Radware DefensePro サービス チェーン (Firepower Threat Defense 用) クイック スタート ガイド

初版:2016 年 12 月 20 日
最終更新日:2018 年 6 月 14 日

1. Firepower Threat Defense 用 Radware DefensePro サービス チェーンについて

Cisco FXOS シャーシは、単一ブレードで複数のサービス(Firepower Threat Defense ファイアウォール、サードパーティの DDoS アプリケーションなど)をサポートできます。これらのアプリケーションは、リンクされてサービス チェーンを形成します。Firepower 4120、4140、4150、および 9300 のセキュリティ アプライアンスで動作する Firepower eXtensible Operating System(FXOS)2.1.1 以降では、ASA や Firepower Threat Defense の前で実行するように、サードパーティ製の Radware DefensePro 仮想プラットフォームをインストールできます。Radware DefensePro は、FXOS シャーシに分散型サービス妨害(DDoS)の検出と緩和機能を提供する KVM ベースの仮想プラットフォームです。FXOS シャーシでサービス チェーンが有効になると、ネットワークからの入力トラフィックは Firepower Threat Defense に到達する前に DefensePro 仮想プラットフォームを通過する必要があります。

Firepower Threat Defense 対応の Radware DefensePro は、次のモードで展開することができます。

- スタンドアロン
- シャーシ内クラスタ
- アクティブ/スタンバイ フェールオーバー

(注) サービス チェーンは、シャーシ内クラスタ コンフィギュレーションではサポートされていません。ただし、Radware DefensePro(vDP)アプリケーションは、シャーシ内クラスタ シナリオのスタンドアロン コンフィギュレーションに導入できます。DefensePro アプリケーションは最大 3 つのセキュリティ モジュールの個別のインスタンスとして動作できます。

(注)

- Radware DefensePro 仮想プラットフォームは、Radware vDP(仮想 DefensePro)、またはシンプルに vDP と呼ばれることがあります。
- Radware DefensePro アプリケーションは、リンク デコーダと呼ばれることもあります。

Radware DefensePro サービス チェーンのライセンス要件

Firepower 4100 および Firepower 9300 シリーズのセキュリティ アプライアンスで動作する Radware Virtual DefensePro アプリケーションのライセンスは、Radware APSolute Vision Manager を通じて処理されます。デバイスのスループット ライセンスを注文するには、Cisco Commerce Workspace(CCW)に移動します。このリクエストを送信すると、Radware ポータルへのログイン情報とリンクが返信され、ライセンス要求が可能になります。

Radware の APSolute Vision Manager および スループット ライセンス要件の詳細については、Radware の Web サイト（htttps://portals.radware.com/Customer/Home/Downloads/Management-Monitoring/?Product=APSolute-Vision）を参照してください。このポータルにアクセスするには、Radware に登録することが必要です。

タイムゾーン同期の要件

Firepower セキュリティ アプライアンスに Radware vDP を展開する前に、シャーシ マネージャが NTP サーバを使用するように Etc/UTC タイム ゾーンで設定されていることを確認する必要があります。

手順

1. Firepower Chassis Manager で [プラットフォームの設定（Platform Settings）] を選択し、[プラットフォームの設定（Platform Settings）] ページで [NTP] 領域を開きます。
2. [タイムゾーン（Time Zone）] ドロップダウン リストで [etc/UTC] を選択します。
3. [時刻源の設定（Set Time Source）] で、[NTPサーバの使用（Use NTP Server）] を選択します。
4. [NTPサーバ（NTP Server）] フィールドに、使用する NTP サーバの IP アドレスまたはホスト名を入力します。
5. [Save] をクリックします。

Firepower シャーシでの日付と時刻の設定についての詳細は、『*Cisco FXOS CLI コンフィギュレーション ガイド*』[英語] または『*Cisco FXOS Firepower Chassis Manager コンフィギュレーション ガイド*』[英語]で、「日付と時刻の設定」のトピックを参照してください（http://www.cisco.com/go/firepower9300-config）。

APSolute Vision Manager のバージョン要件

Radware APSolute Vision は、vDP の主要な管理インターフェイスです。vDP と Firepower Threat Defense サービス チェーンの統合によって提供されるすべての機能を APSolute Vision Manager でサポートするには、APSolute Vision のバージョン R3.40 以上が必要です。

（注）Radware DefensePro の HTTPS 管理には、APSolute Vision Manager が必要です。APSolute Vision Manager なしで Radware DefensePro をローカルで管理するには、FXOS CLI を使用する必要があります。

2. サービス チェーンにおける Radware vDP の導入と設定

はじめる前に

- 論理デバイスに使用するセキュリティ モジュールに、すでに論理デバイスが設定されている場合は、まず既存の論理デバイスを削除してください（「論理デバイスの削除」を参照）。
- Cisco.com から vDP イメージをダウンロードし（「Cisco.com からのイメージのダウンロード」を参照）、次にそのイメージを FXOS シャーシにダウンロードします（「FXOS シャーシへの論理デバイスのソフトウェア イメージのダウンロード」を参照）。

