SOPHOS
Cybersecurity evolved.

Next-Gen Firewall Buyers Guide

Bei aktuellen Befragungen nennen uns Netzwerk-Administratoren und IT-Manager diese größten Probleme mit ihrer derzeitigen Firewall:

- Mangelnde Einsicht in Netzwerkanwendungen, Risiken und Bedrohungen
- Bedenken über Schutzleistung vor neuesten Bedrohungen und Angriffen
- Keine Reaktion oder Unterstützung bei Bedrohungen im Netzwerk

Falls Ihnen einige dieser Antworten bekannt vorkommen, befinden Sie sich in guter Gesellschaft. Denn den meisten derzeit erhältlichen Next-Gen Firewalls fehlen wichtige Sicherheitsfunktionen. Sie sorgen nicht für genügend Transparenz, bieten keinen ausreichenden Schutz oder keine effektive Reaktion auf Bedrohungen.

Wo aber sollten Sie bei der Suche nach einer besseren Firewall ansetzen? Zunächst müssen Sie überlegen, welche Grundvoraussetzungen Ihre Firewall erfüllen sollte. Sobald Sie diese Frage beantwortet haben, beginnt die wirkliche Arbeit: Sie müssen sich durch den Dschungel von Anbieter-Websites und Datenblättern kämpfen, um herauszufinden, welche Firewall Ihre Anforderungen am besten und am zuverlässigsten erfüllt.

Über diesen Guide

Dieser Buyers Guide soll Ihnen dabei helfen, die richtige Firewall für Ihr Unternehmen zu finden, damit Sie Ihre Kaufentscheidung später nicht wie die von uns befragten IT-Netzwerk-Manager bereuen. Wir besprechen alle Funktionen, auf die Sie beim Kauf Ihrer nächsten Firewall achten sollten. Außerdem haben wir wichtige Fragen für Sie zusammengestellt, die Sie Ihrem IT-Partner oder -Anbieter stellen sollten, um sicherzustellen, dass das jeweilige Produkt auch wirklich Ihre Anforderungen erfüllt. Auf den letzten Seiten finden Sie zudem eine praktische Übersicht, die Ihnen dabei hilft, geeignete Firewall-Anbieter in die engere Auswahl zu ziehen.

Der Feind der Netzwerk-Security: Verschlüsselung

Die ständige Zunahme verschlüsselter Datenströme stellt die Sicherheit von Netzwerken vor ungeahnte Herausforderungen. Bedenken Sie folgende wichtige Fakten:

- 90 % des Internetverkehrs sind mittlerweile TLS-verschlüsselt
- 50 % der Malware-, PUA und Hacker-Server setzen gezielt auf Verschlüsselung, um unerkannt zu bleiben.
- Denn die meisten Unternehmen überprüfen verschlüsselten Datenverkehr nicht.

Wenn wir Unternehmen fragen, warum sie verschlüsselten Datenverkehr nicht überprüfen, wird die Performance als Hauptgrund genannt. TLS Inspection ist für die meisten Firewalls schlicht zu ressourcenintensiv, um mit dem enormen Volumen des verschlüsselten Datenverkehrs Schritt zu halten. Ein zweiter wesentlicher Grund, warum verschlüsselter Datenverkehr nicht überprüft wird, sind daraus resultierende Beeinträchtigungen der Internet-Nutzung.

Diese grundlegende Herausforderung mit Verschlüsselungen und die Unfähigkeit der meisten Firewalls, auf diese Problematik einzugehen, führt zu einer Reihe weiterer Probleme: mangelnde Transparenz über riskantes Verhalten und Inhalte, potenzielle Compliance-Verstöße und unzureichender Schutz vor Ransomware, Angriffen und Verstößen. Tatsächlich ist Verschlüsselung die Hauptursache vieler der derzeit größten Herausforderungen im Bereich Netzwerksicherheit. Denn die meisten Netzwerke lassen den Großteil des Datenverkehrs einfach ungeprüft passieren. Das ist jedoch nicht mehr notwendig. Es gibt einen sehr effektiven Weg, diese Herausforderung zu meisten.

Weitere Informationen finden Sie in diesem Dokument: Hat Verschlüsselung Ihre derzeitige Firewall überflüssig gemacht?

