适用于 Firepower 威胁防御解决方案的 Radware DefensePro 服务链快速入门指南

首次发布日期：2016 年 12 月 20 日
最后更新日期：2018 年 6 月 14 日

1. 关于适用于 Firepower 威胁防御解决方案的 Radware DefensePro 服务链

思科 FXOS 机箱可在单个刀片上支持多个服务（例如，Firepower 威胁防御防火墙和第三方 DDoS 应用）。这些应用可以链接在一起形成服务链。在 Firepower 4120、4140、4150 和 9300 安全设备上的 Firepower 可扩展操作系统 (FXOS) 2.1.1 及更高版本中，可以安装第三方 Radware DefensePro 虚拟平台，在 ASA 或 Firepower 威胁防御解决方案外部运行。Radware DefensePro 是基于 KVM 的虚拟平台，可在 FXOS 机箱中提供分布式拒绝服务 (DDoS) 检测和规避功能。当在 FXOS 机箱中启用服务链时，来自网络的入口流量必须先通过 DefensePro 虚拟平台，才能到达 Firepower 威胁防御解决方案。

您可以采用以下模式部署 Radware DefensePro 和 Firepower 威胁防御解决方案：

- 独立式
- 机箱内集群
- 主用/备用故障切换

注意：服务链在机箱间集群配置中不受支持。但是，Radware DefensePro (vDP) 应用可在机箱间集群场景中采用独立配置进行部署。DefensePro 应用可以作为单独实例在最多三个安全模块上运行。

注意：

- Radware DefensePro 虚拟平台可以称为 Radware vDP（虚拟 DefensePro），或者简称为 vDP。
- Radware DefensePro 应用有时可能是指链路修饰器。

Radware DefensePro 服务链的许可要求

在 Firepower 4100 和 Firepower 9300 系列安全设备中，Radware 虚拟 DefensePro 应用的许可由 Radware APSolute Vision 管理器处理。转至思科商务工作空间 (CCW) 为您的设备订购吞吐量许可证。提交此请求后，您将收到 Radware 门户的登录信息和链接，然后您就可在此门户中申请许可证。

有关 Radware APSolute Vision 管理器和吞吐量许可要求的详细信息和文档，请参阅 Radware 网站上的文档 (https://portals.radware.com/Customer/Home/Downloads/Management-Monitoring/?Product=APSolute-Vision)。请注意，您必须注册 Radware 才能访问此门户。

时区同步要求

在 Firepower 安全设备上部署 Radware vDP 之前，您必须确保机箱管理器设置为使用时区为 etc/UTC 的 NTP 服务器。

程序

1. 在 Firepower 机箱管理器中，选择**平台设置**打开**平台设置**页面中的 **NTP** 区域。
2. 在**时区**下拉列表中选择**其他/UTC**。
3. 在**设置时间来源**下，选择**使用 NTP 服务器**：
4. 在 **NTP 服务器**字段中输入要使用的 NTP 服务的 IP 地址或主机名。
5. 点击**保存**。

有关在 Firepower 机箱中设置日期和时间的详细信息，请参阅《*思科 FXOS CLI 配置指南*》或《*思科 FXOS Firepower 机箱管理器配置指南*》(http://www.cisco.com/go/firepower9300-config) 中的“设置日期和时间”主题。

APSolute Vision 管理器版本要求

Radware APSolute Vision 是 vDP 的主管理界面。为使 APSolute Vision 管理器支持 vDP 和 Firepower 威胁防御服务链集成所提供的完整功能，您必须使用 APSolute Vision R3.40 或更高版本。

注意：要使用 Radware DefensePro 进行 HTTPS 管理，必须使用 APSolute Vision 管理器。要在不使用 APSolute Vision 管理器的情况下本地管理 Radware DefensePro，必须使用 FXOS CLI。

2. 在服务链中部署并配置 Radware vDP

准备工作

- 如果您想供逻辑设备使用的安全模块已配置有逻辑设备，必须首先删除现有的逻辑设备（请参阅“删除逻辑设备”）。
- 请从 Cisco.com 下载 vDP 映像（请参阅“从 Cisco.com 下载映像”），然后将该映像下载至 FXOS 机箱（请参阅“将逻辑设备软件映像下载至 FXOS 机箱”）。

