



Sicherheit im Kasten

In Firmennetzwerken lohnen sich Appliances oft mehr als Router, da sie viele Zusatzfunktionen bieten. Der PCpro-Test spürt die Stärken und Schwächen von sechs Appliance-Modellen auf.

STEFAN RUBNER

Apliances sind nur etwas für große Unternehmen, für die 10-Mann-Firma tut's der Router aus dem Elektronikmarkt? Irrtum: Der Billig-Router stößt schnell an die Leistungsgrenze. Viele Geräte schaffen es nicht mal, ein virtuelles privates Netz (VPN) zwischen Firmen-LAN und Home-Office aufzubauen. Dank relativer kleiner interner Tabellen für Routing und Network Address Translation ist auch die Anzahl der unterstützten Clients vergleichsweise gering. Endgültig die Segel streichen müssen einfache Router, wenn es um die Prüfung der Datenströme in Echtzeit auf Viren oder andere Schadprogramme geht.

Deshalb setzen Firmen für die Verbindung mit dem Internet spezielle Geräte ein – die erwähnten Appliances. Das ist meist auf PC-Technik basierende Hardware, die von einer Linux-Distribution gesteuert wird. Der

Hersteller passt die Software auf das Gerät an. Genau wie moderne Router schützen sie das lokale Netz durch eine integrierte Firewall, sind aber wesentlich leistungsfähiger und warten mit erweiterten Funktionen auf. Zum Standard zählen mittlerweile die Unterstützung von mehreren VPN-Verbindungen und Virens Scanner.

Zwei Lager lassen sich unter den Testgeräten ausmachen: Auf der einen Seite Modelle, die vor allem erweiterte Funktionen für den Internetzugang sowie gesicherte Verbindungen bieten. In diese Kategorie fallen Astaro ASG 220, Micro Liss II FL und Sonicwall Pro 2040. Auf der anderen Seite stehen Produkte, die neben den Verbindungsoptionen zusätzliche Services für die Anwender im lokalen Netz bereitstellen. So sind der Defendo Medium wie auch der Intranator von Intra 2net und Ben Hur II von Pyramid mit ei-

nem integrierten Mailserver ausgestattet. Dem Intranator und dem Ben Hur steht zudem auch ein Fax-Server zur Seite.

Für zusätzliche Sicherheit sorgt bei allen Produkten mit Ausnahme der Micro Liss II die Option, einen oder mehrere Virens Scanner zu integrieren. Einmal installiert prüft der Virens Scanner sowohl die per HTTP oder FTP ins lokale Netz geladenen Daten wie auch E-Mails und deren Anhänge auf eventuell enthaltene Schadprogramme. Spam-, Content- und Dateityp-Filter komplettieren die Featureliste aller Probanden. Einzige Ausnahme ist wiederum die Micro Liss II, die sich auf einen Contentfilter beschränkt.

Für Schrank und Schreibtisch

Ein anderes Unterscheidungsmerkmal der Appliances ist die verwendete Hardware. Das Spektrum reicht dabei vom vollwertigen



Pyramid Ben Hur II-20

Die Appliance überzeugt vor allem durch das überragende Feature-Set: Der Ben Hur II-20 deckt mit seiner Firewall, dem integrierten Mail-server sowie den File-, Print- und FTP-Diensten alle Bedürfnisse für LAN und WAN vollständig ab. Dank der gelungenen Integration der verschiedenen Dienste stellt er die ideale All-in-One-Lösung für kleinere Unternehmen dar. Das Handbuch ermöglicht auch Einsteigern die problemlose Konfiguration.



Linogate Defendo Medium

Der leistungsstarke Prozessor verleiht dem Defendo Medium von Linogate Flügel, seine hohe Rechenleistung reicht auch für größere Netzwerke mit etwa 50 Usern aus. Zu den guten Leistungen der All-in-One-Appliance gesellen sich umfangreiche Netzwerk- und Sicherheitsfunktionen. Perfekt: Die Administration mit integrierten kontextbezogenen Hilfeseiten erleichtert unerfahrenen Administratoren die Arbeit.

Empfehlungen der Redaktion

Die besten All-in-One-Appliances

- 1 Ben Hur II-20**
Pyramid 90,4
- 2 Defendo Medium**
Linogate 82,7
- 3 Intranator 2500**
Intra 2net 77,4
- 4 AGS 220**
Astaro 74,4
- 5 Sonicwall Pro 2040**
Sonicwall 72,1

PC für den Serverraum oder eine Ecke im Office über 19-Zoll-Geräte für den Schrankbau bis hin zu lüfterlosen Produkten, die sich auch auf dem Schreibtisch platzieren lassen.

Jede dieser Varianten hat ihre spezifischen Vor- und Nachteile. So kommen Ben Hur II und Micro Liss II wegen der niedrig getakteten 400- beziehungsweise 600-MHz-Celeron-Prozessoren ohne lärmenden Lüfter aus. Der Nachteil dabei: Auch die Zahl der gleichzeitig nutzbaren VPN-Sitzungen liegt niedriger, da diese recht viel Rechenleistung verschlingen. Da alle Probanden mit Ausnahme der Sonicwall Pro 2040 die Zahl der möglichen VPN-Sitzungen nicht künstlich limitieren, spielen hier die PC-basierenden Produkte Intranator 2500 und Defendo Medium den Vorteil ihrer mit 2 beziehungsweise mit 1,7 GHz getakteten CPUs aus. Die Sonicwall lässt nur zehn Verbindungen zu.

