SOPHOS

新機能

Sophos Firewall

Sophos Firewall OS v21.5 の主な新機能

保護機能とパフォーマンスの強化

Sophos NDR Essentials と Sophos Firewall の統合

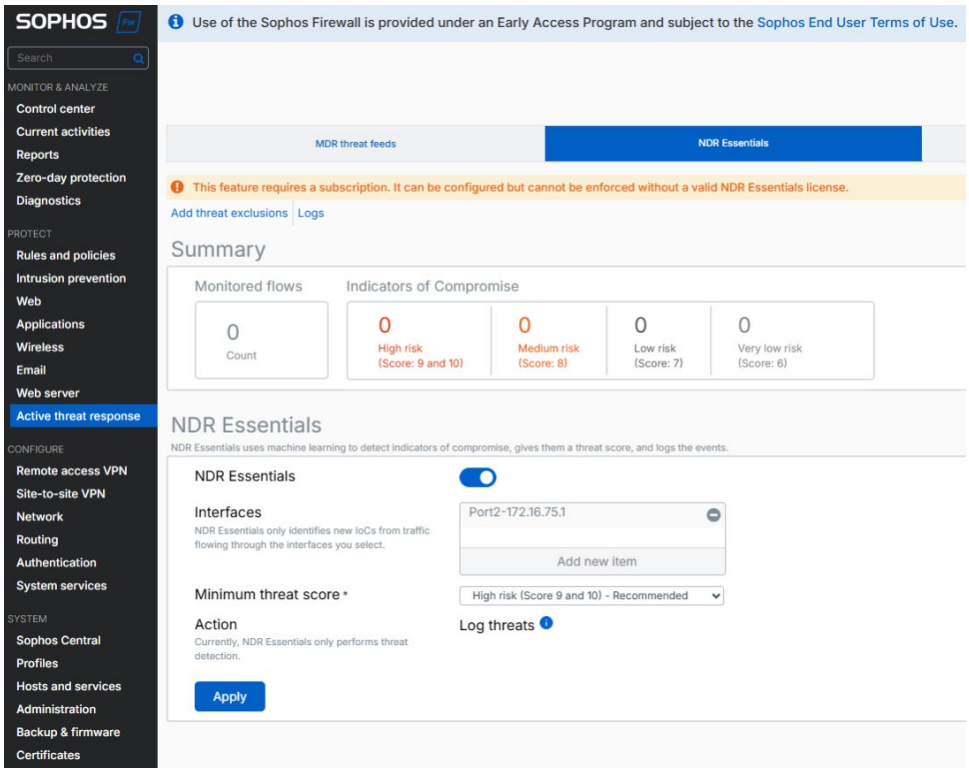
Network Detection and Response (NDR) は、ネットワークセキュリティ製品の一種であり、異常なトラフィックの挙動を検出し、ネットワークで活動するアクティブアドバーサリーを特定できるように設計されています。高度なスキルを有する攻撃者は検出を回避する方法に長けていますが、攻撃を実行するためには、最終的にはネットワークを必ず移動し、ネットワークの外部から通信する必要があります。NDR は通常、ネットワーク内に設置され、ネットワークトラフィックを監視および分析するセンサーを利用して、このような攻撃が疑われるアクティビティを特定します。

NDR 製品は古くから利用されており、Sophos NDR は 2023 年の初めから MDR/XDR 製品ポートフォリオに組み込まれています。しかし、SFOS v21.5 では、業界初の試みとして、Sophos Firewall に NDR を統合し、Xstream Protection を使用している Sophos Firewall のお客様が追加料金なしでご利用いただけるようになりました。

NDR を次世代ファイアウォールと統合することは、一見すると当然のアプローチに思えるかもしれません。しかし、ファイアウォールのパフォーマンスに影響を与えずに統合を実現することは、これまで大きな課題となっていました。NDR のトラフィック解析には、膨大な処理能力が求められます。この課題を解決するため、ソフォスは、NDR ソリューションを Sophos Cloud に展開することで、ファイアウォールの負荷を軽減するという斬新なアプローチを採用しました。

Sophos Firewall v21.5 では、クラウドから NDR プラットフォームを提供する新しい NDR Essentials が導入されました。NDR Essentials は、AI を活用した先進的な検出技術により、アクティブアドバーサリーを特定します。さらに、Active Threat Response の一環として Sophos Firewall の脅威フィード API を通じて情報を共有し、検出された脅威とその相対的リスクをリアルタイムで通知します。

