論理デバイス

- 論理デバイスについて （1 ページ）
- 論理デバイスの要件と前提条件 （2 ページ）
- 論理デバイスに関する注意事項と制約事項 （4 ページ）
- スタンドアロン論理デバイスの追加 （10 ページ）
- ハイ アベイラビリティ ペアの追加 （24 ページ）
- クラスタの追加 （25 ページ）
- Radware DefensePro の設定 （48 ページ）
- 論理デバイスの管理 （59 ページ）
- 論理デバイスのモニタリング （67 ページ）
- サイト間クラスタリングの例 （68 ページ）
- 論理デバイスの履歴 （71 ページ）

論理デバイスについて

1 つの論理デバイスで 1 つのアプリケーション インスタンス（ASA または Firepower Threat Defense）に加え、オプションで 1 つのデコレータ アプリケーション（Radware DefensePro）を実行してサービス チェーンを形成できます。

論理デバイスを追加するときに、アプリケーション インスタンスのタイプおよびバージョンの定義、インターフェイスの割り当て、アプリケーション構成にプッシュされるブートストラップ設定の構成も行います。

（注） Firepower 9300 では、シャーシ内のすべてのモジュールで同じアプリケーション インスタンス タイプ（ASA または Firepower Threat Defense）をインストールする必要があります。現時点では、異なるタイプはサポートされていません。モジュールは異なるバージョンのアプリケーション インスタンス タイプを実行できることに注意してください。

スタンドアロン論理デバイスとクラスタ化論理デバイス

次の論理デバイス タイプを追加できます。

- スタンドアロン：スタンドアロン論理デバイスは、スタンドアロン ユニットまたはハイアベイラビリティ ペアのユニットとして動作します。
- クラスタ：クラスタ化論理デバイスを使用すると複数のユニットをグループ化することで、単一デバイスのすべての利便性（管理、ネットワークへの統合）を提供し、同時に複数デバイスによるスループットの向上と冗長性を実現できます。Firepower 9300 などの複数のモジュールデバイスが、シャーシ内クラスタリングをサポートします。Firepower 9300 のすべての 3 つのモジュール アプリケーション インスタンスは、1 つの論理デバイスに属しています。

（注） Firepower 9300 の場合、すべてのモジュールがクラスタに属している必要があります。1 つのセキュリティ モジュールにスタンドアロン論理デバイスを作成し、残り 2 つのセキュリティ モジュールを使用してクラスタを作成することはできません。

論理デバイスの要件と前提条件

要件と前提条件については、次のセクションを参照してください。

クラスタリングの要件と前提条件

クラスタ モデルのサポート

- Firepower 9300 の ASA：シャーシ内、シャーシ間、およびサイト間クラスタリングでサポート。
- Firepower 4100 シリーズ の ASA：シャーシ間およびシャーシ内クラスタリングでサポート。
- Firepower 9300 の FTD：シャーシ内およびシャーシ間クラスタリングでサポート。
- Firepower 4100 シリーズ の FTD：シャーシ間クラスタリングでサポート。
- Radware DefensePro：ASA によるシャーシ内クラスタリングでサポート。
- Radware DefensePro：FTD によるシャーシ内クラスタリングでサポート。

シャーシ間のクラスタリング ハードウェアおよびソフトウェアの要件

クラスタ内のすべてのシャーシ：

- Firepower4100シリーズ：すべてのシャーシが同一モデルである必要があります。Firepower 9300：すべてのセキュリティ モジュールは同じタイプである必要があります。各シャーシに異なる数のセキュリティ モジュールをインストールできますが、すべての空のスロットを含め、シャーシのすべてのモジュールをクラスタに含める必要があります。
- イメージアップグレード時を除き、同じFXOS ソフトウェアを実行する必要があります。
- クラスタに割り当てるインターフェイスは、管理インターフェイス、EtherChannel、アクティブインターフェイス、スピード、デュプレックスなど、同じインターフェイス構成を含める必要があります。同じインターフェイス ID の容量が一致し、インターフェイスが同じスパンドEtherChannel に内に問題なくバンドルできる限り、シャーシに異なるタイプのネットワーク モジュールを使用できます。シャーシ間クラスタリングでは、すべてのデータ インターフェイスを EtherChannel とする必要があります。（インターフェイス モジュールの追加または削除、あるいはEtherChannel の設定などにより）クラスタリングを有効にした後にFXOS でインターフェイスを変更した場合は、各シャーシで同じ変更を行います（スレーブ ユニットから始めて、マスターで終わります）。
- 同じ NTP サーバを使用する必要があります。 Firepower Threat Defense のため、Firepower Management Center は同じ NTP サーバを使用する必要があります。手動で時間を設定しないでください。
- ASA：各 FXOS シャーシは、License Authority またはサテライト サーバに登録されている必要があります。スレーブ ユニットに追加費用はかかりません。 永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入する必要があります。Firepower Threat Defense では、すべてのライセンスは Firepower Management Center で処理されます。

シャーシ間クラスタリングのスイッチ要件

- Firepower 4100/9300 シャーシのクラスタリングを設定する前に、スイッチの設定を完了し、シャーシからスイッチまですべての EtherChannel を良好に接続してください。
- サポートされているスイッチのリストについては、「Cisco FXOS Compatibility」を参照してください。

サイト間クラスタリング用の Data Center Interconnect のサイジング

次の計算と同等の帯域幅をクラスタ制御リンク トラフィック用にData Center Interconnect（DCI）に確保する必要があります。

$$\frac{\#\text{ of cluster members per site}}{2} \times \text{cluster control link size per member}$$

メンバの数が各サイトで異なる場合、計算には大きい方の値を使用します。DCI の最小帯域幅は、1 つのメンバに対するクラスタ制御リンクのサイズ未満にすることはできません。

次に例を示します。

- 4 サイトの 2 メンバの場合。
  - 合計 4 クラスタ メンバ

- 各サイト 2 メンバ
- メンバあたり 5 Gbps クラスタ制御リンク

予約する DCI 帯域幅 = 5 Gbps（2/2 x 5 Gbps）。

- 3 サイトの 6 メンバの場合、サイズは増加します。
  - 合計 6 クラスタ メンバ
  - サイト 1 は 3 メンバ、サイト 2 は 2 メンバ、サイト 3 は 1 メンバ
  - メンバあたり 10 Gbps クラスタ制御リンク

予約する DCI 帯域幅 = 15 Gbps（3/2 x 10 Gbps）。

- 2 サイトの 2 メンバの場合。
  - 合計 2 クラスタ メンバ
  - 各サイト 1 メンバ
  - メンバあたり 10 Gbps クラスタ制御リンク

予約する DCI 帯域幅 = 10 Gbps（1/2 x 10 Gbps = 5 Gbps、ただし最小帯域幅がクラスタ制御リンク（10 Gbps）のサイズ未満になってはなりません）。

論理デバイスに関する注意事項と制約事項

ガイドラインと制限事項については、以下のセクションを参照してください。

一般的なガイドラインと制限事項

ファイアウォール モード

FTD のブートストラップ設定でファイアウォール モードをルーテッドまたはトランスペアレントに設定できます。 ASA の場合、展開後に、ファイアウォール モードをトランスペアレントに変更することができます。ASA のトランスペアレント ファイアウォール モードへの変更（63 ページ）を参照してください。

ハイ アベイラビリティ

- アプリケーション設定内でハイ アベイラビリティを設定します。
- 任意のデータ インターフェイスをフェールオーバー リンクおよびステート リンクとして使用できます。
- 詳細については、ハイ アベイラビリティのためのアプリケーション設定ガイドの章を参照してください。

コンテキスト モード

- マルチ コンテキスト モードは ASA でのみサポートされています。
- 展開後に、ASA のマルチ コンテキスト モードを有効にします。

クラスタリング ガイドラインと制限事項

シャーシ間クラスタリングのスイッチ

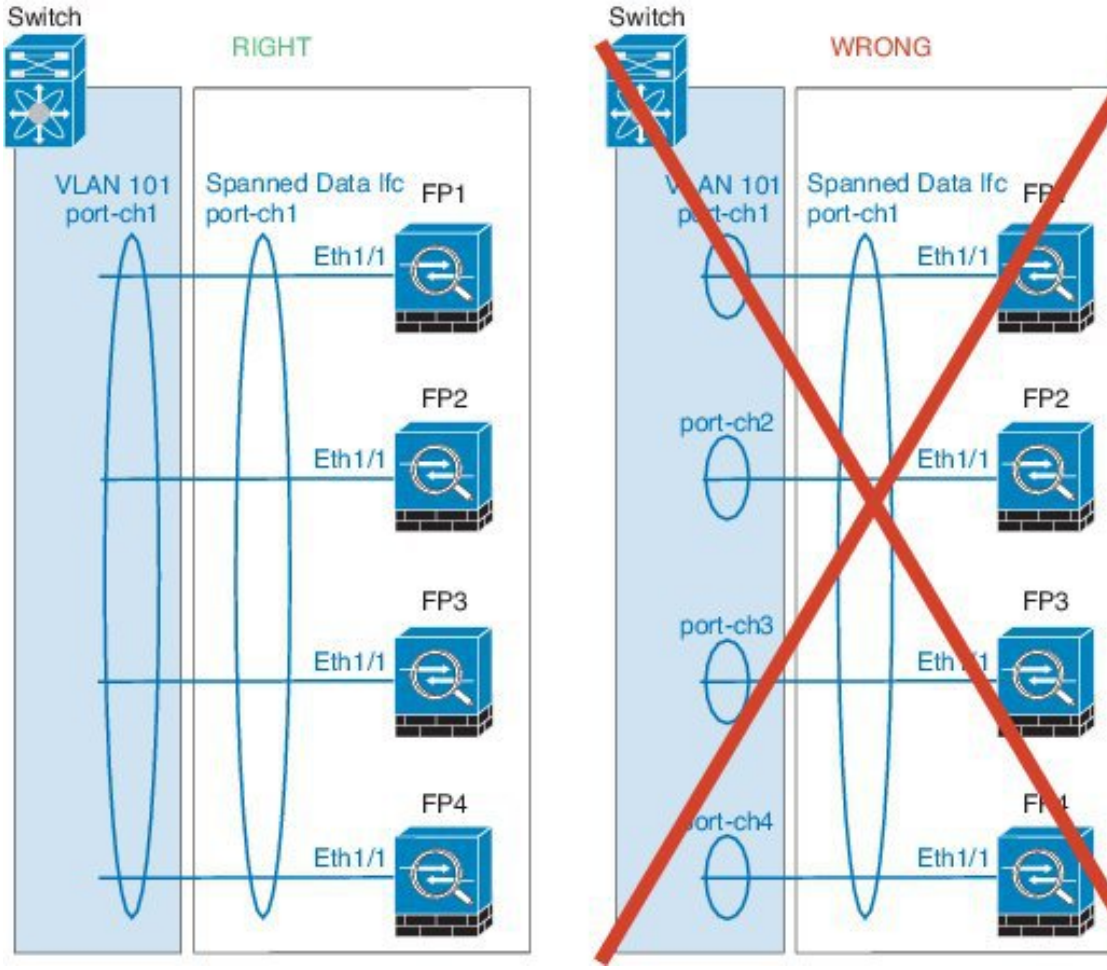
- ASR 9006 では、非デフォルト MTU を設定する場合は、ASR インターフェイス MTU をクラスタ デバイス MTU より 14 バイト大きく設定します。そうしないと、**mtu-ignore** オプションを使用しない限り、OSPF 隣接関係（アジャセンシー）ピアリングの試行が失敗する可能性があります。クラスタ デバイス MTU は、ASR *IPv4* MTU と一致する必要があります。
- クラスタ制御リンク インターフェイスのスイッチでは、クラスタ ユニットに接続されるスイッチ ポートに対してスパニングツリー PortFast をイネーブルにすることもできます。このようにすると、新規ユニットの参加プロセスを高速化できます。
- スイッチ上のスパンド EtherChannel のバンドリングが遅いときは、スイッチの個別インターフェイスに対して LACP 高速レートをイネーブルにできます。Nexus シリーズなど一部のスイッチでは、インサービス ソフトウェア アップグレード（ISSU）を実行する際に LACP 高速レートがサポートされないことに注意してください。そのため、クラスタリングで ISSU を使用することは推奨されません。
- スイッチでは、EtherChannel ロードバランシング アルゴリズム **source-dest-ip** または **source-dest-ip-port**（Cisco Nexus OS および Cisco IOS の **port-channel load-balance** コマンドを参照）を使用することをお勧めします。クラスタのデバイスにトラフィックを不均一に配分する場合があるので、ロード バランス アルゴリズムでは **vlan** キーワードを使用しないでください。
- スイッチの EtherChannel ロードバランシング アルゴリズムを変更すると、スイッチの EtherChannel インターフェイスは一時的にトラフィックの転送を停止し、スパニングツリー プロトコルが再始動します。トラフィックが再び流れ出すまでに、少し時間がかかります。
- クラスタ制御リンク パスのスイッチでは、L4 チェックサムを検証しないようにする必要があります。クラスタ制御リンク経由でリダイレクトされたトラフィックには、正しい L4 チェックサムが設定されていません。L4 チェックサムを検証するスイッチにより、トラフィックがドロップされる可能性があります。
- ポートチャネル バンドルのダウンタイムは、設定されているキープアライブ インターバルを超えてはなりません。
- Supervisor 2T EtherChannel では、デフォルトのハッシュ配信アルゴリズムは適応型です。VSS 設計での非対称トラフィックを避けるには、クラスタ デバイスに接続されているポートチャネルでのハッシュ アルゴリズムを固定に変更します。

router(config)# **port-channel** *id* **hash-distribution fixed**

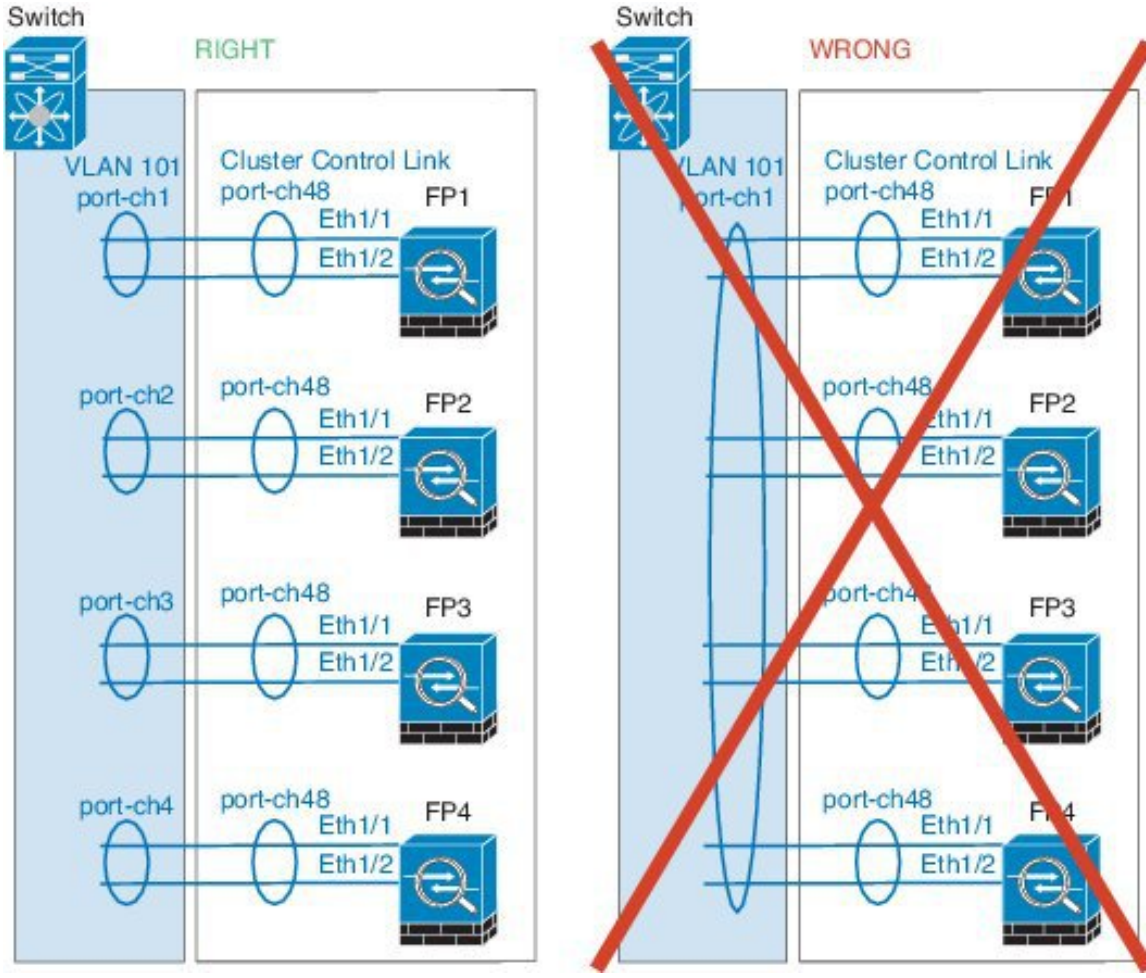
アルゴリズムをグローバルに変更しないでください。VSS ピア リンクに対しては適応型アルゴリズムを使用できます。

