

SOPHOS
Cybersecurity delivered.

Sophos Firewall

Solution Brief



Inhaltsverzeichnis

Sophos Firewall	2
Aufdecken verborgener Risiken	3
Control Center	3
Extra starke TLS Inspection	6
Synchronized Application Control	7
Benutzer mit größtem Risikopotenzial	8
Flexible Reporting-Optionen	9
Blockieren unbekannter Bedrohungen	10
Xstream-Schutz und -Performance	10
Zero-Day-Bedrohungsschutz	11
Statische Machine-Learning-Analyse	12
Dynamische Sandbox-Analyse während der Laufzeit	13
Bedrohungsschutz-Reporting	14
Zentrale Regel-Verwaltung	15
Verwaltung Ihres Sicherheitsstatus auf einen Blick	16
Secure Web Gateway der Enterprise-Klasse	17
Funktionen für Bildungseinrichtungen	18
Vereinfachte NAT-Konfiguration	19
Automatische Reaktion auf Vorfälle	20
Security Heartbeat	20
Willkommen in der „Zero Trust“-Welt	22
Optimierung Ihres SD-WAN-Netzwerks	23
Xstream SD-WAN	23
Xstream-FastPath-Beschleunigung von SD-WAN-VPN-Datenverkehr	26
SD-Anbindung von Zweigstellen	27
VPN-Unterstützung und -Orchestrierung	29
Transparenz über Anwendungen und Routing	30
Einfaches Hinzufügen der Sophos Firewall zu jedem beliebigen Netzwerk	32

Sophos Firewall

Die Sophos Firewall wurde so konzipiert, dass sie die typischen Probleme bisheriger Firewalls beseitigt. Gleichzeitig bietet sie eine effektive Next-Gen-Plattform, um die Herausforderungen durch den heutigen verschlüsselten Internet-Traffic und die sich stetig weiterentwickelnde Bedrohungslandschaft zu meistern. Die Sophos Firewall bietet einen neuartigen Ansatz beim Erkennen verborgener Risiken, dem Schutz vor Bedrohungen und der Reaktion auf Vorfälle, ohne die Performance zu beeinträchtigen. Unsere Xstream-Architektur für die Sophos Firewall nutzt eine Paketverarbeitungs-Architektur, die eine sehr hohe Transparenz, Sicherheit und Performance bietet.

Die Sophos Firewall liefert einzigartige Transparenz über riskante Benutzer, unerwünschte Anwendungen, verdächtige Payloads und Persistent Threats. Sie integriert sich nahtlos in eine umfassende Palette moderner Schutztechnologien, die sich einfach einrichten und verwalten lassen. Und anders als ältere Firewalls kommuniziert die Sophos Firewall mit anderen Sicherheitssystemen im Netzwerk und wird so zu Ihrem zentralen Steuerungspunkt, von dem aus Sie Bedrohungen in Schach halten und verhindern, dass Malware sich ausbreiten oder Daten aus dem Netzwerk abschöpfen kann – automatisch und in Echtzeit.

Die Sophos Firewall hat gegenüber anderen Netzwerk-Firewalls vier wesentliche Vorteile:

1. **Deckt verdeckte Risiken in Ihrem Netzwerk auf:** Die Sophos Firewall deckt verborgene Risiken weit besser auf als andere Lösungen – mit einem visuellen Dashboard, umfassendem On-Box- und Cloud-Reporting und maximaler Transparenz über Risiken.
2. **Blockiert unbekannt Bedrohungen:** Die Sophos Firewall blockiert unbekannt Bedrohungen schneller und effektiver als andere Firewalls – mit einer Vielzahl leistungsstarker Schutzfunktionen, die sich einfach einrichten und verwalten lassen.
3. **Reagiert automatisch auf Vorfälle:** Dank dem Sophos Security Heartbeat™, der in Echtzeit Informationen zwischen Ihren Endpoints und Ihrer Firewall austauscht, reagiert die Sophos Firewall mit Synchronized Security automatisch auf Vorfälle im Netzwerk.
4. **Optimiert Ihr SD-WAN-Netzwerk:** Die Xstream-SD-WAN-Funktionen der Sophos Firewall ermöglichen die Einrichtung komplexer SD-WAN-Overlay-Netzwerke per einfachem „Point-and-Click“. Außerdem können Sie die automatische Performance-basierte WAN-Link-Auswahl mit sofortigen, unterbrechungsfreien Umschaltungen zwischen Verbindungen nutzen, um die Anwendungsleistung, Netzwerk-Resilienz und Geschäftskontinuität zu optimieren und gleichzeitig die Verbindungskosten zu senken.

Aufdecken verborgener Risiken

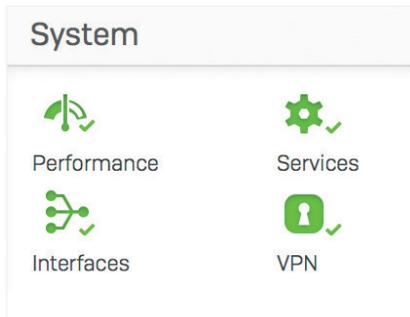
Moderne Firewalls müssen alle von ihnen erfassten Daten analysieren, wenn möglich Daten korrelieren und nur die wichtigsten Informationen so aufbereiten, dass Sie reagieren können – und zwar, bevor es zu spät ist.

Control Center

Das Control Center der Sophos Firewall verschafft Ihnen maximale Transparenz über Aktivitäten, Risiken und Bedrohungen in Ihrem Netzwerk.

Mit Symbolen in Ampelfarben erkennen Sie schnell, wo Sie reagieren müssen:

Ein rotes Symbol bedeutet, dass Sie sofort handeln müssen. Ein gelbes Symbol weist auf ein potenzielles Problem hin. Und wenn alles grün ist, sind keine weiteren Maßnahmen erforderlich.



The screenshot shows the Sophos Firewall Control Center dashboard. The dashboard is divided into several sections: System, Traffic insight, User & device insights, Active firewall rules, Reports, and Messages. Annotations with blue arrows point to specific data points:

- Bedrohungen und gefährdete Systeme:** Points to the Security Heartbeat section, which shows 0 At risk, 0 Missing, 1 Warning, and 3 Connected.
- Unbekannte Anwendungen:** Points to the Synchronized Application Control section, which shows 0 New, 5 Categorized, and 59 Total.
- Verdächtige Payloads:** Points to the Threat intelligence section, which shows 5 Recent, 24 Incidents, and 217 Scanned.
- Riskante Benutzer:** Points to the ATP section, which shows 5 Sources blocked and 1 Acc. for 80% of risk.
- Komplexe Bedrohungen:** Points to the SSL/TLS connections section, which shows <1% of traffic Decrypted and 21.6K Failed.
- Riskante Anwendungen:** Points to the Messages section, which shows a Warning about managing the firewall from Sophos Central.
- Unerwünschte Websites:** Points to the Messages section, which shows a Warning about objectionable websites.
- Einbruchversuche:** Points to the Messages section, which shows a Warning about intrusion attacks.

Jedes Widget im Control Center liefert weitere Informationen, die durch Klicken auf das Widget einfach abgerufen werden können. Der Status von Schnittstellen auf dem Gerät kann beispielsweise abgefragt werden, indem Sie im Control Center auf das Widget „Schnittstellen“ klicken.

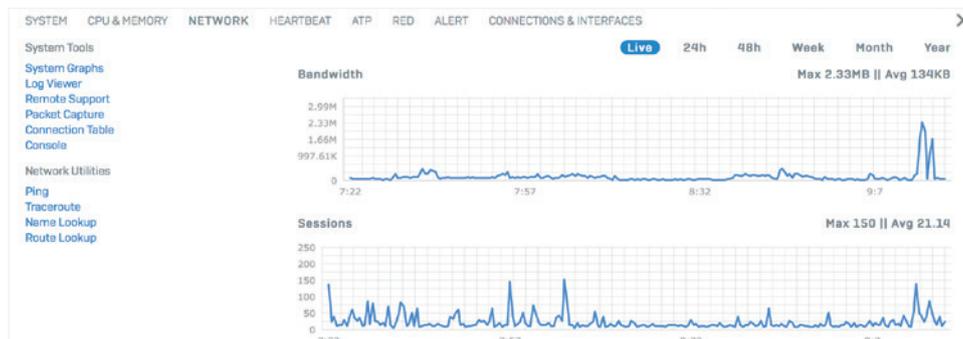
INTERFACE	TYPE	STATUS	RECEIVED KBITS/S	TRANSMITTED KBITS/S
IoT_Bridge	Bridge-pair	Connected	1.98	0.62
Port1	Physical	Connected, 1000 Mbps - Full Duplex	183.91	864.02
Port2	Physical	Connected, 1000 Mbps - Full Duplex	925.65	178.26
Port7	Physical	Unplugged	0.00	0.00
Port8	Physical	Disabled	0.00	0.00

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	●

Der Host, Benutzer und die Quelle einer komplexen Bedrohung können ebenso einfach durch Klicken auf das Widget „ATP“ [Advanced Threat Protection] im Dashboard abgerufen werden.

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

Systemdiagramme zeigen die Performance zudem im zeitlichen Verlauf und Sie können bestimmte Zeitabschnitte auswählen (z. B. letzte zwei Stunden oder letzter Monat bzw. letztes Jahr). Außerdem ermöglichen sie einen schnellen Zugriff auf häufig genutzte Troubleshooting-Tools, um potenzielle Probleme zu beheben.



Den Live Log Viewer können Sie in jeder Ansicht mit nur einem Klick aufrufen. Der Viewer öffnet sich auf Wunsch in einem neuen Fenster, sodass Sie das jeweilige Protokoll beim Arbeiten in der Konsole im Auge behalten können. Es stehen zwei Ansichten zur Verfügung: ein einfacheres Spaltenformat nach Firewall-Modul sowie eine detailliertere zentrale Ansicht mit leistungsstarken Filter- und Sortieroptionen, in der Protokolle vom gesamten System auf einen Blick und in Echtzeit ersichtlich sind.

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 09:48:18	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	54.87.88.218	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 09:48:08	Firewall Rule	Allowed	chris	4	Port1		10.0.1.15	54.198.179.15	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	54.87.88.218	1	00001	Open PCAP	
2017-11-29	Firewall	Allowed	chris	4	Port1	Port2	10.0.1.15	64.58.144.92	2	00001	Open PCAP	

Haben Sie sich wie viele andere Netzwerk-Administratoren auch schon gefragt, ob Sie zu viele Firewall-Regeln haben und ob Sie auf einige verzichten könnten? Mit der Sophos Firewall erübrigen sich diese Fragen.

