従来型デバイスの管理の基本

次のトピックでは、Firepower システムで従来型デバイス（7000 および 8000 シリーズ デバイス、ASA with FirePOWER サービス、NGIPSv）を管理する方法について説明します。

リモート管理の設定

Firepower System デバイスを管理できるようにするには、デバイスと Firepower Management Center との間に双方向の SSL 暗号化通信チャネルをセットアップする必要があります。このチャネルを使用して、両方のアプライアンスが設定とイベント情報を共有します。ハイ アベイラビリティ ピアも、このチャネルを使用します。このチャネルは、デフォルトではポート 8305/tcp に位置します。

（注） この章では、FMC にデバイスを登録する前にローカル Web インターフェイスを使用して、7000 または 8000 シリーズ デバイスのリモート管理の設定方法について説明します。他のモデルのリモート管理の設定の詳細については、適切なクイックスタートガイドを参照してください。

2 つのアプライアンス間の通信を可能にするためには、アプライアンスが互いを認識する手段を提供しなければなりません。Firepower System では 3 つの基準を使用して、通信を許可します。

- 通信を確立する対象のアプライアンスのホスト名または IP アドレス。

  NAT 環境では、ルーティング可能なアドレスがもう一方のアプライアンスにないとしても、リモート管理を設定する際、または管理対象アプライアンスを追加する際には、ホスト名または IP アドレスのいずれかを指定する必要があります。

- 接続を識別するために自己生成される、最大 37 文字の英数字による登録キー。

- Firepower System が NAT 環境で通信を確立するために利用できるオプションの一意の英数字による NAT ID。

NAT ID は、管理対象アプライアンスを登録するために使用されているすべての NAT ID の間で**一意でなければなりません**。

管理対象デバイス上のリモート管理の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	7000 & 8000 シリーズ	該当なし	Admin/Network Admin

手順

ステップ 1 管理するデバイスの Web インターフェイスで、**[設定（Configuration）] > [ASA FirePOWER の設定（ASA FirePOWER Configuration）] > [統合（Integration）] > [リモート管理（Remote Management）]** を選択します。

ステップ 2 [リモート管理（Remote Management）] タブが表示されていない場合は、クリックします。

ステップ 3 [マネージャの追加（Add Manager）] をクリックします。

ステップ 4 [管理ホスト（Management Host）] フィールドに、このアプライアンスを管理するために使用する Firepower Management Center について、次のいずれかを入力します。

- IP アドレス
- 完全修飾ドメイン名またはローカル DNS で有効な IP アドレスに解決される名前（つまり、ホスト名）

注意 ネットワークで IP アドレスの割り当てに DHCP を使用している場合は、IP アドレスではなく、ホスト名を使用します。

NAT 環境では、管理対象アプライアンスを追加する際に IP アドレスまたはホスト名を指定する予定の場合、ここで IP アドレスまたはホスト名を指定する必要はありません。その場合、Firepower システムは後で指定される NAT ID を使用して、管理対象アプライアンスの Web インターフェイス上のリモート マネージャを識別します。

ステップ 5 [登録キー（Registration Key）] フィールドに、アプライアンス間の通信をセットアップするために使用する登録キーを入力します。

ステップ 6 NAT 環境の場合は、[固有 NAT ID（Unique NAT ID）] フィールドに、アプライアンス間の通信をセットアップするために使用する、英数字による一意の NAT ID を入力します。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

- アプライアンスが相互に通信できることを確認し、ステータスとして [登録保留（Pending Registration）] が表示されるまで待ちます。

- このデバイスを Firepower Management Center に追加します。Firepower Management Center へのデバイスの追加を参照してください。

管理対象デバイスでのリモート管理の編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	7000 & 8000 シリーズ	該当なし	Admin/Network Admin

