



Cisco Firepower Next-Generation Firewall

業界初のフル統合型、脅威重視型次世代ファイアウォール

次世代ファイアウォール (NGFW) の多くでは、アプリケーション制御を重視するあまり、脅威防御機能がおろそかになっていました。この問題に対応するため、一連の非連携型アドオン製品で第 1 世代の侵入防御機能を補完しようとする NGFW もあります。しかし、このようなアプローチでは、巧妙な攻撃者や高度なマルウェアが及ぼすリスクに対して、ビジネスを十分に保護できません。その上、感染してしまった後では、感染内容を把握して封じ込めたり、迅速に修復したりすることもできません。

メリット

- より多くの脅威に対応: 既知および未知の脅威に対する業界最高レベルの保護効果
- より多くの情報の把握: ユーザ、アプリケーション、デバイス、脅威、およびネットワークの脆弱性に対する分析と制御
- より早い検出とより速い対処: マルウェアの検出時間を数カ月から数時間まで短縮し、迅速な修復が可能
- 複雑さの緩和: すべてのセキュリティ機能を単一の管理インターフェイスに統合し、業務をシンプル化
- 既存ネットワークの有効活用: シスコの他のセキュリティソリューションやネットワークソリューションとの連携



必要なのは、脅威にフォーカスした統合型の次世代ファイアウォールです。きめ細かなアプリケーション制御に加え、巧妙で検出が困難なマルウェア攻撃による脅威に対して効果的なセキュリティ機能を提供できるものが求められます。

Cisco Firepower™ Next-Generation Firewall (NGFW) は、業界初のフル統合型、脅威重視型の NGFW です。ネットワークからエンドポイントまで、ファイアウォール機能、アプリケーション制御、脅威防御、高度なマルウェア防御における包括的で統合されたポリシー管理を実現します。

Cisco Firepower 4100 および 9300 アプライアンスに導入することで、パフォーマンスと密度が最適化された、インターネット エッジなどの高パフォーマンス環境向けの NGFW セキュリティプラットフォームを提供します。

攻撃前、攻撃中、そして攻撃後も組織を保護

Cisco Firepower NGFW は業界で最も広く導入されているステートフルファイアウォールを搭載し、4,000 を超える商用アプリケーションをきめ細かく制御できます。単一の管理インターフェイスで、ネットワークからエンドポイントまで統合的な可視性を提供します。Firepower NGFW は、アクセスを制御して攻撃を阻止し、マルウェアに対して防御する包括的なポリシー管理を実現します。攻撃側が侵入に成功してしまった場合も、攻撃を追跡して封じ込め、さらに攻撃から回復するためのツールを提供します。

Cisco Firepower NGFW は、以下の特長を備えた唯一の、業界に類のない次世代ファイアウォールです。

- 業界トップクラスの脅威保護を実現できる次世代侵入防御システム (NGIPS) を提供します。
- 既知および未知の脅威に対処できるフル統合型の高度なマルウェア防御 (AMP) を提供し、サンドボックスが統合されています。
- マルウェア感染を追跡して封じ込めます。
- 脅威イベントとネットワークの脆弱性を自動的に関連付けて、優先的に解決すべき脅威を提示します。
- ネットワークの弱点を分析して、導入すべき最適なセキュリティ ポリシーを推奨します。
- シスコの複数のネットワーク セキュリティ製品と連携させて、過去の投資を活用しながらセキュリティを強化できます。

次のステップ

詳細については、シスコの Web サイト www.cisco.com/go/ngfw を参照してください。