Schönheitsfehler im Detail

Egal ob nun Connectivity-Spezialist oder Dienste-Generalist: der Anspruch einer Appliance ist, dass sie die Anforderungen ihres Einsatzgebiets komplett abdeckt. Das ist jedoch nicht immer der Fall und wie so oft steckt der Teufel im Detail. So bieten alle Produkte einen integrierten DHCP-Server zur automatischen Versorgung der Rechner im LAN mit einer passenden IP-Adresse. Einen echten DNS-Server zur Namensauflösung im internen Netz gibt es jedoch nur beim Ben Hur II, beim Defendo Medium und beim Intranator 2500. Die restlichen Geräte begnügen sich damit, DNS-Anfragen an den DNS-Server des Providers oder einen vom Anwender vorgegebenen DNS-Server weiterzuleiten. Da es sich um ein reines Software-Problem handelt, ließe sich der Mangel durch ein Software-Update leicht beheben – allerdings ist das laut Hersteller nicht geplant. Anders sieht es jedoch bei Einschränkungen aus, die ihre Ursache in der Wahl der Hardware haben. So müssen die Micro Liss II und die Sonicwall Pro 2040 ohne Festplatte auskommen. Ent-

sprechend kann ihr Proxy keinen Cache zur Verfügung stellen, mit dessen Hilfe sich Web-Zugriffe beschleunigen und das anfallende Transfervolumen reduzieren lassen.

Bedingt anwenderfreundlich

Angesichts des beträchtlichen Funktionsumfangs der Appliances kommen der Dokumentation sowie dem Benutzer-Interface der Geräte besondere Bedeutung zu. Dazu gehört nicht nur, dass die Darstellung übersichtlich und idealerweise mit Erklärungen der einzelnen Optionen versehen ist. Wichtig ist vor allem, dass das System versucht, Fehlkonfigurationen des Administrators zu erkennen und zu verhindern. Entsprechende Maßnahmen bieten alle Probanden des Tests. Zusätzlich entschärfen der ASG 220, der Ben Hur II, der Defendo Medium, der Intranator 2500 und die Sonicwall Pro 2040 die Firewall-Konfiguration, indem sie bereits aus der Definition der Netzwerke passende Regeln ableiten und so dafür sorgen, dass schnell ein betriebsfähiges System zur Verfügung steht. Aus der Reihe fällt hier lediglich die Micro Liss II. Sie zwingt den Benutzer dazu, direkte Regeln zu erfassen und überfordert damit vor allem Anwender ohne langjährige Praxis. Aber auch für Experten erhöht dieses inzwischen nicht mehr zeitgemäße Verfahren die Gefahr von Fehlkonfigurationen.

Aufpreispflichtig

Ein Punkt, der bei den meisten Kandidaten zu beachten ist, sind die anfallenden Zusatzkosten. So sind sowohl Virens Scanner wie auch Content- und Spamfilter nur durch Zahlung jährlicher Gebühren erhältlich. Gleiches gilt für Updates des Betriebssystems der Geräte. Bei den verwendeten Scannern setzen die Appliance-Hersteller auf namhafte Produkte. Bevorzugt finden sich die Engines von F-Secure, Kaspersky und McAfee, bei Linogate, Pyramid und Sonicwall hat der Anwender sogar die Wahl zwischen den Systemen. Bei den Modellen ohne Festplatte ist

der Scanner im (Flash-)ROM und wird lediglich aktiviert. Die Signaturdateien sind in der Regel nicht so groß, passen also problemlos in nicht-flüchtigen Speicher.

Zusätzlich verlangt zum Beispiel Sonicwall eine Gebühr für das Freischalten des Intrusion Detection Systems, der Contentfilter für Web-Inhalte kostet zusätzlich 1134 Euro, noch einmal dieselbe Summe ist für den Virenschutz fällig. Bei Astaro sind für die Kombination aus Virenschutz und Contentfilter 1136 Euro zu veranschlagen, Spamfilter und Virentest der E-Mail kosten noch einmal 812 Euro. Pyramid verlangt für den Virenschutz auf dem Ben Hur II mindestens 1000 Euro. Lediglich der Intranator kommt bereits ab Werk mit einer für ein Jahr gültigen F-Secure-Lizenz. Dank dieser vielfältigen Aufpreis Pakete sind die Listenpreise der Produkte nicht direkt vergleichbar. Es empfiehlt sich, vor der endgültigen Entscheidung die Preislisten genau zu studieren, um Überraschungen zu vermeiden. Die in der Tabelle erfassten Preise entsprechen daher auch nicht immer den Listenpreisen der Produkte. Zusätzlich wurden die Kosten für den inzwischen verpflichtend einzusetzenden Virens Scanner zum reinen Gerätepreis addiert und auch eventuell anfallende Gebühren für ein Jahr Update-Service aufgeschlagen.

Keine für alle

Eines zeigt der Test ganz klar: Das für alle Einsatzgebiete ideale Produkt gibt es nicht. So bietet beispielsweise der Ben Hur II die größte Funktionsvielfalt, seine schwache Hardware-Ausstattung schränkt den Einsatz jedoch auf kleinere Umgebungen mit nicht mehr als 25 Anwendern ein. Die Geräte von Astaro, Intra 2net und Linogate eignen sich alle in etwa gleich gut für den Stand-alone-Einsatz zum Schutz mittlerer Umgebungen. Die Sonicwall Pro 2040 ist eher für große IT-Installationen mit zentraler Verwaltung konzipiert, da nur sie sich in Management-Systeme integrieren lässt. MBA



Alles dran, alles drin: Beim Ben Hur imponiert das Display an der Frontblende (oben), im Inneren ist ein kompletter PC verbaut (rechts)

Anschlussmöglichkeiten gibt es bei Micro Liss viele, Funktionen eher weniger



Produkte im Detail

Anwender dieser Appliances werden mit jeder Menge Netzwerkfunktionen überhäuft. Das ist Fluch und Segen zugleich: Zwar gibt es alles aus einer Hand, die Gefahr ist aber groß, dass wenig erfahrene Administratoren von der Konfiguration überfordert sind. Aber keine Panik, fast alle Kandidaten meistern diesen Spagat.

Ben Hur II-20 Pyramid

Der Ben Hur II-20 ist das Gerät, das der Bezeichnung All-in-One-Appliance am ehesten gerecht wird. Einziges Handicap: Ausgestattet mit einem 400-MHz-Prozessor eignet er sich nur für kleinere Umgebungen mit 20 bis 25 Nutzern, sonst geht die Performance besonders bei VPN-Verbindungen in die Knie. Dafür bietet der Ben Hur einen beachtlichen Leistungsumfang. An den vier Netzwerk-Interfaces lassen sich nach Belieben LAN-Segmente, Internet oder DMZ anschließen. Für Schutz sorgt eine einfach konfigurierbare Firewall mit Stateful Packet Inspection und Intrusion Detection System.

