Reviewer's Guide

XG Firewall

v18

SOPHOS

Cybersecurity evolved.

Inhaltsverzeichnis

Willkommen bei der XG Firewall

Vielen Dank, dass Sie die Sophos XG Firewall in Betracht ziehen. In diesem Guide erhalten Sie einen Überblick über die vielen Funktionen, die die XG Firewall von anderen auf dem Markt erhältlichen Firewall-Produkten unterscheiden, und hilfreiche Tipps zum Test der XG Firewall in Ihrem eigenen Netzwerk.

Die Sophos XG Firewall wurde von Grund auf entwickelt, um die häufigsten Probleme mit bisherigen Firewalls aus der Welt zu schaffen. Als Hauptprobleme heutiger Firewalls werden uns am häufigsten genannt:

- Mangelnde Transparenz über Risiken und Aktivitäten im Netzwerk. Bei den meisten Firewalls sind wichtige Informationen nicht auf den ersten Blick ersichtlich.
- Unzureichender Schutz und Funktionsumfang oder viel zu komplizierte Einrichtung. Die meisten Firewalls bieten entweder nicht die notwendige Technologie, um die komplexen Bedrohungen von heute zu blockieren, oder ihre Konfiguration ist so kompliziert, dass es nur den wenigsten gelingt, sie optimal einzurichten.
- Mangelnde Reaktion auf Vorfälle im Netzwerk. Die meisten Firewalls haben im besten Fall nur einen geringen Einblick in die Präsenz von Bedrohungen im Netzwerk. Und wenn sie Bedrohungen erkennen, reagieren sie nicht automatisch.

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

1. **Deckt verborgene Risiken auf:** Die XG Firewall deckt verborgene Risiken weit besser auf als andere Firewalls – mit einem visuellen Dashboard, umfassendem On-Box-Reporting und maximaler Transparenz über Risiken.
2. **Blockiert unbekannte Bedrohungen:** Die XG Firewall macht die Blockierung unbekannter 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 XG Firewall mit Synchronized Security automatisch auf Vorfälle im Netzwerk.

Dieser Guide hilft Ihnen dabei, die Vorteile der XG Firewall aus erster Hand kennenzulernen und zu bewerten. Bevor Sie jedoch beginnen, finden Sie hier einige weitere wichtige Informationsquellen, die Ihnen bei der Einrichtung und Konfiguration helfen, damit Sie Ihre XG Firewall optimal nutzen können.

Dokumentation und How-to-Videos

Unsere Dokumentations-Library und Links zu How-to-Videos, mit denen Sie schnell startbereit sind, finden Sie unter www.sophos.de/get-started-xg. Über die Option „Hilfe" in der oberen rechten Ecke der XG-Firewall-Konsole ist außerdem eine umfangreiche kontextsensitive Online-Hilfe verfügbar.

Aktivierung von Synchronized Security

Im Folgenden finden Sie einige Tipps, wie Sie Synchronized Security schnell und einfach aktivieren können, um sich aus erster Hand von den Vorteilen zu überzeugen.

- Wenn Sie noch kein Sophos-Central-Konto haben, können Sie sich unter https://central.sophos.com für eine Testversion anmelden.
- Sobald Sie ein Sophos-Central-Konto haben, stellen Sie sicher, dass Sie einen oder mehrere Computer in Ihrem Netzwerk mit Sophos Intercept X schützen, wodurch der Security Heartbeat mit Ihrer XG Firewall aktiviert wird. Gehen Sie in Sophos Central zu „Geräte schützen" und laden Sie den Installer für die Plattform Ihrer Wahl herunter.
- Melden Sie sich bei Ihrer XG Firewall an und klicken Sie auf die Menüoption „Zentrale Synchronisierung", um Ihre Firewall mit Sophos Central zu verbinden. Sie müssen lediglich Ihre Sophos-Central-Zugangsdaten eingeben, um Ihre XG Firewall bei Sophos Central zu registrieren, und schon sind Security Heartbeat, Synchronized Application Control und die Verwaltung Ihrer XG Firewall über Sophos Central aktiviert.

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.

Xstream SSL Inspection

Rund um verschlüsselten Datenverkehr braut sich ein wahrhaftiger Sturm zusammen. Laut Google sind 80 % 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 XG 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 XG 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 XG Firewall bereitet diese Informationen weit besser auf als andere Lösungen – insbesondere Fehler, die aufgrund von Zertifikatvalidierungen oder Websites auftreten, die nicht die neuesten Verschlüsselungsstandards unterstützen.

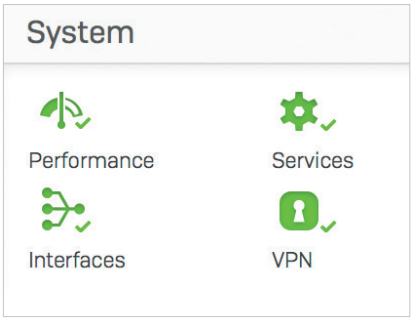
Administratoren können auch ein detailliertes Fenster öffnen, um genau zu sehen, welche Websites warum problematisch sind. Außerdem werden hier Benutzer angezeigt, bei denen Probleme vorliegen. Von dort aus können sie direkt Maßnahmen ergreifen, um die Anwendung oder die Website von der Entschlüsselung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

