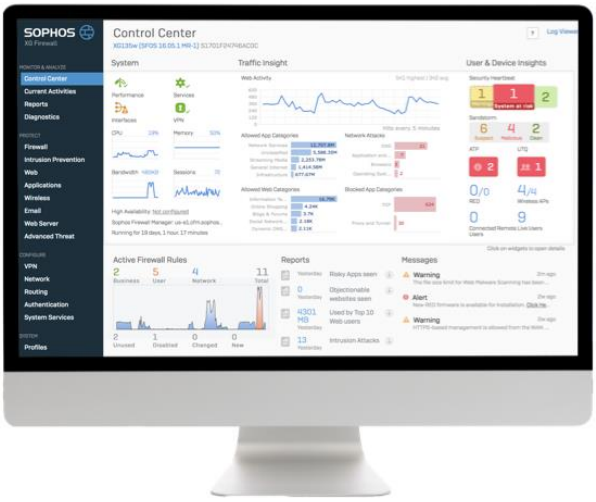
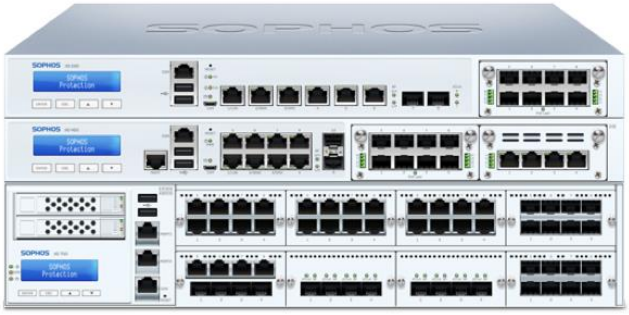
SOPHOS
Security made simple.

XG Firewall

Was ist neu in v17?





Einrichtung, Control Center und Navigation

Setup-Assistent

Im Rahmen eines Maintenance Release wurde ein neuer Setup-Assistent eingeführt, der eine schnelle und einfache Ersteinrichtung ermöglicht. Außerdem ist es jetzt möglich, die Lizenzregistrierung bei der Ersteinrichtung zu umgehen, um den Vorgang effizienter zu gestalten. Der Assistent wurde mit besonderem Augenmerk auf maximalen Komfort für neue XG-Firewall-Kunden entwickelt, kommt ohne Dokumentation aus und ermöglicht versierten Benutzern eine besonders schnelle und effiziente Einrichtung. Im Rahmen des Setup-Vorgangs besteht außerdem die Möglichkeit, die Firmware auf den aktuellen Release upzudaten. So wird sichergestellt, dass Kunden bei der Bereitstellung über die neueste Firmware verfügen.

Synchronized App Control Widget

Dieses neue Widget im Control Center gehört zum neuen Feature Synchronized App Control und informiert auf einen Blick über unidentifizierte Anwendungen.

How-to Guides

Im Rahmen eines Maintenance Release haben wir eine neue Option eingeführt: Sie bietet im oberen Bereich aller Bildschirmansichten über einen Klick Zugriff auf die How-To-Library der XG Firewall mit Videos und Guides zu den wichtigsten Aufgaben in der XG Firewall.

Sicherheit und Kontrolle

Synchronized App Control

Synchronized App Control setzt bei der Netzwerktransparenz neue Standards. Dieses Feature kann bislang unbekannte Anwendungen, die im Netzwerk aktiv sind, mittels Synchronized Security identifizieren, klassifizieren und kontrollieren. Außerdem kann Synchronized App Control Informationen vom Endpoint über Anwendungen anfordern, die keine Signaturen haben oder generische HTTP- oder HTTPS-Verbindungen nutzen. Hierdurch wird ein gravierendes Problem gelöst, mit dem signaturbasierte App-Control-Funktionen aller heutigen Firewalls zu kämpfen haben: Viele Anwendungen werden als „unbekannt", „nicht klassifiziert", „generisches HTTP", „SSL" usw. klassifiziert.

