

SOPHOS
Cybersecurity delivered.

Sophos Firewall

ソリューションの概説



目次

Sophos Firewall	2
隠れたリスクの顕在化	3
Control Center	3
Xstream TLS インスペクション	6
Synchronized Application Control	7
リスクの高いユーザー	8
柔軟なレポート機能	9
未知の脅威をブロック	10
Xstream 対策とパフォーマンス	10
ゼロデイ攻撃対策	11
静的機械学習分析	12
動的なランタイムサンドボックス分析	13
脅威対策レポート	14
統合ルール管理	15
セキュリティ体制の管理が即座に可能	16
エンタープライズクラスのセキュア Web ゲートウェイ	17
教育関連の機能	18
シンプルな NAT 設定	19
インシデントへの自動対応	20
Security Heartbeat	20
これからはゼロトラストの世界	22
SD-WAN ネットワークの最適化	23
Xstream SD-WAN	23
SD-WAN VPN トラフィックの Xstream FastPath アクセラレーション	26
SD-Branch オフィスとの接続	27
VPN のサポートとオーケストレーション	29
アプリケーションの可視性とルーティング	30
Sophos Firewall をあらゆるネットワークに簡単に追加	32

Sophos Firewall

Sophos Firewall は、既存のファイアウォールにある主要な問題に取り組むことをはじめから想定して設計されています。また、最新の暗号化されたインターネットや進化する脅威の動向に対処するための真の次世代型プラットフォームも提供しています。Sophos Firewall は、最適なパフォーマンスを保ちつつ、隠れたリスクを特定、脅威から保護、インシデントに対応する新しいアプローチを提供します。Sophos Firewall の Xstream アーキテクチャは、極めて高いレベルの可視性、保護、およびパフォーマンスを提供する独自のパケット処理を採用しています。

Sophos Firewall では、リスクが高いユーザー、不要と思われるアプリケーション、高度な脅威、不審なペイロードに比類のない可視性を提供します。セットアップと保守が容易で、多様な最新の脅威対策テクノロジーがしっかりと統合されています。また、レガシーファイアウォールとは異なり、Sophos Firewall は、ネットワーク上の他のセキュリティシステムと通信するため、脅威を封じ込め、マルウェアがネットワークから自動的にデータを拡散または侵入するのをブロックするための信頼できるエンフォースメントポイントになります。

Sophos Firewall には、他のネットワークファイアウォールに比べて次の 4 つの大きな利点があります。

1. **隠れたリスクを顕在化** – Sophos Firewall は他社製品に比べ、隠れたリスクを顕在化するのに優れています。たとえば、視覚的にわかりやすいダッシュボードや、充実したレポート機能、独自のリスク分析機能などが搭載されています。
2. **未知の脅威をブロック** – Sophos Firewall は他社製品に比べ、未知の脅威を迅速、簡単かつ効果的にブロックできます。高度な保護機能を完備しており、それらの機能のセットアップや管理は非常に簡単です。
3. **インシデントへ自動対応** – Synchronized Security を備えた Sophos Firewall は、ユーザーのエンドポイントとファイアウォールとの間でリアルタイムにインテリジェンスを共有する Sophos Security Heartbeat™ のおかげでネットワークのインシデントに自動的に対応します。
4. **SD-WAN ネットワークを最適化** – Sophos Firewall の Xstream SD-WAN 機能により、複雑な SD-WAN オーバーレイネットワークをポイントアンドクリックで簡単に設定することができます。また、リンク間をゼロインパクトの即時移行により、自動パフォーマンスベース WAN リンク選択を利用して、アプリケーションパフォーマンス、ネットワークの冗長性、およびビジネス継続性を最適化することもできます。

隠れたリスクの顕在化

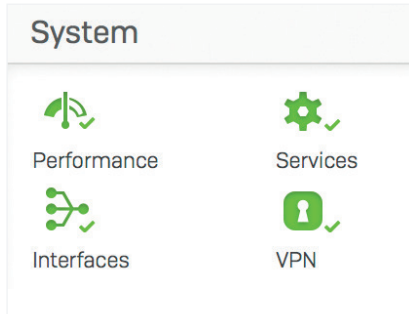
今日のファイアウォールにとって極めて重要なのは、収集した膨大な量の情報を解析し、可能な限りデータを相関させ、アクションを必要とする最も重要な情報のみを（できれば手遅れになる前に）浮き彫りにすることです。

Control Center

Sophos Firewall の Control Center は、ネットワーク上のアクティビティ、リスク、脅威をかつてないレベルで可視化します。

最も重要な情報にユーザーの注意が向けられるように、信号機式のインジケータが使用されています。

赤色は、直ちに対処する必要があることを意味します。黄色は、問題が生じる可能性があることを示しています。すべて緑色の場合は、それ以上のアクションは不要です。



The screenshot shows the Sophos Control Center dashboard for a Sophos Firewall. The dashboard is divided into several sections: System, Traffic insight, User & device insights, Active firewall rules, Reports, and Messages. Blue arrows point to various elements with Japanese annotations:

- Security Heartbeat: 脅威、リスクに晒されているシステム
- Synchronized Application Control: 不明なアプリ
- Threat intelligence: 不審なプログラム
- ATP: 危険なユーザー
- SSL/TLS connections: 高度な脅威
- Messages: 危険なアプリ
- Messages: 不適切な Web サイト
- Messages: 不正侵入攻撃

また、Control Center のすべてのウィジェットは、クリックするだけで追加情報が簡単に表示されます。たとえば、デバイス上のインターフェースのステータスは、Control Center の「インターフェース」ウィジェットをクリックすることで取得できます。

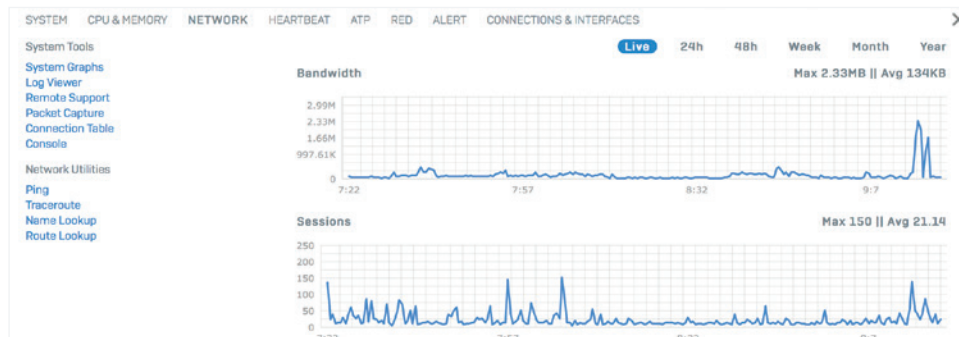
INTERFACE	TYPE	STATUS	RECEIVED KBITS/S	TRANSMITTED KBITS/S
IoT_Bridge	Bridge-pair	Connected	1.98	0.62
Port1	Physical	Connected, 1000 Mbps - Full Duplex	183.91	864.02
Port2	Physical	Connected, 1000 Mbps - Full Duplex	925.65	178.26
Port7	Physical	Unplugged	0.00	0.00
Port8	Physical	Disabled	0.00	0.00

GATEWAY NAME	GATEWAY IP	INTERFACE	TYPE	WEIGHT	STATUS
BACKUP_WAN	128.0.0.1	Port7	Active	1	●
DHCP_Port2_GW	50.68.180.1	Port2	Active	1	●

高度な脅威のホスト、ユーザー、ソースは、ダッシュボードで「ATP」(Advanced Threat Protection) ウィジェットをクリックするだけで簡単に特定できます。

HOSTNAME, IP	THREAT	COUNT
● Mac Server 10.0.1.10	C2/Generic-A /Users/Chris/Desktop/MacBadActor.app/Contents/MacOS/MacBadActor	2

システムグラフには、過去 2 時間、1ヶ月間、または 1年間など、選択した時間枠でのパフォーマンスも表示されます。また、一般的に使用されるトラブルシューティングツールに素早くアクセスして、潜在的な問題を解決します。



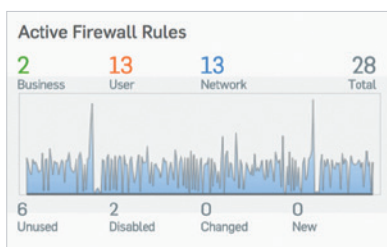
ライブログビューアは、1回クリックするだけでどの画面からもアクセスできます。新しいウィンドウで開かれるので、コンソールで作業しながら、関連するログも監視できます。こうすることで、ファイアウォールモジュールによる単純なカラムベースの表示と、システム全体からのログを単一のリアルタイムビューに集約する強力なフィルタオプションとソートオプションを備えた、より詳細で統合された表示という 2 つのビューが提供されます。

Time	Log Comp	Action	Username	Firewall Rule	In Interface	Out Interface	Source IP	Destination IP	Rule Type	Message ID	Live PCAP	Message
2017-11-29 09:48:16	Invalid Traffic	Denied		0	Port2		23.45.114.117	50.68.180.222	0	01001	Open PCAP	Could not associate packet to any connection
2017-11-29 09:48:14	Firewall Rule	Allowed	mindy	4	Port1	Port2	10.0.1.52	64.58.144.92	2	00001	Open PCAP	
2017-11-29 09:48:13	Firewall Rule	Allowed	chris	4	Port1		10.0.1.15	34.200.43.40	2	00001	Open PCAP	
2017-11-29 09:48:13	Firewall Rule	Allowed		10	Port3	Port2	192.168.1.10	54.87.89.218	1	00001	Open PCAP	
2017-11-29 09:48:12	Firewall Rule	Allowed		10	Port6	Port2	192.168.1.11	12.148.218.73	1	00001	Open PCAP	
2017-11-29 09:48:06	Firewall Rule	Allowed	chris	4	Port1		10.0.1.15	54.186.179.15	2	00001	Open PCAP	
2017-11-29 09:48:03	Firewall Rule	Allowed	chris	4	Port1		10.0.1.15	23.45.114.117	2	00001	Open PCAP	
2017-11-29 09:48:03	Firewall Rule	Allowed	chris	4	Port1		10.0.1.15	23.45.114.117	2	00001	Open PCAP	
2017-11-29 09:48:02	Firewall Rule	Allowed		10	Port3	Port2	192.168.1.10	54.87.89.218	1	00001	Open PCAP	
2017-11-29 09:48:02	Firewall Rule	Allowed	chris	4	Port1	Port2	10.0.1.15	64.58.144.92	2	00001	Open PCAP	

多くのネットワーク管理者は「ファイアウォールのルールが多過ぎるのではないか」、「どれが本当に必要なルールなのか」、「どれが実際には使用されていないルールなのか」などと頭を悩ませています。Sophos Firewall を使用すれば、もう悩む必要はありません。

