Radware DefensePro Service Chain for Firepower Threat Defense Quick Start Guide

First Published: December 20, 2016
Last Updated: June 14, 2018

1. About Radware DefensePro Service Chaining for Firepower Threat Defense

The Cisco FXOS chassis can support multiple services (for example, a Firepower Threat Defense firewall, and a third-party DDoS application) on a single blade. These applications can be linked together to form a Service Chain. In Firepower eXtensible Operating System (FXOS) 2.1.1 and later on the Firepower 4120, 4140, 4150, and 9300 security appliances, the third-party Radware DefensePro virtual platform can be installed to run in front of ASA or Firepower Threat Defense. Radware DefensePro is a KVM-based virtual platform that provides distributed denial-of-service (DDoS) detection and mitigation capabilities on the FXOS chassis. When Service Chaining is enabled on your FXOS chassis, ingress traffic from the network must first pass through the DefensePro virtual platform before reaching Firepower Threat Defense.

You can deploy Radware DefensePro with Firepower Threat Defense in the following modes:

- Standalone
- Intra-chassis cluster
- Active/Standby failover

Note: Service Chaining is not supported in an inter-chassis cluster configuration. However, the Radware DefensePro (vDP) application can be deployed in a standalone configuration in an inter-chassis cluster scenario. The DefensePro application can run as separate instances on up to three security modules.

Note:

- The Radware DefensePro virtual platform may be referred to as Radware vDP (virtual DefensePro), or simply vDP.
- The Radware DefensePro application may occasionally be referred to as a Link Decorator.

Licensing Requirements for the Radware DefensePro Service Chain

Licensing for the Radware Virtual DefensePro application on Firepower 4100 and Firepower 9300 series security appliances is handled through the Radware APSolute Vision Manager. Go to the Cisco Commerce Workspace (CCW) to order a throughput license for your device. After submitting this request, you will receive a login and link to the Radware Portal, where you can then request a license.

For more information and documentation on Radware's APSolute Vision Manager and throughput licensing requirements, see the documentation on Radware's site (htttps://portals.radware.com/Customer/Home/Downloads/Management-Monitoring/?Product=APSolute-Vision). Note that you must be registered with Radware to access this portal.

Timezone Sync Requirements

Prior to deploying Radware vDP on your Firepower security appliance, you must ensure that your Chassis Manager is set to use an NTP Server, with the etc/UTC Time Zone.

Procedure

1. In the Firepower Chassis Manager, choose **Platform Settings** to open the **NTP** area in the **Platform Settings** page.
2. Choose **etc/UTC** in the **Time Zone** drop-down list.
3. Under **Set Time Source**, select **Use NTP Server**:
4. Enter the IP address or hostname of the NTP server you want to use in the **NTP Server** field.
5. Click **Save**.

For more information about setting the date and time in your Firepower chassis, see the "Setting the Date and Time" topic in the *Cisco FXOS CLI Configuration Guide* or *Cisco FXOS Firepower Chassis Manager Configuration Guide* (http://www.cisco.com/go/firepower9300-config).

APSolute Vision Manager Version Requirements

Radware APSolute Vision is the main management interface for vDP. In order for the APSolute Vision manager to support the full functionality offered by vDP and Firepower Threat Defense service chain integration, you must be on APSolute Vision version R3.40 or later.

Note: HTTPS management of Radware DefensePro requires APSolute Vision Manager. To manage Radware DefensePro locally without APSolute Vision Manager, you must use the FXOS CLI.

2. Deploy and Configure Radware vDP in a Service Chain

Before You Begin

- If the security module that you want to use for the logical device already has a logical device configured on it, you must first delete the existing logical device (see Delete a Logical Device).
- Download the vDP image from Cisco.com (see Downloading Images from Cisco.com) and then download that image to the FXOS chassis (see Downloading a Logical Device Software Image to the FXOS chassis).

Configure a Management Interface and Data Interfaces

Configure a Management-type interface on the supervisor that you can include in the deployment configuration for the Firepower Threat Defense logical device and vDP decorator. You must also configure at least one Data-type interface.

