Ein Muss für Netzwerk- und TK-Entscheider
NetworkWorld
Ausgabe 20-2001

Vergleichstest Firewall-Appliances: »Astaro Security Linux« und »Cisco PIX 515«

Cisco kontra Linux

Bernd Klusmann, Christoph Lange

Immer mehr Hersteller setzen auf Linux als Plattform für Firewall-Appliances. Das Open-Source-Betriebssystem erzielt hervorragende Durchsatzwerte und macht damit in diesem Markt etablierten Anbietern wie Cisco ernsthaft Konkurrenz.

In Runde 2 der Vergleichstestreihe »Firewall-Appliances« trafen wiederum zwei sehr unterschiedliche Kandidaten aufeinander: Newcomer Astaro fordert mit einem Linux-gestützten System den etablierten Platzhirsch Cisco mit seiner PIX-Firewall heraus. Auch diesmal lieferten beide Hersteller zwei Geräte in das Berliner Testlabor des EANTC, damit wir die Performance sowohl mit unverschlüsselten als auch mit verschlüsselten Verbindungen testen konnten (zu den Testverfahren siehe Einleitungsartikel NetworkWorld 19/01, Seite 71).

Die Testkandidaten

Die Firma Astaro wurde 1999 gegründet und Anfang 2000 in eine Aktiengesellschaft umgewandelt. Der Anbieter bezeichnet sich selbst als Spezialist für Sicherheitslösungen im Internet. Zielgruppe sind kleinere und mittelständische Unternehmen aller Branchen sowie Tochtergesellschaften und Filialen von großen Unternehmen. Mit dem Produkt »Astaro Security Linux« bietet Astaro eine Linux-gestützte Firewall-Appliance.


Test und Analyse: »Netcom Smartbits 2000« von Spirent Communications.

Die Pyramid Computer Systeme GmbH und Cobalt Networks (letztere wurden mittlerweile von Sun Microsystems gekauft) bieten diese Software vorinstalliert auf Hardware als Appliance-Lösung an. Auf dem Webserver von Astaro ist eine kostenlose Testversion der Software für den privaten Gebrauch verfügbar.

Das nur eine Höheneinheit (1 U) umfassende 19-Zoll-System von Astaro basiert auf dem Linux-Kernel 2.4. Für ordentliche Rechenleistung sorgen ein mit 750 MHz getakteter Intel-Celeron-Prozessor und der Arbeitsspeicher von 128 MByte. Zur Standardausrüstung zählen zudem eine 20-GByte-Festplatte sowie ein CD-ROM-Laufwerk. Die Verbindung zum Netzwerk erfolgt über bis zu sechs 10/100Base-T-Karten. Zwei davon sind »onboard« untergebracht, vier in Steckplätzen. Zum Zeitpunkt unserer Tests lag die Software »Astaro Security Linux« in Version 2.0 vor. Unter dem Link http://www.astaro.de/products/index.html lassen sich weitere Informationen zu Astaro abrufen. Auf dieser Seite ist auch eine Online-Demo der Managementschnittstelle verfügbar. Jedoch ist der Zugriff darauf durch die Anzahl der Nutzer begrenzt und somit oft nicht verfügbar.

Test- und Mess-Equipment

Für die Firewall-Tests setzen wir »Netcom Smartbits 2000« von Spirent Communications ein, mit den Anwendungen »Smart Flow« und »Smart TCP«. Smart Flow generiert für jede Schnittstelle des Analyzers bis zu 1000 TCP/IP-Ströme mit bis zu 64 000 Paketvariationen. Auf diese Weise lassen sich Unternehmensnetze mit sehr vielen Nutzern simulieren. Der Analyzer misst für jeden aufgesetzten Datenstrom Durchsatz, Paketverlust, Paketlaufzeit und Variation der Paketlaufzeit. Smart TCP ermöglicht Tests unterschiedlicher Leistungsparameter in Bezug auf Verbindungskapazitäten sowie Auf- und Abbauraten einer großen Anzahl von TCP-Verbindungen.

