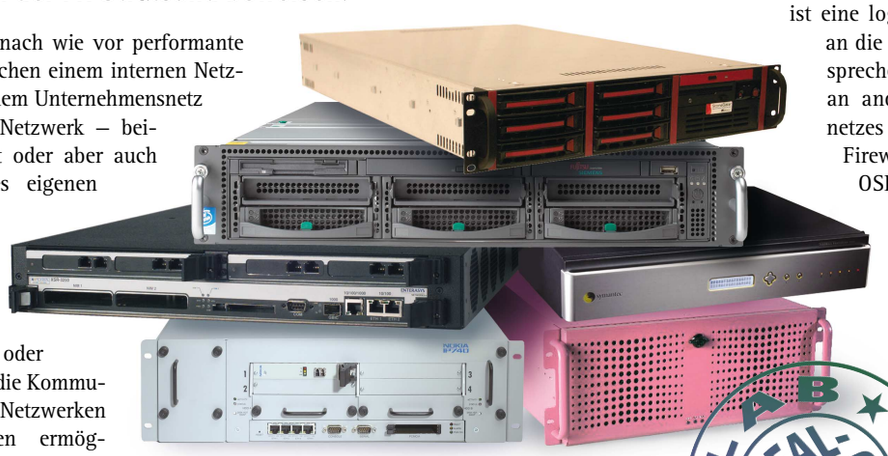
Gigabit-Ethernet-Firewall-Appliances

Mit Volldampf durch die Feuerwand

Mit welcher Geschwindigkeit aktuelle Firewall-Systeme 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.



Für eine sichere aber nach wie vor performante Kommunikation zwischen einem internen Netzwerk – beispielsweise einem Unternehmensnetz – und einem externen Netzwerk – beispielsweise dem Internet oder aber auch anderen Segmenten des eigenen Unternehmensnetzes – sollen Firewalls sorgen. Technisch ist eine Firewall folglich eine aktive Netzwerkkomponente, wie ein Switch oder ein Router, die nicht nur die Kommunikation zwischen zwei Netzwerken oder Netzwerksegmenten ermöglichen soll, sondern zugleich eine Überwachungs- und Kontrollfunktion erfüllt, um das interne zu sichernde Netzwerk vor unerwünschtem Datenverkehr zu schützen. Auf der internen Seite handelt es sich zumeist um Ethernet-basierte Netze, extern können neben LAN- auch die unterschiedlichsten WAN-Verbindungen, wie ISDN, 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 ermöglicht. Hierfür bieten Firewall-Appliances Fast-Ethernet- und – in der Highend-Klasse – 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 erreichbar sein müssen.

Mit zunehmender Komplexität der heutigen Unternehmensnetze und in Anbetracht der Erkenntnis, 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 passieren. In Anbetracht der Datenmengen, der Qualitätsanforderungen in heutigen konvergenten Netzen 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 ist eine logische Konsequenz. Die Anforderungen an die Leistungsfähigkeit solcher Firewalls entsprechen daher logischerweise denen, die auch an andere Komponenten des Unternehmensnetzes gestellt werden.

Firewalls arbeiten 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 können die Netzwerke physikalisch wie logisch entkoppeln und können von jedem Benutzer Identifikation und Authentifikation prüfen. Komplexere Firewall-Systeme kombinieren in der Praxis häufig verschiedene Firewall-Konzepte in einer Lösung.

Report-Card /interaktiv unter www.networkcomputing.de

Firewall-Performance

Max. Durchsatz	Gewichtung	Siemens / Check Point 4 Your Safety RX300	Enterasys XSR 3250	Nokia/ Check Point IP 740 / NG	Symantec Gateway Security	Stonesoft StoneGate	Genua Genugate Enterprise
512 Byte unidirektional	20%	5	5	5	3	3	1
1518 Byte unidirektional	20%	5	5	3	5	5	1
512 Byte bidirektional	20%	5	1	2	1	1	1
1518 Byte bidirektional	20%	5	5	4	4	2	1
64 Byte unidirektional	10%	5	1	1	1	1	1
64 Byte bidirektional	10%	5	1	1	1	1	1
Gesamtergebnis	**100%**	**5**	**3,4**	**3**	**2,8**	**2,4**	**1**
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 -;		**A+**	**C+**	**C**	**C**	**D**	**E**

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

Bewertungsschlüssel für maximalen Datendurchsatz: > 950 MBit/s = 5, > 900 MBit/s = 4, > 800 MBit/s = 3, > 700 MBit/s = 2, </= 700 MBit/s = 1