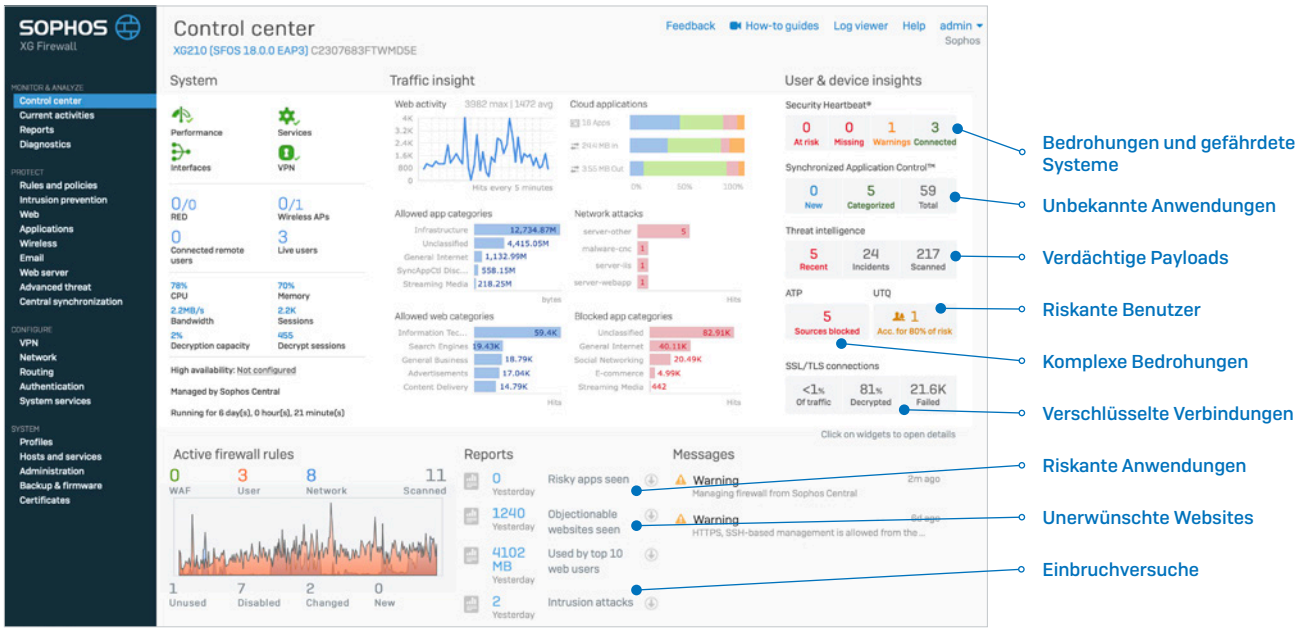
Control Center

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

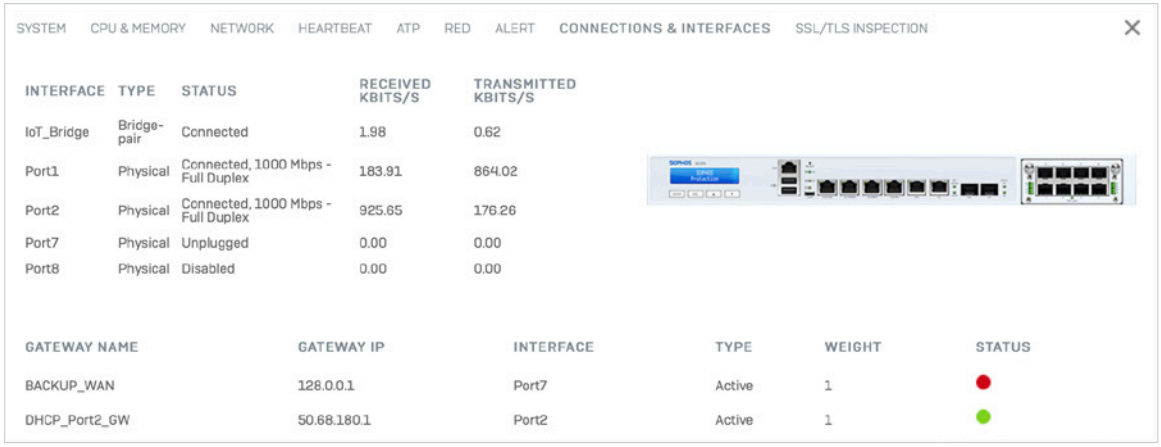
Mit Symbolen in Ampelfarben erkennen Sie schnell, wo Sie reagieren müssen:

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.

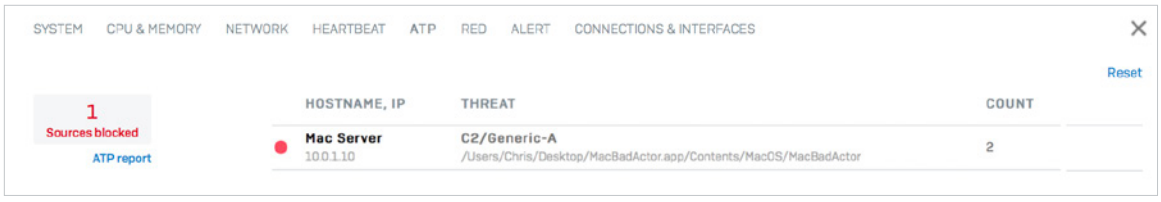




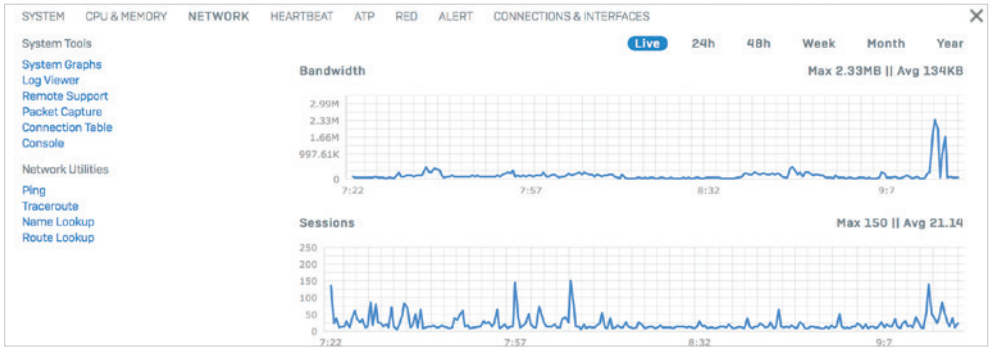
Jedes Widget im Control Center liefert weitere Informationen, die durch Klicken auf das Widget einfach abgerufen werden können. Der Status von Schnittstellen auf dem Gerät kann beispielsweise abgefragt werden, indem Sie im Control Center auf das Widget „Schnittstellen" klicken.



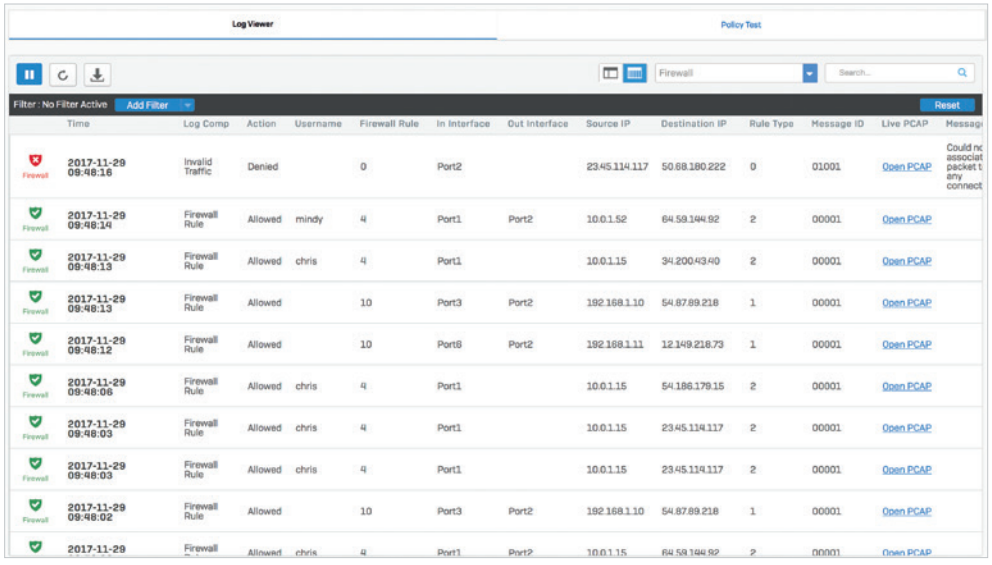
Der Host, Benutzer und die Quelle einer komplexen Bedrohung können ebenso einfach durch Klicken auf das Widget „ATP" (Advanced Threat Protection) im Dashboard abgerufen werden.



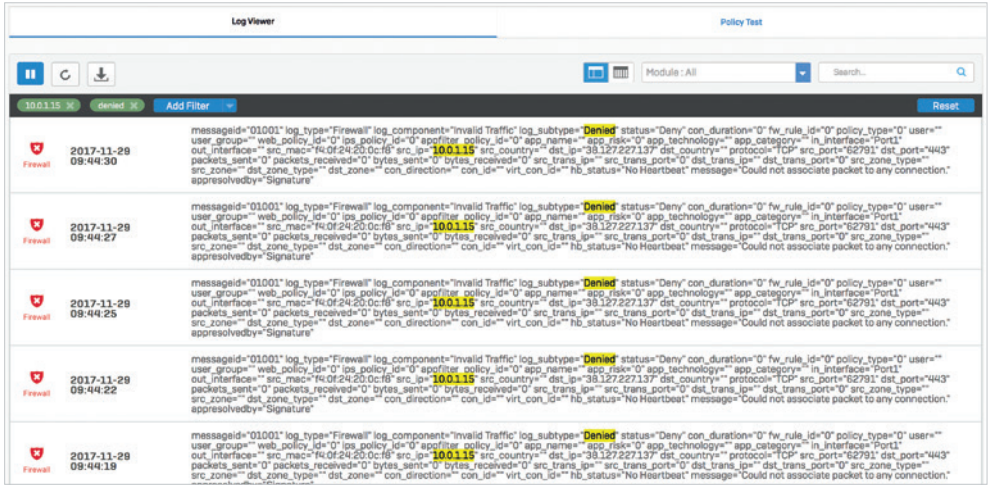
Systemdiagramme zeigen die Performance zudem im zeitlichen Verlauf und Sie können bestimmte Zeitabschnitte auswählen (z. B. letzte zwei Stunden oder letzter Monat bzw. letztes Jahr). Außerdem ermöglichen sie einen schnellen Zugriff auf häufig genutzte Troubleshooting-Tools, um potenzielle Probleme zu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