Die XG Firewall kann nun alle auf Sophos Endpoints genutzten Anwendungen eindeutig identifizieren. Wo es möglich ist, klassifiziert die XG Firewall die Anwendung automatisch und kontrolliert diese mit bestehenden App-Control-Richtlinien. Administratoren können erkannten Anwendungen zudem manuelle Kategorien zuweisen, sodass die App-Control-Durchsetzung die Anwendung wie gewünscht blockieren oder priorisieren kann. Erkannte Anwendungen können auch direkt zu bestehenden App-Control-Richtlinien hinzugefügt werden.

Außerdem bietet ein komplett interaktives Drill-Down Reporting zu Synchronized Applications Informationen darüber, wie Anwendungen identifiziert werden, unter welche Kategorien sie fallen und welche Anwendungen genau genutzt werden – nach Benutzer, Host, Bestimmungsland, Richtlinie und mehr.

Web Keyword Monitoring und Durchsetzung

Bei Web-Richtlinien besteht nun die Möglichkeit, mit Keyword-Listen übereinstimmende Inhalte zu protokollieren und zu überwachen oder 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.

Verbesserte IPS-Richtlinien und Smart-Filter

Die Erstellung benutzerdefinierter IPS-Richtlinien wurde mit einem leistungsstarken, intuitiven neuen Richtlinien-Editor deutlich verbessert. Gewünschte IPS-Muster können nun schnell und einfach nach Kategorie, Schweregrad, Plattform und Zieltyp ausgewählt werden. Außerdem werden permanente Smart-Filter-Listen unterstützt. Diese werden beim Hinzufügen neuer Muster, die mit den ausgewählten Kriterien übereinstimmen, automatisch aktualisiert.

Eine IPS-Richtlinie speziell zum Schutz von Linux-Servern und -Geräten kann beispielsweise einfach durch Auswahl von „Linux" als „Plattform" erstellt werden. Wenn anschließend neue Muster zum Schutz

vor neu aufgedeckten Schwachstellen in Linux hinzugefügt werden, schützt die Firewall automatisch vor diesen.

Verbesserte App-Control-Richtlinien und Smart-Filter

Parallel zu den oben genannten Verbesserungen bei IPS-Richtlinien wurden auch die benutzerdefinierten App-Control-Richtlinien entscheidend verbessert. Ein leistungsstarker, intuitiver neuer Richtlinien-Editor ermöglicht eine schnelle und einfache Auswahl von Anwendungen nach Kategorie, Risiko, Eigenschaften und Technologie. Außerdem werden permanente Smart-Filter-Listen unterstützt. Diese werden beim Hinzufügen neuer Anwendungen, die mit den ausgewählten Kriterien übereinstimmen, automatisch aktualisiert.

Eine App-Control-Richtlinie speziell zum Blockieren von Peer-to-Peer-File-Sharing-Anwendungen kann beispielsweise einfach durch Auswahl von „P2P“ als „Kategorie“ erstellt werden. Werden anschließend neue BitTorrent- oder andere Peer-to-Peer-Anwendungen zu dieser Kategorie hinzugefügt, setzt die Firewall automatisch die Richtlinien für diese neuen Anwendungen durch.

Verbesserte Web-Filterung

Im Rahmen der Web Protection gibt es nun eine Option zum Blockieren von Downloads potenziell unerwünschter Anwendungen.

Die SafeSearch-Durchsetzung wurde für Bing, Google und YouTube (eingeschränkter Modus) um einen DNS-Durchsetzungsmechanismus erweitert, der nun selbst dann eine Durchsetzung während SSL-verschlüsselter Browser-Sitzungen ermöglicht, wenn HTTPS nicht entschlüsselt wird.

Blockierungsseiten für Enduser verfügen über ein neues Design und mehr Details, sodass Benutzer und Administratoren besser verstehen, warum bestimmte Inhalte blockiert wurden.

