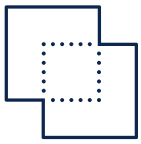
政府機関がファイアウォールを選択するための 5 つのヒント

ハイブリッドの分散環境という新しい環境のために、柔軟で信頼できるセキュリティの基礎としてファイアウォールを再考



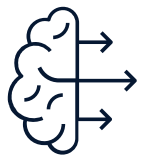
1 | 既成概念にとらわれずに考える

最新のファイアウォールとはどのようなものでしょうか。その特長は、ネットワーク インフラストラクチャと完全に統合していることです。しかし、おそらく最も重要なのは一括管理でどこにでもポリシーを適用できることです。次世代のファイアウォールは、プラットフォーム全体で統一されたポリシー、モバイルデバイスの情報、コンテキストと脅威インテリジェンス（脆弱なモバイルアプリやエンドポイントを介したネットワーク接続に対処するために必要な可視性）を提供します。

2 | 暗号化されたトラフィック内の情報を確認する

暗号化されたトラフィック内で何が起きているかを確実に把握するうえで常に障壁となってきたのは、完全な暗号解読です。これは法的レベルでも運用レベルでも非現実的な、多くのコストがかかるプロセスです。そのため、ネットワークとインフラストラクチャがデータ漏洩（侵害）からランサムウェア攻撃に至るあらゆるものに対して非常に脆弱な状態のままになっています。

真の課題は、暗号化されたトラフィックの内部にある悪意のあるアクティビティを検出する方法を見つけることです。新しいファイアウォールは、最小限の暗号解読支援とコストで最大の可視性を提供するために、これを機能として優先する必要があります。



3 | 脅威インテリジェンスを即時に要求する

ネットワーク、（多くの場合）脆弱で旧式のインフラストラクチャに対する脅威がかつてなく巧妙化していることと相まって、攻撃対象領域が拡大していることで、インテリジェンス フレームワークはサイバー犯罪者の一歩先を行く必要があります。スパム、マルウェア、その他のタイプの攻撃など、入ってくる脅威が何であるかを正確に特定しなければなりません。

この情報はファイアウォールが行うべき動作に関する基礎的な知識の役割を果たします。つまり、ネットワーク全体のデバイス、場所、ユーザーに関するダイナミックコンテキストを提供します。

4 | セキュリティレジリエンスを構築する

ハイブリッド環境では多くの場合、脆弱なデバイスやアプリからユーザーが日常的にネットワークにアクセスしており、ハッカーによるネットワークへの侵入を誘発する点がいくつもあります。旧式のインフラストラクチャは特に脆弱でハッカーにとって魅力的です。これに対する解決策は、セキュリティレジリエンスを構築することです。

セキュリティレジリエンスとは、可用性が高いセキュリティ インフラストラクチャの中核であるファイアウォールを保護することです。リスクに基づいてアラートとタスクに優先順位を付け、次に起こることを予測し、1 時間ごとのセキュリティアップデートと予期しない攻撃に対する対応を自動化でき、最終的には時間とコストの節約、不満の解消につながります。

5 | 包括的なアプローチを行う

可視性やコンテキストをさらに得られるツールや、トラフィックとインテリジェンスを管理するための統一された方法をいくつも活用できるため、ファイアウォールだけにとどまらないでください。ファイアウォールのパフォーマンスを向上させるための一連のツールを使用すれば、追加の出費なしでさらに多くの情報が見え、コンテキストをより深く理解できるようになるはずです。

サービス、複数のダッシュボード、アーキテクチャが分離していると、脅威管理が非常に複雑になります。迅速な意思決定、立ち止まっている時間の削減、有意義で実用的な指標の提供に役立つファイアウォールと拡張機能を追求してください。

Cisco Secure Firewall がセキュリティ態勢を向上させてますます巧妙になった脅威から政府機関を防御する方法をご覧ください。

Cisco Secure Firewall の詳細