

Secure Firewall Management Center と脅威 防御管理ネットワーク管理

初版：2020年4月22日

最終更新：2022年11月28日

Secure Firewall Management Center および Threat Defense 管理ネットワークの管理

このドキュメントでは、Cisco Secure Firewall Management Center と Cisco Secure Firewall Threat Defense 間の管理接続、管理ネットワークの基本、ネットワーク設定の変更方法（Threat Defense または Management Center、またはその両方の IP アドレスの変更を含む）について説明します。

Management Center およびデバイス管理について

Management Center がデバイスを管理するときは、デバイスとの間に、双方向の SSL 暗号化通信チャンネルをセットアップします。Management Center はこのチャンネルを使用して、そのデバイスへのネットワークトラフィックの分析および管理の方法に関する情報をそのデバイスに送信します。そのデバイスはトラフィックを評価すると、イベントを生成し、同じチャンネルを使用してそれらのイベントを Management Center に送信します。

Management Center を使用してデバイスを管理すると、以下の利点があります。

- すべてのデバイスのポリシーを一箇所から設定できるため、設定の変更が容易になります。
- さまざまなタイプのソフトウェアアップデートをデバイスにインストールできます。
- 正常性ポリシーを管理対象デバイスに適用して、Management Center からデバイスのヘルスステータスをモニターできます。



(注) CDO 管理対象デバイスがあり、オンプレミス Management Center を分析のみに使用している場合、オンプレミス Management Center はポリシーの設定またはアップグレードをサポートしません。デバイス設定およびその他のサポートされていない機能に関連するこのガイドの章と手順は、プライマリマネージャが CDO のデバイスには適用されません。

Management Center は、侵入イベント、ネットワーク検出情報、およびデバイスのパフォーマンスデータを集約して相互に関連付けます。そのため、ユーザはデバイスが相互の関連でレ

ポートする情報をモニタして、ネットワーク上で行われている全体的なアクティビティを評価することができます。

Management Center を使用することで、デバイス動作のほぼすべての側面を管理できます。



(注) Management Center は、<http://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html> [英語] で使用可能な互換性マトリックスで指定されている特定の以前のリリースを実行しているデバイスを管理できますが、これらの以前のリリースのデバイスでは新しい機能は利用できません。

デバイス管理インターフェイスについて

各デバイスには Management Center と通信するための専用の管理インターフェイスが1つ含まれています。必要に応じて、専用の管理インターフェイスではなく、管理用のデータインターフェイスを使用するようにデバイスを設定できます。

管理インターフェイスまたはコンソールポートで初期設定を実行できます。

管理インターフェイスは、スマート ライセンス サーバーとの通信、更新プログラムのダウンロード、その他の管理機能の実行にも使用します。

管理接続について

Management Center 情報を使用してデバイスを設定し、デバイスを Management Center に追加した後に、デバイスまたは Management Center のいずれかで管理接続を確立できます。初期設定に応じて、以下ようになります。

- デバイスまたは Management Center のいずれかから開始できる。
- デバイスのみが開始できる。
- Management Center のみが開始できる。

初期化は常に Management Center の eth0 またはデバイスの最も番号が小さい管理インターフェイスから始まります。接続が確立されていない場合は、追加の管理インターフェイスが試行されます。注：イニシエータは、ルーティングテーブルに基づいて最適なインターフェイスを選択しません。Management Center の複数の管理インターフェイスにより、個別のネットワークに接続したり、管理トラフィックとイベントトラフィックを分離したりできます。

Management Center 上の管理インターフェイス

Management Center では、初期セットアップ、管理者の HTTP アクセス、デバイスの管理、ならびにその他の管理機能（ライセンス管理や更新など）に、eth0 インターフェイスが使用されます。

追加の管理インターフェイスを設定することもできます。Management Center がさまざまなネットワーク上で多数のデバイスを管理している場合、管理インターフェイスをさらに追加することで、スループットとパフォーマンスの向上につながります。これらの管理インターフェイスをその他すべての管理機能に使用することもできます。管理インターフェイスごとに、対応する機能を限定することをお勧めします。たとえば、ある特定の管理インターフェイスを HTTP 管理者アクセス用に使用し、別の管理インターフェイスをデバイスの管理に使用するなどです。

デバイス管理用に、管理インターフェイスには 2 つの別個のトラフィック チャンネルがあります。管理トラフィック チャンネルはすべての内部トラフィック（デバイス管理に固有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 チャンネルはすべてイベントトラフィック（Web イベントなど）を伝送します。オプションで、Management Center 上にイベントを処理するためのイベント専用インターフェイスを別個に設定することもできます。設定できるイベント専用インターフェイスは 1 つだけです。管理トラフィックチャンネルの管理インターフェイスも常に必要です。イベントトラフィックは大量の帯域幅を使用する可能性があるため、管理トラフィックからイベントトラフィックを分離することで、Management Center のパフォーマンスを向上させることができます。たとえば、10 GigabitEthernet インターフェイスをイベントインターフェイスとして割り当て、可能なら、1 GigabitEthernet インターフェイスを管理用に使用します。たとえば、イベント専用インターフェイスは完全にセキュアなプライベートネットワーク上に設定し、通常管理インターフェイスはインターネットにアクセスできるネットワーク上で使用することをお勧めします。目的がスループットの向上だけである場合は、管理インターフェイスとイベントインターフェイスを同じネットワーク上で使用することもできます。管理対象デバイスは、管理トラフィックを Management Center の管理インターフェイスに送信し、イベントトラフィックを Management Center のイベント専用インターフェイスに送信します。管理対象デバイスがイベント専用インターフェイスに到達できない場合、フォールバックして管理インターフェイスにイベントを送信します。

Management Center からの管理接続の初期化は、常に eth0 から試行され、その後に他のインターフェイスが順番に試行されます。ルーティングテーブルは、最適なインターフェイスの決定には使用されません。



-
- (注) すべての管理インターフェイスは、アクセスリスト設定による制御に従って HTTP 管理者アクセスをサポートしています。逆に、インターフェイスを HTTP アクセスのみに制限することはできません。管理インターフェイスでは、常にデバイス管理がサポートされます（管理トラフィック、イベントトラフィック、またはその両方）。
-



-
- (注) eth0 インターフェイスのみが DHCP IP アドレスをサポートします。他の管理インターフェイスはスタティック IP アドレスのみをサポートします。
-

Threat Defense の管理インターフェイス

デバイスをセットアップするときに、接続先とする Management Center の IP アドレスを指定します。デバイスが接続を開始すると、初期登録時は、管理トラフィックとイベントトラフィックの両方がこのアドレスに送信されます。注：場合によっては、Management Center が別の管理インターフェイスで初期接続を確立すると、以降の接続では指定した IP アドレスの管理インターフェイスを使用する必要があります。

Management Center に別のイベント専用インターフェイスがある場合、ネットワークが許可する場合、管理対象デバイスは後続のイベントトラフィックを Management Center イベント専用インターフェイスに送信します。さらに、一部の管理対象デバイスモデルには、イベント専用トラフィック用に構成できる追加の管理インターフェイスが含まれています。管理用のデータインターフェイスを設定する場合は、個別管理およびイベントインターフェイスを使用できません。イベントネットワークがダウンすると、イベントトラフィックは、Management Center および/または管理対象デバイスの通常の管理インターフェイスに戻ります。

管理のための Threat Defense データインターフェイスの使用について

Management Center との通信には、専用の管理インターフェイスか、または通常のデータインターフェイスを使用できます。データインターフェイスでのマネージャアクセスは、外部インターフェイスからリモートで Threat Defense を管理する場合、または別の管理ネットワークがない場合に便利です。さらに、データインターフェイスを使用すると、プライマリインターフェイスがダウンした場合に管理機能を引き継ぐように冗長セカンダリインターフェイスを構成できます。

データインターフェイスからのマネージャアクセスには、次の制限があります。

- マネージャアクセスを有効にできるのは、1つの物理的なデータインターフェイスのみです。サブインターフェイスと EtherChannel は使用できません。冗長性を目的として、Management Center の単一のセカンダリインターフェイスでマネージャアクセスを有効にすることもできます。
- このインターフェイスは管理専用にはできません。
- ルーテッドインターフェイスを使用するルーテッドファイアウォールモードのみです。
- PPPoE はサポートされていません。ISP で PPPoE が必要な場合は、PPPoE をサポートするルータを Threat Defense と WAN モデムの上に配置する必要があります。
- インターフェイスを配置する必要があるのはグローバル VRF のみです。
- SSH はデータインターフェイスではデフォルトで有効になっていないため、後で Management Center を使用して SSH を有効にする必要があります。また、管理インターフェイス ゲートウェイがデータインターフェイスに変更されるため、**configure network static-routes** コマンドを使用して管理インターフェイス用の静的ルートを追加しない限り、リモートネットワークから管理インターフェイスに SSH 接続することはできません。Amazon Web Services の Threat Defense Virtual の場合、コンソールポートは使用できないため、管理インターフェイスへの SSH アクセスを維持する必要があります。設定を続行する前に、管理用の静的ルートを追加します。または、マネージャアクセス用のデータインターフェイス

スを設定する前に、すべての CLI 構成 (`configure manager add` コマンドを含む) を終了してから接続を切断します。

- 管理インターフェイスとイベント専用インターフェイスを別々に使用することはできません。
- ハイアベイラビリティはサポートされません。この場合、管理インターフェイスを使用する必要があります。
- クラスタリングはサポートされません。この場合、管理インターフェイスを使用する必要があります。

FMCモデルごとの管理インターフェイスサポート

管理インターフェイスの場所については、ご使用のモデルのハードウェアインストールガイドを参照してください。

各 FMC モデルでサポートされる管理インターフェイスについては、以下の表を参照してください。

表 1: FMCでの管理インターフェイスのサポート

モデル	管理インターフェイス
MC1600、MC2600、MC4600	eth0 (デフォルト) eth1 eth2 eth3 CIMC (Lights-Out Management でのみサポート)
Firepower Management Center Virtual	eth0 (デフォルト)

デバイスモデルごとの管理インターフェイスのサポート

管理インターフェイスの場所については、ご使用のモデルのハードウェアインストールガイドを参照してください。



- (注) Firepower 4100/9300 の場合、MGMT インターフェイスは Threat Defense の論理デバイスを管理するためではなく、シャーシを管理するために使用します。mgmt タイプ (または firepower-eventing タイプあるいはその両方) の別個のインターフェイスを設定してから、そのインターフェイスを Threat Defense 論理デバイスに割り当てる必要があります。



- (注) シャーシ上の Threat Defense の場合、物理管理インターフェイスは、診断論理インターフェイス (SNMP または syslog に利用できて、Management Center でデータインターフェイスと併せて設定されます) と、Management Center 通信用の管理論理インターフェイスの間で共有されます。

管理対象デバイスの各モデルでサポートされる管理インターフェイスについては、以下の表を参照してください。

表 2: 管理対象デバイスでサポートされる管理インターフェイス

モデル	管理インターフェイス	オプションのイベントインターフェイス
Firepower 1000	management0 (注) management0 は管理 1/1 インターフェイスの内部名です。	サポートなし
Firepower 2100	management0 (注) management0 は管理 1/1 インターフェイスの内部名です。	サポートなし
Cisco Secure Firewall 3100	management0 (注) management0 は管理 1/1 インターフェイスの内部名です。	サポートなし
Firepower 4100 および 9300	management0 (注) management0 は、物理インターフェイス ID に関わらず、このインターフェイスの内部名です。	management1 (注) management1 は、物理インターフェイス ID に関わらず、このインターフェイスの内部名です。

モデル	管理インターフェイス	オプションのイベント インターフェイス
ISA 3000	br1 (注) br1 は、管理 1/1 インターフェイスの内部名です。	サポートなし
Secure Firewall Threat Defense Virtual	eth0	サポートなし

Management Center 管理インターフェイス上のネットワーク ルート

管理インターフェイス（イベント専用インターフェイスを含む）は、リモートネットワークに到達するためのスタティック ルートのみをサポートしています。Management Center をセットアップすると、セットアッププロセスにより、指定したゲートウェイ IP アドレスへのデフォルトルートが作成されます。このルートを削除することはできません。また、このルートで変更できるのはゲートウェイ アドレスのみです。

一部のプラットフォームでは、複数の管理インターフェイスを設定できます。デフォルトルートには出力インターフェイスが含まれていないため、選択されるインターフェイスは、指定したゲートウェイアドレスと、ゲートウェイが属するインターフェイスのネットワークによって異なります。デフォルトネットワーク上に複数のインターフェイスがある場合、デバイスは出力インターフェイスとして番号の小さいインターフェイスを使用します。

リモートネットワークにアクセスするには、管理インターフェイスごとに1つ以上のスタティックルートを使用することをお勧めします。他のデバイスから Management Center へのルーティングの問題など、潜在的なルーティングの問題を回避するために、各インターフェイスを個別のネットワークに配置することをお勧めします。



- (注) 管理接続に使用されるインターフェイスは、ルーティングテーブルによって決定されません。接続は常に最初に eth0 を使用して試行され、その後、管理対象デバイスに到達するまで、後続のインターフェイスが順番に試行されます。

管理インターフェイス上のネットワークルート

管理インターフェイス（イベント専用インターフェイスを含む）は、リモートネットワークに到達するためのスタティック ルートのみをサポートしています。管理対象デバイスをセットアップすると、セットアッププロセスにより、指定したゲートウェイ IP アドレスへのデフォルトルートが作成されます。このルートを削除することはできません。また、このルートで変更できるのはゲートウェイ アドレスのみです。



- (注) 管理インターフェイスのルーティングは、データインターフェイスに対して設定するルーティングとは完全に別のものです。専用の管理インターフェイスを使用する代わりに管理用のデータインターフェイスを設定すると、トラフィックはバックプレーンを介してルーティングされ、データルーティングテーブルが使用されます。ここで説明する内容は適用されません。

一部のプラットフォームでは、複数の管理インターフェイス（管理インターフェイスとイベント専用インターフェイス）を設定できます。デフォルトルートには出力インターフェイスが含まれていないため、選択されるインターフェイスは、指定したゲートウェイアドレスと、ゲートウェイが属するインターフェイスのネットワークによって異なります。デフォルトネットワーク上に複数のインターフェイスがある場合、デバイスは出力インターフェイスとして番号の小さいインターフェイスを使用します。

リモートネットワークにアクセスするには、管理インターフェイスごとに1つ以上のスタティックルートを使用することをお勧めします。他のデバイスから Threat Defense へのルーティングの問題など、潜在的なルーティングの問題を回避するために、各インターフェイスを個別のネットワークに配置することをお勧めします。



- (注) 管理接続に使用されるインターフェイスは、ルーティングテーブルによって決定されません。常に最も番号の小さいインターフェイスを最初に使用して接続が試行されます。

NAT 環境

ネットワーク アドレス変換 (NAT) とは、ルータを介したネットワーク トラフィックの送受信方式であり、送信元または宛先 IP アドレスの再割り当てが行われます。NAT の最も一般的な用途は、プライベートネットワークがインターネットと通信できるようにすることです。スタティック NAT は 1:1 変換を実行し、デバイスとの Management Center 通信に支障はありませんが、ポートアドレス変換 (PAT) がより一般的です。PAT では、単一のパブリック IP アドレスと一意のポートを使用してパブリックネットワークにアクセスできます。これらのポートは必要に応じて動的に割り当てられるため、PAT ルータの背後にあるデバイスへの接続は開始できません。

通常は、ルーティングと認証の両方の目的で両方の IP アドレス（登録キー付き）が必要です。デバイスを追加するときに、Management Center がデバイスの IP アドレスを指定し、デバイスが Management Center の IP アドレスを指定します。ただし、IP アドレスの 1 つのみがわかっている場合（ルーティング目的の最小要件）は、最初の通信用に信頼を確立して正しい登録キーを検索するために、接続の両側に一意の NAT ID を指定する必要もあります。Management Center およびデバイスでは、初期登録の認証と承認を行うために、登録キーおよび NAT ID（IP アドレスではなく）を使用します。

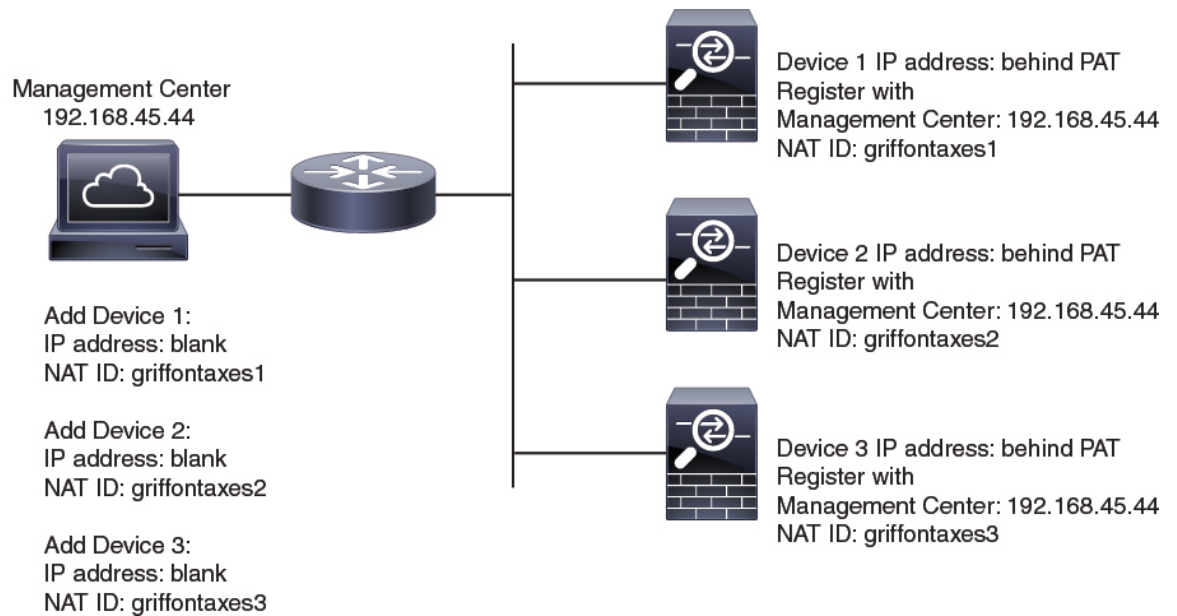
たとえば、デバイスを Management Center に追加したときにデバイスの IP アドレスがわからない場合（たとえばデバイスが PAT ルータの背後にある場合）は、NAT ID と登録キーのみを Management Center に指定します。IP アドレスは空白のままにします。デバイス上で、Management Center の IP アドレス、同じ NAT ID、および同じ登録キーを指定します。デバイスが Management

Center の IP アドレスに登録されます。この時点で、Management Center は IP アドレスの代わりに NAT ID を使用してデバイスを認証します。

NAT 環境では NAT ID を使用するのが最も一般的ですが、NAT ID を使用することで、多数のデバイスを簡単に Management Center に追加することができます。Management Center で、追加するデバイスごとに IP アドレスは空白のままにして一意の NAT ID を指定し、次に各デバイスで、Management Center の IP アドレスと NAT ID の両方を指定します。注：NAT ID はデバイスごとに一意でなければなりません。

