PROTECTSTAR AWARD 2007

PROTECTSTAR™

Check Point

Safe@Office 500 & VPN-1 Edge

SICHERHEIT

In den durchgeführten Testreihen wurden die Gerätemodelle von Safe@Office 500 und VPN-1 Edge des Herstellers Check Point überprüft.

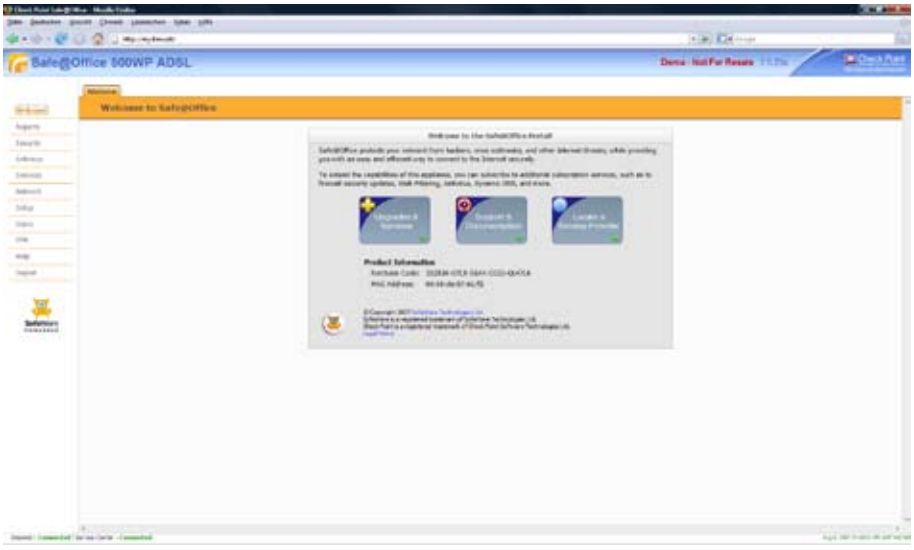
Die integrierte **Stateful Packet Inspection Firewall** von Check Point ist identisch in allen Geräten und Modellen von Safe@Office 500 und VPN-1 Edge. Die Testreichen liefen sowohl unter **Laborbedingungen**, als auch unter **realen Bedingungen ab**. Im Testlabor von **ProtectStar™** wurden die Geräte in der aktuellen Softwareversion (Stand: Oktober 2007) getestet.

Ebenso kam die kommende Version 7.5(.23x) zur Begutachtung. Im Übrigen zeigen die im Testbericht abgebildeten Screenshots bereits die kommende Version 7.5, welche demnächst für alle Anwender bereitstehen wird.

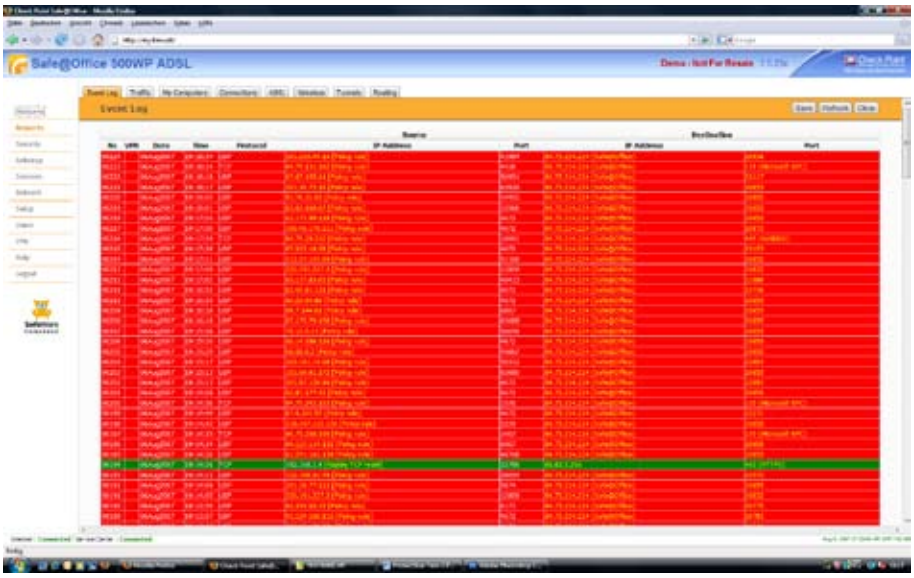
Das Kernstück in allen Gerätemodellen von Safe@ Office und VPN-1 Edge – die integrierte Firewall inkl. dem **SmartDefense -** (ein integriertes IDS/IPS System) von Check Point, hat in den Testverfahren bezüglich des Außenschutzes alle zum Zeitpunkt bekannten **12.419** verschiedenen **Angriffs- und Sicherheitstests** erfolgreich bestanden. Die Sicherheitstests umfassten dabei alle bekannten **Denial of Service** (DoS) **–** Angriffsarten, sowie die **Ausnutzung** aller zum Zeitpunkt der Testverfahren bekannten **Schwachstellen** von allen Betriebssystemen (Windows, Linux, Unix, uvm.), Anwendungen, Brute Force, CGI abuses, Useless Services, Backdoors und Sicherheitschecks. Im Detail zählen zu diesen durchgeführten Sicherheitstests der verschiedenen Gefahrenstufen (Low, Medium, High) im Bereich der **DoS-Angriffe** (241 DoS – Angriffe). beispielsweise „OpenSSL denial of service", „ping of death", „RPC DCOM Interface DoS", „MS Checkpoint Firewall-1 UDP denial of service", „Trend Micro Office Scan Denial of service" und „Linux 2.1.89 - 2.2.3 : 0 length fragment bug".

