SOPHOS
Security made simple.

Firewall Buyers Guide

Sind Sie auf der Suche nach einer neuen Netzwerk-Firewall? Egal, ob Sie alle Sicherheitsfunktionen in einer UTM-Lösung konsolidieren oder ob Sie Next-Generation Features anschaffen möchten: In diesem Guide finden Sie die Antworten auf Ihre Fragen. Sie erfahren, was Sie bei der Wahl Ihrer nächsten Netzwerk-Firewall beachten sollten, und erhalten Informationen über erhältliche Funktionen sowie Listen mit Fragen, die Sie Anbietern stellen sollten. Mit diesem Guide finden Sie ganz einfach die geeignete Lösung für Ihr Unternehmen.

Checkliste zum Firewall-Vergleich

Die folgende Tabelle gibt einen Überblick über die wichtigsten Funktionen, auf die Sie bei der Bewertung von Network-Security-Lösungen achten sollten. Mit Hilfe der Tabelle können Sie leichter entscheiden, welche Lösung Ihre Anforderungen erfüllt.

In den einzelnen Abschnitten des Guides erhalten Sie detaillierte Informationen zu den Sicherheitsfunktionen. Außerdem erfahren Sie, welche Faktoren die Benutzerfreundlichkeit, Sicherheit und Performance einer Lösung beeinflussen.

Funktion	Sophos UTM	Fortinet FG 20-90	Dell SonicWALL TZ Series	WatchGuard XTM Series	Der Sophos Vorteil
Netzwerk-Firewall/ Network Protection	✔	✔	✔	✔	Automatische IPS-Aktualisierung, einfache Konfiguration durch Auswahl benötigter Funktionen per Klick
Advanced Threat Protection	✔	✔	✔	✔	All-in-One-Lösung
Site-to-Site- und Remotebenutzer-VPN	✔	✔	✔	✔	Einfache Einrichtung mit Sophos RED
Secure Web Gateway	✔	✔	✔	✔	Einfache Richtlinienerstellung
Spamschutz	✔	✗*	✗*	✔	Keine separate Appliance erforderlich
E-Mail-Verschlüsselung und DLP	✔	✗	✗	✗*	Automatische Verschlüsselung, keine zusätzliche Infrastruktur erforderlich
Endpoint Protection	✔	✔	✔	✗	Sophos ist Gartner Leader***
Dualer Virenschutz	✔	✗	✗	✗	Wahlweise Einsatz eines oder beider Scanner
Mobile Network Access Control	✔**	✗	✗	✗	Einfache Richtlinienbereitstellung
WLAN	✔	✔	✔	✔	Einfache, vermaschte Netzwerke
Reverse-Proxy	✔	✔	✗	✗	Umfassende Reverseproxy-Funktionen
Web Application Firewall	✔	✗*	✗*	✗	Keine separate Appliance erforderlich
Benutzerportal	✔	✔	✗	✗	Entlastung der IT
Vollständiges Reporting	✔	✗*	✗*	✗*	On-Box, Speicherung auf integrierter Festplatte
Integrierte Zwei-Faktor-Authentifizierung	✔	✗	✗	✗	KOSTENLOS; keine zusätzliche Infrastruktur erforderlich
Zentrale Verwaltung kostenlos inbegriffen	✔	✗	✗	✗	KOSTENLOS; keine separate Appliance erforderlich
Alle TMG-Funktionen	✔	✗	✗	✗	Unabhängige Experten empfehlen Sophos****
Bereitstellungsarten					
Bereitstellung als Hardware, Software, virtuell oder in der Cloud	✔	✗	✗	✗	Alle Funktionen für alle Bereitstellungsarten verfügbar
Active/Active-Cluster mit integriertem Lastausgleich	✔	Größere Modelle	✔	Begrenzt	Cluster aus bis zu 10 Appliances für eine vollständig skalierbare Lösung
Einheitliche Funktionen auf allen Modellen	✔	✗	✗	✗	Keine Anschaffung eines höheren Appliance-Modells erforderlich, um essentielle Funktionen zu erhalten
Bei Bedarf Möglichkeit zum Hinzufügen von Lizenzmodulen	✔	Größere Modelle	✔	✔	Flexible Lizenzierung, für zusätzliche Funktionen kein Hardware-Upgrade notwendig
Zusätzliche Anforderungen					

Bezieht sich ausschließlich auf die in einer UTM-Lösung enthaltenen Funktionen

* Vergleichbare Funktionalität nur mit separater Appliance

** Subscription Sophos Mobile Control erforderlich

*** Sophos ist Leader in den Gartner Magic Quadrants für UTM, Endpoint Protection Platforms und Mobile Data Protection.

**** www.sophos.de/tmg

Einleitung

Verwendung dieses Guides

In diesem Guide geben wir Ihnen Tipps zur Bewertung von Firewall-Lösungen und stellen Ihnen die einzelnen Sicherheitsfunktionen erhältlicher Lösungen genauer vor. Diese Informationen helfen Ihnen herauszufinden, welche Funktionen Ihre zukünftige Netzwerk-Firewall oder UTM-Lösung haben sollte.

Außerdem finden Sie in diesem Guide einen Vergleich zwischen ausgewählten Produkten von Sophos, Dell SonicWALL, WatchGuard und Fortinet.

Nutzen Sie den Guide als Entscheidungshilfe für die Wahl Ihrer nächsten Netzwerk-Firewall – egal, ob Sie nach einer Lösung mit mehr Funktionen suchen, Sie die Anzahl der von Ihnen derzeit verwalteten Network-Security-Produkte reduzieren möchten oder Sie sich eine bessere Übersicht und Kontrolle über Ihre Internetnutzer wünschen.

Unabhängige Produkt-Performancetests

Wir haben vor kurzem das unabhängige Testinstitut Miercom Labs damit beauftragt, unsere Firewall-Produkte mit denen der Konkurrenz zu vergleichen. Getestet wurden unsere SG Series Appliances SG 210 und SG 230. In diesem Buyers Guide beschränken wir uns der Übersichtlichkeit halber auf den Vergleich mit der SG 210.

