



Internet-Access-Appliances

Internet-Zugang mit Mehrwert

Internet-Appliances realisieren den Anschluss des LAN ans Internet und eigenen sich oft noch als File- und Printserver. In den Real-World Labs mussten vier Geräte zeigen, ob sie auch in puncto Sicherheit und Fernwartung zu empfehlen sind.

Internet-Access-Appliances stehen für einfachen und schnell zu realisierenden Zugang zum Internet. Der Anwender benötigt keine Kenntnisse über das Betriebssystem oder die Anwendungssoftware. Das Datenblatt des Internet-Providers und das Handbuch der Appliance müssen ausreichen, um das Gerät zu konfigurieren.

Zielgruppe der Appliances sind SOHO-Netze und unabhängige Arbeitsgruppen bis etwa 50 Clients. Uns interessiert aber, ob sich die Geräte auch in Filialen als Ersatz für PC-Server eignen. Network Computing hat vier, teilweise recht unterschiedliche Appliances unter dem Gesichtspunkt Standortvernetzung getestet. Alle haben gemeinsam, dass sie das lokale Netzwerk mit dem Internet verbinden. Celestix's »Aries« und die »Cube3« von Cobalt agieren mit DSL-Modems. Intels »InBusiness Small Office Network« und der »Defendo« von Linogate sind für den Anschluss an den S₀-Bus und/oder für externe Analog-Modems respektive ISDN-Terminaladapter ausgelegt.

Das können sie alle

Die Clients im lokalen Netzwerk müssen TCP/IP unterstützen, wenn sie auf die Appliance zugreifen wollen. Die IP-Adressen der Clients sind entweder statisch oder die Appliance verteilt die Adressen über das Dynamic-Host-Configuration-Protocol (DHCP). Der Administrator legt dazu einen bestimmten Satz IP-Adressen aus dem privaten Bereich für die Benutzung von Clients fest. Solche Adressen sind nicht für das Internet bestimmt. Daher muss die Internet-Access-Appliance einen Mechanismus vorsehen, mit dem Clients mit einer privaten IP-Adresse Daten ins Internet senden und von dort empfangen können. Dies wird über Network-Address-Translation (NAT), auch IP-Masquerading genannt, erreicht. Die Internet-Appliance merkt sich die IP-Adresse des Clients, ersetzt die IP-Adresse durch seine offizielle IP-Adresse und leitet die Anfrage an den Rechner im Internet weiter. Dessen Antwort durchläuft diesen Prozess dann in umgekehrter Reihenfolge, so dass die Appliance die angeforderten Daten zustellen kann. NAT ist eine Minimal-Firewall, da ein Internet-Host keine Clients im lokalen Netz (mit den privaten IP-Adressen) direkt kontaktieren kann. Neben dem eigentlichen Datenübertragungsprotokoll ist NAT die wichtigste Funktion, die eine Internet-Access-Appliance enthält.

Der Fernzugriff (Remote-Access-Service, RAS) ist eine elementare Funktion, die alle Testkandidaten aufweisen. Der Kontakt erfolgt über ein Modem oder ISDN. Immer mehr Her-



steller setzen zudem auf eine verschlüsselte HTTP-Verbindung (HTTPS). Appliances auf Linux-Basis unterstützen auch Telnet. Beim Login mit Telnet geht das Passwort allerdings im Klartext über die Leitung, weshalb es sich nicht für administrative Tätigkeiten eignet.

Das sollte drin sein

Die Appliance sollte eine Backup-Funktion enthalten, über die der Administrator das Gerät auf die Werkseinstellungen zurücksetzt. Das Experimentieren mit mehreren Einstellungen sollte ebenfalls möglich sein.

Appliances für ISDN müssen dynamische Kanalbündelung unterstützen. Diese soll aber auch deaktivierbar sein. Zudem sollte eine ISDN-Appliance diverse Kompressionsverfahren beherrschen. Damit die Rechnung des Internet-Providers nicht zu hoch ausfällt, muss die Appliance Zugangsbeschränkungen erlauben. Viele Firmen benötigen zum Beispiel keinen Zugriff auf das WWW, sondern geben sich mit dem

Austausch von elektronischer Post zufrieden. Idealerweise lässt sich die Appliance individuell für jeden Anwender konfigurieren. Gerade bei Wählverbindungen ist es wünschenswert, dass sich die Appliance nach einer bestimmten Zeit der Inaktivität vom Internet trennt. Um die Verbindungsgebühren niedrig zu halten, sollte außerdem eine Anpassung an den Gebührentakt des Providers möglich sein. Ein eingebauter Least-Cost-Router senkt die Gebühren noch weiter.

