11 Fast-Ethernet-Firewall-Appliances

Rasant durch die Feuerwand

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

Eine sichere, aber auch schnelle Kommunikation zwischen einem internen Netzwerk – beispielsweise einem 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 auf Ethernet basierende 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 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 und der Leistungsfähigkeit der übrigen Komponenten im Netz erhöht dieses Anwendungsszenario deutlich die Anforderungen an Firewall-Systeme im Hinblick auf Performance und Funktionalität. Angesichts dieser Situation sind auch Durchsatzraten im Gigabit-Bereich durchaus sinnvoll und die Implementierung von Gigabit-Ethernet-Technologie ist eine logische Konsequenz. Die Anforderungen an die Leistungsfähigkeit solcher Firewalls entsprechen 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

Reportcard / interaktiv unter www.networkcomputing.de

Firewall-Performance

	Gewichtung	Clavister M 460	Bintec VPN Access 1000	Sonicwall Pro 3060	Astaro timeNET secuRACK	Lucent Brick 350	Cisco PIX 515E	Bintec VPN Access 25	Gateprotect gateProtect Firewall	Zyxel ZyWALL 70	D-Link DFL-700	Innominate mGUard
Max. Durchsatz 64 Byte unidirektional	10%	5	5	3	2	1	1	1	1	1	1	1
Max. Durchsatz 512 Byte unidirektional	10%	5	5	5	5	5	5	5	5	1	1	4
Max. Durchsatz 1518 Byte unidirektional	10%	5	5	5	5	5	5	5	5	5	1	5
Max. Durchsatz 64 Byte bidirektional	10%	5	1	1	1	1	1	1	1	1	1	1
Max. Durchsatz 512 Byte bidirektional	10%	5	5	5	5	5	5	5	3	1	1	1
Max. Durchsatz 1518 Byte bidirektional	10%	5	5	5	5	5	5	5	5	1	1	5
Max. Durchsatz 64 Byte many to many	10%	5	1	1	1	1	1	1	1	1	1	–
Max. Durchsatz 512 Byte many to many	10%	5	5	5	5	5	3	3	1	1	1	–
Max. Durchsatz 1518 Byte many to many	10%	5	5	5	5	5	4	4	4	1	1	–
Einfluss durch Stör-Traffic	10%	5	5	4	4	5	5	4	3	5	3	–
Gesamtergebnis	100%	5	4,2	3,9	3,8	3,8	3,5	3,4	2,9	1,8	1,2	–*)
		A+	B+	B	B	B	B-	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: >= 95 MBit/s = 5; >= 90 MBit/s = 4; >= 80 MBit/s = 3; >= 70 MBit/s = 2; <= 70 MBit/s = 1;
Bewertungsschlüssel für den Einfluss durch Stör-Traffic: >= 30 MBit/s = 1; >= 20 MBit/s = 2; >= 10 MBit/s = 3; >= 5 MBit/s = 4; <= 5 MBit/s = 5;
*) = Messungen zum Teil nicht möglich, da System mit nur 2 Fast-Ethernet-Ports 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 SG-200
Lucent	VPN Firewall Brick 1100
Netscreen	ISG 2000
Siemens/ Check Point	Four your Safety RX 300
Telco Tech	LiSS II secure gateway pro giga
Watchguard	Firebox Vclass V100

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 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 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 nach den vorhandenen LAN-Ports in Fast-Ethernet- und Gigabit-Ethernet-Systeme eingeteilt.

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-Performance-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 sollten.

Aus diesem Pflichtenheft ergaben sich folgende Anforderungen an die Teststellungen:

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

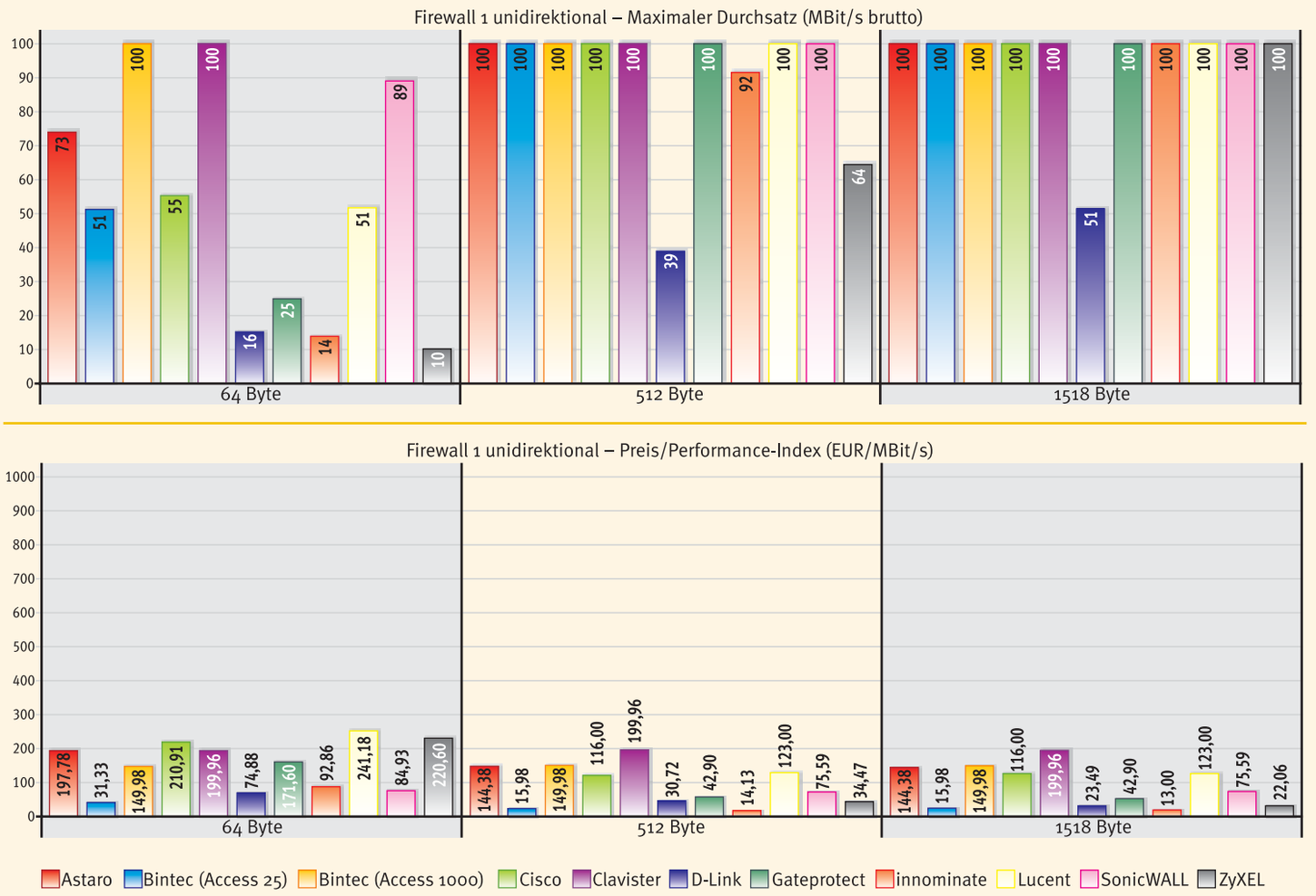
Messen wollten wir die Firewall-Performance, also die unidirektionalen und bidirektionalen Datendurchsatzraten im Firewall-Betrieb, die sich aus den Datenverlustraten unter Last ergibt. Als weitere Parameter haben wir Latency sowie Jitter unter Last ermittelt. Als Test-Equipment dienten die Lastgeneratoren und -analysatoren Smartbits 6000B von Spirent 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 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 SG-200«, 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 Fast-Ethernet-Appliances in unserem Test verhielten, steht im hiermit vorliegenden Testbericht. Die Veröffentlichung der Ergebnisse der Gigabit-Ethernet-Appliances ist dann für die Ausgabe 10-11 2004 der Network Computing vorgesehen.