シャーシ間クラスタリングの EtherChannel

- スイッチ接続用に、EtherChannel モードをアクティブに設定します。クラスタ制御リンクであっても、Firepower 4100/9300 シャーシではオン モードはサポートされません。
- FXOS EtherChannel にはデフォルトで [fast] に設定されている LACP レートがあります。Nexus シリーズなど一部のスイッチでは、インサービス ソフトウェア アップグレード（ISSU）を実行する際に LACP 高速レートがサポートされないため、クラスタリングで ISSU を使用することは推奨されません。
- 15.1(1)S2 より前の Catalyst 3750-X Cisco IOS ソフトウェア バージョンでは、クラスタ ユニットはスイッチ スタックに EtherChannel を接続することをサポートしていませんでした。デフォルトのスイッチ設定では、クラスタ ユニット EtherChannel がクロス スタックに接続されている場合、マスター スイッチの電源がオフになると、残りのスイッチに接続されている EtherChannel は起動しません。互換性を高めるため、**stack-mac persistent timer** コマンドを設定して、十分なリロード時間を確保できる大きな値、たとえば 8 分、0（無制限）などを設定します。または、15.1(1)S2 など、より安定したスイッチ ソフトウェア バージョンにアップグレードできます。
- スパンド EtherChannel とデバイス ローカル EtherChannel のコンフィギュレーション：スパンド EtherChannel と デバイス ローカル EtherChannel に対してスイッチを適切に設定します。
  - スパンド EtherChannel：クラスタ ユニット スパンド EtherChannel（クラスタのすべてのメンバに広がる）の場合は、複数のインターフェイスが結合されてスイッチ上の単一の EtherChannel となります。各インターフェイスがスイッチ上の同じチャネル グループ内にあることを確認してください。



- デバイス ローカル EtherChannel：クラスタ ユニット デバイス ローカル EtherChannel（クラスタ制御リンク用に設定された EtherChannel もこれに含まれます）は、それぞれ独立した EtherChannel としてスイッチ上で設定してください。スイッチ上で複数のクラスタ ユニット EtherChannel を結合して 1 つの EtherChannel としないでください。



サイト間クラスタリング

サイト間クラスタリングについては、次のガイドラインを参照してください。

- クラスタ制御リンクの遅延が、ラウンドトリップ時間（RTT）20 ms 未満である必要があります。
- クラスタ制御リンクは、順序の異常やパケットのドロップがない信頼性の高いものである必要があります。たとえば、専用リンクを使用する必要があります。
- 接続の再分散を設定しないでください。異なるサイトのクラスタ メンバには接続を再分散できません。
- クラスタの実装では、着信接続用の複数のサイトでメンバが区別されません。したがって、特定の接続に対する接続のロールが複数のサイトにまたがる場合があります。これは想定されている動作です。ただし、ディレクタローカリゼーションを有効にすると、接続オーナーと同じサイトからローカル ディレクタ権限が常に選択されます（サイト ID に応じて）。また、元のオーナーに障害が発生するとローカルディレクタは同じサイトの新しいオーナーを選択します（注：サイト間でトラフィックが非対称で、元のオーナーに障害

が発生した後もリモート サイトから継続的なトラフィックがある場合、リモート サイトのユニットが re-hosting ウィンドウ内でデータ パケットを受信する場合はこのリモート サイトのユニットが新しいオーナーとなることがあります）。

- ディレクタ ローカリゼーションでは、次のトラフィック タイプのローカリゼーションをサポートしていません。NAT または PAT のトラフィック、SCTP がインスペクションを行うトラフィック、オーナーのフラグメンテーション クエリ。
- トランスペアレント モードの場合、内部ルータと外部ルータのペア間にクラスタを配置すると（AKA ノースサウス挿入）、両方の内部ルータが同じ MAC アドレスを共有し、両方の外部ルータが同じ MAC アドレスを共有する必要があります。サイト 1 のクラスタ メンバがサイト 2 のメンバに接続を転送するとき、宛先 MAC アドレスは維持されます。MAC アドレスがサイト 1 のルータと同じである場合にのみ、パケットはサイト 2 のルータに到達します。
- トランスペアレント モードの場合、内部ネットワーク間のファイル用に各サイトのデータ ネットワークとゲートウェイ ルータ間にクラスタを配置すると（AKA イーストウェスト挿入）、各ゲートウェイ ルータは、HSRP などの First Hop Redundancy Protocol（FHRP）を使用して、各サイトで同じ仮想 IP および MAC アドレスの宛先を提供します。データ VLAN は、オーバーレイ トランスポート仮想化（OTV）または同様のものを使用してサイト全体にわたって拡張されます。ローカル ゲートウェイ ルータ宛てのトラフィックが DCI 経由で他のサイトに送信されないようにするには、フィルタを作成する必要があります。ゲートウェイ ルータが 1 つのサイトで到達不能になった場合、トラフィックが正常に他のサイトのゲートウェイに到達できるようにフィルタを削除する必要があります。
- スパンド EtherChannel を使用したルーテッド モードでは、サイト固有の MAC アドレスを設定します。OTV または同様のものを使用してサイト全体にデータ VLAN を拡張します。グローバル MAC アドレス宛てのトラフィックが DCI 経由で他のサイトに送信されないようにするには、フィルタを作成する必要があります。クラスタが 1 つのサイトで到達不能になった場合、トラフィックが正常に他のサイトのクラスタ ユニットに到達できるようにフィルタを削除する必要があります。ダイナミック ルーティングは、サイト間クラスタが拡張セグメントのファースト ホップ ルータとして機能する場合はサポートされません。

その他のガイドライン

- 冗長性を持たせるため、VSS または vPC に EtherChannel を接続することを推奨します。
- シャーシ内では、スタンドアロン モードで一部のシャーシ セキュリティ モジュールをクラスタ化し、他のセキュリティ モジュールを実行することはできません。クラスタ内にすべてのセキュリティ モジュールを含める必要があります。

デフォルト

クラスタ制御リンクはポート チャネル 48 を使用します。

スタンドアロン論理デバイスの追加

スタンドアロン論理デバイスは単独またはハイ アベイラビリティ ユニットとして使用できます。ハイ アベイラビリティの使用率の詳細については、ハイ アベイラビリティ ペアの追加（24 ページ）を参照してください。

スタンドアロン ASA の追加

スタンドアロンの論理デバイスは、単独またはハイ アベイラビリティ ペアで動作します。Firepower 9300 などの複数のモジュール デバイスでは、クラスタまたはスタンドアロン デバイスを導入できます。クラスタはすべてのモジュールを使用する必要があるため、たとえば、2 モジュール クラスタと単一のスタンドアロン デバイスをうまく組み合わせることはできません。

Firepower 4100/9300 シャーシからルーテッド ファイアウォール モード ASA を展開できます。ASA をトランスペアレント ファイアウォール モードに変更するには、この手順を完了し、ASA のトランスペアレント ファイアウォール モードへの変更（63 ページ）を参照してください。

マルチ コンテキスト モードの場合、最初に論理デバイスを展開してから、ASA アプリケーションでマルチ コンテキスト モードを有効にする必要があります。

始める前に

- 論理デバイスに使用するアプリケーション イメージを Cisco.com からダウンロードして（Cisco.com からのイメージのダウンロードを参照）、そのイメージを Firepower 4100/9300 シャーシ（Firepower 4100/9300 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） にダウンロードします。

（注） シャーシ内のすべてのモジュールに同じアプリケーション インスタンス タイプ（ASA または Firepower Threat Defense）をインストールする必要があります。現時点では、他のアプリケーション タイプはサポートされていません。モジュールは特定のアプリケーション タイプの異なるバージョンを実行できますが、すべてのモジュールを同じタイプのアプリケーション インスタンスとして設定する必要があります。

- 論理デバイスで使用する管理インターフェイスを設定します。管理インターフェイスが必要です。この管理インターフェイスは、シャーシの管理のみに使用されるシャーシ管理インターフェイスと同じではありません（FXOS では、シャーシ管理インターフェイスは MGMT、management0 のような名前で表示されます）。

手順

ステップ 1 セキュリティ サービス モードを開始します。

scope ssa

例：

```
Firepower# scope ssa
Firepower /ssa #
```

ステップ 2 アプリケーション インスタンスのイメージ バージョンを設定します。

a) 使用可能なイメージを表示します。使用するバージョン番号に注意してください。

show app

例：

```
Firepower /ssa # show app
    Name       Version         Author     Supported Deploy Types CSP Type    Is
Default App
    ---------- --------------- ---------- ---------------------- -----------
--------------
    asa        9.9.1           cisco      Native                 Application No
    asa        9.10.1          cisco      Native                 Application Yes
    ftd        6.2.3           cisco      Native                 Application Yes
```

b) セキュリティ モジュール / エンジン スロットに範囲を設定します。

scope slot *slot_id*

slot_id は、Firepower 4100 の場合は常に 1、Firepower 9300 の場合は 1、2、または 3 です。

例：

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

c) アプリケーション インスタンスを作成します。

enter app-instance asa

例：

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

d) ASA イメージ バージョンを設定します。

set startup-version *version*

例：

```
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
```

e) スロット モードを終了します。

exit

例：

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

f) ssa モードを終了します。

exit

例：

```
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

例：

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance asa ASA1
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

ステップ 3 論理デバイスを作成します。

enter logical-device *device_name* **asa** *slot_id* **standalone**

例：

```
Firepower /ssa # enter logical-device ASA1 asa 1 standalone
Firepower /ssa/logical-device* #
```

ステップ 4 管理およびデータ インターフェイスを論理デバイスに割り当てます。各インターフェイスに対して、手順を繰り返します。

create external-port-link *name interface_id* **asa**

set description *description*

exit

- *name*：name は Firepower 4100/9300 シャーシ スーパーバイザによって使用されます。これは、ASA の設定で使用するインターフェイス名ではありません。
- *description*：フレーズを引用符（"）で囲み、スペースを追加します。

例：

```
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 asa
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
```

```
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 asa
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 asa
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
```

ステップ 5 管理ブートストラップ情報を設定します。

a) ブートストラップ オブジェクトを作成します。

create mgmt-bootstrap asa

例：

```
Firepower /ssa/logical-device* # create mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

b) 管理者を指定し、パスワードを指定します。

create bootstrap-key-secret PASSWORD

set value

値の入力：*password*

値の確認：*password*

exit

例：

事前設定されている ASA 管理者ユーザおよびイネーブル パスワードはパスワードの回復時に役立ちます。FXOS アクセスが可能な場合、管理者ユーザ パスワードを忘れたときにリセットできます。

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

c) IPv4 管理インターフェイス設定を設定します。

create ipv4 *slot_id* **default**

set ip *ip_address* **mask** *network_mask*

set gateway *gateway_address*

exit

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.34 mask
```

```
255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

d) IPv6 管理インターフェイス設定を設定します。

create ipv6 *slot_id* **default**

set ip *ip_address* **prefix-length** *prefix*

set gateway *gateway_address*

exit

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

e) 管理ブートストラップ モードを終了します。

exit

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

ステップ 6 設定を保存します。

commit-buffer

例：

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device #
```

ステップ 7 論理デバイスを導入後、デバイスの前に配置される DDoS 検出および緩和サービスとして、サードパーティの 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 について （48 ページ）を参照してください。

例

```
Firepower# scope ssa
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance asa MyDevice1
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
Firepower /ssa/slot/app-instance* # exit
```

```
Firepower /ssa/slot* # exit
Firepower /ssa* # create logical-device MyDevice1 asa 1 standalone
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 asa
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 asa
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 asa
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: secretglassine
Confirm the value: secretglassine
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.31 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # commit-buffer
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key #
```

スタンドアロン Firepower Threat Defense の追加

スタンドアロンの論理デバイスは、単独またはハイ アベイラビリティ ペアで動作します。Firepower 9300 などの複数のモジュール デバイスでは、クラスタまたはスタンドアロン デバイスを導入できます。クラスタはすべてのモジュールを使用する必要があるため、たとえば、2 モジュール クラスタと単一のスタンドアロン デバイスをうまく組み合わせることはできません。

始める前に

- 論理デバイスに使用するアプリケーション イメージを Cisco.com からダウンロードして（Cisco.com からのイメージのダウンロードを参照）、そのイメージを Firepower 4100/9300 シャーシ（Firepower 4100/9300 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） にダウンロードします。

  （注） シャーシ内のすべてのモジュールに同じアプリケーション インスタンス タイプ（ASA または Firepower Threat Defense）をインストールする必要があります。現時点では、他のアプリケーション タイプはサポートされていません。モジュールは特定のアプリケーション タイプの異なるバージョンを実行できますが、すべてのモジュールを同じタイプのアプリケーション インスタンスとして設定する必要があります。

- 論理デバイスで使用する管理インターフェイスを設定します。管理インターフェイスが必要です。この管理インターフェイスは、シャーシの管理のみに使用されるシャーシ管理イ

ンターフェイスと同じではありません（FXOS では、シャーシ管理インターフェイスは MGMT、management0 のような名前で表示されます）。

- また、少なくとも 1 つのデータ型インターフェイスを設定する必要があります。必要に応じて、すべてのイベントのトラフィック（Web イベントなど）を運ぶ firepower-eventing インターフェイスも作成できます。詳細については、「インターフェイス タイプ」を参照してください。

手順

ステップ 1 セキュリティ サービス モードを開始します。

scope ssa

例：

```
Firepower# scope ssa
Firepower /ssa #
```

ステップ 2 使用する Firepower Threat Defense バージョンのエンドユーザ ライセンス契約書に同意します。このバージョンの EULA をまだ同意していない場合のみ、この手順を実行する必要があります。

a) 使用可能なイメージを表示します。使用するバージョン番号に注意してください。

show app

例：

```
Firepower /ssa # show app
    Name       Version         Author     Supported Deploy Types CSP Type    Is
Default App
    ---------- --------------- ---------- ---------------------- -----------
--------------
    asa        9.9.1           cisco      Native                 Application No
    asa        9.10.1          cisco      Native                 Application Yes
    ftd        6.2.3           cisco      Native                 Application Yes
```

b) イメージ バージョンに範囲を設定します。

scope app ftd *application_version*

例：

```
Firepower /ssa # scope app ftd 6.2.3
Firepower /ssa/app #
```

c) ライセンス契約に同意します。

accept-license-agreement

例：

```
Firepower /ssa/app # accept-license-agreement

End User License Agreement: End User License Agreement

Effective: May 22, 2017

This is an agreement between You and Cisco Systems, Inc. or its affiliates
("Cisco") and governs your Use of Cisco Software. "You" and "Your" means the
individual or legal entity licensing the Software under this EULA. "Use" or
"Using" means to download, install, activate, access or otherwise use the
Software. "Software" means the Cisco computer programs and any Upgrades made
available to You by an Approved Source and licensed to You by Cisco.
"Documentation" is the Cisco user or technical manuals, training materials,
specifications or other documentation applicable to the Software and made
available to You by an Approved Source. "Approved Source" means (i) Cisco or
(ii) the Cisco authorized reseller, distributor or systems integrator from whom
you acquired the Software. "Entitlement" means the license detail; including
license metric, duration, and quantity provided in a product ID (PID) published
on Cisco's price list, claim certificate or right to use notification.
"Upgrades" means all updates, upgrades, bug fixes, error corrections,
enhancements and other modifications to the Software and backup copies thereof.

