Firepower 7000 シリーズ管理対象デバイスのインストール

Firepower システムアプライアンスは、大規模な Firepower システム展開の一部としてネットワーク上に容易に設置できます。デバイスはネットワーク セグメントに設置され、それに適用された侵入ポリシーに基づいてトラフィックを検査し、侵入イベントを生成します。このデータは Firepower Management Center に送信されます。そこでは、データを展開全体で相互に関連付け、セキュリティに対する脅威を調整または処理するように 1 つ以上のデバイスが管理されます。

ヒント　複数の管理インターフェイスを使用することで、パフォーマンスを向上させたり、2 つの異なるネットワークのトラフィックを分離して管理することができます。初期設置中に、デフォルト管理インターフェイス（eth0）を設定します。設置した後、ユーザ インタフェースを介して追加の管理インターフェイスを設定できます。詳細については、*Firepower Management Center Configuration Guide* を参照してください。

複数のアプライアンスを別々の展開場所で使用するように 1 か所で事前設定できます。事前設定に関するガイダンスについては、『*FirePower 7000 シリーズ スタートアップ ガイド*』を参照してください。

アプライアンスの開梱と点検

ヒント　サーバの輸送が必要となる場合に備えて、輸送用の箱は保管しておいてください。

コメント　シャーシは厳密に検査したうえで出荷されています。輸送中の破損や内容品の不足がある場合には、ただちにカスタマー サービス担当者に連絡してください。

梱包内容を確認する手順は、次のとおりです。

ステップ 1　段ボール箱からシャーシを取り出します。梱包材はすべて保管しておいてください。

ステップ 2　次の Firepower 7000 シリーズデバイスに付属のコンポーネントのリストと梱包品を照合してください。システムと関連アクセサリを開梱するときに、次のようにパッケージの中身が完全であることを確認してください。

- アプライアンス × 1
- 電源コード(2 本の電源コードが冗長電源を含むアプライアンスに付属しています)
- カテゴリ 5e イーサネット ストレート ケーブル:Firepower デバイス用に 2 本
- ラックマウント キット(Firepower 7010、7020、7030、および 7050 のそれぞれに使用する必須のトレイとラックマウント キット)× 1

ステップ 3　破損の有無を調べ、内容品の間違いや破損がある場合には、カスタマー サービス担当者に連絡してください。次の情報を用意しておきます。

- 発送元の請求書番号(梱包明細を参照)
- 破損している装置のモデルとシリアル番号
- 破損状態の説明
- 破損による設置への影響

セキュリティの考慮事項

Cisco では、アプライアンスを設置する前に、次の点を考慮することを推奨しています。

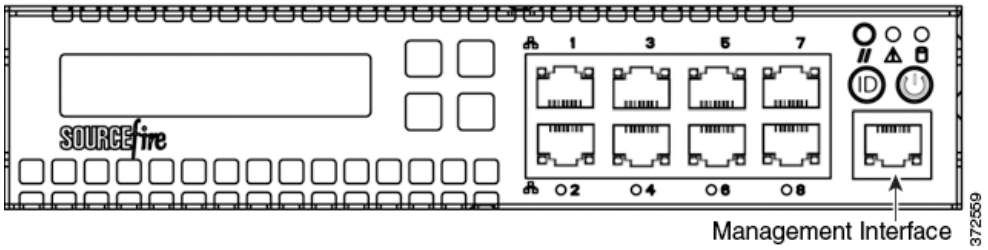
- 無許可ユーザによるアクセスから保護された安全な場所にあるロック付きラックにアプライアンスを配置します。
- アプライアンスの設置、交換、管理、または修理は、訓練を受け、資格要件を満たしている人物にのみ許可します。
- 管理インターフェイスは、必ず、不正アクセスから保護されたセキュアな内部管理ネットワークに接続します。
- アプライアンスへのアクセスを許可可能な特定のワークステーションの IP アドレスを特定します。アプライアンスのシステム ポリシー内のアクセス リストを使用している特定のホストにアプライアンスへのアクセスを限定します。詳細については、*Firepower Management Center Configuration Guide* を参照してください。