VPNs stellt Ben Hur II mit IPsec zur Verfügung. Hierbei lassen sich die Verbindungen per X.509- und RSA-Zertifikat sowie einem Preshared Secret schützen. Der integrierte Proxy-Server ist in der Lage, einen Teil der internen Festplatte als Cache-Speicher zu nutzen, das erhöht die Effizienz. Der Proxy sorgt auf Wunsch zudem für eine Anonymisierung der von den Surfern übermittelten Daten – ein wichtiges Sicherheitsfeature.

Der integrierte Mailserver unterstützt mehrere Domains. Vorhandene externe Postfächer leert er flexibel per POP3, IMAP oder SMTP. Unerwünschte Dateitypen in Mail-An-

hängen filtert Ben Hur ebenso zuverlässig wie Spam-Nachrichten. Der für 730 Euro gesondert zu lizenzierende Virens Scanner von H+B EDV prüft eingehende E-Mails. Bei aktivem Proxy-Server kann der für 1000 Euro pro Jahr erhältliche Virenschutz von Trend Micro per HTTP und FTP eintreffende Files auf Schädlinge testen.

Bei der Arbeit mit Ben Hur II fällt auf, dass das Gerät dem Anwender an vielen Stellen Arbeit abnimmt. So führt das Anlegen lokaler Netze zur automatischen Erstellung von Firewall-Regeln. Die Übergänge zwischen den einzelnen Sub-Netzen und auch dem Internet lassen sich mithilfe einer einfachen Matrix schnell zwischen Direktverbindung, NAT und kompletter Trennung des Datenverkehrs umschalten. Zusätzliche Firewall-Regeln muss der Administrator nicht an zentraler Stelle erfassen: Dies ist direkt bei den betroffenen Netzdefinitionen möglich. Demgegenüber stehen aber auch logische Brüche. Einige Optionen erwarten, dass an einer gänzlich anderen Stelle bereits Vorarbeit geleistet wurde. So ist zum Beispiel zur Definition von Abholintervallen des Mailsammlers vorab mindestens ein so genannter Zeitabschnitt in den Benutzungsrichtlinien anzulegen. Das ist nicht immer nachvollziehbar. Das Handbuch hilft hier aber ebenso gut weiter wie die integrierte Online-Hilfe.

Ben Hur II besticht nicht nur durch extreme Funktionsvielfalt, sondern auch durch die gelungene Integration der einzelnen Dienste. Allerdings hat diese Vielfalt auch ihren Preis. Die Kosten der sinnvollen Optionen wie Virens Scanner und Update-Service übersteigen den günstigen Grundpreis von 1300

Euro deutlich. In der Summe kommt ein vollständig ausgestatteter Ben Hur II somit auf etwas über 3600 Euro. Das ist angesichts des Funktionsumfangs im Vergleich zu den restlichen Kandidaten immer noch günstig.

sehr gut, 90,4 Punkte 1

Defendo Medium Linogate

Der PC-basierte Defendo Medium von Linogate ist für Netzwerke mit bis zu 50 Anwendern konzipiert. Zur Anbindung an lokale Netze und ans Internet dienen zwei LAN-Ports, wobei die WAN-Schnittstelle auch als DMZ konfigurierbar ist. Zusätzlich bietet der Defendo eine ISDN-Karte.

Über virtuelle Interfaces, die der Anwender frei definieren kann, verwaltet der Defendo Medium auch mehrere Sub-Netze. Die Firewall des Defendo arbeitet mit Stateful Packet Inspection und besitzt ein Intrusion Detection System. Port-Weiterleitungen sind ebenso einfach möglich wie der Aufbau einer demilitarisierten Zone. Zudem kann die Firewall aktive Web-Inhalte filtern.

Als Netzwerk-Dienst bietet der Defendo einen DHCP- sowie einen vollwertigen DNS-Server. Zur sicheren Verbindung von Rechnern oder Netzen über das Internet unterstützt die Linogate-Appliance virtuelle private Netze nach IPsec. Dabei können X.509-Zertifikate oder ein Preshared Secret zum Einsatz kommen, RSA-Zertifikate werden nicht unterstützt. Gut: Die Anzahl der gleichzeitig möglichen Sitzungen ist nicht limitiert, dank der mit 1,7 GHz arbeitenden CPU deckt das Gerät die Ansprüche der Zielgruppe (50 Clients) mit Leichtigkeit ab.



»Die zentrale Bereitstellung von Standard-Netzwerkfunktionen erleichtert die Arbeit enorm.«

MARKUS BAUER, LEITENDER REDAKTEUR HARDWARE

Der Proxy-Server des Defendo erlaubt das Kanalisieren des Datenverkehrs ins Internet und bietet neben der Arbeitsweise ohne Authentifizierung auch einen Modus mit erzwingender Benutzeranmeldung – ein wichtiges Sicherheitsfeature. Der optional aktivierbare Proxy-Cache sorgt für reduziertes Transfervolumen und schnellere Antwortzeiten. Schutz vor Viren bietet der für 580 Euro zu lizenzierende Virens Scanner von F-Secure oder Kaspersky. Dieser prüft sowohl über den Proxy eingehende Daten wie auch Mail-Anhänge auf potenzielle Gefahren.

Der integrierte Mailserver ist in der Lage, mehrere Domains zu bedienen. In externen Postfächern lagernde Mails holt er per POP3 und SMTP ab und verteilt sie lokal. Zum Aus-sortieren unerwünschter Werbe-Mails dient ein regelbasierter Spam-Filter. Zusätzlich stellt der Defendo einen integrierten Webserver zur Verfügung. Dessen Inhalte lassen sich per FTP, Windows-Freigabe oder auf Wunsch sogar per Telnet verwalten.

