Infrastruktur

11 Fast-Ethernet-VPN-Appliances

Stau im Tunnel

Für eine gesicherte Kommunikation zwischen zwei Netzen über eine unsichere Verbindung sorgen VPN-Tunnel. Wie schnell Unternehmen in solchen Tunneln unterwegs sein können, sollte ein Vergleichstest in unseren Real-World Labs 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 Securitry-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 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.

Reportcard / interaktiv unter www.networkcomputing.de

VPN-Performance 3DES-Duchsatz

	Gewichtung	Lucent Brick 350	Bintec VPN Access 1000	Clavister M 460	Astaro timeNET secuRACK	Sonicwall Pro 3060	Innominate mGUard	Gateprotect gateProtect Firewall	Zyxel ZyWALL 70	Cisco PIX 515E	Bintec VPN Access 25	D-Link DFL-700
Max. Durchsatz 512 Byte unidirektional	20%	5	5	5	4	4	2	2	2	2	1	1
Max. Durchsatz 512 Byte bidirektional	20%	5	4	3	2	2	1	1	1	1	1	1
Max. Durchsatz 1024 Byte unidirektional	20%	5	5	5	5	4	4	3	3	2	1	1
Max. Durchsatz 1024 Byte bidirektional	20%	5	5	3	3	2	2	2	2	1	1	1
Max. Durchsatz 64 Byte unidirektional	10%	3	2	3	2	3	1	1	1	1	1	1
Max. Durchsatz 64 Byte bidirektional	10%	2	1	2	1	2	1	1	1	1	1	1
Gesamtergebnis	100%	4,5	4,1	3,7	3,1	2,9	2	1,8	1,8	1,4	1	1
		A-	B+	B-	C	C	D	D	D	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: ›= 80 MBit/s = 5; ›= 60 MBit/s = 4; ›= 40 MBit/s = 3; ›= 20 MBit/s = 2; ‹= 20 MBit/s = 1;

Das Real-World-Labs-Test-Szenario

Im Mittelpunkt unseres ersten diesjährigen 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. Eine geeignete, durchsatzstarke Security-Appliance sollte 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 und Produktion, ermöglichen. Um die Server nicht mit der durch die kryptographische 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 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

