ASA FirePOWER モジュールのアップグレード

このドキュメントでは、管理方法の選択に応じて ASDM または Firepower Management Center を使用して ASA FirePOWER モジュールをアップグレードする方法について説明します。スタンドアロン、フェールオーバー、またはクラスタリングの各シナリオで FirePOWER アップグレードを実行するタイミングを判断するには、ASA アプライアンスまたは ASAv のアップグレード を参照してください。

- ASA FirePOWER アップグレード時の動作 （1 ページ）
- ASDM によって管理される ASA FirePOWER モジュールのアップグレード （2 ページ）
- Firepower Management Center のアップグレード （4 ページ）
- FMCによって管理される ASA FirePOWER モジュールのアップグレード （8 ページ）

ASA FirePOWER アップグレード時の動作

ASA FirePOWER module にトラフィックをリダイレクトする ASA サービス ポリシーは、Firepower ソフトウェア アップグレードの間（Snort プロセスを再起動する特定の設定を導入するときなど）にモジュールがトラフィックを処理する方法を決定します。

表 *1 : ASA FirePOWER* アップグレード中のトラフィックの動作

トラフィック リダイレクションのポリシー	トラフィックの動作
フェール オープン（**sfr fail-open**）	インスペクションなしで転送
フェール クローズ（**sfr fail-close**）	ドロップされる
モニタのみ（**sfr {fail-close}|{fail-open} monitor-only**）	パケットをただちに出力、コピーへのインスペクションなし

ASA FirePOWER 展開時のトラフィックの動作

Snort プロセスを再起動している間のトラフィックの動作は、ASA FirePOWER module をアップグレードする場合と同じです。

アップグレード プロセス中には、設定を複数回展開します。Snort は、通常、アップグレード直後の最初の展開時に再起動されます。展開の前に、特定のポリシーまたはデバイス設定を変更しない限り、それ以外の展開時に再起動されることはありません。詳細については、『『Firepower Management Center 構成ガイド』』の「Configurations that Restart the Snort Process when Deployed or Activated」を参照してください。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。 さらに、Snort プロセスを再起動すると、トラフィック インスペクションが中断されます。サービスポリシーにより、中断中にインスペクションせずにトラフィックをドロップするか通過するかが決定されます。

ASDM によって管理される ASA FirePOWER モジュールのアップグレード

次の手順を使用して、ASDM によって管理される ASA FirePOWER モジュールをアップグレードします。

⚠

注意 構成の変更、手動による再起動、またはアップグレードモジュールのシャットダウンは行わないでください。進行中のアップグレードは再開しないでください。事前のチェック中に、アップグレード プロセスが停止しているように見える場合がありますが、これは想定内の動作です。アップグレードに失敗する、アプライアンスが応答しないなど、アップグレードで問題が発生した場合には Cisco TAC にお問い合わせください。

手順

ステップ 1 ASA のサポートされるバージョンを実行していることを確認します。

ASA と ASA FirePOWER のバージョンには広く互換性があります。ただし、厳密には ASA のアップグレードが必要でない場合でも、問題解決のために、サポートされた最新のバージョンへのアップグレードが必要になることがあります。

そのシーケンスで ASA FirePOWER モジュールをアップグレードする場合の、スタンドアロン、フェールオーバー、クラスタリングのシナリオにおける ASA のアップグレード手順を参照してください。ASA ソフトウェアをアップグレードしない場合でも、ASA のフェールオーバーとクラスタリング アップグレード手順を参照する必要があります。これにより、モジュールのアップグレード前に装置でフェールオーバーまたはクラスタリングの無効化を実行して、トラフィックの損失を回避できます。たとえば、クラスタでは、各セカンダリ ユニットを順次

アップグレードし（クラスタリングの無効化、モジュールのアップグレード、クラスタリングの再有効化を含む）、その後プライマリ ユニットをアップグレードする必要があります。