Das Management des Defendo erfolgt über ein per HTTPS erreichbares Web-Interface. Die Benutzerführung ist übersichtlich, zu jeder Eingabemaske wird eine eigene, kontextbezogene Hilfeseite angeboten. Besonders für Einsteiger hilfreich ist die Aufteilung in Administrations- und Konfigurationsaufgaben, Profis hingegen steht über das Expertenmenü der Zugriff auf die direkten Parameter zur Verfügung. Dieses System erleichtert schon nach kurzer Arbeit mit der Appliance die Verwaltung spürbar.

Der Defendo Medium wird den Ansprüchen der Zielgruppe in mittleren Netzen gut gerecht. Für 2990 Euro erhält der Anwender eine Appliance mit guten Netzwerkeigenschaften, umfangreichen Sicherheitsfunktionen und befriedigender Bedienung.

gut, 82,7 Punkte 

Intranator 2500 Intra 2net

Der Intranator 2500 bietet in seinem PC-Gehäuse neben den drei Netzwerk-Anschlüssen eine integrierte ISDN-Karte. Über die sind Fax-Versand und Empfang, ein- und ausgehende Remote-Access-Verbindungen sowie – nach Freischaltung durch den Anwender – die Fernverwaltung möglich. Ein Display an der Front liefert übersichtlich Statusinformationen. Ausgestattet mit einer regelbasierten Firewall und Stateful Packet Inspection bietet der Intranator alle Standardfunktio-

nen wie NAT, Port-Forwarding und DMZ. Schlechter sieht es beim Schutz vor aktiven Web-Inhalten aus. Diese filtert der Intranator ebenso wenig wie Cookies oder den Zugriff auf externe Proxy-Server.

Ein vollwertiger DNS-Server sorgt dafür, dass Clients sowohl über ihre IP-Adresse wie auch über Hostnamen ansprechbar sind. Praktisch: Dabei erfolgt ein automatischer Eintrag für Clients, die ihre IP-Adresse vom integrierten DHCP-Server beziehen. Zusätzlich ist ein Multi-Domain-fähiger Mailserver integriert. Er kann mehrere externe Accounts abfragen und die empfangenen Nachrichten auf die lokalen Postfächer verteilen. Virtuelle private Netze baut der Intranator ausschließlich per IPsec auf, zur Verschlüsselung kommen X.509-Zertifikate oder ein Preshared Secret zum Einsatz, RSA-Zertifikate sind nicht einsetzbar. Dank schneller CPU (2 GHz) und unbegrenzter Zahl gleichzeitig möglicher Sitzungen sind dutzende paralleler VPN-Verbindungen ohne Performance-Verlust möglich. Der interne Proxy-Server des Intranator arbeitet wahlweise als transparenter Proxy oder als Proxy mit Authentifizierung und bietet das Caching von Web-Inhalten.

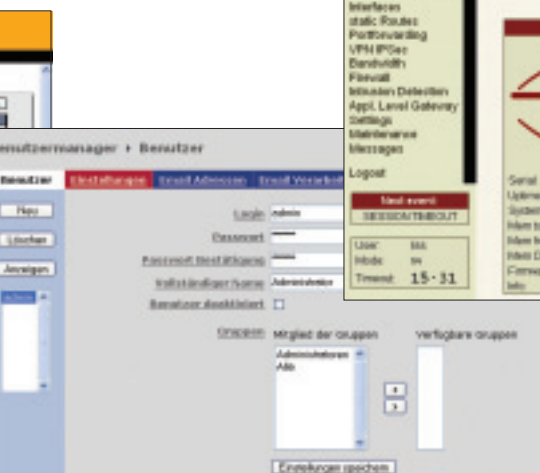
Sehr praktisch: Das Web-Interface zur Konfiguration schützt vor fehlerhaften Einstellungen. In einer Warteschlange werden die Eingaben des Administrators zwischengespeichert und erst freigegeben, wenn die resultierende Konfiguration ein arbeitsfähiges Ergebnis liefert. Zusätzlich prüft Intranator 2500 bei jeder Eingabe, ob geänderte oder neu eingetragene Werte mit bestehenden Einstellungen kollidieren. Bei absichtlich provozierten Fehleinstellungen im Test funktioniert dieses Feature einwandfrei.

Allerdings ist auch das Web-Interface des Intranator nicht frei von Mängeln. So könnte speziell die Benutzerführung besser sein. Multiple Menü-Ebenen mit identischen Funktionen erschweren dem Benutzer die Übersicht, eine zur aktuellen Maske passende Hilfe gibt es auch nicht.

Eine Besonderheit des Intranator ist sein Komplettpreis. Weder für Virenschutz noch für Contentfilter sind zusätzliche Kosten zu kalkulieren. Damit bietet das Gerät das beste Preis-Leistungs-Verhältnis im Testfeld. Die Leistung der 2-GHz-Celeron-CPU reicht auch für eine große Zahl von VPN-Sitzungen, der Hauptspeicherausbau ist mit 256 MByte ausreichend. Dank dieser Leistung eignet sich der Intranator 2500 für den Einsatz in Um-



Sicherheit im Griff: Bei Defendo tut sich der Administrator mit der Konfiguration der Firewall leicht



Das Web-Interface von Intranator schützt sogar vor fehlerhaften Eingaben



Ein Schwachpunkt bei der Micro Liss: das komplizierte Management

gebungen mit bis zu 150 Nutzern. Hier stellt er im Testfeld zusammen mit dem Defendo Medium die ausgewogenste Lösung dar.

befriedigend, 77,4 Punkte 3

ASG 220 Astaro

Der ASG 220 von Astaro bietet mit acht LAN-Ports im 19-Zoll-Gehäuse die meisten physikalischen Anschlüsse im Testfeld. Ein Display an der Frontseite gibt Informationen über den Systemstatus, mehrere Folientasten erlauben den Abruf von Basisfunktionen wie zum Beispiel *Neustart* oder *Rücksetzen in den Auslieferungszustand*. Der bevorzugte Administrationsweg ist der über einen Web-Browser. Hier überrascht der ASG 220 mit einer positiven Eigenheit: Statt eines Standard-Passworts muss der Anwender beim ersten Start die Kennworte für Web-Interface sowie Benutzer- und Admin-Zugang zur Kommandozeile selbst vergeben – ein Sicherheitsrisiko weniger!