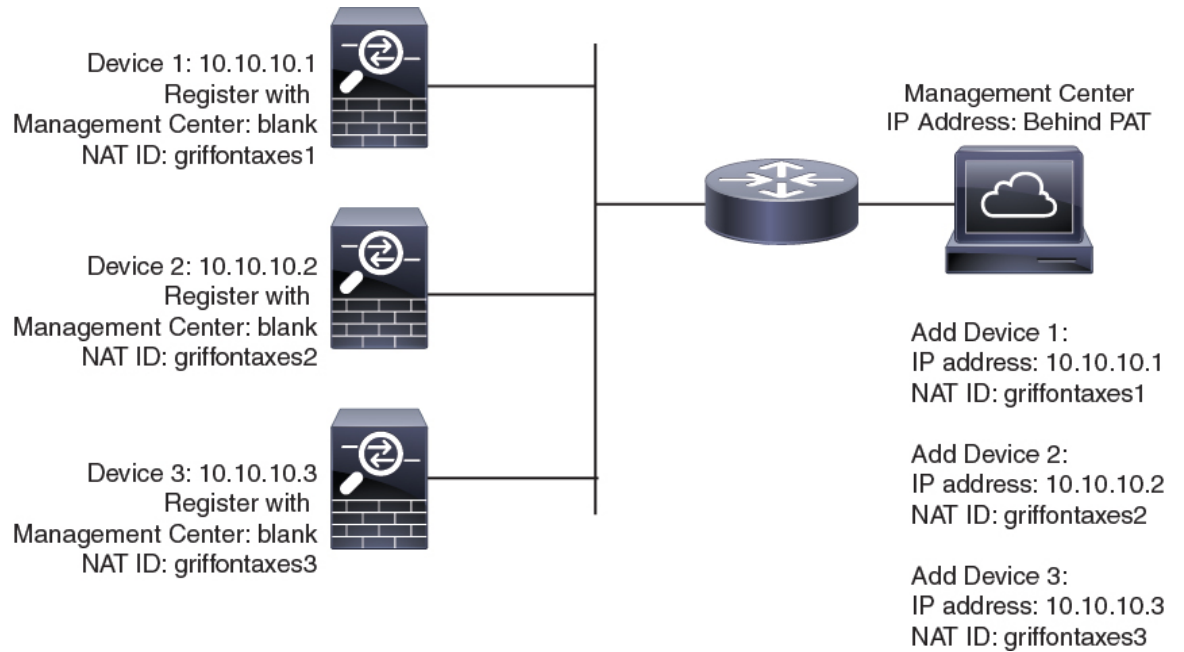
次の例に、PAT IP アドレスの背後にある 3 台のデバイスを示します。この場合、Management Center とデバイスの両方でデバイスごとに一意の NAT ID を指定し、デバイス上の Management Center の IP アドレスを指定します。

図 1: PAT の背後にある管理対象デバイスの NAT ID



次の例に、PAT IP アドレスの背後にある Management Center を示します。この場合、Management Center とデバイスの両方でデバイスごとに一意の NAT ID を指定し、Management Center 上のデバイスの IP アドレスを指定します。

図 2: PAT の背後にある FMC の NAT ID



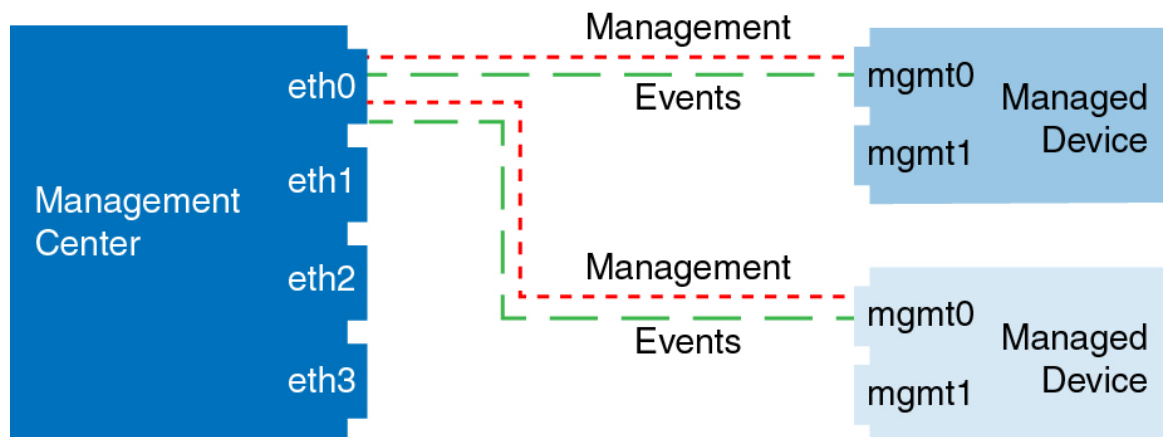
管理およびイベントトラフィック チャンネルの例



(注) 管理用のデータインターフェイスを Threat Defense で使用する場合は、そのデバイスに個別の管理インターフェイスとイベントインターフェイスを使用することはできません。

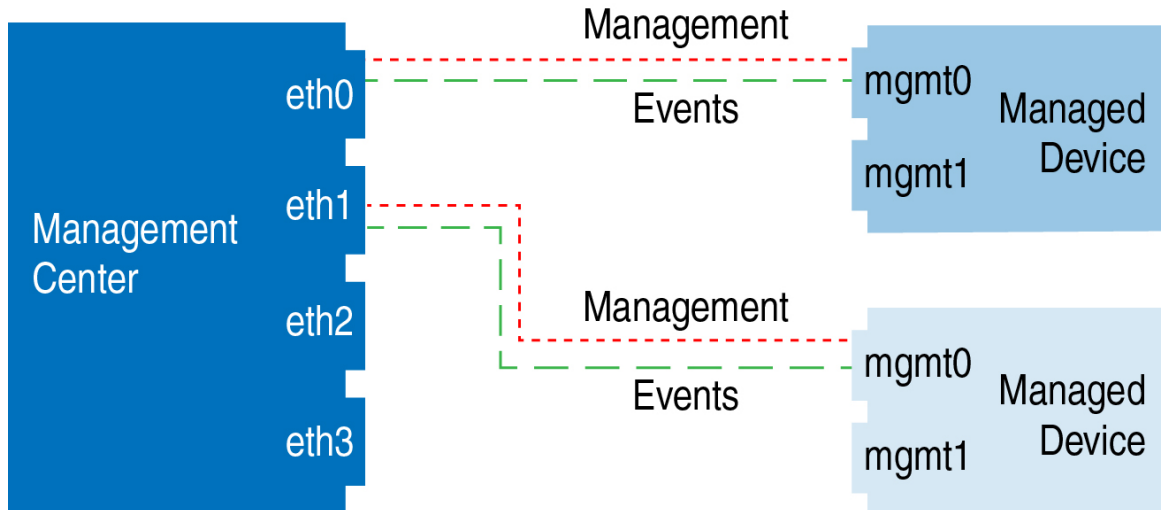
以下に、Management Center と管理対象デバイスでデフォルト管理インターフェイスのみを使用する例を示します。

図 3: Secure Firewall Management Center 上で単一の管理インターフェイスを使用する場合



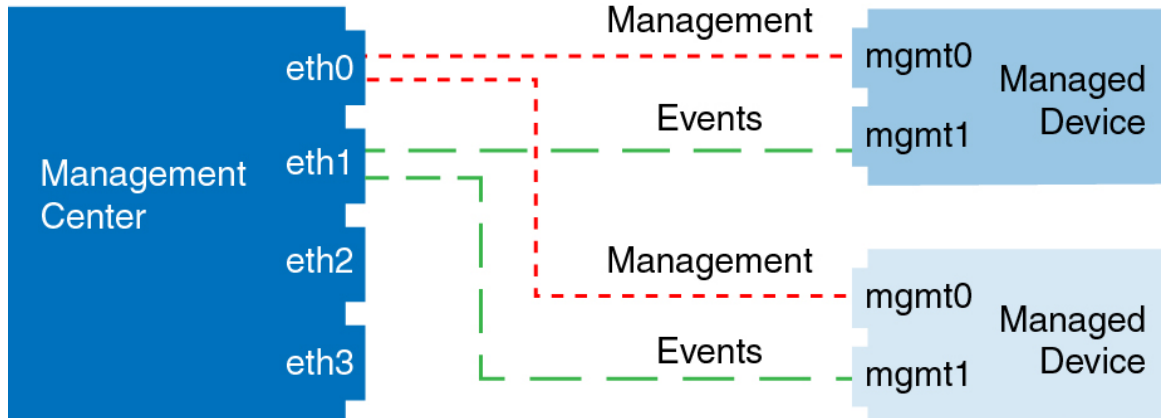
以下に、Management Center でデバイスごとに別個の管理インターフェイスを使用する例を示します。この場合、各管理対象デバイスが1つの管理インターフェイスを使用します。

図 4: Secure Firewall Management Center 上の複数の管理インターフェイスを使用する場合



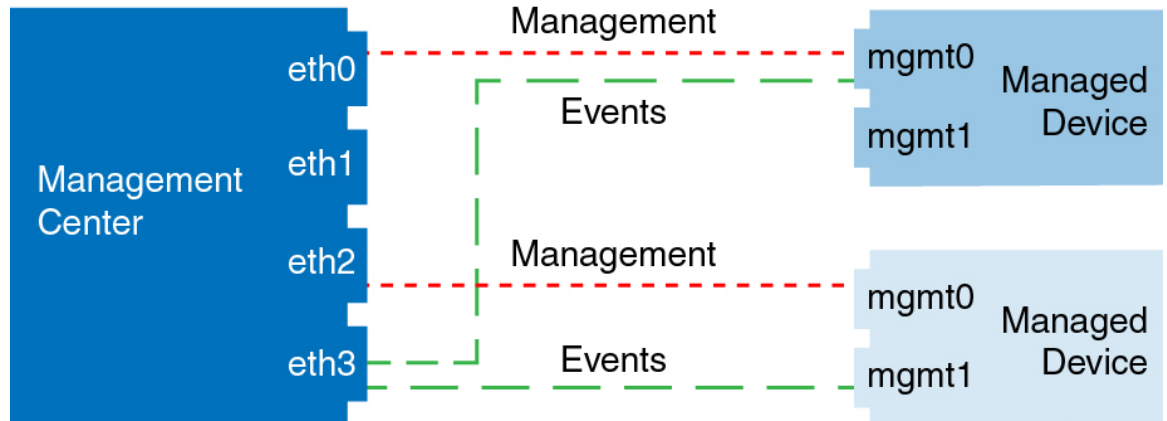
以下に、個別のイベント インターフェイスを使用する Management Center と管理対象デバイスの例を示します。

図 5: Secure Firewall Management Center 上の個別のイベント インターフェイスと管理対象デバイスを使用する場合



以下に、Management Center 上で複数の管理インターフェイスと個別のイベント インターフェイスが混在し、個別のイベント インターフェイスを使用する管理対象デバイスと単一の管理インターフェイスを使用する管理対象デバイスが混在する例を示します。

図 6: 管理インターフェイスとイベントインターフェイスを混在させて使用する場合



Threat Defense の初期設定の完了

Firepower 4100/9300 を除くすべてのモデルについて、CLI または Device Manager を使用して Threat Defense の初期設定を実行できます。Firepower 4100/9300 の場合、論理デバイスを展開する際に初期設定を実行します。

Device Manager を使用した Threat Defense の初期設定の完了

Device Manager に接続して、Threat Defense の初期設定を実行します。Device Manager を使用して初期セットアップを実行すると、管理インターフェイスおよびマネージャアクセス設定に加えて、管理のために Management Center に切り替えたときに、Device Manager で完了したすべてのインターフェイス構成が保持されます。アクセスコントロールポリシーやセキュリティゾーンなどの他のデフォルト設定は保持されないことに注意してください。CLI を使用すると、管理インターフェイスとマネージャアクセス設定のみが保持されます（たとえば、デフォルトの内部インターフェイス構成は保持されません）。

始める前に

- この手順は、Firepower 4100/9300 と ISA 3000 を除くすべてのデバイスに適用されます。Device Manager を使用してこれらのデバイスを Management Center にオンボーディングできますが、他のプラットフォームとはデフォルト設定が異なるため、この手順の詳細はこれらのプラットフォームには適用されない場合があります。
- この手順は、オンプレミスの Management Center を分析のみに使用する CDO 管理対象デバイスには適用されません。Device Manager の構成は、プライマリマネージャを構成するためのものです。分析用にデバイスを構成する方法の詳細については、[CLI を使用した Threat Defense 初期設定の実行の完了 \(19 ページ\)](#) を参照してください。

手順

ステップ1 Device Manager にログインします。

a) ブラウザに次の URL を入力します。

• 内部 : <https://192.168.95.1>。

• 管理 : https://management_ip。管理インターフェイスは DHCP クライアントであるため、IP アドレスは DHCP サーバーによって異なります。この手順の一環として、管理 IP アドレスを静的アドレスに設定する必要があるため、接続が切断されないように内部インターフェイスを使用することをお勧めします。

b) ユーザー名 **admin**、デフォルトパスワード **Admin123** を使用してログインします。

c) エンドユーザー ライセンス契約書を読んで同意し、管理者パスワードを変更するように求められます。

ステップ2 初期設定を完了するには、最初に Device Manager にログインしたときにセットアップウィザードを使用します。必要に応じて、ページの下部にある [デバイスの設定をスキップ (Skip device setup)] をクリックしてセットアップウィザードをスキップできます。

セットアップウィザードを完了すると、内部インターフェイスのデフォルト設定に加えて、Management Center の管理に切り替えるときに維持される外部 (Ethernet1/1) インターフェイスも設定できます。

a) 外部インターフェイスおよび管理インターフェイスに対して次のオプションを設定し、[次へ (Next)] をクリックします。

1. [外部インターフェイスアドレス (Outside Interface Address)]—このインターフェイスは通常インターネット ゲートウェイであり、マネージャ アクセス インターフェイスとして使用される場合があります。デバイスの初期設定時に別の外部インターフェイスを選択することはできません。最初のデータ インターフェイスがデフォルトの外部インターフェイスです。

マネージャアクセスに外部 (または内部) とは異なるインターフェイスを使用する場合は、セットアップウィザードの完了後に手動で設定する必要があります。

[IPv4 の設定 (Configure IPv4)] : 外部インターフェイス用の IPv4 アドレスです。DHCP を使用するか、または手動でスタティック IP アドレス、サブネットマスク、およびゲートウェイを入力できます。[オフ (Off)] を選択して、IPv4 アドレスを設定しないという選択肢もあります。セットアップウィザードを使用して PPPoE を設定することはできません。インターフェイスが DSL モデム、ケーブルモデム、または ISP への他の接続に接続されており、ISP が PPPoE を使用して IP アドレスを提供している場合は、PPPoE が必要になる場合があります。ウィザードの完了後に PPPoE を設定できます。

[IPv6 の設定 (Configure IPv6)] : 外部インターフェイス用の IPv6 アドレスです。DHCP を使用するか、または手動でスタティック IP アドレス、プレフィックス、およびゲートウェイを入力できます。[オフ (Off)] を選択して、IPv6 アドレスを設定しないという選択肢もあります。

2. [管理インターフェイス (Management Interface)]

CLI で初期設定を実行した場合、管理インターフェイスの設定は表示されません。

データインターフェイスでマネージャアクセスを有効にした場合でも、管理インターフェイスの設定が使用されます。たとえば、データインターフェイスを介してバックプレーン経由でルーティングされる管理トラフィックは、データインターフェイス DNS サーバーではなく、管理インターフェイス DNS サーバーを使用して FQDN を解決します。

[DNSサーバ (DNS Servers)]: システムの管理アドレス用の DNS サーバ。名前解決用に 1 つ以上の DNS サーバのアドレスを入力します。デフォルトは OpenDNS パブリック DNS サーバです。フィールドを編集し、デフォルトに戻したい場合は、[OpenDNS を使用 (Use OpenDNS)] をクリックすると、フィールドに適切な IP アドレスがリロードされます。

[ファイアウォールホスト名 (Firewall Hostname)]: システムの管理アドレスのホスト名です。

- b) [時刻設定 (NTP) (Time Setting (NTP))] を設定し、[次へ (Next)] をクリックします。
 1. [タイムゾーン (Time Zone)]: システムのタイムゾーンを選択します。
 2. [NTPタイムサーバ (NTP Time Server)]: デフォルトの NTP サーバを使用するか、使用している NTP サーバのアドレスを手動で入力するかを選択します。バックアップ用に複数のサーバを追加できます。
- c) [登録せずに 90 日間の評価期間を開始 (Start 90 day evaluation period without registration)] を選択します。

Threat Defense を Smart Software Manager に登録しないでください。すべてのライセンスは Management Center で実行されます。
- d) [終了 (Finish)] をクリックします。
- e) [クラウド管理 (Cloud Management)] または [スタンドアロン (Standalone)] を選択するよう求められます。Management Center の管理については、[スタンドアロン (Standalone)] を選択してから、[Got It (了解)] を選択します。

ステップ 3 (必要に応じて) 管理インターフェイスを設定します。

マネージャアクセスにデータインターフェイスを使用する場合でも、管理インターフェイスの設定を変更する必要がある場合があります。Device Manager 接続に管理インターフェイスを使用していた場合は、Device Manager に再接続する必要があります。

- マネージャアクセス用のデータインターフェイス: 管理インターフェイスには、データインターフェイスに設定されたゲートウェイが必要です。デフォルトでは、管理インターフェイスは DHCP から IP アドレスとゲートウェイを受信します。DHCP からゲートウェイを受信しない場合 (たとえば、管理インターフェイスをネットワークに接続していない場合)、ゲートウェイはデフォルトでデータインターフェイスになり、何も設定する必要はありません。DHCP からゲートウェイを受信した場合は、代わりに管理インターフェイス

スに静的 IP アドレスを設定し、ゲートウェイをデータインターフェイスに設定する必要があります。

- マネージャアクセス用の管理インターフェイス：静的 IP アドレスを設定する場合は、デフォルトゲートウェイもデータインターフェイスではなく一意のゲートウェイに設定してください。DHCP を使用する場合は、DHCP からゲートウェイを正常に取得できると仮定して、何も設定する必要はありません。

ステップ 4 マネージャアクセスに使用する外部または内部以外のインターフェイスを含む追加のインターフェイスを設定する場合は、[デバイス (Device)] を選択し、[インターフェイス (Interface)] のサマリーのリンクをクリックします。

Management Center にデバイスを登録すると、Device Manager の他の構成は保持されません。

ステップ 5 [デバイス (Device)] [システム設定 (Device System Settings)] [中央管理 (Central Management)] [Management Center] [Management Center] [デバイス (Device)] [システム設定 (System Settings)] [中央管理 (Central Management)] [Management Center] の順に選択し、[続行 (Proceed)] をクリックして Management Center の管理を設定します。

ステップ 6 [Management Center/CDOの詳細 (Management Center/CDO Details)] を設定します。

図 7: Management Center/CDO の詳細

Configure Connection to Management Center or CDO


Provide details to register to the management center/CDO.

Management Center/CDO Details

Do you know the Management Center/CDO hostname or IP address?

Yes No


Threat Defense



10.89.5.16
fe80::6a87:c6ff:fea6:4c00/64

→

Management Center/CDO



10.89.5.35

Management Center/CDO Hostname or IP Address

10.89.5.35

Management Center/CDO Registration Key

●●●● 👁

NAT ID

Required when the management center/CDO hostname or IP address is not provided. We recommend always setting the NAT ID even when you specify the management center/CDO hostname or IP address.

