# 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それをインストールしてください。FMC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。

FMC 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、FMC 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、FMC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 FMC 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に関係なく、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接続するように設定されています。アプライアンスがインターネットに直接アクセスしないようにするには、プロキシ サーバを設定できます。

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

ほとんどの場合、インターネットにアクセスするのは Firepower Management Center です。ただし、管理対象デバイスがインターネットにアクセスする場合もあります。たとえば、マルウェア保護設定で動的分析を使用する場合、管理対象デバイスはファイルを直接 Cisco Threat Grid クラウドに送信します。または、外部 NTPサーバにデバイスを同期することができます。

さらに、Web 分析トラッキングを無効にした場合を除き、ブラウザは Google Web 分析サーバに連絡し、個人を特定可能でない使用状況データを Cisco に送信することができます。

**ヒント** ネットワーク向け AMP またはエンドポイント向け AMP を使用中の場合、ロケーションによって FMC がアクセスする AMP クラウド リソースが決定されます。「AMP の適切な操作のために必要なサーバ アドレス」トラブルシューティング テクニカルノートには、Firepower アプライアンスだけでなく、コネクタやプライベート クラウド アプライアンスなどの Cisco AMP コンポーネントでも必要なインターネット リソース（静的 IP アドレスを含む）を一覧表示します。

高可用性ペアの FMC の両方にインターネット アクセスがある必要があります。機能に応じて、両方のピアがインターネットにアクセスすることも、アクティブ ピアのみがインターネットにアクセスすることもあります。

**表 *1 : Firepower* のインターネット アクセス要件**

| 機能 | 理由（Reason） | FMCハイ アベイラビリティ | リソース |
|---|---|---|---|
| ネットワーク向け AMP | マルウェア クラウド ルックアップ。 | 両方のピアが検索を実行します。 | この表の上に記載の重要なヒントを参照してください。<br>cloud-sa.amp.cisco.com<br>cloud-sa.eu.amp.cisco.com<br>cloud-sa.apjc.amp.cisco.com<br>cloud-sa-589592150.us-east-1.elb.amazonaws.com |
| | ファイル事前分類とローカルのマルウェア分析のシグニチャ更新をダウンロードします。 | アクティブ ピアでダウンロードが実行され、スタンバイへ同期します。 | updates.vrt.sourcefire.com<br>amp.updates.vrt.sourcefire.com |
| | 動的分析（管理対象デバイス）のファイルを送信します。<br>動的分析結果のクエリ（FMC）。 | 両方のピアが動的分析レポートのクエリを実行します。 | fmc.api.threatgrid.com<br>fmc.api.threatgrid.eu |

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

| 機能 | 理由（Reason） | FMCハイ アベイラビリティ | リソース |
|---|---|---|---|
| AMP for Endpoint の統合 | エンドポイント向け AMP によって検出されたマルウェア イベントを AMP クラウドから受信します。<br>Firepower システムによって検出されたマルウェア イベントを AMP for Endpoints で表示します。<br>AMP クラウドからの性質をオーバーライドするには、AMP for Endpoints で作成された一元的なファイル ブラックリストおよびホワイトリストを使用します。 | 両方のピアがイベントを受信します。<br>両方のピア（設定が同期されていない）でクラウド接続を設定する必要もあります。 | https://www.cisco.com/c/en/us/support/docs/security/sourcefire-amp-appliances/118121-technote-sourcefire-00.html#anc5 の Firepower に関する情報を参照してください。<br>この表の上に記載の重要なヒントも参照してください。 |
| セキュリティ インテリジェンス | セキュリティ インテリジェンス フィードをダウンロードします。 | アクティブ ピアでダウンロードが実行され、スタンバイへ同期します。 | intelligence.sourcefire.com |
| URL フィルタリング | URL カテゴリおよびレピュテーション データをダウンロードします。<br>URL カテゴリおよびレピュテーション データを手動でクエリ（ルックアップ）します。<br>未分類 URL のクエリ。 | アクティブ ピアでダウンロードが実行され、スタンバイへ同期します。 | database.brightcloud.com<br>service.brightcloud.com |
| Cisco Smart Licensing | Cisco Smart Software Manager と通信します。 | アクティブなピアが通信します。 | tools.cisco.com<br>www.cisco.com |
| Cisco Success Network | 使用状況情報および統計情報を送信します。 | アクティブなピアが通信します。 | api-sse.cisco.com:8989 |
| システムの更新プログラム | 更新プログラムを Cisco から直接 FMC にダウンロードします。<br>• システム ソフトウェア<br>• 侵入ルール<br>• 脆弱性データベース（VDB）<br>• 位置情報データベース（GeoDB） | 侵入ルール、VDB、および GeoDB をアクティブなピアで更新し、アクティブなピアはその後スタンバイへ同期します。<br>各ピアで個別にシステム ソフトウェアをアップグレードします。Cisco Firepower Management Center Upgrade Guide を参照してください。 | cisco.com<br>sourcefire.com |