Unverzichtbare Funktionen

Um Ihre größten Herausforderungen bei Netzwerk-Transparenz, Bedrohungsschutz und -reaktion zu lösen, sind hier vier wichtige Funktionen aufgeführt, auf die Sie bei Ihrer nächsten Firewall auf keinen Fall verzichten sollten:

TLS 1.3 Inspection – 90 % des Internet-Verkehrs sind mittlerweile verschlüsselt – Tendenz steigend. Daher muss Ihre nächste Firewall unbedingt über TLS 1.3 Inspection verfügen. Noch wichtiger ist vielleicht, dass diese Firewall intelligent und leistungsstark genug sein muss, um Datenverkehr effizient überprüfen zu können, ohne Engpässe zu erzeugen oder Sie zum Kauf eines teuren Highend-Modells zu zwingen, das Sie eigentlich gar nicht benötigen. Nicht alle verschlüsselten Datenbewegungen müssen überprüft werden und nicht alle verschlüsselten Datenströme unterstützen eine solche Überprüfung. Ihre nächste Firewall sollte alle aktuellen Standards und Verschlüsselungssammlungen unterstützen. Außerdem sollten intelligente Ausnahmen integriert sein, damit genau festgelegt werden kann, welcher Datenverkehr überprüft werden soll. Gleichzeitig sollten die Firewall-Tools bereitstellen, mit denen potenzielle Probleme leicht identifiziert und spontan Ausnahmen zu deren Vermeidung hinzugefügt werden können. Auch die Performance sollte großzügig bemessen sein, damit die Firewall den stetig wachsenden Anteil von verschlüsseltem Datenverkehr heute und in Zukunft bewältigen kann.

Zero-Day-Schutz vor Bedrohungen – Bedrohungen entwickeln sich ständig weiter. Die Ransomware-Variante, mit der ein Unternehmen morgen angegriffen wird, wird sich höchstwahrscheinlich von der Variante unterscheiden, die gestern verwendet wurde. Denn die heutige Bedrohungslandschaft befindet sich in ständigem Wandel. Ihre nächste Firewall muss über künstliche Intelligenz verfügen, die auf mehreren Machine-Learning-Modellen basiert, sowie über Sandboxing mit moderner Exploit-Erkennung und Crypto-Guard-Ransomware-Erkennung von Bedrohungen, damit Zero-Day-Bedrohungen bereits erkannt und gestoppt werden, bevor sie in Ihr Netzwerk gelangen können.

FastPath-Anwendungsbeschleunigung – rund 80 % des Datenverkehrs in Ihrem Netzwerk stammen wahrscheinlich von etwa 20 % Ihrer Anwendungen. Diese sogenannten „Elephant Flows" sind typisch für Meeting- und Collaboration-Tools, Streaming-Medien und VoIP. Die Überprüfung solcher großen Datenverkehrsströme ist ressourcenintensiv und erfordert optimale Performance, da nur so ein ideales Benutzererlebnis sichergestellt werden kann. Ihre nächste Firewall sollte in der Lage sein, diese vertrauenswürdigen Datenströme angemessen zu verarbeiten und auszulagern, um eine optimale Performance zu bieten und zusätzlichen Spielraum für Datenverkehr zu schaffen, bei dem tatsächlich eine eingehendere Paketprüfung erforderlich ist.

Integration mit anderen Cybersecurity-Produkten – IT-Sicherheitsprodukte, die in Isolation arbeiten, werden heutigen Anforderungen nicht mehr gerecht. Zu Abwehr moderner Angriffe sind mehrere Schutzschichten erforderlich, die alle in Koordination arbeiten und Informationen austauschen, um eine synchronisierte Reaktion zu ermöglichen. Ihre nächste Firewall sollte sich in andere Systeme wie Ihr Endpoint-Antivirus integrieren lassen, um den Austausch wichtiger Bedrohungsdaten und Telemetrie-Daten zu ermöglichen. Dadurch können beide Systeme besser zusammenarbeiten und ihre Abwehrmaßnahmen bei einem Angriff koordinieren. Diese Systeme sollten auch über eine gemeinsame Verwaltungsoberfläche verfügen, um die Bereitstellung, tägliche Verwaltung sowie das produktübergreifende Threat Hunting und Reporting zu erleichtern.

