Fast-Ethernet-VPN-Appliances

Private Datenautobahn

Für eine gesicherte Kommunikation zwischen zwei Netzen über eine unsichere Verbindung sorgen Virtual-Private-Networks. 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 Benutzergruppe eine geschützte Kommunikation über ein unsicheres Netz hinweg ermöglichen. Das logisch geschlossene Netz, 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 oder 3DES. 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 VPN-Funktionalität ist in Software abgebildet, was bedeutet, dass die Funktionalität sehr rechenintensiv ist und eine gute Performance eine leistungsfähige Hardware voraussetzt. 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 und in der Regel weitere Security-Funktionalität, wie Firewall oder Content-Security oder auch weitere Kommunikationsfunktionen, bieten.

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.

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 zu nutzen. Auch Betreiber größerer Wireless-LAN-Installationen müssen ihren Usern eine Vielzahl an VPN-gesicherten Verbindungen bieten. Diese Entwicklungen 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 bieten.

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 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 ei-

Report-Card /interaktiv unter www.networkcomputing.de

VPN-Performance

Max. Durchsatz	Gewichtung	Netscreen NS 204 Appliance	Watchguard Firebox Vclass V80 gateway	Telco Tech LiSS II secure RX 100	Siemens/Check Point 4 Your Safety Enterprise	Genua GeNUGate
512 Byte unidirektional	20%	5	5	4	2	2
1518 Byte unidirektional	20%	5	5	5	3	2
512 Byte bidirektional	20%	3	3	2	1	1
1518 Byte bidirektional	20%	4	4	3	2	1
64 Byte unidirektional	10%	1	1	1	1	1
64 Byte bidirektional	10%	1	1	1	1	1
Gesamtergebnis	**100%**	**3,6**	**3,6**	**3**	**1,8**	**1,4**
		B-	**B-**	**C**	**D**	**E**

A>=4,3 B>=3,5 C>=2,5 D>=1,5 E<1,5
Die Bewertungen A bis C beinhalten in ihren Bereichen + oder -;

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

Bewertungsschlüssel für maximalen Datendurchsatz: > 80 MBit/s = 5, > 60 MBit/s = 4, > 40 MBit/s = 3, > 20 MBit/s = 2, </= 20 MBit/s = 1

genständige 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 erlauben, die mit einem baugleichen Gerät ausgestattet werden soll.

Daraus ergaben sich folgende Anforderungen an die Teststellungen:

- 2 Security-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 VPN-Performance, also die unidirektionalen und bidirektionalen Datendurchsatzraten im VPN-Betrieb, die Datenverlustraten, Latency sowie Jitter unter Last. Als Test-Equipment dienten die Lastgeneratoren und -analysatoren Smartbits 6000B von Spirent Communications mit der aktuellen Smartflow-Version.

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 Gruppe 1 der Fast-Ethernet-Appliances bildeten Genuas »GeNUGate Enterprise«, »NetScreen NS-204 Appliance«, Siemens »4 Your Safety RX 100« mit Check Points »VPN1 Pro Express«, Telco Techs »LiSS II secure gateway« sowie 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«, Nokias »IP 740« mit Check Points »NG with Application Intelligence«, Pyramids »BenHur II« sowie Siemens »4 Your Safety RX 300« mit »Corrent Turbo Card« und Check Points »VPN-1 pro«. Das Testfeld vervollständigten Stonesofts »StoneGate« sowie Symantecs »Gateway Security Appliance«. Wie sich die Fast-Ethernet-Appliances in unserem Test verhielten, steht im vorliegenden Artikel. Die Ergebnisse der Gigabit-Ethernet-Appliances folgen in einer der nächsten Ausgaben der Network Computing.

Mit Vollgas durch den Tunnel

Zur Ermittlung der maximal möglichen Durchsatzraten sowie des lastabhängigen Datenrahmenverlustverhaltens haben wir wie auch bei unseren VPN-Tests 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.