Info

Das Testfeld

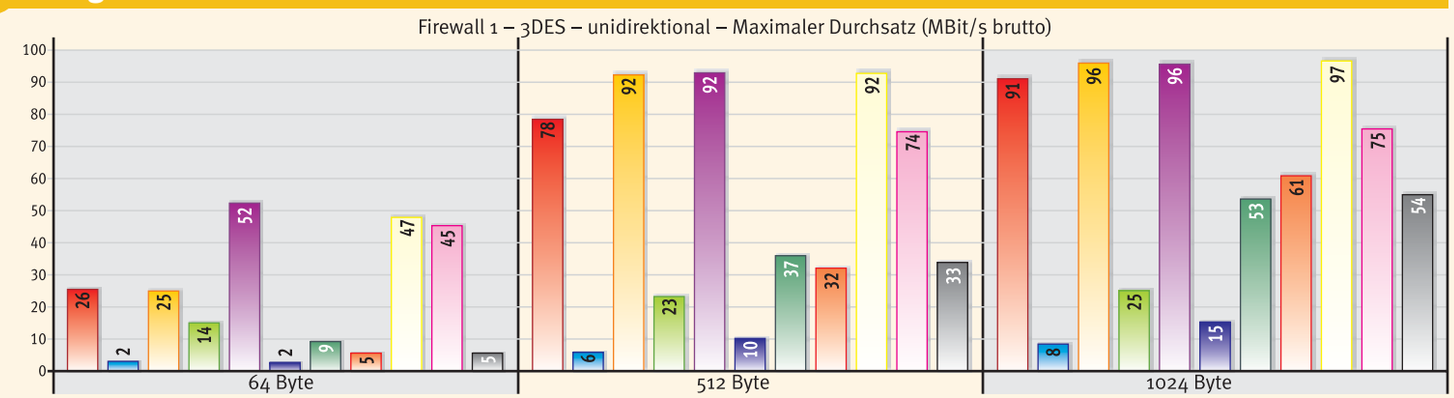
Gruppe 1: Fast-Ethernet-Appliances

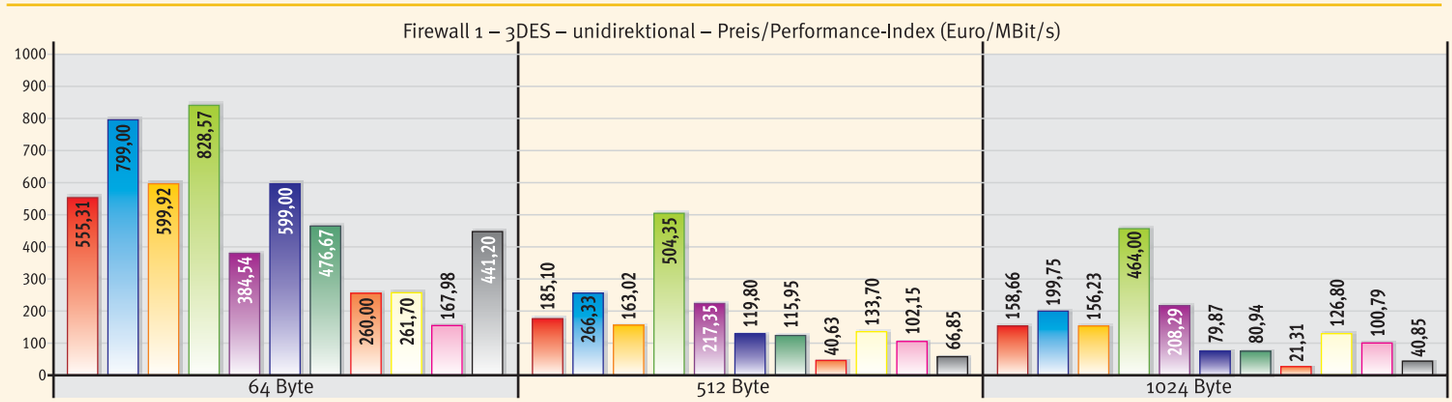
Astaro	timeNET secuRACK Enterprise 2 powered by Astaro Security Linux V5
Bintec	VPN Access 25
Bintec	VPN Access 1000
Cisco	PIX 515E Security Appliance
Clavister	M460
D-Link	DFL-700 Network Security Firewall
Gateprotect	gateProtect Firewall
Innominate	Innominate mGUard
Lucent	VPN Firewall Brick 350
SonicWALL	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	4 your Safety RX 300
Telco Tech	LiSS II secure gateway pro giga
Watchguard	Firebox Vclass V100

Messergebnisse – VPN-Performance





»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 »4 your Safety RX 300«, Telco Techs »LiSS II secure gateway pro giga« sowie Watchguards »Firebox Vclass 100«. Wie sich die Fast-Ethernet-VPN-Appliances in unserem Test verhielten, steht im hiermit vorliegenden Testbericht. Die Veröffentlichung der Ergebnisse der Gigabit-Ethernet-VPN-Appliances ist dann für das Network Computing Special Sicherheit & Sicherung 2004 vorgesehen.

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 100 MBit/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.