管理インターフェイスの識別

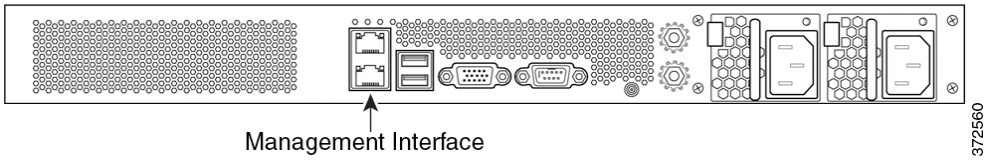
管理インターフェイスを使用して展開内の各アプライアンスをネットワークに接続します。これにより、Firepower Management Center は管理対象デバイスと通信して管理することができます。設置手順に従って作業する際、アプライアンスの正しい図を参照してください。

Firepower 7000 シリーズ

Firepower 7010、7020、7030、および 7050 はシャーシ トレイ幅の半分の 1U アプライアンスです。次のシャーシ前面図に、デフォルトの管理インターフェイスを示します。



Firepower 7110/7120、7115/7125、および AMP7150 は 1U アプライアンスとして提供されます。次のシャーシ背面図は、デフォルトの管理インターフェイスの位置を示しています。



センシング インターフェイスの識別

Firepower デバイスは、センシング インターフェイスを使用してネットワーク セグメントに接続します。1 つのデバイスで監視可能なセグメントの数は、デバイス上のセンシング インターフェイスの数とネットワーク セグメント上で使用する接続タイプ（パッシブ、インライン、ルーテッド、またはスイッチド）によって異なります。

以下の項では、各 Firepower デバイスのセンシング インターフェイスについて説明します。

- 7000 シリーズ上のセンシング インターフェイスを特定するには、Firepower 7000 シリーズ（3-3 ページ）を参照してください。

接続タイプについては、センシング インターフェイスについて（6-2 ページ）を参照してください。

Firepower 7000 シリーズ

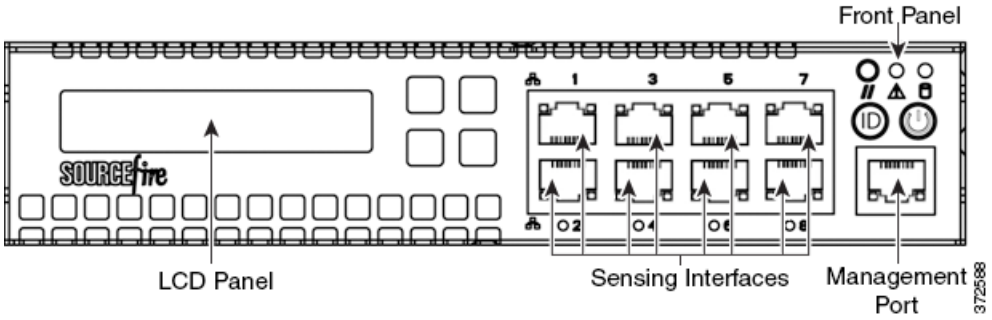
次の設定で、7000 シリーズを使用することができます。

- 個別にバイパス機能を設定可能な 8 つの銅線インターフェイスを備えたラック トレイ幅が半分の 1U デバイス
- 個別にバイパス機能を設定可能な 8 つの銅線インターフェイスまたは 8 つのファイバ インターフェイスを備えた 1U デバイス
- バイパス機能が設定可能な 4 つの銅線インターフェイスとバイパス機能のない 8 つの Small Form-Factor Pluggable（SFP）ポートを備えた 1U デバイス

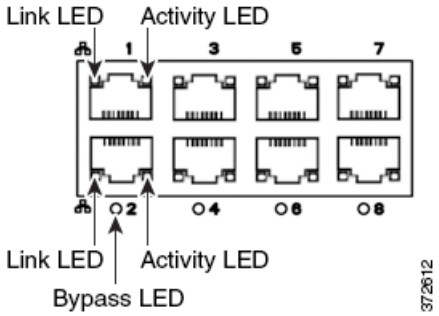
Firepower 7010、7020、7030、7050

Firepower 7010、7020、7030、および 7050 には、それぞれ設定可能なバイパス機能を持つ 8 つの銅線ポート センシング インターフェイスが付属しています。次のシャーシ前面図に、センシング インターフェイスの位置を示します。