11203

Connectivity Configuration

Threat Defense Hostname

1120-3

DNS Server Group

CustomDNSServerGroup ▼

Management Center/CDO Access Interface

Data Interface

Please select an interface ▼

Management Interface [View details](#)

CANCEL
CONNECT

- a) [Management Center/CDOのホスト名またはIPアドレスを知っていますか (Do you know the FMC hostname or IP address)] で、IP アドレスまたはホスト名を使用して Management Center に到達できる場合は [はい (Yes)] をクリックし、Management Center が NAT の背

後にあるか、パブリック IP アドレスまたはホスト名がない場合は[いいえ (No)] をクリックします。

双方向の SSL 暗号化通信チャネルを 2 台のデバイス間に確立するには、少なくとも 1 台以上のデバイス (Management Center または Threat Defense デバイス) に到達可能な IP アドレスが必要です。

- b) [はい (Yes)] を選択した場合は、**管理センター/CDO のホスト名/IP アドレス**を入力します。
- c) **Management Center/CDO 登録キー**を指定します。

このキーは、Threat Defense デバイスを登録するとき Management Center でも指定する任意の 1 回限りの登録キーです。登録キーは 37 文字以下にする必要があります。有効な文字には、英数字 (A~Z、a~z、0~9)、およびハイフン (-) があります。この ID は、Management Center に登録する複数のデバイスに使用できます。
- d) [NAT ID] を指定します。

この ID は、Management Center でも指定する任意の 1 回限りの文字列です。いずれかのデバイスの IP アドレスのみを指定する場合、このフィールドは必須です。両方のデバイスの IP アドレスがわかっている場合でも、NAT ID を指定することを推奨します。NAT ID は 37 文字以下にする必要があります。有効な文字には、英数字 (A~Z、a~z、0~9)、およびハイフン (-) があります。この ID は、Management Center に登録する他のデバイスには使用できません。NAT ID は、正しいデバイスからの接続であることを確認するために IP アドレスと組み合わせて使用されます。IP アドレス/NAT ID の認証後にのみ、登録キーがチェックされます。

ステップ 7 [接続の設定 (Connectivity Configuration)] を設定します。

- a) [FTDホスト名 (FTD Hostname)] を指定します。

Management Center/CDO アクセスインターフェイスのアクセスにデータインターフェイスを使用する場合、この FQDN がこのインターフェイスに使用されます。

- b) [DNSサーバーグループ (DNS Server Group)] を指定します。

既存のグループを選択するか、新しいグループを作成します。デフォルトの DNS グループは **CiscoUmbrellaDNSServerGroup** と呼ばれ、OpenDNS サーバーが含まれます。

Management Center/CDO アクセスインターフェイスにデータインターフェイスを選択する場合は、この設定でデータインターフェイス DNS サーバーを設定します。セットアップウィザードで設定した管理 DNS サーバーは、管理トラフィックに使用されます。データ DNS サーバーは、DDNS (設定されている場合) またはこのインターフェイスに適用されるセキュリティポリシーに使用されます。管理トラフィックとデータトラフィックの両方が外部インターフェイス経由で DNS サーバーに到達するため、管理に使用したのと同じ DNS サーバーグループを選択する可能性があります。

Management Center では、この Threat Defense デバイスに割り当てるプラットフォーム設定ポリシーでデータインターフェイス DNS サーバーが設定されます。Management Center に Threat Defense デバイスを追加すると、ローカル設定が維持され、DNS サーバーはプラットフォーム設定ポリシーに追加されません。ただし、DNS 設定を含む Threat Defense デバ

イスに後でプラットフォーム設定ポリシーを割り当てると、その設定によってローカル設定が上書きされます。Management Center と Threat Defense デバイスを同期させるには、この設定に一致するように DNS プラットフォーム設定をアクティブに設定することをお勧めします。

また、ローカル DNS サーバーは、DNS サーバーが初期登録で検出された場合にのみ Management Center で保持されます。

FMC アクセスインターフェイスに管理インターフェイスを選択する場合は、この設定で管理 DNS サーバーを構成します。

- c) **Management Center/CDO アクセスインターフェイス**については、任意の構成済みインターフェイスを選択してください。

管理インターフェイスは、Threat Defense デバイスを Management Center に登録した後に、管理インターフェイスまたは別のデータインターフェイスのいずれかに変更できます。

- ステップ 8** (任意) 外部インターフェイスではないデータインターフェイスを選択した場合は、デフォルトルートを追加します。

インターフェイスを通過するデフォルトルートがあることを確認するように求めるメッセージが表示されます。外部を選択した場合は、セットアップウィザードの一環としてこのルートがすでに設定されています。別のインターフェイスを選択した場合は、Management Center に接続する前にデフォルトルートを手動で設定する必要があります。

管理インターフェイスを選択した場合は、この画面に進む前に、ゲートウェイを一意的ゲートウェイとして設定する必要があります。

- ステップ 9** (任意) データインターフェイスを選択した場合は、[ダイナミック DNS (DDNS) 方式の追加 (Add a Dynamic DNS (DDNS) method)]をクリックします。

DDNS は、IP アドレスが変更された場合に Management Center が完全修飾ドメイン名 (FQDN) で Threat Defense デバイスに到達できるようにします。[デバイス (Device)]>[システム設定 (System Settings)]>[DDNS サービス (DDNS Service)]を参照して DDNS を設定します。

Management Center に Threat Defense デバイスを追加する前に DDNS を設定すると、Threat Defense デバイスは、Cisco Trusted Root CA バンドルからすべての主要 CA の証明書を自動的に追加し、Threat Defense デバイスが HTTPS 接続のために DDNS サーバー証明書を検証できるようにします。Threat Defense は、DynDNS リモート API 仕様

(<https://help.dyn.com/remote-access-api/>) を使用するすべての DDNS サーバーをサポートします。

マネージャアクセスに管理インターフェイスを使用する場合、DDNS はサポートされません。

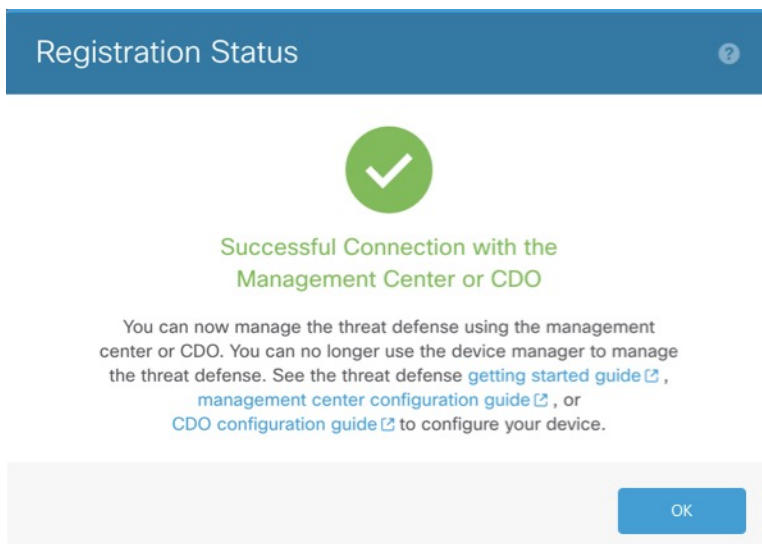
- ステップ 10** [接続 (Connect)]をクリックします。[登録ステータス (Registration Status)]ダイアログボックスには、Management Center への切り替えに関する現在のステータスが表示されます。[Management Center/CDO 登録設定の保存 (Saving Management Center/CDO Registration Settings)]のステップの後、Management Center に移動してファイアウォールを追加します。

Management Center への切り替えをキャンセルする場合は、[登録のキャンセル (Cancel Registration)]をクリックします。キャンセルしない場合は、[Management Center/CDO 登録設

定の保存 (Saving Management Center/CDO Registration Settings)]のステップが完了するまで Device Manager のブラウザウィンドウを閉じないでください。閉じた場合、プロセスは一時停止し、Device Manager に再接続した場合のみ再開されます。

[Management Center/CDO登録設定の保存 (Saving Management Center/CDO Registration Settings)]のステップの後に Device Manager に接続したままにする場合、その後 [Management CenterまたはCDOとの正常接続 (Successful Connection with Management Center or CDO)]ダイアログボックスが表示され、Device Manager から切断されます。

図 8: 正常接続



CLI を使用した Threat Defense 初期設定の実行の完了

Threat Defense CLI に接続して初期設定を実行します。これには、セットアップウィザードを使用した管理 IP アドレス、ゲートウェイ、およびその他の基本ネットワーク設定の指定などが含まれます。専用の管理インターフェイスは、独自のネットワーク設定を持つ特別なインターフェイスです。マネージャアクセスに管理インターフェイスを使用しない場合は、代わりに CLI を使用してデータインターフェイスを設定できます。また、Management Center 通信の設定を行います。Device Manager を使用して初期セットアップを実行すると、管理インターフェイスおよびマネージャアクセスインターフェイスの設定に加えて、管理のために Management Center に切り替えたときに、Device Manager で完了したすべてのインターフェイス構成が保持されます。アクセスコントロールポリシーなどの他のデフォルト設定は保持されないことに注意してください。

始める前に

この手順は、Firepower 4100/9300 を除くすべてのモデルに適用されます。

手順

ステップ 1 コンソールポートから、または管理インターフェイスへの SSH を使用して、Threat Defense CLI に接続します。デフォルトで DHCP サーバーから IP アドレスが取得されます。ネットワーク設定を変更する場合は、切断されないようにコンソールポートを使用することを推奨します。

(Firepower 1000/2100、Cisco Secure Firewall 3100) コンソールポートは FXOS CLI に接続します。SSH セッションは Threat Defense CLI に直接接続します。

ステップ 2 ユーザー名 **admin** およびパスワード **Admin123** でログインします。

(Firepower 1000/2100、Cisco Secure Firewall 3100) コンソールポートで FXOS CLI に接続します。初めて FXOS にログインしたときは、パスワードを変更するよう求められます。このパスワードは、SSH の Threat Defense ログインにも使用されます。

(注) パスワードがすでに変更されていて、パスワードがわからない場合は、デバイスを再イメージ化してパスワードをデフォルトにリセットする必要があります。再イメージ化の手順については、『[FXOS troubleshooting guide](#)』 [英語] を参照してください。手順については、『[Reimage Guide](#)』 [英語] を参照してください。

例：

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: *****
Confirm new password: *****
Your password was updated successfully.

[...]

firepower#
```

ステップ 3 (Firepower 1000/2100、Cisco Secure Firewall 3100) コンソールポートで FXOS に接続した場合は、Threat Defense CLI に接続します。

connect ftd

例：

```
firepower# connect ftd
>
```

ステップ 4 Threat Defense に初めてログインすると、エンドユーザーライセンス契約書 (EULA) に同意し、SSH 接続を使用している場合は、管理者パスワードを変更するよう求められます。その後、CLI セットアップスクリプトが表示されます。

- (注) 設定をクリア (たとえば、イメージを再作成することにより) しないかぎり、CLI セットアップウィザードを繰り返すことはできません。ただし、これらの設定すべては、後から CLI で **configure network** コマンドを使用して変更できます。『[Threat Defense Command Reference](#)』 [英語] を参照してください。

デフォルト値または以前に入力した値がカッコ内に表示されます。以前に入力した値をそのまま使用する場合は、Enter を押します。

- (注) データインターフェイスでマネージャアクセスを有効にした場合でも、管理インターフェイスの設定が使用されます。たとえば、データインターフェイスを介してバックプレーン経由でルーティングされる管理トラフィックは、データインターフェイス DNS サーバーではなく、管理インターフェイス DNS サーバーを使用して FQDN を解決します。

次のガイドラインを参照してください。

- [DHCP経由または手動でIPv4を設定しますか?]: 管理インターフェイスではなくデータインターフェイスをマネージャアクセスに使用する場合は、[手動]を選択します。管理インターフェイスを使用する予定がない場合でも、プライベートアドレスなどの IP アドレスを設定する必要があります。管理インターフェイスが DHCP に設定されている場合、管理用のデータインターフェイスを設定することはできません。これは、**data-interfaces** である必要があるデフォルトルートが DHCP サーバーから受信したルートで上書きされる可能性があるためです。
- [管理インターフェイスのIPv4デフォルトゲートウェイを入力]: 管理インターフェイスではなくデータインターフェイスをマネージャアクセスに使用する場合は、ゲートウェイを [data-interfaces] に設定します。この設定は、マネージャアクセス データ インターフェイスを通じて回送できるように、バックプレーンを介して管理トラフィックを転送します。マネージャアクセスに管理インターフェイスを使用する場合は、管理 1/1 ネットワークでゲートウェイ IP アドレスを設定する必要があります。
- ネットワーク情報が変更された場合は再接続が必要: SSH で接続しているのに、初期セットアップでその IP アドレスを変更すると、接続が切断されます。新しい IP アドレスとパスワードで再接続してください。コンソール接続は影響を受けません。
- [デバイスをローカルで管理しますか (Manage the device locally?)]: Management Center を使用するには「no」を入力します。「yes」と答えると、代わりに Firepower Device Manager を使用することになります。
- [ファイアウォールモードを設定しますか (Configure firewall mode?)]: 初期設定でファイアウォールモードを設定することをお勧めします。初期設定後にファイアウォールモードを変更すると、実行コンフィギュレーションが消去されます。データ インターフェイス マネージャ アクセスは、ルーテッドファイアウォールモードでのみサポートされることに注意してください。

例:

```
You must accept the EULA to continue.  
Press <ENTER> to display the EULA:
```

```

End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress. Please stand by.
You must change the password for 'admin' to continue.
Enter new password: *****
Confirm new password: *****
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...

Update policy deployment information
- add device configuration
- add network discovery
- add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required. In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>

```

ステップ 5 この Threat Defense を管理する Management Center を特定します。

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} reg_key [nat_id]
[display_name]
```

(注) 管理に CDO を使用している場合は、このステップで CDO が生成した **configure manager add** コマンドを使用します。

- `{hostname | IPv4_address | IPv6_address | DONTRESOLVE}`—Specifies either the FQDN or IP address of the Management Center. Management Center を直接アドレス指定できない場合は、**DONTRESOLVE** を使用します。また、`nat_id` も指定します。双方向の SSL 暗号化通信チャンネルを2台のデバイス間に確立するには、少なくとも1台以上のデバイス（Management Center または Threat Defense）に到達可能な IP アドレスが必要です。このコマンドで **DONTRESOLVE** を指定するには、FTD には到達可能な IP アドレスまたはホスト名が必要です。
- `reg_key` : Threat Defense を登録するときに Management Center でも指定する任意のワンタイム登録キーを指定します。登録キーは 37 文字以下にする必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。
- `nat_id` : 一方の側で到達可能な IP アドレスまたはホスト名が指定されていない場合は、Threat Defense を登録するときに Management Center にも指定する任意の一意のワンタイム文字列を指定します。この文字列は、Management Center を **DONTRESOLVE** に設定した場合に必要です。NAT ID は 37 文字以下にする必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。この ID は、Management Center に登録する他のデバイスには使用できません。
 - (注) 管理にデータインターフェイスを使用する場合は、登録用に Threat Defense と Management Center の両方で NAT ID を指定する必要があります。
- `display_name` : `show managers` コマンドでこのマネージャを表示するための表示名を指定します。このオプションは、CDO をプライマリマネージャおよび分析専用のオンプレミス Management Center として識別する場合に役立ちます。この引数を指定しない場合、ファイアウォールは以下のいずれかの方法を使用して表示名を自動生成します。
 - `hostname | IP_address` (**DONTRESOLVE** キーワードを使用しない場合)
 - `manager-timestamp`

例 :

```
> configure manager add MC.example.com 123456
Manager successfully configured.
```

例 :

Management Center が NAT デバイスの背後にある場合は、次の例に示すように、一意の NAT ID とともに登録キーを入力し、ホスト名の代わりに **DONTRESOLVE** を指定します。

```
> configure manager add DONTRESOLVE regk3y78 natid90
Manager successfully configured.
```

例 :

Threat Defense が NAT デバイスの背後にある場合は、次の例に示すように、一意の NAT ID とともに Management Center IP アドレスまたはホスト名を入力します。

```
> configure manager add 10.70.45.5 regk3y78 natid56
Manager successfully configured.
```

ステップ 6 プライマリマネージャとして CDO を使用していて、オンプレミス Management Center を分析のみに使用する場合は、オンプレミス Management Center を特定します。

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} reg_key [nat_id] [display_name]
```

例 :

次の例では、CDO 用に生成されたコマンドに「CDO」という表示名を追加し、分析専用のオンプレミス Management Center を指定しています。

```
> configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
LzmlHOynhVUWhXYWz2swmkj2ZWsn3Lb account1.app.us.cdo.cisco.com
Manager successfully configured.
> configure manager add 10.70.45.5 regk3y78 natid56 analytics-FMC
Manager successfully configured.
```

ステップ 7 (任意) マネージャアクセス用のデータインターフェイスを設定します。

configure network management-data-interface

その後、データインターフェイスの基本的なネットワーク設定を行うように求めるプロンプトが表示されます。

(注) このコマンドを使用する場合は、コンソールポートを使用する必要があります。管理インターフェイスに SSH を使用すると、接続が切断され、コンソールポートに再接続する必要があります。SSH の詳細な使用方法については、次を参照してください。

このコマンドの使用については、次の詳細を参照してください。[管理のための Threat Defense データインターフェイスの使用について \(4 ページ\)](#) も参照してください。

- データインターフェイスを管理に使用する場合、元の管理インターフェイスは DHCP を使用できません。初期セットアップ時に IP アドレスを手動で設定しなかった場合は、**configure network {ipv4 | ipv6} manual** コマンドを使用して設定できるようになりました。管理インターフェイスゲートウェイを **data-interfaces** に設定しなかった場合は、ここでこのコマンドで設定します。
- Threat Defense を Management Center に追加すると、Management Center はインターフェイス設定 (インターフェイス名と IP アドレス、ゲートウェイへの静的ルート、DNS サーバー、DDNS サーバーなど) を検出して維持します。DNS サーバー設定の詳細については、次を参照してください。Management Center では、後でマネージャアクセスインターフェイス構成を変更できますが、Threat Defense または Management Center が管理接続の再確立を妨げるような変更を加えないようにしてください。管理接続が中断された場合、Threat Defense には以前の展開を復元する **configure policy rollback** コマンドが含まれません。
- DDNS サーバー更新の URL を設定すると、Threat Defense は Cisco Trusted Root CA バンドルからすべての主要 CA の証明書を自動的に追加するため、Threat Defense は HTTPS 接続の DDNS サーバー証明書を検証できます。Threat Defense は、DynDNS リモート API 仕様 (<https://help.dyn.com/remote-access-api/>) を使用するすべての DDNS サーバーをサポートします。

- このコマンドは、「データ」インターフェイス DNS サーバーを設定します。セットアップスクリプトで（または **configure network dns servers** コマンドを使用して）設定した管理 DNS サーバーは、管理トラフィックに使用されます。データ DNS サーバーは、DDNS（設定されている場合）またはこのインターフェイスに適用されるセキュリティポリシーに使用されます。

Management Center では、この Threat Defense に割り当てるプラットフォーム設定ポリシーでデータインターフェイス DNS サーバーが設定されます。Management Center に Threat Defense を追加すると、ローカル設定が維持され、DNS サーバーはプラットフォーム設定ポリシーに追加されません。ただし、DNS 設定を含む Threat Defense に後でプラットフォーム設定ポリシーを割り当てると、その設定によってローカル設定が上書きされます。

Management Center と Threat Defense を同期させるには、この設定に一致するように DNS プラットフォーム設定をアクティブに設定することをお勧めします。

また、ローカル DNS サーバーは、DNS サーバーが初期登録で検出された場合にのみ Management Center で保持されます。たとえば、管理インターフェイスを使用してデバイスを登録し、後で **configure network management-data-interface** コマンドを使用してデータインターフェイスを設定した場合、FTD 設定と一致するように、DNS サーバーを含むこれらの設定すべてを Management Center で手動で設定する必要があります。

- 管理インターフェイスは、Threat Defense を Management Center に登録した後に、管理インターフェイスまたは別のデータインターフェイスのいずれかに変更できます。
- セットアップウィザードで設定した FQDN がこのインターフェイスに使用されます。
- コマンドの一部としてデバイス設定全体をクリアできます。このオプションはリカバリシナリオで使用できますが、初期セットアップや通常の操作には使用しないでください。
- データ管理を無効にするには、**configure network management-data-interface disable** コマンドを入力します。

例：

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://jcrichon:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

例：

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
```

```
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

ステップ 8 (任意) 特定のネットワーク上のマネージャへのデータ インターフェイス アクセスを制限します。