ステップ 2 アップグレード パッケージは Cisco.com からダウンロードします。

メジャー バージョンの場合。

- バージョン 6.0 ～ 6.2.2 へのアップグレード：
  Cisco_Network_Sensor_**Upgrade**-[version]-[build].**sh**
- バージョン 6.2.3 以降へのアップグレード：
  Cisco_Network_Sensor_**Upgrade**-[version]-[build].**sh.REL.tar**

パッチの場合。

- 5.4.1.x ～ 6.2.1.x へのアップグレード：Cisco_Network_Sensor_**Patch**-[version]-[build].**sh**
- バージョン 6.2.2.1 以降へのアップグレード：
  Cisco_Network_Sensor_**Patch**-[version]-[build].**sh.REL.tar**

シスコサポートおよびダウンロードサイトから直接ダウンロードします。電子メールでパッケージを転送すると、破損する可能性があります。バージョン 6.2.2+ 以降のアップグレード パッケージは署名付きで、単純な .sh ではなく .sh.REL.tar の末尾になります。署名付きのアップグレード パッケージは解凍しないでください。

ステップ 3 ASDM を使用して ASA に接続し、アップグレード パッケージをアップロードします。

a) **[構成（Configuration）] > [ASA FirePOWER の構成（ASA FirePOWER Configuration）] > [Updates]**を選択します。
b) [更新のアップロード（Upload Update）] をクリックします。
c) [ファイルの選択（Choose File）] をクリックして対象ファイルに移動し、更新を選択します。
d) [Upload] をクリックします。

ステップ 4 保留中の構成の変更を展開します。展開しない場合、アップグレードが失敗することがあります。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。 さらに、いくつかの設定を展開することで Snort が再起動されます。これにより、トラフィックのインスペクションが中断し、デバイスのトラフィックの処理方法によっては、再起動が完了するまでトラフィックが中断する場合があります。詳細については、ASA FirePOWER アップグレード時の動作 （1 ページ） を参照してください。

ステップ 5 （バージョン 6.1 以降へのアップグレード）ASA REST API を無効にします。

REST API を無効にしない場合、アップグレードは失敗します。ASA FirePOWER モジュールのバージョン 6.0 以降も実行している場合、ASA 5506-X シリーズのデバイスでは ASA REST API はサポートされません。

ASA の CLI を使用して、REST API を無効にします。

no rest-api agent

次のコマンドを実行して、アップグレード後に REST API を再度有効にすることができます。

rest-api agent

ステップ 6 **[モニタリング（Monitoring）] > [ASA FirePOWER のモニタリング（ASA FirePOWER Monitoring）] > [タスク ステータス（Task Status）]** の順に選択して、必須タスクが完了していることを確認します。

アップグレードの開始時に実行中のタスクは停止し、失敗したタスクとなり、再開できません。後で失敗ステータス メッセージを手動で削除できます。

ステップ 7 **[構成（Configuration）] > [ASA FirePOWER の構成（ASA FirePOWER Configuration）] > [Updates]**を選択します。

ステップ 8 アップロードしたアップグレード パッケージの横にある [インストール（Install）] アイコンをクリックして、モジュールをアップグレードして再起動することを確認します。

トラフィックは、モジュールの設定方法に応じて、アップグレード中にドロップされるか、または検査されることなくネットワークを通過します。詳細については、ASA FirePOWER アップグレード時の動作 （1 ページ）を参照してください。

ステップ 9 [タスク ステータス（Task Status）] ページでアップグレードの進行状況をモニタします。

モジュールのアップグレード中は、そのモジュールに構成の変更を加えないでください。アップグレード ステータスに進行状況が数分間表示されない、またはアップグレードが失敗したことが示されている場合でも、アップグレードを再開したり、デバイスを再起動したりしないでください。代わりに、Cisco TAC に連絡してください。