Die Benutzerschnittstelle ist sehr übersichtlich gegliedert. Die einzelnen Funktionen sind gut erreichbar, die stets verfügbare kontextsensitive Hilfe erleichtert das Setup. Einziges Manko: Der ASG 220 zwingt den Anwender zu einem Firewall-Setup in mehreren Schritten, da sich zum Beispiel Port-Forwarder nur über zuvor angelegte Dienste, nicht aber direkt über die verwendete Portnummer definieren lassen.

Die Funktionen der Firewall sind komplett. Allerdings muss der Anwender alle Definitionen selbst vornehmen. Eine automatische Regel-Erstellung anhand der definierten Sub-Netze bietet der ASG 220 nicht. Auch eine DMZ ist von Hand anzulegen. Die vorgenommenen Änderungen übernimmt der ASG 220 sofort. Eine Konfigurationswarteschlange oder die Prüfung der Settings auf logische Fehler ist nicht vorgesehen.

Der integrierte Proxy mit Cache-Funktion kann sowohl für HTTP- als auch für FTP- und DNS-Anfragen verwendet werden. Darüber hinaus ist er in der Lage, als Mail-Relay zu arbeiten. In dieser Funktion unterstützt

er den gesondert zu lizenzierenden Virens Scanner für E-Mails und Attachments sowie den Spamfilter. Beide lassen sich nur in Verbindung mit dem Proxy einsetzen und erhöhen im Bundle den Preis um 812 Euro – eine sehr sinnvolle Erweiterung.

An Zusatzdiensten bietet der ASG 220 einen vollwertigen DHCP-Server, dem allerdings nur ein DNS-Relay zur Seite steht. Für Namensauflösung im internen Netz muss also ein zusätzlicher vollwertiger DNS-Server eingesetzt werden. VPN-Verbindungen zum ASG 220 lassen sich per IPsec und L2TP aufbauen, letzteres wird über IPsec getunnelt. Eine künstliche Begrenzung der gleichzeitigen Verbindungen gibt es nicht, die mit 1,2 GHz getaktete Pentium-III-CPU bietet zusammen mit 512 MByte Hauptspeicher genügend Reserven, um auch gehobene VPN-Ansprüche zu befriedigen.

Ausstattung und Funktionsumfang positionieren den ASG 220 im Umfeld mittlerer bis größerer Netze. Hier leisten allerdings die Produkte von Intra 2net und Linogate Vergleichbares für weniger Geld. Mit allen sinnvollen Optionen wie Virens Scanner und Update-Server versehen kostet der ASG 220 mit fast 4700 Euro sogar mehr als die Sonicwall Pro 2040, ohne deren Integrationsfähigkeit aufzuweisen.

befriedigend, 74,4 Punkte 4

Sonicwall Pro 2040 Sonicwall

Bei der Sonicwall Pro 2040 im 19-Zoll-Gehäuse stellen drei Netzwerk-Ports die Anbindung an LAN, Internet und andere Netze her, eine weitere Schnittstelle lässt sich gegen Aufpreis freischalten. Den Schutz der lokalen Rechner übernimmt eine Firewall mit Stateful Packet Inspection, die mit einem Intrusion Detection System aufrüstbar ist. Die restlichen Firewall-Funktionen wie NAT, Port-Weiterleitung oder DMZ sind vollständig vorhanden. Für Letztere ist der optionale Port vorgesehen. Zusätzliche Sicherheit bieten Filter für aktive Inhalte wie ActiveX und Javascript sowie für Cookies und gefälschte

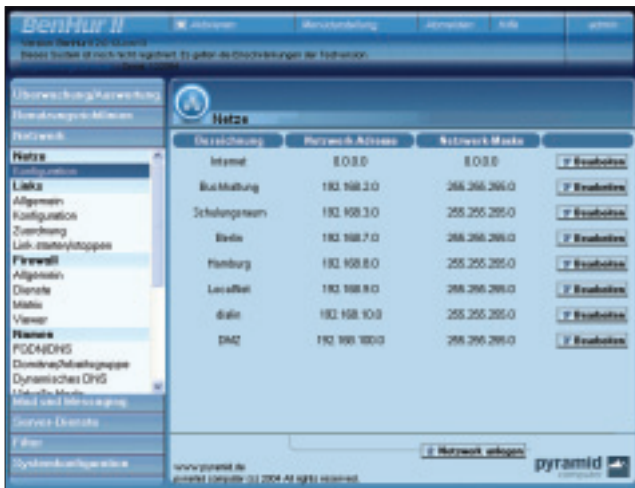
Zertifikate. Einen Proxy bietet das Sonicwall-Produkt nicht. Dafür ist es in der Lage, einen bereits vorhandenen Proxy-Server für die Nutzer transparent einzubinden.

Dem integrierten DHCP-Server steht ein reines DNS-Relay zur Seite, das auf einen DNS-Server im LAN oder beim Provider weiterleitet. Um externe Zweigstellen oder Anwender sicher ans lokale Netz anzubinden, setzt Sonicwall auf VPN-Verbindungen per IPsec. Allerdings sind diese in der Grundversion auf maximal 10 gleichzeitige Sitzungen begrenzt, weitere Lizenzen lassen sich nachkaufen. Zur Verschlüsselung der VPN-Daten stehen X.509-Zertifikate und Pre-shared Secrets zur Wahl.

Einen Mailserver bietet die Sonicwall Pro 2040 nicht. Sie ist aber in der Lage, durchlaufenden Mail-Verkehr auf Viren zu untersuchen und auch unerwünschte Datei-Anhänge filtert die Appliance aus. Für den Virens Scanner ist ebenfalls eine gesonderte Lizenz notwendig (1134 Euro). Gleiches gilt für das Aufrüsten der Standard-Edition des Betriebssystems auf die Enhanced-Version. Für die 800 Euro Aufpreis erhält man dann die Möglichkeit, auch drahtlose Netze mithilfe spezieller Access-Points zu verwalten sowie in das Netzwerk-Management der Sonicwall zu integrieren.