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 09:44:30	Invalid Traffic	Denied					100.115					messageid="01001" log_type="Firewall" log_component="Invalid Traffic" log_subtype="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="0" app_technology="app_category="in_interface="Port1" out_interface="src_mac="fc0f24200c0f8" 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_type="src_zone="dst_zone_type="dst_zone="con_direction="con_id="virt_con_id="hb_status="No Heartbeat" message="Could not associate packet to any connection" appresolvedby="Signature"
2017-11-29 09:44:27	Invalid Traffic	Denied					100.115					messageid="01001" log_type="Firewall" log_component="Invalid Traffic" log_subtype="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="0" app_technology="app_category="in_interface="Port1" out_interface="src_mac="fc0f24200c0f8" 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_type="src_zone="dst_zone_type="dst_zone="con_direction="con_id="virt_con_id="hb_status="No Heartbeat" message="Could not associate packet to any connection" appresolvedby="Signature"
2017-11-29 09:44:25	Invalid Traffic	Denied					100.115					messageid="01001" log_type="Firewall" log_component="Invalid Traffic" log_subtype="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="0" app_technology="app_category="in_interface="Port1" out_interface="src_mac="fc0f24200c0f8" 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_type="src_zone="dst_zone_type="dst_zone="con_direction="con_id="virt_con_id="hb_status="No Heartbeat" message="Could not associate packet to any connection" appresolvedby="Signature"
2017-11-29 09:44:22	Invalid Traffic	Denied					100.115					messageid="01001" log_type="Firewall" log_component="Invalid Traffic" log_subtype="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="0" app_technology="app_category="in_interface="Port1" out_interface="src_mac="fc0f24200c0f8" 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_type="src_zone="dst_zone_type="dst_zone="con_direction="con_id="virt_con_id="hb_status="No Heartbeat" message="Could not associate packet to any connection" appresolvedby="Signature"
2017-11-29 09:44:19	Invalid Traffic	Denied					100.115					messageid="01001" log_type="Firewall" log_component="Invalid Traffic" log_subtype="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="0" app_technology="app_category="in_interface="Port1" out_interface="src_mac="fc0f24200c0f8" 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_type="src_zone="dst_zone_type="dst_zone="con_direction="con_id="virt_con_id="hb_status="No Heartbeat" message="Could not associate packet to any connection" appresolvedby="Signature"

Das Widget „Aktive Firewall-Regeln“ zeigt in einem Echtzeit-Diagramm, welchen Datenverkehr die Firewall nach Regeltyp verarbeitet hat: Geschäftsanwendung, Benutzer und Netzwerkregeln. Auch die aktive Anzahl von Regeln nach Status wird angezeigt, einschließlich ungenutzter Regeln, die ggf. gelöscht werden können. Wie in anderen Bereichen des Control Center sind auch beim Klicken auf diese Elemente weitere Informationen verfügbar – in diesem Fall eine Tabelle zu den Firewall-Regeln, geordnet nach Regeltyp oder -status.

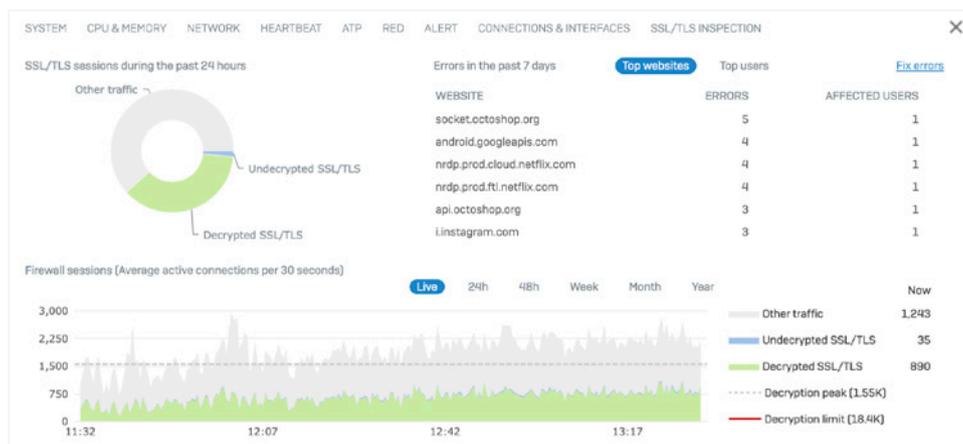


Extra starke TLS Inspection

Rund um verschlüsselten Datenverkehr braut sich ein wahrhaftiger Sturm zusammen. Laut Google sind 90 % des Datenverkehrs in Netzwerken mittlerweile verschlüsselt. Dieser Anstieg bietet Cyberkriminellen die Möglichkeit, versteckte Angriffe zu starten, die nur schwer erkannt werden können. Schließlich können Sie keine Angriffe stoppen, die Sie nicht sehen können. Leider sind die meisten Unternehmen machtlos, da ihre aktuelle Firewall nicht die erforderliche Performance bietet, um TLS/SSL Inspection ohne drastische Leistungseinbußen zu nutzen.

Die Sophos Firewall verfügt dank ihrer neuen Xstream SSL Inspection Engine über eine deutlich höhere Kapazität für gleichzeitige Verbindungen und bietet flexible Richtlinien-Tools, mit denen intelligente Entscheidungen darüber getroffen werden können, was gescannt werden soll und was gegebenenfalls ausgelagert („Offloading“) werden kann. Mithilfe der SSL-Richtlinien-Tools können Unternehmen TLS/SSL-Richtlinien der Enterprise-Klasse erstellen, die sich auf den nicht entschlüsselbaren Datenverkehr, Zertifikate, Protokolle, Optionen zur Verschlüsselungserzwingung und vieles mehr beziehen. Die Sophos Firewall unterstützt TLS 1.3 und alle modernen Crypto Suites für jeden Port und jede Anwendung im System.

Zusätzliche Tools direkt auf dem Dashboard ermöglichen es Administratoren, genau zu sehen, wie viel Netzwerkverkehr verschlüsselt ist und wie dieser verarbeitet wird. Die Sophos Firewall bereitet diese Informationen weit besser auf als andere Lösungen – insbesondere Fehler, die aufgrund von Zertifikat-Validierungen oder Websites auftreten, die nicht die neuesten Verschlüsselungsstandards unterstützen.



Die Sophos Firewall bietet über das Control Center direkten Einblick in verschlüsselte Datenverkehrsflüsse und alle Probleme, die sich aus der TLS Inspection ergeben

Administratoren können auch ein detailliertes Fenster öffnen, um genau zu sehen, welche Websites warum problematisch sind. Außerdem werden hier Benutzer angezeigt, bei denen Probleme vorliegen. Von dort aus können sie direkt Maßnahmen ergreifen, um die Anwendung oder die Website von der Entschlüsselung auszuschließen, damit weitere Probleme vermieden werden. Keine andere SSL-Inspection-Lösung bietet denselben Zugriff auf diese Informationen.

Synchronized Application Control

Das Problem mit Application Control in heutigen Next-Generation Firewalls besteht darin, dass der meiste Anwendungsverkehr nicht identifiziert wird: Die Anwendungen werden entweder nicht klassifiziert oder sie werden markiert als unbekannt, generische HTTP- oder generische HTTPS-Anwendungen.

Hierfür gibt es einen einfachen Grund: Alle Firewall App Control Engines stützen sich zur Identifizierung von Anwendungen auf Signaturen und Muster. Und wie Sie sich vielleicht vorstellen können, existieren für benutzerdefinierte Anwendungen aus vertikalen Märkten (z. B. Medizin- oder Finanzanwendungen) grundsätzlich keine Signaturen. Andere evasive Anwendungen wie BitTorrent Clients und VoIP- sowie Messaging-Apps ändern ständig ihr Verhalten und ihre Signatur, um einer Erkennung und Kontrolle zu entgehen. Viele von ihnen setzen außerdem auf Verschlüsselung, um nicht erkannt zu werden. Andere nutzen generische, Webbrowser-ähnliche Verbindungen für externe Kommunikationen über die Firewall, weil Port 80 und 443 von den meisten Firewalls normalerweise nicht blockiert werden.

Das Ergebnis ist eine mangelnde Transparenz über Anwendungen im Netzwerk und Sie können Dinge, die Sie nicht sehen können, auch nicht kontrollieren. Die Lösung hierfür ist sehr elegant und gleichzeitig effektiv: Sophos Synchronized Application Control, die unsere einzigartige Synchronized-Security-Verbindung zu Sophos-verwalteten Endpoints nutzt.

Das funktioniert folgendermaßen: Erkennt die Sophos Firewall Anwendungsverkehr, den sie mit Signaturen nicht identifizieren kann, fragt sie den Endpoint, welche Anwendung diesen Traffic generiert.

Synchronized Application Control™



The screenshot shows the Sophos Firewall web interface for the 'Applications' section. It features a navigation sidebar on the left and a main content area. The main area is titled 'Synchronized Application Control' and contains a table of detected applications. The table has 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	Info Edit
BitTorrent C:\UserProfile\.\bittorrent.exe C:\UserProfile\.\bittorrent.exe	P2P	Found on 2 Endpoints	3983	2021-06-04 15:16	Info Edit
macOS Big Sur Installer Applications/./InstallersSetup	Infrastructure	Found on 1 Endpoints	7	2021-12-10 11:37	Info Edit
Messages Applications/./MacOS/Messages	Instant Messenger	Found on 2 Endpoints	143	2022-01-12 15:24	Info Edit
Remote Desktop Connection (V7 and Higher) C:\Microsoft Remote Desktop ./MacOS/Microsoft Remote Desktop	Remote Access	Found on 2 Endpoints	724	2021-11-15 17:13	Info Edit

Unbekannte Anwendungen, die von Synchronized Application Control erkannt wurden, können automatisch oder manuell kategorisiert werden.

Der Endpoint kann dann Informationen über die ausführbare Datei, den Pfad und oft auch ihre Kategorie an die Firewall übertragen. Anhand dieser Informationen kann die Firewall die Anwendungen in den meisten Situationen automatisch klassifizieren und kontrollieren.

Falls die Sophos Firewall die passende Anwendungskategorie nicht automatisch ermitteln kann, kann der Administrator die gewünschte Kategorie einrichten oder die Anwendung einer bestehenden Richtlinie zuweisen.

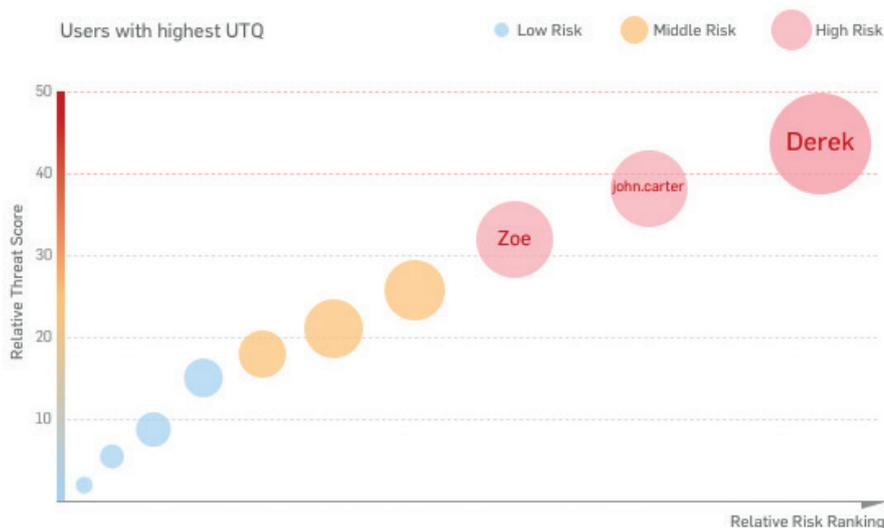
Sobald eine Anwendung klassifiziert wurde – entweder automatisch oder durch den Netzwerkadministrator – unterliegt die Anwendung denselben Richtlinienkontrollen wie alle anderen Anwendungen in dieser Kategorie. So können Sie alle nicht identifizierten, unerwünschten Anwendungen blockieren und erwünschte Anwendungen priorisieren.

Synchronized Application Control setzt neue Standards bei der Transparenz und Kontrolle über Anwendungen und schafft Klarheit über alle Anwendungen – auch solche, die im Netzwerk bislang unidentifiziert und unkontrolliert genutzt wurden.