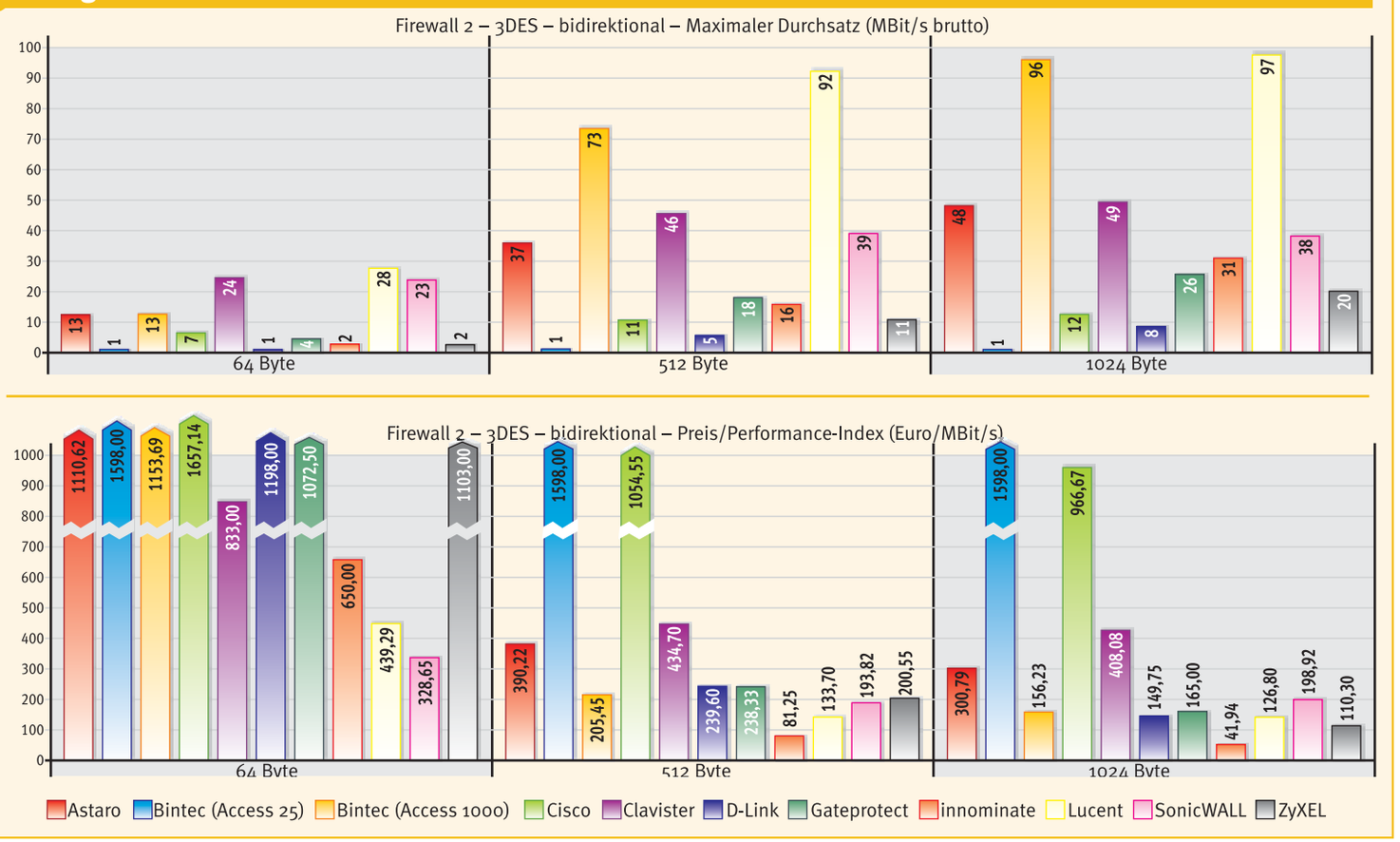
Auswirkungen von Datenverlusten

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 arbeitet mit 214 Byte großen 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 fünf Prozent Verlust ist je nach Codec mit deutlicher Verschlechterung der

Messergebnisse – VPN-Performance



Übertragungsqualität zu rechnen, zehn 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 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.

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 Byte großen Frames gearbeitet haben.