```
configure network management-data-interface client ip_address netmask
```

デフォルトでは、すべてのネットワークが許可されます。

次のタスク

デバイスを Management Center に登録します。

Management Center 管理インターフェイスの変更



注意 Threat Defense で直接終端する VPN トンネル経由で Management Center 展開をプッシュしないでください。Management Center 展開をプッシュすると、トンネルが非アクティブ化され、Management Center と Threat Defense が切断される可能性があります。

この状況からデバイスを回復すると、中断時間が長くなり、ディザスタリカバリ手順の実行が必要になる場合があります。この手順では、マネージャを Management Center からローカルに変更し、デバイスを最初から設定することで、Threat Defense を工場出荷時のデフォルト設定にリセットします。詳細については、『[Firepower Management Center Device Configuration Guide](#)』の「*Best Practices for Deploying Configuration Changes*」を参照してください。

Management Center で管理インターフェイスの設定を変更します。オプションとして追加の管理インターフェイスを有効にしたり、イベントのみのインターフェイスを設定したりできます。



注意 接続されている管理インターフェイスを変更する場合は十分にご注意ください。設定エラーのために再接続できない場合は、Management Center コンソールポートにアクセスして、Linux シェルでネットワーク設定を再設定する必要があります。この操作では、Cisco TAC に連絡する必要があります。



(注) Management Center の IP アドレスを変更する場合は、[Cisco Secure Firewall Management Center デバイス構成ガイド](#) で。Management Center の IP アドレスまたはホスト名を変更する場合は、設定が一致するようにデバイス CLI で値を変更する必要があります。ほとんどの場合、管理接続はデバイスの Management Center IP アドレスまたはホスト名を変更せずに再確立されますが、少なくともデバイスを Management Center に追加して NAT ID のみを指定した場合は、接続が再確立されるようにするために、このタスクを実行する必要があります。他の場合でも、Management Center IP アドレスまたはホスト名を最新の状態に維持して、ネットワークの復元力を高めることを推奨します。



(注) ハイアベイラビリティ構成では、登録された Firepower デバイスの管理 IP アドレスをデバイスの CLI または Management Center から変更した場合、HA 同期後も、セカンダリ Management Center には変更が反映されません。セカンダリ Management Center も更新されるようにするには、2つの Management Center の間でロールを切り替えて、セカンダリ Management Center をアクティブユニットにします。現在アクティブな Management Center のデバイス管理のページで、登録されている Firepower デバイスの管理 IP アドレスを変更します。

始める前に

- デバイス管理の仕組みについては、[Cisco Secure Firewall Management Center デバイス構成ガイド](#)で
- プロキシを使用する場合：
 - NT LAN Manager (NTLM) 認証を使用するプロキシはサポートされません。
 - スマートライセンスを使用しているか、または使用する予定がある場合は、プロキシの FQDN は 64 文字以内にする必要があります。

手順

ステップ 1 システム (⚙️) > [構成 (Configuration)] を選択し、次に [管理インターフェイス (Management Interfaces)] を選択します。



ステップ 2 [インターフェイス (Interfaces)] エリアで、設定するインターフェイスの横にある [編集 (Edit)] をクリックします。


このセクションでは、利用可能なすべてのインターフェイスがリストされます。インターフェイスをさらに追加することはできません。

それぞれの管理インターフェイスに対して、以下のオプションを設定できます。

- [有効にする (Enabled)] : 管理インターフェイスを有効にします。デフォルト eth0 管理インターフェイスを無効にしないでください。eth0 インターフェイスを必要とするプロセスもあります。
- [チャンネル (Channels)] : [管理トラフィック (Management Traffic)] が有効になっているインターフェイスが常に少なくとも1つ必要です。必要に応じて、イベント専用インターフェイスを設定できます。Management Center で設定できるイベントインターフェイスは1つだけです。これを設定するには、[管理トラフィック (Management Traffic)] チェックボックスをオフにして、[イベントトラフィック (Event Traffic)] チェックボックスをオンのままにしておきます。必要に応じて、管理インターフェイスの [イベントトラフィック (Event Traffic)] を無効にすることができます。いずれの場合も、デバイスは、イベントのみのインターフェイスにイベントを送信しようとしています。そのインターフェイスがダウンしていた場合は、イベントチャンネルが無効になっていても、管理インターフェイス上でイベントを送信します。インターフェイス上でイベントチャンネルと管理チャンネルの両方を無効にすることはできません。
- [モード (Mode)] : リンク モードを指定します。GigabitEthernet インターフェイスでは、自動ネゴシエーションの値を変更しても反映されないことに注意してください。
- [MDI/MDIX] : [自動-MDIX (Auto-MDIX)] を設定します。
- [MTU] : 1280 ~ 1500 の最大伝送ユニット (MTU) を設定します。デフォルトは 1500 です。
- [IPv4 設定 (IPv4 Configuration)] : IPv4 IP アドレスを設定します。次のどちらかを選択します。
 - [スタティック (Static)] : **IPv4 の管理 IP アドレス と ネットマスク**を手動で入力します。
 - [DHCP] : DHCP を使用するインターフェイスを設定します (eth0 のみ) 。
 - [無効 (Disabled)] : 無効 IPv4。IPv4 と IPv6 の両方を無効にしないでください。
- [IPv6 設定 (IPv6 Configuration)] : IPv6 IP アドレスを設定します。次のどちらかを選択します。
 - [スタティック (Static)] : **IPv6 の管理 IP アドレス と IPv6 のプレフィックス長**を手動で入力します。
 - [DHCP] : DHCPv6 を使用するインターフェイスを設定します (eth0 のみ) 。
 - [ルータ割当て (Router Assigned)] : ステータス自動設定を有効にします。
 - [無効 (Disabled)] : IPv6 を無効にします。IPv4 と IPv6 の両方を無効にしないでください。

- [IPv6 DAD] : IPv6 を有効にするときに [重複アドレス検出 (DAD)] を有効または無効にします。DAD を使用することによってサービス拒否攻撃の可能性が拡大するため、DAD は無効にすることができます。この設定を無効にした場合は、すでに割り当てられているアドレスがこのインターフェイスで使用されていないことを手動で確認する必要があります。

ステップ 3 [ルート (Routes)] エリアで、静的ルートを [編集 (Edit)] () をクリックして編集するか、または **Add** () をクリックして追加します。

 をクリックしてルートテーブルを表示します。

追加の各インターフェイスがリモート ネットワークに到達するには、スタティック ルートが必要です。新しいルートが必要な場合については、[Management Center 管理インターフェイス上のネットワーク ルート \(7 ページ\)](#) を参照してください。

(注) デフォルト ルートでは、ゲートウェイ IP アドレスのみを変更できます。出力インターフェイスは、指定したゲートウェイをインターフェイスのネットワークに照合することで自動的に選択されます。

次の設定をスタティック ルートに対して設定できます。

- [宛先 (Destination)] : ルートを作成する宛先ネットワークのアドレスを設定します。
- [ネットマスク (Netmask)] または [プレフィックス長 (Prefix Length)] : ネットワークのネットマスク (IPv4) またはプレフィックス長 (IPv6) を設定します。
- [インターフェイス (Interface)] : 出力管理インターフェイスを設定します。
- [ゲートウェイ (Gateway)] : ゲートウェイ IP アドレスを設定します。

ステップ 4 [共有設定 (Shared Settings)] エリアで、すべてのインターフェイスで共有されているネットワーク パラメータを設定します。

(注) eth0 インターフェイスで [DHCP] を選択すると、DHCP サーバから取得する共有設定の一部を手動で指定できなくなります。

次の共有設定を行うことができます。

- [ホスト名 (Hostname)] : Management Center ホスト名を設定します。ホスト名は最大 64 文字を使用でき、アルファベットまたは数字で開始および終了する必要があります。使用できるのはアルファベット、数字、ハイフンのみです。ホスト名を変更する場合、syslog メッセージに反映される新しいホスト名を使用するには、Management Center を再起動します。再起動するまでは、新しいホスト名が Syslog メッセージに反映されません。
- [ドメイン (Domains)] : カンマで区切られた、Management Center の検索ドメインを設定します。これらのドメインは、コマンド (**ping system** など) に完全修飾ドメイン名を指定しない場合にホスト名に追加されます。ドメインは、管理インターフェイスまたは管理インターフェイスを経由するコマンドでのみ、使用されます。

- [プライマリ DNS サーバー (Primary DNS Server)]、[セカンダリ DNS サーバー (Secondary DNS Server)]、[ターシャリ DNS サーバー (Tertiary DNS Server)] : 優先度順に使用される DNS サーバーを設定します。
- [リモート管理ポート (Remote Management Port)] : 管理対象デバイスとの通信用のリモート管理ポートを設定します。Management Center および管理対象デバイスは、双方向の SSL 暗号化通信チャネル (デフォルトではポート 8305) を使用して通信します。
 - (注) シスコは、リモート管理ポートをデフォルト設定のままにしておくことを強く推奨していますが、管理ポートがネットワーク上の他の通信と競合する場合は、別のポートを選択できます。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デバイスの管理ポートを変更する必要があります。

ステップ 5 [ICMPv6] 領域で、ICMPv6 の設定を行います。

- [エコー応答パケットの送信を許可する (Allow Sending Echo Reply Packets)] : エコー応答パケットを有効または無効にします。これらのパケットを無効にすることで、サービス拒否攻撃の可能性から保護します。エコー応答パケットを無効にすると、Management Center の管理インターフェイスにテスト目的で IPv6 ping を使用できなくなります。
- [宛先到達不能パケットの送信を許可する (Allow Sending Destination Unreachable Packets)] : 宛先到達不能パケットを有効または無効にします。これらのパケットを無効にすることで、サービス拒否攻撃の可能性から保護します。

ステップ 6 [プロキシ (Proxy)] エリアで、HTTP プロキシ設定をします。

Management Center は、ポート TCP/443 (HTTPS) および TCP/80 (HTTP) でインターネットに直接接続するように構成されています。HTTP ダイジェスト経由で認証できるプロキシサーバーを使用できます。

このトピックの前提条件のプロキシの要件を参照してください。

- [有効 (Enabled)] チェックボックスをオンにします。
- [HTTP プロキシ (HTTP Proxy)] フィールドに、プロキシサーバの IP アドレスまたは完全修飾ドメイン名を入力します。

このトピックの前提条件の要件を参照してください。

- [ポート (Port)] フィールドに、ポート番号を入力します。
- [プロキシ認証の使用 (Use Proxy Authentication)] を選択してから [ユーザ名 (User Name)] と [パスワード (Password)] を入力して、認証資格情報を設定します。

ステップ 7 [保存 (Save)] をクリックします。

ステップ 8 Management Center の IP アドレスを変更する場合は、Management Center の IP アドレスを変更する場合は、[Cisco Secure Firewall Management Center デバイス構成ガイド](#)で。

Management Center の IP アドレスまたはホスト名を変更する場合は、設定が一致するようにデバイス CLI で値を変更する必要があります。ほとんどの場合、管理接続はデバイスの Management Center IP アドレスまたはホスト名を変更せずに再確立されますが、少なくともデバイスを

Management Center に追加して NAT ID のみを指定した場合は、接続が再確立されるようにするために、このタスクを実行する必要があります。他の場合でも、Management Center IP アドレスまたはホスト名を最新の状態に維持して、ネットワークの復元力を高めることを推奨します。

Threat Defense 管理インターフェイスの変更

Management Center でのホスト名または IP アドレスの更新

(デバイスの CLI を使用するなどして) デバイスを Management Center に追加した後にそのデバイスのホスト名または IP アドレスを編集する場合は、次の手順を使用して管理側の Management Center のホスト名または IP アドレスを手動で更新する必要があります。

Threat Defense 機能の履歴 :

- 7.3 : 冗長マネージャ アクセス データ インターフェイス

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 管理オプションを変更するデバイスの横にある [編集 (Edit)] (✎) 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 [Device] をクリックし、[Management] 領域を表示します。


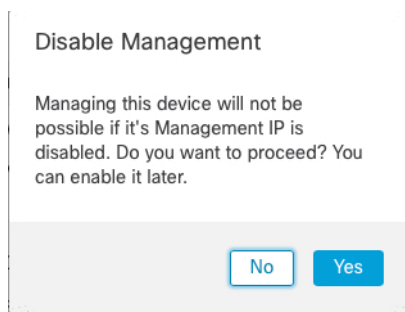
ステップ 4 スライダをクリックして管理を一時的に無効にすることで、() を無効化します。

図 9: 管理を無効にする



管理の無効化を続行するように求められます。[Yes] をクリックします。



管理を無効化すると、Management Center とデバイス間の接続がブロックされますが、Management Center からデバイスは削除されません。

ステップ 5 [リモートホストアドレス (Remote Host Address)] の IP アドレスおよびオプションの [セカンダリアドレス (Secondary Address)] (冗長データインターフェイスを使用する場合) または [編集 (Edit)] (✎) をクリックしてホスト名を編集します。

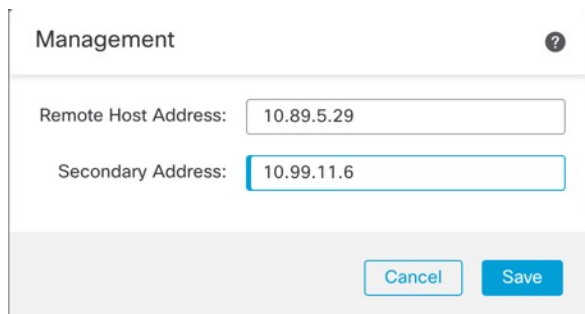
図 10: 管理アドレスの編集



ステップ 6 [管理 (Management)] ダイアログボックスの [リモートホストアドレス (Remote Host Address)] フィールドおよびオプションの [セカンダリアドレス (Secondary Address)] フィールドで名前または IP アドレスを変更し、[保存 (Save)] をクリックします。

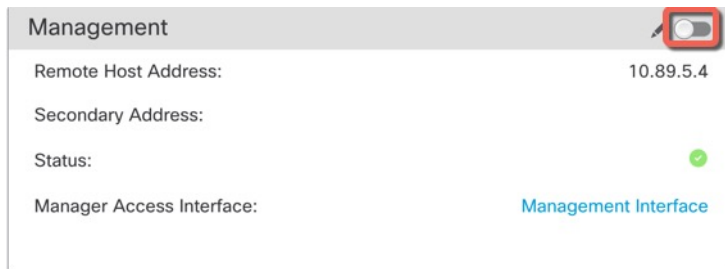
セカンダリ マネージャ アクセス データ インターフェイスの使用については、[冗長マネージャ アクセス用データインターフェイスの設定 \(40 ページ\)](#) を参照してください。

図 11: 管理 IP アドレス



ステップ 7 スライダを有効にして管理を再度有効 (☑) にします。

図 12: 管理接続の有効化



管理アクセスインターフェイスの管理からデータへの変更

専用の管理インターフェイスまたはデータインターフェイスから Threat Defense を管理できます。デバイスを Management Center に追加した後にマネージャアクセスインターフェイスを変更する場合は、次の手順に従って管理インターフェイスからデータインターフェイスに移行します。逆の方向に移行するには、[マネージャアクセスインターフェイスをデータから管理に変更する \(37 ページ\)](#) を参照してください。

管理からデータへのマネージャアクセスの移行を開始すると、Management Center は Threat Defense への展開時にブロックを適用します。ブロックを削除するには、データインターフェイスでマネージャアクセスを有効にします。

次の手順を参照して、データインターフェイスでマネージャアクセスを有効にし、その他の必要な設定も構成します。

手順

ステップ 1 インターフェイスの移行を開始します。

- [デバイス (Devices)] > [デバイス管理 (Device Manage)] ページで、デバイスの [編集 (Edit)] (✎) をクリックします。
- [デバイス (Device)] > [管理 (Management)] セクションに移動し、[マネージャアクセスインターフェイス (Manager Access Interface)] [FMCアクセスインターフェイス (FMC Access Interface)] のリンクをクリックします。 >

[マネージャアクセスインターフェイス (Manager Access Interface)] [FMCアクセスインターフェイス (FMC Access Interface)] フィールドには、現在の管理インターフェイスが表示されます。リンクをクリックしたら、[デバイスの管理 (Manage device by)] ドロップダウンリストで新しいインターフェイスタイプである [データインターフェイス (Data Interface)] を選択します。

図 13: マネージャ アクセス インターフェイス

Manager Access Interface

This is an advanced setting and need to be configured only if needed.
See the [online help](#) for detailed steps.

Manage device by

Data Interface

Switching the manager access interface from Management to Data interface causes the deployment to be blocked. To unblock the deploy, pick a data interface and enable it for manager Access. See the [online help](#) for detailed steps.

Close Save

- c) [保存 (Save)] をクリックします。

データインターフェイスでマネージャアクセスを有効にするには、残りの手順を完了する必要があります。[管理 (Management)] 領域には、[マネージャ アクセス インターフェイス : データインターフェイス (Manager Access Interface: Management Interface)] [FMC アクセスインターフェイス : データインターフェイス (FMC Access Interface: Management Interface)] と、[マネージャアクセスの詳細 : 構成 (Manager Access Details: Configuration)] [FMCアクセスの詳細 : 構成 (FMC Access Details: Configuration)] が表示されます。

図 14: マネージャアクセス

Management

Remote Host Address: 10.10.1.12

Secondary Address:

Status:

Manager Access Interface: Data Interface

Manager Access Details: Configuration

[構成 (Configuration)] をクリックすると、[マネージャアクセス - 構成の詳細 (Manager Access - Configuration Details)] [FMCアクセス - 構成の詳細 (FMC Access - Configuration Details)] ダイアログボックスが開きます。[マネージャアクセスモード (Manager Access Mode)] [FMCアクセスモード (FMC Access Mode)] は、展開保留状態を示しています。

ステップ 2 [デバイス (Devices)]>[デバイス管理 (Device Management)]>[インターフェイス (Interfaces)]>[物理インターフェイスの編集 (Edit Physical Interface)]>[マネージャアクセス (Manager Access)] [FMCアクセス (FMC Access)] ページで、データインターフェイスでのマネージャアクセスを有効にします。 > > > >

マネージャアクセスは1つのルーテッドデータ インターフェイスとオプションのセカンダリ インターフェイスで有効にできます。これらのインターフェイスが名前と IP アドレスで完全に構成され、有効になっていることを確認してください。

冗長性のためにセカンダリインターフェイスを使用する場合は、必要な追加構成について[冗長マネージャアクセス用データインターフェイスの設定 \(40 ページ\)](#)を参照してください。

ステップ 3 (任意) インターフェイスに DHCP を使用する場合は、[デバイス (Devices)]>[デバイス管理 (Device Management)]>[DHCP]>[DDNS]ページで Web タイプ DDNS 方式を有効にします。

DDNS は、FTD の IP アドレスが変更された場合に Management Center が完全修飾ドメイン名 (FQDN) で Threat Defense に到達できるようにします。

ステップ 4 Threat Defense がデータインターフェイスを介して Management Center にルーティングできることを確認します。必要に応じて、[デバイス (Devices)]>[デバイス管理 (Device Management)]>[ルーティング (Routing)]>[スタティックルート (Static Route)]でスタティックルートを追加します。 > > >

ステップ 5 (任意) プラットフォーム設定ポリシーで DNS を構成し、[デバイス (Devices)]>[プラットフォーム設定 (Platform Settings)]>[DNS]でこのデバイスに適用します。

DDNS を使用する場合は DNS が必要です。セキュリティポリシーで FQDN に DNS を使用することもできます。

ステップ 6 (任意) プラットフォーム設定ポリシーでデータインターフェイスの SSH を有効にし、[デバイス (Devices)]> [プラットフォーム設定 (Platform Settings)]>[セキュアシェル (Secure Shell)]でこのデバイスに適用します。

SSH はデータインターフェイスでデフォルトで有効になっていないため、SSH を使用して Threat Defense を管理する場合は、明示的に許可する必要があります。

ステップ 7 設定変更を展開します。

Management Center は、現在の管理インターフェイスを介して設定の変更を展開します。展開後、データインターフェイスを使用できるようになりましたが、管理への元の管理接続はアクティブなままです。

ステップ 8 Threat Defense CLI (できればコンソールポートから) で、静的 IP アドレスを使用するように管理インターフェイスを設定し、データインターフェイスを使用するようにゲートウェイを設定します。

configure network {ipv4 | ipv6} manual ip_address netmask data-interfaces

- *ip_address netmask* : 管理インターフェイスを使用する予定はありませんが、ゲートウェイを [データインターフェイス (data-interfaces)] に設定できるように、プライベートアドレスなどの静的 IP アドレスを設定する必要があります (次の箇条書きを参照) 。

[data-interfaces] である必要があるデフォルトルートは、DHCP サーバーから受信したルートで上書きされる可能性があるため、DHCP は使用できません。

- **data-interfaces** — この設定は、マネージャ アクセス データ インターフェイスを通じて回送できるように、バックプレーンを介して管理トラフィックを転送します。

管理インターフェイスのネットワーク設定を変更すると、SSHセッションが切断されるため、SSH 接続の代わりにコンソールポートを使用することをお勧めします。

ステップ 9 必要に応じて、データインターフェイスの Management Center に到達できるように Threat Defense のケーブルを再接続します。

ステップ 10 Management Center で、管理接続を無効にし、[デバイス (Devices)] > [デバイス管理 (Device Management)] > [デバイス (Device)] > [管理 (Management)] セクションで Threat Defense の [リモートホストアドレス (Remote Host Address)] IP アドレスとオプションの [セカンダリアドレス (Secondary Address)] を更新して、接続を再度有効にします。

Management Center でのホスト名または IP アドレスの更新 (31 ページ) を参照してください。Threat Defense を Management Center に追加したときに Threat Defense ホスト名または NAT ID のみを使用した場合は、値を更新する必要はありません。ただし、接続を再開するには、管理接続を無効にしてから再度有効にする必要があります。

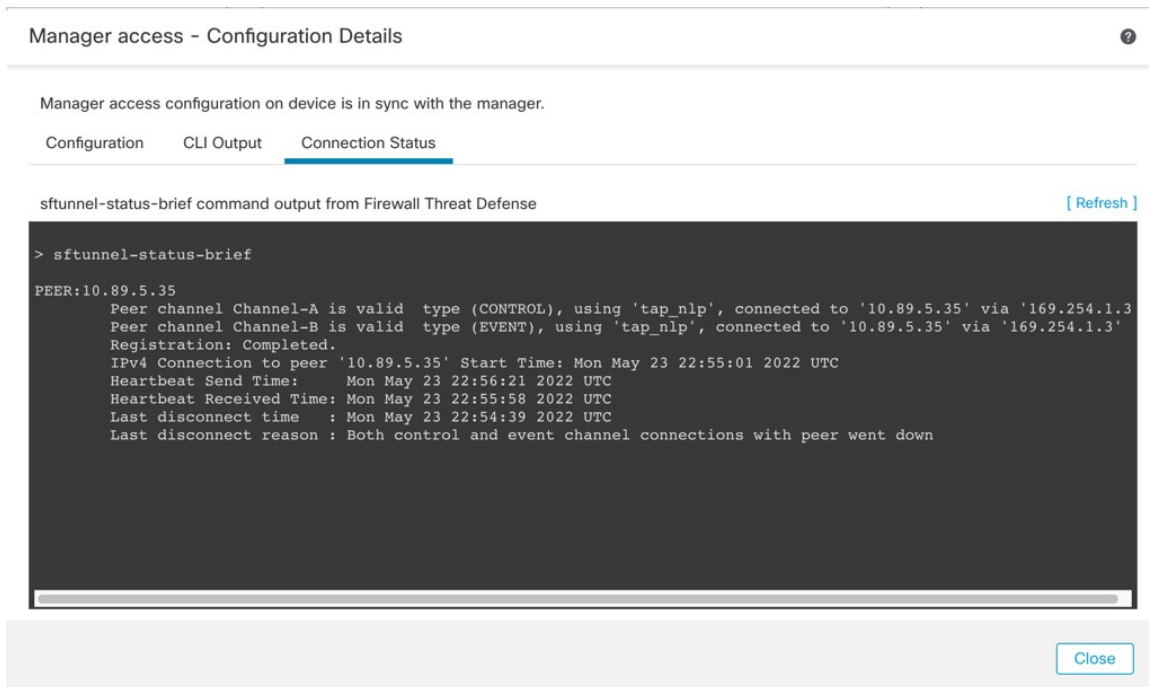
ステップ 11 管理接続が再確立されたことを確認します。

Management Center で、[Devices] [Device Management] [Device] [Management] [Manager Access - Configuration Details] [FMC Access - Configuration Details] [Connection Status] ページで管理接続ステータスを確認します。

管理接続のステータスを表示するには、Threat Defense CLI で、**sftunnel-status-brief** コマンドを入力します。

次のステータスは、データインターフェイスの接続が成功したことを示し、内部の「tap_nlp」インターフェイスを示しています。

図 15: 接続ステータス



Manager access - Configuration Details

Manager access configuration on device is in sync with the manager.

Configuration CLI Output **Connection Status**

sftunnel-status-brief command output from Firewall Threat Defense [Refresh]