Application-Level-Gateways beherrschen Syntax und Semantik der einzelnen Protokolle und prüfen den Datenverkehr auf der Ebene der Application-Level-Protokolle. So erlauben sie die volle Kontrolle der Inhalte und erkennen beispielsweise Angriffe oder Viren. Diese Kontrollfunktionen sollten sich auf die wirklich erforderliche Syntax und auf die notwendigen Daten beschränken, da sie komplexe Algorithmen erfordert. Die Komplexität dieser Systeme ist so groß, dass die Hersteller sie nicht in Hardware abbilden können, sondern sie in Software realisieren. Application-Level-Gateways oder -Proxies analysieren also 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 Gigabit-Ethernet-Wirespeed – eine deutlich leistungsfähigere Hardware erforderlich ist. Um unsere Tests trotzdem fair und vergleichbar zu halten, haben wir an alle Systeme die gleichen Anforderungen gestellt und ein Standard-Rule-Set definiert, das die Hersteller zunächst konfigurieren mussten. Dieses Rule-Set erforderte lediglich eine Paket-Filter- und Stateful-Inspection-Funktionalität.

Info

Das Testfeld

Gruppe 1: Fast-Ethernet-Appliances

- NetScreen NS-204 Appliance
- Siemens/Check Point 4 Your Safety RX 100 / VPN1 Pro Express
- TELCO TECH LiSS II secure gateway
- WatchGuard Firebox Vclass V80

Gruppe 2: Gigabit-Ethernet-Appliances

- Enterasys XSR 3250
- GeNUA GeNUGate Enterprise
- Nokia/Check Point IP 740 Check Point NG with Application Intelligence
- Siemens/Check Point 4 Your Safety RX 300 mit Corrent Turbo Card / VPN-1 pro
- Stonesoft StoneGate
- Symantec Gateway Security 5460

Firewalls bestehen aus Hard- und Softwarekomponenten, die häufig von unterschiedlichen Herstellern stammen und individuell kombiniert werden. Bei den so genannten 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 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.

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 mit Wirespeed ermöglichen. Darüber hinaus interessierte uns, wie viel gesicherten Datenverkehr der IT-Verantwortliche derzeit für sein Budget erhält.

Für die Ausschreibung unseres Vergleichstests haben wir ein Unternehmen unterstellt, das sein heterogenes, konvergentes Netzwerk sowie eine eigenständige DMZ am Unternehmensstandort hochperformant untereinander sowie mit dem Internet verbinden will. Eine geeignete, durchsatzstarke Firewall-Appliance sollte für die notwendige Sicherheit und Performance sorgen. Zugleich sollte die Appliance den Aufbau eines VPNs zu einer entfernten Niederlassung ermöglichen, die mit einem baugleichen Gerät ausgestattet werden soll.

Daraus ergaben sich folgende Anforderungen an die Teststellungen:

- 2 Firewall- und VPN-Appliances inklusive Zubehör und Dokumentation,
- IPSec-VPN mit IKE,
- Verschlüsselung nach 3DES,
- je Gerät mindestens 3 Fast-Ethernet-Ports oder
- 2 Gigabit-Ethernet-Ports und 1 Fast-Ethernet-Port.

Messen wollten wir die Firewall-Performance, also die unidirektionalen und bidirektionalen Datendurchsatzraten im Firewall-Betrieb, die Datenverlustraten, Latency sowie Jitter unter Last. Als Test-Equipment dienten die Lastgeneratoren und -analysatoren Smartbits 6000B von Spirent Communications mit den aktuellen Applikationen Smartflow und Websuite-Firewall.

In einer Ausschreibung haben wir dann 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 elf Hersteller mit ihren Teststellungen an den Start. Die Gruppe 1 der Fast-Ethernet-Appliances bildeten »NetScreen NS-204 Appliance«, Siemens' »4 Your Safety RX 100« mit Check Points »VPN1 Pro Express«, Telco Techs »LiSS II secure gateway« sowie