管理インターフェイスおよびデータ インターフェイスの設定

スーパバイザで、Firepower Threat Defense 論理デバイスおよび vDP デコレータの導入設定に組み込むことのできる管理タイプのインターフェイスを設定します。また、少なくとも 1 つのデータ タイプのインターフェイスを設定する必要があります。

手順

1. Firepower Chassis Manager で、[Interfaces] を選択してインターフェイス ページを開きます。
2. EtherChannel を追加するには、次の手順を実行します。
   a. [Add Port Channel] をクリックします。
   b. [Port Channel ID] に、1 ～ 47 の値を入力します。
   c. [Enable] はオンのままにします。
   d. [Type] で、[Management] または [Data] を選択します。各論理デバイスには、管理インターフェイスを 1 つだけ含めることができます。[Cluster] は選択しないでください。
   e. 必要に応じて、メンバー インターフェイスを追加します。
   f. [OK] をクリックします。
3. 単一インターフェイスの場合:
   a. インターフェイス行で [Edit] アイコンをクリックして、[Edit Interface] ダイアログボックスを開きます。
   b. [Enable] をオンにします。
   c. [Type] で、[Management] または [Data] をクリックします。各論理デバイスには、管理インターフェイスを 1 つだけ含めることができます。
   d. [OK] をクリックします。

Radware DefensePro サービス チェーンを備えたスタンドアロンの Firepower Threat Defense 論理デバイスの導入

Radware DefensePro イメージをインストールして Firepower Threat Defense のスタンドアロン論理デバイスの前に単一のサービス チェーンを設定するには、次の手順に従います。

(注) Firepower 4110 または 4120 デバイスで Firepower Threat Defense に Radware DefensePro をインストールする場合、同時に論理デバイスとしてデコレータを導入する必要があります。デバイスにすでに論理デバイスが設定された後で、デコレータをインストールすることはできません。詳細については、『Cisco FXOS Firepower Chassis Manager コンフィギュレーション ガイド』の「スタンドアロンの Threat Defense 論理デバイスの作成」を参照してください。

1. スタンドアロンの Threat Defense 論理デバイスを作成します(『Cisco FXOS Firepower Manager コンフィギュレーション ガイド』の「スタンドアロンの Threat Defense 論理デバイスの作成」を参照)。
2. FXOS CLI で、セキュリティ サービス モードを開始します。

   ```
   scope ssa
   ```

3. Firepower Threat Defense がインストールされているのと同じスロットに Radware vDP イメージをインストールします。

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

4. 設定をコミットします。

   ```
   commit-buffer
   ```

5. セキュリティ モジュールの vDP の設置とプロビジョニングを確認します。

   ```
   show app-instance
   ```

6. (オプション)サポートされている利用可能なリソース プロファイルを表示します。

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

例:

```
Firepower /ssa/app # show app-resource-profile
コア RAM サイズ(MB)のデフォルト プロファイルのプロファイル名セキュリティ モデル番号
------------------------ --------------- --------------- ---------------
---------------
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. (オプション)前の手順の使用可能なプロファイルの 1 つを使用して、リソース プロファイルを設定します。

   a. 範囲をスロット 1 にします:

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

   b. DefensePro アプリケーション インスタンスを入力します。

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

   c. アプリケーション インスタンスを有効にします。

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

   d. リソース プロファイルを設定します。

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

   e. 設定をコミットします。

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

8. vDP アプリケーションがオンライン状態になった後、論理デバイスにアクセスします。

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

9. Firepower Threat Defense 論理デバイスを入力します。

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

10. vDP に管理インターフェイスを割り当てます。論理デバイスのものと同じ物理インターフェイスを使用することも、別のインターフェイスを使用することもできます。

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

11. vDP の外部管理を設定します。

    a. ブートストラップ オブジェクトを作成します。

       ```
       create mgmt-bootstrap vdp
       ```

    b. 管理 IP アドレスを設定します。

       ```
       create ipv4 slot_id default
       ```

    c. ゲートウェイ アドレスを設定します。

       ```
       set gateway gateway_address
       ```

    d. IP アドレスとマスクを設定します。

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

e. 管理 IP 設定スコープを終了します。

```
exit
```

f. 管理ブートストラップ設定スコープを終了します。

```
exit
```

12. 外部ポート リンクを作成します。

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

13. 外部ポートの範囲を指定します。

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

14. 論理デバイスにサードパーティのアプリケーションを追加します。

```
set decorator vdp
exit
exit
```

15. サードパーティのアプリケーションがインターフェイスに設定されているかどうかを確認します。