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

Messergebnisse – unidirektional

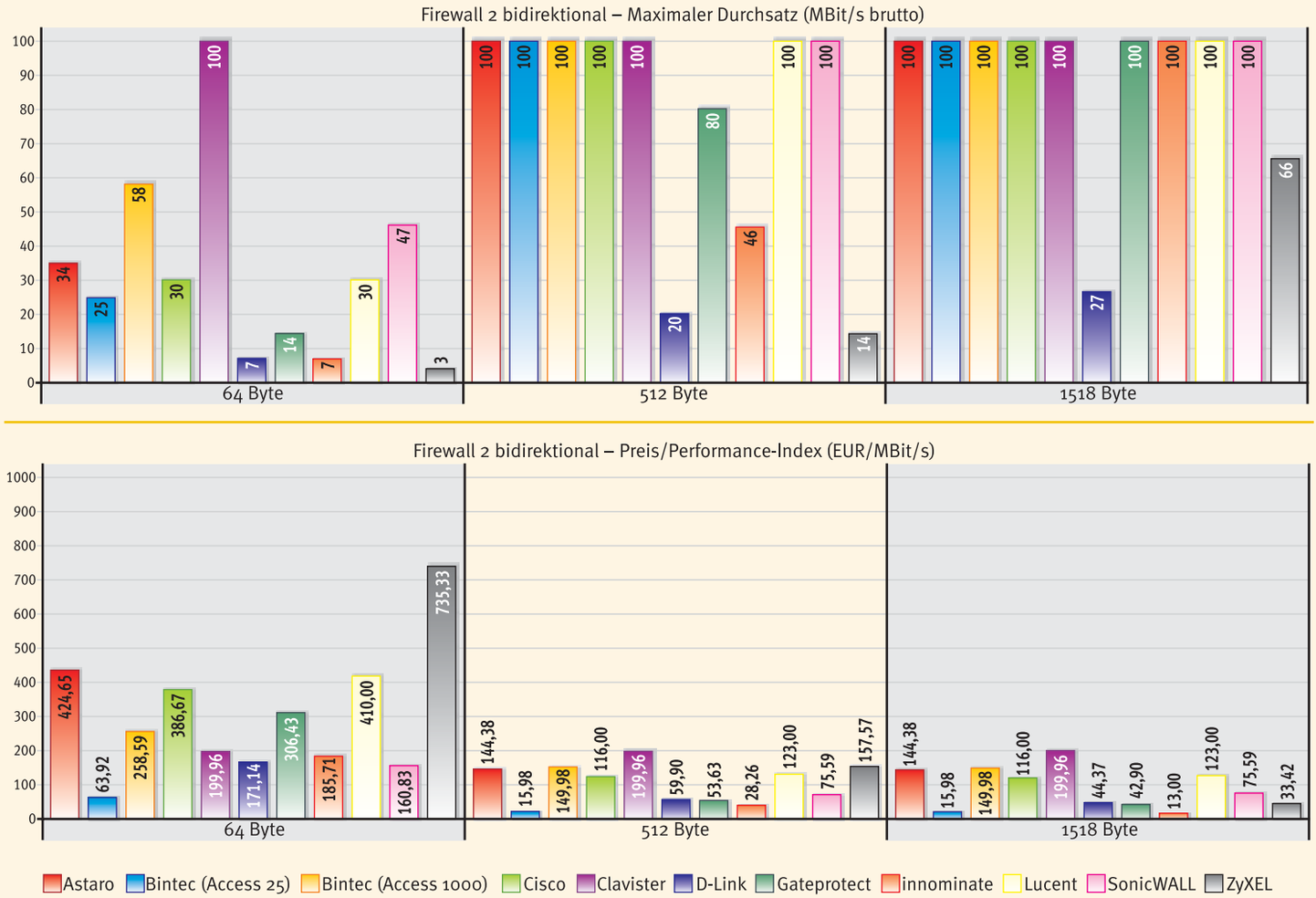


Rate von 100 Prozent oder im Fall des hier vorliegenden Tests 100 MBit/s. Bleibt die Appliance dagegen hinter Wirespeed zurück, dann ist bei einer entsprechenden Auslastung des übrigen Netzwerks davon auszugehen, das die überforderte Appliance für entsprechende Datenverluste sorgt, die diverse »Kommunikationsstörungen« 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-Applikatio-

Messergebnisse – bidirektional



nen 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.

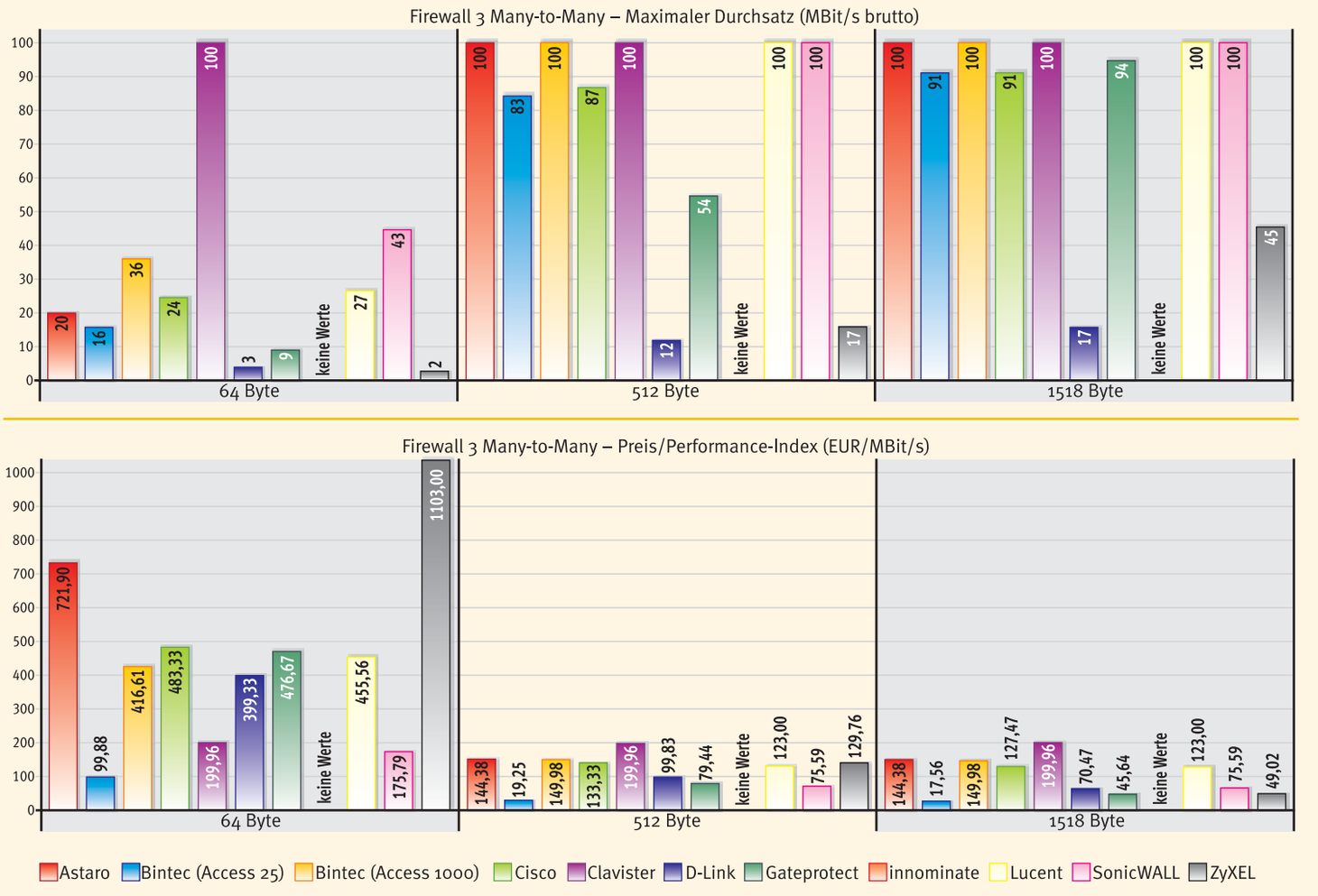
Aktuelle Lösungen überlassen es dem IT-Verantwortlichen selbst festzulegen, mit welchen Frame-Größen die Systeme arbeiten sollen. Dabei sollte der IT-Verantwortliche berücksichtigen, dass der Paketierungs-Delay mit kleiner werdenden Datenrahmen kleiner wird. Dagegen wächst der Overhead, der zu Lasten 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 mit bidirektionalem Verkehr gearbeitet und parallel in beiden Richtungen zwischen dem internen Netz und der DMZ Datenströme gesendet. Bei beiden Testreihen haben wir mit einer Eingangslast von