Aus den Bereichen **CGI-Abuses** gehörten z. B. „PHP < 4.4.7/5.2.3 Multiple Vulnerabilities ", „Socketmail <= 2.2.6 - Remote File Include Vulnerability" und „PHPAdsNew code injection". Darüber hinaus wurden die Geräte mit 33 **bekannten und speziellen Angriffsvariationen** für **Firewalls** attackiert. Alle durchgeführten Sicherheitstests blockierte die Check Point Firewall erfolgreich.

In weiteren Testphasen wurde die integrierte Firewall von Check Point in den verfügbaren Sicherheitsprofilen **LOW**, **MEDIUM**, **HIGH** und **BLOCK ALL** betrieben und mit standardisierten Portscans nach eventuell geöffneten **TCP-** und **UDP- Ports** gescannt. Der Scan erfolgte über das gesamte Spektrum von 0 – 65535 Ports. In einem zusätzlichen Testverfahren erfolgte dann ein **SYN-Portscan** (half-open) - dem so genannten Stealth-Scan.



Das Standardregelwerk der **Stateful Packet Inspection** Firewall blockiert alle Verbindungsversuche aus dem Internet und lässt jede Verbindung vom internen Netzwerk in das Internet zu (Sicherheitsstufe: LOW). Mit den vier Sicherheitsstufen **LOW**, **MEDIUM**, **HIGH** und **BLOCK** kann das Regelwerk der Firewall vom Anwender selbst weiter eingeschränkt werden. Die verfügbaren manuell einstellbaren Sicherheitsstufen sind wie folgt definiert: In der Sicherheitsstufe „**LOW**" wird jegliche Verbindung vom internen Netzwerk zum Internet erlaubt. Alle aus dem Internet stammenden



Verbindungen werden blockiert. Einzige Ausnahme sind ICMP Pakete - so genannte Pings. In der Sicherheitsstufe „**MEDIUM**" werden alle Verbindungen vom internen Netzwerk zum Internet erlaubt. Mit Ausnahme den Windows Datei Freigaben (NTB Ports 137, 138, 139 und 445). Es werden alle aus dem Internet stammenden Verbindungen blockiert.

Die „**HIGH**" Sicherheitsstufe ist die höchste und restriktivste Stufe. Bis auf einige Ausnahmen wird jede Verbindung aus dem internen Netzwerk zum Internet unterbunden. Lediglich die Verbindungen für Standard Internet Anwendungen werden zugelassen. Dazu zählen der Zugriff auf Webseiten (HTTP, HTTPS), E-Mail (IMAP, POP3, SMTP), FTP, NNTP, Telnet, DNS, IKE, Port 2746/ UDP und Port 256/TCP.