[...]

Please "commit-buffer" if you accept the license agreement, otherwise "discard-buffer".

Firepower /ssa/app* #
```

d) 設定を保存します。

commit-buffer

例：

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

e) セキュリティ サービス モードを終了します。

exit

例：

```
Firepower /ssa/app # exit
Firepower /ssa #
```

ステップ 3 アプリケーション インスタンスイメージ バージョンを含む）を設定します。

a) セキュリティ モジュール / エンジン スロットに範囲を設定します。

scope slot *slot_id*

slot_id は、Firepower 4100 の場合は常に 1、Firepower 9300 の場合は 1、2、または 3 です。

例：

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

b) アプリケーション インスタンスを作成します。

enter app-instance ftd

例：

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

c) Firepower Threat Defense イメージ バージョンを設定します。

set startup-version *version*

EULA に同意するときに上記の手順でメモしたバージョン番号を入力します。

例：

```
Firepower /ssa/slot/app-instance* # set startup-version 6.3.0
```

d) スロット モードを終了します。

exit

例：

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

e) （任意） Firepower 4110 または 4120 の Radware DefensePro インスタンスを作成します。このためには、論理デバイスの作成前にアプリケーションインスタンスを作成する必要があります。

enter app-instance vdp

exit

論理デバイス設定を確定したら、続いて Firepower Threat Defense 論理デバイスを使用して、サービス チェーン内に Radware DefensePro デコレータを設定する必要があります。スタンドアロンの論理デバイスでの Radware DefensePro の設定 （50 ページ）の手順 4 を参照してください。

例：

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

f) ssa モードを終了します。

exit

例：

```
Firepower /ssa/slot* # exit
```

```
Firepower /ssa* #
```

例：

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance ftd MyDevice1
Firepower /ssa/slot/app-instance* # set startup-version 6.3.0
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

ステップ 4 論理デバイスを作成します。

enter logical-device *device_name* **ftd** *slot_id* **standalone**

例：

```
Firepower /ssa # enter logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* #
```

ステップ 5 管理およびデータインターフェイスを論理デバイスに割り当てます。各インターフェイスに対して、手順を繰り返します。

create external-port-link *name interface_id* **ftd**

set description *description*

exit

- *name*：name は Firepower 4100/9300 シャーシ スーパーバイザによって使用されます。これは、Firepower Threat Defense の設定で使用するインターフェイス名ではありません。
- *description*：フレーズを引用符（"）で囲み、スペースを追加します。

例：

```
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 ftd
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 ftd
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 ftd
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
```

ステップ 6 管理ブートストラップ パラメータを設定します。

これらの設定は、初期導入専用、またはディザスタリカバリ用です。通常の運用では、アプリケーション CLI の設定でほとんどの値を変更できます。

a) ブートストラップ オブジェクトを作成します。

create mgmt-bootstrap ftd

例：

```
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

b) 管理 Firepower Management Center の IP アドレスを指定します。

create bootstrap-key FIREPOWER_MANAGER_IP

set value *IP_address*

exit

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key
FIREPOWER_MANAGER_IP
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.10.10.7
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

c) ファイアウォール モード（ルーテッドまたはトランスペアレント）を指定します。

create bootstrap-key FIREWALL_MODE

set value {**routed** | **transparent**}

exit

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

d) デバイスと Firepower Management Center との間で共有するキーを指定します。

create bootstrap-key-secret REGISTRATION_KEY

set value

値の入力：*registration_key*

値の確認：*registration_key*

exit

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret
REGISTRATION_KEY
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: gratuitousapples
Confirm the value: gratuitousapples
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

e) 管理者のパスワードを指定します。

create bootstrap-key-secret PASSWORD

set value

値の入力：*password*

値の確認：*password*

exit

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

f) 完全修飾ホスト名を指定します。

create bootstrap-key FQDN

set value *fqdn*

exit

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FQDN
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
ftd1.cisco.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

g) DNS サーバのカンマ区切りリストを指定します。

create bootstrap-key DNS_SERVERS

set value *dns_servers*

exit

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key DNS_SERVERS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
10.9.8.7,10.9.6.5
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

h) 検索ドメインのカンマ区切りリストを指定します。

create bootstrap-key SEARCH_DOMAINS

set value *search_domains*

exit

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key SEARCH_DOMAINS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
cisco.com,example.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

i) IPv4 管理インターフェイス設定を設定します。

create ipv4 *slot_id* **firepower**

set ip *ip_address* **mask** *network_mask*

set gateway *gateway_address*

exit

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.34 mask
255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

j) IPv6 管理インターフェイス設定を設定します。

create ipv6 *slot_id* **firepower**

set ip *ip_address* **prefix-length** *prefix*

set gateway *gateway_address*

exit

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

k) 管理ブートストラップ モードを終了します。

exit

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

ステップ 7 設定を保存します。

commit-buffer

例：

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device #
```

ステップ 8 論理デバイスを導入後、デバイスの前に配置される DDoS 検出および緩和サービスとして、サードパーティの 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 について （48 ページ）を参照してください。

例

```
Firepower# scope ssa
Firepower /ssa* # scope app ftd 6.3.0
Firepower /ssa/app* # accept-license-agreement
Firepower /ssa/app* # commit-buffer
Firepower /ssa/app # exit
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance ftd MyDevice1
Firepower /ssa/slot/app-instance* # set startup-version 6.3.0
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* # create logical-device MyDevice1 ftd 1 standalone
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 ftd
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 ftd
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 ftd
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREPOWER_MANAGER_IP
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.0.0.100
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret
REGISTRATION_KEY
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: juniorwindowpane
Confirm the value: juniorwindowpane
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: secretglassine
Confirm the value: secretglassine
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.31 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FQDN
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value ftd.cisco.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key DNS_SERVERS
```

