管理ネットワークでの展開

Firepower システムは、それぞれ固有のネットワーク アーキテクチャのニーズに応じて展開することができます。Management Center が、Firepower システムの集中管理コンソールおよびデータベース リポジトリとなります。トラフィック接続を収集して分析するために、複数のネットワーク セグメントにデバイスを設置します。

Management Center は管理インターフェイスを使用して、*信頼できる管理ネットワーク*(つまり、公開されている外部トラフィックではない安全な内部ネットワーク)に接続します。デバイスは、管理インターフェイスを使用して Management Center に接続します。

次に、デバイスはセンシング インターフェイスを使用して外部ネットワークに接続して、トラフィックをモニタします。展開におけるセンシング インターフェイスの使用方法の詳細については、『*Firepower 7000 and 8000 Series Installation Guide*』の「Deploying Firepower Managed Devices」を参照してください。

コメント

ASA FirePOWER のデバイスの展開シナリオについて詳しくは、ASA のマニュアルを参照してください。

管理展開に関する考慮事項

管理展開の決定は、さまざまな要因に基づいて行われます。以下の質問に答えることは、最も効率的かつ効果的なシステムを構成するための展開オプションの理解に役立ちます。

- デフォルトの単一の管理インターフェイスを使用してデバイスを Management Center に接続しますか? パフォーマンスを向上したり、Management Center で受信した別のネットワークからのトラフィックを分離するために、追加の管理インターフェイスを有効化しますか? 詳細については、管理インターフェイスについて(4 ～ 2 ページ)を参照してください。
- パフォーマンスを向上するために、トラフィック チャネルを有効化して Management Center と管理対象デバイスの間に 2 つの接続を作成しますか?Management Center と管理対象デバイスの間のスループット容量をさらに増加するために、複数の管理インターフェイスを使用しますか? 詳細については、複数のトラフィック チャネルを持つ場合の展開(4 ～ 3 ページ)を参照してください。
- 単一の Management Center を使用して、別のネットワーク デバイスからのトラフィックを管理および分離しますか? 詳細については、ネットワーク ルートを持つ場合の展開(4 ～ 4 ページ)を参照してください。
- 保護された環境に管理インターフェイスを展開しますか? アプライアンスのアクセスは、特定のワークステーション IP アドレスに制限されますか?セキュリティの考慮事項(4 ～ 5 ページ)には、管理インターフェイスを安全に展開するための考慮事項が説明されています。
- 8000 シリーズ デバイスを展開しますか? 詳細については、特殊なケース:8000 シリーズ デバイスの接続(4 ～ 5 ページ)を参照してください。

管理インターフェイスについて

管理インターフェイスは、防御センターが管理するすべてのデバイスと Management Center の間の通信手段を提供します。アプライアンス間のトラフィック制御を正常に維持することが、展開の成功に不可欠です。

Management Center および Firepower デバイス上では、Management Center またはデバイス上、あるいは両方の管理インターフェイスを使用して、アプライアンス間のトラフィックを 2 種類のトラフィック チャネルに分類できます。*管理トラフィック チャネル*は、すべての内部トラフィック（アプライアンスおよびシステムの管理専用のデバイス間トラフィックなど）を伝送し、*イベント トラフィック チャネル*は、すべてのイベント トラフィック（すなわち、侵入イベントやマルウェア イベントなどの大容量イベント トラフィック）を伝送します。トラフィックを 2 つのチャネルに分割することにより、アプライアンス間に 2 つの接続ポイントが作成されてスループットが増大するために、パフォーマンスが向上します。また、*複数の管理インターフェイス*を有効化して、アプライアンス間のスループットをさらに向上させたり、異なるネットワーク上のデバイス間のトラフィックの管理と分離を行うこともできます。

デバイスを Management Center に登録した後、各アプライアンスの Web ブラウザを使用してデフォルト設定を変更し、トラフィック チャネルや複数の管理インターフェイスの有効化ができます。設定については、*『Firepower Management Center Configuration Guide』*の「Configuring Appliance Settings」を参照してください。

