SOPHOS

Sophos Firewall の機能

Sophos Firewall

主な特長

- Xstream アーキテクチャが、ストリームベースのパケット処理により、最高レベルの可視性、保護、パフォーマンスを提供
- Xstream TLS インスペクションが、高性能、ダウングレードなしの TLS 1.3 のサポート、ポートに依存しない、あらかじめ例外を組み込んだエンタープライズレベルのポリシー、独自のダッシュボードの可視性、および互換性のトラブルシューティングを提供
- Xstream DPI エンジンが、単一の高パフォーマンスエンジンを備えた IPS、AV、Web、アプリ制御、および TLS インスペクションのストリームスキャン保護を提供
- Xstream Network Flow FastPath が、ポリシーベースでインテリジェントに信頼できるトラフィックを高速で処理
- インタラクティブなコントロールセンターを備えた専用設計のユーザーインターフェースで、信号機のようなわかりやすい色分け（赤、黄、緑）で、注意が必要な情報を一目で確認可能
- Control Center が、エンドポイントのセキュリティ状態、不明な Mac および Windows アプリケーション、クラウドアプリケーションとシャドー IT、不審なペイロード、リスクの高いユーザー、高度な脅威、ネットワーク攻撃、不適切な Web サイトなどに関する情報を即座に提供
- 2 回クリックするだけで目的の画面に移動できる最適化されたナビゲーション
- ポリシーコントロールセンターのウィジェットは、ビジネスに関するポリシーアクティビティ、ユーザーおよびネットワークポリシーを監視し、使用されていないポリシー、無効化されているポリシー、変更されたポリシー、および新しいポリシーを追跡
- 統合型のポリシーモデルで、すべてのビジネス、ユーザー、およびネットワークファイアーウォールルールをグループ化、フィルタリング、および検索オプションを備えた単一の画面に統合
- 自動および手動でカスタムグループを作成でき、一目で分かるマウスオーバー機能と強制インジケーターを備えた大規模なルールセット向けの合理化されたファイアウォールルールの管理
- すべてのファイアウォールルールは、アンチウィルス、サンドボックス、IPS、Web、アプリ、トラフィックシェーピング (QoS)、およびハートビートに適用されるセキュリティとコントロールの概要を分かりやすく提供
- 事前に定義された IPS、Web、アプリ、およびトラフィックシェーピング (QoS) ポリシーにより、一般的な展開シナリオ (CIPA、一般的な職場ポリシーなど) の迅速なセットアップと簡単なカスタマイズが可能
- IPS、Web、アプリ、およびトラフィックシェーピング（QoS）ポリシーは、ファイアウォールルールに適用され、インプレースで編集可能。セキュリティやコントロールを設定したり、管理するための強力かつ直感的なモデルを提供
- Sophos Security Heartbeat™ が、ソフォスのエンドポイントをファイアウォールに接続して、セキュリティの状態とテレメトリを共有し、感染したエンドポイントや侵害されたエンドポイントを即座に識別可能
- エンドポイントのセキュリティ状態に対する動的なファイアウォールルールのサポート (Sophos Security Heartbeat) は、侵害されたエンドポイントへのネットワークアクセスを自動的に隔離して制限
- Synchronized Application Control が、ネットワーク上のすべての不明な Mac/Windows アプリケーションを自動的に識別、分類、制御
- Cloud Application Visibility が、シャドー IT の検出を即座に有効にし、ワンクリックでトラフィックシェーピングを提供
- ポリシーの検証シミュレータツールを使用することで、ファイアウォールルールと Web ポリシーのシミュレーション、ユーザ、IP、時刻ごとのテストを実行可能
- ユーザー脅威指数により、Web 閲覧履歴や ATP トリガー回数に基づいてリスクの高いユーザーを特定
- RMM/PSA 統合のすべての機能向けの構成 API
- Synchronized Security をサポートするトライアルと PoC でのシームレスな統合のためのディスカバーモード (TAP モード)
- SD-WAN は、地理的に分散したネットワークを介してリモートサイトや支社サイトを接続
- Windows/Mac 向けの無料で簡単に使用できるクライアントを備えたリモートアクセス VPN
- クラウドベースの管理およびレポート機能を提供する Sophos Central は複数のファイアウォールをサポートし、すべてのソフォスの IT セキュリティ製品に対応するグループポリシー管理と一元的なコンソールを提供
- 簡単で合理化されたセットアップウィザードにより、数分で導入可能
- 新しいファイアウォール向けの Sophos Central のゼロタッチ導入とゼロタッチ設定

