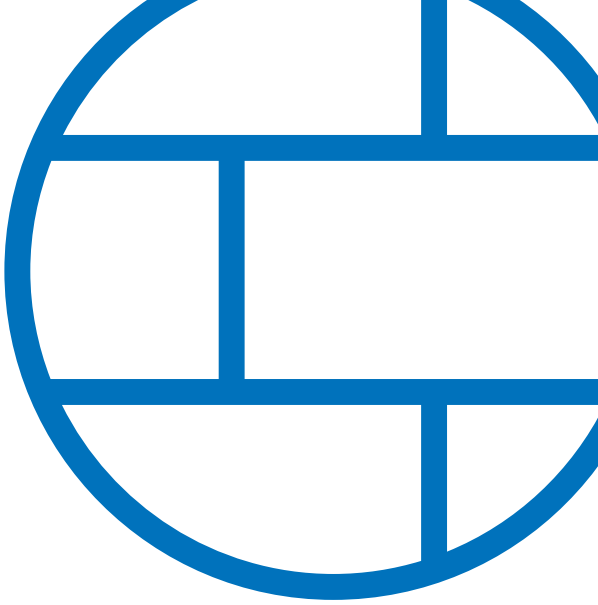
SOPHOS
Cybersecurity made simple.



Next-Gen Firewall Buyers Guide

Bei einer Befragung baten wir IT-Netzwerk-Manager, uns die größten Probleme mit ihrer derzeitigen Firewall zu nennen. Diese Probleme schilderten Sie uns:

- Transparenz über Anwendungsverkehr, Risiken und Bedrohungen
- Schutz vor komplexen Bedrohungen
- 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 gehen auf alle Features und Funktionen ein, auf die Sie beim Kauf Ihrer nächsten Firewall achten sollten. Außerdem haben wir eine Reihe wichtiger Fragen für Sie zusammengestellt, die Sie Ihrem IT-Partner oder -Anbieter stellen sollten, um herauszufinden, ob das jeweilige Produkt auch wirklich Ihre Anforderungen erfüllt. Auf der letzten Seite finden Sie zudem eine praktische Übersicht, die Ihnen dabei hilft, geeignete Firewall-Anbieter in die engere Auswahl zu ziehen.

Next-Generation Firewall Awareness und Control

Die Anbieter von Next-Gen-Firewalls werben seit langem damit, Transparenz über den Anwendungsverkehr und das Nutzungsverhalten im Netzwerk zu schaffen, jedoch scheitern die meisten an dieser wichtigen Aufgabe. Dies liegt an der traditionellen, signaturbasierten Technologie zur Identifizierung von Anwendungen, die alle modernen Firewalls nutzen. Sie ist nicht mehr wirksam bei der Erkennung von verschlüsselten, evasiven oder benutzerdefinierten Anwendungen oder von Anwendungen, die sich mit generischen HTTP oder HTTPS als Internet-Browser tarnen. Deshalb werden P2P-Anwendungen, VPN-Tunnel-Clients und Games in den meisten Netzwerken überhaupt nicht erkannt. Es werden neue Vorgehensweisen und Technologien zur Lösung dieses Problems benötigt.

Um adäquate Next-Generation Awareness und Control zu bieten, muss Ihre Firewall über vier Schlüsseltechnologien verfügen:

Application Control – Application Control ermöglicht Ihnen, wichtigen Anwendungsverkehr zu priorisieren und unerwünschten Datenverkehr zu beschränken oder zu blockieren. Die meisten Next-Gen-Firewalls sind oft nicht in der Lage, für genügend Transparenz und Kontrolle zu sorgen, da die Effektivität signaturbasierter Erkennungstechniken für Anwendungen beschränkt ist. Daher sollten Sie darauf achten, dass Ihre nächste Firewall unterschiedliche und innovative Techniken zur Lösung dieses Problems nutzt. So werden Hunderte von Anwendungen erkannt, die in Ihrem Netzwerk bislang vermutlich unerkannt bleiben.

Web Control – URL-Filter-Richtlinien sind wichtig zur Durchsetzung der Compliance und gewährleisten eine sichere Umgebung für alle Benutzer, insbesondere im Bildungswesen. Zwar verfügen mittlerweile fast alle Firewalls über diese Funktion, es gibt jedoch eklatante Unterschiede bei der Benutzerfreundlichkeit, mit der komplexe benutzer- und gruppenbasierte Richtlinien implementiert und täglich verwaltet werden können. Sorgen Sie dafür, dass Ihre nächste Firewall einfache und flexible Richtlinientools bietet, mit denen die tägliche Verwaltung einfach und zeitsparender wird.

