7 Gigabit-Ethernet-Firewall-Appliances

Rasant durch die Feuerwand

Vor Gefahren von innen und außen sollen Firewalls Unternehmensnetze effektiv schützen – doch Sicherheit geht häufig zu Lasten der Performance. Mit welcher Geschwindigkeit aktuelle Firewall-Appliances heute eine gesicherte Kommunikation in Unternehmensnetzen realisieren können, musste eine Reihe von Firewall-Appliances der unterschiedlichen Leistungsklassen in unseren Real-World Labs an der FH Stralsund beweisen.

Eine sichere aber auch schnelle Kommunikation zwischen einem internen Netzwerk – beispielsweise einen Unternehmensnetz oder einem besonders zu schützenden Segment eines solchen – und einem externen Netzwerk – beispielsweise dem Internet aber auch anderen Segmenten des eigenen Unternehmensnetzes – sollen Firewalls ermöglichen. Technisch ist eine Firewall folglich eine aktive Netzwerkkomponente, wie ein Switch oder ein Router, die nicht nur die Kommunikation zwischen zwei Netzwerken oder Netzwerksegmenten ermöglicht, sondern zugleich eine Überwachungs- und Kontrollfunktion erfüllt, um das interne Netzwerk vor unerwünschtem Datenverkehr zu schützen. Auf der internen Seite handelt es sich zumeist um Ethernet-basierte Netze, extern können auch die unterschiedlichsten WAN-Verbindungen, wie ISDN, xDSL, Mietleitungen, Datendirektverbindungen, Standleitungen oder X.25, angeschlossen sein. Platziert werden Firewalls in der Regel zwischen dem internen Netz und einem entsprechenden Remote-Access-System oder einer anderen aktiven Komponente, die die WAN- oder LAN-Anbindung ins externe Netz oder benachbarte LAN-Segment ermöglicht. Hierfür bieten Firewall-Appliances heute Fast-Ethernet- und – in der Oberklasse – auch Gigabit-Ethernet-Ports an. Manche Systeme stellen darüber hinaus auch eigene WAN-Anschlüsse wie ISDN oder xDSL zur Verfügung. Häufig lässt sich über einen der LAN-Ports zusätzlich eine »demilitarisierte Zone«, kurz DMZ, einrichten, in der beispielsweise Web-Server stehen, die von außen und innen erreichbar sein müssen.

Mit zunehmender Komplexität der heutigen Unternehmensnetze und in Anbetracht der Erkenntnisse, dass das Gros der virtuellen Gefahren aus dem eigenen Unternehmensnetz und nicht aus dem Internet drohen, gehen Netzwerkdesigner mehr und mehr dazu über, auch das interne Unternehmensnetz in einzelne Segmente zu parzellieren, die gegeneinander durch Firewalls gesichert sind. Durch die Integration der Firewalls in das Unternehmensnetz muss nun aber nicht nur der Datenverkehr intern – extern, sondern auch ein Großteil des internen Datenverkehrs das entsprechende System passieren. In Anbetracht der Datenmengen, der Qualitätsanforderungen in heutigen konvergenten Netzen mit ihren Voice- und Video-Applikationen und der Leistungsfähigkeit der übrigen Komponenten im Unternehmensnetz erhöht dieses Anwendungsszenario deutlich die Anforderungen an Firewall-Systeme im Hinblick auf Performance und Funktionalität. In Anbetracht dieser Situation machen auch Durchsatzraten im Gigabit-Bereich durchaus Sinn und die Implementierung von Gigabit-Ethernet-Technologie

Reportcard / interaktiv unter www.networkcomputing.de

Firewall-Performance

	Gewichtung	Netscreen/Juniper ISG 2000	Siemens 4YourSafety/Check Point VPN-1/FireWall-1	Lucent VPN Firewall Brick 1100	Astaro Sun Fire V20z Server	Telco Tech LiSS II secure gateway pro giga	Borderware SteelGate	Watchguard Firebox Vclass V100
Max. Durchsatz 64 Byte unidirektional	10%	5	5	1	1	1	1	1
Max. Durchsatz 512 Byte unidirektional	10%	5	5	5	5	1	1	1
Max. Durchsatz 1518 Byte unidirektional	10%	5	5	5	5	5	1	1
Max. Durchsatz 64 Byte bidirektional	10%	4	5	1	1	1	1	1
Max. Durchsatz 512 Byte bidirektional	10%	5	5	5	1	1	1	1
Max. Durchsatz 1518 Byte bidirektional	10%	5	5	5	5	3	1	1
Max. Durchsatz 64 Byte multidirektional	10%	1	1	1	1	1	1	keine Werte*)
Max. Durchsatz 512 Byte multidirektional	10%	5	4	2	1	1	1	keine Werte*)
Max. Durchsatz 1518 Byte multidirektional	10%	4	4	2	3	1	1	keine Werte*)
Einfluss durch Störtraffic	10%	5	5	5	5	3	3	5
Gesamtergebnis	100%	4,4	4,4	3,2	2,8	1,8	1,2	-*)
		A-	A-	C+	C	D	E	

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.

Bewertungsschlüssel für den maximalen Durchsatz: >= 950 MBit/s = 5; >= 900 MBit/s = 4; >= 800 MBit/s = 3; >= 700 MBit/s = 2; < 700 MBit/s = 1;
Bewertungsschlüssel für den Einfluss durch Stör-Traffic: >= 300 MBit/s = 1; >= 200 MBit/s = 2; >= 100 MBit/s = 3; >= 50 MBit/s = 4; < 50 MBit/s = 5;
*) = Messung nicht möglich, da System nur mit zwei Gigabit-Interfaces ausgestattet.

Info

Das Testfeld

Gruppe 1: Fast-Ethernet-Appliances

Astaro	timeNET secuRACK Enterprise 2 powered by Astaro Security Linux V5
Bintec	VPN Access 25
Bintec	VPN Access 1000
Cisco	PIX 515E Security Appliance
Clavister	M460
D-Link	DFL-700 Network Security Firewall
Gateprotect	gateProtect Firewall
Innominate	Innominate mGUard
Lucent	VPN Firewall Brick 350
SonicWALL	Pro 3060
ZyXEL	ZyWALL 70

Gruppe 2: Gigabit-Ethernet-Appliances

Astaro	Sun Fire V20z Opteron powered by Astaro Security Linux V5
Borderware	SteelGate Firewall + VPN-Appliance
Lucent	VPN Firewall Brick 1100
Netscreen/ Juniper	ISG 2000
Siemens/ Check Point	4YourSafety RX 300
Telco Tech	LiSS II secure gateway pro giga
Watchguard	Firebox Vclass V100

ist eine logische Konsequenz. Die Anforderungen an die Leistungsfähigkeit solcher Firewalls entsprechen logischerweise denen, die auch an andere Komponenten des Unternehmensnetzes, wie LAN-Switches, gestellt werden.

Unabhängig vom individuellen Konzept arbeiten Firewalls generell auf den Ebenen 2 bis 7 des OSI-Referenzmodells. Funktional ist zwischen Paket-Filtern, Stateful-Inspection-Firewalls und Application-Gateways zu unterscheiden. Paket-Filter-Systeme lesen die ein- und ausgehenden Datenpakete auf den Ebenen 2 bis 4 und gleichen sie mit einer vorgegebenen Tabelle ab. Unerwünschte Daten werden so herausgefiltert. Stateful-Inspection-Firewalls sind gegenüber einfachen Paketfiltern »intelligenter« und arbeiten als zustandsabhängige Paket-Filter, die auch die Status- und Kontextinformationen der Kommunikationsverbindungen analysieren und protokollieren. Application-Level-Gateways oder -Proxys realisieren aufwändige Sicherheitsmechanismen über mehrere Schichten hinweg. Sie entkoppeln die Netzwerke physikalisch wie logisch und können beispielsweise von jedem Benutzer Identifikation und Authentisierung prüfen. Komplexere Firewall-Systeme kombinieren in der Praxis häufig verschiedene Firewall-Konzepte in einer Lösung.

