Firepower 管理対象デバイスの展開

Firepower Management Center にデバイスを登録したら、侵入検知システムを使用してトラフィックを監視するため、または侵入防御システムを使用してネットワークを脅威から保護するために、デバイスのセンシング インターフェイスをネットワーク セグメントに展開します。

センシングの展開に関する考慮事項

センシングの展開に関する決定は、さまざまな要素に基づいて行います。以下の質問に答えることで、自分のネットワークの脆弱な領域を理解し、侵入検知と侵入防御のニーズを明確にすることができます。

- パッシブ インターフェイスまたはインライン インターフェイスを使用して管理対象デバイスを展開するのか。デバイスはインターフェイスの混在（一部がパッシブで、その他はインライン）をサポートするのか。詳細については、「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。
- 管理対象デバイスをネットワークに接続する手段は何か。ハブ、タップ、スイッチ上のスパニング ポート、または仮想スイッチを使用するのか。詳細については、「ネットワークへのデバイスの接続（6-5 ページ）」を参照してください。
- ネットワーク上のすべての攻撃を検出する必要があるのか、またはファイアウォールを通過する攻撃についてのみ知りたいのか。特殊なセキュリティ ポリシーを必要とする、財務、会計、人事記録、生産コード、その他の機密性の高い保護された情報など、特定の資産がネットワーク上に存在しますか。詳細については、「展開オプション（6-7 ページ）」を参照してください。
- 管理対象デバイスの複数のセンシング インターフェイスを、ネットワーク タップからのさまざまな接続を再結合するために使用しますか、またはさまざまなネットワークからのトラフィックをキャプチャして評価するために使用しますか。複数のセンシング インターフェイスを、仮想ルータまたは仮想スイッチのどちらとして機能するように使用しますか。詳細については、「管理対象デバイスでの複数のセンシング インターフェイスの使用（6-18 ページ）」を参照してください。
- リモートの作業者が VPN またはモデムでアクセスできるようにするのか。侵入防御の展開を必要とするリモート オフィスがありますか。契約社員やその他の臨時スタッフを雇用しているか。それらのスタッフを特定のネットワーク セグメントに制限しているか。自社のネットワークを、顧客、サプライヤ、ビジネス パートナーなどの他の組織のネットワークと統合するか。詳細については、「複雑なネットワーク展開（6-20 ページ）」を参照してください。

センシング インターフェイスについて

以下の項では、さまざまなセンシング インターフェイスが Firepower システムの機能に与える影響について説明します。パッシブ インターフェイスとインライン インターフェイスに加え、ルーテッド インターフェイス、スイッチド インターフェイス、ハイブリッド インターフェイスを使用することもできます。

センシング インターフェイスはデバイスの前面にあります。センシング インターフェイスを識別するには、センシング インターフェイスの識別（3-3 ページ）を参照してください。

パッシブ インターフェイス

スイッチの SPAN、仮想スイッチ、またはミラー ポートを使用して、ネットワークで送られるトラフィックを監視するパッシブ展開を設定し、スイッチ上の他のポートからトラフィックをコピーできるようにすることができます。パッシブ インターフェイスでは、ネットワーク内のトラフィックを、そのネットワーク トラフィック フローの外部から検査できます。パッシブ展開で構成されたシステムでは、特定のアクション（トラフィックのブロッキングやシェーピングなど）を実行することができません。パッシブ インターフェイスは、すべてのトラフィックを無条件で受信し、受信したトラフィックを再送信しません。

インライン インターフェイス

2 つのポートを一緒にバインドすることで、インライン構成をネットワーク セグメントにトランスペアレントに設定します。インライン インターフェイスを使用すれば、隣接するネットワーク デバイスを設定することなく、任意のネットワーク コンフィギュレーションでデバイスを設置できます。インライン インターフェイスは、すべてのトラフィックを無条件に受信し、明示的にドロップされたトラフィックを除くすべての受信トラフィックを再送信します。インライン インターフェイスがインライン展開環境のトラフィックを処理するには、その前に、インライン インターフェイスのペアをインライン セットに割り当てる必要があります。

コメント　インターフェイスをインライン インターフェイスとして設定すると、そのインターフェイスの NetMod 上の隣接ポートも自動的にインライン インターフェイスとなり、インライン インターフェイスのペアが完成します。

設定可能なバイパス インライン セットを使用して、ハードウェアが完全に故障した場合（たとえば、デバイスが電力を失った場合など）にトラフィックを処理する方法を選択できます。たとえば、あるネットワーク セグメントでは接続が不可欠であり、別のネットワーク セグメントでは未検査のトラフィックを許可できないと指定することができます。設定可能なバイパス インライン セットを使用することで、次のいずれかの方法でネットワークのトラフィック フローを管理できます。

- *バイパス*：バイパスとして設定したインターフェイスのペアを使用して、デバイスで故障が発生した場合でも、すべてのトラフィックのフローを維持します。トラフィックは、デバイスをバイパスし、そのデバイスによる検査や他の処理をバイパスします。バイパスでは、検査が行われないトラフィックがネットワーク セグメント間を通過する可能性がありますが、ネットワークの接続性は保持されます。

- *非バイパス*:非バイパスに設定されているインターフェイス ペアは、デバイスに障害が発生した場合、すべてのトラフィックを停止させます。障害が発生したデバイスに到達したトラフィックは、そのデバイスに入りません。非バイパスでは、未検査のトラフィックがネットワーク セグメントを通過することを許可しませんが、デバイスに障害が発生すると、ネットワーク セグメントは接続を失います。ネットワーク セキュリティの重要性がトラフィックの損失よりも優先される展開環境では、非バイパス インターフェースを使用します。

デバイスに障害が発生しても、トラフィック フローが維持されるようにする場合は、インライン セットをバイパスとして設定します。デバイスに障害が発生した場合にトラフィックを停止するには、インライン セットを非バイパスとして設定します。再イメージ化によって、バイパス モードの Firepower デバイスが非バイパスの設定にリセットされて、バイパス モードを再設定するまでは、ネットワーク上のトラフィックが中断されることに注意してください。詳細については、*FirePower 8000 シリーズ スタートアップ ガイド*を参照してください。

設定可能なバイパス インターフェイスは、すべての Firepower デバイスに含めることができます。8000 シリーズデバイスには、バイパスに設定できないインターフェイスを持つ NetMods を含めることもできます。NetMods の詳細については、Firepower 8000 シリーズモジュール（2-13 ページ）を参照してください。他の拡張インターフェイス オプションには、タップ モード、リンク ステート伝搬、トランスペアレント インライン モード、ストリクト TCP モードが含まれます。インライン インターフェイス セットを設定する方法については、『*Firepower Management Center Configuration Guide*』の「Configuring Inline Sets」を参照してください。インライン インターフェイスの使用方法について詳しくは、ネットワークへのデバイスの接続（6-5 ページ）を参照してください。

Firepower Management Center を使用して ASA FirePOWER デバイスのバイパス インターフェイスを設定することはできません。インライン モードの ASA FirePOWER デバイスを設定する方法について詳しくは、ASA のドキュメントを参照してください。

スイッチド インターフェイス

レイヤ 2 展開環境の Firepower デバイスにスイッチド インターフェイスを設定することで、複数のネットワーク間でのパケット スイッチングに対応できます。また、Firepower デバイスにスタンドアロン ブロードキャスト ドメインとして機能する仮想スイッチを設定して、ネットワークを論理セグメントに分割することもできます。仮想スイッチは、ホストからの Media Access Control（MAC）アドレスを使用して、パケットの送信先を判別します。

スイッチド インターフェイスには、物理構成または論理構成を使用できます。

- *物理スイッチド インターフェイス*は、スイッチングが設定された物理インターフェイスです。タグなし VLAN トラフィックを処理するには、物理スイッチド インターフェイスを使用します。
- *論理スイッチド インターフェイス*は、物理インターフェイスと VLAN タグとの間のアソシエーションです。VLAN タグが指定されたトラフィックを処理するには、論理インターフェイスを使用します。

仮想スイッチはスタンドアロン ブロードキャスト ドメインとして機能し、ネットワークを論理セグメントに分割します。仮想スイッチは、ホストからの Media Access Control（MAC）アドレスを使用して、パケットの送信先を判別します。仮想スイッチを設定すると、スイッチはまず、スイッチ上の使用可能なすべてのポートからパケットをブロードキャストします。その後は、タグ付きのリターン トラフィックを使用して、各ポートに接続されたネットワーク上にどのホストが存在するのかを学習していきます。

デバイスを仮想スイッチとして設定し、残りのインターフェイスを使用して、モニタ対象のネットワーク セグメントに接続できます。デバイス上で仮想スイッチを使用するには、物理スイッチド インターフェイスを作成した後、『*Firepower Management Center Configuration Guide*』の「Setting Up Virtual Switches」に記載されている手順に従ってください。

ルーテッド インターフェイス

レイヤ 3 展開の Firepower デバイスにルーテッド インターフェイスを設定し、複数のインターフェイス間でトラフィックをルーティングすることができます。各インターフェイスに IP アドレスを割り当て、これらのインターフェイスを、トラフィックをルーティングする仮想ルータに割り当てる必要があります。

ゲートウェイのバーチャル プライベート ネットワーク（ゲートウェイ VPN）または Network Address Translation（NAT）と併用するための、ルーテッド インターフェイスを設定できます。詳細については、ゲートウェイ VPN の展開（6-11 ページ）およびポリシー ベースの NAT を使用した展開（6-12 ページ）を参照してください。

また、宛先アドレスに応じてパケットの転送決定を行って、パケットをルーティングするようにシステムを設定することもできます。ルーテッド インターフェイスとして設定されたインターフェイスは、レイヤ 3 トラフィックを受信し、転送します。ルータは、転送基準に基づく発信インターフェイスからの宛先を取得します。適用するセキュリティ ポリシーは、アクセス制御ルールによって指定されます。

ルーテッド インターフェイスには、物理構成または論理構成を使用できます。

- *物理ルーテッド インターフェイス*は、ルーティングが設定された物理インターフェイスです。タグなし VLAN トラフィックを処理するには、物理ルーテッド インターフェイスを使用します。
- *論理スイッチド インターフェイス*は、物理インターフェイスと VLAN タグとの間のアソシエーションです。VLAN タグが指定されたトラフィックを処理するには、論理インターフェイスを使用します。