ステップ 10 アップグレードが完了したら、ASDM を ASA に再接続します。

ステップ 11 **[構成（Configuration）] > [ASA FirePOWER の構成（ASA FirePOWER Configuration）]** の順に選択して、[更新（Refresh）] をクリックします。そうしない場合、インターフェイスが予期しない動作を示すことがあります。

ステップ 12 **[構成（Configuration）] > [ASA FirePOWER の構成（ASA FirePOWER Configuration）] > [システム情報（System Information）]** の順に選択して、モジュールのソフトウェア バージョンが正しいことを確認します。

ステップ 13 サポート サイトで利用可能な侵入ルールの更新や脆弱性データベース（VDB）が現在実行中のバージョンより新しい場合は、新しいバージョンをインストールします。

ステップ 14 リリース ノートに記載されているアップグレード後の構成の変更をすべて完了します。

ステップ 15 構成を再展開します。

Firepower Management Center のアップグレード

Firepower Management Center を使用して ASA FirePOWER モジュールを管理している場合は、モジュールをアップグレードする前に Management Center をアップグレードする必要があります。

スタンドアロンの FMC のアップグレード

この手順を使用して、Firepower Management Center Virtual などのスタンドアロン Firepower Management Center をアップグレードします。

⚠

注意 アップグレードしているアプライアンスとの間での変更の展開、またはアップグレードしているアプライアンスの手動での再起動やシャットダウンは行わないでください。進行中のアップグレードを再開しないでください。事前のチェック中に、アップグレードプロセスが停止しているように見える場合がありますが、これは想定内の動作です。アップグレードに失敗する、アプライアンスが応答しないなど、アップグレードで問題が発生した場合には Cisco TAC にお問い合わせください。

始める前に

ホスト環境と管理対象デバイス アップグレードを含む、アップグレード パスでの位置を確認します。この手順を完全に計画して準備していることを確認します。

手順

ステップ 1 構成が古い管理対象デバイスに展開します。

メニューバーで、[展開（Deploy）]をクリックします。FMCデバイスを選択し、[展開（Deploy）]をもう一度クリックします。アップグレードする前に展開すると、失敗する可能性が減少します。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。 さらに、いくつかの設定を展開することで Snort が再起動されます。これにより、トラフィックのインスペクションが中断し、デバイスのトラフィックの処理方法によっては、再起動が完了するまでトラフィックが中断する場合があります。

ステップ 2 アップグレード前の最終的なチェックを実行します。

- 正常性のチェック：メッセージ センターを使用します（メニュー バーの [System Status] アイコンをクリックします）。導入環境内のアプライアンスが正常に通信していること、およびヘルス モニタによって報告された問題がないことを確認します。
- タスクの実行：また、メッセージセンターで、必須タスクが完了していることを確認します。アップグレードの開始時に実行中のタスクは停止し、失敗したタスクとなり、再開できません。後で失敗ステータス メッセージを手動で削除できます。
- ディスク容量のチェック：最終的なディスク容量のチェックを実行します。空きディスク容量が十分でない場合、アップグレードは失敗します。

ステップ 3 **[System]** > **[Updates]** を選択します。

ステップ 4 使用するアップグレード パッケージの横にある [インストール（Install）] アイコンをクリックして、FMC を選択します。

ステップ 5 [Install] をクリックすると、アップグレードが開始されます。

アップグレードして、FMC を再起動することを確認します。

ステップ 6 ログアウトするまで、メッセージ センターで事前チェックの進行状況をモニタします。

FMC のアップグレード中は、構成に変更を加えたり、デバイスに構成を展開したりしないでください。メッセージセンターに進行状況が数分間表示されない、またはアップグレードが失敗したことが示されている場合でも、アップグレードを再開したり、FMC を再起動したりしないでください。代わりに、Cisco TAC にお問い合わせください。

