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、インターネット アクセス、および通信ポートについて

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システム アプライアンス間の通信が中断、ブロック、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。

また、Firepowerシステムの機能によってはインターネット接続が必要となることにも注意してください。デフォルトでは、システム アプライアンスがインターネットに直接接続するように設定されます。加えて、システムで特定のポートを開いたままにしておく必要があります。その目的

は基本的なアプライアンス間通信、セキュアなアプライアンス アクセス、および特定のシステム機能を正しく動作させるために必要なローカル/インターネット リソースへのアクセスを可能にすることです。

インターネット アクセス要件

デフォルトでは、システム 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。ほとんどのシステム 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。プロキシ サーバはwhoisアクセスに使用できない点にも注意が必要です。

Firepowerシステム機能のインターネット アクセス要件

次の表に、Firepowerシステム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*：*Firepower* システム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	アプライアンス
AMP for Firepower	マルウェア クラウド検索を実行します。	Management Center
Cisco Advanced Malware Protection（Cisco AMP）統合	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。	Management Center
動的分析：照会	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。	Management Center
動的分析：送信	動的分析用にファイルを AMP Threat Grid クラウドに送信します。	あらゆるデバイス
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。	Management Center
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	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。	Management Center

機能	インターネット アクセスの用途	アプライアンス
RSS フィード ダッシュボード ウィジェット	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。	Management Center 7000 & 8000 シリーズ
セキュリティ インテリジェンス フィルタリング	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。	Management Center
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。	すべて（NGIPSv を除く）
URL フィルタリング	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。	Management Center
whois	外部ホストの whois 情報を要求します。	Management Center

通信ポートの要件

Firepower Management Center およびその管理対象デバイスは、（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。基本的なプラットフォーム間通信用にこのポートを開いたままにする**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 インターフェイスへのアクセス
- デバイスまたは Firepower Management Center へのセキュアなリモート接続
- 特定のシステム機能を正しく動作させるために必要なローカル/インターネット リソースへのアクセスを可能にする

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。たとえば、Firepower Management Centerをユーザ エージェントに接続するまでは、エージェント通信ポート（3306/tcp）は閉じたままになります。別の例として、LOM を有効にするまでは、7000 および 8000 シリーズ デバイス上のポート 623/udp が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、管理対象デバイスでポート 25/tcp（SMTP）アウトバウンドを閉じると、このデバイスが個々の侵入イベントに関する電子メール通知を送信できなくなります。別の例として、ポート 443/tcp（HTTPS）を閉じることにより物理管理対象デバイスの Web インターフェイスへのアクセスを無効にできますが、それと同時に、動的分析のためにデバイスから疑わしいマルウェア ファイルを AMP Threat Grid クラウドに送信できなくなります。

次のように、システムのいくつかの通信ポートを変更できることに注意してください。

- 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、相互に通信する必要がある展開内のすべての Firepower Management Center およびその管理対象デバイスの管理ポートを変更する必要があります。
- ポート 32137/tcp を使用して、アップグレード対象の Management Center とシスコ AMP クラウドの通信を可能にすることができます。ただし、シスコではバージョン 5.3 以降の新規インストールのデフォルトであるポート 443 に切り替えることを推奨しています。

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

次の表は、Firepower システムの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。
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。

[ポート（Port）]	説明	方向（Direction）	開いているアプライアンス	目的
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。
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

[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	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。
		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。
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。
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。