Application-Level-Gateways oder -Proxys analysieren den Inhalt der Datenströme, nicht nur wie Paket-Filter- und Stateful-Inspection-Firewalls die Header der Datenpakete, was zur Folge hat, dass ihr Rechenaufwand deutlich größer ist und das Mehr an Sicherheit zu Lasten der Performance geht. Das bedeutet, dass für die gleiche Performance – beispielsweise Fast-Ethernet-Wirespeed – eine deutlich leistungsfähigere Hardware erforderlich ist. Um unsere Tests trotzdem fair und vergleichbar zu halten, haben wir an alle Teststellungen die gleichen Anforderungen gestellt und ein Standard-Rule-Set definiert, das die Hersteller zunächst konfigurieren mussten. Dieses Rule-Set erforderte lediglich eine Paket-Filter-Funktionaltät.

Firewalls bestehen aus Hard- und Softwarekomponenten, die häufig von unterschiedlichen Herstellern stammen und individuell kombiniert werden. Bei den sogenannten Firewall-Appliances handelt es sich um Komplettlösungen, die in den unterschiedlichsten Leistungsklassen angeboten werden und für die unterschiedlichsten Einsatzszenarien gedacht sind. Neben der Firewall-Funktionalität integrieren die Hersteller weitere Funktionalität in die Boxen, so dass immer mehr universelle Security-Appliances angeboten werden, die neben der Firewall-Funktionalität Virtual-Private-Networks, Intrusion-Detection/Prevention und andere Security- und Kommunikationsfunktionen integrieren. Andererseits verleihen die Hersteller der »klassischen« aktiven Komponenten, wie Switches oder Routern, diesen zunehmend Firewall- und andere Security-Funktionalität, so dass insgesamt derzeit ein recht heterogenes Feld von Systemen auf dem Markt ist.

Die Hersteller teilen die verschiedenen Firewall-Appliances in Leistungsklassen ein, die für die entsprechenden Anwendungsszenarien entwickelt werden und sich deutlich in Leistungsvermögen und Preis unterscheiden. Die preisgünstigsten Geräte bilden die Gruppe der Small-Office/Home-Office-Systeme. Dann folgt das breite und heterogene Feld der Mittelklasse, häufig neudeutsch Medium-Business genannt. Die leistungsfähigen Highend-Systeme bilden dann die Enterprise- und Carrier-Klasse. Das Feld der in unseren Labs befindlichen Firewall-Appliances haben wir dagegen schlicht nach den vorhandenen LAN-Ports in Fast-Ethernet- und Gigabit-Ethernet-Systeme eingeteilt. Um das Preis-Leistungverhältnis entsprechend zu würdigen haben wir darüber hinaus unseren Preis-Performance-Index ermittelt.

Das Real-World-Labs-Test-Szenario

Gegenstand unseres ersten diesjährigen Firewall-Vergleichstests, den wir in unseren Real-World Labs an der FH Stralsund durchführten, war die Performance, die solche Systeme derzeit zur Verfügung stellen. Wir wollten wissen, wie stark die Firewall-Funktionalität die Leistungsfähigkeit der reinen Hardware vermindert, beziehungsweise ob die heute verfügbaren Systeme sichere Verbindungen insbesondere zwischen einzelnen Netzwerksegmenten an einem Standort mit Wirespeed ermöglichen, wie die Ausstattung mit entsprechenden Ports zumeist von der Papierform her suggeriert. Darüber hinaus interessierte es uns, wie viel gesicherten Datenverkehr der IT-Verantwortliche derzeit für sein Budget erhält. Hierzu ermittelten wir erneut den Preis-Perfor-

mance-Index, der ein entsprechendes Ranking ermöglicht.

Für die Ausschreibung unseres Vergleichstests haben wir ein Unternehmen unterstellt, das sein heterogenes, konvergentes Netzwerk in einzelne, gegeneinander abgesicherte Segmente und eine eigenständige DMZ teilen und am Unternehmensstandort hochperformant untereinander sowie mit dem Internet verbinden will. Eine geeignete, durchsatzstarke Security-Appliance sollte für die notwendige Sicherheit und Performance sorgen und möglichst die einzelnen Netzsegmente am Standort mit der gewohnten Wirespeed, also mit 100 oder gar 1000 MBit/s verbinden. Zugleich sollte die Appliance den Aufbau eines VPNs zwischen zwei Netzsegmenten ermöglichen, die mit baugleichen Geräten ausgestattet werden sollen.

Aus diesem Pflichtenheft ergaben sich folgende Anforderungen an die einzelnen Teststellungen:

- 2 Firewall- und VPN-Appliances inklusive Zubehör und Dokumentation,
- IPSec-VPN,
- Verschlüsselung nach 3DES,
- je Gerät mit mindestens drei Fast-Ethernet-Ports oder
- zwei Gigabit-Ethernet-Ports und einen Fast-Ethernet-Port.

Messen wollten wir die Firewall-Performance, also die unidirektionalen und bidirektionalen Datendurchsatzraten im Firewall-Betrieb, die sich aus den Datenverlustraten unter Last ergibt. Als weitere Parameter haben wir Latency sowie Jitter unter Last ermittelt. Als Test-Equipment dienten die Lastgeneratoren und -analysatoren Smartbits 6000B von Spirent Communications mit der aktuellen Version der Applikation Smartflow.