図 3-1　　8 ポート 1000BASE-T 銅線設定可能バイパス インターフェイス



これらの接続を使用して、最大 8 つのネットワーク セグメントを受動的に監視できます。また、インラインでまたはバイパス モードのインラインでペア化されたインターフェイスを使用して、デバイスを最大 4 つのネットワーク上に侵入防御システムとして展開できます。



デバイスの自動バイパス機能を利用する場合は、2 つのインターフェイスをネットワーク セグメントに垂直に接続します(インターフェイス 1 と 2、3 と 4、5 と 6、または 7 と 8)。自動バイパス機能を使用すれば、デバイスで障害が発生した場合や電源を消失した場合でもトラフィックを伝送することができます。インターフェイスを接続したら、Web インターフェイスを使用して、インターフェイスのペアをインライン セットとして設定し、そのインライン セット上でバイパス モードを有効にします。

Firepower 7110 および 7120

Firepower 7110 および 7120 には、個別にバイパス機能を設定可能な 8 つの銅線ポート センシング インターフェイスまたは 8 つのファイバ ポート センシング インターフェイスが付属しています。次のシャーシ前面図に、センシング インターフェイスの位置を示します。

図 3-2　　Firepower 7110 および 7120 銅線インターフェイス

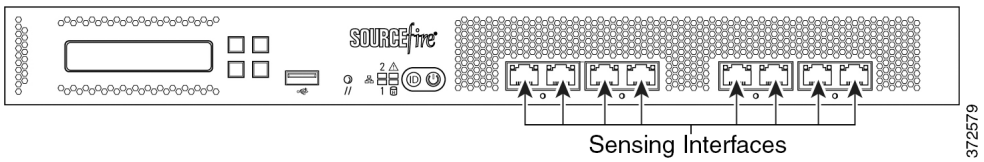
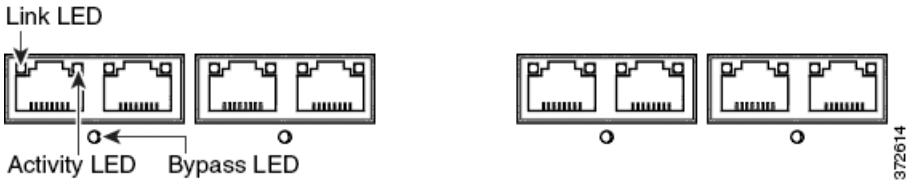


図 3-3　8 ポート 1000BASE-T 銅線インターフェイス



これらの接続を使用して、最大 8 つのネットワーク セグメントを受動的に監視できます。また、インラインでまたはバイパス モードのインラインでペア化されたインターフェイスを使用して、デバイスを最大 4 つのネットワーク上に侵入防御システムとして展開できます。

デバイスの自動バイパス機能を利用する場合は、ネットワーク セグメントの左側にある 2 つのインターフェイスまたはネットワーク セグメントの右側にある 2 つのインターフェイスを接続する必要があります。自動バイパス機能を使用すれば、デバイスで障害が発生した場合や電源を消失した場合でもトラフィックを伝送することができます。インターフェイスを接続したら、Web インターフェイスを使用して、インターフェイスのペアをインライン セットとして設定し、そのインライン セット上でパイパス モードを有効にします。

図 3-4　Firepower 7110 および 7120 ファイバ インターフェイス

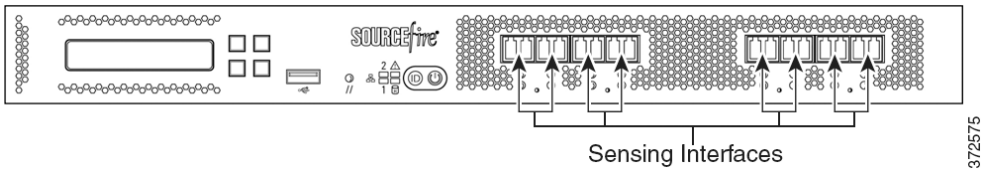


図 3-5　8 ポート 1000BASE-SX ファイバ設定可能バイパス

8 ポート 1000BASE-SX ファイバ設定可能バイパス設定では、LC タイプ（ローカル コネクタ）光トランシーバが使用されます。

これらの接続を使用して、最大 8 つのネットワーク セグメントを受動的に監視できます。また、インラインでまたはバイパス モードのインラインでペア化されたインターフェイスを使用して、デバイスを最大 4 つのネットワーク上に侵入防御システムとして展開できます。