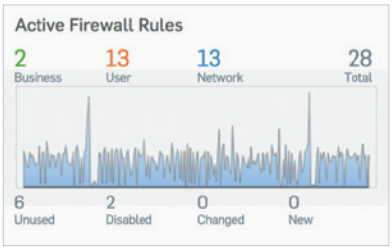
Den Live Log Viewer können Sie in jeder Ansicht mit nur einem Klick aufrufen. Der Viewer öffnet sich auf Wunsch in einem neuen Fenster, sodass Sie das jeweilige Protokoll beim Arbeiten in der Konsole im Auge behalten können. Es stehen zwei Ansichten zur Verfügung: eine einfachere Ansicht mit Spalten für die einzelnen Firewall-Module sowie eine detailliertere Gesamtansicht mit leistungsstarken Filter- und Sortieroptionen, in der Protokolle vom gesamten System auf einen Blick und in Echtzeit zu sehen sind.



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 XG Firewall erübrigen sich diese Fragen.

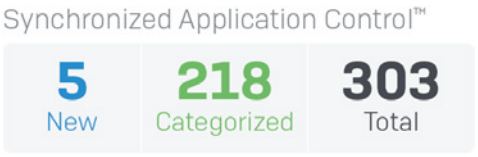


Das Widget „Aktive Firewall-Regeln" zeigt in einem Echtzeit-Diagramm, welchen Datenverkehr die Firewall nach Regeltyp verarbeitet hat: Geschäftsanwendung, Benutzer und Netzwerkregeln. Auch die aktive Anzahl von Regeln nach Status wird angezeigt, einschließlich ungenutzter Regeln, die ggf. gelöscht werden 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.



Synchronized Application Control

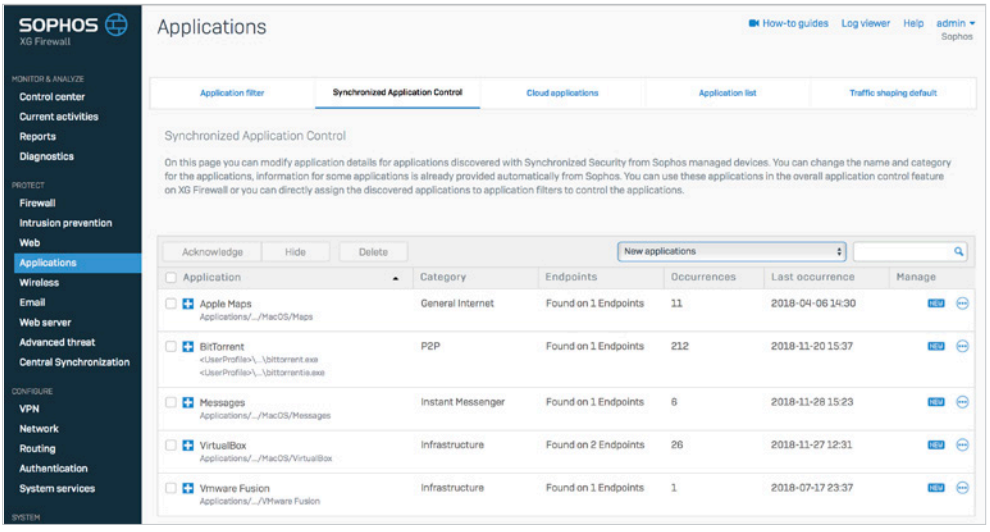
Das Problem mit Application Control in heutigen Next-Generation Firewalls besteht darin, dass der meiste Anwendungsverkehr nicht identifiziert wird: Die Anwendungen werden entweder nicht klassifiziert oder sie werden markiert als unbekannt, generische HTTP- oder generische HTTPS-Anwendungen.



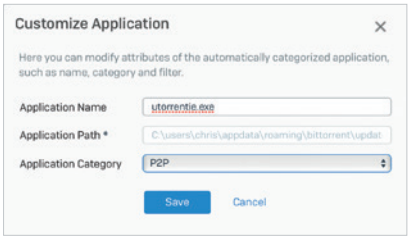
Hierfür gibt es einen einfachen Grund: Alle Firewall App Control Engines stützen sich zur Identifizierung von Anwendungen auf Signaturen und Muster. Und wie Sie sich vielleicht vorstellen können, existieren für benutzerdefinierte Anwendungen aus vertikalen Märkten (z. B. Medizin- oder Finanzanwendungen) 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 XG Firewall Anwendungsverkehr, den sie mit Signaturen nicht identifizieren kann, fragt sie den Endpoint, welche Anwendung diesen Traffic generiert.



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

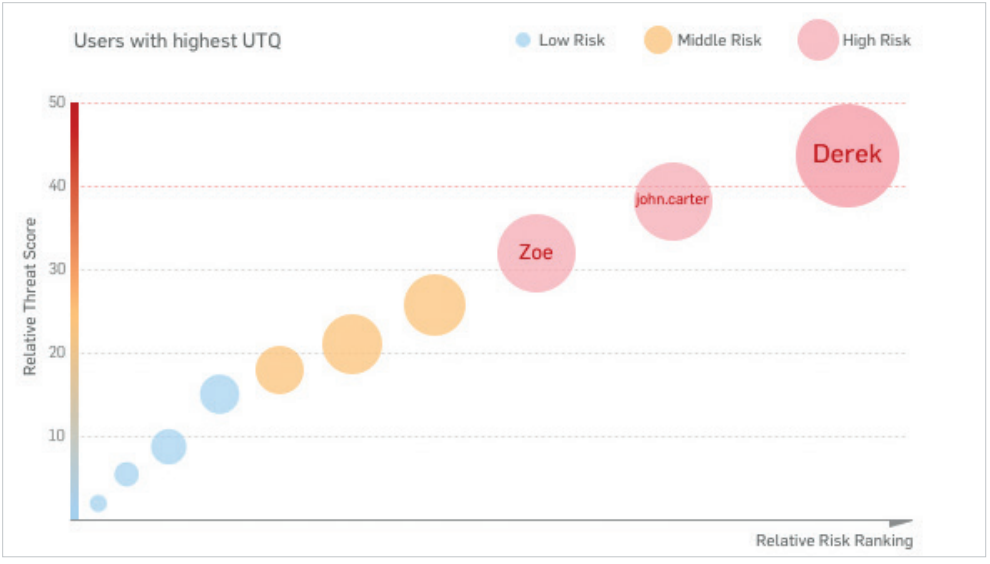
Sobald eine Anwendung klassifiziert wurde – entweder automatisch oder durch den Netzwerkadministrator – unterliegt die Anwendung denselben Richtlinienkontrollen wie alle anderen Anwendungen in dieser Kategorie. So können Sie alle nicht identifizierten, unerwünschten Anwendungen blockieren und erwünschte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