リモート マネージャを編集するには、次の点に注意してください。

- [ホスト（Host）] フィールドでは、完全修飾ドメイン名またはローカル DNS で有効な IP アドレスに解決される名前（つまり、ホスト名）を指定します。
- [名前（Name）] フィールドには、Firepower システムのコンテキストでのみ使用される、管理アプライアンスの表示名を指定します。別の表示名を入力しても、管理デバイスのホスト名は変更されません。

手順

ステップ 1 デバイスの Web インターフェイスで、**[システム（System）] > [統合（Integration）]** を選択します。

ステップ 2 まだ表示されていない場合は、[リモート管理（Remote Management）] タブをクリックします。

ステップ 3 次の操作を実行できます。

- リモート管理の無効化：マネージャの横にあるスライダをクリックして、これを有効または無効にします。管理を無効化すると、Firepower Management Center とデバイス間の接続がブロックされますが、Firepower Management Center からデバイスは削除**されません**。デバイスを管理する必要がなくなった場合は、Firepower Management Center からのデバイスの削除を参照してください。
- マネージャ情報の編集：変更するマネージャの横にある編集アイコン（）をクリックして、[名前（Name）] および [ホスト（Host）] フィールドをクリックし、[保存（Save）] をクリックします。

管理ポートの変更

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	7000 & 8000 シリーズ Management Center	グローバルだけ	Admin/Network Admin

アプライアンスは、双方向の SSL 暗号化通信チャネルを使用して通信します。このチャネルは、デフォルトではポート 8305 に位置します。

設定をデフォルトのままにすることを**強く**奨励します。管理ポートがネットワークでの他の通信と競合する場合には、他のポートを選択できます。通常、管理ポートの変更は、Firepower System のインストール時に行います。

⚠

注意 管理ポートを変更する場合は、導入内の相互に通信する必要があるすべてのアプライアンスの管理ポートを変更する必要があります。

手順

ステップ 1 **[システム（System）] > [設定（Configuration）]**を選択します。

ステップ 2 [管理インターフェイス（Management Interfaces）] をクリックします。

ステップ 3 [共有設定（Shared Settings）] セクションで、[リモート管理ポート（Remote Management Port）] フィールドに使用するポート番号を入力します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

- このアプライアンスと通信する必要がある、展開環境内のすべてのアプライアンスについて、この手順を繰り返します。

インターフェイス構成時の設定

アプライアンス エディタの [インターフェイス（Interfaces）] ページには、詳細なインターフェイス設定情報が表示されます。このページは、物理ハードウェア ビューとインターフェイス テーブル ビューで構成されており、構成の詳細情報にドリルダウンできます。このページからインターフェイスを追加したり編集したりできます。

物理的なハードウェア ビュー

[インターフェイス（Interfaces）] ページの一番上には、7000 または 8000 シリーズ デバイスの物理的なハードウェア ビューがグラフィカル表示されます。

物理的なハードウェア ビューは、次の目的で使用します。

- ネットワーク モジュールのタイプ、部品番号、およびシリアル番号を確認する
- インターフェイス テーブル ビューでインターフェイスを選択する
- インターフェイス エディタを開く
- インターフェイスの名前、タイプ、リンクの有無、速度設定、およびインターフェイスがバイパス モードになっているかを確認する
- エラーまたは警告の詳細を参照する

インターフェイス アイコン

表 *1*: インターフェイス アイコンのタイプと説明

アイコン	インターフェイス タイプ	詳細
	物理的：未設定の物理インターフェイス。	物理スイッチド インターフェイスの設定 または 物理ルーテッド インターフェイスの設定
	パッシブ：パッシブ展開でトラフィックを分析するように設定されているセンシング インターフェイス。	パッシブ インターフェイスの設定
	インライン：インライン展開でトラフィックを処理するように設定されているセンシング インターフェイス。	インライン インターフェイスの設定
	スイッチド：レイヤ 2 展開でトラフィックを切り替えるように設定されているインターフェイス。	スイッチド インターフェイスの設定
	ルーテッド：レイヤ 3 展開でトラフィックをルーティングするように設定されているインターフェイス。	ルーテッド インターフェイス