Gerade die vielfältigen Schnittstellen zu externen Servern und Diensten sowie die über Firmware-Upgrades und Aktivierungsschlüssel freischaltbaren Optionen erschweren das Setup der Sonicwall Pro 2040. Gelegentlich gibt das Interface verwirrende Statusmeldungen oder meldet die Nicht-Verfügbarkeit einer Option aufgrund fehlender Lizenzen erst bei dem Versuch, die Einstellungen abzurufen. Mehr als einmal laufen die Tester deshalb in eine Konfigurations-Sackgasse. Die gewünschte Funktion wird zwar angezeigt, ist aber nicht verfügbar.

In puncto Feature-Liste bietet die Sonicwall Pro 2040 eher wenig für einen vergleichsweise hohen Preis. Ihre Stärke liegt jedoch nicht im Funktionsumfang, sondern in der Integration in bestehende Netzstruk-



Die übersichtliche Konfiguration ist nur eine der vielen Stärken der Ben-Hur-II-Appliance

turen. Hier kann die Sonicwall ihr Potenzial ausspielen und die bereits existierenden Dienste optimal versorgen – vorausgesetzt, der Nutzer kämpft sich durch die Konfiguration.

befriedigend, 72,1 Punkte 5

Micro Liss II FL Telcotech

Die Micro Liss II bietet drei frei konfigurierbare Netzwerk-Schnittstellen zur Anbindung an lokale Netze, das Internet oder eine demilitarisierte Zone. Über virtuelle Netzwerk-Interfaces kann die Appliance auch mehrere Sub-Netze adressieren.

Ein Intrusion Detection System erkennt Angriffe auf das lokale Netz, wehrt diese ab und informiert auf Wunsch per E-Mail über aufgetretene Vorfälle. Potenziell gefährliche Web-Inhalte wie ActiveX- oder Javascripts filtert das Gerät nicht, Gleiches gilt für Cookies. Die restlichen Firewall-Funktionen wie Port-Weiterleitung, DMZ oder NAT sind vollzählig vorhanden.

VPNs unterstützt die Micro Liss II via IPsec. Die Zahl der gleichzeitig möglichen Sitzungen ist nicht beschränkt, die mit 600 MHz getaktete CPU setzt erfahrungsgemäß eine natürliche Grenze bei etwa 10 Sitzungen. Zum Aufbau einer VPN-Verbindung können X.509- und RSA-Zertifikate sowie Preshared Secrets dienen.

Ein integrierter Proxy sorgt für kontrollierten Zugriff der Anwender auf HTTP- und FTP-Dienste. Zusätzlich kann der Proxy von den Anwendern eine Authentifizierung verlangen. Mangels interner Festplatte stellt der Proxy keinen Cache zur Verfügung. Ein DHCP-Server sorgt für die Adressvergabe an Clients, ein vollwertiger DNS-Server ist für die Auflösung von Rechnernamen in IP-Adressen zuständig. Datenabgleich zwischen beiden findet jedoch nicht statt. Einen Mailserver bietet das Gerät nicht, Virenschutz gibt es auch optional nicht.

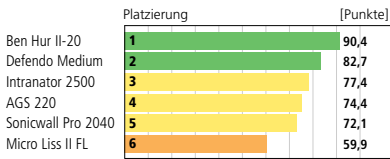
Aus der Steinzeit der Benutzerschnittstellen stammt die Verwaltungsoberfläche. Automatismen suchen die Tester hier ebenso vergebens wie komfortable Assistenten. Im Gegenteil, die Micro Liss II bietet Hardcore pur: Die Firewall wird nicht wirklich konfiguriert. Der Vorgang ähnelt eher einer Programmierung in der Iptables-Syntax. Das überfordert nicht nur Einsteiger, es erhöht aufgrund der Unübersichtlichkeit auch die Gefahr von Fehlern beim Firewall-Setup. Bei den Settings des Intrusion Detection Systems streichen auch Profis schnell die Segel.

Die 1550 Euro teure Micro Liss II bietet im Vergleich zu den anderen Produkten den geringsten Leistungsumfang. Dafür besitzt sie als einziges Gerät im Test eine integrierte Intrusion Detection. Diese Tatsache in Verbindung mit den flexiblen Routing-Funktionen würde das Produkt zum Einsatz in kleineren Netzen geeignet erscheinen lassen – wären da nicht die anspruchsvolle Konfiguration und der fehlende Virenschutz.

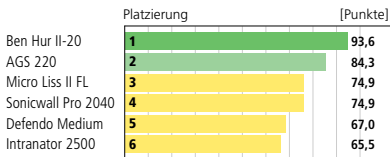
ausreichend, 59,9 Punkte 6

Wertungen

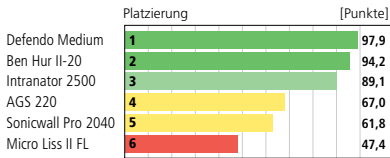
Gesamtwert 100 %



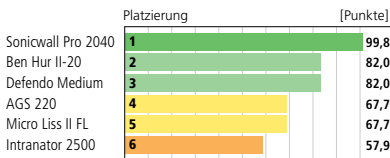
Bedienung 30 %



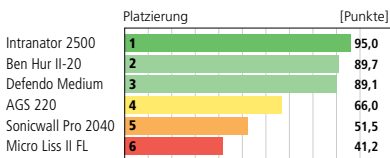
Netzwerkfunktion 20 %



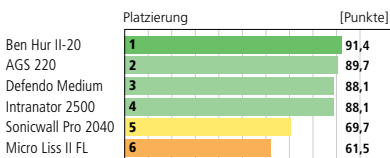
Sicherheitsfunktion 20 %



Ausstattung 20 %



Service 10 %



Aus dem Testlabor

Die getesteten Appliances unterscheiden sich in Leistungsumfang und in der Umsetzung einzelner Funktionen zum Teil stark voneinander. Um den verschiedenen Voraussetzungen gerecht zu werden, werden für den Test zwei unterschiedliche Szenarien simuliert: zum einen die Arbeit der Appliance als Gateway ins Internet, das mehrere Subnetze mit privaten IP-Adressen verwaltet. Zum anderen wird überprüft, wie sich die Appliance als Abteilungs-Gateway schlägt, das ein Subnetz innerhalb eines privaten Adressraums schützt und zur Kommunikation mit Gegenstellen im Internet einen weiteren Router anspricht.