Messergebnisse – Many-to-Many



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 festgestellt, bei welcher Last die jeweilige Appliance gerade noch keine – oder präziser gesagt – teils unter einem Prozent der Daten verliert. Die hierbei erzielbaren Werte liegen 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 100 MBit/s. Bidirektional liegen dann natürlich maximal 200 MBit/s an.

Verhalten der Systeme im Test

Astaros Timenet-Securack-Enterprise-2 schaffte bei der Messung mit unidirektionalem Datenverkehr und 64-Byte-Paketen einen maximalen Durchsatz unter optimalen Bedingungen von 73 MBit/s. Bei weiter steigenden Lasten ging die Leistung dann noch ein wenig zurück, so dass der maximale Durchsatz bei Volllast des Systems noch gut 60 MBit/s betrug. Bei den Messungen mit größeren Frames und unidirektionalem Datenverkehr leistete das Astaro-System dann in allen Fällen Wirespeed. Schwerer tat sich die Timenet-Securack-Enterprise-2 bei den Messungen mit bidirektionalem Traffic und kleinen Frameformaten. So erreichte das System hier bei der Messung mit 64-Byte-Paketen noch einen maximalen Durchsatz von rund 34 Prozent. Unter Volllast machte die Appliance dann bei der Messung mit 64-Byte-Pakteten fast vollständig »dicht« und schaffte so gerade noch einen Durchsatz von rund 1,7 MBit/s. Mit größeren Frames hatte die Astaro-Firewall auch unter Volllast keine Probleme. Im Many-to-Many-Test mit 64-Byte-Paketen kam die Timenet-Securack-Enterprise-2 noch mehr in Stress und erreichte einen Maximaldurchsatz von 20 MBit/s. Bei Volllast blieb hier kein nennenswerter Durchsatz mehr übrig. Aber auch in der dritten Messreihe kam die Astaro-Appliance mit größeren Frame-Formaten recht gut zurecht. So betrug der Durchsatz bei Volllast mit 512-Byte-Frames gut 99 MBit/s und mit 1518-Byte-Frames volle 100 MBit/s. Als Maximaldurchsatz lag Wirespeed an. Bei unserer Messung des unidirektionalen Durchsatzes mit Stör-Traffic ließ sich die Timenet-Securack-Enterprise-2 lediglich wiederum bei der Messung mit 64-Byte-Paketen in ihrer Leistung vom Stör-Traffic beeinflussen, dieser reduzierte hier den Durchsatz um zusätzliche 9 MBit/s. Insgesamt zeigte die Timenet-Securack-Enterprise-2 recht ordentliche Durchsatzleistungen. Allerdings kann die Leistungsschwäche bei entsprechenden Lasten mit kleinen Frame-Formaten zu deutlichen Engpässen im Netz führen.

Bintecs VPN-Access-25 verhielt sich ähnlich wie das Astraro-System und schaffte bei allen Messungen mit 64-Byte-Paketen noch ein etwas weniger Durchsatz als das Astaro-System. So betrug der maximale unidirektionale Durchsatz mit 64-Byte-Paketen 51, bidirektional 25 und im Many-to-Many-Szenario noch 16 MBit/s. Diese Mindestdurchsätze blieben dann aber unter allen Umständen – auch bei Volllast – erhalten. An seine Grenzen geriet das kleine Bintec-System dann auch bei den Many-to-Many-Messungen mit größeren Datenrahmen. Hier betrugen die Maximalwerte 83 MBit/s bei 512 Byte und 91 MBit/s bei 1518 Byte. Unter Volllast gingen die Durchsätze hier dann noch leicht zurück, so dass die VPN-Access-25 hierbei in den gleichen Disziplinen noch Raten von knapp 82 beziehungsweise gut 65 MBit/s schaffte. Mit einer Verminderung des unidirektionalen Durchsatzes um 7 MBit/s bei der 64-Byte-Messung ließ sich das kleine Bintec-System im Test noch bisschen weniger beeinträchtigen als die Astaro-Firewall. Da Bintecs VPN-Access-25 zwar nicht immer Wirespeed, aber doch recht ordentliche und verlässliche Durchsatzleistungen in allen Lebenslagen bot – und das zu einem Preis, der um Größenordnungen unter denen beispielsweise von Astaro oder Cisco liegt –, ist uns diese Leistung schon die Preis-Leistungs-Auszeichnung von Network Computing wert.