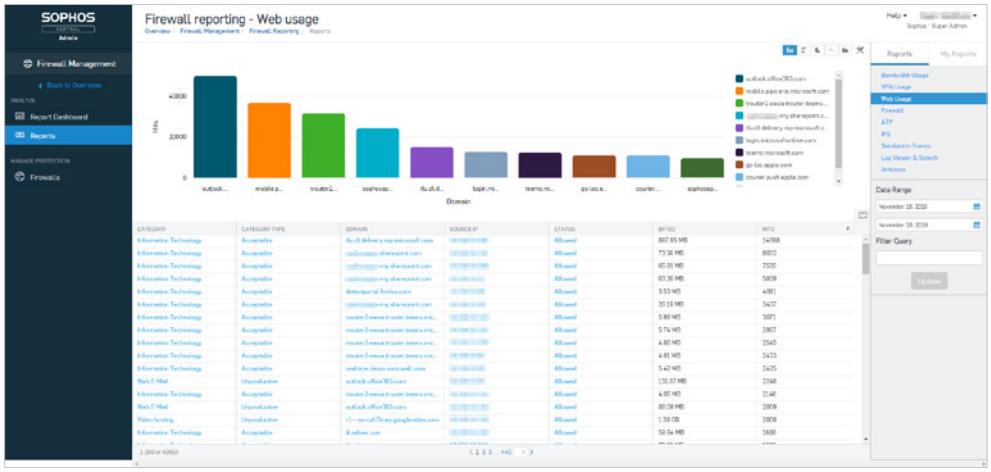
Der Sophos User Threat Quotient (UTQ) hilft Sicherheits-Administratoren dabei, Benutzer frühzeitig zu erkennen, die aufgrund ihres verdächtigen Verhaltens im Internet sowie ihres Bedrohungs- und Infektionsverlaufs ein Risiko darstellen. Hohe UTQ-Risikobewertungen von Benutzern können auf unbeabsichtigtes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



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.

Flexible Reporting-Optionen

Die XG Firewall ist einzigartig unter den NGFW- und UTM-Produkten, da sie flexible, cloudbasierte On-Box-Reporting-Optionen mit einem hohen Maß an Anpassungsmöglichkeiten ganz ohne Aufpreis bietet. Sophos Central Firewall Reporting (CFR) liefert Unternehmen mit seinen Analysen einen besonders detaillierten Einblick in Netzwerkaktivitäten. Mit seiner umfangreichen Auswahl integrierter Reports und Tools zur Erstellung Hunderter Variationen liefert CFR aussagekräftige Informationen über das Benutzerverhalten, die Anwendungsnutzung, Sicherheitsereignisse und viele weitere Parameter. Interaktive Reports und ein übersichtliches Report Dashboard ermöglichen Administratoren, die in Ihrem Sophos-Central-Konto gespeicherten Syslog-Daten für eingehendere Analysen aufzurufen. Diese werden zum besseren Verständnis in einem visuellen Format dargestellt. Die Daten lassen sich dann auf Trends analysieren, die möglicherweise auf Sicherheitslücken hinweisen und Richtlinienänderungen erfordern.



Die XG Firewall bietet auch On-Box-Reporting. Sie haben eine Vielzahl von Reports zur Auswahl, die praktisch nach Typ geordnet sind – mit mehreren integrierten Dashboards. Ihnen stehen Hunderte von Reports mit individuell anpassbaren Parametern für alle Bereiche der Firewall zur Verfügung, einschließlich Datenverkehrsaktivitäten, Sicherheit, Benutzer, Anwendungen, Web, Netzwerk, Bedrohungen, VPN, E-Mail und Compliance. Zudem können Sie in regelmäßigen Abständen automatisch Reports generieren lassen, die dann per E-Mail an Sie oder andere Empfänger gesendet werden, und Reports im HTML-, PDF- oder CSV-Format speichern.

Blockieren unbekannter Bedrohungen

Zum Schutz vor aktuellen Netzwerkbedrohungen ist ein „Orchester" von Technologien erforderlich, das optimal aufeinander abgespielt 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.

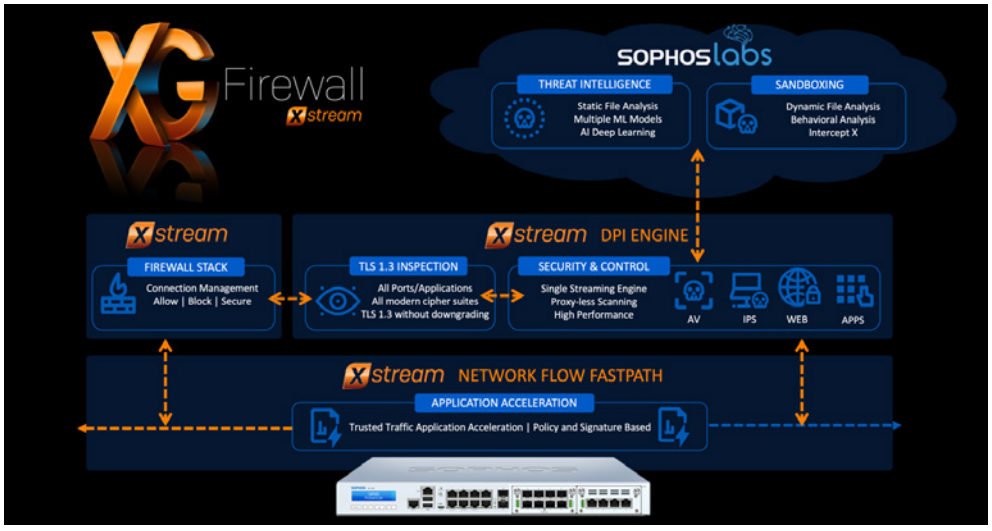
Bei Sophos sind wir nicht nur der Meinung, dass Sie die marktweit leistungsstärkste Schutztechnologie erhalten sollten. Wir wissen auch, dass die Konfiguration, Bereitstellung und tägliche Verwaltung einfach sein müssen, denn schlecht konfigurierter Schutz ist oft gefährlicher als gar kein Schutz.

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 XG 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 XG Firewall Xstream-Paketverarbeitungsarchitektur 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.



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.

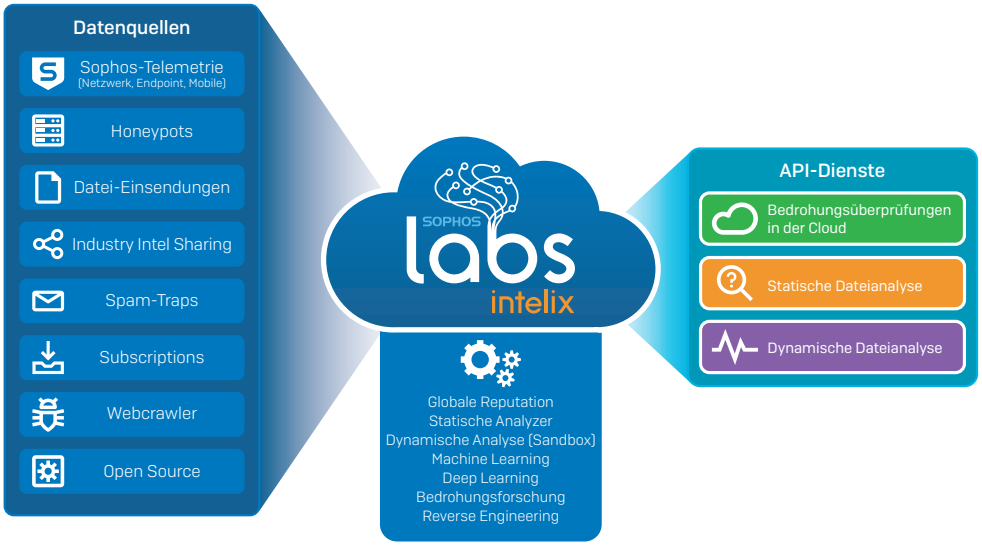
Wenn der Stream als sicher eingestuft wird und keine weitere Überprüfung mehr erforderlich ist, kann die DPI Engine den Flow vollständig an den Sophos Network Flow FastPath auslagern, der einen beschleunigten Pfad für vertrauenswürdigen Datenverkehr bereitstellt. Dies steigert die Performance dramatisch,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