Ressourcen gemeinsam nutzen

Internet-Access-Appliances kann man grob in zwei Anwendungsgebiete einteilen. Die einen offerieren über den Anschluss des lokalen Netzes ans Internet keine weiteren Dienste. Die anderen enthalten zusätzlich zum Beispiel einen Mail-Server. Darüber hinaus enthalten solche Appliances weitere Internet-Dienste wie DNS, FTP oder HTTP. Der Trend geht außerdem dahin, neben Internet-Diensten auch Intranet-Dienste wie Datei- und Drucker-Sharing für verschiedene Protokolle zu integrieren. So können neben Windows-Clients auch Apple- und Linux-/Unix-Workstations an der gemeinsamen Nutzung von Ressourcen teil haben.

Enthält die Appliance einen Mail-Server, muss sie auch einen Virens Scanner integrieren. Fehlt diese Funktion, muss der Virenwächter auf allen Clients installiert sein, was den Administrationsaufwand gewaltig erhöht. Wer auf dem Gerät eine Datensicherung machen möchte, benötigt ebenfalls entsprechende Software auf der Appliance. Zumindest muss sie eine Schnittstelle für den Anschluss eines Backup-Laufwerks aufweisen. Dies ist idealerweise eine externe SCSI-Schnittstelle. Datensicherungsgeräte können aber auch an der parallelen oder einer der USB-Schnittstellen angebracht werden. Das Problem ist eher die Software: Enthält die Appliance kein Backup-Programm, muss es von einem Client oder einem anderen Server aus gestartet werden.

In der Regel sind die Appliances mit einer Paketfilter-Firewall ausgestattet. Diese entscheiden auf Grund der vom Administrator vorgegebenen Richtlinien, ob ein Paket ins Internet beziehungsweise vom Internet ins lokale Netz darf. Die Konfiguration eines Paketfilters ist nicht so einfach und hier wird bereits ein in Sicherheitsfragen erfahrener Administrator benötigt. Man kann sogar so weit gehen und sagen: Alles, was sich nicht innerhalb

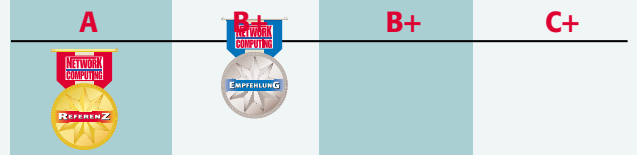
Report-Card /interaktiv unter www.networkcomputing.de

Internet-Access-Appliances

Feature	Gewichtung	Linogate Defendo	Celestix Aries	Cobalt Cube3	Intel InBusiness
Funktionsvielfalt	30%	4,5	4	4	2
Bedienung	20%	4,5	4	5	4,5
Dokumentation	20%	5	4,5	2,5	4
Preis/Leistung	30%	5	4,5	5	3
Gesamtergebnis		4,75	4,25	4,2	3,2

A>=4,3 B>=3,5 C>=2,5 D>=1,5 E<1,5
Die Bewertungen A bis C beinhalten in ihren Bereichen + oder -;

Gesamtergebnisse und gewichtete Ergebnisse basieren auf einer Skala von 0 bis 5.



von fünf Minuten einstellen lässt, gehört in die Hände von geschultem EDV-Personal. Hier greift also das Hersteller-Argument von easy-to-use nicht mehr, sondern der Fachmann muss sich der Konfiguration annehmen.

Celestix Aries

Der Aries ist mit 950 Gramm ein Leichtgewicht. Klein ist er noch dazu. Kaum größer als ein Milchkarton schließt er das LAN an einen Breitbandanschluß (xDSL) an. Mail-Server und die Protokolle für Datei- und Drucker-Sharing sind für Windows-, Linux- und Apple-Clients integriert. Zum Lieferumfang gehören alle nötigen Kabel, sowie ein Installationsposter und die Companion-CD, auf der sich das Handbuch im PDF-Format befindet. Die Dokumentation ist mit 110 Seiten üppig, aber leider nur in englischer Sprache. Deutsche Dokumentation ist laut Celestix ab Juni verfügbar. Im Inneren des Server-Zwergs arbeitet ein Slim-Size-Mainboard und eine Cyrix-MediaGX-CPU mit 200 MHz. Das Netzteil ist bei diesen Dimensionen natürlich extern. Neben dem Vorteil, dass das Netzteil damit keinen Laut von sich gibt, ist es auch noch schnell ersetzbar. Daten speichert der Aries auf einem 2,5-Zoll-Notebook-Laufwerk. Die Kapazität von 19,5 GByte sollte auch in Arbeitsgruppen von mehreren Dutzend Mitarbeitern eine Zeitlang reichen. Davon stehen jeweils 250 MByte als System und Backup-Partition zur Verfügung. 136 MByte sind als Sekundärspeicher (Swap) konfiguriert. Bleiben 18,8 GByte für Daten übrig. Unser Testgerät lief mit Redhat-Linux und Kernel-Version 2.2.16. Die neue Version wird dann schon auf dem 2.4er-Kernel aufsetzen und volle USB-Unterstützung enthalten. Einzigartig im Testfeld sind die beiden PC-Card-Slots. Diese kann der Administrator beispielsweise mit einer Wireless-LAN-Karte zur Funkvernetzung und einem Modem für RAS bestücken.