レイヤ 3 展開でルーテッド インターフェイスを使用するには、仮想ルータを設定し、それらの仮想ルータにルーテッド インターフェイスを割り当てる必要があります。仮想ルータは、レイヤ 3 トラフィックをルーティングするルーテッド インターフェイスのグループです。

デバイスを仮想ルータとして設定し、残りのインターフェイスを使用して、モニタ対象のネットワーク セグメントに接続できます。また、厳密な TCP 適用を有効にして、TCP セキュリティを最大限に強化することもできます。デバイス上で仮想ルータを使用するには、デバイスに物理ルーテッド インターフェイスを作成した後、『*Firepower Management Center Configuration Guide*』の「Setting Up Virtual Routers」に記載されている手順に従ってください。

ハイブリッド インターフェイス

Firepower デバイス上に論理ハイブリッド インターフェイスを設定することで、Firepower システムが仮想ルータと仮想スイッチの間でトラフィックをブリッジできるようになります。仮想スイッチのインターフェイスで受信した IP トラフィックの宛先が、そのスイッチに関連付けられたハイブリッド論理インターフェイスの MAC アドレスとなっている場合、システムは、そのトラフィックをレイヤ 3 トラフィックとして処理し、宛先 IP アドレスに応じてトラフィックをルーティング（またはトラフィックに応答）します。それ以外の宛先が設定されたトラフィックを受信した場合、システムはそのトラフィックをレイヤ 2 トラフィックとして処理し、適切なスイッチングを行います。

ハイブリッド インターフェイスを作成するには、まず、仮想スイッチと仮想ルータを設定し、それらの仮想スイッチと仮想ルータをハイブリッド インターフェイスに追加します。仮想スイッチと仮想ルータの両方に関連付けられていないハイブリッド インターフェイスは、ルーティングに使用できません。したがって、トラフィックを生成することも、トラフィックに応答することもしません。

ネットワーク アドレス変換（NAT）を使用するハイブリッド インターフェイスを設定すると、ネットワーク間でのトラフィックの受け渡しが可能になります。詳細については、ポリシー ベースの NAT を使用した展開（6-12 ページ）を参照してください。

デバイス上でハイブリッド インターフェイスを使用するには、デバイスにハイブリッド インターフェイスを定義した後、『*Firepower Management Center Configuration Guide*』の「Setting Up Hybrid Interfaces」に記載されている手順に従ってください。

ネットワークへのデバイスの接続

管理対象デバイスのセンシング インターフェイスは複数の方法でネットワークに接続できます。パッシブまたはインライン インターフェイスを使用してハブまたはネットワーク タップを設定するか、またはパッシブ インターフェイスを使用して Span ポートを設定します。

ハブの使用

管理対象デバイスがネットワーク セグメントのすべてのトラフィックを認識できるようにするには、イーサネット ハブが簡単な手段となります。このタイプのほとんどのハブは、セグメント上のいずれかのホストを目的とする IP トラフィックを取得し、そのトラフィックをハブに接続されているすべてのデバイスにブロードキャストします。設定したインターフェイスをハブに接続して、セグメントのすべての着信および発信トラフィックをモニタします。トラフィック量が大きいネットワークでは、パケット衝突の可能性があるため、ハブを使用しても検出エンジンがすべてのパケットを認識するとは限りません。この問題は、低トラフィックの単純なネットワークではほとんど発生しません。トラフィック量の大きいネットワークでは、ハブ以外のオプションのほうが良い結果を得られる場合があります。ハブに障害が発生した場合、またはハブが電源を失った場合は、ネットワーク接続が切断されることに注意してください。その場合、単純なネットワークでは、ネットワークがダウンします。

一部のデバイスはハブとして販売されていますが、実際にはスイッチとして機能し、各パケットをすべてのポートにブロードキャストするわけではありません。管理対象デバイスをハブに接続してもすべてのトラフィックが表示されない場合は、別のハブを購入するか、SPAN ポートを備えたスイッチを使用してください。

SPAN ポートの使用

多くのネットワーク スイッチには、1 つ以上のポートのトラフィックをミラーリングする SPAN ポートが組み込まれています。設定したインターフェイスを SPAN ポートに接続することで、すべてのポートのトラフィック（通常は着信トラフィックと発信トラフィックの両方）をまとめてモニタできます。この機能を備えたスイッチをすでにネットワーク上の適切な場所で使用している場合、管理対象デバイスのコストの他にはほとんど機器にコストをかけることなく、複数のセグメントで検出機能を展開できます。トラフィックの多いネットワークの場合、このソリューションには制限があります。SPAN ポートが 200Mbps を処理することができ、3 つのミラー対象ポートのそれぞれが 100Mbps まで処理できる場合、SPAN ポートはオーバーサブスクライブされてパケットをドロップするようになり、管理対象デバイスの効率が減少する可能性があります。

ネットワーク タップの使用

ネットワーク タップを使用すると、ネットワーク フローを中断したり、ネットワー トポロジーを変更したりすることなく、トラフィックをパッシブにモニタできます。タップはさまざまな帯域幅ですぐに使用できます。タップを使用することで、ネットワーク セグメントの着信パケットと発信パケットの両方を分析できます。通常、タップでモニタできるネットワーク セグメントは 1 つに限られるため、スイッチ上の 8 個のポートのうち、2 個のポートでトラフィックをモニタする必要がある場合には、タップは有効なソリューションになりません。その場合は、ルータとスイッチの間にタップを設置し、スイッチへの IP ストリーム全体にアクセスします。

仕様上、ネットワーク タップは着信トラフィックと発信トラフィックを 2 つの異なるケーブルで 2 つのストリームに分割します。管理対象デバイスは、通信の 2 つの部分を再結合する複数センシング インターフェイスのオプションを提供し、トラフィック ストリーム全体がデコーダ、プリプロセッサ、および検出エンジンによって評価されるようにします。

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

ネットワークでデバイスをインライン展開する場合、デバイスのパイパス機能を使用して、デバイスに障害が発生してもネットワーク接続を維持できるようにするには、ケーブル配線に特に注意する必要があります。

ファイバ バイパス対応インターフェイスを備えたデバイスを展開する場合は、接続がしっかり固定されていて、ケーブルがよじれていないことを確認する以外に、ケーブル配線に関する特別な懸念事項はありません。一方、ファイバ ネットワーク インターフェイスではなく銅線インターフェイスを使用したデバイスを展開する場合、デバイスのモデルによって使用するネットワーク カードが異なるため、使用するデバイス モデルに注意する必要があります。一部の 8000 シリーズ NetMods ではバイパス設定が許可されないことに注意してください。

デバイスのネットワーク インターフェイス カード（NIC）でサポートしている Auto-Medium Dependent Interface Crossover（Auto-MDI-X）と呼ばれる機能を使用すると、ネットワーク インターフェイスは、ストレート イーサネット ケーブルまたはクロス イーサネット ケーブルのどちらを使用して別のネットワーク デバイスに接続するかを自動的に設定します。Firepower デバイスは、クロスオーバー接続としてバイパスされます。

デバイスを展開することなく通常どおりにデバイスを配線します。デバイスへの電源供給が失われても、リンクは機能する必要があります。通常は、2 本のストレート ケーブルを使用して、2 つのエンドポイントにデバイスを接続します。

図 6-1　　クロス接続でバイパスする場合のケーブル配線

次の表は、ハードウェア バイパス設定で、クロス ケーブルまたはストレート ケーブルを使用するケースを示しています。展開環境では、レイヤ 2 ポートがストレート（MDI）エンドポイントとして機能し、レイヤ 3 ポートがクロス（MDIX）エンドポイントとして機能することに注意してください。バイパスが正常に機能するには、クロス（ケーブルおよびアプライアンス）の合計が奇数でなければなりません。

表 6-1　ハードウェア バイパスの有効な設定

エンドポイント 1	ケーブル	管理対象デバイス	ケーブル	エンドポイント 2
MDIX	ストレート	ストレート	ストレート	MDI
MDI	クロス	ストレート	ストレート	MDI
MDI	ストレート	ストレート	クロス	MDI
MDI	ストレート	ストレート	ストレート	MDIX
MDIX	ストレート	クロス	ストレート	MDIX
MDI	ストレート	クロス	ストレート	MDI
MDI	クロス	クロス	クロス	MDI
MDIX	クロス	クロス	ストレート	MDI

すべてのネットワーク環境が一意であり、エンドポイントの Auto-MDI-X のサポートの組み合わせが異なっていることに注意してください。デバイスが正しいケーブル配線で設置されていることを確認する最も簡単な方法は、まずデバイスの電源をオフにした上で、1 本のクロス ケーブルと 1 本のストレート ケーブルを使用してデバイスを 2 つのエンドポイントに接続することです。この 2 つのエンドポイントが通信できることを確認します。通信できない場合は、一方のケーブルのタイプが誤っています。その場合は、ケーブルの一方だけを別のタイプ（ストレート ケーブルまたはクロス ケーブル）と交換します。

インライン デバイスの電源が入っていない状態で、2 つのエンドポイントが正常に通信できるようになったら、デバイスの電源を投入します。Auto-MDI-X 機能により、2 つのエンドポイント間の通信は維持されます。インライン デバイスを交換する必要がある場合は、元のデバイスと交換デバイスのバイパス特性が異なっている場合に備え、新しいデバイスの電源が入っていない状態で、エンドポイントが通信できることを確認するプロセスを再度実行してください。

Auto-MDI-X 設定は、ネットワーク インターフェイスの自動ネゴシエーションを許可している場合にのみ、正常に機能します。[Network Interface] ページの [Auto Negotiate] オプションを無効にする必要があるネットワーク環境の場合は、インライン ネットワーク インターフェイスに適切な MDI/MDIX オプションを指定する必要があります。詳細については、『*Firepower Management Center Configuration Guide*』の「Configuring Inline Interfaces」を参照してください。

特殊なケース：Firepower 8000 シリーズデバイスの接続

Firepower 8000 シリーズの管理対象デバイスを Firepower Management Center に登録するときは、接続の両側で自動ネゴシエーションを使用するか、またはその両側を同じ固定速度に設定して、ネットワーク リンクが安定したものとなるようにする必要があります。8000 シリーズの管理対象デバイスは、半二重のネットワーク リンクをサポートしません。また、接続の反対側の速度構成やデュプレックス構成の違いもサポートしません。

展開オプション

ネットワーク セグメントに管理対象デバイスを配置すると、侵入検知システムを使用してトラフィックをモニタすることや、侵入防御システムを使用してネットワークを脅威から保護することが可能になります。

