



Symantec SGS 320

VS.

Check Point Safe@Office 410 W



PROTECTSTAR
for your security

Einleitung

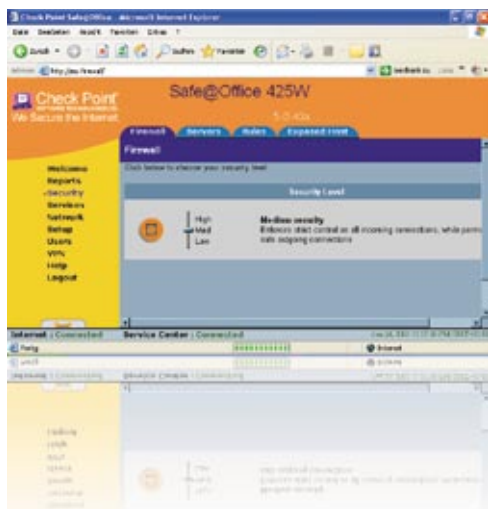
Netzwerke in kleinen Unternehmen stellen hohe Anforderungen an die Sicherheit. Jedoch verfügen diese Unternehmen nur selten über die erforderlichen Ressourcen, die für den Betrieb kostenintensiver Lösungen mit hohem Verwaltungsaufwand erforderlich sind.

Um diese Probleme zu lösen, wurden von den beiden renommierten Unternehmen Symantec und Check Point Software Technologies zwei Sicherheitslösungen für diese Unternehmen entwickelt: Die Symantec Gateway Security 320 (SGS 320) und die Safe@Office 410W von Check Point.

Während Symantec in die SGS 320 ein Intrusion Detection und Prevention System, statisches Content Filtering und Funktionen zur Richtliniendurchsetzung für über Symantec verbundene Virenschutz-Clients integriert, setzt Check Point mit der Safe@Office 410W auf optionale und individuell benötigte Services wie Web-Filtering, Anti-Spam, Anti-Virens Scanner, Dynamic-DNS und Dynamic VPN.

Beide Geräte verbinden umfassende Sicherheit mit einem zuverlässigen Internet-Gateway und einer sicheren Wireless-LAN-Option in einer einzigen Lösung.

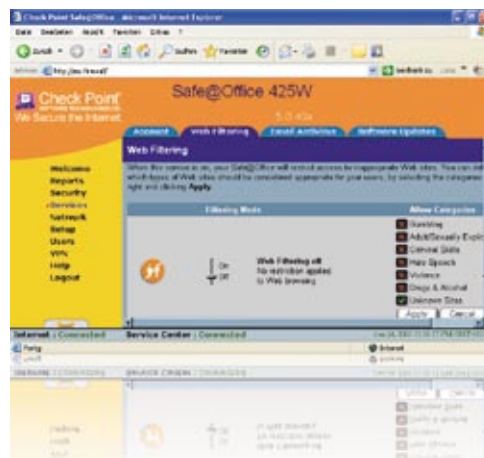
In diesem Vergleichstest haben wir die zwei Sicherheitsappliances detailliert unter die Lupe genommen und einem umfassenden Härtestest unterzogen.



Sicherheit

Zunächst wurde bei der SGS 320 von Symantec eine mögliche Sicherheitslücke gefunden, da das Gerät den ICMP-Leak-Test nicht bestand. Bei der Safe@Office 410W von Check Point meldeten unsere Sicherheitsscanner, dass das Gerät den Denial of Service (DoS) Angriff namens „Racoon invalid cookie malloc bug“ nicht bestanden hat.

Nach genauer Überprüfung und Rückfragen an die Hersteller stellte sich heraus, dass es sich bei beiden gefundenen Schwachstellen um klassische „False Positiv“ handelte und keinerlei Auswirkungen auf die Sicherheitsfunktionen der Appliances haben.



Die SGS 320 und Safe@Office 410W haben an den Tagen unseres Testverfahrens alle zum Zeitpunkt bekannten 5858 verschiedenen Angriffs- und Sicherheitstest erfolgreich abgewehrt.

In diesen Testreihen wurden beispielsweise verschiedene Arten von Portscans, über zweihundertdreißig Arten von Denial of Service Angriffen, alle bekannten Schwachstellen von Firewalls und Betriebssystemen, sowie Sicherheitslücken in bestimmten Anwendungen, unter realen Bedingungen getestet. Unseren vierstündigen Dauer-Penetrationstest haben die beiden Geräte ebenfalls erfolgreich absolviert. Die Schutzfunktionen „IP-Spoof-Schutz“ und „TCP-Flag-Validierung“, die sowohl in der SGS 320 als auch in der Safe@Office 410W



standardmäßig integriert sind, funktionieren tadellos: Der IP-Spoof-Schutz blockierte zuverlässig alle Nicht-Broadcast- und Multicast-Pakete, Ebenfalls beim Kauf einer Safe@Office 410W erhalten Anwender ein Jahr lang Garantie und Softwareupdates inklusive. Interessenten können die Appliances jedoch nicht direkt bei Symantec oder Check Point erwerben, sondern nur bei einem autorisierten Reseller. Dieser ist dann für den Support und die gesetzlichen Gewährleistungen zuständig und erneuert auf Wunsch hin auch den Supportvertrag.