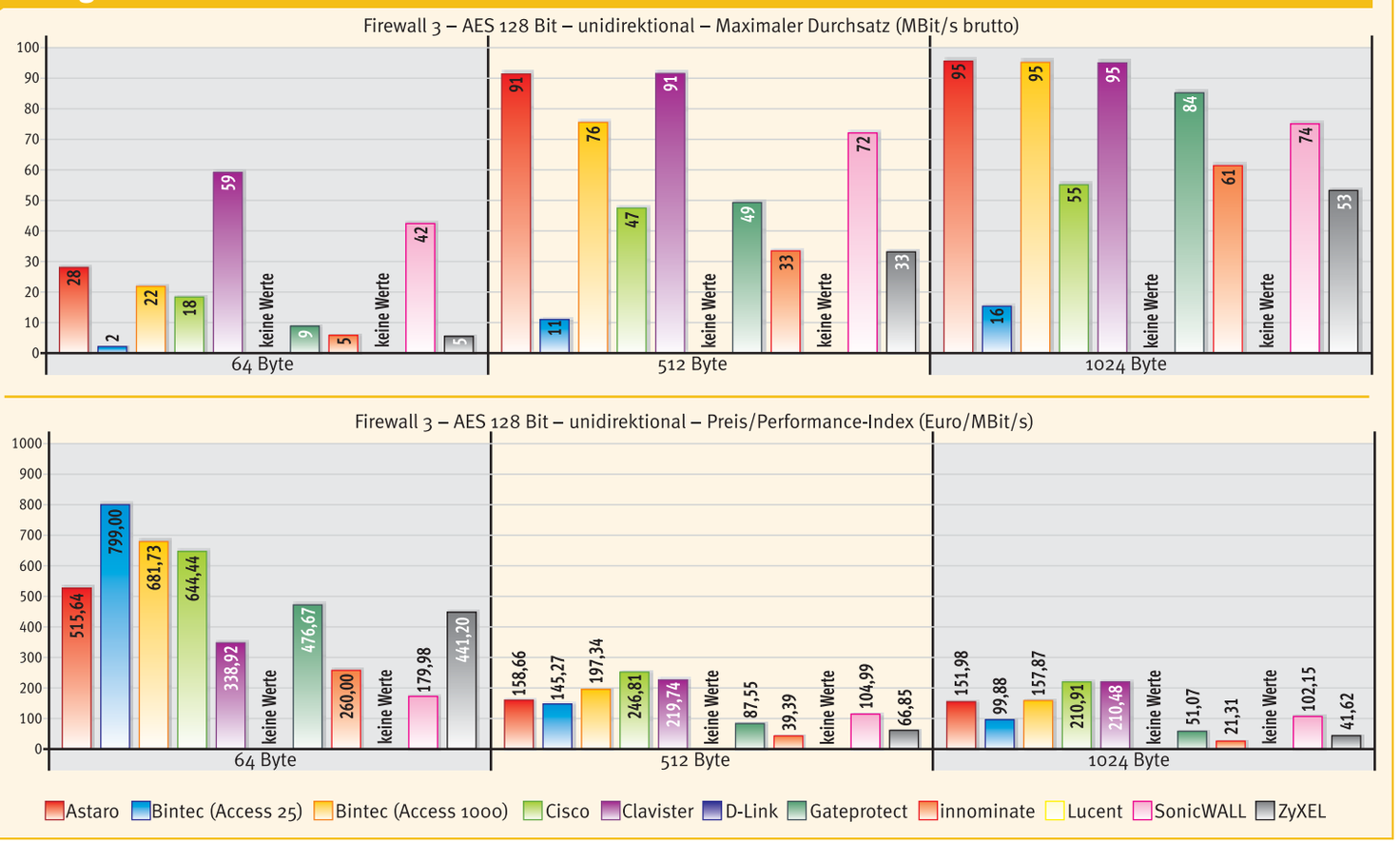
Außerdem haben wir für jede Messreihe neben den standardisierten, in immer gleichen Lastschritten erfolgenden Verlustratenmessungen für jedes System und jede Framegröße den Punkt der optimalen Last und somit die maximalen technisch möglichen Durchsatzraten unter optimalen Bedingungen ermittelt. Hierzu 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 100 MBit/s. Bidirektional liegen dann natürlich maximal 200 MBit/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 und zum Teil auch mit 256 Bit ermöglichten, haben wir die Messungen dann mit den anderen kryptographischen Verfahren wiederholt.

Verhalten der Systeme im Test

Deutliche Probleme mit kleinen Datenrahmen hatte Astaros Timenet-Securack-Enterprise-2, so schaffte das Asttro-Gerät hier unter optimalen Bedingungen einen Bruttodurchsatz von 26 MBit/s bei der unidirektionalen 3DES-Messung. Bidirektional mussten sich die Datenströme die Performance teilen, so dass je Senderichtung noch rund 13 MBit/s anlagen. Unter weiter ansteigender Last gingen die Durchsatzraten dann noch spürbar zurück, so dass die Appliance unter Volllast bei der bidirektionalen Messung quasi völlig dicht machte: Durchsatz 0,09 MBit/s. Bei den Messungen mit AES-Verschlüsselung war die Appliance geringfügig schneller, so erreichte sie beispielsweise mit AES-128-Bit-Verschlüsselung im unidirektionalen Betrieb mit 64-Byte-Paketen 28 MBit/s und mit 1024-Byte-Paketen 91 MBit/s. Mit größeren Datenrahmen kam das Astaro-System insgesamt deutlich besser zurecht, so er-

Messergebnisse – VPN-Performance



Features

VPN-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.

reichte es unidirektional mit 3DES-Verschlüsselung und 512-Byte-Paketen einen maximalen Durchsatz von 78 und mit 1024-Byte-Paketen von 91 MBit/s. Insgesamt kam die Astaro auf moderate Durchsatzraten, wobei die Schwäche im Bereich der kleinen Datenrahmen durchaus zu Problemen führen kann und die Performance insbesondere im bidirektionalen Betrieb noch verbessert werden sollte.

