



セキュリティ、インターネットアクセス、および通信ポート

ASA FirePOWER モジュールを保護するには、保護された内部ネットワークにインストールする必要があります。ASA FirePOWER モジュールには、使用可能なサービスとポートのうち必要なものだけが設定されていますが、攻撃がファイアウォールの外からモジュールに到達できないことを確認する必要があります。

また、ASA FirePOWER モジュールの機能によってはインターネット接続が必要になります。デフォルトでは、ASA FirePOWER モジュールはインターネットに直接接続するように設定されます。また、システムでは、セキュアなアプライアンスアクセスのため、さらに特定のシステム機能が正しく動作するのに必要なローカルまたはインターネット上のリソースにそれらのシステムがアクセスできるようにするため、特定のポートをオープンしたままにする必要があります。

- [インターネットアクセス要件 \(1 ページ\)](#)
- [通信ポートの要件 \(2 ページ\)](#)

インターネットアクセス要件

デフォルトでは、ASA FirePOWER モジュールはポート 443/tcp (HTTPS) および 80/tcp (HTTP) でインターネットに直接接続するよう設定されます。これらのポートは、デフォルトで、ASA FirePOWER モジュール上でオープンになっています。[通信ポートの要件 \(2 ページ\)](#) を参照してください。

次の表に、ASA FirePOWER モジュールの特定の機能におけるインターネットアクセス要件を示します。

表 1: ASA FirePOWER モジュール機能のインターネットアクセス要件

機能	インターネットアクセスの用途
侵入ルール、VDB、および GeoDB の更新	侵入ルール、GeoDB、または VDB の更新をアプライアンスに直接ダウンロードするか、ダウンロードをスケジュールします。

機能	インターネット アクセスの用途
ネットワークベースのAMP	マルウェア クラウド検索を実行します。
Security Intelligence フィルタリング	インテリジェンス フィードを含む、外部ソースからのセキュリティインテリジェンスフィードデータをダウンロードします。
システム ソフトウェアの更新	システム更新をアプライアンスに直接ダウンロードするか、ダウンロードをスケジュールします。
URL フィルタリング	<p>クラウドベースの URL カテゴリおよびレピュテーションデータをアクセス制御用にダウンロードし、カテゴリライズされていない URL に対してルックアップを実行します。</p> <p>https://regsvc.sco.cisco.com</p> <p>https://est.sco.cisco.com</p> <p>https://updates-talos.sco.cisco.com</p> <p>http://updates.ironport.com</p> <p>IPv4 :</p> <ul style="list-style-type: none"> • 146.112.62.0/24 • 146.112.63.0/24 • 146.112.255.0/24 • 146.112.59.0/24 <p>IPv6</p> <ul style="list-style-type: none"> • 2a04:e4c7:ffff::/48 • 2a04: e4c7: fffe::/48
whois	外部ホストに whois 情報を要求する。

通信ポートの要件

オープン ポートでは、以下が可能です。

- アプライアンスのユーザ インターフェイスにアクセスする
- アプライアンスへのセキュアなリモート接続
- システムの特定の機能が正しく機能するために必要なローカルまたはインターネット上のリソースへのアクセス

一般に、機能関連のポートは、該当する機能を有効化または設定する時点まで、閉じたままになります。



注意 開いたポートを閉じると展開にどのような影響が及ぶか理解するまでは、開いたポートを閉じないでください。

たとえば、管理デバイス上のポート 25/tcp (SMTP) アウトバウンドを閉じた場合、個別の侵入イベントに関する電子メール通知をデバイスから送信できなくなります ([侵入ルールに関する外部アラートの設定](#)を参照)。

次の表は、ASA FirePOWER モジュールの機能を最大限に活用するために必要なオープンポートを示しています。

表 2: ASA FirePOWER モジュールの機能と運用のためのデフォルト通信ポート

ポート	説明	方向	開く目的
22/tcp	SSH/SSL	双方向	アプライアンスへのセキュアなリモート接続を許可します。
25/tcp	SMTP	発信	アプライアンスから電子メール通知とアラートを送信します。
53/tcp	DNS	発信	DNS を使用します。
67/udp 68/udp	DHCP	発信	DHCP を使用します。 (注) これらのポートはデフォルトで閉じられています。
		双方向	HTTP 経由でのカスタムおよびサードパーティのセキュリティインテリジェンス フィードの更新。 URL カテゴリおよびレピュテーションデータのダウンロード (ポート 443 も必要)。
161/udp	SNMP	双方向	SNMP ポーリング経由でアプライアンスの MIB にアクセスできるようにします。
162/udp	SNMP	発信	リモートトラップサーバに SNMP アラートを送信します。
389/tcp 636/tcp	LDAP	発信	外部認証用に LDAP サーバと通信します。
389/tcp 636/tcp	LDAP	発信	検出された LDAP ユーザのメタデータの取得。
443/tcp	HTTPS	着信	アプライアンスのユーザインターフェイスにアクセスする

ポート	説明	方向	開く目的
443/tcp	HTTPS クラウド通信	双方向	次のものを取得します。 <ul style="list-style-type: none"> ソフトウェア、侵入ルール、VDB、およびGeoDBの更新 URL カテゴリおよびレピュテーションデータ（さらにポート 80 も必要） インテリジェンス フィードおよび他のセキュアなセキュリティ インテリジェンス フィード ファイルに関してネットワーク トラフィックで検出されたマルウェアの性質
			デバイスのローカルユーザ インターフェイスを使用してソフトウェア更新をダウンロードします。
514/udp	syslog	発信	リモート syslog サーバにアラートを送信します。
8305/tcp	アプライアンス通信	双方向	展開におけるアプライアンス間で安全に通信します。 必須です。
8307/tcp	ホスト入力クライアント	双方向	ホスト入力クライアントと通信します。