Gigabit-Ethernet-VPN-Appliances

Private Datenautobahn

VPN-Systeme schaffen exklusive, kryptografisch geschützte Verbindungen zwischen zwei Netzen, die als unsicher gelten. Wie schnell Unternehmen auf solchen »privaten Datenautobahnen« unterwegs sein können, sollte ein Vergleichstest in unseren Real-World Labs an der FH Stralsund klären.

Virtual-Private-Networks, oder kurz VPNs, sollen einer geschlossenen Benutzergruppe eine geschützte Kommunikation über ein unsicheres Netz hinweg erlauben. 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 offerieren. 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 im LAN als Standard geltenden Durchsatzraten offerieren.

Das Real-World-Labs-Test-Szenario

Im Mittelpunkt unserer VPN-Vergleichstestreihe, die 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 uns, wie viel gesicherten Datenverkehr der IT-Verantwortliche derzeit für sein Budget erhält.

Report-Card /interaktiv unter www.networkcomputing.de

VPN-Performance

Features	Gewichtung	Siemens / Check Point Four your safety RX 300 mit Corrent Turbo Card / VPN pro	Symantec Gateway Security 5460	Enterasys XSR 3250	Nokia / Check Point IP740 mit Nokia Encryption Accelerator Card / Check Point NG	Stonesoft StoneGate SG-3000
Max. Durchsatz 512 Byte unidirektional	20%	5	3	2	1	1
Max. Durchsatz 1518 Byte unidirektional	20%	5	4	3	2	1
Max. Durchsatz 512 Byte bidirektional	20%	5	2	1	1	1
Max. Durchsatz 1518 Byte bidirektional	20%	5	2	2	1	1
Max. Durchsatz 64 Byte unidirektional	10%	5	1	1	1	1
Max. Durchsatz 64 Byte bidirektional	10%	5	1	1	1	1
Gesamtergebnis	**100%**	**5**	**2,4**	**1,8**	**1,2**	**1**
		A+	**D**	**D**	**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 maximalen Datendurchsatz: > 500 MBit/s = 5, > 400 MBit/s = 4, > 250 MBit/s = 3, > 100 MBit/s = 2, </= 100 MBit/s = 1