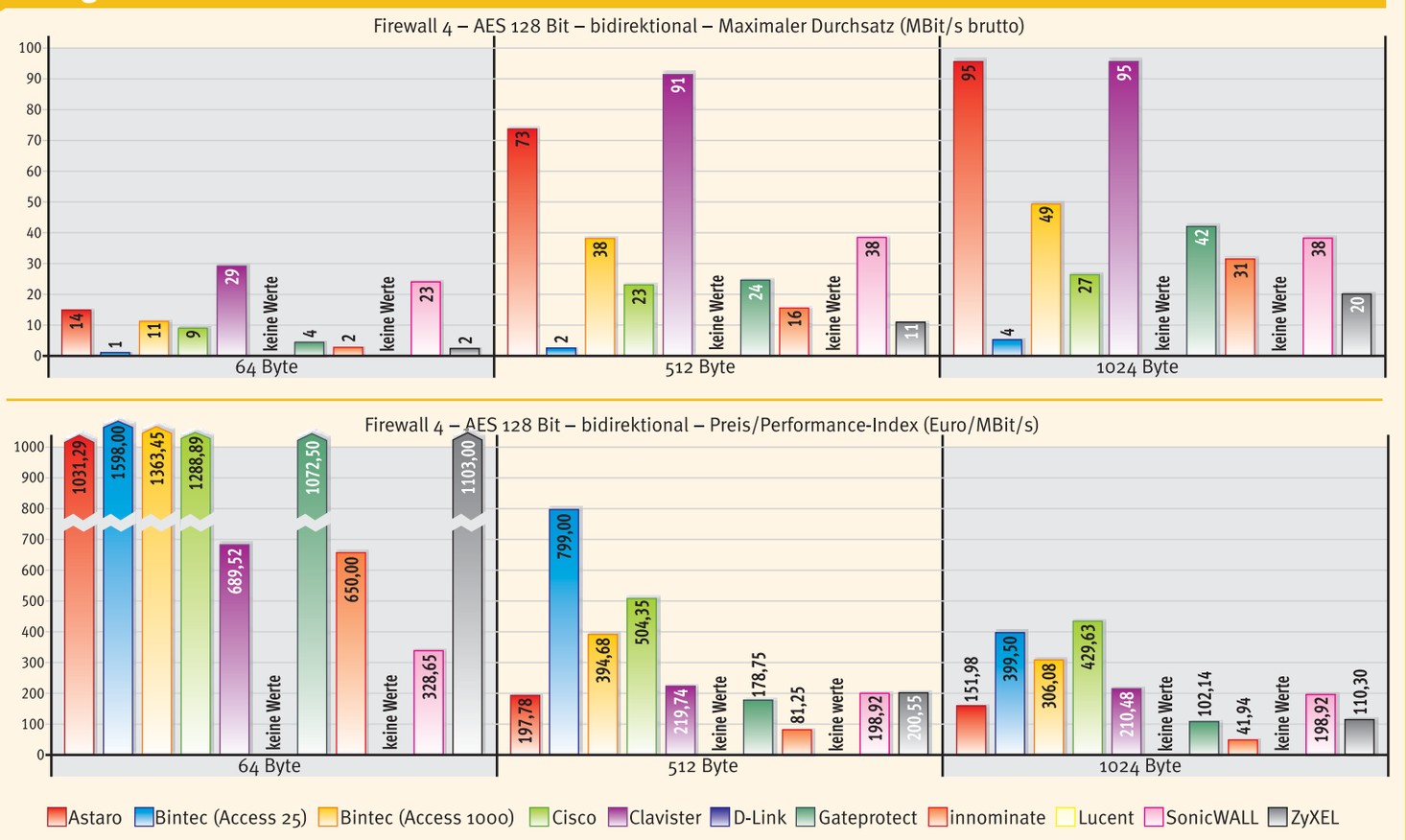
Bintecs kleine VPN-Access-25 war ihrer Aufgabe nicht unbedingt gewachsen. Schon der unidirektionale Datenverkehr mit 3DES-Verschlüsselung überforderte das System weitgehend, so schaffte die kleine Bintec hier mit 64-Byte-Rahmen einen Durchsatz von 2 MBit/s und auch bei der Messung mit 1024-Byte-Frames schaffte sie gerade mal 8 MBit/s Durchsatz. Diese Durchsätze lagen aber dann auch noch unter Volllast an, so dass die kleine Bintec vorhersehbar reagierte. Mit AES-128-Bit-Verschlüsselung kam die VPN-Access-25 dann etwas besser zurecht, so erreichte sie hier unidirektional mit 1024-Byte-Paketen einen Maximaldurchsatz von 16 MBit/s. Auf Grund der vorliegenden Messergebnisse ist klar, dass die kleine und preisgünstige VPN-Access-25 für unser Szenario nicht geeignet ist. Dieses schlechte Testergebnis sollte aber nicht darüber hinwegtäuschen, dass die VPN-Access-25 eine durchaus interessante Lösung für die Absicherung entsprechend »langsamer« WAN-Verbindungen sein kann – dort sind 2 MBit/s auch schon ein Wort.