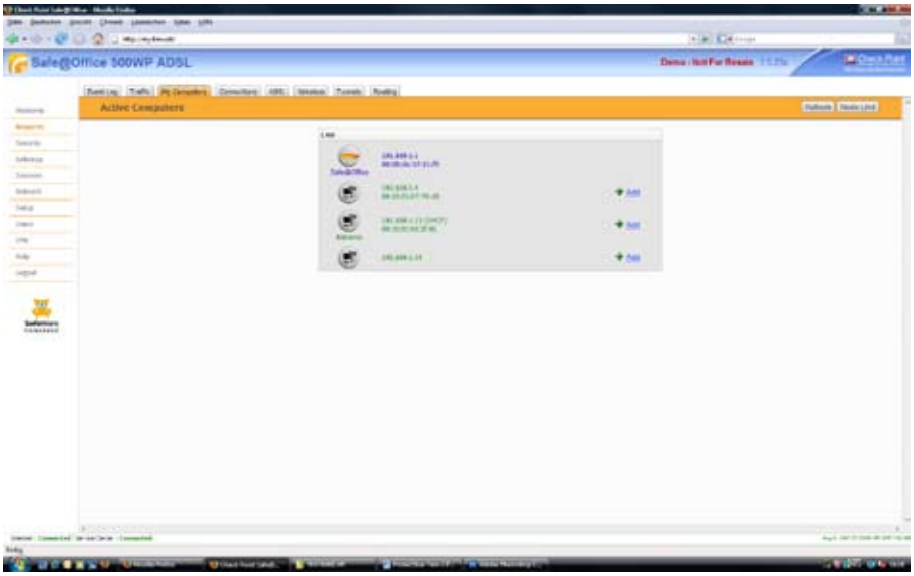
In der Sicherheitsstufe „**BLOCK ALL**" wird jegliche Verbindung von außen nach innen und von innen nach außen vollständig unterbunden. Eingestellt werden können die genannten Sicherheitsstufen mit Hilfe eines Schiebereglers im Hauptmenü (http://my.firewall) unter dem Menüpunkt SICHERHEIT. Auch wenn solche „Schieberegler" bei Firewalls unter Experten nicht beliebt sind, so muss hier eine Ausnahme gemacht werden, denn die unterschiedlichen Sicherheitslevels sind sehr an die Bedürfnisse von Unternehmen und kleinen Außenstellen angepasst. Im Rahmen der durchgeführten Portscans (tcp-connect und syn/half-open) fanden sich **keine** geöffneten Ports und **keine** unnötigen Dienste, die für gewöhnlich zu Sicherheitsproblemen führen können. Sowohl durch die **automatisch** ablaufenden Testreihen des hauseigenen **ProtectStar™ Security-Scanners**, der zusätzlich **9666** (Stand: 06.08.2007) weitere Sicherheitstests und Angriffstaktiken durchführte, als auch durch die **manuell** ausgeführten Prüfungen, wurden **keine** Schwachstellen oder Sicherheitsrisiken festgestellt.

Den **vierstündigen** Dauer-**Penetrationstest** absolvierte die Firewall von Check Point uneingeschränkt und **erfolgreich** – ohne nennenswerte Performanceverluste. Das integrierte **SmartDefense** von Check Point – ein Intrusion Detection und Prevention System, welches auf der Check Point Application Intelligence technology basiert – zeigte durchwegs sehr gute Resultate. Es schützt beispielsweise pro aktiv vor Netzwerkwürmern, Denial of Service Attacken und erkennt Anomalien im Netzwerkverkehr.

In einem weiteren Testverfahren wurde geprüft, ob sich die Geräte Safe@Office 500 und VPN-1 Edge manipulieren lassen, wenn ein **Angreifer/ Hacker direkt am LAN Port** der Check Point Firewall angeschlossen ist. So lässt sich praktisch auch analysieren, was passieren könnte wenn ein Angreifer sich bereits Zugang zu einem vertrauenswürdigen Netzwerk verschafft hat.

Ein solches Angriffsszenario stellte das Testcenter von ProtectStar™ nach. Dabei fand sich im Bezug auf die **TCP Sequence prediction**, dass der TCP/IP Stack nicht vollständig geschützt ist. Dies hätte zur Folge, dass ein Angreifer die Sequenz-Nummer vorhersagen bzw. erraten, und somit bestehende Verbindungen manipulieren könnte.

Als (interne) offene Ports wurden Port 22, 53,80, 443 und 981 erkannt. Ferner ließen sich Teile des VPN Zertifikates auslesen sowie die aktuelle **Uhrzeit** der Safe@Office 500 oder VPN-1 Edge Appliance.