Die erste Inbetriebnahme funktionierte problemlos. Der Aries kam sich nicht mit dem existierenden DHCP-Server ins Gehege. Statt dessen bezog er eine Adresse und begnügte sich mit der Rolle als Client. Der Administrator kann sofort per Web-Browser auf den Server zugreifen. Der Shutdown funktioniert über das LCD-Menü an der Front des Servers.

Die grundlegenden IP-Einstellungen sind vor-konfiguriert. Auf das Share Public des File-Servers kann der Benutzer sofort zugreifen. Die Konfiguration der Servers erledigt der Administrator mit einem Wizard im Browser. Celestix liefert auf der Companion-CD den Netscape-Communicator 4.75 und Microsoft-IE-5 für Windows und Linux mit. Gerade der Communicator ist wichtig, denn stimmt die Version nicht, kann man den Server wegen Javascript-Fehlern nicht konfigurieren.

Zuerst spezifiziert der Systemverwalter die Benutzer-Accounts für den Zugriff auf den Fileserver. Positiv ist hier, dass jedem Benutzer eine bestimmte Kapazität der Festplatte in MByte zugewiesen werden kann (Quotas). Weiterhin bestimmt der Administrator, ob sich der Benutzer ins Internet verbinden darf. Dies geschieht ganz simpel über eine Checkbox. Ebenfalls über eine Checkbox wird das Verbinden zum Server als Administrator erlaubt. Dieselbe Maske dient gleichzeitig zur Konfiguration der beiden Mail-Optionen Forwarding zu einem externen Postfach und Auto-Antwort bei Abwesenheit.

Der Mail-Server ist schnell konfiguriert. Besitzt die Firma keine MX-Domain arbeitet der Aries auch mit dem Mail-Server des Providers als Relayhost. Zum Abholen von Nachrichten loggt sich Aries per POP3 beim Provider-Server ein. Dafür sind Intervalle vorgesehen, die sich sehr gut an der Realität orientieren, zum Beispiel jede Stunde von 9.00 Uhr bis 18.00 Uhr von Montag bis Freitag. Falls der Server nicht ständig online ist, speichert er ausgehende E-Mails in einer Warteschlange. Sehr einfach ist auch die Behandlung von Multidrop-Mailboxen gestaltet. Diese wird einfach über den Platzhalter * eingestellt. Aries kümmert sich dann um die Auslieferung in die lokalen Postfächer. Für den Einsatz des E-Mail-Servers sind zuerst alle Benutzer anzulegen. Dabei sind Aliase wie »buchhaltung« möglich. Ein Virens Scanner fehlt allerdings.

Aries enthält noch weitere Internet-Server wie Web, FTP und DNS. Alle Services laufen per Default, so dass sie gegebenenfalls erst deaktiviert werden müssen. Dies geschieht über ein Menü im Browser. Der Mini-Server kann nicht nur selbst als DNS dienen, sondern auch bereits laufende lokale DNS-Server verwalten. Der Web-Server taugt eher für das Intranet, da Aries nicht auf den Dauerbetrieb getrimmt ist. Für das Experimentieren mit eigenen Seiten oder für Bekanntmachungen reicht der Web-Server jedoch allemal. Interessant ist natürlich der FTP-Server, falls große Dateien zum Transfer anstehen. Der FTP-Server ist ebenfalls sehr einfach einzustellen. Zur Beschränkung bekommt der Benutzer ein Nur-Lese-Recht und kann damit Dateien herunterladen. Von Außen ist der Server auch per Anonymous-Login erreichbar. Der Remote-Access-Dienst wird ebenfalls über Checkboxes und dem Usernamen eingestellt. Möglich ist der Zugriff über ein serielles oder ein PC-Card-Modem. Der VPN-Service wird sogar mit nur einer Checkbox aktiviert. Dann muss aber noch der VPN-Adapter am Client eingestellt werden.

Updates lädt der Administrator von der Webseite des Herstellers auf einen erreichbaren PC herunter. Celestix benachrichtigt registrierte Benutzer per E-Mail vom Update. Über eine Funktion des Web-Interface-System spielt der Verwalter das Update ein. Hier sind auch die Funktionen zum Backup und Restore zu finden. Es können Aries-Konfigurationen gespeichert und hergestellt werden.

Für eine höhere Sicherheit schützt der Administrator den Internet-Zugang mit Passwörtern auf Anwenderbasis. So müssen sich die User jedesmal gegen den eingebauten Proxy authentifizieren. Die integrierte Paketfilter-Firewall ist sehr einfach einzustellen. Per Checkbox erlaubt der Verwalter das Durchlassen von Services wie Web, FTP, Mail, Telnet oder DNS von Innen und Außen. Weitere Einstellungen der Firewall sind nicht möglich.

