



ASA FirePOWER モジュール設定の設定

次の表は、ASA FirePOWER モジュールのローカル構成をまとめたものです。

表 44-1 ローカル設定のオプション

オプション	説明	詳細
情報	アプライアンスに関する現在の情報が表示されます。アプライアンスの名前を変更することもできます。	アプライアンス情報の表示と変更 (44-1 ページ)
Cisco CSI	Collective Security Intelligence クラウドから URL フィルタリングデータをダウンロードしたり、未分類の URL を検索したり、検出されたファイルの診断情報をシスコに送信したりできます。	クラウド通信の有効化 (44-2 ページ)

アプライアンス情報の表示と変更

ライセンス:任意 (Any)

[情報 (Information)] ページには、ASA FirePOWER モジュールに関する情報が表示されます。これには、製品名とモデル番号、オペレーティング システムとバージョン、現在のシステム ポリシーなどの読み取り専用情報が含まれます。このページには、アプライアンスの名前を変更するオプションも用意されています。

次の表で、各フィールドについて説明します。

表 44-2 アプライアンス情報

フィールド	説明
[名前 (Name)]	アプライアンスに割り当てられた名前。この名前は ASA FirePOWER モジュールのコンテキスト内でのみ使用されることに注意してください。ホスト名をアプライアンスの名前として使用できますが、このフィールドに別の名前を入力しても、ホスト名は変更されません。
製品モデル (Product Model)	アプライアンスのモデル名。
シリアル番号 (Serial Number)	アプライアンスのシャーシのシリアル番号。
ソフトウェア バージョン (Software Version)	現在インストールされているソフトウェアのバージョン。

表 44-2 アプライアンス情報(続き)

フィールド	説明
オペレーティング システム (Operating System)	アプライアンス上で現在実行されているオペレーティング システム。
オペレーティング システム バージョン (Operating System Version)	アプライアンス上で現在実行されているオペレーティング システムのバージョン。
IPv4 アドレス (IPv4 Address)	アプライアンスのデフォルトの管理インターフェイス (eth0) の IPv4 アドレス。アプライアンスで IPv4 の管理が無効になっている場合は、このフィールドにそのことが示されます。
IPv6 アドレス (IPv6 Address)	アプライアンスのデフォルトの管理インターフェイス (eth0) の IPv6 アドレス。アプライアンスで IPv6 の管理が無効になっている場合は、このフィールドにそのことが示されます。
現在のポリシー (Current Policies)	現在適用されているアプライアンスレベルのポリシー。ポリシーが最後に適用された後で更新されていると、ポリシーの名前がイタリック体で表示されます。
モデル番号 (Model Number)	アプライアンスのモデル番号。この番号は、トラブルシューティングで重要になる場合があります。

アプライアンスの情報を変更するには、次の手順を実行します。

-
- 手順 1 [設定 (Configuration)] > [ASA FirePOWER 設定 (ASA FirePOWER Configuration)] > [ローカル (Local)] > [設定 (Configuration)] の順に選択します。
[情報 (Information)] ページが表示されます。
- 手順 2 アプライアンス名を変更するには、[名前 (Name)] フィールドに新しい名前を入力します。
名前は、英数字である**必要があり**、数字だけで構成することはできません。
- 手順 3 変更を保存するには、[保存 (Save)] をクリックします。
ページが更新され、変更が保存されます。
-

クラウド通信の有効化

ライセンス: URL Filtering または Malware

ASA FirePOWER モジュールは、シスコの Collective Security Intelligence クラウドに接続してさまざまなタイプの情報を取得します。

- アクセス コントロール ルールに関連付けられたファイル ポリシーにより、デバイスは、ネットワークトラフィックで送信されるファイルを検出できます。ASA FirePOWER モジュールは、シスコクラウドからのデータを使用して、ファイルがマルウェアに相当するかどうかを判定します。[ファイル ポリシーの概要と作成 \(35-5 ページ\)](#) を参照してください。

- URL フィルタリングを有効にすると、ASA FirePOWER モジュールは、一般的にアクセスされる多数の URL のカテゴリとレピュテーションデータを取得し、さらに未分類 URL の検索も実行します。その後、アクセス コントロール ルールの URL 条件をすばやく作成できます。[レピュテーションベースの URL ブロックングの実行\(8-9 ページ\)](#)を参照してください。

ASA FirePOWER モジュールのローカル構成を使用して、次のオプションを指定します。

URL フィルタリングを有効にする (Enable URL Filtering)

カテゴリおよびレピュテーションベースの URL フィルタリングを実行するには、このオプションを有効にする必要があります。

メモリの制約上、一部のモデルでは、小規模でそれほど細分化されていないカテゴリとレピュテーションによって URL フィルタリングが実行されます。たとえば、親 URL のサブサイトがそれぞれ異なる URL カテゴリとレピュテーションを持っている場合、一部のデバイスでは、すべてのサブサイトに対して親 URL のデータが使用されます。具体的な例として、システムは google.com カテゴリとレピュテーションを使用して mail.google.com を評価します。影響を受けるデバイスには、次の ASA モデルが含まれます。ASA 5506-X、ASA 5506H-X、ASA 5506W-X、ASA 5508-X、ASA 5512-X、ASA 5515-X、ASA 5516-X、ASA 5525-X。