```
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 192.168.1.1
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key SEARCH_DOMAINS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value search.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # commit-buffer
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key #
```

ハイ アベイラビリティ ペアの追加

Firepower Threat DefenseまたはASAハイ アベイラビリティ（フェールオーバーとも呼ばれる）は、FXOS ではなくアプリケーション内で設定されます。ただし、ハイ アベイラビリティのシャーシを準備するには、次の手順を参照してください。

始める前に

- ハイ アベイラビリティ要件については、ハイ アベイラビリティのためのアプリケーション設定ガイドの章を参照してください。

手順

ステップ 1 各論理デバイスは個別のシャーシ上にある必要があります。Firepower 9300 のシャーシ内のハイ アベイラビリティは推奨されず、サポートされない可能性があります。

ステップ 2 各論理デバイスに同一のインターフェイスを割り当てます。

ステップ 3 フェールオーバー リンクとステート リンクに 1 つまたは 2 つのデータ インターフェイスを割り当てます。

これらのインターフェイスは、2つのシャーシ間でハイアベイラビリティ トラフィックを交換します。統合されたフェールオーバーリンクとステートリンクには、10 GB のデータインターフェイスを使用することを推奨します。使用可能なインターフェイスがあれば、別のフェールオーバーおよびステートのリンクを使用できます。ステートリンクには、ほとんどの帯域幅が必要です。フェールオーバー リンクまたはステート リンクに管理タイプのインターフェイスを使用することはできません。同じネットワーク セグメント上で他のデバイスをフェールオーバーインターフェイスとして使用せずに、シャーシ間でスイッチを使用することをお勧めします。

ステップ 4 論理デバイスでハイ アベイラビリテを有効にします。

ステップ 5 ハイアベイラビリティを有効にした後にインターフェイスを変更する必要がある場合は、スタンバイ ユニットを最初に変更し、次にアクティブ ユニットを変更します。

（注） ASA の場合、FXOS でインターフェイスを削除すると（たとえば、ネットワーク モジュールの削除、EtherChannel の削除、または EtherChannel へのインターフェイスの再割り当てなど）、必要な調整を行うことができるように、ASA 設定では元のコマンドが保持されます。設定からインターフェイスを削除すると、幅広い影響が出る可能性があります。ASA OS の古いインターフェイス設定は手動で削除できます。

クラスタの追加

クラスタリングを利用すると、複数のデバイスをグループ化して1つの論理デバイスとすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。複数のモジュールを含む Firepower 9300 は、1 つのシャーシ内のすべてのモジュールをクラスタにグループ化する、シャーシ内クラスタリングをサポートします。複数のシャーシをまとめてグループ化する、シャーシ間クラスタリングも使用できます。シャーシ間クラスタリングは、Firepower 4100 シリーズなどの単一モジュール デバイスの唯一のオプションです。

Firepower 4100/9300 シャーシでのクラスタリングについて

クラスタは、単一の論理ユニットとして機能する複数のデバイスから構成されます。Firepower 4100/9300 シャーシ にクラスタを展開すると、以下の処理が実行されます。

- ユニット間通信用のクラスタ制御リンク（デフォルトのポート チャネル 48）を作成します。シャーシ内クラスタリングでは（Firepower 9300のみ）、このリンクは、クラスタ通信にFirepower 9300バックプレーンを使用します。シャーシ間クラスタリングでは、シャーシ間通信のために、このEtherChannelに物理インターフェイスを手動で割り当てる必要があります。
- アプリケーション内のクラスタブートストラップコンフィギュレーションを作成します。

  クラスタを展開すると、クラスタ名、クラスタ制御リンクインターフェイス、およびその他のクラスタ設定を含む各ユニットに対して、最小限のブートストラップ構成がFirepower 4100/9300シャーシスーパーバイザからプッシュされます。クラスタリング環境をカスタマイズする場合、ブートストラップコンフィギュレーションの一部は、アプリケーション内でユーザが設定できます。
- スパンドインターフェイスとして、クラスタにデータインターフェイスを割り当てます。

  シャーシ内クラスタリングでは、スパンドインターフェイスは、シャーシ間クラスタリングのようにEtherChannelに制限されません。Firepower 9300スーパーバイザは共有インターフェイスの複数のモジュールにトラフィックをロードバランシングするために内部でEtherChannelテクノロジーを使用するため、スパンドモードではあらゆるタイプのデータインターフェイスが機能します。 シャーシ間クラスタリングでは、すべてのデータ インターフェイスでスパンド EtherChannel を使用します。

（注） 管理インターフェイス以外の個々のインターフェイスはサポートされていません。

- 管理インターフェイスをクラスタ内のすべてのユニットに指定します。

ここでは、クラスタリングの概念と実装について詳しく説明します。

標準出荷単位とセカンダリ単位の役割

クラスタのメンバーの1つが標準出荷単位です。標準出荷単位は自動的に決定されます。他のすべてのメンバーはセカンダリ単位です。

すべてのコンフィギュレーション作業は標準出荷単位でのみ実行する必要があります。コンフィギュレーションはその後、セカンダリ単位に複製されます。

クラスタ制御リンク

クラスタ制御リンクは、ポートチャネル 48 インターフェイスを使用して自動的に作成されます。シャーシ間クラスタリングでは、このインターフェイスにメンバインターフェイスはありません。 シャーシ間クラスタリングでは、EtherChannel に 1 つ以上のインターフェイスを追加する必要があります。このクラスタ タイプの EtherChannel は、シャーシ内クラスタリング用のクラスタ通信に Firepower 9300 バックプレーンを使用します。

2 メンバシャーシ間クラスタの場合、シャーシと別のシャーシとの間をクラスタ制御リンクで直接接続しないでください。インターフェイスを直接接続した場合、一方のユニットで障害が発生すると、クラスタ制御リンクが機能せず、他の正常なユニットも動作しなくなります。スイッチを介してクラスタ制御リンクを接続した場合は、正常なユニットについてはクラスタ制御リンクは動作を維持します。

クラスタ制御リンク トラフィックには、制御とデータの両方のトラフィックが含まれます。

シャーシ間クラスタリングのクラスタ制御リンクのサイズ

可能であれば、各シャーシの予想されるスループットに合わせてクラスタ制御リンクをサイジングする必要があります。そうすれば、クラスタ制御リンクが最悪のシナリオを処理できます。

クラスタ制御リンク トラフィックの内容は主に、状態アップデートや転送されたパケットです。クラスタ制御リンクでのトラフィックの量は常に変化します。転送されるトラフィックの量は、ロードバランシングの有効性、または中央集中型機能のための十分なトラフィックがあるかどうかによって決まります。次に例を示します。

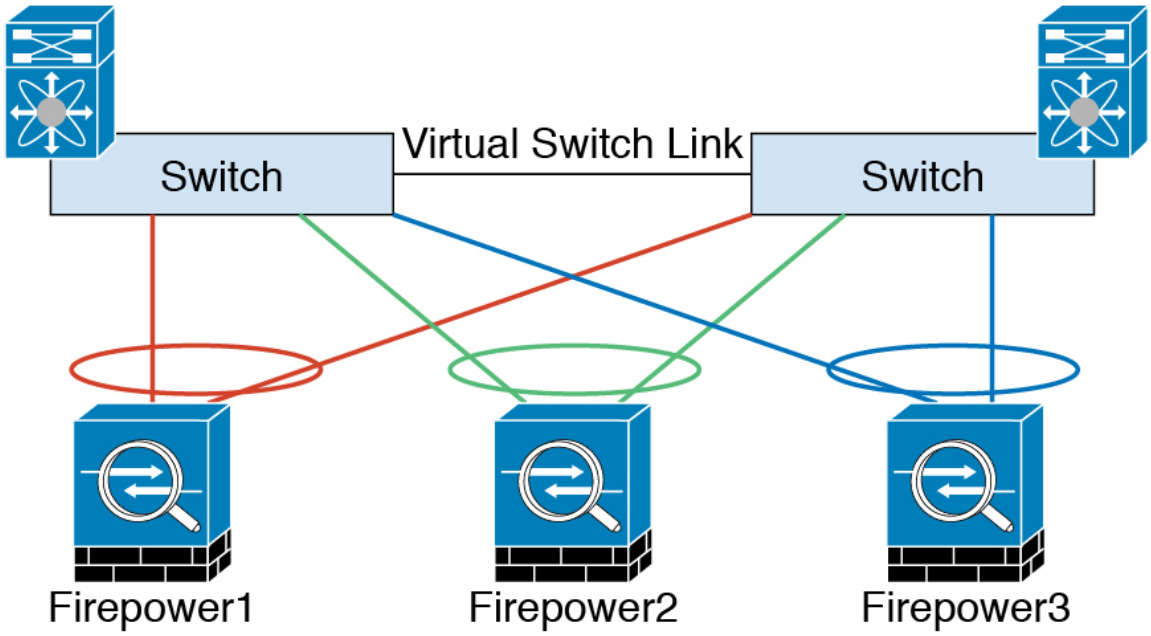
- NAT では接続のロード バランシングが低下するので、すべてのリターン トラフィックを正しいユニットに再分散する必要があります。
- メンバーシップが変更されると、クラスタは大量の接続の再分散を必要とするため、一時的にクラスタ制御リンクの帯域幅を大量に使用します。

クラスタ制御リンクの帯域幅を大きくすると、メンバーシップが変更されたときの収束が高速になり、スループットのボトルネックを回避できます。

（注） クラスタに大量の非対称（再分散された）トラフィックがある場合は、クラスタ制御リンクのサイズを大きくする必要があります。

シャーシ間クラスタリングのクラスタ制御リンク冗長性

次の図は、仮想スイッチングシステム（VSS）または仮想ポートチャネル（vPC）環境でクラスタ制御リンクとして EtherChannel を使用する方法を示します。EtherChannel のすべてのリンクがアクティブです。スイッチが VSS または vPC の一部である場合は、同じ EtherChannel 内の Firepower 4100/9300 シャーシ インターフェイスをそれぞれ、VSS または vPC 内の異なるスイッチに接続できます。スイッチ インターフェイスは同じ EtherChannel ポートチャネル インターフェイスのメンバです。複数の個別のスイッチが単一のスイッチのように動作するからです。この EtherChannel は、スパンド EtherChannel ではなく、デバイス ローカルであることに注意してください。



シャーシ間クラスタリングのクラスタ制御リンクの信頼性

クラスタ制御リンクの機能を保証するには、ユニット間のラウンドトリップ時間（RTT）が 20 ms 未満になるようにします。この最大遅延により、異なる地理的サイトにインストールされたクラスタ メンバとの互換性が向上します。遅延を調べるには、ユニット間のクラスタ制御リンクで ping を実行します。

クラスタ制御リンクは、順序の異常やパケットのドロップがない信頼性の高いものである必要があります。たとえば、サイト間の導入の場合、専用リンクを使用する必要があります。

クラスタ制御リンク ネットワーク

Firepower 4100/9300 シャーシは、シャーシ ID およびスロット ID（127.2.*chassis_id*.*slot_id*）に基づいて、各ユニットのクラスタ制御リンク インターフェイス IP アドレスを自動生成します。FXOS とアプリケーション内のどちらでも、この IP アドレスを手動で設定することはできません。クラスタ制御リンク ネットワークには、ユニット間のルータを含めることはできません。レイヤ 2 スイッチングのみが許可されます。 サイト間トラフィックには、オーバーレイ トランスポート仮想化（OTV）を使用することをお勧めします。

管理ネットワーク

すべてのユニットを単一の管理ネットワークに接続することを推奨します。このネットワークは、クラスタ制御リンクとは別のものです。

管理インターフェイス

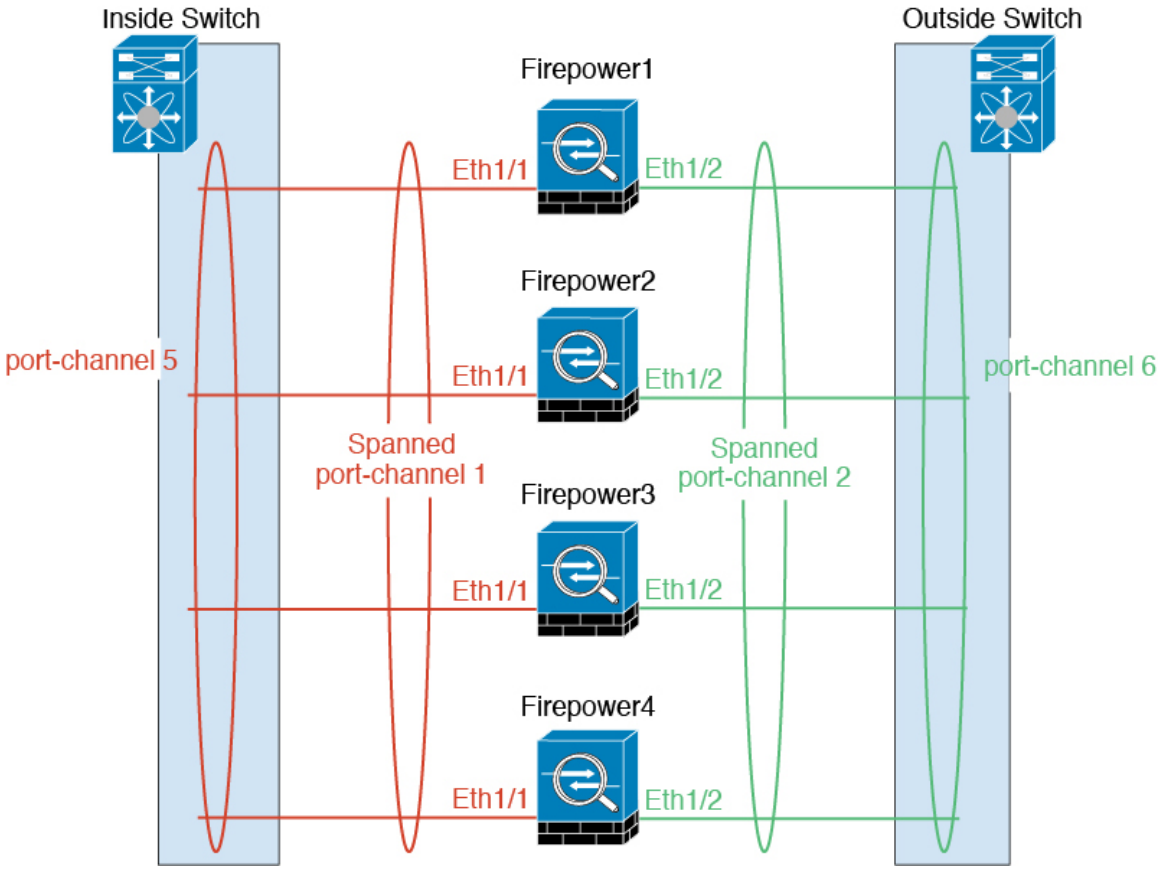
管理タイプのインターフェイスをクラスタに割り当てる必要があります。このインターフェイスはスパンド インターフェイスではなく、特別な個別インターフェイスです。管理インターフェイスによって各単位に直接接続できます。

ASA の場合は、メイン クラスタ IP アドレスはそのクラスタの固定アドレスであり、常に現在の標準出荷単位に属します。アドレス範囲も設定して、現在の標準出荷単位を含む各単位がその範囲内のローカル アドレスを使用できるようにする必要があります。このメイン クラスタ IP アドレスによって、管理アクセスのアドレスが一本化されます。標準出荷単位が変更されると、メイン クラスタ IP アドレスは新しい標準出荷単位に移動するので、クラスタの管理をシームレスに続行できます。ローカル IP アドレスは、ルーティングに使用され、トラブルシューティングにも役立ちます。たとえば、クラスタを管理するにはメイン クラスタ IP アドレスに接続します。このアドレスは常に、現在の標準出荷単位に関連付けられています。個々のメンバを管理するには、ローカル IP アドレスに接続します。TFTP や syslog などの発信管理トラフィックの場合、標準出荷単位を含む各単位は、ローカル IP アドレスを使用してサーバに接続します。

Firepower Threat Defense では、同じネットワークの各単位に管理 IP アドレスを割り当てます。各単位を FMCに追加するときは、次の IP アドレスを使用します。

スパンド EtherChannel

シャーシあたり 1 つ以上のインターフェイスをグループ化して、クラスタのすべてのシャーシに広がる EtherChannel とすることができます。EtherChannel によって、チャネル内の使用可能なすべてのアクティブ インターフェイスのトラフィックが集約されます。スパンド EtherChannel は、ルーテッドとトランスペアレントのどちらのファイアウォール モードでも設定できます。ルーテッド モードでは、EtherChannel は単一の IP アドレスを持つルーテッド インターフェイスとして設定されます。トランスペアレント モードでは、IP アドレスはブリッジグループ メンバーではなく BVI に割り当てられます。EtherChannel は初めから、ロードバランシング機能を基本的動作の一部として備えています。



サイト間クラスタリング

サイト間インストールの場合、次の推奨ガイドラインに従う限り、クラスタリングを利用できます。

各クラスタ シャーシを個別のサイト ID に属するように設定できます。

サイト ID は、サイト固有の MAC アドレスおよび IP アドレスと連動します。クラスタから送信されたパケットは、サイト固有の MAC アドレスおよび IP アドレスを使用するのに対し、クラスタで受信したパケットは、グローバル MAC アドレスおよび IP アドレスを使用します。この機能により、MAC フラッピングの原因となる 2 つの異なるポートで両方のサイトから同じグローバル MAC アドレスをスイッチが学習するのを防止します。代わりに、スイッチはサイトの MAC アドレスのみを学習します。サイト固有の MAC アドレスおよび IP アドレスは、スパンド EtherChannel のみを使用したルーテッド モードでサポートされます。

サイト ID は、LISP インスペクションを使用したフロー モビリティの有効化、データセンターのサイト間クラスタリングのパフォーマンス向上とラウンドトリップ時間の遅延短縮のためのディレクタ ローカリゼーションの有効化、およびトラフィック フローのバックアップ オーナーが常にオーナーとは異なるサイトに存在する接続に対するサイト冗長性の有効化のためにも使用されます。

サイト間クラスタリングの詳細については、以下の項を参照してください。

- Data Center Interconnect のサイジング：クラスタリングの要件と前提条件 （2 ページ）
- サイト間のガイドライン：クラスタリング ガイドラインと制限事項 （5 ページ）
- サイト間での例：サイト間クラスタリングの例 （68 ページ）

ASA クラスタの追加

単独の Firepower 9300 シャーシをシャーシ内クラスタとして追加することも、複数のシャーシをシャーシ間クラスタリングに追加することもできます。シャーシ間クラスタリングでは、各シャーシを別々に設定します。1 つのシャーシにクラスタを追加したら、次のシャーシにほぼ同じ設定を入力します。

ASA クラスタの作成

Firepower 4100/9300 シャーシにクラスタを展開します。

マルチ コンテキスト モードの場合、最初に論理デバイスを展開してから、ASA アプリケーションでマルチ コンテキスト モードを有効にする必要があります。

Firepower 4100/9300 シャーシからルーテッド ファイアウォール モード ASA を展開できます。ASA をトランスペアレント ファイアウォール モードに変更するには、初期導入を完了し、ASA CLI 内でファイアウォール モードを変更します。

始める前に

- モジュールがインストールされていない場合でも、Firepower 9300 シャーシの 3 つすべてのモジュール スロットでクラスタリングを有効にする必要があります。3 つすべてのモジュールを設定していないと、クラスタは機能しません。
- [Interfaces] タブで、ポート チャネル 48 クラスタ タイプのインターフェイスは、メンバ インターフェイスが含まれていない場合は、[Operation State] を [failed] と表示します。シャーシ内クラスタリングの場合、この EtherChannel はメンバインターフェイスを必要としないため、この動作状態は無視して構いません。

手順

ステップ 1 クラスタを導入する前に、少なくとも 1 つのデータ タイプのインターフェイスまたは EtherChannel（別名ポート チャネル）を設定します。EtherChannel（ポート チャネル）の追加または物理インターフェイスの設定を参照してください。

デフォルトでは、すべてのインターフェイスがクラスタに割り当てられます。導入後にクラスタにデータ インターフェイスを追加することもできます。

シャーシ間クラスタリングでは、全データ インターフェイスは 1 つ以上のメンバー インターフェイスを持つ EtherChannel である必要があります。各シャーシに EtherChannel を追加します。

ステップ 2 管理タイプのインターフェイスまたは EtherChannel を追加します。EtherChannel（ポート チャネル）の追加または物理インターフェイスの設定を参照してください。

管理インターフェイスが必要です。この管理インターフェイスは、シャーシの管理のみに使用されるシャーシ管理インターフェイスと同じではありません（FXOS では、シャーシ管理インターフェイスは MGMT、management0 のような名前で表示されます）。

ステップ 3 ポート チャネル 48 はクラスタ制御リンクとして予約されます。シャーシ間クラスタリングでは、ポート チャネル 48 に少なくとも 1 つのインターフェイスを追加します。

ステップ 4 セキュリティ サービス モードを開始します。

scope ssa

例：

```
Firepower # scope ssa
Firepower /ssa #
```

ステップ 5 クラスタを作成します。

enter logical-device *device_name* **asa** *slots* **clustered**

- *device_name*：Firepower 4100/9300 シャーシ スーパーバイザがクラスタリングを設定してインターフェイスを割り当てるために使用します。これはセキュリティ モジュール設定で使用されるクラスタ名ではありません。まだハードウェアをインストールしていなくても、3 つのセキュリティ モジュールすべてを指定する必要があります。
- スロット: シャーシ モジュールをクラスタに割り当てます。Firepower 4100 の場合は、**1** を指定します。Firepower 9300 の場合は、**1、2、3** を指定します。モジュールがインストールされていない場合でも、Firepower 9300 シャーシの 3 つすべてのモジュール スロットでクラスタリングを有効にする必要があります。3 つすべてのモジュールを設定していないと、クラスタは機能しません。

例：

```
Firepower /ssa # enter logical-device ASA1 asa 1,2,3 clustered
Firepower /ssa/logical-device* #
```

ステップ 6 管理ブートストラップ オブジェクトを作成します。

enter mgmt-bootstrap asa

例：

```
Firepower /ssa/logical-device* # enter mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

ステップ 7 管理者ユーザのパスワードを指定します。

enter bootstrap-key-secret PASSWORD

set value

exit

exit

事前設定されている ASA 管理者ユーザはパスワードの回復時に役立ちます。FXOS アクセスができる場合、管理者ユーザ パスワードを忘れたときにリセットできます。

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: happytuesday
Confirm the value: happytuesday
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

ステップ 8 クラスタ パラメータを設定します。

enter cluster-bootstrap

例：

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* #
```

ステップ 9 セキュリティ モジュール設定のクラスタ グループ名を設定します。

set service-type *cluster_name*

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

名前は 1 ～ 38 文字の ASCII 文字列であることが必要です。

ステップ 10 クラスタ インターフェイス モードを設定します。

set mode spanned-etherchannel

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* #
```