Features

VPN-Teststellungen

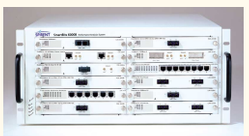
Features	Enterasys Networks XSR-3250	Nokia/ Check Point IP 740/ Check Point NG	Siemens/ Check Point 4 Your Safety RX 300/ VPN-1 Pro	Stonesoft StoneGate SG-3000	Symantec Gateway Security 5460
Anz. unabhäng. (nicht geswitchter) LAN-Ports					
Anzahl Gigabit-Ethernet-Ports	3	max. 6	5	max. 10	8 x 10/100/1000
Anzahl Fast-Ethernet-Ports	6	max. 20	2	max. 10	8 x 10/100/1000
Anzahl WAN-Ports					
PPoE auf LAN-Port(s)	9	0	k.A.	k.A.	0
X.21	24	max. 8	0	k.A.	0
X.25	0	0	0	k.A.	0
ISDN S_0	12	max. 4	0	k.A.	0
ISDN S_{2M}	24	0	0	k.A.	0
xDSL	24	0	k.A.	k.A.	8
E1	24	max. 4	k.A.	k.A.	8
Hardware/Betriebssystem					
Prozessor (Typ)	Broadcom 1250	Intel PIII-1000	P4 Xeon 2.4 Ghz.	1-2 Xeon CPUs 2,4 - 3,0 GHz	k.a.
Arbeitsspeicher in MByte	max.512	max. 2048	1024	max. 1024	k.a.
Betriebssystem Name/Version	EOS 5.00.05	IPSO 3.7	Red Hat Linux 7.3	gehärteter Linux-Kernel	Linux, Redhat
Firewall-Technik					
Stateful-Inspection-Firewall	●	●	●	●	●
Layer-7-Application-Gateway-Proxies	●	●	●	○	●
anpassbare Proxies	○	○	●	●	●
Stateful-Inspection und Proxy kombiniert	●	○	●	●	●
transp. Firewallfunktionalität konfigurierbar	○	●	●	●	●
spezielle Firewall-ASICs integriert	○	○	○	○	○
Netzprozessor mit Firewall Teilfunkt. auf NIC	○	○	●	○	○
VPN-Protokolle					
L2TP	●	●	●	○	○
PPTP	●	●	○	○	○
Secure-Socket-Layer/TLS	○	●	●	○	○
IPSEC über X.509/IKE	●	●	●	●	●
Routing-Protokolle					
RIPv1	●	●	●	○	○
RIPv2	●	●	●	○	○
OSPF	●	●	●	○	○
BGP-4	●	●	○	○	○
Cluster					
Maximale Clustergröße (Zahl der Systeme)	unbegrenzt	4	8	16	8
Cluster über 3-Party-Software etabliert	○	○	●	○	●
Cluster über externen Load-Balancer-Switch	●	●	●	○	●
Cluster über Netzwerk-Links etabliert	●	●	●	k.A.	●
Management					
Telnet	●	●	●	○	○
rollenbasierte Verwaltung	●	●	●	●	●
Auditing-fähig	●	●	●	●	●
SSH-Support für CLI	●	●	●	●	○
HTTP/S	●	●	●	●	●
Automatische Synchronisierung im Cluster	○	●	●	●	●
Synchronisierung über multiple Pfade möglich	●	●	●	●	●
Out-Band-Management	●	●	●	●	●
Monitoring					
CPU überwacht	●	●	●	●	○
Speicherauslastung gemessen	●	●	●	●	○
Port-Auslastung gemessen	●	●	●	●	○
Synchronisierung überwacht	○	●	●	●	●
Die Firewall-Software wird überwacht	○	●	●	●	●
Schwellenwerte für Auslastung möglich	●	●	●	○	○
Logging-Daten und -Events					
per SNMP exportiert	●	●	●	●	●
per WELF-Format exportiert	○	○	○	○	●
an Syslog-Server exportieren	●	●	●	●	○
Events zentralisier	●	●	●	●	●
Event-Management korelliert einzelne Einträge	●	●	●	○	●
Authentisierung/Autorisierung					
NT-Domain	●	VPN Client	●	●	●
TACACS/TACACS+	○	●	●	●	●
Radius	●	●	●	●	●
LDAP über TLS	●	VPN Client	●	●	○
X.509-digitale Zertifkate	●	VPN Client	●	●	●
Token-basierend	●	VPN Client	●	●	●
Sicherheitsfeatures					
DMZ	●	●	●	●	●
Intrusion-Detection	●	●, mit Smart Defense	●	○	●
AAA-Support	●	●	○	●	●
DHCP	●	●	●	○	○
NAT-Support	●	●	●	●	●
Content-Filter	○	●, über OPSEC Schnittstelle	●, Drittanbieter	●, Redirect z. Content Filter	●
Virenscanner	○	●, über OPSEC Schnittstelle	●, Drittanbieter	●, Redirect z. Virenscanner	●
Website	www.enterasys.com/products/routing/XSR-3000/	www.nokia.com	www.checkpoint.com www.4ys.de	www.stonesoft.com	http://enterprisesecurity.symantec.de/
Listenpreis in Euro für Teststellung *)	27 100	123 594,53	61 200	38 950	32 093,30

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

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 können 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.
In Folge 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 Routing-Geschwindigkeit mit ausgeschalteter VPN-Funktionalität ermittelt. Der Smartbits-Lastgenerator/Analysator hat die empfangenen Datenströme auf die eingestellten Parameter hin untersucht und die Ergebnisse gesichert.

Für die Ausschreibung unseres Vergleichstests haben wir ein Unternehmen unterstellt, das Segmente seines heterogenen, konvergenten Netzwerks 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 zu einer entfernten Niederlassung ermöglichen, 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 neun Hersteller mit zehn Teststellungen an den Start. Die 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 der »Nokia Encryption Accelerator Card« und Check Points »NG with Application Intelligence« sowie Siemens »4 Your Safety RX 300« mit der »Corrent Turbo Card« und Check Points »VPN-1 pro«. Das Testfeld vervollständigten Stonesofts »StoneGate SG-3000« sowie Symantecs »Gateway Security 5460«. Wie sich die Gigabit-Ethernet-Appliances in unserem Test verhielten, steht im vorliegenden Artikel. Die Ergebnisse der Fast-Ethernet-Appliances haben wir in der Ausgabe 19/2003 der Network Computing veröffentlicht.