Die Firewall-Appliance von Cisco Systems hört auf den Namen »Cisco PIX Firewall«. Neben Add-on-Varianten für die Software »Cisco IOS« oder für Intrusion-Detection-Systeme bildet die PIX-Familie die Basis der Sicherheitsprodukte von Cisco. Sie deckt ein sehr breites Spektrum ab, das vom Teleworker bis zu großen Unternehmenskunden und Serviceprovidern reicht. Zum Test trat Cisco mit der »PIX 515« an, die für kleine und mittelständische Unternehmen konzipiert ist.

Cisco lieferte beide Geräte mit einer Beschleunigerkarte für die Verschlüsselung. Um die Testergebnisse mit den bereits durchgeführten und künftigen Tests vergleichen zu können, wurden für die Bewertung nur die Messungen ohne Hardwareunterstützung berücksichtigt. Bei einigen Testszenarien haben wir zusätzlich mit Beschleunigerkarte gemessen, um die Unterschiede zu sehen. Diese Ergebnisse sind in den entsprechenden Tabellen in Klammern angegeben.

Im Inneren der PIX 515 arbeitet ein Pentium-MMX-Prozessor mit einer Taktrate von 200 MHz. Das Gerät verfügt über einen Arbeitsspeicher von 64 MByte.

Standardmäßig ist die Firewall mit zwei »festen« 10/100Base-T-Schnittstellen ausgerüstet. Über eine 4-Port-Karte lässt sich die Box auf sechs Fast-Ethernet-Anschlüsse erweitern. Die Tests führten wir mit der PIX-Firewall-Version 6.1 und der Firmware »Phoenix Picobios 4.0 Release 6.0« durch. Weitere Produktinformationen sind erhältlich unter http://www.cisco.com/univercd/cc/td/doc/pcat/fw.htm.

Handhabung der Firewalls

Beide Testkandidaten ließen sich sehr schnell und einfach konfigurieren. Die Einbindung ins Netzwerk erfolgt über ein Terminalprogramm oder einen Webbrowser. Die weiteren Einstellungen kann der Administrator dann von beliebiger Stelle aus mit einem Standardbrowser durchführen.

		Astaro/Pyramid	Cisco PIX 515
Ohne Verschlüsselung	Durchsatz unidirektional	73 MBit/s	92 MBit/s
	Durchsatz bidirektional	68 MBit/s	48 MBit/s
	Latenz unidirektional	160 µs	512 µs
	Latenz bidirektional	268 µs	1343 µs
Mit Verschlüsselung	Durchsatz unidirektional	33 MBit/s	11 (50) MBit/s
	Durchsatz bidirektional	17 MBit/s	5 (25) MBit/s
	Latenz unidirektional	1521 µs	14 175 (2502) µs
	Latenz bidirektional	5429 µs	17 212 (3577) µs

Alle Messungen wurden durchgeführt mit 512-Byte-Paketen und 20 parallel aktiven IP-Clients (bei Cisco sind in runden Klammern auch die Werte angegeben, die beim Einsatz der VPN-Beschleunigerkarten gemessen wurden). Die Latenzmessungen erfolgten bei den ohne Verschlüsselung durchgeführten Tests mit 40 MBit/s Last. Mit Verschlüsselung wurde Astaro unter einer Last von 16 MBit/s gemessen, bei Cisco betrug die Last 4 MBit/s.

Ergebnisse IP-Leistungsmessung

Eine Erstinstallation war bei der Astaro-Firewall, die wir von Pyramid erhielten, nicht nötig, da sie bereits mit vorinstallierter Software ausgeliefert wird. Mithilfe der beiliegenden CD-ROM oder einer zu erstellenden Boot-Diskette lässt sich die Software auch auf andere Hardware aufspielen. In diesem Fall gliedert sich die Installation in zwei Teile. Die ersten Schritte werden in einem Installationsmenü durchgeführt, die weitere Konfiguration erfolgt über das Web-gestützte Konfigurations-Tool »WebAdmin«. Dieses stellt ein klar strukturiertes und

intuitives Menü zur Verfügung. In den Untermenüs »System«, »Service- und Benutzerdefinitionen«, »Netzwerk«, »Paketfilter«, »Proxy«, »VPN« und »Reporting« lassen sich detaillierte Einstellungen der Firewall vornehmen. Die Online-Hilfe liegt allerdings nur auf Englisch vor. Als Entschädigung bietet Astaro über den Link http://docs.astaro.org/ viele interessante Dokumente an, zum Beispiel aktuelle Handbücher in Deutsch und Englisch oder Howtos (Konfigurationsanleitungen zu speziellen Themen). Ebenfalls hilfreich ist ein Diskussionsforum mit Hinweisen auf neue Software oder der Austausch über Erfahrungen mit dem Astaro-Firewallsystem (http://www.astaro.org).

