6 Gigabit-Ethernet-VPN-Appliances

Stau am Ende des Tunnels

Virtual-Private-Networks sollen eine gesicherte Kommunikation zwischen zwei Netzen über eine unsichere Verbindung garantieren. Hierfür schaffen solche VPN-Systeme exklusive, kryptografisch geschützte Verbindungen. Wie schnell Unternehmen auf solchen »privaten Datenautobahnen« unterwegs sein können, sollte ein Vergleichstest in unseren Real-World Labs an der FH Stralsund klären.

Virtuelle private Netzwerke, neudeutsch Virtual-Private-Networks oder kurz VPN, sollen einer geschlossenen Gruppe von Rechnern eine geschützte Kommunikation über ein unsicheres Netz hinweg erlauben. Die logisch geschlossene Verbindung, auch VPN-Tunnel genannt, wird durch kryptografische Algorithmen realisiert, die die zu schützenden Datenströme verschlüsseln und an der Gegenstelle wieder entschlüsseln. Für diese Verschlüsselung gibt es eine ganze Reihe von Standards, wie DES, 3DES oder AES. Über die Sicherheit solcher Verbindungen entscheidet wie bei anderen kryptografischen Verfahren auch nicht zuletzt die Länge der verwandten Schlüssel. Mechanismen wie Authentisierung und Autorisierung sorgen zusätzlich dafür, dass keine unerwünschten User in das private Netz eindringen. Technisch realisieren Unternehmen ein solches VPN, indem sie an den Übergangsstellen zwischen sicherem und unsicherem Netzwerk ein VPN-System installieren.

Die wesentliche Verschlüsselungsfunktionalität ist zumeist in Software abgebildet, was bedeutet, dass die Funktionalität sehr rechenintensiv ist und eine gute Performance eine entsprechend leistungsfähige Hardware voraussetzt. Es gibt aber auch VPN-Lösungen, die Hardware-näher realisiert sind und dann entsprechend leistungsfähiger sein können. In vielen Fällen bietet es sich an, VPN-Appliances einzusetzen, das sind quasi schlüsselfertige Lösungen, die aus der VPN-Software und der dazugehörenden Hardware bestehen. Die VPN-Appliance-Hersteller teilen die verschiedenen VPN-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 VPN-Appliances haben wir dagegen schlicht nach den vorhandenen LAN-Ports in Fast-Ethernet- und Gigabit-Ethernet-Systeme eingeteilt.

In den seltensten Fällen sind VPN-Appliances dedizierte VPN-Geräte. Zumeist handelt es sich um IT-Security-Geräte, die neben der VPN-Funktionalität weitere Security-Features wie Firewall oder Intrusion-Detection/Prevention in sich vereinen und dann auch als »All-in-one-Appliances« angeboten werden. Darüber hinaus integrieren die Hersteller auch zunehmend IT-Security-Funktionalität in die klassischen aktiven Netzwerkkomponenten, wie Switches oder Router. Und auch Kommunikationsserver werden zunehmend mit Security-Features ausgestattet, so dass das Feld der Produkte, die VPN-Funktionalität bieten, recht vielfältig und heterogen ist.

So lange VPN-Systeme über öffentliche WAN-Verbindungen und via Internet genutzt werden, ist der Flaschenhals zumeist das WAN. Hier sind 100 MBit/s oder gar 1000 MBit/s Datendurchsatz nur in seltenen Fällen ein Thema. Das Gros der Sicherheitsbedrohungen liegt aber heutzutage innerhalb der Unternehmensnetze. Daher gehen immer mehr Unternehmen dazu über, VPN- und Firewall-Systeme einzusetzen, um einzelne Segmente oder Teilnetze des eigenen Unternehmensnetzes gegen interne Bedrohungen einzusetzen und schützenswerte Datenströme mit VPNs intern abzusichern. Auch Betreiber größerer Wireless-LAN-Installationen müssen

Report-Card / interaktiv unter www.networkcomputing.de

VPN-Performance 3DES-Durchsatz

	Gewichtung	Siemens 4YourSafety	Netscreen/Juniper ISG 2000	Lucent VPN Firewall Brick 1100	Astaro SunFireV20z Server	Borderware Steelgate	Telco Tech Liss II
Max. Durchsatz 512 Byte unidirektional	20%	5	5	4	1	1	1
Max. Durchsatz 512 Byte bidirektional	20%	5	5	2	1	1	1
Max. Durchsatz 1024 Byte unidirektional	20%	5	5	5	1	1	1
Max. Durchsatz 1024 Byte bidirektional	20%	5	5	3	1	1	1
Max. Durchsatz 64 Byte unidirektional	10%	4	4	1	1	1	1
Max. Durchsatz 64 Byte bidirektional	10%	4	3	1	1	1	1
Gesamtergebnis	**100%**	**4,8**	**4,7**	**3**	**1**	**1**	**1**
		A+	**A**	**C**	**E**	**E**	**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: >= 800 MBit/s = 5; >= 600 MBit/s = 4; >= 400 MBit/s = 3; >= 200 MBit/s = 2; < 200 MBit/s = 1;

ihren Usern eine Vielzahl an VPN-gesicherten Verbindungen offerieren. Diese Trends bedeuten aber, dass die Anforderungen an die verfügbaren Bandbreiten mit den Anforderungen an andere aktive LAN-Komponenten identisch sind und die private Datenautobahn auch in geschützten Bereichen die heute als Standard geltenden Durchsatzraten offerieren muss.