Celestix hat wirklich gute Arbeit geleistet. Der Server ist sowohl als Stand-alone-Lösung für kleine Büros geeignet als auch zur Standortvernetzung via VPN. Aries ist so leicht zu bedienen, dass jeder Windows-9x-Benutzer damit umgehen kann. Die Bedienung über das Frontpanel ist gelungen und einfach zu verstehen. Da er dank der Notebook-Technik ohne Lüfter auskommt, kann er auch direkt auf einem Schreibtisch plaziert werden. Außerdem ist er klein und sieht auch noch nicht wie ein Computer aus. Leider ist das Web-Interface und die Dokumentation englisch, und ein Schutz vor Viren fehlt.

Sun Cube3

Mit der neuen Version liefert Sun Microsystems die dritte Generation des blauen Server-Würfels. Das uns vorliegende Testgerät verfügt über zwei 10/100-MBit/s-Ethernet-Ports für xDSL sowie einen seriellen und einen USB-Anschluss. Eine Version mit eingebautem ISDN-Port führt Sun nicht im Portfolio. Soll ISDN zum Einsatz kommen, wird ein externer Terminaladapter benötigt. Die Bedienung erfolgt über einen Web-Browser oder mit einigen Knöpfen und dem zweizeiligen LCD auf der Rückseite.

Cobalt nimmt auf bestehende Netzwerke Rücksicht, deren Clients per DHCP versorgt werden. Findet die Cube3 einen DHCP-Server, bezieht es eine IP-Adresse. Ansonsten agiert es auf Wunsch selbst als DHCP-Server. Dies kann der Administrator gleich zu Beginn umgehen, indem er die manuelle Konfiguration der Auto-Konfiguration vorzieht. Der acht-seitige Quick-Start-Guide steht einem lediglich bei der Netzwerkkonfiguration bei. Über die weiteren Schritte klärt das gute Handbuch auf. Nach der Grundkonfiguration über das LCD stellt der Administrator alles weitere im Browser ein.

Cobalt setzt zur Konfiguration einen Web-basierenden Wizard ein. Das Anlegen von Benutzer-Accounts ist gut gelungen. Alle relevanten Daten wie Name, Passwort und E-Mail-Alias sind auf einer Seite zusammengefasst. Auch die Cube ist in der Lage Quotas zu verwalten, um jedem Benutzer nur eine bestimmte Menge der für File-Services reservierten 7 GByte belegen zu lassen. Im gleichen Formular nimmt der Verwalter die Zuordnung der Zugriffsrechte vor. Als File-Sharing-Protokolle unterstützt die Cube SMB und AppleShare. Als einzige Maschine im Test wartet die Cube mit Unterstützung eines Directory-Service, nämlich LDAP, auf. Auch Backups unterstützt der Würfel. Möglich sind Datensicherungen per FTP, SMB oder NFS. Neben einem vollen Backup des Dateibereichs kann die Sicherung auch inkrementell durchgeführt werden. Als Intervall sind »jeden Tag«, »einmal in der Woche« und »einmal im Monat« vorgegeben.

Im Inneren setzt die Cube auf AMD. Ein K6-3D mit 300 MHz kommt zum Einsatz. Der Hauptspeicher ist mit 32 MByte ein wenig knapp bemessen.

Die Administration ist über SNMP, das Browser-Interface, Telnet oder FTP möglich. Der Telnet-Zugang für den Benutzer root ist aus Sicherheitsgründen deaktiviert. Wer sich mit Linux auskennt, kann den Server von der Konsole aus konfigurieren. Auch die Syslog-Datei ist so erreichbar. Eine Export-Option an einen Syslog-Server ist nicht integriert. Herunterfahren lässt sich die Cube nur über das LCD. Der Reboot ist hingegen auch über den Browser möglich. Zur Remote-Administration stehen HTTPS und Telnet zur Verfügung. Das Public-Directory des SMB-Fileservers ist sofort frei zur Benutzung. Ebenso startet die Cube den DNS, den Web- und den Mail-Server. Der Web-Server unterstützt Frontpage-2000-Extensions, Perl- und PHP-Skripts, womit der Server durchaus auch für den eigenen Web-Auftritt geeignet ist.

Für die Konfiguration der Firewall sollte der Administrator gute Kenntnisse über Paketfilter besitzen. Cobalt spart sich eine abstrakte Schnittstelle, was die Konfiguration für unerfahrene Administratoren schwierig macht. Der Anschluss ans Internet gestaltet sich hingegen sehr simpel. Für PPPoE sind lediglich der Username und das Passwort anzugeben.



ben. Network-Address-Translation ist standardmäßig aktiv. Eine statische IP-Adresse sowie vom Provider per DHCP zugewiesene Adressen sind ebenfalls benutzbar. Für ISDN- und Modem-Verbindungen sind die üblichen Angaben zu machen.