Features

Firewall-Teststellungen

	Enterasys Networks XSR-3250	GeNUA GeNUGate Enterprise	Nokia/Check Point IP 740/Check Point NG	Siemens/Check Point 4 Your Safety RX 300/ VPN-1 Pro	Stonesoft StoneGate SG-3000	Symantec Gateway Security 5460
Anz. unabhäng. (nicht geswitchter) LAN-Ports						
Anzahl Gigabit-Ethernet-Ports	3	max. 9	max. 6	5	max. 10	8 x 10/100/1000
Anzahl Fast-Ethernet-Ports	6	max. 20	max. 20	2	max. 10	8 x 10/100/1000
Anzahl WAN-Ports						
PPoE auf LAN-Port(s)	9	0	0	k.A.	k.A.	0
X.21	24	0	max. 8	0	k.A.	0
X.25	0	0	0	0	k.A.	0
ISDN S_0	12	0	max. 4	0	k.A.	0
ISDN S_{2M}	24	0	0	0	k.A.	0
xDSL	24	0	0	k.A.	k.A.	8
E1	24	0	max. 4	k.A.	k.A.	8
Hardware/Betriebssystem						
Prozessor (Typ)	Broadcom 1250	Intel P4 bzw. Xeon	Intel PIII-1000	P4 Xeon 2.4 Ghz.	1-2 Xeon CPUs 2,4 - 3,0 GHz	k.a.
Arbeitsspeicher in MByte	max.512	max. 2048	max. 2048	1024	max. 1024	k.a.
Betriebssystem Name/Version	EOS 5.00.05	BSD/OS	IPSO 3.7	Red Hat Linux 7.3	gehärteter Linux-Kernel	Linux, Redhat
Firewall-Technik						
Stateful-Inspection-Firewall	●	k.A.	●	●	●	●
Layer-7-Application-Gateway-Proxies	●	●	●	●	○	●
anpassbare Proxies	○	●	○	●	●	●
Stateful-Inspection und Proxy kombiniert	●	●	○	●	●	●
transp. Firewallfunktionalität konfigurierbar	○	●	●	●	●	●
spezielle Firewall-ASICs integriert	○	○	○	○	○	○
Netzprozessor mit 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)	unbegrenzt	unbegrenzt	4	8	16	8
Cluster über 3-Party-Software etabliert	○	○	○	●	○	●
Cluster über externen Load-Balancer-Switch	●	○	●	●	○	●
Cluster über Netzwerk-Links etabliert	●	○	●	●	k.A.	●
Management						
Telnet	●	●	●	●	○	○
rollenbasierte Verwaltung	●	●	●	●	●	●
Auditing-fähig	●	●	●	●	●	●
SSH-Support für CLI	●	●	●	●	●	○
HTTP/S	●	●	●	●	●	●
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 zentralisier	●	●	●	●	●	●
Event-Management korelliert einzelne Einträge	●	●	●	●	○	●
Authentisierung/Autorisierung						
NT-Domain	●	über Zusatzprodukt	VPN Client	●	●	●
TACACS/TACACS+	○	○	●	●	●	●
Radius	●	●	●	●	●	●
LDAP über TLS	●	●	VPN Client	●	●	○
X.509-digitale Zertifkate	●	●	VPN Client	●	●	●
Token-basierend	●	●	VPN Client	●	●	●
Sicherheitsfeatures						
DMZ	●	● , bis zu 16 Netze	●	●	●	●
Intrusion-Detection	●	Host-IDS integriert	●, mit Smart Defense	●	○	●
AAA-Support	●	k.A.	●	○	●	●
DHCP	●	○	●	●	○	○
NAT-Support	●	●	●	●	●	●
Content-Filter	○	●	●, über OPSEC Schnittstelle	● , Drittanbieter	● , Redirect z. Content Filter	●
Virenscanner	○	über Zusatzprodukt	●, über OPSEC Schnittstelle	● , Drittanbieter	● , Redirect z. Virenscanner	●
Website	www.enterasys.com/ products/routing/XSR-3000/	www.genua.de	www.nokia.com	www.checkpoint.com www.4ys.de	www.stonesoft.com	http://enterprisesecurity. symantec.de/
Listenpreis in Euro für Teststellung zzgl. MwSt. (*)	27 100	40 000	123 594,53	61 200	38 950	32 093,30

● = ja; ○ = nein; * 2 Appliances (Hard- und Software) inkl. Lizenzen für mindestens 100 User und vollständige Managementlösung

