SOPHOS

新機能

Sophos Firewall

Sophos Firewall OS v21 の主な新機能

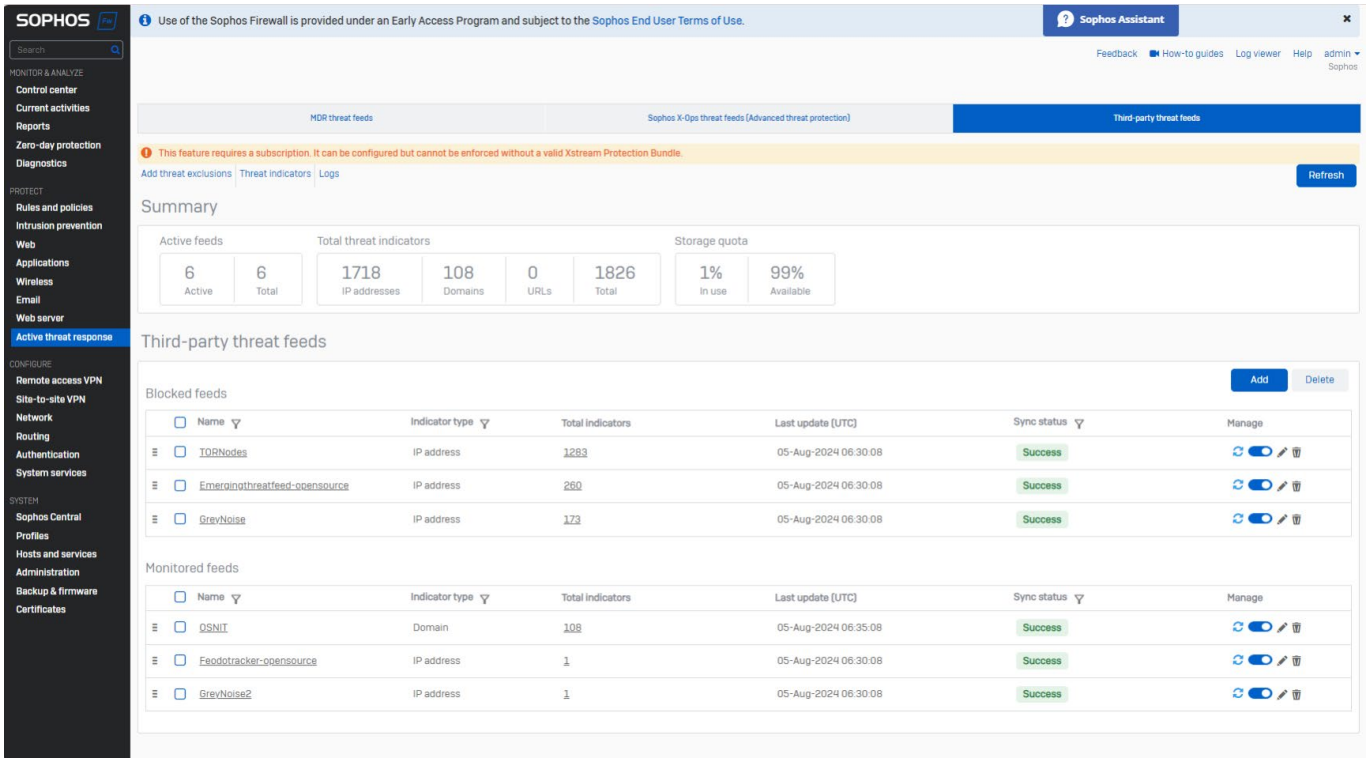
保護機能の追加：

サードパーティの脅威フィード

v20 で追加された Active Threat Response により、Sophos Firewall に新しい拡張可能な脅威フィードフレームワークが導入されました。当初は、Sophos X-Ops からの動的な脅威インテリジェンスフィードがサポートされていました。また、Sophos MDR により、このフレームワークを通じて公開されたすべての脅威へのアクセスをブロックすることで、ファイアウォールが自動対応するできるようになりました。