Base Firewall

一般的な管理

- 目的に合わせて構築された合理的なユーザーインターフェースと、一目で分かるルール機能と強制インジケーターを備えた大規模なルールセットに対応するファイアウォールルールの管理
- 管理者アクセス、ユーザーポータル、IPSec、および SSL VPN に対する 2 要素認証 (ワンタイムパスワード) のサポート
- GUI で利用できる高度なトラブルシューティングツール (パケットキャプチャなど)
- 2 台のデバイスをアクティブ / アクティブまたはアクティブ / パッシブモードでクラスタリングする高可用性 (HA) をサポートし、プラグアンドプレイで素早く HA を設定可能
- GUI からアクセス可能な完全なコマンドラインインターフェイス (CLI)
- ロールベースの管理
- 自動化されたアップデートプロセスとロールバック機能により、ファームウェアアップデート通知を自動化
- ネットワーク、サービス、ホスト、時間帯、ユーザーとグループ、クライアント、サーバーの再利用可能なシステムオブジェクト定義
- セルフサービスユーザーポータル
- 構成変更のトラッキング
- ゾーン別のサービスに対する柔軟なデバイスアクセス制御
- メールまたは SNMP トラップ通知オプション
- SNMP v3 および NetFlow のサポート
- Sophos Central からの集中管理
- バックアップと復元の構成 : ローカル、FTP またはメール経由、オンデマンド (毎日、毎週、または毎月)
- サードパーティ統合のための API
- インターフェイス名の変更
- Sophos サポートのためのリモートアクセスオプション
- MySophos アカウントを使用したクラウドベースのライセンス管理

Sophos Central の管理

- クラウドベースの管理およびレポート機能を提供する Sophos Central は複数のファイアウォールをサポートし、すべてのソフォスの IT セキュリティ製品に対応するグループポリシー管理と一元的なコンソールを提供
- グループポリシー管理により、オブジェクト、設定、およびポリシーを一度変更すると、グループ内のすべてのファイアウォールに自動的に同期可能
- タスクマネージャーでは、グループポリシーの変更に関する完全な履歴の監査証跡とステータスの監視が可能
- Sophos Central のバックアップとファームウェア管理では、各ファイアウォールの過去 5 回分の構成バックアップファイルが保存され、永続的な保存して簡単にアクセス可能
- Sophos Central からあらゆるデバイスにワンクリックでファームウェアアップデートを実行可能
- ゼロタッチ展開では、Sophos Central で初期の構成を実行し、デバイスの起動時にフラッシュドライブからロードしてデバイスを自動的に Sophos Central に接続できるようにエクスポート可能