Mit Vollgas durch den Tunnel

Zur Ermittlung 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 Input-Rate, 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 1000 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 und Lasten zu rechnen ist. Bei klassischen Dateitransfers arbeitet das Netzwerk mit möglichst großen Rahmen. Bei Echtzeit-Applikationen teilt sich das Feld. Video-Übertragungen nutzen ähnlich den Dateitransfers relativ große Datenrahmen. Messungen mit Ethernet-LAN-Phones in unseren Real-World Labs haben beispielsweise ergeben, dass diese Voice-over-IP-Lösung die Sprache mit konstant großen Rahmen von 534 Byte überträgt. Noch deutlich kürzere Rahmen sind beispielsweise bei der TCP-Signalisierung mit 64 Byte zu messen. Für die Sprachdatenübertragung wie auch für andere echtzeitfähige Applikationen ist das Datenverlustverhalten von entscheidender Bedeutung. Ab 5 Prozent Verlust ist je nach Voice-over-IP-Codec mit deutlicher Verschlechterung der Sprachqualität zu rechnen, 10 Prozent führen zu einer massiven Beeinträchtigung, ab 20 Prozent Datenverlust ist die IP-Telefonie definitiv nicht mehr möglich. So verringert sich der R-Wert für die Sprachqualität gemäß E-Modell nach ITU G.107 schon bei 10 Prozent Datenverlust um je nach Codec 25 bis weit über 40 Punkte, also Werte, die massive Probleme im Telefoniebereich sehr wahrscheinlich machen. Erzielt 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.

Die Routing-Messungen, die wir zusätzlich zu den Performance-Messungen im VPN-Modus durchgeführt haben, ermöglichen es, die bidirektionalen Datendurchsatzraten der Systeme ohne Verschlüsselung zu ermitteln und geben so Hinweise auf die Leistungsfähigkeit der reinen Hardware, da die zusätzliche Rechenarbeit für die Verschlüsselung entfällt. – Doch nun zu den ermittelten Messergebnissen.

Enterasys XSR-3250 hatte insbesondere bei unseren Messungen mit den 64 Byte kleinen Datenpaketen deutliche Performance-Probleme. Mit unidirektional maximal möglichen 29,3 und direktional maximalen 13,9 MBit/s bleibt das Gigabit-Ethernet-System deutlich unter Fast-Ethernet-Wirespeed. Ein Blick in die Ergebnisse des Frame-Loss-Tests zeigt, dass bereits bei weniger als 10 Prozent Eingangslast deutliche Datenverluste zu verzeichnen waren. Mit den größeren Datenframes kam das Enterasys-System dann klar besser zurecht. So schaffte der XSR-3250 beispielsweise unidirektional gut 203 MBit/s bei 512-Byte-Paketen beziehungsweise fast 393 MBit/s bei 1024-Byte-Paketen. Bidirektional halbierte sich der maximal mögliche Datendurchsatz ziemlich genau. Insgesamt zeigten die Frame-Loss-Messungen des Enterasys-XSR-3250, dass spätestens ab 30 bis 40 Prozent Eingangslast mit teils erheblichen Datenverlustraten zu rechnen ist. Das Enterasys-System ist zwar signifikant schneller als Fast-Ethernet-VPN-Geräte, bleibt aber deutlich unter Wirespeed-Durchsatz. Auch bei den Messungen im Routing-Modus kam die XSR-3250 lediglich bei den größten Frames auf die Nennleistung von 1 GBit/s. Verwendeten wir hier 64-Byte-Pakete, dann blieb das System noch knapp unter Fast-Ethernet-Wirespeed.