スパンド EtherChannel モードは、サポートされている唯一のモードです。

ステップ 11 管理 IP アドレス情報を設定します。

この情報は、セキュリティ モジュール設定で管理インターフェイスを設定するために使用されます。

a) ローカル IP アドレスのプールを設定します。このアドレスの 1 つが、このインターフェイス用に各クラスタ ユニットに割り当てられます。

set ipv4 pool *start_ip end_ip*

set ipv6 pool *start_ip end_ip*

最低でも、クラスタ内のユニット数と同じ数のアドレスが含まれるようにしてください。Firepower 9300 の場合、すべてのモジュール スロットが埋まっていないとしても、シャーシごとに 3 つのアドレスを含める必要があることに注意してください。クラスタを拡張する予定の場合は、アドレスを増やします。現在のマスター ユニットに属する仮想 IP アドレス（メイン クラスタ IP アドレスと呼ばれる）は、このプールの一部ではありません。必ず、同じネットワークの IP アドレスの 1 つをメイン クラスタ IP アドレス用に確保してください。IPv4 アドレスと IPv6 アドレス（どちらか一方も可）を使用できます。

b) 管理インターフェイスのメイン クラスタ IP アドレスを設定します。

set virtual ipv4 *ip_address* **mask** *mask*

set virtual ipv6 *ip_address* **prefix-length** *prefix*

この IP アドレスは、クラスタ プール アドレスと同じネットワーク上に存在している必要がありますが、プールに含まれていてはなりません。

c) ネットワーク ゲートウェイ アドレスを入力します。

set ipv4 gateway *ip_address*

set ipv6 gateway *ip_address*

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv4 gateway 10.1.1.254
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv4 pool 10.1.1.11 10.1.1.27
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv6 gateway 2001:DB8::AA
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv6 pool 2001:DB8::11 2001:DB8::27
Firepower /ssa/logical-device/cluster-bootstrap* # set virtual ipv4 10.1.1.1 mask
255.255.255.0
Firepower /ssa/logical-device/cluster-bootstrap* # set virtual ipv6 2001:DB8::1
prefix-length 64
```

ステップ 12 シャーシ ID を設定します。

set chassis-id *id*

クラスタの各シャーシは一意の ID が必要です。

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set chassis-id 1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

ステップ 13 サイト間クラスタリングの場合、サイト ID は 1 ～ 8 の範囲で設定します。

set site-id *number*.

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set site-id 1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

ステップ 14 クラスタ制御リンクの制御トラフィックの認証キーを設定します。

set key

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set key
Key: diamonddogs
```

共有秘密を入力するように求められます。

共有秘密は、1 ～ 63 文字の ASCII 文字列です。共有秘密は、キーを生成するために使用されます。このオプションは、データパス トラフィック（接続状態アップデートや転送されるパケットなど）には影響しません。データパス トラフィックは、常にクリア テキストとして送信されます。

ステップ 15 クラスタ ブートストラップ モードおよび論理デバイス モードを終了します。

exit

exit

ステップ 16 使用可能なソフトウェア バージョンを表示し、使用するバージョンを設定します。

a) 使用可能なバージョンを表示します。

show app

例：

```
/ssa # show app

Application:
    Name       Version    Description Author     Deploy Type  CSP Type    Is Default
 App
    ---------- ---------- ----------- ---------- -----------  -----------
--------------
    asa        9.1.4.152  N/A         cisco      Native       Application Yes
    asa        9.4.2      N/A         cisco      Native       Application No
    asa        9.5.2.1    N/A         cisco      Native       Application No
```

b) 使用するバージョンのアプリケーション モードに入ります。

scope app asa *version_number*

c) このバージョンをデフォルトとして設定します。

set-default

d) アプリケーション モードを終了します。

exit

例：

```
/ssa* # scope app asa 9.5.2.1
/ssa/app* # set-default
/ssa/app* # exit
```

```
/ssa* #
```

ステップ 17 設定をコミットします。

commit-buffer

Firepower 4100/9300 シャーシ スーパーバイザは、デフォルトのセキュリティ モジュール ソフトウェアバージョンをダウンロードし、各セキュリティモジュールにクラスタブートストラップコンフィギュレーションと管理インターフェイス設定をプッシュすることで、クラスタを導入します。

ステップ 18 クラスタに別のシャーシを追加する場合は、この手順を繰り返しますが、固有の **chassis-id** と正しい **site-id** を設定する必要があります。それ以外の場合は、両方のシャーシで同じ設定を使用します。

ステップ 19 マスター ユニット ASA に接続して、クラスタリング設定をカスタマイズします。

例

シャーシ 1：

```
scope eth-uplink
  scope fabric a
    enter port-channel 1
      set port-type data
      enable
      enter member-port Ethernet1/1
        exit
      enter member-port Ethernet1/2
        exit
      exit
    enter port-channel 2
      set port-type data
      enable
      enter member-port Ethernet1/3
        exit
      enter member-port Ethernet1/4
        exit
      exit
    enter port-channel 3
      set port-type data
      enable
      enter member-port Ethernet1/5
        exit
      enter member-port Ethernet1/6
        exit
      exit
    enter port-channel 4
      set port-type mgmt
      enable
      enter member-port Ethernet2/1
        exit
      enter member-port Ethernet2/2
        exit
      exit
    enter port-channel 48
      set port-type cluster
```

```
      enable
      enter member-port Ethernet2/3
        exit
      exit
    exit
  exit
commit-buffer

scope ssa
  enter logical-device ASA1 asa "1,2,3" clustered
    enter cluster-bootstrap
      set chassis-id 1
      set ipv4 gateway 10.1.1.254
      set ipv4 pool 10.1.1.11 10.1.1.27
      set ipv6 gateway 2001:DB8::AA
      set ipv6 pool 2001:DB8::11 2001:DB8::27
      set key
      Key: f@arscape
      set mode spanned-etherchannel
      set service-type cluster1
      set virtual ipv4 10.1.1.1 mask 255.255.255.0
      set virtual ipv6 2001:DB8::1 prefix-length 64
      exit
    exit
  scope app asa 9.5.2.1
    set-default
    exit
  commit-buffer
```

シャーシ 2：

```
scope eth-uplink
  scope fabric a
    create port-channel 1
      set port-type data
      enable
      create member-port Ethernet1/1
        exit
      create member-port Ethernet1/2
        exit
      exit
    create port-channel 2
      set port-type data
      enable
      create member-port Ethernet1/3
        exit
      create member-port Ethernet1/4
        exit
      exit
    create port-channel 3
      set port-type data
      enable
      create member-port Ethernet1/5
        exit
      create member-port Ethernet1/6
        exit
      exit
    create port-channel 4
      set port-type mgmt
      enable
      create member-port Ethernet2/1
        exit
```

```
      create member-port Ethernet2/2
        exit
      exit
    create port-channel 48
      set port-type cluster
      enable
      create member-port Ethernet2/3
        exit
      exit
    exit
  exit
commit-buffer

scope ssa
  enter logical-device ASA1 asa "1,2,3" clustered
    enter cluster-bootstrap
      set chassis-id 2
      set ipv4 gateway 10.1.1.254
      set ipv4 pool 10.1.1.11 10.1.1.15
      set ipv6 gateway 2001:DB8::AA
      set ipv6 pool 2001:DB8::11 2001:DB8::19
      set key
      Key: f@rscape
      set mode spanned-etherchannel
      set service-type cluster1
      set virtual ipv4 10.1.1.1 mask 255.255.255.0
      set virtual ipv6 2001:DB8::1 prefix-length 64
      exit
    exit
  scope app asa 9.5.2.1
    set-default
    exit
  commit-buffer
```

クラスタ メンバの追加

ASA クラスタ メンバを追加または置き換えます。

（注） この手順は、シャーシの追加または置換にのみ適用されます。クラスタリングがすでに有効になっている Firepower 9300 にモジュールを追加または置換する場合、モジュールは自動的に追加されます。

始める前に

- 既存のクラスタに、この新しいメンバ用の管理 IP アドレスプール内で十分な IP アドレスが割り当てられているようにしてください。それ以外の場合は、この新しいメンバを追加する前に、各シャーシ上の既存のクラスタブートストラップ設定を編集する必要があります。この変更により論理デバイスが再起動します。
- インターフェイスの設定は、新しいシャーシでの設定と同じである必要があります。

- マルチ コンテキスト モードでは、最初のクラスタ メンバの ASA アプリケーションでマルチ コンテキスト モードを有効にします。追加のクラスタ メンバはマルチ コンテキスト モード設定を自動的に継承します。

手順

クラスタに別のシャーシを追加する場合は、ASA クラスタの作成 （30 ページ） の手順を繰り返しますが、一意の **chassis-id** と正しい **site-id** を設定する必要があります。それ以外の場合は、新しいシャーシに同じ設定を使用します。

Firepower Threat Defense Cluster の追加

単独の Firepower 9300 シャーシをシャーシ内クラスタとして追加することも、複数のシャーシをシャーシ間クラスタリングに追加することもできます。 シャーシ間クラスタリングでは、各シャーシを別々に設定します。1 つのシャーシにクラスタを追加したら、次のシャーシにほぼ同じ設定を入力します。

Firepower Threat Defense クラスタの作成

クラスタは、Firepower 4100/9300 シャーシ スーパバイザから簡単に展開できます。すべての初期設定が各ユニットに自動的に生成されます。 シャーシ間クラスタリングでは、各シャーシを別々に設定します。展開を容易にするために、1 つのシャーシにクラスタを展開し、その後、最初のシャーシから次のシャーシにブートストラップ コンフィギュレーションをコピーできます。

始める前に

- モジュールがインストールされていない場合でも、Firepower 9300 シャーシの 3 つすべてのモジュール スロットでクラスタリングを有効にする必要があります。3 つすべてのモジュールを設定していないと、クラスタは機能しません。
- [Interfaces] タブで、ポート チャネル 48 クラスタ タイプのインターフェイスは、メンバ インターフェイスが含まれていない場合は、[Operation State] を [failed] と表示します。シャーシ内クラスタリングの場合、この EtherChannel はメンバインターフェイスを必要としないため、この動作状態は無視して構いません。

手順

ステップ 1 クラスタを展開する前に、1 つ以上のデータ型のインターフェイスまたは EtherChannel（別名ポート チャネル）を設定します。EtherChannel（ポート チャネル）の追加または物理インターフェイスの設定を参照してください。

また、データ インターフェイスはクラスタを展開した後でも、そのクラスタに追加できます。

シャーシ間クラスタリングでは、全データ インターフェイスは 1 つ以上のメンバー インターフェイスを持つ EtherChannel である必要があります。各シャーシに EtherChannel を追加します。

ステップ 2 （任意）クラスタを展開する前に Firepower-eventing タイプのインターフェイスを設定します。物理インターフェイスの設定を参照してください。

このインターフェイスは、FTD デバイスのセカンダリ管理インターフェイスです。このインターフェイスを使用するには、FTD CLI で IP アドレスなどのパラメータを設定する必要があります。たとえば、イベント（Web イベントなど）から管理トラフィックを分類できます。Firepower Management Center コマンド リファレンスの **configure network** コマンドを参照してください。

ステップ 3 管理タイプのインターフェイスまたは EtherChannel を追加します。EtherChannel（ポート チャネル）の追加または物理インターフェイスの設定を参照してください。

管理インターフェイスが必要です。この管理インターフェイスは、シャーシの管理のみに使用されるシャーシ管理インターフェイスと同じではありません（FXOS では、シャーシ管理インターフェイスは MGMT、management0 のような名前で表示されます）。

ステップ 4 ポート チャネル 48 はクラスタ制御リンクとして予約されます。シャーシ間クラスタリングでは、ポート チャネル 48 に少なくとも 1 つのインターフェイスを追加します。

ステップ 5 セキュリティ サービス モードを開始します。

scope ssa

例：

```
Firepower # scope ssa
Firepower /ssa #
```

ステップ 6 クラスタを作成します。

enter logical-device *device_name* **ftd "1,2,3" clustered**

例：

```
Firepower /ssa # enter logical-device FTD1 ftd "1,2,3" clustered
Firepower /ssa/logical-device* #
```

device_name は、Firepower 4100/9300 シャーシ スーパーバイザがクラスタリングを設定してインターフェイスを割り当てるために使用します。これはセキュリティ モジュール設定で使用されるクラスタ名ではありません。

（注） モジュールがインストールされていない場合でも、シャーシの 3 つすべてのモジュール スロットでクラスタリングを有効にする必要があります。3 つすべてのモジュールを設定していないと、クラスタは機能しません。

ステップ 7 クラスタ ブートストラップ パラメータを設定します。

a) クラスタ ブートストラップ オブジェクトを作成します。

enter cluster-bootstrap

b) シャーシ ID を設定します。

set chassis-id *id*

クラスタの各シャーシは一意の ID が必要です。

c) サイト間クラスタリングの場合、サイト ID は 1 ～ 8 の範囲で設定します。

set site-id *number*.

サイト ID を削除するには、値を **0** に設定します。

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set site-id 1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

d) セキュリティ モジュール設定のクラスタ キーを設定します。

set key

共有秘密を入力するように求められます。

共有秘密は、1 ～ 63 文字の ASCII 文字列です。共有秘密は、キーを生成するために使用されます。このオプションは、データパス トラフィック（接続状態アップデートや転送されるパケットなど）には影響しません。データパス トラフィックは、常にクリア テキストとして送信されます。

e) クラスタ インターフェイス モードを設定します。

set mode spanned-etherchannel

スパンド EtherChannel モードは、サポートされている唯一のモードです。

f) セキュリティ モジュール設定のクラスタ グループ名を設定します。

set service-type *cluster_name*

名前は 1 ～ 38 文字の ASCII 文字列であることが必要です。

g) クラスタ ブートストラップ モードを終了します。

exit

例：

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* # set chassis-id 1
Firepower /ssa/logical-device/cluster-bootstrap* # set key
  Key: f@arscape
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* # exit
Firepower /ssa/logical-device/* #
```

ステップ 8 管理ブートストラップ パラメータを設定します。

a) 管理ブートストラップ オブジェクトを作成します。

enter mgmt-bootstrap ftd

b) 管理 Firepower Management Center の IP アドレスを指定します。

enter bootstrap-key FIREPOWER_MANAGER_IP

set value *IP_address*

exit

c) 論理デバイスが動作するモードを指定します（ルーテッドまたはトランスペアレント）。

enter bootstrap-key FIREWALL_MODE

set value {**routed** | **transparent**}

exit

d) デバイスと Firepower Management Center との間で共有するキーを指定します。

enter bootstrap-key-secret REGISTRATION_KEY

set value

registration_key

exit

e) 論理デバイスで使用するパスワードを指定します。

enter bootstrap-key-secret PASSWORD

set value

password

exit

f) 論理デバイスの完全修飾ホスト名を指定します。

enter bootstrap-key FQDN

set value *fqdn*

exit

g) 論理デバイスが使用する DNS サーバのカンマ区切りのリストを指定します。

enter bootstrap-key DNS_SERVERS

set value *dns_servers*

exit

h) 論理デバイスの検索ドメインのカンマ区切りのリストを指定します。

enter bootstrap-key SEARCH_DOMAINS

set value *search_domains*

exit

i) クラスタ内の各セキュリティ モジュールの管理 IP アドレスを設定します。

（注） Firepower 9300 の場合、モジュールがインストールされていない場合でも、シャーシの 3 つすべてのモジュール スロットで IP アドレスを設定する必要があります。3 つすべてのモジュールを設定していないと、クラスタは機能しません。

IPv4 管理インターフェイス オブジェクトを作成するには、次の手順を実行します。

1. 管理インターフェイス オブジェクトを作成します。

   enter ipv4 *slot_id* **firepower**

2. ゲートウェイ アドレスを設定します。

   set gateway *gateway_address*

3. IP アドレスとマスクを設定します。

   set ip *ip_address* **mask** *network_mask*

4. 管理 IP モードを終了します。

   exit

5. シャーシの残りのモジュールに対して手順を繰り返します。

IPv6 管理インターフェイス オブジェクトを作成するには、次の手順を実行します。

1. 管理インターフェイス オブジェクトを作成します。

   enter ipv6 *slot_id* **firepower**

2. ゲートウェイ アドレスを設定します。

   set gateway *gateway_address*

3. IP アドレスとプレフィックスを設定します。

   set ip *ip_address* **prefix-length** *prefix*

4. 管理 IP モードを終了します。

   exit

5. シャーシの残りのモジュールに対して手順を繰り返します。

j) 管理ブートストラップ モードを終了します。

   exit

例：