Liegen die maximal möglichen Durchsatzraten unter der theoretischen Wirespeed, dann kann es auch in realen Unternehmensnetzen bei entsprechenden Eingangslasten zu teils massiven Datenverlusten kommen. Dabei ist das Verhalten des gesamten Systems von einer ganzen Reihe von Faktoren abhängig – 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

Features

VPN-Teststellungen

	GeNUA GeNUGate Enterprise	Netscreen NS-204	Siemens / Check Point Four your safety RX 100 / VPN1 Pro Express	TELCO TECH LiSS II secure gateway	Watchguard Firebox Vclass V80
Anz. unabhäng. (nicht geswitchter) LAN-Ports					
Anz. Gigabit-Ethernet-Ports	max. 9	0	1	0	0
Anz. Fast-Ethernet-Ports	max. 20	4	3	6	4
Anz. WAN-Ports					
PPoE auf LAN-Port(s)	0	1	1	1	1, auf public
X.21	0	0	0	0	0
X.25	0	0	0	0	0
ISDN $_{S0}$	0	0	0	0	0
ISDN $_{S2M}$	0	0	0	0	0
xDSL	0	0	1	0	0
E1	0	0	1	0	0
Hardware/Betriebssystem					
Prozessor (Typ)	Intel P4 bzw. Xeon	keine Angabe	Celeron P4, 2 GHz	Pentium 4, 3.06 GHz	Asic mit vier RISC CPUs
Arbeitsspeicher in MByte	max. 2048	keine Angabe	256	512	256
Betriebssystem Name/Version	BSD/OS	ScreenOS 4.0.1r8	Red Hat Linux 7.3 gehärtet	gehärteter Linux-Kernel	gehärteter Linux-Kernel
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	○	●	○	○	optional
Cluster					
Maximale Clustergröße (Zahl der Systeme)	unbegrenzt	2	8	beliebig	2
Cluster über 3-Party-Software etabliert	○	○	●	○	○
Cluster über externen Load-Balancer-Switch	○	○	●	●	●
Cluster über Netzwerk-Links etabliert	○	●	●	○	○ , zwei dedizierte Ports
Management					
Telnet	●	●	●	○	●
rollenbasierte Verwaltung	●	●	●	●	●
Auditing-fähig	●	●	●	○	keine Angabe
SSH-Support für CLI	●	●	●	○	●
HTTP/S	●	●	●	● , HTTPS	● , HTTPS
Automatische Synchronisierung im Cluster	●	●	●	●	●
Synchronisierung über multiple Pfade möglich	○	●	●	●	● , über beide HA Ports
Out-Band-Management	●	●	●	●	●
Monitoring					
CPU überwacht	●	●	●	●	●
Speicherauslastung gemessen	●	●	●	●	●
Port-Auslastung gemessen	●	●	●	in Vorbereitung	●
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	● , über Radius	●	in Vorbereitung	● , über Radius
TACACS/TACACS+	○	○	●	○	○
Radius	●	●	●	○	●
LDAP über TLS	●	●	●	in Vorbereitung	○
X.509-digitale Zertifkate	●	●	●	○	●
Token-basierend	●	●	●	○	●
Sicherheitsfeatures					
DMZ	● , bis zu 16 Netze	●	●	●	●
Intrusion-Detection	Host-IDS integriert	in Vorbereitung	●	●	●
AAA-Support	k.A.	●	●	●	○
DHCP	○	●	○	●	●
NAT-Support	●	●	●	●	●
Content-Filter	●	in Vorbereitung	● ,Drittanbieter	●	●
Virenscanner	über Zusatzprodukt	in Vorbereitung	● ,Drittanbieter	optional	○
Website	www.genua.de	www.netscreen.com	www.4ys.de, www.checkpoint.com	www.telco-tech.de, www.liss.de	www.watchguard.com
Listenpreis in Euro für Teststellung zzgl. MwSt. (*)	40 000	26 000	24 210	7600	24 800 Dollar

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

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 ein System 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. Doch nun zu den Messergebnissen.

