バックアップと復元の使用

バックアップ/復元は、システム保守プランの重要な部分です。各組織のバックアップ計画は高度に個別化されていますが、ASA FirePOWER モジュールにはデータをアーカイブするメカニズムがあり、障害発生時にはデータを復元できます。

バックアップ対象は次のとおりです。

- アクセス ポリシー、侵入ポリシー、およびアイデンティティ ポリシー
- ローカル データベース
- イベント

バックアップと復元に関する次の制限事項に注意してください。

- バックアップは、バックアップを作成した製品バージョンに対してのみ有効です。
- バックアップの復元は、そのバックアップの作成に使用したものと同じバージョンの ASA FirePOWER モジュール ソフトウェアを実行している場合のみ可能です。

注意 ASA FirePOWER モジュール間で設定ファイルをコピーするために、バックアップおよび復元プロセスを使用しないでください。設定ファイルには、ASA FirePOWER モジュールを一意に識別する情報が含まれているため、共有することはできません。

注意 侵入ルールのアップデートを適用した場合、それらのアップデートはバックアップされません。復元**後に**、最新のルールのアップデートを適用する必要があります。

アプライアンスまたはローカル コンピュータにバックアップ ファイルを保存できます。

- バックアップ ファイルの作成 （2 ページ）
- バックアップ プロファイルの作成 （3 ページ）
- ローカル ホストからのバックアップのアップロード （4 ページ）
- バックアップ ファイルからのアプライアンスの復元 （5 ページ）

バックアップ ファイルの作成

ライセンス：任意

ASA FirePOWER モジュールのバックアップは、モジュール インターフェイスを使用して実行できます。既存のシステム バックアップを表示して使用するには、[Backup Management] ページに移動します。イベントデータに加えて、アプライアンスの復元に必要なすべてのコンフィギュレーション ファイルを含むバックアップ ファイルを定期的に保存する必要があります。設定の変更をテストする際にも、システムをバックアップして、必要に応じて保存されている設定に戻せるようにすることができます。バックアップ ファイルを、アプライアンスに保存するか、ローカル コンピュータに保存するかを選択できます。

アプライアンスに十分なディスク スペースがない場合は、バックアップ ファイルを作成できません。バックアップ プロセスが使用可能なディスク スペースの 90% 以上を使用する場合、バックアップは失敗することがあります。必要に応じて、古いバックアップ ファイルを削除するか、古いバックアップ ファイルをアプライアンスの外部に転送してください。

あるいは、バックアップ ファイルが 4GB を超える場合は、SCP 経由でリモート ホストにコピーします。バックアップ ファイルが 4 GB を超えている場合、ローカル コンピュータからのバックアップのアップロードは実行できません。

⚠

注意 セキュリティ ゾーンとのインターフェイスのアソシエーションを設定してある場合、それらのアソシエーションはバックアップされません。それらは、復元後に再設定する必要があります。詳細はセキュリティ ゾーンの操作を参照してください。

ASA FirePOWER モジュールのバックアップ ファイルを作成するには、次の手順を実行します。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Tools] > [Backup/Restore] の順に選択します。

[Backup Management] ページが表示されます。

ステップ 2 [Device Backup] をクリックします。

[Create Backup] ページが表示されます。

ステップ 3 [Name] フィールドに、バックアップ ファイルの名前を入力します。英数字、句読記号、およびスペースを使用できます。

ステップ 4 オプションで、バックアップの完了時に通知を受けるためには、[Email] チェック ボックスをオンにして、用意されているテキスト ボックスに電子メール アドレスを入力します。

（注） 電子メール通知を受信するには、メール リレー ホストおよび通知アドレスの設定で説明されているように、リレー ホストを設定する必要があります。

ステップ 5 必要に応じて、Secure Copy Protocol（SCP）を使用してバックアップ アーカイブを異なるマシンにコピーするには、[Copy when complete] チェックボックスをオンにしてから、用意されているテキスト ボックスに以下の情報を入力します。

- [Host] フィールド：バックアップのコピー先となるマシンのホスト名または IP アドレス
- [Path] フィールド：バックアップのコピー先となるディレクトリへのパス
- User] フィールド：リモート マシンへのログインに使用するユーザ名
- [Password] フィールド：そのユーザ名のパスワード。パスワードの代わりに SSH 公開キーを使用してリモートマシンにアクセスする場合は、[SSH Public Key] フィールドの内容を、そのマシンの指定ユーザの authorized_keys ファイルにコピーします。