ファイアウォール、ネットワーク、およびルーティング

- ステートフルディープパケットインスペクションを実行するファイアウォール
- Xstream のパケット処理のアーキテクチャは、ストリームベースのパケット処理により、最高レベルの可視性、保護、パフォーマンスを提供
- Xstream TLS インスペクションは、高性能、ダウングレードなしの TLS 1.3 のサポート、ポートに依存しない、エンタープライズレベルのポリシー、独自のダッシュボードの可視性、および互換性のトラブルシューティングを提供
- Xstream DPI エンジンが、単一の高パフォーマンスエンジンを備えた IPS、AV、Web、アプリ制御、および TLS インスペクションのストリームスキャン保護を提供
- Xstream Network Flow FastPath が、ポリシーベースでインテリジェントに信頼できるトラフィックを高速で処理
- ユーザー、グループ、時間、またはネットワークベースのポリシー
- ユーザー / グループ別のアクセス時間ポリシー
- ゾーンやネットワーク全体、あるいはサービスタイプ別にポリシーを適用
- ゾーン分離とゾーンベースのポリシーのサポート。
- LAN、WAN、DMZ、ローカル、VPN、Wi-Fi のデフォルトゾーン
- LAN または DMZ 上のカスタムゾーン
- カスタマイズ可能な NAT ポリシー (IP マスカレード、フルオブジェクトのサポート) により、複数のサービスを単一のルールの元でリダイレクトまたは転送可能であり、便利な NAT ルールウィザードにより、複雑な NAT ルールであっても数回クリックするだけですばやく簡単に作成可能
- フラッド攻撃対策 : DoS、DDoS、ポートスキャンのブロック
- GeoIP に基づき国別にブロック
- ルーティング : スタティック、マルチキャスト (PIM-SM)、およびダイナミック (RIP、BGP、OSPF)
- アップストリームプロキシ対応
- IGMP スヌーピングを使用したプロトコルに依存しないマルチキャストルーティング

- STP 対応のブリッジングと ARP ブロードキャスト転送
- VLAN DHCP 対応とタグ付け
- VLAN ブリッジのサポート
- ジャンボフレームのサポート
- WAN リンクバランシング：複数のインターネット接続、自動リンクヘルスチェック、自動フェールオーバー、自動および重み付けバランシング、およびきめ細かいマルチパスルール
- ワイヤレス WAN のサポート (仮想環境では不可)
- 802.3ad インターフェイスのリンクアグリゲーション
- DNS、DHCP、および NTP の完全な構成
- ダイナミック DNS (DDNS)
- IPv6 Ready Logo Program 承認証明書
- IPv6 トンネリングのサポート。 IPSec を介した 6in4、6to4、4in6、および IPv6 Rapid Deployment (6rd) に対応

SD-WAN

- 複数の WAN リンクオプションをサポートし、VDSL、DSL、ケーブル、3G/4G/LTE/ 携帯に対応し、必要不可欠な監視、負荷分散、フェールオーバーなどの機能に対応
- VoIP などの重要アプリケーションの遅延を最小化し、品質を保証するアプリケーションのパス選択およびルーティング
- Synchronized Security の機能の 1 つである Synchronized SD-WAN は、ソフォスが管理するエンドポイントと Sophos Firewall 間で Synchronized Application Control の情報を共有することで、アプリケーション識別の明瞭性と信頼性をさらに向上
- ファイアウォールルールやポリシーベースのルーティングにより、最適なリンクを介してアプリケーションをルーティング
- 手頃な価格で柔軟性があり、ゼロタッチまたはロータッチでの展開が可能
- IPSec や SSL VPN などの堅牢な VPN に対応
- 一元的な VPN オーケストレーション
- ルーティング機能を備えた独自の RED レイヤー 2 トンネル

基本的なトラフィックシェーピングおよびクオータ

- ネットワークまたはユーザーベースの柔軟なトラフィックシェーピング (QoS) (Web プロテクションサブスクリプションに含まれる拡張 Web およびアプリトラフィックシェーピングオプション)
- アップロード / ダウンロード、総トラフィックを基準とする、周期的 / 非周期的なユーザーベースのトラフィッククオータを設定
- リアルタイムでの VoIP 最適化
- DSCP マーキング

セキュアワイヤレス

- ソフォスのワイヤレスアクセスポイント (AP) をプラグアンドプレイで簡単に導入でき、ファイアウォールのコントロールセンターに自動的に表示できます。
- 内蔵ワイヤレスコントローラーにより、AP や無線クライアントを一元的に監視および管理可能
- クライアントの隔離オプションを使用して、LAN、VLAN、または個別のゾーンに AP をブリッジ
- 隠し SSID を含む複数の SSID を無線ごとにサポート
- WPA2 パーソナルやエンタープライズなど、さまざまなセキュリティおよび暗号化標準に対応
- チャネル幅の選択オプション
- IEEE 802.1X (RADIUS 認証) に対応し、プライマリおよびセカンダリサーバーをサポート
- 802.11R (高速移行) のサポート
- (カスタム) バウチャー、今日のパスワード、利用規約 (T&C) の合意のためのホットスポットのサポート
- ウォールドガーデンオプションによるワイヤレスゲストインターネットアクセス
- 時間帯ベースのワイヤレスネットワークアクセス
- サポートされている AP を使用したワイヤレスリピートおよびブリッジングメッシュネットワークモード
- 自動チャネル選択のバックグラウンド最適化
- HTTPS ログインのサポート