ステップ 7 可能なときに、FMC に再度ログインします。

- マイナーアップグレード（パッチとホットフィックス）：アップグレードが完了し、FMC が再起動した後にログインできます。
- メジャー アップグレード：アップグレードが完了する前にログインできます。アップグレードの進行状況をモニタし、アップグレード ログとエラー メッセージを確認するために使用できるページが FMC に表示されます。アップグレードが完了し、FMC が再起動すると再度ログアウトされます。リブート後に、再ログインしてください。

ステップ 8 プロンプトが表示されたら、エンド ユーザ ライセンス契約書（EULA）を確認し、承認します。

ステップ 9 アップグレードが成功したことを確認します。

ログイン時に、FMC からアップグレードの成功メッセージが表示されない場合は、**[ヘルプ（Help）]** > **[バージョン情報（About）]** を選択して、現在のソフトウェアのバージョン情報を表示します。

ステップ 10 メッセージ センターを使用して、導入環境に問題がないことを再度確認します。

ステップ 11 侵入ルール（SRU）および脆弱性データベース（VDB）を更新します。

シスコ サポート & ダウンロード サイトで利用可能な SRU や VDB が現在実行中のバージョンより新しい場合は、新しいバージョンをインストールします。詳細については、『Firepower Management Center 構成ガイド』を参照してください。侵入ルールを更新する場合、ポリシーを自動的に再適用する必要はありません。後で適用します。

ステップ 12 リリース ノートに記載されているアップグレード後の構成の変更をすべて完了します。

ステップ 13 構成を再展開します。

すべての管理対象デバイスに再展開します。デバイスに構成を展開しない場合、最終的なアップグレードが失敗し、イメージの再作成が必要になることがあります。

ハイ アベイラビリティ FMC のアップグレード

この手順を使用して、ハイ アベイラビリティ ペアに含まれる Firepower Management Center の Firepower ソフトウェアをアップグレードします。

一度に 1 つのピアをアップグレードします。同期を一時停止した状態で、最初にスタンバイをアップグレードし、次にアクティブをアップグレードします。スタンバイ FMC で事前チェックが開始されると、ステータスがスタンバイからアクティブに切り替わり、両方のピアがアクティブになります。この一時的な状態は *split-brain* と呼ばれていて、アップグレード中を除き、サポートされていません。ペアが split-brain の状況で、構成の変更または展開を行わないでください。同期の再開後は変更内容が失われます。

⚠

注意 アップグレードしているアプライアンスとの間での変更の展開、またはアップグレードしているアプライアンスの手動での再起動やシャットダウンは行わないでください。進行中のアップグレードを再開しないでください。事前のチェック中に、アップグレードプロセスが停止しているように見える場合がありますが、これは想定内の動作です。アップグレードに失敗する、アプライアンスが応答しないなど、アップグレードで問題が発生した場合には Cisco TAC にお問い合わせください。

始める前に

管理対象デバイスのアップグレードなどに関するアップグレードパス内の場所を確認します。この手順を完全に計画して準備していることを確認します。

手順

ステップ 1 アクティブな FMC で、構成が古い管理対象デバイスに展開します。

メニューバーで、[展開（Deploy）]をクリックします。FMCデバイスを選択し、[展開（Deploy）]をもう一度クリックします。アップグレードする前に展開すると、失敗する可能性が減少します。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。 さらに、いくつかの設定を展開することで Snort が再起動されます。これにより、トラフィックのインスペクションが中断し、デバイスのトラフィックの処理方法によっては、再起動が完了するまでトラフィックが中断する場合があります。

ステップ 2 同期を一時停止する前に、メッセージセンターを使用して導入環境に問題がないことを確認します。

FMC メニューバーで、[システム ステータス（System Status）]アイコンをクリックして、メッセージセンターを表示します。導入環境内のアプライアンスが正常に通信していること、およびヘルス モニタによって報告された問題がないことを確認します。

ステップ 3 同期を一時停止します。

a) **[システム（System）]** > **[統合（[Integration）]**を選択します。

b) [ハイ アベイラビリティ（High Availability）] タブで、[同期の一時停止（Pause Synchronization）] をクリックします。

