SOPHOS
Cybersecurity evolved.

次世代型ファイアウォール バイヤーズガイド

ソフォスが実施した最新の調査で、現在使用しているファイアウォールにおける最も重大な課題についてネットワーク管理者と IT マネージャーに尋ねたところ、次のような回答がありました。

- ネットワークアプリケーション、リスク、および脅威を可視化できていない
- 最新のランサムウェアや攻撃からの保護に懸念がある
- ネットワークで発生した脅威への対応力が欠如している

これらの課題について共感できる方も多いのではないでしょうか。問題は、現在利用されている大半の次世代型ファイアウォールは適切に機能していないことです。十分な可視性や適切な保護機能を提供したり、発生した問題に対処したりすることができません。

次に導入するファイアウォールを選択する場合に、何を重視すれば良いのかさえわからないこともあります。重要な要件を特定することから始めたいと思われるでしょう。しかし、要件を確立した後でも、実際に仕様どおりに動作するファイアウォールを各ベンダーの Web サイトやデータシートから調べ上げて特定するという作業は非常に困難です。

このガイドの使用方法

このバイヤーズガイドは、貴社にとって最適なソリューションを選択できるように作成されており、ファイアウォールの購入で後悔しないことを目的にしています。こちらでは、ファイアウォールを今後購入するときに、検討する必要があるすべての機能について説明します。また、お客様の IT パートナーまたはベンダーの製品が、お客様のニーズを満たしているかどうかを確認するために役立つ重要な質問も記載しました。最後のいくつかのページには、最適なファイアウォールベンダーを絞り込むために役立つチャートを追加しています。

ネットワークセキュリティにおける パーフェクトストーム (壊滅的な事態) - 暗号化

増加し続ける暗号化されたトラフィックフローが、壊滅的な事態を引き起こすケースが増えており、その対応は差し迫った課題となっています。次のような現状があります。

- インターネットトラフィックの 90% が TLS で暗号化されている。
- マルウェア、 PUA 、およびハッカーサーバーの 50% が、検出を回避するために暗号化を利用している。
- 多くの組織は、暗号化されたトラフィックを検査していない。

暗号化されたトラフィックを検査していない理由を組織に尋ねると、一番の理由としてパフォーマンスの問題を挙げています。TLS インスペクションを実行するためには、膨大なリソースが必要となりますが、多くのファイアウォールは単純にリソースの制約によって大量の暗号化トラフィックに対応することができません。暗号化されたトラフィックを検査しない 2 番目に大きな理由として、ユーザビリティの問題が挙げられています。つまり、インターネットアクセスが切断されることが多くなるのです。

このような暗号化に存在している根本的な課題と、多くのファイアウォールで暗号化に対応できない状況が、リスクのある挙動やコンテンツの可視化、コンプライアンス対応、ランサムウェア、サイバー攻撃、情報漏洩の保護でさまざまな問題を引き起こしています。実際、今日のネットワークセキュリティの最重要課題の多くの根本原因は暗号化トラフィックにあります。残念ながら、ほとんどのネットワークでは、暗号化トラフィックの多くのがネットワークを通過するのを黙認しているのです。しかし、暗号化トラフィックに目をつむる必要はもうありません。この課題に対処できる非常に効果的な方法があります。

この詳細については、ホワイトペーパー『ファイアウォールの効果を無力化する暗号化トラフィック』を参照してください。

最重要の機能

ネットワークの可視化、保護、脅威への応答に関する最重要課題を解決するために、新たに導入するファイアウォールで必要となる 4 つの必須機能を紹介します。

TLS 1.3 のインスペクション – インターネットトラフィックの 90% が暗号化されるようになり、その割合が今も増加していることから、次に導入するファイアウォールには TLS 1.3 のインスペクション機能が含まれていなければなりません。さらに重要なのは、ファイアウォールがトラフィック処理のボトルネックになることがなく、実際に必要とされるよりもはるかに高価なファイアウォールを購入することを余儀なくされることもなく、効率的に実行できるインテリジェンスとパフォーマンスを提供できることです。すべての暗号化されたトラフィックについて検査をする必要はなく、またすべての暗号化されたトラフィックを検査できるわけでもありません。次に導入するファイアウォールでは、最新の標準および暗号スイートのすべてに対応しなければなりません。また、検査するべきトラフィックを適切に選択できるように、インテリジェントな例外処理が組み込まれていなければならず、さらに、潜在的な問題を簡単に特定し、オンザフライで例外を追加して問題を回避するツールも提供しなければなりません。また、現在、そして将来にわたって、増え続ける暗号化トラフィックに対応できる十分なパフォーマンスを提供できる必要があります。