Das Real-World-Labs-Test-Szenario

Im Mittelpunkt unseres VPN-Vergleichstests, den wir in unseren Real-World Labs an der FH Stralsund durchführten, stand die Performance, die solche Systeme derzeit zur Verfügung stellen. Wir wollten wissen, wie stark die VPN-Funktionalität die Leistungsfähigkeit der reinen Hardware vermindert, beziehungsweise ob die heute verfügbaren Systeme sichere Verbindungen mit Wirespeed erlauben. Darüber hinaus interessierte es 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. Geeignete, durchsatzstarke Security-Appliance-Systeme sollten für die notwendige Sicherheit und Performance sorgen. Zugleich sollte die Appliance den Aufbau eines VPNs im LAN ermöglichen. Dieses VPN sollte die performante und gegen interne Bedrohungen gesicherte Kommunikation zwischen den Servern der verschiedenen Abteilungen, beispielsweise Forschung & Entwicklung oder Produktion, ermöglichen. Um die Server nicht mit der durch die kryptografische Verarbeitung der Daten erforderliche Rechenarbeit zusätzlich zu belasten, sollten vorgeschaltete VPN-Appliances den Betrieb des performanten VPNs zwischen den Servern garantieren.

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 VPN-Performance, also die unidirektionalen und bidirektionalen Datendurchsatzraten im VPN-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 Verfü-

