VMware 向け Cisco Firepower 仮想アプライアンスの展開例

仮想デバイスと仮想 Cisco Firepower Management Center を使用して、仮想環境内にセキュリティ ソリューションを展開し、物理資産と仮想資産の両方の保護を向上させることができます。仮想デバイスと仮想 Cisco Firepower Management Center により、VMware プラットフォームでセキュリティ ソリューションを容易に実装できます。仮想デバイスはまた、リソースが制限されることがあるリモート サイトのデバイスの展開および管理を容易にします。

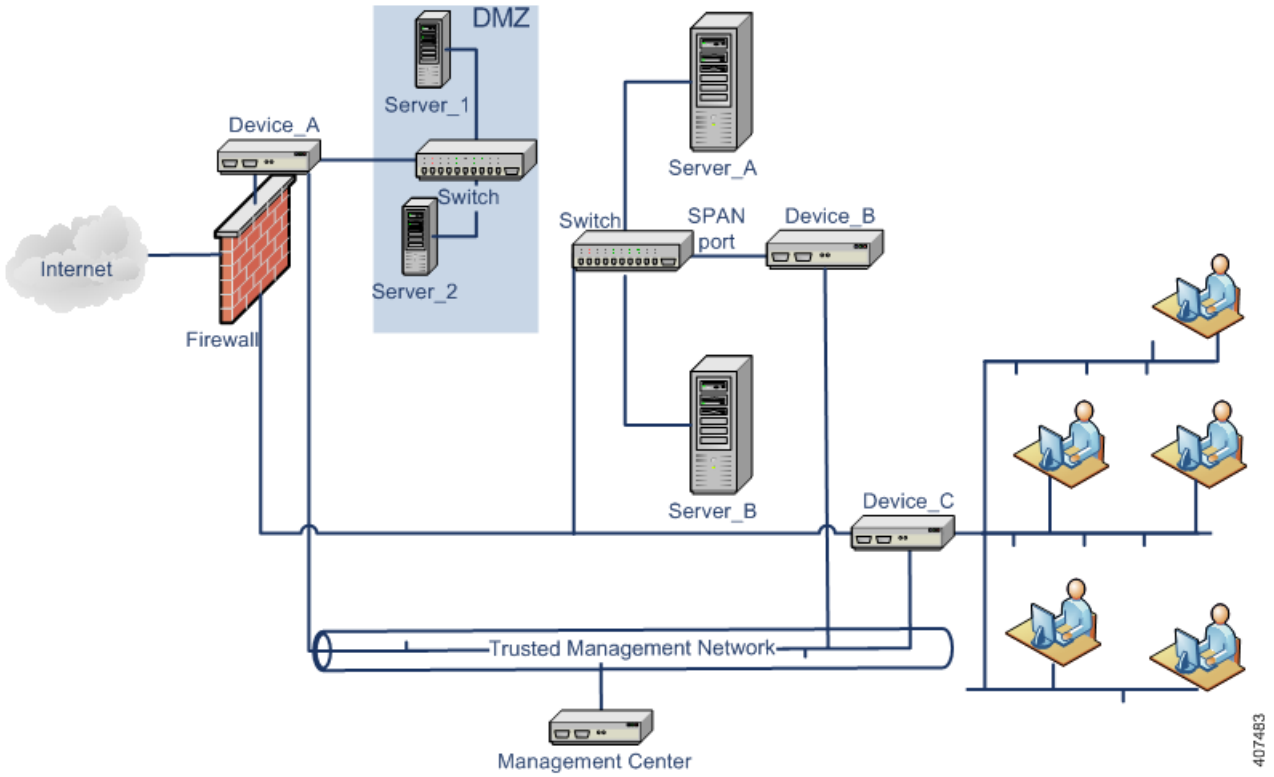
次の例では、物理デバイスまたは仮想デバイスを管理するために物理または仮想の Cisco Firepower Management Center を使用できます。IPv4 または IPv6 のネットワークに展開できます。また、Cisco Firepower Management Center に複数の管理インターフェイスを設定することにより、2 つの異なるネットワークを分離して監視したり、単一ネットワークの内部トラフィックとイベント トラフィックを分離することもできます。仮想デバイスは複数の管理インターフェイスをサポートしていないことに注意してください。