ヒント　最高のパフォーマンスを得るために、インターフェイス セットを連続的に使用します。インターフェイスをスキップすると、パフォーマンスが低下する可能性があります。

デバイスの自動バイパス機能を利用する場合は、ネットワーク セグメントの左側にある 2 つのインターフェイスまたはネットワーク セグメントの右側にある 2 つのインターフェイスを接続する必要があります。自動バイパス機能を使用すれば、デバイスで障害が発生した場合や電源を消失した場合でもトラフィックを伝送することができます。インターフェイスを接続したら、Web インターフェイスを使用して、インターフェイスのペアをインライン セットとして設定し、そのインライン セット上でパイパス モードを有効にします。

Firepower 7115、7125、および AMP7150

Firepower 7115、7125、および AMP7150 デバイスには、バイパス機能を設定可能な 4 ポート銅線インターフェイスとバイパス機能のない 8 つのホットスワップ可能な Small Form-Factor Pluggable（SFP）ポートが付属しています。次のシャーシ前面図に、センシング インターフェイスの位置を示します。

図 3-6　Firepower 7115、7125 および AMP7150 の銅線インターフェイスと SFP インターフェイス

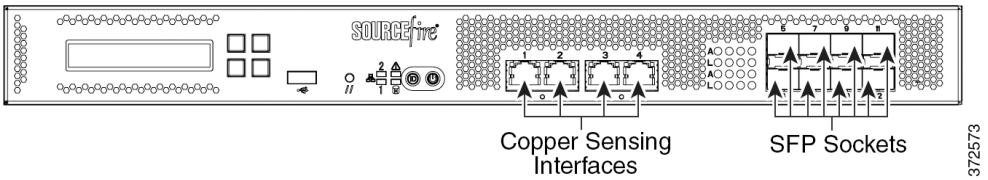
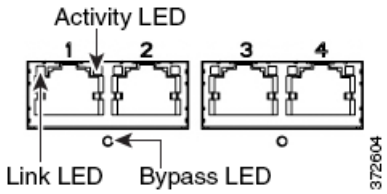


図 3-7　4 つの 1000BASE-T 銅線インターフェイス



銅線インターフェイスを使用して、4 つのネットワーク セグメントを受動的に監視することができます。また、インラインでまたはバイパス モードのインラインでペア化されたインターフェイスを使用して、デバイスを最大 2 つのネットワーク上に侵入防御システムとして展開できます。

デバイスの自動バイパス機能を利用する場合は、ネットワーク セグメントの左側にある 2 つのインターフェイスまたはネットワーク セグメントの右側にある 2 つのインターフェイスを接続する必要があります。自動バイパス機能を使用すれば、デバイスで障害が発生した場合や電源を消失した場合でもトラフィックを伝送することができます。インターフェイスを接続したら、Web インターフェイスを使用して、インターフェイスのペアをインライン セットとして設定し、そのインライン セット上でバイパス モードを有効にします。

SFP インターフェイス

Cisco SFP トランシーバを SFP ソケットに取り付ければ、最大 8 つのネットワーク セグメントを受動的に監視することができます。また、インライン非バイパス モードでペア化されたインターフェイスを使用して、デバイスを最大 4 つのネットワーク上に侵入防御システムとして展開できます。

Cisco SFP トランシーバは、1G 銅線、1G 短距離ファイバ、または 1G 長距離ファイバで使用し、ホットスワップ可能です。デバイス内の銅線またはファイバ トランシーバの任意の組み合わせをパッシブ設定とインライン設定のどちらかで使用できます。SFP トランシーバはバイパス機能を備えていないため、侵入防御展開で使用しないようにする必要があることに注意してください。互換性を保証するために、Cisco から入手可能な SFP トランシーバだけを使用してください。詳細については、「Firepower 71x5 および AMP7150 デバイスでの SFP トランシーバの使用（B-1 ページ）」を参照してください。