2017-11-29 09:44:30	Invalid Traffic	Denied		messageId="01001" log_type="Firewall" log_component="Invalid Traffic" log_sub_type="Denied" status="Deny" con_duration="0" fw_rule_id="0" policy_type="0" user="user_group="" web_policy_id="0" ips_policy_id="0" appfilter_policy_id="0" app_name="app_risk" app_technology="app_category" in_interface="Port1" out_interface="" src_mac="f40f24200c0f8" src_ip="100.115" src_country="" dst_ip="38.127.227.137" dst_country="" protocol="TCP" src_port="82791" dst_port="443" packets_sent="0" packets_received="0" bytes_sent="0" bytes_received="0" src_trans_ip="" src_trans_port="0" dst_trans_ip="" dst_trans_port="0" src_zone="" src_zone_type="" dst_zone="" dst_zone_type="" con_direction="" con_id="" virt_con_id="" hb_status="No Heartbeat" message="Could not associate packet to any connection" appressedby="Signature"
2017-11-29 09:44:27	Invalid Traffic	Denied		messageId="01001" log_type="Firewall" log_component="Invalid Traffic" log_sub_type="Denied" status="Deny" con_duration="0" fw_rule_id="0" policy_type="0" user="user_group="" web_policy_id="0" ips_policy_id="0" appfilter_policy_id="0" app_name="app_risk" app_technology="app_category" in_interface="Port1" out_interface="" src_mac="f40f24200c0f8" src_ip="100.115" src_country="" dst_ip="38.127.227.137" dst_country="" protocol="TCP" src_port="82791" dst_port="443" packets_sent="0" packets_received="0" bytes_sent="0" bytes_received="0" src_trans_ip="" src_trans_port="0" dst_trans_ip="" dst_trans_port="0" src_zone="" src_zone_type="" dst_zone="" dst_zone_type="" con_direction="" con_id="" virt_con_id="" hb_status="No Heartbeat" message="Could not associate packet to any connection" appressedby="Signature"
2017-11-29 09:44:25	Invalid Traffic	Denied		messageId="01001" log_type="Firewall" log_component="Invalid Traffic" log_sub_type="Denied" status="Deny" con_duration="0" fw_rule_id="0" policy_type="0" user="user_group="" web_policy_id="0" ips_policy_id="0" appfilter_policy_id="0" app_name="app_risk" app_technology="app_category" in_interface="Port1" out_interface="" src_mac="f40f24200c0f8" src_ip="100.115" src_country="" dst_ip="38.127.227.137" dst_country="" protocol="TCP" src_port="82791" dst_port="443" packets_sent="0" packets_received="0" bytes_sent="0" bytes_received="0" src_trans_ip="" src_trans_port="0" dst_trans_ip="" dst_trans_port="0" src_zone="" src_zone_type="" dst_zone="" dst_zone_type="" con_direction="" con_id="" virt_con_id="" hb_status="No Heartbeat" message="Could not associate packet to any connection" appressedby="Signature"
2017-11-29 09:44:22	Invalid Traffic	Denied		messageId="01001" log_type="Firewall" log_component="Invalid Traffic" log_sub_type="Denied" status="Deny" con_duration="0" fw_rule_id="0" policy_type="0" user="user_group="" web_policy_id="0" ips_policy_id="0" appfilter_policy_id="0" app_name="app_risk" app_technology="app_category" in_interface="Port1" out_interface="" src_mac="f40f24200c0f8" src_ip="100.115" src_country="" dst_ip="38.127.227.137" dst_country="" protocol="TCP" src_port="82791" dst_port="443" packets_sent="0" packets_received="0" bytes_sent="0" bytes_received="0" src_trans_ip="" src_trans_port="0" dst_trans_ip="" dst_trans_port="0" src_zone="" src_zone_type="" dst_zone="" dst_zone_type="" con_direction="" con_id="" virt_con_id="" hb_status="No Heartbeat" message="Could not associate packet to any connection" appressedby="Signature"
2017-11-29 09:44:19	Invalid Traffic	Denied		messageId="01001" log_type="Firewall" log_component="Invalid Traffic" log_sub_type="Denied" status="Deny" con_duration="0" fw_rule_id="0" policy_type="0" user="user_group="" web_policy_id="0" ips_policy_id="0" appfilter_policy_id="0" app_name="app_risk" app_technology="app_category" in_interface="Port1" out_interface="" src_mac="f40f24200c0f8" src_ip="100.115" src_country="" dst_ip="38.127.227.137" dst_country="" protocol="TCP" src_port="82791" dst_port="443" packets_sent="0" packets_received="0" bytes_sent="0" bytes_received="0" src_trans_ip="" src_trans_port="0" dst_trans_ip="" dst_trans_port="0" src_zone="" src_zone_type="" dst_zone="" dst_zone_type="" con_direction="" con_id="" virt_con_id="" hb_status="No Heartbeat" message="Could not associate packet to any connection" appressedby="Signature"

「アクティブなファイアウォール ルール」ウィジェットには、ファイアウォールによって処理されているトラフィックのリアルタイムグラフがルールタイプ別に表示されます(タイプはビジネスアプリケーションルール、ユーザールール、ネットワークルール)。また、保守を行うことが可能な未使用のルールを含めて、アクティブなルールの数もステータス別に表示されます。Control Center の他の領域と同様に、これらのどれかをクリックするとドリルダウンします。この場合は、ルールのタイプまたはステータスでソートされたファイアウォールルールテーブルにドリルダウンします。

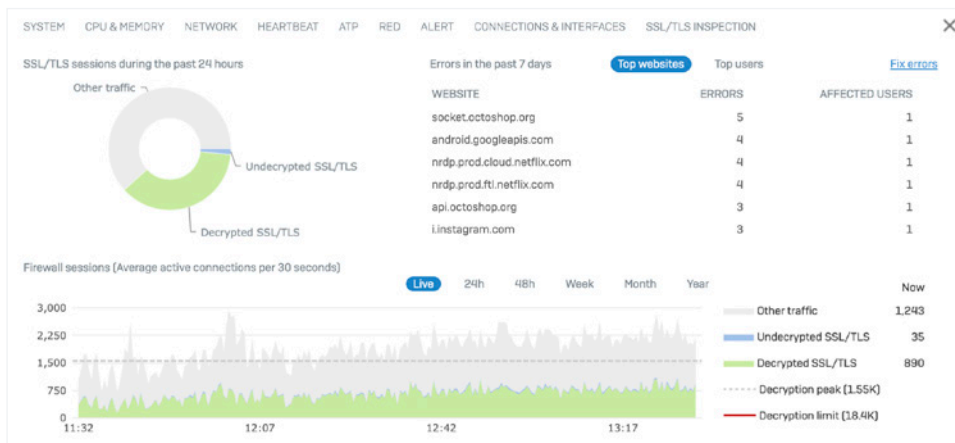


Xstream TLS インスペクション

暗号化されたトラフィックは、問題が発生しやすい環境です。Google によると、ネットワーク上の暗号化トラフィックの量は 90% を超えています。この増加は、隠れているため検出が困難な攻撃をサイバー犯罪者に実行させるチャンスを与えます。結局、探ることができないものは、止めることができないのです。残念ながら、現在のファイアーウォールでは、大幅な速度の低下を避けて、TLS/SSL インスペクションを利用するには、必要なパフォーマンスが不足しているという理由から、ほとんどの組織では何もできない状態に置かれています。

新しい Xstream SSL インスペクションエンジンを搭載している Sophos Firewall では、同時接続に必要な容量が大幅に増加しています。また、必要に応じてスキャンの対象について賢い選択ができるよう柔軟なポリシーツールも提供しています。SSL ポリシーツールを使用すると、組織は、非復号化トラフィック、証明書、プロトコル、暗号の適用オプションなどに関連した大企業向けの TLS/SSL ポリシーを作成できます。Sophos Firewall は、TLS 1.3 およびシステムにあるすべてのポートとアプリケーションにまたがるすべての最新暗号スイートをサポートしています。

ダッシュボードにある追加ツールを使用して、管理者は、暗号化されているネットワークトラフィックの量や実行されている処理方法を正確に確認できます。Sophos Firewall は、他の製品と比べて、この情報を表面化することにより優れています。特に、最新の暗号化基準をサポートしない証明書検証やウェブサイトによって遭遇するエラーを検出する方法において長けています。



Sophos Firewall は、暗号化されたトラフィックフローとコントロールセンターの TLS インスペクションから発生する問題に関する洞察を提供します

管理者は、詳細ウィンドウを表示して、問題が発生しているサイトとその原因、およびユーザー側で発生している問題について正確に確認することもできます。そこから、アプリケーションまたはサイトを復号化から除外して、それ以上の問題を回避するためのアクションを直接実行できます。他の SSL インスペクションのソリューションでは、この情報に同じアクセシビリティを提供しません。

Synchronized Application Control

今日の次世代型ファイアウォールでのアプリケーションコントロールの問題は、ほとんどのアプリケーショントラフィックが識別されずに、未知、もしくは一般的な HTTP/HTTPS として分類もしくは仕分けのいずれかがされているということです。

その理由は簡単です。すべてのファイアウォールのアプリケーション制御エンジンがシグネチャとパターンに基づいてアプリケーションを識別しているからです。また、当然ながら、医療用アプリや金融用アプリのようなカスタマイズされた特定の業界用のアプリにはシグネチャはありません。また、メッセージングアプリだけでなく BitTorrent クライアント、VoIP などの他の回避型アプリなどは、挙動やシグネチャを絶えず変化させて、検出およびコントロールを回避します。多くのアプリケーションが検出を逃れる目的で暗号化を使用している一方で、大半のファイアウォールではポート 80 と 443 は通常ブロックされないという理由から、ファイアウォール経由で通信するための接続に一般的な Web ブラウザを使用するアプリケーションも存在します。

その結果、ネットワーク上のアプリケーションをほとんど把握できないという状況が生まれます。見えないものは、制御することもできません。この問題を解決するには、非常に洗練されていながら効果的な方法があります。それは、ソフォスのマネージドエンドポイントとの独自の Synchronized Security 接続を使用する Sophos Synchronized Application Control です。

Synchronized Application Control の仕組みをご説明しましょう。Sophos Firewall は、シグネチャでは識別できないアプリケーショントラフィックを検出すると、そのトラフィックを生成しているアプリケーションをエンドポイントに問い合わせます。

Synchronized Application Control™



The screenshot shows the Sophos Firewall web interface for the 'Applications' section. The 'Synchronized Application Control' tab is active, displaying a table of discovered applications. The table includes columns for Application, Category, Endpoints, Occurrences, Last occurrence, and Manage. The following table represents the data shown in the screenshot:

Application	Category	Endpoints	Occurrences	Last occurrence	Manage
Apple Maps Applications/./MacOS/Maps	General Internet	Found on 2 Endpoints	24	2020-06-22 10:23	[Ack] [Info]
BitTorrent ~/UserProfiles/./bittorrent.exe ~/UserProfiles/./bittorrent.exe	P2P	Found on 2 Endpoints	3983	2021-06-04 15:16	[Ack] [Info]
macOS Big Sur Installer Applications/./Installers/Setup	Infrastructure	Found on 1 Endpoints	7	2021-12-10 11:37	[Ack] [Info]
Messages Applications/./MacOS/Messages	Instant Messenger	Found on 2 Endpoints	143	2022-01-12 15:24	[Ack] [Info]
Remote Desktop Connection [V7 and Higher] ~/Microsoft/Remote Desktop ~/MacOS/Microsoft Remote Desktop	Remote Access	Found on 2 Endpoints	724	2021-11-15 17:13	[Ack] [Info]

Synchronized Application Control によって検出された未知のアプリケーションは、自動または主導で分類できます。

問い合わせを受けたエンドポイントは、実行可能ファイル、パス、および場合によってはそのカテゴリを共有し、その情報をファイアウォールに返します。すると、ファイアウォールはこの情報に基づいて、大抵の場合アプリケーションを自動的に分類し、コントロールします。

Sophos Firewall がアプリケーションのカテゴリを自動判別できない場合には、管理者が適切なカテゴリを設定したり、アプリケーションを既存のポリシーに割り当てたりできます。

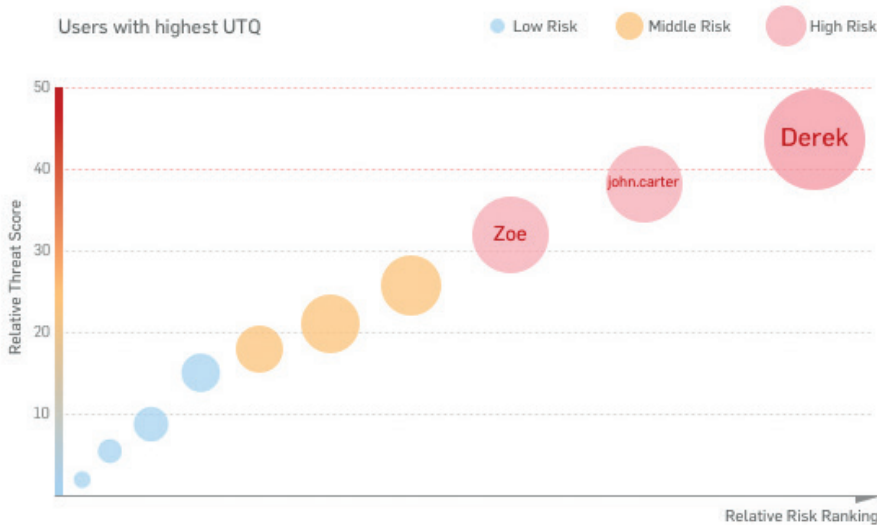
アプリケーションが自動的にまたはネットワーク管理者によって分類されると、そのカテゴリの他のすべてのアプリケーションと同じポリシーコントロールが適用されます。これにより、不要な未特定のアプリをすべてブロックし、必要なアプリに優先順位を付けることが非常に簡単になります。