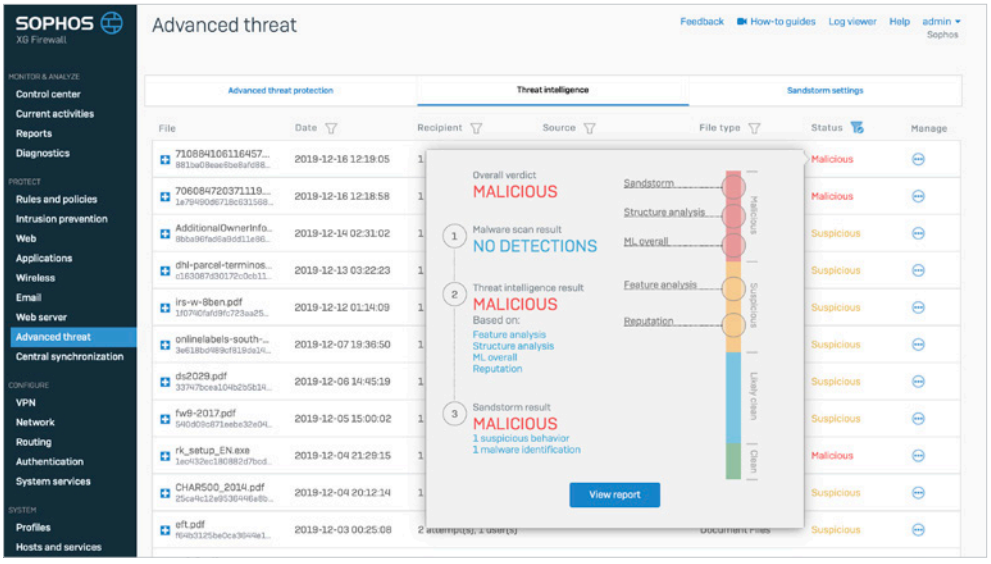
1. **Statische Machine-Learning-Analyse** – Diese ermöglicht eine prädiktive Analyse und Erkennung durch mehrere Machine-Learning-Modelle aus künstlichen neuronalen Netzwerken, kombiniert mit globaler Reputation und Deep File Scanning, ohne die Datei in Echtzeit ausführen zu müssen.
2. **Dynamische Laufzeit-Sandbox-Analyse** – 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 unbekannten Bedrohung aufdecken.

In der XG Firewall sind beide dieser wichtigen Schutztechnologien enthalten, diese nutzen 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 unbekannten Bedrohungen.



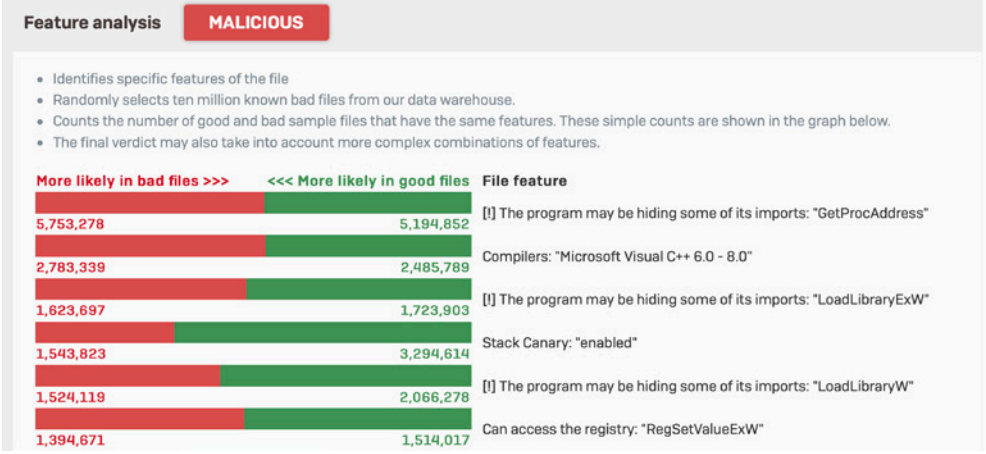
Wird im Zuge der Antivirus-Analyse einer Datei aktiver Code festgestellt, so behält die Xstream DPI Engine die Datei vorübergehend ein und sendet sie zur statischen und dynamischen Datei-Analyse an den SophosLabs Intelix Service in der Cloud. Eine Zusammenfassung der Ergebnisse wird anschließend im XG 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 freigeben, 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.



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).

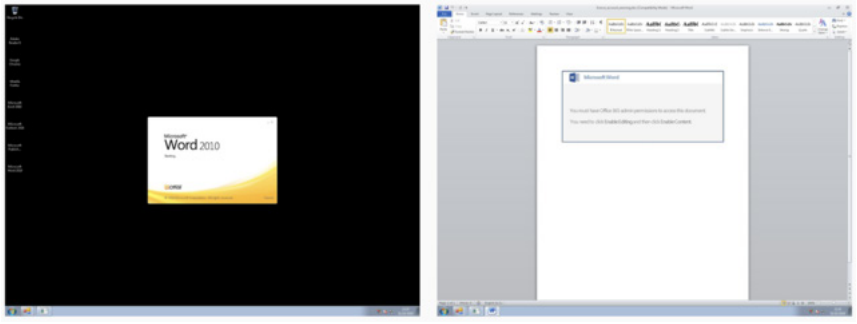


Dynamische Laufzeit-Sandboxing-Analyse

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.