アイコン	インターフェイス タイプ	詳細
	集約：1つの論理リンクとして設定されている複数の物理インターフェイス。	集約インターフェイスについて
	集約スイッチド：レイヤ 2 展開で 1 つの論理リンクとして設定されている複数の物理インターフェイス。	集約スイッチド インターフェイスの追加
	集約ルーテッド：レイヤ 3 展開で 1 つの論理リンクとして設定されている複数の物理インターフェイス。	集約ルーテッド インターフェイスの追加
	ハイブリッド：仮想ルータと仮想スイッチ間でトラフィックをブリッジするように設定されている論理インターフェイス。	論理ハイブリッド インターフェイス
	ASA FirePOWER：ASA FirePOWER モジュールがインストールされた ASA デバイスに設定されているインターフェイス。	Cisco ASA FirePOWER インターフェイスの管理 （11 ページ）

物理ハードウェア ビューの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	7000 & 8000 シリーズ	任意（Any）	Admin/Network Admin

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]**を選択します。

ステップ 2 管理するデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 グラフィカル インターフェイスを使用して、以下を実行できます。

- 選択：インターフェイスを選択する場合、インターフェイスアイコンをクリックします。システムは、インターフェイス テーブルの関連項目を強調表示します。
- 編集：インターフェイスエディタを開く場合、インターフェイスアイコンをダブルクリックします。
- エラーまたは警告情報の表示：エラーまたは警告に関する詳細を表示するには、ネットワーク モジュール上の影響を受けるポートの上にカーソルを置きます。
- インターフェイス情報の表示：インターフェイスの名前、インターフェイスのタイプ、インターフェイスにリンク画が存在するかどうか、インターフェイスの速度設定、インターフェイスが現在バイパスモードであるかどうかについて表示するには、インターフェイス上にカーソルを置きます。
- ネットワーク モジュール情報の表示：ネットワーク モジュールのタイプ、製品番号、シリアル番号を表示するには、ネットワークモジュールの左下隅にある黒い円の上にカーソルを置きます。

センシング インターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	従来型（Classic）	リーフのみ	Admin/Network Admin

アプライアンス エディタの [インターフェイス（Interfaces）] ページで、Firepower システムの展開に応じて、管理対象デバイスのセンシングインターフェイスを設定できます。管理対象デバイスには、合計 1024 個のインターフェイスを設定できることに注意してください。

（注） Firepower Management Center では、ASA FirePOWER が SPAN ポート モードで展開されている場合、ASA インターフェイスを表示しません。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]**を選択します。

ステップ 2 インターフェイスを設定するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 設定するインターフェイスの横にある編集アイコン（）をクリックします。

ステップ 4 インターフェイス エディタを使用して、センシング インターフェイスを設定します。

- [HA リンク（HA Link）]：デバイスのハイアベイラビリティペアの各メンバーに設定されたインターフェイスを、（ハイアベイラビリティリンクインターフェイスとも呼ばれる）デバイス間の冗長通信チャネルとして機能させるには、[HA リンク（HA Link）]をクリックし、HA リンク インターフェイスの設定 （8 ページ）の説明に従って続行します。
- [インライン（Inline）]：設定されたインターフェイスでインライン展開のトラフィックを処理するように設定するには、[インライン（Inline）]をクリックし、インラインインターフェイスの設定の説明に従って続行します。
- [パッシブ（Passive）]：設定されたインターフェイスでパッシブ展開のトラフィックを分析するように設定するには、[パッシブ（Passive）]をクリックし、パッシブインターフェイスの設定の説明に従って続行します。
- [ルーテッド（Routed）]：設定されたインターフェイスでレイヤ 3 展開のトラフィックをルーティングするように設定するには、[ルーテッド（Routed）] をクリックし、ルーテッドインターフェイスの説明に従って続行します。
- [スイッチド（Switched）]：設定されたインターフェイスでレイヤ 2 展開のトラフィックをスイッチングするように設定するには、[スイッチド（Switched）]をクリックし、スイッチドインターフェイスの設定の説明に従って続行します。