Benutzer mit größtem Risikopotenzial

Studien haben gezeigt, dass Benutzer das schwächste Glied in der Sicherheitskette sind. Die gute Nachricht: Muster menschlichen Verhaltens können analysiert werden, um Angriffe vorherzusagen und zu verhindern. Nutzungsmuster können außerdem veranschaulichen, wie effizient Unternehmensressourcen genutzt werden und ob Benutzerrichtlinien angepasst werden müssen.

Der Sophos User Threat Quotient (UTQ) hilft Sicherheits-Administratoren dabei, Benutzer frühzeitig zu erkennen, die aufgrund ihres verdächtigen Verhaltens im Internet sowie ihres Bedrohungs- und Infektionsverlaufs ein Risiko darstellen. Hohe UTQ-Risikobewertungen von Benutzern können auf unbeabsichtigtes Fehlverhalten infolge mangelnden Sicherheitsbewusstseins, eine Malware-Infektion oder bewusstes Fehlverhalten hindeuten.



Die Sophos Firewall zeigt Ihnen auf einen Blick Benutzer mit besonders hohem Risikopotenzial.

Kennen die Netzwerksicherheits-Administratoren den Benutzer und die Aktivitäten, die ein Risiko verursacht haben, können sie leichter erforderliche Maßnahmen ergreifen. So können sie Benutzer, von denen ein besonders hohes Risiko ausgeht, entweder gezielt schulen oder striktere bzw. geeignetere Richtlinien durchsetzen, um das Benutzerverhalten zu kontrollieren.

Blockieren unbekannter Bedrohungen

Zum Schutz vor aktuellen Netzwerkbedrohungen ist ein „Orchester“ von Technologien erforderlich, das optimal aufeinander abgestimmt ist und von einem Dirigenten – dem Netzwerkadministrator – geleitet wird. Die meisten Firewalls gleichen jedoch eher einem Alleinunterhalter, der gleichzeitig singt, Gitarre spielt und mit Messern jongliert: Die Einrichtung von Firewall-Regeln erfolgt in einem Bereich, Web-Richtlinien befinden sich in einem komplett anderen Bereich, TLS/SSL Inspection wieder woanders und App Control gar in einem gänzlich separaten Teil des Produkts.

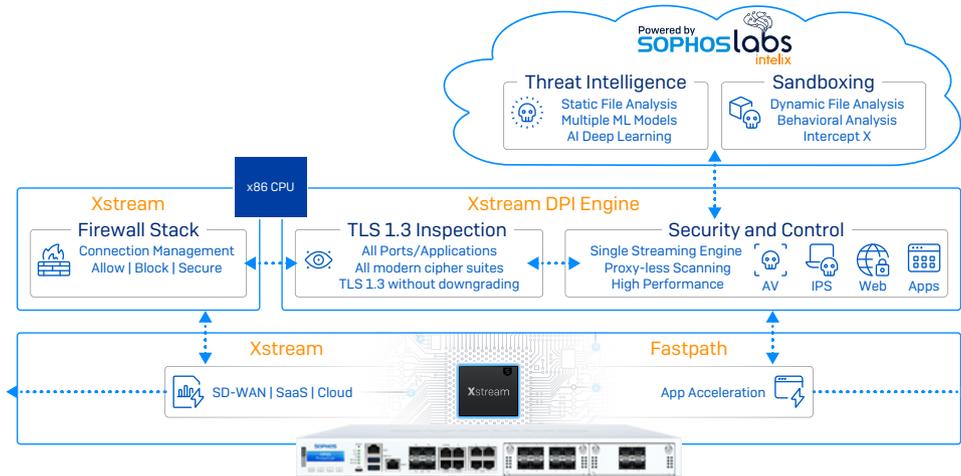
Bei Sophos sind wir nicht nur der Meinung, dass Sie die marktwert leistungsstärkste Schutztechnologie erhalten sollten. Wir wissen auch, dass die Konfiguration, Bereitstellung und tägliche Verwaltung einfach sein müssen, denn schlecht konfigurierter Schutz ist oft gefährlicher als gar kein Schutz.

Das Ziel, IT-Security so einfach wie möglich zu gestalten, ist tief in der Unternehmensphilosophie von Sophos verankert. Noch wichtiger ist vielleicht jedoch, dass Sophos großen Mut zur Veränderung hat und offen dafür ist, seine Vorgehensweise zu ändern, wenn sich dadurch der Schutz oder das Benutzererlebnis verbessern lässt.

Die Sophos Firewall macht vieles anders – und damit einen großen Unterschied.

Xstream-Schutz und -Performance

Die Firewall-Performance sollte auch dann konstant bleiben, wenn Sie die Sicherheitsfunktionen zum Schutz Ihres Netzwerks vor Bedrohungen aktivieren. Eine der Kernkomponenten der Sophos Firewall Xstream-Paketverarbeitungs-Architektur ist eine leistungsstarke Deep Packet Inspection (DPI) Engine. Die DPI Engine bietet proxylose Sicherheits-Scans in einem Arbeitsgang für IPS, Web, Antivirus und App Control sowie unsere Xstream SSL Inspection.



Die Xstream-Architektur der Sophos Firewall mit programmierbaren Xstream-Flow-Prozessoren bietet leistungsstarke Sicherheit und Performance.

Wenn eine neue Verbindung hergestellt wird, wird sie vom Firewall-Stack verarbeitet, der Entscheidungen darüber trifft, ob der Datenverkehr zugelassen, blockiert oder auf Bedrohungen überprüft werden soll.

Wenn für den Datenverkehr Sicherheits-Scans erforderlich sind, werden die Pakete an die proxylose Hochleistungs-Streaming-DPI-Engine weitergeleitet, die die Pakete scannt, auch wenn sie verschlüsselt sind. Dieses Verfahren wird nur bei den ersten paar Paketen angewendet. Danach gibt der Firewall-Stack die Verarbeitung vollständig an die DPI Engine ab. Dadurch werden die Latenz und Performance deutlich verbessert.

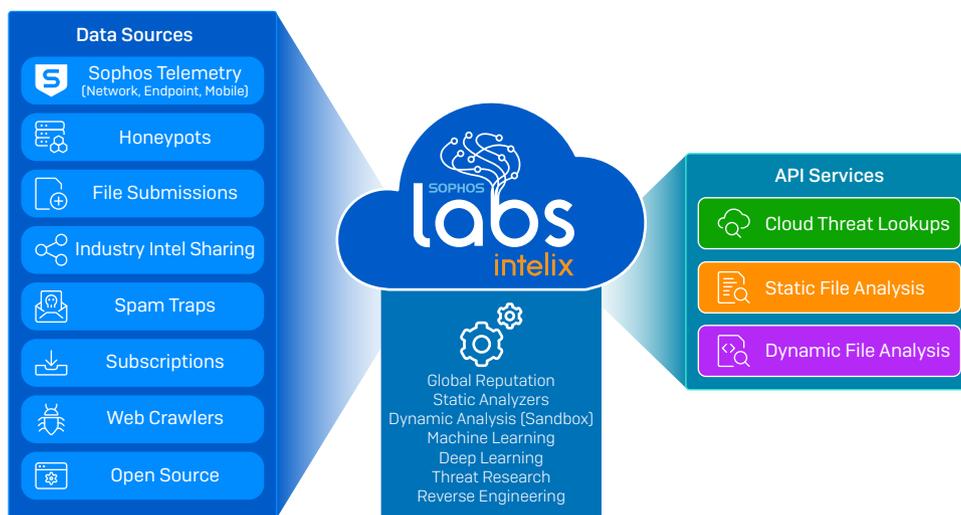
Wenn der Stream als sicher eingestuft wird und keine weitere Überprüfung mehr erforderlich ist, kann die DPI Engine den Flow vollständig an den Sophos Network Flow FastPath auslagern, der einen beschleunigten Pfad für vertrauenswürdigen Datenverkehr bereitstellt. Dies steigert die Performance dramatisch, da mehr Ressourcen für anderen Traffic zur Verfügung stehen.

Zero-Day-Bedrohungsschutz

Da komplexe Bedrohungen wie Ransomware immer gezielter und evasiver werden, besteht dringender Bedarf für prädiktive Lösungen zur Identifizierung und Abwehr von Zero-Day-Bedrohungen. Die ultimative Lösung dafür sind zwei verschiedene Analyseformen:

1. **Statische Machine-Learning-Analyse** – Diese ermöglicht eine prädiktive Analyse und Erkennung durch mehrere Machine-Learning-Modelle aus künstlichen neuronalen Netzwerken, kombiniert mit globaler Reputation und Deep File Scanning, ohne die Datei in Echtzeit ausführen zu müssen.
2. **Dynamische Laufzeit-Sandbox-Analyse** – Bei dieser Analyse wird Malware unter kontrollierten Bedingungen in Echtzeit in einer Cloud-Sandbox-Umgebung ausgeführt. So erhalten Sie einzigartige Transparenz über die Dateiaktivität und können die wahren Eigenschaften und Fähigkeiten einer unbekanntenen Bedrohung aufdecken.

In der Sophos Firewall sind beide diese wichtigen Schutztechnologien enthalten, mit Unterstützung durch SophosLabs Intelix. Unser renommiertes, globales Threat Research Lab „die SophosLabs“ hat die ultimative Bedrohungsanalyse- und Intelligence-Plattform in SophosLabs Intelix entwickelt. Mit neuestem Machine Learning, jahrzehntelanger Bedrohungsforschung und Petabytes an Daten sorgt diese für branchenführenden Schutz vor neuen, bisher unbekanntenen Bedrohungen.



Der Zero-Day-Schutz der Sophos Firewall wird durch die Machine-Learning-Analyse von SophosLabs Intelix unterstützt.

Wird im Zuge der Antivirus-Analyse einer Datei aktiver Code festgestellt, so behält die Xstream DPI Engine die Datei vorübergehend ein und sendet sie zur statischen und dynamischen Datei-Analyse an den SophosLabs Intelix Service in der Cloud. Eine Zusammenfassung der Ergebnisse wird anschließend im Sophos Firewall Control Center über das Threat Intelligence Widget und einen über eine Schaltfläche aufrufbaren Report (siehe folgende Abbildung) zur Verfügung gestellt. Die Datei wird nur dann an die Person freigegeben, die den Download gestartet oder die E-Mail erhalten hat, wenn die Datei unbedenklich ist.

Dieser letzte Schritt ist wichtig, denn viele moderne Malware-Lösungen in Firewalls geben Dateien bereits frei, bevor die Analyse abgeschlossen ist. Erweist sich eine Datei dann doch als Bedrohung, muss evtl. eine sehr zeit- und kostenaufwändige Bereinigung durchgeführt werden.

Threat intelligence

5
Recent

24
Incidents

217
Scanned

The screenshot shows the 'Zero-day protection' section of the Sophos Firewall interface. A table lists scanned files with columns for File, Date, Recipient, Source, File type, Status, and Manage. A modal window is open over one of the entries, displaying a detailed threat intelligence report. The report includes an overall verdict of 'MALICIOUS', a 'NO DETECTIONS' result from the malware scan, and a 'MALICIOUS' result from the threat intelligence engine. It also shows a 'SANDSTORM' result of 'MALICIOUS' based on suspicious behavior and malware identification. A vertical bar chart on the right of the modal shows scores for Sandstorm, Structure analysis, ML overall, Feature analysis, and Reputation, with Sandstorm and ML overall being the highest.

Der Zero-Day-Schutz der Sophos Firewall erkennt neue, komplett unbekannte Bedrohungen, bevor sie in Ihr Netzwerk gelangen.