```
> sftunnel-status-brief
PEER:10.89.5.35
Peer channel Channel-A is valid type (CONTROL), using 'tap_nlp', connected to '10.89.5.35' via '169.254.1.3'
Peer channel Channel-B is valid type (EVENT), using 'tap_nlp', connected to '10.89.5.35' via '169.254.1.3'
Registration: Completed.
IPv4 Connection to peer '10.89.5.35' Start Time: Mon May 23 22:55:01 2022 UTC
Heartbeat Send Time: Mon May 23 22:56:21 2022 UTC
Heartbeat Received Time: Mon May 23 22:55:58 2022 UTC
Last disconnect time : Mon May 23 22:54:39 2022 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

Close

接続の再確立に 10 分以上かかる場合は、接続のトラブルシューティングを行う必要があります。データインターフェイスでの管理接続のトラブルシューティング (61 ページ) を参照してください。

マネージャ アクセス インターフェイスをデータから管理に変更する

専用の管理インターフェイスまたはデータインターフェイスから Threat Defense を管理できます。デバイスを Management Center に追加した後にマネージャ アクセス インターフェイスを変更する場合は、次の手順に従ってデータインターフェイスから管理インターフェイスに移行します。逆の方向に移行するには、[管理アクセスインターフェイスの管理からデータへの変更 \(33 ページ\)](#) を参照してください。

データから管理へのマネージャアクセスの移行を開始すると、Management Center は Threat Defense への展開時にブロックを適用します。ブロックを削除するには、データインターフェイスでマネージャアクセスを無効にする必要があります。

次の手順を参照して、データインターフェイスでマネージャアクセスを無効にし、その他の必要な設定も構成します。

手順

ステップ 1 インターフェイスの移行を開始します。

- a) [デバイス (Devices)] > [デバイス管理 (Device Management)] ページで、デバイスの [編集 (Edit)] (✎) をクリックします。
- b) [デバイス (Device)] > [管理 (Management)] セクションに移動し、[マネージャアクセスインターフェイス (Manager Access Interface)] [FMCアクセスインターフェイス (FMC Access Interface)] のリンクをクリックします。 >

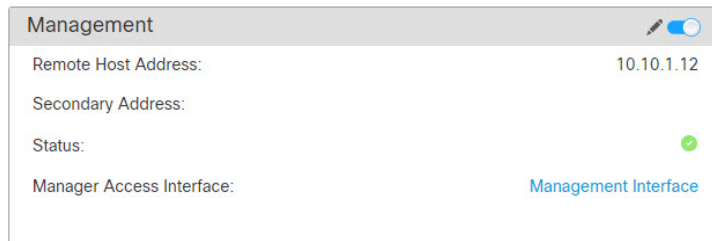
[マネージャアクセスインターフェイス (Manager Access Interface)] [FMCアクセスインターフェイス (FMC Access Interface)] フィールドには、現在の管理インターフェイスが表示されます。リンクをクリックしたら、[デバイスの管理 (Manage device by)] ドロップダウンリストで新しいインターフェイスタイプである [管理インターフェイス (Management Interface)] を選択します。

図 16: マネージャアクセスインターフェイス

- c) [保存 (Save)] をクリックします。

管理インターフェイスでマネージャアクセスを有効にするには、残りの手順を完了する必要があります。[管理 (Management)] 領域には、[マネージャアクセスインターフェイス: 管理インターフェイス (Manager Access Interface: Management Interface)] [FMCアクセスインターフェイス: 管理インターフェイス (FMC Access Interface: Management Interface)] と、[マネージャアクセスの詳細: 構成 (Manager Access Details: Configuration)] [FMCアクセスの詳細: 構成 (FMC Access Details: Configuration)] が表示されます。

図 17: マネージャアクセス



[構成 (Configuration)] をクリックすると、[マネージャアクセス - 構成の詳細 (Manager Access - Configuration Details)] [FMCアクセス - 構成の詳細 (FMC Access - Configuration Details)] ダイアログボックスが開きます。[マネージャアクセスモード (Manager Access Mode)] [FMCアクセスモード (FMC Access Mode)] は、展開保留状態を示しています。

ステップ 2 [デバイス (Devices)] > [デバイス管理 (Device Management)] > [インターフェイス (Interfaces)] > [物理インターフェイスの編集 (Edit Physical Interface)] > [マネージャアクセス (Manager Access)] ページで、データインターフェイスでのマネージャアクセスを無効にします。

この手順により、展開時のブロックが削除されます。

ステップ 3 まだ行っていない場合は、プラットフォーム設定ポリシーでデータインターフェイスの DNS 設定を構成し、[デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] > [DNS] でこのデバイスに適用します。

データインターフェイスでマネージャアクセスを無効にする Management Center 展開では、ローカル DNS 設定が削除されます。その DNS サーバーがアクセスルールの FQDN などのセキュリティポリシーで使用されている場合は、Management Center を使用して DNS 設定を再適用する必要があります。

ステップ 4 設定変更を展開します。

Management Center は、現在のデータインターフェイスを介して設定の変更を展開します。

ステップ 5 必要に応じて、管理インターフェイスの Management Center に到達できるように Threat Defense のケーブルを再接続します。

ステップ 6 Threat Defense CLI で、静的 IP アドレスまたは DHCP を使用して、管理インターフェイスの IP アドレスとゲートウェイを設定します。

最初にマネージャアクセス用のデータインターフェイスを設定したとき、管理ゲートウェイはデータインターフェイスに設定されていました。これにより、バックプレーン経由で管理トラフィックが転送され、マネージャアクセス データ インターフェイスを介してルーティングできるようになりました。ここで、管理ネットワーク上のゲートウェイの IP アドレスを設定する必要があります。

スタティック IP アドレス :

```
configure network {ipv4 | ipv6} manual ip_address netmask gateway_ip
```

DHCP :

configure network {ipv4 | ipv6} dhcp

ステップ 7 Management Center で、管理接続を無効にし、[デバイス (Devices)] > [デバイス管理 (Device Management)] > [デバイス (Device)] > [管理 (Management)] セクションで Threat Defense の [リモートホストアドレス (Remote Host Address)] IP アドレスを更新してオプションの [セカンダリアドレス (Secondary Address)] を削除し、接続を再度有効にします。

Management Center でのホスト名または IP アドレスの更新 (31 ページ) を参照してください。Threat Defense を Management Center に追加したときに Threat Defense ホスト名または NAT ID のみを使用した場合は、値を更新する必要はありません。ただし、接続を再開するには、管理接続を無効にしてから再度有効にする必要があります。

ステップ 8 管理接続が再確立されたことを確認します。

Management Center で、[デバイス (Devices)] [デバイス管理 (Device Management)] [デバイス (Device)] [管理 (Management)] [ステータス (Status)] フィールドで管理接続ステータスを確認するか、Management Center で通知を表示します。 > > >

管理接続のステータスを表示するには、Threat Defense CLI で、**sftunnel-status-brief** コマンドを入力します。

接続の再確立に 10 分以上かかる場合は、接続のトラブルシューティングを行う必要があります。データインターフェイスでの管理接続のトラブルシューティング (61 ページ) を参照してください。

冗長マネージャアクセス用データインターフェイスの設定

マネージャのアクセスにデータインターフェイスを使用する場合、プライマリインターフェイスがダウンした場合に管理機能を引き継ぐよう、セカンダリインターフェイスを構成できます。セカンダリインターフェイスは1つだけ構成できます。デバイスは、SLA モニタリングを使用して、スタティックルートの実行可能性と、両方のインターフェイスを含む ECMP ゾーンを追跡し、管理トラフィックで両方のインターフェイスが使用できるようにします。

始める前に

- セカンダリインターフェイスは、プライマリインターフェイスとは別のセキュリティゾーンにある必要があります。
- プライマリインターフェイスに適用されるのと同じすべての要件がセカンダリインターフェイスに適用されます。管理のための Threat Defense データインターフェイスの使用について (4 ページ) を参照してください。

手順

ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] ページで、デバイスの [編集 (Edit)] (✎) をクリックします。

ステップ 2 セカンダリインターフェイスのマネージャアクセスを有効にします。

この設定は、インターフェイスの有効化、名前の設定、セキュリティゾーンの設定、スタティック IPv4 アドレスの設定などの標準のインターフェイス設定に加えて行われます。

- [**インターフェイス (Interfaces)**] > [**物理インターフェイスの編集 (Edit Physical Interface)**] > [**マネージャアクセス (Manager Access)**] を選択します。
- [このインターフェイス上の管理をマネージャに対して有効にする (Enable management on this interface for the Manager)] をオンにします。
- [OK] をクリックします。

どちらのインターフェイスも、インターフェイスリストに [(マネージャアクセス (Manager Access))] と表示されます。

図 18: インターフェイスリスト

Interface	Logical Name	Type	Security Zones
Diagnostic1/1	diagnostic	Physical	
Ethernet1/1 (Manager Access)	outside	Physical	outside
Ethernet1/2		Physical	
Ethernet1/3		Physical	
Ethernet1/4		Physical	
Ethernet1/5		Physical	
Ethernet1/6		Physical	
Ethernet1/7		Physical	
Ethernet1/8 (Manager Access)	redundant	Physical	mgmt

ステップ 3 [管理 (Management)] 設定にセカンダリアドレスを追加します。

- [Device] をクリックし、[Management] 領域を表示します。
- [.] をクリックします。[編集 (Edit)] (✎)

図 19: 管理アドレスの編集

Management ✎ 🔍

Remote Host Address: 10.89.5.29

Secondary Address:

Status: ✔

Manager Access Interface: Data Interface

Manager Access Details: Configuration

- [管理 (Management)] ダイアログボックスで、[セカンダリアドレス (Secondary Address)] フィールドの名前または IP アドレスを変更します。

図 20: 管理 IP アドレス

d) [保存 (Save)] をクリックします。

ステップ 4 両方のインターフェイスで ECMP ゾーンを作成します。

- [Routing] をクリックします。
- 仮想ルータドロップダウンから、プライマリインターフェイスとセカンダリインターフェイスが存在する仮想ルータを選択します。
- [ECMP] をクリックし、[追加 (Add)] をクリックします。
- [名前 (Name)] に ECMP ゾーンの名前を入力します。
- [使用可能なインターフェイス (Available Interfaces)] ボックスでプライマリおよびセカンダリインターフェイスを選択し、[追加 (Add)] をクリックします。

図 21: ECMP ゾーンの追加

f) [OK] をクリックし、[保存 (Save)] をクリックします。

ステップ 5 両方のインターフェイスに等コストのデフォルトスタティックルートを追加し、両方で SLA トラッキングを有効にします。

ルートはゲートウェイを除いて同一であること、および両方のメトリックが1であることが必要です。プライマリインターフェイスには、編集可能なデフォルトルートがすでに存在している必要があります。

図 22: Add/Edit Static Route

The screenshot shows the 'Edit Static Route Configuration' window. At the top, there's a title bar with a question mark icon. Below it, the 'Type' is set to 'IPv4' (selected with a radio button). The 'Interface*' dropdown is set to 'outside'. A note below says '(Interface starting with this icon [lock icon] signifies it is available for route leak)'. There are two panes: 'Available Network' and 'Selected Network'. The 'Available Network' pane has a search bar and a list of networks: '10.99.11.1', 'any-ipv4', 'IPv4-Benchmark-Tests', 'IPv4-Link-Local', 'IPv4-Multicast', and 'IPv4-Private-10.0.0.0-8'. The 'any-ipv4' network is selected and moved to the 'Selected Network' pane. An 'Add' button is between the panes. Below the panes, there's a section 'Ensure that egress virtualrouter has route to that destination'. It contains a 'Gateway' dropdown set to '10.89.5.1', a 'Metric' input field set to '1' (with a range of '(1 - 254)' below it), a 'Tunneled' checkbox (unchecked) with the text '(Used only for default Route)', and a 'Route Tracking' dropdown. At the bottom right, there are 'Cancel' and 'OK' buttons.

- [Static Route] をクリックします。
- [ルートを追加 (Add Route)] をクリックして新しいルートを追加するか、既存のルートの場合は [編集 (Edit)] (✎) をクリックします。
- [インターフェイス (Interface)] ドロップダウンリストから、インターフェイスを選択します。
- 宛先ネットワークとして、[使用可能なネットワーク (Available Networks)] ボックスから [any-ipv4] を選択し、[追加 (Add)] をクリックします。
- デフォルトの [ゲートウェイ (Gateway)] を入力します。

- f) [ルートトラッキング (Route Tracking)] の場合、**Add (+)** をクリックして新しい SLA モニターオブジェクトを追加します。
- g) 次を含む必要なパラメータを入力します。
- Management Center IP アドレスとしての [モニターアドレス (Monitor Address)]。
 - [使用可能なゾーン (Available Zones)] のプライマリまたはセカンダリ管理インターフェイスのゾーン。たとえば、プライマリインターフェイスオブジェクトには外部ゾーンを選択し、セカンダリインターフェイスオブジェクトには管理ゾーンを選択します。

図 23: SLA モニターの追加

New SLA Monitor Object ?