ゼロデイ脅威からの保護 – 脅威は常に進化しています。組織を攻撃するために現在使用されているランサムウェアの亜種は、ほぼ確実に、次に使用されるランサムウェアとは異なります。これが、現在の脅威の特徴です。次に導入するファイアウォールには、最新のゼロデイ脅威を特定し、ネットワークに侵入する前に脅威を阻止するための、いくつもの機械学習モデルに基づく人工知能と、高度なエクスプロイト検出機能とランサムウェアによる暗号化を検出して防止する機能を備えたサンドボックス機能が必要です。

FastPath アプリケーションアクセラレーション –ネットワークトラフィックの約 80% は、約 2 割のアプリケーションから発生している場合があります。特定のアプリケーションが多くのネットワークを占有している状況はエレファントフローと呼ばれます。これらのエレファントフローは、会議やコラボレーションツール、ストリーミングメディア、および VoIP で一般的に見られます。これらの膨大なトラフィックフローを検査するためには大量のリソースが消費され、優れたユーザーエクスペリエンスを実現するためにパフォーマンスを最適化する必要があります。これは、大きな課題をもたらします。次に導入するファイアウォールは、これらの信頼できるトラフィックフローを適切に処理してオフロードすることで、最適なパフォーマンスを実現し、余裕が生まれたパフォーマンスを詳細なパケットインスペクションを必要とするトラフィックに向けることができるようにする必要があります。

他のサイバーセキュリティ製品との統合 – 単体の IT セキュリティ製品を使用するだけでは十分な効果を得ることはできなくなっています。現在の高度な攻撃では、多層防御が必要であり、各セキュリティレイヤーのすべてが連携して情報を共有し、同期された応答を実現しなければなりません。次に導入するファイアウォールは、エンドポイントのアンチウィルスプロテクションなどの他のシステムと統合でき、重要な脅威インテリジェンスとテレメトリを共有する必要があります。これにより、攻撃が発生した場合に、両方のシステムが連携して防御のための処置を調整できるようになります。また、これらのシステムの管理インターフェイスが一元化されており、展開や通常の管理のほか、製品横断的な脅威ハンティングやレポート作成を簡単に実施できる必要があります。