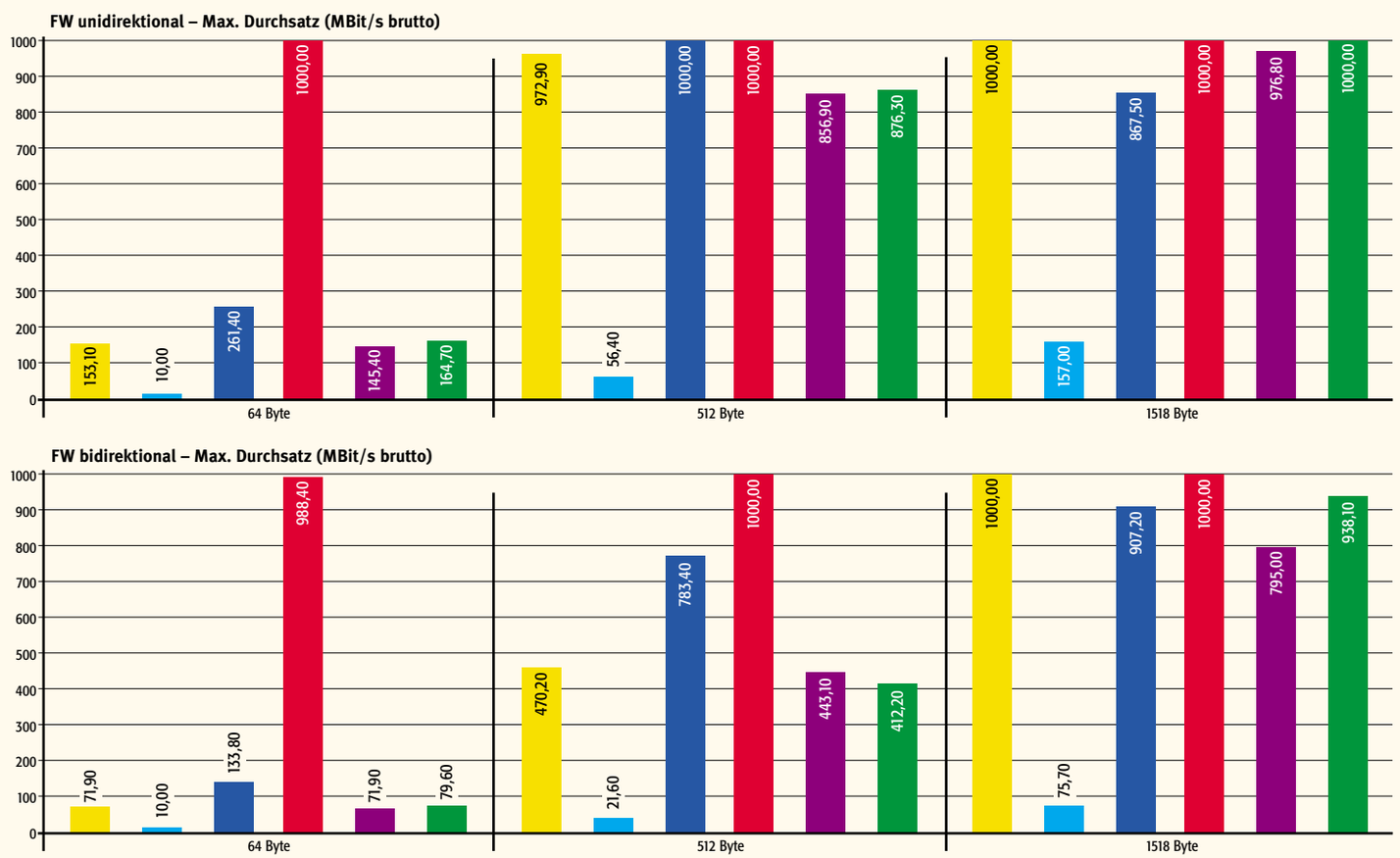
Watchguards »Firebox Vclass V80«. Die übrigen Hersteller zogen es vor, gleich Gigabit-Ethernet-Maschinen ins Rennen zu schicken. Zur Gruppe der Gigabit-Ethernet-Systeme gehören Enterasys »XSR 3250«, Genuas »GeNUGate Enterprise«, Nokias »IP 740« mit »Nokia Encryption Accelerator Card« und Check Points »NG with Application Intelligence« sowie Siemens »4 Your Safety RX 300« mit »Corrent Turbo Card« und Check Points »VPN-1 pro«. Das Testfeld vervollständigten Stonesofts »StoneGate SG-3000« sowie Symantecs »Gateway Security 5460«. Wie sich die Fast-Ethernet-Appliances in unserem Test verhielten, steht im kürzlich erschienenen Network Computing-Sonderheft Sicherheit & Sicherung. Die Ergebnisse der Gigabit-Ethernet-Appliances liegen mit diesem Artikel vor.

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.