パフォーマンスを向上させるため、または 2 つの異なるネットワーク上のトラフィックを別個に管理するため、仮想 Cisco Firepower Management Center で 2 つ目の管理インターフェイスを設定できます。2 つ目の管理インターフェイスを 2 つ目のネットワーク上の管理対象デバイスに接続するように、追加のインターフェイスおよび追加の仮想スイッチを設定します。仮想アプライアンスに 2 つ目の管理インターフェイスを追加する方法については、VMware vSphere（http://vmware.com）を参照してください。複数の管理インターフェイスの詳細については、『*Firepower System Configuration Guide*』の「Managing Devices」を参照してください。

注意：Ciscoは、実稼動ネットワーク トラフィックと信頼される管理ネットワーク トラフィックを、異なるネットワーク セグメントに保持することを強く推奨します。アプライアンスと管理トラフィック データ ストリームのセキュリティを保証するための対策を実施する必要があります。

一般的な Firepower システム の展開

物理アプライアンス環境で、一般的な Firepower システム の展開には、物理デバイスと物理 Cisco Firepower Management Center を使用します。次の図は展開の例を表します。以下に示すように、Device_A および Device_C をインライン構成で、Device_B をパッシブ構成で展開できます。



ほとんどのネットワーク スイッチでポート ミラーリングを設定して、1 つのスイッチ ポート（または VLAN 全体）で発生するネットワーク パケットのコピーをネットワーク監視接続に送信できます。主要なネットワーク機器プロバイダーでは SPAN（スイッチ ポート アナライザ）とも呼ばれるポート ミラーリングを使用することで、ネットワーク トラフィックを監視できます。Device_B は、Server_A と Server_B の間のスイッチの SPAN ポートを経由して、Server_A と Server_B の間のトラフィックを監視することに注意してください。