Procedure

1. In the Firepower Chassis Manager, choose **Interfaces** to open the Interfaces page.
2. To add an EtherChannel:
   a. Click **Add Port Channel**.
   b. For the Port Channel ID, enter a value between 1 and 47.
   c. Leave **Enable** checked.
   d. For the Type, choose **Management** or **Data**. You can only include one management interface per logical device. Do not choose **Cluster**.
   e. Add member interfaces as desired.
   f. Click **OK**.
3. For a single interface:
   a. Click the **Edit** icon in the interface row to open the Edit Interface dialog box.
   b. Check **Enable**.
   c. For the Type, click **Management** or **Data**. You can only include one management interface per logical device.
   d. Click **OK**.

Deploy a Standalone Firepower Threat Defense Logical Device with a Radware DefensePro Service Chain

The following procedure shows how to install the Radware DefensePro image, and configure it in a Service Chain in front of a Firepower Threat Defense standalone logical device.

Note: If you are installing Radware DefensePro on Firepower Threat Defense on a Firepower 4110 or 4120 device, you must deploy the decorator at the same time as the logical device. You cannot install the decorator after the logical device is already configured on the device. For more information, see Create a Standalone Threat Defense Logical Device in the Cisco FXOS Firepower Chassis Manager Configuration Guide.

1. Create a standalone Threat Defense logical device (see Create a Standalone Threat Defense Logical Device in the Cisco FXOS Firepower Chassis Manager Configuration Guide).
2. In the FXOS CLI, enter security services mode:

   ```
   scope ssa
   ```

3. Install the Radware vDP image on the same slot that the Firepower Threat Defense is installed on:

   ```
   scope slot_id
   create app-instance vdp
   ```

4. Commit the configuration:

   ```
   commit-buffer
   ```

5. Verify the installation and provisioning of vDP on the security module:

   ```
   show app-instance
   ```

6. (Optional) Show the available supported resource profiles:

   ```
   Firepower /ssa/app # show app-resource-profile
   ```

Example:

```
Firepower /ssa/app # show app-resource-profile
Profile Name Security Model Number of Cores RAM Size (MB) Default Profile
------------------------ -------------- --------------- ---------------
---------------
DEFAULT-4110-RESOURCE FPR4K-SM-12 4 16384 Yes
DEFAULT-RESOURCE FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44,
FPR4K-SM-36,
FPR4K-SM-24
6 24576 Yes
VDP-10-CORES FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44,
FPR4K-SM-36,
FPR4K-SM-24
```

7. (Optional) Set the resource profile, using one of the available profiles from the previous step:
   a. Scope to slot 1:

      ```
      Firepower /ssa*# scope slot 1
      ```

   b. Enter the DefensePro application instance:

      ```
      Firepower /ssa/slot* # enter app-instance vdp
      ```

   c. Enable the application instance:

      ```
      Firepower /ssa/slot/app-instance* # enable
      ```

   d. Set the resource profile:

      ```
      Firepower /ssa/slot/app-instance* # set resource-profile-name resource_profile_name
      ```

   e. Commit the configuration:

      ```
      Firepower /ssa/slot/app-instance* # commit-buffer
      ```

8. After the vDP application is in an Online state, access the logical device:

   ```
   Firepower /ssa # scope logical-device device_name
   ```

9. Enter the Firepower Threat Defense logical device:

   ```
   scope ssa
   scope logical-device ld_ftd
   ```

10. Assign the management interface to vDP. You can use the same physical interface as for the logical device, or you can use a separate interface.

    ```
    Firepower /ssa/logical-device # enter external-port-link name interface_id vdp
    Firepower /ssa/logical-device/external-port-link* # exit
    ```

11. Configure the external management for vDP:
    a. Create bootstrap object:

       create mgmt-bootstrap vdp

    b. Configure management IP address:

       create ipv4 *slot_id* **default**

    c. Set gateway address:

       set gateway *gateway_address*

    d. Set IP address and mask:

```
set ip ip_address mask network mask
```

e. Exit management IP configuration scope:

```
exit
```

f. Exit management bootstrap configuration scope:

```
exit
```

12. Create external port link:

```
create external-port-link mgmt_vdp interface_id vdp
```

13. Scope external port:

```
scope external-port-link port
```

14. Add the third-party application to the logical device:

```
set decorator vdp
exit
exit
```

15. Verify whether the third-party application is set for the interface:

```
show logical-device
```

16. Commit the configuration:

```
commit-buffer
```

17. Set a password for the DefensePro application. Note that the application does not come online until you set a password. For more information, see the Radware DefensePro DDoS Mitigation User Guide on cisco.com.