Diese vier Funktionen stellen sicher, dass die größten Probleme mit Ihrer aktuellen Firewall der Vergangenheit angehören und Ihr Netzwerk-Schutz für die Zukunft gewappnet ist.

Unverzichtbare Funktionen	Fragen an Ihren Anbieter
TLS 1.3 Inspection Bietet Einblick in das zunehmende Aufkommen von verschlüsseltem Datenverkehr, der Ihr Netzwerk passiert	‣ Unterstützt Ihre TLS Inspection den neuesten 1.3-Standard? ‣ Funktioniert die Inspection über alle Ports und Protokolle hinweg? ‣ Arbeitet sie Streaming-basiert oder Proxy-basiert? ‣ Welche Auswirkungen bestehen auf die Performance? ‣ Werden verschlüsselte Datenströme im Dashboard angezeigt? ‣ Werden im Dashboard Websites angezeigt, die keine Entschlüsselung unterstützen? ‣ Sind einfache Tools verfügbar, mit denen sich Ausnahmen für problematische Websites hinzufügen lassen? ‣ Gibt es eine umfassende Ausschlussliste? ‣ Wer pflegt die Liste und wird sie regelmäßig aktualisiert?
Zero-Day-Bedrohungsschutz Schutz vor neuesten unbekannten Bedrohungen durch Machine Learning und Sandboxing	‣ Verfügt Ihre Firewall über Technologie zur Erkennung bislang unbekannter Bedrohungen? ‣ Werden Dateien mittels Machine Learning analysiert? ‣ Wie viele Mashine-Learning-Modelle werden angewendet? ‣ Umfasst Ihre Lösung Sandboxing? ‣ Lässt das Sandboxing Dateien vor Abschluss der Analyse passieren? ‣ Wird die Sandboxing-Lösung vor Ort oder in der Cloud ausgeführt? ‣ Umfasst die Sandboxing-Lösung führende Endpoint-Protection-Technologie, um Bedrohungen wie Ransomware in der Sandbox-Umgebung zu identifizieren? ‣ Welche Endpoint-Technologie wird beim Sandboxing eingesetzt? ‣ Welche Reports sind standardmäßig enthalten (im Gegensatz zu einem separaten Reporting-Produkt)? ‣ Wie viel Transparenz bietet das Dashboard?
FastPath-Anwendungsbeschleunigung Offloading von vertrauenswürdigem Anwendungsverkehr auf einen FastPath zur Performance-Steigerung und Kostenreduktion	‣ Unterstützt Ihre Firewall die FastPath-Beschleunigung von vertrauenswürdigem Datenverkehr und Elephant Flows? ‣ Erfolgt dies Software- oder Hardware-basiert? ‣ Wie werden Anwendungen für die FastPath-Beschleunigung identifiziert? ‣ Welche Richtlinien-Tools stehen Administratoren zur Verfügung, um zu kontrollieren, welche Anwendungen ausgelagert werden? ‣ Werden Signaturen mitgeliefert, um bestimmte Anwendungen zu beschleunigen und auf dem FastPath zu übertragen? ‣ Sind Ihre FastPath-Packet-Flow-Prozessoren programmierbar, erweiterbar und zukunftssicher?
Integration mit anderen Sicherheitsprodukten Die Integration ist für einen angemessenen mehrschichtgen Schutz und die produktübergreifende Weitergabe von Informationen zur Reaktion auf Bedrohungen, für forensische Analysen und zum Threat Hunting unerlässlich	‣ Lässt sich Ihre Firewall in eine Endpoint-Technologie integrieren? ‣ Welche Informationen werden zwischen den beiden Produkten ausgetauscht? ‣ Informieren sich die Produkte gegenseitig über erkannte Bedrohungen? ‣ Wann erfolgen nach Erkennung einer Bedrohung Reaktionsmaßnahmen? Können Bedrohungen automatisch isoliert werden? Wie läuft dieser Vorgang ab? ‣ Stellt der Endpoint der Firewall Informationen über Benutzer und die Anwendungsnutzung zur Verfügung? ‣ Können Firewall und Endpoint über dieselbe Konsole verwaltet werden? Ist die Firewall cloudbasiert? ‣ Kann produktübergreifendes Threat Hunting (XDR) durchgeführt werden? ‣ Bietet der Anbieter einen Fully-Managed Service zur Netzwerk-Überwachung und Reaktion auf Bedrohungen an? ‣ Lässt sich die Firewall mit anderen Produkten wie WLAN, ZTNA, Edge-Geräten oder Netzwerk-Switches integrieren?