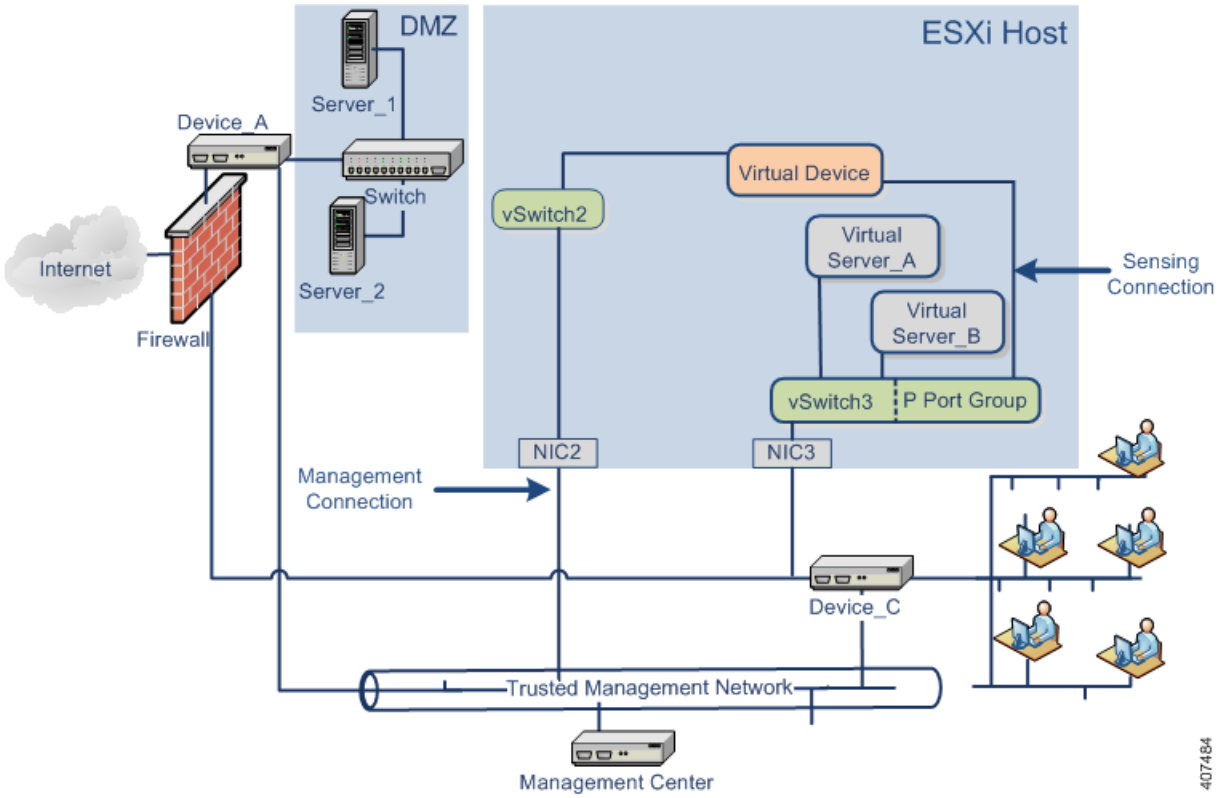
仮想 Firepower アプライアンスの導入VMware

仮想化と仮想デバイスの追加

仮想インフラストラクチャを使用することにより、一般的な Firepower システム の展開（21 ページ）で物理的な内部サーバを置き換えることができます。次の例では、ESXi ホストを使用して、Server_A および Server_B を仮想化できます。