Zusammen mit dem Kauf einer SGS 320 oder Safe@Office 410W können dann auch optional die Support-Pakete „Silver Support“, „Gold Support“ und „Platinum Support“ bzw. die verschiedenen Services, wie Web-Filtering, Dynamic-DNS und eMail Anti-Virens Scanner erworben werden.

Preis / Leistung

Die SGS 320 Appliance kostet aktuell 399,00 Euro (netto) und ist im Verhältnis zu anderen Hardware-Firewalls auf dem IT-Sicherheitsmarkt, preiswert. Mit einem Preis von 115,00 Euro jedoch ist das Zusatzmodul für die Nutzung des WLAN Access Point relativ hoch. So belaufen sich die Gesamtkosten unseres SGS 320 Testgerätes auf 514,00 Euro. Die Safe@Office 410W kostet mit 799,00 Euro über zweihundertfünfzig Euro mehr als die SGS 320, bietet jedoch mehr Leistung bei den Durchsatzraten (Firewall & VPN), einen USB-Printserver, einen zusätzlichen DMZ-



Port und hat den **WLAN Access Point** bereits integriert, der die Standards IEEE 802.11b (11 Mbps), 802.11g (54 Mbps) und Super-G (108 Mbps) unterstützt. Alternativ ist auch das kleinste Modell, die **Safe@Office 405W** zu nennen.

Sie ist mit **499,00 Euro** günstiger als die SGS 320 Appliance, hat jedoch keinen DMZ-Port und unterstützt maximal fünf angeschlossene Clients. Die Preise für die verschiedenen Services der **Safe@Office 410W**, wie Antiviren-Scanner, Web-Filtering, Dynamic-DNS, Dynamic-VPN, usw. sind je nach Händler unterschiedlich.

Einige rechnen nach der Anzahl der an der Appliance angeschlossenen Benutzer und andere bieten günstige Komplettpakete einschließlich einer Safe@Office Appliance an. In der Regel bewegen sich die Preise für die **optionalen Services** zwischen **120,00 Euro** und **280,00 Euro** pro Jahr. Sie sind im Vergleich zu separaten Softwareprodukten, kostengünstig und zugleich empfehlenswert.

Fazit

Testsieger dieses Vergleichstest ist die **Safe@Office 410W Appliance** von **Check Point**. Die Sicherheitslösung vereint umfassenden Schutz vor Attacken durch **Check Points** bewährte Sicherheitskomponenten wie VPN Gateway, E-Mail-Antivirus, URL Filter, automatische Sicherheitsupdates alle zwei Stunden, DynDNS und Reporting. Der zusätzliche **USB-Printserver** für bis zu vier USB-Drucker, die Sicherung des Wireless LAN mittels höchstmöglicher Sicherheit **IPSEC** VPN und außerordentlich hoher Übertra-

gungsrate von bis zu **108 Mbit** (Super-G), dem vorhandenen DMZ-Port sowie der Schutz auf der Netzwerk- (**Layer 3**) und auf der Applikationsebene (**Layer 7**) machen die Safe@Office 410W zu einer „**State of the Art**“ Firewalllösung auf dem IT-Sicherheitsmarkt. Punkteabzug erhält die Sicherheitslösung aufgrund der Beschränkung von bis zu zehn angeschlossenen Clients, das fehlende Intrusion Detection System und dem höheren Kaufpreis gegenüber der SGS 320.



Die **SGS 320 Appliance** von **Symantec** können wir dagegen für Unternehmen empfehlen, die bereits mit verschiedenen Lösungen von Symantec ausgestattet sind. Zum Beispiel ist die SGS 320 auch als Erweiterung zur SGS Appliances der 5400er Serie von Symantec in Umgebungen mit einem Hub geeignet. Die **SGS 320** konnte in unseren Testreihen vor allem durch das integrierte **Intrusion Detection and Prevention System**, das **statische Content Filtering** und durch den niedrigeren Kaufpreis überzeugen. Zudem hat die Appliance **keine** Begrenzung

für die an dem Gerät angeschlossenen Clients. Der Hersteller empfiehlt aber, nicht mehr als 50 Clients mit der Appliance zu vernetzen. Punkteabzug erhält die SGS 320 aufgrund des fehlenden verschlüsselten Zugriffs über den Port 443 (https) auf die Web-Konfigurationskonsole, den fehlenden USB-Printserver und DMZ-Port sowie die niedrigeren Performancewerte und des nicht unterstützten WLAN-Standards Super-G mit 108 Mbps gegenüber der Safe@Office 410W von Check Point.



Impressum:

PROTECTSTAR

for your security

ProtectStar Inc.
Testcenter

Postfach 10 25 08
D-86015 Augusburg
Germany

www.protectstar.com
testcenter@protectstar.com

Gestaltung und Konzeption:



wo-pro werbung -agentur für
klassische und neue medien
Wettringer Str. 32
D-74585 Kleinansbach

Fon: 07958 92 57 14
Fax: 07958 92 68 98
E-Mail: info@wo-pro.de
Web: www.wo-pro.de