また、仮想スイッチ、仮想ルータ、またはゲートウェイ VPN として機能する管理対象デバイスを展開することもできます。さらに、ポリシーを使用してトラフィックをルーティングしたり、ネットワークでのトラフィックへのアクセスを制御したりすることもできます。

仮想スイッチを使用した展開

インライン インターフェイスをスイッチド インターフェイスとして設定することで、管理対象デバイス上に*仮想スイッチ*を作成できます。仮想スイッチは、展開環境でレイヤ 2 パケット スイッチングを行います。拡張オプションには、スタティック MAC アドレスの設定、スパニング ツリー プロトコルの有効化、厳密な TCP 適用の有効化、ドメイン レベルでのブリッジ プロトコル データ ユニット（BPDU）のドロップが含まれます。スイッチド インターフェイスの詳細については、スイッチド インターフェイス（6-3 ページ）を参照してください。

仮想スイッチがトラフィックを処理するには、仮想スイッチに複数のスイッチド インターフェイスがなければなりません。仮想スイッチごとに、システムはスイッチド インターフェイスとして設定されたポートのセットにのみトラフィックをスイッチングします。たとえば、4 つのスイッチド インターフェイスを使用して仮想スイッチを設定した場合、システムは 1 つのポートからトラフィック パケットを受信すると、それらのパケットをスイッチ上の残りの 3 つのポートにブロードキャストします。

トラフィックを許可するように仮想スイッチを設定するには、まず、物理ポートに複数のスイッチド インターフェイスを設定します。そして、仮想スイッチを追加して設定した後、その仮想スイッチを、物理ポートに設定したスイッチド インターフェイスに割り当てます。システムは、スイッチド インターフェイスが待機していない、外部物理インターフェイスで受信したすべてのトラフィックをドロップします。システムが VLAN タグなしのパケットを受信した場合、該当するポートに物理スイッチド インターフェイスが設定されていなければ、パケットはドロップされます。システムが VLAN タグ付きのパケットを受信した場合、論理スイッチド インターフェイスが設定されていなければ、同じくパケットはドロップされます。

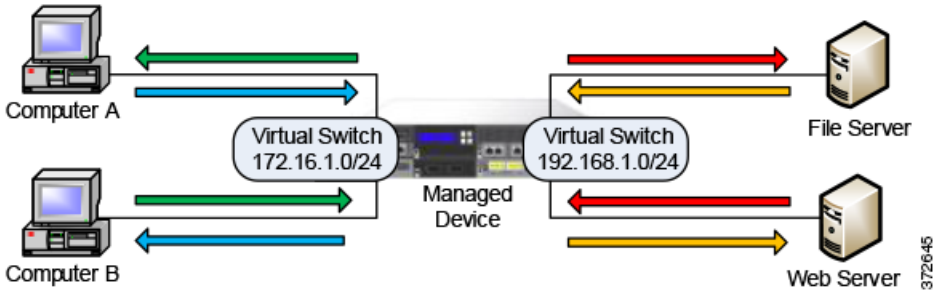
物理ポートには、必要に応じて追加の論理スイッチド インターフェイスを定義できます。ただし、論理スイッチド インターフェイスを仮想スイッチに割り当てなければ、トラフィックは処理されません。

仮想スイッチには、スケーラビリティに関する利点があります。物理スイッチを使用する場合、スイッチ上の使用可能なポートの数が制限されています。物理スイッチを仮想スイッチに置き換えると、帯域幅と展開環境に導入する複雑さのレベルのみによって制限されます。

ワークグループの接続やネットワークのセグメント化など、レイヤ 2 スイッチを使用する場合は、仮想スイッチを使用してください。レイヤ 2 スイッチは、作業者が時間の大半をローカル セグメントで費やす場合には特に有効です。大規模な展開環境（たとえば、ブロードキャスト トラフィック、VoIP、または複数のネットワークが含まれる環境）では、展開環境を複数のネットワーク セグメントに分割して、それぞれのセグメントで仮想スイッチを使用できます。

同じ管理対象デバイスに複数の仮想スイッチを展開すると、各ネットワークのニーズに応じた異なるレベルのセキュリティ レベルを維持できます。

図 6-2　　管理対象デバイス上の仮想スイッチ



この例では、管理対象デバイスが、2 つの異なるネットワーク（172.16.1.0/20 および 192.168.1.0/24）からのトラフィックをモニタしています。両方のネットワークを同じ管理対象デバイスでモニタしていますが、仮想スイッチは、同じネットワーク上にあるコンピュータまたはサーバにのみトラフィックを渡します。トラフィックは、172.16.1.0/24 仮想スイッチを介してコンピュータ A からコンピュータ B に（青色の線で示されているように）渡し、同じ仮想スイッチを介してコンピュータ B からコンピュータ A に（緑色の線で示されているように）渡すことができます。同様に、192.168.1.0/24 仮想スイッチを介してファイル サーバおよび Web サーバ間でトラフィックが受け渡されます（赤色の線とオレンジ色の線）。ただし、コンピュータと Web サーバまたはファイル サーバとの間でトラフィックを受け渡すことはできません。これらのコンピュータとサーバは、それぞれ異なる仮想スイッチ上にあるためです。

スイッチド インターフェイスおよび仮想スイッチの設定の詳細については、『*Firepower Management Center Configuration Guide*』の「*Setting Up Virtual Switches*」を参照してください。

仮想ルータを使用した展開

管理対象デバイス上に*仮想ルータ*を作成すると、複数のネットワーク間でトラフィックをルーティングすることや、プライベート ネットワークをパブリック ネットワーク（インターネットなど）に接続することが可能になります。仮想ルータは、2 つのルーテッド インターフェイスを接続し、宛先アドレスに応じて、展開環境でのレイヤ 3 パケット転送を決定します。オプションで、仮想ルータの厳密な TCP 適用を有効にすることができます。ルーテッド インターフェイスの詳細については、ルーテッド インターフェイス（6-4 ページ）を参照してください。仮想ルータは、ゲートウェイ VPN と併せて使用する必要があります。詳細については、ゲートウェイ VPN の展開（6-11 ページ）を参照してください。

仮想ルータには、同じブロードキャスト ドメイン内の 1 つ以上の個々のデバイスの物理インターフェイスまたは論理ルーテッド インターフェイス設定を含めることができます。物理インターフェイスで受信した VLAN タグ付きのトラフィックは、各論理インターフェイスにその特定のタグが関連付けられていなければ処理されません。トラフィックをルーティングするには、論理ルーテッド インターフェイスを仮想ルータに割り当てる必要があります。

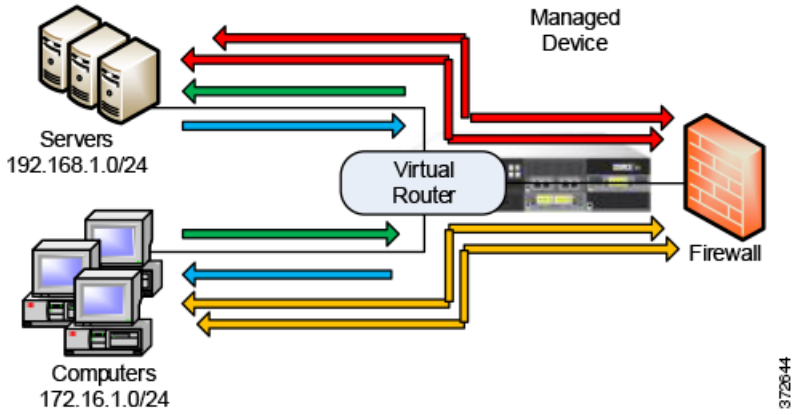
仮想ルータを設定するには、物理または論理設定のいずれかを使用したルーテッド インターフェイスを設定します。タグなし VLAN トラフィックを処理する、物理ルーテッド インターフェイスを設定できます。指定の VLAN タグ付きトラフィックを処理する、論理ルーテッド インターフェイスを作成することもできます。システムは、ルーテッド インターフェイスが待機していない、外部物理インターフェイスで受信したすべてのトラフィックをドロップします。システムが VLAN タグなしのパケットを受信した場合、該当するポートに物理ルーテッド インターフェイスが設定されていなければ、パケットはドロップされます。システムが VLAN タグ付きのパケットを受信した場合、論理ルーテッド インターフェイスが設定されていなければ、同じくパケットはドロップされます。

仮想ルータには、スケーラビリティに関する利点があります。物理ルータによって、接続可能なネットワークの数が制限される場合、同じ管理対象デバイスに複数の仮想ルータを設定できます。同じデバイスに複数のルータを配置すると、展開環境の物理的な複雑さが軽減され、1 台のデバイスから複数のルータをモニタおよび管理することが可能になります。

展開環境内の複数のネットワーク間でトラフィックを転送する場合、あるいはプライベート ネットワークをパブリック ネットワークに接続する場合は、レイヤ 3 物理ルータを使用する代わりに仮想ルータを使用してください。多数のネットワークまたはネットワーク セグメントにそれぞれ異なるセキュリティ要件が伴う大規模な展開環境では、仮想ルータが特に有効です。

管理対象デバイスに仮想ルータを展開すると、1 台のアプライアンスで複数のネットワークを相互接続することや、複数のネットワークをインターネットに接続することが可能になります。

図 6-3　　管理対象デバイスの仮想ルータ



この例では、管理対象デバイスに含まれる仮想ルータによって、ネットワーク 172.16.1.0/20 上のコンピュータ間、およびネットワーク 192.168.1.0/24 上のサーバ間でトラフィックを受け渡すことができます（青色と緑色の線）。仮想ルータの 3 番目のインターフェイスでは、各ネットワークとファイアウォールとの間でトラフィックを受け渡すことができます（赤色とオレンジ色の線）。

詳細については、『*Firepower Management Center Configuration Guide*』の「Setting Up Virtual Routers」を参照してください。

ハイブリッド インターフェイスを使用した展開

管理対象デバイス上に*ハイブリッド インターフェイス*を作成すると、仮想スイッチと仮想ルータを使用して、レイヤ 2 ネットワークとレイヤ 3 ネットワークの間でトラフィックをルーティングできます。これにより、1 つのインターフェイスで、スイッチ上のローカル トラフィックのルーティングと、外部ネットワークとの間でのトラフィックのルーティングの両方に対応できます。最適な結果を得るためには、インターフェイスにポリシー ベースの NAT を設定して、ハイブリッド インターフェイスでネットワーク アドレス変換を行えるようにしてください。ポリシー ベースの NAT を使用した展開（6-12 ページ）を参照してください。