<p>Name: <input type="text" value="mgmt-secondary"/></p> <p>Frequency (seconds): <input type="text" value="60"/> <small>(1-604800)</small></p> <p>Threshold (milliseconds): <input type="text"/> <small>(0-60000)</small></p> <p>Data Size (bytes): <input type="text" value="28"/> <small>(0-16384)</small></p> <p>Number of Packets: <input type="text" value="1"/></p> <p>Available Zones ↕</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <input type="text" value="Search"/> </div> <div style="border: 1px solid #ccc; padding: 5px;"> <div style="background-color: #0070c0; color: white; padding: 2px 5px; margin-bottom: 5px;">mgmt</div> <div style="padding: 2px 5px;">outside</div> </div>	<p>Description: <input type="text"/></p> <p>SLA Monitor ID*: <input type="text" value="2"/></p> <p>Timeout (milliseconds): <input type="text" value="5000"/> <small>(0-604800000)</small></p> <p>ToS: <input type="text"/></p> <p>Monitor Address*: <input type="text" value="10.89.5.35"/></p> <p>Selected Zones/Interfaces</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <div style="padding: 2px 5px;">mgmt 🗑</div> </div>
---	---

- h) [保存 (Save)] をクリックし、[ルートトラッキング (Route Tracking)] ドロップダウンリストで、作成した SLA オブジェクトを選択します。
- i) [OK] をクリックし、[保存 (Save)] をクリックします。
- j) 他の管理インターフェイスのデフォルトルートについてこの手順を繰り返します。

ステップ 6 構成の変更を展開しますを参照してください。

この機能の展開において、Management Center は管理トラフィック用のセカンダリインターフェイスを有効にします。これには、管理トラフィックが適切なデータインターフェイスに到達するための自動生成されたポリシーベースのルーティング設定が含まれます。Management Center は、**configure network management-data-interface** コマンドの 2 番目のインスタンスも展開します。CLI でセカンダリインターフェイスを編集する場合、このインターフェイスのスタティックルートは Management Center でのみ編集できるため、ゲートウェイを設定したり、デフォルトルートを変更したりすることはできません。

データインターフェイス管理用のマネージャアクセスの詳細を表示する

モデルのサポート : Threat Defense

専用の管理インターフェイスを使用する代わりに、Management Center 管理にデータインターフェイスを使用する場合は、Management Center でデバイスのインターフェイスとネットワークの設定を変更するときに接続を中断しないように注意します。デバイスのデータインターフェイス設定をローカルで変更することもできます。その場合は、Management Center でそれらの変更を手動で調整する必要があります。[デバイス (Devices)] > [デバイス管理 (Device Management)] > [デバイス (Device)] > [管理 (Management)] > [マネージャアクセス - 構成詳細 (Manager Access - Configuration Details)] [FMC アクセス - 構成詳細 (FMC Access - Configuration Details)] ダイアログボックスは、Management Center と Threat Defense のローカル設定の間の矛盾を解決するために役立ちます。 > > >

通常、Threat Defense を Management Center に追加する前に、Threat Defense の初期設定の一環としてマネージャアクセスデータインターフェイスを構成します。Threat Defense を Management Center に追加すると、Management Center はインターフェイス設定 (インターフェイス名と IP アドレス、ゲートウェイへの静的ルート、DNS サーバー、DDNS サーバーなど) を検出して維持します。DNS サーバーの場合、登録中に検出された場合、構成はローカルに保持されます。ただし、Management Center のプラットフォーム設定ポリシーには追加されません。

Threat Defense を Management Center に追加した後、**configure network management-data-interface** コマンドを使用してローカルで Threat Defense のデータインターフェイス構成を変更すると、Management Center が構成変更を検出し、Threat Defense への展開をブロックします。Management Center は、以下のいずれかの方法を使用して構成の変更を検出します。

- Threat Defense への展開。Management Center の展開の前に、構成の差異を検出してデプロイを停止します。
- [インターフェイス (Interfaces)] ページの [同期 (Sync)] ボタン。

- [マネージャアクセス - 構成の詳細 (Manager Access - Configuration Details)] [FMCアクセス - 構成の詳細 (FMC Access - Configuration Details)] ダイアログボックスの [更新 (Refresh)] ボタン

ブロックを削除するには、[マネージャアクセス - 構成詳細 (Manager Access - Configuration Details)] [FMCアクセス - 構成詳細 (FMC Access - Configuration Details)] ダイアログボックスに移動し、[確認 (Acknowledge)] をクリックする必要があります。Management Center 設定は、次回展開時に Threat Defense の残りの競合する設定を上書きします。再展開の前に Management Center の設定を手動で修正する必要があります。

このダイアログボックスに関する以下のページを参照してください。

設定

Management Center および Threat Defense のマネージャ アクセス データ インターフェイスの構成比較を表示します。

次の例は、**configure network management-data-interface** コマンドが Threat Defense に入力された Threat Defense の構成詳細を示しています。ピンクのハイライトは、相違点を確認したものの、Management Center の構成と一致しない場合、Threat Defense の構成が削除されることを示しています。青色のハイライトは、Threat Defense で変更される構成を示しています。緑のハイライトは、Threat Defense に追加される構成を示しています。

Manager access - Configuration Details ?

Manager access configuration on device have been updated outside of Manager. Review the differences and update Manager values accordingly.

Configuration CLI Output Connection Status

Last updated: 2022-09-02 at 20:35:58 UTC [\[Refresh \]](#)

	Configuration on Manager	Configuration on Device
4. Ethernet1/1		
Interface Configuration		
FMC Access Enabled	Disabled	Enabled
FMC Access - Allowed Networks		any
Interface Name		outside
IPv4/IPv6 Address		10.89.5.29/26
Static Route Configuration		
IPv4 Gateway		10.89.5.1
IPv6 Gateway		
5. Ethernet1/8		

Legend: Above configurations will be ■ added, ■ modified or ■ disassociated from manager access interface on next deploy to device.

[Close](#) [Acknowledge](#)

Management Center でインターフェイスを設定した後のこのページの例を以下に示します。インターフェイス設定が一致し、ピンクのハイライトが消えています。

Manager access - Configuration Details



Manager access configuration on device is different from Manager. Review the differences and deploy the changes.

Configuration CLI Output Connection Status

Last updated: 2022-09-09 at 07:10:54 UTC [\[Refresh \]](#)

	Configuration on Manager	Configuration on Device
Web Update Type		
4. GigabitEthernet0/0		
Interface Configuration		
FMC Access Enabled	Enabled	Enabled
FMC Access - Allowed Networks	any	any
Interface Name	outside	outside
IPv4/IPv6 Address	10.89.5.29 255.255.255.192	10.89.5.29 255.255.255.192
Static Route Configuration		
IPv4 Gateway		10.89.5.1
IPv6 Gateway		

Legend: Above configurations will be added, modified or disassociated from manager access interface on next deploy to device.

[Close](#)

CLI 出力

マネージャ アクセス データ インターフェイスの CLI 構成を表示します。これは、基盤となる CLI に精通している場合に役立ちます。

図 24: CLI 出力

Manager access - Configuration Details



Manager access configuration on device is different from Manager. Review the differences and deploy the changes.

Configuration CLI Output Connection Status

Show command output of Manager Access associated configuration from Firewall Threat Defense

```
> show running-config dns
DNS server-group DefaultDNS

> show sftunnel interfaces
Physical Interface      Name of the Interface

> show running-config interface

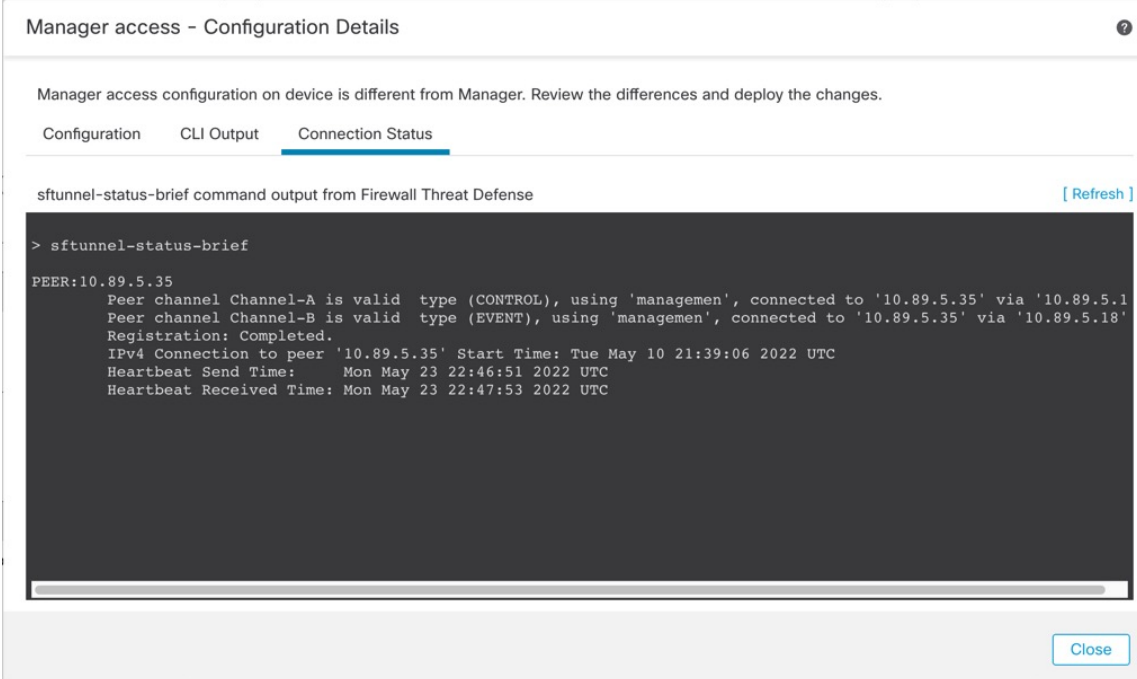
> show version
-----[ 1010-2 ]-----
Model      : Cisco Firepower 1010 Threat Defense (78) Version 7.2.0 (Build 2028)
UUID      : ebf1f518-d0a0-11ec-bb8f-90ce044ba76f
LSP version : lsp-rel-20220519-1116
VDB version  : 354
-----
Cisco Adaptive Security Appliance Software Version 9.18(0)104
```

[Close](#)

接続ステータス

管理接続ステータスの表示次の例は、管理接続で引き続き管理「management0」インターフェイスが使用されていることを示しています。

図 25: 接続ステータス



Manager access - Configuration Details

Manager access configuration on device is different from Manager. Review the differences and deploy the changes.

Configuration CLI Output **Connection Status**

sftunnel-status-brief command output from Firewall Threat Defense [\[Refresh \]](#)

```
> sftunnel-status-brief
PEER:10.89.5.35
Peer channel Channel-A is valid type (CONTROL), using 'managemen', connected to '10.89.5.35' via '10.89.5.1'
Peer channel Channel-B is valid type (EVENT), using 'managemen', connected to '10.89.5.35' via '10.89.5.18'
Registration: Completed.
IPv4 Connection to peer '10.89.5.35' Start Time: Tue May 10 21:39:06 2022 UTC
Heartbeat Send Time: Mon May 23 22:46:51 2022 UTC
Heartbeat Received Time: Mon May 23 22:47:53 2022 UTC
```

[Close](#)

次のステータスは、データインターフェイスの接続が成功したことを示し、内部の「tap_nlp」インターフェイスを示しています。

図 26: 接続ステータス

Manager access - Configuration Details ?

Manager access configuration on device is in sync with the manager.

Configuration CLI Output Connection Status

sftunnel-status-brief command output from Firewall Threat Defense [Refresh]

```

> sftunnel-status-brief
PEER:10.89.5.35
Peer channel Channel-A is valid type (CONTROL), using 'tap_nlp', connected to '10.89.5.35' via '169.254.1.3'
Peer channel Channel-B is valid type (EVENT), using 'tap_nlp', connected to '10.89.5.35' via '169.254.1.3'
Registration: Completed.
IPv4 Connection to peer '10.89.5.35' Start Time: Mon May 23 22:55:01 2022 UTC
Heartbeat Send Time: Mon May 23 22:56:21 2022 UTC
Heartbeat Received Time: Mon May 23 22:55:58 2022 UTC
Last disconnect time : Mon May 23 22:54:39 2022 UTC
Last disconnect reason : Both control and event channel connections with peer went down

```

Close

ダウン状態の接続の出力例を次に示します。ピアチャネルの「接続先」情報やハートビート情報が表示されていません。

```

> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down

```

アップ状態の接続の出力例を次に示します。ピアチャネルとハートビート情報が表示されています。

```

> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC

```

Threat Defense 管理インターフェイスの CLI での変更

CLIを使用して、管理対象デバイスの管理インターフェイスの設定を変更します。これらの設定の多くは、初期セットアップ時に設定されたものです。この手順に従うことで、それらの設

定を変更でき、さらに設定を追加できます（例：モデルでサポートされる場合にイベントインターフェイスを有効化する、スタティック ルートを追加する）。



- (注) このトピックは、専用管理インターフェイスに適用されます。代わりに、管理用のデータインターフェイスを設定することもできます。このインターフェイスのネットワーク設定を変更する場合は、CLI ではなく Management Center 内で行う必要があります。切断された管理接続をトラブルシューティングする必要があり、Threat Defense で直接変更する必要がある場合は、[管理に使用される Threat Defense データインターフェイスの CLI での変更 \(57 ページ\)](#) を参照してください。

Threat Defense CLI の詳細については、[Cisco Secure Firewall Threat Defense コマンドリファレンス](#) を参照してください。



- (注) SSH を使用する際は、慎重に管理インターフェイスに変更を加えてください。構成エラーで再接続できなくなると、デバイスのコンソールポートへのアクセスが必要になります。



- (注) デバイス管理 IP アドレスを変更する場合は、**configure manager add** コマンド ([新しい Management Center の特定 \(67 ページ\)](#) を参照) を使用してデバイスの初期設定時に Management Center を特定した方法に応じて、Management Center 接続に関する次のタスクを参照してください。

- **IP アドレス—アクションなし。** 到達可能な IP アドレスを使用して Management Center を特定した場合、管理接続は数分後に自動的に再確立されます。情報の同期を維持するために、Management Center に表示されるデバイス IP アドレスも変更することを推奨します。[Management Center でのホスト名または IP アドレスの更新 \(31 ページ\)](#) を参照してください。このアクションは、接続の再確立を高速化するのに役立ちます。注：到達不能な Management Center IP アドレスを指定した場合は、以下の NAT ID の手順を参照してください。
- **NAT ID のみ：接続を手動で再確立。** NAT ID のみを使用して Management Center を識別した場合、接続は自動的に再確立されません。この場合、[Management Center でのホスト名または IP アドレスの更新 \(31 ページ\)](#) に従って Management Center のデバイス管理 IP アドレスを変更します。



- (注) ハイアベイラビリティ構成では、登録された Firepower デバイスの管理 IP アドレスをデバイスの CLI または Management Center から変更した場合、HA 同期後も、セカンダリ Management Center には変更が反映されません。セカンダリ Management Center も更新されるようにするには、2つの Management Center の間でロールを切り替えて、セカンダリ Management Center をアクティブユニットにします。現在アクティブな Management Center のデバイス管理のページで、登録されている Firepower デバイスの管理 IP アドレスを変更します。

始める前に

- **configure user add** コマンドを使用して CLI にログイン可能なユーザー アカウントを作成できます。

手順

- ステップ 1** コンソール ポートから、または SSH を使用して、デバイス CLI に接続します。
- ステップ 2** 管理者のユーザー名とパスワードでログインします。
- ステップ 3** (Firepower 4100/9300 のみ) 2 番目の管理インターフェイスをイベント専用インターフェイスとして有効にします。

configure network management-interface enable management1

configure network management-interface disable-management-channel management1

管理トラフィック用の管理インターフェイスが常に必要です。デバイスに 2 番目の管理インターフェイスがある場合は、イベント専用トラフィックに対してそのインターフェイスを有効にすることができます。

Secure Firewall Management Center イベント専用インターフェイスは管理チャンネルのトラフィックを受け入れることができないので、デバイス イベント インターフェイスで管理チャンネルを単に無効にしてください。

必要に応じて、**configure network management-interface disable-events-channel** コマンドを使用してメイン管理インターフェイスのイベントを無効にできます。いずれの場合も、デバイスは、イベントのみのインターフェイス上でイベントを送信しようとします。そのインターフェイスがダウンしていた場合は、イベントチャンネルが無効になっていても、管理インターフェイス上でイベントを送信します。

インターフェイス上でイベントチャンネルと管理チャンネルの両方を無効にすることはできません。

例：

```
> configure network management-interface enable management1
Configuration updated successfully
```

```
> configure network management-interface disable-management-channel management1
Configuration updated successfully
```

>

ステップ 4 管理インターフェイスまたはイベント インターフェイスのネットワーク設定をします。

management_interface 引数を指定しない場合は、デフォルトの管理インターフェイスのネットワーク設定を変更します。イベントインターフェイスを設定する際は、必ず *management_interface* 引数を指定してください。イベントインターフェイスは、管理インターフェイスの個別のネットワーク、または同じネットワークに配置できます。自分で設定するインターフェイスに接続すると、切断されます。新しい IP アドレスに再接続できます。

a) IPv4 アドレスを設定します。

- 手動設定

configure network ipv4 manual ip_address netmask gateway_ip [management_interface]

このコマンド内の *gateway_ip* は、デバイスのデフォルトルートを作成するために使用されることに注意してください。イベント専用インターフェイスを設定する場合は、コマンドの一部として *gateway_ip* を入力する必要があります。ただし、このエントリは、指定した値にデフォルトルートを設定するだけで、イベントインターフェイスの個別のスタティックルートは作成しません。管理インターフェイスと別のネットワークでイベント専用インターフェイスを使用している場合は、管理インターフェイスと共に使用するように *gateway_ip* を設定し、**configure network static-routes** コマンドを使用してイベント専用インターフェイス用に個別にスタティックルートを作成することを推奨します。

例 :

```
> configure network ipv4 manual 10.10.10.45 255.255.255.0 10.10.10.1 management1
Setting IPv4 network configuration.
Network settings changed.
```

>

- DHCP (デフォルト管理インターフェイスのみでサポート)。

configure network ipv4 dhcp

b) IPv6 アドレスを設定します。

- ステートレス自動設定

configure network ipv6 router [management_interface]

例 :

```
> configure network ipv6 router management0
Setting IPv6 network configuration.
Network settings changed.
```

>

- 手動設定

```
configure network ipv6 manual ipv6_address ipv6_prefix_length [ipv6_gateway_ip]  
[management_interface]
```

このコマンド内の *ipv6_gateway_ip* は、デバイスのデフォルトルートを作成するために使用されることに注意してください。イベント専用インターフェイスを設定する場合は、コマンドの一部として *ipv6_gateway_ip* を入力する必要があります。ただし、このエントリは、指定した値にデフォルトルートを設定するだけで、イベントインターフェイスの個別のスタティックルートは作成しません。管理インターフェイスと別のネットワークでイベント専用インターフェイスを使用している場合は、管理インターフェイスと共に使用するように *ipv6_gateway_ip* を設定し、**configure network static-routes** コマンドを使用してイベント専用インターフェイス用に個別にスタティックルートを作成することを推奨します。

例：

```
> configure network ipv6 manual 2001:0DB8:BA98::3210 64 management1  
Setting IPv6 network configuration.  
Network settings changed.
```

```
>
```

- DHCPv6 (デフォルト管理インターフェイスのみでサポート)。

```
configure network ipv6 dhcp
```

ステップ 5 IPv6 の場合、ICMPv6 エコー応答と宛先到達不能メッセージを有効または無効にします。デフォルトでは、これらのメッセージは有効になっています。

```
configure network ipv6 destination-unreachable {enable | disable}
```

```
configure network ipv6 echo-reply {enable | disable}
```

これらのパケットを無効にすることで、サービス拒否攻撃の可能性から保護します。エコー応答パケットを無効にすると、デバイスの管理インターフェイスにテスト目的で IPv6 ping を使用できなくなります。

例：

```
> configure network ipv6 destination-unreachable disable  
> configure network ipv6 echo-reply disable
```

ステップ 6 デフォルト管理インターフェイスの DHCP サーバーが、接続されているホストに IP アドレスを提供することを可能にします。

```
configure network ipv4 dhcp-server-enable start_ip_address end_ip_address
```

例：

```
> configure network ipv4 dhcp-server-enable 10.10.10.200 10.10.10.254  
DHCP Server Enabled
```

```
>
```

管理インターフェイスの IP アドレスを手動で設定するときのみ、DHCP サーバーを設定できます。このコマンドは、Management Center Virtual ではサポートされません。DHCP サーバーのステータスを表示するには、**show network-dhcp-server** を入力します。

```
> show network-dhcp-server
DHCP Server Enabled
10.10.10.200-10.10.10.254
```

ステップ 7 Management Center がリモート ネットワーク上にある場合は、イベント専用インターフェイスのスタティック ルートを追加します。追加しないと、すべてのトラフィックが管理インターフェイスを通じてデフォルト ルートと一致します。

```
configure network static-routes {ipv4 | ipv6} add management_interface destination_ip netmask_or_prefix gateway_ip
```

デフォルト ルートの場合は、このコマンドを使用しないでください。デフォルト ルート ゲートウェイの IP アドレスの変更は、**configure network ipv4** コマンドまたは **ipv6** コマンドを使用した場合のみ可能です（ステップ 4 を参照）。

例：

```
> configure network static-routes ipv4 add management1 192.168.6.0 255.255.255.0 10.10.10.1
Configuration updated successfully
```

```
> configure network static-routes ipv6 add management1 2001:0DB8:AA89::5110 64
2001:0DB8:BA98::3211
Configuration updated successfully
```

```
>
```

スタティック ルートを表示するには、**show network-static-routes** を入力します（デフォルト ルートは表示されません）。

```
> show network-static-routes
-----[ IPv4 Static Routes ]-----
Interface           : management1
Destination         : 192.168.6.0
Gateway             : 10.10.10.1
Netmask             : 255.255.255.0
[...]
```

ステップ 8 ホスト名の設定

```
configure network hostname name
```

例：

```
> configure network hostname farscapel.cisco.com
```

Syslog メッセージは、再起動するまで新しいホスト名を反映しません。

ステップ 9 検索ドメインを設定します。

```
configure network dns searchdomains domain_list
```

例 :

```
> configure network dns searchdomains example.com,cisco.com
```

カンマで区切ったデバイスの検索ドメインを設定します。これらのドメインは、コマンド (**ping system** など) に完全修飾ドメイン名を指定しない場合にホスト名に追加されます。ドメインは、管理インターフェイスまたは管理インターフェイスを経由するコマンドでのみ、使用されます。