配置管理接口和数据接口

在可以包括在 Firepower 威胁防御逻辑设备和 vDP 修饰器部署配置中的管理引擎上配置管理类型的接口。您还必须至少配置一个数据类型的接口。

程序

1. 在 Firepower 机箱管理器中，选择**接口**打开“接口”页面。
2. 添加一个 EtherChannel：
   a. 点击**添加端口通道**。
   b. 在“端口通道 ID”字段中，输入一个介于 1 和 47 之间的值。
   c. 选中**启用**。
   d. 对于“类型”，选择**管理**或**数据**。每个逻辑设备只能包括一个管理接口。请勿选择**集群**。

e. 根据需要添加成员接口。

f. 点击**确定**。

3. 对单个接口执行以下操作：

a. 点击接口行中的**编辑**图标，打开“编辑接口”对话框。

b. 选中**启用**。

c. 对于“类型”，点击**管理**或**数据**。每个逻辑设备只能包括一个管理接口。

d. 点击**确定**。

在 Radware DefensePro 服务链中部署独立的 Firepower 威胁防御逻辑设备

以下程序显示如何安装 Radware DefensePro 映像，并在 Firepower 威胁防御独立逻辑设备之前的服务链中配置此映像。

注意：如果您要在 Firepower 4110 或 4120 设备上为 Firepower 威胁防御解决方案安装 Radware DefensePro，则必须与逻辑设备一同部署修饰器。在设备上配置了逻辑设备后，无法安装修饰器。有关详细信息，请参阅《思科 FXOS Firepower 机箱管理器配置指南》的创建独立的威胁防御逻辑设备部分。

1. 创建独立的威胁防御逻辑设备（请参阅《思科 FXOS Firepower 机箱管理器配置指南》的创建独立的威胁防御逻辑设备部分）。

2. 在 FXOS CLI 中，进入安全服务模式：

```
scope ssa
```

3. 在安装 Firepower 威胁防御解决方案的插槽上安装 Radware vDP 映像：

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

4. 提交配置：

```
commit-buffer
```

5. 验证 vDP 在安全模块上的安装和调配：

```
show app-instance
```

6. （可选）显示受支持的可用资源配置文件：

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

示例：

```
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. （可选）使用上一步中可用的配置文件之一设置资源配置文件：

   a. 确定插槽 1 的范围：

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

   b. 输入 DefensePro 应用实例：

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

   c. 启用应用实例：

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

   d. 设置资源配置文件：

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

   e. 提交配置：

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

8. vDP 应用处于在线状态后，访问逻辑设备：

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

9. 输入 Firepower 威胁防御逻辑设备：

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

10. 将管理接口分配给 vDP。您可以使用与逻辑设备相同的物理接口，也可以使用单独的接口。

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

11. 为 vDP 配置外部管理：

    a. 创建引导程序对象：

    create mgmt-bootstrap vdp

    b. 配置管理 IP 地址：

    create ipv4 *slot_id* **default**

    c. 设置网关地址：

    set gateway *gateway_address*

    d. 设置 IP 地址和掩码：

    set ip *ip_address* **mask** *network mask*

    e. 退出管理 IP 配置范围：

    exit

    f. 退出管理引导程序配置范围：

    exit

12. 创建外部端口链路：

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

13. 确定外部端口范围：

    scope external-port-link *port*

14. 向逻辑设备添加第三方应用：

