适用于 ASA 的 Radware DefensePro 服务链快速入门指南

首次发布日期：2016 年 1 月 27 日

最后更新日期：2017 年 3 月 11 日

1. 关于适用于 ASA 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， ASA 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) 1.1.4 及更高版本中，可以安装第三方 Radware DefensePro 虚拟平台，在 ASA 防火墙之外运行。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 机箱上启用服务链时，来自网络的入口流量必须先通过 DefensePro 虚拟平台，然后再到达 ASA 防火墙。

注意：

- 可以在独立配置中或在具有 ASA 防火墙的机箱内集群配置中启用 Radware DefensePro 服务链。
- DefensePro 应用可以作为单独实例在最多三个安全模块上运行。
- 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 ASA 防火墙的链路修饰器。

Radware DefensePro 服务链的许可要求

在 Firepower 4100 和 9300 系列设备中，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 站点中的文档 (htttps://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 (Platform Settings)** 可打开**平台设置 (Platform Settings)** 页面中的 **NTP** 区域。
2. 在**时区 (Time Zone)** 下拉列表中选择 **etc/UTC**。
3. 在**设置时间来源 (Set Time Source)** 下，选择**使用 NTP 服务器 (Use NTP Server)**：

4. 在 **NTP 服务器 (NTP Server)** 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 (Save)**。

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 ASA 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。

2. 在服务链中部署并配置 Radware vDP

您可以使用 Firepower 机箱管理器在独立 ASA 或 ASA 集群上部署 Radware DefensePro 服务链。有关 CLI 完整操作步骤，请参阅 《FXOS CLI 配置指南》。

准备工作

从 Cisco.com 下载 vDP 映像，然后将该映像上传到 FXOS 机箱。

配置管理接口和数据接口

在可以包括在 ASA 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 (Interfaces)** 打开 “接口” (Interfaces) 页面。
2. 添加一个 EtherChannel：
   a. 点击**添加端口通道 (Add Port Channel)**。
   b. 在 “端口通道 ID” (Port Channel ID) 字段中，输入一个介于 1 和 47 之间的值。
   c. 选中**启用 (Enable)**。
   d. 对于 “类型” (Type)，选择**管理 (Management)** 或**数据 (Data)**。每个逻辑设备只能包括一个管理接口。请勿选择**集群 (Cluster)**。
   e. 根据需要添加成员接口。
   f. 点击**确定 (OK)**。
3. 对单个接口执行以下操作：
   a. 点击接口行中的**编辑 (Edit)** 图标，打开 “编辑接口” (Edit Interface) 对话框。
   b. 选中**启用 (Enable)**。
   c. 对于 “类型” (Type)，点击**管理 (Management)** 或**数据 (Data)**。每个逻辑设备只能包括一个管理接口。
   d. 点击**确定 (OK)**。