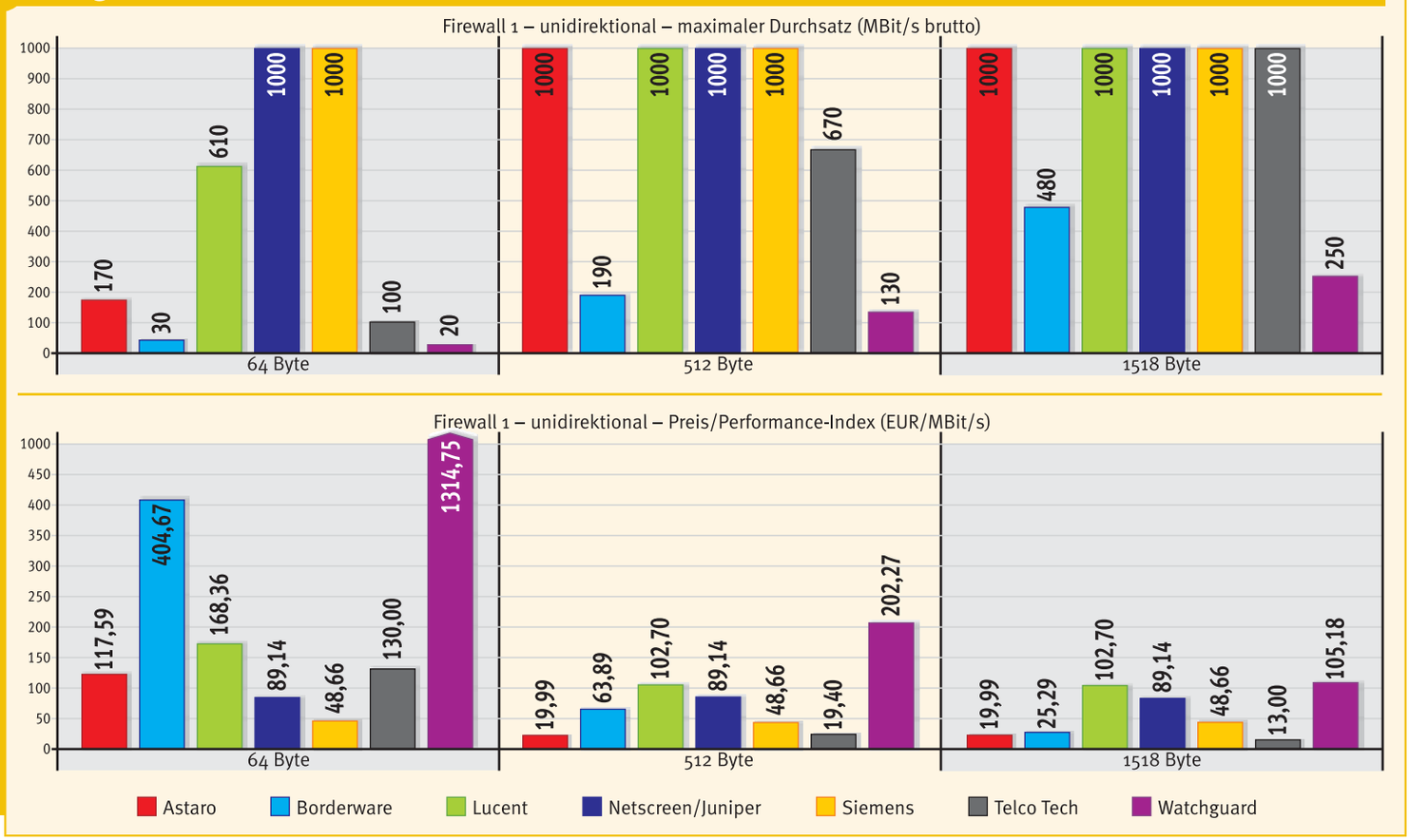
In einer Ausschreibung haben wir alle einschlägigen Hersteller von Security-Appliances eingeladen, uns eine entsprechende Teststellung zur Verfügung zu stellen und ihr System in unserem Vergleichstest in unseren Labs an der FH Stralsund zu begleiten. Jedem Hersteller standen unsere Labs exklusiv für einen Tag zur Verfügung. Insgesamt gingen 15 Hersteller mit ihren Teststellungen an den Start. Die Gruppe Gruppe 1 der Fast-Ethernet-Appliances bildeten Astaros »timeNET secuRACK Enterprise 2 powered by Astaro Security Linux V5«, Bintecs »VPN Access 25« sowie »VPN Access 1000« aus gleichem Hause, Ciscos »PIX 515E Security Appliance«, Clavisters »M460«, D-Links »DFL-700 Network Security Firewall«, die »gateProtect Firewall«, Innominates »Innominate mGUard«, Lucent Technologies »VPN Firewall Brick 350«, »SonicWALL Pro 3060« sowie Zyxels »ZyWALL 70«.

Die Gruppe 2 der Gigabit-Ethernet-Appliances bilden derzeit Astaro mit ihrer »Sun Fire V20z Opteron powered by Astaro Security Linux V5«, Borderwares »SteelGate Firewall + VPN-Appliance«, Lucent Technologies »VPN Firewall Brick 1100«, Netscreens »NS Appliance«, Siemens/Check Points »Four your Safety RX 300«, Telco Techs »LiSS II secure gateway pro giga« sowie Watchguards »Firebox Vclass 100«. Wie sich die Gigabit-Ethernet-Appliances in unserem Test verhielten, steht im vorliegenden Artikel. Die Ergebnisse der Fast-Ethernet-Appliances haben wir in Ausgabe 8-9 2004 der Network Computing veröffentlicht.

Durchsatzraten und Datenverlustverhalten

Zur Messung der maximal möglichen Durchsatzraten sowie des lastabhängigen Datenrahmenverlustverhaltens haben wir mit Hilfe der Spirent-Smartbits-Lastgeneratoren/Analysatoren die Firewall-Appliances mit unidirektionalem und bidirektionalem Datenverkehr mit verschieden Framegrößen belastet. Die Messung der maximalen Durchsatzraten ermittelt den jeweiligen optimalen Durchsatz bei einer für das System idealen Inputrate, zeigt also die maximale Leistungsfähigkeit der Appliance unter optimalen Bedingungen. Die Messung des Datenrahmenverlustverhaltens in Abhängigkeit zur Input-Last zeigt das Verhalten der jeweiligen Appliance unter variierenden Lastbedingungen. Arbeitet eine so getestete Firewall-Appliance mit Wirespeed, so verliert sie unter keinen Umständen Datenrahmen, da die Geräte mit maximal 100 Prozent Last belastet wurden und wir somit keine Überlastsituationen provoziert haben. Erreicht das jeweilige System im Test Wirespeed, dann bedeutet das für den Durchsatzratentest eine maximale zu messende Rate von 100 Prozent oder im Fall des hier vorliegenden Tests 1 GBit/s. Bleibt die Appliance dagegen hinter Wirespeed zurück, dann ist bei einer entsprechenden Auslastung des übrigen Netzwerks davon auszugehen, das die überfor-

Messergebnisse – Firewall-Performance



derte Appliance für entsprechende Datenverluste sorgt, die diverse »Kommunikationsstörungen« im Netz- und Arbeitsbetrieb verursachen können.

Auswirkungen von Datenverlusten

Für die Beurteilung des Verhaltens der Systeme im Testfeld, die wir mit Datenströmen bestehend aus den unterschiedlichsten Frame-Formaten belastet haben, ist es von besonderem Interesse, zu betrachten, welche Lasten und Frame-Größen in realen Netzen vorkommen. Bei klassischen Dateitransfers arbeitet das Netzwerk mit möglichst großen Datenrahmen. Bei Echtzeit-Applikationen teilt sich das Feld. Video-Übertragungen nutzen ähnlich den Dateitransfers relativ große Datenrahmen. Voice-over-IP bewegt sich dagegen im Mittelfeld. Messungen mit Ethernet-LAN-Phones der ersten Generation in unseren Real-World Labs haben beispielsweise ergeben, dass diese Voice-over-IP-Lösung die Sprache mit konstant großen Rahmen von 534 Byte überträgt, ein aktuelles SIP-Phone überträgt 214 Byte große Rahmen.

Aktuelle Lösungen überlassen es dem IT-Verantwortlichen selbst festzulegen, mit welchen Frame-Größen die Systeme arbeiten sollen. Dabei sollte der IT-Verantwortliche berücksichtigen, dass der Paketierungs-Delay mit kleiner werdenden Datenrahmen kleiner wird. Dagegen wächst der Overhead, der zu Lasten der Nutzdatenperformance geht, je kleiner die verwendeten Pakete sind. Generell kann man bei der IP-Sprachübertragung davon ausgehen, dass kleine Frames verwendet werden. Die meisten Web-Anwendungen nutzen mittelgroße Datenrahmen. Die kleinstmöglichen Frames von 64 Byte sind dagegen beispielsweise bei den TCP-Bestätigungspaketen oder interaktiven Anwendungen wie Terminalsitzungen zu messen.