Nokias IP-740, in unserem Fall mit einer Nokia-Encryption-Accelerator-Card und der bewährten Check-Point-Software ausgestattet, liegt in der Preisklasse deutlich über dem gesamten Mitbewerb. So erhält der Enterasys-Kunde beispielsweise rund 4,5 Systeme für den Preis einer Nokia-Lösung. Im Bereich der VPN-Durchsatzleistung vermochte die Nokia-Lösung allerdings nicht so zu punkten, wie von der Preisrelation innerhalb des

Testfeldes vielleicht zu erwarten gewesen wäre. So lag die Nokia-Lösung beispielsweise bei allen Messungen hinter dem Enterasys-System. 64-Byte-Datenrahmen mochte die Nokia-Appliance überhaupt nicht, hier waren maximal 10 MBit/s zu erreichen. Zusätzliche Testmessungen mit deaktivierter Accelerator-Card kamen zu noch schlechteren Ergebnissen, was bedeutet, dass die Funktionalität gegeben war. Ihren »persönlichen Bestwert« erreichte das Nokia-System mit 114,4 MBit/s bei der unidirektionalen Messung mit 1024-Byte-Paketen. Ein Blick auf die Messergebnisse im bidirektionalen Routing-Modus zeigt, dass das Nokia-System auch ohne VPN-Betrieb Wirespeed nicht zu erreichen vermochte. Die hier erreichbare Höchstgeschwindigkeit lag zwischen gut 114 MBit/s mit 64-Byte-Rahmen und 644 MBit/s bei 1024-Byte-Rahmen.

Dass es heute möglich ist, Gigabit-Ethernet-VPNs nahezu mit Wirespeed zu betreiben, hat Siemens mit ihrer 4-Your-Safety-RX-300 bewiesen, die in unserem Test mit einer Corrent-Turbo-Card und der VPN-pro-Software von Check Point ausgestattet war. Bereits bei den Messungen mit 64-Byte-Paketen ließ die Siemens-Appliance das restliche Feld mit über 630 MBit/s deutlich hinter sich, um dann bei den Messungen mit größeren Frames auf fast 930 MBit/s bei 512-Byte-Paketen und gut 965 MBit/s bei 1024-Byte-Paketen zu kommen. Dabei spielte es auch keine Rolle, ob das System uni- oder bidirektional arbeiten musste, das Design des Systems ist offensichtlich insofern für den bidirektionalen Einsatz optimiert, als sich die Datenströme der gegenseitigen Senderichtungen keine System-Ressourcen teilen müssen, was in den vielen Fällen die Performance im bidirektionalen Betrieb deutlich senkt. Noch schneller war die Siemens-Appliance dann im Routing-Modus. Bei den größeren Frames erreichte sie problemlos Wirespeed und selbst mit 64-Byte-Paketen schaffte das System rund 977 MBit/s bidirektional. Auch die Frameloss-Ergebnisse können sich sehen lassen. Erste Datenverluste waren bei 64-Byte-Paketen bei immerhin 70 Prozent Last festzustellen. Bei größeren Datenrahmen kam es erst bei Volllast zu vergleichsweise geringen Datenverlusten.

Stonesofts Stonegate-SG-3000 enttäuschte bei unseren VPN-Messungen dagegen. Den besten Durchsatz konnten wir noch unidirektional mit den größten Frames messen. Hier lag die Marke bei 68 MBit/s. Bidirektional ging der Durchsatz auf gut 37 MBit/s zurück. Ihren schlechtesten Durchsatz erreichte die Stonegate-Appliance bei der bidirektionalen Messung mit 64-Byte-Rahmen. Hier fuhr sie den Durchsatz auf knapp 14 MBit/s zurück. Unter Volllast lagen die Datenverlustraten der Stonesoft-Appliance durchgehend über 90 Prozent. Bei dementsprechend geringeren Eingangslasten sind dann auch schon früh spürbare Datenverlustrate messbar.