ステップ 4 FMC を一度に 1 つずつアップグレード： 最初はスタンバイ、次はアクティブです。

「スタンドアロンの FMC のアップグレード （5 ページ）」の手順に従います。ただし、初期の展開は省略し、各 FMC で更新が成功したことを確認したら停止します。要約すると、それぞれの FMC で以下の手順を実行します。

a) 最終的なアップグレード前チェック（健全性、実行中のタスク、ディスク容量）を実行します。
b) [System][Updates] > ページで、アップグレードをインストールします。
c) ログアウトするまで進行状況をモニタし、可能な場合な再度ログインします（これは主なアップグレードで 2 回行われます）。
d) アップグレードが成功したことを確認します。

ペアが split-brain の状況で、構成の変更または展開を行わないでください。

ステップ 5 アクティブ ピアにする FMC で、同期を再開します。

a) **[システム（System）] > [統合（Integration）]** の順に選択します。
b) [ハイ アベイラビリティ（High Availability）] タブで、[アクティブにする（Make-Me-Active）] をクリックします。
c) 同期が再開し、その他の FMC がスタンバイ モードに切り替わるまで待ちます。

ステップ 6 メッセージ センターを使用して、導入環境に問題がないことを再度確認します。

ステップ 7 侵入ルール（SRU）および脆弱性データベース（VDB）を更新します。

シスコ サポート & ダウンロード サイトで利用可能な SRU や VDB が現在実行中のバージョンより新しい場合は、新しいバージョンをインストールします。詳細については、『Firepower Management Center 構成ガイド』を参照してください。侵入ルールを更新する場合、ポリシーを自動的に再適用する必要はありません。後で適用します。

ステップ 8 リリース ノートに記載されているアップグレード後の構成の変更をすべて完了します。

ステップ 9 構成を再展開します。

すべての管理対象デバイスに再展開します。デバイスに構成を展開しない場合、最終的なアップグレードが失敗し、イメージの再作成が必要になることがあります。

FMCによって管理されるASAFirePOWERモジュールのアップグレード

この手順を使用して、FMC によって管理される ASA FirePOWER module をアップグレードします。モジュールをいつアップグレードするかは、ASAをアップグレードするかどうか、およびASAの展開によって異なります。

- スタンドアロン ASA デバイスをアップグレードする場合：ASA もアップグレードする場合は、ASA をアップグレードしてリロードした直後に、FMC を使用して ASA FirePOWER モジュールをアップグレードします。
- ASA クラスタとフェールオーバ ペアをアップグレードする場合：トラフィック フローとインスペクションの中断を避けるには、これらのデバイスを 1 つずつ完全にアップグレードします。ASA をアップグレードする場合、各ユニットをリロードして ASA をアップグレードする直前に、FMC を使用して ASA FirePOWER モジュールをアップグレードします。

詳細については、「Asa FirePOWER アップグレードパス：FMC 搭載アップグレードパス：ASA FirePOWER」と ASA アップグレード手順を参照してください。

⚠

注意 アップグレードしているアプライアンスとの間での変更の展開、またはアップグレードしているアプライアンスの手動での再起動やシャットダウンは行わないでください。進行中のアップグレードを再開しないでください。事前のチェック中に、アップグレードプロセスが停止しているように見える場合がありますが、これは想定内の動作です。アップグレードに失敗する、アプライアンスが応答しないなど、アップグレードで問題が発生した場合には Cisco TAC にお問い合わせください。