認証

- Synchronized User ID は、Synchronized Security を利用して、Active Directory サーバーやクライアントにエージェントを設置することなく、ソフォスのエンドポイントとファイアウォールの間で、現在ログインしている Active Directory ユーザー ID を共有
- 認証方法：Active Directory、eDirectory、RADIUS、LDAP および TACACS+
- Active Directory SSO、STA、SATC のためのサーバー認証エージェント
- シングルサインオン：Active Directory、eDirectory、RADIUS アカウンティング
- Windows、Mac OS X、Linux 32/64 対応のクライアント認証エージェント
- ブラウザ SSO 認証：透過型、プロキシ認証 (NTLM)、Kerberos
- ブラウザキャプティブポータル
- iOS および Android の証明書認証
- IPSec、SSL、L2TP、PPTP の認証サービス

- Active Directory と Google G Suite を使用する環境での Google Chromebook 認証のサポート
- API ベースの認証

ユーザー向けセルフサービスポータル

- Sophos Authentication Client のダウンロード
- SSL リモートアクセスクライアント (Windows) と構成ファイル (他の OS 向け) のダウンロード
- ホットスポットのアクセス情報
- ユーザー名とパスワードの変更
- 個人のインターネット利用状況の表示
- 隔離されたメッセージへのアクセスと、ユーザーベースの送信者ブロック / 許可リストの管理 (Email Protection が必要)

基本的な VPN オプション

- サイト間 VPN : SSL、IPSec、256 ビット AES/3DES、PFS、RSA、X.509 証明書、事前共有キー
- Sophos RED サイト間 VPN トンネル (堅牢で軽量)
- L2TP および PPTP
- ルートベースの VPN
- リモートアクセス : SSL、IPSec、iPhone/iPad/Cisco・Android VPN クライアントに対応
- IKEv2 のサポート
- Windows 用の SSL クライアントと、ユーザーポータルからの構成のダウンロード

Sophos Connect クライアント

- 認証 : 事前共有鍵 (PSK)、PKI (X.509)、トークン、および XAUTH
- リモート接続ユーザーに対して、Synchronized Security と Security Heartbeat を有効化
- 最適なトラフィックルーティングを実現するインテリジェントなスプリットトンネリング
- NAT トラバーサルをサポート
- 接続状況をグラフィカルに表示するクライアントモニター
- Mac および Windows のサポート

Network Protection

侵入防御 (IPS)

- 高性能な次世代 IPS ディープパケットインスペクションエンジン、ファイアウォールルールを基準として適用可能な選択的な IPS パターンにより、最高クラスのパフォーマンスと保護を実現
- 数千のシグニチャ
- 詳細なカテゴリ選択
- カスタム IPS シグニチャに対応
- IPS ポリシースマートフィルタにより、新しいパターンが追加されると自動的に更新される動的なポリシーを有効化

ATP と Security Heartbeat

- 高度な脅威からの保護 (DNS、AFC、ファイアウォールの多層防御により、コマンド & コントロールサーバーとの通信を試みるネットワークトラフィックを検知してブロック)
- Security Heartbeat は、セキュリティが侵害されたエンドポイントを即座に特定し、ホスト、ユーザー、プロセス、インシデント数、侵害された時間などの情報を提供
- Security Heartbeat のポリシーにより、ネットワークリソースへのアクセスを制限したり、セキュリティが侵害されたシステムが完全に安全になるまで隔離することが可能
- ラテラルムーブメントの保護機能を使用して、ソフォス製品で管理されている正常なエンドポイントが、健全でないエンドポイントからのすべてのトラフィックを拒否するようにして、同じブロードキャストドメインにおける脅威の拡散を防止し、セキュリティが侵害されたシステムを隔離