ハイブリッド インターフェイスには、1 つ以上のスイッチド インターフェイスと 1 つ以上のルーテッド インターフェイスを含める必要があります。一般的な展開環境は、ローカル ネットワーク上でトラフィックを渡す仮想スイッチとして設定されたスイッチド インターフェイスと、プライベート ネットワークまたはパブリック ネットワークにトラフィックをルーティングする仮想ルータとして設定されたルーテッド インターフェイスの 2 つで構成されます。

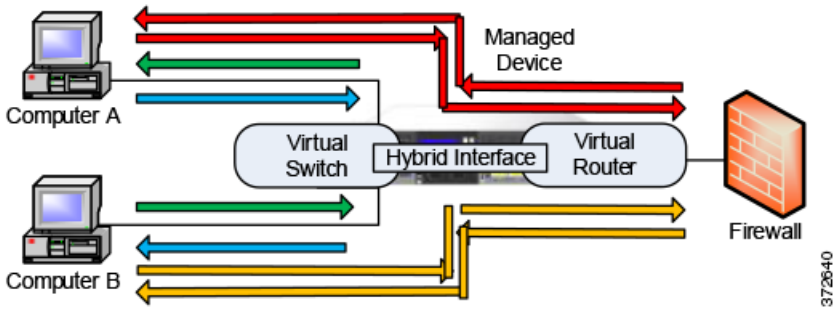
ハイブリッド インターフェイスを作成するには、まず、仮想スイッチと仮想ルータを設定し、それらの仮想スイッチと仮想ルータをハイブリッド インターフェイスに追加します。仮想スイッチと仮想ルータの両方に関連付けられていないハイブリッド インターフェイスは、ルーティングに使用できません。したがって、トラフィックを生成することも、トラフィックに応答することもしません。

ハイブリッド インターフェイスには、簡潔さとスケーラビリティに関する利点があります。レイヤ 2 とレイヤ 3 両方のトラフィック ルーティング機能が結合された単一のハイブリッド インターフェイスを使用することで、展開環境内の物理アプライアンスの数が減り、トラフィックを 1 つの管理インターフェイスで管理できます。

レイヤ 2 とレイヤ 3 の両方のルーティング機能が必要な場合は、ハイブリッド インターフェイスを使用してください。この展開は、スペースやリソースが限られた小規模な展開環境の小さなセグメントに最適です。

ハイブリッド インターフェイスを展開すると、トラフィックをローカル ネットワークから外部またはパブリック ネットワーク（インターネットなど）に渡すことができると共に、ハイブリッド インターフェイスでの仮想スイッチと仮想ルータに関する個別のセキュリティ上の考慮事項に対応することができます。

図 6-4　　管理対象デバイス上のハイブリッド インターフェイス



この例では、コンピュータ A とコンピュータ B が同じネットワーク上にあり、管理対象デバイス上に設定されたレイヤ 2 仮想スイッチを使用して通信しています（青色と緑色の線）。管理対象デバイス上に設定された仮想ルータは、ファイアウォールへのレイヤ 3 アクセスを提供します。ハイブリッド インターフェイスには仮想スイッチと仮想ルータのレイヤ 2 およびレイヤ 3 機能が統合されているため、各コンピュータからのトラフィックをハイブリッド インターフェイスを介してファイアウォールに渡すことができます（赤色とオレンジ色の線）。

詳細については、『*Firepower Management Center Configuration Guide*』の「Setting Up Hybrid Interfaces」を参照してください。

ゲートウェイ VPN の展開

ライセンス：VPN

ローカル ゲートウェイとリモート ゲートウェイの間のセキュア トンネルを確立するには、*ゲートウェイ バーチャル プライベート ネットワーク*（ゲートウェイ VPN）接続を作成します。ゲートウェイ間のセキュア トンネルにより、ゲートウェイの間での通信が保護されます。

Cisco 管理対象デバイスの仮想ルータからリモート デバイスや他のサードパーティ VPN エンドポイントへのセキュア VPN トンネルを作成するには、インターネット プロトコル セキュリティ（IPSec）プロトコル スイートを使用して Firepower システムを設定します。VPN 接続が確立されると、ローカル ゲートウェイの背後にあるホストは、セキュア VPN トンネルを介して、リモート ゲートウェイの背後にあるホストに接続できるようになります。VPN エンドポイントは、Internet Key Exchange（IKE）バージョン 1 またはバージョン 2 のプロトコルを使用して相互認証することで、トンネルのセキュリティ アソシエーションを確立します。システムは、IPsec 認証ヘッダー（AH）モードまたは IPsec Encapsulating Security Payload（ESP）モードのいずれかで稼動します。AH と ESP は両方とも認証を提供します。ESP は、さらに暗号化も提供します。

ゲートウェイ VPN は、ポイントツーポイント展開、スター型展開、またはメッシュ型展開で使用できます。

- ポイントツーポイント展開では、2 つのエンドポイントを直接 1 対 1 の関係で相互接続します。両方のエンドポイントがピア デバイスとして設定され、いずれのデバイスもセキュア接続を開始できます。少なくともどちらかのデバイスが、VPN 対応の管理対象デバイスである必要があります。

  リモートに位置するホストがパブリック ネットワークを使用してネットワーク内のホストに接続する場合は、ポイントツーポイント展開を使用してネットワークのセキュリティを確保してください。

- スター型展開では、ハブと複数のリモート エンドポイント（リーフ ノード）間のセキュア接続を確立します。ハブ ノードと個々のリーフ ノードとの間の接続が、それぞれ別個の VPN トンネルとなります。通常、ハブ ノードとなるのは、本社に配置される VPN 対応の管理対象デバイスです。リーフ ノードは支社に配置します。トラフィックの大部分は、これらのリーフ ノードから開始されます。

  インターネットまたは他のサードパーティ ネットワークでセキュア接続を使用して組織の本社と各支社を接続するには、スター型展開を使用して、従業員全員が、組織のネットワークに管理された形でアクセスするようにしてください。

- メッシュ型展開では、VPN トンネルを使用してすべてのエンドポイントを同時に接続します。これにより、あるエンドポイントで障害が発生しても、残りのエンドポイントの相互通信は維持されるという冗長性が提供されます。

  1 つ以上の VPN トンネルで障害が発生しても、トラフィック フローが維持されるようにするには、メッシュ型展開を使用して、分散された場所に位置する一連の支社を接続してください、冗長性のレベルは、この設定で展開する VPN 対応の管理対象デバイスの数によって決まります。

ゲートウェイ VPN の設定の詳細については、『*Firepower Management Center Configuration Guide*』の「Gateway VPN」を参照してください。

ポリシー ベースの NAT を使用した展開

ポリシー ベースのネットワーク アドレス変換（NAT）を使用してポリシーを定義し、NAT の実行方法を指定できます。ポリシーのターゲットは、単一のインターフェイス、1 つ以上のデバイス、またはネットワーク全体に設定できます。

静的（1 対 1）変換または動的（1 対多）変換を設定できます。動的変換は順序に依存することに注意してください、つまり、最初に一致するルールが適用されるまで、ルールが順に検索されます。

一般に、ポリシー ベースの NAT は以下の展開で機能します。

- プライベート ネットワーク アドレスを非公開にする展開。

  プライベート ネットワークからパブリック ネットワークにアクセスする際に、NAT がプライベート ネットワーク アドレスをパブリック ネットワーク アドレスに変換します。特定のプライベート ネットワーク アドレスは、パブリック ネットワークから隠されます。

- プライベート ネットワーク サービスへのアクセスを許可する展開。

  パブリック ネットワークがプライベート ネットワークにアクセスする際に、NAT がパブリック アドレスをプライベート ネットワーク アドレスに変換します。これにより、パブリック ネットワークは、特定のプライベート ネットワーク アドレスにアクセスできます。

- 複数のプライベート ネットワーク間でトラフィックをリダイレクトする展開。

  プライベート ネットワーク上のサーバが接続先のプライベート ネットワーク上のサーバにアクセスする際に、プライベート アドレスの重複がなく、これらのプライベート ネットワーク間でのトラフィック フローが可能になるように、NAT が 2 つのプライベート ネットワーク間でプライベート アドレスを変換します。

ポリシー ベースの NAT を使用すると、ハードウェアを追加する必要がなくなり、侵入検知または防御システムの設定と NAT が 1 つのユーザ インターフェイスに統合されます。詳細については、『*Firepower Management Center Configuration Guide*』の「Using NAT Policies」を参照してください。

アクセス制御による展開

アクセス制御は、ネットワークへの出入りあるいはネットワーク内での移動を許可するトラフィックを指定、検査、および記録するために使用できる、ポリシー ベースの機能です。ここでは、アクセス制御が展開でどのように機能するのかを説明します。この機能の詳細については、『*Firepower Management Center Configuration Guide*』を参照してください。

アクセス制御ポリシーは、ネットワーク上のトラフィックをシステムがどのように処理するかを決定します。ポリシーにアクセス制御ルールを追加することで、ネットワーク トラフィックの処理方法やロギング方法をよりきめ細かく制御できます。

アクセス制御ルールが含まれないアクセス制御ポリシーは、以下のいずれかのデフォルト アクションを使用してトラフィックを処理します。

- すべてのトラフィックをブロックして、ネットワークに入れない
- すべてのトラフィックを信頼してネットワークに入ることを許可し、検査は行わない
- すべてのトラフィックがネットワークに入ることを許可し、ネットワーク ディスカバリ ポリシーのみを使用してトラフィックを検査する
- すべてのトラフィックがネットワークに入ることを許可し、侵入ポリシーとネットワーク ディスカバリ ポリシーを使用してトラフィックを検査する

アクセス制御ルールはさらに、ターゲット デバイスでのトラフィックの処理方法を定義します。その方法には、単純な IP アドレスのマッチングから、異なる複数のユーザ、アプリケーション、ポート、URL が関与する複雑なシナリオまでがあります。それぞれのルールについて、ユーザはルールのアクション、つまり侵入またはファイル ポリシーと一致するトラフィックを信頼、監視、ブロック、または検査するかどうかを指定します。

アクセス制御では、セキュリティ インテリジェンスのデータに基づいてトラフィックをフィルタリングできます。セキュリティ インテリジェンスとは、アクセス制御ポリシーごとに、送信元 IP アドレスまたは宛先 IP アドレスに基づいて、ネットワークを移動できるトラフィックを指定するための機能です。この機能では、許可されない IP アドレスのブラックリストを作成できます。ブラックリストに含まれる IP アドレスからのトラフィックはブロックされ、検査されません。