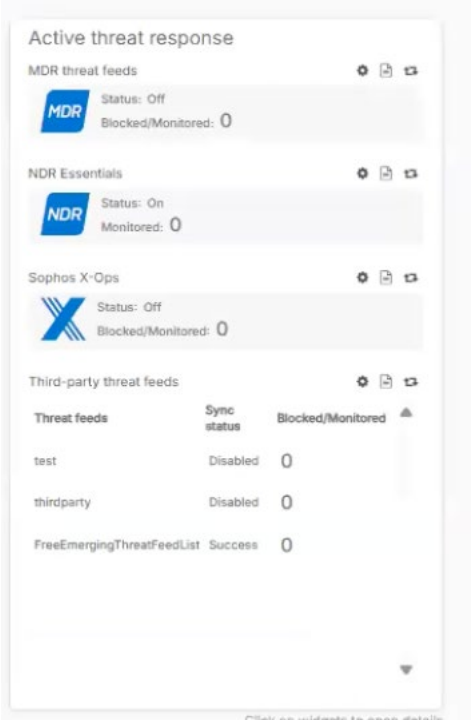
Sophos Firewall と NDR Essentials の連携の仕組み：Sophos Firewall は、TLS で暗号化されたトラフィックと DNS クエリからメタデータを取得し、その情報を Sophos Cloud 内の NDR Essentials に送信し、複数の AI エンジンを使用してデータが分析されます。TLS トラフィックを復号することなく、暗号化された悪意のあるペイロードを検出できるほか、侵害の重要な兆候となるアルゴリズム生成ドメイン (DGA) や異常なドメインも識別します。メタデータの抽出は、Xstream FastPath に実装された新しい軽量なエンジンによって実行されるため、XGS シリーズハードウェアのファイアウォールでのみ利用可能です。仮想ファイアウォール、ソフトウェアファイアウォール、クラウドファイアウォールは、将来的にこの NDR が統合される可能性がありますが、v21.5 では統合されていません。



Active Threat Response 内で、他の脅威フィードとあわせて NDR Essentials フィードを設定および監視します。

新しい NDR Essentials 脅威フィードは、上のスクリーンショットに示すように、ファイアウォールの Active Threat Response エリアで他の脅威フィード (Sophos X-Ops フィード、MDR フィード、サードパーティフィード) と共に管理されます。容易なセットアップ：スイッチをオンにして、監視する内部インターフェースを選択し、検出リスクの最小しきい値を設定するだけでセットアップは完了します。

NDR Essentials によって検出された脅威は、1 (低リスク) から 10 (高リスク) の範囲でスコアが付けられます。アラートを発行するしきい値とするリスクスコアは、お客様の環境に合わせて決定してください。推奨されるデフォルトスコアは、高リスクを示すスコア 9 ～ 10 です。検出されたスコアが 6 以上の脅威はすべてログに記録されますが、しきい値を以上となった場合にのみが通知し、新しいコントロールセンターのダッシュボードウィジェットにアラートとして表示されます。スコアが 6 未満の検出は誤検出の可能性があるため、ログには記録されません。NDR Essentials の検出は現在ブロックされませんが、将来的にはブロックするオプションを追加する可能性があります。すべての検出結果は、Active Threat Response レポートで確認できます。これはオンボックスレポートおよび Sophos Central Firewall Reporting の両方で利用できます。



リスクしきい値の設定値を以上となった NDR Essentials の検出は、新しくなったコントロールセンターのウィジェットに表示されます。

検出された脅威に対するさらに詳細な洞察と脅威ハンティング機能を必要とされる場合は、新しい NDR の調査コンソールが追加され Sophos NDR のすべての機能を実装する、Sophos XDR (Extended Detection and Response) を利用されることを強くお勧めします。また、24 時間 365 日体制で稼働する MDR サービスもご検討ください。これらの製品やサービスはすべて、Sophos Firewall と連携してさらに優れた効果を発揮します。

リモートアクセス VPN SSO

Sophos Connect クライアントと VPN ポータルでの Entra ID (Azure AD) シングルサインオン

最も多く寄せられたご要望のひとつが、Sophos Connect クライアントやファイアウォールの VPN ポータルで企業ネットワークの認証情報を使用できるようにして、エンドユーザーがリモートアクセス VPN をより簡単に利用できるようにすることでした。Entra ID (Azure AD) シングルサインオンと Sophos Connect および VPN ポータルの統合が SFOS v21.5 に追加されました。業界標準である OAuth 2.0 および OpenID Connect プロトコルを活用することで、クラウドネイティブな統合を実現し、シームレスなユーザーエクスペリエンスを提供します。Microsoft Windows では、Sophos Connect クライアント 2.4 以降に対応しています。

その他の VPN と拡張性の強化

ユーザーインターフェースと利便性の向上：直感的に理解できるように、接続タイプの名前が「サイト間接続 (site-to-site)」から「ポリシーベース接続 (policy-based)」に変更され、トンネルインターフェースの名前も「ルートベース (route-based)」に変更されました。

IP リースプールの検証を向上:IP リースプールは、SSLVPN、IPsec、L2TP、PPTP などのリモートアクセス VPN 間で、IP アドレスの競合を防ぐために使用されます。

