VMware 向け仮想 Cisco Firepower Management Center のセットアップ

Cisco Firepower システム仮想アプライアンスをインストールしたら、設定プロセスを完了する必要があります。このプロセスにより、信頼された管理ネットワーク上で新しいアプライアンスが通信できるようになります。また、管理者パスワードを変更し、エンドユーザ ライセンス契約書（EULA）に同意する必要もあります。

設定プロセスを使用すると、時間の設定、デバイスの登録とライセンス認証、更新のスケジューリングなどのさまざまな管理レベルの初期タスクを実行することもできます。設定と登録中に選択されたオプションによって、システムで作成され、適用されるデフォルト インターフェイス、インライン セット、ゾーン、およびポリシーが決定されます。

これらの初期設定とポリシーの目的は、オプションを制限することではなく、すぐに使用できるエクスペリエンスを提供し、短時間で展開を設定できるようにすることです。仮想アプライアンスをどのように初期設定したかに関係なく、その設定はいつでも Cisco Firepower Management Center を使用して変更できます。つまり、設定中に、たとえば検出モードやアクセス制御ポリシーを選択しても、特定のデバイス、ゾーン、またはポリシー設定に固定されることはありません。

どのように展開する場合でも、最初に、初期化するアプライアンスの電源を入れてください。初期化が完了したら、VMware コンソールを使用してログインし、設定を完了します。

VI OVF テンプレートで展開すると、展開でウィザードを使用してネットワークを設定することができます。セットアップ ウィザードを使用しない場合、または ESXi OVF テンプレートを使用して展開することを選択した場合は、スクリプトを使用してネットワークを設定します。ネットワークを設定した後で、管理ネットワーク上のコンピュータを使用して、Cisco Firepower Management Center の Web インターフェイスを参照するための設定プロセスを完了します。

（注） 複数のアプライアンスを展開している場合は、先に Firepower NGIPSv アプライアンスを設定してから、管理元の Firepower Management Center を設定します。デバイスの初期設定プロセスを使用すれば、デバイスを Firepower Management Center に事前登録できます。Firepower Management Center の設定プロセスを使用すれば、事前登録した管理対象デバイスを追加してライセンス認証できます。

仮想アプライアンスの初期化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	管理者

仮想アプライアンスをインストールした後、仮想アプライアンスに初めて電源を入れると初期化が自動的に開始されます。

注意：起動時間は、サーバ リソースの可用性など、さまざまな要因によって異なります。初期化が完了するまでに最大で 40 分かかることがあります。初期化は中断しないでください。中断すると、アプライアンスを削除して、最初からやり直さなければならないことがあります。

仮想アプライアンスを初期化するには、次の手順を使用します。

手順

1. アプライアンスの電源をオンにします。

   vSphere Client で、インベントリ リストからインポートした仮想アプライアンスの名前を右クリックし、コンテキスト メニューで [電源(Power)] > [電源オン(Power On)] を選択します。

2. VMware コンソール タブで初期化を監視します。

次の作業

- 設定を完了するには、仮想 Cisco Firepower Management Center の設定(16 ページ)を参照してください。

仮想 Cisco Firepower Management Center の設定

仮想 Cisco Firepower Management Center の設定に必要な手順は、VI OVF テンプレートまたは ESXi OVF テンプレートのいずれを使用して展開したかによって異なります。

- VI OVF テンプレートを使用して展開し、セットアップ ウィザードを使用した場合は、Firepower システム の必須設定を行ったときに指定したパスワードを使用して、仮想 Firepower Management Center にログインし、Firepower システム を使用してローカル アプライアンスの設定、ライセンスとデバイスの追加、トラフィックを監視および管理するためのポリシーの適用を行います。詳細については、『*Firepower System Configuration Guide*』を参照してください。
- ESXi OVF テンプレートを使用して展開した場合、または VI OVF テンプレートを使用して展開したときに Firepower システム の必須設定を行っていない場合は、仮想 Firepower Management Center の設定は 2 段階のプロセスになります。仮想 Firepower Management Center を初期化した後で、VMware コンソールでスクリプトを実行します。これにより、管理ネットワーク上で通信するアプライアンスを設定できます。次に、管理ネットワーク上のコンピュータを使用して、アプライアンスの Web インターフェイスを参照するための設定プロセスを完了します。
- ESXi OVF テンプレートを使用して仮想 Firepower Management Center を展開し、VI OVF テンプレートを使用してすべての仮想デバイスを展開する場合は、1 ページのセットアップ ウィザードを使用して仮想 Firepower Management Center へすべてのデバイスを同時に登録できます。詳細については、初期設定ページ:Cisco Firepower Management Center Virtual(17 ページ)を参照してください。