ほとんどのお客様にはこれだけで十分ですが、カスタムの脅威フィードが推奨される、または必須となる地域や業種もあります。また、パートナーコミュニティ、SoC (セキュリティオペレーションセンター) プロバイダー、そして多くのお客様から、既存の、または新しい脅威検出・対応ソリューションやサービスをサポートする拡張可能な脅威フィード機能への関心が寄せられています。

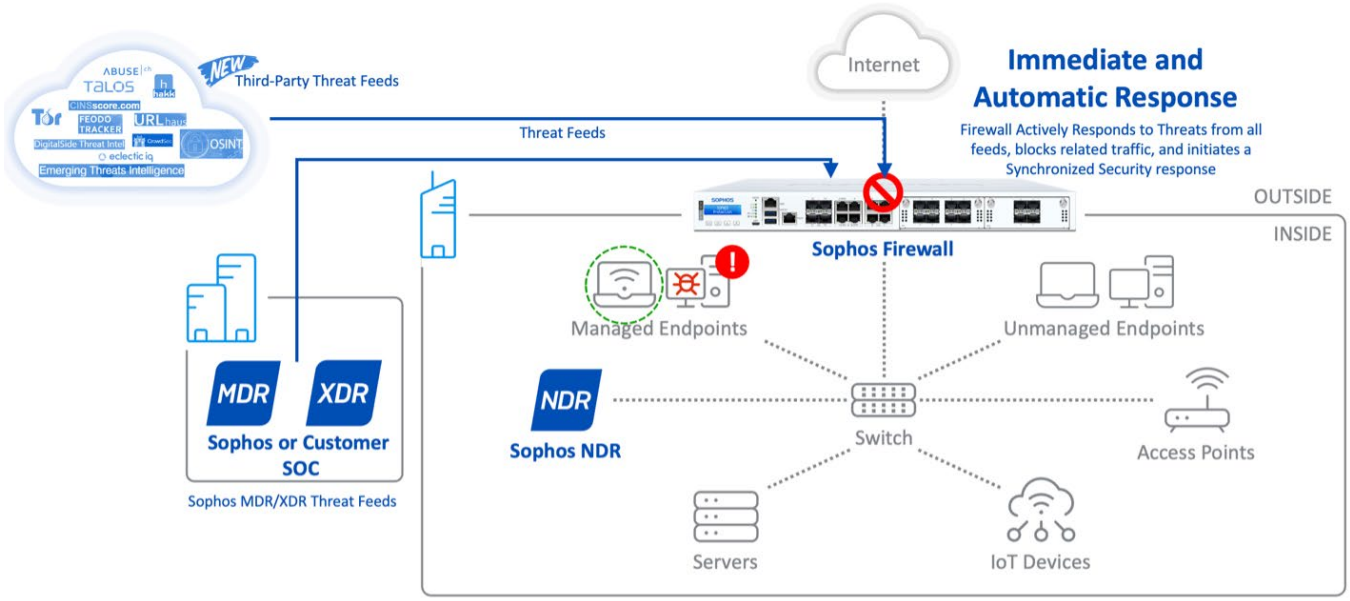
Sophos Firewall v21 ではそうしたユースケースを実現できるよう、サードパーティの脅威フィードをサポートする脅威フィードフレームワークが拡張されました。これにより、業種別やカスタムの脅威フィードを簡単にファイアウォールに追加し、すべてのセキュリティエンジンで自動的に同じ方法で監視・対応し、関連するすべての活動をブロックできるようになりました。しかも、ファイアウォールにルールを追加する必要もありません。



サードパーティの脅威フィードの設定と監視は、Active Threat Response メニューから実行できます。

MSP サービスもサポートされているので、ソフォスパートナーは、この機能を自社の MDR (Managed Threat Detection and Response) サービスの一環として最大限に活用することができます。競合する MDR ソリューションもサポートされており、Sophos Firewall をお客様がお使いの脅威検出・対応環境とより緊密に統合できます。