```
Firepower /ssa/logical-device* # enter mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key FIREPOWER_MANAGER_IP
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.0.0.100
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key-secret REGISTRATION_KEY
```

```
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
  Value: ziggy$tardust
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
  Value: $pidersfrommars
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key FQDN
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value example.cisco.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key DNS_SERVERS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 192.168.1.1
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key SEARCH_DOMAINS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value example.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter ipv4 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.31 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter ipv4 2 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.32 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter ipv4 3 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.33 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

ステップ 9 論理デバイス モードを終了します。

exit

ステップ 10 使用可能なソフトウェア バージョンを表示し、使用するバージョンを設定します。

a) 使用可能なバージョンを表示します。

show app

例：

```
/ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default
 App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------

    ftd        6.0.1.37   N/A         cisco      Native      Application Yes
    ftd        6.1.0.11   N/A         cisco      Native      Application No
    ftd        6.1.0.21   N/A         cisco      Native      Application No
```

b) 使用するバージョンのアプリケーション モードに入ります。

scope app ftd *version_number*

c) このバージョンをデフォルトとして設定します。

set-default

d) このバージョンのエンドユーザ ライセンス契約書に同意します。

accept-license-agreement

e) アプリケーション モードを終了します。

exit

例：

```
/ssa # scope app ftd 6.1.0.21
/ssa/app # set-default
/ssa/app* # accept-license-agreement
/ssa/app* # exit
/ssa* #
```

ステップ 11 設定をコミットします。

commit-buffer

Firepower 4100/9300 シャーシ スーパーバイザは、デフォルトのセキュリティ モジュール ソフトウェア バージョンをダウンロードし、各セキュリティ モジュールにクラスタ ブートストラップ コンフィギュレーションと管理インターフェイス設定をプッシュすることで、クラスタを導入します。

ステップ 12 クラスタに別のシャーシを追加するには、この手順を繰り返しますが、固有の **chassis-id** および固有の管理IPアドレスを設定する必要がある場合は設定し、そうでない場合は両方のシャーシで同じ設定を使用します。

ステップ 13 各セキュリティ モジュールを、管理 IP アドレスを使用する Firepower Management Center に追加してから、Web インターフェイスでクラスタにグループ化します。

すべてのクラスタ ユニットは、Firepower Management Center に追加する前に、FXOS で正常な形式のクラスタ内に存在している必要があります。

例

```
scope eth-uplink
  scope fabric a
    enter port-channel 1
      set port-type data
      enable
      create member-port Ethernet1/1
        exit
      create member-port Ethernet1/2
        exit
      exit
    enter port-channel 2
      set port-type data
      enable
      create member-port Ethernet1/3
        exit
      create member-port Ethernet1/4
        exit
```

```
      exit
    enter port-channel 3
      set port-type firepower-eventing
      enable
      create member-port Ethernet1/5
        exit
      create member-port Ethernet1/6
        exit
      exit
    enter port-channel 4
      set port-type mgmt
      enable
      create member-port Ethernet2/1
        exit
      enter member-port Ethernet2/2
        exit
      exit
    enter port-channel 48
      set port-type cluster
      enable
      enter member-port Ethernet2/3
        exit
      exit
    exit
  exit
commit-buffer

scope ssa
  enter logical-device FTD1 ftd "1,2,3" clustered
    enter cluster-bootstrap
      set chassis-id 1
      set key cluster_key
      set mode spanned-etherchannel
      set service-type ftd-cluster
      exit
    enter mgmt-bootstrap ftd
      enter bootstrap-key FIREPOWER_MANAGER_IP
        set value 10.0.0.100
        exit
      enter bootstrap-key FIREWALL_MODE
        set value transparent
        exit
      enter bootstrap-key-secret REGISTRATION_KEY
        set value
          Value: alladinsane
        exit
      enter bootstrap-key-secret PASSWORD
        set value
          Value: widthofacircle
        exit
      enter bootstrap-key FQDN
        set value ftd.cisco.com
        exit
      enter bootstrap-key DNS_SERVERS
        set value 192.168.1.1
        exit
      enter bootstrap-key SEARCH_DOMAINS
        set value search.com
        exit
      enter ipv4 1 firepower
        set gateway 10.0.0.1
        set ip 10.0.0.31 mask 255.255.255.0
        exit
      enter ipv4 2 firepower
```

```
        set gateway 10.0.0.1
        set ip 10.0.0.32 mask 255.255.255.0
        exit
      enter ipv4 3 firepower
        set gateway 10.0.0.1
        set ip 10.0.0.33 mask 255.255.255.0
        exit
      exit
    exit
  scope app ftd 6.0.0.837
    accept-license-agreement
    exit
  commit-buffer
```

シャーシ 2：

```
scope eth-uplink
  scope fabric a
    enter port-channel 1
      set port-type data
      enable
      create member-port Ethernet1/1
        exit
      create member-port Ethernet1/2
        exit
      exit
    enter port-channel 2
      set port-type data
      enable
      create member-port Ethernet1/3
        exit
      create member-port Ethernet1/4
        exit
      exit
    enter port-channel 3
      set port-type firepower-eventing
      enable
      create member-port Ethernet1/5
        exit
      create member-port Ethernet1/6
        exit
      exit
    enter port-channel 4
      set port-type mgmt
      enable
      create member-port Ethernet2/1
        exit
      enter member-port Ethernet2/2
        exit
      exit
    enter port-channel 48
      set port-type cluster
      enable
      enter member-port Ethernet2/3
        exit
      exit
    exit
  exit
commit-buffer

scope ssa
  enter logical-device FTD1 ftd "1,2,3" clustered
    enter cluster-bootstrap
```

```
    set chassis-id 2
    set key cluster_key
    set mode spanned-etherchannel
    set service-type ftd-cluster
    exit
  enter mgmt-bootstrap ftd
    enter bootstrap-key FIREPOWER_MANAGER_IP
      set value 10.0.0.100
      exit
    enter bootstrap-key FIREWALL_MODE
      set value transparent
      exit
    enter bootstrap-key-secret REGISTRATION_KEY
      set value
        Value: alladinsane
      exit
    enter bootstrap-key-secret PASSWORD
      set value
        Value: widthofacircle
      exit
    enter bootstrap-key FQDN
      set value ftd.cisco.com
      exit
    enter bootstrap-key DNS_SERVERS
      set value 192.168.1.1
      exit
    enter bootstrap-key SEARCH_DOMAINS
      set value search.com
      exit
    enter ipv4 1 firepower
      set gateway 10.0.0.1
      set ip 10.0.0.31 mask 255.255.255.0
      exit
    enter ipv4 2 firepower
      set gateway 10.0.0.1
      set ip 10.0.0.32 mask 255.255.255.0
      exit
    enter ipv4 3 firepower
      set gateway 10.0.0.1
      set ip 10.0.0.33 mask 255.255.255.0
      exit
    exit
  exit
scope app ftd 6.0.0.837
  accept-license-agreement
  exit
commit-buffer
```

クラスタ メンバの追加

既存のクラスタ内の FTD クラスタ メンバを追加または置き換えます。

（注） この手順における FXOS の手順は、新しいシャーシの追加のみに適用されます。クラスタリングがすでに有効になっている Firepower 9300 に新しいモジュールを追加する場合、モジュールは自動的に追加されます。ただし、Firepower Management Center に新しいモジュールを追加する必要があります。Firepower Management Center の手順までスキップします。

始める前に

- 置き換える場合は、Firepower Management Center から古いクラスタ メンバを削除する必要があります。新しいユニットに置き換えると、Firepower Management Center 上の新しいデバイスとみなされます。
- インターフェイスの設定は、新しいシャーシでの設定と同じである必要があります。

手順

ステップ 1 別のシャーシをクラスタに追加するには、Firepower Threat Defense クラスタの作成 （38 ページ） の手順を繰り返します（次の設定を固有のものとして設定する必要のある場合を除きます。そうでない場合には、両方のシャーシに同じ設定を使用します）。

- シャーシ ID（Chassis ID）
- 管理 IP アドレス

ステップ 2 Firepower Management Center で、**[Devices]** > **[Device Management]** を選択してから **[Add]** > **[Add Device]** を選択して、新しい論理デバイスを追加します。

ステップ 3 **[Add]** > **[Add Cluster]** を選択します。

ステップ 4 ドロップダウン リストから現在の [Master] デバイスを選択します。

クラスタにすでに含まれているマスターデバイスを選択した場合、既存のクラスタの名前が自動入力され、[Slave Devices] ボックスに選択可能なすべてのスレーブ デバイスが表示されます。これには、FMC に追加したばかりの新しいユニットが含まれます。

ステップ 5 [Add] をクリックし、次に [Deploy] をクリックします。

クラスタは新しいメンバを追加して更新されます。

Radware DefensePro の設定

Cisco Firepower 4100/9300 シャーシは、単一ブレードで複数のサービス（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とサービスは、リンクされて、サービス チェーンを形成します。

Radware DefensePro について

現在サービスされているサービス チェーン コンフィギュレーションでは、サードパーティ製の Radware DefensePro 仮想プラットフォームを ASA ファイアウォールの手前、または Firepower Threat Defense の手前で実行するようにインストールできます。Radware DefensePro は、Firepower 4100/9300 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。Firepower 4100/9300 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トラフィックは主要な ASA または Firepower Threat Defense ファイアウォールに到達する前に DefensePro 仮想プラットフォームを通過する必要があります。

（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 仮想プラットフォームは、リンク デコレータと呼ばれることもあります。

Radware DefensePro の前提条件

Radware DefensePro を Firepower 4100/9300 シャーシに導入する前に、**etc/UTC** タイムゾーンで NTP サーバを使用するように Firepower 4100/9300 シャーシを構成する必要があります。Firepower 4100/9300 シャーシの日付と時刻の設定の詳細については、日時の設定を参照してください。

サービス チェーンのガイドライン

モデル

- Radware DefensePro（vDP）プラットフォームは、次のセキュリティ アプライアンスの ASA でサポートされています。
  - Firepower 9300
  - Firepower 4120：このプラットフォームでは、CLI を使用して Radware DefensePro を導入する必要があります。Firepower Chassis Manager は、この機能をサポートしていません。
  - Firepower 4140：このプラットフォームでは、CLI を使用して Radware DefensePro を導入する必要があります。Firepower Chassis Manager は、この機能をサポートしていません。
  - Firepower 4150
- Radware DefensePro プラットフォームは、次のセキュリティ アプライアンスの Firepower Threat Defense でサポートされています。
  - Firepower 9300
  - Firepower 4110：論理デバイスと同時に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。

- Firepower 4120：論理デバイスと同時に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。
- Firepower 4140
- Firepower 4150

その他のガイドライン

- 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。

スタンドアロンの論理デバイスでの Radware DefensePro の設定

スタンドアロン ASA または Firepower Threat Defense 論理デバイスの前にある単一のサービス チェーンに Radware DefensePro をインストールするには、次の手順に従います。

始める前に

- vDP イメージを Cisco.com からダウンロードして（Cisco.com からのイメージのダウンロードを参照）、そのイメージを Firepower 4100/9300 シャーシにダウンロードします（Firepower 4100/9300 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）。
- Radware DefensePro アプリケーションは、シャーシ内クラスタのスタンドアロン構成で導入できます。シャーシ内クラスタリングについては、シャーシ内クラスタの Radware DefensePro の設定 （53 ページ）を参照してください。

手順

ステップ 1 vDP で別の管理インターフェイスを使用する場合は、物理インターフェイスの設定に従ってインターフェイスを有効にし、そのタイプが mgmt になるように設定してください。そうしない場合、アプリケーション管理インターフェイスを共有できます。

ステップ 2 スタンドアロン構成で ASA または Firepower Threat Defense 論理デバイスを作成します（スタンドアロン ASA の追加 （10 ページ）またはスタンドアロン Firepower Threat Defense の追加 （15 ページ）を参照）。 Firepower 4110 または 4120 セキュリティ アプライアンス上にイメージをインストールする場合には、設定をコミットする前に、vDP を Firepower Threat Defense イメージとともにインストールする必要があることに注意してください。

ステップ 3 セキュリティ サービス モードを開始します。

```
Firepower# scope ssa
```

ステップ 4 Radware vDP インスタンスを作成します。

Firepower /ssa # **scope slot** *slot_id*

Firepower /ssa/slot # **create app-instance vdp**

Firepower /ssa/slot/app-instance* # **exit**

Firepower /ssa/slot/* # **exit**

ステップ 5 設定をコミットします。

commit-buffer

ステップ 6 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。

Firepower /ssa # **show app-instance**

例：

```
Firepower /ssa # show app-instance
App Name   Slot ID    Admin State Oper State      Running Version Startup Version Cluster
 State   Cluster Role
---------- ---------- ----------- ---------------- --------------- ---------------
--------------- ------------
ftd        1          Enabled     Online           6.2.1.62        6.2.1.62        Not
Applicable  None
vdp        1          Disabled    Installing                       8.10.01.16-5    Not
Applicable  None
```

ステップ 7 （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
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
10 40960 No
VDP-2-CORES all 2 8192 No
VDP-4-CORES all 4 16384 No
VDP-8-CORES FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36,
 FPR4K-SM-24
8 32768 No
```

ステップ 8 （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**

ステップ 9 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*

ステップ 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** *nameinterface_id* **vdp**

Firepower /ssa/logical-device/external-port-link* # **exit**

ステップ 11 vDP の外部管理インターフェイス設定を設定します。

a) ブートストラップ オブジェクトを作成します。

Firepower /ssa/logical-device* # **create mgmt-bootstrap vdp**

b) 管理 IP アドレスを設定します。

Firepower /ssa/logical-device/mgmt-bootstrap* #**create ipv4** *slot_id* **default**

c) ゲートウェイ アドレスを設定します。

Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* #**set gateway** *gateway_address*

d) IP アドレスとマスクを設定します。

Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* #**set ip** *ip_address* **mask** *network_mask*

e) 管理 IP 設定スコープを終了します。

Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* #**exit**

f) 管理ブートストラップ設定スコープを終了します。

Firepower /ssa/logical-device/mgmt-bootstrap* #**exit**

ステップ 12 ASA または Firepower Threat Defense フローの前に vDP を配置するデータ インターフェイスを編集します。

Firepower /ssa/logical-device* # **scope external-port-link** *name*

show external-port-link コマンドを入力して、インターフェイス名を表示します。

ステップ 13 論理デバイスに vDP を追加します。

Firepower /ssa/logical-device/external-port-link* # **set decorator vdp**

vDP を使用するインターフェイスごとに手順を繰り返します。

ステップ 14 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ことを確認します。

Firepower /ssa/logical-device/external-port-link* # **show detail**

例：