このオプションをオフにする場合、バックアップ中に使用された一時ファイルがシステムによってリモート サーバに保存されます。このオプションをオンにする場合は、一時ファイルはリモート サーバに保存されません。

ヒント Cisco は、システム障害が発生した場合にアプライアンスを復元できるように、バックアップをリモート ロケーションに定期的に保存することを推奨します。

ステップ 6 次の選択肢があります。

- バックアップ ファイルをアプライアンスに保存するには、[Start Backup] をクリックします。

バックアップ ファイルは /var/sf/backup ディレクトリに保存されます。

バックアップ プロセスが完了すると、[Restoration Database] ページでファイルを参照できます。バックアップ ファイルを復元する方法について詳しくは、バックアップ ファイルからのアプライアンスの復元 （5 ページ）を参照してください。

- この設定を後で使用できるバックアップ プロファイルとして保存するには、[Save as New] をクリックします。

バックアップ プロファイルを変更または削除するには、[Configuration] > [ASA FirePOWER Configuration] > [Tools] > [Backup/Restore] の順に選択して、[Backup Profiles] をクリックします。詳細については、「バックアップ プロファイルの作成 （3 ページ）」を参照してください。

バックアップ プロファイルの作成

ライセンス：任意

[Backup Profiles] ページを使用して、さまざまな種類のバックアップに使用する設定値を含むバックアップ プロファイルを作成できます。後にアプライアンスのファイルをバックアップするときに、これらのプロファイルの 1 つを選択できます。

ヒント　バックアップ ファイルの作成 （2 ページ）で説明されているようにバックアップ ファイルを作成すると、バックアップ プロファイルが自動的に作成されます。

バックアップ プロファイルの作成方法：

ステップ 1　[Configuration] > [ASA FirePOWER Configuration] > [Tools] > [Backup/Restore] の順に選択します。

[Backup Management] ページが表示されます。

ステップ 2　[Backup Profiles] タブをクリックします。

[Backup Profiles] ページが開き、既存のバックアップ プロファイルのリストが表示されます。

ヒント　編集アイコンをクリックして既存のプロファイルを変更するか、または削除アイコンをクリックしてリストからプロファイルを削除することができます。

ステップ 3　[Create Profile] をクリックします。

[Create Backup] ページが表示されます。

ステップ 4　バックアップ プロファイルの名前を入力します。英数字、句読記号、およびスペースを使用できます。

ステップ 5　バックアップ プロファイルを必要に合わせて設定します。

このページのオプションについて詳しくは、バックアップ ファイルの作成 （2 ページ）を参照してください。

ステップ 6　バックアップ プロファイルを保存するには、[Save as New] をクリックします。

[Backup Profiles] ページが開き、新しいプロファイルがリストに表示されます。

ローカル ホストからのバックアップのアップロード

ライセンス：任意

表「バックアップ管理」で説明されているダウンロード機能を使用してローカルホストにバックアップ ファイルをダウンロードした場合は、ASA FirePOWER モジュールにそのファイルをアップロードできます。

バックアップ ファイルに PKI オブジェクトが含まれている場合、内部 CA と内部証明書オブジェクトに関連付けられた秘密キーは、アップロードの際にランダムに生成されるキーによって再暗号化されます。

ヒント　ローカルホストからは、4GB より大きいバックアップはアップロードできません。代わりに、バックアップを SCP 経由でリモート ホストにコピーし、そこから取得することができます。

ローカル ホストからバックアップをアップロードする方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Tools] > [Backup/Restore] の順に選択します。

[Backup Management] ページが表示されます。

ステップ 2 [Upload Backup] をクリックします。

[Upload Backup] ページが表示されます。

ステップ 3 [Choose File] をクリックして、アップロードするバックアップ ファイルに移動します。

アップロードするファイルを選択した後に、[Upload Backup] をクリックします。

ステップ 4 [Backup Management] をクリックして、[Backup Management] ページに戻ります。

バックアップ ファイルがアップロードされ、バックアップ リストに表示されます。ASA FirePOWER モジュールによってファイルの整合性が検証されたら、[Backup Management] ページを更新して、詳細なファイル システム情報を確認します。