Für den Vergleich wurden Konkurrenzprodukte mit einer Eignung für Unternehmen mit 50–100 Benutzern ausgewählt:

- DELL SonicWALL NSA 2600
- Fortinet FortiGate 100D
- WatchGuard XTM 525

Bitte beachten: Bei den von Anbietern veröffentlichten Modellempfehlungen handelt es sich lediglich um Richtwerte. Faktoren wie Benutzertyp, Infrastruktur usw. können die individuellen Anforderungen beeinflussen. Wir empfehlen daher allen Kunden, ihren Anbieter oder Reseller zu kontaktieren, um das geeignete Appliance-Modell für ihre individuellen Anforderungen zu ermitteln.

UTM oder Next-Gen Firewall?

Was ist der Unterschied zwischen einer UTM und einer Next-Generation Firewall? Viele glauben, dass es sich bei beiden Begriffen um das gleiche handelt, in Wahrheit gibt es aber sehr wohl Unterschiede.

Bei einer UTM sind in den meisten Fällen verschiedene Sicherheitslösungen in einer einzigen Plattform integriert. Zu diesen Sicherheitslösungen können u. a. Netzwerk-, Web-, E-Mail-, Endpoint- und WLAN-Verwaltung zählen.

Eine Next-Generation Firewall (NGFW) verfügt oft über weniger Funktionen und benötigt ergänzende Sicherheitslösungen wie ein E-Mail-Gateway oder Endpoint Protection. Bei ihr liegt der Fokus in der Regel auf detaillierten Web-Kontrollen und anwendungsbasierter Sicherheit. Sie besitzt daher Funktionen für Anwendungstransparenz und -kontrolle, die optimierte Nutzung von Internetverbindungen, klare, verständliche Intrusion Prevention Systems (IPS) und nahtlose VPNs zur Anbindung von Außenstellen und für komfortablen Remotezugriff.

Bei der Wahl Ihrer zukünftigen Lösung sollten Sie sich allerdings weniger an der begrifflichen Unterscheidung zwischen UTM und NGFW orientieren. Viel wichtiger ist es zu verstehen, was genau Sie schützen möchten und welche Funktionen Sie dafür benötigen. Nur so können Sie entscheiden, welches die am besten geeignete Lösung für Ihre individuellen Geschäftsanforderungen ist.

Teil 1: Lösungen vergleichen

Die folgenden fünf Punkte sollten Sie bei der Auswahl Ihrer nächsten Firewall unbedingt berücksichtigen:

1. Benutzerkomfort
2. Performance
3. Sicherheitsfunktionen
4. Reporting
5. Qualität des Schutzes

1. Benutzerkomfort

Früher war es üblich, dass eine Netzwerk-Firewall zu Beginn von einer Person konfiguriert wurde und es dann bei diesen Einstellungen blieb. Heute führt dies oft zu Problemen, denn in vielen Fällen kannte sich nur diese eine Person mit der Firewall aus und hat mittlerweile das Unternehmen verlassen. Folglich haben viele Unternehmen ein Gerät im Serverraum stehen, an das sich keiner mehr herantraut – aus bloßer Angst, etwas kaputt zu machen.

Wenn Sie gewohnt sind, Ihre Firewall über die Befehlszeile zu konfigurieren, wird Ihnen ein Security-Gateway-Produkt mit einer bedienfreundlichen Benutzeroberfläche wahrscheinlich wie purer Luxus vorkommen. Network-Security-Produkte haben sich über viele Jahre hinweg weiterentwickelt und Anbieter haben gelernt, dass Produkte mit einfacher Bedienung oft auch effektiver sind. Denn erweiterte Funktionen sind wenig wert, wenn ihr Einsatz zu kompliziert ist.

Die Benutzeroberfläche sollte grundsätzlich über klar definierte Workflows verfügen, damit Konfigurationsschritte für unterschiedliche Module des Produkts nicht wiederholt werden müssen.

Da Mitarbeiter heutzutage auf viele verschiedene Orte verteilt sind, sind Installationen auf Endbenutzer-Clients für viele Unternehmen mittlerweile nicht mehr praktikabel. Beispielsweise können IT-Administratoren viel Zeit sparen, wenn die eingesetzte Firewall einen vollständig transparenten Modus bietet und weder Proxyserver konfiguriert noch NAT-Regeln eingerichtet werden müssen. Eine Verwaltungsoberfläche, die von überall und jedem Gerät abrufbar ist, spart zudem in Notfällen die Fahrt ins Büro.

Ebenso sollte das Richtlinien-Setup für Benutzer im Büro gleichermaßen auf mobile Mitarbeiter anwendbar sein. Web-Filtering-Regeln müssen Benutzer beispielsweise außerhalb des Unternehmensnetzwerks schützen. Und um der Gerätevielfalt Ihrer Benutzer Rechnung zu tragen, sollte die Authentifizierung möglichst benutzerfreundlich sein.

Einige Dinge, die Sie beachten sollten:

- Wie schnell können Sie an Informationen gelangen, die Sie benötigen, um Benutzerprobleme (z. B. gesperrte Websites) zu beheben?
- Wie einfach lässt sich die Lösung aktualisieren?
- Wie viele Schritte sind für Standardaufgaben wie die Erstellung von Web-Filtering-Richtlinien erforderlich?
- Können Sie die Dashboard-Ansicht individuell an Ihre Bedürfnisse anpassen?

2. Performance

Egal, ob Sie nach einer UTM-Lösung für ein Kleinunternehmen oder nach Next-Generation Firewall Features der Enterprise-Klasse suchen: Die Performance ist meist ein wichtiges Kriterium bei der Kaufentscheidung.

Anbieter veröffentlichen Modellempfehlungen. Da es sich bei diesen Angaben jedoch immer nur um Richtwerte handelt, sollten Sie bei der Modellwahl auf jeden Fall auch die Besonderheiten Ihrer Infrastruktur beachten. Berücksichtigen Sie die Arbeitsweise Ihrer Benutzer, ihr unterschiedliches Nutzungsverwalten, welche Anwendungen und Server Sie schützen müssen und welche Features Ihrer Firewall Sie aktivieren möchten.