Info

Das Testfeld

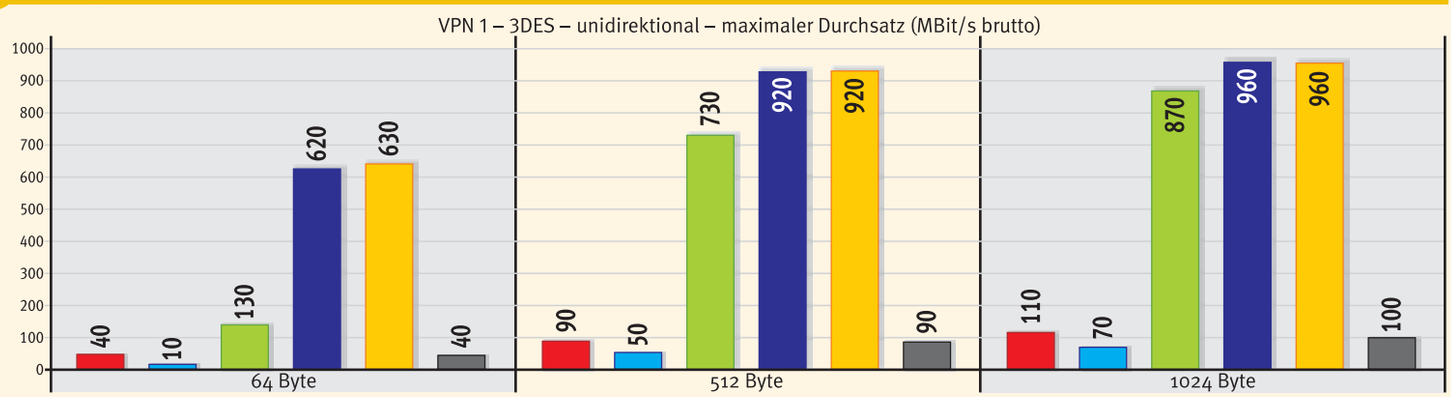
Gruppe 1: Fast-Ethernet-Appliances

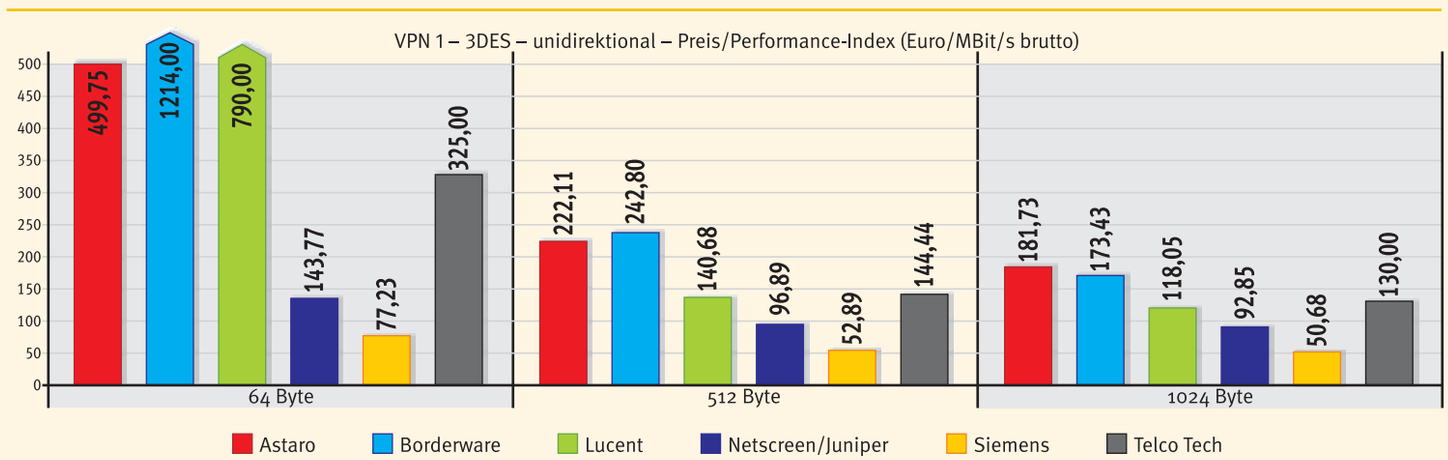
Astaro	timeNET secuRACK Enterprise 2 powered by Astaro Security Linux V5
Bintec	VPN Access 25
Bintec	VPN Access 1000
Cisco	PIX 515E Security Appliance
Clavister	M460
D-Link	DFL-700 Network Security Firewall
Gateprotect	gateProtect Firewall
Innominate	Innominate mGUard
Lucent	VPN Firewall Brick 350
SonicWALL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

Messergebnisse – VPN-Performance





gung. Insgesamt gingen 14 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 bildeten 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 »4YourSafety RX 300« sowie Telco Techs »LiSS II secure gateway pro giga«. Wie sich die Fast-Ethernet-VPN-Appliances in unserem Test verhielten, steht im Testbericht, den wir im Network Computing Spezial Infrastruktur veröffentlicht haben. Die Testergebnisse der Gigabit-Ethernet-VPN-Appliances sind dem vorliegenden Artikel zu entnehmen.

Durchsatzraten und Datenverlustverhalten

Zur Messung der maximal möglichen Durchsatzraten sowie des lastabhängigen Datenrahmenverlustverhaltens haben wir mit Hilfe der Spirent-Smartbits-Lastgeneratoren/Analysatoren die VPN-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 VPN-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, dass die überforderte Appliance für entsprechende Datenverluste sorgt, die diverse »Kommunikationsstörungen« im Netz- und Arbeitsbetrieb verursachen können.