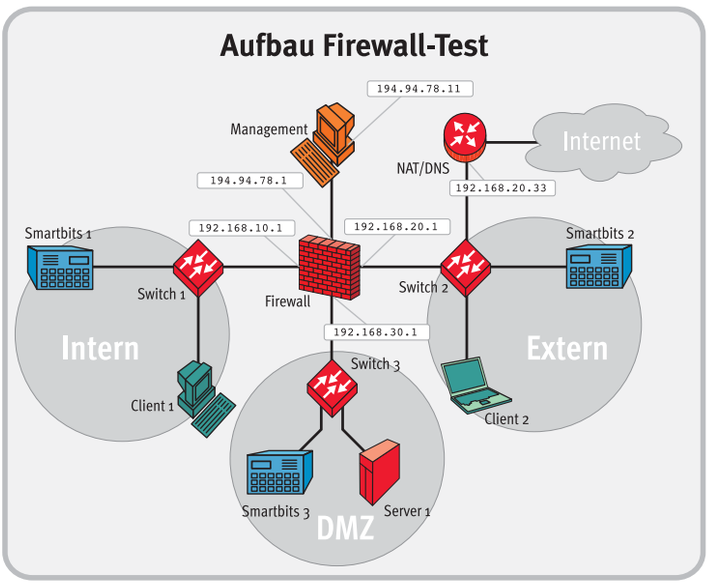
Die Analyse der Verteilung der Framegrößen, die für das NCI-Backbone dokumentiert ist, sowie die Ergebnisse der Analyse typischer Business-DSL-Links haben ergeben, dass rund 50 Prozent aller Datenrahmen in realen Netzwerken 64 Byte groß sind. Die übrigen rund 50 Prozent der zu transportierenden Datenrahmen streuen über alle Rahmengrößen von 128 bis 1518 Byte. Für die Übertragung von Real-Time-Applikationen ist zunächst das Datenverlustverhalten von entscheidender Bedeutung. Für Voice-over-IP gilt beispielsweise: Ab 5 Prozent Verlust ist je nach Codec mit deutlicher Verschlechterung der Übertragungsqualität zu rechnen, 10 Prozent führen zu einer massiven Beeinträchtigung, ab 20 Prozent Datenverlust ist beispielsweise die Telefonie definitiv nicht mehr möglich. So verringert sich der R-Wert für die Sprachqualität gemäß E-Modell nach ITU G.107 schon bei 10 Prozent Datenverlust um je nach Codec 25 bis weit über 40 Punkte, also Werte, die massive Probleme im Telefoniebereich sehr wahrscheinlich machen. Auf Grund ihrer Bedeutung für die Übertragungsqualität haben wir daher das Datenrahmenverlustverhalten als K.O.-Kriterium für unsere Tests definiert. Die Parameter Latency und Jitter sind dann für die genauere Diagnose und weitere Analyse im Einzelfall wichtig. Sind jedoch die Datenverlustraten von Hause aus schon zu hoch beziehungsweise die maximal möglichen Durchsätze zu gering, können gute Werte für Latency und Jitter die Sprachqualität auch nicht

mehr retten. Dafür, dass es zu solchen massiven Datenverlusten im Ethernet-LAN erst gar nicht kommt, sollen entsprechend gut funktionierende Priorisierungsmechanismen sorgen. Bei entsprechender Überlast im Netz sind Datenverluste ganz normal, jedoch sollen sie durch die Priorisierungsmechanismen in der Regel auf nicht echtzeitfähige Applikationen verlagert werden. Arbeitet diese Priorisierung nicht ausreichend, kommt es auch im Bereich der höher priorisierten Daten zu unerwünschten Verlusten. Dieses Priorisierungsverhalten wird Thema eines unserer nächsten Firewall- und VPN-Tests sein. So lange die Netzwerkkomponenten nicht mit Wirespeed arbeiten, bringen Priorisierungsverfahren aber keine Qualitätsgarantie, deshalb haben wir bisher auf Prioritätsmessungen bei Firewalls verzichtet.

Testverfahren

Insgesamt haben wir vier Firewall-Testreihen durchgeführt. In der ersten Testreihe haben wir unidirektional von der DMZ in das interne Netz gesendet und jeweils einen UDP-Port adressiert. In der zweiten Testreihe haben wir dann mit bidirektionalem Datenverkehr gearbeitet und parallel in beiden Richtungen zwischen dem internen Netz und der DMZ Datenströme gesendet. Bei beiden Testreihen haben wir mit einer Eingangslast von 10 Prozent begonnen und die Last dann in 10-Prozent-Schritten bis auf 100 Prozent erhöht.

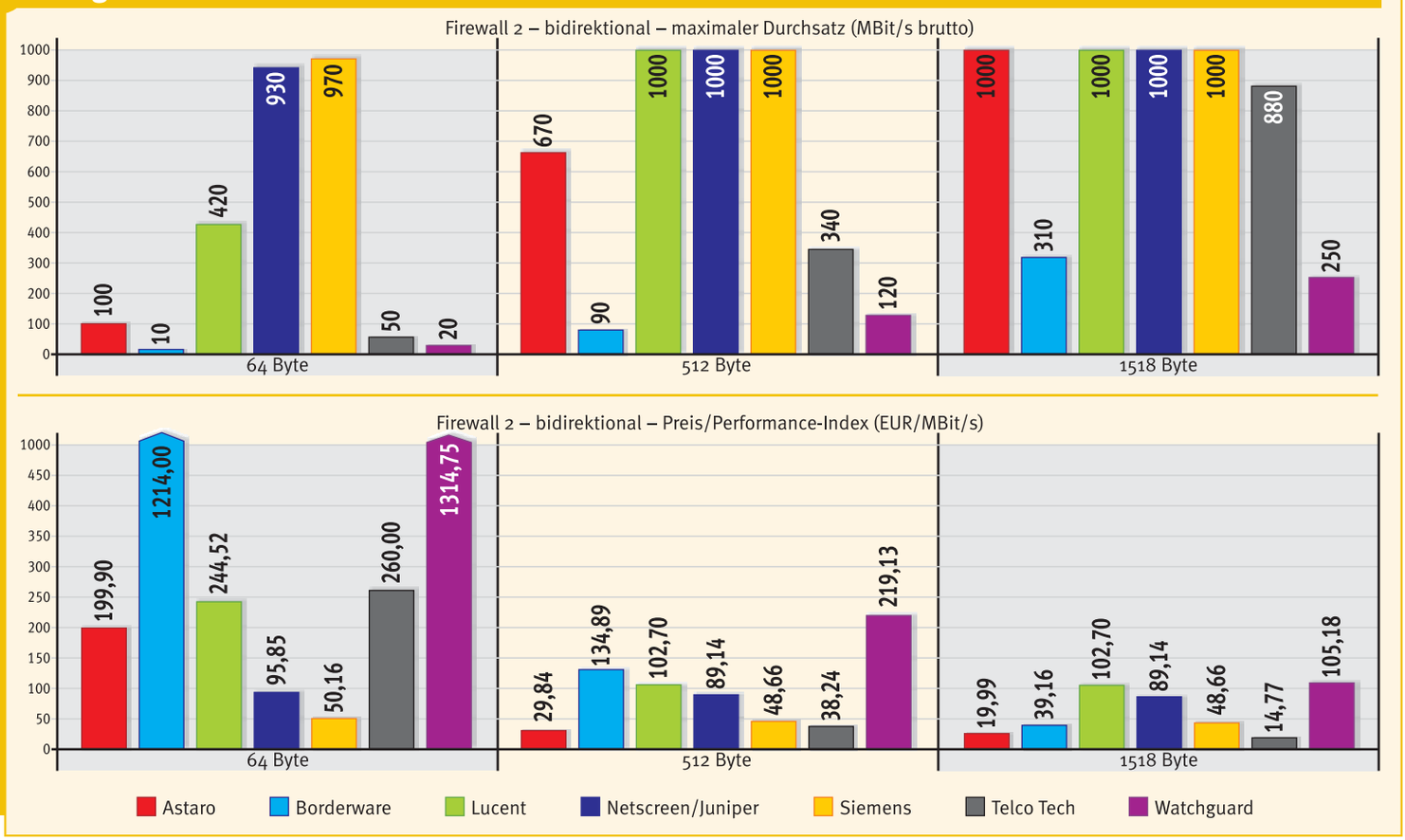
In der dritten Messreihe haben wir mit einem vermaschten Testaufbau nach dem Many-to-Many-Setup gearbeitet. Hierbei senden die Smartbits-Lastgeratoren aus jedem Segment – dem internen Netz, dem externen Netz und der DMZ – in die beiden anderen Segmente. Dort erfassen die Smartbits-Analysatoren die Datenströme und werten sie aus. In diesem Szenario arbeiten alle Ports wieder bidirektional, da die sendenden Ports ihre Last jeweils auf zwei Datenströme an die beiden anderen Segmente aufteilen müssen, beträgt hier die Last per Flow maximal 50 Prozent, die Last per Ausgangs- wie per Eingangs-Port kommt auf maximal 100 Prozent. Bei dieser Messreihe haben wir mit einer Eingangslast von 5 Prozent pro Flow begonnen und dann in 5-Prozent-Schritten bis auf 50 Prozent erhöht.