ステップ 5 [保存（Save）] をクリックして構成を完了します。

次のタスク

- 設定変更を展開します。設定変更の導入を参照してください。

HA リンク インターフェイスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
該当なし	任意（Any）	7000 & 8000 シリーズ	リーフのみ	Admin/Network Admin

7000 または 8000 シリーズ デバイスの高可用性ペアを確立した後、物理インターフェイスをハイアベイラビリティ（HA）リンク インターフェイスとして設定する必要があります。このリンクは、ペアリングされたデバイス間でヘルス情報を共有するために使用する、冗長通信チャネルとして機能します。1 つのデバイスに HA リンク インターフェイスを設定すると、自動的に 2 番目のデバイスにインターフェイスが設定されます。同じブロードキャスト ドメインに、両方の HA リンクを設定する必要があります。

ダイナミック NAT は、他の IP アドレスとポートにマップする IP アドレスとポートの動的割り当てに依存します。HA リンクがなければ、これらのマッピングはフェールオーバーで失われます。その場合、変換されたすべての接続は高可用性ペアで新しくアクティブになったデバイスを介してルーティングされることになるため、それらの接続は失敗します。

同様に、高可用性状態共有、ダイナミック NAT、または VPN が設定された 7000 または 8000 シリーズ デバイスには、HA リンク インターフェイスが必要です。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]**を選択します。

ステップ 2 HA リンク インターフェイスを設定するピアの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 HA リンク インターフェイスとして設定するインターフェイスの横にある編集アイコン（  ）をクリックします。

ステップ 4 [HA リンク（HA Link）] をクリックします。

ステップ 5 [有効（Enabled）] チェックボックスをオンにします。

（注） チェックボックスをオフにした場合、システムはインターフェイスを管理上停止し、無効にします。

ステップ 6 [モード（Mode）] ドロップダウン リストからリンク モードを指定するオプションを選択するか、[自動ネゴシエーション（Autonegotiation）] を選択して、速度とデュプレックスの設定を自動ネゴシエートするようにインターフェイスを設定します。

ステップ 7 [MDI/MDIX] ドロップダウン リストから、インターフェイスの設定対象として MDI（メディア依存型インターフェイス）、MDIX（メディア依存型インターフェイス クロスオーバー）、または自動 MDIX のいずれかを指定するオプションを選択します。

（注） 通常、[MDI/MDIX] は [自動 MDIX（Auto-MDIX）] に設定します。これにより、MDI と MDIX の間の切り替えが自動的に処理され、リンクが確立されます。

ステップ 8 [MTU] フィールドに最大伝送ユニット（MTU）を入力します。

MTU 値の範囲は管理対象デバイスのモデルとインターフェイス タイプによって異なる場合があります。詳細については、7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲（12 ページ）を参照してください。

注意 デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作を参照してください。

ステップ 9 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の導入を参照してください。

関連トピック

Snort® の再起動シナリオ
7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲 （12 ページ）

インターフェイスの無効化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	7000 & 8000 シリーズ NGIPSv	リーフのみ	Admin/Network Admin

インターフェイス タイプを [なし（None）] に設定することで、インターフェイスを無効にすることができます。無効にされたインターフェイスは、インターフェイスリストでグレー表示されます。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]**を選択します。

ステップ 2 インターフェイスを無効にするデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 無効にするインターフェイスの横にある編集アイコン（  ）をクリックします。

ステップ 4 [なし（None）] をクリックします。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の導入を参照してください。

Cisco ASA FirePOWER インターフェイスの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
脅威（Threat）	Protection	ASA FirePOWER	リーフのみ	Admin/Network Admin

ASA FirePOWER インターフェイスを編集する際に、Firepower Management Center から設定できるのは、インターフェイスのセキュリティ ゾーンのみです。