Deploy a Firepower Threat Defense Cluster with a Radware DefensePro Service Chain

The following procedure shows how to install the Radware DefensePro image, and configure it in a Service Chain in front of a Firepower Threat Defense intra-chassis cluster.

Note: Service Chaining is not supported in an inter-chassis cluster configuration. However, the Radware DefensePro (vDP) application can be deployed in a standalone configuration in an inter-chassis cluster scenario.

1. Configure Firepower Threat Defense cluster (see Configure Firepower Threat Defense Clustering in the Cisco FXOS Firepower Chassis Manager Configuration Guide).

2. Decorate external (client-facing) port with Radware DefensePro:

```
enter external-port-link name interface_name ftd
set decorator vdp
set description ''''
exit
```

3. Assign the external management port for Firepower Threat Defense:

```
enter external-port-link mgmt_ftd interface_name ftd
set decorator ''''
set description ''''
exit
```

4. Assign the external management port for DefensePro:

```
enter external-port-link mgmt_vdp interface_name ftd
set decorator ''''
set description ''''
exit
```

5. Optional) Show the available supported resource profiles:

```
Firepower /ssa/app # show app-resource-profile
```

Example:

```
Firepower /ssa/app # show app-resource-profile
Profile Name Security Model Number of Cores RAM Size (MB) Default Profile
------------------------ -------------- --------------- ---------------
---------------
DEFAULT-4110-RESOURCE FPR4K-SM-12 4 16384 Yes
DEFAULT-RESOURCE FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44,
FPR4K-SM-36,
FPR4K-SM-24
6 24576 Yes
VDP-10-CORES FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44,
FPR4K-SM-36,FPR4K-SM-24
```

6. (Optional) Set the resource profile, using one of the available profiles from the previous step:

   a. Scope to slot 1:

   ```
   Firepower /ssa*# scope slot 1
   ```

   b. Enter the DefensePro application instance:

   ```
   Firepower /ssa/slot* # enter app-instance vdp
   ```

   c. Enable the application instance:

   ```
   Firepower /ssa/slot/app-instance* # enable
   ```

   d. Set the resource profile:

   ```
   Firepower /ssa/slot/app-instance* # set resource-profile-name resource_profile_name
   ```

   e. Commit the configuration:

   ```
   Firepower /ssa/slot/app-instance* # commit-buffer
   ```

7. Configure cluster port channel:

```
enter external-port-link port-channel48 Port-channel48 ftd
set decorator ''''
set description ''''
exit
```

8. Configure management bootstrap for all three DefensePro instances:

```
enter mgmt-bootstrap vdp
enter ipv4 slot_id default
set gateway gateway_address
set ip ip_address mask network_mask
exit
```

For example:

```
enter mgmt-bootstrap vdp
    enter ipv4 1 default
        set gateway 172.16.0.1
        set ip 172.16.4.219 mask 255.255.0.0
    exit
    enter ipv4 2 default
        set gateway 172.16.0.1
        set ip 172.16.4.220 mask 255.255.0.0
```

```
exit
enter ipv4 3 default
    set gateway 172.16.0.1
    set ip 172.16.4.221 mask 255.255.0.0
exit
```

9. Exit management bootstrap configuration scope:

```
exit
```

10. On the master blade, set the management IP and enable clustering:

```
device clustering management-channel ip
device clustering master set management-channel ip
device clustering state set enable
```

11. Commit the configuration:

```
commit-buffer
```

12. Set a password for the DefensePro application. Note that the application does not come online until you set a password. For more information, see the Radware DefensePro DDoS Mitigation User Guide on cisco.com.