Grundlegende Firewall-Funktionen

Die folgenden Technologien sind ebenfalls wichtige Komponenten jeder Firewall-Lösung. Die meisten dieser Funktionen sind ausgereifte, gut etablierte Firewall-Basisfunktionen. Daher unterscheiden sich Anbieter häufig bei der Benutzerfreundlichkeit und der gebotenen Transparenz.

Stellen Sie sicher, dass Ihre nächste Firewall nicht nur diese Funktionen umfasst, sondern auch eine einfache Verwaltung bietet – und vor allem eine bessere Transparenz über Risiken und Probleme in jedem dieser Bereiche.

Kernfunktionen	Fragen an Ihren Anbieter
Deep Packet Inspection und Intrusion Prevention Bietet Entschlüsselung und Analyse auf Bedrohungen und Exploits	▸ Unterstützt Ihre TLS Inspection den neuesten 1.3-Standard? ▸ Funktioniert die Inspection über alle Ports und Protokolle hinweg? ▸ Arbeitet sie Streaming-basiert oder Proxy-basiert? ▸ Welche Auswirkungen bestehen auf die Performance? ▸ Werden verschlüsselte Datenströme im Dashboard angezeigt? ▸ Werden im Dashboard Websites angezeigt, die keine Entschlüsselung unterstützen? ▸ Sind einfache Tools verfügbar, mit denen sich Ausnahmen für problematische Websites hinzufügen lassen? ▸ Gibt es eine umfassende Ausschlussliste? ▸ Wer pflegt die Liste und wird sie regelmäßig aktualisiert?
Modernster Schutz vor Bedrohungen Identifiziert Bots und andere komplexe Bedrohungen sowie Malware, die Call-Home-Versuche startet oder versucht, mit Command-and-Control-Servern zu kommunizieren.	▸ Verfügt Ihre Firewall über Technologie zur Erkennung bislang unbekannter Bedrohungen? ▸ Werden Dateien mittels Machine Learning analysiert? ▸ Wie viele Mashine-Learning-Modelle werden angewendet? ▸ Umfasst Ihre Lösung Sandboxing? ▸ Lässt das Sandboxing Dateien vor Abschluss der Analyse passieren? ▸ Wird die Sanboxing-Lösung vor Ort oder in der Cloud ausgeführt? ▸ Umfasst die Sandboxing-Lösung führende Endpoint-Protection-Technologie, um Bedrohungen wie Ransomware in der Sandbox-Umgebung zu identifizieren? ▸ Welche Endpoint-Technologie wird beim Sandboxing eingesetzt? ▸ Welche Reports sind standardmäßig enthalten (im Gegensatz zu einem separaten Reporting-Produkt)? ▸ Wie viel Transparenz bietet das Dashboard?
Web-Schutz und URL-Filterung Schützt vor webbasierter Malware, kompromittierten Websites und Downloads aus dem Internet.	▸ Unterstützt Ihre Firewall die FastPath-Beschleunigung von vertrauenswürdigem Datenverkehr und Elephant Flows? ▸ Erfolgt dies Software- oder Hardware-basiert? ▸ Wie werden Anwendungen für die FastPath-Beschleunigung identifiziert? ▸ Welche Richtlinien-Tools stehen Administratoren zur Verfügung, um zu kontrollieren, welche Anwendungen ausgelagert werden? ▸ Werden Signaturen mitgeliefert, um bestimmte Anwendungen zu beschleunigen und auf dem FastPath zu übertragen? ▸ Sind Ihre FastPath-Packet-Flow-Prozessoren programmierbar, erweiterbar und zukunftssicher?
Application Control Transparenz und Kontrolle über den Anwendungsverkehr, um unerwünschten Datenverkehr gezielt zu leiten oder zu blockieren und wichtigen Anwendungsverkehr zu beschleunigen und zu priorisieren	▸ Welche Informationsquellen werden zur Identifizierung von Anwendungen herangezogen? ▸ Kann die Application Engine auf Informationen vom Endpoint zurückgreifen, um die Identifizierung von Anwendungen entscheidend zu verbessern, oder ist sie auf die Informationen beschränkt, die die Firewall aus dem Paket entnehmen kann? ▸ Können Anwendungen dem FastPath zugewiesen und mithilfe von Richtlinienregeln über bevorzugte WAN-Links weitergeleitet werden? ▸ Bietet das System Dashboard-Einblicke in Cloud-Anwendungen und Schatten-IT?
VPN und SD-WAN Standort-zu-Standort- und Remote-Access-VPN-Funktionen, SD-WAN Overlays und Verwaltung mehrerer WAN-Verbindungen	▸ Lässt sich Ihre Firewall in eine Endpoint-Technologie integrieren? ▸ Welche Informationen werden zwischen den beiden Produkten ausgetauscht? ▸ Informieren sich die Produkte gegenseitig über erkannte Bedrohungen? ▸ Wann erfolgen nach Erkennung einer Bedrohung Reaktionsmaßnahmen? Können Bedrohungen automatisch isoliert werden? Wie läuft dieser Vorgang ab? ▸ Stellt der Endpoint der Firewall Informationen über Benutzer und die Anwendungsnutzung zur Verfügung? ▸ Können Firewall und Endpoint über dieselbe Konsole verwaltet werden? Ist die Firewall cloudbasiert? ▸ Kann produktübergreifendes Threat Hunting (XDR) durchgeführt werden? ▸ Bietet der Anbieter einen Fully-Managed Service zur Netzwerk-Überwachung und Reaktion auf Bedrohungen an? ▸ Lässt sich die Firewall mit anderen Produkten wie WLAN, ZTNA, Edge-Geräten oder Netzwerk-Switches integrieren?