Die Optionen des E-Mail-Service sind ein wenig mager ausgefallen. Zwar unterstützt der Server neben SMTP und POP3 auch IMAP4 und sogar ETRN, man kann jedoch nur ein durchgehendes Abfrage-Intervall in Minuten angeben. Eine feinere Einstellung etwa für die Zeit zwischen 9.00 und 18.00 Uhr ist nicht möglich. Mit der POP-before-SMTP-Funktion lassen sich aber öffentliche Mail-Server wie GMX nutzen. E-Mail-User können mit Aliassen versorgt werden. Mail-Forwarding und Abwesenheits-Responder sind ebenfalls vorhanden. Auch Mailinglisten kann die Cube3 verwalten. Prima ist die eingebaute Web-Mail. Somit kann man sich den Einsatz von Clients sparen und behält immer alle Nachrichten auf dem Server. Ein Virens Scanner fehlt dem Würfel ebenfalls.

Die Cube3 überzeugt durch ihren Funktionsreichtum. Die Konfiguration ist relativ einfach. Außer der Firewall lässt sich alles im Handumdrehen konfigurieren. Die Cube kann mit Standleitungen, Dial-Up-Verbindungen sowie mit Breitbandanschlüssen zum Internet umgehen. Sehr positiv sind außerdem die Backup-Funktionen. Da Unterstützung für VPNs fehlt, ist die Cube aber nur bedingt zur Standortvernetzung geeignet. Der zu geringe Hauptspeicher behindert die Arbeit auf dem File-Server. Der Mail-Server sollte außerdem einen Virens Scanner enthalten.

Linogate Defendo

Die Augsburger Linogate offeriert ihre Internet-Appliance Defendo in drei Größen. Network Computing testet die Version »medium«, mit der bis zu 50 Benutzer das Internet nutzen. Die große Variante bietet nicht mehr Funktionen, sondern kommt als Gerät für 19-Zoll-Racks und ohne Beschränkung der Benutzerzahl. Der kleine Defendo ist auf zehn User beschränkt.

Das All-in-One-Gerät bindet kleine Netze per ISDN-Karte (maximal 128 KBit/s) ans Internet an. Mit der VPN-Funktionalität kann das Gerät zur Standortvernetzung eingesetzt werden. Die Remote-Access-Komponente erlaubt die Fernwartung. Diese ist bei einer statischen IP-Adresse auch via HTTPS möglich. Der integrierte E-Mail-Server ist bei unserer Version auf 50 User beschränkt – trotz Linux und einer 600-MHz-CPU. Auf Anfrage erhöht Linogate aber die Anzahl der E-Mail-Konten auf 250. Als einziges Gerät im Test enthält der Defendo einen Virens Scanner, den der Administrator vom Hersteller McAfee allerdings erst registrieren lassen muss.

Die Erstinstallation des Defendo verläuft reibungslos. Der integrierte DHCP-Server schaltet auf Secondary-Betrieb um, sofern bereits ein DHCP-Server im Netz vorhanden ist. Für die IP-Adressvergabe kann man drei verschiedene Wege gehen: Über die Terminalemulation per serieller Verbindung, per Setup-CD und über TCP/IP, wenn sich der Client-PC im Segment 192.168.0 befindet.

Steht die Verbindung zum Server setzt der Administrator die Konfiguration per Web-Browser fort. Die Verbindung wird dabei über Secure-HTTP (https) verschlüsselt. Bei der Konfiguration helfen Assistenten. Damit können den Defendo auch we-