Die Routing-Messung ermöglicht es, die bidirektionalen Datendurchsatzraten ohne Verschlüsselung zu ermittelten und gibt so Hinweise auf die Leistungsfähigkeit der reinen Hardware, da die zusätzliche Rechenarbeit für die Verschlüsselung entfällt. Schon bei dieser Messung erwies sich Genuas Genugate-Enterprise schnell als Flaschenhals. Insbesondere bei den Messungen mit kleinen Datenrahmen wurde es schnell eng im System, so erreichte die Genugate-Enterprise beim Transport von 64-Byte-Paketen einen maximalen Durchsatz von 17,24 MBit/s. Das war dann schon der Best-Case, bei Volllast verlor die Genua-Appliance 99,79 Prozent der Input-Daten. Aber auch beim Transport größerer Datenrahmen im Routing-Modus blieben die maximalen Durchsatzraten unter 60 MBit/s. Mit eingeschalteter VPN-Verschlüsselung gingen die erzielbaren Durchsatzraten dann noch deutlich zurück. So kam die Genugate-Enterprise bei der bidirektionalen Durchsatzmessung und 1024-Byte-Paketen auf gut 16 MBit/s. Unidirektional stiegen die Durchsatzraten dann um rund den Faktor 2 an. Der höchste erzielbare Daten-

durchsatz lag dann knapp über 30 MBit/s. Insgesamt blieb die Genugate-Enterprise deutlich hinter den theoretisch möglichen Durchsatzwerten zurück.

Netscreens NS-204-Appliance erreichte als einzige Appliance im Testfeld der Fast-Ethernet-Systeme volle Wirespeed bei den Messungen mit 512- und 1024-Byte-Paketen im Routing-Modus, also ohne Verschlüsselung. Als sie dann 64-Byte-Pakete transportieren sollte, wurden ihre technischen Grenzen sichtbar, hier erreichte die Netscreen-Appliance maximal gut 30 MBit/s. Mit VPN-Verschlüsselung und bidirektionalem Datenverkehr und 64-Byte-Paketen blieben von dieser Durchsatzrate dann noch gut 11 MBit/s übrig. Galt es dann größere Datenpakete zu transportieren, stiegen die Durchsatzraten des Netscreen-Systems deutlich an. Bestes Ergebnis erzielte die Netscreen-Appliance mit respektablen gut 96 MBit/s im unidirektionalen Datenverkehr mit 1024-Byte-Paketen.

Auch Siemens 4-Your-Safety-RX-100, auf der die Check-Point-Software VPN1-Pro-Express installiert ist, mochte keine kleinen Datenrahmen. So erreichte sie beim reinen Routing mit 64-Byte-Paketen eine Maximaldurchsatz von knapp 8 MBit/s. Mit bidirektionalem VPN-Verkehr ging dieser Wert dann auf gut 3 MBit/s zurück und auch unidirektional schaffte die Siemens-Appliance gerade mal gut 6 MBit/s. Mit größeren Datenrahmen kam die 4-Your-Safety-RX-100 dann deutlich besser zurecht. Im Routing-Modus schaffte sie bei der Messung mit 1024-Byte-Frames sogar Wirespeed. Als das Siemens-System aber bidirektional verschlüsseln musste, ging die Leistung auch bei größeren Datenrahmen wieder deutlich zurück. So erreichte das System beispielsweise bei der Messung mit 1024-Byte-Paketen eine maximalen Durchsatz von gut 24 MBit/s. Unidirektional sahen die Leistungen auch dieser Appliance dann besser aus. Ein Maximalwert von knapp 46 MBit/s bei der Messung mit 1024-Byte-Frames bleibt aber immer noch weit von Wirespeed entfernt.

Auch Telco Techs LiSS-II-Secure-Gateway schaffte ohne VPN-Verschlüsselung und mit 1024-Byte-großen Datenrahmen Wirespeed. Kleine Datenrahmen »mochte« sie aber schon in diesem Modus nicht, so kam sie bei der Messung mit 64-Byte-Rahmen gerade mal auf gut 16 MBit/s. Mit VPN-Verschlüsselung und bidirektionalem Datenverkehr bremste die Liss-II bei der Messung mit 1024-Byte-Paketen auf knapp 46 MBit/s herunter, mit 64-Byte-Paketen schaffte sie nur noch gut 10 MBit/s. Im unidirektionalen Datenverkehr sah dann auch die Telco-Tech-Appliance wieder besser aus. Ihre Bestleistung mit Verschlüsselung schaffte sie unidirektional mit 1024-Byte-Frames mit knapp 94 MBit/s.