Bintecs zweites System im Testfeld, die VPN-Access-1000, erwies sich als deutlich performanter. Auch wenn sie zum Teil deutlich hinter Wirespeed zurück blieb, reichte es insgesamt immerhin für den zweiten Platz im Testfeld. Eine deutliche Schwäche zeigte die große Bintec-Appliance im 64-Byte-Bereich. Bei der Messung mit 3DES-Verschlüsselung und unidirektionalem Datenstrom schaffte sie hier einen Durchsatz von 25 MBit/s, von dem im bidirektionalen Betrieb dann noch rund 13 MBit/s je Senderichtung übrig blieben. Unter Volllast ging die Leistung dann noch etwas zurück, so dass die VPN-Access-1000 im bidirektionalen Betrieb mit 64-Byte-Paketen und 3DES noch einen Durchsatz von gut 13 MBit/s schaffte. Unter Volllast ging der Durchsatz bei den gleichen Parametern dann noch auf gut 9 MBit/s zurück. Mit größeren Datenrahmen kam dann auch die große Bintec-Appliance deutlich besser zurecht. So lagen unidirektional schon bei der Messung mit 512-Byte-Paketen rund 92 MBit/s an, waren die Datenrahmen 1024 Byte groß, schaffte die VPN-Access-1000 rund 96 MBit/s. Und auch im bidirektionalen Modus arbeitete das große Bintec-System mit Ausnahme der 64-Byte-Messungen recht performant. So waren hier 73 und 96 MBit/s zu messen. Im Betrieb mit AES-Verschlüsselung erreichte die VPN-Access-1000 nahezu identische Ergebnisse.

Ciscos PIX-515E-Security-Appliance blieb in praktisch allen Disziplinen deutlich hinter der großen Bintec-Appliance zurück. Neben einer ausgeprägten Schwäche bei den Messungen mit 64-Byte-Paketen blieben auch die Durchsätze bei den Messungen mit größeren Datenrahmen deutlich hinter Wirespeed zurück. So schaffte das Cisco-System bei der unidirektionalen Messung mit 1024-Byte-Paketen und 3DES-Verschlüsselung gerade mal 25 MBit/s. Im bidirektionalen Betrieb blieben dann gerade mal 12 MBit/s pro Senderichtung übrig. Diese Durchsätze standen aber dann auch noch unter Volllast zur Verfügung. Besser arbeitete das Cisco-System mit AES-128-Bit-Verschlüsselung, hier war unidirektional und mit großen Datenrahmen eine Geschwindigkeit von maximal 55 MBit/s zu messen. Insgesamt ist die PIX-515E-Security-Appliance für unser Szenario nicht zu empfehlen.

Deutlich besser waren dann wieder die Ergebnisse der Clavister-M460, die sich mit einem guten dritten Platz nur dem Lucent-System und

Messergebnisse – VPN-Performance



der großen Bintec geschlagen geben musste. Dabei konnte der schwedische Newcomer in einzelnen Disziplinen durchaus mit den besser platzierten Systemen mithalten. So schaffte die M460 unidirektional mit 3DES-Verschlüsselung und 64-Byte-Paketen einen Durchsatz von immerhin 52 MBit/s. Bidirektional blieben davon noch im Schnitt 24 MBit/s übrig. Dicht an Wirespeed heran kam das Clavister-System dann bei den Messungen unidirektional mit größeren Datenrahmen. Hier konnte sie beispielsweise bei 1024-Byte-Rahmen maximal 96 MBit/s verkraften und so mit der großen Bintec- und der Lucent-Appliance gleichziehen. Bidirektional halbierten sich allerdings die Durchsatzwerte. Die AES-Messungen ergaben keine signifikanten Unterschiede im Verhalten des Systems im Vergleich mit den 3DES-Werten. Interessant ist die Clavister-Lösung insbesondere wegen ihrer Stärke im 64-Byte-Bereich, Wirespeed bleibt hier allerdings auch immer noch unerreicht.