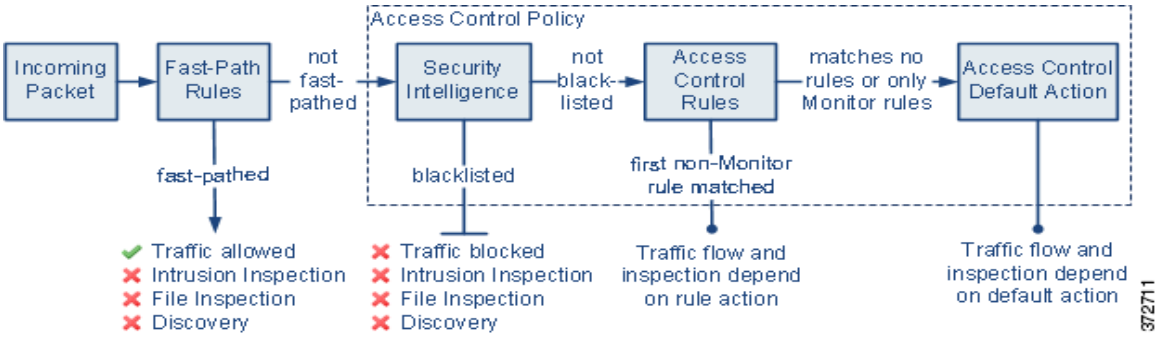
展開の例に、共通のネットワーク セグメントが示されています。各場所に展開された管理対象デバイスは、それぞれに異なる目的を果たします。ここでは、配置場所に関する一般的な推奨事項を説明します。

- ファイアウォールの内側（6-14 ページ）では、ファイアウォールを通過するトラフィックに対してアクセス制御がどのように機能するかを説明しています。
- DMZ（6-15 ページ）では、DMZ 内のアクセス制御がネットワーク外部と接触するサーバを保護する仕組みについて説明しています。
- 内部ネットワーク（6-16 ページ）では、アクセス制御が内部ネットワークを侵入や不測の攻撃から保護する仕組みについて説明しています。
- コア ネットワーク（6-16 ページ）では、厳密なルールを使用したアクセス制御ポリシーで重要な資産を保護する方法を説明しています。
- リモート ネットワークまたはモバイル ネットワーク（6-17 ページ）では、アクセス制御ポリシーでトラフィックをモニタし、リモートの場所やモバイル デバイスでのトラフィックからネットワークを保護する方法を説明しています。

ファイアウォールの内側

ファイアウォールの内側に配置された管理対象デバイスは、ファイアウォールによって許可された着信トラフィック、あるいは誤った設定が原因でファイアウォールを通過したトラフィックをモニタします。共通のネットワーク セグメントには、DMZ、内部ネットワーク、コア ネットワーク、モバイル アクセス ネットワーク、リモート ネットワークがあります。

以下の図に、Firepower システムを介したトラフィック フローと、トラフィックに対して行われるタイプのインスペクションの詳細を示します。高速パスで処理されたトラフィックやブラックリストに登録されたトラフィックに対しては、インスペクションが行われないことに注意してください。アクセス制御ルールまたはデフォルト アクションで処理されたトラフィックの場合、そのフローとインスペクションは、ルール アクションによって異なります。簡潔にするために、この図にはルール アクションを示していませんが、信頼されたトラフィックまたはブロックされたトラフィックに対しては、インスペクションは一切行われません。また、ファイル インスペクションは、デフォルト アクションでサポートされていません。



着信パケットは、最初に高速パス ルールについてチェックされます。一致が見つかった場合、トラフィックは高速パスで処理されます。一致しない場合、セキュリティ インテリジェンス ベースのフィルタリングにより、パケットがブラックリストに登録されているかどうかが判別されます。登録されていない場合、アクセス制御ルールが適用されます。パケットがルールの条件を満たす場合、そのトラフィック フローとインスペクションは、ルール アクションによって異なります。パケットに一致するルールがない場合、そのトラフィック フローとインスペクションは、デフォルトのポリシー アクションによって異なります。(モニタ ルールの場合は例外です。この場合は、トラフィックが引き続き評価されます)。各アクセス コントロール ポリシーのデフォルト アクションは、高速パス処理またはブラックリスト登録が行われなかったトラフィック、あるいはモニタ ルール以外のルールと一致したトラフィックを管理します。高速パスが使用できるのは、8000 シリーズデバイスのみです。

アクセス制御ルールを作成することで、ネットワーク トラフィックの処理方法やロギング方法をよりきめ細かく制御できます。ルールごとに、特定の基準を満たすトラフィックに適用するアクション(信頼、モニタ、ブロック、またはインスペクション)を指定します。

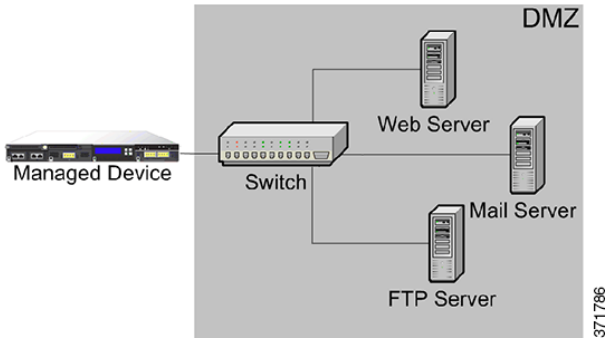
DMZ

DMZ 内には、ネットワーク外部と接触するサーバ(Web、FTP、DNS、メールなど)があり、DMZ が内部ネットワークでメール中継や Web プロキシなどのサービスをユーザに提供する場合もあります。

DMZ に保管されるコンテンツは静的であり、変更の計画および実行は、明確なコミュニケーションと事前予告によって行われます。このセグメント内での攻撃は、一般に着信トラフィックによって行われますが、DMZ 内のサーバーでは計画された変更しか行われないことから、すぐに明らかになります。このセグメントに効果的なアクセス制御ポリシーは、サービスに対するアクセスを厳密に制御し、あらゆる新規ネットワーク イベントを検索するポリシーです。

DMZ 内のサーバには、DMZ がネットワークを介して問い合わせできるデータベースを含めることができます。DMZ と同じく、データベースに対しても予定外の変更は行われないはずですが、データベースのコンテンツはより機密性が高いため、Web サイトや他の DMZ サービスより保護を強化する必要があります。DMZ のアクセス制御ポリシーに加え、強力な侵入防御ポリシーを使用することが、効果的な戦略となります。

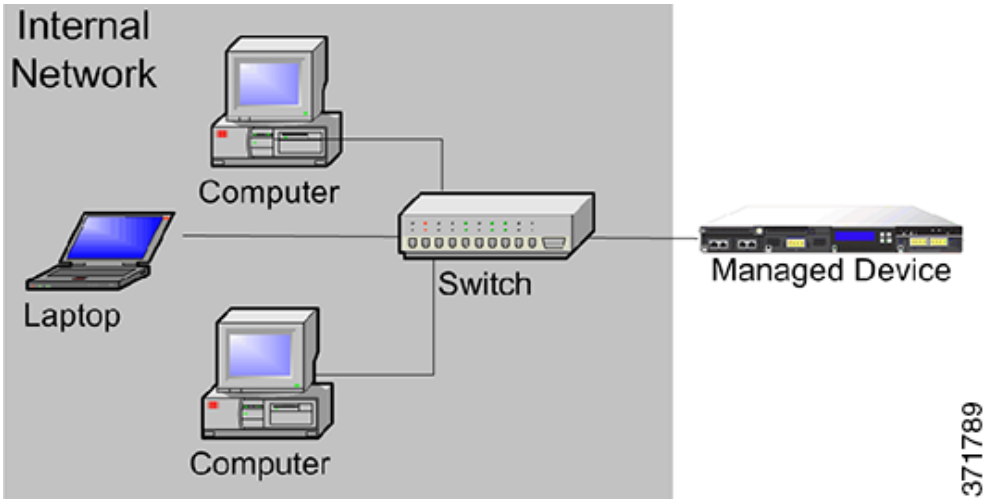
このセグメントに展開された管理対象デバイスでは、DMZ 内のセキュリティが侵害されたサーバから開始されてインターネットに送信された攻撃を検出できます。ネットワーク ディスカバリを使用してネットワーク トラフィックをモニタすることで、DMZ 内のサーバのセキュリティ侵害の兆候として、これらの公開されたサーバの変更(たとえば、予期しないサービスが突然出現したことなど)をモニタすることができます。



内部ネットワーク

不正な攻撃が、内部ネットワーク上のコンピュータから開始される可能性もあります。これらの攻撃は、作為的であることも（たとえば、不明なコンピュータがネットワーク上に突然現れるなど）、予想外の感染であることもあります（たとえば、オフサイトで感染した職場のラップトップがネットワークに接続されて、ウイルスが拡散するなど）。内部ネットワークでのリスクは、発信トラフィックで生じる場合もあります（たとえば、コンピュータが疑わしい外部 IP アドレスに情報を送信するなど）。

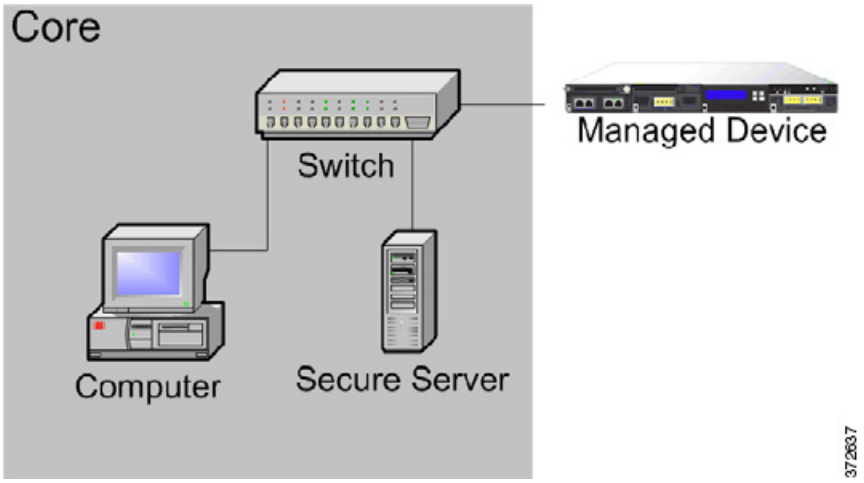
この動的なネットワークには、発信トラフィックに加え、すべての内部トラフィックに対して厳密なアクセス制御ポリシーが必要になります。ユーザとアプリケーションの間のトラフィックを厳密に制御するアクセス制御ルールを追加してください。