Die erlangten Informationen sind der Kategorie **Low-Risk** zuzuordnen. Da das Angriffsszenario eher ~~als~~ theoretischer Natur ist, muss man diesem kaum Beachtung schenken. Sowohl theoretisch als auch praktisch wäre es möglich das Zugangspasswort der Adminkonsole (http[s]: my.firewall) einer Safe@Office oder VPN-1 Edge zu hacken bzw. zu erraten. Aus diesem Grund sollte als Zugangskennwort ein sicheres Passwort, bestehend aus Sonderzeichen, Zahlen sowie Groß- und Kleinbuchstaben gewählt werden (weitere Informationen:http://www.protectstar-research.com/de.informationen-passworter.html).

LEAKTESTS

„**Leaktests**" überprüfen bei softwarebasierten Firewalls, wie z. B. Personal Firewall, ob verschiedene Techniken erkannt werden, um Informationen wie beispielsweise Passwörter, persönliche Daten, usw. von einem Computer aus, vorbei an der Firewall in das Internet zu schleusen.
Bei einer hardwarebasierten Firewall wie der Safe@Office 500 oder VPN-1 Edge muss daher entsprechend vorsichtig agiert werden, um Resultate nicht zu verfälschen.

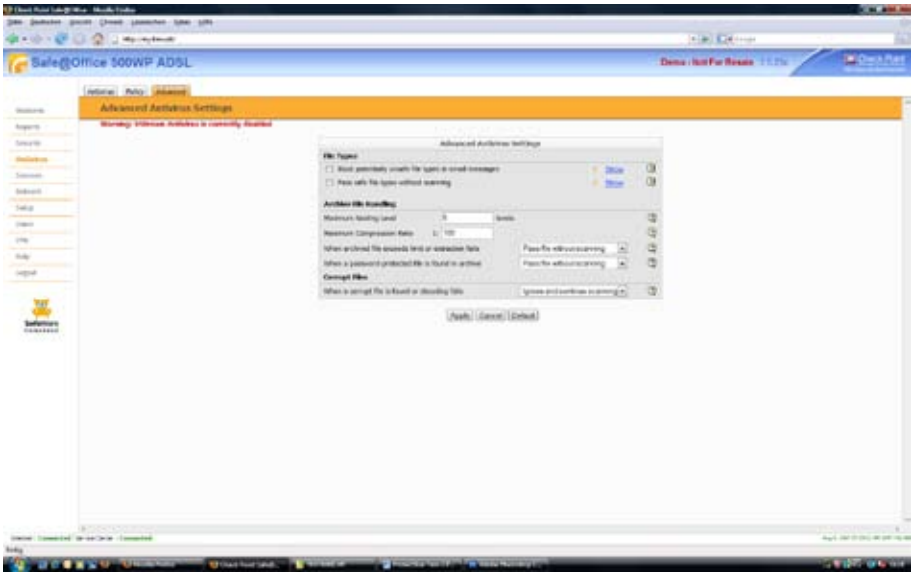
Getestet wurde daher, ob die Leaktests blockiert werden, wenn das Standardprofil „MEDIUM" der Check Point Firewall aktiviert ist. Allerdings ist dabei festgestellt worden, dass das Regelwerk der Safe@Office 500 und VPN-1 Edge in diesem Sicherheitsprofil nicht ausreicht, um Leaktests zu unterbinden. Das Profil „HIGH" bietet mehr Schutz.

Die Erkennungs- bzw. Erfolgsrate bei den Leaktests fällt durch die manuelle **Konfiguration** des Regelwerks der Check Point Firewall höher aus. So würde sich ebenfalls realisieren lassen, dass 100% der bekannten Leaktests erkannt werden.
Um die Schutzfunktionen des **Anti-Virenscanners** (ClamAV) testen zu können, wurden mehrere umfangreiche Viren- und Malwarearchive erstellt. Diese Archive umfassten insgesamt über **zweitauend** verschiedene Schädlinge. Von ganz neuen und aktuellen Viren, Würmern, Trojanern, Dialern und Spyware, bis hin zu alten MS-DOS Bootviren und selbstentwickelten unbekannten Schädlingen. Zusammenfassend konnte die **Malware-Erkennungsrate** auf **99,38%** bestimmt werden, welche zeigt, dass der in der Safe@Office 500 bzw. VPN-1 Edge integrierte Anti-Virenscanner sehr gute Leistungen besitzt.