Synchronized Application Control は、アプリケーションの可視化と制御に画期的な機能をもたらし、これまで特定や制御もされずにいたものを含みネットワーク上で動作していたすべてのアプリケーションを完全に明確化します。

リスクの高いユーザー

調査によると、ユーザーはセキュリティチェーンで最も脆弱なリンクであることが実証されています。幸いなく、人間の行動パターンを分析、使用することで、攻撃を予想したり防止することができます。また、使用パターンを分析すれば、企業リソースがどの程度効率的に利用されているかや、ユーザーポリシーの微調整が必要かどうかを把握するのに役立ちます。

Sophos User Threat Quotient (UTQ: ユーザー脅威指数) を使用すれば、セキュリティ管理者は不審な Web の挙動や脅威と感染の履歴に基づいてリスクを引き起こすユーザーを特定することができます。ユーザーの UTQ リスクスコアが高い場合、セキュリティ意識の欠如から誤った行為をしてしまった、マルウェアに感染した、あるいは意図的に不正行為が行われたことを表している可能性があります。

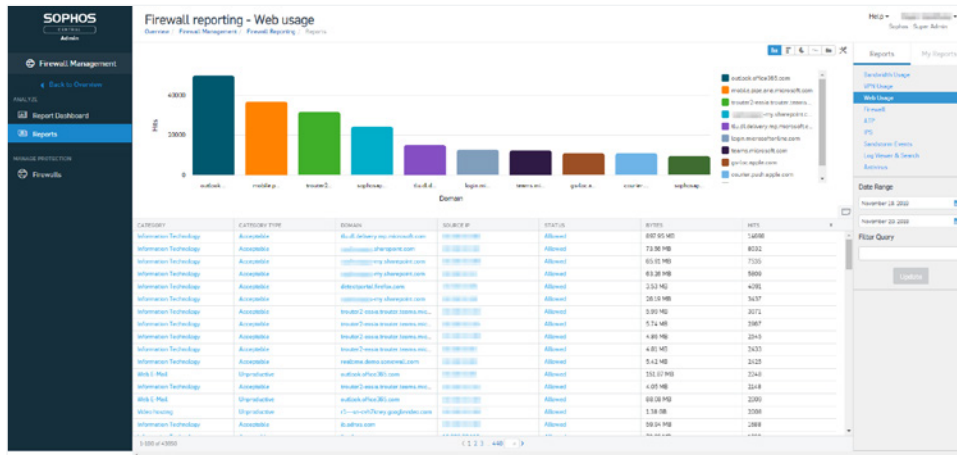


Sophos Firewall は、リスクの高いユーザーを一目で確認できます。

リスクを引き起こしたユーザーとアクティビティを把握することで、ネットワークセキュリティ管理者は必要な措置を講じることができ、トップリスクユーザーを教育したり、より厳密で適切なポリシーを強制適用したりしてユーザーの行動を制御できます。

柔軟なレポート機能

Sophos Firewall は、NGFW および UTM 製品の中でも優れ、柔軟なクラウドベースおよびオンボックスのレポート機能を提供し、追加料金なしで高度なカスタマイズを実行することができます。Sophos Central Firewall Reporting (CFR) により、企業は、解析を通してネットワークのアクティビティに関するさらに深い洞察を得ることができます。CFR では、包括的な組み込みレポートと数百種類のバリデーションを作成するツールを使用して、ユーザーの挙動、アプリケーションの使用状況、セキュリティイベントなどに関する実用的な情報が提供します。インタラクティブなレポートと一目で分かるレポートダッシュボードにより、管理者は、Sophos Central アカウントに保存されている syslog データを掘り下げることができ、視覚的なフォーマットで示される詳細な表示で、簡単に理解できます。その後、データは、セキュリティポスチャのギャップを特定し、ポリシー変更の必要性を強調する傾向を分析します。



Sophos Firewall は、広範なオンボックス、およびセントラル クラウドベース レポート オプションを提供します。

Sophos Firewall は、オンボックスのレポート機能も提供します。組み込まれているダッシュボードを使用して、タイプ別に便利に整理された包括的なレポートセットから選択します。トラフィックアクティビティ、セキュリティ、ユーザー、アプリケーション、Web、ネットワーク、脅威、VPN、メール、コンプライアンスなど、ファイアウォールのすべての領域でカスタマイズ可能なパラメータを含んだ数百種類のレポートがあります。定期レポートのスケジュールは設定が簡単ですので、ユーザー自身または指定の受信者にメールで送信したり、レポートをHTML、PDF、またはCSV形式で保存したりできます。

未知の脅威をブロック

最新のネットワーク脅威から保護するためには、すべての技術がオーケストラのように協調し、指揮者であるネットワーク管理者によって調整される必要があります。残念ながら、大部分のファイアウォール製品は、ある領域にファイアウォールルール設定し、またある別の領域で Web ポリシーを設定したり、他の場所では TLS/SSL インспекションを実施したり、さらには製品の全く異なる部分でアプリケーションコントロールを実行するようなものです。

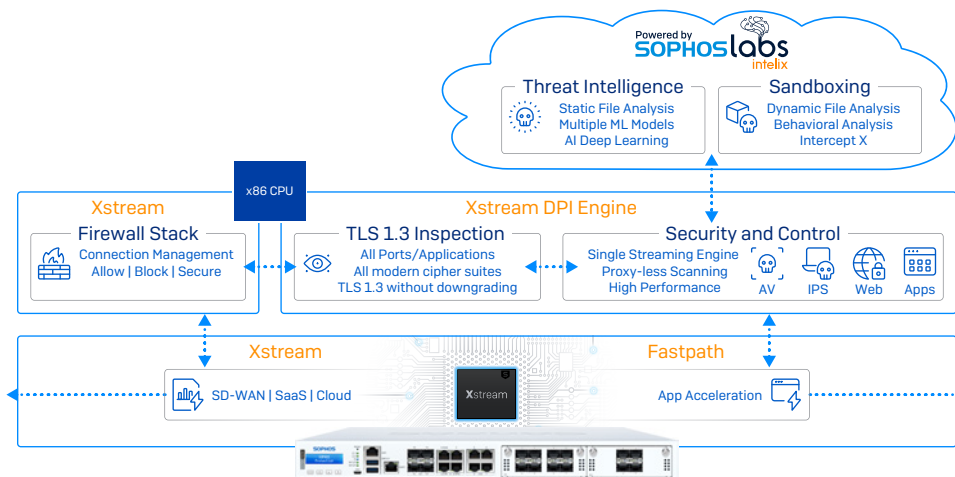
お客様に必要なのは単なる最先端の保護技術ではなく、毎日の設定、導入と管理が容易な技術でなければならないとソフォスは考えます。なぜなら、保護機能の設定が間違っていると、保護機能を導入していないときよりも深刻な状況に陥る可能性があるからです。

シンプルさの実現は、ソフォスにとって常に重要な目標の 1 つです。さらには、ソフォスのように保護の強化とユーザーエクスペリエンスの向上を同時に提供するために、変化を受け入れ、新たな試みに向けて必要な一歩を踏み出す企業はそう多くはありません。

Sophos Firewall 独自の仕組みこそ、他の製品と大きく差別化される理由です。

Xstream 対策とパフォーマンス

ネットワークを脅威から安全に保護するために必要なセキュリティをオンにしても、ファイアウォールのパフォーマンスが低下することはありません。Sophos Firewall の Xstream パケット処理アーキテクチャの主要コンポーネントの一つは、高速のディープパケットインспекション (DPI) エンジンです。DPI エンジンは、IPS、Web、AV、およびアプリケーションコントロールに対してプロキシレスのシングルパスセキュリティスキャンと、Xstream SSL インспекションを提供します。



Sophos Firewall の Xstream アーキテクチャは、プログラム可能な Xstream Flow プロセッサを備え、強力な保護とパフォーマンスを提供します。

新しい接続が確立されると、ファイアウォールスタックによって処理され、トラフィックの脅威を許可、ブロック、またはスキャンするかどうかを判断します。トラフィックにセキュリティスキャンが必要な場合、パケットはプロキシレスの高性能ストリーミング DPI エンジンに転送され、パケットが暗号化されていたとしてもパケットをスキャンします。これは、最初の数パケットだけに使用されます。その後、ファイアウォールスタックは処理から手を引き、DPI エンジンに完全にオフロードします。これにより、待ち時間とパフォーマンスが大幅に向上します。

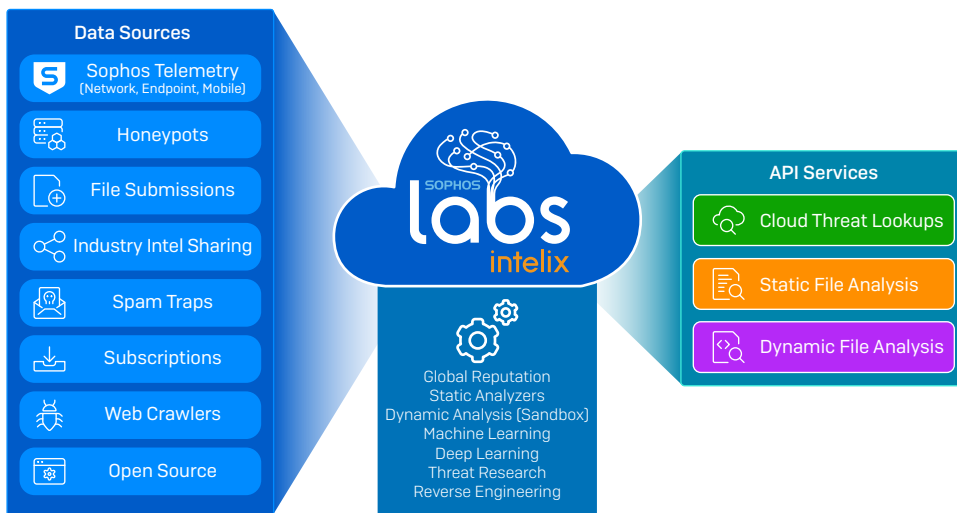
次に、ストリームが安全と判断され、もはや検査が不要になった場合、DPI エンジンは完全にフローを Sophos Network Flow FastPath にオフロードにして、信頼できるトラフィックへ高速パスを提供します。これにより、不要なトラフィックの検査から他のリソースが解放され、パフォーマンスが大幅に向上します。

ゼロデイ攻撃対策

ランサムウェアなどの高度な攻撃はますます標的型になり、検出を回避するようになるにつれて、予測的なゼロデイ脅威の特定と保護が非常に大切です。これに対する最終的な解決策は2つあります。

1. **静的機械学習分析** – リアルタイムでファイルを実行する必要はなく、グローバルレピュテーション、ファイルのディープスキャンを組み合わせた人工ニューラルネットワークの複数の機会学習モデルを介して、予測分析と検出を行います。
2. **動的ランタイムサンドボックス分析** – ファイルアクティビティへの比類のない洞察のためにクラウドサンドボックス環境にあるマルウェアをリアルタイムで駆除し、未知の脅威の性質と機能を明らかにします。