仮想デバイスを使用して、Server_A と Server_B の間のトラフィックを監視できます。

下図のように、仮想デバイスセンシング インターフェイスは、無差別モード トラフィックを受け入れるスイッチまたはポート グループに接続する必要があります。



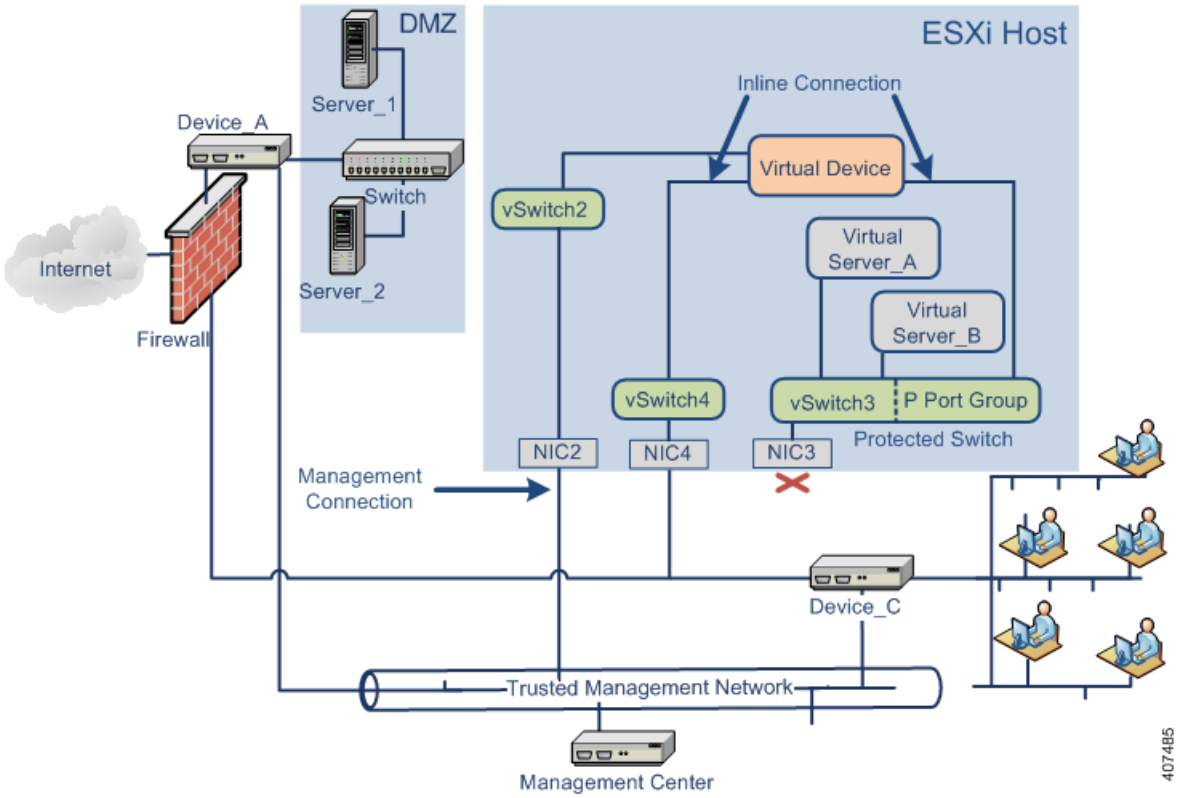
(注) すべてのトラフィックを検知するには、デバイス センシング インターフェイスが接続する仮想スイッチまたはポート グループで無差別モード トラフィックを許可します。