たとえば、Sophos Firewall は、脅威フィードの配信元を介して公開された C2 サーバーと通信しているデバイスを特定した場合、自動的に Active Threat Response を開始して、ネットワーク上のホストからその C2 サーバーに接続しようとするすべての要求とトラフィックをブロックし、侵害されたデバイスのセキュリティハートビートステータスを赤色に変更します。ファイアウォールルールの設定は不要です。



サードパーティの脅威フィードがサポートされ、Active Threat Response が拡張されました。

セキュリティ企業、業界コンソーシアム、コミュニティベース / オープンソースの脅威インテリジェンスソースなど、以下のようなさまざまな専門的かつ業界に特化した脅威フィードがサポートされています。

- Cisco Talos
- GreyNoise Intelligence
- Abuse.ch/URLhaus
- Hakk Solutions
- OSINT (オープンソースインテリジェンス)/DigitalSide
- CINS Score
- CrowdSec
- EclicticIQ
- Feodo Tracker

その他多数

すべての脅威フィードに対応する Synchronized Security

Active Threat Response は、他のセキュリティハートビートが赤色になっている状態と同じ Synchronized Security の対応をトリガーとします。この対応には、ハートビートの状態を含むファイアウォールルールの適用が含まれます。また、ファイアウォールはラテラルムーブメント保護を調整します。これにより、LAN 上に侵害されたホストがあることを正常に管理されているすべてのエンドポイントに通知し、そのデバイスからトラフィックをブロックできるようにします。

拡張性の強化

Sophos Firewall v21 ではネットワーク機能が強化されているので、多くの組織においてパフォーマンスと拡張性が向上します。

高可用性の強化

耐障害性の向上、シームレスな移行、ダウンタイムの短縮：高可用性 (HA) 環境は、動的ルートのシームレスなフェイルオーバーによって強化されています。SD-RED トンネルのフェイルオーバーも大幅に改善されているため、HA フェイルオーバーから数秒以内にトンネルが再確立されるようになり、ダウンタイムが短縮されます。HA フェイルオーバー時の Active Directory ドメインとの連携も改善され、よりスムーズな移行が可能になりました。

IPsec VPN の機能強化

サイト間 IPsec パフォーマンスの向上：FQDN ベースのリモートゲートウェイが最適化され、分散デプロイのスケーラビリティが向上しました。さらに、ファイアウォールの背後に配置された DHCP サーバーへのトラフィックに対して、XFRM インターフェイスを介した DHCP リレーを使用できるようになりました。RBVPN のデプロイでは、XFRM インターフェイスのアップタイムが最大 20 倍改善されており、トンネルのフラップやリブート時の中断を大幅に短縮します。

管理機能の強化：接続の一括有効化および無効化オプションが利用可能になりました。VPN 管理ページのフィルタリングが強化され、複数ページにまたがる情報が統合されるようになりました。また、インターフェイスページに XFRM インターフェイス固有のビューが追加され、RBVPN インターフェイスのフィルタリングが容易になりました。

認証と Web プロテクションの強化

認証機能の強化：LDAP クライアントと Google Chromebook SSO を介した Google Workspace の統合がサポートされるようになりました。Radius SSO、STAS、Synchronized User ID のバーストログイン処理のパフォーマンスが最大 4 倍向上しました。これにより、複数の SSO 環境 (STAS、Radius SSO、Synchronized User ID が混在する環境) でも数千件の同時ログイン要求に対応できます。さらに、HSTS が適用されている場合、HTTP または HTTPS 上で Kerberos および NTLM ハンドシェイクを可能にする、透過的な AD SSO エクスペリエンスのサポートが追加されました。

Web プロテクションのパフォーマンス強化：SafeSearch、YouTube の制限、Google App のログインドメイン、Azure AD テナントの制限を実施することで、システム負荷が大幅に軽減され、パフォーマンスが向上します。