Dabei kontrollieren die PC-Professionell-Tester als Erstes, ob die wichtigsten Funktionen vorhanden sind. Dazu zählen etwa die Network Address Translation oder die Möglichkeit, per Port-Forwarding Server im LAN aus dem Internet heraus erreichbar zu machen. In einen eigenen Teil der Bewertung fließt außerdem mit ein, wie leicht sich die für die verschiedenen Szenarien notwendigen Konfigurationseinstellungen vornehmen lassen und wie gut die integrierte Verwaltung den Anwender dabei unterstützt. Dazu gehört auch die Frage, welche Mechanismen eingesetzt werden, um Konfigurationsfehler zu vermeiden. Als einziges Gerät im Test übernimmt die Appliance von Astaro Änderungen an den Einstellungen sofort. Die anderen Produkte speichern geänderte Settings zunächst in einem eigenen Puffer. Bevor die Änderungen als Betriebseinstellung übernommen werden, überprüfen sie entweder selbstständig, ob sich beispielsweise logische Fehler eingeschlichen haben, oder geben dem Anwender zumindest Gelegen-

heit, die Einstellungen selbst noch einmal zu kontrollieren und eventuell zu verwerfen.

Ein besonderes Augenmerk wird im PC-Professionell-Test auf die vielen integrierten Sonderfunktionen gelegt, die sich auf den meisten Geräten finden. Die Tester prüfen hierbei speziell, ob ein Feature vollständig und sinnvoll umgesetzt wurde. So ist es beispielsweise nicht zweckmäßig, IP-Adressen per DHCP zu vergeben, aber die so ins Netz integrierten Clients nicht zugleich automatisch in die Hostliste eines ebenfalls vorhandenen DNS-Servers zu übernehmen. Die Produkte von Astaro, Sonicwall und Telco Tech kommen gar nicht erst in die Verlegenheit, sich diesen Schnitzer zu leisten, da sie statt eines vollwertigen DNS-Servers lediglich einen DNS-Relay bieten.

Proxy als Sicherheitsfunktion?

Sofern sie bei den Appliances vorhanden sind, werden auch integrierte Proxy-Server einem Test unterzogen. Hierbei kommt es vor allem darauf an, welche zusätzlichen Funktionen mit Hilfe des Proxys realisiert sind. Alle Kandidaten des PCpro-Tests benötigen den Einsatz des Proxys, um den Download bestimmter Dateitypen zu verhindern. Bei den Appliances ASG 220, Ben Hur II, Intranator 2500 und Defendo Medium arbeitet der Proxy zudem auf Wunsch als Cache und senkt so die zwischen Internet und LAN übertragene Datenmenge. Die Effektivität dieser Funktion ist bei allen genannten Geräten in etwa gleich, da sie ausnahmslos Squid als Proxy-Cache verwenden. Die Sonicwall Pro 2040 und die Micro Liss II dagegen bieten dieses Feature mangels einer integrierter Festplatte nicht an. *Stefan Rubner/MBA*

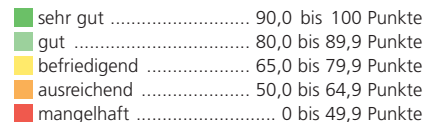
Bedienung (30 %) Inbetriebnahme, Management-Funktionen, Management-Oberflächen, Sicherheitsfunktionen für das Management

Netzwerkfunktion (20 %) Routing-Möglichkeiten, DHCP-, DNS-Server, Sub-Netze, IP-Verwaltung

Sicherheitsfunktion (20 %) Firewall-Betriebsarten und -Funktionen, integrierter oder optionaler Virenschutz, Spam-Mail-Schutz, Contentfilter

Ausstattung (20 %) Hardware-Ausstattung, Festplatte, Schnittstellen, Display

Service (10 %) Garantiezeit, Hotlinekosten, Verfügbarkeit der Hotline



Besser in den Serverraum: Die vielen Lüfter sorgen bei den 1HE-Geräten für eine laute Geräuschkulisse