Ergänzende Firewall-Produkte

Die folgenden ergänzenden Produkte können wichtig sein, um Ihr Netzwerk und den Schutz auf weitere Standorte auszuweiten. Stellen Sie sicher, dass diese zusätzlichen Produkte bei Ihrem Anbieter im Sortiment sind und sich einfach in Ihre Firewall integrieren lassen, entweder direkt von der Firewall und/oder über dieselbe zentrale Management-Konsole wie die Firewall.

Ergänzende Produkte	Fragen an Ihren Anbieter
SD-WAN-Edge-Geräte für Zweigstellen Kostengünstige, einfach implementierbare Geräte zur Anbindung kleiner Außenstellen	▸ Haben Sie ein Gerät im Angebot, mit dem Remote-Standorte über ein dediziertes VPN mit der Haupt-Firewall verbunden werden können? ▸ Wird eine Zero-Touch-Bereitstellung angeboten? ▸ Wie viel kostet diese? ▸ Wird sowohl ein dedizierter als auch Split-Tunnel unterstützt? ▸ Welche modularen Konnektivitätsoptionen werden unterstützt (z. B. WLAN oder LTE)?
Wireless Access Points Erweitern Sie das Netzwerk um Wireless	▸ Verfügt die Firewall über einen integrierten Wireless Controller? ▸ Wie viel kostet dieser? ▸ Sind Ihre Wireless Access Points Plug-and-Play-fähig? ▸ Werden mehrere Sender und SSIDs unterstützt? ▸ Werden Mesh-Netzwerke unterstützt?
ZTNA Zero-Trust-Netzwerkzugriff ermöglicht eine sichere Verbindung von Remote-Benutzern mit Anwendungen und Daten	▸ Bieten Sie eine ZTNA-Lösung an? ▸ Ist diese in irgendeiner Weise in Ihre Firewall und/oder Ihr Endpoint-Produkt integriert? ▸ Wird die Lösung über dieselbe zentrale Management-Konsole verwaltet wie die Firewall? ▸ Wird der ZTNA-Agent zusammen mit Ihrem Endpoint-Agenten bereitgestellt? ▸ Wie wird der Gerätestatus in Ihre ZTNA-Lösung integriert?
Email Protection Schutz für E-Mails vor Spam, Phishing und unerwünschten E-Mails	▸ Bieten Sie eine standardmäßig integrierte E-Mail-Schutzlösung an? ▸ Bieten Sie Cloud-verwalteten E-Mail-Schutz an? ▸ Ist Sandboxing verdächtiger Attachments enthalten? ▸ Werden E-Mail-Verschlüsselung und DLP unterstützt? ▸ Werden Domain-basiertes Routing und ein vollständiger MTA-Modus angeboten? ▸ Gibt es ein Benutzer-Portal zur Verwaltung der Quarantäne?
WAF Web Application Firewall für Reverse-Proxy-Schutz von lokalen Servern, die mit dem Internet verbunden sind	▸ Bieten Sie standardmäßig eine integrierte WAF-Funktion an? ▸ Vereinfacht diese die Einrichtung mit vorkonfigurierten Vorlagen für gängige Server-gehostete Anwendungen? ▸ Bietet die Funktion Hardening, CSS und Cookie-Manipulationsschutz? ▸ Beinhaltet sie Reverseproxy-Authentifizierung-Offloading?