```
Firepower /ssa/logical-device/external-port-link # show detail

External-Port Link:
    Name: Ethernet11_ftd
    Port or Port Channel Name: Ethernet1/1
    App Name: ftd
    Description:
    Link Decorator: vdp
```

ステップ 15 設定をコミットします。

commit-buffer

次のタスク

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。

シャーシ内クラスタの Radware DefensePro の設定

（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 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。

始める前に

- vDP イメージを Cisco.com からダウンロードして（Cisco.com からのイメージのダウンロードを参照）、そのイメージを Firepower 4100/9300 シャーシにダウンロードします（Firepower 4100/9300 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）。

手順

ステップ 1 vDP で別の管理インターフェイスを使用する場合は、物理インターフェイスの設定に従ってインターフェイスを有効にし、そのタイプが mgmt になるように設定してください。そうしない場合、アプリケーション管理インターフェイスを共有できます。

ステップ 2 ASA シャーシ内クラスタ（ASA クラスタの作成 （30 ページ）を参照）、または Firepower Threat Defense シャーシ内クラスタ（Firepower Threat Defense クラスタの作成 （38 ページ）を参照）を設定します。

ステップ 3 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* { **asa** | **ftd** }

set **decorator vdp**

set **description ""**

exit

ステップ 4 論理デバイスの外部管理ポートを割り当てます。

enter **external-port-link** *{ mgmt_asa | mgmt_ftd } interface_id { asa | ftd }*

set **decorator ""**

set **description ""**

exit

ステップ 5 DefensePro の外部管理ポートを割り当てます。

enter **external-port-link mgmt_vdp** *interface_name { asa | ftd }*

set **decorator ""**

set **description ""**

ステップ 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
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
10 40960 No
VDP-2-CORES all 2 8192 No
VDP-4-CORES all 4 16384 No
VDP-8-CORES FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36,
 FPR4K-SM-24
8 32768 No
```

ステップ 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。

（注） この変更をコミットすると、FXOS シャーシが再起動します。

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**

ステップ 8 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 *{ asa | ftd }*

set **decorator ""**

set **description ""**

exit

ステップ 9 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

例：

```
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
```

ステップ 10 管理ブートストラップ設定スコープを終了します。

exit

ステップ 11 マスター ブレード上の DefensePro アプリケーション インスタンスを入力します。

connect module *slot* **console**

connect vdp

ステップ 12 マスター ブレードで、管理 IP を設定します。

device clustering management-channel ip

ステップ 13 前のステップで確認した IP を使用して、マスター IP を設定します。

device clustering master set *management-channel ip*

ステップ 14 クラスタを有効化します。

device clustering state set enable

ステップ 15 アプリケーション コンソールを終了して FXOS モジュール CLI に戻ります。

Ctrl]

ステップ 16 ステップ 10、12、13、14 を繰り返してステップ 11 で確認したマスター IP を設定し、各ブレード アプリケーション インスタンスに対してクラスタを有効化します。

ステップ 17 設定をコミットします。

commit-buffer

（注） 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。

ステップ 18 DefensePro アプリケーションのすべてがクラスタに参加していることを確認します。

device cluster show

ステップ 19 以下のいずれかの方法で、「primary」と「secondary」の DefensePro インスタンスがどれであるかを確認します。

a) DefensePro インスタンスの範囲を指定し、DefensePro のアプリケーション属性のみを表示します。

scope ssa

scope slot *slot_number*

scope app-instance vdp

show app-attri

b) スロットの範囲を指定し、DefensePro インスタンスの詳細を表示します。このアプローチでは、スロット上の論理デバイスと vDP 両方のアプリケーション インスタンス情報が表示されます。

scope ssa

scope *slot_number*

show app-instance expand detail

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。

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

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。

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

例

```
scope ssa
  enter logical-device ld asa "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 asa
         set decorator vdp
         set description ""
     exit
     enter external-port-link Ethernet1-3_asa Ethernet1/3 asa
         set decorator ""
         set description ""
     exit
     enter external-port-link mgmt_asa Ethernet1/1 asa
         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 asa
         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
    App Attribute:
        App Attribute Key: cluster-role
        Value: unknown
```

次のタスク

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。

UDP/TCP ポートのオープンと vDP Web サービスの有効化

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**

Radware 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、FXOS CLI を使用して vDP Web サービスを有効にする必要があります。

手順

ステップ 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

ステップ 2 vDP Web サービスを有効化します。

manage secure-web status set enable

ステップ 3 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]

論理デバイスの管理

論理デバイスを削除し、ASA をトランスペアレント モードに変換し、インターフェイス コンフィギュレーションを変更し、既存の論理デバイスで他のタスクを実行できます。

アプリケーションのコンソールへの接続

次の手順に従ってアプリケーションのコンソールに接続します。

手順

ステップ 1 モジュール CLI に接続します。

connect module *slot_number* **console**

複数のセキュリティ モジュールをサポートしないデバイスのセキュリティ エンジンに接続するには、常に *slot_number* として **1** を使用します。

例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

ステップ 2 アプリケーションのコンソールに接続します。 デバイスの適切なコマンドを入力します。

connect asa

connect ftd

connect vdp *name*

例：

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

例：

```
Firepower-module1> connect ftd
Connecting to ftd(ftd-native) console... enter exit to return to bootCLI
>
```

ステップ 3 アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

- ASA：**Ctrl-a, d** と入力
- FTD：**Ctrl-a, d** と入力
- vDP：**Ctrl-], .** と入力

トラブルシューティングのために FXOS モジュールの CLI を使用する場合があります。

ステップ 4 FXOS CLI のスーパバイザ レベルに戻ります。

a) ~ と入力

Telnet アプリケーションに切り替わります。

b) Telnet アプリケーションを終了するには、次を入力します。

telnet>**quit**

例

次に、セキュリティ モジュール 1 の ASA に接続してから、FXOS CLI のスーパバイザ レベルに戻る例を示します。

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect asa
asa> ~
telnet> quit
Connection closed.
Firepower#
```

論理デバイスの削除

手順

ステップ 1 セキュリティ サービス モードを開始します。

Firepower# **scope ssa**

ステップ 2 シャーシ上の論理デバイスの詳細を表示します。

Firepower /ssa # **show logical-device**

ステップ 3 削除する論理デバイスごとに、次のコマンドを入力します。

Firepower /ssa # **delete logical-device** *device_name*

ステップ 4 論理デバイスにインストールされているアプリケーションの詳細を表示します。

Firepower /ssa # **show app-instance**

ステップ 5 削除するアプリケーションごとに、次のコマンドを入力します。

a) Firepower /ssa # **scope slot** *slot_number*
b) Firepower /ssa/slot # **delete app-instance** *application_name*
c) Firepower /ssa/slot # **exit**

ステップ 6 設定をコミットします。

commit-buffer

トランザクションをシステムの設定にコミットします。

例

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

Logical Device:
    Name       Description Slot ID    Mode       Operational State        Template Name
    ---------- ----------- ---------- ---------- ------------------------ -------------
    FTD                    1,2,3      Clustered  Ok                       ftd
Firepower /ssa # delete logical-device FTD
Firepower /ssa* # show app-instance
Application Name     Slot ID     Admin State     Operational State    Running Version
Startup Version Cluster Oper State
-------------------- ----------- --------------- -------------------- ---------------
--------------- ------------------
ftd                              1 Disabled        Stopping             6.0.0.837
6.0.0.837       Not Applicable
ftd                              2 Disabled        Offline              6.0.0.837
6.0.0.837       Not Applicable
ftd                              3 Disabled        Not Available
6.0.0.837       Not Applicable
Firepower /ssa* # scope slot 1
Firepower /ssa/slot # delete app-instance ftd
Firepower /ssa/slot* # exit
Firepower /ssa* # scope slot 2
Firepower /ssa/slot # delete app-instance ftd
Firepower /ssa/slot* # exit
Firepower /ssa* # scope slot 3
Firepower /ssa/slot # delete app-instance ftd
Firepower /ssa/slot* # exit
Firepower /ssa* # commit-buffer
```

論理デバイスに関連付けられていないアプリケーションインスタンスの削除

論理デバイスを削除すると、その論理デバイスのアプリケーション設定も削除するかどうかが尋ねられます。アプリケーション設定を削除しない場合、そのアプリケーションインスタンスが削除されるまで、別のアプリケーションを使用して論理デバイスを作成することはできません。セキュリティモジュール/エンジンが論理デバイスとすでに関連付けられていない場合は、アプリケーション インスタンスを削除するために以下の手順を使用できます。

手順

ステップ 1 セキュリティ サービス モードを開始します。

Firepower# **scope ssa**

ステップ 2 インストール済みアプリケーションの詳細を表示します。

Firepower /ssa # **show app-instance**

ステップ 3 削除するアプリケーションごとに、次のコマンドを入力します。

a) Firepower /ssa # **scope slot** *slot_number*
b) Firepower /ssa/slot # **delete app-instance** *application_name*
c) Firepower /ssa/slot # **exit**

ステップ 4 設定をコミットします。

commit-buffer

トランザクションをシステムの設定にコミットします。

例

```
Firepower# scope ssa
Firepower /ssa* # show app-instance
Application Name     Slot ID     Admin State     Operational State    Running Version
Startup Version Cluster Oper State
-------------------- ----------- --------------- -------------------- ---------------
--------------- ------------------
ftd                              1 Disabled        Stopping             6.0.0.837
6.0.0.837       Not Applicable
ftd                              2 Disabled        Offline              6.0.0.837
6.0.0.837       Not Applicable
ftd                              3 Disabled        Not Available
6.0.0.837       Not Applicable
Firepower /ssa* # scope slot 1
Firepower /ssa/slot # delete app-instance ftd
Firepower /ssa/slot* # exit
Firepower /ssa* # scope slot 2
Firepower /ssa/slot # delete app-instance ftd
Firepower /ssa/slot* # exit
Firepower /ssa* # scope slot 3
```

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

ASA のトランスペアレント ファイアウォール モードへの変更

Firepower 4100/9300 シャーシのルーテッド ファイアウォール モード ASA のみを導入できます。ASA をトランスペアレント ファイアウォール モードに変更するには、初期導入を完了し、ASA CLI 内でファイアウォール モードを変更します。スタンドアロン ASA の場合、ファイアウォール モードを変更すると設定が消去されるため、Firepower 4100/9300 シャーシから設定を再導入して、ブートストラップ設定を回復する必要があります。ASA はトランスペアレント モードのままで、ブートストラップ設定が機能した状態になっています。クラスタ化 ASA の場合、設定は消去されないため、FXOS からブートストラップ設定を再導入する必要はありません。

手順

ステップ 1 アプリケーションのコンソールへの接続 （59 ページ）に従って、ASA コンソールに接続します。クラスタの場合、プライマリ ユニットに接続します。フェールオーバー ペアの場合、アクティブ ユニットに接続します。

ステップ 2 コンフィギュレーション モードに入ります。

enable

configure terminal

デフォルトでは、イネーブル パスワードは空白です。

ステップ 3 ファイアウォール モードをトランスペアレントに設定します。

firewall transparent

ステップ 4 設定を保存します。

write memory

クラスタまたはフェールオーバー ペアの場合、この設定はセカンダリ ユニットに複製されます。

```
asa(config)# firewall transparent
asa(config)# write memory
Building configuration...
Cryptochecksum: 9f831dfb 60dffa8c 1d939884 74735b69

3791 bytes copied in 0.160 secs
[OK]
asa(config)#
Beginning configuration replication to Slave unit-1-2
 End Configuration Replication to slave.

asa(config)#
```

ステップ 5 Firepower Chassis Manager の [Logical Devices] ページで、[Edit] アイコンをクリックして ASA を編集します。

[Provisioning] ページが表示されます。

ステップ 6 デバイスのアイコンをクリックして、ブートストラップ設定を編集します。設定の値を変更し、[OK] をクリックします。

少なくとも 1 つのフィールド（[Password] フィールドなど）の値を変更する必要があります。

ブートストラップ設定の変更に関する警告が表示されます。[Yes] をクリックします。

ステップ 7 ASA に設定を再展開するには、[Restart Now] をクリックします。シャーシ間クラスタまたはフェールオーバーペアの場合、各シャーシでステップ 5 ～ 7 を繰り返してブートストラップ設定を再導入します。

シャーシ/セキュリティ モジュールがリロードし、ASA が再度稼働するまで数分待ちます。ASA は、これでブートストラップ設定が機能するようになりますが、トランスペアレントモードのままです。

Firepower Threat Defense 論理デバイスのインターフェイスの変更

Firepower Threat Defense 論理デバイスでは、インターフェイスの割り当てや割り当て解除、を行うことができます。その後、Firepower Management Center でインターフェイス設定を同期できます。

始める前に

- 物理インターフェイスの設定およびEtherChannel（ポート チャネル）の追加に従って、インターフェイスを設定し、EtherChannel を追加します。
- 論理デバイスに影響を与えず、かつ Firepower Management Center での同期を必要とせずに、割り当てられた EtherChannel のメンバーシップを編集できます。
- すでに割り当てられているインターフェイスを EtherChannel に追加するには（たとえば、デフォルトではすべてのインターフェイスがクラスタに割り当てられます）、まず論理デバイスからインターフェイスの割り当てを解除し、次に EtherChannel にインターフェイスを追加する必要があります。新しい EtherChannel の場合、デバイスに EtherChannel を割り当てることができます。
- クラスタリングや高可用性のため、Firepower Management Center で設定を同期する前に、すべてのユニットでインターフェイスを追加または削除していることを確認してください。最初にスレーブ / スタンバイ ユニットでインターフェイスを変更してから、マスター / アクティブ ユニットで変更することをお勧めします。新しいインターフェイスは管理上ダウンした状態で追加されるため、インターフェイス モニタリングに影響を及ぼさないことに注意してください。

手順

ステップ 1 セキュリティ サービス モードを開始します。

Firepower# **scope ssa**

ステップ 2 論理デバイスを編集します。

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

ステップ 3 論理デバイスからインターフェイスの割り当てを解除します。

Firepower /ssa/logical-device # **delete external-port-link** *name*

show external-port-link コマンドを入力して、インターフェイス名を表示します。

ステップ 4 論理デバイスに新しいインターフェイスを割り当てます。

Firepower /ssa/logical-device* # **create external-port-link** *name interface_id* **ftd**

ステップ 5 設定をコミットします。

commit-buffer

トランザクションをシステムの設定にコミットします。

ステップ 6 Firepower Management Center にログインします。

ステップ 7 **[Devices]** > **[Device Management]** の順に選択し、FTD デバイスの編集アイコン（  ）をクリックします。[Interfaces] タブがデフォルトで選択されています。

ステップ 8 [Interfaces] タブの左上にある [Sync Interfaces from device] ボタンをクリックします。

ステップ 9 [Save] をクリックします。

これで、[Deploy] をクリックして割り当てられているデバイスにポリシーを展開できます。変更を展開するまで、変更は有効ではありません。

ASA 論理デバイスのインターフェイスの変更

ASA 論理デバイスでは、管理インターフェイスの割り当て、割り当て解除、または置き換えを行うことができます。ASDM は、新しいインターフェイスを自動的に検出します。

始める前に

- 物理インターフェイスの設定およびEtherChannel（ポート チャネル）の追加に従って、インターフェイスを設定し、EtherChannel を追加します。
- 論理デバイスに影響を与えずに、割り当てられた EtherChannel のメンバーシップを編集できます。

- すでに割り当てられているインターフェイスを EtherChannel に追加するには（たとえば、デフォルトではすべてのインターフェイスがクラスタに割り当てられます）、まず論理デバイスからインターフェイスの割り当てを解除し、次に EtherChannel にインターフェイスを追加する必要があります。新しい EtherChannel の場合、デバイスに EtherChannel を割り当てることができます。
- FXOS で割り当てられたインターフェイスを削除すると（たとえば、ネットワークモジュールの削除、EtherChannel の削除、または割り当てられたインターフェイスの EtherChannel への再割り当てなど）、必要な調整を行うことができるように、ASA 設定では元のコマンドが保持されます。設定からインターフェイスを削除すると、幅広い影響が出る可能性があります。ASA OS の古いインターフェイス設定は手動で削除できます。
- クラスタ リングまたはフェールオーバーを追加するか、すべてのユニット上のインターフェイスの削除を確認します。最初にスレーブ/スタンバイ ユニットでインターフェイスを変更してから、マスター/アクティブ ユニットで変更することをお勧めします。新しいインターフェイスは管理上ダウンした状態で追加されるため、インターフェイスモニタリングに影響を及ぼしません。