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機能が向上しています。

Let's Encrypt 証明書のサポート：以前から要望の多かった機能である Let's Encrypt 証明書のサポートにより、証明書署名要求 (CSR) に基づく証明書の自動展開と更新が可能になりました。Let’s Encrypt 証明書は、WAF、SMTP、TLS 構成、ホットスポットのサインイン、Web 管理コンソール、ユーザーポータル、キャプティブポータル、VPN ポータル、および SPX ポータルでサポートされています。

静的ルート管理：ユーザーは静的ルートの複製、有効化 / 無効化、および説明の追加を行うことができます。ブラックホールルートオプションが追加され、負荷分散のための等価コストマルチパス (ECMP) がサポートされるようになりました。

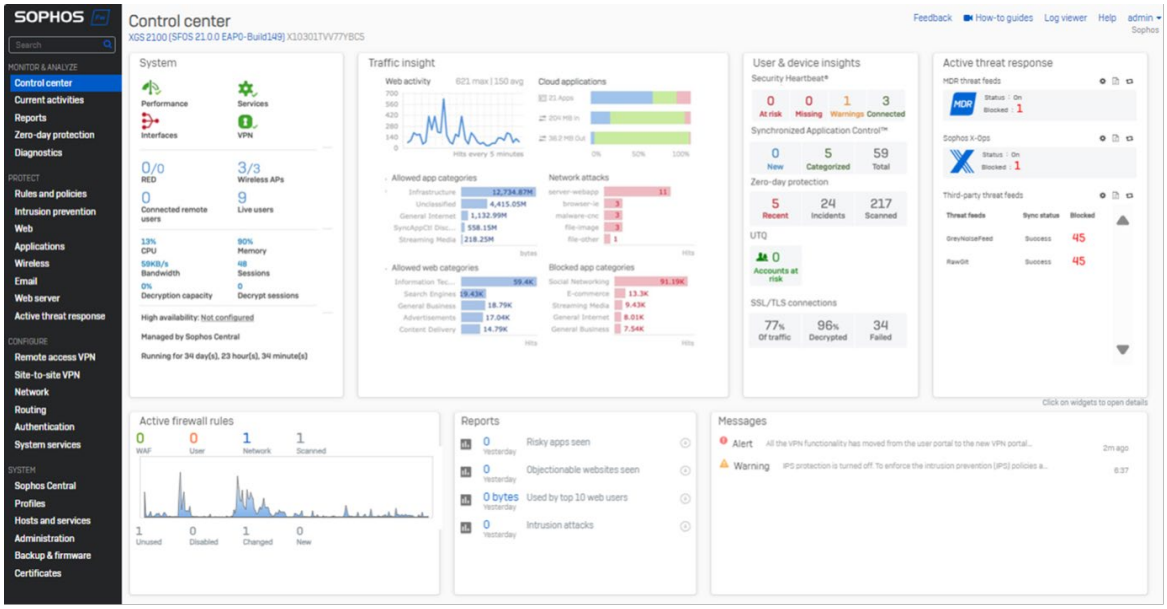
オブジェクト参照の拡張：インターフェイス、ゾーン、ゲートウェイ、SD-WAN プロファイルに関して、ネットワークオブジェクト参照 (使用状況) の可視性が向上しました。また、オブジェクト参照 (使用状況) のカウントを取得するための XML API サポートにも対応しているので、使用されていないオブジェクトも可視化されます。

VPN 構成の向上：Sophos Firewall は、リモートアクセスやサイト間 VPN のネットワーク、サブネット、ユーザーなどの VPN 構成において、フリーテキスト検索とバリューベース検索をサポートするようになりました。

動的ルーティング：BGP ルートを OSPFv3 に再分配する新しいオプションが追加されました。

カードビューによる Control Center の改良：Sophos Firewall Control Center に新しいカードビューが追加され、重要なネットワークイベントやデータに対する可視性をさらに向上しました。まったく新しい Active Threat Response カードにより、MDR、Sophos X-Ops、およびサードパーティの脅威フィードからの脅威情報が 1 つの見やすいセクションに集約されています。