Die automatische Update-Funktion (my.firewall -> SERVICES -> SOFTWARE UPDATE) sorgt für einen lückenlosen Schutz gegen neue Bedrohungen und sich schnell verbreitende Attacken. Alle **60 Minuten** sucht eine Safe@Office 500 oder VPN-1 Edge Appliance **automatisch** nach möglichen verfügbaren Updates bezüglich Firmware-Updates, Anti-Viren Signaturen, SmartDefense Regeln oder Signaturen für den Webfilter. Es ist aber auch möglich, bei bekannt werden von neuen Threads entsprechende Patches zum optimierten Schutz vom Managed Service Provider **sofort** eingespielt zu bekommen.

Zu beachten ist jedoch, dass einzelne Sicherheitsfeatures wie Anti-Virenscanner, SmartDefense, Webfilter oder auch die automatischen Updatefunktionen nur über einen entsprechenden Servicevertrag freigeschaltet und benutzt werden können.

BENUTZER-FREUNDLICHKEIT



Die beiden Check Point Geräte **Safe@Office 500** und **VPN-1 Edge** sind in verschiedenen Modellen erhältlich. So gibt es beide Modelle auch mit integriertem WLAN Hotspot und/ oder zusätzlich integriertem ADSL Modem.

Hat sich ein Unternehmen für ein Modell entschieden, so muss ~~nun~~ die Anzahl der Benutzer definiert werden. Die Geräte sind für 5, 25 und unbegrenzte Benutzer bei Safe@Office 500 und 8, 16, 32 und unbegrenzte Anzahl an Benutzern bei VPN-1 Edge verfügbar. Selbstverständlich kann die Anzahl der Benutzer auch später durch einen Servicevertrag erhöht werden.

Die Installation einer Safe@Office oder VPN-1 Edge ist äußerst **anwenderfreundlich** und der Installationswizard hilft dem Anwender das Gerät in einfachen Schritten zu konfigurieren. Überhaupt werden Anwender von Anfang an von der Vielzahl an individuellen Konfigurationsmöglichkeiten beeindruckt sein, die kaum Wünsche offen lassen. Das Web-Interface ist optisch ansprechend und übersichtlich gehalten, so dass alle Funktionen und Einstellungen leicht vorgenommen werden können.

Bei der Installation und Konfiguration dürfte es im Regelfall keinerlei Komplikationen geben. Sollten sich dennoch Schwierigkeiten ergeben, so helfen das als PDF verfügbare uns sehr ausführliche 605seitige (Safe@Office) bzw. 633seitige (VPN-1 Edge) **Handbuch** sowie die mitgelieferte Schnellanleitung, die alle relevanten Schritte und Fragen detailliert und anschaulich beantworten.

Zusätzlich steht dem Benutzer jederzeit auf der linken Seite des Web-Interfaces durch anklicken des „**Help**"-Button eine praktische Online-Hilfe zur Verfügung. Hier sollte jedoch nachgebessert werden, da sich die Hilfe zum Teil auf vergangene Software-Versionen bezieht oder keine Hilfestellungen zu vorhandenen bzw. neuen Einstellungsmöglichkeiten bieten.

Auf der Rückseite einer Safe@Office 500 und VPN-1 Edge ist ebenfalls ein zusätzlicher **DMZ** (De-Militarized-Zone) Port angebracht, der es Unternehmen erlaubt, einen öffentlichen Server, wie beispielsweise einen Webserver, ohne zusätzlichen Switch anzuschließen und gleichzeitig durch die Stateful Packet Inspection Firewall des Gerätes schützen zu lassen. Weitere logische DMZs können zudem manuell eingerichtet werden.

Ebenso sind zwei USB-Ports mit integriertem Printserver vorhanden, an die bis zu zwei Drucker via USB-Kabel angeschlossen werden können, die dann für alle an der Safe@Office / VPN-1 Edge angeschlossenen Benutzer im Netzwerk verwendet werden können. Die zusätzlichen Funktionen wie Gateway High Availibility, Backup ISP, VPN Server, Dial Backup VLAN-Unterstützung, Remote Access VPN Gateway, Bridge Mode und Static NAT sind für Unternehmen nützliche Werkzeuge, die in allen Safe@Office und VPN-1 Edge Geräten standardmäßig integriert sind. Optisch besonders hervorgehoben ist unter dem Menüpunkt **„Reports" -> „Active Computers"** die grafische Darstellung für die an der Safe@ Office angeschlossenen Computersysteme (einschließlich Computername & MAC-Adresse).