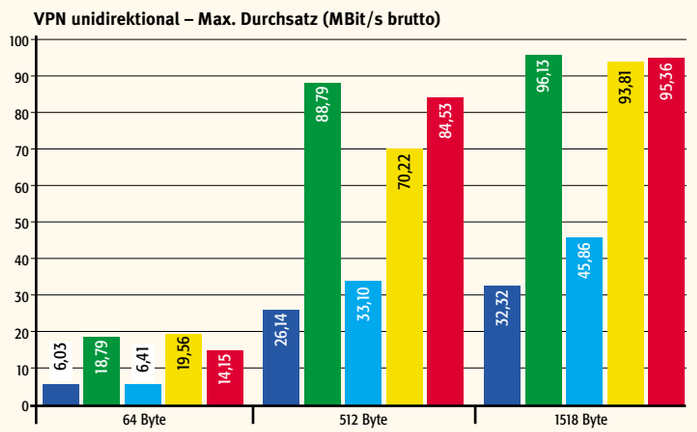
Watchguards Firebox-Vclass-V80 verfehlte im Routing-Modus mit 1024- und mit 512-Byte-Paketen Wirespeed nur knapp. Bei dieser Messung mit 64-Byte-Paketen schaffte sie dann noch gut 21 MBit/s. Von diesem Durchsatz blieben mit VPN-Verschlüsselung noch bidirektional knapp 8 MBit/s übrig. Bei den bidirektionalen und unidirektionalen Messungen mit Verschlüsselung und größeren Datenrahmen schob sich die Watchguard-Lösung dagegen noch knapp vor die Netscreen-Appliance und erreichte so die Spitzenwerte in diesem Testfeld.

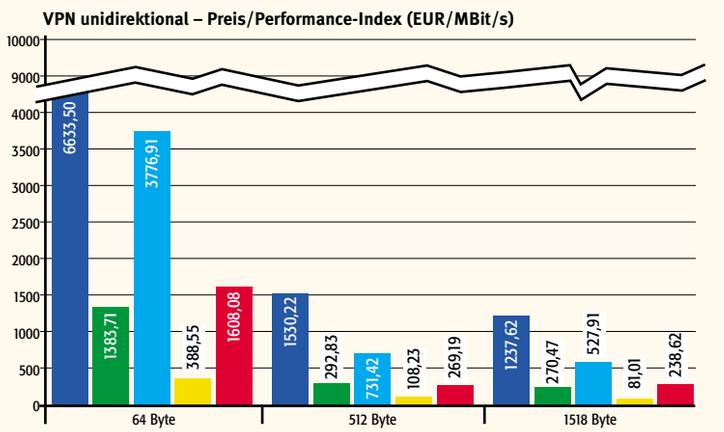
Fazit

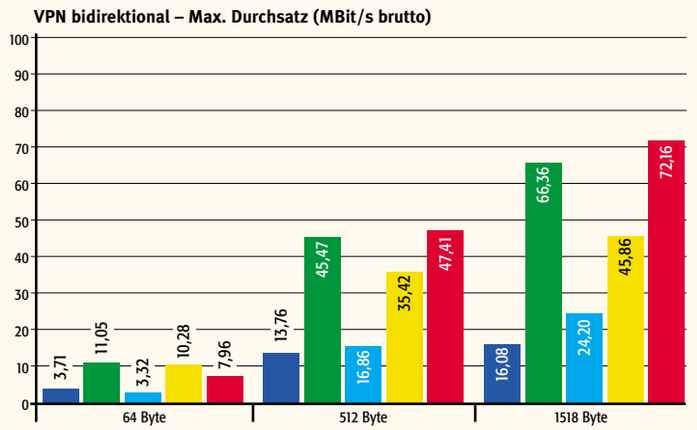
Die Ver- und Entschlüsselung kryptografisch geschützter Daten ist mit entsprechend aufwändiger Rechenarbeit verbunden. Dabei gilt generell – analog zu Firewall-Systemen –, dass ein höheres Sicherheitsniveau auch mit einer größeren erforderlichen Rechenleistung verbunden ist. Wenn nun VPN-Appliances beispielsweise innerhalb performanter Fast- oder Gigabit-Ethernet-Netze eingebunden werden, 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 ausstatten.