Vertrauen Sie auf keinen Fall blind auf Online-Tools zur Ermittlung geeigneter Firewall-Modelle: Ein Anbieter attestiert Ihnen wahrscheinlich, dass Sie eine Firewall mit einem Durchsatz von 1 MBit/s pro Benutzer benötigen, während der nächste behauptet, dass alle Modelle bis 20 MBit/s geeignet seien usw. Selbst die erfahrensten Netzwerkexperten schätzen die Durchsatzanforderungen oft falsch ein – entweder wird ein zu kleines Modell gewählt, was letztendlich zu Performance-Problemen führt, oder es wird ein völlig überdimensioniertes Modell empfohlen, das absolut nicht im Rahmen des Budgets liegt.

Die Performance hängt auch von der Architektur der jeweiligen Hardware-Appliance ab und davon, wie Software und Hardware zusammenarbeiten. Eine Appliance mit ASICs-Chips kann z. B. gute Durchsatzergebnisse für einen bestimmten Zweck erzielen, lässt sich jedoch nur begrenzt upgraden und erfordert oftmals eine besondere Anschlussart. Außerdem weichen die Performance-Werte für ASICs-Hardware stark von virtuellen Installationen des gleichen Anbieters ab.

Tests von Drittanbietern wie die im Folgenden beschriebenen von Miercom Labs bieten meist eine realistischere Darstellung der zu erwarteten Durchsatzraten in einer produktiven Umgebung. Hier ist es allerdings immer wichtig, sich die angewendeten Testmethoden genau anzusehen.

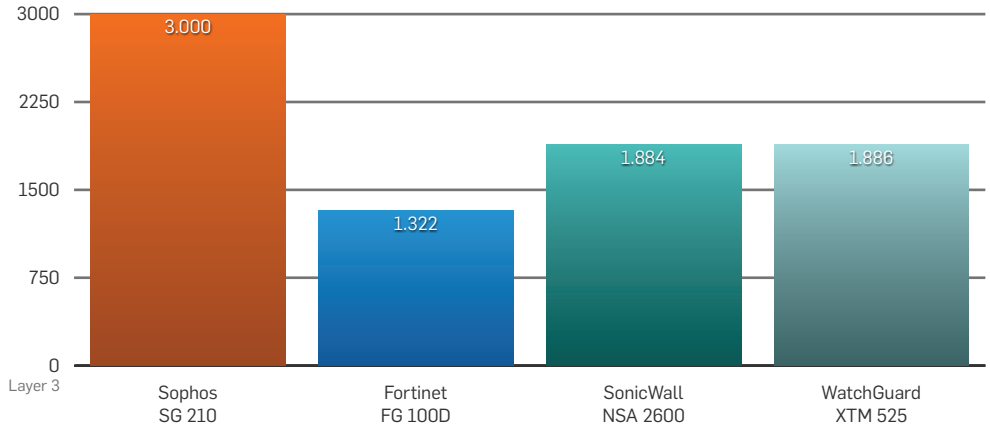
Testergebnisse können entscheidend beeinflusst werden durch:

- die in der Hardware verwendete Architektur, z. B. ASICs im Vergleich zu Standard-Multicore-Prozessoren wie Intel
- die Port-Anzahl einer Appliance – Übertragungsrate der Leitung wird in aufgerundeten Zahlen angegeben
- die Art des gemessenen Datenverkehrs – unidirektional oder bidirektional
- die Vergleichbarkeit der Tests (z. B. proxybasierter Virenschutz (langsamer, aber sicherer) im Vergleich zu flussbasiertem Virenschutz (schneller, aber nicht so effektiv)

Miercom-Test: Firewall-Durchsatz

Die Firewall ist die Grundfunktion Ihrer UTM. Wenn es hier zu Verzögerungen kommt, ist der gesamte Datenverkehr betroffen, der das Gerät passiert. Der Firewall-Durchsatz sollte idealerweise Verbindungen auf Niveau der Leitungsrate ermöglichen. Dieser Test wurde mit drei 1 GBit/s-Ports durchgeführt, die über einen theoretischen Maximaldurchsatz von 3 GBit/s/3.000 MBit/s verfügen.

Unidirektionaler Firewall-Durchsatz (MBit/s)



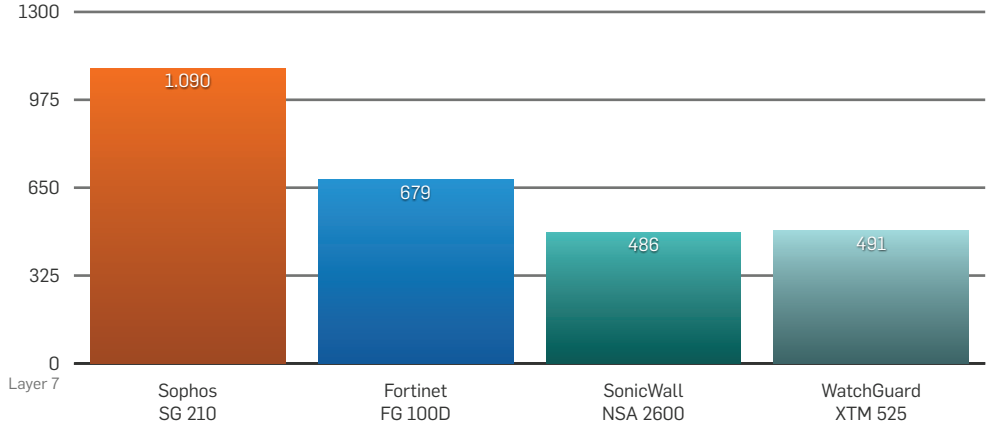
Quelle: Miercom, Juni 2014

Da die Sophos SG 210 beim ersten Firewall-Durchsatztest nicht an ihre Grenzen gebracht werden konnte, wurde ein weiterer Test mit mehr Ports und bidirektionalem Datenverkehr durchgeführt. Die Sophos SG 210 erreichte einen maximalen Durchsatz von 10.441 MBit/s.

Miercom-Test: Application-Control-Durchsatz

Mit Application Control können Sie unterschiedliche Arten von Datenverkehr, der Ihr Gateway passiert (z. B. VPN, YouTube oder Facebook), kontrollieren und verwalten, ohne den Datenverkehr komplett blockieren zu müssen. Bei diesem Test wurde der Durchsatz an Layer 7 (Application Layer) gemessen.