仮想 Firepower Management Center ネットワーク設定の自動化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス(Access)
任意(Any)	任意(Any)	Management Center	グローバルのみ	管理者

新しい仮想 Cisco Firepower Management Center を初期化した後で、管理ネットワーク上でアプライアンスが通信できるようにするための設定を行う必要があります。VMware コンソールでスクリプトを実行して、この手順を完了します。

Firepower システム は、IPv4 と IPv6 の両方の管理環境にデュアル スタック実装を提供します。最初に、スクリプトから IPv4 管理設定を構成(または無効に)するように要求されてから、IPv6 に移ります。IPv6 展開では、ローカル ルータから設定値を取得できます。IPv4 または IPv6 管理 IP アドレス、ネットマスクまたはプレフィックス長、およびデフォルト ゲートウェイを指定する必要があります。

スクリプトのプロンプトに従う場合に、複数の選択肢がある質問では、選択肢が `(y/n)` のように括弧で囲まれて示されます。デフォルト値は、`[y]` のように大カッコ内に列挙されます。Enter キーを押して、選択を確定します。

はじめる前に

仮想アプライアンスの初期化(15 ページ)に示すように、デバイスを初期化します。

手順

1. ユーザ名 `admin` と、VI OVF テンプレートを使用して展開したときにセットアップ ウィザードで指定した管理者アカウントのパスワードを使用して、VMware コンソールで仮想 Firepower Management Center にログインします。

   ウィザードを使用してパスワードを変更していない場合、または ESXi OVF テンプレートを使用して展開している場合は、パスワードとして `Admin123` を使用します。

2. admin プロンプトで、次のスクリプトを実行します。

   ```
   sudo /usr/local/sf/bin/configure-network
   ```

3. スクリプトのプロンプトに従ってください。最初に IPv4 管理設定を構成（または無効に）してから、IPv6 に移ります。ネットワーク設定を手動で指定する場合は、次の手順を実行する必要があります。

   — ネットマスクを含む IPv4 アドレスをドット付き 10 進形式で入力します。たとえば、`255.255.0.0` のネットマスクを指定できます。

   — IPv6 アドレスをコロン区切りの 16 進形式で入力します。IPv6 プレフィックスの場合、ビット数を指定します（たとえば、`112` のプレフィックス長）。

4. 設定値が正しいことを確認します。

   設定値を誤って入力した場合は、プロンプトで「`n`」と入力して、Enter キーを押します。その後、正しい情報を入力できます。VMware コンソールには、設定が実装されるときにメッセージが表示されることがあります。

5. アプライアンスからログアウトします。

次の作業

- Cisco Firepower Management Center の Web インターフェイスを使用して設定を完了するには、初期設定ページ：Cisco Firepower Management Center Virtual（17 ページ）に進みます。

初期設定ページ：Cisco Firepower Management Center Virtual

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	Management Center	グローバルだけ	管理者

仮想 Cisco Firepower Management Center では、アプライアンスの Web インターフェイスにログインして、設定ページで初期設定オプションを指定することによって、設定プロセスを完了する必要があります。管理者パスワードを変更して、まだの場合はネットワーク設定を指定し、EULA に同意します。

設定プロセスでは、デバイスの登録およびライセンス付与を行うこともできます。デバイスを登録する前に、Firepower Management Center をリモート マネージャとして追加するだけでなく、そのデバイス自体の設定プロセスを完了する必要があります。完了していない場合、デバイスの登録が失敗します。

手順

1. 管理ネットワーク上のコンピュータから、サポートされているブラウザで `https://`*`MC_name`*`/` にアクセスします。ここで *`MC_name`* は、前の手順で Firepower Management Center の管理インターフェイスに割り当てたホスト名または IP アドレスです。

2. ユーザ名 `admin` と、VI OVF テンプレートによる展開でセットアップ ウィザードに指定した管理者アカウントのパスワードを使用してログインします。ウィザードを使用してパスワードを変更していない場合は、パスワードとして `Admin123` を使用します。