Verwaltungsfunktionen

Die Benutzerfreundlichkeit der Verwaltung ist bei Firewall-Produkten ein wichtiges Unterscheidungsmerkmal. Viele Firewalls sind bereits seit Jahrzehnten auf dem Markt. Im Laufe der Zeit wurden viele neue Funktionen mit unterschiedlichen Benutzeroberflächen-Konzepten auf das Produkt aufgesetzt, was zu großen Unterschieden zwischen den einzelnen Produktkomponenten geführt hat. Die folgenden Funktionen können bei der Bereitstellung und täglichen Verwaltung einen großen Unterschied machen.

Verwaltungsfunktionen	Fragen an Ihren Anbieter
Zentrale Verwaltung Verwaltung mehrerer Firewalls oder IT-Sicherheitsprodukte	‣ Bieten Sie eine Cloud-Management-Lösung an? ‣ Wie werden über diese Lösung mehrere Firewalls verwaltet? ‣ Welche anderen Produkte werden über dieselbe Cloud-Konsole verwaltet? ‣ Werden zwischen den Produkten Bedrohungsdaten ausgetauscht und ist produktübergreifendes Threat Hunting möglich?
Reporting Welche Reporting-Funktionen werden angeboten?	‣ Speichert die Firewall Protokolldaten auf der Box („on-box")? In welchem Umfang? ‣ Ist On-Box-Reporting inklusive? Wie viel kostet es? ‣ Wird Cloud-Reporting unterstützt? Wie viel kostet es? ‣ Können benutzerdefinierte Reports erstellt, gespeichert, exportiert oder geplant werden? ‣ Wird ein Syslog-Export unterstützt? ‣ Werden produktübergreifendes Reporting und Threat Hunting unterstützt?
Verwaltungskomfort Wie gut vereinfacht die Firewall die tägliche Verwaltung und hebt wichtige Informationen hervor?	‣ Bietet Ihr Produkt ein umfassendes Dashboard mit Drill-Down-Funktionen? ‣ Befinden sich Richtlinien für Web, App Control, IPS und Traffic Spaping an einem zentralen Ort oder muss ich diese Komponenten in verschiedenen Bereichen des Produkts einrichten? ‣ Ist das Benutzererlebnis innerhalb der einzelnen Produktkomponenten konsistent? ‣ Gibt es umfangreiche integrierte kontextbezogene Hilfefunktionen, Begleitmaterialien, Videos und andere Inhalte für neue Firewall-Kunden?
Benutzerportal Portal für Benutzer zur Selbsthilfe	‣ Gibt es bei Ihrer Firewall ein Benutzerportal, über das Benutzer VPN Clients und Einstellungen herunterladen sowie Quarantäne-E-Mails verwalten können?

Bereitstellungsoptionen

Ein weiterer wichtiger Faktor bei der Wahl Ihrer nächsten Firewall ist die Frage, wie einfach sich die Firewall heute und in Zukunft in Ihr Netzwerk integrieren lässt. Sie benötigen eine Firewall, die zu Ihrem Netzwerk passt, und keine, auf die sich Ihr Netzwerk anpassen muss. Stellen Sie sicher, dass Ihr Anbieter eine Vielzahl von Bereitstellungsoptionen anbietet, einschließlich Unterstützung von Public Cloud-Plattformen wie AWS und Azure sowie beliebte Virtualisierungsplattform und flexible, modulare Hardware-Appliance-Optionen.