Verbesserungen bei Streaming-Medien

Streaming-Medien-Anwendungen, die bei Aktivierung von Antivirus-Scans zu Problemen führen konnten, werden nun intelligenter gehandhabt, wodurch die Unterstützung von Services zum Streamen von Audio und Video verbessert wird.

Verwaltung und Problembehebung

Verwaltung von Firewall-Regeln

Die Verwaltung von Firewall-Regeln ist in v17 noch leistungsstärker und effizienter, sodass die Arbeit mit ihnen insbesondere in Umgebungen mit vielen Firewall-Regeln noch einfacher wird.

Firewall-Regeln sind nun kompakter und bieten trotzdem mehr Informationen auf einen Blick – mehr als doppelt so viele Regeln können gemeinsam angezeigt werden und die Eigenschaften einzelner Regeln sind einfacher zu erkennen. Regeln können zudem in Gruppen zusammengefasst sowie auf- und zugeklappt und als einzelnes Objekt verschoben werden.

Jede Regel gibt einen kompletten Überblick über den Ursprung, das Ziel, Service-Details sowie über die für sie geltenden Sicherheits- und Durchsetzungsfunktionen. Ein Mouse-over-Popup-Fenster liefert noch mehr Informationen, u. a. grundlegende Anweisungen zur Bearbeitung von Regeln, zum Verschieben von Regeln und zur Erstellung von Gruppen.

Gruppen können über das Menü „Aktion“ einfach erstellt werden und verfügen über Namen und Beschreibung. Weitere Regeln können bei ihrer Erstellung zu Gruppen hinzugefügt werden oder, im Falle von bereits bestehenden Regeln, durch Auswahl der Gruppe im Menü „Aktion“. Per Drag und Drop lassen sich Gruppen in der Regelliste einfach nach oben oder unten verschieben.

Filter- und Suchanfragen werden vollständig unterstützt und Ergebnisse werden so aufbereitet, dass die Gruppenstruktur erhalten bleibt.

Unified Log Viewer und detaillierte Protokolle

Verbesserungen des Log Viewers und der Protokollierung sind geplant und kommen voraussichtlich im nächsten Release.

Testsimulator für Firewall-Regeln und Richtlinien

Ein komplett neues Feature in der XG Firewall v17 ist der neue Testsimulator für Firewall-Regeln und Richtlinien. Dieser ermöglicht eine sofortige und komfortable Simulation von Firewall-Regeln und Web-Filter-Richtlinien auf Basis des Benutzers, Protokolls, Ursprungs, Ziels und der Tageszeit. Mit diesem Tool lässt sich schnell und einfach feststellen, ob eine Richtlinie oder Regel wie erwartet funktioniert. Außerdem ist der Testsimulator im Falle einer unerwarteten Blockierung von Benutzern oder Datenverkehr ein nützliches Tool zur Problembehebung.

Aus den Ergebnissen des Richtlinien- oder Regelsimulationstest geht hervor, ob der Datenverkehr erlaubt oder blockiert wird und welche Regel oder Web-Richtlinie für den Datenverkehr gilt.

Reporting

Synchronized Applications Report

Dieser Report liefert komplette historische Berichtdaten zu allen Anwendungen, die von der Synchronized App Control identifiziert wurden – mit Details zu Anwendungsklassifizierungen, Benutzern, Hosts, Richtlinien und Bestimmungsländern.

Web Keyword Content Report

Identifiziert Benutzer, die bestimmte Keywords eingegeben haben, damit Sie Präventivmaßnahmen ergreifen können, bevor ein potenzielles Problem zum echten Problem wird.

Security Audit Report (SAR)

Dieser Report ist Teil einer Discover-Modus-Bereitstellung (TAP-Modus) und umfasst nun einen Report über von Synchronized App Control erkannte Anwendungen sowie weitere Details zur Client-Integrität und zum Security Heartbeat.

Planung von Reports

Für geplante Reports sind nun Optionen für Reporting-Zeiträume –„vorheriger Tag“ oder aktueller Tag „seit Mitternacht“ – verfügbar.