Transparenz über Risiken – Informationen über Ihre riskantesten Benutzer und Anwendungen sind entscheidend, damit Sie geeignete Richtlinien durchsetzen können, bevor es zu einem schweren Sicherheitsvorfall kommt. Stellen Sie sicher, dass Ihre nächste Firewall einen Report zur Risikobewertung für Benutzer generieren kann, der Netzwerkaktivitäten korreliert, um die riskantesten Benutzer zu identifizieren. Dazu sollte es klare Hinweise geben bei riskanter Nutzung von Cloud-Anwendungen, Schatten-IT, riskanten Downloads, bedenklichen Websites und vorhandenen Bedrohungen.

HTTPS-Scans – Da der meiste Internet-Verkehr heutzutage verschlüsselt ist, kann eine lückenlose Compliance-Durchsetzung nur mit adäquaten HTTPS-Scans sichergestellt werden. HTTPS-Scans können allerdings in einigen Fällen aufdringlich und störend sein. Daher sollten Sie darauf achten, dass Ihre nächste Firewall selektive Scans und einfache Lösungen zur Verwaltung von Ausschlüssen bietet.

Empfohlene Funktionen	Beschreibung	Fragen an Ihren Anbieter
Transparenz und Kontrolle über Anwendungen	Nur wenn Sie wissen, welche Anwendungen tatsächlich genutzt werden, können Sie sinnvolle Entscheidungen darüber treffen, welche Anwendungen erlaubt, priorisiert oder blockiert werden sollen. So nutzen Sie Ihre Bandbreite optimal aus und verschwenden keine Zeit damit, Anwendungen zu blockieren, die gar keine Probleme verursachen. In den Reports der meisten Firewalls erscheint ein Großteil des Netzwerkverkehrs als „nicht klassifiziert" oder als „normaler Internet-Verkehr". Das liegt daran, dass viele Anwendungen benutzerdefiniert, verschleiert oder evasiv sind oder aber generisches HTTP oder HTTPS verwenden und daher unerkannt bleiben.	‣ Kann Ihre Firewall mit den Hosts im Netzwerk zur Erkennung aller evasiver oder unbekannter Anwendungen integriert werden, die verschlüsselten oder HTTP-Datenverkehr erzeugen? ‣ Können Sie einen Beispiel-Firewall-Report zur Verfügung stellen, aus dem hervorgeht, welcher Datenverkehr tatsächlich identifiziert wurde? ‣ Können Sie mit Ihrer Anwendungskontrolle die Nutzung von Anwendungen für einzelne Benutzer oder Gruppen nachverfolgen und benutzer- oder gruppenbasierte Richtlinien durchsetzen? ‣ Kann die Anwendungskontrolle nach Kategorie, Risikostufe, Technologie oder Eigenschaften (z. B. unsachgemäßer Gebrauch, geringe Produktivität) erfolgen?
Traffic Shaping für Web und Anwendungen	Erweiterte Traffic Shaping (QoS)-Optionen nach Web-Kategorie oder Anwendung zur Beschränkung oder Garantie von Upload/Download oder komplette Datenverkehrspriorität und individuelle oder geteilte Bitrate	‣ Ermöglicht Ihre Lösung Traffic Shaping oder QoS auf Anwendungs-, Kategorie-, Benutzer-, Gruppen- oder Regelbasis?
URL-Filterung	Kontrolliert die Internet-Nutzung, um nicht richtlinienkonformes Surfen zu unterbinden und unangemessene Inhalte und Malware aus dem Netzwerk fernzuhalten.	‣ Verfügt Ihre Firewall über eine auf Vererbung basierende Web-Gateway-Richtlinien-Engine? Müssen Sie beispielsweise eine komplett neue Web-Richtlinie erstellen, wenn Sie nur eine kleine Änderung für einen Benutzer vornehmen möchten? Oder müssen Sie explizit nur das angeben, was geändert werden soll, und können die übrigen Einstellungen von bereits bestehenden Richtlinien übernehmen? Sind vorkonfigurierte Richtlinien für Arbeitsplätze, CIPA-Compliance usw. vorhanden? ‣ Kann die Firewall neben einfachem Blockieren auch vor potenziell unangemessenen Websites warnen und dem Benutzer die Entscheidung überlassen, ob er fortfahren möchte? ‣ Verfügt Ihre Firewall über Funktionen zum Web Keyword Monitoring und kann ich eigene Listen hochladen, die für meine Branche oder Region relevant sind?
Web-Compliance-Funktionen	Stellt Compliance sicher und erkennt riskantes Verhalten beim Surfen, Suchen oder Nutzen von Google Apps.	‣ Kann Ihre Web-Control-Lösung unsere Google Apps-Domain durchsetzen? ‣ Setzt sie SafeSearch- und YouTube-Beschränkungen mit benutzer- oder gruppenbasierten Richtlinien durch? ‣ Kann eine zusätzliche Bild-Filterung durchgesetzt werden (z. B. nur Bilder mit Creative Commons-Lizenz)? ‣ Kann sie potenziell problematische Verhaltensweisen in Zusammenhang mit Themen wie Mobbing, Selbstverletzung oder Radikalisierung basierend auf dynamischer Inhaltsfilterung und Keyword Monitoring erkennen? ‣ Können Mitarbeiter wie z.B. Lehrkräfte vorübergehende Richtlinien-Ausnahmen für Benutzer oder Gruppen festlegen?
Risikobewertung – Benutzer	Gibt einen Überblick über die riskantesten Benutzer auf Basis ihrer Netzwerkaktivitäten und ihres aktuellen Verlaufs.	‣ Gibt Ihre Firewall Einblick in hochriskante Benutzer auf Basis ihres aktuellen Netzwerkverhaltens und ihrer Netzwerkaktivitäten? ‣ Gibt es ein Widget auf dem Dashboard? ‣ Gibt es einen vollständigen detaillierten Report?
Risikobewertung – Anwendungen	Misst das Gesamtrisiko Ihres Unternehmensnetzwerks.	‣ Nimmt Ihre Firewall eine Bewertung des Anwendungsgesamtrisikos vor? ‣ Gibt es detaillierte Verlaufsreports zur Nutzung von Anwendungen?
HTTPS-Scanning	Ermöglichen Einsicht in verschlüsselten Internetverkehr, um die Compliance sicherzustellen.	‣ Bietet Ihre Firewall eine HTTPS-Man-in-the-Middle-Entschlüsselung? ‣ Gibt es Optionen zur Handhabung von Ausschlüssen? ‣ Können unbekannte SSL-Protokolle und ungültige Zertifikate blockiert werden?