Sophos Firewall には、SophosLabs Intelix が提供するこの両方の重要な保護テクノロジーが搭載されています。SophosLabs は、非常に高い評価を受けている Tier-1 サイバーセキュリティ脅威解析の研究所で、SophosLabs Intelix における究極の脅威解析およびインテリジェンスプラットフォームを開発しました。最新の機械学習テクノロジーを活用し、数十年にわたる脅威の調査、大容量のインテリジェンスにより、最新で未知の脅威に対し卓越した保護を提供します。



Sophos Firewall の Zero-Day Protection は、SophosLabs Intelix の機械学習分析によって強化されています。

Sophos Firewall の Xstream DPI エンジン、ネットワークに入ってくるファイルに対して AV 分析を実行します。アクティブなコードがある場合はファイルを一時的に保持し、静的および動的 (サンドボックス) 解析の両方を実施するためクラウド内の SophosLabs Intelix サービスに送信します。次に、脅威インテリジェンスウィジェットとこのクリックスルーレポート (以下を参照) より Sophos Firewall Control Center の結果の概要を提供し、ファイルがクリーンな場合にのみファイルをダウンロード、またはメール受信者へリリースします。

多くのファイアウォールの高度なマルウェア対策では、解析が完了する前にエンドユーザーにファイルをリリースすることが多いため、最終的にファイルを脅威として確定した場合に、厄介でコストのかかるクリーンアップになるつながる可能性があります。

Threat intelligence

5
Recent

24
Incidents

217
Scanned

The screenshot shows the Sophos Firewall Zero-day protection interface. A modal window displays the analysis for a file named 'rs-w-8ben.pdf'. The overall verdict is 'MALICIOUS'. The analysis includes:

- Malware scan result: NO DETECTIONS
- Threat intelligence result: MALICIOUS (Based on: Feature analysis, Structure analysis, ML overall, Reputation)
- Sandstorm result: MALICIOUS (1 suspicious behavior, 1 malware identification)

The background shows a table of scanned files with columns for File, Date, Recipient, Source, File type, Status, and Manage.

Sophos Firewall の Zero-Day Protection は、これまでに見られなかった新しい未知の脅威がネットワークに侵入する前に特定します。

静的機械学習分析

静的ファイル分析では、多数の機会学習モデルを活用して、さまざまな特性、機能、遺伝子的要素、およびファイルのレピュテーション要素を分析し、それを SophosLabs データベース内で数百万もの既知の良好なファイルと不正なファイルと比較して、新しいファイルや以前表示されなかったファイルの判定を数秒で行います。これにより、新しい脅威や既存の脅威の新しい亜種を迅速かつ効果的に特定できます。特に、パスワードで保護されたマルウェアを含むドキュメントのような簡単にサンドボックス化できない脅威に効果的です。

The screenshot shows a 'Feature analysis' for a 'MALICIOUS' file. It lists features that are more likely in bad files (red bars) compared to good files (green bars).

More likely in bad files >>>	<<< More likely in good files	File feature
5,753,278	5,194,852	[!] The program may be hiding some of its imports: "GetProcAddress"
2,783,339	2,485,789	Compilers: "Microsoft Visual C++ 6.0 - 8.0"
1,623,697	1,723,903	[!] The program may be hiding some of its imports: "LoadLibraryExW"
1,543,823	3,294,614	Stack Canary: "enabled"
1,524,119	2,066,278	[!] The program may be hiding some of its imports: "LoadLibraryW"
1,394,671	1,514,017	Can access the registry: "RegSetValueExW"

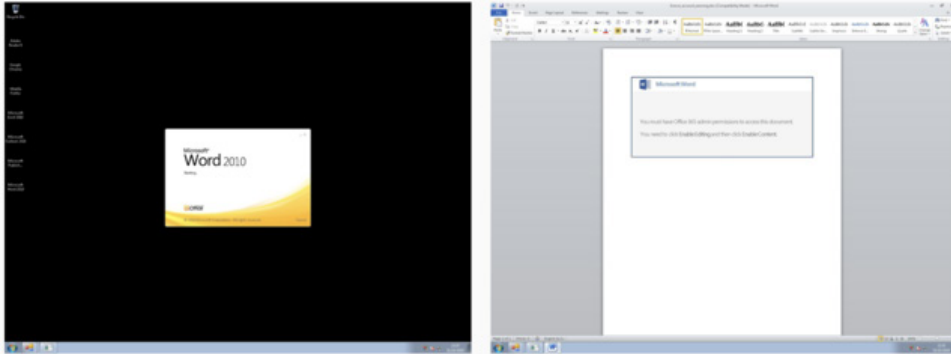
複数の機械学習モデルを使用して、不審なファイルを解析し、ゼロデイ脅威を検出します。

動的なランタイムサンドボックス分析

サンドボックステクノロジーが初めて登場したときは、大企業にとってのみが手の届く価格でした。しかし、Sophos Sandstorm を始めとするクラウドベースのサンドボックスソリューションが登場したことで、小規模ビジネスのお客様にとっても驚くほど手頃な価格になっています。2、3年前は大企業が数百万ドルをかけて導入していたオンプレミスの専用サンドボックスソリューションをはるかに上回るような機能、ディープラーニング技術を駆使したサンドボックス機能を中小企業のお客様も初めて利用できるようになりました。

クラウドベースなので、追加のソフトウェアやハードウェアは不要です。また、ファイアウォールのパフォーマンスに影響を与えません。Xstream DPI エンジンによって、メールの添付ファイルや Web ダウンロードなどアクティブなコードが含まれていると判断されたすべてのファイルは、お客様のネットワーク上に許可される前にそのランタイム動作を決定する静的解析 (上記参照) と並行して SophosLabs Intelix クラウドサンドボックスに自動的にアップロードされ、デトネーション (爆発) されます。

脅威を特定するために、SophosLabs は業界をリードするソフォスの Intercept X 次世代型エンドポイント製品の最新の保護テクノロジーをディープラーニング、エクスプロイト検出、CryptoGuard (リアルタイムでアクティブなランサムウェア暗号化ファイルを検出) などを含んだ Sophos Sandstorm に統合しました。また、すべてのファイル、メモリ、レジストリ、およびネットワークアクティビティを監視して、判定を行おうとする悪意のある特性を検出します。他社のファイアウォール製品では、最も優れた脅威防御である Intercept X を使用したこのようなランタイム解析は提供できません。また、Sophos Firewall が提供する、ファイルを実行した時に何が発生したかが分かるスクリーンショットのフルセットのような情報やレポートレベルも提供しません。



サンドボックスランタイム解析は、動作を判断するために安全な環境でファイルをデトネートして、レビュー用のスクリーンショットを提供します。

サンドボックス化は、悪意の特性を明らかに持っていないと思われる、通常無害なファイルに潜む脅威を検出する際に特に効果的です。マクロを含む Office ファイル、または無害な実行可能なファイル、もしくは破壊されたアプリケーションの更新です。

脅威対策レポート

Sophos Firewall により分析されたすべてのファイルには、さまざまな分析結果と判決結果の詳細が分かるレポートが付いてきます。レポートには、さまざまな機械学習の分析、ファイルのレピュテーション、サンドボックス、さらには第三者機関の Virustotal データを含む6つの異なる要素があります。

Investigation and actions

[drive]\[redacted]\file.exe

Blocked 5 times for 3 users. [Source details](#)

Time of analysis
 Static: 2019-07-26 21:09:08
 Sandstorm: 2019-04-16 17:40:58

Overall verdict


MALICIOUS

Analysis summary

MALICIOUS	MALICIOUS	MALICIOUS	SUSPICIOUS	NOT DETECTED	9/71	None
Machine learning Overall analysis	Machine learning File features	Machine learning File structure	File reputation	Sandstorm	VirusTotal detections	XG malware scan

Information about your file

File name [drive]\[redacted]\file.exe
 File type application/x-dosexec
 SHA1 41b68b777b6fd365e72f1344ae29fcdaf2f2e9af
 SHA256 6f14a34560d2076523ae95ae66b126d363d5552730459399a9cb3d9a4f2172086
 File size 10,096,640 bytes
[All details](#)



Machine learning

MALICIOUS

Overall verdict based on the Sophos deep learning model

Our model identifies many attributes of the file and compares their occurrence, individually and in different combinations, with millions of known good and known malware samples. The reports below show probabilities based on key components of the overall score. Each component isn't a strong indicator on its own but, in combination, they provide a critical insight. This model identifies many different characteristics of your file and compares the occurrence of those characteristics, individually and in combinations, across millions of known good and known malware samples.

Feature analysis

- Identifies specific features of the file.
- Randomly selects one million (out of **2,906,531**) known good and one million (out of **20,045,125**) known bad files.
- Counts the number of good and bad sample files that have the same features. These simple counts are shown in the graph below.
- The verdict may also take into account more complex combinations of features
- This test rates **file.exe** as **MALICIOUS**.

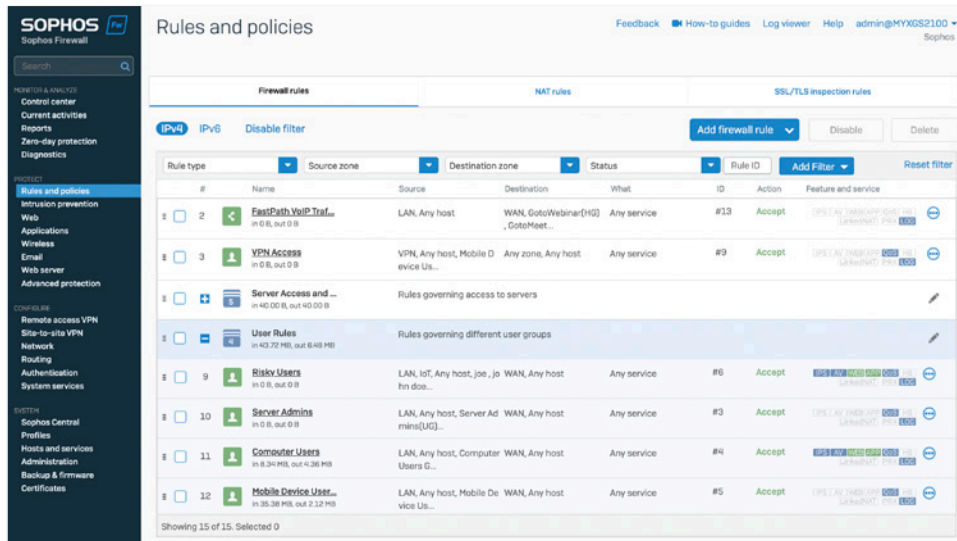
More likely in bad files	<<< More likely in good files	File feature
6,747	5,292	Can access the registry: "RegDeleteKeyW"
30,962	31,332	[!] The program may be hiding some of its imports: "GetProcAddress"
23,868	22,093	[!] The program may be hiding some of its imports: "LoadLibraryA"
48,199	49,165	Stack Canary: "disabled"
122	30	Packer: "Unusual section name found: .vmp0"
108	24	Packer: "Unusual section name found: .vmp1"

Feature combinations

統合ルール管理

ファイアウォールの管理は、非常に困難な場合があります。複数のルール、ポリシー、セキュリティ設定がさまざまな機能領域に分散し、また、必要な保護を提供するには異なるいくつかのルールがあるため、対処すべきことがたくさんあります。

Sophos Firewall では、ファイアウォールルールの編成方法とお客様のセキュリティ体制の管理方法が完全に見直されています。管理コンソールの中で適切なポリシーを探し回らずに済むように、すべてのファイアウォールルールと実施管理機能が1つの画面に統合されています。これにより、すべてのファイアウォールルールの表示、フィルタリング、検索、編集、追加、変更、整理を1つの場所でできるようになりました。



Sophos Firewall は、アクセスポリシー、NAT、TLS インスペクションのすべてのルールを1か所にまとめているため、管理が容易です。

ユーザー、ビジネスアプリケーション、NAT、TLS/SSL インスペクション、およびネットワーク用のルールを指定することで、必要なポリシーのみを表示できると同時に、すべてを単一の画面から管理することができます。

インジケータアイコンを見れば、ポリシーの種類、ステータス、適用状況など、ポリシーに関する重要な情報がわかります。

セキュリティ体制の管理が即座に可能

クラウドにある Sophos Central のアカウントを使用している場合でも、Sophos Firewall のユーザーインターフェースを使用している場合でも、ソフォス製品を使用すると、最新の保護に必要なすべての設定や管理が1つの画面から実行できるので、非常に簡単になります。

The screenshot shows the 'Security features' configuration page. Blue arrows point from various settings to Japanese labels on the right:

- デュアル AV (Dual AV) points to 'Malware and content scanning'.
- サンドボックス (Sandbox) points to 'Detect zero-day threats with Sandstorm'.
- SSL インспекション (SSL Inspection) points to 'Filtering common web ports'.
- ハートビート (Heartbeat) points to 'Configure Synchronized Security Heartbeat'.
- アプリの制御 (App Control) points to 'Identify and control applications (App control)'.
- QoS (Quality of Service) points to 'Shape traffic'.
- 優先順位の設定 (Priority Setting) points to 'DSCP marking'.
- IPS (侵入防御システム) (IPS - Intrusion Prevention System) points to 'Detect and prevent exploits (IPS)'.

