Stau im Tunnel

Vergleichstest Security-Appliances, Teil 1 – Firewall und VPN bieten einen recht guten Schutz in modernen Netzen. Zu kurz kommt aber immer noch die VPN-Performance. Dies hat ein Vergleichstest der Real-World Labs von Network Computing ergeben.

Dafür, dass es in modernen Unternehmensnetzen gar nicht erst eng wird sollen Security-Appliances sorgen. Diese Appliances stellen Funktionalität wie Firewall und VPN aber auch weitere Security-Features zur Verfügung und sichern ganze Netzwerke aber auch einzelne Segmente gegeneinander ab.

Damit diese Systeme nicht nur die erforderliche Sicherheit, sondern auch die notwendige Performance liefern, statten die Hersteller ihre Systeme heute zumeist mit Gigabit-Ethernet-Ports aus. Denn darin sind sich die Security-Hersteller zumindest in der Theorie einig: Security-Appliances sind aktive Netzwerkkomponenten, die ebenso wie LAN-Switches möglichst mit Wirespeed arbeiten sollen und nicht zum Flaschenhals werden dürfen.

Wie gut solche Systeme diese Anforderungen erfüllen, sollte ein Vergleichstest in unseren Real-World Labs an der FH Stralsund zeigen. Getestet haben wir Security-Appliances auf ihre Tauglichkeit für den performanten Schutz von Unternehmensnetzen und deren einzelnen Segmenten.

Die Network Computing Musterfirma

Im Zentrum unserer Testausschreibung stand die Network Computing Musterfirma. Sie ist ein innovatives Unternehmen, das im Bereich der Automobilzubehörindustrie tätig ist. Die Musterfirma verteilt sich auf mehrere Standorte:

Firmenhauptsitz in Stralsund mit den Abteilungen

- Forschung & Entwicklung (250 PC-Arbeitsplätze),
- Marketing (150 PC-Arbeitsplätze),
- Sales (200 PC-Arbeitsplätze),
- Verwaltung (80 PC-Arbeitsplätze),
- Rechenzentrum (Serverfarm, SAN, Administration, 5 PC-Arbeitsplätze) und
- Geschäftsführung (20 PC-Arbeitsplätze).

Produktionsstandort in Rostock mit

- Produktion in vier Betrieben mit insgesamt 300 PC-Arbeitsplätzen und

REPORTCARD VPN-PERFORMANCE

interaktiv unter www.networkcomputing.de

	Gewichtung in Prozent	Alcatel-Lucent VPN Firewall Brick 1200	Fortinet FortiGate 3600A	Clavister SG4250	Juniper SSG-550	Siemens 4YourSafety RX300S3	Stonesoft FW-5100	Phion netfence nf-850	Zyxel ZyWALL 1050	Gateprotect X-Serie Enterprise Box
Max.VPN-Durchsatz 64 Byte unidir.	13,33	3	2	2	2	2	2	1	1	1
Max. VPN-Durchsatz 512 Byte unidir.	13,33	5	4	4	3	3	3	2	2	2
Max. VPN Durchsatz 1280 Byte unidir.	13,33	5	4	5	4	3	3	3	3	2
Max. VPN-Durchsatz 64 Byte bidir.	13,33	2	2	1	1	2	1	1	1	1
Max. VPN-Durchsatz 512 Byte bidir.	13,33	4	3	3	3	2	2	2	2	2
Max. VPN-Durchsatz 1280 Byte bidir.	13,33	4	3	4	3	2	3	2	2	2
Latency 512 Byte 50 % unidir.	5,00	5	5	5	5	5	5	5	4	5
Latency 512 Byte 100 % unidir.	5,00	4	4	2	4	3	1	4	3	3
Latency 512 Byte 50 % bidir.	5,00	5	5	5	5	5	5	5	4	5
Latency 512 Byte 100 % bidir.	5,00	4	4	2	3	3	1	3	3	2
Gesamtergebnis	**100**	**3,97**	**3,30**	**3,23**	**2,98**	**2,67**	**2,47**	**2,32**	**2,17**	**2,08**
		B	**C +**	**C +**	**C**	**C -**	**D**	**D**	**D**	**D**

A › 4,3; B › 3,5; C › 2.5; D › 1,5; E ‹ 1,5; Die Bewertungen A bis C enthalten in ihren Bereichen + oder -; Gesamtergebnisse und gewichtete Ergebnisse basieren auf einer Skala von 0 bis 5.

Max. Durchsatz	Latency
›/= 70 % = 5	‹ 1000 µs = 5
›/= 35 % = 4	›/= 1000 µs = 4
›/= 15 % = 3	›/= 10 000 µs = 3
›/= 5 % = 2	›/= 100 000 µs = 2
‹ 5 % = 1	›/= 1 000 000 µs = 1

DAS TESTFELD

Fast-Ethernet-Appliances
- Alcatel-Lucent VPN Firewall Brick 1200
- Clavister SG4250
- Fortinet FortiGate 3600A
- Gateprotect X-Serie Enterprise Box
- Juniper SSG-550
- Phion netfence nf-850
- Siemens 4YourSafety RX300S3
- Stonesoft FW-5100
- Zyxel ZyWALL 1050

◆ Backup-Rechenzentrum (Serverfarm, SAN, Administration, 5 PC-Arbeitsplätze).