```
show logical-device
```

16. 設定を確定します。

```
commit-buffer
```

17. DefensePro アプリケーションのパスワードを設定します。パスワードを設定するまでは、アプリケーションはオンラインにならないことに注意してください。詳細については、cisco.com に用意されている『Radware DefensePro DDoS Mitigation User Guide』を参照してください。

Radware DefensePro サービス チェーンを備えた Firepower Threat Defense クラスタの導入

Radware DefensePro イメージをインストールして Firepower Threat Defense シャーシ内クラスタの前にサービス チェーンを設定するには、次の手順に従います。

(注) サービス チェーンは、シャーシ内クラスタ コンフィギュレーションではサポートされていません。ただし、Radware DefensePro（vDP）アプリケーションは、シャーシ内クラスタ シナリオのスタンドアロン コンフィギュレーションに導入できます。

1. Firepower Threat Defense クラスタを設定します（『Cisco FXOS Firepower Chassis Manager コンフィギュレーション ガイド』の「Firepower Threat Defense クラスタの設定」を参照）。
2. 外部（クライアント側）ポートを Radware DefensePro でデコレートします。

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

3. Firepower Threat Defense の外部管理ポートを割り当てます。

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

4. DefensePro の外部管理ポートを割り当てます。

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

5. （オプション）サポートされている利用可能なリソース プロファイルを表示します。

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

例:

```
Firepower /ssa/app # show app-resource-profile
コア RAM サイズ(MB)のデフォルト プロファイルのプロファイル名セキュリティ モデル番号
------------------------ --------------- --------------- ---------------
---------------
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. （オプション）前の手順の使用可能なプロファイルの 1 つを使用して、リソース プロファイルを設定します。

   a. 範囲をスロット 1 にします:

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

   b. DefensePro アプリケーション インスタンスを入力します。

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

   c. アプリケーション インスタンスを有効にします。

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

   d. リソース プロファイルを設定します。

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

   e. 設定をコミットします。

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

7. クラスタ ポート チャネルを設定します。

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

8. DefensePro の 3 つのすべてのインスタンスの管理ブートストラップを設定します。

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

次に例を示します。

```
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. 管理ブートストラップ設定スコープを終了します。

```
exit
```

10. マスター ブレードで、管理 IP を設定し、クラスタリングを有効にします。

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

11. 設定をコミットします。

```
commit-buffer
```

12. DefensePro アプリケーションのパスワードを設定します。パスワードを設定するまでは、アプリケーションはオンラインにならないことに注意してください。詳細については、cisco.com に用意されている『Radware DefensePro DDoS Mitigation User Guide』を参照してください。

13. この手順を完了したら、DefensePro インスタンスがクラスタに設定されているかどうかを確認する必要があります。これを行うには、DefensePro インスタンスの範囲を指定してアプリケーションの属性を表示し、DefensePro インスタンスのどれがプライマリで、どれがセカンダリかを確認します。

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

DefensePro アプリケーションがオンラインでもクラスタ化されていない場合は、CLI に次のように表示されます。

```
アプリケーションの属性:
    アプリケーションの属性のキー:クラスタロール
    値:不明
```

この「unknown」値が表示された場合は、vDP クラスタを作成するために、DefensePro アプリケーションを入力してマスター IP アドレスを設定する必要があります。

DefensePro アプリケーションがオンラインでクラスタ化されている場合は、CLI に次のように表示されます。

```
アプリケーションの属性:
    アプリケーションの属性のキー:クラスタロール
    値:プライマリ/セカンダリ
```

完全な手順の例

```
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. vDP Web サービスの有効化

APSolute Vision で FXOS シャーシ内に配置される Virtual DefensePro アプリケーションを管理するために、vDP Web インターフェイスを有効にする必要があります。

手順

1. FXOS CLI から、vDP のアプリケーション インスタンスに接続します。

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

2. DefensePro アプリケーション インスタンスにログインするには、特定のユーザ名とパスワード（radware/radware）を使用します。
3. vDP Web サービスを有効化します。

   manage secure-web status set enable

4. vDP アプリケーションのコンソールを終了して FXOS モジュール CLI に戻ります。

   Ctrl]

4. UDP/TCP ポートのオープン

Radware APSolute Vision Manager インターフェイスは、さまざまな UDP/TCP ポートを使用して Radware vDP のアプリケーションと通信します。vDP のアプリケーション が APSolute Vision Manager と通信するために、これらのポートがアクセス可能でありファイアウォールによってブロックされないことを確認します。オープンする特定のポートの詳細については、『APSolute Vision ユーザ ガイド』の次の表を参照してください。

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

5. 次の作業

- すべての FXOS、Firepower 4100、および Firepower 9300 のマニュアルのリンクについては、Cisco FXOS マニュアルのナビゲーションを参照してください。
- すべての Firepower Threat Defense のマニュアルのリンクについては、Cisco Firepower System マニュアルのロードマップを参照してください。
- 『**Radware DefensePro DDoS 緩和ユーザ ガイド**』は、http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-installation-and-configuration-guides-list.html からダウンロードできます。
- 『**Radware DefensePro DDoS 緩和リリース ノート**』は、http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-installation-and-configuration-guides-list.html からダウンロードできます。
- Radware の APSolute Vision Manager の詳細については、Radware の Web サイトでマニュアルのポータル（https://portals.radware.com/Customer/Home/Downloads/Management-Monitoring/?Product=APSolute-Vision）を参照してください。このポータルにアクセスするには、Radware に登録することが必要です。