刷新され、応答性が向上した Web 管理コンソール：Sophos Firewall の Web 管理コンソールは、Sophos Central とマッチするように、最新のソフォスデザインスタイルガイドを採用しています。また、レスポンス性が大幅に向上し、より快適な管理エクスペリエンスを提供します。



リニューアルされた Sophos Firewall Control Center は、新しいカードビューと最新のデザインを採用しています。

シームレスなアップグレード

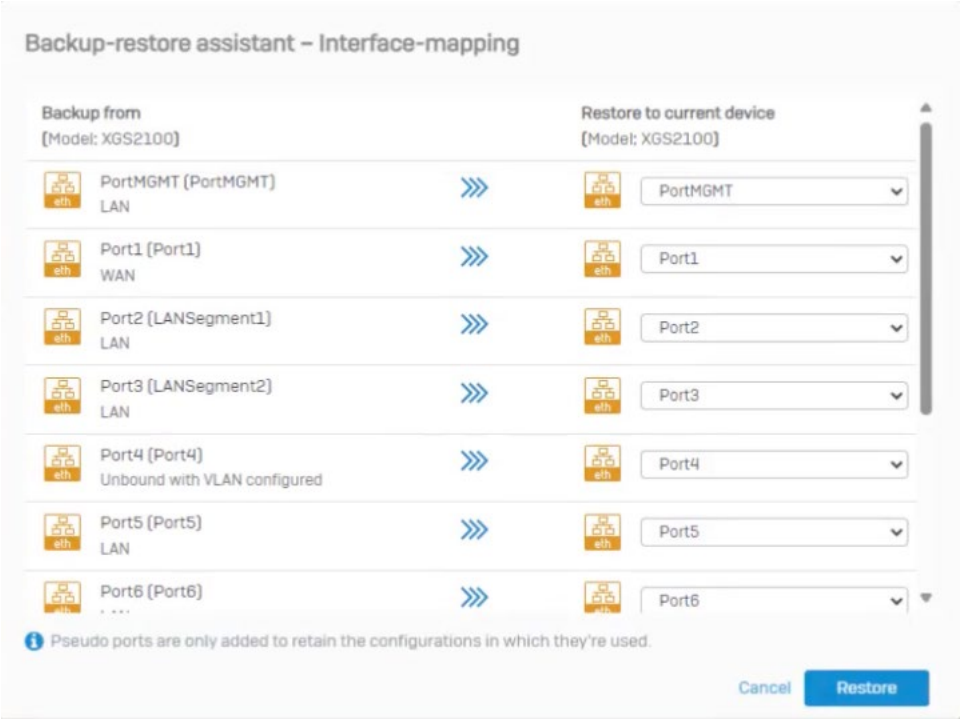
Sophos Firewall v21 には、v20 MR2 で初めて導入された便利な機能が搭載されており、最新の XGS シリーズへのアップグレードが簡単に実行できます。

ポートマッピング機能を使用した、あらゆる組み合わせでのバックアップと復元

新しい Sophos Firewall のバックアップと復元アシスタントでは、柔軟なインターフェイスマッピングオプションを使用して、ファイアウォール設定のバックアップを別のファイアウォールアプライアンスに簡単に復元できます。

これにより、Sophos Firewall XG シリーズから XGS シリーズへのアップグレード、XGS シリーズから他の XGS シリーズへのアップグレード、さらにはソフトウェアアプライアンスや仮想アプライアンスに簡単に移行できます。また、新しいファイアウォールやアップグレードしたファイアウォールの高速ポートにインターフェイスを簡単に移行できます。

さらに、仮想アプライアンスから構成テンプレートを作成およびエクスポートし、いくつものハードウェアまたは仮想環境で復元して、マルチデバイス環境のアップグレードを簡素化できます。



旧アプライアンスから新アプライアンスへのインターフェイスのマッピングが容易に

アップグレードの手順および新しいバックアップ / 復元アシスタントの詳細については、こちらの記事をご覧ください。

ソフォス株式会社営業部
Email: sales@sophos.co.jp

2024-10-16 JA (PC)

SOPHOS