13. After completing this procedure, you must verify whether the DefensePro instances are configured in a cluster. To do so, scope the DefensePro instance and show the application attributes to verify which DefensePro instance is primary, and which one is secondary:

```
scope ssa
scope slot_number
scope app-instance vdp
show app-attri
```

If the DefensePro application is online but not yet formed in a cluster, the CLI displays:

```
App Attribute:
    App Attribute Key: cluster-role
    Value: unknown
```

If the system displays this "unknown" value, you must enter the DefensePro application and configure the master IP address to create the vDP cluster.

If the DefensePro application is online and formed in a cluster, the CLI displays:

```
App Attribute:
    App Attribute Key: cluster-role
    Value: primary/secondary
```

Full Procedure Example

```
scope ssa
  enter logical-device ld ftd "1,2,3" clustered
     enter cluster-bootstrap
         set chassis-id 1
         set ipv4 gateway 172.16.0.1
         set ipv4 pool 172.16.4.216 172.16.4.218
         set ipv6 gateway 2010::2
         set ipv6 pool 2010::21 2010::26
         set key secret
         set mode spanned-etherchannel
         set name cisco
         set virtual ipv4 172.16.4.222 mask 255.255.0.0
         set virtual ipv6 2010::134 prefix-length 64
     exit
     enter external-port-link Ethernet1-2 Ethernet1/2 ftd
         set decorator vdp
```

```
            set description ""
        exit
        enter external-port-link Ethernet1-3_ftd Ethernet1/3 ftd
            set decorator ""
            set description ""
        exit
        enter external-port-link mgmt_ftd Ethernet1/1 ftd
            set decorator ""
            set description ""
        exit
        enter external-port-link mgmt_vdp Ethernet1/1 vdp
            set decorator ""
            set description ""
        exit
        enter external-port-link port-channel48 Port-channel48 ftd
            set decorator ""
            set description ""
        exit
        enter mgmt-bootstrap vdp
            enter ipv4 1 default
                set gateway 172.16.0.1
                set ip 172.16.4.219 mask 255.255.0.0
            exit
            enter ipv4 2 default
                set gateway 172.16.0.1
                set ip 172.16.4.220 mask 255.255.0.0
            exit
            enter ipv4 3 default
                set gateway 172.16.0.1
                set ip 172.16.4.221 mask 255.255.0.0
            exit
     exit
    commit-buffer
    scope ssa
       scope slot 1
       scope app-instance vdp
       show app-attri
```

3. Enable vDP Web Services

In order for APSolute Vision to manage the Virtual DefensePro application deployed on the FXOS chassis, you must enable the vDP web interface.

Procedure

1. From the FXOS CLI, connect to the vDP application instance.

   connect module *slot* **console**
   connect vdp

2. Use the given username and password (radware/radware) to log into the DefensePro application instance.
3. Enable vDP web services:

   manage secure-web status set enable

4. Exit the vDP application console and return to the FXOS module CLI.

   Ctrl]

4. Open UDP/TCP Ports

The Radware APSolute Vision Manager interfaces communicate with the Radware vDP application with various UDP/TCP ports. In order for the vDP application to communicate with the APSolute Vision Manager, you must ensure that these ports are accessible and not blocked by your firewall. For more information on which specific ports to open, see the following tables in the APSolute Vision User Guide:

- **Ports for APSolute Vision Server-WBM Communication and Operating System**
- **Communication Ports for APSolute Vision Server with Radware Devices**

5. Where to Go Next

- You can find links to all FXOS, Firepower 4100, and Firepower 9300 documentation at Navigating the Cisco FXOS Documentation.
- You can find links to all Firepower Threat Defense documentation at Cisco Firepower System Documentation Roadmap.
- Download the **Radware DefensePro DDoS Mitigation User Guide**, available at http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-installation-and-configuration-guides-list.html
- Download the **Radware DefensePro DDoS Mitigation Release Notes**, available at http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-installation-and-configuration-guides-list.html
- For more information and documentation on Radware's APSolute Vision Manager, see the documentation portal on Radware's site (https://portals.radware.com/Customer/Home/Downloads/Management-Monitoring/?Product=APSolute-Vision). Note that you must be registered with Radware to access this portal.