Features

Internet-Access-Appliances

	Celestix Networks Aries	Sun Cube3	Linogate Defendo	Intel InBusiness Small Office Network
Technische Daten:				
Abmessungen (L x B x H)	14,5 x 11 x 17	18,5 x 19 x 19,5	32,4 x 37,4 x 9,3	33 x 21 x 47
Gewicht	0,95 kg	5 kg	7 kg	17 kg
CPU	Cyrix MediaGX 200 MHz	AMD K6-3D 300 MHz	Intel Celeron 700 MHz	Intel Celeron 533 MHz
RAM	128 MByte; 2xSDRAM PC-100 (max. 256 MByte)	32 MByte; 2xSDRAM PC-100 (max. 512 MByte)	64 MByte; 2xSDRAM PC-133 (max. 512 MByte)	64 MByte; 2xSDRAM PC-100 (max. 512 MByte)
NIC	2 x RealTek 8129 (NE2000-kompatibel)	2 x National Semiconductor MacPhyter (dp83815)	Intel EE100/Pro (GD82559C)	Intel EE100 (GD82559)
PS/2, USB	1, 2	○, 1	2, 2	2, ○
Seriell/Parallel	1, 1	1, ○	2, 1	2, 1
Netzteil	extern	extern	80 W	145 W
Sound	Soundblaster 1b	○	National Semiconductor PC87363	○
ISDN	○	○	Elsa Microlink (Infineon PSB 2115 H), aktiv	Eicon Diva 2.01 (Infineon PSB 2115 H)
Modem-/Telefon-Adapter	○	○	○	Digitan Systems DS560-558-WW (2 x RJ-11)
HDD Kapazität	19,5 GByte	9,5 GByte	9,8 GByte	2 x 15 GByte
Software:				
Betriebssystem	Linux 2.2.16	Linux 2.2.16	Linux 2.0.38	Windows for Express Networks
Mail	Sendmail	Sendmail	Sendmail	POP3-Client
News	○	○	○	○
Web	Apache	Apache	Apache	○
Telnet	●	●	●	○
FTP	○	●	●	○
SSH	○	○	○	○
ISDN integriert	○	○	●	●
PPPoE	●	●	○	○
DHCP	●	●	●	●
DNS	named (bind)	named (bind)	named (bind)	○
RAS	●	●	●	●
SMB	●	●	●	●
NFS	○	●	○	○
Appleshare	●	●	○	○
Sicherheit:				
VPN	●	○	●	○
Virens Scanner	○	○	●	○
Firewall	IPchains-Paketfilter	IPchains-Paketfilter	IPchains-Paketfilter, DMZ	MS-Proxy
Besonderes:	2 PC-Card-Slots	Web-Mail vollst. Backup, LDAP-Support, SNMP	Virens Scanner, Support für NT-Domains	vollst. Backup, Backup-Laufwerk (Wechsel-ahmen) 10MBit/s-Hub (8 Ports), 2 x 10/100-MBit/s-NICs
Web	www.celestix.de	www.cobalt.com	www.linogate.de	www.intel.com
Preis	2 900 Mark	4 500 Mark	3 500 Mark	4 700 Mark

● = ja, ○ = nein

niger erfahrene Administratoren schnell konfigurieren. Gleich zu Beginn kann der Verwalter die Fernwartungsfunktion einstellen.

Die Konfiguration ist sehr einfach gehalten. Es müssen nie mehr als zwei Daten pro Seite eingegeben werden. Optionen sind meist in Pull-Down-Menüs untergebracht. Die Online-Hilfe ist unter den Optionsfeldern angebracht und damit immer verfügbar. Die ISDN-Komponente unterstützt Euro-ISDN sowie das alte nationale 1TR6-Protokoll. Die Verbindung wird nach einer definierbaren Zeitspanne der Inaktivität abgebaut. Auch die Option, den Defendo an den Gebührentakt des Providers anzupassen, ist vorhanden. Für die Ferneinwahl eignet sich ISDN oder ein serielles Modem. VPN-Funktionalität ist ebenfalls integriert.

Für die E-Mail-Accounts verlangt der Defendo Benutzernamen und Passwort. Aliase anzulegen ist

möglich. Die Appliance kommt mit SMTP und POP3 zurecht und unterstützt auch ETRN. Der Mail-Server kann sich selbst um das Abholen und Zustellen von Nachrichten kümmern, aber auch als Forwarder dienen, sofern ein anderer Rechner als Mail-Server im lokalen Netz fungiert. Defendo unterstützt Single- und Multi-Drop-Postfächer und beherrscht auch das zeitversetzte Senden und Empfangen.

Die Benutzerverwaltung ist recht gelungen. Per Hinzufügen-Schaltfläche weist der Administrator jedem Benutzer Rechte für die Server-Dienste zu. Der Verwalter kann auch das Ändern des Passwortes für die verschiedenen Dienste erlauben. Mit Benutzerdaten aus Verzeichnis-Diensten kann Defendo jedoch nichts anfangen.

Die Backup-Funktion eignet sich, um mit mehreren Konfigurationen zu experimentieren. Auch die Werkzeugeinstellungen sind darüber wieder

herzustellen. Updates lädt der Nutzer von der Linogate-Webseite herunter und spielt sie über eine Option ein. Eine Benachrichtigung bei der Verfügbarkeit eines neuen Updates führt Linogate hingegen nicht durch.

Gut geregelt ist auch das Herunterfahren. Einfach vorne den Aus-/Ein-Schalter drücken und Defendo fährt herunter. Optional kann der Rechner auch über den Browser neu gestartet respektive heruntergefahren werden. An weiteren Internet-Diensten enthält der Defendo einen Web-Server und einen DNS-Server. Den Web-Server hält Linogate allerdings ein bisschen sehr einfach. Die fehlende Unterstützung für Skriptsprachen wie ASP oder PHP schränkt den Einsatz im Web doch erheblich ein.