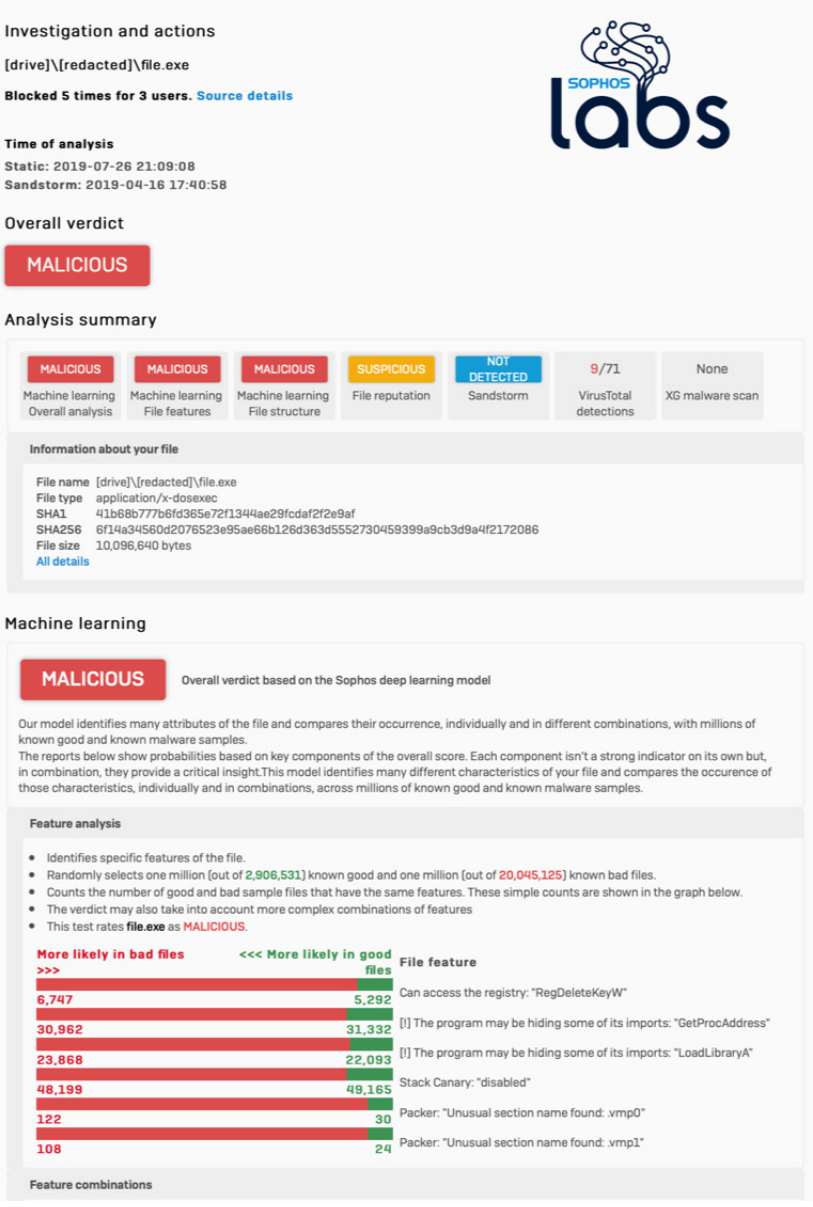
Zur Identifizierung von Bedrohungen haben die SophosLabs die neuesten Schutztechnologien unseres branchenführenden Next-Gen-Endpoint-Produkts Intercept X in Sophos Sandstorm integriert, einschließlich Deep Learning, Exploit-Erkennung und CryptoGuard (zur Erkennung aktiver Ransomware-Verschlüsselungen 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 führender Threat Protection (Intercept X). Auch Transparenz und Reporting-Kapazitäten der XG Firewall (z. B. vollständige Screenshot-Serie zu den Ereignissen bei der Dateiausführung) sind branchenweit einzigartig.



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

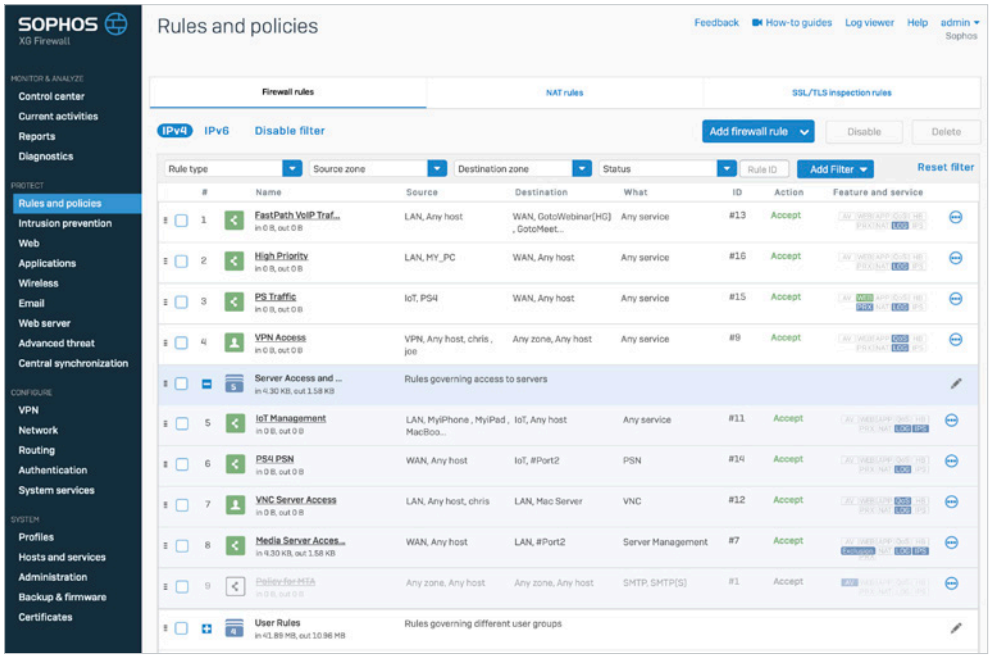
Für jede von der XG Firewall analysierte Datei wird ein begleitender Report erstellt, der alle Details zu den Ergebnissen der verschiedenen Analysen und Bewertungen enthält. Der Report besteht aus 6 Elementen, darunter die verschiedenen Machine-Learning-Analysen, Datei-Reputation, Sandboxing und externe VirusTotal-Daten.



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.

Mit der XG Firewall haben wir die Gelegenheit genutzt, die Gliederung von Firewall-Regeln und die Verwaltung Ihres Sicherheitsstatus komplett zu überdenken. 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.

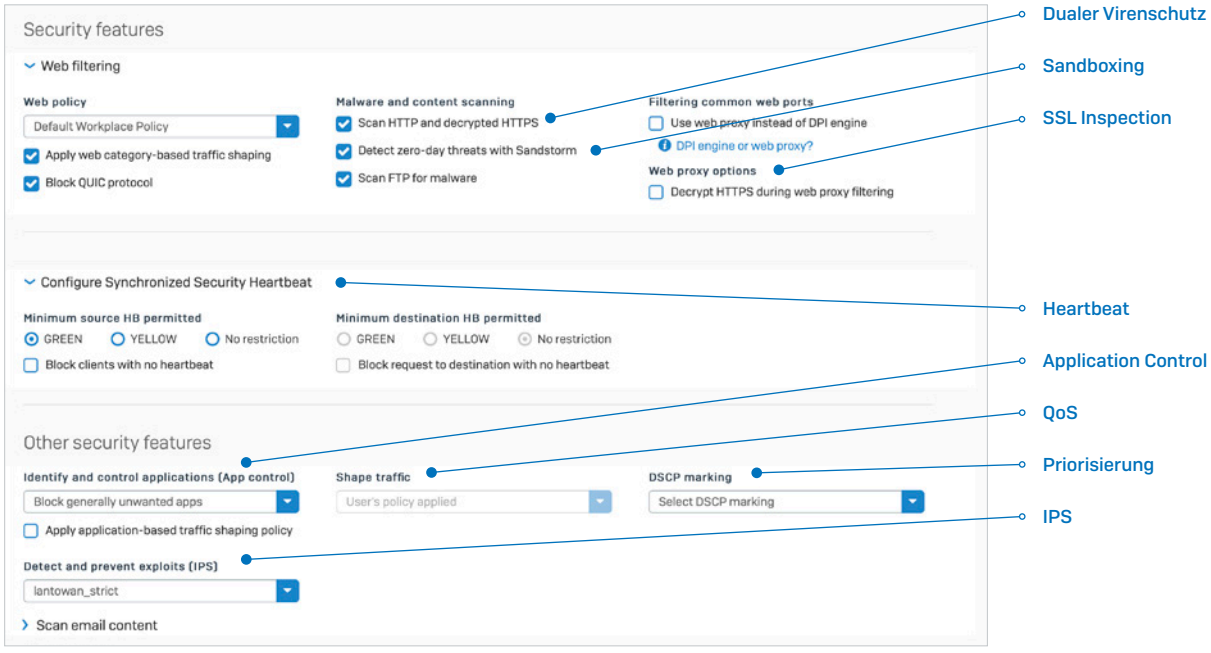


Regeln für Benutzer, Geschäftsanwendungen, NAT, TLS/SSL Inspection und Netzwerk können Sie sich gezielt die jeweils relevanten Richtlinien anzeigen lassen und die Verwaltung über eine praktische zentrale Ansicht erledigen.