コア ネットワーク

コア資産とは、ビジネスの成功に不可欠な資産であり、いかなる代償を払っても保護しなければなりません。コア資産はビジネスの特性によって異なりますが、一般的なコア資産としては、財務管理センターや知的財産のリポジトリが挙げられます。コア資産のセキュリティが侵害されると、ビジネスが壊滅的損害を被る恐れがあります。

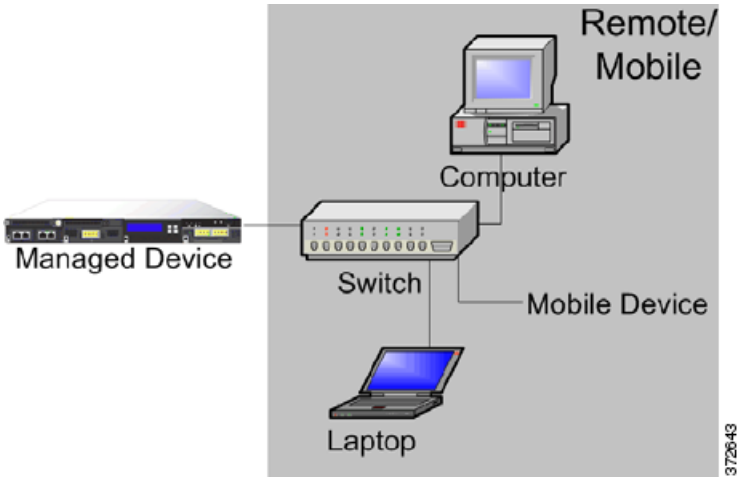
ビジネスが機能するためには、このセグメントをすぐに利用できるようにする必要がありますが、それと同時に厳重に制限および制御しなければなりません。アクセス制御によって、リスクの高いネットワーク セグメント（リモート ネットワークやモバイル デバイスなど）からはコア資産にアクセスできないようにする必要があります。このセグメントには常に、ユーザとアプリケーションによるアクセスに対する厳密なルールを含む、最も積極的なアクセス制御ルールを適用してください。



リモート ネットワークまたはモバイル ネットワーク

オフサイトに位置するリモート ネットワークでは、多くの場合、仮想プライベート ネットワーク（VPN）を使用してプライマリ ネットワークへのアクセスを提供します。モバイル デバイスやパーソナル デバイスをビジネスで使用することが次第に一般的になってきています（たとえば、「スマートフォン」を使用して会社の電子メールにアクセスするなど）。

これらのネットワークは、急速かつ継続的に変化する、極めて動的な環境です。専用のモバイル ネットワークまたはリモート ネットワークに管理対象デバイスを展開すると、不明な外部ソースとの間で送受信されるトラフィックをモニタおよび管理する、厳密なアクセス制御ポリシーを作成できます。コア リソースに対するユーザ、ネットワーク、アプリケーションのアクセスをポリシーによって厳しく制限することで、リスクを軽減できます。



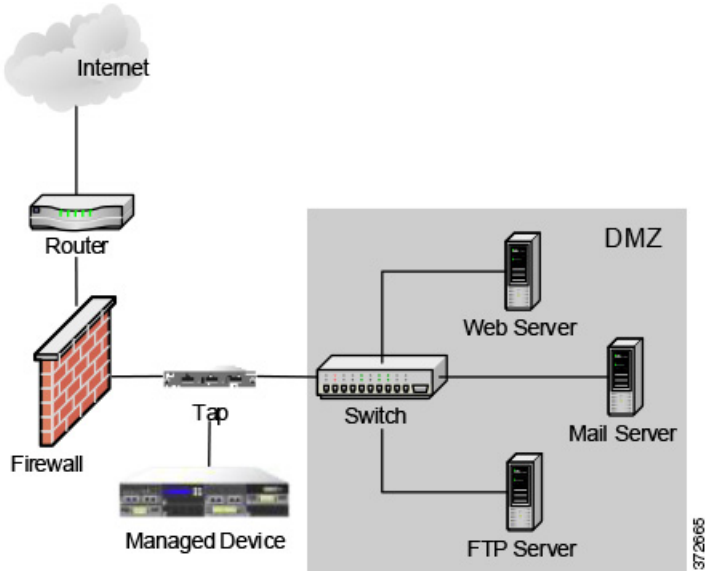
管理対象デバイスでの複数のセンシング インターフェイスの使用

管理対象デバイスのネットワーク モジュールには、複数のセンシング インターフェイスが用意されています。以下の目的で、管理対象デバイスにおいて複数のセンシング インターフェイスを使用できます。

- ネットワーク タップからの個別の接続を再結合する
- 複数の異なるネットワークからトラフィックを捕捉して評価する
- 仮想ルータとして機能させる
- 仮想スイッチとして機能させる

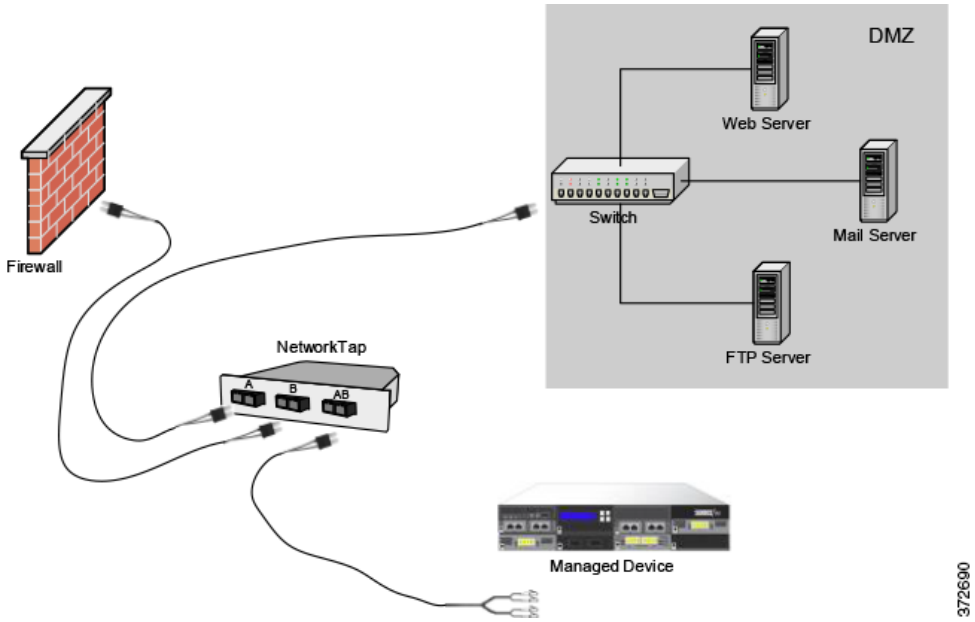
コメント　各センシング インターフェイスは、デバイスの評価対象となる完全なスループットを受信できますが、管理対象デバイスでの合計トラフィックが帯域幅の評価を超えるとパケットの消失が発生します。

ネットワーク タップのある管理対象デバイス上に複数のセンシング インターフェイスを展開することは、簡単なプロセスです。以下の図に、トラフィック量の多いネットワーク セグメントに設置されたネットワーク タップを示します。

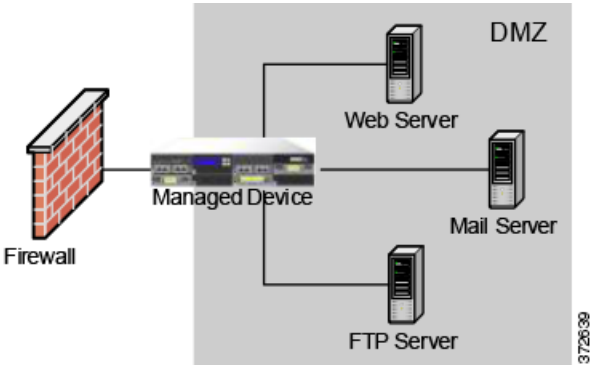


このシナリオでは、タップが別個のセンシング インターフェイスを介して着信および発信トラフィックを伝送します。管理対象デバイス上で複数のセンシング インターフェイス アダプタ カードをタップに接続すると、管理対象デバイスはトラフィックを単一のデータ ストリームに組み合わせます。これにより、トラフィックが分析可能になります。

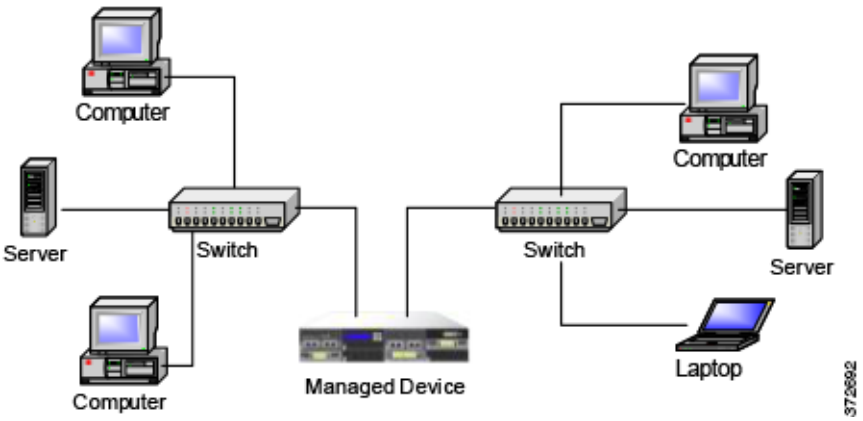
以下の図に示すようなギガビット光タップでは、管理対象デバイス上にある 2 組のセンシング インターフェイスは、どちらもタップのコネクタによって使用されることに注意してください。