D-Links kostengünstige DFL-700-Network-Security-Firewall erwies sich in unserem Szenario als hoffnungslos überfordert. So erreichte sie unidirektional mit 3DES-Verschlüsselung und 1024-Byte-Paketen einen Durchsatz von 15 MBit/s. Waren die Pakete noch 64 Byte groß, blieb ein Durchsatz von rund 2 MBit/s übrig. Im bidirektionalen Betrieb blieben die Durchsatzwerte noch hinter diesen Ergebnissen zurück. Unter Volllast standen dann auch nicht mehr die unter optimalen Bedingungen ermittelten Durchsätze zur Verfügung. So blieb unidirektional und mit 64-Byte-Paketen noch ein Durchsatz von rund 0,7 MBit/s übrig. Für unser Szenario ist das D-Link-Sytem bei weitem nicht performant genug und daher nicht geeignet. Für die gesicherte Kommunikation über WAN-Verbindungen kann sie aber sicherlich eine interessante Wahl sein.

Auch die Gateprotect-Firewall vermochte nicht zu überzeugen. Neben einer ausgeprägten Schwäche bei den Messungen mit 64-Byte-Paketen zeigte sie insbesondere bei den bidirektionalen Messungen Schwächen. So schaffte die Gateprotect bidirektional mit 3DES-Verschlüsselung und 512-Byte-Paketen einen Durchsatz von 18 MBit/s. Ihre »persönliche Bestleistung« erreichte sie im unidirektionalen Betrieb mit 1024-Byte-Paketen. Hier waren immerhin 53 MBit/s zu messen. Deutlich schneller war die Gateprotect-Firewall bei den Messungen mit AES-128-Bit-Verschlüsselung. Im unidirektionalen Betrieb mit den ganz großen Datenrahmen schaffte sie hier einen Durchsatz von 84 MBit/s.

Dass auch Innominates kleine Mguard nicht für unser Szenario gedacht und auch nicht unbedingt geeignet ist, war dem Hersteller ebenso wie uns schon vor den Messungen klar. Trotzdem wollten wir wissen, wie sich der Security-David im Wettbewerb mit den Goliaths der Disziplin schlagen würde. Und das hat er gar nicht so schlecht gemacht, immerhin war die Mguard performanter als beispielsweise die fast um den Faktor 10 teurere Cisco-Lösung. So schaffte die kleine Mguard bei der unidirektionalen Messung mit 1024-Byte-Paketen und 3DES-Verschlüsselung immerhin 61 MBit/s an Durchsatz. Waren die Datenrahmen 64 Byte klein, dann blieben davon noch 5 MBit/s übrig. Im bidirektionalen Betrieb halbierten sich die Durchsätze je Senderichtung dann noch mal. Bei den Vergleichsmessungen mit AES-128-Bit-Verschlüsselung zeigte die Mguard praktisch identische Ergebnisse. Insgesamt ist Innominates kleine Mguard sicherlich eine interessante Lösung, die für unser Szenario aber nicht geeignet und auch nicht gedacht ist.

Mit Lucents VPN-Firewall-Brick-350 stand dann wieder eine ausgewachsene, recht performante Lösung in unseren Real-World Labs an der FH Stralsund, die in ihrer Leistungscharakteristik der Clavister-Lösung ähnelt und auf Grund ihrer guten Ergebnisse im bidirektionalen Modus den Vergleichstest für sich entscheiden konnte. Deshalb erhält die Brick-350 auch die »Referenz«-Auszeichnung von Network Computing. So erreichte die Lucent-Lösung bei der Messung mit 3DES-Verschlüsselung und unidirektionalem Datenfluss schon mit 64-Byte-Paketen einen Durchsatz von 47 MBit/s. Bei größeren Paketen verfehlte die Appliance Wirespeed mit 92 beziehungsweise 97 MBit/s nur knapp. Und auch bidirektional lagen ab 512 Byte durchgehend über 90 MBit/s an. Da sich die Lucent-Firewall auch preislich in der gleichen Gewichtsklasse bewegt wie die große Bintec oder die Cisco, vermag sie am ehesten zu überzeugen, auch wenn die Leistung im bidirektionalen Modus mit den kleinsten Frames bis auf 28 MBit/s herunter ging.