バックアップ ファイルからのアプライアンスの復元

ライセンス：任意

[Backup Management] ページを使用して、バックアップ ファイルからアプライアンスを復元できます。バックアップを復元するには、バックアップ ファイル内の VDB のバージョンが、アプライアンスの現在の VDB のバージョンと一致している必要があります。復元プロセスが完了したら、シスコの最新のルール アップデートを適用する必要があります。

⚠

注意 仮想 Firepower Management Center で作成されたバックアップを物理 Firepower Management Center に復元しないでください。システム リソースに負荷をかける可能性があります。仮想バックアップを物理 Firepower Management Center に復元する必要がある場合は、サポートに連絡してください。

バックアップ ファイルに PKI オブジェクトが含まれている場合、内部 CA と内部証明書オブジェクトに関連付けられた秘密キーは、アップロードの際にランダムに生成されるキーによって再暗号化されます。

ローカル ストレージを使用する場合、バックアップ ファイルは /var/sf/backup に保存されて、/var パーティションで使用されているディスク領域の量とともに [Backup Management] ページの下部に一覧表示されます。

（注） バックアップが完了した後にライセンスを追加した場合は、このバックアップを復元するときに、それらのライセンスが削除されたり上書きされたりすることはありません。復元の際の競合を防止するためにも、バックアップを復元する前に、これらのライセンスを（それらが使用されている場所をメモした上で）削除し、バックアップを復元した後で、追加して再設定してください。競合が発生した場合は、サポートに連絡してください。

次の表では、[Backup Management] ページの各列とアイコンについて説明します。

表 *1:* バックアップ管理（*Backup Management*）

機能	説明
System Information	元のアプライアンスの名前、タイプ、バージョン。バックアップを復元できるのは、同一のアプライアンス タイプとバージョンに対してだけであることに注意してください。
Date Created	バックアップ ファイルが作成された日時
File Name	バックアップ ファイルのフルネーム
VDB Version	バックアップ時にアプライアンスで実行されている脆弱性データベース（VDB）のビルド。
Location	バックアップ ファイルの場所
Size (MB)	バックアップ ファイルのサイズ（メガバイト）
View	バックアップ ファイルの名前をクリックすると、圧縮されたバックアップ ファイルに含まれるファイルのリストが表示されます。
Restore	バックアップ ファイルが選択された状態でクリックすると、そのバックアップ ファイルがアプライアンスに復元されます。VDB バージョンがバックアップ ファイルの VDB のバージョンと一致しない場合、このオプションは無効になります。
Download	バックアップ ファイルが選択された状態でクリックすると、そのバックアップ ファイルがローカル コンピュータに保存されます。
Delete	バックアップ ファイルが選択された状態でクリックすると、そのバックアップ ファイルが削除されます。
Move	以前に作成したローカル バックアップを選択した状態でクリックすると、そのバックアップが指定のリモート バックアップ ロケーションに送信されます。

バックアップ ファイルからのアプライアンスの復元方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Tools] > [Backup/Restore] の順に選択します。

[Backup Management] ページが表示されます。

ステップ 2 バック アップ ファイルの内容を確認するには、ファイルの名前をクリックします。

マニフェストが表示され、各ファイルの名前、所有者と権限、およびファイル サイズと日付がリストされます。

ステップ 3 [Backup Management] をクリックして、[Backup Management] ページに戻ります。

ステップ 4 復元するバックアップ ファイルを選択して、[Restore] クリックします。

[Restore Backup] ページが表示されます。

バックアップの VDB バージョンがアプライアンスに現在インストールされている VDB のバージョンと一致しない場合、[Restore] ボタンはグレー表示されることに注意してください。

注意 この手順では、すべての設定ファイルが上書きされます。

ステップ 5 ファイルを復元するには、[Replace Configuration Data] を選択します。

ステップ 6 [Restore] クリックして、復元を開始します。

アプライアンスが、指定したバックアップ ファイルを使用して復元されます。

ステップ 7 アプライアンスをリブートします。

ステップ 8 シスコの最新のルール アップデートを適用して、ルール アップデートを再適用します。

ステップ 9 復元されたシステムにポリシーを展開します。