始める前に

ASA や FMC のアップグレードなどに関するアップグレード パス内の場所を確認します。この手順を完全に計画して準備していることを確認します。

手順

ステップ 1 アップグレード対象デバイスに構成を展開します。

メニューバーで、[展開（Deploy）]をクリックします。FMCデバイスを選択し、[展開（Deploy）]をもう一度クリックします。アップグレードする前に展開すると、失敗する可能性が減少します。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。 さらに、いくつかの設定を展開することで Snort が再起動されます。これにより、トラフィックのインスペクションが中断し、デバイスのトラフィックの処理方法によっては、再起動が完了するまでトラフィックが中断する場合があります。詳細については、ASA FirePOWER アップグレード時の動作 （1 ページ） を参照してください。

ステップ 2 （バージョン 6.1 以降へのアップグレード）ASA REST API を無効にします。

REST API を無効にしない場合、アップグレードは失敗します。ASA FirePOWER モジュールのバージョン 6.0 以降も実行している場合、ASA 5506-X シリーズのデバイスでは ASA REST API はサポートされません。

ASA の CLI を使用して、REST API を無効にします。

no rest-api agent

次のコマンドを実行して、アップグレード後に REST API を再度有効にすることができます。

rest-api agent

ステップ 3 アップグレード前の最終的なチェックを実行します。

- 正常性のチェック：メッセージ センターを使用します（メニュー バーの [System Status] アイコンをクリックします）。導入環境内のアプライアンスが正常に通信していること、およびヘルス モニタによって報告された問題がないことを確認します。
- タスクの実行：また、メッセージセンターで、必須タスクが完了していることを確認します。アップグレードの開始時に実行中のタスクは停止し、失敗したタスクとなり、再開できません。後で失敗ステータス メッセージを手動で削除できます。
- ディスク容量のチェック：最終的なディスク容量のチェックを実行します。空きディスク容量が十分でない場合、アップグレードは失敗します。

ステップ 4 **[System]** > **[Updates]** を選択します。

ステップ 5 使用するアップグレード パッケージの横にある [インストール（Install）] アイコンをクリックして、アップグレードするデバイスを選択します。

アップグレードするデバイスがリストに表示されない場合は、間違ったアップグレード パッケージを選択しています。

（注） 同時にアップグレードするデバイスは 5 台までにすることを強く推奨します。FMC では選択したすべてのデバイスがそのプロセスを完了するまで、アップグレードを停止することはできません。いずれかのデバイスのアップグレードに問題がある場合、問題を解決する前に、すべてのデバイスのアップグレードを完了する必要があります。

ステップ 6 [Install] をクリックし、アップグレードして、デバイスを再起動することを確認します。

トラフィックは、デバイスの設定および展開方法に応じて、アップグレードの間ドロップするか、検査なしでネットワークを通過します。詳細については、ASA FirePOWER アップグレード時の動作 （1 ページ） を参照してください。

ステップ 7 メッセージ センターでアップグレードの進行状況をモニタします。

デバイスのアップグレード中は、構成をそのデバイスに展開しないでください。メッセージセンターに進行状況が数分間表示されない、またはアップグレードが失敗したことが示されている場合でも、アップグレードを再開したり、デバイスを再起動したりしないでください。代わりに、Cisco TAC にお問い合わせください。

ステップ 8 成功したことを確認します。

アップグレードが完了したら、**[デバイス（Devices）]**>**[デバイス管理（Device Management）]** を選択し、アップグレードしたデバイスのソフトウェア バージョンが正しいことを確認します。

ステップ 9 メッセージ センターを使用して、導入環境に問題がないことを再度確認します。

ステップ 10 侵入ルール（SRU）および脆弱性データベース（VDB）を更新します。

シスコ サポート & ダウンロード サイトで利用可能な SRU や VDB が現在実行中のバージョンより新しい場合は、新しいバージョンをインストールします。詳細については、『Firepower Management Center 構成ガイド』を参照してください。侵入ルールを更新する場合、ポリシーを自動的に再適用する必要はありません。後で適用します。

ステップ 11 リリース ノートに記載されているアップグレード後の構成の変更をすべて完了します。

ステップ 12 アップグレードしたデバイスに構成を再度展開します。