| 機能 | 理由（Reason） | FMCハイ アベイラビリティ | リソース |
|---|---|---|---|
| 時刻の同期 | 展開内で時間を同期します。<br>プロキシサーバではサポートされません。 | 外部 NTP サーバを使用するアプライアンスはインターネットにアクセスできる必要があります。 | 0.sourcefire.pool.ntp.org<br>1.sourcefire.pool.ntp.org<br>2.sourcefire.pool.ntp.org<br>3.sourcefire.pool.ntp.org |
| RSS フィード | ダッシュ ボードで Cisco 脅威調査ブログを表示します。 | RSS フィードを表示するアプライアンスはインターネットにアクセスできる必要があります。 | blogs.cisco.com/talos<br>cloud.google.com |
| [Whois] | 外部ホストの whois 情報を要求します。<br>プロキシサーバではサポートされません。 | whois 情報を要求するすべてのアプライアンスがインターネットにアクセスできる必要があります。 | whois クライアントは、クエリ対象の適切なサーバの推測を試みます。推測できない場合、次を使用します。<br>• NIC ハンドル：whois.networksolutions.com<br>• IPv4 アドレスとネットワーク名：whois.arin.net |

# 通信ポートの要件

Firepower アプライアンスはポート 8305/tcp 上の双方向 SSL 暗号化通信チャネルを使用して通信します。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。

他のポートでは、特定の機能に必要な外部リソースへのアクセスとともにセキュアな管理をすることができます。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。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、開いたポートを変更したり閉じたりしないでください。

**表 *2 : Firepower* 通信ポートの要件**

| ポート | プロトコル/機能 | プラットフォーム | [方向（Direction）] | 詳細（Details） |
|---|---|---|---|---|
| 7/UDP | UDP/監査ロギング | FMC、クラシック | 発信 | 監査ロギングの設定時の syslog サーバとの接続を確認します。 |
| 22/tcp | SSH | FMC<br>あらゆるデバイス | 着信 | アプライアンスへのリモート接続を保護します。 |
| 25/tcp | SMTP | FMC | 発信 | 電子メール通知とアラートを送信。 |