SD-RED デバイス管理

- すべての SD-RED デバイスの一元管理
- 構成なしで、クラウドベースのプロビジョニングサービスから自動設定
- X.509 デジタル証明書と AES 256 ビット暗号を使用した安全な暗号化トンネル
- 仮想イーサネットにより、ロケーション間のすべてのトラフィックを信頼性の高い方法で転送
- DHCP および DNS サーバー構成を一元的に定義して、IP アドレスを管理
- 一定期間使用されていない SD-RED デバイスの認証をリモートから解除
- トンネルトラフィックの圧縮
- VLAN ポート構成オプション

クライアントレス VPN

- RDP、HTTP、HTTPS、SSH、Telnet、VNC に対応するソフォス独自の暗号化された HTML5 のセルフサービスポータル

Web Protection

Web の保護と制御

- マルウェア対策や Web フィルタリングのための完全透過型プロキシ
- 高度な脅威からの保護の強化
- SophosLabs が提供する 92 のカテゴリにおよぶ数百万のサイトに対応する URL フィルタデータベース

- ユーザー / グループ別のネットサーフィンのクオータ時間ポリシー
- ユーザー / グループ別のアクセス時間ポリシー
- マルウェアスキャン:HTTP/S、FTP、および Web ベースのメールのあらゆる形態のウイルス、Web マルウェア、トロイの木馬、およびスパイウェアをブロック
- JavaScript エミュレーションによる高度な Web マルウェアプロテクション
- 最新の脅威情報をクラウド上でリアルタイムに検索する Live Protection
- 独立した第 2 のマルウェア検出エンジン (Avira) によるデュアルスキャン
- リアルタイムまたはバッチモードスキャン
- ファーミングからの保護
- 詳細にカスタマイズ可能なルールと例外を備えた、あらゆるネットワークとユーザーポリシーに対する HTTP および HTTPS のスキャンと強制
- SSL プロトコルトンネリングの検出と強制
- 証明書の検証
- ハイパフォーマンスな Web コンテンツキャッシング
- エンドポイントアップデートの強制キャッシュ
- MIME タイプ、拡張子、アクティブコンテンツタイプ (Activex、アプレット、Cookie など) によるファイルタイプのフィルタリング。
- ユーザー / グループ別の YouTube for Schools ポリシーの適用
- ポリシー (ユーザー / グループ) 別に主要な検索エンジンでセーフサーチを強制 (DNS ベース)
- Web キーワードによるモニタリングと強制的な措置により、キーワードリストに一致する Web コンテンツを記録、レポート、またはブロック可能。また、カスタムリストをアップロードするオプションも利用可能
- 不要と思われるアプリケーション (PUA) のブロック
- 教師やスタッフがブロックされたサイトやカテゴリに一時的にアクセスできるようにする Web ポリシーオーバーライドオプション。これは、完全にカスタマイズ可能で、特定のユーザーが管理可能
- Google Chromebooks でのユーザー / グループポリシーの強制

クラウドアプリケーションの可視化

- コントロールセンターのウィジェットには、クラウドアプリケーションにアップロードおよびダウンロードされたデータ量が、新規、承認済み、未承認、または許容として分類されて表示される
- シャドー IT の状況を一目で確認可能
- ユーザー、トラフィック、データの詳細を表示するドリルダウン機能
- トラフィックシェーピングポリシーへのワンクリックアクセス
- クラウドアプリケーションの使用状況をカテゴリやボリュームでフィルタリング
- クラウドアプリケーションの使用状況レポートをカスタマイズして、過去の利用状況を詳細にレポート可能