図 3-8　　サンプル SFP トランシーバ

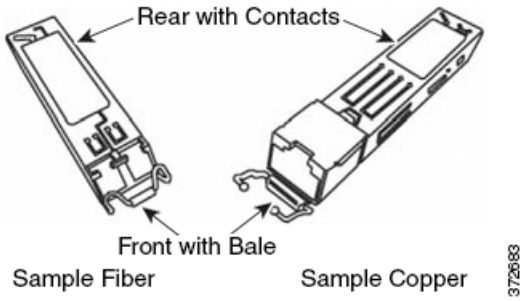
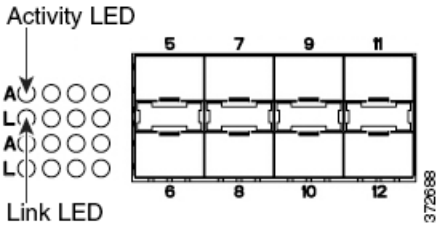


図 3-9　　SFP ソケット



ラックへの Firepower デバイスの設置

すべての Firepower デバイスをラックマウントできます（Firepower 7010、7020、7030、および 7050 用の 1U マウント キットを購入した場合）。アプライアンスを設置するときに、アプライアンスのコンソールにアクセスできることを確認する必要もあります。初期設定でコンソールにアクセスするには、次のいずれかの方法で 1 つのアプライアンスに接続します。

キーボードとモニタ/KVM

USB キーボードと VGA モニタを 1 つの Firepower デバイスに接続できます。これは、キーボード、ビデオ、およびマウス（KVM）スイッチに接続される、ラックマウント アプライアンスで便利です。

注意　アプライアンスは大容量ストレージ デバイスをブート デバイスとして使用する可能性があるため、初期セットアップのためにアプライアンスにアクセスするときには、KVM コンソールと一緒に USB 大容量ストレージを**使用しない**でください。

管理インターフェイスへのイーサネット接続

次のネットワーク設定を使用して、インターネットに接続してはならないローカル コンピュータを設定します。

- IP アドレス：`192.168.45.2`
- ネットマスク：`255.255.255.0`
- デフォルト ゲートウェイ：`192.168.45.1`

イーサネット ケーブルを使用して、ローカル コンピュータ上のネットワーク インターフェイスをアプライアンス上の管理インターフェイスに接続します。管理インターフェイスは、デフォルト IPv4 アドレスで事前に設定されていることに注意してください。ただし、設定プロセスの一部として、管理インターフェイスを IPv6 アドレスで再設定できます。

初期設定後に、次の追加の方法でコンソールにアクセスできます。

シリアル接続/ラップトップ

物理シリアル ポートを使用して、コンピュータを任意の Firepower デバイスに接続できます。適切なロールオーバー シリアル ケーブル（ヌル モデム ケーブルまたはシスコ コンソール ケーブルとも呼ばれる）を常に接続した状態で、デフォルト VGA 出力をシリアル ポートにリダイレクトするようリモート管理コンソールを設定してください。アプライアンスと通信するには、HyperTerminal や Xmodem などの端末エミュレーション ソフトウェアを使用します。このソフトウェアの設定は、9600 ボー、8 データ ビット、パリティ チェックなし、1 ストップ ビット、およびフロー制御なしです。

シリアル ポートには、アプライアンスによって RJ-45 接続と DB-9 接続のどちらかが実装されています。アプライアンス別のコネクタについては、次の表を参照してください。

表 3-1　モデル別のシリアル コネクタ

Firepower アプライアンス	コネクタ
70xx ファミリ	RJ-45
71xx ファミリ	DB-9（メス）

適切なロールオーバー ケーブルをデバイスに接続した後、*FirePower 7000 シリーズ スタートアップ ガイド*に記載されているようにコンソール出力をリダイレクトします。各アプライアンスのシリアル ポートを特定するには、ハードウェア仕様（2-1 ページ）の図を使用してください。