Der »große Bruder« der VPN-Access-25, Bintecs VPN-Access-1000, konnte dann alles noch besser als die VPN-Access-25, was man ja

Features

Firewall-Appliances

	Astaro timeNET	Bintec VPN Access 25	Bintec VPN Access 1000	Cisco Systems Cisco PIX 515E	Clavister M460	D-Link DFL-700	gateProtect Firewall Server	Innominate mGUard	Lucent Brick 350	SonicWALL Pro 3060	ZyXEL ZyWALL 70
Anzahl unabh. (nicht geswitchter) LAN-Ports											
Anzahl Gigabit-Ethernet-Ports	2	–	–	–	–	–	–	–	1	–	–
Anzahl Fast-Ethernet-Ports	2	3	3	3	6	3	6	1	7	5	1
Anzahl WAN-Ports											
PPoE auf LAN-Port(s)	4	3	3	3	6	1	1	1	1	1	2
X.21	–	–	–	–	–	–	–	–	–	–	–
X.25	–	–	–	–	–	–	–	–	–	–	–
ISDN $_{S0}$	–	1	1	–	–	–	–	–	–	–	–
ISDN $_{S2M}$	–	–	–	–	–	–	–	–	–	–	–
xDSL	–	3	3	–	–	1	–	–	–	1	–
E1	–	–	–	–	–	–	–	–	–	–	–
Sonstige (Angabe Typ)	–	–	–	–	–	COM Console Port	–	–	–	–	serieller Port [3]
Hardware/Betriebssystem											
Prozessor	Intel Xeon 2800	Motorola 8241 RISC	PCB 750 FX, 733 MHz RISC	Intel Celeron 600MHz	k.A.	Intel IXP425 400MHz	Intel Celeron 2000 MHz	533 MHZ	2.4 GHz Xeon	Intel P IV 2 Ghz	Intel IxP425, 533MHz
Arbeitsspeicher in MByte	1024	32	64	128	k.A.	64	256	32	512	256	64 + 16 (Flash)
Betriebssystem Name/Version	Astaro Security Linux V5	Boss 7.1	Boss 7.1	PIX 6.3(3)	Clavister OS	proprietär	Linux / Kernel 2.4.22	Innominate Secure Linux	Inferno OS [2]	Eigen-entwicklung	ZyNOS 3.62
IPv6-Unterstützung für alle Firewall-Funktionen	○	○	○	○	○	○	○	○	○	○	○
Firewall-Technik											
Stateful-Inspection-Firewall	●	●	●	●	●	●	●	●	●	●	●
Layer-7-Application-Gateway-Proxies	●	○	○	●	●	●	●	○	●	○	○
anpassbare Proxies	●	●	●	○	○	○	●	○	○	●	○
Stateful-Inspection und Proxy kombiniert	●	●	●	●	●	○	●	○	●	○	○
transp. Firewallfunktionalität konfigurierbar	○	●	●	●	●	●	●	●	●	●	○
spezielle Firewall-ASICs integriert	○	○	○	○	○	●	○	○	●	●	○
Netzwerkproz. m. Firewall Teilfunkt. auf NIC	○	○	○	○	○	○	○	○	●	○	○
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)	–	–	–	● [1]	2	–	1	–	2	2	1
Cluster über 3-Party-Software etabliert	○	●	●	○	○	○	○	○	○	○	○
Cluster über externen Load-Balancer-Switch	●	●	●	●	○	○	○	○	○	●	○
Cluster über Netzwerk-Links etabliert	○	●	●	●	●	○	○	○	●	●	○
Management											
Telnet	○	●	●	●	○	●	○	○	○	○	●
rollenbasierte Verwaltung	○	○	○	●	○	○	●	●	●	mit GMS	○
Auditing-fähig	●	○	○	●	●	●	○	○	●	mit GMS	○
SSH-Support für CLI	●	●	●	●	○	○	●	●	○	○	●
HTTP/S	●	●	●	●	●	●	nur VirusWall	●	○	●	●
automatische Synchronisierung im Cluster	○	○	○	●	●	○	○	○	●	●	○
Synchronisierung über multiple Pfade möglich	○	○	○	●	●	○	○	○	●	○	○
Out-Band-Management	●	○	○	●	●	●	○	○	●	○	●
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	●	●	●	●	●	○	○	○	●	k.A.	●
DHCP	●	●	●	●	●	●	○	●	●	●	●
NAT-Support	●	●	●	●	●	●	●	●	●	●	●
Content-Filter	●	●	●	●	●	●	○	○	●	○	●
Virenscanner	●	○	○	●	○	○	○	○	●	○	○
Website	www.astaro.com	www.bintec.de	www.bintec.de	www.cisco.com/go/pix	www.clavister.com	www.dlink.de	www.gateProtect.de	www.innominate.de	www.lucent.com/security	www.sonicwall.de	www.zyxel.de
Listenpreis in Euro für Teststellung zzgl. MwSt.	14 438	1598	14 998	11 600	19 996	1198	4290	1300	12 300	7559	2206