部署具有 Radware DefensePro 服务链的独立 ASA

操作步骤

1. 选择**逻辑设备 (Logical Devices)** 打开 “逻辑设备” (Logical Devices) 页面。
2. 点击**添加设备 (Add Device)** 打开 “添加设备” (Add Device) 对话框。
3. 在**设备名称 (Device Name)** 字段中，为逻辑设备提供一个名称。
4. 对于**模板 (Template)**，选择 **asa**。
5. 在**映像版本 (Image Version)** 部分，选择 ASA 软件版本。
6. 在**设备模式 (Device Mode)** 中，点击**独立 (Standalone)** 单选按钮。
7. 点击**确定 (OK)**。屏幕将显示调配 - *设备名称* (Provisioning - *device name*) 窗口。
8. 展开**数据端口 (Data Ports)** 区域，然后点击要分配给 ASA 的每个接口。
9. 点击屏幕中心的设备图标。系统将显示 **ASA 配置 (ASA Configuration)** 对话框。
10. 按照提示配置部署选项。
11. 点击**确定 (OK)** 关闭 “ASA 配置” (ASA Configuration) 对话框。
12. 在 “修饰器” (Decorators) 区域中，选择 vDP。系统将显示 **Radware：虚拟 DefensePro - 配置 (Radware: Virtual DefensePro - Configuration)** 对话框。配置**常规信息 (General Information)** 选项卡下的以下字段。
13. 如果您已将多个 vDP 版本上传到 FXOS 机箱，请在**版本 (Version)** 下拉列表中选择要使用的版本。
14. 在**管理接口 (Management Interface)** 下拉列表下，选择您之前在此操作步骤中创建的管理接口。
15. 选择要使用的**地址类型 (Address Type)**：仅 IPv4。
16. 请根据您在上一步中选择的**地址类型 (Address Type)** 来配置以下字段。
    a. 在**管理 IP (Management IP)** 字段中，配置本地 IP 地址。
    b. 输入**网络掩码 (Network Mask)**。
    c. 输入**网络网关 (Network Gateway)** 地址。
17. 选中要分配给 vDP 修饰器的每个数据端口旁边的复选框。对于您选择的各个数据端口，所有入口流量将首先通过 vDP 修饰器后再到达 ASA。所有出口流量将首先通过 ASA 发送，然后再发送到 vDP。
18. 点击 **OK**。
19. 点击 **Save**。

    FXOS 机箱通过下载指定的软件版本，并将引导程序配置和管理接口设置推送到指定的安全模块来部署逻辑设备和 vDP 修饰器。

部署具有 Radware DefensePro 服务链的 ASA 集群

注意：在 Firepower 9300 上部署集群时，系统会自动创建端口通道 48，用于进行安全的模块间通信。要将 ASA 集群部署为集群控制链路，必须将集群配置在默认端口通道 （端口通道 48）上，而且不能有任何成员接口。

操作步骤

1. 选择**逻辑设备 (Logical Devices)** 打开 “逻辑设备” (Logical Devices) 页面。
2. 点击**添加设备 (Add Device)** 打开 “添加设备” (Add Device) 对话框。
3. 在**设备名称 (Device Name)** 字段中，为逻辑设备提供一个名称。
4. 对于**模板 (Template)**，选择 **asa**。

5. 在**映像版本 (Image Version)** 部分，选择 ASA 软件版本。
6. 在 **设备模式 (Device Mode)** 中，点击**集群 (Cluster)** 单选按钮。
7. 点击**创建新集群 (Create New Cluster)** 单选按钮。
8. 点击**确定 (OK)**。屏幕将显示调配 - *设备名称* (Provisioning - *device name*) 窗口。
9. 展开**数据端口 (Data Ports)** 区域，然后点击要分配给 ASA 的每个接口。
10. 点击屏幕中心的设备图标。系统将显示 **ASA 配置 (ASA Configuration)** 对话框。
11. 按照提示配置部署选项。
12. 点击**确定 (OK)** 关闭 “ASA 配置” (ASA Configuration) 对话框。

