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

以下のトピックでは、システム セキュリティ、インターネット アクセス、および通信ポートに関する情報を提供します。

セキュリティ要件

Firepower Management Center 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してください。Firepower Management Center は必要なサービスとポートだけを使用するよう設定されますが、ファイアウォール外部からの攻撃がそこまで（または管理対象デバイスまで）決して到達できないようにする必要があります。

Firepower Management Center とその管理対象デバイスが同じネットワーク上に存在する場合は、デバイス上の管理インターフェイスを、Firepower Management Center と同じ保護された内部ネットワークに接続できます。これにより、Firepower Management Center からデバイスを安全に制御することができます。また、他のネットワーク上のデバイスからのトラフィックを Firepower Management Center で管理および分離できるように、複数の管理インターフェイスを設定することもできます。

アプライアンスの展開方法とは無関係に、アプライアンス間通信は暗号化されます。それでも、分散型サービス拒否（DDoS）や中間者攻撃などの手段でアプライアンス間の通信が中断、ブロック、または改ざんされないよう何らかの対策を講じる必要があります。

インターネット アクセス要件

デフォルトでは、Firepower アプライアンスは、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、Firepower

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

システムのすべてのアプライアンスでデフォルトで開かれています。ほとんどの Firepower アプライアンスでは、プロキシ サーバの利用がサポートされている点に注意してください。

次の表に、Firepower 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*: インターネット アクセス要件

機能	[アプライアンス（Appliances）]	インターネット アクセスの用途
ネットワーク向け AMP	Management Center	マルウェア クラウド検索を実行します。
Cisco Advanced Malware Protection（Cisco AMP）統合	Management Center	エンドポイントベース（AMP for Endpoints）のマルウェア イベントを Cisco AMP クラウドから受信します。
動的分析：照会	Management Center	動的分析のために、送信済みファイルの脅威スコアを AMP Threat Grid クラウドに照会します。
動的分析：送信	あらゆるデバイス	動的分析用にファイルを AMP Threat Grid クラウドに送信します。
侵入ルール、VDB、および GeoDB の更新	Management Center	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。
ローカルマルウェア分析およびファイル事前分類の署名アップデート	Management Center	ローカルマルウェア分析および事前分類エンジンに署名アップデートをダウンロードします。
RSS フィード ダッシュボード ウィジェット	Management Center 7000 & 8000 シリーズ	シスコを含む外部ソースから RSS フィード データをダウンロードします。
セキュリティ インテリジェンス フィルタリング	Management Center	シスコが提供するインテリジェンス 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	すべて（NGIPSv を除く）	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	Management Center	URL カテゴリおよびレピュテーション データをアクセス コントロール用にダウンロードし、分類されていない URL に対してクエリを実行します。

機能	[アプライアンス（Appliances）]	インターネット アクセスの用途
whois	Management Center	外部ホストの whois 情報を要求します。

通信ポートの要件

FirePOWER アプライアンスは、（デフォルトでポート 8305/tcp を使用する）双方向 SSL 暗号化通信チャネルを使って通信します。このポートは、基本的なプラットフォーム内通信のためにオープンの状態で保持する必要があります。

他のオープン ポートの役割は次のとおりです。

- Web インターフェイス（Firepower Management Center および 7000 & 8000 シリーズ）へのアクセス。
- セキュア リモート接続。
- 特定の機能により必要となるローカルまたはインターネット リソースへのアクセス。

開いているポートを閉じると展開にどのような影響が生じるかを理解するまで、開いているポートを閉じないでください。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。

いくつかの通信ポートを変更することができます。

- システムと認証サーバ間の接続を設定するときに、LDAP および RADIUS 認証用のカスタム ポートを指定できます。
- 管理ポート（8305/tcp）を変更できます。ただし、シスコではデフォルト設定を維持することを**強く**推奨しています。管理ポートを変更する場合は、展開内のすべてのアプライアンスについて変更する必要があります。
- ポート 32137/tcp を使用して Cisco AMP クラウドと通信できます。ただし、シスコはデフォルトのポート 443 を使用することをお勧めします。