アプリケーションの保護と制御

- ソフォスが管理するエンドポイントとファイアウォールの間で情報を共有し、ネットワークのすべての未知の Windows および Mac アプリケーションを自動的に識別、分類、制御する Synchronized App Control
- 何千ものアプリケーションのパターンを使用したシグネチャベースのアプリケーション制御
- クラウドアプリケーションの可視化と制御によるシャドー IT の検出
- 新しいパターンが追加されると自動的に更新される動的なポリシーを有効にするアプリケーションコントロールスマートフィルタ
- マイクロアプリケーションの検出と制御
- カテゴリ、特性 (帯域幅や生産性への影響など)、テクノロジー (P2P など)、リスクレベルに応じたアプリケーション制御
- ユーザーまたはネットワーク単位でのアプリケーション制御ポリシーの強制

Web およびアプリケーションのトラフィックシェーピング

- Web カテゴリまたはアプリケーションによるトラフィックシェーピング (QoS) オプションを強化して、アップロード / ダウンロードまたはトータルトラフィックの優先度とビットレートを個別または総合的に制限または保証

Zero-Day Protection

動的なサンドボックス分析

- ソフォスのセキュリティ製品のダッシュボードに完全統合
- 実行ファイルおよび実行ファイルを含むドキュメント (.exe、.com、.dll、.doc、.docx、docm、.rtf、PDF など)、および上記のファイルタイプを含むアーカイブ (ZIP、BZIP、GZIP、RAR、TAR、LHA/LZH、7Z、Microsoft Cabinet など) を検査します。
- 積極的な挙動、ネットワーク、およびメモリ分析
- サンドボックス分析を回避する挙動の検出
- ディープラーニングを使用する機械学習テクノロジーにより、ドロップされたすべての実行可能ファイルをスキャン
- Sophos Intercept X のエクスプロイト防御機能とランサムウェア対策機能 (CryptoGuard) を搭載
- スクリーンショットを含む悪意のあるファイルの詳細レポートと、ダッシュボードからのファイル解放機能

- オプションのデータセンター選択機能と、ファイルの種類に基づく処理や、除外、分析結果に基づく処理など、柔軟なユーザーとグループのポリシーオプションを提供
- ワンタイムダウンロードのリンクをサポート

静的な脅威情報解析

- Web 経由でダウンロードされたアクティブコードを含むすべてのファイル、またはメールの添付ファイルとしてファイアウォール内に送信された実行ファイルや実行可能なコンテンツを含むドキュメント (.exe、.com、.dll、.doc、.docx、docm、.rtf、PDF など)、および上記のいずれかのファイルタイプを含むアーカイブ (ZIP、BZIP、GZIP、RAR、TAR、LHA/LZH、7Z、Microsoft Cabinet など) が、脅威情報分析のために自動的に送信される
- ファイルは SophosLabs の膨大な脅威インテリジェンスデータベースと照合され、複数の機械学習モデルを用いて新規および未知のマルウェアを識別
- 分析されたファイルを表示するダッシュボードウィジェット、分析したファイルと分析結果の詳細なリスト、各機械学習モデルの結果をまとめた広範で詳細なレポートを利用可能

Central Orchestration

(近日発売予定)

SD-WAN オーケストレーション

- SD-WAN と VPN のオーケストレーションは、最適なアーキテクチャ (ハブアンドスポーク、フルメッシュ、またはそれらの組み合わせ) を使用して、ネットワーク間のサイト間 VPN トンネルをウィザードベースで簡単かつ自動的に作成可能 IPSec、SSL、RED VPN トンネルに対応 SD-WAN 機能とシームレスに統合され、アプリケーションの優先順位付け、ルーティングの最適化、複数の WAN リンクを活用した耐障害性とパフォーマンスを向上

Central Firewall Reporting Advanced

- 30 日分のクラウドデータを保存でき、カスタムレポートの保存、スケジュール設定、エクスポートなどの高度な機能を備えた、ファイアウォールの履歴レポートを作成可能

XDR と MTR コネクタ

- Sophos XDR (Extended Threat Detection and Response) と統合し、製品横断的な脅威ハンティングと分析を実施
- 24 時間 365 日対応のソフォスの MTR (Managed Threat Response) サービスに対応