ASA FirePOWER インターフェイスを完全に設定するには、ASA 専用ソフトウェアおよび CLI を使用します。ASA FirePOWER およびスイッチを編集して、マルチ コンテキスト モードからシングル コンテキスト モード（またはその逆）に切り替えると、ASA FirePOWER はそのインターフェイスの名前をすべて変更します。ASA FirePOWER の更新されたインターフェイス名を使用するように、すべての Firepower System セキュリティ ゾーン、相関ルール、関連する設定を再設定する必要があります。ASA FirePOWERインターフェイスの設定の詳細については、ASA のマニュアルを参照してください。

（注） ASA FirePOWER インターフェイスのタイプは変更できません。また、Firepower Management Center からインターフェイスを無効にすることもできません。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]**を選択します。

ステップ 2 インターフェイスを編集するデバイスの横にある編集アイコン（）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 [インターフェイス（Interfaces）] タブが表示されていない場合は、そのタブをクリックします。

ステップ 4 編集するインターフェイスの横にある編集アイコン（）をクリックします。

ステップ 5 [セキュリティ ゾーン（Security Zone）] ドロップダウンリストから既存のセキュリティ ゾーンを選択するか、[新規（New）] を選択して新しいセキュリティ ゾーンを追加します。

ステップ 6 [保存（Save）] をクリックして、セキュリティ ゾーンを設定します。

次のタスク

- 設定変更を展開します。設定変更の導入を参照してください。

7000 および 8000 シリーズ デバイスおよび NGIPSv の MTU 範囲

デバイス上のすべての非管理インターフェイスの中で最大 MTU 値を変更し、設定変更を展開すると、Snort プロセスが再起動され、トラフィック インスペクションが一時的に中断されます。インスペクションは、変更したインターフェイスだけでなく、すべての非管理インターフェイスで中断されます。この中断によってトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作を参照してください。

（注） システムは、設定された MTU 値から 18 バイトを切り捨てます。594 より小さい IPv4 MTU または 1298 より小さい IPv6 MTU を設定しないでください。

従来のデバイス モデル	MTU 範囲
7000 & 8000 シリーズ	576 ～ 9234（管理インターフェイス） 576 ～ 10172（インライン セット、パッシブ インターフェイス） 576 ～ 9922（その他）
NGIPSv	576 ～ 9018（すべてのインターフェイス、インライン セット）

関連トピック

MTU について

セキュリティ ゾーン オブジェクトのリビジョンの同期

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	7000 & 8000 シリーズ NGIPSv	リーフのみ	Admin/Network Admin

セキュリティ ゾーン オブジェクトを更新すると、システムはそのオブジェクトの新しいリビジョンを保存します。その結果、同じセキュリティ ゾーン内の管理対象デバイスに、インターフェイスで設定されたセキュリティ オブジェクトの異なるリビジョンがある場合、接続が重複しているようなログが記録される可能性があります。

接続の重複が報告されていることに気づいた場合、同じリビジョンのオブジェクトを使用するよう、すべての管理対象デバイスを更新できます。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]**を選択します。

ステップ 2 セキュリティ ゾーンの選択を更新するデバイスの横にある編集アイコン（  ）をクリックします。

マルチドメイン展開では、リーフ ドメインにいない場合、システムによって切り替えるように求められます。

ステップ 3 重複する接続のイベントを記録しているインターフェイスのそれぞれについて、[セキュリティ ゾーン（Security Zone）] を別のゾーンに変更して [保存（Save）] をクリックした後、目的のゾーンに再び設定し、もう一度 [保存（Save）] をクリックします。

ステップ 4 重複イベントを記録しているデバイスごとに、ステップ 2 から 3 を繰り返します。続行する前に、すべてのデバイスを編集する必要があります。

次のタスク

- 設定変更を展開します。設定変更の導入を参照してください。

⚠

注意 同期させるすべてのデバイスでインターフェイスのゾーン設定を編集するまでは、デバイスに設定変更を展開しないでください。すべての管理対象デバイスに同時に展開する必要があります。