次世代ファイアウォールを選択する際の 5 つのヒント

以下を実現できる新しい次世代ファイアウォール（NGFW）に投資しましょう。

1 侵害の阻止と高度なセキュリティ

攻撃を阻止し、内部に侵入したマルウェアを迅速に検出

ファイアウォールの最も重要な役割は、侵害を阻止して組織を保護することにあります。ただし、予防策が 100% 効果的であることはないため、ファイアウォールにも高度な機能を組み込んで、最前線の防御ラインをすり抜けた高度なマルウェアを迅速に検出できるようにする必要があります。投資に値するのは、次のような機能を備えたファイアウォールです。

- 内部に侵入する前に攻撃を阻止する機能
- 気づかれることなく脅威を特定して迅速に阻止する、最高レベルの組み込み型次世代 IPS
- 数億の URL にポリシーを適用する URL フィルタリング
- 絶えずファイルの動作を分析し、迅速に脅威を検出して排除する、組み込み型のサンドボクシングと高度なマルウェア防御
- 新たな脅威を阻止するための最新のインテリジェンスをファイアウォールに提供する、世界屈指の脅威インテリジェンス組織

2 包括的なネットワークの可視性

より多くの脅威を阻止できるよう、より多くの脅威を検出

見えないものを防ぐことはできません。異常な動作を特定して迅速に阻止できるようにするには、ネットワークで起きていることを常に監視する必要があります。ファイアウォールは、アクティビティを包括的に可視化して次の状況を完全に認識できるものであるべきです。

- ユーザ、ホスト、ネットワーク、およびデバイス全体の脅威アクティビティ
- いつどこで脅威が発生したのか、広範なネットワークのどの部分に広がっているのか、今何が行われているのか
- アクティブなアプリケーションと Web サイト
- 仮想マシン間の通信やファイル転送など

その他のリソース

ファイアウォールにより多くの機能を求めているなら、Cisco Firepower NGFW をご覧ください。

Cisco NGFW の概要
Cisco NGFW のデモ
お客様の声 : Downer Group [英語]

cisco.com/jp/go/ngfw をご覧ください。

3 柔軟な管理および導入オプション

あらゆる組織の独自のニーズに対応するカスタマイズ

小規模企業、中規模企業、または大企業であるかどうかにかかわらず、ファイアウォールは独自の要件に対応するものであるべきです。

- すべての使用例の管理: オンボックス マネージャかすべてのアプライアンスをカバーする一元管理機能を選択できる。
- 仮想ファイアウォールを介してオンプレミスかクラウドに導入できる。
- ニーズに合った機能によるカスタマイズ: サブスクリプションを有効にするだけで高度な機能を利用できる。
- 幅広いスループット速度を選択できる。

4 最短時間での検出

マルウェアを迅速に検出してリスクを軽減

現在の業界標準の脅威検出時間は 100～200 日と、長くかかりすぎます。
次世代ファイアウォールには、次のような機能が求められます。

- 数秒で脅威を検出する。
- 数時間から数分以内に成功した侵害の有無を検出する。
- 迅速かつ正確なアクションで脅威を排除できるようアラートの優先順位付けを行う。
- 維持しやすい一貫したポリシーを導入し、組織のあらゆる部分に自動的に適用することで負荷を軽減する。

5 個別に動作するのではなく連携する機能

統合セキュリティ アーキテクチャが自動化を実現して複雑性を低減

次世代ファイアウォールは、サイロ化されたツールではなく、セキュリティ アーキテクチャの他の部分と通信し、それらと連携するものであるべきです。次のようなファイアウォールを選択する必要があります。

- 同じベンダーの他のツールとシームレスに統合される。
- 脅威情報、イベント データ、ポリシー、コンテキスト情報を、電子メール、Web、エンドポイント、およびネットワーク セキュリティ ツールで自動的に共有する。
- インパクト アセスメント、ポリシーの調整、ユーザの識別などのセキュリティ タスクを自動化する。