In der vierten Messreihe haben wir wie in der ersten Messreihe einen unidirektionalen Datenstrom von der DMZ ins interne Netzwerk generiert und mit einer schrittweise ansteigenden Last von 10 bis 100 Prozent gearbeitet. Zusätzlich haben wir Datenströme mit jeweils 5 Prozent Stör-Traffic erzeugt und diese unidirektional vom externen Netz in die DMZ und in das interne Netz gesendet. Diese Datenströme sollten geblockt werden. Ein Vergleich mit den Messungen der ersten Reihe zeigt dann, ob das jeweilige System im Test sich in der Performance vom Stör-Traffic beeinflussen lässt.

Außerdem haben wir für jede Messreihe neben den standardisierten, in immer gleichen Lastschritten erfolgenden Verlustratenmessungen für jedes System und jede Framegröße den Punkt der optimalen Last und somit die maximalen technisch möglichen Durchsatzrate unter optimalen Bedingungen ermittelt. Hierzu haben wir mit Laststeigerungen in Ein-Prozent-Schritten im betroffenen Zehn-Prozent-Intervall festge-

Messergebnisse – Firewall-Performance



stellt, bei welcher Last die jeweilige Appliance gerade noch keine oder präziser gesagt kleiner 1 Prozent der Daten verliert. Die hierbei erzielbaren Werte liegen in der Regel deutlich über dem Datendurchsatz bei Volllast. Die Durchsatzraten haben wir aus den Datenverlustraten errechnet und in Mittelwerten der entsprechenden Flows je Port und Senderichtung in MBit/s angegeben. Wirespeed ist in unserer Darstellung daher ein Bruttodurchsatz von 1 GBit/s. Bidirektional liegen dann natürlich maximal 2 GBit/s an.

Verhalten der Systeme im Test

Astaros Sun-Fire-V20z-Opteron mit Astaro-Security-Linux V5 erreichte bei der unidirektionalen Messung mit 64-Byte-Frames einen maximalen Datendurchsatz von 170 MBit/s, unter Volllast lagen dann noch rund 165 MBit/s, was eine Datenverlustrate von rund 84 Prozent bedeutet. Im bidirektionalen Betrieb blieben davon dann noch rund 100 MBit/s je Senderichtung übrig, eine Leistung, die gerade Fast-Ethernet-Wirespeed entspricht. Im multidirektionalen Betrieb mit 64-Byte-Paketen gingen die Durchsatzraten noch weiter zurück, so dass hier maximal rund 60 MBit/s möglich waren. Mit größeren Datenrahmen kam die Astaro-Appliance dann deutlich besser zurecht. So schaffte sie im unidirektionalen Setup mit 512- und 1518-Byte-Paketen Wirespeed. Die volle Bandbreite von Gigabit-Ethernet stand dann auch bidirektional bei den Messungen mit 1518-Byte-Paketen unter optimalen Bedingungen zur Verfügung. Multidirektional lagen bei der Messung mit den großen Datenrahmen noch 840 MBit/s an. Mit 512 Byte großen Frames waren dann noch Durchsätze von bidirektional 670 und multidirektional 370 MBit/s je Senderichtung möglich. Der Einfluss durch Störtraffic war zwar spürbar, hielt sich aber im Vergleich zu anderen Systemen im Testfeld noch in Grenzen. Trotz der deutlichen Schwäche im 64-Byte-Bereich zeigte die Astaro-Appliance im Testfeld insgesamt eine passable Leistung, die in Anbetracht des vergleichsweise geringen Preises für die Preis-Leistungs-Auszeichnung von Network Computing reicht.

Borderwares Steelgate-Appliance erwies sich schon in den anspruchslosesten Messungen unserer Szenarien als überfordert und blieb deutlich hinter den Leistungen der Astaro-Appliance zurück. So kam das preislich recht günstige Borderware-System bei den unidirektionalen Messungen mit 64-Byte-Paketen auf einen Maximaldurchsatz von 30 MBit/s, mit 512-Byte-Paketen lag eine Geschwindigkeit von 190 MBit/s und mit dem größten Frame-Format schaffte das System 480 MBit/s. Unter Volllast gingen die möglichen Durchsatzraten dann noch weiter zurück, so dass die Firewall dann bei den Messungen mit 64-Byte-Paketen praktisch völlig dicht machte. Bei den Messungen mit bi- und multidirektionalen Datenströmen ging die Performance dann – wie zu erwarten war – noch weiter zurück, so dass die Steelgate-Appliance beispielsweise multidirektional mit 512-Byte-Paketen noch einen Durchsatz von 50 MBit/s und mit 1518-Byte-Paketen von 160 MBit/s schaffte. Der Test der Steelgate-Appliance zeigt, dass es nicht viel bringt, wenn ein Hersteller seine Security-Appliance mit Gigabit-Ethernet-Adaptern aufrüstet, aber nicht für genügend Performance des Gesamtsystems sorgt. Im Testfeld der Fast-Ethernet-Systeme wäre das Borderware-System sicherlich besser aufgehoben, dann kann sich der IT-Verantwortliche aber auch gleich die Investition in Gigabit-Ethernet-Anschlüsse sparen.

Mit Lucent Technologies VPN-Firewall-Brick-1100 stand dann ein System in unseren Real-World Labs an der FH Stralsund, das sich nicht allzu deutlich in der Leistungscharakteristik von der Astaro-Lösung unterscheidet – Lucent bietet diese Leistung allerdings für den fünffachen Preis. Ob sie diesen wert ist, ist von der individuellen Bewertung aller gebotenen Features abhängig, die ein reiner Performance-Test nicht leisten kann. Stellte die Lucent-Firewall bei den unidirektionalen und bidirektionalen Messungen noch Wirespeed zur Verfügung, so erreichte sie ihre Grenzen bei den Messungen mit 64-Byte-Paketen und – dann auch mit größeren Paketen – im multidirektionalen Betrieb relativ schnell. So betrug hier der maximal erzielbare Durchsatz multidirektional mit 64-Byte-Paketen 270 MBit/s, mit 512- und 1518-Byte-Paketen waren

maximal 790 MBit/s möglich. Diese Werte lagen dann aber auch noch bei Volllast an. Echte Wirespeed bot das Lucent-System dann uni- wie bidirektional mit 512- und mit 1518-Byte-Paketen. Von Störtraffic ließ sich die Brick-1100 relativ wenig beeinflussen.

Mit der ISG-2000 schickte Netscreen, die nun zu Juniper gehört, ein echtes Highend-System ins Rennen, das auch in der Preisskala weit oben rangiert. Im Gegensatz zum noch teueren Lucent-System vermochte die Netscreen-Lösung aber gut in Sachen Performance zu überzeugen. Bei den Messungen mit unidirektionalen Datenströmen lag durchgehend Wirespeed an und auch im bidirektionalen Modus vermochte das System mit 930 MBit/s mit 64-Byte-Rahmen und mit 1 GBit/s mit den größeren Frames zu punkten. Hier war nur die Siemens/Checkpoint-Lösung noch etwas schneller. Dass auch aktuelle Highend-Systeme im multidirektionalen Test-Setup an ihre Grenzen stoßen, zeigten die anschließenden Messungen mit multidirektionalen Datenströmen. Hier kam die ISG-2000 mit 64-Byte-Paketen auf einen Bruttodurchsatz von 640 MBit/s je Senderichtung. Mit größeren Frames kam das Firewall-System von Netscreen/Juniper auch hier wieder besser zurecht, blieb aber mit Durchsatzraten von 950 MBit/s mit 512-Byte-Frames und mit 930 MBit/s mit 1518-Byte-Frames klar hinter der theoretischen Höchstgeschwindigkeit zurück. Durch Störtraffic ließ sich das Netscreen-System nicht nennenswert beeinträchtigen.