Sehr gut gefallen hat uns die Reporting-Funktion des Systems, die in Histogrammen Performance-Daten darstellt, beispielsweise zu Systemhardware, Netzwerkauslastung oder Proxyaktivitäten. Für die Fehlersuche bei der Anpassung der Firewall-Konfigurationen waren Debugging-Tools auf Basis von Linux wie »snoop« oder »tcpdump« sehr hilfreich. Der telefonische Support während der Tests erwies sich als sehr qualifiziert und hilfreich. Probleme aufgrund unterschiedlicher Zeitzonen oder der Sprache traten beim deutschen Hersteller Astaro erwartungsgemäß nicht auf.

Funktionsmerkmal	
Konfiguration über Webbrowser ohne Zusatzsoftware	Ja
Backup der Konfigurationsdaten auf Firewall oder PC	Ja
ISDN-Interface	Nein
Ethernet als Standardschnittstellen	Ja
TCP/IP-Support	Ja
Network Address Translation (NAT)	Ja
Unterstützung von Tri-homed Firewalls	Ja
Port-Forwarding vom Internet ins LAN	Ja
Intrusion-Detection-Mechanismen	Ja (Port-Scan-Detection)
Routing-Modus	Ja
IPSec-kompatibel	Ja
Fernwartungszugang über Modem/ISDN	Nein
Reset-Factory-Default	Ja
Konsolen-Port für Recovery	Ja
Bewertung Standardfunktionen	**4,0**
1 = mangelhaft, 2 = ausreichend, 3 = gut, 4 = sehr gut, 5 = ausgezeichnet Weitere Funktionsmerkmale online unter www.networkworld.de/testcenter	

Standardfunktionen Astaro Security Linux

Leichte Stabilitätsprobleme zeigte die 4-Port-Netzwerkkarte von Tulip mit den verfügbaren Treibern. Zur Durchführung der Test verwendeten wir deshalb nur die beiden Onboard-Ethernet-Schnittstellen. Die Umstellung der Netzwerkkarten auf 100 MBit/s im Full-Duplex-Betrieb gestaltete sich etwas umständlich, da Modulparameter von Linux geändert werden mussten. Besser wäre es, wenn sich diese Einstellung auch über die webbasierte Oberfläche ändern ließe.

Die PIX-Firewall 515 von Cisco ist in der Erstinstallation ebenfalls sehr einfach zu bedienen. Über eine Terminalverbindung haben wir zunächst die Adressen der Ethernet-Ports angepasst. Für die Konfiguration verwendeten wir den von Cisco bekannten Kommandozeilenmodus. Nachdem wir auf diese Weise den Zugriff aus unserem LAN heraus auf die Firewalls hergestellt hatten, setzten wir einen Konfigurationsassistenten der PIX-Firewall ein. Die einzelnen Schritte sind sehr gut dokumentiert und alle einzustellenden Parameter über eine Online-Hilfe erläutert. Die Eingabe von Regeln erfolgt in selbsterklärenden Menüs. Eine grafisch aufbereitete Liste aller momentan vorhandenen Regeln verschafft dem Administrator einen schnellen Überblick über die aktuelle Konfiguration.

Astaro Security Linux

Während der Tests verzichteten wir meist auf die browsergestützte Konfiguration, da sich die VPN-Funktion bislang noch nicht darüber konfigurieren lässt. Nach Aussage von Cisco soll dies bis zum Jahresende möglich sein. Eine besondere Konfiguration der Zusatzhardware zur Verschlüsselung war nicht nötig. Der Einbau der Karte reichte aus, um diese zu aktivieren.