Bereitstellungsoptionen	Fragen an Ihren Anbieter
Hardware-Appliances Stellen Sie sicher, dass Ihre nächste Firewall so zukunftssicher wie möglich ist	‣ Wie viele Appliance-Modelle bieten Sie an, die meinen Anforderungen entsprechen? ‣ Welche Anschlussmöglichkeiten sind enthalten? ‣ Welche modularen Anschlussmöglichkeiten sind enthalten? ‣ Sind redundante Stromversorgungen erhältlich? ‣ Welche Hochverfügbarkeitsoptionen werden angeboten? ‣ Sind Firmware-Upgrades in der Lizenz enthalten? ‣ Welche Hardware-Gewährleistung wird angeboten?
Cloud, virtuell, Software Public-Cloud- und virtuelle Unterstützung für Hybrid-Netzwerke, die heute oder in Zukunft wichtig sein könnte	‣ Ist Ihre Firewall über Marktplätze für Public-Cloud-Plattformen wie AWS und Azure erhältlich? ‣ Unterstützen Sie alle gängigen Virtualisierungsplattform? ‣ Ist Ihre Appliance als Softwarelösung zur Ausführung auf X86-Hardware erhältlich?

Firewall-Funktionen – Checkliste

	Sophos	Cisco	Fortinet	PAN	SW	WG
Grundlegende Firewall-Funktionen						
Testsimulator für Firewall-Regeln und Web-Richtlinien	✓		✓	✓		✓
FastPath Packet Optimization	✓		✓	✓		
Intrusion Protection System	✓	✓	✓	✓	✓	✓
Application Control	✓	Teilweise	✓	✓	✓	✓
Zwei Antivirus-Engines	✓					✓
Cloud App Visibility für Schatten-IT	✓		✓	✓	✓	✓ - OEM
Blockierung potenziell unerwünschter Anwendungen (PUAs)	✓		✓	✓	✓	
Web Protection and Control	✓	✓	✓	✓	✓	✓
Web Keyword Monitoring und Durchsetzung	✓		✓	✓	✓	✓
DPI Engine: Streaming, Proxy oder beides?	✓	Flow	✓	Flow	Stream	Proxy
Transparenz über Benutzer- und Anwendungsrisiko (User Threat Quotient)	✓		Eingeschränkt			
Modernster Schutz vor Bedrohungen	✓	✓	✓	✓	✓	✓
On-Box-Protokollierung und Verlaufsreports	✓		Eingeschränkt	Eingeschränkt		

	Sophos	Cisco	Fortinet	PAN	SW	WG
Server und Email Protection						
Sofort einsatzbereite WAF mit vollem Funktionsumfang	✓					
Integrierter E-Mail-Schutz: Antivirus, Anti-Spam, Verschlüsselung, DLP	✓					

	Sophos	Cisco	Fortinet	PAN	SW	WG
Core VPN und SD-WAN						
Unbegrenztes kostenloses Remote Access VPN mit vollem Funktionsumfang	✓	Aufpreis*	✓	Aufpreis*	Aufpreis*	Aufpreis*
IPSEC- und SSL-Standort-zu-Standort-VPN	✓	✓	✓	✓	✓	✓
SD-RED Layer-2 Standort-zu-Standort-VPN	✓					
Standortübergreifende SD-WAN-VPN-Orchestrierung über die Cloud	In Kürze	✓	Aufpreis*			
SD-WAN Routing und Link Management	✓	✓	✓	✓	✓	✓

	Sophos	Cisco	Fortinet	PAN	SW	WG
TLS Inspection						
TLS 1.3 Inspection	✓		✓	✓	✓	✓
Dashboard-Transparenz über Probleme mit verschlüsseltem Datenverkehr	✓					
Erstellen von TLS-Ausnahmen über das Dashboard	✓					