Siemens 4-Your-Safety-RX-300, die in ähnlicher Ausstattung bereits unseren letzten Gigabit-Ethernet-Firewall-Vergleichstest (siehe Network Computing 19/2003, S.12 ff.) für sich entscheiden konnte, bewährte sich auch in unserem aktuellen Vergleichstest und zog mit der ISG-2000 von Netscreen/Juniper in der Wertung gleich auf. Unidirektional lag in allen Fällen Wirespeed an, bidirektional lag das Siemens-System bei der Messung mit 64-Byte-Paketen mit einem Durchsatz von 970 MBit/s noch vor der ISG-2000. Mit größeren Frames lieferte die RX-300 dann wieder den vollen Gigabit-Etherent-Durchsatz. Ihre technischen Grenzen zeigte auch die Siemens-Checkpoint-Lösung analog zur ISG-2000 bei den Messungen mit multidirektionalem Datenverkehr. Auch hier lieferte sich die RX-300 ein Kopf-an-Kopf-Rennen mit dem Netsceen-System. Je Senderichtung lagen bei diesen Messungen je nach Format der verwendeten Frames zwischen 650 und 940 MBit/s. Dass die RX-300 sich auch bezüglich Störtraffic unbeirrbar zeigte, verwundert vor diesem Hintergrund kaum.

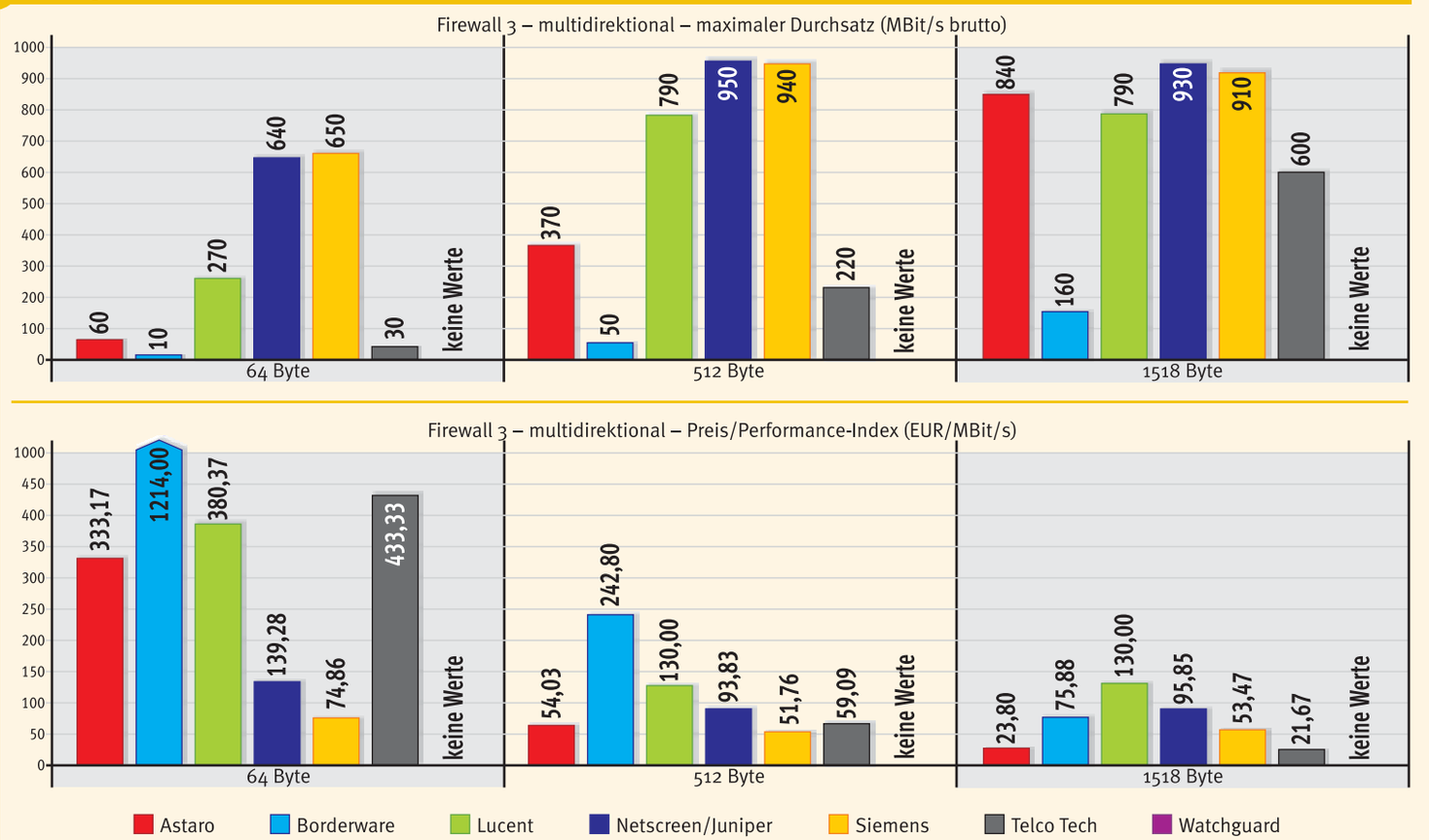
Telco Techs Liss-II vermochte dagegen in unserem Szenario nicht zu überzeugen. Wirespeed lieferte das System nur bei der Messung mit unidirektionalen Datenströmen und 1518 Byte großen Datenrahmen. Wurden die Frames kleiner, dann ging auch der Datendurchsatz spürbar zurück. So schaffte die Liss-II bei der Messung mit 64-Byte-Paketen gerade mal 100 MBit/s, also Fast-Ethernet-Wirespeed. Im bidirektionalen Betrieb und noch deutlicher im multidirektionalen Betrieb ging die Leistung der Liss-II dann weiter zurück. So schaffte das System multidirektional mit 64-Byte-Paketen gerade 30 MBit/s. Mit 1518-Byte-Paketen erreichte sie dagegen multidirektional noch akzeptable 600 MBit/s. Gegenüber Störtraffic erwies sich die Liss-II als relativ empfindlich, so ging beispielsweise die Leistung um weitere 150 MBit/s bei der Messung mit 512-Byte-Paketen zurück, wenn Störtraffic das System belastete.

Auch Watchguards Firebox-Vclass-V100 vermochte nicht zu überzeugen. Maximal waren uni- wie bidirektional 250 MBit/s bei den Messungen mit den größten Datenrahmen drin. Waren die Frames kleiner, gingen auch hier wieder die Durchsatzleitungen zurück. So schaffte die aktuelle Firebox im Testfeld noch einen Durchsatz von 20 MBit/s bei der Messung mit 64-Byte-Paketen. Die Messung mit multidirektionalem Datenverkehr war nicht möglich, da ein Testsystem schadhaft war und das andere nur über zwei Gigabit-Ethernet-Interfaces verfügte.