設定ページが表示されます。設定の完了方法については、次の項を参照してください。

パスワードの変更（Change Password）（18 ページ）

ネットワーク設定（18 ページ）

時刻設定（19 ページ）

ルール更新の定期インポート（19 ページ）

地理情報の定期的な更新（19 ページ）

自動バックアップ（20 ページ）

ライセンス設定（20 ページ）

ライセンス設定（20 ページ）

エンド ユーザ ライセンス契約（21 ページ）

3. 完了したら、[適用（Apply）] をクリックします。

   仮想 Firepower Management Center が選択内容に従って設定されます。

4. 初期設定が正常に終了したことを確認するには、[タスクステータス（Task Status）] ページ（[システム（System）] > [モニタリング（Monitoring）] > [タスクステータス（Task Status）]）を使用します。

   ページは 10 秒ごとに自動的に更新されます。最初のデバイス登録およびポリシーの適用のタスクについて、[完了（Completed）] ステータスが表示されるまでページを監視します。設定の一部として、侵入ルールまたは位置情報の更新を設定した場合は、これらのタスクも監視することができます。

Cisco Firepower Management Center を使用する準備が整いました。展開の設定の詳細については、『*Firepower System Configuration Guide*』を参照してください。

次の作業

- 次のステップ（22 ページ）に進みます。

パスワードの変更（Change Password）

`admin` アカウントのパスワードを変更する必要があります。このアカウントは管理者特権が付与されているため、削除できません。Cisco では、大文字と小文字が混在する 8 文字以上の英数字で、1 つ以上の数字を含む強力なパスワードを使用することを推奨しています。辞書に掲載されている単語の使用は避けてください。

ネットワーク設定

Cisco Firepower Management Center のネットワーク設定によって、それが管理ネットワーク上で通信できるようになります。スクリプトを使用してすでにネットワークを設定しているため、ページのこの項には情報が設定されています。

事前入力された設定を変更する場合は、Firepower システム によって IPv4 と IPv6 の両方の管理環境にデュアル スタック実装が提供されることに注意してください。管理ネットワーク プロトコル（[IPv4]、[IPv6]、または [両方（Both）]）を指定する必要があります。選択した内容に応じて、設定のページにはさまざまなフィールドが表示されます。ここで IPv4 または IPv6 の管理 IP アドレス、ネットマスクまたはプレフィックスの長さ、およびデフォルトのゲートウェイを設定する必要があります。

- IPv4 の場合、ドット付き 10 進表記でアドレスおよびネットマスクを設定する必要があります（例：`255.255.0.0` のネットマスク）。
- IPv6 ネットワークの場合は、[ルータ自動設定を使用してIPv6アドレスを割り当てる（Assign the IPv6 address using router autoconfiguration）] チェックボックスをオンにして IPv6 のネットワーク設定を自動的に割り当てることができます。このチェックボックスを選択しない場合は、コロンで区切られた 16 進表記のアドレスおよびプレフィックス内のビット数（たとえば、`112` のプレフィックス長）を設定する必要があります。

また、デバイスに対してホスト名とドメインの他に、3 つまでの DNS サーバを指定することもできます。

時刻設定

Firepower Management Center の時刻は、手動で設定することも、ネットワーク タイム プロトコル（NTP）サーバから NTP 経由で設定することもできます。

また、**admin** アカウント用のローカル Web インターフェイスで使用されるタイム ゾーンを指定することもできます。現在のタイム ゾーンをクリックし、ポップアップ ウィンドウを使用してそのタイム ゾーンを変更します。Firepower Management Center

管理対象デバイスの時刻が、管理している Firepower Management Center と同期している必要があります。Firepower Management Center は NTP ソースとしてサポートされていないため、物理 NTP サーバを使用して時刻を設定することをお勧めします。

注意：Firepower Management Center Virtual を手動時刻で VMware に設定すると、（デフォルトでは）ホストからの実行に時間がかかります。ESX/ESXi ホストを NTP サーバとして設定できますが、この方法は VMware のベスト プラクティスではありません。VMware では、ESX/ESXi ホストを正式な時刻（NTP）サーバに設定することをベスト プラクティスと見なします。

ルール更新の定期インポート

新しい脆弱性が発見された場合、Cisco の脆弱性調査チーム（VRT）は侵入ルールの更新を公開します。ルールの更新では、新規および更新された侵入ルールおよびプリプロセッサ ルール、既存のルールの変更されたステータス、変更されたデフォルト侵入ポリシーの設定が提供されます。ルールの更新では、ルールを削除して、新しいルール カテゴリおよびシステム変数を提供する場合もあります。