Linogate hat umfangreiche Accounting-Tools integriert. Damit ist es möglich, den Durchsatz der Verbindung zu überwachen. Per Intrusion-Detection erkennt der Defendo Attacken von außen. Als Gegenmaßnahme kann das Gerät die betreffenden Ports dicht machen. Auch das Herunterfahren des Systems ist bei einem Angriff vorgesehen. Sehr gut gefällt uns die Option das IP-Routing zu deaktivieren. Wird der Rechner zum Beispiel als Internet-Webserver betrieben, ist so das lokale Netz vor Amateur-Crackern weitgehend geschützt.

Die Firewall ist nicht einfach zu konfigurieren. Darum sollte sich ein Fachmann kümmern. Die Grundregeln reichen allerdings für Netze aus, die keine unternehmenskritischen Daten enthalten. Das Handbuch ist mit fast 200 Seiten sehr umfangreich. Die einzelnen Funktionen sind gut erklärt. Zudem ist das Buch auf Deutsch. Für die initiale Konfiguration ist ein Quick-Install-Heftchen beigelegt. Das Handbuch geht auch detailliert auf die Firewall-Konfiguration ein, so dass experimentierfreudige Laien durchaus ein sicheres System zusammenstellen können. Negativ fällt auf, dass das Gerät keine Kontrollanzeige hat. Man weiss also nicht, wann der Rechner gebootet hat. Zwei LEDs zeigen, dass der Defendo angeschaltet ist und das irgendein Mail-Vorgang läuft (oder auch nicht). Eine dritte LED gehört zu einem undefinierbaren Zeichen, das auch das Handbuch nicht erläutert. Nur wer auf die Rückseite schaut, kann den Status der Netzwerkkarte prüfen. Den Status der S₀-Schnittstelle kann man hingegen nur errahnen.

Defendo ist eine Internet-Access-Lösung, die höheren Sicherheitsansprüchen gerecht wird. Das Gerät eignet sich sowohl zur Standortvernetzung als auch als Stand-alone-Lösung. Da der Virens Scanner auf dem Server arbeitet, können die Clients zusätzlich mit einem Konkurrenzprodukt gesichert werden. Die Firewall ist gut vorkonfiguriert. Experten bleiben aber alle Möglichkeiten für eigene Anpassungen. Die Unterstützung für VPNs und die umfangreichen Monitoring-Funktionen sind weitere Pluspunkte.

Intel InBusiness Small Office Network

Intels Small-Office-Lösung ist in einem Midi-Tower untergebracht, der nochmals von einem Plastik-Hülle umgeben ist. Hauptgrund dafür dürfte das ansonsten nicht zu integrierende LCD an der Front sein. Als einzige Appliance im Testfeld liefert Intel mehr als nur die benötigten Kabel mit. Zwei 10/100-

MBit/s-Ethernet-Adapter und eine 10-MBit/s-Hub mit acht Ports gehören zum Lieferumfang. Um Patchkabel für die Verbindung der Clients zum Hub muss sich der Anwender allerdings selbst kümmern.

Die Appliance eignet sich für die lokale Vernetzung und Internet-Anbindung kleiner Büros, die ausschließlich Windows-Clients einsetzen. Microsoft-fremde Protokolle wie Appleshare oder NFS unterstützt das Gerät nicht. Als Betriebssystem fungiert eine OEM-Variante von Windows-2000.

Die Inbetriebnahme des Servers verläuft reibungslos. Auffällig ist lediglich das konstante Dröhnen des Lüfters. Aber nach nur 5 Minuten steht die Verbindung zum Internet. Nach weiteren 10 Minuten sind auch die Benutzer für Mail und File-/Printer-Sharing eingetragen. Einen eigenen Mail-Server spart sich Intel. Statt dessen ist ein einfacher POP3-Client installiert.

Für die Anbindung der Clients sorgt ein DHCP-Server. Er vergewissert sich erst, ob bereits ein anderer DHCP-Server IP-Adressen an die Clients verteilt. Ist dies der Fall, konfiguriert er sich selbst als Secondary-DHCP-Server.

Die getestete Version enthält eine Kombikarte für ISDN und ein V.90-Modem. Den Zugang konfiguriert der Administrator mit einem einfachen Wizard. Kanalbündelung ist nur statisch verfügbar (immer oder nie). Nach einer gewissen, einzustellenden Zeit der Inaktivität trennt der Server die Verbindung. Weitere Optionen zur Internet-Verbindung wie Kompressionsverfahren gibt es nicht.

Der File-Server offeriert eine Kapazität von maximal 15 GByte (die ganze Platte).

Ein optionales Mirror-Laufwerk im Wechselrahmen von gleicher Kapazität erhöht die Datensicherheit. Von dort spielt der Administrator die Server-Konfiguration sowie die Anwenderdaten zurück. Negativ fällt die alte Microsoft-Krankheit ins Gewicht, keine Speicherbeschränkungen für die einzelnen Benutzer (Quotas) angeben zu können. Die Benutzerverwaltung ist einfach zu bedienen. Doch für die Integration in eine bestehende NT-Domäne gibt es keine Unterstützung.