Deutlich schwächer als das Lucent-System zeigte sich die Sonicwall-Pro-3060, die aber auch preislich eine Klasse tiefer angesiedelt ist. Im unidirektionalen Betrieb mit 3DES-Verschlüsselung schaffte sie noch im Vergleich recht gute 45 MBit/s bei der Messung mit 64-Byte-Paketen. Bei größeren Paketen lagen jeweils über 70 MBit/s an. Im bidirektionalem Modus ging die Performance dann um fast 50 Prozent zurück. Unter Volllast standen auch noch die unter optimalen Bedingungen gemessenen Maximaldurchsätze zur Verfügung. Somit verhielt sich die Sonicwall-Pro-3060 recht vorhersehbar. Dabei kommt die Sonicwall-Pro-3060 auf ein nicht uninteressantes Preis-Leistungsverhältnis. Für unser Szenario ist sie allerdings nicht performant genug.

Zyxels Zywall-70 gehört zu den günstigeren Systemen, vermochte aber mit ihren Durchsatzleistungen auch nicht zu punkten. Mit kleinen Paketen kam sie nur schlecht zurecht, so schaffte sie mit 3DES unidirektional gerade 5 MBit/s, bidirektional waren noch 2 MBit/s je Senderichtung drin. Auch bei den größeren Datenrahmen war die Leistung eher bescheiden. Ihre Höchstleistung erreichte die Zywall-70 mit 1024-Byte-Paketen im unidirektionalen Betrieb, hier lagen dann 54 MBit/s an. Die Messergebnisse mit AES-128-Bit-Verschlüsselung unterscheiden sich nicht signifikant von denen mit 3DES.

Fazit

»Datenstau im Tunnel« lautete in mehr oder weniger allen Fällen das Fazit unserer VPN-Tests. Ein Blick in die Report-Card genügt, um zu erkennen, dass alle Systeme im Testfeld ihre Schwächen haben und im einen oder anderen Szenario

deutlich hinter Wirespeed zurück fallen. Weit verbreitet war die mehr oder weniger stark ausgeprägte Schwäche bei der Verarbeitung von kleinen Datenpaketen. Hier kamen auch die besten Systeme im Test auf maximal rund 50 Prozent der Wirespeed im unidirektionalen Betrieb. Bidirektional sah es noch schlechter aus, hier erreichte unser Testsieger, Lucents Brick-350, den Bestwert mit 28 MBit/s. Die Brick-350 konnte sich letztendlich im Testfeld durchsetzen, weil sie im bidirektionalen Betrieb pro Senderichtung genauso performant arbeitete, wie unidirektional. Ein ähnliches Verhalten schaffte sonst nur noch die zweitplatzierte VPN-Access-1000 von Bintec.

Alle anderen Systeme im Test fuhren ihre Leistung beim Wechsel auf bidirektionalen Betrieb bezogen auf eine Senderichtung um rund 50 Prozent zurück. Auf Grund dieses Verhaltens reichte es auch für die Clavister-M460 sowie für die Astaro-Lösungen nur für einen guten dritten beziehungsweise vierten Platz. Hier sind die Produktentwickler gefragt, Lucent und Bintec haben hier derzeit einen konzeptionellen Vorteil. Enttäuschend war auch die Leistung der Cisco-PIX-515E, die deutlich hinter den vergleichbaren Systemen von Lucent bis Astaro zurück blieb. Ein maximaler Durchsatz von 25 MBit/s im 3DES-Betrieb ist nicht »state of the art«, wie die besser platzierten Systeme im Testfeld beweisen.

Schlicht für unsere Zwecke unterdimensioniert waren die kleineren und preisgünstigeren Lösungen von Bintecs VPN-Access-25 bis zur Zywall-70. Das heißt natürlich nicht, dass die schlechter platzierten VPN-Lösungen generell unbrauchbar wären. So bietet beispielsweise Innominate mit ihrer Mguard eine durchaus interessante Lösung an. Eines haben die Verlierer im Feld aber gemein, sie sind nicht oder nur sehr bedingt dafür geeignet, ein hochperformantes VPN innerhalb eines Fast-Ethernet-LANs aufzubauen. Für die getunnelte WAN-Kommunikation reicht ihre Performance dagegen in der Regel völlig aus.

Die Ver- und Entschlüsselung kryptografisch geschützter Daten ist generell mit entsprechend 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 Netzwerks 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.

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 möglichst genau ihre 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]

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