Die Bedeutung einer mehrschichtigen Bedrohungsabwehr

Cyberkriminelle ändern ständig ihre Methoden, um nicht entdeckt zu werden. Heutzutage ist fast jede Malware eine neue Zero-Day-Variante, die raffinierter, verschleierter und gezielter ist als ihre Vorgänger. Dagegen sind herkömmliche signaturbasierte Erkennungstechnologien machtlos. Sie benötigen mehrschichtige Abwehrmaßnahmen, die eine Vielzahl von Vektoren abdecken, jeweils Verhaltensanalysen, Deep Learning und andere Next-Gen-Techniken anwenden, um adäquaten Schutz zu bieten.

Um moderne Bedrohungen hinreichend abwehren zu können, benötigen Sie an Ihrer Netzwerkgrenze sieben Schlüsseltechnologien:

Advanced Threat Protection – Advanced Threat Protection ist entscheidend, um Bots, APTs und andere Bedrohungen zu identifizieren, die in Ihrem Netzwerk operieren. Stellen Sie sicher, dass Ihre nächste Firewall über Malicious Traffic Detection, Botnet Detection und Command and Control (C&C) Call-Home Traffic Detection verfügt. Die Firewall sollte einen kombinierten Ansatz aus IPS, DNS und Web-Telemetrie nutzen, um Call-Home-Traffic zu identifizieren. Sie sollte zudem nahtlos mit den Hosts im Netzwerk zusammenarbeiten, um Transparenz über deren Sicherheit und eine eventuelle Kompromittierung haben.

Identifizieren und Isolieren kompromittierter Systeme – Um Datenverluste und weitere Infektionen zu verhindern und die Bereinigung zu beschleunigen, sollte Ihre Firewall bei einem Zwischenfall in der Lage sein, den infizierten Host, den Benutzer und den Prozess sofort zu identifizieren. Idealerweise sollte sie auch kompromittierte Systeme bis zu deren Analyse und Bereinigung automatisch blockieren oder isolieren.