Fazit

Als performanteste Systeme im Testfeld der Gigabit-Ethernet-Firewall-Appliances haben sich die Siemens- und die Netscreen-Systeme erwiesen. Auch wenn diese Highend-Systeme noch nicht generell Gigabit-Ethernet-Wirespeed garantieren, sie bieten doch schon Durchsatzraten, die den Einsatz von Gigabit-Ethernet-Security-Appliances in den entsprechenden Szenarien sinn-

Messergebnisse – Firewall-Performance



Features

Firewall-Appliances

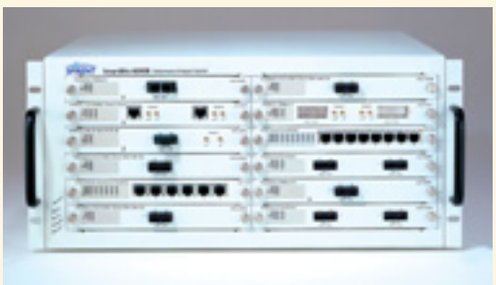
	Astaro Sun Fire V20z Server	Borderware Steelgate	Lucent VPN Firewall Brick 1100	Netscreen ISG 2000	Siemens/Check Point 4YourSafety/Check Point VPN-1/FireWall-1	Telco Tech LiSS II secure gateway pro giga	Watchguard Firebox Vclass V100
Anzahl unabhängiger (nicht geswitchter) LAN-Ports							
Anzahl Gigabit-Ethernet-Ports	6	6	4	8	5	6	2
Anzahl Fast-Ethernet-Ports	–	6	7	28	–	–	2 (für High Availability)
Anzahl WAN-Ports							
PPoE auf LAN-Port(s)	6	1	●	–	●	1	–
X.21	–	–	–	–	–	–	–
X.25	–	–	–	–	–	–	–
ISDN $_{S0}$	–	–	–	–	–	–	–
ISDN $_{S2M}$	–	–	–	–	–	–	–
xDSL	–	–	–	–	●	–	–
E1	–	–	–	–	–	–	–
Sonstige (Angabe Typ)	k.A.	k.A.	k.A.	k.A.	k.A.	k.A.	k.A.
Hardware/Betriebssystem							
Prozessor	AMD Opteron 1800	3000 MHz	2.4 GHz	Dual Power PC 1000Mhz	P4 Xeon 2.4 Ghz.	Intel Xeon 2800 MHz	CPU 850 MHz PIII, 2x RapidCore 66 Mhz
Arbeitsspeicher in MByte	2048	2000	2000	1000	512	512	128 MB Flash, 512 DRAM
Betriebssystem Name/Version	Astaro Security Linux V5 - 64 Bit Controlled Release	Score (eigenes)	Inferno OS / LSMS Version 7.1	Screen OS 5.0	Linux Secure Platform	prop., linuxbasiert Version 2.8.1	eigenes OS, inuxbasiert Version 5.1.1
IPv6-Unterstützung für alle Firewall-Funktionen	○	○	○	●	●	○	○
Firewall-Technik							
Stateful-Inspection-Firewall	●	●	●	●	●	●	●
Layer-7-Application-Gateway-Proxies	●	●	●	●	●	●	●
anpassbare Proxies	●	●	○	●	●	●	●
Stateful-Inspection und Proxy kombiniert	●	●	●	●	●	●	●
transparente Firewallfunktionalität konfigurierbar	○	●	●	●	●	○	●
spezielle Firewall-ASICs integriert	○	○	● (Hardware Appliance)	●	○	○	●
Netzwerkprozessor mit Firewall Teilfunktionen auf NIC	○	○	● (Hardware Appliance)	○	●	○	○
VPN-Protokolle							
L2TP	●	○	○	●	●	○	○
PPTP	●	●	○	○	○	○	○
Secure-Socket-Layer/TLS	○	○	○	○	●	○	○
IPSec über X.509/IKE	●	●	●	●	●	●	●
Routing-Protokolle							
RIPv1	○	○	○	○	●	○	●
RIPv2	○	○	○	●	●	○	●
OSPF	○	○	○	●	●	○	●
BGP-4	○	○	○	●	○	○	●
Cluster							
Maximale Clustergröße (Zahl der Systeme)	–	offen	2	2	8	unbegrenzt	2
Cluster über 3-Party-Software etabliert	○	eigene	○	○	●	○	○
Cluster über externen Load-Balancer-Switch	●	●	○	○	●	●	○
Cluster über Netzwerk-Links etabliert	○	●	●	●	●	○	●
Management							
Telnet	○	○	○	●	●	○	●
rollenbasierte Verwaltung	○	○	●	●	●	●	●
Auditing-fähig	●	○	●	●	●	●	●
SSH-Support für CLI	●	●	○	●	●	○	●
HTTP/S	●	●	○	●	●	●	●
automatische Synchronisierung im Cluster	○	●	●	●	●	○	●
Synchronisierung über multiple Pfade möglich	○	●	●	●	●	○	○
Out-Band-Management	●	serielle Console	●	●	●	●	●
Monitoring							
CPU überwacht	●	●	●	●	●	●	●
Speicherauslastung gemessen	●	●	●	●	●	●	●
Port-Auslastung gemessen	●	○	●	●	●	○	●
Synchronisierung überwacht	●	○	●	●	●	●	●
die Firewall-Software wird überwacht	●	●	●	●	●	●	●
Schwellenwerte für Auslastung möglich	○	○	●	●	●	○	●
Logging-Daten und -Events							
per SNMP exportiert	○	●	●	●	●	○	●
per WELF-Format exportiert	○	○	●	●	○	○	●
an Syslog-Server exportieren	●	●	●	●	●	●	●
Events zentralisiert	●	●	●	●	●	●	●
Event-Management korelliert einzelne Einträge	○	○	●	●	●	●	●
Authentisierung/Autorisierung							
NT-Domain	●	●	○	●	●	○	○
TACACS/TACACS+	○	○	○	○	●	○	○
Radius	●	●	●	●	●	○	●
LDAP über TLS	○	●	●	○	●	○	○
X.509-digitale Zertifkate	●	●	●	●	●	○	●
Token-basierend	●	●	●	●	●	○	●
Sicherheitsfeatures							
DMZ	●	●	●	●	●	●	●
Intrusion-Detection/-Prevention	●	○	●	●	●	●	●
AAA-Support	●	○	●	●	●	●	○
DHCP	●	●	●	●	●	●	●
NAT-Support	●	●	●	●	●	●	●
Content-Filter	●	●	●	●	●	●	●
Virenscanner	●	○	●	●	●	●	○
Website	www.astaro.com	www.borderware.de	www.lucent.com/security	www.netscreen.com	www.checkpoint.com www.4ys.de	www.telco-tech.de	www.watchguard.com
Listenpreis in Euro für Teststellung zzgl. MwSt.	19 990	12 140	102 700	89 140	48657,24	13 000	26 295

ja = ●; nein = ○; k.A. = keine Angabe;

Info

So testete Network Computing

Als Lastgenerator/Analysator haben wir in unseren Real-World Labs den bekannten »Smartbits 6000B« von Spirent eingesetzt. Das in dieser Konfiguration gut 250 000 Euro teuere Gerät war mit der Software »Smartflow 3.10« ausgestattet und mit 24 Fast-Ethernet-Ports sowie vier Kupfer- und fünf Multimode-LWL-Gigabit-Ethernet-Ports bestückt. Alle Ports arbeiten im Full-Duplex-Modus und können somit gleichzeitig Last mit Wirespeed generieren und analysieren.



Um vergleichbare, gültige und aussagefähige Ergebnisse zu erzielen, haben wir im Vorfeld die Einstellungen der Firewalls festgelegt und ein für alle Firewall-Tests verbindliches Standard-Rule-Set vorgegeben. Für die korrekte Konfiguration haben wir gemeinsam mit den Ingenieuren des jeweiligen Herstellers gesorgt, die ihr eigenes System im Test begleitet haben.

Zur Ermittlung des Datenrahmenverlustverhaltens haben wir mit dem Smartbits-Lastgenerator/Analysator Datenströme generiert und diese unidirektional beziehungsweise bidirektional mit verschiedenen Paketgrößen gesendet. Die Eingangslast haben wir in regelmäßigen 10-Prozent-Schritten bis auf Volllast erhöht. Lagen die ermittelten Performance-Werte unter der minimalen Eingangslast oder tauchten andere Unregelmäßigkeiten auf, haben wir weitere Detail-Messungen in 1-Prozent-Schritten durchgeführt, um die Leistungsgrenze beziehungsweise das Problem zu analysieren.