事前定義されたポリシー、またはカスタムポリシーを使用して、1つの画面で完全なセキュリティポリシーを構成します。

ウイルス対策、TLS/SSL インспекション、サンドボックス、IPS、トラフィックシェーピング、Web コントロール、アプリケーションコントロール、Security Heartbeat、NAT、ルーティング、優先順位の調整など1つの画面で設定したり、セキュリティやコントロールを実行することができます。

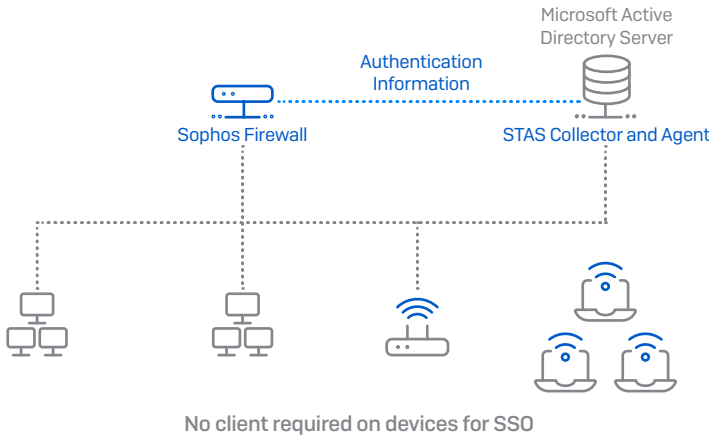
スナップインポリシーがどのような機能を果たしているのかを正確に把握したい場合や、変更を加えたい場合には、同じ画面上で編集することができます。ファイアウォールルール画面を離れて、製品の別の部分にアクセスする必要はありません。

The screenshot shows the 'Edit web policy' configuration page. It includes a form for Name and Description, and a table of rules. The table has columns for Users, Activities, Action, Constraints, Manage, and Status.

Users	Activities	Action	Constraints	Manage	Status
chris joe	All web traffic and with content Ethnicity terms [Canada] Objectionable Terms	Block		+ (edit) (trash)	ON
Anybody	Anonymizers	Block		+ (edit) (trash)	ON
Anybody	Weapons	Block		+ (edit) (trash)	ON
Anybody	Extreme	Block		+ (edit) (trash)	ON
Anybody	Phishing & Fraud	Block		+ (edit) (trash)	ON
Anybody	Militancy & Extremist	Block		+ (edit) (trash)	ON
Anybody	Gambling	Block		+ (edit) (trash)	ON

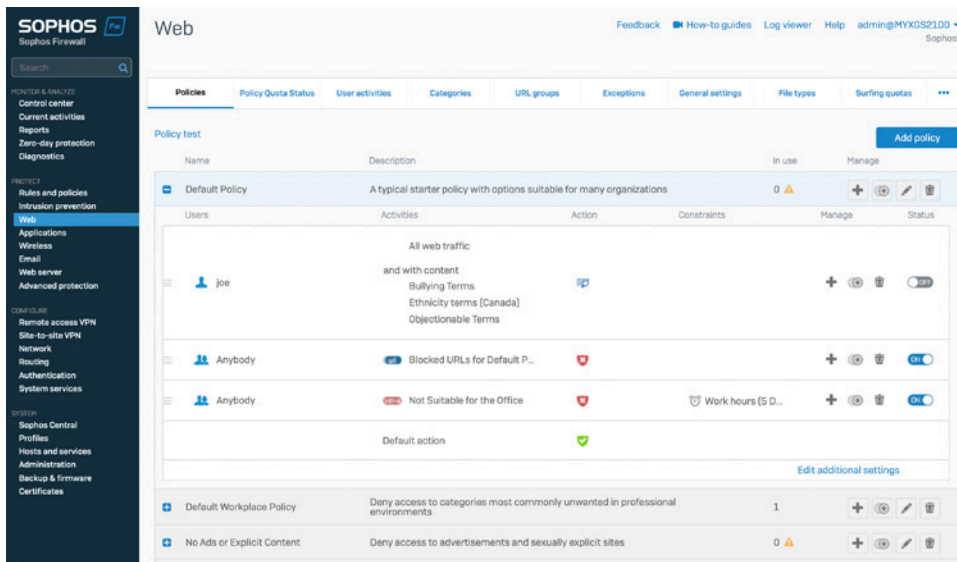
一目でポリシーの詳細を確認でき、ファイアウォールルール画面にいたままで変更が可能です。

柔軟な認証オプションにより、ユーザーの確認が容易なうえ、Active Directory、eDirectory、LDAP などのディレクトリサービスのほか、NTLM、Kerberos、RADIUS、TACACS+、RSA、クライアントエージェント、キャプティブポータルを使用できます。また、Sophos Transparent Authentication Suite (STAS) が Microsoft Active Directory などのディレクトリサービスとの統合を提供し、信頼性と透明性の高いシングルサインオン認証を実現します。



エンタープライズクラスのセキュア Web ゲートウェイ

Web プロテクションとコントロールは、どのファイアウォールにとっても不可欠なものです。残念ながら多くのファイアウォール実装では後回しになりがちです。ソフォスは、エンタープライズクラスの Web プロテクションソリューションを構築してきた経験から、通常 10 倍のコストがかかるようなエンタープライズ SWG (Secure Web Gateway) ソリューションでしか利用できない Web ポリシーコントロールの実装に必要な知識やノウハウを獲得しました。トップダウン型継承ポリシーモデルが実装されているので、高度なポリシーを簡単かつ直感的に作成できます。標準的な職場環境、教育機関の CIPA 準拠など、一般的な導入向けには、そのまま使用が可能な定義済みポリシーテンプレートが用意されています。テンプレートでは微調整やカスタマイズのオプションをすぐに使用できるため、即座に要件を満たすことができます。



強力なエンタープライズレベルの Web ポリシーにより、細部にわたる制御が可能です。

実際、ファイアウォールで日常的に変更される頻度が最も高い要素の 1 つが Web ポリシーであることがわかっています。そこでソフォスは、ユーザーやビジネスのニーズに基づいてポリシーを簡単に管理、微調整できるようにする技術への多額の投資を継続してきました。ユーザーとグループ、アクティビティ (URL、カテゴリ、コンテンツフィルタ、ファイルタイプで構成される)、アクション (ブロック、許可、警告) のカスタマイズ、時間帯と曜日の制約の追加/調整が簡単にできます。

教育関連の機能

Sophos Firewall では、Web ポリシーやコンプライアンスが重要な要件である教育現場に対し最適な機能をいくつかご用意しています。教育関連の機能は次のとおりです。

- ▶ CIPA 準拠のためにパッケージ化された Web ポリシー
- ▶ キーワードのコンテンツフィルタとレポート
- ▶ SafeSearch およびユーザー/グループポリシーベースで YouTube 制限設定
- ▶ 教師が管理できるブロックページのオーバーライド
- ▶ 潜在的な問題を早期に特定するための包括的な組み込みレポート機能

Web ポリシーには、キーワードリストに基づいて動的コンテンツ関連のポリシーを記録して監視、または強制適用するオプションが追加されました。この機能は、教育機関で特に重要です。たとえば、学生のオンラインでの安全を確保したり、自傷行為、いじめ、過激な思想、不適切なコンテンツなどに関連するキーワードに基づいて知見を提供したりします。そのためには、キーワードライブラリをファイアウォールにアップロードして Web フィルタリングポリシーに適用し、記録や監視を行ったり、特定のキーワードを含んだ検索結果や Web サイトをブロックするなどの条件を追加で指定します。

キーワードとの一致情報や、特定のキーワードを含むコンテンツを検索/参照しているユーザーなど、詳しい情報が記載された包括的レポートが作成されます。この情報に基づき、リスクのあるユーザーが実際に問題に変わる前に対策を講じることができます。

Sophos Firewall は、CIPA (児童インターネット保護法) ポリシーへのコンプライアンスをすぐに使用できるので、迅速なコンプライアンスを実現します。また、SafeSearch および YouTube の制限をユーザー/グループポリシーベースで柔軟かつ強力に制御できます。また、教師には独自のポリシーオーバーライドを設定して管理するオプションが与えられ、クラスはカリキュラムの一部として通常ブロックされる Web サイトにアクセスできるようになります。

ソフォスの Web ポリシーはパワフルでありながらシンプルです。

シンプルな NAT 設定

NAT (ネットワークアドレス変換) ルールを設定しようとした方はご存じかもしれませんが、これはとても困難なことです。しかし、そうである必要はありません。Sophos Firewall には、強力で柔軟な NAT の設定を可能にするエンタープライズ NAT 機能がすべて含まれています。これには、詳細な選択基準を持つ単一のルールで Source NAT (SNAT) や Destination NAT (DNAT) などが含まれます。複雑な DNAT をシンプルにするために、使いやすいウィザードを使用して、わずか数クリックで完全な NAT の設定を作成するプロセス実行できます。

管理者は、ファイアウォールルールを作成する際にリンクされた便利な NAT オプションを活用することもできます。リンクされた NAT では、対応する NAT の設定ルールが自動的に作成されるので、NAT ルールの作成や設定にかかる時間がさらに短縮します。

The screenshot shows a configuration wizard window titled "Server access assistant (DNAT)". The main content area is titled "Review your selection" and contains the following information:

- Select Save to add NAT rules and firewall rules with the following configuration:**
- Internal server to access from the internet:**
 - IP host: 10.0.1.10
 - Hostname: Mac Server
- Public IP address through which users access the internal server:**
 - IP host: 50.68.180.222
 - Hostname: #Port2
- Services that users can access:**
 - Server Port Forwarding
- Sources from which users can access the server:**
 - Any
- Creates three NAT rules:**
 - Inbound NAT (DNAT): Traffic destined to the public IP address 50.68.180.222 is translated to the internal server address 10.0.1.10.
 - Outbound NAT (SNAT): Masquerades outbound traffic from the internal server 10.0.1.10 with the public IP address 50.68.180.222.
 - Loopback NAT: Internal network uses the same public IP address 50.68.180.222 to access the internal server 10.0.1.10.
- Creates one firewall rule:**
 - Allows access to the internal server for Server Port Forwarding services from the sources Any.
- The rules are added at the top of the table and are turned on by default.

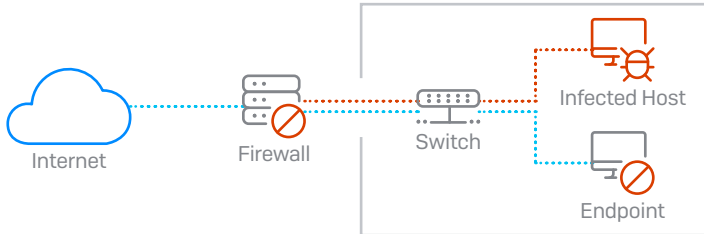
At the bottom of the window, there are navigation buttons: "Cancel", "5 of 5", "Back", and "Save and finish".

