VMware 向け Cisco Firepower Virtual の設定

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。これにより、新しいアプライアンスは信頼された管理ネットワーク上で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。

設定プロセスにより、時間の設定、デバイスの登録とライセンシング、スケジュールの更新など、管理レベルの多数の初期タスクを実行することもできます。設定および登録時に選択したオプションにより、システムが作成および適用するデフォルトのインターフェイス、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。

これらの初期設定およびポリシーの目的は、すぐに使用できるエクスペリエンスを提供し、オプションを制限せずにユーザが展開を迅速に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、アプライアンスのタイプに応じて次のいずれかの方法で設定を完了します。

Cisco Firepower NGIPSv

Cisco Firepower NGIPSv 仮想アプライアンスには Web インターフェイスがありません。VI OVF テンプレートで展開すると、展開ウィザードを使用してアプライアンスを Firepower Management Center へ登録するなど、初期設定を行うことができます。ESXi OVF テンプレートで展開する場合は、対話式のコマンドライン インターフェイス（CLI）を使用して初期設定を実行する必要があります。

仮想 Cisco Firepower Management Center

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）	Admin

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. 以下のようにして、アプライアンスの電源をオンにします。
   - VMware vCloud Director の Web ポータルで、ディスプレイから [vApp] を選択して [Start] をクリックします。
   - 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

VI OVF テンプレートを使用し、展開中に Firepower システムの必須設定を行った場合は、これ以上の設定は必要ありません。

ESXi OVF テンプレート使用した場合、または VI OVF テンプレートで展開したときに Firepower システム の必須設定を行わなかった場合は、CLI を使用した Firepower NGIPSv デバイスの設定(16 ページ)に進みます。

CLI を使用した Firepower NGIPSv デバイスの設定

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)	NGIPSv	任意(Any)	Admin

Firepower NGIPSv デバイスには Web インターフェイスがないため、ESXi OVF テンプレートで展開した場合には、CLI を使用して仮想デバイスを設定する必要があります。VI OVF テンプレートを使用して展開し、かつ展開時にセットアップ ウィザードを使用しなかった場合、CLI を使用して Firepower システムで必要な設定を行うことができます。

(注) VI OVF テンプレートで展開しており、セットアップ ウィザードを使用した場合は、仮想デバイスが設定されているため、これ以上の処理は必要ありません。

新しく設定されたデバイスに初めてログインするときに、EULA を読んで同意する必要があります。次に、セットアップ プロンプトに従って管理者パスワードを変更し、デバイスのネットワーク設定と検出モードを設定します。

セットアップ プロンプトに従う際に、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。選択を確定するには、Enter キーを押します。

CLI では、物理デバイスのセットアップ Web ページで要求される設定情報とほぼ同じ情報が要求されます。詳細については、『*Firepower 7000 and 8000 Series Installation Guide*』を参照してください。

(注) 初期セットアップの完了後に仮想デバイスに関するこれらの設定を変更するには、CLI を使用する必要があります。詳細については、『*Firepower Management Center Configuration Guide*』の「Command Line Reference」の章を参照してください。

デバイス ネットワークの設定について

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。ユーザは 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。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。デバイスを再起動するまで、ホスト名は syslog に反映されないので注意してください。

検出モードについて

仮想デバイスに対して検出モードを選択すると、システムが最初にデバイス インターフェイスをどのように設定するか、およびこれらのインターフェイスがインライン セットとセキュリティ ゾーンのどちらに属するかが決定されます。検出モードの設定を後で変更することはできません。これは、システムによるデバイス初期設定の調整を容易にするために、セットアップ中にユーザが選択するオプションに過ぎません。一般的には、デバイスがどのように展開されているかに基づいて検出モードを選択する必要があります。

パッシブ

デバイスがパッシブ展開されている場合は、このモードを侵入検知システム（IDS）として選択します。パッシブ展開では、仮想デバイスは、ネットワークベース ファイルとマルウェアの検出、セキュリティ インテリジェンス モニタリング、およびネットワーク検出を実行できます。