展開で侵入検知および防御を実行するよう計画している場合、Cisco は、[ルール更新の定期インポートを有効にする（Enable Recurring Rule Update Imports）] を選択することを推奨しています。

それぞれのルール更新の後で、システムが侵入についての [ポリシーの再適用（Policy Reapply）] を実行するよう設定するだけでなく、[インポート頻度（Import Frequency）] も指定することができます。初期設定プロセスの一部としてルールの更新を実行するには、[今すぐインストール（Install Now）] を選択します。

（注） ルールの更新には、新しいバイナリが含まれている場合があります。ルール更新のダウンロードおよびインストールのプロセスが、自身のセキュリティ ポリシーに適合していることを確認します。加えて、ルール更新のサイズが大きい場合があるため、ネットワーク使用率の低い時間帯にルールをインポートするようにしてください。

地理情報の定期的な更新

仮想 Cisco Firepower Management Center を使用して、ダッシュボードおよび Context Explorer の地理情報統計を監視するだけでなく、システムで生成されたイベントに関連付けられているルーテッド IP アドレスの地理情報を表示することができます。

Cisco Firepower Management Center の地理情報データベース（GeoDB）には、IP アドレスに関連するインターネット サービス プロバイダ（ISP）、接続タイプ、プロキシ情報、正確な位置情報などの情報が含まれています。定期的な GeoDB の更新を有効にすることで、システムが常に最新の地理情報を使用するようにすることができます。展開で地理情報システムに関連する分析の実行を計画する場合、Cisco は [定期的な週次更新を有効にする（Enable Recurring Weekly Updates）] を選択することを推奨しています。

GeoDB について、週次の更新頻度を指定できます。ポップアップ ウィンドウを使用してタイム ゾーンを変更するには、そのタイム ゾーンをクリックします。初期設定プロセスの一部としてデータベースをダウンロードするには、[今すぐインストール（Install Now）] を選択します。

（注） GeoDB の更新はサイズが大きくなることがあるため、ダウンロードの後のインストールに最大で 45 分かかることがあります。GeoDB は、ネットワークの使用量が少ないときに更新してください。

自動バックアップ

Firepower Management Center には、障害時に設定を復元できるように、データをアーカイブするためのしくみが用意されています。初期設定の一部として、[自動バックアップを有効にする（Enable Automatic Backups）] を選択することができます。

この設定を有効にすると、スケジュールされたタスクが作成され、このタスクによって Firepower Management Center の設定のバックアップが週次に作成されます。

ライセンス設定

組織にとって最適な Firepower システム の展開を実現するために、さまざまな機能のライセンスを取得することができます。Firepower Management Center を使用して、それ自体およびその管理対象のデバイスを管理できます。Firepower システム によって提供されるライセンスのタイプは、管理するデバイスのタイプによって異なります。

- Firepower、ASA FirePOWER、および NGIPSv の各デバイスの場合は、従来のライセンスを使用する必要があります。

デフォルトで、Firepower Management Center はドメイン制御、ホスト、アプリケーション、ユーザ ディスカバリの実行と、SSL および TLS で暗号化されたトラフィックの復号化と検査を行うことができます。機能別の従来のライセンスを取得すると、管理対象デバイスでさまざまな機能を実行することができます。ライセンスに関する完全な情報については、*Firepower System Configuration Guide* または Firepower Management Center のオンライン ヘルプを参照してください。

デバイスの登録（Device Registration）

仮想 Cisco Firepower Management Center は、Firepower システム が現在サポートしているすべての物理的および仮想的なデバイスを管理することができます。初期設定のプロセス中に、事前に登録したほとんどのデバイスを Firepower Management Center に追加できます。ただし、デバイスと Firepower Management Center が NAT デバイスによって分離されている場合は、設定プロセスが完了した後で、デバイスを追加する必要があります。

Firepower Management Center に管理対象デバイスを登録する際、登録時にアクセス制御ポリシーを自動的にデバイスに適用する場合は、[デフォルトのアクセス制御ポリシーを適用する（Apply Default Access Control Policies）] チェックボックスをオンのままにしておきます。Firepower Management Center が各デバイスに対してどのポリシーを適用するかは、選択できません。選択できるのはポリシーを適用するかどうかのみであることに注意してください。各デバイスに適用されるポリシーは、デバイスの設定時に選択した検出モードによって異なります。これを次の表に示します。