Die Auswirkungen gegenüber Wirespeed reduzierter Durchsatzraten und damit verbundener Datenverluste bei entsprechender Last sind natürlich in realen Unternehmensnetzen abhängig von einer ganzen Reihe von Faktoren – wie den eingesetzten Applikationen oder der Gesamtauslastung des Netzwerks. Generell gilt, dass klassische Datenanwendungen weniger anfällig für entsprechende Engpässe im Netz sind, als moderne konvergente Anwendungen, wie Voice- oder Video-over-IP. Für eine Beurteilung der Testergebnisse für die Praxis ist auch eine Einschätzung wichtig, mit welchen Datenrahmengrößen zu rechnen ist. Bei klassischen Dateitransfers arbeitet das Netzwerk mit möglichst großen Rahmen. Bei Echtzeit-Applikationen teilt sich das Feld. Video-Übertragungen nutzen ähnlich den Dateitransfers relativ große Datenrahmen. Messungen mit Ethernet-LAN-Phones in unseren Real-World Labs haben beispielsweise ergeben, dass diese Voice-over-IP-Lösung die Sprache mit konstant großen Rahmen von 534 Byte überträgt. Noch deutlich kürzere Rahmen sind beispielsweise bei der TCP-Signalisierung mit 64 Byte zu messen. Für die Sprachdatenübertragung wie auch für andere echtzeitfähige Applikationen ist das Datenverlustverhalten von entscheidender Bedeutung. Ab 5 Prozent Verlust ist je nach Voice-over-IP-Codec mit deutlicher Verschlechterung der Sprachqualität zu rechnen, 10 Prozent führen zu einer massiven Beeinträchtigung, ab 20 Prozent Datenverlust ist die IP-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. Erzielt eine Firewall maximale Durchsatzraten, die unter Wirespeed liegen, dann ist bei Wirespeed-Input mit Datenverlusten zu rechnen, die der Differenz zwischen tatsächlichem Maximaldurchsatz und der nominellen Wirespeed entsprechen.

Messergebnisse



Info

So testete Network Computing

Als Lastgenerator/Analysator haben wir in unseren Real-World Labs den bekannten »Smartbits 6000B Traffic Generator/Analyser« von Spirent eingesetzt. Das in dieser Konfiguration gut 250 000 Euro teuere Gerät war mit der Software »Smartflow 2.20.005.1« sowie »Websuite Firewall 2.10.001« ausgestattet und mit 24 Fast-Ethernet-Ports sowie vier Kupfer- und fünf Multimode-LWL-Gigabit-Ethernet-Ports bestückt. Alle Ports arbeiten wahlweise im Half- oder 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 von Frameloss, Latency und Jitter haben wir mit dem Smartbits-Lastgenerator/Analysator Datenströme generiert und diese unidirektional und bidirektional mit verschiedenen Paketgrößen gesendet. Die Eingangslast haben wir in 10-Prozent-Schritten von 10 bis auf 100 Prozent erhöht. Lagen die ermittelten Performance-Werte unter 10 Prozent oder tauchten weitere Unregelmäßigkeiten auf, haben wir weitere Detail-Messungen gemacht, um das Problem zu analysieren.

Den maximalen Durchsatz haben wir mit einem speziellen Mess-Algorithmus der Smartbits ermittelt, in dem der Lastgenerator alternierende Lasten erzeugt, die sich in kleiner werdenden Intervallen dem optimalen Input nähern, bis sie der maximalen Last entsprechen, die gerade noch ohne nennenswerte Datenverluste möglich ist. Nacheinander haben wir für beide Messreihen Datenströme mit konstanten Rahmengrößen von 64, 512 und 1518 Byte erzeugt.

Nacheinander haben wir drei Firewall-Testreihen durchgeführt. In der ersten und zweiten Testreihe haben wir unidirektional von intern nach extern gesendet und jeweils einen beziehungsweise zehn UDP-Ports adressiert und entsprechend viele Streams erzeugt. In der dritten Testreihe haben wir dann mit bidirektionalem Datenverkehr gearbeitet. Der Smartbits-Lastgenerator/Analysator hat die empfangenen Datenströme auf die eingestellten Parameter hin untersucht und die Ergebnisse gesichert. Die Performance-Messungen haben wir ausschließlich mit UDP-Paketen durchgeführt, weil sich hierbei im Gegensatz zu TCP-Datenströmen Eigenschaften des Protokolls wie Retransmisson nicht auswirken.