これらの 4 つの機能があれば、現在使用しているのファイアウォールで発生している最大の課題を解消することができ、将来にわたってネットワークの保護を強化できます。

重要な機能	ベンダーへの質問
TLS 1.3 インスペクション ネットワークを通過する膨大な暗号化トラフィックを可視化できます。	‣ TLS インスペクションは最新の 1.3 標準をサポートしているか？ ‣ すべてのポートとプロトコルに対応するか？ ‣ ストリーミングベースかプロキシベースか？ ‣ パフォーマンスに与える影響は？ ‣ 暗号化されたトラフィックフローをダッシュボードで可視化できるか？ ‣ 復号化をサポートしていないサイトをダッシュボードで可視化できるか？ ‣ 問題のあるサイトに例外を追加するための簡単なツールがあるか？ ‣ 包括的な例外リストが付属しているか？ ‣ そのリストを管理しているのは誰か？またリストは定期的に更新しているか？
ゼロデイ攻撃対策 機械学習とサンドボックスによる最新で未知の脅威から保護できます。	‣ ファイアウォールには、未知の脅威を検出するテクノロジーが含まれているか？ ‣ 機械学習を使用してファイルを分析しているか？ ‣ 適用している機械学習モデルはいくつあるか？ ‣ ソリューションにサンドボックスが含まれているか？ ‣ サンドボックス機能は、分析中にファイルを通過させることができるか？ ‣ サンドボックスソリューションはオンプレミスでもクラウドでも実行できるか？ ‣ サンドボックスソリューションには、サンドボックス環境でランサムウェアなどの脅威を特定できる主要なエンドポイントプロテクションテクノロジーが含まれているか？ ‣ サンドボックス機能を支援するために使用されるエンドポイントテクノロジーは何か？ ‣ 個別のレポート作成製品ではなく、どのような種類のレポート機能がオンボックスで提供されているか？ ‣ どのような種類のダッシュボードの可視化が提供されているか？
FastPath アプリケーション アクセラレーション 信頼されるアプリケーショントラフィックを FastPath にオフロードし、パフォーマンスを向上させ、オーバーヘッドを削減します。	‣ ファイアウォールは、信頼できるトラフィックやエレファントフローの FastPath アクセラレーションをサポートしているか？ ‣ これはソフトウェアまたはハードウェアで実行されているか？ ‣ FastPath アクセラレーションの対象となるアプリケーションはどのように特定されるか？ ‣ オフロードするアプリケーションを制御するために、どのようなポリシーツールが管理者に提供されているか？ ‣ FastPath アプリケーションアクセラレーションを実現するためにすぐに使用できるシグネチャが提供されているか？ ‣ FastPath パケットフロープロセッサはプログラムやアップグレードが可能であり、長期間にわたって利用できるか？
他の IT セキュリティ製品との統合 脅威への対応やフォレンジック調査や脅威ハンティングを行うためには、適切な多層防御を提供して製品間で情報を共有できるようにする統合が不可欠です。	‣ ファイアウォールはエンドポイントテクノロジーと統合されているか？ ‣ 2 つの製品間でどのような情報が共有されているか？ ‣ 特定の製品によって識別された脅威が他の製品と共有されるか？ ‣ 脅威が検出されるときにどのような応答が可能か？脅威を自動的に隔離できるか？隔離の仕組みはどうなっているか？ ‣ エンドポイントは、ユーザーやアプリケーションの使用状況に関する情報をファイアウォールに提供しているか？ ‣ ファイアウォールとエンドポイントは同じコンソールから管理できるか？クラウドベースか？ ‣ 製品横断的な脅威ハンティング (XDR) は可能か？ ‣ ベンダーは、フルマネージドのネットワーク可視および脅威応答サービスを提供しているか？ ‣ ファイアウォールは、Wi-Fi、ZTNA、エッジデバイス、ネットワークスイッチなどの他の製品と統合されているか？

主なファイアウォール機能

次のテクノロジーも、あらゆるファイアウォールソリューションにとって重要なコンポーネントです。これらの機能の多くは、あらゆるファイアウォールに搭載されている成熟した定番の機能であり、ベンダーは管理のしやすさと可視化の実用性のレベルに基づいて差別化されること多くあります。

次に導入するファイアウォールにはこれらの機能が含まれているだけでなく、管理が容易であることを確認してください。さらに重要なのは、これらの各領域におけるリスクと問題を明確に可視化できることです。