次の表は、Firepower機能を最大限に活用できるように、各アプライアンス タイプで必要なオープン ポートを示しています。

表 *2 : Firepower* システムの機能と運用のためのデフォルト通信ポート

[ポート（Port）]	説明	方向（Direction）	開いているアプライアンス	目的
22/tcp	SSH/SSL	双方向	任意（Any）	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。

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

[ポート（**Port**）]	説明	方向（**Direction**）	開いているアプライアンス	目的
25/tcp	SMTP	発信	任意（Any）	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	任意（Any）	DNS を使用します。
67/udp 68/udp	DHCP	発信	任意（Any）	DHCP を使用します。これらのポートはデフォルトで**閉じられている**ことに注意してください。
80/tcp	HTTP	発信	Management Center 7000 & 8000 シリーズ	RSS フィードダッシュボードウィジェットからリモート Web サーバに接続できるようにします。
		双方向	Management Center	HTTP 経由で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を更新します。 URL カテゴリおよびレピュテーションデータをダウンロードします（さらにポート 443 も必要）。
161/udp	SNMP	双方向	任意（Any）	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	任意（Any）	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	すべて（NGIPSv を除く）	外部認証用に LDAP サーバと通信します。
389/tcp 636/tcp	LDAP	発信	Management Center	検出された LDAP ユーザに関するメタデータを取得します。

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

[ポート（Port）]	説明	方向（Direction）	開いているアプライアンス	目的
443/tcp	HTTPS	着信	すべて（NGIPSv を除く）	アプライアンスの Web インターフェイスにアクセスします。
443/tcp	HTTPS AMQP AMP クラウド、AMP Threat Grid クラウド、および脅威インテリジェンスの通信設定	双方向	Management Center	次のものを取得します。 • 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 • エンドポイントベース（AMP for Endpoints）のマルウェア イベント • 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 • 送信されたファイルに関する動的分析情報
		双方向	Management Center、7000 & 8000 シリーズ	デバイスのローカル Web 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。

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

[ポート（Port）]	説明	方向（Direction）	開いているアプライアンス	目的
		双方向	すべての管理対象デバイス	動的分析のためにファイルを送信します。
514/udp	syslog	発信	任意（Any）	リモート syslog サーバにアラートを送信します。
623/udp	SOL/LOM	双方向	7000 & 8000 シリーズ	Serial Over LAN（SOL）接続を使用して Lights-Out Management を実行できるようにします。
1500/tcp 2000/tcp	データベース アクセス	着信	Management Center	サードパーティ クライアントによるデータベースへの読み取り専用アクセスを可能にします。
1812/udp 1813/udp	RADIUS	双方向	すべて（NGIPSv を除く）	外部認証とアカウンティングのために RADIUS サーバと通信します。
3306/tcp	ユーザ エージェント	着信	Management Center	ユーザエージェントと通信します。
6514/tcp	syslog への監査ログのストリーミング	発信	Management Center、従来のデバイス	リモート syslog サーバに監査ログ レコードを送信します。
8302/tcp	eStreamer	双方向	Management Center 、 7000 & 8000 シリーズ	eStreamer クライアントと通信します。
8305/tcp	アプライアンス通信	双方向	任意（Any）	展開におけるアプライアンス間で安全に通信します。**必須作業です。**
8307/tcp	ホスト入力クライアント	双方向	Management Center	ホスト入力クライアントと通信します。

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

[ポート（Port）]	説明	方向（Direction）	開いているアプライアンス	目的
32137/tcp	AMP クラウドおよび脅威インテリジェンスの通信設定	双方向	Management Center	アップグレード対象の Management Center と Cisco AMP クラウドの通信を可能にします。

関連トピック

LDAP 認証サーバの特定

RADIUS 接続の設定

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