Intrusion Prevention – Intrusion-Prevention-Systeme (IPS) können erkennen, wenn Hacker versuchen, sich Zugang zu Ihren Netzwerk-Ressourcen zu verschaffen. Stellen Sie sicher, dass Ihre Firewall über ein Next-Gen IPS verfügt, das in der Lage ist, komplexe Angriffsmuster in Ihrem Netzwerkverkehr zu identifizieren. So können Sie Hacking-Versuche und Malware erkennen, die sich seitwärts über Netzwerksegmente fortbewegt. Ziehen Sie außerdem eine Lösung in Betracht, mit der Sie ganze Geo-IP-Bereiche für Regionen blockieren können, in denen Ihr Unternehmen nicht tätig ist. So können Sie Ihre Angriffsfläche weiter verringern.

Sandboxing – Sandboxing kann neueste evasive Malware und komplexe Bedrohungen wie Ransomware und Botnet-Malware einfach abfangen, bevor diese auf Ihre Computer gelangen. Stellen Sie sicher, dass Ihre Firewall über eine leistungsstarke Sandboxing-Funktion mit modernsten Technologien wie Deep Learning, Exploit-Erkennung, Ransomware-Erkennung, Verhaltensanalyse, Netzwerkaktivität und Speichernutzung verfügt.

Web Protection – Effektive Web Protection kann bereits im Vorfeld verhindern, dass moderne webbasierte Bedrohungen wie Cryptojacking- und Botnet-Malware überhaupt in Ihr Netzwerk gelangen. Stellen Sie sicher, dass Ihre Firewall über zwei Antivirus-Engines und eine verhaltensbasierte Web Protection verfügt. Diese sollte in der Lage sein, JavaScript-Code in Web-Inhalten zu emulieren bzw. zu simulieren, um festzustellen, welche Absichten und Verhaltensweisen vorliegen, bevor die Inhalte an den Browser des Benutzers übermittelt werden.

Email Protection – E-Mails sind nach wie vor der Haupteintrittspunkt für Bedrohungen und Social Engineering Exploits. Achten Sie darauf, dass Ihre nächste Firewall oder E-Mail-Filter-Lösung über leistungsstarke Anti-Spam- und Anti-Phishing-Technologien verfügt, damit Sie neueste Malware in E-Mails und E-Mail-Anhängen erkennen können.

Web Application Firewall – Eine WAF kann Ihre Server, Geräte und Geschäftsanwendungen vor Hacks schützen. Falls Sie interne Server oder Geschäftsanwendungen verwalten, die den Zugriff auf das Internet erfordern, sollten Sie unbedingt darauf achten, dass Ihre Firewall umfassenden WAF-Schutz bietet. Eine Web Application Firewall sollte einen Reverseproxy und Offload-Authentifizierung beinhalten und die Systeme außerdem gegen Hacking-Versuche härten.