主要な機能	ベンダーへの質問
ディープパケットインスペクションと侵入防止 脅威とエクスプロイトを復号化して検査する機能を提供します。	‣ TLS インスペクションは最新の 1.3 標準をサポートしているか？ ‣ すべてのポートとプロトコルに対応するか？ ‣ ストリーミングベースかプロキシベースか？ ‣ パフォーマンスに与える影響は？ ‣ 暗号化されたトラフィックフローをダッシュボードで可視化できるか？ ‣ 復号化をサポートしていないサイトをダッシュボードで可視化できるか？ ‣ 問題のあるサイトに例外を追加するための簡単なツールがあるか？ ‣ 包括的な例外リストが付属しているか？ ‣ そのリストを管理しているのは誰か？またリストは定期的に更新しているか？
高度な脅威防御 (ATP) C&C サーバーへのコールホームや通信を行うボットやその他の高度な脅威とマルウェアを特定します。	‣ ファイアウォールには、未知の脅威を検出するテクノロジーが含まれているか？ ‣ 機械学習を使用してファイルを分析しているか？ ‣ 適用している機械学習モデルはいくつあるか？ ‣ ソリューションにサンドボックスが含まれているか？ ‣ サンドボックス機能は、分析中にファイルを通過させることができるか？ ‣ サンドボックスソリューションはオンプレミスでもクラウドでも実行できるか？ ‣ サンドボックスソリューションには、サンドボックス環境でランサムウェアなどの脅威を特定できる主要なエンドポイントプロテクションテクノロジーが含まれているか？ ‣ サンドボックス機能を支援するために使用されるエンドポイントテクノロジーは何か？ ‣ 個別のレポート作成製品ではなく、どのような種類のレポート機能がオンボックスで提供されているか？ ‣ どのような種類の可視化がダッシュボードで提供されているか？
Web プロテクションと URL フィルタリング Web ベースのマルウェア、侵害された Web サイト、および Web ダウンロードから保護します。	‣ ファイアウォールは、信頼できるトラフィックやエレファントフローの FastPath アクセラレーションをサポートしているか？ ‣ これはソフトウェアまたはハードウェアで実行されているか？ ‣ FastPath アクセラレーションの対象となるアプリケーションはどのように特定されるか？ ‣ オフロードするアプリケーションを制御するために、どのようなポリシーツールが管理者に提供されているか？ ‣ FastPath アプリケーションアクセラレーションを実現するためにすぐに使用できるシグネチャが提供されているか？ ‣ FastPath パケットフロープロセッサはプログラムやアップグレードが可能であり、長期間にわたって利用できるか？
アプリケーション制御 アプリケーショントラフィックを可視化および制御して、不要なトラフィックをシェーピングまたはブロックし、重要なアプリケーショントラフィックの処理を優先して高速化します。	‣ アプリケーションを識別するために使用される情報ソースは何か？ ‣ アプリケーションエンジンは、エンドポイントから取得した情報を使用してアプリケーションを識別をさらに強化できるか？それとも、ファイアウォールがパケットから収集できる情報だけに制限されているか？ ‣ ポリシールールを使用して、FastPath にアプリケーションを割り当て、優先的に WAN リンクからルーティングできるか？ ‣ クラウドアプリケーションとシャドウ IT に関するインサイトをダッシュボードで提供しているか？
VPN と SD-WAN サイト間およびリモートアクセス VPN 機能、 SD-WAN オーバーレイを提供し、複数 WAN 接続を管理します。	‣ ファイアウォールはエンドポイントテクノロジーと統合されているか？ ‣ 2 つの製品間でどのような情報が共有されているか？ ‣ 特定の製品によって識別された脅威が他の製品と共有されるか？ ‣ 脅威が検出されるときにどのような応答が可能か？脅威を自動的に隔離できるか？隔離の仕組みはどうなっているか？ ‣ エンドポイントは、ユーザーやアプリケーションの使用状況に関する情報をファイアウォールに提供しているか？ ‣ ファイアウォールとエンドポイントは同じコンソールから管理できるか？クラウドベースか？ ‣ 製品横断的な脅威ハンティング (XDR) は可能か？ ‣ ベンダーは、フルマネージドのネットワーク可視および脅威応答サービスを提供しているか？ ‣ ファイアウォールは、Wi-Fi、ZTNA、エッジデバイス、ネットワークスイッチなどの他の製品と統合されているか？

補完的なファイアウォール製品

次の補完的な製品は、ネットワークと保護を拡張するために重要な役割を果たす場合があります。選択するベンダーがこれらの製品も提供しており、ファイアウォールとの簡単に統合できるようにしていることを確認します。また、ファイアウォールからこれらの追加製品を直接管理することも、ファイアウォールと同じ一元的な管理コンソールから管理できることを確認します。

