Firewall Management Center Virtual 初期管理および設定

Firewall Management Center Virtual の初期セットアッププロセスが完了し、正常にセットアップされたことを確認したら、展開の管理を容易にするさまざまな管理タスクを実行することを推奨します。また、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、およびデプロイメントの設定を開始する方法の詳細については、ご使用のバージョンの『Secure Firewall Management Center Configuration Guide』『』の全文を参照してください。

個別のユーザー アカウント

初期設定が完了した時点で、システム上の唯一の Web インターフェイスのユーザーは、管理者ロールとアクセス権を持つ**admin**ユーザーです。その役割を持つユーザーはシステムへのすべてのメニューと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、**admin**アカウント（およびAdministrator ロール）の使用を制限することをお勧めします。ユーザーアカウントは、Firewall Management Center Virtual GUI の **[システム（System）]** > **[ユーザー（Users）]** > **[ユーザー（User）]** ページで管理します。

（注） シェルを使用した Firewall Management Center Virtual へのアクセスと Web インターフェイスを使用した Firewall Management Center Virtual へのアクセスのための **admin** アカウントは異なるため、別のパスワードを使用できます。

システムを使用する各ユーザーに対して個別のアカウントを作成すると、各ユーザー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、各ユーザーに関連付けられたユーザーア

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 Firewall Management Center Virtual 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、Webインターフェイスを使用して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ー 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 ユーザー ロールを作成することもできます。

デバイス登録

は、現在システムでサポートされているすべてのデバイス（物理または仮想）を管理できます。

- Firewall Threat Defense：統合した次世代ファイアウォールと次世代 IPS デバイスを提供します。
- Firewall Threat Defense Virtual：複数のハイパーバイザ環境で作業し、管理オーバーヘッドを削減し、運用効率を向上させるために設計された 64 ビットのバーチャル デバイス。
- Cisco ASA with FirePOWER Services（または ASA FirePOWER モジュール）：最も重要なシステムポリシーを提供し、検出とアクセス制御のために、システムにトラフィックを渡します。ただし、 の Web インターフェイスを使用して ASA FirePOWER のインターフェイスを設定することはできません。Cisco ASA with FirePOWER Services には、ASA プラットフォームに一意なソフトウェアと CLI があり、これらを使用してシステムをインストールし、他のプラットフォーム固有の管理タスクを実行することができます。
- 7000 および 8000 シリーズ アプライアンス：システム用に特別に設計された物理デバイス。7000 および 8000 シリーズ デバイスのスループットはさまざまですが、多くの同じ機能が共有されます。一般に、8000 シリーズ デバイスは 7000 シリーズ デバイスよりも高性能で、8000 シリーズ 高速パス ルール、リンク集約、およびスタックなどの追加機能もサポートします。デバイスを に登録する前に、そのデバイス上でリモート管理を設定する必要があります。
- NGIPSv：VMware vSphere 環境で展開する 64 ビットのバーチャル デバイス。NGIPSv のデバイスは、冗長性とリソースの共有、スイッチ、およびルーティングのようなシステムのハードウェアベースの機能のどちらもサポートしていません。

に管理対象デバイスを登録するには、 GUI の**[デバイス（Device）]** > **[デバイス管理（Device Management）]**ページを使用します。ご使用のバージョンの『Secure Firewall Management Center Configuration Guide』でデバイス管理情報を参照してください。

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。シスコでは、を使用して、それ自体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、 にはヘルス ポリシーも適用されます。ヘルスポリシーは、ヘルスモニター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。シスコでは、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。展開環境内のすべてのアプライアンスでシステムの最新のバージョンを実行することを推奨します。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 システムの一部分を更新する前に、その更新に関する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。

でバージョン 6.5 以降を実行している場合は、次のようになります。

は設定の一環として次のアクティビティを確立し、システムを最新の状態に保ち、データをバックアップします。

- 週次自動 GeoDB 更新
- とその管理対象デバイスにおける最新ソフトウェアをダウンロードする週次タスク。

重要 このタスクは、 にソフトウェアの更新のみをダウンロードします。ユーザーは、このタスクがダウンロードした更新をインストールする必要があります。詳細については、『*Cisco Secure Firewall Management Center Upgrade Guide*』および『』を参照してください。

- ローカルに保存された設定のみの バックアップを実行する週次タスク。

でバージョン 6.6 以降を実行している場合、初期設定の一環として、はシスコのサポートサイトから最新の脆弱性データベース（VDB）の更新をダウンロードしてインストールします。これは 1 回限りの操作です。

Web インターフェイスのメッセージセンターを使用して、これらのアクティビティのステータスを確認できます。システムがこれらのアクティビティのいずれかを設定できず、がインター

ネットにアクセスできる場合は、ご使用のバージョンの『*Secure Firewall Management Center Configuration Guide*』およびの説明に従って、これらのアクティビティをご自身で設定することをお勧めします。

トラブルシューティング

このセクションでは、仮想マシンへの Firewall Management Center Virtual デプロイメントに関連する基本的な障害対応手順について説明します。

SSH 接続の失敗

Firewall Management Center Virtual は完全に動作しており、SSH 接続を除き、ユーザーインターフェイスとコンソール接続は正しく機能しています。特定のシナリオでは、Firewall Management Center Virtual の初回起動中に SSH ホストキーファイルが破損して、SSH 接続が失敗することがあります。

SSH 接続の失敗を示唆する次のような兆候を確認できます。

1. Firewall Management Center Virtual の初回起動中、特に SSH デーモン（sshd）が起動しているときに、ディスク I/O エラーが発生する場合があります。これにより、SSH キーファイル（sshd によって生成される ssh_host* ファイル）が空になります。

   ls -lrt /etc/ssh total 16

   ```
   -rw-r--r-- 1 root root 1746 Jan 17 23:31 ssh_config-openssh
   -rw-r--r-- 1 root root 6027 Jan 17 23:42 sshd_config
   -rw-r--r-- 1 root root 1293 Jan 17 23:42 ssh_config
   -rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_dsa_key
   -rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_dsa_key.pub
   -rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_ecdsa_key
   -rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_ecdsa_key.pub
   -rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_ed25519_key
   -rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_ed25519_key.pub
   -rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_rsa_key
   -rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_rsa_key.pub
   ```

2. ディスク I/O の問題については、`/var/log/messages` ファイルを確認できます。このファイルには、SSH キーファイルが生成されたときと同じタイムスタンプの前後に（I/O エラーを示す）誤ったデータが含まれている可能性があります。

前述したような、Firewall Management Center Virtual の初回起動中に発生する可能性のある SSH 障害を解決するには、次の手順を実行する必要があります。

1. Firewall Management Center Virtual にログインします。
2. Firewall Management Center Virtual CLI で**エキスパート**モードで **sudo reboot** コマンドを実行し、正常なリブートを開始します。
3. 次のコマンドを実行して、空の SSH キーファイルを削除します。

   ```
   cd /etc/ssh/
   rm ssh_host*
   ```

4. 次のコマンドを実行して sshd サービスを再起動し、SSH キーファイルを適切に再生成します。

```
/etc/rc.d/init.d/sshd stop
/etc/rc.d/init.d/sshd start
```

（注） SSH キーファイルが空であることがわかっている場合にのみ、この回避手順を実行してください。不明な場合は、TAC ケースを送信して詳細に調査することをお勧めします。

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。