Serial over LAN を使用した Lights-Out Management

LOM 機能を使用すると、SOL 接続を通して Firepower Management Center または Firepower デバイスに対して限定的なアクション セットを実行できます。LOM 対応アプライアンスを工場出荷時設定に復元する必要があるが、このアプライアンスに物理的にアクセスできない場合は、LOM を使用して復元プロセスを実行できます。LOM を使用してアプライアンスに接続した後で、物理シリアル接続を使用する場合と同様の方法で、復元ユーティリティに対してコマンドを発行します。詳細については、*FirePower 7000 シリーズ スタートアップ ガイド*を参照してください。

コメント　Lights-Out Management は、デフォルト（`eth0`）管理インターフェイス上でのみ使用可能です。

LOM を使用してアプライアンスを工場出荷時設定に復元するには、ネットワーク設定を削除**しないでください**。ネットワーク設定を削除すると、LOM 接続もドロップされます。詳細については、*FirePower 7000 シリーズ スタートアップ ガイド*を参照してください。

アプライアンスを設置するには:

ステップ 1　取り付けキットと付属の手順を使用して、アプライアンスをラックに取り付けます。

ステップ 2　キーボードとモニタまたはイーサネット接続を使用してアプライアンスに接続します。

ステップ 3　キーボードとモニタを使用してアプライアンスを設定している場合は、ここでイーサネット ケーブルを使用して管理インターフェイスを保護されたネットワーク セグメントに接続します。

コンピュータを直接アプライアンスの管理インターフェイスに接続することによって初期設定プロセスを実行する予定の場合は、設定の完了時に、管理インターフェイスを保護されたネットワークに接続します。

ステップ 4　Firepower デバイスの場合は、インターフェイスに対して適切なケーブルを使用して、センシング インターフェイスを分析対象のネットワーク セグメントに接続します。

- 銅線センシング インターフェイス：デバイスに銅線センシング インターフェイスがある場合は、適切なケーブルを使用してデバイスがネットワークに接続されていることを確認します。銅線インターフェイスでのインライン展開のケーブル配線（6-6 ページ）を参照してください。
- ファイバ アダプタ カード：ファイバ アダプタ カードを備えたデバイスの場合は、オプションのマルチモード ファイバ ケーブルの LC コネクタを、任意の順序でアダプタ カード上の 2 つのポートに接続します。SC プラグを分析対象のネットワーク セグメントに接続します。
- ファイバ タップ：オプションの光ファイバ タップを備えたデバイスを展開している場合は、オプションのマルチモード ファイバ ケーブルの SC プラグをタップ上の「アナライザ」ポートに接続します。タップを分析対象のネットワーク セグメントに接続します。
- 銅線タップ：オプションの銅線タップを備えたデバイスを展開している場合は、タップの左側にある A ポートと B ポートを分析対象のネットワーク セグメントに接続します。タップの右側にある A ポートと B ポート（「アナライザ」ポート）をアダプタ カード上の 2 つの銅線ポートに接続します。

管理対象デバイスを展開するためのオプションについては、Firepower 管理対象デバイスの展開（6-1 ページ）を参照してください。

バイパス インターフェイスを備えたデバイスを展開している場合は、デバイスで障害が発生してもネットワーク接続を維持できるデバイスの能力を活用できることに注意してください。設置と遅延のテストについては、インライン バイパス インターフェイスの設置のテスト（3-10 ページ）を参照してください。

ステップ 5　電源コードをアプライアンスに接続し、電力源に差し込みます。

アプライアンスに冗長電源がある場合は、電源コードを両方の電源に接続し、別々の電源に差し込みます。

ステップ 6　アプライアンスの電源をオンにします。

直接イーサネット接続を使用してアプライアンスを設定する場合は、ローカル コンピュータ上のネットワーク インターフェイスとアプライアンス上の管理インターフェイスの両方のリンク LED が点灯していることを確認してください。管理インターフェイスとネットワーク インターフェイスの LED が点灯していない場合は、クロス ケーブルを使用してみてください。詳細については、銅線インターフェイスでのインライン展開のケーブル配線（6-6 ページ）を参照してください。