強力が直感的な NAT ルールウィザードを活用し、数回クリックするだけで複雑なアクセス制御を作成できます。

インシデントへの自動対応

ネットワーク管理者が最も求めるファイアウォール機能の1つは、ネットワーク上のセキュリティインシデントに自動対応する機能です。

Sophos Firewall は、ネットワーク上の感染源を完全に特定し、自動的に他のネットワークリソースへ感染したデバイスをアクセスする制限ができる唯一のネットワークセキュリティソリューションです。これを可能にしているのが、ソフォスのマネージドエンドポイントとファイアウォールの間でテレメトリとヘルスステータスを共有するユニークな Sophos Security Heartbeat です。



Sophos Firewall および Security Heartbeat は、ネットワーク上の感染したホストを自動的に隔離することができます。

Sophos Firewall 独自の手法により、接続されているホストのセキュリティ状態に応じてファイアウォールのルールを適用することで、感染したシステムが除去されるまで自動的に隔離し、機密情報を含むネットワークリソースへのアクセスを制限することができます。

Sophos Firewall は、ファイアウォールでネットワークの他の部分にアクセスできないようにエンドポイントを隔離するだけでなく、ネットワーク上の正常なすべてのエンドポイントに協力を求めて、エンドポイントレベルで侵害されたホストをさらに隔離することもできます。

当社が呼んでいるこのラテラルムーブメント対策により、脅威や攻撃者がファイアウォールが通常介入できない同じネットワークセグメントやブロードキャストドメインにいる場合でも、ネットワーク全体にわたり他のシステムへと横方向に移動することから隔離したり阻止したりします。これは、ネットワーク上で動作するアクティブな敵の課題に対する非常にシンプルで効果的なソリューションです。また、エンドポイントとファイアウォールが協調防御もしくは同期防御で相互連携して動作している場合にのみ可能です。

Security Heartbeat

Sophos Security Heartbeat は、ソフォスのエンドポイントと Sophos Firewall 間の安全なリンクを使用して、リアルタイムで情報を共有します。以前は単独で動作していたセキュリティ製品を同期するというこの単純な手順を踏むことで、高度なマルウェアや標的型攻撃に対する保護機能の効果が向上します。



HOSTNAME, IP	USER	STATUS CHANGED
Mac-Server 10.0.1.10	Chris	5 days ago
Joe's Laptop 192.168.1.2	joe	54 seconds ago
MacBook 10.0.1.55	Mindy	36 seconds ago
Macbook-CA-GN-42527 10.0.1.15	chrismccormack	13 hours ago

ネットワークの Security Heartbeat™ ステータスは、コントロールセンターで確認できます。

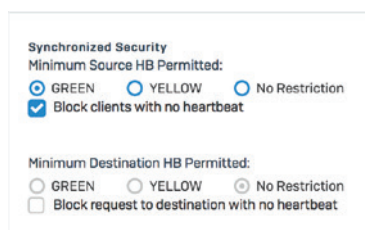
Security Heartbeat は、高度な脅威の存在を即座に特定できるだけでなく、脅威の性質、ホストシステム、およびユーザーに関する重要情報を伝達するためにも使用できます。また、Security Heartbeat の最大の特長は、マルウェアが消滅するまでの間、自動的に感染したシステムの隔離をしたり、アクセスを制限したりすることもできることです。これは、IT セキュリティソリューションによる高度な脅威の特定方法と対応方法に革命をもたらすテクノロジーです。

ファイアウォールの背後にある管理対象エンドポイントでは、Security Heartbeat の状態は次の3つのいずれかです。

緑色のハートビートステータスは、エンドポイントデバイスが正常であり、適切なすべてのネットワークリソースにアクセスできることを示します。

黄色のハートビートステータスは、デバイスに PUA (迷惑なアプリケーション) が存在する可能性がある場合、コンプライアンス違反である場合、またはその他の問題が存在する場合の警告です。問題を解決するまでの間、黄色のハートビートがアクセスできるネットワークリソースを選択できます。

赤色のハートビートステータスは、高度な脅威に感染する危険性があり、ボットネットまたは C&C サーバーへのコールホームを試みている可能性のあるデバイスを示します。ファイアウォールで Security Heartbeat ポリシー設定を使用することで、クリーンアップするまでの間ステータスが赤いハートビートのシステムを簡単に隔離して、データ損失や感染拡大のリスクを低減できます。



ファイアウォールルールの一部として、Security Heartbeat の要件を設定します。

Security Heartbeat のようなソリューションを提供できるのは、エンドポイントとネットワークの両方をカバーするセキュリティソリューションのリーダーであるソフォスだけです。他のベンダーは IT セキュリティの未来の姿をようやく認識し始め、慌てて同様のソリューションを導入しようとしているところですが、いずれのベンダーも明らかに不利な立場にあります。なぜなら、ソフォスのように業界をリードするエンドポイントソリューションとファイアウォールソリューションの両方を所有していないからです。

これからはゼロトラストの世界

信頼が、IT 業界において当たり前と感じている場合には、これは危険な言葉となりました。企業が外部から隔離された大規模な境界を造り上げ、内部のすべてを信頼することは、間違っただesignであると証明されています。

ゼロトラストとは、こうした変化に対応するセキュリティへの総合的なアプローチで、組織が脅威に対してどのように取り組み、対応するかを示します。これは、セキュリティについて熟考し、どのように対応するかを考える哲学です。

企業ネットワークの内部であれ外部であれ、疑うことなく誰かを信じたり、何かを信じたりするべきではありません。そうは言っても、最終的には何かを信頼する必要があります。ゼロトラストでは、この信頼は一時的なものであり、複数のデータソースから確立され、常に再評価されます。

ゼロトラストでは、オフィス内から使用するクラウドプラットフォームまで、企業全体を管理できます。企業の境界外での制御が不足したり、リモートユーザーとの連携に苦労したりすることはもうありません。

ゼロトラストに移行して、そのメリットのすべて活用するにはどうすればよいでしょうか？ゼロトラストを単一のソリューションとして提供できる企業はありませんが、ソフォスでは、ゼロトラストへの移行を短期化したり、簡素化するセキュリティテクノロジーとコントロールの幅広い製品ラインが用意されています。

Sophos Central – 業界で最も信頼性の高いサイバーセキュリティプラットフォームでは、異種で補完的なテクノロジーを単一のクラウド管理コンソールに統合し、ゼロトラストネットワークをオーケストレーション、および管理します。

Synchronized Security – サイバーセキュリティは、エンドポイント、ZTNA、ファイアウォール、またはその他のシステム間で継続的に情報を共有し、相互に詳細や可視性を提供します。

Sophos ZTNA – 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ための、真の Zero Trust Network Access ソリューションを提供します。

Sophos Firewall ユーザー、デバイス、アプリケーション、ネットワークなどの周囲にセグメントまたはマイクロ境界を作成します。

Server Protection と Intercept X – 全てのデバイスにデバイスのセキュリティ状態を割り当てて、1つが侵害された場合に備えて、デバイスを自動的に接続から隔離したり、ブロックすることができるようにします。

MTR (Managed Threat Response) サービス – ネットワーク全体のすべてのユーザーアクティビティを監視し、侵害された可能性のあるユーザーの認証情報を特定します。

SD-WAN ネットワークの最適化

SD-WAN (ソフトウェア定義型広域ネットワーク) ほど話題を呼ぶネットワーク用語はほとんどありません。話題となるものはすべて、有益な情報と複雑な言い回しが同時に混在してきました。その結果、SD-WAN はさまざまな人にとって異なる意味を持つようになりましたが、一部の人は、その意味を正確に把握しようとしています。

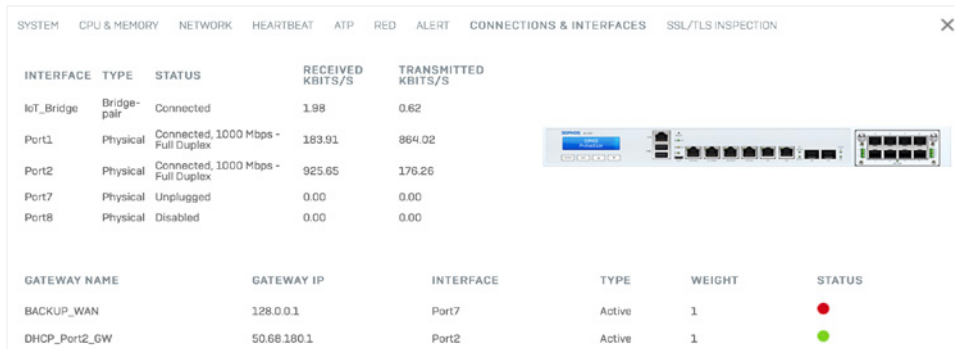
SD-WAN は本来、以下の 4つのネットワークの目標のうち 1つまたは複数を実現することを目的としています。

- ▶ **接続コストの削減** – 従来の MPLS (Multi-Protocol Label Switching) 接続は高価であるため、企業は、ケーブル、DSL、3G/4G/LTE のようなより安価なブロードバンド WAN 方式のオプションに切り替えが進んでいる
- ▶ **ビジネスの継続性** – WAN で障害や停止が発生したときに、冗長性、ルーティング、フェールオーバー、セッションの保持といった機能が必要
- ▶ **重要アプリケーションの品質** – 重要度の高い業務アプリケーションのセッション品質を維持するために、アプリケーションのトラフィックやパフォーマンスをリアルタイムで可視化できるようなソリューションが必要
- ▶ **VPN オーケストレーションの簡素化** – 複数の支社間で接続する VPN オーケストレーションは、複雑で時間がかかる。そのため、VPN の導入やセットアップを簡素化したり自動的に行えるようなツールが期待される

Xstream SD-WAN を搭載した Sophos Firewall は、SD-WAN オーケストレーション、管理、およびパフォーマンスと信頼性の最適化オプションの包括的なセットにより、最も壮大な SD-WAN の目標をシンプルかつ手頃な価格で達成することが可能です。

Xstream SD-WAN

複数の WAN リンクを介したアプリケーショントラフィックのルーティングを管理することは、SD-WAN の重要な考え方です。Xstream SD-WAN を備えた Sophos Firewall は、複数の MPLS、DSL、ケーブル、セルラー接続を使用している場合でも、強力かつ柔軟なリンク管理ソリューションを提供します。



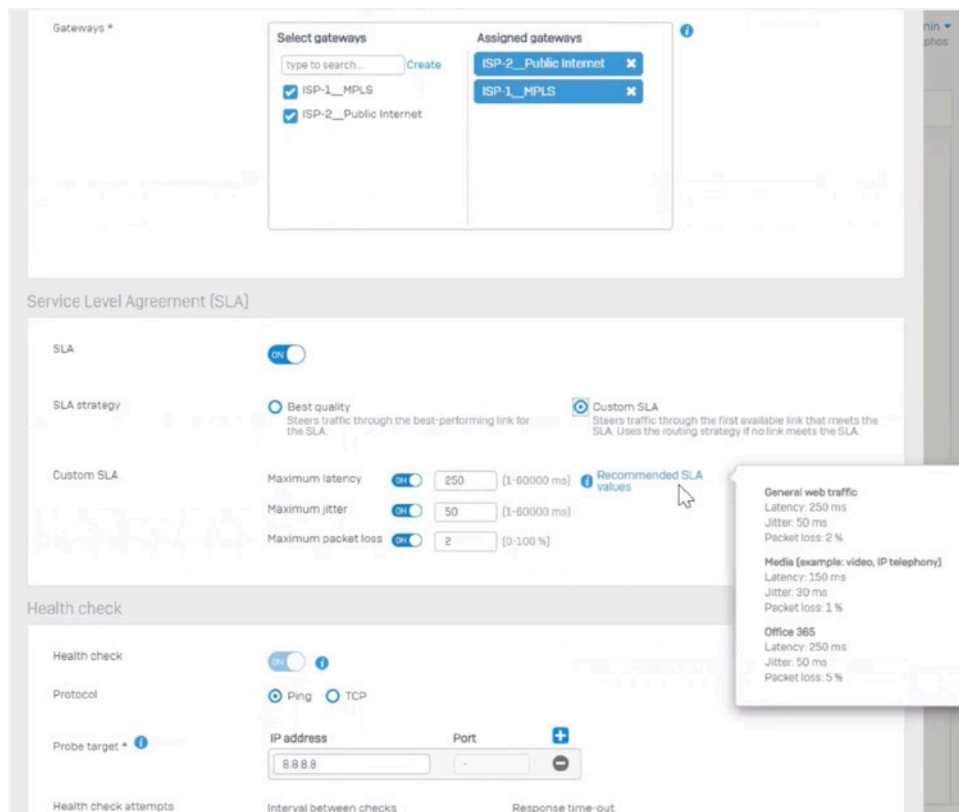
The screenshot shows the 'CONNECTIONS & INTERFACES' section of the Sophos Firewall dashboard. It contains two tables: one for interface status and one for gateway configuration.