この例で示しているセンシング インターフェイスは 1 つのみですが、仮想デバイスではデフォルトで 2 つのセンシング インターフェイスを使用できます。仮想デバイスの管理インターフェイスは、信頼できる管理ネットワークと Cisco Firepower Management Center に接続します。

インライン検出のための仮想デバイスの使用

仮想デバイスのインライン インターフェイス セットを介してトラフィックを渡すことにより、仮想サーバの周囲にセキュアな境界を実現できます。このシナリオは一般的な Firepower システム の展開 (21 ページ)と仮想化と仮想デバイスの追加 (22 ページ)に示す例の上に構築します。

はじめに、保護された仮想スイッチを作成し、それを仮想サーバに接続します。次に、保護されたスイッチを、仮想デバイスを通じて外部ネットワークに接続します。詳細については、*Firepower System Configuration Guide*を参照してください。



(注) すべてのトラフィックを検知するには、デバイス センシング インターフェイスが接続する仮想スイッチまたはポート グループで無差別モード トラフィックを許可します。

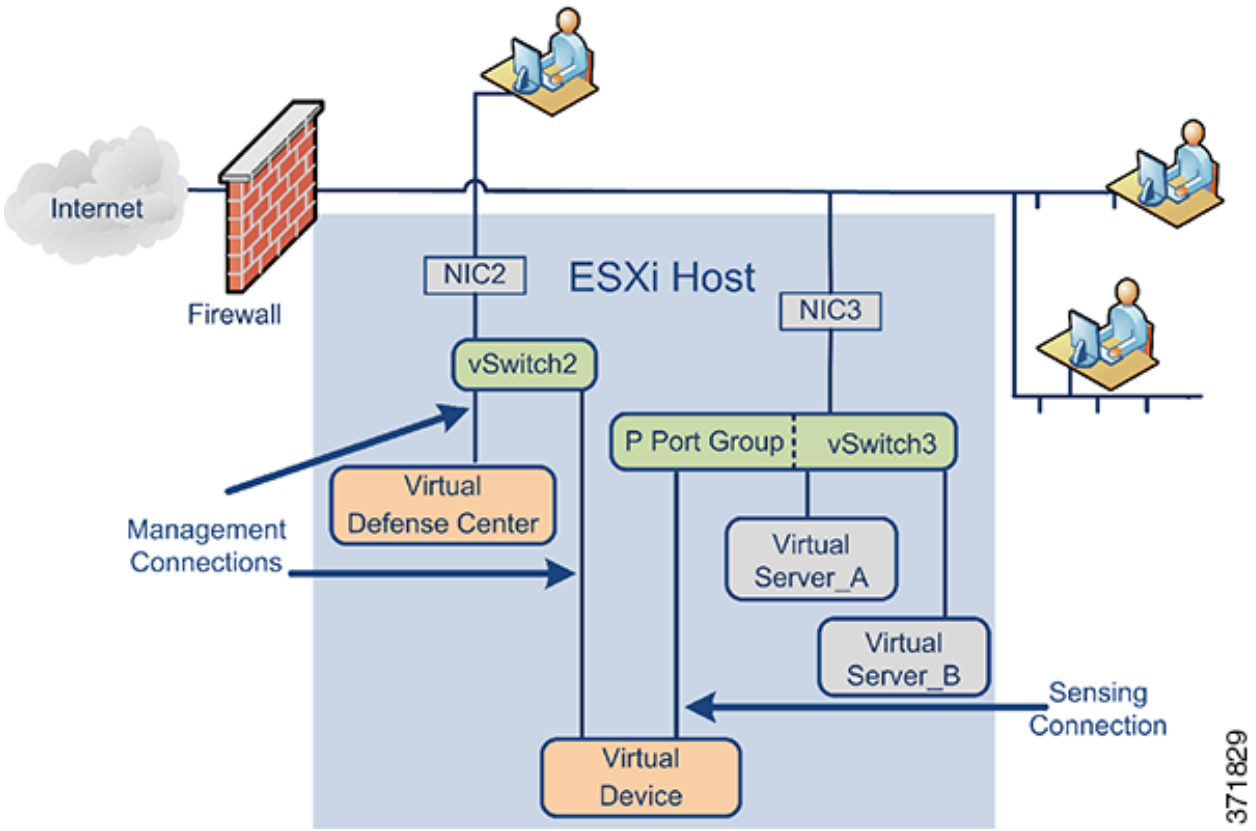
仮想デバイスは、侵入ポリシーに応じて、Server_A および Server_B への悪意のある任意のトラフィックを監視およびドロップします。