通常、管理インターフェイスは、アプライアンスの背面に配置されています。詳細については、管理インターフェイスの識別（3 ～ 2 ページ）を参照してください。

単一の管理インターフェイス

デバイスを Management Center に登録すると、Management Center 上の管理インターフェイスとデバイス上の管理インターフェイスとの間のすべてのトラフィックを伝送する単一通信チャネルが確立されます。

以下の図に、デフォルトの単一通信チャネルを示します。1 つのインターフェイスにより、管理トラフィックとイベント トラフィックの両方が 1 つの通信チャネルで伝送されます。

複数の管理インターフェイス

複数の管理インターフェイスを有効化および設定して、それぞれに固有の IPv4 または IPv6 アドレス（および必要に応じてホスト名）を割り当て、各トラフィック チャネルを異なる管理インターフェイスに送信することによって、トラフィック スループットを大幅に向上できます。負荷が軽い管理トラフィックの搬送用には小さなインターフェイスを構成し、負荷が大きいイベント トラフィックの搬送用には大きなインターフェイスを構成します。デバイスを別々の管理インターフェイスに登録し、同一のインターフェイスに対して両方のトラフィック チャネルを構成したり、Management Center によって管理されるすべてのデバイスのイベント トラフィック チャネルを専用の管理インターフェイスで伝送することができます。

また、Management Center 上の特定の管理インターフェイスから別のネットワークまでのルートを作成することにより、あるネットワーク上のデバイスからのトラフィックと別のネットワーク上のデバイスからのトラフィックを、Management Center で別々に管理することもできます。

追加の管理インターフェイスは、以下の例外を使用して、デフォルト管理インターフェイスと同じように機能します。

- DHCP は、デフォルト（`eth0`）管理インターフェイスにのみ設定できます。追加のインターフェイス（`eth1` など）には、固有の静的 IP アドレスとホスト名が必要です。Cisco では、追加の管理インターフェイスの DNS エントリを設定する代わりに、これらのインターフェイスに対する IP アドレスのみを使用して Management Center およびデバイスを登録することを推奨しています。
- デフォルト以外の管理インターフェイスを使用して Management Center と管理対象デバイスを接続する場合、それらのアプライアンスが NAT デバイスによって分離されているならば、同じ管理インタフェースを使用するよう両方のトラフィック チャネルを設定する必要があります。
- Lights-Out Management は、デフォルトの管理インターフェイスでのみ使用できます。
- 70xx ファミリでは、トラフィックを 2 つのチャネルに分離して、Management Center上の 1 つ以上の管理インターフェイスにトラフィックを送信するようにそれらのチャネルを設定できます。ただし、70xx ファミリには 1 つの管理インターフェイスしかないため、デバイスは唯一の管理インターフェイス上で Management Center から送信されたトラフィックを受信します。

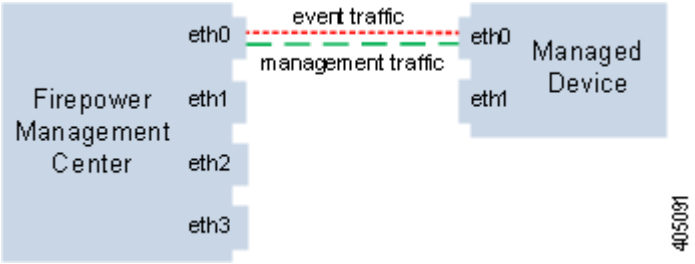
展開オプション

トラフィック チャネルを使用してトラフィック フローを管理することで、1 つ以上の管理インターフェイスを使用してシステムのパフォーマンスを向上させることができます。さらに、Management Center およびその管理対象デバイス上の専用の管理インターフェイスを使用して別のネットワークまでのルートを作成することにより、異なるネットワーク上のデバイス間のトラフィックを分離することもできます。詳細については、次の項を参照してください。

複数のトラフィック チャネルを持つ場合の展開

1 つの管理インターフェイス上で 2 つのトラフィック チャネルを使用する場合、Management Center と管理対象デバイスの間に 2 つの接続を作成します。同じインターフェイス上の 2 つのチャネルのうちの一方が管理トラフィックを伝送し、もう一方がイベント トラフィックを伝送します。