Zudem erfährt der Anwender unter diesem Menüpunkt, welche IP-Adresse die entsprechende Workstation oder Server hat und ob diese IP-Adresse statisch oder via DHCP an das jeweilige System vergeben wurde. Dies gilt ebenso für alle Computer, die via Wireless-LAN mit einer Safe@ Office oder VPN-1 Edge verbunden sind.

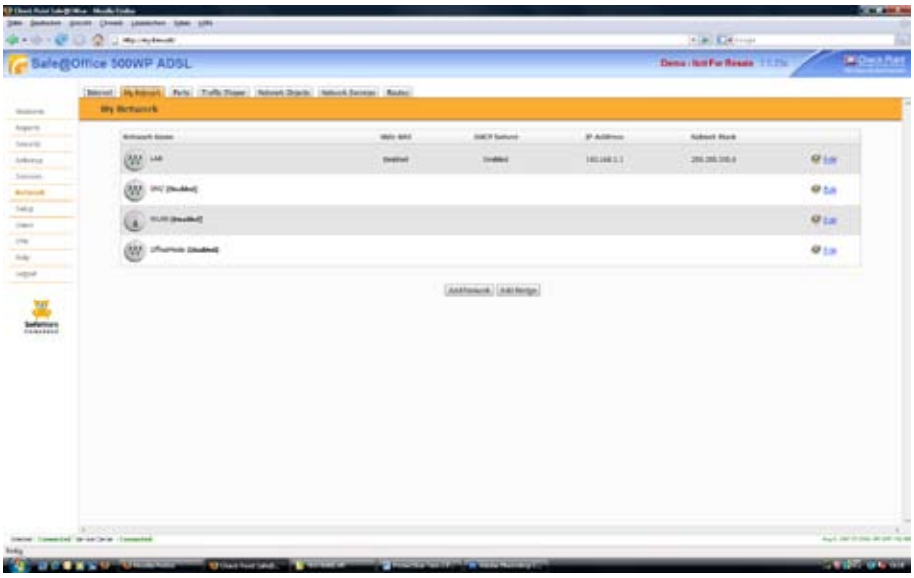
Die Log-Dateien sind ausreichend und können bei Abschluss eines entsprechenden Servicevertrages zusätzlich in Form eines übersichtlichen und grafisch aufbereiteten Reports bereitgestellt werden.

Anwendern können unter „**Reports**" -> „**Event Log**" auf eine farbige Tabelle zurückgreifen, auf der rot untermalte Einträge einen erfolgreich abgewehrten Angriff und blau untermalte Einträge eine Änderung in der Konfiguration der Safe@ Office kennzeichnen. Das Protokoll kann zudem als **Excel-Tabelle** abgespeichert werden.

Aus den Einträgen kann der Administrator erfahren, ob ein Angriff erfolgte und zu welchem Zeitpunkt. Über die Protokolle TCP oder UDP lassen sich Computer/Server ~~auf~~ und attackierte Ports feststellen. Durch einen Mausklick auf die IP-Adresse des Angreifers öffnet sich ein **WHOIS**-Fenster, in dem der Administrator mehr Informationen über den Angreifer bzw. dessen Provider erhalten kann. Mit einem zusätzlichen Reporting-Servicevertrag werden den Safe@Office oder VPN-1 Edge Benutzern über eine zentrale Service Management Plattform (SMP) ein monatliches Reporting in grafischer Auswertung zugesandt. Der optional erhältliche und kostenpflichtige **eMail Anti-Virenscanner** kommt aus dem Hause **ClamAV.** Auf Wunsch kann er ein- und/oder ausgehende (**SMTP/ POP3/IMAP**) E-Mails nach Viren, Würmern und Trojanern durchsuchen. Besonders praktisch ist hier, dass der Anwender mit Hilfe eines Wizards individuell einstellen kann, welches Protokoll und welcher Port bei ein- und/oder ausgehenden Verbindungen nach Malware suchen soll. Ebenso können ganze Port Ranges (bspw. Von Port 1-1024) eingestellt werden.

Der integrierte Virenscanner, der über einen Servicevertrag freigeschaltet werden kann, funktionierte hervorragend und erkannte alle Testviren und Trojaner, die per E-Mail verschickt oder empfangen wurden. Sobald der Anwender beispielsweise eine E-Mail mit einer virenverseuchten Anlage erhält, entfernt der Anti-Virenscanner zuverlässig diese Datei und fügt in der ursprünglich eMail-Nachricht, statt der verseuchten Anlage eine Textdatei ein, in der die entsprechende Warnung über den Virenfund dokumentiert wird.