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 | プロトコル/機能 | プラットフォーム | [方向（**Direction**）] | 詳細（**Details**） |
|---|---|---|---|---|
| 53/tcp<br>53/udp | DNS | FMC<br>あらゆるデバイス | 発信 | DNS 用です。 |
| 67/udp<br>68/udp | DHCP | FMC<br>あらゆるデバイス | 発信 | DHCP 用です。 |
| 80/tcp | HTTP | FMC<br>7000 & 8000 シリーズ | 発信 | RSS フィードをダッシュ ボードに表示します。 |
| 80/tcp | HTTP | FMC | 発信 | 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またはクエリします（さらにポート 443 も必要）。 |
| 80/tcp | HTTP | FMC | 発信 | HTTP 経由でカスタム セキュリティ インテリジェンス フィードをダウンロードします。 |
| 123/udp | NTP | FMC<br>あらゆるデバイス | 発信 | 時刻を同期します。 |
| 161/udp | SNMP | FMC<br>あらゆるデバイス | 着信 | SNMP ポーリング経由で MIB にアクセスできるようにします。 |
| 162/udp | SNMP | FMC<br>あらゆるデバイス | 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<br>636/tcp | LDAP | FMC<br>FTD<br>7000 & 8000 シリーズ | 発信 | 外部認証用に LDAP サーバと通信します。<br>検出された LDAP ユーザに関するメタデータを取得します（FMC のみ）。<br>設定可能。 |
| 443/tcp | HTTPS | FMC<br>7000 & 8000 シリーズ | 着信 | Web インターフェイスにアクセスします。 |
| 443/tcp | リモート アクセス VPN（SSL/IPSec） | FTD | 着信 | リモート ユーザからネットワークへのセキュアな VPN 接続を許可します。 |
| 500/udp<br>4500/udp | リモート アクセス VPN（IKEv2） | FTD | 着信 | リモート ユーザからネットワークへのセキュアな VPN 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 | プロトコル/機能 | プラットフォーム | [方向（Direction）] | 詳細（Details） |
|---|---|---|---|---|
| 443/tcp | HTTPS | FMC<br>FTD | 着信 | Cisco Terminal Services（TS）エージェントを含め、Firepower REST API を使用して、統合製品やサードパーティ製品と通信します。 |
| 443/tcp | HTTPS | FMC | 発信 | クエリを Cisco Security Packet Analyzer に送信します。 |
| 443/tcp | HTTPS | FMC<br>あらゆるデバイス | 発信 | インターネットからデータを送受信します。詳細は、インターネット アクセス要件 （1 ページ）を参照してください。 |
| 443 | HTTPS | FMC | 発信 | AMP クラウドとの通信（パブリックまたはプライベート）<br>ポート 32137 の情報も参照してください。 |
| 443 | HTTPS | FMC | 着信および発信（Inbound and Outbound） | AMP for Endpoints との統合 |
| 514/udp | Syslog（アラート） | FMC<br>あらゆるデバイス | 発信 | リモート syslog サーバにアラートを送信します。 |
| 623/udp | SOL/LOM | FMC<br>7000 & 8000 シリーズ | 着信 | Serial Over LAN（SOL）接続を使用した Lights-Out Management（LOM）。 |
| 885/tcp | キャプティブ ポータル | あらゆるデバイス | 着信 | キャプティブ ポータルのアイデンティティ ソースと通信します。 |
| 1500/tcp<br>2000/tcp | データベース アクセス | FMC | 着信 | サードパーティ クライアントによるイベント 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<br>1813/udp | RADIUS | FMC<br>FTD<br>7000 & 8000 シリーズ | 発信 | 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。<br>設定可能。 |
| 3306/tcp | ユーザ エージェント | FMC | 着信 | ユーザ エージェントと通信します。 |
| 5222/tcp | ISE | FMC | 発信 | ISE アイデンティティ ソースと通信します。 |

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 | プロトコル/機能 | プラットフォーム | [方向（Direction）] | 詳細（Details） |
|---|---|---|---|---|
| 6514/tcp | Syslog（監査イベント） | FMC<br>7000 & 8000 シリーズ<br>NGIPSv<br>ASA FirePOWER | 発信 | TLS の設定時にリモート syslog サーバに監査ログを送信します。 |
| 8302/tcp | eStreamer | FMC<br>7000 & 8000 シリーズ | 着信 | eStreamer クライアントと通信します。 |
| 8305/tcp | アプライアンス通信 | FMC<br>あらゆるデバイス | 両方 | 展開におけるアプライアンス間で安全に通信します。<br>設定可能。この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。デフォルトを維持することをお勧めします。 |
| 8307/tcp | ホスト入力クライアント | FMC | 着信 | ホスト入力クライアントと通信します。 |
| 8989/tcp | Cisco Success Network | FMC | 発信 | 使用状況情報および統計情報を送信します。 |
| 32137/tcp | ネットワーク向け AMP | FMC | 発信 | Cisco AMP クラウドと通信します。<br>これはレガシー設定です。デフォルト（443）を使用することをお勧めします。 |

**関連トピック**

LDAP 外部認証オブジェクトの追加

RADIUS 外部認証オブジェクトの追加

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