IP-Leistungsmessungen

Die Messergebnisse der IP-Leistungsmessungen sind bei beiden Herstellern sehr gut. Wie zu erwarten, erreichen die Geräte bei sehr großen Paketen (1518 Byte) die höchsten Durchsatzwerte. Beide Firewall-Appliances erzielen im unidirektionalen Modus bei unverschlüsselter Übertragung einen Durchsatz von 100 Prozent. Mit bidirektionalem Traffic zeigen sich erste Unterschiede: Cisco kommt hier auf 95 Prozent Durchsatz, Astaro nur auf 81 Prozent.

Mit kleineren Paketen tritt die Leistungsgrenze noch deutlicher zu Tage. Da pro Zeiteinheit deutlich mehr Pakete weitergeleitet werden müssen, sind die Anforderungen an die Firewall höher. Cisco zeigt ein sehr stabiles Verhalten. Bei Paketen mit einer Länge von 80 Byte erreicht die PIX-Firewall unidirektional noch einen Durchsatz von 22 Prozent, bidirektional exakt die Hälfte (11 Prozent). Da im bidirektionalen Modus die Anzahl der Pakete pro Sekunde doppelt so hoch ist, entsprechen die 11 Prozent bidirektional den 22 Prozent unidirektional.

		Astaro Security Linux		Cisco PIX 515	
	Anzahl IP-Clients x Verbindungen	keine Regeln	mit Regeln	keine Regeln	mit Regeln
1000 legale Verbindungen	1 IP x 1000	1000 100 % 238 µs	1000 100 % 236 µs	1000 100 % 214 µs	1000 100 % 214 µs
	200 IP x 5	1000 100 % 230 µs	1000 100 % 231 µs	1000 100 % 251 µs	999 99,9 % 236 µs
4096 legale Verbindungen	1 IP x 4096	1607 39,23 % 643 µs	1005 24,54 % 1348 µs	4096 100 % 213 µs	4096 100 % 213 µs
	200 IP x 21	4096 100 % 232 µs	4096 100 % 232 µs	4096 100 % 236 µs	4096 100 % 236 µs
6144 legale Verbindungen	1 IP x 6144	1421 23,13 % 1132 µs	1741 28,34 % 794 µs	6144 100 % 236 µs	6144 100 % 213 µs
	200 IP x 31	6144 100 % 233 µs	6144 100 % 233 µs	6144 100 % 236 µs	6144 100 % 236 µs
1000 legale Verbindungen bei 4000 illegalen Verbindungen	20 IP x 50	1000 100 % 1042 µs	1000 100 % 1042 µs	1000 100 % 1042 µs	1000 100 % 1041 µs

Ergebnisse für jeweils 5000 Verbindungen pro Sekunde (weitere Messwerte online unter www.networkworld.de/testcenter).

Ergebnisse TCP-Rate-Tests

Die Ergebnisse der Durchsatztests von Astaro waren nicht so stabil. Für jeden einzelnen Messwert führten wir insgesamt drei identische Testreihen (trials) durch. Die Schwankungen zwischen den einzelnen Testreihen betrugen bei Astaro teilweise mehr als zehn Prozent. Diese nach den Erfahrungen des EANTC unüblichen Schwankungen konnte Astaro im eigenen Labor nachstellen. Den Grund für dieses Verhalten haben die Techniker jedoch nicht herausfinden können. Die in den Ergebnistabellen angegebenen Werte sind eine Mittelung der durchgeführten Testreihen.

Bei den unidirektionalen Tests mussten wir auf den Astaro-Firewalls statische ARP-Einträge (Address Resolution Protocol) vornehmen. Die dynamischen Einträge, die der Lastgenerator zu Beginn jeder Messreihe durch ARP-Anfragen auf der Firewall generierte, löschte die Firewall bereits nach zehn Sekunden. Ohne diese ARP-Einträge war eine weitere Paketübertragung nicht möglich. Da eine Veränderung der entsprechenden Parameter, zum Beispiel auf eine Dauer von zehn Minuten, auf der Firewall sehr kompliziert gewesen wäre, haben wir uns mit statischen ARP-Einträgen beholfen.

Ganz ohne Probleme überstand auch die Firewall von Cisco den Leistungstest nicht. Einmal musste das System vom Support neu gestartet werden, da keine Pakete mehr übertragen wurden. Dies blieb jedoch ein Einzelfall.