補完的な製品	ベンダーへの質問
ブランチオフィス向けの SD-WAN エッジデバイス 小規模なリモートブランチオフィスを接続するための手頃な価格で導入しやすいデバイス。	‣ 専用の VPN を介してリモートロケーションをメインファイアウォールに接続するデバイスを提供しているか？ ‣ ゼロタッチの導入は可能か？ ‣ 価格はどれぐらいか？ ‣ 専用トンネルとスプリットトンネルの両方をサポートしているか？ ‣ Wi-Fi や LTE など、どのようなモジュール設計の接続オプションをサポートしているか？
ワイヤレスアクセスポイント ワイヤレスに対応するようにネットワークを拡張します。	‣ ファイアウォールにワイヤレスコントローラが内蔵されているか？ ‣ 価格はどれぐらいか？ ‣ ワイヤレスアクセスポイントはプラグアンドプレイが可能か？ ‣ 複数の無線と SSID をサポートしているか？ ‣ メッシュネットワークをサポートしているか？
ZTNA リモートユーザーをアプリケーションやデータに安全に接続するゼロトラストネットワークアクセス。	‣ ZTNA ソリューションを提供しているか？ ‣ ファイアウォールやエンドポイントと何らかの形で統合されているか？ ‣ ファイアウォールと同じ一元的なコンソールで管理されているか？ ‣ ZTNA エージェントはエンドポイントエージェントと一緒に展開されるか？ ‣ デバイスヘルスはZTNA ソリューションとどのように統合されるか？
メール保護 スパム、フィッシング、迷惑メールから保護します。	‣ 統合型のオンボックスメールプロテクションを提供しているか？ ‣ クラウドマネージドのメールプロテクションを提供しているか？ ‣ 攻撃が疑われる添付ファイルをサンドボックス環境で分析できるか？ ‣ メールの暗号化と DLP に対応しているか？ ‣ ドメインベースのルーティングと完全な MTA モードを提供しているか？ ‣ 隔離管理のためのユーザーポータルを利用できますか？
WAF インターネットに公開されているオンプレミスサーバのリバースプロキシ保護のための Web アプリケーションファイアウォール。	‣ 統合型のオンボックス WAF 機能を提供しているか？ ‣ 一般的なサーバーでホスティングされるアプリケーション向けの定義済みテンプレートを使用して、簡単にセットアップできるか？ ‣ セキュリティ強化、 CSS、および Cookie の改ざん防止機能を提供しているか？ ‣ リバースプロキシの認証オフロードを提供しているか？

管理機能

ファイアウォール製品は、管理の容易さによって差別化されることが多くあります。数十年前から販売されている多くのファイアウォールは、時間の経過とともに新しい機能が追加されており、その時々で異なるユーザーインターフェイスコンセプトを採用しているため、製品の各セクションがまったく別製品のように見える問題があります。次の機能は、展開と日々の管理で大きな差異をもたらす可能性があります。

管理機能	ベンダーへの質問
一元管理 複数のファイアウォールまたは IT セキュリティ製品の管理。	‣ クラウド管理ソリューションを提供しているか？ ‣ このソリューションでは、複数のファイアウォールがどのように管理されるか？ ‣ 同じクラウドコンソールから管理されている製品は他にあるか？ ‣ 脅威インテリジェンスは製品間で共有されているか？製品横断的な脅威ハンティングが可能か？
レポート 提供されるレポート機能。	‣ ファイアウォールにログデータ用のオンボックスストレージが含まれているか？価格はいくらか？ ‣ オンボックスレポート機能は含まれているか？価格はどれぐらいか？ ‣ クラウドレポート機能はサポートされているか？価格はどれぐらいか？ ‣ 独自のレポートを作成、保存、エクスポート、スケジュールできるか？ ‣ syslog エクスポートはサポートされているか？ ‣ 製品横断的なレポート作成と脅威ハンティングはサポートされているか？
管理エクスペリエンス ファイアウォールの日々の管理をどれほど簡単に行うことができるか、何が重要かを強調します。	‣ 使用している製品のダッシュボードでは、ドリルダウン機能などの豊富な機能を利用できるか？ ‣ Web、アプリケーションコントロール、IPS、およびトラフィックシェーピングのポリシーがすべて 1 か所にまとめられているか？または、これらのコンポーネントを製品の各領域で設定する必要があるか？ ‣ ユーザーエクスペリエンスは製品のあらゆる部分で一貫しているか？ ‣ 新しいファイアウォールのオーナーのための、コンテキスト依存ヘルプ、ドキュメント、ビデオ、その他の充実したコンテンツが組み込まれているか？
ユーザーポータル セルフサービス方式でユーザーが操作できるポータル。	‣ ファイアウォールは、ユーザーが VPN クライアントや設定をダウンロードしたり、隔離されたメールを管理したりするユーザーポータルを提供しているか？