Email Protection

メールの保護と制御

- SMTP、POP3、IMAP に対応するメールスキャン
- 特許取得済みの再発パターン検知 (Recurrent-Pattern-Detection) テクノロジーに基づくスパム発生モニタリング機能を搭載するレピュテーションサービス
- SMTP トランザクションにおけるスパムやマルウェアのブロック
- DKIM および BATV によるスパム対策
- スパムグレーリストと SPF (Sender Policy Framework) による保護
- メールアドレスの誤入力に対する受信者認証
- 独立した第 2 のマルウェア検出エンジン (Avira) によるデュアルスキャン
- 最新の脅威情報をクラウド上でリアルタイムに検索する Live Protection
- シグネチャとパターンの自動更新
- アウトバウンドリレーのスマートホストサポート
- 添付ファイルのファイルタイプ検出 / ブロック / スキャン
- サイズ超過メッセージの受け入れ、拒否、削除
- メール内のフィッシング URL の検出
- 定義済みのコンテンツスキャンルールを使用することも、詳細なポリシーオプションと例外を使用し、さまざまな条件に基づいて独自のカスタムルールを作成することも可能
- SMTP、POP、IMAP の TLS 暗号化をサポート
- すべての送信メッセージに自動的に署名を追加
- メールアーカイバー
- 各ユーザーが、ブロックおよび許可する送信者リストをユーザーポータルで保守可能

メール隔離管理

- 隔離したスパムの処理および通知オプション
- 日付、送信者、受信者、件名、および理由で検索およびフィルタリングしてマルウェアおよびスパムを隔離可能。また、隔離したメッセージをリリースおよび削除するオプションも利用可能
- 隔離されたメッセージを表示およびリリースするセルフサービスユーザーポータル

メール暗号化、DLP

- 特許出願中の SPX 暗号による一方向性メッセージの暗号化
- 受信者による自己登録 SPX パスワード管理
- SPX のセキュアな返信に添付ファイルを追加
- 完全に透過的で、追加のソフトウェアやクライアントが不要
- メールと添付ファイルに機密データが含まれていないかどうか自動スキャンする DLP エンジン

- SophosLabs が管理する PII、PCI、HIPAA などの機密データタイプのコンテンツコントロールリスト (CCL) をあらかじめパッケージ化

Web Server Protection

Web アプリケーションファイアウォール (WAF) プロテクション

- リバースプロキシ
- URL ハードニングエンジン。ディープリンクとディレクトリトラバーサルを防止
- フォームハードニングエンジン
- SQL インジェクション対策
- クロスサイト スクリプティング対策
- デュアル型のマルウェア対策エンジン (Sophos および Avira)
- HTTPS (TLS/SSL) 暗号化のオフロード
- 署名付きクッキー (デジタル署名に対応)
- パスベースのルーティング
- Outlook Anywhere プロトコルのサポート
- サーバーアクセス時のフォームベース認証とベーシック認証のリバース認証 (オフロード)
- 仮想サーバーと物理サーバーの抽象化
- 統合型ロードバランサーによる訪問者の複数サーバーへの分散化
- 必要に応じて、個別のチェックを詳細な指定の元でスキップ
- ソースネットワークのリクエストまたは指定されたターゲット URL の照合
- 論理演算子 (AND/OR) のサポート
- さまざまな構成および非標準環境との互換性の問題をサポート
- Web アプリケーションファイアウォールのパフォーマンスパラメータを変更するオプション
- スキャンサイズ制限オプション
- 許可 / ブロックする IP 範囲の設定
- サーバーパスとドメインでのワイルドカードのサポート
- 認証用の接頭辞 / 接尾辞の自動追加

レポート

Central Firewall Reporting

- 柔軟なカスタマイズオプションを利用可能な事前定義レポート
- Sophos Firewall のレポート – ハードウェア、ソフトウェア、仮想、およびクラウド
- 直感的なユーザーインターフェースにより、データをグラフィカルに表現
- レポートダッシュボードでは、過去 24 時間のイベントを一目で把握
- ネットワークアクティビティ、トレンド、潜在的な攻撃を簡単に特定
- ログを簡単にバックアップでき、監査で必要となる場合には迅速に取得可能
- 技術的な専門知識を必要としない簡素化された導入