インライン

デバイスがインラインで展開されている場合は、このモードを侵入防御システム（IPS）として選択します。

（注）IPS 展開の一般的な方法はフェール オープンにし、一致しないトラフィックを許可することですが、仮想デバイスのインライン セットにはバイパス機能がありません。

アクセス コントロール

デバイスがアクセス制御展開の一部としてインライン展開されている場合、つまり、アプリケーション、ユーザ、および URL 制御を実行する場合に、このモードを選択します。アクセス制御を実行するように設定されているデバイスは、通常、フェール クローズであり、一致しないトラフィックをブロックします。ルールで、通過させるトラフィックが明示的に指定されます。

アクセス制御の展開では、高度なマルウェア対策、ファイル制御、セキュリティ インテリジェンス フィルタリング、およびネットワーク検出も実行できます。

ネットワーク ディスカバリ

デバイスがパッシブ展開されている場合は、ホスト、アプリケーション、およびユーザ ディスカバリのみを実行するためにこのモードを選択します。

次の表に、選択された検出モードに基づいてシステムが作成するインターフェイス、インライン セット、およびゾーンを示します。

表 1　検出モードに基づく初期設定

検出モード	セキュリティ ゾーン	インライン セット	インターフェイス
インライン	内部と外部	デフォルトのインライン セット	デフォルトのインライン セットに追加された最初のペア（内部ゾーンに 1 つと外部ゾーンに 1 つ）
パッシブ	パッシブ	なし	パッシブ ゾーンに割り当てられた最初のペア
アクセス制御	なし	なし	なし
ネットワーク ディスカバリ	パッシブ	なし	パッシブ ゾーンに割り当てられた最初のペア

セキュリティ ゾーンは Firepower Management Center レベルの設定であり、ユーザが実際にデバイスを Firepower Management Center に追加するまで作成されないことに注意してください。その時点で、Firepower Management Center 上に適切なゾーン（内部、外部、またはパッシブ）がすでに存在している場合、システムは一覧で示されたインターフェイスを既存のゾーンに追加します。ゾーンが存在しない場合は、システムがそれを作成してインターフェイスを追加します。インターフェイス、インライン セット、およびセキュリティ ゾーンの詳細については、『*Firepower Management Center Configuration Guide*』を参照してください。

手順

1. VMware コンソールを開きます。
2. VMware コンソールで、ユーザ名として `admin`、および展開のセットアップ ウィザードで指定した新しい admin アカウント パスワードを使用して、仮想デバイスにログインします。

   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。

   直後に、デバイスから EULA を読むようにプロンプトが表示されます。
3. EULA を読んで同意します。
4. `admin` アカウントのパスワードを変更します。このアカウントには Configuration CLI アクセス レベルが付与されており、削除することはできません。

   (注) 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。
5. デバイスのネットワーク設定を構成します。最初に IPv4 の管理設定を行い(または無効にして)、次に IPv6 を設定します。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)。

   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。
6. デバイスをどのように展開したかに基づいて、検出モードを指定します。

   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。完了したら、このデバイスを Cisco Firepower Management Center に登録するよう要求され、CLI プロンプトが表示されます。

次の作業

- 次の Cisco Firepower Management Center への仮想デバイスの登録(18 ページ)へ進み、CLI を使用してデバイスをその管理元となる Cisco Firepower Management Center に登録します。デバイスは Cisco Firepower Management Center を使用して管理する必要があります。今すぐデバイスを登録しない場合は、後でデバイスにログインしてそれを登録するまで Cisco Firepower Management Center に追加できません。

Cisco Firepower Management Center への仮想デバイスの登録

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)	NGIPSv	任意(Any)	Admin CLI Configuration

仮想デバイスには Web インターフェイスがないため、CLI を使用して仮想デバイスを Cisco Firepower Management Center に登録する必要があります(物理でも仮想でも可)。初期設定プロセス中にデバイスを Firepower Management Center に登録する方が簡単です。これは、すでにデバイスの CLI にログインしているためです。

デバイスを登録するには、`configure manager add` コマンドを使用します。デバイスを Firepower Management Center へ登録するには、自己生成の一意の英数字登録キーが必ず必要です。これはユーザが指定する簡単なキーで、ライセンス キーとは異なります。