```
set decorator vdp
exit
exit
```

15. 验证是否为接口设置了第三方应用：

```
show logical-device
```

16. 提交配置：

```
commit-buffer
```

17. 为 DefensePro 应用设置密码。请注意，在您完成密码设置之前，DefensePro 应用无法联网。有关更多信息，请参阅 Cisco.com 上的《Radware DefensePro DDoS 攻击缓解用户指南》。

在 Radware DefensePro 服务链中部署 Firepower 威胁防御集群

以下程序显示如何安装 Radware DefensePro 映像，并在 Firepower 威胁防御机箱内集群之前的服务链中配置此映像。

注意：服务链在机箱间集群配置中不受支持。但是，Radware DefensePro (vDP) 应用可在机箱间集群场景中采用独立配置进行部署。

1. 配置 Firepower 威胁防御集群（请参阅《思科 FXOS Firepower 机箱管理器配置指南》的配置 Firepower 威胁防御集群部分）。

2. 用 Radware DefensePro 修饰外部（面向客户端）端口：

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

3. 为 Firepower 威胁防御分配外部管理端口：

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

4. 为 DefensePro 分配外部管理端口：

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

5. （可选）显示受支持的可用资源配置文件：

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

示例：

```
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. （可选）使用上一步中可用的配置文件之一设置资源配置文件：

   a. 确定插槽 1 的范围：

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

   b. 输入 DefensePro 应用实例：

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

   c. 启用应用实例：

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

   d. 设置资源配置文件：

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

   e. 提交配置：

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

7. 配置集群端口通道：

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

8. 为所有的三个 DefensePro 实例配置管理引导程序：

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

   例如：

   ```
   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. 退出管理引导程序配置范围：

   ```
   exit
   ```

10. 在主刀片上，请设置管理 IP 并启用集群：

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

11. 提交配置：

    ```
    commit-buffer
    ```

12. 为 DefensePro 应用设置密码。请注意，在您完成密码设置之前，DefensePro 应用无法联网。有关更多信息，请参阅 Cisco.com 上的《Radware DefensePro DDoS 攻击缓解用户指南》。
13. 完成此程序后，必须验证是否已在集群中配置 DefensePro 实例。要达到此目的，您需要确定 DefensePro 实例的范围，并通过显示应用属性来确认主 DefensePro 实例和次要 DefensePro 实例的具体对象：

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

如果 DefensePro 应用在线，但尚未在集群中形成，CLI 将显示：

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

如果系统显示此“unknown”值，您必须进入 DefensePro 应用，配置主 IP 地址，创建 vDP 集群。

如果 DefensePro 应用已联网并在集群中形成，CLI 将显示：

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

完整程序示例

```
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. 启用 vDP Web 服务

为使 APSolute Vision 管理部署在 FXOS 机箱上的虚拟 DefensePro 应用，您必须启用 vDP 网络界面。

程序

1. 从 FXOS CLI 连接到 vDP 应用实例。

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

2. 使用给定用户名和密码 (radware/radware) 登录 DefensePro 应用实例。
3. 启用 vDP Web 服务：

   manage secure-web status set enable

4. 退出 vDP 应用控制台并返回 FXOS 模块 CLI。

   Ctrl]

4.打开 UDP/TCP 端口

Radware APSolute Vision 管理器接口使用各类 UDP/TCP 端口与 Radware vDP 应用进行通信。为使 vDP 应用与 APSolute Vision 管理器通信，您必须确保这些端口可访问，并且未被防火墙拦截。有关打开哪些特定端口的详细信息，请参阅《PSolute Vision 用户指南》中的以下表格：

- **APSolute Vision Server-WBM 通信和操作系统端口**
- **APSolute Vision 服务器与 Radware 设备的通信端口**

5. 后续步骤

- 您可以在思科 FXOS 文档导航页面中找到与 FXOS、Firepower 4100 和 Firepower 9300 相关的所有文档的链接。
- 您可以在思科 Firepower 系统文档规划图页面中找到与 Firepower 威胁防御解决方案相关的所有文档的链接。

- 下载**《Radware DefensePro DDoS 缓解用户指南》**，地址为：http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-installation-and-configuration-guides-list.html。
- 下载**《Radware DefensePro DDoS 缓解版本说明》**，地址为：http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-installation-and-configuration-guides-list.html。
- 有关 Radware APSolute Vision 管理器的详细信息和文档，请参阅 Radware 网站上的文档门户 (https://portals.radware.com/Customer/Home/Downloads/Management-Monitoring/?Product=APSolute-Vision)。请注意，您必须注册 Radware 才能访问此门户。