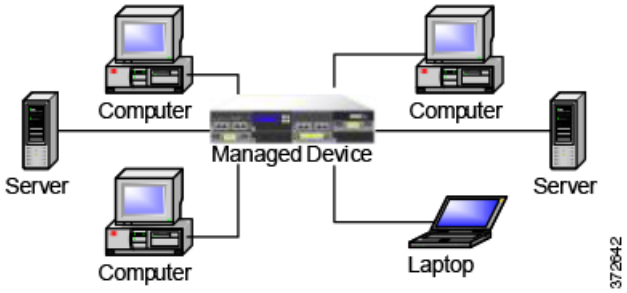
展開環境のタップとスイッチの両方を、仮想スイッチで置き換えることができます。タップを仮想スイッチに置き換えると、タップ パケット配信が保証されなくなることに注意してください。



個別のネットワークからデータを捕捉するインターフェイスを作成することもできます。次の図は、デュアル センシング インターフェイスのアダプタがある単一のデバイスと、2 つのネットワークに接続された 2 つのインターフェイスを示しています。



1 台のデバイスで両方のネットワーク セグメントをモニタできるだけでなく、デバイスの仮想スイッチ機能を使用して、展開環境内の両方のスイッチを置き換えることもできます。



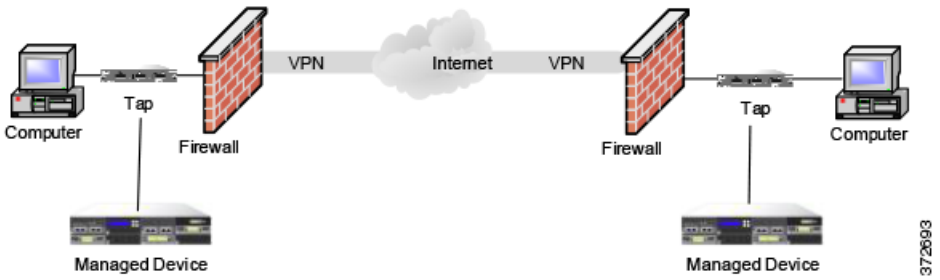
複雑なネットワーク展開

企業のネットワークには、例えば VPN を使用したリモート アクセスが必要になったり、ビジネス パートナーやバンキング接続などの複数のエントリ ポイントを使用したりする場合があります。

VPN の統合

バーチャル プライベート ネットワーク（VPN）では、IP トンネリング手法を使用して、インターネットを介したローカル ネットワークとリモート ユーザ間のセキュリティを提供します。一般に、VPN ソリューションでは IP パケットのデータ ペイロードを暗号化します。他のパケットと同様に、パブリック ネットワークでパケットを送信できるようにするために、IP ヘッダーは暗号化されません。パケットが宛先ネットワークに到達すると、ペイロードが暗号解除されて、パケットが適切なホストに送信されます。

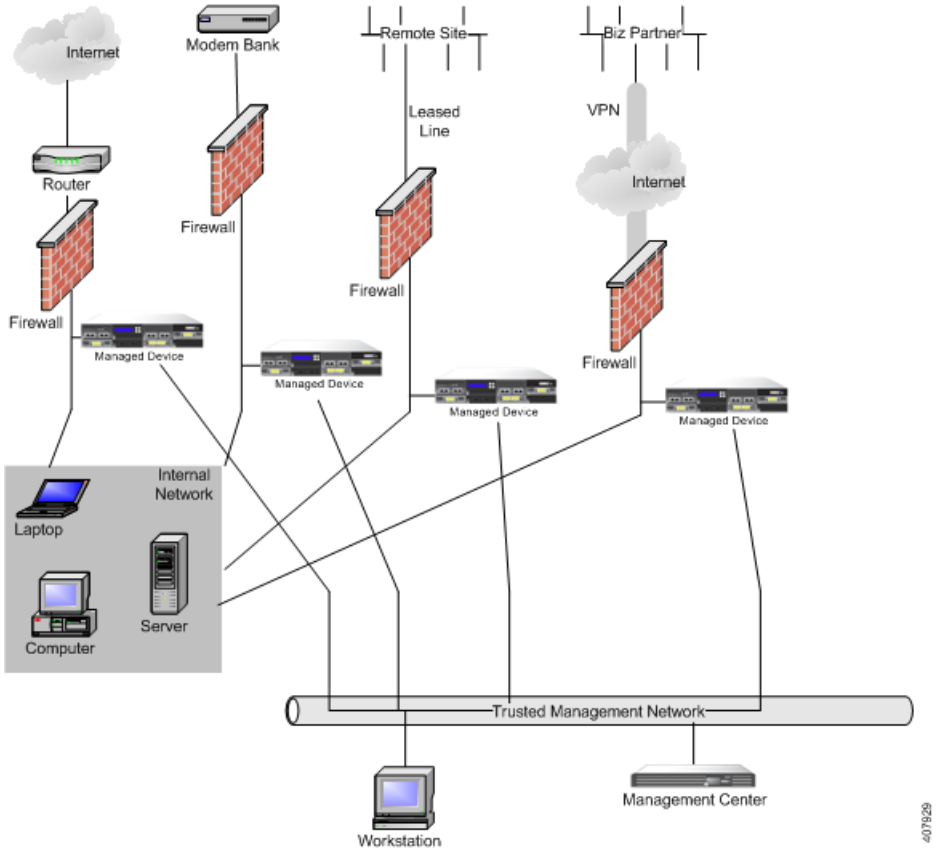
ネットワーク アプライアンスでは VPN パケットの暗号化されたペイロードを分析できないため、すべてのパケット情報にアクセスできるように、管理対象デバイスは VPN 接続の終端エンドポイント外部に配置します。以下の図に、管理対象デバイスを VPN に展開する方法を示します。



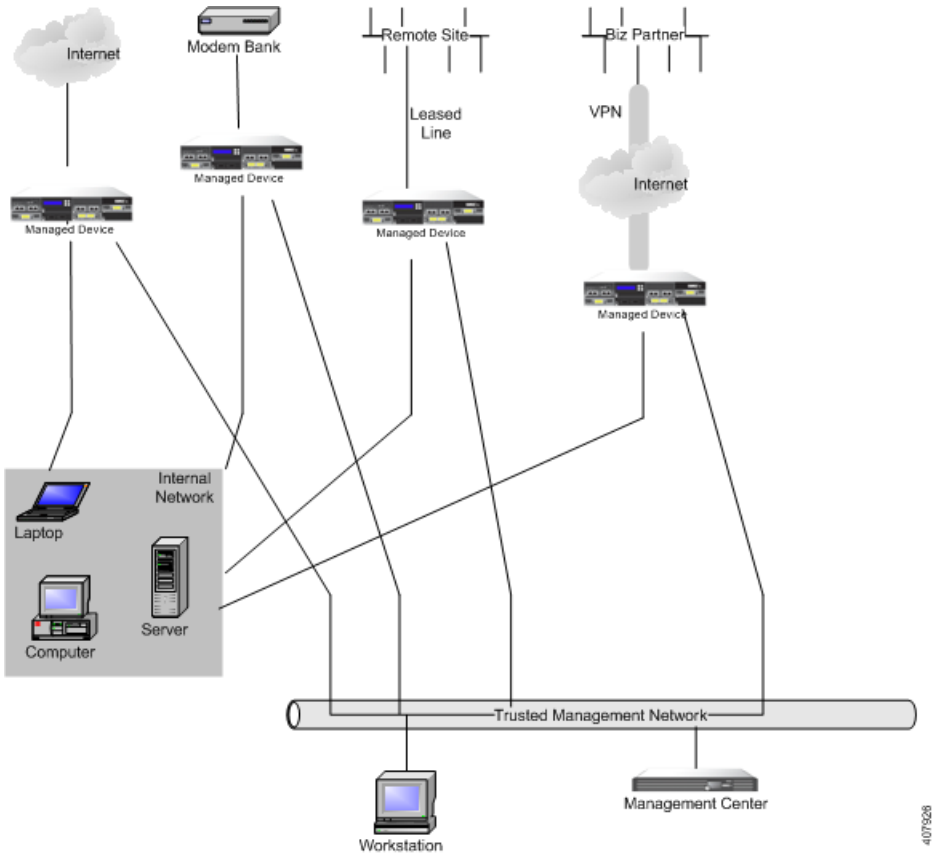
VPN 接続の一方の終端で、ファイアウォールまたはタップを管理対象デバイスに置き換えることができます。タップを管理対象デバイスに置き換えると、タップ パケット配信が保証されなくなることに注意してください。

他のエントリ ポイントでの侵入検知

多くのネットワークには、複数のアクセス ポイントが含まれます。単一の境界ルータでインターネットに接続する代わりに、一部の企業では、インターネット、モデム バンク、およびビジネス パートナー ネットワークへの直接リンクを組み合わせて使用しています。通常、管理対象デバイスを展開する場所は、ファイアウォールの近く（ファイアウォール内部または外部、あるいはその両方）の、ビジネス データの整合性および機密性にとって重要なネットワーク セグメント上でなければなりません。以下の図に、複数のエントリ ポイントがある複雑なネットワーク上の重要な場所に管理対象デバイスを設置する方法を示します。