ほとんどの場合は、登録キーと一緒に Firepower Management Center の IP アドレスを指定する必要があります。たとえば次のようにします。

```
configure manager add XXX.XXX.XXX.XXX my_reg_key
```

XXX.XXX.XXX.XXX は、管理している Firepower Management Center の IP アドレスで、*my_reg_key* は、仮想デバイスに入力した登録キーです。

(注) vSphere Client を使用して仮想デバイスを Firepower Management Center へ登録する場合は、管理元の Firepower Management Center の（ホスト名ではなく）IP アドレスを使用する必要があります。

ただし、デバイスと Firepower Management Center がネットワーク アドレス変換（NAT）デバイスによって分けられている場合は、登録キーと一緒に一意の NAT ID を入力し、IP アドレスの代わりに DONTRESOLVE を指定します。たとえば次のようにします。

```
configure manager add DONTRESOLVE my_reg_key my_nat_id
```

my_reg_key は仮想デバイスに入力した登録キーで、*my_nat_id* は NAT デバイスの NAT ID です。

デバイス（Firepower Management Center ではない）が NAT デバイスの背後にある場合は、一意の NAT ID を登録キーと共に入力し、Firepower Management Center のホスト名または IP アドレスを指定します。次に例を示します。

```
configure manager add [hostname | ip address] my_reg_key my_nat_id
```

my_reg_key は仮想デバイスに入力した登録キーで、*my_nat_id* は NAT デバイスの NAT ID です。

手順

1. CLI 設定（管理者）の権限を持つユーザとして仮想デバイスにログインします。
   - VMware コンソールから初期設定を実行している場合は、admin ユーザとしてすでにログインしています。このユーザは必要なアクセス レベルを持っています。
   - そうでない場合は、VMware コンソールを使用してデバイスにログインします。または、デバイスのネットワーク設定が完了している場合は、SSH を使用してデバイスの管理 IP アドレスまたはホスト名にログインします。
2. プロンプトで、次のような構文の configure manager add コマンドを使用してデバイスを Cisco Firepower Management Center に登録します。

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

値は次のとおりです。

- {*hostname* | *IPv4_address* | *IPv6_address* | DONTRESOLVE} は、Firepower Management Center の IP アドレスを表します。Firepower Management Center が直接アドレス指定できない場合は、DONTRESOLVE を使用します。
- *reg_key* は、デバイスを Firepower Management Center へ登録するのに必要な一意の英数字による登録キーです。
- *nat_id* は、Cisco Firepower Management Center とデバイス間の登録プロセス中に使用されるオプションの英数字文字列です。ホスト名が DONTRESOLVE に設定されている場合に必須です。

3. アプライアンスからログアウトします。

次の作業

- Firepower Management Center をすでに設定している場合は、Web インターフェイスにログインし、[デバイス管理（Device Management）ページ（[デバイス（Device）] > [デバイス管理（Device Management）]）を使用してデバイスを追加します。詳細については、『*Firepower Management Center Configuration Guide*』の「Managing Devices」の章を参照してください。
- Firepower Management Center をまだ設定していない場合、仮想 Firepower Management Center については『*Cisco Firepower Management Center Virtual Quick Start Guide for VMware*』、物理 Firepower Management Center については『*Cisco Firepower Management Center Installation Guide*』を参照してください。

VMware ツールの有効化

VMware Tools 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

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設定した後、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）を使用して、仮想アプライアンスの VMware ツールを有効化できます。

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）	NGIPSv	任意（Any）	Admin

仮想デバイスにログインし、次のコマンドの 1 つ以上を入力できます。

- `show vmware-tools` は、VMware ツールがシステム上で実行されているかどうかを表示します。
- `configure vmware-tools enable` </code> は、仮想デバイスで VMware ツールを有効にします。
- `configure vmware-tools disable` は、仮想デバイスで VMware ツールを無効にします。

仮想デバイスで VMware ツールを有効にするには:

1. コンソールで仮想デバイスにログインし、CLI プロンプトで、VMware ツールを有効または無効にするコマンド、あるいは、VMware ツールが有効であるかどうかを表示するコマンドを入力して、**Enter** を押します。

次の手順

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 Management Center 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。**

次の手順