FAQ

Cisco FirePOWER Threat Defense for ISR

Q. Cisco FirePOWER™ Threat Defense for ISR とは何ですか。

A. Cisco FirePOWER Threat Defense for ISR は、業界をリードするシスコの脅威防御機能を、ネットワーク エッジやデータセンターから、ブランチ オフィスで使用されるプラットフォームである Cisco Integrated Services Router（ISR）にまで拡張するものです。

Q. この製品が必要な理由を教えてください。

A. ブランチ サイトからインターネットに直接アクセス（DIA）することで、コスト削減やユーザ エクスペリエンスの向上というメリットを享受しながら、デバイスやホストの配置場所を問わずに、これらの機器を高度な脅威から保護することができるようになります。

Q. Cisco FirePOWER Threat Defense for ISR には何が含まれていますか。

A. この製品には、以下の 5 つのコンポーネントが含まれています。

- **FirePOWER 次世代侵入防御システム（NGIPS）**：リアルタイムのコンテキスト認識、インテリジェントなセキュリティ自動化、および業界トップクラスの有効性を示す脅威防御機能が統合されており、高度な脅威防御における標準となる製品です。
- **Application Visibility and Control（AVC）**：数千ものアプリケーションをきめ細かく制御し、モバイル アプリケーション ポリシー、ソーシャル メディア アプリケーション ポリシー、およびアクセプタブル ユース ポリシーを適用することによって、攻撃対象となる可能性のある領域を縮小します。
- **Advanced Malware Protection（AMP）**：非常に巧妙な攻撃、標的型攻撃、ゼロデイ攻撃、連続的で高度なマルウェアといった脅威からネットワークを保護します。AMP は、ファイルやネットワーク トラフィックを継続的に分析して防御の最前線を突破する脅威を把握し、脅威のアクティビティと動作を詳細に可視化します。さらに、わずか数回のクリックで、アクティブな攻撃の影響範囲を特定し封じ込めます。
- **レピュテーションベースの URL フィルタリング**：80 を超えるカテゴリに含まれる 2 億 8,000 万超の URL へのアクセスを制御し、疑わしいドメインや許容されないドメインに関連するリスクを削減することにより、クライアント側での巧妙な攻撃を最小化し、従業員の生産性を向上させます。
- **Cisco FireSIGHT® Management Center**：FirePOWER Threat Defense for ISR の全コンポーネントのイベントおよびポリシーを一元的に管理します。お客様のネットワークに関するあらゆる情報（物理ホストと仮想ホスト、オペレーティング システム、アプリケーション、サービス、プロトコル、ユーザ、位置情報、コンテンツ、ネットワークの動作、ネットワークへの攻撃、およびマルウェアなど）を可視化します。また、繰り返し実行するセキュリティ分析や管理タスクが自動化され、運用が合理化されるため、お客様のコスト削減にもつながります。

Q. FirePOWER Threat Defense を実行できる ISR モデルはどれですか。

A. FirePOWER Threat Defense は、ISR G2 および ISR 4000 シリーズ プラットフォームの両方で利用できます。具体的には次のとおりです。

- Cisco ISR G2 シリーズ
  - 2911 ISR
  - 2921 ISR
  - 2951 ISR

    - 3925 ISR
    - 3945 ISR
    - 3925E ISR
    - 3945E ISR
  - Cisco ISR 4000 シリーズ
    - 4331 ISR
    - 4351 ISR
    - 4451 ISR
    - 4321 および 4431 ISR（2015 年にリリース予定）

Q. Cisco FirePOWER Threat Defense for ISR の管理方法を教えてください。

A. FireSIGHT Management Center で一元的に管理できます。この管理センターは、アプライアンスと仮想フォーム ファクタの両方で利用できます。

Q. 管理センターでは、FirePOWER NGIPS アプライアンス、Cisco ASA with FirePOWER Services（シスコの次世代ファイアウォール）の脅威防御機能、および Cisco FirePOWER Threat Defense for ISR を同時に管理することはできますか。

A. はい。最大 300 の FirePOWER センサー（仮想および物理センサーの両方）を、1 つの管理センター インスタンスで管理できます。

Q. FireSIGHT Management Center にはインターネットへのアクセス機能がありませんが、シグネチャの更新は、フラッシュ ドライブや CD ROM などのリムーバブル メディアを使用してオフラインでアップロードできるのですか。

A. はい。製品の更新は、当社のソフトウェア ダウンロード [英語] ページで入手できます。

Q. Cisco FirePOWER Threat Defense for ISR はどのような状況に最適ですか。

A. この製品は、分散したブランチ オフィスや小売店のある企業に特に適しています。そのような企業では、クラウド アプリケーション、ビデオ、個人所有デバイスの持ち込み（BYOD）ポリシーにより、帯域幅の需要が大幅に増大して、コストが増加しているため最適です。帯域幅への需要やコストの増加が原因で、分散型の企業のブランチ オフィスでは、データセンター経由のバックホール トラフィックではなく、インターネットへの直接アクセス（DIA）を要望する声が高まっています。DIA によりコストを削減することはできますが、データセンターのエンタープライズレベルの脅威防御機能を使用できなくなります。この問題を解決するのが、Cisco FirePOWER Threat Defense for ISR です。

Q. 統合された脅威防御機能を、ファイアウォールではなくルータに導入するのはどのような場合ですか。また、両方に導入する必要があるのはどのような場合ですか。

A. セキュア トンネルを使用して、ブランチからの全トラフィックが検査のためにデータセンターにバックホールされる場合、セキュリティ要件に適しているのはステートフル ファイアウォールです。ブランチのトラフィックがインターネットに直接送信される場合は、ステートフル ファイアウォールと FirePOWER Threat Defense for ISR の両方の機能が必要です。

Q. ワイヤレス デバイスからのトラフィックを検査する場合に FirePOWER Threat Defense for ISR を導入する方法をおしえてください。

A. FirePOWER Threat Defense for ISR は、ワイヤレス ネットワークのターミネーション ポイントの直後に導入する必要があります。脅威防御機能を強化する場合は、モバイル デバイス用のバージョンである Cisco AMP for Endpoint をご利用ください。AMP for Endpoint からのアラートは、FireSIGHT Management Center にも送信されます。

Q. Cisco FirePOWER Threat Defense for ISR に関する技術的な設定情報はどこで入手できますか。

A. 詳細な技術情報については、こちら [英語] を参照してください。ただし、このリンクには、「Cisco FirePOWER Threat Defense for ISR」ブランドの情報はまだ含まれていません。

Q. Cisco FirePOWER Threat Defense for ISR の発注方法を教えてください。

A. シスコのアカウント担当者またはシスコ パートナーの担当者が支援しますので、これらの担当者にご連絡ください。

Q. FirePOWER Threat Defense for ISR の詳細情報はどこで入手できますか。

A. 特定の製品に関する詳細情報はこちらで入手できます。また、FirePOWER Threat Defense ソリューションに関する詳細情報はこちら [英語] から入手できます。

お問い合せ先

シスコシステムズ合同会社

〒107 - 6227 東京区都港赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

C67-734837-00JA 16.04