ja = ●; nein = ○; k.A. = keine Angabe; 1) keine Beschränkung (über Load-balancing Produkte); 2) (Lucent propriatary) / LSMS Version 7.1; 3) für Dial-Backup

Die Übersicht basiert auf Angaben der Hersteller. Network Computing übernimmt keine Garantie für die Richtigkeit und Vollständigkeit dieser Angaben.

gewöhnlich von großen Brüdern auch erwartet. Bei unseren Messungen mit unidirektionalen Datenströmen lieferte die VPN-Access-1000 durchgehend und auch bei Volllast Wirespeed von 100 MBit/s. Im bidirektionalen Modus und bei den Many-to-Many-Messungen – jeweils wieder mit den kleinen 64-Byte-Paketen – kam aber auch die große Bintec-Appliance an ihre Grenzen. So erreichte das System bei der bidirektionalen Messung mit 64-Byte-Frames einen maximalen Durchsatz von 58 MBit/s, der aber auch noch unter Volllast zur Verfügung stand. Die Werte für die Many-to-Many-Messungen liegen noch ein wenig darunter, so schaffte die VPN-Access-1000 hier noch einen maximalen Durchsatz von 36 MBit/s, der aber auch noch bei Volllast zur Verfügung stand. Bei größeren Datenrahmen stellte die große Bintec-Appliance dann wieder durchgängig Wirespeed zur Verfügung. Und auch von Stör-Traffic ließ sich die Firewall nicht erschüttern. Insgesamt zeigte die VPN-Access-1000 ein ordentliches Leistungsvermögen – Schwächen erlaubt sie sich bei den Messungen mit kleinen Datenrahmen.

Auch Ciscos PIX-515E-Security-Appliance hatte ihre Probleme mit kleinen Datenrahmen. Was die Durchsätze bei unseren Messungen mit 64-Byte-Paketen anbelangt, war das Cisco-System nur unwesentlich schneller als die kleine Bintec-Maschine. So schaffte die PIX-515E im unidirektionalen Betrieb mit 64-Byte-Paketen einen maximalen Durchsatz von 55 MBit/s. Bidirektional kam sie dann noch auf 30 MBit/s und Many-to-Many auf 24 MBit/s im Mittel je Senderichtung. Unter Volllast lagen die Messwerte dann noch mal unter den ermittelten Maximalwerten unter optimalen Bedingungen. Dabei verlor das Cisco-System im Many-to-Many-Setup auch Daten bei den Messungen mit größeren Frames, so dass die PIX-515E hier um die 80 MBit/s zur Verfügung stellte. Eine deutliche Schwäche bei kleinen Frame-Formaten und im Many-to-Many-Betrieb sorgen dafür, dass die PIX-515E über das Mittelfeld nicht hinaus kommt – da hilft es auch nicht mehr, dass sich das Cisco-System nur sehr gering von Stör-Traffic beeinflussen ließ.

Mit der Clavister-M460 stand dann ein Newcomer erstmals in unseren Labs, der für Überraschung sorgte. Die Firewall-Appliance des 1997 gegründeten schwedischen Herstellers stellte bis auf die dritte Stelle hinter dem Komma Wirespeed zur Verfügung und ließ sich weder von 64-Byte-Paketen noch von Many-to-Many-Szenarien oder Stör-Traffic beeindrucken. Die M460 ist das einzige System im Testfeld, dem wir bescheinigen können, dass es in unseren Szenarien in keinem Fall zum Flaschenhals wird. Im Preis-Leistungsverhältnis hat die teuerste und performanteste Appliance im Testfeld zwangsläufig überall dort die Nase vorn, wo der Mitbewerb Performance-Enpässe erkennen lässt.

Am anderen Ende des Testfeldes lag dagegen D-Links DFL-700-Network-Security-Firewall nicht nur preislich, sondern auch in Sachen Performance. So schaffte die DFL-700 schon im unidirektionalen Betrieb mit 64-Byte-Paketen einen maximalen Durchsatz von 16 MBit/s. Galt es im gleichen Szenario 1518 Byte große Frames zu transportieren, dann stieg der Datendurchsatz auf maximal 51 MBit/s. Anspruchvollere Szenarien und Messungen mit Volllast quittierte das D-Link-System mit einer entsprechend schlechteren Performance. Dabei waren es wieder einmal die 64-Byte-Pakete, die das System am meisten stressten. Kombinierten wir 64-Byte-Pakete mit Volllast im Many-to-Many-Setup, dann machte das System quasi dicht; im letztgenannten Szenario blieben noch 0,01 MBit/s Durchsatz übrig. Auch in Bezug auf den Einfluss von Stör-Traffic erwies sich die D-Link-Firewall als recht anfällig. So verlor sie durch diesen Einfluss bei der 64-Byte-Messung und bei der 1518-Byte-Messung je zusätzlich 14, bei der 512-Byte-Messung sogar weitere 21 MBit/s an Datendurchsatz.