Statische Machine-Learning-Analyse

Mit mehreren Machine-Learning-Modellen analysiert die statische Dateianalyse verschiedene Eigenschaften, Merkmale, das genetische Profil und Reputations-Elemente der Datei und gleicht sie mit Millionen bekannt unbedenklicher und schädlicher Dateien in der SophosLabs-Datenbank ab. So kann in Sekundenschnelle entschieden werden, ob eine bislang unbekannte Datei eine Bedrohung darstellt. Diese Methode ist sehr schnell und effizient beim Erkennen neuer Bedrohungen und neuer Varianten bekannter Bedrohungen. Sie eignet sich besonders gut für Bedrohungen, die sich nicht einfach an die Sandbox schicken lassen (z. B. passwortgeschützte Dateien, die Malware enthalten).

The screenshot shows the 'Feature analysis' section for a 'MALICIOUS' file. It lists specific features of the file and compares their frequency in bad files (red bars) versus good files (green bars). The features include hidden imports, compiler versions, hidden imports, Stack Canary status, and registry access.

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

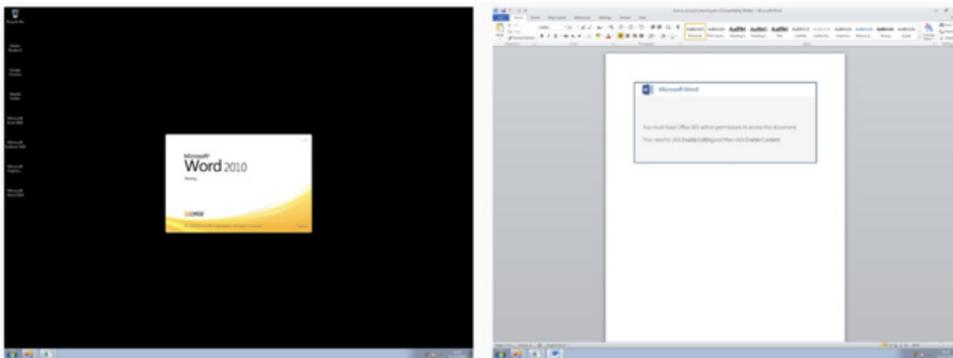
Verdächtige Dateien werden unter Verwendung mehrerer Machine-Learning-Modelle auf Zero-Day-Bedrohungen analysiert.

Dynamische Sandbox-Analyse während der Laufzeit

Sandbox-Technologie der ersten Generation war nur für sehr große Unternehmen erschwinglich. Dank der Einführung cloudbasierter Sandboxing-Lösungen wie Sophos Sandstorm wird die Technologie nun jedoch für Unternehmen jeder Größe erschwinglich. Erstmals erhalten kleine und mittlere Unternehmen eine Sandboxing-Lösung mit Deep-Learning-Technologie, die weit mehr kann, als die speziellen, vor Ort installierten Sandboxing-Lösungen, die noch vor wenigen Jahren von Großunternehmen für Millionenbeträge implementiert wurden.

Da die Analyse in der Cloud stattfindet, ist keine zusätzliche Hardware oder Software erforderlich und die Performance der Firewall wird nicht beeinträchtigt. Jede Datei, die laut Xstream DPI-Engine aktiven Code enthält, z. B. einen E-Mail-Anhang oder Web-Download, wird automatisch hochgeladen und parallel zur statischen Analyse (oben) in der Cloud-Sandbox von SophosLabs Intelix unter kontrollierten Bedingungen ausgeführt, um vor Eintritt ins Netzwerk das Laufzeitverhalten zu bestimmen.

Zur Identifizierung von Bedrohungen haben die SophosLabs die neuesten Schutztechnologien unseres branchenführenden Next-Gen-Endpoint-Produkts Intercept X in Sophos Sandstorm integriert, einschließlich Deep Learning, Exploit-Erkennung und CryptoGuard (zur Erkennung aktiver Ransomware-Verschlüsselungen von Dateien in Echtzeit). Hier werden auch alle Datei-, Speicher-, Registry- und Netzwerkaktivitäten auf Merkmale böswilliger Absichten überwacht, um zu entscheiden, ob diese schädlich oder unbedenklich sind. Keine andere Firewall bietet eine vergleichbare Laufzeitanalyse mit der marktweit führenden Threat Protection – Intercept X. Auch Transparenz und Reporting-Kapazitäten der Sophos Firewall (z. B. vollständige Screenshot-Serie zu den Ereignissen bei der Dateiausführung) sind branchenweit einzigartig.



Die Sandbox-Laufzeitanalyse führt Dateien zur Ermittlung ihres Verhaltens in einer sicheren Umgebung aus und stellt Ihnen Screenshots zur Prüfung zur Verfügung.

Sandboxing erweist sich insbesondere bei der Erkennung von Bedrohungen als effizient, die sich in normalerweise unbedenklichen Dateien ohne offensichtliche schädliche Eigenschaften verbergen, z. B. in

Office-Dateien mit Makros, gutartigen ausführbaren Dateien oder manipulierten Anwendungs-Updates.

Bedrohungsschutz-Reporting

Für jede von der Sophos Firewall analysierte Datei wird ein begleitender Report erstellt, der alle Details zu den Ergebnissen der verschiedenen Analysen und Bewertungen enthält. Der Report besteht aus sechs Elementen, darunter die verschiedenen Machine-Learning-Analysen, Datei-Reputation, Sandboxing und externe VirusTotal-Daten.

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 41b68b777b6fd365e72f1344ae29fcdf2f2e9af
SHA256 6f14a34560d2076523e95ae66b126d363d5552730459399a9cb3d9a4f2172086
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

Zentrale Regel-Verwaltung

Eine Firewall zu verwalten, ist oft alles andere als einfach. Mit einer Vielzahl von Regeln, Richtlinien und Sicherheitseinstellungen, die sich auf verschiedenste Funktionsbereiche erstrecken – nicht selten mit mehreren unterschiedlichen Regeln, die erforderlich sind, um den nötigen Schutz zu gewährleisten – gibt es eine Menge zu tun.

Bei der Konzeption der Sophos Firewall haben wir die Gliederung von Firewall-Regeln und die Verwaltung Ihres Sicherheitsstatus ganz neu überdacht, um beides noch besser zu gestalten. Anstatt in der Management-Konsole nach den geeigneten Richtlinien suchen zu müssen, haben wir die gesamte Verwaltung für Firewall-Regeln und deren Durchsetzung in einer zentralen Ansicht zusammengefasst. Ab sofort können Sie Ihre Firewall-Regeln an einem zentralen Ort anzeigen, filtern, suchen, bearbeiten, hinzufügen und organisieren.

The screenshot displays the 'Rules and policies' management console. At the top, there are tabs for 'Firewall rules', 'NAT rules', and 'SSL/TLS inspection rules'. Below these, there are filters for 'IPv4', 'IPv6', and 'Disable filter'. A table lists various rules with their details:

Rule type	#	Name	Source zone	Destination zone	Status	Rule ID	Action	Feature and service
2	2	FastPath VoIP Traf...	LAN, Any host	WAN, Goto/Webinar(HG), Goto/Meet...	Any service	#13	Accept	...
3	3	VPN Access	VPN, Any host, Mobile D...	Any zone, Any host	Any service	#9	Accept	...
8	8	Server Access and ...	Rules governing access to servers					
8	8	User Rules	Rules governing different user groups					
9	9	Risky Users	LAN, IoT, Any host, Joe, Jo...	WAN, Any host	Any service	#6	Accept	...
10	10	Server Admins	LAN, Any host, Server Ad...	WAN, Any host	Any service	#3	Accept	...
11	11	Computer Users	LAN, Any host, Computer	WAN, Any host	Any service	#4	Accept	...
12	12	Mobile Device Us...	LAN, Any host, Mobile De...	WAN, Any host	Any service	#5	Accept	...

Die Sophos Firewall kombiniert alle Ihre Regeln für Zugriffsrichtlinien, NAT und TLS Inspection in einer zentralen Ansicht und vereinfacht so die Verwaltung.

Regeln für Benutzer, Geschäftsanwendungen, NAT, TLS/SSL Inspection und Netzwerk können Sie gezielt die jeweils relevanten Richtlinien anzeigen lassen und die Verwaltung über eine praktische zentrale Ansicht erledigen.

Symbolanzeigen liefern wichtige Informationen über Richtlinien (z. B. Typ, Status, Durchsetzung usw.).

Verwaltung Ihres Sicherheitsstatus auf einen Blick

Ob über Ihr Sophos-Central-Konto in der Cloud oder über die Benutzeroberfläche der Sophos Firewall – mit Sophos wird es ganz einfach, die Konfiguration und Verwaltung von modernem Schutz über eine zentrale Konsole zu erledigen.

The screenshot shows the 'Security features' configuration page. Callouts point to the following features:

- Dualer Virenschutz**: Malware and content scanning (Scan HTTP and decrypted HTTPS, Detect zero-day threats with Sandstorm, Scan FTP for malware)
- Sandboxing**: Filtering common web ports (DPI engine or web proxy?)
- SSL Inspection**: Web proxy options (Decrypt HTTPS during web proxy filtering)
- Heartbeat**: Configure Synchronized Security Heartbeat (Minimum source HB permitted, Minimum destination HB permitted)
- App Control**: Identify and control applications (App control)
- QoS**: Shape traffic
- Priorisierung**: DSCP marking
- IPS**: Detect and prevent exploits (IPS)

Konfigurieren Sie Ihren kompletten Sicherheitsstatus mithilfe vordefinierter oder benutzerdefinierter Richtlinien in einer zentralen Ansicht.

Sie können Sicherheits- und Kontrollfunktionen für Antivirus, TLS/SSL Inspection, Sandboxing, IPS, Traffic Shaping, Web und Application Control, Security Heartbeat, NAT, Routing und Priorisierung an einem Ort einrichten und aktivieren – und zwar nach Regel, Benutzer oder Gruppe.

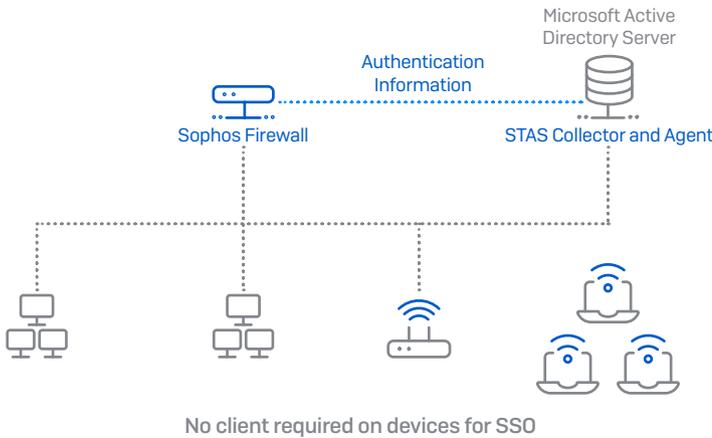
Und wenn Sie genau sehen möchten, was Ihre Richtlinien tun, oder Änderungen vornehmen möchten, können Sie dies direkt an Ort und Stelle erledigen, ohne die Firewall-Regel schließen oder in einen anderen Teil des Produkts wechseln zu müssen.