手順

ステップ 1 セキュリティ サービス モードを開始します。

Firepower# **scope ssa**

ステップ 2 論理デバイスを編集します。

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

ステップ 3 論理デバイスからインターフェイスの割り当てを解除します。

Firepower /ssa/logical-device # **delete external-port-link** *name*

show external-port-link コマンドを入力して、インターフェイス名を表示します。

管理インターフェイスの場合、新しい管理インターフェイスを追加する前に、現在のインターフェイスを削除し、**commit-buffer** コマンドを使用して変更をコミットします。

ステップ 4 論理デバイスに新しいインターフェイスを割り当てます。

Firepower /ssa/logical-device* # **create external-port-link** *name interface_id* **asa**

ステップ 5 設定をコミットします。

commit-buffer

トランザクションをシステムの設定にコミットします。

論理デバイスのモニタリング

- **show app**

  使用可能なイメージを表示します。

```
Firepower# scope ssa
Firepower /ssa # show app
    Name       Version         Author     Supported Deploy Types CSP Type    Is
Default App
    ---------- --------------- ---------- ---------------------- -----------
--------------
    asa        9.10.1          cisco      Native                 Application Yes
    ftd        6.2.3           cisco      Native                 Application Yes
    vdp        8.13.01.09-2    radware    Vm                     Application Yes
```

- **show app-instance**

  アプリケーション インスタンス ステータスを表示します。

```
Firepower# scope ssa
Firepower /ssa # show app-instance
App Name   Slot ID    Admin State Oper State       Running Version Startup Version
Cluster State   Cluster Role
---------- ---------- ----------- ---------------- --------------- ---------------
--------------- ------------
ftd        1          Enabled     Online           6.2.1.62        6.2.1.62
Not Applicable  None
vdp        1          Disabled    Installing                       8.10.01.16-5
Not Applicable  None
```

- **show logical-device**

  論理デバイスの詳細を表示します。

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

Logical Device:
    Name       Description Slot ID    Mode       Oper State               Template
Name
    ---------- ----------- ---------- ---------- ----------------------- -------------

    asa1                   1          Standalone Ok                      asa
```

- **show app-resource-profile**

  vDP のリソース プロファイルを表示します。

```
Firepower# scope ssa
Firepower /ssa # scope app vdp 8.13.01.09-2
Firepower /ssa/app # show app-resource-profile
Profile Name              Security Model  CPU Logical Core Count 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
                                                                10           40960 No
VDP-2-CORES               all                                    2            8192 No
VDP-4-CORES               all                                    4           16384 No
VDP-8-CORES               FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36, FPR9K-SM-24,
FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24
                                                                 8           32768 No
```

サイト間クラスタリングの例

次の例ではサポートされるクラスタの導入を示します。

スパンド EtherChannel トランスペアレント モード ノースサウス サイト間の例

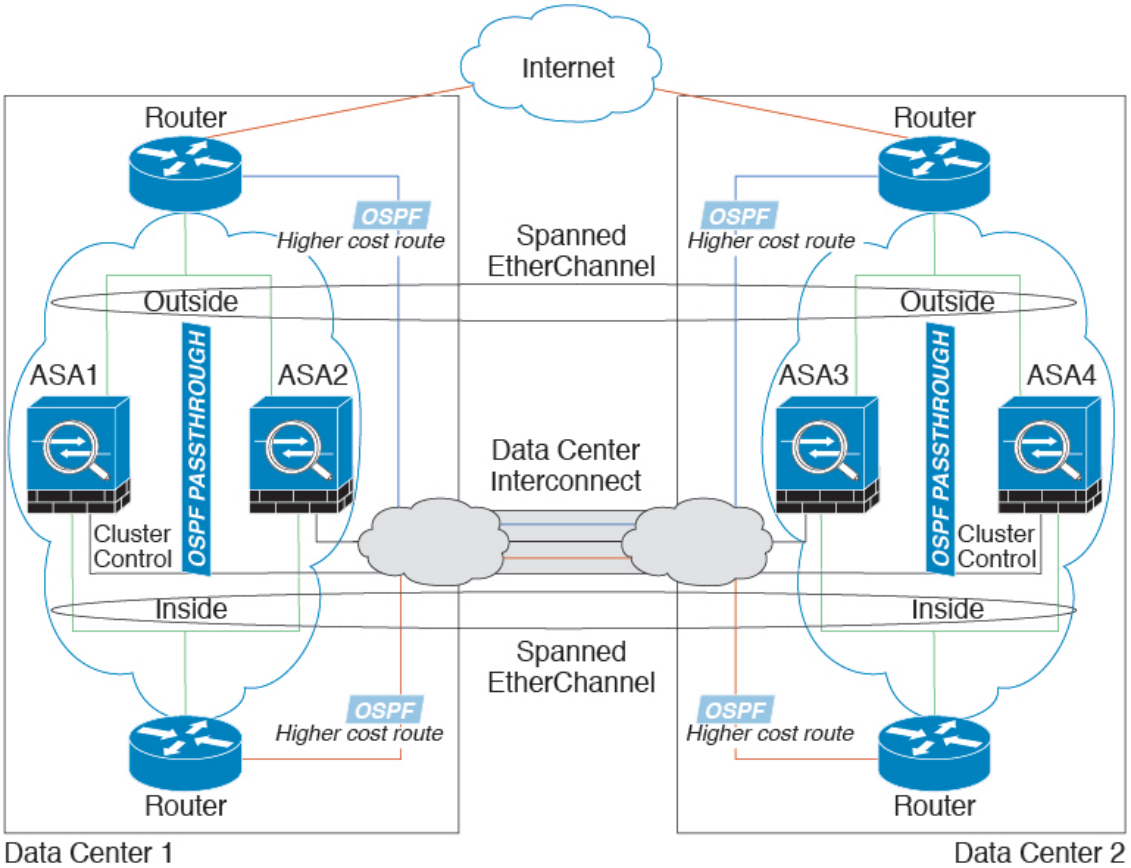
次の例では、内部ルータと外部ルータの間に配置された（ノースサウス挿入）2 つのデータセンターのそれぞれに 2 つのクラスタ メンバがある場合を示します。クラスタ メンバは、DCI 経由のクラスタ制御リンクによって接続されています。各サイトのクラスタ メンバは、内部および外部のスパンド EtherChannels を使用してローカル スイッチに接続します。各 EtherChannel は、クラスタ内のすべてのシャーシにスパンされます。

各データセンターの内部ルータと外部ルータは OSPF を使用し、トランスペアレント ASA を通過します。MAC とは異なり、ルータの IP はすべてのルータで一意です。DCI に高コストルートを割り当てることにより、特定のサイトですべてのクラスタ メンバがダウンしない限り、トラフィックは各データセンター内に維持されます。クラスタが非対称型の接続を維持するため、ASA を通過する低コストのルートは、各サイトで同じブリッジ グループを横断する必要があります。1 つのサイトのすべてのクラスタ メンバに障害が発生した場合、トラフィックは各ルータから DCI 経由で他のサイトのクラスタ メンバに送られます。

各サイトのスイッチの実装には、次のものを含めることができます。

- サイト間 VSS/vPC：このシナリオでは、データセンター 1 に 1 台のスイッチをインストールし、データセンター 2 に別のスイッチをインストールします。1 つのオプションとして、各データセンターのクラスタ ユニットはローカル スイッチだけに接続し、VSS/vPC トラフィックは DCI を経由します。この場合、接続のほとんどの部分は各データセンターに対してローカルに維持されます。オプションとして、DCI が余分なトラフィック量を処理できる場合、各ユニットを DCI 経由で両方のスイッチに接続できます。この場合、トラフィックは複数のデータセンターに分散されるため、DCI を非常に堅牢にするためには不可欠です。

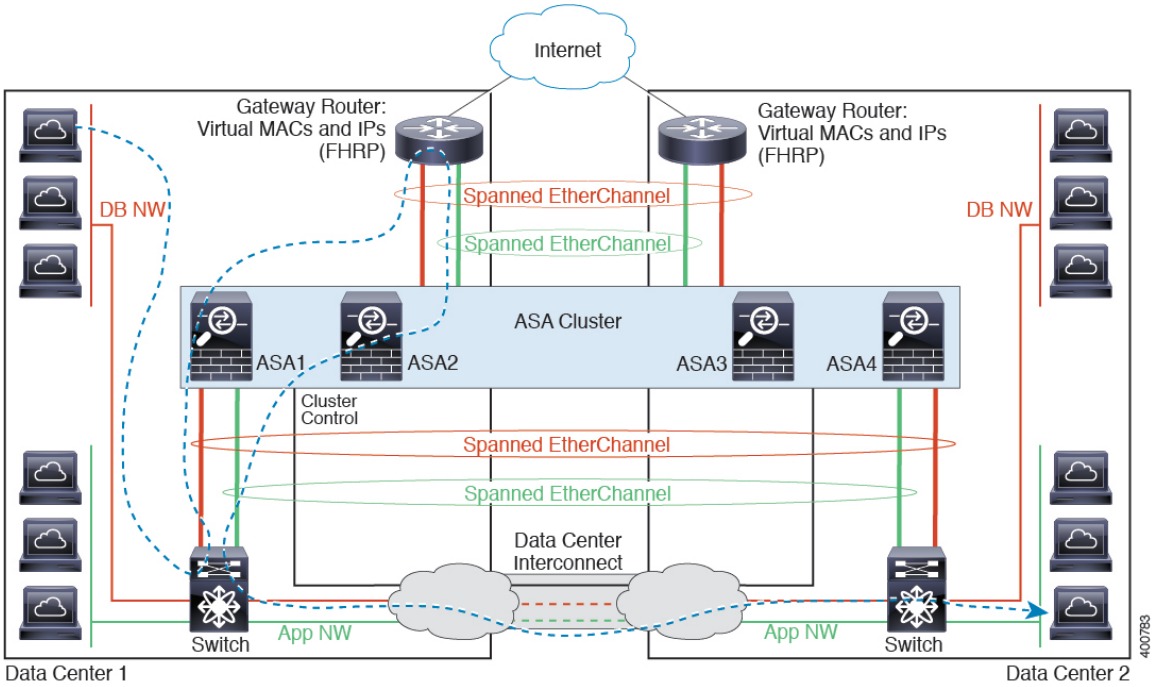
- 各サイトのローカル VSS/vPC：スイッチの冗長性を高めるには、各サイトに 2 つの異なる VSS/vPC ペアをインストールできます。この場合、クラスタ ユニットは、両方のローカル スイッチだけに接続されたデータセンター 1 のシャーシおよびこれらのローカル スイッチに接続されたデータセンター 2 のシャーシとはスパンド EtherChannel を使用しますが、スパンド EtherChannel は基本的に「分離」しています。各ローカル VSS/vPC は、スパンド EtherChannel をサイトローカルの EtherChannel として認識します。



スパンド EtherChannel トランスペアレント モード イーストウェスト サイト間の例

次の例では、各サイトのゲートウェイ ルータと 2 つの内部ネットワーク（アプリケーション ネットワークと DB ネットワーク）間に配置された（イーストウェスト挿入）2 つのデータセンターのそれぞれに 2 つのクラスタ メンバがある場合を示します。クラスタ メンバは、DCI 経由のクラスタ制御リンクによって接続されています。各サイトのクラスタ メンバは、内部および外部のアプリケーション ネットワークと DB ネットワークの両方にスパンド EtherChannels を使用してローカル スイッチに接続します。各 EtherChannel は、クラスタ内のすべてのシャーシにスパンされます。

各サイトのゲートウェイ ルータは、HSRP などの FHRP を使用して、各サイトで同じ宛先の仮想 MAC アドレス と IP アドレスを提供します。予期せぬ MAC アドレスのフラッピングを避けるために推奨されている方法は **mac-address-table static** *outside_interface mac_address* コマンドを使用して、ゲートウェイ ルータの実際の MAC アドレスを ASA MAC アドレス テーブルに静的に追加することです。これらのエントリがないと、サイト 1 のゲートウェイがサイト 2 のゲートウェイと通信する場合に、そのトラフィックが ASA を通過して、内部インターフェイスからサイト 2 に到達しようとして、問題が発生する可能性があります。データ VLAN は、オーバーレイ トランスポート仮想化（OTV）（または同様のもの）を使用してサイト間に拡張されます。トラフィックがゲートウェイ ルータ宛てである場合にトラフィックが DCI を通過して他のサイトに送信されないようにするには、フィルタを追加する必要があります。1 つのサイトのゲートウェイ ルータが到達不能になった場合、トラフィックが他のサイトのゲートウェイに送信されるようにフィルタを削除する必要があります。



vPC/VSS オプションについては、スパンド EtherChannel トランスペアレント モード ノースサウス サイト間の例 （68 ページ）を参照してください。

論理デバイスの履歴

機能名	プラットフォーム リリース	機能情報
Firepower 4100/9300 シャーシ 上の ASA のサイト間クラスタリングの改善	2.1(1)	ASA クラスタを展開すると、それぞれの Firepower 4100/9300 シャーシのサイト ID を設定できます。以前は、ASA アプリケーション内でサイト ID を設定する必要がありました。この新機能により初期展開が簡単になります。ASA 構成内でサイト ID を設定することはできないことに注意してください。また、サイト間クラスタリングとの互換性を高めるために、安定性とパフォーマンスに関する複数の改善が含まれる ASA 9.7(1) および FXOS 2.1.1 にアップグレードすることを推奨します。 **set site-id** コマンドが変更されました
6 つの FTD モジュールのシャーシ間クラスタリング	2.1(1)	FTD のシャーシ間クラスタリングを有効化できます。最大 6 つのシャーシに最大 6 つのモジュールを含めることができます。
Firepower 9300 の FTD でのシャーシ内クラスタリング サポート	1.1.4	Firepower 9300 が FTD アプリケーションでシャーシ内クラスタリングをサポートするようになりました。 次のコマンドが導入されました。**enter mgmt-bootstrap ftd**、**enter bootstrap-key FIREPOWER_MANAGER_IP**、**enter bootstrap-key FIREWALL_MODE**、**enter bootstrap-key-secret REGISTRATION_KEY**、**enter bootstrap-key-secret PASSWORD**、**enter bootstrap-key FQDN**、**enter bootstrap-key DNS_SERVERS**、**enter bootstrap-key SEARCH_DOMAINS**、**enter ipv4 firepower**、**enter ipv6 firepower**、**set value**、**set gateway**、**set ip**、**accept-license-agreement**

機能名	プラットフォーム リリース	機能情報
6つのASAモジュールのシャーシ間クラスタリング	1.1.3	ASAのシャーシ間クラスタリングが実現されました。最大6つのシャーシに最大6つのモジュールを含めることができます。
Cisco ASA のシャーシ内クラスタリング	1.1.1	Firepower 9300 シャーシ内のすべてのASA セキュリティ モジュールをクラスタ化できるようになりました。 **enter cluster-bootstrap**、**enter logical-device clustered**、**set chassis-id**、**set ipv4 gateway**、**set ipv4 pool**、**set ipv6 gateway**、**set ipv6 pool**、**set key**、**set mode spanned-etherchannel**、**set port-type cluster**、**set service-type**、**set virtual ipv4**、**set virtual ipv6** コマンドを導入しました