Bei den Messungen mit 3DES-Verschlüsselung zeigen sich zum Teil erhebliche Unterschiede zwischen den Herstellern. Ohne Beschleunigerkarte ist Cisco bei 512-Byte-Paketen unidirektional mit einem Durchsatz von 11 Prozent deutlich langsamer als Astaro, die 33 Prozent schafft. Im bidirektionalen Betrieb war das Verhältnis mit 5 Prozent für Cisco und 17 Prozent für Astaro ähnlich.

Cisco PIX 515

Ganz anders sieht es jedoch aus, wenn die Cisco-Firewall mit Beschleunigungskarten betrieben wird. Damit erreicht PIX bei 512 Byte langen Paketen unidirektional 51 Prozent und bidirektional 25 Prozent Durchsatz. Bei dieser Paketlänge bringen Hardwarebeschleuniger also eine Verbesserung der Performance um den Faktor 5. Aufgrund der hohen Prozessorkapazität sind die mit einer rein softwarebasierten Verschlüsselung erzielten Durchsatzwerte von Astaro sehr gut.

Bei den Latenzwerten zeigen beide Geräte Ergebnisse im oberen Leistungsbereich. Obwohl die Lastwerte, bei denen wir die Paketlaufzeiten gemessen haben, bei beiden Kandidaten ähnlich knapp unter den Durchsatzwerten liegen, weichen die Ergebnisse leicht voneinander ab. Die etwas besseren Resultate zeigt Astaro, zum Beispiel 0,2 bis 0,3 ms ohne Verschlüsselung und 1 bis 5 ms mit Verschlüsselung. Sehr groß sind die Unterschiede, wenn die Firewall von Cisco ohne die Beschleunigungskarte eingesetzt wird. Dann kommt es nämlich bei verschlüsselten Übertragungen zu Paketlaufzeiten von durchschnittlich 17 ms. Die Zusatzhardware reduziert diesen Wert auf knapp 4 ms.

TCP-Session-Rate-Tests

Die Tabelle »TCP-Session-Rate-Tests« zeigt die Ergebnisse für eine Messung mit 5000 Requests in einer Sekunde. In den Tabellenfeldern sind folgende Werte untereinander dargestellt:

- Gesamtanzahl der aufgebauten Verbindungen

- Anteil der aufgebauten Verbindungen an den gesamten Verbindungen (in Prozent)

- Durchschnittliche Aufbauzeit für die Verbindungen

Für den Test der maximalen Anzahl der parallel aktiven Verbindungen mussten wir das bisherige Testszenario erweitern, da beide Firewall-Appliances wesentlich mehr Sessions aufbauen können als die bisher getesteten Geräte. Der zusätzlich durchgeführte Test bestand aus 200 simulierten Clients und Aufbauraten zwischen 500 und 2500 Verbindungen pro Sekunde. Jeder Client versuchte, 700 Connections aufzubauen, wodurch maximal 140 000 parallele Sessions möglich sind. Cisco erreichte 103 000 Verbindungen, Astaro 65 000, womit die Ergebnisse deutlich über dem bisher ermittelten Maximalwert von 6144 Sessions liegen. Die große Verbindungsanzahl erzielte Cisco allerdings nur in Testläufen direkt nach dem Systemstart. In den darauf folgenden Testläufen konnte PIX immerhin noch etwa 66 000 Verbindungen gleichzeitig halten.

Produkt	Performance- und Session-Rate-Tests	Handhabung und Service	Feature-Liste	Gesamtergebnis
	40 %	40 %	20 %	
Astaro/Pyramid	★★★★☆ (3,8)	★★★★☆ (4,3)	★★★☆☆(3,0)	★★★★☆ (3,8)
Cisco PIX 515	★★★★☆ (4,3)	★★★★★(4,5)	★★★☆☆(3,3)	★★★★☆ (4,2)
★= mangelhaft, ★★= ausreichend, ★★★= gut, ★★★★= sehr gut, ★★★★★= ausgezeichnet				