Central Firewall Reporting Advanced

- 複数のファイアウォールの情報を集約したレポート
- カスタムレポートテンプレートの保存
- 定期的なレポート作成
- レポートを PDF、CFV、HTML 形式で出力
- 各ファイアウォールで最大 1 年分のデータを保管
- MTR / XDR コネクタ

オンボックスのレポート機能

注 : Sophos Firewall のレポート機能は追加料金なしで利用できますが、各プロテクションモジュールのライセンスによっては個々のログ、レポート、ウィジェットの利用について料金が発生する場合があります。

- 数百種類のオンボックスレポートに加え、次のようなカスタムレポートオプションも利用可能。ダッシュボード (トラフィック、セキュリティ、ユーザー脅威指数)、アプリケーション (アプリケーションリスク、ブロックされたアプリ、Synchronized Apps、検索エンジン、Web サーバー、Web キーワード一致、FTP)、ネットワークと脅威 (IPS、ATP、ワイヤレス、Security Heartbeat、Sandstorm)、VPN、メール、コンプライアンス (HIPAA、GLBA、SOX、FISMA、PCI、NERC CIP v3、CIPA)。
- 現在のアクティビティモニタリング : システムヘルス、ライブユーザー、IPSec 接続、リモートユーザー、ライブ接続、ワイヤレスクライアント、隔離、DoS 攻撃
- レポートの匿名化
- レポートグループを設定して複数の受信者向けに、さまざまな頻度を設定してレポートを作成可能
- レポートを HTML、PDF、Excel (XLS) で出力。
- レポートブックマーク
- カテゴリ別にログ保管期間をカスタマイズ
- カラムビューと詳細ビューを備え、豊富な機能を搭載したログビューアを利用可能。このビューアでは、強力なフィルタと検索オプション、ハイパーリンク付きのルール ID 、データビューのカスタマイズが可能

サブスクリプション別の Sophos Firewall の機能概要

	Xstream Protection Bundle					別売		
	Standard Protection Bundle			別売				
	Base Firewall	Network Protection	Web Protection	Zero-Day Protection	Central Orchestration*	Central Firewall Reporting Adv.	Email Protection	Web Server Protection
一般的な管理 (HA を含む)	●							
Xstream アーキテクチャ	●							
ファイアウォール、ネットワーク、およびルーティング	●							
基本的なトラフィックシェーピングおよびクオータ	●							
セキュアワイヤレス	●							
認証	●							
セルフサービスユーザーポータル	●							
基本的な VPN オプション	●							
RED サイト間 VPN	●							
Sophos Connect VPN クライアント	●							
侵入防御 (IPS)		●						
ATP および Security Heartbeat ™		●						
SD-RED デバイス管理		●						
クライアントレス VPN		●						
Synchronized Application Control			●					
Web の保護と制御			●					
アプリケーションの保護と制御			●					
クラウドアプリケーションの可視化			●					
Web およびアプリケーションのトラフィックシェーピング			●					
動的なサンドボックス分析				●				
脅威情報の解析				●				
SD-WAN オーケストレーション					●			
Central Firewall Reporting (CFR)	7 日間				30 日間	最大 1 年間		
CFR アドバンスド機能					●	●		
XDR と MTR コネクタ					●	●		
メールの保護と制御							●	
メール隔離管理							●	
メール暗号化、DLP							●	
Web アプリケーションファイアウォール (WAF) プロテクション								●
ログとレポート	●	●	●	●	●	●	●	●
Sophos Central の管理	●	●	●	●	●	●	●	●

* 近日発売予定

注：

- 一部の機能は (オンボックスレポート、デュアル AV スキャン、 WAF AV スキャン、メールメッセージ転送エージェント (MTA) 機能)、XGS 87 および XG 86 モデルではサポートされません。
- MSP のライセンスオプションは、上記とは若干異なります
- XG シリーズハードウェア / 仮想ライセンスについては、sophos.com/compare-xg にある資料をご覧ください。

ソフォス株式会社営業部
sales@sophos.co.jp

21-04-09 FL-EN (PC)