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

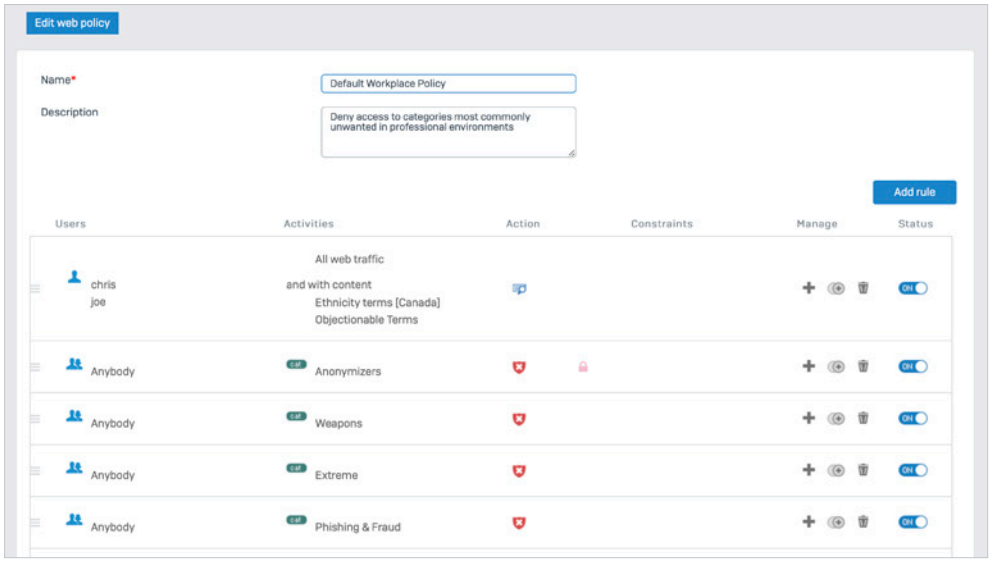
Verwaltung Ihres Sicherheitsstatus auf einen Blick

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

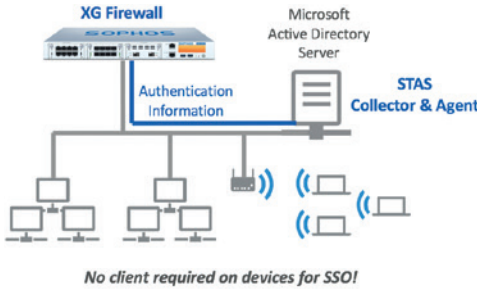


Sie können Sicherheits- und Kontrollfunktionen für Antivirus, TLS/SSL Inspection, Sandboxing, IPS, Traffic Shaping, Web und Application Control, Security Heartbeat, NAT, Routing und Priorisierung an einem Ort einrichten und aktivieren – und zwar nach Regel, Benutzer oder Gruppe.

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.

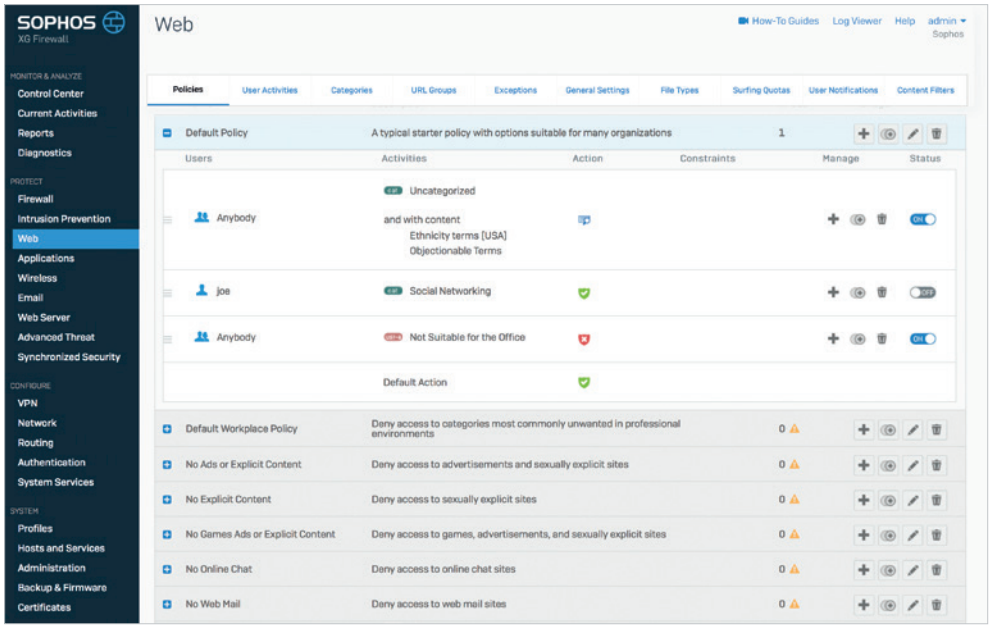


Flexible Authentifizierungsoptionen ermöglichen Ihnen eine einfache Identifizierung und umfassen Verzeichnisdienste wie Active Directory, eDirectory, LDAP sowie NTLM, Kerberos, RADIUS, TACACS+, RSA, Client-Agenten oder Captive Portal. Zudem ermöglicht die Sophos Transparent Authentication Suite (STAS) 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.



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 XG 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.

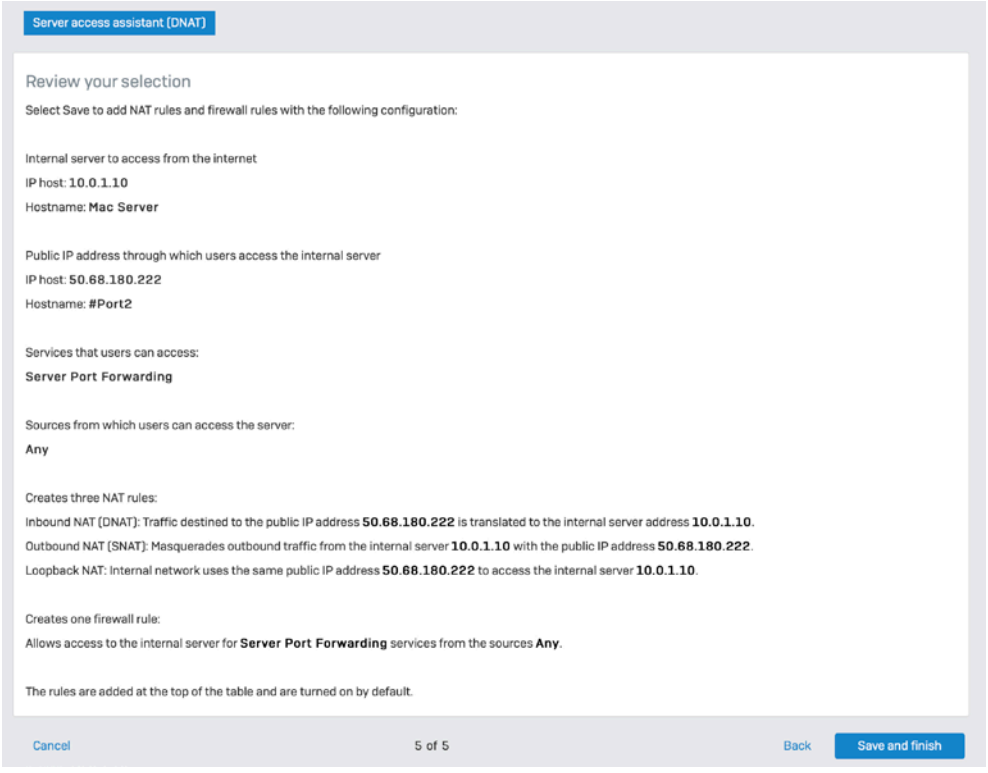
Mit vorkonfigurierten Web-Richtlinien für Bildungseinrichtungen sorgt die XG Firewall für schnelle Compliance mit geltenden Vorschriften. Außerdem bietet sie flexible und leistungsstarke Kontrollen über SafeSearch- und YouTube-Beschränkungen auf Basis von Benutzer-/Gruppenrichtlinien. Lehrer können außerdem 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 XG 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.