INTERFACE	TYPE	STATUS	RECEIVED KBYTES/S	TRANSMITTED KBYTES/S
IoT_Bridge	Bridge-pair	Connected	1.98	0.62
Port1	Physical	Connected, 1000 Mbps - Full Duplex	183.91	864.02
Port2	Physical	Connected, 1000 Mbps - Full Duplex	925.65	176.26
Port7	Physical	Unplugged	0.00	0.00
Port8	Physical	Disabled	0.00	0.00

GATEWAY NAME	GATEWAY IP	INTERFACE	TYPE	WEIGHT	STATUS
BACKUP_WAN	128.0.0.1	Port7	Active	1	● (Red)
DHCP_Port2_GW	50.68.180.1	Port2	Active	1	● (Green)

ダッシュボードから、このインターフェースステータスウィジェットにアクセスすると、下部に WAN リンクステータスが表示されます。

SD-WAN プロファイルとは、複数の WAN リンクゲートウェイのルーティング方法を定義する仕組みで、WAN リンクのパフォーマンスに基づき、アプリケーション接続をシームレスかつ効率的に再ルーティングを可能にします。リンク間の移行は、アプリケーションセッションにゼロインパクトで瞬時に行われ、最も中断の多い、または不安定な ISP 環境内ですえもシームレスな継続性、アプリケーションパフォーマンス、および最高のエンドユーザーエクスペリエンスを中断することなく提供します。



パフォーマンスベースの SD-WAN プロファイルの設定は、直感的かつ簡単です。

SD-WAN プロファイルのルーティング方法としては、最初に利用可能であるリンクか、またはパフォーマンスに基づくリンクを選択できます。パフォーマンスを監視する方法を選択した場合は、遅延、ジッタ、パケット損失の条件を指定できます。また、PING または TCP によるプローブ対象を複数指定できます。

SD-WAN プロファイルは、パフォーマンスに基づいて、もしくは許容可能なジッタ、レイテンシ、パケットロスの最大値の特定の値を定義するカスタム SLA ポリシーに従って、自動的に最適なリンクを選択してから、アクティブな接続にゼロインパクトでよりパフォーマンスの高いリンクに再ルーティングされるという仕組みになっています。

SD-WAN ネットワークのパフォーマンスの監視は、レイテンシ、ジッタ、パケットロスのリアルタイムおよび履歴グラフを使用して簡単に確認することができます。リアルタイム監視の期間は、過去 24 時間、48 時間、1 週間、1 カ月を選択できます。SD-WAN パフォーマンスとルーティングの高度なログも含まれます。



さまざまな WAN リンクのパフォーマンスをリアルタイムで監視します。

SD-WAN VPN トラフィックの Xstream FastPath アクセラレーション

Sophos Firewall は、XGS シリーズアプライアンスに統合された Xstream Flow プロセッサを利用して、IPsec VPN トンネルトラフィックのハードウェアアクセラレーションを提供します。これにより、ESP によるカプセル化/暗号化とカプセル解除/復号化など、IPsec トンネルに必要な CPU 負荷の高い処理の一部が Xstream Flow プロセッサに移行されるため、パフォーマンスが劇的に向上します。この新機能は Xstream Flow プロセッサ内のハードウェア暗号化機能を最大限に活用しており、CPU リソースを解放して必要なトラフィックのディープパケットインスペクションなど他のタスクに使用できるという利点もあります。IPsec トラフィックの Xstream FastPath アクセラレーションは、サイト間およびリモートアクセス VPN トラフィックの両方で機能します。

The screenshot displays the configuration interface for a WAN link manager. It is divided into two main sections: 'Gateway detail' and 'Failover rules'.

Gateway detail:

- Name:** DHCP_Port2_GW
- IP address:** 50.68.180.1
- Interface:** Port2-50.68.180.222/255.255.252.0
- Type:** Active (selected), Backup
- Weight:** 1 (range 1-100)
- Default NAT policy:** MASQ

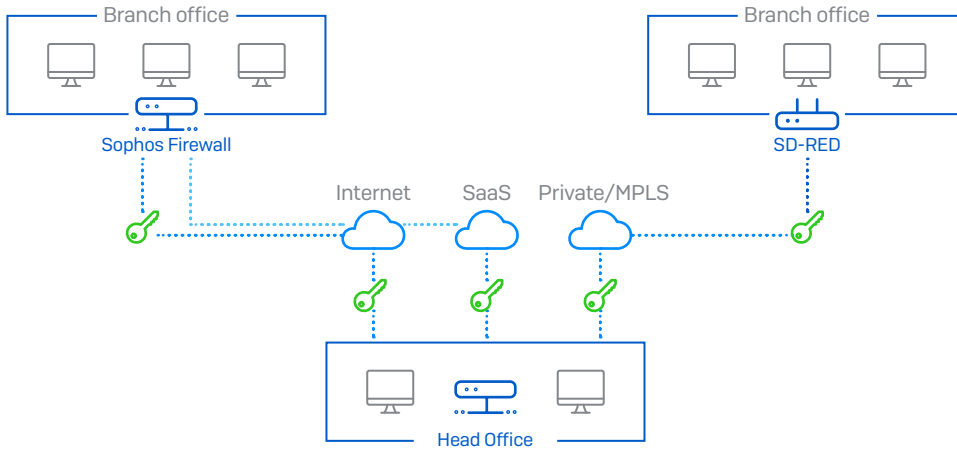
Failover rules:

- If ...**
 - Not able to Connect: PING, Port *, on IP address: 50.68.180.1
 - AND
 - Not able to Connect: TCP, Port, on IP address:
- Then ...**
 - *SHIFT to another available gateway*

Sophos Firewall WAN のリンクマネージャでは、負荷分散やフェールオーバーのルールを確認できます。

SD-Branch オフィスとの接続

ソフォスは独自の SD-RED デバイスを提供しており、ゼロタッチ式の支社間の導入および接続にかけては長年の実績を誇り、業界をリードする存在です。これらのデバイスは安価かつ導入しやすいのが特徴で、技術者でなくても、中心拠点にあるファイアウォールとデバイス間にセキュアで堅牢なレイヤー 2 トンネルをととても簡単に確立することができます。



Sophos Firewall と独自の SD-RED デバイスは、トンネルオプションを提供しており、支社間を SD-WAN で簡単に、低コストで接続することが可能です。



ソフォスの SD-RED デバイスを使えば、比較的安価でゼロタッチ式で簡単に支社と接続が可能です。

SD-RED デバイスの導入はこれまで以上に簡単になりました。まず、ファイアウォールがある側のサイトで、デバイスのシリアル番号を書きとめてから、デバイスをリモートロケーションに郵送します。リモート側で作業を担当するのは技術者でなくても構いません。受け取ったデバイスを接続して、ソフォスのクラウドプロビジョニングサービスに通知するだけで、自動的に Sophos Firewall との間に安全なトンネルが確立されます。

The screenshot shows the configuration page for a Sophos Firewall SD-RED device. The interface is divided into three main sections: RED settings, Uplink settings, and RED network settings. At the bottom, there are 'Save' and 'Cancel' buttons.

RED settings

- Branch name * [Text input field]
- Type: RED 15 [Dropdown menu]
- RED ID * [Text input field]
- Tunnel ID * : Automatic [Dropdown menu]
- Unlock code * [Text input field]
- Firewall IP/hostname * [Text input field]
- 2nd firewall IP/hostname [Text input field]
- Use 2nd IP/hostname for: Failover Load balancing
- Description [Text area]
- Device deployment: Automatically via provisioning service Manually via USB stick

Uplink settings

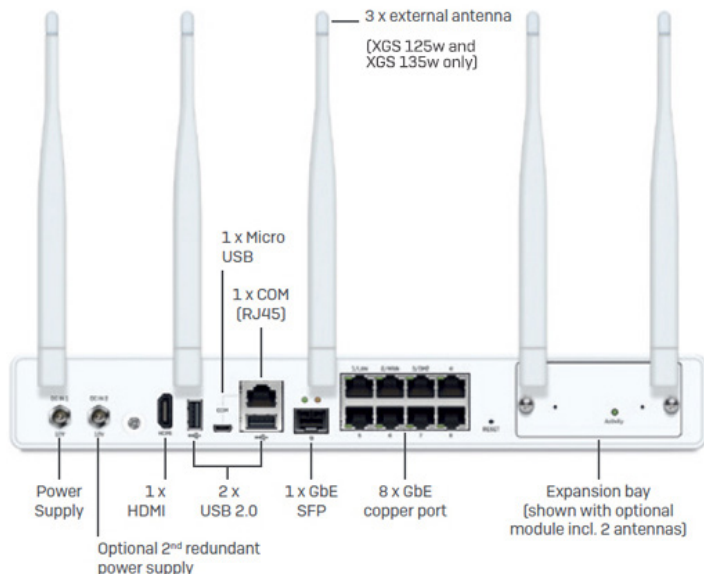
- Uplink connection: DHCP Static
- 3G/UMTS failover: Enable

RED network settings

- RED operation mode: Standard/unified Standard/split Transparent/split
- RED IP * [Text input field]
- RED netmask: /24 (255.255.255.0) [Dropdown menu]
- Zone: LAN [Dropdown menu]
- Configure DHCP: ON
- RED DHCP range: [Text input field] [Text input field]
- MAC filtering type: No configured MAC address lists found
- Tunnel compression: Enable
- RED MTU: 1500 [Text input field] (576 to 1500)

Sophos SD-RED は、柔軟、セキュア、手頃な価格という特徴を兼ね備えた、SD-WAN 支社接続ソリューションです。

デスクトップ型の XGS シリーズアプライアンスは、銅線、ファイバインターフェースに加えて、VDSL や携帯インターフェースなどの柔軟な接続オプションで SD-WAN 接続ソリューションを本社に提供し、堅牢な SD-RED トンネルをサポートしているのが特徴です。



XGS 135w のデスクトップモデルには、ご覧のように LTE/携帯、VDSL、銅線、ファイバー などの WAN 接続オプションがあります。

VPN のサポートとオーケストレーション

異なるファイアウォール間で 2 つ以上の VPN トンネルを設定したことがあれば、これがどれほど時間のかかる面倒な作業かご存知ではないでしょうか。Sophos Firewall は、Sophos Central で豊富な SD-WAN オーケストレーションをサポートしているため、ファイアウォール間の複数のトンネルをすばやく簡単に相互接続できます。

SD-WAN の接続グループに参加させたい管理下のファイアウォールを選択して、各サイトにアクセスさせたいネットワークリソースを選択するだけです。スイッチを切り替えるだけで、必要なファイアウォールルールや冗長性を含むすべてのトンネルが自動的に作成されるため、SD-WAN VPN オーバーレイネットワークが実現されます。



数回クリックするだけで、複雑な SD-WAN オーバーレイネットワークを迅速にセットアップし、Sophos Central から監視できるようになります。

Sophos Central は、フルメッシュ型ネットワークやハブアンドスポークトポロジなどさまざまなネットワークの形態に対応し、SD-WAN オーバーレイネットワークを有効にするためにバックエンドで設定する必要があるすべてのトンネルやファイアウォールを自動的に構成します。