Info

Das Testfeld

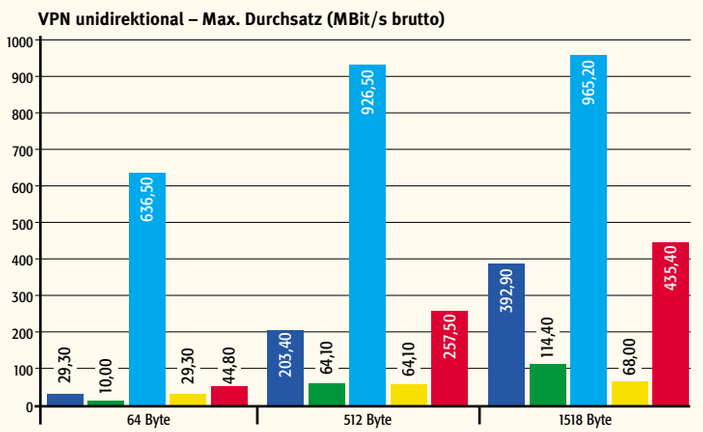
Gruppe 1: Fast-Ethernet-Appliances

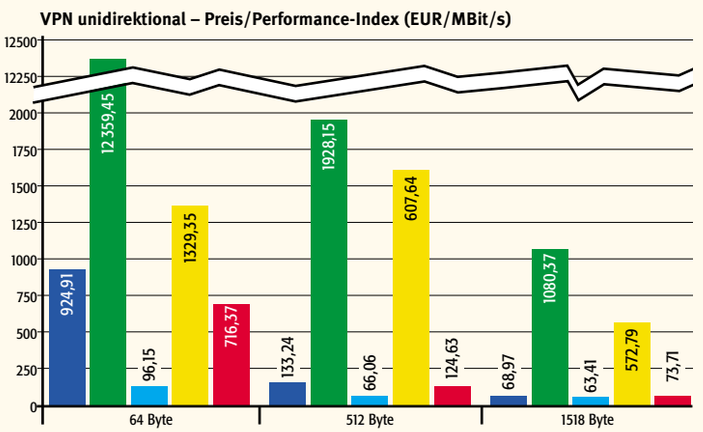
- GeNUA GeNUGate Enterprise
- NetScreen: NS-204 Appliance
- Siemens / Check Point: 4 Your Safety RX 100 / VPN1 Pro Express
- TELCO TECH: LiSS II secure gateway
- WatchGuard: Firebox Vclass V80

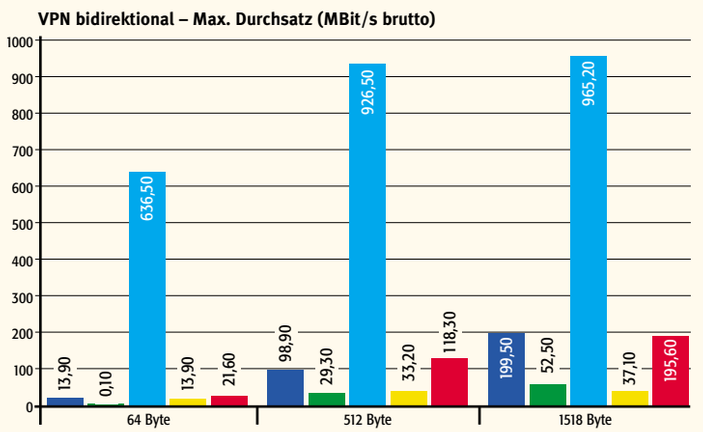
Gruppe 2: Gigabit-Ethernet-Appliances

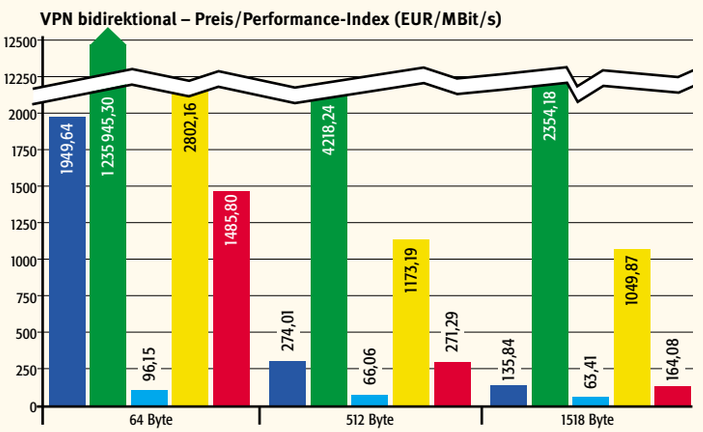
- Enterasys: XSR 3250
- Nokia / Check Point: IP 740 mit Nokia Encryption Accelerator Card / Check Point NG
- Siemens / Check Point: 4 your safety RX 300 mit Corrent Turbo Card / VPN pro
- Stonesoft: StoneGate SG-3000
- Symantec: Gateway Security 5460