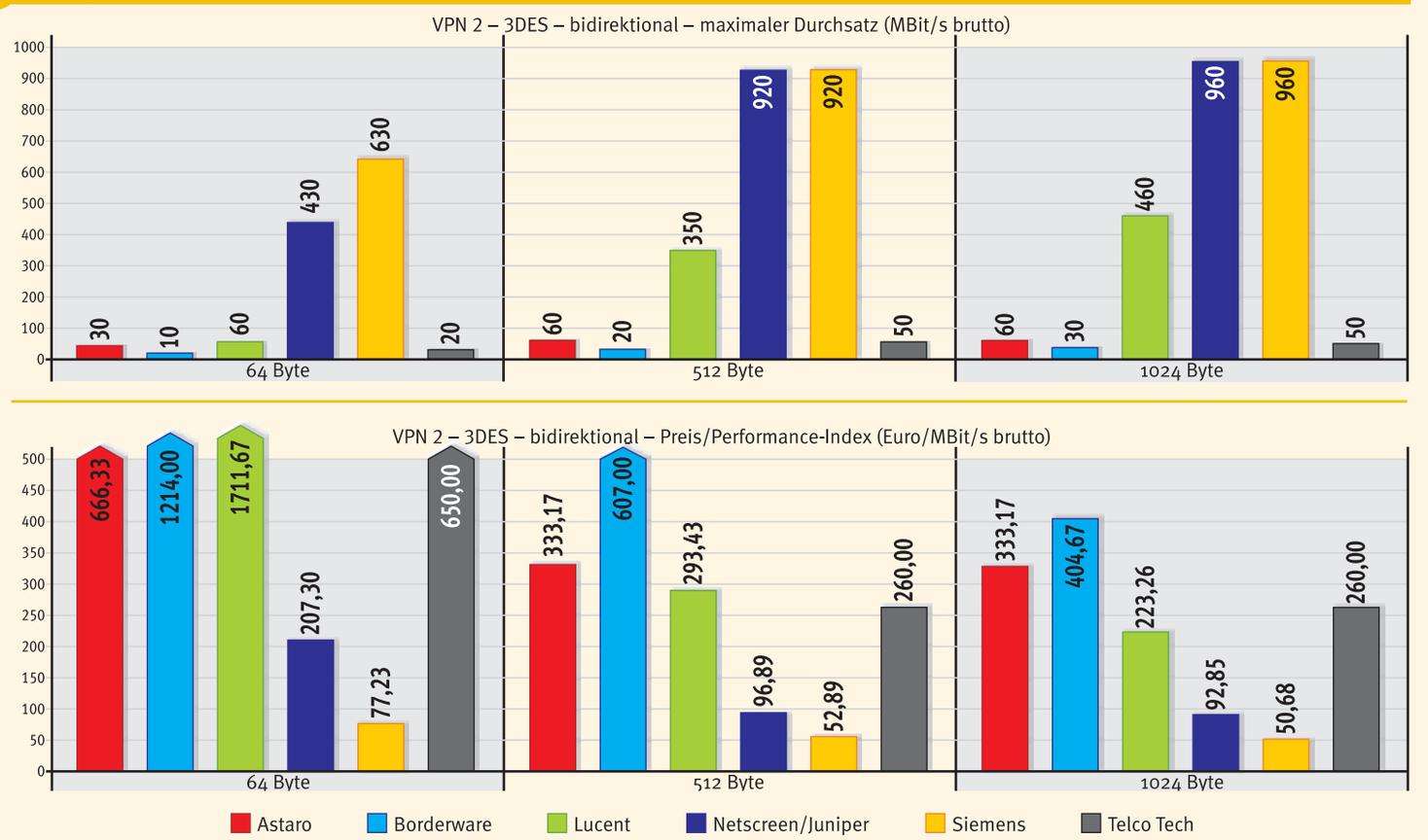
Auswirkungen von Datenverlusten

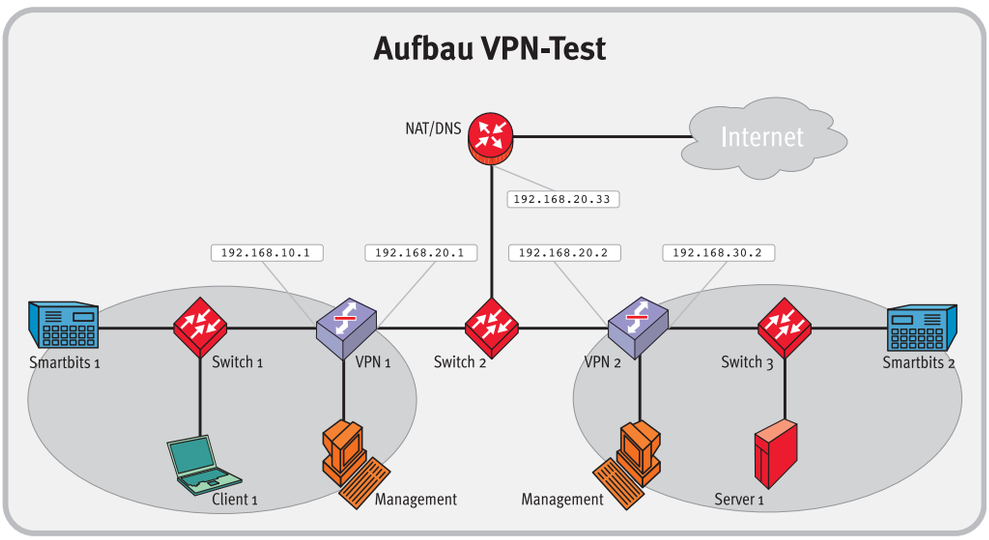
Für die Beurteilung des Verhaltens der Systeme im Testfeld, die wir mit Datenströmen bestehend aus den unterschiedlichsten Frame-Formaten belastet haben, ist es von besonderem Interesse, zu betrachten, welche Lasten und Frame-Größen in realen Unternehmensnetzen vorkommen. Bei klassischen Dateitransfers 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