Empfohlene Funktionen	Beschreibung	Fragen an Ihren Anbieter
Advanced Threat Protection	Identifiziert Bots und andere komplexe Bedrohungen sowie Malware, die Call-Home-Versuche startet oder versucht, mit Command-and-Control-Servern zu kommunizieren.	› Wie leistungsstark ist die Advanced Threat Protection Ihrer Firewall? › Werden Informationen aus verschiedenen Quellen koordiniert, um schädlichen Datenverkehr zu erkennen, oder wird nur auf eine einfache Botnet-Datenbank zurückgegriffen? › Kann Ihre Firewall mit den Hosts im Netzwerk integriert werden und Kompromittierungen erkennen, auch wenn es im Netzwerk keine Anzeichen dafür gibt?
Erkennen kompromittierter Systeme	Identifiziert infizierte Systeme in Ihrem Netzwerk.	› Kann Ihre Firewall den infizierten Host, Benutzer und Prozess exakt identifizieren? › Ist Ihre Firewall über den Integritätsstatus der Endpoints informiert? › Können Sie den Integritätsstatus Ihrer Endpoints auf einen Blick einsehen?
Isolieren kompromittierter Systeme	Nutzt Firewall-Regeln, um kompromittierte Systeme zu isolieren, bis diese bereinigt werden können.	› Kann Ihre Firwall infizierte oder möglicherweise kompromittierte Systeme im Netzwerk ohne Eingreifen des Benutzers oder Administrators automatisch isolieren? › Wird der normale Zugriff automatisch wiederhergestellt, sobald die Endpoints bereinigt wurden?
Sandboxing	Schützt vor Zero-Day-Bedrohungen, indem potenziell schädliche Dateien zur Cloud Sandbox gesendet und dort in einer sicheren Umgebung kontrolliert ausgeführt und beobachtet werden.	› Muss ich zusätzliche Hardware anschaffen, um ergänzende Schutzschichten zu implementieren? › Wie viel Zeit benötigt Ihre Lösung zur Analyse verdächtiger Dateien? › Nutzt Ihre Sandboxing-Lösung Next-Gen-Technologien wie Deep Learning, Exploit- und Verschlüsselungserkennung zur Identifizierung von Zero-Day-Bedrohungen wie komplexer Ransomware?
Web Protection	Schützt vor webbasierter Malware, kompromittierten Websites und Downloads aus dem Internet.	› Bietet Ihre Web Protection Engine signaturlose Verhaltensanalysen von Web-Code wie JavaScript? › Kann Ihre Web Protection auf mehrere Antivirus-Engines zurückgreifen? › Sind Live-Updates verfügbar?
HTTPS-Scanning	Bietet Einblick in verschlüsselten Internet-Datenverkehr, um das Netzwerk vor Bedrohungen zu schützen, die über HTTPS übertragen werden können.	› Bietet Ihre Firewall eine HTTPS-Man-in-the-Middle-Entschlüsselung? › Gibt es Optionen zur Handhabung von Ausschlüssen? › Können unbekannte SSL-Protokolle und ungültige Zertifikate blockiert werden?
Anti-Spam und Anti-Phishing für E-Mails	Stoppt die Zustellung von Spam, Phishing und anderen unerwünschten E-Mails in die Posteingänge von Mitarbeitern.	› Wie hoch sind Ihre Spamerkennungs- und False Positive-Raten? › Mit welchen Verfahren identifizieren Sie Spam und Phishing? › Bietet Ihre E-Mail-Lösung Domain-basiertes Routing und einen vollständigen MTA-Modus zum Speichern und Weiterleiten von Nachrichten? › Gibt es ein Benutzer-Portal zur Verwaltung der Quarantäne?
Web Application Firewall	Schützt Server und Geschäftsanwendungen, die über das Internet erreichbar sind.	› Verfügt Ihre Firewall über eine WAF? › Gibt es Vorlagen? › Schützt sie vor Hacks und Angriffen mit Form Hardening, URL Hardening, Cookie-Manipulationsschutz und Cross-Site-Scripting-Schutz? › Beinhaltet sie einen Reverseproxy mit Authentifizierungs-Offloading?

Firewall-Lösungen vergleichen

Beim Vergleich von Firewall-Lösungen sollten Sie neben Sicherheits- und Kontrollfunktionen eine Reihe weiterer Punkte beachten.

VPN- und Wireless-Konnektivität

Jede Firewall-Lösung sollte über Standort-zu-Standort- und Remote-Zugriff-VPN verfügen. Stellen Sie sicher, dass Ihre nächste Firewall alle von Ihnen benötigten standardbasierten VPN-Anbindungen unterstützt, und prüfen Sie, welche anderen Optionen zur Verbindung von Benutzern mit internen Ressourcen bzw. zur Absicherung Ihrer Remote-Standorte verfügbar sind. Achten Sie darauf, dass diese anderen Optionen leichtgewichtig und einfach sind.

WLAN gehört in praktisch jedem Netzwerk heute zum Standard. Ziehen Sie daher eine Firewall in Betracht, die mit einem funktionsstarken Wireless Controller ausgestattet ist, der eine Vielzahl von Hochleistungs-Wireless-Access-Points unterstützt.

Flexible Bereitstellungsoptionen

Achten Sie bei der Wahl Ihrer nächsten Firewall-Lösung darauf, dass diese zu Ihrem Unternehmen passt und nicht andersherum. Berücksichtigen Sie nicht nur Ihre aktuelle Topologie und Infrastruktur, sondern auch die zukünftige Entwicklung in ein oder mehreren Jahren. Entscheiden Sie sich unbedingt für eine Firewall, die eine flexible Auswahl an lokalen und Cloud-Bereitstellungsmodellen mit darauf abgestimmten Verwaltungstools bietet. Wenn Sie mehrere kleine Remote-Standorte haben, sollten Sie berücksichtigen, wie Sie diese sicher und ohne viel Kosten- und Zeitaufwand an Ihr Netzwerk anbinden können.