* Diese Funktionen sind gegen Aufpreis erhältlich

	Sophos	Cisco	Fortinet	PAN	SW	WG
Zero-Day-Bedrohungsschutz						
Analyse verdächtiger Dateien mithilfe mehrerer ML-Modelle	✓	✓	✓	✓	✓	
Dynamisches Sandboxing verdächtiger Dateien	✓	✓	✓	✓	✓	✓
Cloudbasierte Dateianalyse	✓	✓	✓	✓	✓	✓
Große Auswahl integrierter Reports zur Bedrohungsanalyse	✓	✓			✓	
SD-WAN Routing und Link Management	✓	✓	✓	✓	✓	✓

	Sophos	Cisco	Fortinet	PAN	SW	WG
FastPath Packet Optimization						
FastPath Offloading von SD-WAN-, Cloud- und SaaS-Datenverkehr	✓		✓	✓		
Richtlinie und automatisches FastPath Offloading	✓		✓	✓		
Hardware-Offloading und -Beschleunigung	✓		✓	✓		
Programmierbare Packet-Flow-Prozessoren	✓			✓		

	Sophos	Cisco	Fortinet	PAN	SW	WG
Endpoint-Protection-Integrationsfunktionen						
Identifizierung kompromittierter Hosts	✓	✓	Aufpreis*	✓	✓	✓
Automatisches Isolieren von Hosts an der Firewall von anderen Teilen des Netzwerks	✓					✓
Automatisches Isolieren von Hosts auf EP-Ebene, um laterale Bewegungen zu verhindern	✓			Aufpreis*		✓
Erkennen unbekannter Netzwerkanwendungen (Synchronized App Control)	✓			✓		
Möglichkeit zum Aktivieren von produktübergreifendem Threat Hunting (XDR)	✓			✓		
Möglichkeit zur Inanspruchnahme eines Fully Managed Threat Response Service	✓			✓		

	Sophos	Cisco	Fortinet	PAN	SW	WG
Integration ins Network-Access-Portfolio						
Integrierte Wireless-Controller- und Access-Point-Lösung	✓	✓	✓		✓	✓
Integration in ZTNA-Lösung	✓	✓	✓	✓	✓	
Integration in Netzwerk-Switch-Produkte	In Kürze	✓	✓		✓	
Integration mit Remote Service Access Edge-Geräten (SD-RED)	✓					

* Diese Funktionen sind gegen Aufpreis erhältlich

	Sophos	Cisco	Fortinet	PAN	SW	WG
Cloud-Verwaltung						
Firewall-Verwaltung mit vollem Funktionsumfang über die Cloud – ohne Aufpreis	✓	✓	Aufpreis*		Aufpreis*	✓
Eine einzige Cloud-Konsole für EP, Server, mobile Geräte, E-Mails, Verschlüsselung und Firewall	✓					✓
Group Firewall Management über die Cloud	✓	✓	Aufpreis*		✓	
Planen von Firmware-Updates über die Cloud	✓	✓	✓		✓	✓
Bereitstellen neuer Firewalls über die Cloud (Zero-Touch)	✓	✓	Aufpreis*		✓	✓
Cloud Firewall Reporting	✓	✓	✓		✓	✓
Über die Cloud verwaltetes, produktübergreifendes Threat Hunting (XDR)	Aufpreis*			Aufpreis*		

	Sophos	Cisco	Fortinet	PAN	SW	WG
Virtuelle und Cloud-Bereitstellungsoptionen						
AWS	✓	✓	✓	✓	✓	✓
Azure	✓	✓	✓	✓	✓	✓
Google	In Zukunft	✓	✓	✓		
Nutanix	✓		✓	✓	✓	
FWaaS	In Zukunft		✓	✓		
Virtualisierungsplattformen	✓	✓	✓	✓	✓	✓
Software-Appliance (x86)	✓					

* Diese Funktionen sind gegen Aufpreis erhältlich

Sophos Firewall

Weitere Informationen über die Sophos Firewall erhalten Sie in den folgenden Begleitmaterialien:

- Sophos Firewall Solution Brief
- Sophos Firewall Feature-Liste
- Sophos Firewall Broschüre

Jetzt kostenfrei testen

XGS Firewall jetzt kostenlos online testen unter www.sophos.de/demo

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

21-06-10 DE (DD)

SOPHOS