Messergebnisse – VPN-Performance





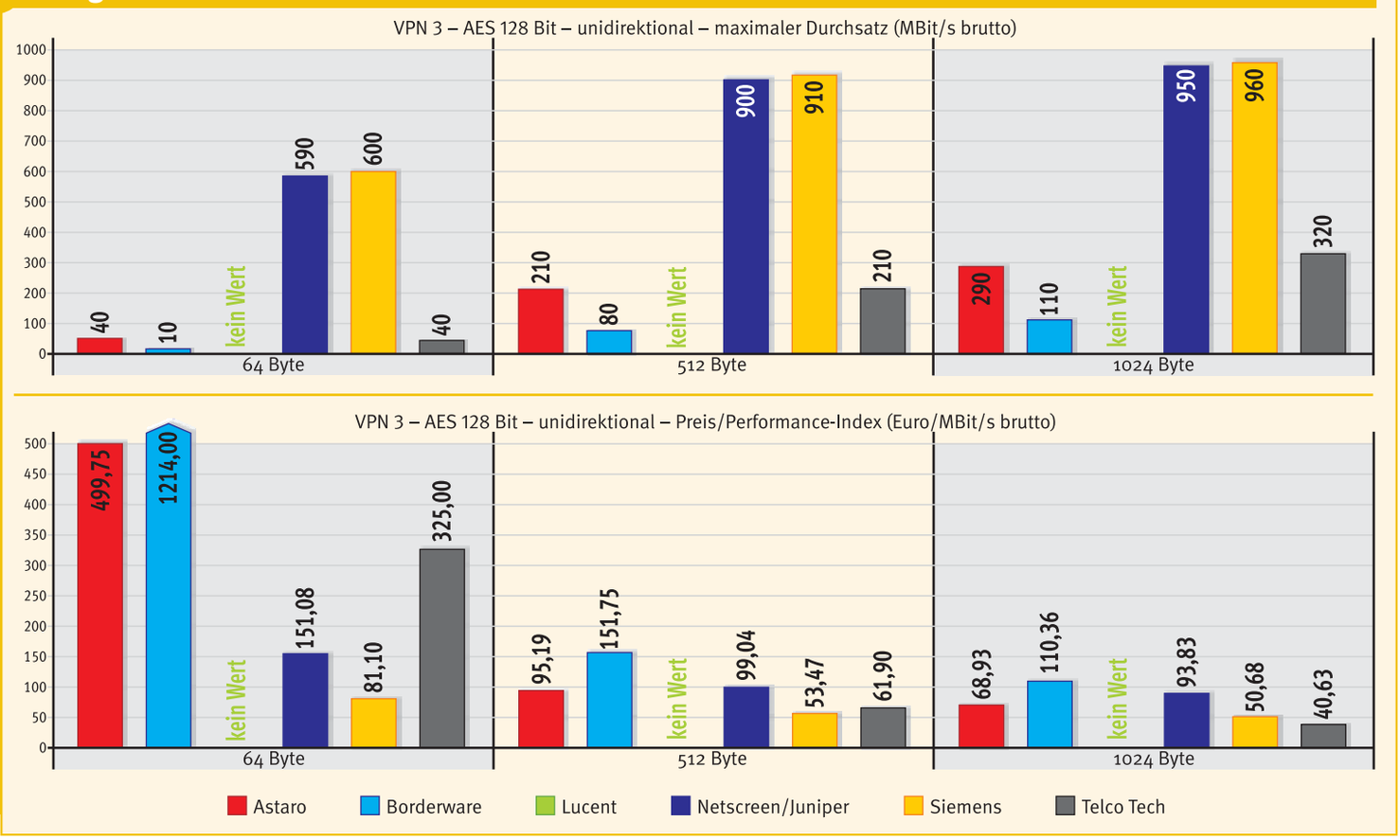
64 Byte groß sind. Die übrigen rund 50 Prozent der zu transportierenden Datenrahmen streuen über alle Rahmengrößen von 128 bis 1518 Byte. Für die Übertragung von Real-Time-Applikationen ist zunächst das Datenverlustverhalten von entscheidender Bedeutung. Für Voice-over-IP gilt beispielsweise: Ab fünf Prozent Verlust ist je nach Codec mit deutlicher Verschlechterung der Übertragungsqualität zu rechnen, zehn Prozent führen zu einer massiven Beeinträchtigung, ab 20 Prozent Datenverlust ist die Telefonie definitiv nicht mehr möglich. So verringert sich der R-Wert für die Sprachqualität gemäß E-Modell nach ITU G.107 schon bei zehn 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 Security-Appliances verzichtet.

Das Testverfahren

Insgesamt haben wir sechs VPN-Testreihen durchgeführt. In der ersten Testreihe haben wir einen VPN-Tunnel zwischen den jeweils zu testenden Appliances gleichen Typs aufgebaut und unidirektionale Datenströme erzeugt. In der zweiten Testreihe haben wir dann mit bidirektionalem Datenverkehr gearbeitet und parallel in beiden Richtungen zwischen den VPN-Systemen 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. Die Datenströme bestanden jeweils aus Datenrahmen konstanter Größe, wobei wir mit 64, 512 und 1024

Messergebnisse – VPN-Performance



Features

VPN-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
Anzahl unabhängiger (nicht geswitchter) LAN-Ports						
Anzahl Gigabit-Ethernet-Ports	6	6	4	8	5	6
Anzahl Fast-Ethernet-Ports	–	6	7	28	–	–
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.
Hardware/Betriebssystem						
Prozessor	AMD Opteron 1800	3000 MHz	2.4 GHz	Dual Power PC 1000Mhz	P4 Xeon 2.4 Ghz.	Intel Xeon 2800 MHz
Arbeitsspeicher in MByte	2048	2000	2000	1000	512	512
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
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
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
Listenpreis in Euro für Teststellung zzgl. MwSt.	19 990	12 140	102 700	89 140	48657,24	13 000

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

Byte großen Frames gearbeitet haben. 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 Durchsatzraten 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 weniger als ein Prozent der Daten verliert. Die hierbei erzielbaren Werte liegen zum Teil 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 insgesamt maximal 2 GBit/s an.

In der ersten und zweiten Testreihe mussten die VPN-Geräte das VPN mit 3DES aufbauen. Da die meisten Teststellungen auch eine Verschlüsselung nach AES mit 128 Bit ermöglichten, haben wir die Messungen dann mit dem anderen kryptografischen Verfahren wiederholt. In unsere Report-Card-Wertung fließen allerdings nur die Messergebnisse mit 3DES ein, da wir in unserer Real-World-Labs-Test-Ausschreibung ausschließlich diesen Algorithmus verlangt hatten.