ステップ 10 カンマで区切った 3 つの DNS サーバーを設定します。

```
configure network dns servers dns_ip_list
```

例 :

```
> configure network dns servers 10.10.6.5,10.20.89.2,10.80.54.3
```

ステップ 11 Management Center で通信のリモート管理ポートを設定します。

```
configure network management-interface tcpport number
```

例 :

```
> configure network management-interface tcpport 8555
```

Management Center および管理対象デバイスは、双方向の SSL 暗号化通信チャネル (デフォルトではポート 8305) を使用して通信します。

(注) シスコは、リモート管理ポートをデフォルト設定のままにしておくことを強く推奨していますが、管理ポートがネットワーク上の他の通信と競合する場合は、別のポートを選択できます。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デバイスの管理ポートを変更する必要があります。

ステップ 12 (Threat Defense のみ) 管理インターフェイスまたはイベントインターフェイスの MTU を設定します。デフォルトの MTU は 1500 バイトです。

```
configure network mtu [bytes] [interface_id]
```

- *bytes* : MTU をバイト単位で設定します。管理インターフェイスでは、IPv4 を有効にした場合は 64~1500、IPv6 を有効にした場合は 1280~1500 の値を指定できます。イベントインターフェイスでは、IPv4 を有効にした場合は 64~9000、IPv6 を有効にした場合は 1280~9000 です。IPv4 と IPv6 の両方を有効にした場合、最小値は 1280 です。*bytes* を入力しない場合、値の入力を求められます。
- *interface_id* : MTU を設定するインターフェイス ID を指定します。プラットフォームに応じて使用可能なインターフェイス ID (management0、management1、br1、eth0 など) を表

示するには、**show network** コマンドを使用します。インターフェイスを指定しない場合は、管理インターフェイスが使用されます。

例：

```
> configure network mtu 8192 management1
MTU set successfully to 1500 from 8192 for management1
Refreshing Network Config...
NetworkSettings::refreshNetworkConfig MTU value at start 8192

Interface management1 speed is set to '10000baseT/Full'
NetworkSettings::refreshNetworkConfig MTU value at end 8192
>
```

ステップ 13 HTTP プロキシを設定します。デバイスは、ポート TCP/443 (HTTPS) および TCP/80 (HTTP) でインターネットに直接接続するように設定されています。HTTP ダイジェスト経由で認証できるプロキシサーバを使用できます。コマンド発行後に、HTTP プロキシのアドレスとポート、プロキシの認証が必要かどうかをユーザーは尋ねられます。認証が必要な場合はプロキシのユーザー名、プロキシのパスワード、およびプロキシのパスワードの確認を入力するよう要求されます。

(注) Threat Defense のプロキシパスワードには、A~Z、a~z と 0~9 の文字のみを使用できます。

configure network http-proxy

例：

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address: 10.100.10.10
Enter HTTP Proxy Port: 80
Use Proxy Authentication? (y/n) [n]: Y
Enter Proxy Username: proxyuser
Enter Proxy Password: proxypassword
Confirm Proxy Password: proxypassword
```

ステップ 14 デバイス管理 IP アドレスを変更する場合は、**configure manager add** コマンド ([新しい Management Center の特定 \(67 ページ\)](#)) を参照) を使用してデバイスの初期設定時に Management Center を特定した方法に応じて、Management Center 接続に関する次のタスクを参照してください。

- **IP アドレス—アクションなし**。到達可能な IP アドレスを使用して Management Center を特定した場合、管理接続は数分後に自動的に再確立されます。情報の同期を維持するために、Management Center に表示されるデバイス IP アドレスも変更することを推奨します。[Management Center でのホスト名または IP アドレスの更新 \(31 ページ\)](#) を参照してください。このアクションは、接続の再確立を高速化するのに役立ちます。**注**：到達不能な Management Center IP アドレスを指定した場合は、[Management Center でのホスト名または IP アドレスの更新 \(31 ページ\)](#) を使用して手動で接続を再確立する必要があります。
- **NAT ID のみ：接続を手動で再確立**。NAT ID のみを使用して Management Center を識別した場合、接続は自動的に再確立されません。この場合、[Management Center でのホスト名](#)

または [IP アドレスの更新 \(31 ページ\)](#) に従って Management Center のデバイス管理 IP アドレスを変更します。

管理に使用される Threat Defense データインターフェイスの CLI での変更

Threat Defense と Management Center の間の管理接続が中断され、古いインターフェイスを置き換える新しいデータインターフェイスを指定する場合は、Threat Defense CLI を使用して新しいインターフェイスを設定します。この手順では、同じネットワーク上の古いインターフェイスを新しいインターフェイスに置き換えることを想定しています。管理接続がアクティブな場合は、Management Center を使用して既存のデータインターフェイスを変更する必要があります。データ管理インターフェイスの初期設定については、「[CLI を使用した Threat Defense 初期設定の実行の完了 \(19 ページ\)](#)」の `configure network management-data-interface` コマンドを参照してください。



- (注) このトピックは、専用の管理インターフェイスではなく、管理用に設定したデータインターフェイスに適用されます。管理インターフェイスのネットワーク設定を変更する場合は、[Threat Defense 管理インターフェイスの CLI での変更 \(49 ページ\)](#) を参照してください。

Threat Defense CLI の詳細については、[Cisco Secure Firewall Threat Defense コマンドリファレンス](#) を参照してください。

始める前に

- `configure user add` コマンドを使用して CLI にログイン可能なユーザー アカウントを作成できます。

手順

- ステップ 1** データ管理インターフェイスを新しいインターフェイスに変更する場合は、現在のインターフェイスケーブルを新しいインターフェイスに移動します。
- ステップ 2** デバイスの CLI に接続します。
- これらのコマンドを使用する場合は、コンソールポートを使用する必要があります。初期設定の実行中に、管理インターフェイスから切断される可能性があります。管理接続が中断されたために設定を編集しており、専用管理インターフェイスに SSH アクセスできる場合は、その SSH 接続を使用できます。
- ステップ 3** 管理者のユーザー名とパスワードでログインします。
- ステップ 4** インターフェイスを無効にして、設定を再構成できるようにします。

`configure network management-data-interface disable`

例 :

```
> configure network management-data-interface disable
```

```
Configuration updated successfully..!!
```

```
Configuration disable was successful, please update the default route to point to a gateway on management interface using the command 'configure network'
```

ステップ 5 マネージャアクセス用の新しいデータインターフェイスを設定します。

configure network management-data-interface

その後、データインターフェイスの基本的なネットワーク設定を行うように求めるプロンプトが表示されます。

データ管理インターフェイスを同じネットワーク上の新しいインターフェイスに変更する場合は、インターフェイス ID を除き、前のインターフェイスと同じ設定を使用します。さらに、

Do you wish to clear all the device configuration before applying ? (y/n) [n]: オプションに **y** を選択します。この選択により、古いデータ管理インターフェイスの設定がクリアされるため、IP アドレスとインターフェイス名を新しいインターフェイスで正常に再利用できます。

```
> configure network management-data-interface
Data interface to use for management: ethernet1/4
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]: y
```

```
Configuration done with option to allow manager access from any network, if you wish to change the manager access network use the 'client' option in the command 'configure network management-data-interface'.
```

```
Setting IPv4 network configuration.
Network settings changed.
```

```
>
```

ステップ 6 (任意) 特定のネットワーク上の Management Center へのデータ インターフェイス アクセスを制限します。

configure network management-data-interface client ip_address netmask

デフォルトでは、すべてのネットワークが許可されます。

ステップ 7 接続は自動的に再確立されますが、Management Center で接続を無効にしてから再度有効にすると、接続の再確立を速く実行できます。「[Management Center でのホスト名または IP アドレスの更新 \(31 ページ\)](#)」を参照してください。

ステップ 8 管理接続が再確立されたことを確認します。

sftunnel-status-brief

アップ状態の接続の出力例を次に示します。ピアチャネルとハートビート情報が表示されています。

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

ステップ 9 Management Center で、[デバイス (Devices)] > [デバイス管理 (Device Management)] > [デバイス (Device)] > [管理 (Management)] > [マネージャアクセス - 構成詳細 (Manager Access - Configuration Details)] > [FMCアクセス - 構成詳細 (FMC Access - Configuration Details)] を選択し、[更新 (Refresh)] をクリックします。

Management Center はインターフェイスとデフォルトルートの設定変更を検出し、Threat Defense への展開をブロックします。デバイスのデータインターフェイス設定をローカルで変更する場合は、Management Center でそれらの変更を手動で調整する必要があります。[構成 (Configuration)] タブで、Management Center と Threat Defense の不一致を確認できます。

ステップ 10 [Devices] > [Device Management] > [Interfaces] の順に選択して、次の変更を行います。

- 古いデータ管理インターフェイスから IP アドレスと名前を削除し、このインターフェイスのマネージャアクセスを無効にします。
- 古いインターフェイス (CLI で使用したインターフェイス) の設定を使用して新しいデータ管理インターフェイスを設定し、マネージャアクセスを有効にします。

ステップ 11 [Devices] > [Device Management] > [Routing] > [Static Route] を選択し、デフォルトルート古いデータ管理インターフェイスから新しいインターフェイスに変更します。

ステップ 12 [マネージャアクセス - 構成詳細 (Manager Access - Configuration Details)] [FMCアクセス - 構成詳細 (FMC Access - Configuration Details)] ダイアログボックスに戻り、[確認 (Acknowledge)] をクリックして展開ブロックを削除します。

Management Center 設定は、次回展開時に Threat Defense の残りの競合する設定を上書きします。再展開の前に Management Center の設定を手動で修正する必要があります。

「Config was cleared」および「Manager Access changed and acknowledged」という想定されるメッセージが表示されます。

Management Center の接続が失われた場合の構成のロールバック

Threat Defense でマネージャアクセス用にデータインターフェイスを使用し、ネットワーク接続に影響する Management Center からの構成変更を展開する場合、Threat Defense の構成を最後に展開した構成にロールバックして、管理接続を復元できます。その後、ネットワーク接続が維持されるように Management Center で構成設定を調整し、再展開できます。ロールバック機能は、接続が失われていない場合でも使用でき、このトラブルシューティングの状況以外でも使用できます。

次のガイドラインを参照してください。

- 前回の展開のみ Threat Defense でローカルに使用できます。さらに以前の展開にロールバックすることはできません。
- ロールバックは、高可用性ではサポートされていますが、クラスタリングの展開ではサポートされていません。
- ロールバックは、Management Center で設定できる構成にのみ影響します。たとえば、ロールバックは、Threat Defense CLI でのみ設定できる専用管理インターフェイスに関連するローカル構成には影響しません。 **configure network management-data-interface** コマンドを使用した最後の Management Center 展開後にデータインターフェイス設定を変更し、rollback コマンドを使用すると、それらの設定は保持されないことに注意してください。最後に展開された Management Center 設定にロールバックされます。
- UCAPL/CC モードはロールバックできません。
- 以前の展開中に更新されたアウトオブバンド SCEP 証明書データはロールバックできません。
- ロールバック中に、現在の設定がクリアされるため、接続がドロップされます。

手順

ステップ 1 Threat Defense CLI で、以前の構成へロールバックします。

configure policy rollback

ロールバック後、Threat Defense はロールバックが正常に完了したことを Management Center に通知します。Management Center では、構成がロールバックされたことを示すバナーが展開画面に表示されます。

(注) ロールバックが失敗し、Management Center 管理が復元された場合、一般的な展開の問題について <https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.html> を参照してください。場合によっては、Management Center 管理アクセスの復元後にロールバックが失敗することがあります。この場合、Management Center 構成の問題を解決して、Management Center から再展開できます。

例：

マネージャアクセスにデータインターフェイスを使用する Threat Defense の場合：

```
> configure policy rollback
```

```
The last deployment to this FTD was on June 1, 2020 and its status was Successful.
Do you want to continue [Y/N]?
```

```
Y
```

```
Rolling back complete configuration on the FTD. This will take time.
.....
```

```
Policy rollback was successful on the FTD.  
Configuration has been reverted back to transaction id:  
Following is the rollback summary:  
.....  
.....  
>
```

ステップ 2 管理接続が再確立されたことを確認します。

Management Center で、[Devices] [Device Management] [Device] [Management] [Manager Access - Configuration Details] [FMC Access - Configuration Details] [Connection Status] ページで管理接続ステータスを確認します。

管理接続のステータスを表示するには、Threat Defense CLI で、**sftunnel-status-brief** コマンドを入力します。

接続の再確立に 10 分以上かかる場合は、接続のトラブルシューティングを行う必要があります。[データインターフェイスでの管理接続のトラブルシューティング \(61 ページ\)](#) を参照してください。

データインターフェイスでの管理接続のトラブルシューティング

専用の管理インターフェイスを使用する代わりに、マネージャアクセスにデータインターフェイスを使用する場合は、Management Center で Threat Defense のインターフェイスとネットワークの設定を変更する際、接続を中断しないように注意します。Threat Defense を Management Center に追加した後に管理インターフェイスタイプを変更する場合（データから管理へ、または管理からデータへ）、インターフェイスとネットワークの設定が正しく構成されていないと、管理接続が失われる可能性があります。

このトピックは、管理接続が失われた場合のトラブルシューティングに役立ちます。

管理接続ステータスの表示

Management Center で、[Devices] [Device Management] [Device] [Management] [Manager Access - Configuration Details] [FMC Access - Configuration Details] [Connection Status] ページで管理接続ステータスを確認します。

管理接続のステータスを表示するには、Threat Defense CLI で、**sftunnel-status-brief** コマンドを入力します。**sftunnel-status** を使用して、より完全な情報を表示することもできます。

ダウン状態の接続の出力例を次に示します。ピアチャネルの「接続先」情報やハートビート情報が表示されていません。

```
> sftunnel-status-brief  
PEER:10.10.17.202  
Registration: Completed.  
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC  
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC  
Last disconnect reason : Both control and event channel connections with peer went down
```

アップ状態の接続の出力例を次に示します。ピアチャンネルとハートビート情報が表示されています。

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to
'10.10.17.202' via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to
'10.10.17.202' via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

Threat Defense ネットワーク情報の表示

Threat Defense CLI で、管理および マネージャ アクセス データ インターフェイスのネットワーク設定を表示します。

show network

```
> show network
===== [ System Information ] =====
Hostname                : 5516X-4
DNS Servers             : 208.67.220.220,208.67.222.222
Management port        : 8305
IPv4 Default route
  Gateway               : data-interfaces
IPv6 Default route
  Gateway               : data-interfaces

===== [ br1 ] =====
State                   : Enabled
Link                    : Up
Channels                : Management & Events
Mode                    : Non-Autonegotiation
MDI/MDIX                : Auto/MDIX
MTU                     : 1500
MAC Address             : 28:6F:7F:D3:CB:8D
----- [ IPv4 ] -----
Configuration           : Manual
Address                 : 10.99.10.4
Netmask                 : 255.255.255.0
Gateway                 : 10.99.10.1
----- [ IPv6 ] -----
Configuration           : Disabled

===== [ Proxy Information ] =====
State                   : Disabled
Authentication          : Disabled

===== [ System Information - Data Interfaces ] =====
DNS Servers             :
Interfaces              : GigabitEthernet1/1

===== [ GigabitEthernet1/1 ] =====
State                   : Enabled
Link                    : Up
Name                    : outside
MTU                     : 1500
MAC Address             : 28:6F:7F:D3:CB:8F
```

```

-----[ IPv4 ]-----
Configuration      : Manual
Address            : 10.89.5.29
Netmask           : 255.255.255.192
Gateway           : 10.89.5.1
-----[ IPv6 ]-----
Configuration      : Disabled

```

Management Center への Threat Defense の登録の確認

Threat Defense CLI で、Management Center 登録が完了したことを確認します。このコマンドは、管理接続の現在のステータスを表示するものではないことに注意してください。

show managers

```

> show managers
Type                : Manager
Host                : 10.10.1.4
Display name       : 10.10.1.4
Identifier          : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration       : Completed
Management type    : Configuration

```

Management Center に ping する

Threat Defense CLI で、次のコマンドを使用して、データインターフェイスから Management Center に ping します。

ping fmc_ip

Threat Defense CLI で、次のコマンドを使用して、管理インターフェイスから Management Center に ping します。これは、バックプレーンを介してデータインターフェイスにルーティングされます。

ping system fmc_ip

Threat Defense 内部インターフェイスでのパケットのキャプチャ

Threat Defense CLI で、内部バックプレーンインターフェイス (nlp_int_tap) でパケットをキャプチャして、管理パケットが送信されているかどうかを確認します。

capture name interface nlp_int_tap trace detail match ip any any

show capturename trace detail

内部インターフェイスのステータス、統計、およびパケット数の確認

Threat Defense CLI で、内部バックプレーンインターフェイス (nlp_int_tap) に関する情報を参照してください。

show interace detail

```

> show interface detail
[...]
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
(Full-duplex), (1000 Mbps)
Input flow control is unsupported, output flow control is unsupported
MAC address 0000.0100.0001, MTU 1500

```

```

IP address 169.254.1.1, subnet mask 255.255.255.248
37 packets input, 2822 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 pause input, 0 resume input
0 L2 decode drops
5 packets output, 370 bytes, 0 underruns
0 pause output, 0 resume output
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops
input queue (blocks free curr/low): hardware (0/0)
output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
37 packets input, 2304 bytes
5 packets output, 300 bytes
37 packets dropped
   1 minute input rate 0 pkts/sec,  0 bytes/sec
   1 minute output rate 0 pkts/sec,  0 bytes/sec
   1 minute drop rate, 0 pkts/sec
   5 minute input rate 0 pkts/sec,  0 bytes/sec
   5 minute output rate 0 pkts/sec,  0 bytes/sec
   5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
Interface number is 14
Interface config status is active
Interface state is active

```

ルーティングと NAT の確認

Threat Defense CLI で、デフォルトルート (S*) が追加されていること、および管理インターフェイス (nlp_int_tap) に内部 NAT ルールが存在することを確認します。

show route

```

> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF

Gateway of last resort is 10.89.5.1 to network 0.0.0.0

S*      0.0.0.0 0.0.0.0 [1/0] via 10.89.5.1, outside
C       10.89.5.0 255.255.255.192 is directly connected, outside
L       10.89.5.29 255.255.255.255 is directly connected, outside

>

```

show nat

```

> show nat

Auto NAT Policies (Section 2)
1 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_intf3 interface
service tcp 8305 8305

```



```

    translate_hits = 0, untranslate_hits = 6
2 (nlp_int_tap) to (outside) source static nlp_server_0_ssh_intf3 interface service
  tcp ssh ssh
    translate_hits = 0, untranslate_hits = 73
3 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_ipv6_intf3 interface
  ipv6 service tcp 8305 8305
    translate_hits = 0, untranslate_hits = 0
4 (nlp_int_tap) to (outside) source dynamic nlp_client_0_intf3 interface
  translate_hits = 174, untranslate_hits = 0
5 (nlp_int_tap) to (outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
  translate_hits = 0, untranslate_hits = 0
>

```

その他の設定の確認

次のコマンドを参照して、他のすべての設定が存在することを確認します。これらのコマンドの多くは、Management Center の [Devices] [Device Management] [Device] [Management] [Manager Access - Configuration Details] [FMC Access - Configuration Details] [CLI Output] ページでも確認できます。

show running-config sftunnel

```

> show running-config sftunnel
sftunnel interface outside
sftunnel port 8305

```

show running-config ip-client