Performance

Berücksichtigen Sie unbedingt Ihre Anforderungen an die Netzwerk-Performance. Planen Sie dabei nicht zu knapp, um auch für wachsende Anforderungen an Ihr Netzwerk in der Zukunft gewappnet zu sein. Benutzer nutzen mehrere Geräte und immer mehr Services ziehen in die Cloud um. Demzufolge werden Netzwerk-Bandbreite und Firewall-Durchsatz immer höheren Belastungen ausgesetzt.

Entscheiden Sie sich für eine Lösung, die Sie einfach skalieren und mit Funktionen wie Hochverfügbarkeit und WAN Link Balancing für Redundanz oder Performance auf Ihre wachsenden Anforderungen anpassen können. Achten Sie außerdem auf Firewalls mit leistungssteigernden Technologien wie FastPath Packet Optimization, die bekannten Datenverkehr zur Beschleunigung der Performance über den Schnellpfad durch den Firewall Stack schicken.

Integration mit anderen IT-Security-Lösungen

Die Integration von IT-Security-Lösungen (z. B. Firewall und Endpoint) bietet entscheidende Vorteile, u. a. koordinierter Schutz, sofortige Identifizierung infizierter Systeme im Netzwerk, verbesserte App-Control-Funktionen und automatische Reaktion durch Isolieren infizierter Systeme bis zur Bereinigung. Dieses relativ neue Prinzip der Sicherheits-Synchronisierung hat sich als äußerst effektiv erwiesen und wird von immer mehr Unternehmen als unverzichtbare Funktion eingestuft. Entscheiden Sie sich nach Möglichkeit für einen Anbieter, der führende Technologien sowohl im Bereich Firewall als auch in anderen IT-Security-Bereichen wie Endpoint-, Server-, Daten- und Mobile-Security vorweisen kann sowie eine koordinierte und synchronisierte Zusammenarbeit dieser Komponenten ermöglicht.

Reporting und Alarmmeldungen

Wie bereits erwähnt, ist mangelnde Transparenz über die Vorgänge im Netzwerk eines der Hauptprobleme heutiger Firewalls. Um diesem Problem aus dem Weg zu gehen, sollten Sie sich für eine Firewall entscheiden, die umfassende Verlaufsreports beinhaltet mit der Option, bei Bedarf ein zentrales Reporting für alle Firewalls in Ihrer Umgebung zu ergänzen. Prüfen Sie außerdem, wie viel Transparenz die Firewall im Dashboard und in anderen wichtigen Bereichen der Firewall bietet. Vermeiden Sie Firewalls, bei denen Sie viel Zeit für die Suche nach erforderlichen Informationen aufwenden müssen.

Benutzerfreundlichkeit

Die Konfiguration und Verwaltung einer Firewall kann je nach Modell einfach bis nervenaufreibend sein. Sie sollten nicht bei der Einrichtung Ihrer Firewall verzweifeln müssen, weil der Anbieter keinen Wert auf Benutzerfreundlichkeit gelegt hat. Entscheiden Sie sich für eine Lösung, die denkt wie Sie und von einem Anbieter stammt, dem es wichtig ist, die tägliche Verwaltung für Sie so einfach und effizient wie möglich zu gestalten.

Ein weiterer zeitsparender Faktor wird häufig übersehen: Ihre Nutzer sollten die Möglichkeit haben, sich in bestimmten Fällen selbst zu helfen. Suchen Sie nach einer Firewall, die ein sicheres Self-Service-Portal für Benutzer zum Download von VPN-Clients und zur Verwaltung der E-Mail-Quarantäne bietet.

Direktvergleich

Entscheiden Sie anhand der Checkliste zum Produktvergleich auf der folgenden Seite, welche Lösungen Sie in die engere Auswahl nehmen möchten. Testen Sie diese Lösungen anschließend und bewerten Sie das Preis-Leistungs-Verhältnis.

Checkliste zum Produktvergleich

Nachdem Sie anhand der vorhergehenden Abschnitte Ihre Mindestanforderungen ermittelt haben, können Sie mit der folgenden Tabelle die verschiedenen Lösungen vergleichen und entscheiden, welche in die engere Auswahl kommen. Bei Bedarf können Sie die Checkliste mit spezifischen Anforderungen Ihres Unternehmens ergänzen.