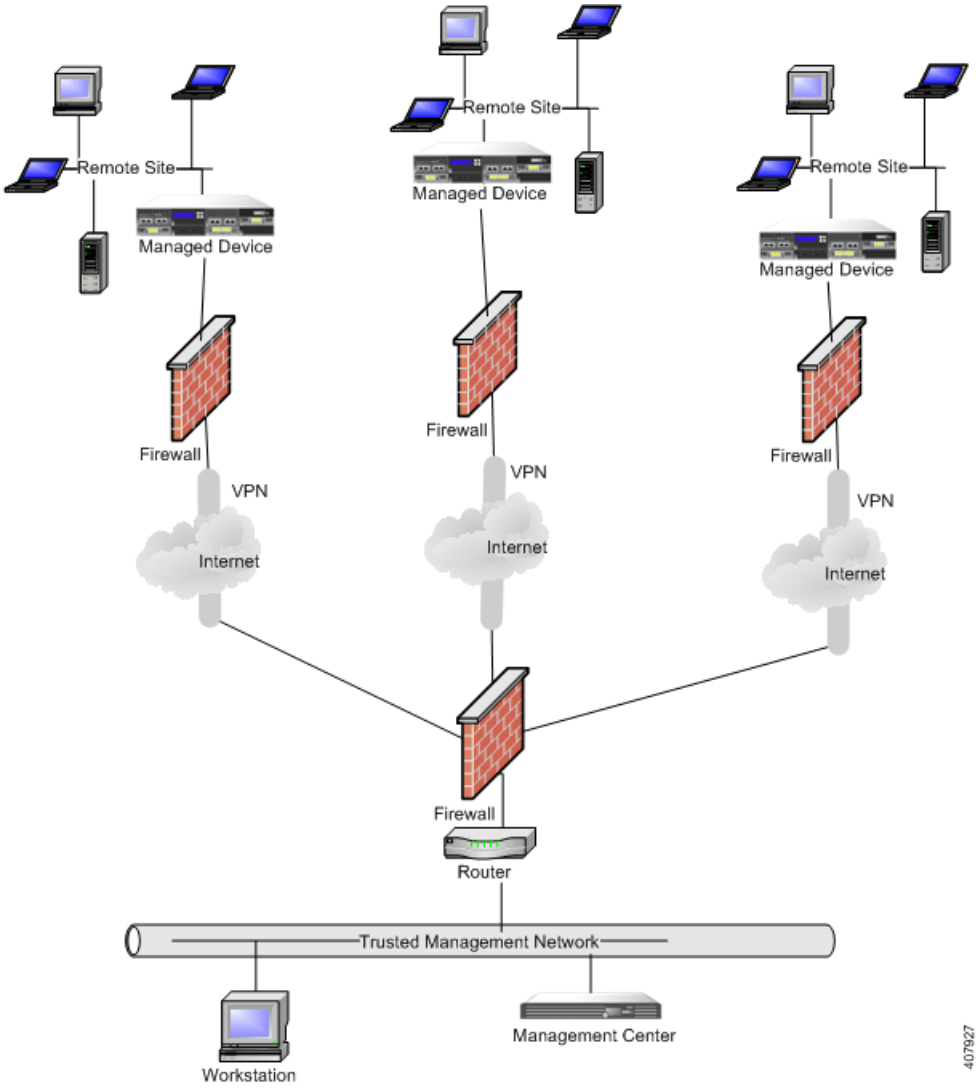


ファイアウォールとルータは、そのネットワーク セグメント上に展開された管理対象デバイスに置き換えることができます。

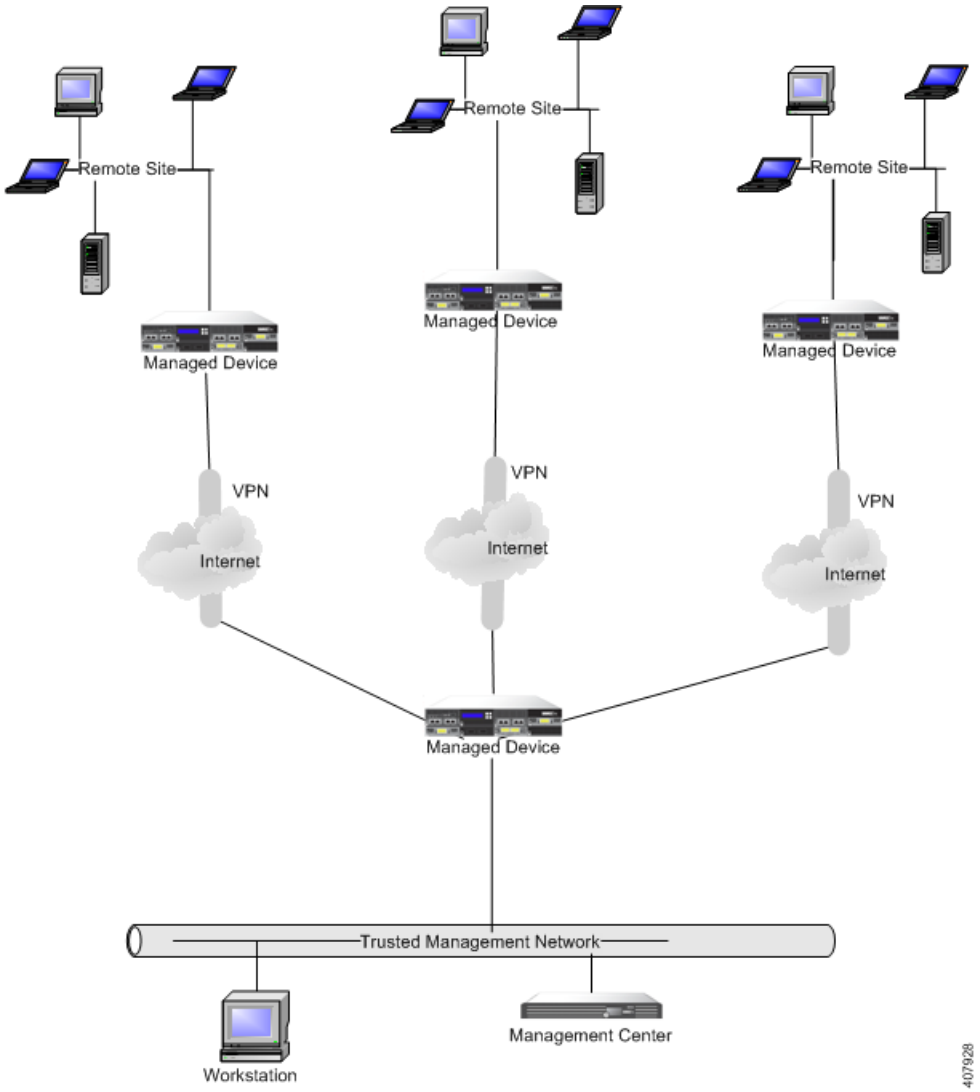


マルチサイト環境での展開

多くの組織では、地理的に分散している企業全体で侵入検知を展開し、1 か所からすべてのデータを分析することを望んでいます。この形態をサポートするために、Firepower システムで提供している Firepower Management Center は、組織のさまざまな場所に展開されている管理対象デバイスからのイベントを集約して相互に関連付けます。同じ地理的な場所で同じネットワークに複数の管理対象デバイスと Firepower Management Center を展開する場合とは異なり、分散した地理的な場所に管理対象デバイスを展開する場合には、管理対象デバイスおよびデータ ストリームのセキュリティが確保されるように注意しなければなりません。データを保護するには、管理対象デバイスと Firepower Management Center を、保護されていないネットワークから隔離する必要があります。これは、VPN を介した管理対象デバイスからのデータ ストリームを送信することによって、または次の図のように他のセキュアなトンネリング プロトコルによって実行できます。



ファイアウォールとルータは、各ネットワーク セグメントに展開された管理対象デバイスに置き換えることができます。



複雑なネットワーク内にある複数の管理インターフェイスの統合

任意の展開内の複数の管理インターフェイスを設定して、さまざまなネットワークを監視しており、同じ Firepower Management Center によって管理されるデバイスからトラフィックを分離できます。複数の管理インターフェイスを使用して、固有の IP アドレス（IPv4 または IPv6）を持つ管理インターフェイスを Firepower Management Center に追加し、その管理インターフェイスから管理対象のデバイスを含むネットワークへのルートを作成できます。新しい管理インターフェイスにデバイスを登録すると、そのデバイスのトラフィックは、Firepower Management Center のデフォルト管理インターフェイスに登録されたデバイスのトラフィックから分離されます。

ヒント　デバイスを、デフォルト（eth0）の管理インターフェイス以外の管理インターフェイスの静的 IP アドレスに登録する必要があります。DHCP は、デフォルトの管理インターフェイスだけでサポートされています。

トラフィック チャネルのために別個の管理インターフェイスを使用する場合を除いて、複数の管理インターフェイスが NAT 環境でサポートされます。詳細については、「管理ネットワークでの展開（5-1 ページ）」を参照してください。Lights-Out Management は、追加の管理インターフェイスではなく、デフォルトの管理インターフェイスでのみサポートされることに注意してください。

Firepower Management Center をインストールした後に、Web インターフェイスを使用して、複数の管理インターフェイスを設定します。詳細については、『*Firepower Management Center Configuration Guide*』の「Configuring Appliance Settings」を参照してください。

複雑なネットワーク内での管理対象デバイスの統合

単純な複数セクタからなるネットワークよりも複雑なネットワーク トポロジに管理対象デバイスを展開できます。ここでは、プロキシ サーバ、NAT デバイス、および VPN が存在する環境に管理対象デバイスを展開する場合に、ネットワーク ディスカバリおよび脆弱性の分析に伴う問題に加え、Firepower Management Center を使用して複数の管理対象デバイスを管理する方法、およびマルチサイト環境での管理対象デバイスの展開と管理について説明します。

プロキシ サーバと NAT の統合

ネットワーク アドレス変換（NAT）デバイスまたはソフトウェアをファイアウォールの境界に導入することで、内部ホストの IP アドレスを効果的にファイアウォールの背後に隠すことができます。管理対象デバイスがこれらのデバイスまたはソフトウェアとモニタ対象のホストの間に位置していると、システムがプロキシまたは NAT デバイスの背後にあるデバイスを正しく識別できない可能性があります。この場合、Cisco では、ホストが正しく検出されるように、管理対象デバイスをプロキシまたは NAT で保護されたネットワーク セグメントの内部に配置することを推奨しています。

ロード バランシング方式の統合

一部のネットワーク環境では、「サーバ ファーム」構成を使用して、Web ホスティング、FTP ストレージ サイトといったサービスに対するネットワーク ロード バランシングを実行します。ロード バランシング環境では、それぞれに固有のオペレーティング システムを使用した複数のホストの間で IP アドレスが共有されます。この場合、システムはオペレーティング システムの変更を検出しても、信頼度の高い静的オペレーティング システム ID を提供できません。影響を受けるホストで使用している異なる種類のオペレーティング システムの数によっては、システムが大量のオペレーティング システム変更イベントを生成したり、信頼度の低い静的オペレーティング システム ID を提示したりすることがあります。

検出に関するその他の考慮事項

識別対象のホストの TCP/IP スタックが変更されている場合、システムはホスト オペレーティング システムを正確に識別できない可能性があります。TCP/IP スタックの変更は、パフォーマンスを向上するために行われる場合があります。たとえば、Internet Information Services（IIS）Web サーバを実行する Windows ホストの管理者には、パフォーマンスを向上させる方法として、大量のデータを受信できるように TCP ウィンドウ サイズを大きくすることが推奨されています。また、実際のオペレーティング システムを曖昧にして正確な識別を不可能にし、攻撃の対象にならないようにするために TCP/IP スタックが変更されることもあります。TCP/IP スタックの変更によって対処する同様のシナリオには、攻撃者がネットワークの予備調査スキャンを実行して、特定のオペレーティイング システムを使用するホストを識別した後、それらのホストを対象に、そのオペレーティング システムに固有の攻撃を仕掛けるというシナリオもあります。