Bewertung des Gesamtsystems

Bei den weiteren Tests zum TCP-Leistungsverhalten zeigten beide Firewalls bei 200 simulierten Clients eine deutliche bessere Performance als mit einem simulierten Client. Diesen Effekt konnten wir auch bei einigen anderen Firewalls beobachten. Der Grund dafür liegt in der unterschiedlichen Implementierung der Hash-Algorithmen. Diese sorgen dafür, dass dynamisch anfallende Daten in Speicherbereichen mit fester Größe effizient sortiert werden. In unserem Fall sind dies die Verbindungsdaten, also IP-Adresse, TCP-Quell- und Zieladresse, der Zustand der TCP-Verbindung oder die Sequenznummer der Pakete. Ein Algorithmus, der diese Sortierung beispielsweise nur anhand der IP-Adresse des Clients berechnet, führt bei den Tests mit nur einem Client zu einer ineffizient sortierten Datenmenge beziehungsweise Hash-Tabelle. Die Tabelle der Verbindungsdaten würde in diesem Fall nur aus einer einzigen Hash-Spalte bestehen. Bei weiteren Zugriffen auf die Verbindungsdaten muss in der Tabelle lange gesucht werden, was die Leistungsdaten reduziert.

In diesem Test stellten wir die Linux-gestützte Lösung des jungen deutschen Unternehmens Astaro gegen die Firewall-Appliance von Cisco, einem der Marktführer in der Internetworking-Branche. Ähnlich wie schon das System »Defendo« von Linogate im letzten Test, zeigt auch Astaro, dass Appliances auf der Basis von Linux sehr gute Leistungswerte erzielen. Zwar kommt Astaro trotz hervorragender Stabilität nicht ganz an die PIX-Firewall von Cisco heran. Dafür sind die Linux-Appliances preislich etwas günstiger. Die Software von Astaro ist für den privaten Gebrauch sogar als kostenlose Testversion zu haben. Wer mit knappem Budget möglichst viel Leistung erwerben möchte, ist mit der Firewall-Appliance von Astaro sicher gut beraten.
Um auch bei verschlüsselter Übertragung über VPN-Verbindungen mit den leistungsfähigen Linux-Lösungen mitzuhalten, beziehungsweise diese sogar zu übertrumpfen, schickte Cisco seine beiden Firewalls mit Beschleunigungskarten für die Verschlüsselung in unser Labor. Die mit diesen Karten erzielten Durchsatzwerte sind beeindruckend, jedoch haben sie ihren Preis. Für die Bewertung der Performance legten wir die ohne Beschleunigerkarte erzielten Messergebnisse zu Grunde, um die Vergleichbarkeit der Testkandidaten zu gewährleisten.

Kommentar von Bernd Klussmann: Kopf-an-Kopf-Rennen

Bei Astaro zeigten sich diese Auswirkungen in den Testläufen mit nur einem simulierten Client deutlich. Schon bei mittleren Aufbaugeschwindigkeiten ging eine grössere Anzahl von Verbindungen verloren. Dieser Effekt ließ sich insbesondere bei steigender Gesamtzahl der Verbindungen beobachten. Bei insgesamt 6144 Verbindungen fielen bei 1000 Verbindungen pro Sekunde bereits 28 Prozent der Verbindungen aus. Immerhin wurden diese Werte mit einer größeren Anzahl von Regeln nur geringfügig schlechter. Deutlich bessere Leistungswerte konnte die Appliance von Astaro bei 200 simulierten Clients erreichen. Bei keinem der Tests gingen Verbindungen verloren. Dies gilt auch für den Test mit teilweise illegalen Verbindungen.

Die für den Aufbau der Verbindungen benötigte Zeit ist nahezu unabhängig von der Anzahl der simulierten Clients und der Anzahl der Regeln. Die einzelnen Testergebnisse weichen kaum voneinander ab. Nur wenn die Firewall Verbindungen verliert, steigt die Zeit für den Aufbau von Connections.

Cisco zeigte in den Tests mit einem simulierten Client so gut wie keine Beeinträchtigung durch die erläuterte Hashing-Problematik. Lediglich bei sehr hohen Aufbauraten von 10 000 Verbindungen pro Sekunde beginnt die Firewall, Verbindungen zu verlieren. Dabei gilt wie erwartet: Je grösser die Gesamtanzahl der Sessions, desto grösser der Verlust. Die hohe Leistungsfähigkeit der PIX mit nur einem simulierten Client zeigt sich auch bei den Aufbauzeiten. Die Werte sind sehr stabil und im Vergleich zu Astaro relativ niedrig. Mit 200 simulierten Clients konnte Cisco ebenfalls sehr gute Ergebnisse erzielen. Abgesehen von kleinen Ausnahmen - zweimal 0,1 und einmal 0,05 Prozent Verlust - gab es in diesen Testreihen keine Verluste.