Für die Sicherheit vor Eindringlingen sorgt der Microsoft-Proxy-Server in der Version 2.0. Die Konfiguration wird in der englischen Dokumentation allerdings nicht erklärt.

Zur längerfristigen Überwachung liefert Intel einen Monitor mit, der sich in einstellbaren Intervallen per E-Mail meldet. Zur Auswertung der Daten muss auf einem Client allerdings extra Software installiert werden. Die gesammelten Daten sind etwas mager. So kann die Hardware auf Fehler überwacht werden. Die Möglichkeit des Auto-Reboot bei einem Hardware-bedingten Problem wie der Überhitzung der CPU fehlt jedoch. Der Administrator kann also nur im Nachhinein tätig werden. Eine feine Sache ist die Möglichkeit, eine Nachricht an Pager zu senden, falls die Maschine einen bestimmten Fehler aufweist. Leider hat Intel vergessen, die Firewall mit in das Alert-System zu integrieren, womit die Hauptgrund für eine schnelle Benachrichtigung ausgelassen wurde.

Ansonsten sammelt die Monitoring-Software Daten über die Auslastung des Systems und die Benutzung einzelner Dienste. Ein detaillierteres Mapping zum Beispiel auf einzelne Benutzer ist nicht möglich. Die Appliance enthält umfangreiche

Info

So testete Network Computing

Am meisten hat uns interessiert, ob die Geräte bei aller Einfachheit auch flexibel genug sind. Dabei kamen zwei Szenarien zum Einsatz: Als Stand-alone-Gerät für SOHO-Netze und zur Anbindung an ein Unternehmensnetz. Die Geräte sollten nach 10 Minuten die ersten Web-Seiten an Clients liefern. Weiterhin haben wir die Benutzerführung unter die Lupe genommen. Schließlich ist eines der Hauptargumente der Hersteller, dass die Appliances auch ohne geschultes EDV-Personal einsetzbar sind. Sicherheits- und Fernwartungs-Funktionen standen ebenfalls ganz oben auf der Testliste. Die Firewalls haben wir mit einem einfachen Portscan geprüft.

Funktionen zur Fernwartung per RAS. Intel weist in der Dokumentation auch darauf hin, dass das Gerät von einem Dienstleister ferngewartet werden kann. Der Zugriff erfolgt über HTTPS.

Administratoren, die es gewohnt sind, genauestens über ihre Windows-Server im Bilde zu sein, wird die Appliance nicht zufrieden stellen. Dafür ist das Gerät zu sehr auf einfach á la Windows-9x getrimmt. Für den Aufbau eines kleinen Windows-Netzes, das ohne Directory-Service auskommt, ist das Gerät durchaus geeignet.

Fazit

Alle Appliances haben sich ruck-zuck in unser lokales Testnetz integriert. Auch die Anbindung ans Internet schafften alle Teilnehmer problemlos. Den besten Gesamteindruck macht der Defendo von Linogate, der in diesem Test auch die Auszeichnung »Referenz« erhielt. Die Appliance enthält jegliche Internet-Dienste, kann als File-Server dienen und schützt am besten vor Gefahren aus dem Internet.

Bei der Konfiguration der integrierten E-Mail-Server sind kleine, aber feine Unterschiede auszumachen. Der Aries-Server schneidet hier am besten ab. Die Abfrage-Intervalle sind sehr fein abgestuft und dadurch ideal für Wahlzugänge. Leider fehlt wie auch bei der Cube3 ein Virens Scanner. Den liefert aber Linogate in seinem Defendo mit. Der Defendo macht bei den Sicherheits-Optionen die beste Figur, da das Gerät über die Regelerstellung hinaus noch weitere sinnvolle Optionen wie das automatische Schließen von Ports integriert. Für die Anbindung von Linux- und Apple-Workstations eignen sich die Cube3 und Aries. Nur sie enthalten alle notwendigen Protokolle. Defendo und Intels In-Business-Server kommen hingegen nur mit SMB-Clients zurecht.

Neben dem meist fehlenden Virenwächter fällt auch die nicht existente Unterstützung für Directory-Services ins Gewicht. Hier hat Sun die Nase vorne. Die Cube3 enthält Support für LDAP. Der Defendo kann Benutzer immerhin gegen einen NT-PDC verifizieren. Für die Anbindung ans Firmennetz per VPN sind nur Aries und Defendo geeignet.

Die Benutzerführung der Testkandidaten ist durchweg gelungen und die Konfiguration mit ein wenig Know-how auch ohne Handbuch zu schaffen. Celestix hat sich außerdem durch die kleine Bauweise und die PC-Card-Slots die Empfehlung der Redaktion verdient. [jr]