Ebenfalls zuverlässig verrichtete das **Web-Filtering** seine Arbeit. Der URL Web-Filter kommt von **SurfControl** und kann optional durch einen entsprechenden Servicevertrag erworben werden. Über die Konfigurationskonsole des Gerätes kann man dann den Filter wahlweise ein- oder ausschalten, sowie den Zugriff auf bestimmte Kategorien erlauben und blockieren. Der Benutzer kann zwischen den Kategorien „**Violence**", „**Drugs & Alcohol**", „**Adult**", „**Criminal Skill**", „**Gambling**", „**Hate Speech**", „**News**", „**Travel**", „**Sport**", „**Unknown Sites**", und vielen weiteren auswählen. Unter die Kategorie „**Adult**" fällt zum Beispiel die Webseite von Playboy und alle anderen bekannten Webseiten, die keine jugendfreien oder anstößige Inhalte haben. Gerade für größere Unternehmen ist die Kategorie „**Unknown Sites**" wertvoll. Hier wird unter



anderem der Zugriff auf die Suchmaschine Google und auf das Online-Auktionshaus Ebay blockiert. Dies kann verhindern, dass Angestellte während der regulären Arbeitszeit diese Dienste verwenden.

Hier haben wir die Option vermisst, das Web-Filtering zu bestimmten Uhrzeiten ein- oder auszuschalten, so dass beispielsweise der Zugriff auf Suchmaschinen oder andere Portale während der täglichen Mittagspause eines Unternehmens erlaubt und zu allen anderen Zeiten wieder blockiert werden kann.

PERFORMANCE

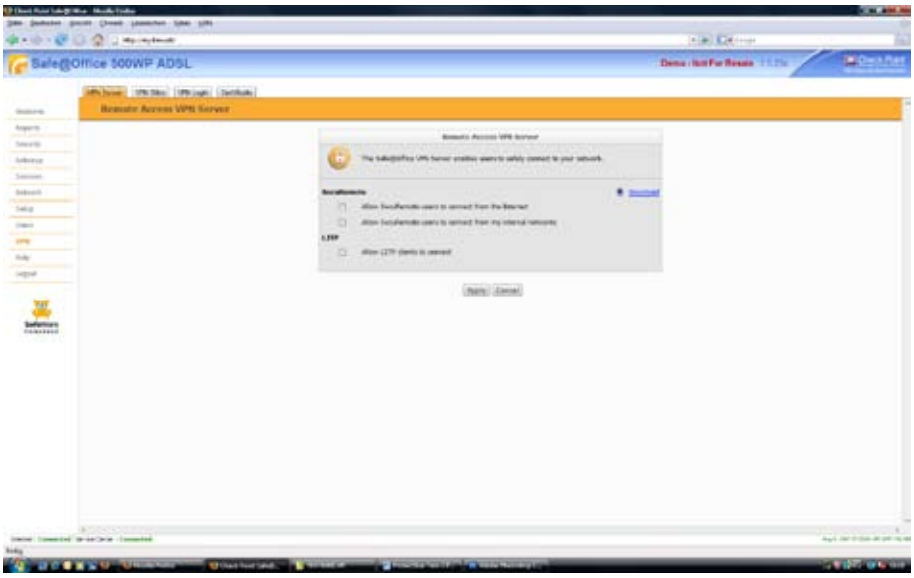
Die Safe@Office 500 und VPN-1 Edge Geräte arbeiteten in den durchgeführten Testreihen **schnell** und sehr **zuverlässig**. Es konnten keine Leistungseinbußen oder Mängel bei der Performance in irgendeiner Weise festgestellt werden.Selbst während des **vierstündigen** Dauer-Penetrationstest konnte mit den Safe@Office und VPN-1 Edge Geräten weiterhin unter kleinen Leistungseinbußen gearbeitet werden. Keines der Geräte konnte zum „Absturz" gebracht werden.

Die verfügbaren Safe@Office 500 und VPN-1 Edge Gerätemodelle sind in unterschiedlichen Performanceeingeschaften ausgestattet: So bewegen sich die Durchsatzraten der Firewall zwischen **80 – 150 Mbps** und die Durchsatzraten für VPN zwischen **20 – 30 Mbps**. Die maximale Anzahl an gleichzeitigen Verbindungen gibt der Hersteller Check Point mit 8000 an.