Messergebnisse









Enterasys, XSR 3250
Nokia/Check Point, IP 740/CP-NG
Siemens/Check Point, RX 300/VPN Pro
Stonesoft, StoneGate SG-3000
Symantec, Gateway Security 5460

Auch Symantecs Gateway-Security-5460, die als Beta-Version im Test war, vermochte nicht so recht zu begeistern. Bei kleinen Datenrahmen drosselte sie den Datendurchsatz unidirektional auf knapp 45 MBit/s und bidirektional auf rund 22 MBit/s. Mit größeren Datenrahmen kam das neue Symantec-System dann besser zurecht. Den besten Datendurchsatz erreichte das Symantec-Gerät unidirektional mit 1024-Byte-Paketen. Bei dieser Messung kam die VPN-Appliance auf rund 435 MBit/s. Bidirektional reduzierte sich der Durchsatz aber auch bei den größten Frames im Test auf gut 195 MBit/s.

Fazit

VPN-Systeme müssen von Hause aus deutlich performanter sein, wenn sie mit aktiven Komponenten wie LAN-Switches mithalten sollen. Denn 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.

Unser Vergleichstest von Gigabit-Ethernet-VPN-Appliances hat gezeigt, dass die Systeme in unserem Testfeld unter Last und mit Verschlüsselung generell nicht in der Lage sind, Wirespeed von 1 GBit/s zu garantieren. Unidirektionale Durchsatzraten von um die 500 MBit/s gehören hier schon zu den Spitzenwerten. Das bedeutet, dass die getesteten Gigabit-Ethernet-VPN-Systeme den Datendurchsatz eines Wirespeed leistenden LANs auf alle Fälle reduzieren, wenn sie entsprechend gefordert werden, und das sie umgebende Netzwerk mit Wirespeed zu arbeiten vermag. So hat der vorhergehende Vergleichstest von Fast-Ethernet-VPN-Systemen gezeigt, dass die besseren Fast-Ethernet-VPNs durchaus ebenso schnell sein können, wie die langsameren Gigabit-Ethernet-Appliances – dann allerdings zu einem besseren Preis-Leistungsverhältnis, denn die Gigabit-Ethernet-Ports lassen sich die meisten Hersteller zusätzlich gut bezahlen, auch wenn die Performance mancher Systeme ihren Einbau derzeit nicht rechtfertigt.

Rühmliche Ausnahme in unserem Testfeld ist die Siemens-Appliance, die – nicht zuletzt wohl dank der Corrent-Beschleuniger-Karte – von der geforderten Wirespeed nicht mehr allzu weit entfernt war. Die rund doppelt so teuere Nokia-Lösung, die auch über einen entsprechende Beschleuniger-Karte verfügte, vermochte im direkten Performance-Vergleich nicht zu überzeugen. Hier stehen die Nokia-Entwickler sicherlich vor einer dringenden Aufgabe, wenn sie den Abstand zu Siemens wieder einholen möchten. Noch schlechtere Messergebnisse mussten wir dem Stonesoft-System bescheinigen, das seine Performance allerdings zu einem deutlich geringeren Preisniveau offeriert. Das Mittelfeld unseres Gigabit-Ethernet-Vergleichstests bilden die Systeme von Symantec und Enterasys, die sich sicherlich zu einem akzeptablen Preis-Leistungs-Verhältnis einsetzen lassen. Allerdings bleiben beide System deutlich hinter Wirespeed zurück. Auch hier sind noch die Produktentwicker gefordert. Denn die Integration von Gigabit-Ethernet-Interfaces in VPN-Appliances nutzt nicht viel, wenn das übrige System dann mehr oder weniger stark überfordert ist.

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 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]