次の例は、同じインターフェイス上に 2 つの独立したトラフィック チャネルを持つ通信チャネルを示しています。

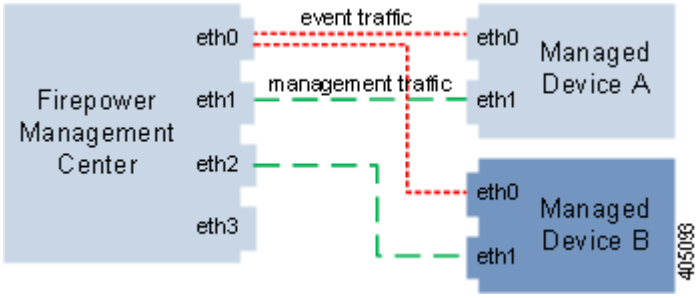


複数の管理インターフェイスを使用する場合、トラフィック チャネルを 2 つの管理インターフェイスに分割することによりパフォーマンスを向上できます。それによって両方のインターフェイス容量が増し、トラフィック フローが増加します。一方のインターフェイスで管理トラフィック チャネルを伝送し、もう一方のインターフェイスでイベント トラフィック チャネルを伝送します。いずれかのインターフェイスで障害が発生した場合は、すべてのトラフィックがアクティブ インターフェイスに再ルーティングされるため、接続が維持されます。

次の図は、2 つの管理インターフェイス上にある管理トラフィック チャネルとイベント トラフィック チャネルを示しています。

専用の管理インターフェイスを使用して、複数のデバイスからのイベント トラフィックのみを伝送することができます。この設定では、管理トラフィック チャネルを伝送する別の管理インターフェイスに各デバイスを登録し、すべてのデバイスからのすべてのイベント トラフィックを、Management Center 上の 1 つの管理インターフェイスで伝送します。インターフェイスで障害が発生した場合は、トラフィックがアクティブ インターフェイスに再ルーティングされるため、接続が維持されます。すべてのデバイスのイベント トラフィックが同じインターフェイスで伝送されることから、トラフィックはネットワーク間で分離されないことに注意してください。

以下の図では、2 台のデバイスが別々の管理チャネル トラフィック インターフェイスを使用し、イベント トラフィック チャネルに対しては同じ専用インターフェイスを共有しています。



ネットワーク ルートを持つ場合の展開

Management Center 上の特定の管理インターフェイスから別のネットワークまでのルートを作成できます。そのネットワークのデバイスを Management Center 上の指定された管理インターフェイスに登録すると、別のネットワーク上のデバイスと Management Center の間で独立した接続が実現されます。両方のトラフィック チャネルが同じ管理インターフェイスを使用するように設定することで、そのデバイスからのトラフィックが他のネットワーク上のデバイス トラフィックから確実に分離された状態を維持できます。ルーテッド インターフェイスは Management Center 上の他のすべてのインターフェイスから分離されているため、ルーテッド管理インターフェイスに障害が発生した場合、接続が失われます。

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、デフォルト管理インターフェイスだけでサポートされています。

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。詳しくは、『*Firepower Management Center Configuration Guide*』の「Configuring Appliance Settings」を参照してください。

次の図では、2 つのデバイスですべてのトラフィックに対して別々の管理インターフェイスを使用することにより、ネットワーク トラフィックを分離しています。さらに管理インターフェイスを追加して、デバイスごとに独立した管理トラフィック チャネル インターフェイスとイベント トラフィック チャネル インターフェイスを構成できます。

セキュリティの考慮事項

管理インターフェイスを安全な環境に展開するために、Ciscoでは次の事項を考慮することを推奨しています。

- 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信頼できる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。

特殊なケース：8000 シリーズ デバイスの接続

サポートされるデバイス：8000 シリーズ

Management Center に 8000 シリーズ のデバイスを登録するときは、接続の両側で自動ネゴシエーションするか、または両側を同じ固定速度に設定して安定したネットワーク リンクを確保する必要があります。8000 シリーズ のデバイスは、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。