Enterasys »XSR 3250«, ein Router mit implementierten Security-Funktionalitäten, zeigte deutliche Probleme bei den Messungen mit 64-Byte-Paketen. So bremste diese Messung die Enterasys-Lösung von theoretisch möglichen 1 GBit/s unidirektional auf rund 157 beziehungsweise 153 MBit/s herunter. Im bidirektionalen Test reduzierte sich der maximal erreichbare Durchsatz sogar auf knapp 72 MBit/s. Was in ihm steckt zeigte das Enterasys-System dann bei den unidirektionalen Messungen mit größeren Datenrahmen. Hier erreichte es Wirespeed oder blieb nur unbedeutend hinter den möglichen Maximalwerten zurück. Im bidirektionalen Betrieb reduzierte sich dann der Datendurchsatz auch noch bei den Messungen mit 512-Byte-Paketen auf 470 MBit/s. Bei den ganz großen Datenpaketen stand dann auch hier die theoretische Höchstgeschwindigkeit von 1 GBit/s zur Verfügung.

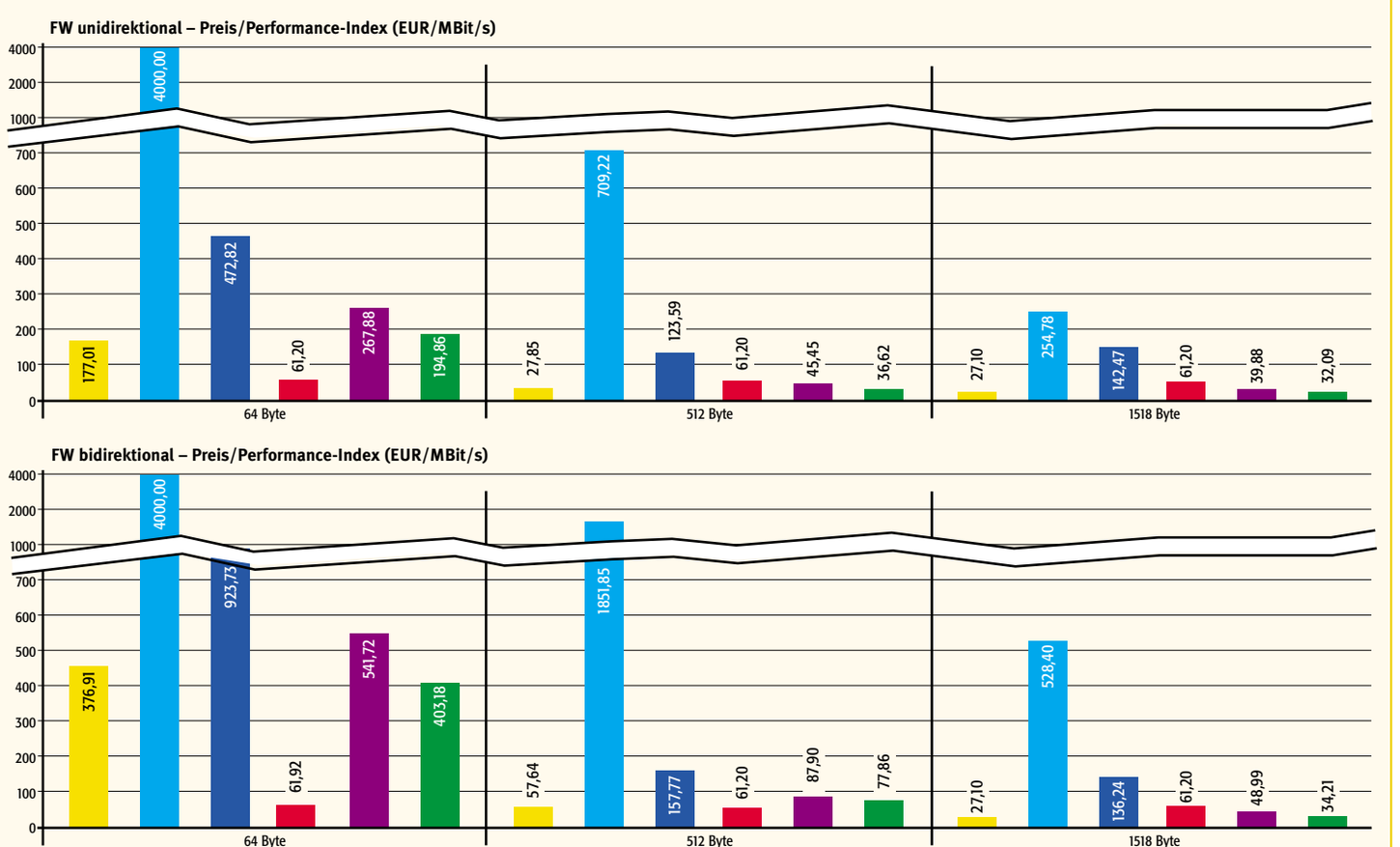
Massive Probleme unter Last zeigte dann Genuas Genugate-Enterprise trotz aller Konfigurationsarbeiten der Genua-Experten. Mit 64-Byte-Paketen