Dort, wo das D-Link-System auf passable Durchsätze kam – und das konnten auch gut 50 MBit/s sein – erreicht die D-Link-Firewall auf Grund ihres geringen Preises respektable Preis-Performance-Werte, die nur noch Innominate übertrifft. Wegen der für unser Szenario aber eindeutig zu schlechten Leistungswerte ändert das jedoch nichts an der Platzierung.

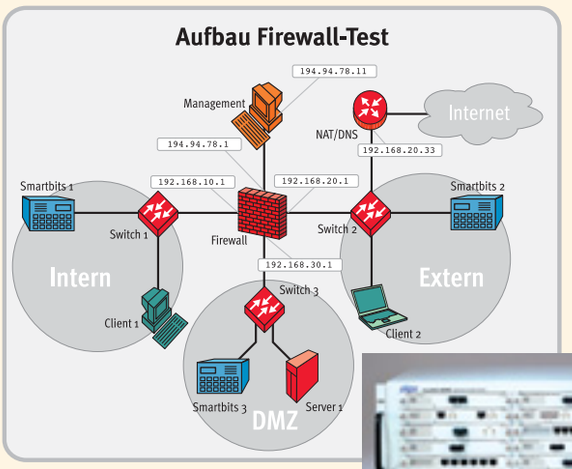
Auch die Gateprotect-Firewall hatte deutliche Probleme insbesondere mit kleinen Datenrahmen. So schaffte sie bereits bei den Messungen mit unidirektionalen Datenströmen und 64-Byte-Paketen maximal 25 MBit/s. Unter Volllast ging dieser Wert noch auf gut 7 MBit/s zurück. Andererseits arbeitete auch diese Firewall im unidirektionalen Betrieb mit größeren Frames Wirespeed. Bei den anspruchsvolleren Setups zeigte

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 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 zu analysieren.

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 100 MBit/s. Bidirektional liegen dann natürlich maximal 200 MBit/s an.

das Gateprotect-System dann aber auch bei größeren Frames Schwächen. So kamen beispielsweise im Many-to-Many-Setup bei der Messung mit 512-Byte-Paketen noch 54 MBit/s und bei der Messung mit 1518-Byte-Paketen 94 MBit/s durch. Außerdem ließ sich die Gateprotect-Firewall recht stark vom Stör-Traffic bei der 64-Byte-Messung beeinträchtigen. Hier verlor sie zusätzliche 18 MBit/s. Da, wo die Gateprotect-Firewall auf brauchbare Messwerte kommt, liegt sie dann auf Grund ihres vergleichsweise günstigen Preises im Preis-Leistungsverhältnis auf einem guten Niveau. Für unser hochperformantes Szenario reicht das Leistungsvermögen der Gateprotect-Firewall aber nicht aus.

Dass auch Innominates Mguard für unser Szenario eigentlich unterdimensioniert ist, war Innominate ebenso wie uns schon zu Testbeginn klar. Trotzdem ließen wir diesen Firewall-David gegen die Goliaths dieser Zunft antreten, denn wir wollten wissen, wie leistungsfähig solche schlanken Lösungen heute schon sind. Auf Grund der Bestückung der Mguard mit lediglich zwei Fast-Ethernet-Ports konnten wir auch nur die Messungen mit uni- beziehungsweise bidirektionalen Datenströmen durchführen. Die Einrichtung einer DMZ oder eines anderen dritten Netzsegments, wie sie für unser Many-to-Many-Setup erforderlich ist, gestattet die Mguard hardwareseitig nicht. Mit 64-Byte-Paketen hatte auch die Mguard ihre Probleme, hier erreichte sie unidirektional wie bidirektional einen Durchsatz von 14 MBit/s. Mit größeren Paketen kam sie dagegen recht gut zurecht, und so lieferte die Innominate-Firewall uni- wie bidirektional im Betrieb mit 1518-Byte-Frames Wirespeed. Hier kommt die Mguard dann auch auf sehr gute Preis-Performance-Werte, die beispielsweise für die beiden 1518-Byte-Messungen, die das Gerät hardwareseitig erlaubte, noch geringfügig vor der kleinen Bintec-Maschine liegen.

Mit Lucents VPN-Firewall-Brick-350 stand dann wieder eine ausgewachsenere Lösung in unserem Lab. Nichtsdestotrotz zeigten sich auch hier wieder Probleme mit kleinen Frame-Größen. So betrug der maximale Durchsatz im unidirektionalen Modus 51 MBit/s, bidirektional lagen dann noch 30 MBit/s und Many-to-Many 27 MBit/s je Senderichtung an. Bei Volllast stiegen die Verlustraten in diesen Disziplinen noch deutlich an, so dass die Brick-350 bei der Many-to-Many-Messung mit 64-Byte-Paketen praktisch dicht machte und lediglich 0,07 MBit/s an Daten passieren ließ. Wohlgemerkt beschränken sich diese Probleme auf den 64-Byte-Bereich, ansonsten lieferte die Lucent-Firewall Wirespeed, und auch durch Stör-Traffic ließ sich die Brick-350 nicht nennenswert beeinträchtigen.