展開オプション

次に導入するファイアウォールを検討するときの別の重要事項は、現在および将来的に、いかに簡単にネットワークに統合できるかということです。ファイアウォールにネットワークを合わせるのではなく、ネットワークに柔軟に適合できるファイアウォールが必要です。AWS や Azure などのパブリッククラウドや、一般的な仮想化プラットフォーム、柔軟なモジュール式のハードウェアアプライアンスなど、さまざまな展開オプションを提供していることを確認してください。

展開オプション	ベンダーへの質問
ハードウェアアプライアンス 次に導入するファイアウォールは、できるだけ長期間使用できることを確認します。	‣ 自社のニーズに合ったアプライアンスのモデルがいくつ提供されているか？ ‣ どのような接続オプションが含まれているか？ ‣ どのようなモジュール設計の接続オプションが含まれているか？ ‣ 電源は冗長化されているか？ ‣ どのような高可用性オプションがあるか？ ‣ ファームウェアアップグレードはライセンスに含まれているか？ ‣ ハードウェアの保証はどうなっているか？
クラウド、仮想化、ソフトウェア 現在または将来的に重要となる可能性のあるハイブリッドネットワークのパブリッククラウドと仮想化への対応。	‣ ファイアウォールは、 AWS や Azure などのパブリッククラウドプラットフォームのマーケットプレイスで利用できるか？ ‣ 一般的なすべての仮想化プラットフォームをサポートしているか？ ‣ x86 ハードウェア上で動作するソフトウェアソリューションとしてアプライアンスを利用できるか？

ファイアウォール機能のチェックリスト

	Sophos	Cisco	Fortinet	PAN	SW	WG
主要なファイアウォール機能						
ファイアウォールルールと Web ポリシーのテストシミュレーター	✔		✔	✔		✔
FastPath パケット最適化	✔		✔	✔		
侵入防御システム	✔	✔	✔	✔	✔	✔
アプリケーションコントロール	✔	部分的に対応	✔	✔	✔	✔
デュアルエンジン型マルウェア対策	✔					✔
シャドー IT クラウドアプリの可視化	✔		✔	✔	✔	✔ - OEM
不要と思われるアプリケーション (PUA) のブロック	✔		✔	✔	✔	
Web プロテクションとコントロール	✔	✔	✔	✔	✔	✔
キーワードによる Web 監視機能と施行	✔		✔	✔	✔	✔
DPI エンジン：ストリーミング、プロキシ、またはその両方？	✔	フロー	✔	フロー	ストリーム	プロキシ
ユーザーとアプリケーションリスクの可視化 (ユーザー脅威指数)	✔		制限付き			
高度な脅威防御 (ATP)	✔	✔	✔	✔	✔	✔
オンボックスログ / 履歴レポート機能	✔		制限付き	制限付き		

	Sophos	Cisco	Fortinet	PAN	SW	WG
サーバーおよびメールプロテクション						
オンボックスのフル機能の WAF	✔					
オンボックスのメール機能：アンチウイルス、アンチスパム、暗号化、DLP	✔					

	Sophos	Cisco	Fortinet	PAN	SW	WG
コアの VPN および SD-WAN						
無制限に無料で利用できるフル機能のリモートアクセス VPN	✔	要追加コスト*	✔	要追加コスト*	要追加コスト*	要追加コスト*
IPSEC および SSL サイト間 VPN	✔	✔	✔	✔	✔	✔
SD- RED レイヤー 2 サイト間 VPN	✔					
SD-WAN クラウドマルチサイト VPN オーケストレーション	間もなく利用可能	✔	要追加コスト*			
SD-WAN のルーティングとリンク管理	✔	✔	✔	✔	✔	✔

	Sophos	Cisco	Fortinet	PAN	SW	WG
TLS インスペクション						
TLS 1.3 インスペクション	✔		✔	✔	✔	✔
暗号化されたトラフィックの問題をダッシュボードで可視化	✔					
ダッシュボードから TLS 例外を作成	✔					