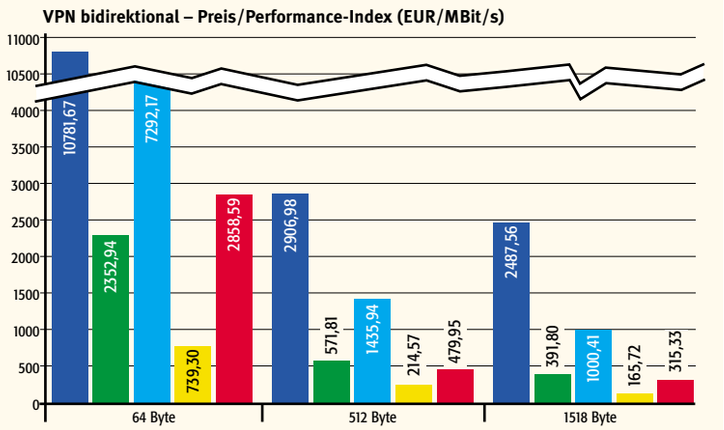
Insgesamt hat unser Vergleichstest von Fast-Ethernet-VPN-Appliances ergeben, dass die Systeme in unserem Testfeld unter Last und mit Verschlüsselung generell nicht in der Lage sind, Wirespeed von

Messergebnisse









GeNUA GeNUGate Enterprise
Siemens/Check Point, 4 Your Safety RX 100
Watchguard, Firebox Vclass V80
Netscreen, Netsreen-NS 204 Appliance
Telco Tech, LiSS II secure gateway

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 einzusetzenden Krypto-Verfahren auf 3DES, SHA1 und DH2 festgelegt. 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 maximalem 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 1024 Byte erzeugt.

Nacheinander haben wir vier VPN-Testreihen durchgeführt. In der ersten und zweiten Testreihe haben wir unidirektional gesendet und jeweils einen beziehungsweise zehn Tunnel etabliert und entsprechend viele Streams erzeugt. In der dritten Testreihe haben wir dann mit bidirektionalem Datenverkehr und zehn Tunneln gearbeitet. In der vierten Testreihe haben wir als Vergleichswert die reine Routinggeschwindigkeit mit ausgeschalteter VPN-Funktionalität ermittelt. Der Smartbits-Lastgenerator/Analysator hat die empfangenen Datenströme auf die eingestellten Parameter hin untersucht und die Ergebnisse gesichert.

100 MBit/s zu bieten. Unidirektionale Durchsatzraten von rund 80 Prozent gehören hier schon zu den Spitzenwerten. Das bedeutet, dass die getesteten Fast-Ethernet-VPN-Systeme den Datendurchsatz eines Wirespeed leistenden LANs auf alle Fälle reduzieren, wenn sie entsprechend gefordert werden. Recht gut waren die Systeme von Netscreen und Watchguard, die in unserer Punktewertung gleich auf liegen. Die Preis-Leistungs-Empfehlung erhält Telco Techs Liss-II, sie bietet insbesondere bei den unidirektionalen Messungen Durchsatzleitungen, die nicht allzu weit von denen der Testsieger entfernt sind – und zwar zu einem im Testfeld mit Abstand günstigsten Preis-Performance-Index.

Deutlich schlechtere Leistungswerte als die Telco-Tech-Appliance boten 4-Your-Safety-RX-100 sowie Genuas Genugate-Enterprise, obwohl beide Systeme im Preis deutlich über der Liss-II liegen. Ob die Gründe hierfür in einer zu schwachen Hardware zu suchen sind, oder -– insbesondere vor dem Hintergrund des Verhaltens der Genua-Appliance in unserem Firewall-Vergeichstest – zusätzliche Sicherheits-Features, die konfigurationsseitig nicht abschaltbar sind, die Performance zusätzlich reduzieren, ist messtechnisch nicht feststellbar. Entscheidend sind auf alle Fälle die erzielbaren Durchsatzwerte, und die zeigen, dass die Siemens- wie auch die Genua-Appliance den Datenverkehr deutlich einbremsen.

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. IT-Verantwortliche sollten möglichst genau ihre Sicherheits- und Performance-Anforderungen analysieren, klar definieren und auf ausführliche Tests und einen Probebetrieb setzen.

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