kam das System überhaupt nicht zurecht. Der maximal erzielbare Datendurchsatz im Test belief sich auf rund 10 MBit/s. Mit rund 60 MBit/s unidirektional und nicht ganz 22 MBit/s bei den Messungen blieb die Genua-Lösung auch hier deutlich hinter den Erwartungen zurück. Mit gut 157 beziehungsweise 172 MBit/s erreichte die Genugate-Enterprise ihre höchsten Ergebnisse in unserem Test bei der Messung mit 1518-Byte-Frames unidirektional. Auch dieser Wert halbierte sich rund im bidirektionalen Modus auf gut 75 MBit/s – absolut mit Abstand die schwächste Durchsatzleistung. Auch wenn die Genua-Lösung hierbei ein höheres Sicherheits-Level als gefordert zur Verfügung gestellt haben sollte, erwecken doch die im maximalen Ausbau verfügbaren neun Gigabit-Ethernet-Ports falsche Erwartungen. Denn wie Genua selbst in einem aktuellen Whitepaper mit dem Titel »Firewall-Typen: Vom Paketfilter zum Applicationlevel-Gateway« schreibt: »Eine Firewall darf nicht zum Flaschenhals der Netzkopplung werden, sondern muss ausreichend Reserven besitzen, um auch die Spitzen der Netzlast zufriedenstellend bedienen zu können.« Dies ist Genua in unserem Test jedenfalls nicht gelungen, denn IT-Verantwortliche werden wohl nur in Gigabit-Systeme investieren, wenn sie nicht lediglich schmalbandige WAN-Verbindungen absichern wollen, sondern entsprechend performante Systeme benötigen, um verschieden Netze oder Netzsegmente entsprechend hochperformant miteinander zu verbinden und entsprechend zu schützen. Ob die Experten von Genua wirklich das Potenzial ihrer Genugate-Enterprise in unserem Test ausgeschöpft haben, ist nicht mit letzter Gewissheit zu sagen.

Nokia schickte mit ihrer IP-740 eine etablierte Firewall-Lösung ins Rennen, die in ihrer aktuellen Version softwareseitig mit Check Points NG-with-Application-Intelligence ausgestattet ist. Schwächen zeigte die Nokia-Firewall in erster Linie bei der Übertragung der 64-Bye-Pakete. In dieser Disziplin schaffte sie unidirektional einen maximalen Datendurchsatz von gut 261 MBit/s. Im bidirektionalen Modus halbierte sich der maximale Datendurchsatz dann und ging auf rund 134 MBit/s zurück. Beim Test mit 512-Byte-Paketen lieferte das Nokia-System dann unidirektional die volle Wirespeed und beeindruckte im bidirektionalen Betrieb mit immerhin über 780 MBit/s. Der Transport der ganz großen Pakete bremste das Nokia-System dann wieder, so dass die maximalen Durchsatzraten unidirektional bei gut 500 beziehungsweise 860 MBit/s und bidirektional bei rund 900 MBit/s lagen.

Ein Vertreter der Formel 1 der Firewall-Systeme stand dann mit 4-Your-Safety-RX-300 einschließlich einer Corrent-Turbo-Card von Siemens in unseren Labs. Auf dem System läuft VPN-1-pro von Check Point. Als einziges System im Test lieferte die Siemens-Lösung bei nahezu allen Messungen mit 1 GBit/s Wirespeed. Lediglich bei der Messung mit 64-Byte-Paketen wurden die Grenzen des Systems sichtbar. Hier ging der Datendurchsatz auf immer noch sehr gute fast 990 MBit/s zurück. Die Siemens-Lösung war ohne Zweifel die leistungsfähigste, aber auch relativ teuere Lösung im Testfeld.

Messergebnisse



Deutliche Probleme mit kleinen Datenrahmen zeigte dagegen Stonesofts Stonegate-SG-3000. Die Stonesoft-Firewall erreichte hier unidirektional rund 145 und bidirektional lediglich 72 MBit/s. Bei den Messungen mit größeren Datenrahmen und im unidirektionalen Modus näherte sich das System dann schon deutlich der Wirespeed, so schaffte die Stonegate-SG-3000 bei der Messung mit den größten Datenrahmen fast 977 MBit/s. Im bidirektionalen Datenverkehr reduzierten sich dann aber wieder die maximal möglichen Durchsatzraten. So schaffte die Stonesoft-Firewall hier bei der Messung mit 512-Byte-Paketen 443 und bei der Messung mit 1518-Byte-Paketen immerhin respektable 795 MBit/s.