Application-Control-Durchsatz (MBit/s)

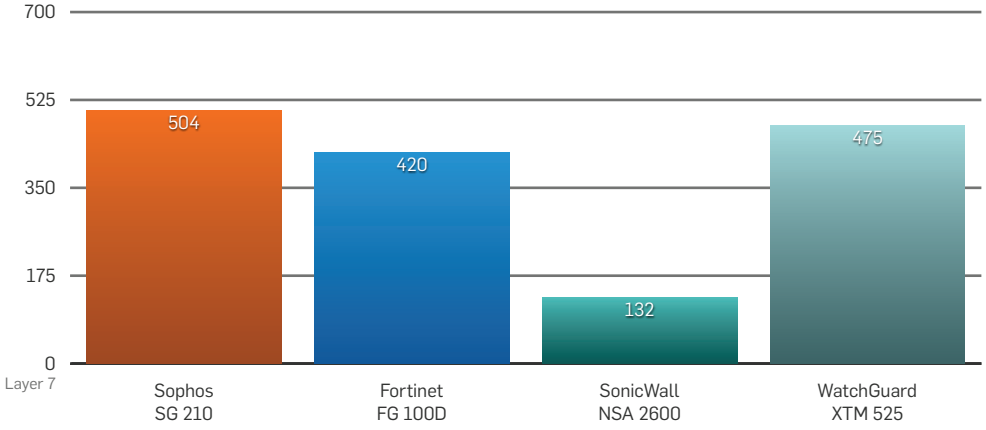


Quelle: Miercom, Juni 2014

Miercom-Test: IPS-Durchsatz

Intrusion-Prevention-Systeme (IPS) überprüfen das Netzwerk auf verdächtigen Datenverkehr und können die Ausnutzung bekannter Schwachstellen verhindern. Ähnlich wie Application Control ist auch dieser Prozess ressourcenintensiv, da Pakete zusammengesetzt und untersucht werden.

Firewall- + IPS-Durchsatz (MBit/s)



Quelle: Miercom, Juni 2014

Weitere Informationen über den unabhängigen Testbericht von Miercom finden Sie unter www.sophos.de/miercom

Bereitstellungsarten

Manche Anbieter heben sich durch ihre Bereitstellungsflexibilität von der breiten Masse ab und bieten Hardware-, Software-, virtuelle (z. B. VMware, Hyper-V und Citrix Xen) oder cloudbasierte Versionen an.

Wenn Sie sich für eine Software-Version oder für eine virtuelle Installation entscheiden, sollten Sie berücksichtigen, ob diese auf einer beliebigen Intel X86-kompatiblen Hardware ausgeführt werden kann oder ob speziell gefertigte Hardware-Komponenten notwendig sind. Natürlich bleiben Sie mit Standard-Hardware flexibler, da sich diese einfacher erweitern lässt.

Je nachdem, welche Architektur der Anbieter nutzt, werden Sie ggf. erhebliche Performance-Unterschiede zwischen der Firewall-Appliance eines Anbieters und einer virtuellen Installation des gleichen Anbieters auf Standard-Hardware beobachten.

Alternativ können Sie Ihre Network-Security-Lösung auch in der Cloud bereitstellen. Hierzu können in vielen Fällen die Amazon Web Services oder ein Datencenter Ihrer Wahl genutzt werden.

Wie in der Tabelle unten zu sehen, bieten nicht alle Anbieter alle Bereitstellungsarten an. Entscheiden Sie sich für das Bereitstellungsmodell, das Ihre Anforderungen am besten erfüllt und Ihnen die Flexibilität bietet zu wachsen.

Bereitstellung	Sophos UTM	Fortinet FG 20-70	Dell SonicWALL TZ Series	WatchGuard XTM Series
Hardware	✔	✔	✔	✔
Software	✔	✗	✗	✗
Virtuell	✔	✔	✗	✔
Cloud	✔	✔	✗	✗

3. Sicherheitsfeatures

Wenn Ihr Ziel darin besteht, Ihre vorhandene Infrastruktur in einer Lösung zu konsolidieren, möchten Sie aller Wahrscheinlichkeit nach auf keine der gewohnten Sicherheitsfunktionen verzichten. Sollten Sie beispielsweise die Anschaffung einer UTM-Lösung zum Schutz Ihrer E-Mails planen, achten Sie darauf, dass diese Funktionen wie Spamfilter, E-Mail-Verschlüsselung und DLP enthält.

Wenn ein Anbieter in Ihrer engeren Auswahl keine mit Ihrem E-Mail-Gateway vergleichbaren Features vorweisen kann, sollten Sie ihn von der Liste streichen.

Gleiches gilt für Web Protection. Eine UTM-Lösung sollte Funktionen bieten, die mit einem Web Security Gateway vergleichbar sind. Selbst wenn Sie nicht alle Funktionen Ihres Network-Security-Produkts nutzen, verfügen Sie über die notwendigen Funktionen zur optimalen Unterstützung Ihrer Geschäftsabläufe.

Wenn Sie ein eingestelltes Produkt wie Microsoft Forefront Threat Management Gateway (TMG) ersetzen möchten, können Sie die Gelegenheit nutzen und auf eine UTM wechseln, die mehr oder bessere Funktionen bietet als Ihre bisherige Lösung. Wenn Ihr TMG-Ersatz auch Funktionen für Network, Web und Email Protection beinhaltet, können Sie dadurch Kosten sparen und Ihren Verwaltungsaufwand reduzieren.

In der Checkliste zum Firewall-Vergleich auf Seite 2 sind die Funktionen aufgeführt, die Sie u. U. von Ihrem Network Security Gateway erwarten. Der Vergleich zeigt, welche Anbieter Funktionen als Teil einer UTM-Lösung anbieten.

Zwar können die meisten Anbieter fast alle Funktionen bieten, jedoch in vielen Fällen nur mit mehreren Appliances oder Sicherheitslösungen. Zudem bieten viele Anbieter nicht alle Funktionen auf allen Appliance-Modellen an.

Wenn Sie beispielsweise ein Kleinunternehmen haben und eine begrenzte Anzahl an Benutzern schützen möchten, sollten Sie keine für Ihre Anforderungen überdimensionierte Lösung kaufen müssen, nur um die notwendigen Funktionen zu erhalten.

Genaue Informationen zu einzelnen Sicherheitsfunktionen finden Sie in **Teil 2** dieses Guides.