* これらの機能は追加料金で利用可能

	Sophos	Cisco	Fortinet	PAN	SW	WG
ゼロデイ攻撃対策						
疑わしいファイルを複数の機械学習モデルで分析	✔	✔	✔	✔	✔	
疑わしいファイルを動的にサンドボックスで解析	✔	✔	✔	✔	✔	✔
クラウドベースのファイル分析	✔	✔	✔	✔	✔	✔
広範なオンボックス脅威分析レポート	✔	✔			✔	
SD-WAN のルーティングとリンク管理	✔	✔	✔	✔	✔	✔

	Sophos	Cisco	Fortinet	PAN	SW	WG
FastPath パケット最適化						
SD-WAN 、クラウド、 SaaS トラフィックの FastPath オフロード	✔		✔	✔		
ポリシーおよび自動 FastPath オフロード	✔		✔	✔		
ハードウェアのオフロードと高速化	✔		✔	✔		
プログラマブルなパケットフロープロセッサ	✔			✔		

	Sophos	Cisco	Fortinet	PAN	SW	WG
エンドポイントプロテクションの統合機能						
セキュリティが侵害されたホストの識別	✔	✔	要追加コスト*	✔	✔	✔
ファイアウォールでホストをネットワークの他の部分から自動的に隔離	✔					✔
EP レベルでホストを自動隔離して、水平方向の移動を防止	✔			要追加コスト*		✔
不明なネットワークアプリケーションの識別 (Synchronized App Control)	✔			✔		
製品横断的な脅威ハンティング (XDR) の有効化	✔			✔		
フルマネージド脅威応答サービスの有効化	✔			✔		

	Sophos	Cisco	Fortinet	PAN	SW	WG
ネットワークアクセスポートフォリオの統合						
統合型ワイヤレスコントローラとアクセスポイントソリューション	✔	✔	✔		✔	✔
ZTNA ソリューションとの統合	✔	✔	✔	✔	✔	
ネットワークスイッチ製品との統合	間もなく利用可能	✔	✔		✔	
リモートサービスアクセスエッジデバイス (SD-RED) との統合	✔					

* これらの機能は追加料金で利用可能

	Sophos	Cisco	Fortinet	PAN	SW	WG
クラウド管理						
豊富な機能でクラウドからファイアウォールを管理 - 追加料金なし	✔	✔	要追加コスト*		要追加コスト*	✔
EP、サーバー、モバイル、メール、暗号化、ファイアウォールに対応する一元的なクラウドコンソール	✔					✔
クラウドでのファイアウォール管理のグループ化	✔	✔	要追加コスト*		✔	
クラウドからのファームウェアアップデートのスケジュール	✔	✔	✔		✔	✔
クラウドから新しいファイアウォールの展開(ゼロタッチ)	✔	✔	要追加コスト*		✔	✔
クラウドファイアウォールのレポート	✔	✔	✔		✔	✔
クラウドマネージドの製品横断的な脅威ハンティング(XDR)	要追加コスト*			要追加コスト*		

	Sophos	Cisco	Fortinet	PAN	SW	WG
クラウドおよび仮想展開オプション						
AWS	✔	✔	✔	✔	✔	✔
Azure	✔	✔	✔	✔	✔	✔
Google	今後追加予定	✔	✔	✔		
Nutanix	✔		✔	✔	✔	
FWaaS	今後追加予定		✔	✔		
仮想化プラットフォーム	✔	✔	✔	✔	✔	✔
ソフトウェアアプライアンス (x86)	✔					

* これらの機能は追加料金で利用可能

Sophos Firewall

Sophos Firewall の特長や機能の詳細については、次の資料を参照してください。

- Sophos Firewall ソリューションの概説
- Sophos Firewall の機能一覧
- Sophos Firewall の製品カタログ

21-06-10 EN (DD)

SOPHOS

AXIS 株式会社アクシス

〒164-8721
東京都中野区本町 1-32-2 ハーモニータワー 2F
https://www.axisjp.co.jp/

※株式会社アクシスはソフォスの販売代理店です。製品、サービス詳細、価格等については弊社までご相談ください。
※掲載されている情報は予告なしに変更する場合があります。　※会社名および製品名は、各社の商標または登録商標です。

アクシス事務センター ソフォス販売係
Mail : contact_sophos@axisjp.co.jp
TEL : 050-3196-5333（平日 9:30 ～ 11:30 / 13:30 ～ 17:30）

21-08-20