もちろん、Sophos Firewall は、IPsec や SSL などの一般的なサイト間 VPN オプションをサポートしています。堅牢なルーティングで、遅延が多い状況 (サテライトリンク経由など) でも高い信頼性を発揮する当社独自の SD-RED レイヤー 2 トンネルも提供しています。

アプリケーションの可視性とルーティング

そのほかの SD-WAN の重要機能として、アプリケーションのパス選択およびルーティングがあります。この機能によって、VoIP などの重要アプリケーションの遅延を最小化し、品質を保証することができますようになります。

特定できないアプリケーションをルーティングすることはできません。そのため、アプリケーションを特定・可視化する機能の正確性、信頼性が重要となってきます。アプリケーションの特定・可視化は、Sophos Firewall と Sophos Synchronized Security が特に得意とする分野です。Synchronized Application Control では、ネットワーク上のすべてのアプリケーションを明確に識別することができます。業務上重要なアプリケーションには、判別しにくいものやカスタムアプリケーションも含まれますが、特にこうしたアプリケーションの識別において優れた能力を発揮するのが特徴です。

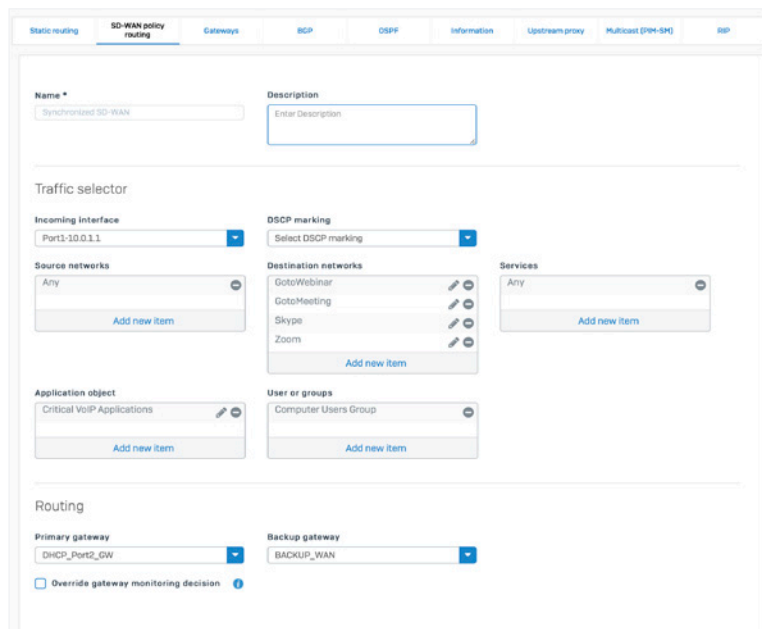
Synchronized SD-WAN の Synchronized Security 機能は、SD-WAN のアプリケーションルーティングでさらなるメリットを提供しています。Synchronized SD-WAN は、ソフォスが管理するエンドポイントと Sophos Firewall 間で Synchronized Application Control の情報を共有することで、アプリケーション識別の明瞭性と信頼性をさらに高めます。以前は識別されなかったアプリケーションも SD-WAN ルーティングポリシーにも追加できるようになり、他のファイアウォールでは一致しないアプリケーションルーティング制御や信頼性を提供します。

The screenshot displays the 'Applications' page in the Sophos Firewall management console. It features a navigation bar with 'How-to guides', 'Log viewer', 'Help', and 'admin' (Sophos). Below the navigation bar, there are tabs for 'Application filter', 'Synchronized Application Control', 'Cloud applications', 'Application list', and 'Traffic shaping default'. The 'Synchronized Application Control' tab is active, showing a table of applications. The table has columns for 'Application', 'Category', 'Endpoints', 'Occurrences', 'Last occurrence', and 'Manage'. The 'Application' column includes a checkbox, a plus icon, and the application name. The 'Category' column shows 'VoIP'. The 'Endpoints' column shows 'Found on 1 Endpoints' or 'Found on 2 Endpoints'. The 'Occurrences' column shows the number of occurrences. The 'Last occurrence' column shows the date and time of the last occurrence. The 'Manage' column includes buttons for 'PREFED' and 'CUSTOMED'.

Application	Category	Endpoints	Occurrences	Last occurrence	Manage
<input type="checkbox"/> Skype ..\office16\ync.exe	VoIP	Found on 1 Endpoints	739	2017-10-10 07:39	<input type="checkbox"/> PREFED
<input type="checkbox"/> Skype <ProgramFiles>\..\phone\skype.exe	VoIP	Found on 1 Endpoints	739	2017-10-10 07:39	<input type="checkbox"/> PREFED
<input type="checkbox"/> Skype Applications\..\MacOS\Skype	VoIP	Found on 1 Endpoints	15270	2019-03-26 19:31	<input type="checkbox"/> CUSTOMED
<input type="checkbox"/> Skype for Business Applications\..\Skype for Business	VoIP	Found on 2 Endpoints	154797	2019-04-05 15:28	<input type="checkbox"/> CUSTOMED

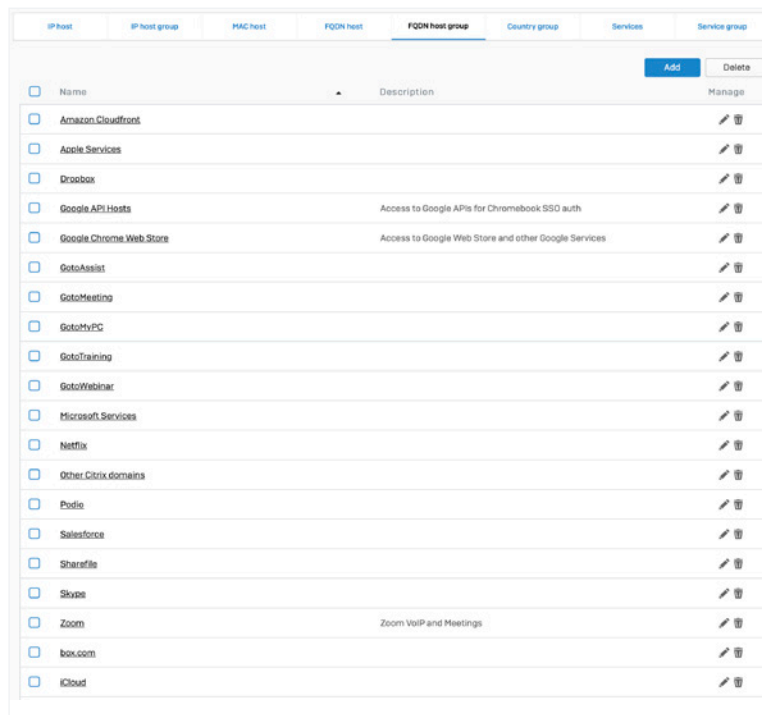
Synchronized Application Control は、ネットワーク上のアプリケーションを 100% 識別可能。業務上重要なアプリケーションを、優先度に応じて簡単にルーティングできます。

また Sophos Firewall では、ユーザーやグループ別などすべてのファイアウォールルールで、アプリケーションベースのルーティングおよびパス選択も可能です。詳細なポリシーベースルーティング (PBR) の制御により、プライマリまたはバックアップゲートウェイの WAN 接続を介したルーティングの定義を提供し、再生方向を設定できます。これらの機能を組み合わせることで、重要なアプリケーショントラフィックを最適な WAN インターフェースに簡単に転送できます。



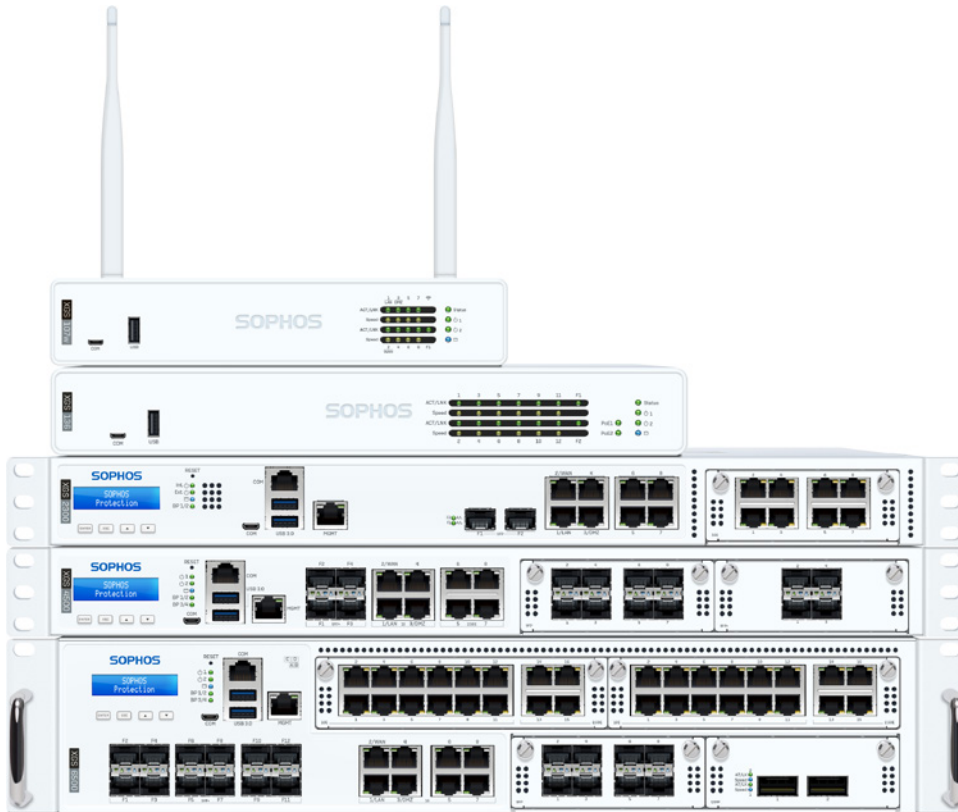
SD-WANのポリシーベースのルーティングによって、重要アプリケーションのトラフィックを柔軟にルーティングすることができます。

Sophos Firewall には、一般的な SaaS クラウドサービスの完全修飾ドメイン名 (FQDN) オブジェクトがあらかじめ定義されています。定義済みの FQDN ホスト数は数千件におよび、すぐに使用したり、新たな定義を追加するのも簡単です。



FQDN ホストオブジェクトがあらかじめ定義されており、パス選択やアプリケーションベースのルーティングをすばやく簡単に行えます。

Sophos Firewall をあらゆるネットワークに簡単に追加



Sophos Firewall シリーズハードウェアアプライアンスは、すべての 1U モデルに標準のフェールオープンバイパスポートを備えた柔軟性の高い導入オプションを提供します。この機能は、Flexi-Port モジュールで利用できるので、2U アプライアンスでも有効にできます。バイパスポートを使用すると、Sophos Firewall を既存のファイアウォールに合わせてブリッジモードでインストールできます。Sophos Firewall をシャットダウンまたは再起動をしてファームウェアをアップデートする必要がある場合は、トラフィックを許可して、ネットワークを中断せずに継続的な流れができることにより、バイパスポートはビジネスコンティニュイティを提供します。この機能により、既存のネットワークインフラを置き換えることなく、まったくリスクのない新しい導入オプションが実現できます。さらに、次世代型のエンドポイント保護製品である Intercept X は、既存のデスクトップウイルス対策製品と併用が可能であるため、置き換えを一切行うことなく、完全な Sophos Synchronized Security ソリューションを任意のネットワークに導入できます。

Sophos Firewall: シンプルなサイバーセキュリティを実現します。

価格についてのお問い合わせ

お客様のニーズに合わせてカスタマイズしたお見積りを作成します (無料)。sophos.com/firewall-quote までご依頼ください。

ソフォス株式会社営業部
Email: sales@sophos.co.jp