The screenshot shows the 'Edit web policy' configuration page. The table below lists the rules:

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

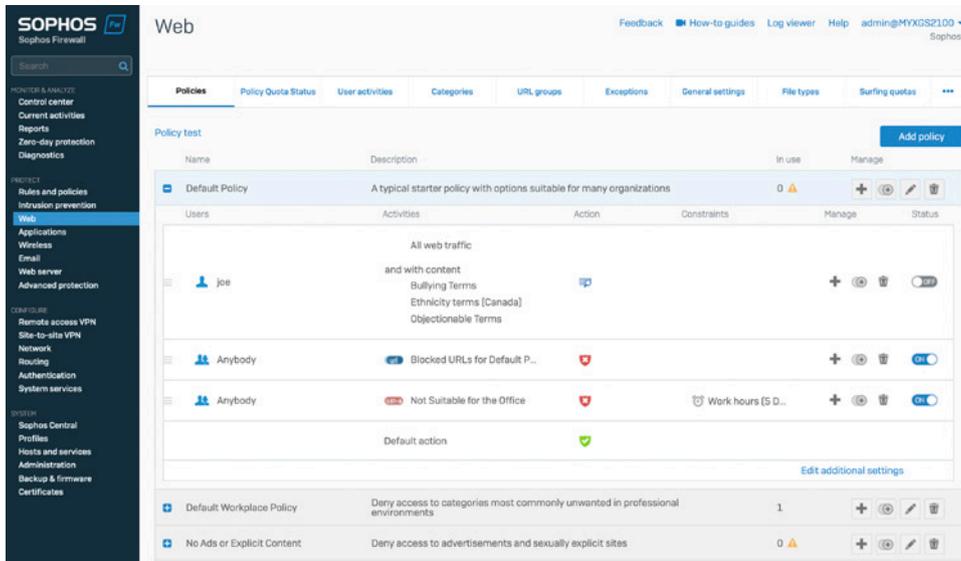
Sehen Sie alle Richtliniendetails auf einen Blick und nehmen Sie direkt in der Ansicht der Firewall-Regeln Änderungen vor.

Flexible Authentifizierungsoptionen ermöglichen Ihnen eine einfache Identifizierung und umfassen Verzeichnisdienste wie Active Directory, eDirectory, LDAP sowie NTLM, Kerberos, RADIUS, TACACS+, RSA, Client-Agenten oder Captive Portal. Zudem ermöglicht die Sophos Transparent Authentication Suite (STAS) eine Integration mit Verzeichnisdiensten wie Microsoft Active Directory für eine einfache, zuverlässige und transparente Single-Sign-On-Authentifizierung.



Secure Web Gateway der Enterprise-Klasse

Web-Schutz- und Kontrollfunktionen gehören bei Firewalls zwar zum Standard, werden in den meisten Firewall-Implementierungen jedoch stiefkindlich behandelt. Nicht so bei Sophos: Mit unserem Erfahrungsschatz bei der Entwicklung von Web-Protection-Lösungen der Enterprise-Klasse hatten wir die Basis und das notwendige Know-how zur Bereitstellung von Web-Richtlinienkontrollen, die normalerweise nur in zehnmal so teuren Enterprise-SWG(Secure Web Gateway)-Lösungen angeboten werden. Wir haben ein auf Vererbung basierendes Top-Down-Richtlinienmodell implementiert, mit dem die Einrichtung intelligenter Richtlinien einfach und intuitiv wird. Vorkonfigurierte Richtlinienvorlagen für die meisten üblichen Bereitstellungen sind bereits im Standard-Umfang enthalten – z. B. für typische Arbeitsumgebungen, Bildungseinrichtungen usw. So können Sie Ihre Compliance im Handumdrehen sicherstellen und bei Bedarf jederzeit weitere Anpassungen vornehmen.



Leistungsstarke Web-Richtlinien der Enterprise-Klasse bieten detaillierte Kontrollmöglichkeiten.

Wir wissen, dass Web-Richtlinien zu den am häufigsten geänderten Elementen in Ihrer Firewall gehören – deshalb haben wir viel Zeit investiert, um die Verwaltung und Anpassung dieser Richtlinien auf Basis Ihrer Benutzer- und Geschäftsanwendungen so einfach wie möglich zu gestalten. Sie können individuelle Richtlinien für Benutzer und Gruppen, Aktivitäten (kompromittierte URLs, Kategorien, Inhaltsfilter und Dateitypen) und Aktionen (blockieren, zulassen, warnen) definieren sowie Tageszeit-/Wochentag-Beschränkungen hinzufügen oder anzupassen.

Funktionen für Bildungseinrichtungen

Die Sophos Firewall bietet mehrere Funktionen, die sich ideal für Bildungseinrichtungen eignen, bei denen Web-Richtlinien und Compliance wichtige Anforderungen darstellen. Zu den spezifischen Funktionen für Bildungseinrichtungen gehören:

- Vorkonfigurierte Web-Richtlinien für Bildungseinrichtungen
- Inhaltsfilterung und Keyword-Reporting
- SafeSearch- und YouTube-Einstellungen für Einschränkungen auf Basis von Benutzer-/Gruppenrichtlinien
- Blockseiten-Überschreibungen, die von Lehrern verwaltet werden können
- Umfassendes integriertes Reporting zur frühzeitigen Erkennung potenzieller Probleme

Bei Web-Richtlinien besteht nun die Möglichkeit, mit Keyword-Listen übereinstimmende dynamische Inhalte zu protokollieren, zu überwachen und sogar diesbezügliche Richtlinien durchzusetzen. Diese Funktion eignet sich insbesondere für Bildungseinrichtungen, in denen der Kinder- und Jugendschutz sichergestellt werden muss. Außerdem kann festgestellt werden, ob Schüler Keywords nutzen, die mit Selbstverletzung, Mobbing, Radikalisierung oder anderweitig unangemessenen Themen in Zusammenhang stehen. Keyword Libraries können in die Firewall hochgeladen werden und lassen sich als zusätzliches Kriterium auf Web-Filter-Richtlinien anwenden, mit verschiedenen Maßnahmen (Protokollieren und Überwachen oder Blockieren von Suchergebnissen/Websites, die bestimmte Schlüsselwörter enthalten).

Aus umfassenden Reports sind Keyword-Übereinstimmungen und Benutzer ersichtlich, die nach bestimmten Keyword-Inhalten suchen oder diese nutzen. So kann bereits proaktiv interveniert werden, bevor ein riskantes Benutzerverhalten zum echten Problem wird.

Mit vorkonfigurierten Web-Richtlinien für Bildungseinrichtungen sorgt die Sophos Firewall für schnelle Compliance mit geltenden Vorschriften. Außerdem bietet sie flexible und leistungsstarke Kontrollen über SafeSearch- und YouTube-Beschränkungen auf Basis von Benutzer-/Gruppenrichtlinien. Lehrer können außerdem Erlaubnis erhalten, Richtlinien zu überschreiben und diese zu verwalten, damit ihre Klassenräume auf Websites zugreifen können, die im Rahmen des Lehrplans normalerweise blockiert würden.

Das Ergebnis sind einfache und gleichzeitig leistungsstarke Richtlinien für die Internet-Nutzung.

Vereinfachte NAT-Konfiguration

Jeder, der schon einmal versucht hat, NAT[Network Address Translation]-Regeln zu konfigurieren, weiß, dass man an dieser Aufgabe verzweifeln kann. Aber es geht auch anders: Die Sophos Firewall bietet umfassende NAT-Funktionen auf Enterprise-Niveau für leistungsstarke und flexible NAT-Konfigurationen, einschließlich Source NAT (SNAT) und Destination NAT (DNAT) in einer einzigen Regel mit granularen Auswahlkriterien. Um komplexe DNAT-Konfigurationen zu vereinfachen, führt Sie ein benutzerfreundlicher Assistent mit nur wenigen Klicks durch den Prozess der Erstellung einer vollständigen NAT-Konfiguration.

Administratoren können beim Erstellen einer Firewall-Regel auch die praktische Option „Verknüpfte NAT“ nutzen. Hiermit wird automatisch eine entsprechende NAT-Konfigurationsregel erstellt und der Zeitaufwand für die Erstellung und Konfiguration von NAT-Regeln weiter reduziert.

Server access assistant (DNAT)

Review your selection

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.

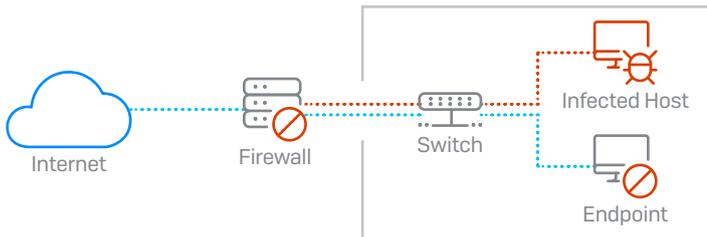
Cancel 5 of 5 Back Save and finish

Erstellen Sie mit dem leistungsstarken, intuitiven NAT-Regel-Assistenten und wenigen Klicks komplexe Zugriffskontrollen.

Automatische Reaktion auf Vorfälle

Eine der von Netzwerk-Administratoren am häufigsten gewünschten Firewall-Funktionen ist die Möglichkeit zur automatischen Reaktion auf Sicherheitsvorfälle im Netzwerk.

Die Sophos Firewall identifiziert als einzige Netzwerk-Security-Lösung die Quelle einer Infektion in Ihrem Netzwerk vollständig und beschränkt als Reaktion automatisch den Zugriff des infizierten Geräts auf andere Netzwerkressourcen. Ermöglicht wird dies durch unseren einzigartigen Sophos Security Heartbeat, der Telemetrie- und Statusdaten zwischen Sophos-verwalteten Endpoints und Ihrer Firewall austauscht.



Die Sophos Firewall und Security Heartbeat können infizierte Hosts in Ihrem Netzwerk automatisch isolieren.

Die Sophos Firewall integriert den Sicherheitsstatus verbundener Hosts auf völlig neuartige Weise in Ihre Firewall-Regeln, sodass Sie den Zugriff kompromittierter Systeme auf sensible Netzwerkressourcen bis zu ihrer vollständigen Bereinigung automatisch beschränken können.

Die Sophos Firewall kann nicht nur Endpoints vom Zugriff auf andere Teile des Netzwerks auf Firewall-Ebene isolieren, sondern auch die Hilfe aller nicht betroffenen Endpoints im Netzwerk in Anspruch nehmen, um einen kompromittierten Host auf Endpoint-Ebene weiter zu isolieren.

Diese von uns als Lateral Movement Protection bezeichnete Schutzfunktion Isoliert und verhindert, dass Bedrohungen oder Angreifer sich lateral durch Ihr Netzwerk auf andere Systeme fortbewegen, selbst wenn sie sich in demselben Netzwerksegment oder derselben Broadcast Domain befinden, wo die Firewall normalerweise nicht eingreifen kann. Auf diese Weise lassen sich aktive Angreifer in Ihrem Netzwerk sehr einfach und effektiv bekämpfen. Ermöglicht wird dies durch die Zusammenarbeit von Endpoints und Firewall im Rahmen eines koordinierten bzw. synchronisierten Abwehrsystems.

Security Heartbeat

Sophos Security Heartbeat tauscht über einen sicheren Kommunikationskanal Daten in Echtzeit zwischen Ihren Sophos-verwalteten Endpoints und der Sophos Firewall aus. Durch diese neuartige Synchronisierung von Sicherheitsprodukten, die bisher unabhängig voneinander operierten, erhalten Sie wirksameren Schutz vor komplexer Malware und gezielten Angriffen als je zuvor.

1 At Risk 1 Missing 1 Warnings 2 Connected

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

Der Security Heartbeat™-Status Ihres Netzwerk wird im Control Center angezeigt.

