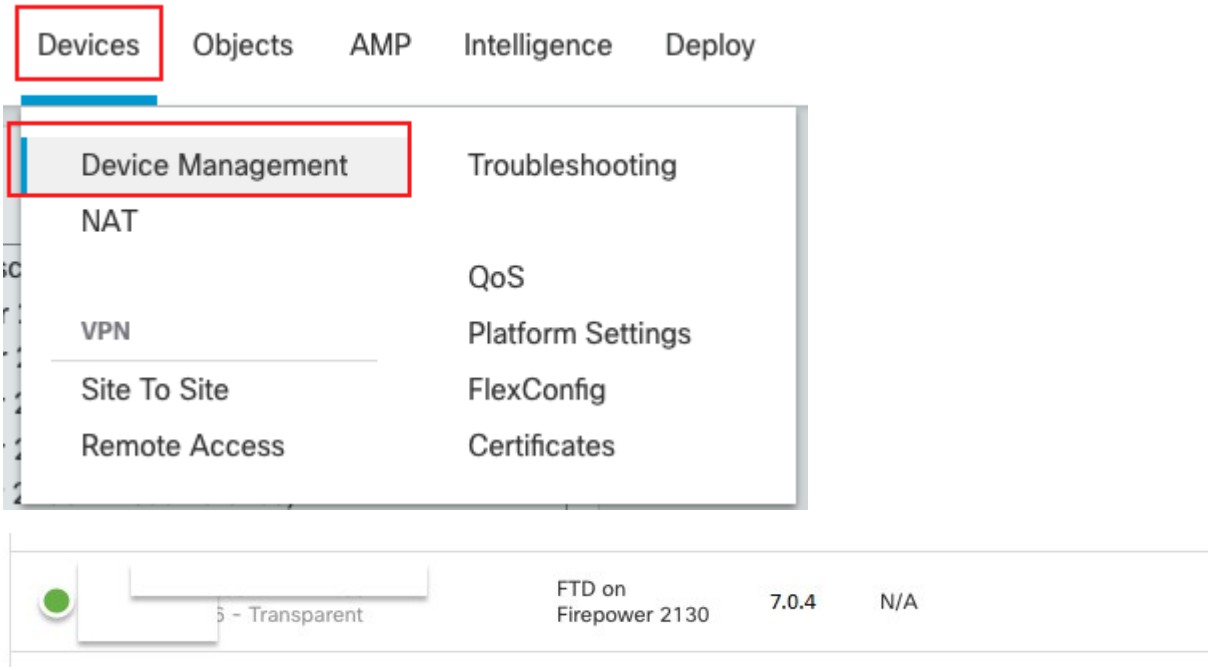
- **configure manager add 10.70.45.5 regk3y78 natid56**

Manager successfully configured.

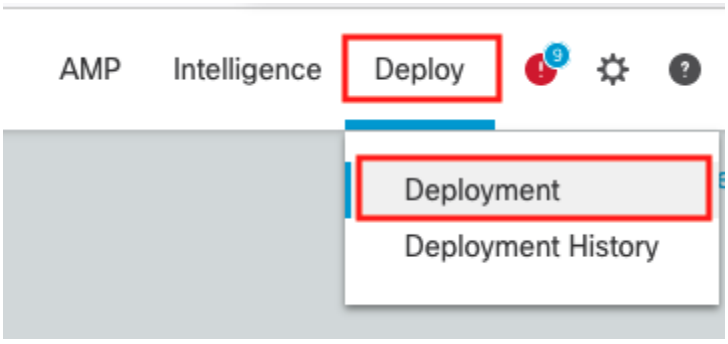
See page 20 to register your firewall to the management center.

Upgrade Firepower Threat Defense with FMC

7. **Verify upgrade success.**
   - After the upgrade completes, choose Devices > Device Management and confirm that the devices you upgraded have the correct software version.



8. **Redeploy configurations to the devices you just upgraded.**
   - Deploy -> Deployment -> Select device -> Deploy



Contact Us!

We provided a complete initial guide for :

- Deploying the Cisco Secure Threat Defense Virtual Appliance
- Completing initial steps for adding to the management center
- Deploying the Cisco Secure Management Center Virtual Appliance
- Completing initial steps for the management center
- Registering the threat defense to the management center
- Configure a basic security policy

We offer efficient and advanced network security training, workshops, and custom services with easy to follow guide.

Contact Us Today!

accendnetworks®

www.accendnetworks.com

accendnetworks®

Contact Us Today!

For any questions, customer training or workshops, or if you need assistance with your Cisco Secure Threat Deployment or Cisco Secure Management Center deployment Projects, reach out to us by one of the methods below:

Paula Wong, CEO/Founder, CCIE #13062, PNCSE, C-7#1086962
Email: paula@accendnetworks.com
Phone: 408-784-2345 Local / 855-8ACCEND (822-8363) Toll Free

We love helping our customers!
Reach out today!