4. Reporting

Reports sorgen für einen klaren Überblick über alle Vorgänge im Netzwerk und ermöglichen es Ihnen, qualifizierte Entscheidungen zur optimalen Unterstützung Ihrer Geschäftsabläufe zu treffen.

Wenn z. B. ein Großteil Ihrer Bandbreite von einer bestimmten Anwendung verbraucht wird, kann sich das negativ auf andere Prozesse auswirken. Außerdem geben Reports Einblick in Infektionen auf Ihrem System.

Echtzeitdaten sind wichtig, um schnell Entscheidungen treffen zu können und um sicherzustellen, dass Sie die Service-Qualität bieten, die Ihre Benutzer benötigen. Mit Echtzeit-Reports zur Internetnutzung können Sie Ihre Lösung dynamisch anpassen, Engpässe beseitigen, die durch ein bestimmtes Nutzungsverhalten hervorgerufen werden, und mehr Ressourcen für bestimmte Abteilungen organisieren, wenn Spitzenlasten zu erwarten sind.

Lösungen, die nur in festgelegten Intervallen Reports generieren, sind nicht für alle Unternehmen und Einrichtungen geeignet. Viele IT-Abteilungen benötigen beispielsweise Daten sofort und können nicht warten, bis der nächste Report verfügbar ist.

Außerdem möchten Sie ggf. Vergangenheitsdaten abrufen, um qualifiziertere Entscheidungen über das optimale Setup zu treffen oder um bestimmte Vorfälle zu analysieren. Mit einer On-Box-Speicherung ist ein Zugriff auf solche Daten problemlos möglich.

Jedes Reporting-Modell muss auf Ihre Bedürfnisse anpassbar sein und Ihnen die gewünschten Daten liefern – und sollte keine Daten speichern, die für Sie uninteressant sind.

Konsolidierte Reports, die mehrere Funktionen umfassen, können in manchen Bereichen von Vorteil sein. Nicht alle Angriffe stammen zwangsläufig aus nur einer bestimmten Quelle. Eine Einzelansicht, z. B. für Zugriffsversuche auf einen Command-and-Control-Server, kann Ihnen dabei helfen, Probleme schnell zu beheben.

Wenn Sie über die Auswirkungen des Reportings auf die Performance besorgt sind, sollten Sie Lösungen mit einer rotierenden Festplatte meiden und stattdessen Lösungen mit integrierter SSD bevorzugen. Da sie keine beweglichen Teile enthalten, sind SSDs nicht nur robust, sondern auch schnell, und sie beeinträchtigen die Performance Ihrer Lösung selbst bei der Erstellung komplexer Reports nur minimal.

Funktion	Sophos UTM	Fortinet FG 20-90	Dell SonicWALL TZ Series	WatchGuard XTM Series
Standardmäßig enthaltene Reports	Tausende	Wenige	Wenige	Wenige
On-Box-Speicherung für lokale Quarantäne, Protokolldateien und Reports	Umfassend	Begrenzt	Begrenzt	Begrenzt

5. Bewährter Schutz

Bei der Wahl einer Firewall sollten Sie auch auf die Qualität des Schutzes achten. Empfehlungen von Drittanbietern können Aufschluss darüber geben, welche Anbieter den besten Schutz vor verschiedenen Bedrohungen bieten.

Für viele Unternehmen gilt außerdem der Gartner Magic Quadrant als Benchmark zur Wahl eines geeigneten Anbieters.

Da jedoch viele Netzwerk-Firewalls heutzutage umfassende Sicherheit liefern, muss die Technologie als Ganzes berücksichtigt werden. Außerdem sollten Sie prüfen, ob der Anbieter über genügend Erfahrung verfügt, auf die Sie vertrauen können.

Teil 2: Sicherheitsfunktionen vergleichen

In diesem Abschnitt sehen wir uns die verschiedenen erhältlichen Sicherheitsfunktionen genauer an. Ermitteln Sie anhand der folgenden Informationen, welche Funktionen Sie benötigen und welche Fragen Sie Anbietern stellen sollten.

Network Protection

Ein Network-Security-Produkt sollte Sie bereits schützen, bevor Sie kostenpflichtige Subscriptions oder Lizenzen hinzufügen. Die Mindestanforderungen an Ihre Lösung sind: Statisches Routing, DNS-Proxy-Dienste, DHCP-Serveroptionen, NTP-Funktion, Stateful Firewall, Network Address Translation, grundlegender Remotezugriff über VPN, lokale Benutzerauthentifizierung, lokale Protokollierung und tägliche Reports sowie grundlegende Verwaltungsfunktionen.