次の作業

- 新しいアプライアンスが信頼された管理ネットワークで通信できるようにするセットアップ プロセスを実行します。*FirePower 7000 シリーズ スタートアップ ガイド*を参照してください。
- バイパス インターフェイスを使用してデバイスを展開している場合は、それらのデバイスが正しく設置されているかどうかをテストします。インライン バイパス インターフェイスの設置のテスト（3-10 ページ）を参照してください。

インライン バイパス インターフェイスの設置のテスト

バイパス インターフェイスを備えた管理対象デバイスは、デバイスの電源がオフになっていても、デバイスが動作不能でもネットワーク接続を維持することができます。このようなデバイスが適切に設置され、それによる遅延が定量化されていることを確認することが重要です。

コメント　スイッチのスパニング ツリー ディスカバリ プロトコルは 30 秒のトラフィック遅延を引き起こす可能性があります。Cisco では、次の手順でスパニング ツリーを無効にすることを推奨しています。

銅線インターフェイスにのみ適用可能な次の手順では、インライン バイパス インターフェイスの設置と ping の遅延をテストする方法について説明します。ping テストを実行するネットワークに接続し、管理対象デバイスのコンソールに接続する必要があります。

はじめる前に

- Firepower デバイスのインターフェイス セット タイプがインライン バイパス モード用に設定されていることを確認します。インターフェイス セットをインライン バイパス モード用に設定する手順については、『*Firepower Management Center Configuration Guide*』の「Configuring Inline Sets」を参照してください。

インライン バイパス インターフェイスが設置されたデバイスをテストするには:

アクセス: Admin

ステップ 1　スイッチ上のすべてのインターフェイス、ファイアウォール、およびデバイスのセンシング インターフェイスを自動ネゴシエーションに設定します。

コメント　Firepower システムデバイスでは、自動 MDIX を使用する場合に自動ネゴシエーションが必要です。

ステップ 2　デバイスの電源をオフにして、すべてのネットワーク ケーブルを外します。

デバイスを再接続して、適切なネットワーク接続が存在することを確認します。デバイスからスイッチおよびファイアウォールへのクロス ケーブルとストレート ケーブルの配線手順を確認します。銅線インターフェイスでのインライン展開のケーブル配線（6-6 ページ）を参照してください。

ステップ 3　デバイスの電源をオフにして、デバイス経由でファイアウォールからスイッチに ping できることを確認します。

ping が失敗した場合は、ネットワーク配線を修正します。

ステップ 4　ステップ 9 が完了するまで継続的に ping を実行します。

ステップ 5　デバイスの電源をオンにします。

ステップ 6　キーボード/モニタまたはシリアル接続を使用し、管理者特権を持つアカウントでデバイスにログインします。パスワードは、デバイスの Web インターフェイスのパスワードと同じです。

デバイスのプロンプトが表示されます。

ステップ 7　「`system shutdown`」と入力して、デバイスをシャットダウンします。

また、Web インターフェイスを使用してデバイスをシャットダウンすることもできます。『*Firepower Management Center Configuration Guide*』の「Managing Devices」の章を参照してください。ほとんどのデバイスで電源をオフにすると、カチッという音がします。この音は、リレーが切り替わって、デバイスがハードウェア バイパスに移行した音です。

ステップ 8　30 秒間待機します。

ping トラフィックが再開したことを確認します。

ステップ 9　デバイスの電源をオンにして、ping トラフィックが継続的に通過していることを確認します。

ステップ 10　タップ モードをサポートする Firepower デバイスの場合は、次の条件下で ping 遅延結果をテストして記録できます。

- デバイスの電源がオフ
- デバイスの電源がオン、ポリシーにルールが適用されていない、インライン侵入ポリシー保護モード
- デバイスの電源がオン、ポリシーにルールが適用されていない、インライン侵入ポリシー保護タップ モード
- デバイスの電源がオン、ポリシーに調整済みのルールが適用されている、インライン侵入ポリシー保護モード

設置の遅延期間が容認できる範囲であることを確認します。過剰な遅延の問題の解決方法については、『*Firepower Management Center Configuration Guide*』の「Configuring Packet Latency Thresholding and Understanding Rule Latency Thresholding」を参照してください。