Produkt	Ben Hur II-20		Defendo Medium		Intranator 2500		AGS 220		Sonicwall Pro 2040		Micro Liss II FL		
Hersteller	Pyramid		Linogate		Intra 2net		Astaro		Sonicwall		Telcotech		
Internet	www.pyramid.de		www.linogate.de		www.Intra 2net.de		www.astaro.de		www.sonicwall.de		www.telcotech.de		
Preis	3260 Euro		2992 Euro		2760 Euro		4680 Euro		4323 Euro		1550 Euro		
Gesamturteil	Punkte	sehr gut 90,4		gut 82,7		befriedigend 77,4		befriedigend 74,4		befriedigend 72,1		ausreichend 59,9	
Bedienung (30%)	Punkte	sehr gut 93,6		befriedigend 67,0		befriedigend 65,5		gut 84,3		befriedigend 74,9		befriedigend 74,9	
Netzwerkfunktion (20%)	Punkte	sehr gut 94,2		sehr gut 97,9		gut 89,1		befriedigend 67,0		ausreichend 61,8		mangelhaft 47,4	
Sicherheitsfunktion (20%)	Punkte	gut 82,0		gut 82,0		ausreichend 57,9		befriedigend 67,7		sehr gut 99,8		befriedigend 67,7	
Ausstattung (20%)	Punkte	gut 89,7		gut 89,1		sehr gut 95,0		befriedigend 66,0		ausreichend 51,5		mangelhaft 41,2	
Service (10%)	Punkte	sehr gut 91,4		gut 88,1		gut 88,1		gut 89,7		befriedigend 69,7		ausreichend 61,5	
Fazit	<p>Der Ben Hur II von Pyramid strotzt nur so vor sinnvollen Funktionen und Features. Und das Beste daran: Die zahlreichen Netzwerk- und Sicherheitsfeatures lassen sich sehr leicht administrieren.</p> <p>Eine robuste Security-Appliance für Netze mit bis zu 50 Anwendern ist der Defendo Medium. Hier bietet er zu einem recht günstigen Preis alle notwendigen Features, gepaart mit ordentlicher Bedienbarkeit.</p> <p>Der Intranator 2500 bietet alle notwendigen Funktionen zum Schutz eines mittleren Netzes. Alle sinnvollen Optionen sind im Basispreis enthalten. Einziges Manko ist die fehlende SNMP-Unterstützung.</p> <p>Eine übersichtliche Benutzeroberfläche vereint das Astaro Security Gateway 220 mit sinnvollen Funktionen. Die Ausstattung mit allen wichtigen Optionen hat allerdings einen relativ hohen Preis.</p> <p>Vor allem in zentral verwalteten Netzen spielt die Sonicwall 2040 ihre Stärken aus. Sie bietet aber auch als Stand-alone-Gerät befriedigende Funktionen.</p> <p>Die Micro Liss II hat ihre besten Jahre bereits hinter sich. Weder beim Bedienkomfort noch beim gebotenen Funktionsumfang kann sie mit den aktuellen Produkten der Konkurrenz mithalten.</p>												
Router													
Dynamische Routen	ja		ja		ja		ja		ja		ja		
Virtuelle Interfaces	ja		ja		nein		ja		ja		ja		
Externer Default Gateway	ja		ja		ja		ja		ja		ja		
Fail-over	nein		ja		ja		ja		ja		optional		
Firewall													
Intrusion Detection	ja		ja		nein		nein		ja		ja		
E-Mail-Notification	nein		ja		nein		ja		ja		ja		
SMS-Notification	nein		nein		nein		nein		nein		nein		
SNMP-Notification	ja		nein		nein		ja		ja		nein		
dynamisches NAT	ja		ja		ja		ja		ja		ja		
Statisches NAT	ja		ja		nein		ja		ja		ja		
Port-Weiterleitung	ja		ja		ja		ja		ja		ja		
Contentfilter	manuell, Cobion, Dansguardian		manuell		manuell, Dansguardian		manuell, Cobion		Sonicwall ¹⁾ , N2H2, Websense		Cobion		
ActiveX-Blocker	nein		ja		nein		nein		ja		nein		
Java-Blocker	nein		ja		nein		nein		ja		nein		
Cookie-Blocker	nein		nein		nein		nein		ja		nein		
Proxy-Blocker	nein		nein		nein		nein		ja		nein		
Zertifikat-Blocker	nein		nein		nein		nein		ja		nein		
Virens Scanner	ja ¹⁾		ja ¹⁾		ja ⁴⁾		ja ¹⁾		ja ¹⁾		nein		
Sonderfunktionen													
DHCP-Server	ja		ja		ja		ja		ja		ja		
Echter DNS-Server	ja		ja		ja		nein		nein		nein		
Bandwidth-Management	ja		nein		ja		ja		ja		ja		
VPN	IPsec		IPsec, L2TP		IPsec		IPsec, L2TP		IPsec		IPsec		
Preshared Key	ja		ja		ja		ja		ja		ja		
RSA	ja		nein		ja		ja		nein		ja		
X.509-Zertifikat	ja		ja		ja		ja		ja		ja		
Proxy-Server	ja		ja		ja		ja		nein ³⁾		ja		
Proxy-Cache	ja		ja		ja		ja		nein		nein		
Anonymizer	ja		nein		nein		ja		nein		nein		
Web-Server	ja		ja		nein		nein		nein		nein		
File-Server	SMB, NFS, Appletalk		nein ²⁾		nein		nein		nein		nein		
Windows PDC	ja		nein		nein		nein		nein		nein		
FTP-Server	ja		nein ²⁾		nein		nein		nein		nein		
Datenbank-Server	MySQL		nein		nein		nein		nein		nein		
Instant-Messaging-Server	Jabber		nein		nein		nein		nein		nein		
Fax-Server	ja		nein		ja		nein		nein		nein		
SMS-Server	ja		nein		nein		nein		nein		nein		
Zeit-Server	ja		ja		nein		nein		ja		nein		
Verwaltung													
HTTP/HTTPS	nein/ja		ja/ja		ja/ja		nein/ja		ja/ja		nein/ja		
Telnet/SSH	nein/ja		ja/nein		nein/ja		nein/ja		nein/nein		nein/nein		
SNMP	ja		nein		nein		ja		ja		nein		
Group-Policies	ja		ja		ja		nein		ja		ja		
Mail-Server													
Multi-Domain	ja		ja		ja		nein		nein		nein		
POP3	ja		ja		ja		nein		nein		nein		
IMAP	ja		ja		ja		nein		nein		nein		
Mailsammler	ja		ja		ja		nein		nein		nein		
per POP/IMAP/SMTP	ja/ja/ja		ja/nein/ja		ja/nein/ja		nein/nein/nein		nein/nein/nein		nein/nein/nein		
Service													
Garantie	24 Monate		24 Monate		24 Monate		24 Monate		24 Monate		24 Monate		
Hotline	(07 61) 451 40		(08 21) 259 60		(070 71) 56 51 00		(07 21) 490 06 90		(089) 244 45 20 30		(033 28) 43 08 10		

¹⁾gesonderte Lizenz erforderlich ²⁾spezielle Freigaben zur Verwaltung des Web-Server vorhanden ³⁾externer Proxy-Server wird mit automatischer Weiterleitung unterstützt (HTTP)

⁴⁾Lizenz für 12 Monate im Preis enthalten