Sehr positiv aufgefallen ist uns die Translation-Tabelle von Cisco, die alle Verbindungsdaten enthält. Während wir bei einigen der bisher getesteten Firewalls einzelne Verbindungen aus dieser Tabelle mit TCP-Reset-Paketen löschen konnten, die mit einer falschen Sequenznummer versehen waren, ließ PIX dies nicht zu. Damit erschwert Cisco das so genannte »Session Hijacking«, also das Entführen von legalen Verbindungen, die dann als Schlupfloch in das gesicherte System dienen.

Fazit

In der Gesamtbewertung schneiden beide Geräte sehr gut ab. Cisco hat aufgrund der besseren Performance-Werte die Nase vorn. Der Unterschied liegt weniger in der Leistung des Paketfilters, also den IP-Leistungsmessungen, sondern bei den TCP-Tests. Hier schlagen die von Astaro bei einem simulierten Client verlorenen Sessions negativ zu Buche. Ohne diese Verluste kämen beide etwa auf die gleiche Benotung der Performance.

Auch bei der Bewertung der Feature-Liste schnitt Astaro etwas schlechter ab. Dies lag daran, dass einige der geforderten Funktionen noch nicht verfügbar waren. So sind zum Beispiel Failover-Betrieb oder Zugriffsbeschränkungen auf definierbare URLs für künftige Versionen geplant.

Funktionsmerkmal	
Konfiguration über Webbrowser ohne Zusatzsoftware	Ja (browserbasiertes grafisches Tool »PIX Device Manager«)
Backup der Konfigurationsdaten auf Firewall oder PC	Ja
ISDN-Interface	Nein
Ethernet als Standardschnittstellen	Ja
TCP/IP-Support	Ja
Network Address Translation (NAT)	Ja
Unterstützung von Tri-homed Firewalls	Ja
Port-Forwarding vom Internet ins LAN	Ja
Intrusion-Detection-Mechanismen	Ja (über »Cisco Secure Intrusion Detection System«)
Routing-Modus	Ja
IPSec-kompatibel	Ja
Fernwartungszugang über Modem/ISDN	Ja
Reset-Factory-Default möglich	Ja (zunächst muss die IP-Adresse per Konsole gesetzt werden)
Konsolen-Port für Recovery	Ja
Bewertung Standardfunktionen	**4,0**
1 = mangelhaft, 2 = ausreichend, 3 = gut, 4 = sehr gut, 5 = ausgezeichnet Weitere Funktionsmerkmale online unter www.networkworld.de/testcenter	

Standardfunktionen Cisco PIX 515

Die Handhabung der Geräte und der Support waren sowohl bei Cisco als auch bei Astaro sehr gut. Den Diskussionsserver und die ausführliche Dokumentation auf der Website von Astaro haben wir bereits erwähnt. Der Telefonsupport, den wir beispielsweise in Anspruch nahmen, um die Konfigurations-Files unter Linux zu ändern, konnte uns in allen Fällen weiterhelfen.

Die Handhabung der PIX-Firewall von Cisco war sehr einfach, sowohl im browsergesteuerten Administrations-Tool als auch per Kommandozeile. Gerade der Kommandozeilenmodus in Verbindung mit festen, auf die Testszenarios zugeschnittenen Konfigurationsfiles ließ keine Fehlkonfigurationen zu. Die PIX-Firewall war der erste Testkandidat, bei dem wir nach der gemeinsam mit dem Hersteller durchgeführten Basisinstallation keinen weiteren Support in Anspruch nehmen mussten. Wir konnten alle Testszenarien durchführen, ohne auf weitere Hilfe zurückzugreifen.

Zur Person

Bernd Klusmann
studierte an der TU Berlin Elektrotechnik und ist als Projektmanager beim EANTC tätig.

NetWorkWorld 20-01 – 26.10.2001, Deutschland
(http://www.networkworld.de)