厳格なプロファイルの適用：トンネルが正常に確立されない問題やパケットの断片化を防ぐために、デフォルト値を除外した IPsec プロファイルが使用されます。これにより、ハンドシェイクを確実に成功させます。

ルートベースの VPN の拡張性の強化：最大 3,000 トンネルをサポートし、ルートベース VPN のキャパシティを倍増しました。

SD-RED の拡張性の強化：Sophos Firewall は現在、最大 1,000 個のサイト間 RED トンネルと最大 650 台の SD-RED デバイスをサポートしています。

Sophos DNS Protection

Sophos DNS Protection がさらに使いやすく進化

昨年、ソフォスは DNS Protection サービスを開始し、Xstream Protection ライセンスが含まれるファイアウォールを利用されているすべてのお客様が無料で利用できるようにしました。今回のリリースでは、Sophos DNS Protection と Sophos Firewall の統合がさらに強化されました。サービスの状態を確認できる新しいコントロールセンターウィジェットの追加に加え、ログや通知によるトラブルシューティングの効率化が図られています。さらに、Sophos DNS Protection の設定を簡単に行えるガイド付きチュートリアルも新たに提供されています。

管理の合理化と利便性を高める機能

Sophos Firewall の他のすべてのリリースと同様、本バージョンでは日常の管理業務をより簡単にするいくつかの機能が向上しています。

テーブル列のサイズ変更：長らくご要望をいただいていた機能として、多くのファイアウォールのステータスおよび設定画面で列幅の調整が可能になりました。調整した列幅はブラウザのメモリに保存されるため、次回アクセス時にもその設定が維持されます。SD-WAN、NAT、SSL、ホストとサービス、サイト間 VPN などの多くの画面で、この新機能が適用されます。

拡張フリーテキスト検索:SD-WAN ルートを、ルート名や ID、オブジェクト、IP アドレスやドメインなどのオブジェクト値、またはその他の条件によって検索できるようになりました。ローカル ACL ルールは、コンテンツベースの検索など、オブジェクト名と値による検索もサポートされるようになりました。

デフォルト設定：多くのご要望にお応えして、新しいファイアウォールのセットアップ時に自動的に作成されていたデフォルトのファイアウォールルールおよびルールグループは削除され、初期設定時にはデフォルトのネットワークルールと MTA ルールのみが提供されるようになりました。デフォルトのファイアウォールルールグループとカスタムゲートウェイのデフォルトゲートウェイ調査は、どちらもデフォルトで「None」(なし) に設定されています。

新しいフォント：Sophos Firewall のユーザーインターフェースは、より軽量で明瞭なデザインとシャープなフォントに変更され、視認性とパフォーマンスが向上しました。

その他の機能強化

仮想、ソフトウェア、クラウドライセンス：Sophos Firewall のすべての仮想、ソフトウェア、クラウドライセンス (BYOL) に RAM の制限がなくなりました。ライセンスはコア数によって厳密に制限され、RAM の制限はありません。

WAF のファイルサイズ制限の拡大：Web アプリケーションファイアウォール (WAF) のリクエスト (アップロード) ファイルサイズの制限を設定できるようになり、最大で 1 GB のファイルをスキャンできるようになりました。

セキュリティを基盤とした設計：Sophos Firewall のセキュリティは継続的に強化されており、今回のリリースでは、安全なハッシュ検証を活用し、コア OS ファイルに予期しない変更があった場合にリアルタイムでフラグを立てるテレメトリ収集機能が追加されました。これにより、Sophos の監視チームは、潜在的なセキュリティインシデントが実際の問題に発展する前に、プロアクティブかつ迅速に問題を特定できるようになりました。

DHCP プレフィックスの委任の緩和：/48 と /64 のプレフィックスをサポートし、ISP との相互運用性が向上しました。ルーター広告 (RA) と DHCPv6 サーバーもデフォルトで有効になりました。

経路 MTU 探索：このプロトコルにより、ブラウザの最新の ML-KEM (Kyber) 鍵交換サポートに起因する TLS 復号エラーが解決されます。Sophos Firewall のディープパケットインスペクションエンジンは、各フローの MTU を自動的に検出・調整し、ネットワーク条件に応じて最適なパフォーマンスを提供します。

NAT64 (IPv6 から IPv4 へのトラフィックの処理)：NAT64 は、明示的なプロキシモードを使用して、IPv6 から IPv4 へのトラフィックを処理します。このモードでは、IPv6 のみのクライアントが IPv4 の Web サイトにアクセスできます。ファイアウォールはまた、IPv6 のみのクライアントのための IPv4 アップストリームプロキシもサポートしています。

ソフォス株式会社営業部
Email: sales@sophos.co.jp

2025-03-31 JA (DD)