Empfohlene Funktionen	Beschreibung	Fragen an Ihren Anbieter
IPS	Stärkt die Sicherheitsrichtlinien Ihrer Firewall, indem genehmigter Datenverkehr auf schädliche Pakete überprüft wird. Kann Pakete aussondern, die eine Übereinstimmung mit einer Signaturliste oder mit Bedrohungsmustern aufweisen.	‣ Welche Art von Fachwissen ist erforderlich, um das System richtig verwenden zu können? ‣ Wie werden Regeln bereitgestellt und konfiguriert? ‣ Lässt sich das IPS einfach an Ihre individuelle Netzwerkinfrastruktur anpassen?
Advanced Threat Protection/Command-and-Control/Botnet-Erkennung	Überprüft ausgehenden Datenverkehr, um Kommunikationsversuche mit schädlichen Hosts wie Command-and-Control- und Botnet-Servern zu erkennen und zu unterbinden.	‣ Wie viel Fachwissen ist für die Bedienung des Systems erforderlich? ‣ Ist die Erkennung von Bedrohungen über das Web enthalten? ‣ Ist konsolidiertes Reporting für alle Quellen verfügbar?
Bandbreitenkontrolle/Quality of Service	Priorisiert Datenverkehr basierend auf den von Ihnen eingestellten Regeln. Sie können festlegen, wie eine bestimmte Ressource unter verschiedenen Bedingungen verwendet wird.	‣ Wie viele WAN-Verbindungen können Sie auf einer einzelnen Appliance unterstützen? ‣ Wie einfach lässt sich die von Anwendungen genutzte Bandbreite ermitteln und steuern?
Site-to-Site-VPN-Optionen	Vernetzt entfernte Standorte mit der Zentrale, sodass Benutzer Informationen über eine sichere Verbindung senden und empfangen können. Ermöglicht Mitarbeitern die Verwendung von Geräten wie Dateiservern und Druckern, die sich nicht im selben Büro befinden.	‣ Welche Protokolle unterstützt Ihr VPN? ‣ Wie viel Fachwissen zu VPN ist erforderlich, um eine VPN-Verbindung einzurichten?
Remotezugriff-Optionen	Ermöglicht Benutzern, von jedem Ort aus eine sichere Verbindung zur Network-Security-Appliance herzustellen.	‣ Bieten Sie mehrere Optionen für Remotezugriff einschließlich Clientless VPN an? ‣ Wird der Remotezugriff für jedes Betriebssystem und/oder Gerät unterstützt? ‣ Kommt das Clientless VPN tatsächlich ohne Client aus, oder sind auf dem Endbenutzergerät Applets erforderlich? ‣ Sind zusätzliche Lizenzen notwendig?
Remotestandort-Unterstützung	Verbindet Remotestandort-Netzwerke mit der Network Security Appliance, damit diese Netzwerke mit denselben Richtlinien und Funktionen geschützt werden.	‣ Wie einfach ist es, eine Verbindung zu Remotestandorten herzustellen? ‣ Sind Techniker erforderlich? ‣ Können Remotestandorte zentral verwaltet werden? ‣ Sind zusätzliche Subscriptions oder Lizenzen erforderlich?
Detaillierte Reports	Bietet detaillierte Echtzeit- und Verlaufsstatistiken sowie Reports zur Netzwerk-/Bandbreitenauslastung, Netzwerksicherheit usw.	‣ Ist eine integrierte Festplatte vorhanden? ‣ Welche Arten von Reports sind ohne eine separate Anwendung verfügbar?

Web Protection

Sie benötigen eine Sicherheitslösung, mit der Sie Nutzungsbedingungen für die Online-Aktivitäten von Benutzern festlegen und Spyware und Viren stoppen können, bevor sie in das Netzwerk eindringen. Detaillierte Reports sollten aufzeigen, wie effektiv Ihre Richtlinien sind, sodass Sie diese ggf. anpassen können.

Empfohlene Funktionen	Beschreibung	Fragen an Ihren Anbieter
URL-Filterung	Kontrolliert die Internetnutzung der Mitarbeiter, um privates Surfen im Internet zu verhindern und das Netzwerk vor unangemessenen Inhalten und Malware zu schützen.	› Sind Live-Updates verfügbar? › Wie viele Websurfprofile können erstellt und verwendet werden? › Werden potenziell unangemessene Websites nur blockiert oder kann auch vor ihnen gewarnt werden?
Spyware-Schutz	Verhindert, dass sich schädliche Software auf den Computern der Mitarbeiter installiert, die Bandbreite verbraucht und vertrauliche Daten aus dem Netzwerk nach außen sendet.	› Sind Live-Updates verfügbar?
Antivirus-Scans	Scannt Inhalte vor dem Eintritt ins Netzwerk, um eine Infektion des Netzwerks mit Viren, Würmern und anderer Malware zu vermeiden.	› Sind Live-Updates verfügbar?
HTTPS-Scans	Bietet Einblick in verschlüsselten Internet-Datenverkehr, um das Netzwerk vor Bedrohungen zu schützen, die über HTTPS übertragen werden können.	› Kann HTTPS-Datenverkehr untersucht und dahingehend geprüft werden, ob er gemäß den Richtlinien zulässig ist?
Application Control	Bietet Einblick in die Internetnutzung der Mitarbeiter und kontrolliert, welche Anwendungen wie verwendet werden können.	› Sind Live-Updates verfügbar?
Interaktives Web Reporting	Bietet flexible Funktionen zur Reporterstellung, mit denen Administratoren ihre eigenen Reports zusammenstellen können.	› Sind Echtzeit- und Verlaufsreports zur Nutzung verfügbar? › Können Reports automatisch zugestellt werden? › Ist eine Reporting-Anwendung eines Drittanbieters erforderlich?

Email Protection

E-Mails vor Spam und Viren zu schützen, ist kein neues Problem. Sicherheitsbedrohungen, die sich per E-Mail verbreiten, entwickeln sich jedoch kontinuierlich weiter. Der E-Mail-Schutz wird so zum nie endenden Fulltime-Job. Um Ihre E-Mails und damit Ihr Unternehmen vor weit verbreiteten Gefahren wie Spam, Viren und Datenverlust zu bewahren, benötigen Sie einen zuverlässigen Schutz für Ihren E-Mail-Verkehr.

Empfohlene Funktionen	Beschreibung	Fragen an Ihren Anbieter
Spamfilter (Anti-Spam)	Verhindert, dass Spam und andere unerwünschte E-Mails in den Posteingang der Mitarbeiter gelangen.	› Wie hoch sind Ihre Spamerkennungs- und False Positive-Raten? › Mit welchen Techniken arbeitet Ihre Spamerkennung?
Antivirus-Scans	Blockiert schädliche Inhalte nach dem Scan am Gateway, sodass die Computer nicht mit Viren und anderer Malware infiziert werden.	› Wie viele Antivirus-Engines werden in Ihrer Lösung verwendet? › Wie oft führt Ihre Lösung einen Scan des Inhalts durch?
E-Mail-Verschlüsselung	Macht E-Mails unleserlich, sodass nicht legitime Empfänger keine vertraulichen Informationen erlangen können.	› Was muss der Benutzer tun, um E-Mails zu ver- und entschlüsseln? › Wie wird die Verschlüsselung verwaltet? › Welche Infrastruktur ist für die Schlüsselverwaltung erforderlich?
Data Loss Prevention (DLP)	Verhindert, dass sensible Daten absichtlich oder versehentlich per E-Mail versendet werden.	› Wird die Funktion automatisch oder manuell ausgelöst? › Ist eine Integration in die E-Mail-Verschlüsselung möglich? › Welche Datentypen können erkannt werden?
Benutzerportal	Ermöglicht den Benutzern die Verwaltung ihrer E-Mails, einschließlich Spam-Quarantäne und Nachrichtenaktivitäten.	› Können Endbenutzer ihre E-Mail-Quarantäne selbst verwalten?