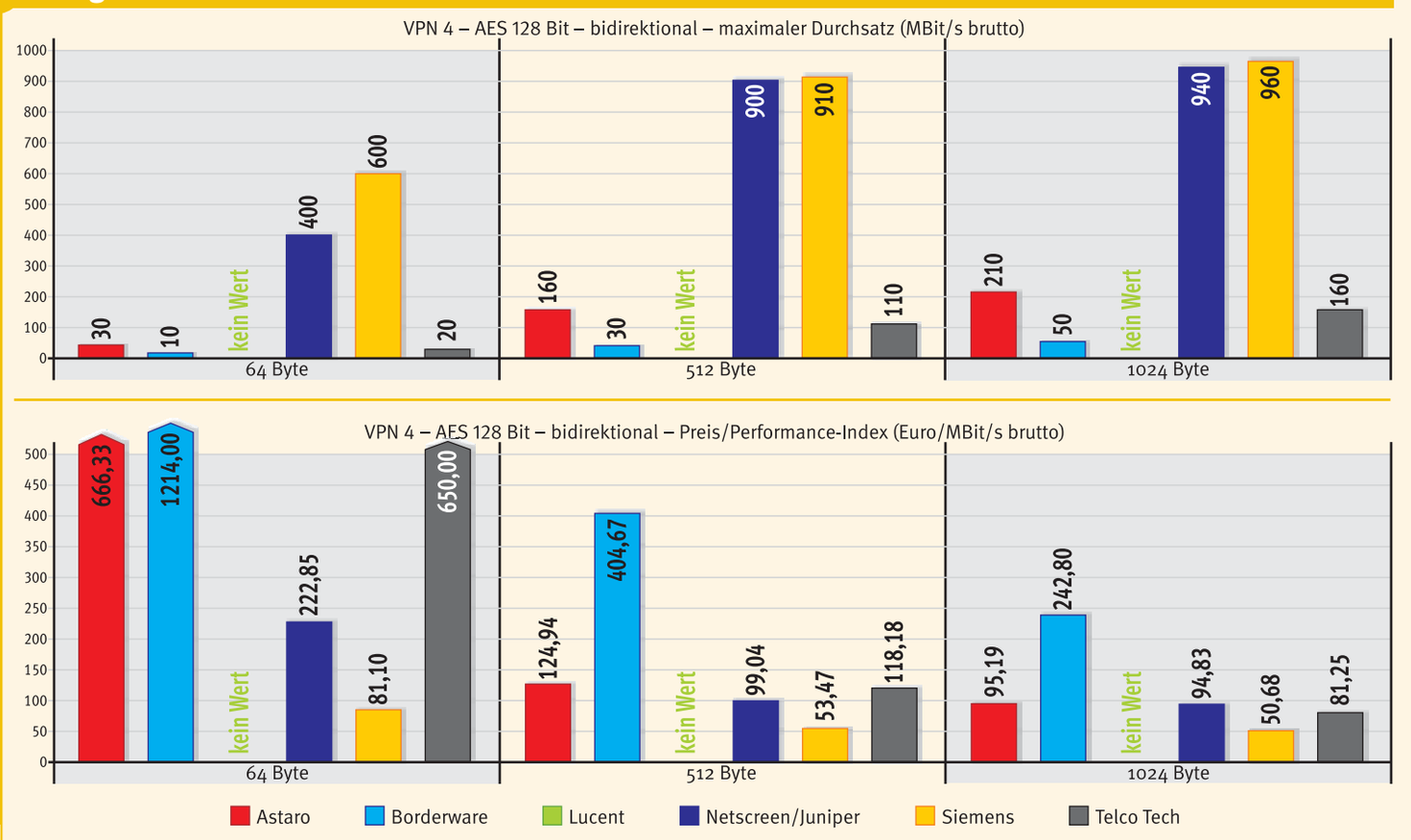
Verhalten der Systeme im Test

Kein Test hat bislang unser Testfeld so stark gespalten wie unser Gigabit-VPN-Test. Schon im anspruchlosesten Szenario, der 3DES-Verschlüsselung im unidirektionalen Betrieb, hat sich deutlich gezeigt, dass Gigabit-Performance heute nur mit Highend-Hardware möglich ist. Leistungsschwächere Systeme mit Gigabit-Ethernet-Schnittstellen auszustatten bringt dagegen nicht allzu viel an Leistungsplus gegenüber guten Fast-Ethernet-Lösungen.