Nur die große Astaro- und die Clavister-Firewall arbeiteten durchsatzstärker als Sonicwalls Pro-3060. Wenn auch dieses System deutliche Probleme mit 64-Byte-Paketen hatte, so lagen die erreichten Durchsatzraten doch über denen der meisten anderen Systeme im Testfeld. So schaffte die Pro-3060 im unidirektionalen Betrieb mit 64-Byte-Paketen einen Durchsatz von 89 MBit/s. Bei der Many-to-Many-Messung mit den kleinsten Paketen erreichte sie noch 43 MBit/s. diese Bandbreiten lagen dann aber auch noch bei Volllast des Systems an. Sendeten wir Datenströme, die aus größeren Frame-Formaten bestanden, dann arbeitete das Sonicwall-System dagegen fehlerfrei und lieferte je Senderichtung ihre 100 MBit/s. Durch Stör-Traffic ließ sich die Pro-3060 lediglich wieder bei den 64-Byte-Messungen beeinträchtigen. Hier ging der Durchsatz um zusätzliche 8 MBit/s zurück.

Auch Zyxels Zywall-70 zeigte in unserem Real-World-Labs-Test Schwächen im Bereich der 64-Byte-Messungen – und nicht nur dort. So lieferte die Zyxel-Firewall schon bei den unidirektionalen Messungen deutliche Performance-Einbußen. Maximal erreichte sie hier Durchsatzraten von 10 MBit/s bei der 64-Byte-Messung bis

zu 100 MBit/s bei 1518-Byte-Paketen. Bei den übrigen Test-Setups war dann endgültig Schluss mit Wirespeed. So kam die Zywall-70 bei den Many-to-Many-Messungen auf Durchsätze zwischen 2 MBit/s mit 64-Byte-Paketen und 45 MBit/s mit 1518-Byte-Paketen. Diese Werte konnte das System dann aber auch mit Volllast halten, so dass es nie völlig dicht machte und somit vorhersehbar arbeitete. Die Anfälligkeit gegen Stör-Traffic war dagegen gering. Auch die Zyxel-Firewall erwies sich als für unser Szenario unterdimensioniert und auch im Preis-Performance-Index vermochte sich das System nicht sonderlich zu bewähren, obwohl es zu den preisgünstigen Lösungen im Testfeld gehört.

Fazit

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 mit Ausnahme der Clavister-Lösung mehr oder weniger aller Systeme im Testfeld, wenn große Datenmengen mit kleinen Paketen zu erwarten sind. 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.

Als performantestes System im Testfeld der Fast-Ethernet-Firewall-Appliances hat sich auf alle Fälle die Newcomer-Lösung aus Schweden, die Clavister-M460, erwiesen. Als einzige Firewall-Appliance arbeitete das System in allen Tests souverän und mit Wirespeed. Auch wenn dieses System das teuerste im Testfeld der Fast-Ethernet-Geräte ist; es garantiert als einziges Gerät im Testfeld der Fast-Etherent-Appliances Wirespeed ohne Wenn und Aber. Das macht die Clavister-Lösung für unsere Aufgabenstellung zum System erster Wahl. Einen guten zweiten Platz erreichte die große Bintec-Lösung, die abgesehen von der weit verbreiteten 64-Byte-Schwäche gut arbeitete. Das Mittelfeld bilden die Systeme von Sonicwall, Astaro, Lucent und Cisco, deren Verhalten von unterschiedlich ausgeprägten Stärken und Schwächen gekennzeichnet ist. In Anbetracht ihres gegenüber den übrigen gut platzierten Systemen deutlich günstigeren Preises verdient die kleine Bintec-VPN-Access-25 sicherlich die Preis-Leistungs-Empfehlung. Sie fällt nicht allzu sehr hinter dem Mittelfeld ab, bietet dieses Potential aber zu einem deutlich günstigeren Preis.

Die Systeme von Gateprotect, Zyxel und D-Link fallen in der Leistung stark hinter den Anforderungen zurück, so dass sie für das ausgeschriebene Szenario nicht empfehlenswert sind, was auch ihre Platzierung in der Report-Card zeigt. Sicherlich liegen sie auch in der Preisklasse deutlich hinter den besser platzierten Lösungen, was aber keinen Einfluss auf die Eignung für unser hochperformantes Szenario haben kann, da sie einfach nicht genügend Performance für unsere Zwecke bieten. Für die sichere Anbindung von LANs über relativ langsame WAN-Verbindungen mögen sie durchaus gut geeignet sein. Interessanter Exot in unserem Testfeld war die kleine, in der Performance gar nicht so schlechte Innominate-Lösung, die natürlich gleichfalls für unser Szenario weder geeignet noch ernsthaft gedacht ist.

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