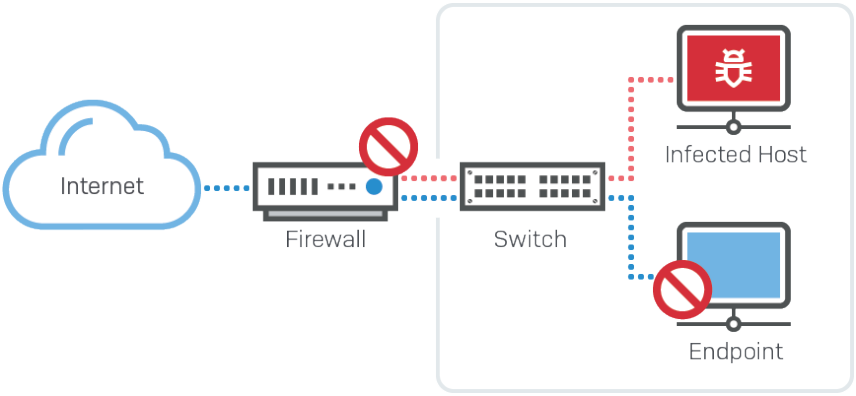
Administratoren können beim Erstellen einer Firewall-Regel auch die praktische Option „Verknüpfte NAT" nutzen. Hiermit wird automatisch eine entsprechende NAT-Konfigurationsregel erstellt und der Zeitaufwand für die Erstellung und Konfiguration von NAT-Regeln weiter reduziert.



Automatische Reaktion auf Vorfälle

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

Die Sophos XG 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.



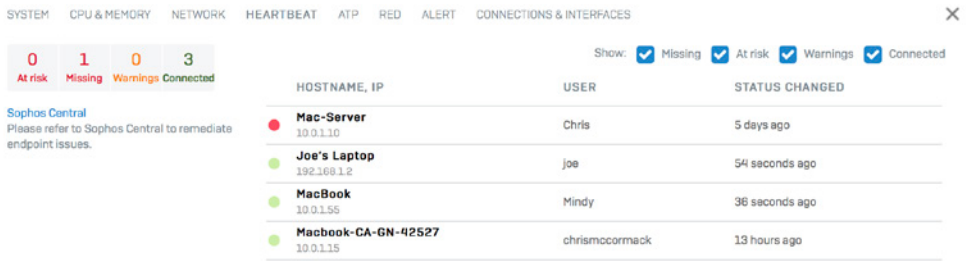
Die XG Firewall integriert den Sicherheitsstatus verbundener Hosts auf völlig neuartige Weise in Ihre Firewall-Regeln, sodass Sie den Zugriff kompromittierter Systeme auf sensible Netzwerkressourcen bis zu ihrer Dekontaminierung automatisch beschränken können.

Die XG 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 XG 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.



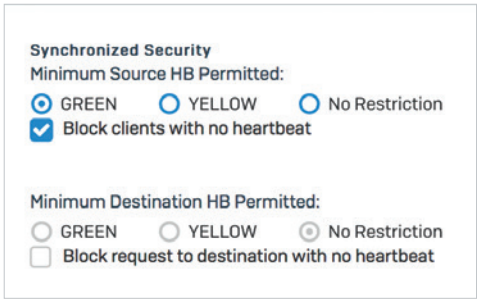
Security Heartbeat identifiziert komplexe Bedrohungen nicht nur unmittelbar, sondern kommuniziert auch wichtige Informationen über die Eigenschaften der Bedrohung, des Hostsystems und des Benutzers. Und vielleicht am wichtigsten: Dank Security Heartbeat können kompromittierte Systeme automatisch isoliert 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 zeigt 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 oder dass ein Gerät die Compliance nicht einhält. Sie können selbst entscheiden, auf welche Netzwerk-Ressourcen ein System mit gelbem Hearbeat 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.



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 brachenführende 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 jedoch temporär, ergibt sich aus mehreren Datenquellen und wird ständig neu bewertet.

Mit Zero Trust lässt sich die gesamte Infrastruktur kontrollieren – im Büro bis hin zu den 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: Unsere cloudbasierte Cybersecurity-Plattform stellt diese unterschiedlichen und sich ergänzenden Technologien in einem einzigen Hub zur Verfügung, über den Sie Ihr Zero-Trust-Netzwerk organisieren und kontrollieren können.

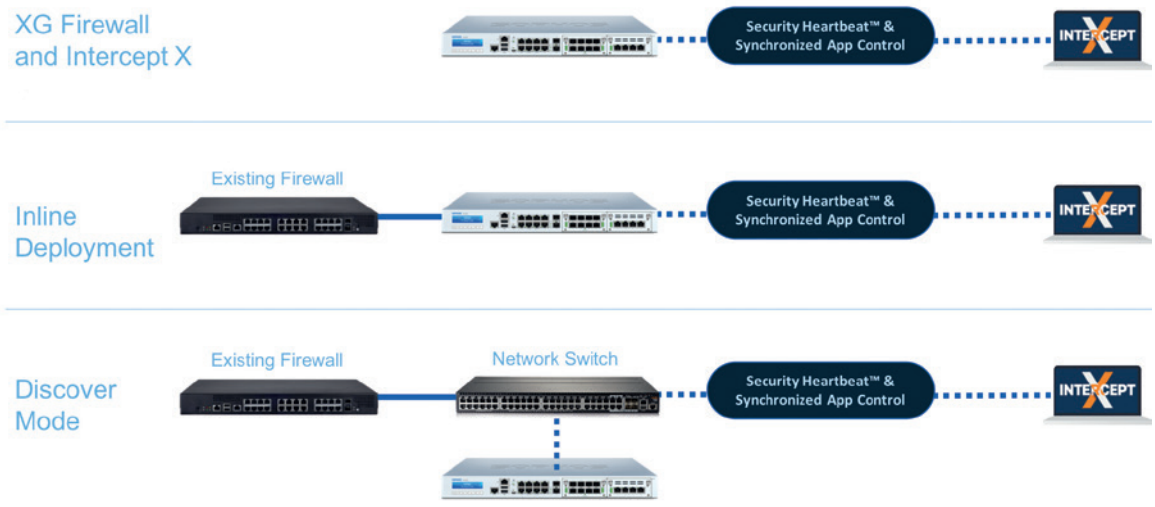
Synchronized Security: Cybersicherheit, die für maximale Transparenz kontinuierlich Informationen zwischen Systemen austauscht.

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

Server Protection und Intercept X: Weisen Sie jedem Gerät einen Integritätsstatus 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.

Einfaches Hinzufügen der XG Firewall zu jedem beliebigen Netzwerk



Die Hardware Appliances der XG 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 XG Firewall im Bridge-Modus inline mit bestehenden Firewalls. Wenn die XG 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 XG Firewall: Sie erhalten einfache und zuverlässige Cybersecurity.

Preisanfrage

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

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

SOPHOS

20-09-30 WP-DE (DD)