仮想 Cisco Firepower Management Center の追加

次に示すように、ESXi ホストに仮想 Cisco Firepower Management Center を展開し、仮想ネットワークおよび物理ネットワークに接続できます。このシナリオは一般的な Firepower システム の展開 (21 ページ)とインライン検出のための仮想デバイスの使用 (23 ページ)に示す例の上に構築します。

仮想 Firepower Management Center から NIC2 を経由した信頼できる管理ネットワークへの接続により、仮想 Firepower Management Center は物理デバイスと仮想デバイスの両方を管理できます。

Cisco 仮想アプライアンスは必須のアプリケーション ソフトウェアとともに事前に構成されているので、ESXi ホストに展開後すぐに動作可能です。このことにより、ハードウェアとソフトウェアの複雑な互換性問題が減り、展開時間が短縮されて、Firepower システム の機能を最大限に活用できます。次に示すように、ESXi ホスト上に仮想サーバ、仮想 Firepower Management Center、および仮想デバイスを展開し、仮想 Firepower Management Center からその展開を管理することができます。

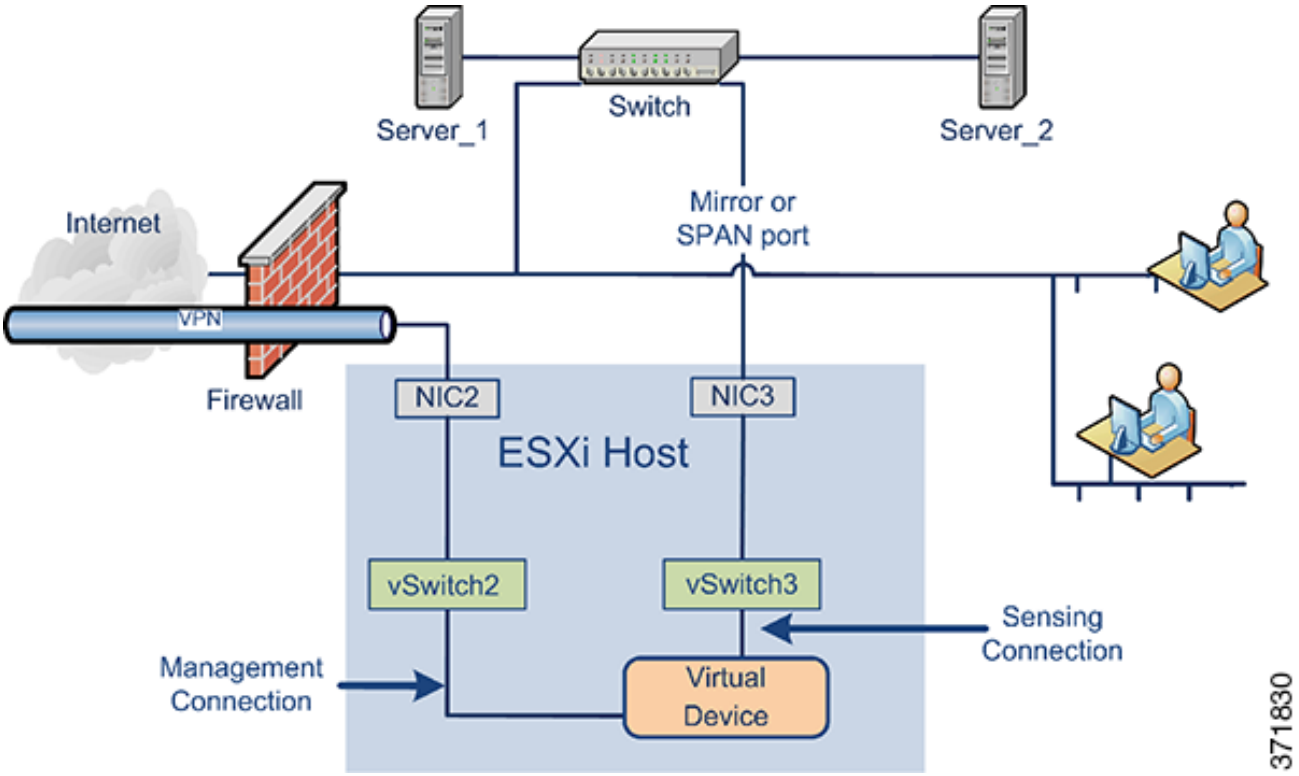


仮想デバイスの検知接続は、ネットワーク トラフィックを監視できるようにする必要があります。仮想スイッチまたは仮想インターフェイスが接続するスイッチ上のポート グループは、無差別モードのトラフィックを受け入れる必要があります。これにより、仮想デバイスは他のマシンまたはネットワーク デバイス向けのパケットを読み取ることができます。例では、P ポート グループが無差別モード トラフィックを受け入れるように設定されています。

仮想アプライアンスの管理接続のほうがより一般的な差別モード接続です。仮想 Firepower Management Center によって、仮想デバイスのコマンドと制御が提供されます。ESXi ホストのネットワーク インタフェース カード（この例では NIC2）を経由した接続により、仮想 Firepower Management Center にアクセスできます。仮想 Firepower Management Center および仮想デバイスの管理接続のセットアップについては、仮想 Firepower Management Center ネットワーク設定の自動化（14 ページ）と『*Cisco NGIPSv Quick Start Guide for VMware*』を参照してください。

リモート オフィス展開の使用

仮想デバイスは、リソースが限られているリモート オフィスを監視するための理想的な方法です。次に示すように、ESXi ホストに仮想デバイスを展開し、ローカル トラフィックを監視できます。



仮想デバイスの検知接続は、ネットワーク トラフィックを監視できるようにする必要があります。これを行うには、仮想スイッチまたはセンシング インターフェイスが接続するスイッチのポート グループが、無差別モード トラフィックを受け入れる必要があります。これにより、仮想デバイスは他のマシンまたはネットワーク デバイス向けのパケットを読み取ることができます。この例では、vSwitch3 のすべてが無差別モード トラフィックを受け入れるように設定されています。vSwitch3 は、NIC3 を経由して SPAN ポートにも接続されているため、リモート オフィスのスイッチを通過するトラフィックも監視できます。

仮想デバイスは Firepower Management Center で管理する必要があります。ESXi ホストのネットワーク インターフェイス カード（この例では NIC2）を経由した接続により、リモート Firepower Management Center を使用して、仮想デバイスにアクセスできます。

さまざまな地理的位置にデバイスを展開する場合、保護されていないネットワークからデバイスを隔離して、デバイスおよびデータ ストリームのセキュリティを保証するための対策を実施する必要があります。デバイスから VPN または別のセキュアなトンネリング プロトコルを使用してデータ ストリームを送信することによりこれを実現できます。