Networking und VPN

IKEv2-Unterstützung

Für eine bessere Kompatibilität mit anderen Systemen unterstützen IPSec-VPN-Verbindungen nun Internet Key Exchange (IKE) v2. Ein IKEv2-IPsec-Profil ist bereits standardmäßig enthalten und ermöglicht ein einfaches Setup von IKEv2-IPsec-VPN-Verbindungen.

Verbesserungen der Benutzeroberfläche im Bereich VPN

Die Ansichten zur IPsec-Profilkonfiguration und zur IPsec-Verbindungseinrichtung wurden intuitiver gestaltet. Außerdem machen automatische Feldprüfungen die Einrichtung effizienter und reduzieren die Fehlerquote.

Wildcard-Unterstützung für Domain-Name-Host-Objekte

Vollständig qualifizierte Domain-Name(FQDN)-Host-Objekte unterstützen nun Wildcards, wodurch die Objekte deutlich leistungsstärker werden. Darüber hinaus ist bereits eine Reihe beliebter Cloud-Service-Host-Objekte vollständig vordefiniert und kann einfach auf Firewall-Regeln und Web-Richtlinien angewendet werden.

Verbesserte NAT-Regeln

Geschäftsregeln sind nun vollständig objektbasiert und unterstützen die Weiterleitung mehrerer Ports und Services in einer einzigen Regel. Beispielsweise können Sie nun RDP, Web und VoIP an einen einzigen Server in einer einzigen Geschäftsanwendungsregel weiterleiten. So sind weniger Regeln zur Unterstützung derselben Services erforderlich und eingehende NAT-Regeln werden viel intuitiver.

Email Protection

Smart Host

Ausgehende Smart Host Relays steigern die Verlässlichkeit Ihrer E-Mail-Zustellung und geben Ihnen die Möglichkeit, E-Mails nicht direkt an den Server des Empfängers, sondern über eine Reihe von alternativen Servern (Smart Host) zu routen. Perfekt für komplexere Umgebungen und wenn E-Mails nicht direkt über das Sophos Gateway geroutet werden.

Greylisting

Mit Greylisting lässt sich mehr Spam am Gateway blockieren. Da die meisten Spam-Nachrichten und Viren nur einen Zustellungsversuch unternehmen, verweigert Greylisting den ersten Versuch temporär und teilt dem sendenden E-Mail-Server mit, es erneut zu versuchen. Beim nächsten Versuch wird die Nachricht akzeptiert und wie gewohnt gescannt. Wenn ein E-Mail-Server diesen Test oft genug besteht, wird er automatisch in die Whitelist aufgenommen. Alternativ kann der Administrator die Whitelist-Datensätze manuell aktualisieren oder integrierte Voreinstellungen für häufige Absender verwenden.

Empfängerverifizierung

Durch diese Funktion wird die E-Mail-Verarbeitung der XG Firewall entlastet und Absender (einschließlich Kunden und Sophos-Partner) werden sofort informiert, wenn sie eine E-Mail-Adresse falsch eingegeben haben. Mittels Empfängerverifizierung kann die XG Firewall beim Verzeichnisdienst des Empfängers über

SMTP abfragen, ob ein gültiger Posteingang existiert. Wenn dies der Fall ist, wird die Nachricht wie gewohnt auf Spam und Viren überprüft. Wenn nicht, wird die E-Mail abgelehnt und der Absender wird darüber informiert, dass die Zustellung fehlgeschlagen ist.

Synchronized Security

Synchronized Security in Discover (TAP)-Modus-Bereitstellungen

Die XG Firewall unterstützt bei einer Bereitstellung im Discover (TAP)-Modus nun Security Heartbeat™-Transparenz und -Bedrohungsidentifizierung über einen einfachen Anschluss an einen Mirror Port oder Switch. So kann die XG Firewall gemeinsam mit einer bestehenden Kunden-Firewall eingesetzt werden und bietet mehr Transparenz über Bedrohungen und den Integritätsstatus von Sophos Endpoints im Netzwerk.