Next-Generation Firewall Protection

Bei einer NGFW handelt es sich um eine Weiterentwicklung herkömmlicher, portbasierter Schutzmaßnahmen, die in den meisten Netzwerksicherheitskonzepten Verwendung finden. Anstatt Datenverkehr auf Ports wie HTTP oder HTTPS ganz einfach zu erlauben, besitzen NGFWs Anwendungssignaturen, mit denen sie Datenverkehr weit detaillierter aufschlüsseln können. So können Administratoren beispielsweise auf Facebook die Funktion Sofortnachrichten blockieren, den allgemeinen Zugriff auf Facebook aber weiterhin erlauben.

Mit NGFWs ist außerdem eine umfassende und schnelle Paketüberprüfung möglich. NGFWs erkennen und blockieren mit hoher Zuverlässigkeit Exploits, Malware und weitere Bedrohungen. Viele Angriffe werden heute über das Internet gestartet. Firewalls, die nur nach Port filtern, können Gefahren deshalb nur begrenzt abwehren.

Mit einer NGFW können Unternehmen zudem strategischer vorgehen, indem sie ihre Netzwerknutzung auf Basis leistungsstarker Gestaltungsregeln priorisieren. So können Sie beispielsweise VoIP-Telefongespräche erlauben oder Salesforce.com-Datenverkehr Priorität einräumen und gleichzeitig den Durchsatz von Anwendungen wie Bittorrent limitieren oder unerwünschte Anwendungen komplett sperren.

Empfohlene Funktionen	**Beschreibung**	**Fragen an Ihren Anbieter**
Einsicht und Kontrolle für 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.	› Lässt sich der Zugriff auf Anwendungen priorisieren und kontrollieren und ist in Echtzeit einsehbar, wie und von wem der Internet-Zugang genutzt wird? › Wie einfach ist das Einrichten einer Richtlinie aus der Live-Ansicht Ihrer aktuellen Aktivitäten?
Optimierte Nutzung der Internetverbindung(en)	Ihre Bandbreite ist begrenzt und sollte daher optimal ausgenutzt werden, beispielsweise, indem unternehmensrelevante Anwendungen wie salesforce.com Priorität erhalten.	› Wie einfach ist es, die Bandbreite zu gestalten? › Verfügen Sie über ein Quality of Service (QoS)-Toolkit?
Klare, verständliche IPS	Viele webbasierte Angriffe können sich mittlerweile als seriöser Datenverkehr tarnen. Mit einem effektiven IPS können Sie nicht nur die Art, sondern auch das Verhalten Ihres Internet-Datenverkehrs beobachten.	› Wie einfach ist die Verwaltung von IPS? › Wie viel Fachwissen ist notwendig – müssen Sie beispielsweise unterschiedliche Bedrohungstypen verstehen?
Nahtloses VPN für Remoteverbindungen	Mobiles und Remote-Arbeiten gehören immer häufiger zum Arbeitsalltag. Unternehmen benötigen schnelle, einfache und sichere VPNs, damit Benutzer sich mit dem Netzwerk verbinden und von überall produktiv arbeiten können.	› Wie einfach ist die Einrichtung von Client-VPNs für Remote-Mitarbeiter? › Mit welchen Geräten kann eine Verbindung zum Netzwerk hergestellt werden? › Haben Sie eine HTML5-Lösung ohne Client im Angebot?

Webserver Protection

Eine funktionierende Webserver Protection hindert Hacker daran, mit Angriffen wie SQL Injection und Cross Site Scripting sensible Daten wie Kreditkartendaten oder persönliche Gesundheitsdaten zu stehlen. Zudem hilft eine solche Lösung Ihnen bei der Einhaltung von Compliance-Bestimmungen, wenn eine Web Application Firewall erforderlich ist.

Eine Web Application Firewall scannt die Webaktivitäten und erkennt den Missbrauch von Webanwendungen. Auf diese Weise lassen sich Netzwerksondierungen und Angriffe vermeiden.

Empfohlene Funktionen	Beschreibung	Fragen an Ihren Anbieter
Form Hardening	Prüft und verifiziert Informationen, die Besucher Ihrer Website über Online-Formulare übermitteln. Verhindert, dass ungültige Daten aus Formularen an Ihren Server übertragen werden.	› Wird eine komplette Formularanalyse durchgeführt? › Erkennt das System manipulierte Formulare?
Reverseproxy-Authentifizierung	Ermöglicht eine manipulationssichere Benutzerauthentifizierung durch Integration mit Ihren Back-End-DMZ-Services wie Exchange. Häufig gewünscht bei der Suche nach einer Alternative zu Microsoft TMG.	› Mit welchen Systemen ist eine nahtlose Integration möglich? › Welche Authentifizierungsarten werden unterstützt?
Antivirus-Scans	Blockiert schädliche Inhalte nach dem Scan am Gateway, sodass die Computer nicht mit Viren und anderer Malware infiziert werden.	› Wie viele Antivirus-Engines werden in Ihrer Lösung verwendet? › Wie oft führt Ihre Lösung einen Scan des Inhalts durch?
URL Hardening	Verhindert, dass Besucher Ihrer Website auf Inhalte zugreifen können, die sie nicht sehen sollen.	› Muss ich die Struktur meiner Website manuell eingeben, oder kann dies mit dynamischen Updates automatisch erfolgen?
Cookie-Schutz	Verhindert, dass an Ihre Website-Besucher ausgegebene Cookies manipuliert werden.	› Schützt das System meine E-Commerce-Website vor einer Manipulation der Produktpreise?

Wireless Protection

WLAN-Netzwerke benötigen dieselben Sicherheitsrichtlinien und denselben Schutz wie das Standardnetzwerk. Das drahtgebundene und das drahtlose Netzwerk werden von den Netzwerkadministratoren jedoch oftmals als zwei separate Netzwerke betrieben. Wireless-Schutz von Ihrem Network-Security-Anbieter sollte die Durchsetzung einheitlicher Sicherheitsrichtlinien innerhalb Ihres Unternehmens deutlich vereinfachen. Stellen Sie sicher, dass Ihre Wireless Protection die Network-Security-Sicherheitsfunktionen auch auf Ihre WLANs ausweitet. Sie sollten außerdem die Möglichkeit haben, das WLAN-Netzwerk zentral zu verwalten.