Die Nase vorn hatte erneut Siemens mit ihrer 4-Your-Safety-RX-300, auf der Check Points VPN-1 und Firewall-1 liefen. Die Appliance schaffte einen maximalen Durchsatz bei den unidirektionalen Messungen mit 3DES-Verschlüsselung von immerhin 630 MBit/s mit 64-Byte-Paketen. Mit größeren Frames kam das System dann noch deutlich besser zurecht, so lagen bei der Messung mit 512-Byte-Paketen 920 und mit 1024-Byte-Paketen von 960 MBit/s an. Diese Bandbreiten standen dann auch noch bei Volllast zur Verfügung. Und auch bei den bidirektionalen Messungen schaffte die RX-300 praktisch identische Durchsatzraten – je Senderichtung versteht sich. Auch der Wechsel auf AES-128-Bit-Verschlüsselung änderte an den Durchsatzraten nicht viel, diese gingen hier dann beispielsweise bei der unidirektionalen Messung mit 64-Byte-Frames auf 600 MBit/s zurück. Insgesamt reicht die Leistung des Siemens-Systems für die Referenz-Auszeichnung von Network Computing. Deutlich aber im Vergleich zu anderen Systemen nicht dramatisch hinter Wirespeed zurück blieb das System nur bei unseren Messungen mit den kleinsten Frames.

Nur ganz knapp hinter der Siemens-RX-300 lag die ISG-2000 von Netscreen/Juniper. Bei den unidirektionalen 3DES-Messungen lieferte sich die ISG-2000 ein Kopf-an-Kopf-Rennen mit Siemens. Bei der Messung mit 64-Byte-Paketen kam die ISG-2000 auf 620 MBit/s – 10 MBit/s weniger als die RX-300. Verwendeten wir größere Frames,

Messergebnisse – VPN-Performance



dann konnte das System von Netscreen/Juniper mit Siemens gleichauf ziehen. Ähnlich sehen auch die Ergebnisse der bidirektionalen Messungen aus. Einen kleineren Ausrutscher leistete sich die ISG-2000 hier lediglich bei der Messung mit 64-Byte-Frames. Hier lag das System mit einem Durchsatz von 430 MBit/s um immerhin 200 MBit/s hinter Siemens. Waren die Frames größer, dann konnte die Netscreen/Juniper-Appliance wieder mit Siemens gleich ziehen. Und auch durch Volllast ließ sich die ISG-2000 nicht weiter beeinträchtigen, die gemessenen Maximaldurchsätze standen praktisch immer zur Verfügung. Bei Vergleichsmessungen mit AES-128-Bit-Verschlüsselung ging auch die Performance der ISG-2000 ähnlich wie die der RX-300 etwas zurück.

Nicht langsam, aber signifikant langsamer als die Systeme von Siemens und Netscreen/Juniper arbeitete Lucents VPN-Firewall-Brick-1100. Insbesondere mit 64-Byte-Frames kam die Brick-1100 deutlich schlechter zurecht. Hier standen unidirektional mit 3DES-Verschlüsselung noch 130 MBit/s zur Verfügung. Mit größeren Frames kam auch das Lucent-System besser zurecht. So schaffte die Brick-1100 mit 1024-Byte-Frames dann immerhin unidirektional 870 MBit/s. Bei den bidirektionalen Messungen ging die Leistung der Lucent-Appliance dann noch einmal spürbar zurück, so dass bei der bidirektionalen Messung mit 64-Byte-Paketen gerade noch 60 MBit/s zur Verfügung standen. Und auch bei den größeren Frames waren maximal 460 MBit/s drin.

Deutlich überfordert zeigte sich Astaros Sun-Fire-V20z-Opteron mit Astaro-Security-Linux V5, die sich im Firewall-Performance-Test (siehe Network Computing 10-11/2004, S.12 ff.) noch recht gut behaupten konnte. So lagen hier unidirektional mit 64-Byte-Frames und 3DES-Verschlüsselung noch 40 MBit/s an. Mit 1024-Byte-Frames schaffte das Astaro-System dann 110 MBit/s – nur geringfügig mehr, als Fast-Ethernet-Wirespeed, und zu wenig, als noch über den günstigeren Preis punkten zu können. Im bidirektionalen Betrieb mit 3DES-Verschlüsselung blieb das System dann durchweg unter Fast-Ethernet-Wirespeed. Mit AES-128-Bit-Verschlüsselung war die Performance der Astaro-Appliance etwas besser. Bestleistung war hier ein Durchsatz von 290 MBit/s mit den größten Frames.

Borderwares Steelgate-Firewall+VPN-Appliance war ebenso wie Telco Techs Liss-II-Secure-Gateway-Pro-Giga in der Gigabit-Ethernet-Liga schlecht platziert. Beide Systeme blieben generell bei den Messungen mit 3DES-Verschlüsselung hinter Fast-Ethernet-Wirespeed zurück. Bei den Messungen mit AES-128-Bit-Verschlüsselung sahen die Ergebnisse insbesondere bei der Liss-II etwas besser aus, aber wir hatten als entscheidendes Kriterium 3DES-Verschlüsselung verlangt. Die Ergebnisse der Systeme von Borderware und Telco Tech zeigen, dass es nicht viel bringt, relativ preisgünstige Systeme, die im Fast-Ethernet-Segment durchaus gut aufgehoben sein mögen, mit Gigabit-Ethernet-Schnittstellen zu versehen, ohne für die notwendige Performance der übrigen Komponenten zu sorgen.