Synchronized Security und das neue Feature Synchronized App Control werden bei einer Inline-Bereitstellung der XG Firewall mit einer bestehenden Firewall ebenfalls komplett unterstützt. So profitieren Kunden von allen Synchronized-Security-Vorteilen (mehr Transparenz und besserer Schutz), ohne ihre bestehende Netzwerkinfrastruktur verändern zu müssen. Mit den neuen Fail-Open Bypass Ports, über die alle neuen 1U Appliances der XG Serie verfügen, wird dies einfach und risikofrei.

Bei gemeinsamer Ausführung bilden Intercept X (kann parallel zu bestehendem Endpoint-Schutz anderer Anbieter bereitgestellt werden) und die XG Firewall eine umfassende Synchronized-Security-Lösung, die sich ohne Störungen oder Veränderungen der bestehenden IT-Security-Infrastruktur bereitstellen lässt.

Synchronized App Control

Wie im Abschnitt „Sicherheit und Kontrolle“ dieses Dokuments erwähnt, ist Synchronized App Control eine revolutionäre neue Synchronized-Security-Funktion, mit der bislang unbekannte Anwendungen identifiziert, klassifiziert und kontrolliert werden können.

Synchronized App Control fordert für Datenverkehr, der mit keiner App-Control-Signatur übereinstimmt, vom Endpoint Anwendungsinformationen an. Hierdurch wird ein gravierendes Problem mit der signaturbasierten App Control aller heutigen Firewalls gelöst, die viele Anwendungen als „unbekannt“, „nicht klassifiziert“, „generisches HTTP“ oder „SSL“ klassifiziert.

Die XG Firewall kann nun alle auf Sophos Endpoints genutzten Anwendungen eindeutig identifizieren. Wo es möglich ist, klassifiziert die XG Firewall die Anwendung automatisch und kontrolliert diese mit bestehenden App-Control-Richtlinien. Administratoren können erkannten Anwendungen zudem manuelle Kategorien zuweisen, sodass die App-Control-Durchsetzung die Anwendung wie gewünscht blockieren oder priorisieren kann.

Bereitstellung und Hardware

Hochverfügbarkeit mit Microsoft Azure

Mit seiner Flexibilität und globalen Dimension bietet Microsoft Azure Kunden unmittelbare Redundanz- und Business-Continuity-Vorteile. In v17 können Kunden nun noch effektiver von diesen Funktionen profitieren, wenn sie die XG in Hochverfügbarkeitsszenarien auf Azure bereitstellen.

Mit von Sophos erstellten Azure Resource Manager (ARM) Templates können Kunden die XG auf Azure bereitstellen und Azure Load Balancer Probes nutzen, um den Integritätsstatus der XG zu ermitteln und bei Bedarf ein automatisches Failover durchzuführen. Unsere ARM Templates finden Sie in unserem GitHub Repository oder testen Sie die XG und berichten Sie uns von Ihren Erfahrungen.

Unterstützung neuer Hardware

Mit den neuesten Anschlussmöglichkeiten und Funktionen der aktuellen XG Series Hardware (u. a. die neuen Fail-Open Bypass Ports, die bei allen neuen 1U Appliances der XG Serie Standard sind) werden Inline-Bereitstellungen parallel zu bereits vorhandenen Firewalls einfach und risikofrei.

Zentrale Verwaltung

Die Firewall-Konfiguration für die zentrale Verwaltung des Sophos Firewall Manager/Sophos Central Firewall Manager wurde umgestaltet und ist nun sehr viel einfacher und intuitiver.

Problembehebung

Behobene Probleme

Neben neuen Funktionen haben dieser Release und die 2017 bereits veröffentlichten Maintenance Releases die übergreifende Performance, Zuverlässigkeit und Stabilität der XG Firewall in allen Produktbereichen deutlich verbessert.

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

SOPHOS