    注意：在**管理 IP 池 (Management IP Pool)** 字段中，通过输入以连字符分隔的开始和结束地址来配置本地 IP 地址池，其中一个地址将分配给接口的各集群设备。至少包含与集群中的设备数量相同的地址。如果计划扩展集群，则应包含更多地址。属于当前主设备的**虚拟 IP 地址 (Virtual IP address)**（称为主集群 IP 地址）不是此池的一部分；请务必在同一网络中为虚拟 IP 地址保留一个 IP 地址。
13. 在 “修饰器” (Decorators) 区域中，选择 **vDP**。系统将显示 **Radware：虚拟 DefensePro - 配置 (Radware: Virtual DefensePro - Configuration)** 对话框。配置**常规信息 (General Information)** 选项卡下的以下字段。
14. 如果您已将多个 vDP 版本上传到 FXOS 机箱，请在**版本 (Version)** 下拉列表中选择要使用的 vDP 版本。
15. 在**管理接口 (Management Interface)** 下拉列表下，选择管理接口。
16. 选中要分配给 vDP 修饰器的每个数据端口旁边的复选框。对于您选择的各个数据端口，所有入口流量将首先通过 vDP 修饰器后再到达 ASA。所有出口流量将首先通过 ASA 发送，然后再发送到 vDP。
17. 点击**接口信息 (Interface Information)** 选项卡。
18. 选择要使用的**地址类型 (Address Type)**：仅 IPv4。
19. 为每个安全模块配置以下字段。请注意，显示的字段取决于您在上一步中选择的**地址类型 (Address Type)**。
    a. 在**管理 IP (Management IP)** 字段中，配置本地 IP 地址。
    b. 输入**网络掩码 (Network Mask)**。
    c. 输入**网络网关 (Network Gateway)** 地址。
20. 点击 **OK**。
21. 点击 **Save**。

    FXOS 机箱通过下载指定的软件版本，并将引导程序配置和管理接口设置推送到指定的安全模块来部署逻辑设备和 vDP 修饰器。

验证是否在集群中配置了 DefensePro 实例

在 ASA 集群上安装 vDP 应用实例后，您必须验证是否已在集群中配置了 DefensePro 实例。

操作步骤

1. 选择**逻辑设备 (Logical Devices)** 打开 “逻辑设备” (Logical Devices) 页面。
2. 滚动已配置的逻辑设备列表至 vDP 条目。验证**管理 IP (Management IP)** 列中列出的属性。
   - 如果**集群角色 (CLUSTER-ROLE)** 元素针对 DefensePro 实例显示为未知 (unknown)，则您必须进入 DefensePro 应用并配置主 IP 地址来完成 vDP 集群的创建。为此，请遵循以下 **vDP 应用实例集群 (Cluster the vDP Application Instances)** 中详述的操作步骤。
   - 如果**集群角色 (CLUSTER-ROLE)** 元素针对 DefensePro 实例显示为 “主要” (primary) 或 “辅助” (secondary)，则说明应用在线，并且已在集群中形成。

vDP 应用实例集群

在 ASA 集群上安装 vDP 实例后，您必须进入 vDP CLI 将 vDP 实例集群。请注意，如果已经在独立配置中设置了 vDP 服务链，则无需执行这些步骤。

程序

1. 连接到 FXOS CLI。
2. 连接到 vDP 应用实例。

   connect module *slot* **console**
   connect vdp
3. 使用给定用户名和密码 (radware/radware) 登录 DefensePro 应用实例。
4. 显示 FXOS 平台分配给 vDP 实例的集群 IP。

   device clustering management-channel ip
5. 将主 IP 设置为所分配的此 IP。

   device clustering set *master ip*
6. 启用集群状态。

   device clustering state set enable
7. 退出 vDP 应用并返回 FXOS CLI。

   Ctrl]
8. 连接到下一个 vDP 应用实例。

   connect module *slot_2* **console**
   connect vdp
9. 将主 IP 设置为您在此操作步骤的步骤 4 和 5 中所发现和分配的集群 IP。

   device clustering set *master ip*
10. 启用集群状态。

    device clustering state set enable
11. 退出 vDP 应用并返回 FXOS CLI。

    Ctrl]
12. 在第三个 vDP 应用实例上重复步骤 8-11 （如果适用）。对全部三个 vDP 实例配置了主 IP 后，向第一个实例分配集群中的主集群角色，而向其他两个实例分配辅助集群角色。
13. 验证集群已配置。

    device clustering show
14. 退出 vDP 应用控制台并返回 FXOS 模块 CLI。

    Ctrl]

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 ASA 系列文档导航页面中找到与 ASA/ASDM 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。
- 有关 Radware APSolute Vision 管理器的详细信息和文档，请参阅 Radware 站点上的文档门户 (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。