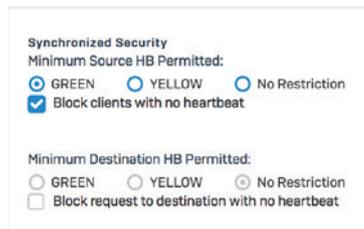
Security Heartbeat identifiziert komplexe Bedrohungen nicht nur unmittelbar, sondern kommuniziert auch wichtige Informationen über die Eigenschaften der Bedrohung, des Hostsystems und des Benutzers. Und vielleicht am wichtigsten: Dank Security Heartbeat können kompromittierte Systeme automatisch isoliert bzw. vom Zugriff auf bestimmte Ressourcen ausgeschlossen werden, bis sie frei von Malware sind. Security Heartbeat ist eine revolutionäre Technologie, die es IT-Sicherheitslösungen ermöglicht, komplexe Bedrohungen auf völlig neue Art zu identifizieren und zu bekämpfen.

Der Security Heartbeat für verwaltete Endpoints hinter Ihrer Firewall kann grün, gelb oder rot sein:

Ein grüner Heartbeat-Status gibt an, dass das Endpoint-Gerät sicherheitstechnisch unbedenklich ist und Zugriff auf alle verfügbaren Netzwerkressourcen erhält.

Ein gelber Heartbeat-Status warnt davor, dass auf einem Gerät eine potenziell unerwünschte Anwendung (PUA) oder ein anderes Problem vorhanden ist bzw. dass ein Gerät die Compliance nicht einhält. Sie können selbst entscheiden, auf welche Netzwerk-Ressourcen ein System mit gelbem Heartbeat bis zur Behebung des Problems zugreifen darf.

Ein roter Heartbeat-Status weist auf das Risiko hin, dass ein Gerät ggf. mit einer komplexen Bedrohung infiziert ist, die Call-Home-Versuche zu einem Botnet oder einem „Command-and-Control“-Server unternehmen könnte. Über die Security-Heartbeat-Richtlinieneinstellungen in Ihrer Firewall können Sie Systeme mit rotem Heartbeat-Status bis zur erfolgten Bereinigung einfach isolieren, um Datenverlusten und einer Infektionsausbreitung vorzubeugen.



[Legen Sie Security-Heartbeat-Anforderungen innerhalb von Firewall-Regeln fest.](#)

Sophos hat als einziger Anbieter eine Lösung wie den Security Heartbeat im Angebot und ist derzeit der einzige Leader sowohl im Bereich Endpoint- als auch Netzwerk-Security. Andere Anbieter werden sich bewusst, dass dies die Zukunft der IT-Security ist, und versuchen, eine ähnliche Technologie zu implementieren. Sie haben jedoch einen entscheidenden Nachteil: Sie können nicht gleichzeitig eine branchenführende Endpoint-Lösung und eine branchenführende Firewall-Lösung vorweisen, die sie integrieren könnten.

Willkommen in der „Zero Trust“-Welt

Vertrauen ist in der IT zum kontrovers diskutierten Thema geworden – besonders wenn dieses Vertrauen vorbehaltlos ist. Ein hermetisch abgeriegeltes Unternehmensnetzwerk, hinter dessen Mauern allem und jedem vertraut wird, hat sich als fehlerhaftes Design erwiesen.

Zero Trust ist ein ganzheitlicher Sicherheitsansatz, der dieser Entwicklung Rechnung trägt und darauf eingeht, wie Unternehmen arbeiten und auf Bedrohungen reagieren. Es ist ein Modell und eine Philosophie über die Herangehensweise an das Thema Sicherheit.

Nichts und niemandem darf automatisch vertraut werden, ob innerhalb oder außerhalb des Unternehmensnetzwerks. Ganz ohne Vertrauen geht es jedoch letztendlich nicht. Mit Zero Trust ist dieses Vertrauen temporär, ergibt sich aus mehreren Datenquellen und wird ständig neu bewertet.

Mit Zero Trust können wir unsere gesamte Infrastruktur kontrollieren – vom Büro bis hin zu den von uns verwendeten Cloud-Plattformen. Auch außerhalb der Unternehmensgrenzen ist die Kontrolle gewährleistet und Remote-Benutzer können genauso Zugriff erhalten wie Mitarbeiter im Büro.

Aber wie können Sie auf Zero Trust umstellen und alle damit verbundenen Vorteile nutzen? Niemand kann Zero Trust in einer einzigen Lösung anbieten. Sophos verfügt jedoch über ein breites Portfolio an Sicherheitstechnologien und -kontrollen, die Ihre Umstellung auf Zero Trust beschleunigen und vereinfachen.

Sophos Central: Die cloudbasierte Cybersecurity-Plattform, der weltweit die meisten Kunden vertrauen, stellt diese unterschiedlichen und sich ergänzenden Technologien in einer einzigen Cloud-Management-Konsole zur Verfügung, über den Sie Ihr Zero-Trust-Netzwerk organisieren und kontrollieren können.

Synchronized Security: Cybersicherheit, die kontinuierlich Informationen zwischen Endpoints, ZTNA, Firewall und anderen Systemen austauscht und damit für maximale Transparenz sorgt.

Sophos ZTNA: Bietet eine effektive Zero-Trust-Network-Access-Lösung, mit der Benutzer eine sichere Verbindung zu Anwendungen und Daten herstellen können.

Sophos Firewall: Erstellen Sie Segmente oder Mikroperimeter rund um Benutzer, Geräte, Anwendungen, Netzwerke etc.

Server Protection und Intercept X: Weisen Sie jedem Gerät einen Integritäts-Status zu, damit die Geräte im Falle einer Kompromittierung automatisch isoliert und vom Zugriff auf andere Geräte gesperrt werden können.

Managed Threat Response (MTR) Service: Kontrolliert alle Benutzeraktivitäten im Netzwerk und erkennt potenziell kompromittierte Zugangsdaten.

Optimierung Ihres SD-WAN-Netzwerks

Nur wenige Begriffe im Bereich Networking haben für so viel Wirbel gesorgt wie SD-WAN (oder Software Defined Networking in a Wide Area Network). Innerhalb der Diskussion finden sich zu gleichen Teilen nützliche Informationen und verwirrende Phrasen. Die Folge des Ganzen: SD-WAN bedeutet nicht für jeden das Gleiche, und einige fragen sich immer noch, was genau sich hinter der Bezeichnung „SD-WAN“ eigentlich verbirgt.

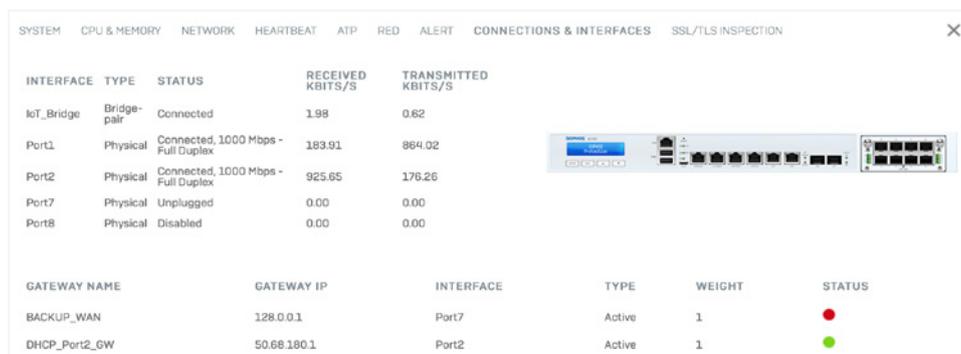
Kunden erhoffen sich von SD-WAN vor allem Folgendes für ihr Netzwerk:

- **Geringere Konnektivitätskosten:** Traditionelle MPLS(Multi-Protocol Label Switching)-Verbindungen sind teuer, weshalb Unternehmen vermehrt auf günstigere WAN-Optionen wie Kabel, DSL und 3G/4G/LTE zurückgreifen.
- **Geschäftskontinuität:** Unternehmen benötigen Lösungen, die im Falle von WAN-Ausfällen- oder Unterbrechungen Redundanz, Routing und Failover sowie eine Beibehaltung der Sitzung gewährleisten können.
- **Qualität kritischer Anwendungen:** Unternehmen möchten Datenverkehr und Performance von Anwendungen in Echtzeit sehen, um die Sitzungsqualität unternehmenskritischer Anwendungen aufrechterhalten zu können
- **Einfachere VPN-Orchestrierung für Zweigstellen:** Die standortübergreifende VPN-Orchestrierung ist oft kompliziert und zeitaufwändig. Daher sind Tools zum Vereinfachen und Automatisieren der Bereitstellung und Einrichtung so wichtig.

Die Sophos Firewall mit Xstream SD-WAN bietet Ihnen umfassende Optionen zur SD-WAN-Orchestrierung, -Verwaltung sowie zur Optimierung von Performance und Zuverlässigkeit, damit Sie selbst ehrgeizige SD-WAN-Ziele einfach und kostengünstig realisieren können.

Xstream SD-WAN

Das Anwendungsverkehr-Routing über mehrere WAN-Links zu verwalten, ist eines der Grundprinzipien von SD-WAN, und die Sophos Firewall mit Xstream SD-WAN bietet eine leistungsstarke und flexible Link-Management-Lösung – unabhängig davon, ob Sie mehrere MPLS-, DSL-, Kabel- oder Mobilfunkverbindungen nutzen.



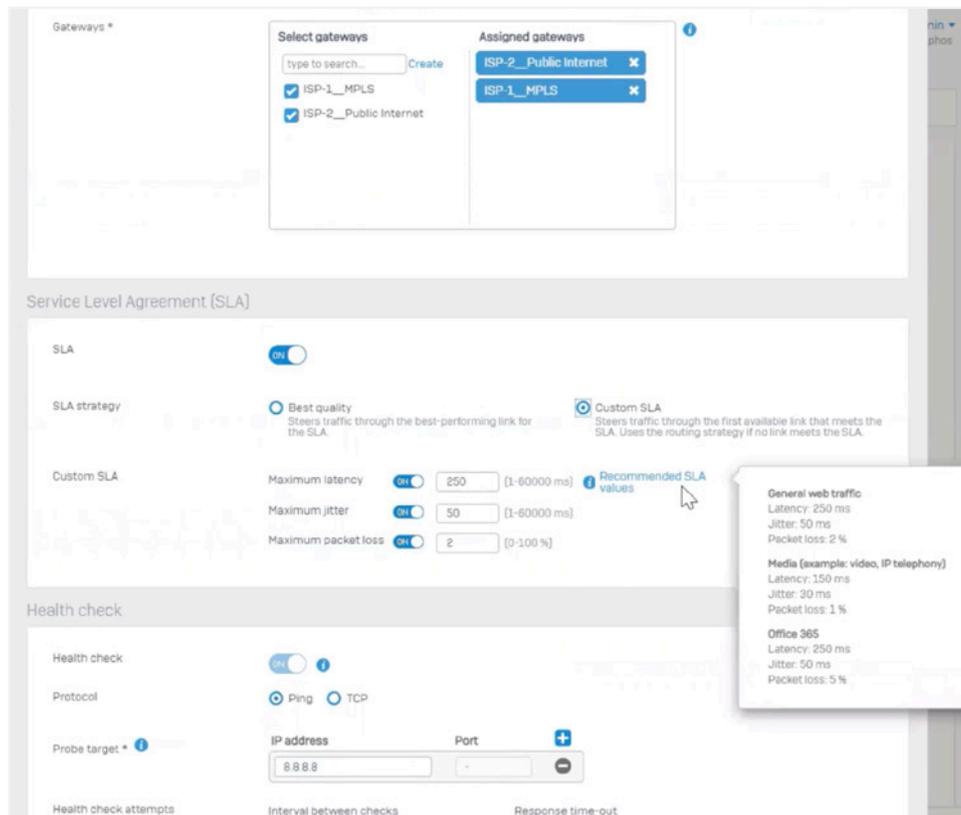
The screenshot displays the 'CONNECTIONS & INTERFACES' section of the Sophos Firewall dashboard. It features two tables: one for interface statistics and another for gateway configuration. An inset image shows a physical network switch with several ports lit up.