表 1　検出モードごとに適用されるデフォルトのアクセス制御ポリシー

検出モード	デフォルトのアクセス コントロール ポリシー
インライン	[デフォルト侵入防御（Default Intrusion Prevention）]
パッシブ	[デフォルト侵入防御（Default Intrusion Prevention）]
アクセス制御	[デフォルト アクセス制御（Default Access Control）]
ネットワーク ディスカバリ	[デフォルト ネットワーク ディスカバリ（Default Network Discovery）]

Firepower Management Center を使用して以前にデバイスを管理しており、そのデバイスの最初のインターフェイス設定を変更すると、例外が発生します。このような場合、新しい Firepower Management Center のページによって適用されるポリシーは、変更した（現在の）デバイスの設定によって異なります。設定されたインターフェイスがある場合、Firepower Management Center は Default Intrusion Prevention ポリシーを適用します。そうでない場合、Firepower Management Center は Default Access Control ポリシーを適用します。

仮想デバイスの検出モードの詳細については、『*Cisco NGIPSv Quick Start Guide for Vmware*』を参照してください。物理デバイスについては、『*Firepower システム Installation Guide*』を参照してください。

(注) デバイスがアクセス制御ポリシーに適合していない場合は、ポリシーの適用に失敗します。この不適合には、複数の要因が考えられます。たとえば、ライセンスの不一致、モデルの制限、パッシブとインラインの問題、その他の構成ミスなどです。最初のアクセス コントロール ポリシーの適用が失敗すると、最初のネットワーク ディスカバリ ポリシーの適用も失敗します。障害の原因となる問題を解決した後は、アクセス コントロール ポリシーおよびネットワーク ディスカバリ ポリシーを手動でデバイスに適用する必要があります。アクセス コントロール ポリシーの適用に失敗する原因となる問題の詳細については、*Firepower System Configuration Guide* を参照してください。

デバイスを追加するには、デバイスの登録時に指定した**登録キー**のほかに、**ホスト名**または **IP アドレス**を入力します。これは、ユーザが指定した単純なキーで、ライセンス キーとは異なりますので注意してください。

次に、チェックボックスを使用して、ライセンスが付与された機能をデバイスに追加します。すでに Cisco Firepower Management Center に追加したライセンスしか選択できないので注意してください。また、いくつかのライセンスについては、他の機能を有効にするまで、有効にできません。たとえば、最初に Protection を有効にするまで、デバイス上で Control を有効にすることはできません。

アーキテクチャとリソースの制限のために、すべての管理対象デバイスですべてのライセンスがサポートされるわけではありません。ただし、セットアップ ページでは、管理対象デバイスでサポートされていないライセンスの有効化は**可能な**状態です。これは、後にならないと Cisco Firepower Management Center がデバイス モデルを判別できないためです。システムは無効なライセンスを有効にすることはできません。また、無効なライセンスを有効にしようとしても、ユーザが使用できるライセンス数は減少しません。

ライセンスを有効にした後で [追加(Add)] をクリックしてデバイスの登録設定を保存します。必要に応じてデバイスを追加します。間違ったオプションを選択した場合、またはデバイス名を誤って入力した場合は、[削除(Delete)] をクリックして削除します。その後で、デバイスをもう一度追加できます。

エンド ユーザ ライセンス契約

EULA をよく読んで、規定に従う場合はチェックボックスをオンにします。指定した情報がすべて正しいことを確認して、[適用(Apply)] をクリックします。

Cisco Firepower Management Center が選択内容に従って設定されます。管理者ロールを持つ `admin` ユーザとして Web インターフェイスにログインします。Firepower Management Center の初期設定を完了するには、初期設定ページ:Cisco Firepower Management Center Virtual(17 ページ)の手順 3. に進みます。

VMware ツールの有効化

VMware ツールは仮想マシンのオペレーティング システム上にインストールされるユーティリティのスイートで、仮想マシンのパフォーマンスを強化し、VMware 製品で使い勝手のよい多数の機能を実現します。このシステムは、すべての仮想アプライアンスで次のプラグインをサポートします。