```

> show running-config ip-client
ip-client outside

```

show conn address fmc_ip

```

> show conn address 10.89.5.35
5 in use, 16 most used
Inspect Snort:
  preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap 10.89.5.29(169.254.1.2):51231 outside 10.89.5.35:8305, idle 0:00:04,
  bytes 86684, flags UxIO
TCP nlp_int_tap 10.89.5.29(169.254.1.2):8305 outside 10.89.5.35:52019, idle 0:00:02,
  bytes 1630834, flags UIO
>

```

DDNS の更新が成功したかどうかを確認する

Threat Defense CLI で、DDNS の更新が成功したかどうかを確認します。

debug ddns

```

> debug ddns
DDNS update request = /v3/update?hostname=domain.example.org&myip=209.165.200.225
Successfully updated the DDNS sever with current IP addresses
DDNS: Another update completed, outstanding = 0
DDNS: IDB SB total = 0

```

更新に失敗した場合は、**debug http** コマンドと **debug ssl** コマンドを使用します。証明書の検証が失敗した場合は、ルート証明書がデバイスにインストールされていることを確認します。

```
show crypto ca certificates trustpoint_name
```

DDNS の動作を確認するには :

```
show ddns update interface fmc_access_ifc_name
```

```
> show ddns update interface outside
```

```
Dynamic DNS Update on outside:
  Update Method Name Update Destination
  RBD_DDNS not available
```

```
Last Update attempted on 04:11:58.083 UTC Thu Jun 11 2020
Status : Success
FQDN : domain.example.org
IP addresses : 209.165.200.225
```

Management Center ログファイルの確認

<https://cisco.com/go/fmc-reg-error> を参照してください。

デバイスのマネージャを変更する

以下の状況では、デバイスのマネージャを変更する必要がある場合があります。

- [デバイスの Management Center IP アドレスまたはホスト名を編集する \(66 ページ\)](#) — FMC の IP アドレスまたはホスト名を変更する場合は、デバイスの新しい IP アドレスまたはホスト名と一致させることをお勧めします。
- [新しい Management Center の特定 \(67 ページ\)](#) — 以前の FMC からデバイスを削除した後、存在する場合は新しい FMC 用にデバイスを設定してから、それを FMC に追加できます。
- [Device Manager から Management Center への切り替え \(68 ページ\)](#) — 同じデバイスに対して、FDM と FMC の両方を同時に使用することはできません。FDM から FMC に変更すると、FTD 設定が消去され、最初からやり直す必要があります。
- [Management Center から Device Manager への切り替え \(73 ページ\)](#) — 同じデバイスに対して、FDM と FMC の両方を同時に使用することはできません。FMC から FDM に変更すると、FTD 設定が消去され、最初からやり直す必要があります。

デバイスの Management Center IP アドレスまたはホスト名を編集する

Management Center の IP アドレスまたはホスト名を変更する場合は、設定が一致するようにデバイス CLI で値を変更する必要があります。ほとんどの場合、管理接続はデバイスの Management Center IP アドレスまたはホスト名を変更せずに再確立されますが、少なくともデバイスを Management Center に追加して NAT ID のみを指定した場合は、接続が再確立されるようにするために、このタスクを実行する必要があります。他の場合でも、Management Center IP アドレスまたはホスト名を最新の状態に維持して、ネットワークの復元力を高めることを推奨します。

手順

ステップ 1 Threat Defense CLI で、Management Center 識別子を表示します。

show managers

例 :

```
> show managers
Type                : Manager
Host                : 10.10.1.4
Display name       : 10.10.1.4
Identifier          : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration       : Completed
Management type    : Configuration
```

ステップ 2 Threat Defense CLI で、Management Center IP アドレスまたはホスト名を編集します。

configure manager edit identifier {hostname {ip_address | hostname} | displayname display_name}

Management Center が **DONTRESOLVE** と NAT ID によって最初に識別された場合、このコマンドを使用して値をホスト名または IP アドレスに変更できます。IP アドレスまたはホスト名を **DONTRESOLVE** に変更することはできません。

管理接続がダウンした後、再確立されます。**sftunnel-status** コマンドを使用して、接続の状態をモニターできます。

例 :

```
> configure manager edit f7ffad78-bf16-11ec-a737-baa2f76ef602 hostname 10.10.5.1
```

新しい Management Center の特定

この手順は、管理対象デバイスの新しい Management Center を識別する方法を示します。新しい Management Center が古い Management Center の IP アドレスを使用している場合でも、次の手順を実行する必要があります。

手順

ステップ 1 古い Management Center に管理対象デバイスが存在する場合はこれを削除します。

Management Center とのアクティブな接続がある場合は、Management Center IP アドレスを変更できません。

ステップ 2 SSH などを使用して、デバイスの CLI に接続します。

ステップ 3 新しい Management Center を設定します。

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} regkey [nat_id] [display_name]
```

- {*hostname* | *IPv4_address* | *IPv6_address*} : Management Center のホスト名、IPv4 アドレス、または IPv6 アドレスを設定します。
- **DONTRESOLVE** : Management Center を直接アドレス指定できない場合は、ホスト名または IP アドレスの代わりに **DONTRESOLVE** を使用します。 **DONTRESOLVE** を使用する場合は、*nat_id* が必要です。このデバイスを Management Center に追加する場合は、デバイスの IP アドレスと *nat_id* の両方を必ず指定してください。接続の片側で IP アドレスを指定し、両側で同じ一意の NAT ID を指定する必要があります。
- *regkey* : 登録時に Management Center とデバイス間で共有する登録キーを作成します。このキーには、1 ~ 37 文字の任意のテキスト文字列を選択できます。Threat Defense を追加するときに、Management Center に同じキーを入力します。
- *nat_id* : 一方が IP アドレスを指定しない場合に、Management Center とデバイス間の登録プロセス中のみ使用する 1 ~ 37 文字の英数字文字列を作成します。この NAT ID は、登録時にのみ使用されるワンタイムパスワードです。NAT ID が一意であり、登録を待機している他のデバイスによって使用されていないことを確認します。Threat Defense を追加するときに、Management Center で同じ NAT ID を指定します。
- *display_name* : **show managers** コマンドでこのマネージャを表示するための表示名を指定します。このオプションは、CDO をプライマリマネージャおよび分析専用のオンプレミス Management Center として識別する場合に役立ちます。この引数を指定しない場合、ファイアウォールは以下のいずれかの方法を使用して表示名を自動生成します。
 - *hostname* | *IP_address* (**DONTRESOLVE** キーワードを使用しない場合)
 - **manager-timestamp**

例 :

```
> configure manager add DONTRESOLVE abc123 efg456
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
>
```

ステップ 4 デバイスを Management Center に追加します。

Device Manager から Management Center への切り替え

Device Manager から Management Center へ切り替えると、管理インターフェイスとマネージャアクセス設定に加えて、すべてのインターフェイス構成が保持されます。アクセスコントロールポリシーやセキュリティゾーンなどの他の設定は保持されないことに注意してください。

Management Center に切り替えると、Device Manager を使用して Threat Defense デバイスを管理できなくなります。

始める前に

ファイアウォールが高可用性用に設定されている場合は、まず、Device Manager（可能な場合）または **configure high-availability disable** コマンドを使用して、高可用性設定を中断する必要があります。アクティブなユニットから高可用性を中断することをお勧めします

手順

ステップ 1 Device Manager で、Cisco Smart Software Manager からデバイスを登録解除します。

ステップ 2 （必要に応じて）管理インターフェイスを設定します。

マネージャアクセスにデータインターフェイスを使用する場合でも、管理インターフェイスの設定を変更する必要がある場合があります。Device Manager 接続に管理インターフェイスを使用していた場合は、Device Manager に再接続する必要があります。

- マネージャアクセス用のデータインターフェイス：管理インターフェイスには、データインターフェイスに設定されたゲートウェイが必要です。デフォルトでは、管理インターフェイスは DHCP から IP アドレスとゲートウェイを受信します。DHCP からゲートウェイを受信しない場合（たとえば、管理インターフェイスをネットワークに接続していない場合）、ゲートウェイはデフォルトでデータインターフェイスになり、何も設定する必要はありません。DHCP からゲートウェイを受信した場合は、代わりに管理インターフェイスに静的 IP アドレスを設定し、ゲートウェイをデータインターフェイスに設定する必要があります。
- マネージャアクセス用の管理インターフェイス：静的 IP アドレスを設定する場合は、デフォルトゲートウェイもデータインターフェイスではなく一意のゲートウェイに設定してください。DHCP を使用する場合は、DHCP からゲートウェイを正常に取得できると仮定して、何も設定する必要はありません。

ステップ 3 [デバイス (Device)] [システム設定 (Device System Settings)] [中央管理 (Central Management)] [Management Center] [Management Center] [デバイス (Device)] [システム設定 (System Settings)] [中央管理 (Central Management)] [Management Center] の順に選択し、[続行 (Proceed)] をクリックして Management Center の管理を設定します。

ステップ 4 [Management Center/CDOの詳細 (Management Center/CDO Details)] を設定します。

図 27: Management Center/CDO の詳細

Configure Connection to Management Center or CDO


Provide details to register to the management center/CDO.

Management Center/CDO Details

Do you know the Management Center/CDO hostname or IP address?

Yes No


Threat Defense



10.89.5.16
fe80::6a87:c6ff:fea6:4c00/64

→

Management Center/CDO



10.89.5.35

Management Center/CDO Hostname or IP Address

10.89.5.35

Management Center/CDO Registration Key

●●●● 👁

NAT ID

Required when the management center/CDO hostname or IP address is not provided. We recommend always setting the NAT ID even when you specify the management center/CDO hostname or IP address.

11203

Connectivity Configuration

Threat Defense Hostname

1120-3

DNS Server Group

CustomDNSServerGroup ▼

Management Center/CDO Access Interface

Data Interface

Please select an interface ▼

Management Interface [View details](#)

CANCEL
CONNECT

- a) [Management Center/CDOのホスト名またはIPアドレスを知っていますか (Do you know the FMC hostname or IP address)] で、IP アドレスまたはホスト名を使用して Management Center に到達できる場合は [はい (Yes)] をクリックし、Management Center が NAT の背

後にあるか、パブリック IP アドレスまたはホスト名がない場合は[いいえ (No)] をクリックします。

双方向の SSL 暗号化通信チャネルを 2 台のデバイス間に確立するには、少なくとも 1 台以上のデバイス (Management Center または Threat Defense デバイス) に到達可能な IP アドレスが必要です。

- b) [はい (Yes)] を選択した場合は、**管理センター/CDO のホスト名/IP アドレス**を入力します。
- c) **Management Center/CDO 登録キー**を指定します。

このキーは、Threat Defense デバイスを登録するとき Management Center でも指定する任意の 1 回限りの登録キーです。登録キーは 37 文字以下にする必要があります。有効な文字には、英数字 (A~Z、a~z、0~9)、およびハイフン (-) があります。この ID は、Management Center に登録する複数のデバイスに使用できます。
- d) [NAT ID] を指定します。

この ID は、Management Center でも指定する任意の 1 回限りの文字列です。いずれかのデバイスの IP アドレスのみを指定する場合、このフィールドは必須です。両方のデバイスの IP アドレスがわかっている場合でも、NAT ID を指定することを推奨します。NAT ID は 37 文字以下にする必要があります。有効な文字には、英数字 (A~Z、a~z、0~9)、およびハイフン (-) があります。この ID は、Management Center に登録する他のデバイスには使用できません。NAT ID は、正しいデバイスからの接続であることを確認するために IP アドレスと組み合わせて使用されます。IP アドレス/NAT ID の認証後にのみ、登録キーがチェックされます。

ステップ 5 [接続の設定 (Connectivity Configuration)] を設定します。

- a) [FTDホスト名 (FTD Hostname)] を指定します。

Management Center/CDO アクセスインターフェイスのアクセスにデータインターフェイスを使用する場合、この FQDN がこのインターフェイスに使用されます。

- b) [DNSサーバーグループ (DNS Server Group)] を指定します。

既存のグループを選択するか、新しいグループを作成します。デフォルトの DNS グループは **CiscoUmbrellaDNSServerGroup** と呼ばれ、OpenDNS サーバーが含まれます。

Management Center/CDO アクセスインターフェイスにデータインターフェイスを選択する場合は、この設定でデータインターフェイス DNS サーバーを設定します。セットアップウィザードで設定した管理 DNS サーバーは、管理トラフィックに使用されます。データ DNS サーバーは、DDNS (設定されている場合) またはこのインターフェイスに適用されるセキュリティポリシーに使用されます。管理トラフィックとデータトラフィックの両方が外部インターフェイス経由で DNS サーバーに到達するため、管理に使用したものと同一 DNS サーバーグループを選択する可能性があります。

Management Center では、この Threat Defense デバイスに割り当てるプラットフォーム設定ポリシーでデータインターフェイス DNS サーバーが設定されます。Management Center に Threat Defense デバイスを追加すると、ローカル設定が維持され、DNS サーバーはプラットフォーム設定ポリシーに追加されません。ただし、DNS 設定を含む Threat Defense デバ

イスに後でプラットフォーム設定ポリシーを割り当てると、その設定によってローカル設定が上書きされます。Management Center と Threat Defense デバイスを同期させるには、この設定に一致するように DNS プラットフォーム設定をアクティブに設定することをお勧めします。

また、ローカル DNS サーバーは、DNS サーバーが初期登録で検出された場合にのみ Management Center で保持されます。

FMC アクセスインターフェイスに管理インターフェイスを選択する場合は、この設定で管理 DNS サーバーを構成します。

- c) **Management Center/CDO アクセスインターフェイス**については、任意の構成済みインターフェイスを選択してください。

管理インターフェイスは、Threat Defense デバイスを Management Center に登録した後に、管理インターフェイスまたは別のデータインターフェイスのいずれかに変更できます。

- ステップ 6** (任意) 外部インターフェイスではないデータインターフェイスを選択した場合は、デフォルトルートを追加します。

インターフェイスを通過するデフォルトルートがあることを確認するように求めるメッセージが表示されます。外部を選択した場合は、セットアップウィザードの一環としてこのルートがすでに設定されています。別のインターフェイスを選択した場合は、Management Center に接続する前にデフォルトルートを手動で設定する必要があります。

管理インターフェイスを選択した場合は、この画面に進む前に、ゲートウェイを一意的ゲートウェイとして設定する必要があります。

- ステップ 7** (任意) データインターフェイスを選択した場合は、[ダイナミック DNS (DDNS) 方式の追加 (Add a Dynamic DNS (DDNS) method)]をクリックします。

DDNS は、IP アドレスが変更された場合に Management Center が完全修飾ドメイン名 (FQDN) で Threat Defense デバイスに到達できるようにします。[デバイス (Device)]>[システム設定 (System Settings)]>[DDNS サービス (DDNS Service)]を参照して DDNS を設定します。

Management Center に Threat Defense デバイスを追加する前に DDNS を設定すると、Threat Defense デバイスは、Cisco Trusted Root CA バンドルからすべての主要 CA の証明書を自動的に追加し、Threat Defense デバイスが HTTPS 接続のために DDNS サーバー証明書を検証できるようにします。Threat Defense は、DynDNS リモート API 仕様

(<https://help.dyn.com/remote-access-api/>) を使用するすべての DDNS サーバーをサポートします。

マネージャアクセスに管理インターフェイスを使用する場合、DDNS はサポートされません。

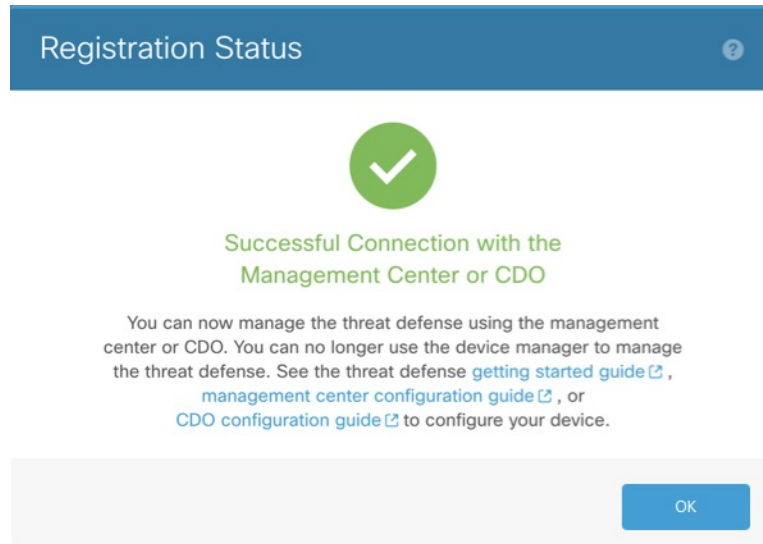
- ステップ 8** [接続 (Connect)]をクリックします。[登録ステータス (Registration Status)]ダイアログボックスには、Management Center への切り替えに関する現在のステータスが表示されます。[Management Center/CDO 登録設定の保存 (Saving Management Center/CDO Registration Settings)]のステップの後、Management Center に移動してファイアウォールを追加します。

Management Center への切り替えをキャンセルする場合は、[登録のキャンセル (Cancel Registration)]をクリックします。キャンセルしない場合は、[Management Center/CDO 登録設

定の保存（Saving Management Center/CDO Registration Settings）]のステップが完了するまで Device Manager のブラウザウィンドウを閉じないでください。閉じた場合、プロセスは一時停止し、Device Manager に再接続した場合のみ再開されます。

[Management Center/CDO登録設定の保存（Saving Management Center/CDO Registration Settings）]のステップの後に Device Manager に接続したままにする場合、その後 [Management Center または CDO との正常接続（Successful Connection with Management Center or CDO）] ダイアログボックスが表示され、Device Manager から切断されます。

図 28: 正常接続



Management Center から Device Manager への切り替え

代わりに Device Manager を使用するよう、オンプレミスまたはクラウド提供型の Management Center によって現在管理されている Threat Defense デバイスを設定できます。

ソフトウェアを再インストールすることなく、Management Center から Device Manager に切り替えることができます。Management Center から Device Manager に切り替える前に、Device Manager がすべての設定要件を満たしていることを確認します。Device Manager から Management Center に切り替える場合は、[Device Manager から Management Center への切り替え \(68 ページ\)](#) を参照してください。



注意 Device Manager に切り替えると、デバイスの設定は削除され、システムはデフォルト設定に戻ります。ただし、管理 IP アドレスとホスト名は維持されます。

手順

ステップ 1 Management Center で、[デバイス (Devices)] > [デバイス管理 (Device Management)] ページからファイアウォールを削除します。

ステップ 2 SSH またはコンソールポートを使用して、Threat Defense CLI に接続します。SSH の場合、管理 IP アドレスへの接続を開き、**admin** ユーザー名 (または管理者権限を持つ他のユーザー) で Threat Defense CLI にログインします。

(Firepower モデル) コンソールポートはデフォルトで FXOS CLI になります。**connect ftd** コマンドを使用して、Threat Defense CLI に接続します。SSH セッションは Threat Defense CLI に直接接続します。

管理 IP アドレスに接続できない場合、次のように対処します。

- 管理物理ポートが、機能しているネットワークに接続されていることを確認します。
- 管理 IP アドレスとゲートウェイが管理ネットワーク用に設定されていることを確認します。**configure network ipv4/ipv6 manual** コマンドを使用します。

ステップ 3 現在リモート管理モードになっていることを確認します。

show managers

例 :

```
> show managers
Type                : Manager
Host                : 10.89.5.35
Display name       : 10.89.5.35
Identifier          : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration       : Completed
```

ステップ 4 リモート マネージャを削除すると、マネージャなしのモードになります。

configure manager delete uuid

リモート管理からローカル管理に直接移行することはできません。複数のマネージャが定義されている場合は、識別子 (UUID と呼ばれます。**show managers** コマンドを参照) を指定する必要があります。各マネージャ エントリを個別に削除します。

例 :

```
> configure manager delete
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

ステップ 5 ローカル マネージャを設定します。

configure manager local

これで、Web ブラウザで <https://management-IP-address> にアクセスしてローカル マネージャを開くことができるようになりました。

例：

```
> configure manager local  
Deleting task list  
  
> show managers  
Managed locally.
```

【注意】 シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023 Cisco Systems, Inc. All rights reserved.

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。