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	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	●
DHCP_Port2_GW	50.68.180.1	Port2	Active	1	●

Der WAN-Linkstatus (im unteren Bereich des Schnittstellenstatus-Widgets angezeigt) ist über das Dashboard verfügbar.

SD-WAN-Profilen eine Routing-Strategie für mehrere WAN-Link-Gateways. So lassen sich Anwendungsverbindungen auf Basis der WAN-Link-Performance nahtlos und effizient umleiten. Die Umschaltungen zwischen den Verbindungen erfolgt sofort – ohne Auswirkungen auf Anwendungssitzungen und ohne Unterbrechungen – und bietet selbst in besonders störungsanfälligen und instabilen ISP-Umgebungen nahtlose Kontinuität, Anwendungsleistung und ein optimales Nutzererlebnis.



Die Einrichtung Performance-basierter SD-WAN-Profilen ist intuitiv und einfach.

Dabei können die SD-WAN-Profil-Routingstrategien auf der ersten verfügbaren Verbindung oder der Performance basieren. Performance-Monitoring berücksichtigt unter anderem Störungen, Latenz und Paketverlust und unterstützt mehrere Prüfziele für PING- und TCP-Tests.

SD-WAN-Profilen können auf Basis der Performance oder benutzerdefinierter SLA-Richtlinien automatisch die beste Verbindung auswählen. In den SLA-Richtlinien können Ihre Kunden Höchstwerte zu Störungen, Latenz und Paketverlust festlegen, die vor der Umleitung zu einer besseren Verbindung ganz ohne Beeinträchtigung aktiver Verbindungen erreicht werden dürfen.

Die Überwachung der Performance Ihres SD-WAN-Netzwerks ist mit Echtzeit- und Verlaufsdiagrammen für Latenz, Störungen und Paketverlust einfach und unkompliziert. Dabei lassen sich Daten der letzten 24 oder 48 Stunden, der letzten Woche, des letzten Monats sowie Echtzeit-Daten abrufen. Eine erweiterte Protokollierung von SD-WAN-Performance und -Routing ist ebenfalls enthalten.



Überwachen Sie die Performance Ihrer verschiedenen WAN-Links in Echtzeit.

Xstream-FastPath-Beschleunigung von SD-WAN-VPN-Datenverkehr

Die Sophos Firewall nutzt die integrierten Xstream-Flow-Prozessoren in den Appliances der XGS-Serie zur Hardware-Beschleunigung von IPsec-VPN-Tunnelverkehr. Dies führt zu einer erheblichen Steigerung der Performance: Die Xstream-Flow-Prozessoren übernehmen rechenintensive Aufgaben, die für IPsec-Tunnel erforderlich sind (z. B. ESP-Kapselung/-Verschlüsselung und ESP-Entkapselung/-Entschlüsselung). Diese neue Funktion nutzt die Hardware-Crypto-Funktionen des Xstream-Flow-Prozessors optimal aus und setzt so CPU-Ressourcen für andere wichtige Funktionen frei, wie Deep Packet Inspection. Xstream-FastPath-Beschleunigung für IPsec-Datenverkehr funktioniert sowohl für Site-to-Site- als auch für Remote-Access-VPN-Datenverkehr.

The screenshot displays the configuration interface for a WAN link manager. The top navigation bar includes tabs for interfaces, Zones, WAN link manager (selected), DNS, DHCP, IPv6 router advertisement, Cellular WAN, IP tunnels, Neighbors (ARP-NDP), and Dynamic DNS. The main content area is titled 'Gateway detail' and contains the following fields:

- 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

Below the gateway details is the 'Failover rules' section. It shows a rule configuration with the following conditions:

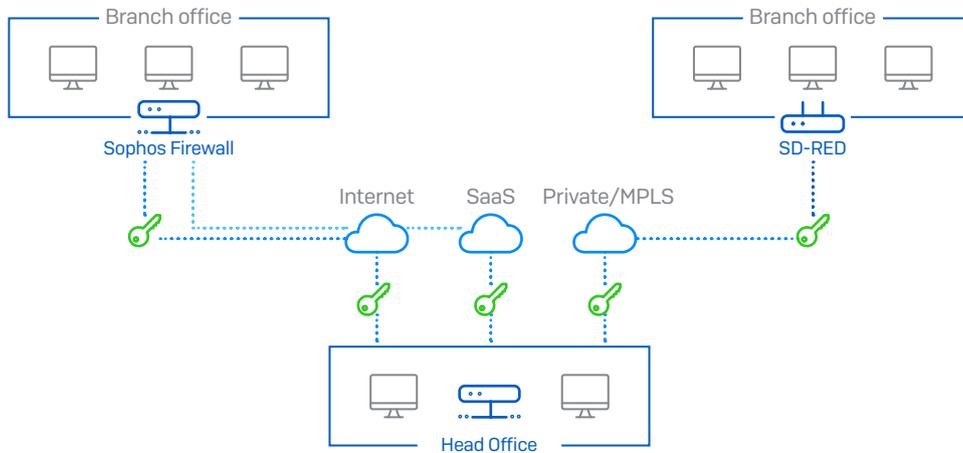
- If ...
- Not able to Connect: PING Port * on IP address 50.68.180.1 AND
- Not able to Connect: TCP Port * on IP address *

The action for this rule is: "SHIFT to another available gateway".

WAN-Link-Management in der Sophos Firewall, inklusive Balancing- und Failover-Regeln.

SD-Anbindung von Zweigstellen

Dank unserer SD-RED-Geräte sind wir Vorreiter bei der Zero-Touch-Bereitstellung und -Anbindung von Zweigstellen. Unsere erschwinglichen Geräte lassen sich ganz einfach ohne Techniker einrichten und stellen einen robusten, sicheren Layer-2-Tunnel zwischen dem Gerät und einer zentralen Firewall her.



Die Sophos Firewall und SD-RED-Geräte bieten Tunneloptionen, mit denen sich Zweigstellen komfortabel und erschwinglich per SD-WAN anbinden lassen.



Sophos SD-RED-Geräte bieten eine erschwingliche Zero-Touch-Lösung für die Zweigstellen-Anbindung per SD-WAN.

Die Bereitstellung von SD-RED-Geräten könnte nicht einfacher sein: Sie müssen nur die Seriennummer des Geräts in Ihrer Firewall vermerken und das Gerät an die Zweigstelle senden. Nach Anschluss des Geräts in der Zweigstelle verbindet es sich mit unserem cloudbasierten Einrichtungsservice und stellt automatisch eine sichere Tunnelverbindung zu Ihrer Sophos Firewall her. Dafür sind keinerlei technische Kenntnisse erforderlich.

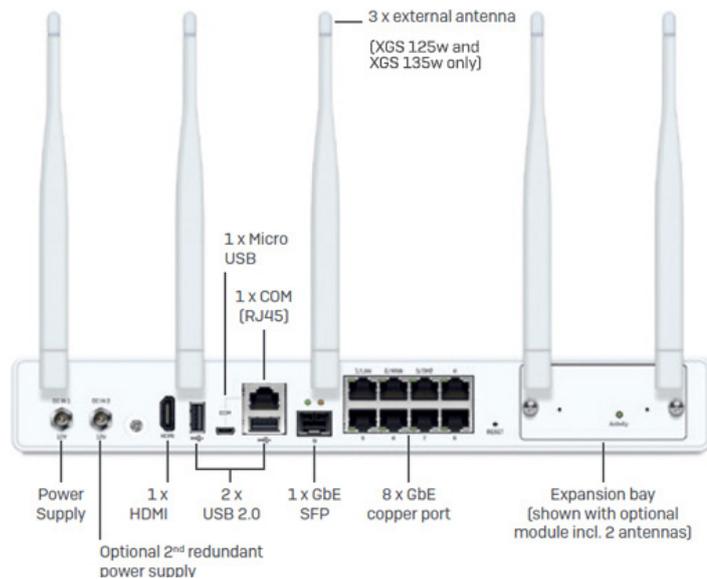
The screenshot shows the configuration page for SD-RED in the Sophos Firewall management console. The top navigation bar includes tabs for various settings like Interfaces, Zones, WAN link manager, DNS, DHCP, IPv6 router advertisement, Cellular WAN, IP tunnels, Neighbors (ARP-NDP), and Dynamic DNS. The main content area is titled 'RED settings' and is organized into three sections:

- RED settings:** Contains fields for 'Branch name *', 'Type' (set to RED 15), 'RED ID *', 'Tunnel ID *' (set to Automatic), 'Unlock code *', 'Firewall IP/hostname *', '2nd firewall IP/hostname', 'Use 2nd IP/hostname for' (with radio buttons for Failover and Load balancing), 'Description', and 'Device deployment' (with radio buttons for Automatically via provisioning service and Manually via USB stick).
- Uplink settings:** Contains 'Uplink connection' (with radio buttons for DHCP and Static) and '3G/UMTS failover' (with an unchecked 'Enable' checkbox).
- RED network settings:** Contains 'RED operation mode' (with radio buttons for Standard/unified, Standard/split, and Transparent/split), 'RED IP *', 'RED netmask' (set to /24 [255.255.255.0]), 'Zone' (set to LAN), 'Configure DHCP' (with a toggle switch set to ON), 'RED DHCP range' (with two empty input fields), 'MAC filtering type' (displaying 'No configured MAC address lists found'), 'Tunnel compression' (with an unchecked 'Enable' checkbox), and 'RED MTU' (set to 1500, with a range of 576 to 1500).

At the bottom of the configuration area, there are 'Save' and 'Cancel' buttons.

Sophos SD-RED ermöglicht eine flexible, sichere und erschwingliche Anbindung von Zweigstellen per SD-WAN.

Unsere XGS Series Desktop Appliances eignen sich ebenfalls ideal als SD-WAN-Konnektivitäts-Lösungen für Zweigstellen. Sie bieten flexible Konnektivitäts-Optionen wie VDSL und Wireless als Ergänzung zu Kupfer- und Glasfaserschnittstellen und unterstützen unsere robusten SD-RED-Tunnel.



Ausgewählte Desktop-Modelle, wie die hier angezeigte XGS 135w, bieten LTE-/Wireless-, VDSL-, Kupfer- und Glasfaser-WAN-Verbindungsoptionen.

VPN-Unterstützung und -Orchestrierung

Haben Sie schon einmal mehrere VPN-Tunnel zwischen unterschiedlichen Firewalls eingerichtet? Dann wissen Sie bestimmt, wie zeitaufwändig und kompliziert diese Aufgabe sein kann. Die Sophos Firewall unterstützt eine umfassende SD-WAN-Orchestrierung in Sophos Central. Sie können also mehrere Tunnel zwischen diversen Firewalls schnell und einfach vernetzen.

