ASA FirePOWER モジュール設定の構成

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

表 *1*: ローカル構成のオプション

オプション	説明
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。
[Cisco CSI][クラウドサービス（Cloud Services）]	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。

アプライアンス情報の表示と変更

ライセンス：任意

[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。情報には、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の情報が含まれます。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 *2 : Appliance Information*

フィールド	説明
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ます。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。
Product Model	アプライアンスのモデル名。
Serial Number	アプライアンスのシャーシのシリアル番号。
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。
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。
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 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 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。
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。
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方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Local] > [Configuration] の順に選択します。

[Information] ページが表示されます。

ステップ 2 アプライアンス名を変更するには、[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。

ステップ 3 変更を保存するには、[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。

URL フィルタリングとマルウェア検出のクラウドコミュニケーションのオプション

ライセンス：URL Filtering または Malware

ASA FirePOWER モジュールは、さまざまな種類の情報を取得するためにシスコの Collective Security Intelligence クラウドにアクセスします。

- 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、Cisco Cloud 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 モジュールはよくアクセスされる多くの URL のカテゴリとレピュテーション データを取得し、未分類の URL を検索できます。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。URL カテゴリとレピュテーションに基づく URL のブロッキングを参照してください。

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

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。

Enable Automatic Updates

システムが定期的にクラウドに接続し、アプライアンスのローカルデータセット内の URL カテゴリとレピュテーションのデータに対する更新を取得できるようにしますクラウドでは通常、データが 1 日に 1 回更新されますが、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。その場合、アップデート自体の実行にも最大 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） Cisco 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ル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、システムによるクラウドへの定期的な接続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。

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 にカテゴリやレピュテーションを手動で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 Cisco Cloud 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。

キャッシュされた URL の期限切れ

この設定は、[不明 URL を Cisco CSI に問い合わせる（Query Cisco CSI for Unknown URL）][不明 URL を Cisco Cloud に問い合わせる（Query Cisco Cloud for Unknown URLs）] が有効になっている場合にのみ該当します。

古いデータと一致する URL のインスタンスを最小限に抑えるため、キャッシュ内の URL を期限切れに設定できます。脅威データの正確性と即時性を向上させるため、短い有効期限を選択します。

カテゴリおよびレピュテーション データのキャッシングにより、Web ブラウジングが高速化されます。デフォルトでは、最速のパフォーマンスを得るため、URL のキャッシュされたデータの有効期限はありません。

キャッシュされた URL は、指定された時間が経過した後、ネットワーク上のユーザが初めてアクセスした後に更新されます。最初のユーザに更新済みの結果は表示されませんが、この URL に次にアクセスしたユーザには更新済みの結果が表示されます。

Licensing

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を参照）。

ASA FirePOWER モジュールに URL Filtering ライセンスがない場合、クラウド接続オプションを設定することはできません。クラウドサービスのローカル設定ページには、ライセンスが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のに加えて、[Enable URL Filtering] と [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。

Internet Access

Cisco Cloud への接続にはポート 80/HTTP および 443/HTTPS が使用されます。

次の手順では、Cisco Cloud との通信を有効にする方法と、URL データのオンデマンド更新を実行する方法について説明します。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。

クラウド通信の有効化

クラウドとの通信を有効にする方法：

ステップ 1 アプライアンスが次のすべての URL で Cisco Cloud と通信できることを確認します。

https://regsvc.sco.cisco.com

https://est.sco.cisco.com

https://updates-talos.sco.cisco.com

http://updates.ironport.com

https://v3.sds.cisco.com

ステップ 2 [Configuration] > [ASA FirePOWER Configuration] > [Integration] > **[Cloud Services]** を選択します。

[Information] ページが表示されます。

ステップ 3 **[Cloud Services]** をクリックします。

[Cloud Services] 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。

ステップ 4 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。

[Enable Automatic Updates] または [Query Cloud for Unknown URLs] を有効にするには、あらかじめ [Enable URL Filtering] を有効にする必要があります。

ステップ 5 [**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、URL フィルタリングが最後に有効になってからの経過時間、または URL フィルタリングを初めて有効にしたかどうかに応じて、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。

次のタスク

- システムの URL データのオンデマンド更新を実行する方法：

1. [Configuration] > [ASA FirePOWER Configuration] > [Local] > [Configuration] の順に選択します。

   [Information] ページが表示されます。

2. [URL Filtering] をクリックします。

[URL Filtering] ページが表示されます。

3. [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、更新が利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。

システム情報

時刻（Time）

ASA FirePOWER モジュールの現在時刻と時刻源は、[Time] ページを使用して確認できます。