	Sophos XG	Cisco Meraki	Fortinet FortiGate	SonicWall NSA	WatchGuard Firebox
NEXT-GEN FIREWALL FEATURES					
Testsimulator für Firewall-Regeln und Web-Richtlinien	✓		✓		✓
Zwei Antivirus-Engines	✓				
FastPath Packet Optimization	✓		✓		
Intrusion Protection System	✓	✓	✓	✓	✓
Application Control	✓	Teilweise	✓	✓	✓
Synchronized App Control (auf Basis von Endpoint-Telemetrie)	✓				
Cloud App Visibility für Schatten-IT	✓		✓	✓	
Blockierung potenziell unerwünschter Anwendungen (PUAs)	✓		✓	✓	
Web Protection and Control	✓	✓	✓	✓	✓
Web Keyword Monitoring und Durchsetzung	✓		✓	✓	✓
Transparenz über Benutzer- und Anwendungsrisiko (UTQ)	✓		Teilweise		
Filterung von HTTPS-Daten	✓	✓	✓	✓	✓
ADVANCED THREAT PROTECTION					
Advanced Threat Protection	✓	✓	✓	✓	✓
Erkennen kompromittierter Systeme	✓		+1Box *		
Isolieren kompromittierter Systeme	✓		+1Box *		
Lateral Movement Protection	✓				
Sandboxing	✓	✓	✓	✓	✓
SERVER und EMAIL PROTECTION					
Funktionsstarke WAF	✓		+1Box *	+1Box *	
Komplette E-Mail-Security: Antivirus, Anti-Spam, Verschlüsselung, DLP	✓		+1Box *	+1Box *	

	Sophos XG	Cisco Meraki	Fortinet FortiGate	SonicWall NSA	WatchGuard Firebox
ANBINDUNG VON BENUTZERN/REMOTE-STANDORTEN					
IPSec und SSL VPN	✓	Kein SSL VPN	✓	✓	✓
HTML5 VPN Portal	✓		✓	✓	
Vermaschte WLANs	✓	✓	✓	✓	✓
Sofort einsetzbare Lösung zur Sicherung von Außenstellen (RED)	✓				
EINFACHE BEREITSTELLUNG UND NUTZUNG					
Flexible Bereitstellung (HW, SW, WM, IaaS)	✓	Nur HW	Keine SW	Keine SW	Keine SW
Mögliche Integration mit anderen IT-Security-Produkten (z. B. Endpoint)	✓		✓	✓	
Synchronized Security in Discover (TAP)-Modus-Bereitstellungen	✓				
Vollständige Verlaufsreports	✓		+1Box *	+1Box *	+1Box *
Kostenlose zentrale Verwaltung	✓	✓	Teilweise		
Zentrale Verwaltung für Partner	✓	✓	✓	✓	
Self-Service-Portal für Benutzer	✓		✓	✓	

* Zur Nutzung dieser Funktionen benötigen Sie ein zusätzliches Produkt/Gerät. Dadurch entstehen Ihnen mehr Kosten und Komplexität.

In diesem Dokument enthaltene Aussagen basieren auf öffentlich verfügbaren Informationen (Stand: November 2018). Dieses Dokument wurde von Sophos und nicht von den anderen aufgeführten Anbietern erstellt. Änderungen der Eigenschaften und Funktionen der verglichenen Produkte, die direkten Einfluss auf die Richtigkeit oder Gültigkeit dieses Vergleichs haben können, sind vorbehalten. Die in diesem Vergleich enthaltenen Informationen sollen ein allgemeines Verständnis sachlicher Informationen zu verschiedenen Produkten vermitteln und sind möglicherweise nicht vollständig. Alle dieses Dokument verwendenden Personen sollten auf Basis ihrer Anforderungen ihre eigene Kaufentscheidung treffen und sollten auch Originalinformationsquellen zu Rate ziehen und sich bei der Wahl eines Produkts nicht nur auf diesen Vergleich verlassen. Sophos gibt keine Garantie für die Zuverlässigkeit, Richtigkeit, Zweckmäßigkeit oder Vollständigkeit dieses Dokuments. Die Informationen in diesem Dokument werden in der vorliegenden Form und ohne jegliche Garantie, weder ausdrücklich noch implizit, bereitgestellt. Sophos behält sich das Recht vor, dieses Dokument jederzeit zu ändern oder zurückzuziehen.

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

15.11.2018 BG-DE (RP)

SOPHOS