Wählen Sie einfach die verwalteten Firewalls aus, die Sie in die SD-WAN-Verbindungsgruppe aufnehmen möchten, und geben Sie an, auf welche Netzwerkressourcen alle Standorte zugreifen sollen – und schon ist Ihr SD-WAN-Overlay-Netz fertig. Alle erforderlichen Firewall-Zugriffsregeln und Tunnel (einschließlich Redundanz) werden automatisch für Sie erstellt.

Connection group	Status	# of firewalls	# of shared resources	Description
▼ Core_VPN	Good	3 (1 Resource sharing firewall)	1 (1 TCP/UDP)	
C242753M7W0F5H	Good	1 Remote firewall	1 Local network	Initiator
C242753M7W500C	Good	2 Remote firewalls	1 Local network, Sharing 1 TCP/UDP	Responder
X23001F9W8C0CA8	Good	1 Remote firewall	5 Local networks	Initiator
▼ VPN_to_int	Good	1 (0 Resource sharing firewalls)	0	

Richten Sie mit wenigen Klicks schnell komplexe SD-WAN-Overlay-Netzwerke ein und überwachen Sie diese über Sophos Central.

Sie können ein Full-Mesh-Netzwerk, eine Hub-and-Spoke-Topologie oder ähnliche Infrastrukturen einrichten, und Sophos Central konfiguriert automatisch den erforderlichen Tunnel- und Firewall-Zugriff für Ihr SD-WAN-Overlay-Netz auf dem Backend.

Die Sophos Firewall unterstützt alle Standard-Site-to-Site-VPN-Optionen, einschließlich IPsec und SSL. Wir bieten sogar unseren eigenen einzigartigen SD-RED-Layer-2-Tunnel mit Routing an, der in Situationen mit hoher Latenz, z. B. über Satellitenverbindungen, äußerst robust und zuverlässig ist.

Transparenz über Anwendungen und Routing

Anwendungspfad-Auswahl und -Routing spielen für das Erreichen von SD-WAN-Zielen ebenfalls eine große Rolle, da sie für unternehmenskritische Anwendungen wie VoIP die Qualität gewährleisten und die Latenz minimieren.

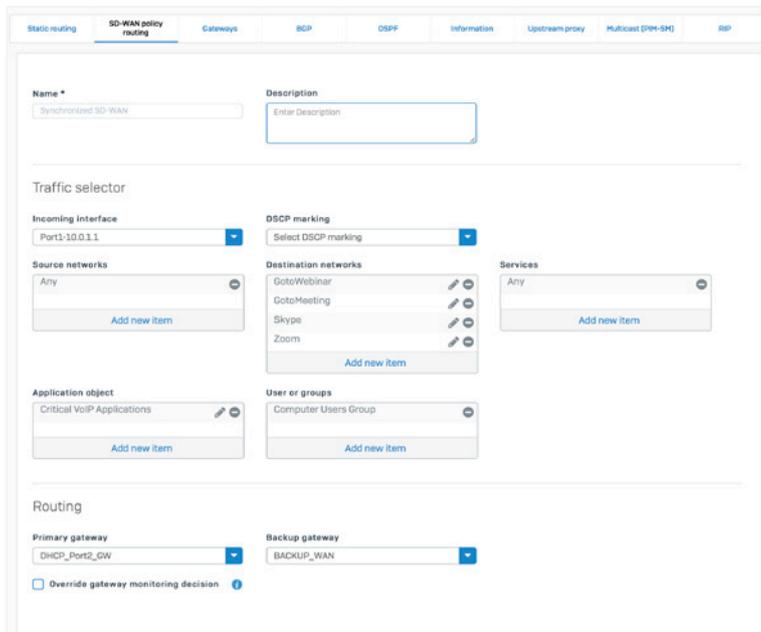
Natürlich lässt sich nur das routen, was auch erkannt wird. Aus diesem Grund sind eine verlässliche Identifizierung von Anwendungen und Transparenz entscheidend. Hier bieten die Sophos Firewall und Sophos Synchronized Security enorme Vorteile. Synchronized Application Control liefert 100%ige Transparenz über alle Anwendungen im Netzwerk und erleichtert so die Identifizierung unternehmenskritischer, verschleierte und benutzerdefinierter Anwendungen.

Synchronized SD-WAN, eine Funktion von Synchronized Security, bietet weitere Vorteile für das SD-WAN-Anwendungs-Routing. Synchronized SD-WAN macht sich den Umstand zunutze, dass Anwendungen durch den Austausch synchronisierter Application-Control-Daten zwischen mit Sophos verwalteten Endpoints und der Sophos Firewall eindeutig und zuverlässig bestimmt werden können. Jetzt lassen sich auch bisher nicht identifizierte Anwendungen zu den SD-WAN-Routing-Richtlinien hinzufügen. Kunden profitieren so von einer Application-Routing-Kontrolle und -Zuverlässigkeit, bei der andere Firewalls nicht mithalten können.

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

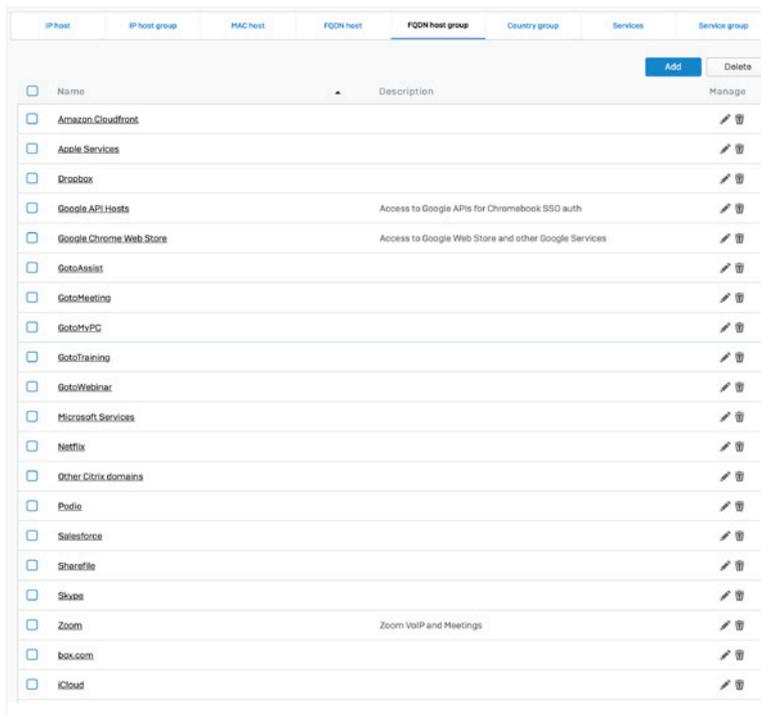
Synchronized Application Control erkennt alle Anwendungen im Netzwerk, wodurch sich unternehmenskritische Anwendungen einfacher priorisieren und routen lassen.

Darüber hinaus ermöglicht die Sophos Firewall anwendungs-basiertes Routing und Pfadauswahl in jeder Firewall-Regel, auch nach Benutzer und Gruppe. Mit richtlinienbasierten Routing-Kontrollen können Sie das Routing entweder über die primäre oder die Backup-Gateway-WAN-Verbindung definieren und für eine Replay-Ausrichtung konfigurieren. In Kombination sorgen diese Funktionen dafür, dass wichtiger Anwendungsverkehr einfach über die optimale WAN-Schnittstelle geleitet werden kann.



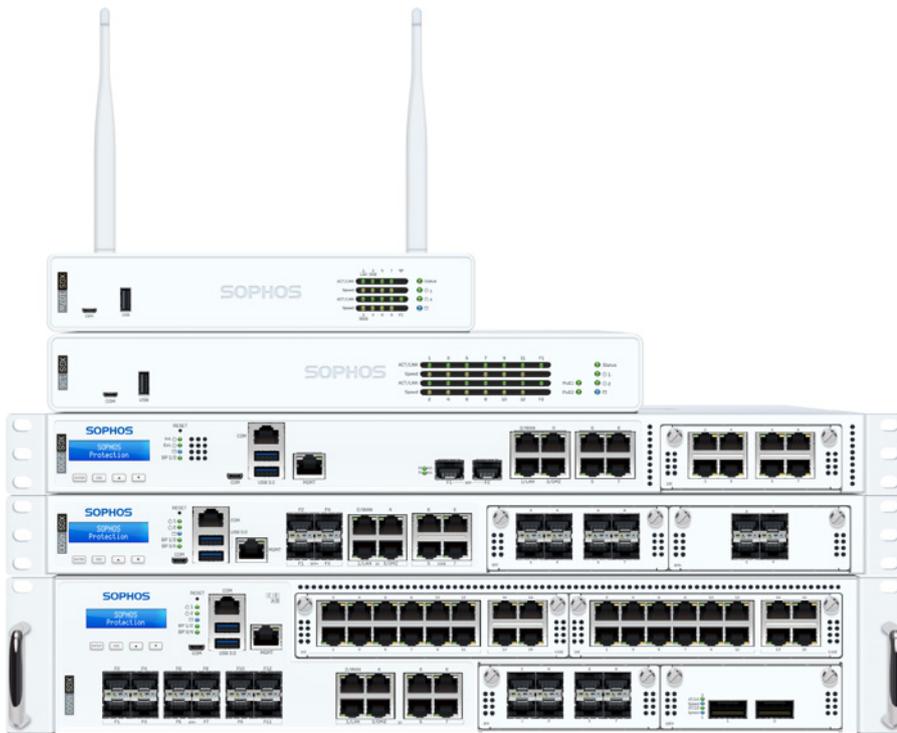
Richtlinienbasiertes SD-WAN-Routing bietet flexible Tools zum Routen von kritischem Anwendungsdatenverkehr.

Die Sophos Firewall enthält zudem vollständig qualifizierte Domain-Name[FQDN]-Objekte für gängige SaaS-Cloud-Dienste und wird mit Tausenden FQDN-Host-Definitionen ausgeliefert, die sich ganz einfach erweitern lassen.



Vordefinierte FQDN-Host-Objekte erleichtern die Pfadauswahl und anwendungsbasierendes Routing.

Einfaches Hinzufügen der Sophos Firewall zu jedem beliebigen Netzwerk



Die Hardware Appliances der Sophos-Firewall-Serie lassen sich flexibel bereitstellen und alle 1U-Modelle sind standardmäßig mit Fail-Open Bypass Ports ausgestattet. Diese sind auch in den Flexi-Port-Modulen verfügbar, sodass dieses Feature auch auf unseren 2U Appliances genutzt werden kann. Die neuen Bypass Ports ermöglichen eine Installation der Sophos Firewall im Bridge-Modus inline mit bestehenden Firewalls. Wenn die Sophos Firewall heruntergefahren oder neu gestartet werden muss, um die Firmware zu aktualisieren, sorgen die Bypass Ports für Geschäftskontinuität, da der Datenverkehr weiter fließt und der Betrieb des Netzwerks nicht unterbrochen wird. Dieses Feature eröffnet neue Bereitstellungsmöglichkeiten, die komplett risikofrei sind – ganz ohne Änderungen der bestehenden Netzwerk-Infrastruktur. Außerdem kann unsere Next-Gen Endpoint Protection Lösung Intercept X gemeinsam mit jedem bestehenden Desktop-Antivirus-Produkt ausgeführt werden. Eine komplette Sophos Synchronized Security Lösung kann also in jedem Netzwerk ohne weitere Änderungen der Infrastruktur bereitgestellt werden.

Sophos Firewall: Sie erhalten einfache und zuverlässige Cybersecurity.

Preisfrage

Stellen Sie jetzt eine unverbindliche Preisfrage und holen Sie Ihr persönliches Angebot ein:
sophos.de/firewall-quote

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de