不明 URL のクエリ クラウド (Query Cloud for Unknown URL)

監視対象ネットワーク上で誰かがローカル データ セットに存在しない URL を参照しようとしたときに、システムがクラウドを照会できるようにします。

クラウドが URL のカテゴリまたはレピュテーションを識別できない場合や、ASA FirePOWER モジュールがクラウドに接続できない場合、その URL は、カテゴリまたはレピュテーションベースの URL 条件を含むアクセス コントロール ルールと一致しません。URL に手動でカテゴリやレピュテーションを割り当てることはできません。

プライバシー上の理由などで、未分類の URL をシスコクラウドでカタログ化したくない場合は、このオプションを無効にします。

自動アップデートを有効にする (Enable Automatic Updates)

システムが定期的にクラウドに接続して、アプライアンスのローカル データ セットに含まれる URL データの更新を取得できるようにします。クラウドはそのデータを通常 1 日に 1 回更新しますが、自動更新を有効にすると ASA FirePOWER モジュールによるチェックが 30 分ごとに強制的に行われ、常に最新の情報が保持されるようになります。

通常、毎日の更新は小規模ですが、最終更新日から 5 日を超えると、帯域幅によっては新しい URL フィルタリング データのダウンロードに最長 20 分かかる場合があります。その後、更新自体を実行するのに最長で 30 分かかることがあります。

システムがクラウドに接続するタイミングを厳密に制御する必要がある場合は、[URL フィルタリング更新の自動化\(42-8 ページ\)](#)で説明しているように、自動更新を無効にして、代わりにスケジューラを使用できます。



(注) シスコでは、自動更新を有効にするか、またはスケジューラを使用して更新をスケジューリングすることを推奨しています。手動でオンデマンド更新を実行することもできますが、定期的にクラウドに接続するようにシステムを自動化することで、最も関連性の高い最新の URL データを取得できます。

ライセンス

カテゴリおよびレピュテーションベースの URL フィルタリングとデバイスベースのマルウェア検出を実行するには、ASA FirePOWER モジュールで適切なライセンスを有効にする必要があります(ASA FirePOWER モジュールのライセンス(45-1 ページ)を参照)。

ASA FirePOWER モジュールに URL Filtering ライセンスがない場合は、クラウド接続オプションを設定できません。Cisco CSI のローカル設定ページは、ライセンス供与されているオプションのみが表示されます。ライセンスが期限切れになっている ASA FirePOWER モジュールでは、クラウドに接続できません。

ASA FirePOWER モジュールに URL Filtering ライセンスを追加すると、URL フィルタリングの設定オプションが表示されることに加えて、[URL フィルタリングを有効にする (Enable URL Filtering)] と [自動アップデートを有効にする (Enable Automatic Updates)] が自動的に有効になります。必要な場合は、手動でこれらのオプションを無効にすることができます。

インターネットアクセス(Internet Access)

システムは、シスコクラウドへの接続にポート 80/HTTP および 443/HTTPS を使用します。

次の手順は、シスコクラウドとの通信を有効にする方法、および URL データのオンデマンド更新を実行する方法を示しています。更新がすでに進行中である場合は、オンデマンド更新を開始できません。

クラウドとの通信を有効にするには、次の手順を実行します。

-
- 手順 1** [設定 (Configuration)] > [ASA FirePOWER 設定 (ASA FirePOWER Configuration)] > [統合 (Integration)] > [Cisco CSI] の順に選択します。
- [情報 (Information)] ページが表示されます。
- 手順 2** [Cisco CSI] をクリックします。
- [Cisco CSI] ページが表示されます。URL Filtering ライセンスがある場合は、このページに URL データの最終更新時間が表示されます。
- 手順 3** 上記の説明に従って、クラウド接続のオプションを構成します。
- [自動アップデートを有効にする (Enable Automatic Updates)] または [不明 URL のクエリクラウド (Query Cloud for Unknown URL)] を有効にするには、あらかじめ [URL フィルタリングを有効にする (Enable URL Filtering)] を有効にする必要があります。
- 手順 4** [保存 (Save)] をクリックします。
- 設定が保存されます。URL フィルタリングを有効にした場合は、URL フィルタリングが最後に有効になってから経過した時間に応じて、または URL フィルタリングを今回初めて有効にしたかどうかによって、ASA FirePOWER モジュールがクラウドから URL フィルタリング データを取得します。
-

システムの URL データのオンデマンド更新を実行するには、次の手順を実行します。

-
- 手順 1** [設定 (Configuration)] > [ASA FirePOWER 設定 (ASA FirePOWER Configuration)] > [ローカル (Local)] > [設定 (Configuration)] の順に選択します。
- [情報 (Information)] ページが表示されます。
- 手順 2** [URL フィルタリング (URL Filtering)] をクリックします。
- [URL フィルタリング (URL Filtering)] ページが表示されます。

手順 3 [今すぐ更新(Update Now)] をクリックします。

ASA FirePOWER モジュール がクラウドに接続し、更新が使用可能な場合はその URL フィルタリング データを更新します。

時刻

[時刻(Time)] ページを使用して、現在の時刻と時刻源をASA FirePOWER モジュールに表示できます。