Empfohlene Funktionen	Beschreibung	Fragen an Ihren Anbieter
Bereitstellung per Plug-and-Play	Ermöglicht dank konfigurationsfreier Access Points eine schnelle und einfache Einrichtung.	› Wie lange dauert die Einrichtung und Bereitstellung von Access Points und Richtlinien?
Zentrale Verwaltung	Vereinfacht die Verwaltung des WLAN-Netzwerks durch die Zentralisierung von Konfiguration, Protokollierung und Fehlerbehebung in einer einzigen Konsole.	› Muss ich die Access Points einzeln nacheinander in der lokalen Benutzeroberfläche oder Befehlszeile konfigurieren?
Integrierte Sicherheit	Bietet dank umfassender UTM-Sicherheit sofortigen Schutz für alle Wireless-Clients.	› Kann der gesamte WLAN-Datenverkehr direkt an das Security-Gateway weitergeleitet werden?
WPA/WPA 2-Verschlüsselungsoptionen	Verschlüsselung auf Enterprise-Level. Sie macht die Daten für nicht autorisierte Empfänger unleserlich und schützt auf diese Weise vor Datenverlust und Diebstahl.	› Werden mehrere Verschlüsselungs- und Authentifizierungsmethoden unterstützt? › Ist eine Schnittstelle zu meinem RADIUS-Server verfügbar?

Internet-Gastzugang	Schützt mehrere WLAN-Zonen mit jeweils verschiedenen Authentifizierungs- und Datenschutzeinstellungen. Aktiviert und unterstützt WLAN-Hotspots.	› Wie viele verschiedene WLAN-Zonen werden unterstützt?
		› Welche Arten von Hotspots werden unterstützt?
		  › Akzeptieren der Nutzungsbedingungen
		  › Täglich geändertes Passwort
		  › Voucher-basiert

Detailliertes Reporting	Liefert Informationen zu verbundenen Wireless-Clients und zur Netzwerknutzung.	› Gibt es eine integrierte Reporting-Funktion? › Ist für die Reporterstellung ein separates Tool erforderlich?

Endpoint Protection

Um die Sicherheit in Ihrem Netzwerk aufrechtzuerhalten, benötigen Sie eine Komponente zum Schutz Ihrer Endpoints, die neu angeschlossene Geräte auf aktuelle Updates und Sicherheitsrichtlinien überprüft. Ihre Endpoint Protection muss alle firmeneigenen Geräte innerhalb und außerhalb des Netzwerks schützen. Verringern Sie Ihren Verwaltungsaufwand und sparen Sie Kosten, indem Sie Ihre Endpoints direkt in Ihre Network Security Appliance integrieren. Diese Integration hilft Ihnen auch bei der Einhaltung von Compliance-Vorschriften, wenn am Gateway und Endpoint unterschiedliche Antivirus-Engines ausgeführt werden.

Empfohlene Funktionen	Beschreibung	Fragen an Ihren Anbieter
Einfache Bereitstellung	Ermöglicht dem Unternehmen die einfache Bereitstellung und Verwaltung von Endpoint-Clients zur Vermeidung von Malware-Angriffen und Datenverlust.	› Wie wird der Endpoint-Client bereitgestellt? › Ist die Einbindung einer bestehenden Endpoint-Lösung möglich?
Antivirus-Scans	Scannt Endpoints auf Viren und andere Malware, damit diese nicht in das Netzwerk gelangen.	› Wie viele verschiedene Antivirus-Engines werden verwendet? › Ermöglicht die Lösung Live-Updates über die Cloud?
Device Control	Ermöglicht dem Unternehmen, die Verwendung von Modems, Bluetooth, USB-Ports, CD/DVD-Laufwerken usw. zu unterbinden.	› Welche Geräte können mit Ihrer Lösung gesteuert werden? › Funktioniert der Endpoint-Schutz nur dann, wenn sich die Endpoints in der Domain befinden oder über einen VPN-Tunnel verbunden sind?
Echtzeit-Reporting	Bietet mit aktuellen Statistiken Einblick in den Status der Endpoints.	› Gibt es eine integrierte Echtzeit-Reporterstellung?
Support für mobile Mitarbeiter	Überall der gleiche Benutzerschutz – innerhalb und außerhalb des Netzwerks	› Wie werden Endpoints geschützt, die sich außerhalb des Unternehmensnetzwerks befinden?

Fazit

Die Anschaffung einer neuen Firewall ist eine wichtige Entscheidung. Schließlich werden Sie die neue Firewall im Normalfall mindestens drei Jahre nutzen und das gewählte Modell muss demzufolge sowohl jetzt als auch in Zukunft Ihre Anforderungen erfüllen. Mit diesem Firewall Buyers Guide können Sie ermitteln, welche Firewall-Funktionen Sie benötigen, und anschließend die einzelnen Lösungen auf Grundlage unabhängiger Drittanbietertests vergleichen.

Über Sophos

Sophos entwickelt schon seit fast 30 Jahren Antivirus- und Verschlüsselungsprodukte. Heute sichern unsere Produkte Netzwerke, die von 100 Mio. Menschen in 150 Ländern und 100.000 Unternehmen genutzt werden – u. a. bei Pixar, Xerox, Ford, Avis und Toshiba, aber auch in vielen kleinen und mittelständischen Unternehmen weltweit.

Mit unseren Produkten können Sie alle Endpoints in Ihrem Netzwerk schützen – Laptops, virtuelle Desktops, Server, Internet- und E-Mail-Verkehr sowie mobile Geräte. Wir bei Sophos wissen: Die Lösung für komplexe IT-Sicherheit kann nicht noch mehr Komplexität sein. Daher konzentrieren wir uns darauf, unsere Produkte so einfach wie möglich zu gestalten, ohne Abstriche bei der Funktionalität, Performance oder Sicherheit zu machen – denn einfache Sicherheit ist die bessere Sicherheit.

Jetzt kostenfrei testen

Kostenlose 30-Tage-Testversion
unter www.sophos.de/firewall

Advantix.
Groupware AG

Bahnhofstrasse 33b
CH - 8703 Erlenbach
Tel +41 44 914 88 44
Fax +41 44 914 88 45
welcome@advantix.ch

SOPHOS