Symantec ging mit der Beta-Version ihrer neuen Gateway-Security-5460 ins Rennen. Auch dieses Gerät zeigte Probleme mit den 64-Byte-Frames. Mit über 160 MBit/s unidirektional und gut 79 MBit/s bidirektional liegt die Symantec-Lösung ungefähr mit dem Enterasys-Gerät gleich auf. Bei größeren Datenrahmen und unidirektionaler Senderichtung kommt dann auch für Symantec Wirespeed in Sicht, die das Gerät bei der Messung mit den ganz großen Datenrahmen dann voll erreicht. Kamen 512-Byte-Frames zum Einsatz, lagen maximal immerhin 876 MBit/s an. Im bidirektionalen Betrieb gelangte die neue Symantec-Box mit 938 MBit/s allerdings nur bei der Messung mit ganz großen Datenrahmen in Wirespeed-Regionen und bremste noch bei der Verwendung von 512-Byte-Datenrahmen den Durchsatz auf 412 MBit/s herunter.

Fazit

Volle beziehungsweise nahezu volle Wirespeed bei allen Messungen schaffte lediglich die Siemens/Check-Point-Lösung 4-Your-Safety-RX-300, der die Corrent-Turbo-Card zusätzliche Flügel verlieh. Allerdings spielt diese Highend-Lösung neben der etablierten Nokia-Lösung, die nahezu doppelt so teuer ist wie das Siemens-Pendant, auch in einer anderen Preis-Liga, als die übrigen Systeme im Gigabit-Ethernet-Testfeld. Siemens zeigt, was technisch möglich ist, wer Gigabit-Durchsatz benötigt und bereit ist, den entsprechenden Turbo-Zuschlag zu bezahlen, kann hier sicherlich ein sehr performantes System bekommen. Recht wacker hat sich auch Enterasys mit ihrem XSR-3250-Router geschlagen, er zeigte zwar deutliche Probleme mit kleinen Datenrahmen, ist aber im Preis-Performance-Index der mehr als doppelt so teueren Lösung von Siemens/Check Point überlegen. Nokia, Symantec und Stonesoft bilden dann das Mittelfeld der Gigabit-Ethernet-Firewall-Systeme, sie schwächeln insbesondere bei der Übertragung kleiner Datenrahmen, erzielen aber auch schon bei größeren und großen Frames spürbare Leistungseinbrüche. Da das Nokia-System von der Positionierung her dabei mit Abstand das teuerste System im Testfeld ist, fällt es im Preis-Leistungs-Verhältnis deutlich zurück. In dieser Preisregion bekommt der IT-Verantwortliche derzeit bei Siemens spürbar mehr Power.

In den ermittelten Durchsatzraten hinkt das relativ teuere Genua-System deutlich hinter dem übrigen Testfeld her. Ursache hierfür ist, dass sich bei der Genua-Firewall die Application-Level-Gateway-Funktionalität nicht abschalten lässt und die Appliance deshalb bei vergleichbarer Hardware deutlich schlechtere Durchsatzraten erzielt, als der weniger sichere Wettbewerb. Die anderen Firewall-Systeme ließen sich flexibler konfigurieren und so unserer Testspezifikation besser anpassen. Messmethode und Ergebnisse haben jedenfalls allen unseren Überprüfungen standgehalten und die Systemkonfiguration lag in den Händen erfahrener Experten des jeweiligen Herstellers selbst.

IT-Verantwortliche, die die Anschaffung einer Firewall-Lösung erwägen, müssen wissen, dass sie immer einen Kompromiss zwischen Sicherheit und Performance schließen müssen. Und dabei soll ja das System auch noch ein möglichst günstiges Preis-Leistungsverhältnis bieten. Wichtig ist aber für die Aufrechterhaltung der Geschäftsprozesse, dass die Firewall die zu transportierenden Daten nicht ins Daten-Nirvana schickt. Denn ein hohes Sicherheitsniveau alleine nützt dann auch nicht mehr viel. Dann ist ein Seitenschneider die bessere Lösung, er schafft kostengünstig nahezu absolute Sicherheit – allerdings klappt es dann nicht mehr mit der Kommunikation. IT-Verantwortliche sollten möglichst genau ihre Sicherheits- und Performance-Anforderungen analysieren, klar definieren und auf ausführliche Tests und einen der Anschaffung vorhergehenden Probebetrieb setzen. *Dipl.-Ing. Thomas Rottenau, Prof. Dr. Bernhard G. Stütz, [dg]*