SUPPORT

Mit dem Erwerb einer Safe@Office Appliance erhalten Anwender ein Jahr lang Garantie und Softwareupdates inklusive.Unter http://www.checkpoint.com/techsupport hat der Anwender von Produkten aus dem Hause Check Point, Zugriff auf eine umfangreiche Wissensdatenbank (Knowledgebase) und die am häufigsten gestellten Fragen (FAQ). Interessenten können die Appliances bei einem autorisierten Reseller erwerben - dieser ist dann für den Support und die gesetzlichen Gewährleistungen zuständig und erneuert auf Wunsch hin auch den Supportvertrag – oder direkt beim Hersteller Check Point / Sofaware unter www.sofaware.com

Zusammen mit dem Kauf einer Safe@Office oder VPN-1 Edge können dann auch optional die verschiedenen Services, wie Web-Filtering, Dynamic-DNS und eMail Anti-Virenscanner, uvm. erworben werden. Einige Händler bieten individuelle Dienstleistungen oder vollständige Service-Komplettpakete an, die speziell auf die Bedürfnisse der Anwender zugeschnitten werden können. Hervorragend zeigte sich auch der Onlinesupport (Live-Help) von Check Point / Sofaware, welcher nahezu immer erreichbar war und adäquate Lösungen bereitstellen konnte. Ebenso tadellos vollzog sich der Austausch eines defekten VPN-1 Edge Gerätes, welches innerhalb von drei Tagen international getauscht werden konnte.



PREIS- und LEISTUNG

Die Preisspannen der Safe@Office und VPN-1 Edge - Serie bewegen sich - je nach Modell und Anzahl der Benutzer - zwischen **299,00 Euro** und **2.300,00 Euro**.

Eine Safe@Office 500 Appliance, die für 5 User ausgelegt bzw. lizenziert ist, ist bereits für Euro 299,00 erhältlich. Eine VPN-1 Edge ADSL WU mit unbegrenzter Anzahl an Benutzern und integriertem Wireless-LAN HotSpot und ADSL Modem kann für Euro 2.300,00 erworben werden.

Hinzu kommen dann bei Bedarf noch die Kosten für die unterschiedlichen Serviceleistungen wie Anti-Virenscanner, Webfilter, SmartDefense Service, Softwareupdate, Austauschservice, uvm. So kostet der Anti-Viren Servicevertrag – je nach Anbieter – zwischen Euro 179,00 – 449,00 und der Service für die automatischen Firmwareupdates inkl. dynDNS Service zwischen Euro 54,00 und Euro 324,00 im Jahr.

Aufgrund der nahtlosen Schutzwirkung, der Vielzahl an Sicherheitsfunktionen und den nahezu unbegrenzten Einsatzmöglichkeiten, sind die Safe@Office und VPN-1 Edge Appliances, vor allem auch im Verhältnis zu anderen Hardware-Firewalls auf dem IT-Sicherheitsmarkt – sowohl für Unternehmen, Zweigstellen und kleinen Büros - preiswert.

FAZIT

Die durchgeführten Testreihen haben wieder eindrucksvoll gezeigt, dass das Unternehmen Check Point mit seiner Safe@Office 500 und VPN-1 Edge starke Sicherheits- und Firewallösungen entwickelt, die sicher, modern, anwenderfreundlich und zugleich „State of the Art" sind. Die Geräte verbinden umfassende Sicherheit mit einem zuverlässigen Internet-Gateway in einer kostengünstigen Lösung. Hier sind vor allem die minutenschnelle Installation, die leicht einzurichtenden Sicherheitsregeln mit Hilfe von Konfigurationsassistenten (One-Click-Technologie), sowie der Schutz auf der Netzwerk- (**Layer 3**) und auf der Applikationsebene (**Layer 7**), besonders erwähnenswert. Den optionalen Erwerb der Servicedienste wie Web-Filtering, Anti-Virenscanner, Dynamic-DND, uvm. können die Sicherheitsexperten des ProtectStar™ Testcenters in jedem Fall empfehlen.

Safe@Office 500 und **VPN-1 Edge** von **Check Point** werden aufgrund der durchwegs sehr guten Testresultate mit dem „**ProtectStar™ AWARD 2007**" ausgezeichnet.

PROTECTSTAR™
Inc.

1901 60th Place
Suite L 3604
Bradenton, FL
34203 USA
http://www.protectstar.com
testcenter@protectstar.com