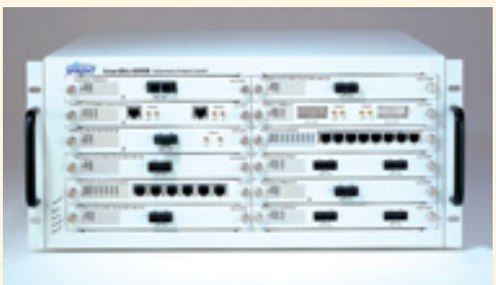
Fazit

In Gigabit-Ethernet-VPN-Appliances investieren IT-Verantwortliche, die durchsatzstarke geschützte Verbindungen – zumeist innerhalb eines LANs – benötigen. Andernfalls genügen deutlich preisgünstigere Fast-Ethernet-Systeme. Und für solche Szenarien ist der »Stau im Tunnel« schon vorprogrammiert, wenn die Verantwortlichen beim Netzdesign davon ausgehen, dass Gigabit-Durchsätze drin sind, wenn Gigabit-Ethernet drauf steht, was IT-Verantwortliche von anderen Netzwerkkomponenten in der Regel auch erwarten. Denn über eine Tatsache sollten die vorliegenden Testergebnisse nicht hinweg täuschen: Von wirklicher Wirespeed sind

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 einzusetzenden Krypto-Verfahren auf 3DES festgelegt. Wenn die Systeme auch AES mit 128- und/oder 256-Bit-Verschlüsselung unterstützten, dann haben wir die Messungen mit diesen Algorithmen wiederholt. 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. 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 Durchsatzraten 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 weniger als ein Prozent der Daten verliert. Die hierbei erzielbaren Werte liegen zum Teil 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.

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 feststellen 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 und 1024 Byte verwendet.

Die einzelnen Netzsegmente des Testaufbaus 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 VPN-Konfiguration und -Funktion jeweils vor den einzelnen Testläufen überprüft.

auch die gut platzierten Highend-Systeme noch mehr oder weniger weit entfernt.

Mit Abstand am besten arbeiteten im aktuellen Test die Lösungen von Siemens und Netscreen/Juniper, aber auch sie blieben insbesondere beim Betrieb mit kleinen Frames deutlich hinter Wirespeed zurück. Dabei sollten IT-Verantwortliche nicht übersehen, dass in den meisten Netzen rund 50 Prozent aller Frames nur 64 Byte lang sind. Hier kann es also auch bei den derzeit besten Systemen noch durchaus zu Problemen kommen. Mit Abstand am meisten Performance fürs Geld bekommen IT-Verantwortliche derzeit bei Siemens, so lag die RX-300 preislich deutlich günstiger als die ISG-2000. Die teuerste Lösung im Test, Lucents Brick-1100, vermochte mit den beiden besser platzierten Systemen dagegen nicht mitzuhalten. Lucent wäre sicherlich gut beraten, ihre Hardware zu überarbeiten, um nicht nur im Preis, sondern auch in der Durchsatzleistung Highend-Regionen zu erreichen.

Die Verantwortlichen bei Astaro sind sicherlich auf dem richtigen Weg, in Sachen 3DES-Performance reicht die aktuelle Sun-Plattform aber noch nicht aus. Bei entsprechend performanterer Hardware und einer weiterhin moderaten Preispolitik hätte Astraro durchaus Chancen im Highend-VPN-Segment. Schlicht überfordert waren die preislich noch einmal deutlich unter Astaro angesiedelten Systeme von Borderware und Telco Tech. Mit Fast-Ethernet-Adaptern ausgestattet wären die beiden Systeme im 100-MBit/s-Segment sicherlich besser aufgehoben. Denn der Einbau von Gigabit-Ethernet-Schnittstellen macht eine VPN-Appliance noch nicht zum Highend-System.

Generell ist die Ver- und Entschlüsselung kryptografisch geschützter Daten mit aufwändiger Rechenarbeit verbunden. Dabei gilt, dass ein höheres Sicherheitsniveau auch mit einer größeren erforderlichen Rechenleistung verbunden ist. Wenn nun VPN-Appliances innerhalb performanter Fast- oder Gigabit-Ethernet-Netze eingebunden werden, um vor internen Bedrohungen zu schützen, dann müssen sie in ihren Durchsatzraten und Leistungseigenschaften den übrigen aktiven Komponenten des Netzes entsprechen. Dies geht auf Grund der erforderlichen Rechenleitung nur, wenn die Hersteller ihre VPN-Appliances mit sehr leistungsfähiger Hardware in Form von Haupt-CPU oder speziellen Krypto-Prozessoren ausstatten, was Astaro, Borderware und Telco Tech dringend zu empfehlen wäre.

IT-Verantwortliche, die die Anschaffung einer VPN-Lösung planen, 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. Ein hohes Sicherheitsniveau alleine nützt nicht viel, wenn die Security-Appliance zum Flaschenhals wird. IT-Verantwortliche sollten daher 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]