- guestInfo
- powerOps
- timeSync
- vmbackup
- スナップショット

VMware ツールのサポートされるプラグインおよびすべての機能の詳細については、VMware Web サイト(http://www.vmware.com/)を参照してください。

仮想アプライアンスをセットアップした後、管理対象デバイスでコマンド ライン インターフェイス（CLI）を使用するか、または仮想 Firepower Management Center でブラウザを使用して、仮想アプライアンスの VMware ツールを有効にできます。詳細については、仮想 Firepower Management Center での VMware ツールの設定（22 ページ）を参照してください。

仮想 Firepower Management Center での VMware ツールの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	仮想 Management Center	任意（Any）	管理者

Web インターフェイスを使用して [設定（Configuration）] メニューのチェックボックスをオンまたはオフにできます。CLI を使用して仮想 Cisco Firepower Management Center で VMware ツールを有効にすることはできません。

仮想 Cisco Firepower Management Center で VMware ツールを有効または無効にするには、次の手順に従います。

1. Web ブラウザを使用して、Cisco Firepower Management Center にログインし、[システム（System）] > [設定（Configuration）] > [VMware ツール（VMware Tools）] を選択します。それから、[VMware ツールの有効化（Enable VMware Tools）] チェックボックスをオンまたはオフにし、[保存（Save）] をクリックします。

次のステップ

仮想アプライアンスの初期設定プロセスが完了し、正常に終了したことが確認できたら、Cisco では、展開での管理を容易にするためのさまざまな管理タスクを完了することを推奨しています。また、デバイスの登録やライセンスの取得など、初期設定で省略したタスクも完了する必要があります。以下のセクションで説明するタスクの詳細、および展開の設定を開始する方法の詳細については、『*Firepower System Configuration Guide*』を参照してください。

個別のユーザ アカウント

初期セットアップが完了した時点で、システム上の唯一のユーザは、管理者ロールとアクセス権を持つ `admin` ユーザです。このロールを所有しているユーザは、シェルまたは CLI を介したアクセスを含め、システムのすべてのメニューおよび設定にアクセスできます。セキュリティおよび監査上の理由から、Cisco では、`admin` アカウント（および Administrator ロール）の使用を制限することを推奨しています。

システムを使用する各ユーザに対して個別のアカウントを作成すると、各ユーザによって行われたアクションと変更を組織で監査できるほか、各ユーザに関連付けられたユーザ アクセス ロールを制限することができます。これは、ほとんどの設定および分析タスクを実行する Cisco Firepower Management Center で特に重要です。たとえば、アナリストはネットワークのセキュリティを分析するためにイベント データにアクセスする必要がありますが、展開の管理機能にアクセスする必要はありません。

システムには、さまざまな管理者およびアナリスト用に設計された 10 個の事前定義のユーザ ロールが用意されています。また、特別なアクセス権限を持つカスタム ユーザ ロールを作成することもできます。

ヘルス ポリシーとシステム ポリシー

デフォルトでは、すべてのアプライアンスにシステムの初期ポリシーが適用されます。システム ポリシーは、メール リレー ホストのプリファレンスや時間同期の設定など、展開内の複数のアプライアンスで共通している可能性が高い設定を管理します。Cisco では、Firepower Management Center を使用して、防御センター自身およびその管理対象デバイスすべてに同じシステム ポリシーを適用することを推奨しています。

デフォルトで、Firepower Management Center にはヘルス ポリシーも適用されます。ヘルス ポリシーは、ヘルス モニタリング機能の一部として、システムが展開環境内でアプライアンスのパフォーマンスを継続して監視するための基準を提供します。Cisco では、Firepower Management Center を使用して、その管理対象デバイスすべてにヘルス ポリシーを適用することを推奨しています。

ソフトウェアとデータベースの更新

展開を開始する前に、アプライアンス上でシステム ソフトウェアを更新する必要があります。Cisco では、展開環境内のすべてのアプライアンスが Firepower システム の最新のバージョンを実行することを推奨しています。展開環境でこれらのアプライアンスを使用する場合は、最新の侵入ルール更新、VDB、および GeoDB もインストールする必要があります。

注意 : Firepower システム のいずれかの部分を更新する前に、更新に付属のリリース ノートまたはアドバイザリテキストを読んでおく必要があります。リリース ノートでは、サポートされるプラットフォーム、互換性、前提条件、警告、特定のインストールおよびアンインストールの手順など重要なデータが提供されます。

次のステップ