



Cisco Firepower REST API

サードパーティ プラットフォームからの Cisco Firepower ポリシーの管理

企業では、一般的に多数のセキュリティ テクノロジーを同時に使用します。その中には、ポリシーやセキュリティ ポスチャに関する情報を各種ソースから収集するツールが含まれています。Cisco Firepower™ REST API を利用すれば、さまざまなアプリケーションで、ポリシー、重要なポリシー要素、オブジェクトに Cisco Firepower Management Center プラットフォームおよび接続された Cisco Firepower デバイスからアクセスして解析することができます。

REST API は、独自の管理プラットフォームを使用するお客様にとっても、AlgoSec、FireMon、Skybox、Tufin などのベンダーによるファイアウォールポリシー管理 (FPM) ソリューションやネットワーク セキュリティ ポリシー管理 (NSPM) ソリューションを使用するお客様にとっても強力なツールです。FPM、NSPM、および類似するテクノロジーで、API の読み書き機能を使用して幅広い管理機能を実行できます。これには、完全なポリシー移行や、特定の Cisco Firepower 要素 (監査レコード、デバイスおよびグループの情報、物理インターフェイス、仮想スイッチなど) の操作などが含まれます。

Cisco Firepower テクノロジーには拡張性があり、外部の管理アプリケーションとの連動が可能であるため、複数のファイアウォールを同時に実行しているお客様には実用的です。また、以前のテクノロジーから Cisco Firepower への移行も容易になります。

効率とセキュリティ双方の向上

次世代のファイアウォール ポリシーは、単一の REST API により外部管理やリスク モデリングに使用できます。Cisco Firepower ユーザにサービスを提供するマネージド セキュリティ サービス プロバイダー (MSSP) は、API を使用することで、大規模なマルチテナント インフラストラクチャでの効率の向上を実現できます。MSSP は、お客様全員を対象とするポリシー更新を容易に実行できます。

エンド カスタマーの場合、このような効率性の高さにより、セキュリティの大幅な向上が可能になります。Cisco Firepower の次世代ファイアウォールで運用可能になった最新のポリシーをさらに迅速に入手して、攻撃者に隙を与えないようにすることができます。

次のステップ

Cisco Firepower の REST API の詳細については、<https://developer.cisco.com/site/firepower/> [英語] を参照してください。

Cisco Firepower API に関して連携している戦略的パートナーおよびその他の Cisco Security Technical Alliance (CSTA) パートナーの統合と利点については、<http://www.cisco.com/c/en/us/products/security/partner-ecosystem.html> [英語] を参照してください。

利点

- Cisco Firepower の完全なファイアウォール ポリシーとポリシー コンポーネントにアクセスして管理
- Cisco Firepower ポリシーを容易にエクスポート
- Cisco Firepower Management Center の重要なポリシーおよび管理コンポーネントへの読み書きアクセス権限を取得
- セキュリティ管理およびリスクモデリング アプリケーションに API の軽量で柔軟な操作を使用
- 複数のファイアウォール テクノロジーが使用されている Cisco Firepower の導入環境を管理
- 外部アプリケーションによるきめ細かいポリシー管理を許可