



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](#) (1 ページ)
- [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](#) (4 ページ)

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に設定されますが、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、FMCと同じ保護された内部ネットワークにデバイス上の管理インターフェイスを接続できます。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。

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があります。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。 cloud-sa.amp.cisco.com cloud-sa.eu.amp.cisco.com cloud-sa.apjc.amp.cisco.com 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 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。 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 fmc.api.threatgrid.eu

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	<p>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。</p> <p>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。</p> <p>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。</p>	<p>両方のピアがイベントを受信します。</p> <p>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。</p>	<p>https://www.cisco.com/c/en/us/support/docs/security/sourcefire-amp-appliances/118121-technote-sourcefire-00.html#anc5</p> <p>で、Firepowerに関する情報を参照してください。</p> <p>この表の上に記載の重要なヒントも参照してください。</p>
セキュリティインテリジェンス	<p>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。</p>	<p>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。</p>	<p>intelligence.sourcefire.com</p>
URL フィルタリング	<p>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。</p> <p>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。</p> <p>未分類 URL のクエリ。</p>	<p>アクティブ FMC でダウンロードが実行され、スタンバイへ同期します。</p>	<p>database.brightcloud.com</p> <p>service.brightcloud.com</p>
Cisco Smart Licensing	<p>Cisco Smart Software Manager と通信します。</p>	<p>アクティブなピアが通信します。</p>	<p>tools.cisco.com</p> <p>www.cisco.com</p>
Cisco Success Network	<p>使用状況情報および統計情報を送信します。</p>	<p>アクティブなピアが通信します。</p>	<p>api-sse.cisco.com:8989</p>
システムの更新プログラム	<p>更新プログラムを Cisco から直接 FMC にダウンロードします。</p> <ul style="list-style-type: none"> • システム ソフトウェア • 侵入ルール • 脆弱性データベース (VDB) • 位置情報データベース (GeoDB) 	<p>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。</p> <p>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。</p>	<p>cisco.com</p> <p>sourcefire.com</p>

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。 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 1.sourcefire.pool.ntp.org 2.sourcefire.pool.ntp.org 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 cloud.google.com
[Whois]	外部ホストの whois 情報を要求します。 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。 <ul style="list-style-type: none"> • NIC ハンドル : whois.networksolutions.com • 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	詳細
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 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。

ポート	プロトコル/機能	プラットフォーム	方向	詳細
53/tcp 53/udp	DNS	FMC あらゆるデバイス	発信	DNS 用です。
67/udp 68/udp	DHCP	FMC あらゆるデバイス	発信	DHCP 用です。
80/tcp	HTTP	FMC 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 あらゆるデバイス	発信	時刻を同期します。
161/udp	SNMP	FMC 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 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 636/tcp	LDAP	FMC FTD 7000 & 8000 シリーズ	発信	外部認証用に LDAP サーバと通信します。 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）。 設定可能。
443/tcp	HTTPS	FMC 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 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。

ポート	プロトコル/機能	プラットフォーム	方向	詳細
443/tcp	HTTPS	FMC 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 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) 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 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 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 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 1813/udp	RADIUS	FMC FTD 7000 & 8000 シリーズ	発信	外部認証とアカウントिंगのために RADIUS サーバと通信します。 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。

ポート	プロトコル/機能	プラットフォーム	方向	詳細
6514/tcp	Syslog (監査イベント)	FMC 7000 & 8000 シリーズ NGIPSv 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 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 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。 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。 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](#)