Nacheinander haben wir vier Firewall-Testreihen durchgeführt. In der ersten Testreihe haben wir unidirektional von der DMZ in das interne Netz gesendet und jeweils einen UDP-Port adressiert. In der zweiten Testreihe haben wir dann mit bidirektionalem Datenverkehr gearbeitet und parallel in beiden Richtungen zwischen dem internen Netz und der DMZ Datenströme gesendet. Bei beiden Testreihen haben wir mit einer Eingangslast von 10 Prozent begonnen und die Last dann in 10-Prozent-Schritten bis auf 100 Prozent erhöht.

In der dritten Messreihe haben wir mit einem vermaschten Testaufbau nach dem Many-to-Many-Setup gearbeitet. Hierbei senden die Smartbits-Lastgeratoren aus jedem Segment – dem internen Netz, dem externen Netz und der DMZ – in die beiden anderen Segmente. Dort erfassen die Smartbits-Analysatoren die Datenströme und werten sie aus. In diesem Szenario arbeiten alle Ports wieder bidirektional, da die sendenden Ports ihre Last jeweils auf zwei Datenströme an die beiden anderen Segmente aufteilen müssen, beträgt hier die Last per Flow maximal 50 Prozent, die Last per Ausgangs- wie per Eingangs-Port kommt auf maximal 100 Prozent. Bei dieser Messreihe haben wir mit einer Eingansglast von 5 Prozent pro Flow begonnen und dann in 5-Prozent-Schritten bis auf 50 Prozent erhöht.

In der vierten Messreihe haben wir wie in der ersten Messreihe einen unidirektionalen Datenstrom von der DMZ ins interne Netzwerk generiert und mit einer schrittweise ansteigenden Last von 10 bis 100 Prozent gearbeitet. Zusätzlich haben wir Datenströme mit jeweils 5 Prozent Stör-Traffic erzeugt und diese unidirektional vom externen Netz in die DMZ und in das interne Netz gesendet. Diese Datenströme sollten durch die Firewall per Regel geblockt werden. Ein Vergleich mit den Messungen der ersten Reihe zeigt dann, ob das jeweilige System im Test sich in der Performance vom Stör-Traffic beeinflussen lässt.

Der Smartbits-Lastgenerator/Analysator hat die empfangenen Datenströme auf die eingestellten Parameter hin untersucht und die gemessenen Ergebnisse gesichert. Aus den ermittelten Datenverlustraten lässt sich dann rechnerisch die maximal erzielbare Bandbreite in den einzelnen Szenarien ermitteln und in ein Preis-Leistungs-Verhältnis setzen.

Die Performance-Messungen haben wir ausschließlich mit UDP-Paketen durchgeführt, weil sich hierbei im Gegensatz zu TCP-Datenströmen Eigenschaften des Protokolls wie Retransmisson nicht auf das Verhalten der Systeme auswirken. Die Datenströme setzten sich aus jeweils homogenen Frame-Größen zusammen. Wie haben für die einzelnen Tests Datenrahmen der Größen 64, 512, 1024 und 1518 Byte verwendet.

Die einzelnen Netzsegmente haben wir über LAN-Switches vom Typ »Extreme Networks Summit 48si« realisiert. Diese Systeme leisteten in den den einzelnen Tests vorhergehenden Kontrollmessungen volle Wirespeed und sind aus diesem Grund in Hinsicht auf das Datenrahmenverlustverhalten des Testaufbaus vollständig transparent. Mit Hilfe der drei Linux-Intel-PC-Clients in den einzelnen Netzsegmenten haben wir die korrekte Firewall-Konfiguration und -Funktion jeweils vor den einzelnen Testläufen überprüft.

Die Durchsatzraten haben wir aus den Datenverlustraten errechnet und in Mittelwerten der entsprechenden Flows je Port und Senderichtung in MBit/s angegeben. Wirespeed ist in unserer Darstellung daher ein Bruttodurchsatz von 1 GBit/s. Bidirektional liegen dann natürlich maximal 2 GBit/s an.

voll machen. Diese Performance hat allerdings nach wie vor ihren Preis. Dabei liegt die RX-300 von Siemens im Preis-Leistungsverhältnis klar vor der Netscreen/Juniper-Lösung, die das RX-300-Potential zu einem deutlich höheren Listenpreis offeriert.

Akzeptable Leistung für viel Geld bietet Lucent mit ihrer Brick-1100. Entwicklungsbedarf hat Lucent im direkten Vergleich mit den beiden Testsiegern im Bereich der Verarbeitung kleiner Frames. Auch im multidirektionalen Betrieb blieb die Brick dann deutlich hinter den besser platzierten Systemen zurück. Im direkten Vergleich mit der Brick-1100 noch etwas ausgeprägtere Schwächen zeigte die Astaro-Lösung, die aber zu einem um den Faktor 5 gegenüber der Lucent-Lösung oder den Faktor 2,5 gegenüber dem Siemens-System günstigeren Preis zu haben ist. Aus diesem Grund haben wir Astaro auch die Preis-Leistungs-Auszeichnung verliehen. Wer aber ultimative Leistung fordert, der kommt an unseren beiden Testsiegern nicht vorbei – Performance hat im Segment der Security-Appliances halt ihren Preis, da sie leistungsfähige Hardware voraussetzt.

Die schlechter platzierten Systeme von Telco Tech und Borderware zeigen, dass in vielen Fällen für weniger Geld auch weniger Performance geboten wird, da reicht es auch nicht, wenn die Systeme mit Gigabit-Ethernet-Schnittstellen ausgestattet werden. Um wirklich in Gigabit-Regionen vorstoßen zu können, ist deutlich leistungsfähigere und teils spezialisierte Hardware wie Beschleunigerkarten erforderlich. Das heißt natürlich nicht, dass die letztgenannten Systeme für Szenarien, die weniger Performance erfordern, ungeeignet sind. Dann stellt sich allerdings die Frage, ob nicht auch preisgünstige Fast-Ethernet-Lösungen ausreichen. Enttäuschend war auch die Leistung des Watchguard-Systems, das deutlich hinter den Anforderungen zurück blieb. Hier besteht noch deutlicher Entwicklungsbedarf.

Dass die Firewall-Appliances im Bereich der kleinsten Pakete und bei größeren Paketen bei bi- oder multidirektionalem Datenverkehr als erstes schwächeln, war zu erwarten, da sie hier deutlich mehr Header lesen und Rechenarbeit leisten müssen, als bei großen Paketen. Richtig problematisch würde der Einsatz mehr oder weniger aller Systeme im Testfeld, wenn große Datenmengen mit kleinen Paketen zu erwarten sind und Gigabit-Ethernet-Wirespeed erforderlich ist. Dabei ist zu beachten, dass in den meisten realen Netzwerken 64-Byte-Pakete rund 50 Prozent der Gesamtzahl an Datenpaketen ausmachen, die diese Netze zu bewältigen haben. Für Anwendungen mit großen Datenrahmen, wie den meisten klassischen Datenanwendungen oder der Übertragung von Video-Streams sind weniger Probleme zu erwarten. Soll aber beispielsweise ein größeres Call-Center mit Voice-over-IP durch eine Firewall hindurch telefonieren, dann ist der IT-Verantwortliche gut beraten, wenn er für die Performance seiner Firewall ohne vorhergehende Analysen, Lastprognosen und fundierte Tests keinesfalls Wirespeed unterstellt.

Dipl.-Ing. Thomas Rottenau,
Prof. Dr. Bernhard G. Stütz, [dg]