Hinzu kommen vier Niederlassungen in Frankfurt, Berlin, München und Passau mit jeweils 30 PC-Arbeitsplätzen sowie zwei Auslandsniederlassungen in New York und Hongkong mit jeweils 40 PC-Arbeitsplätzen.

Die Network Computing Musterfirma möchte alle Standorte sowie Partnerfirmen in einem Intranet auf IP-Basis integrieren. Neben den klassischen Datenanwendungen soll über dieses Intranet auch Telefonie und Videoübertragung realisiert werden. Dabei soll das Unternehmensnetz in Segmente unterteilt werden, die den verschiedenen Abteilungen an den Hauptstandorten beziehungsweise den einzelnen Niederlassungen zugeordnet werden sollen. Die Segmente sollen hochperformant miteinander verbunden werden aber zugleich auch durch die entsprechenden Sicherheitstechnologien gegeneinander abgesichert werden.

Die Ausgangssituation

Die Network Computing Musterfirma möchte die verschiedenen Segmente ihres heterogenen, konvergenten Netzwerks sowie eine eigenständige DMZ am Unternehmensstandort hochperformant untereinander sowie mit dem Internet verbinden. Geeignete, durchsatzstarke Security-Appliances sollen mit ihrer Firewall- und IPS-Funktionalität für die notwendige Sicherheit und Performance sorgen. Zugleich sollen die Firewall-Geräte den Aufbau von VPNs ermöglichen. Daraus ergeben sich folgende Anforderungen an die Teststellungen, die wir in zwei Gruppen eingeteilt haben.

Ethernet-Seurity-Appliances:
- 2 Appliances inklusive Zubehör und Dokumentation,
- VPN-Funktionalität,
- Verschlüsselung nach AES mit 256 Bit,
- je Gerät mindestens 3 Ethernet-Ports (RJ45-Stecker),
- zusätzlicher Management-Port (Ethernet mit RJ45-Stecker),
- High-Avalibility (HA),
- Datenpriorisierung sowie
- Bandbreiten-Management.

Folgende Testparameter sollten untersucht werden:
- Überprüfung der VPN- und HA-Funktionalität,
- Überprüfung der Datenpriorisierung und des Bandbreiten-Managements,
- Firewall- und VPN-Performance (Datendurchsatzraten uni- und bidirektional)
- Packet-Loss,
- Latency sowie
- Jitter.

Die gesamte Funktionalität sollte durch dokumentierte Konfigurationseinstellungen gewährleistet sein, so dass sie auch jedem Anwender zugänglich ist.

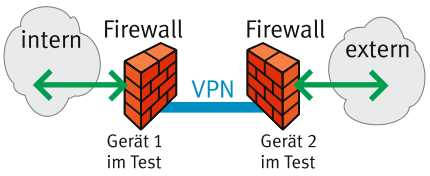
Unsere Testausschreibung haben wir dann wie gewohnt an alle relevanten Hersteller gesandt und diese eingeladen, sich an unserem Test zu beteiligen. Das Testfeld bildeten die »VPN Firewall Brick 1200« von Alcatel-Lucent, Clavisters »SG4250«, Fortinets »FortiGate 3600A«, Gateprotects »X-Serie Enterprise Box«, Junipers »SSG-550«, Phions »netfence nf-850«, Siemens »4YourSafety RX300S3«, Stonesofts »FW-5100« und Zyxels »ZyWALL 1050«.

In unseren Tests haben wir die Aspekte Firewall- und VPN-Performance, Quality-of-Service, Hochverfügbarkeit und Exploit-Erkennung untersucht. In unserem ersten hiermit vorliegenden Bericht stellen wir die Ergebnisse der Performance-Messungen im VPN-Betrieb dar. Die weiteren Folgen unseres Security-Vergleichstests werden dann die Performance-Messungen im Firewall-Betrieb sowie Quality-of-Service, Hochverfügbarkeit und Exploit-Erkennung zum Thema haben.

VPN-UDP-Durchsatz

In einer Messreihe haben wir den VPN-UDP-Durchsatz ermittelt. Hierzu haben wir zwei identische Appliances miteinander verbunden. Dann haben wir den Smartbits-Lastgenerator/Analysator über jeweils einen Port an beide Appliances angeschlossen, so dass wir erneut ein Zangenmessung durchführen konnten. Die Smartbits generierten dann Flows aus UDP-Paketen jeweils mit konstant 64, 256, 512, 1024 und 1280 Byte Größe. Neben konstant großen Frame-Formaten haben

Testaufbau VPN-UDP-Durchsatz



wir dann noch einen Frame-Mix erzeugt und Real-World Traffic genannt. Dieser entspricht der gemessenen Verteilung der Frame-Formate im MCI-Backbone. Hier sind rund 50 Prozent aller Frames 64 Byte groß. Die übrigen 50 Prozent streuen über alle möglichen Frame-Formate. Der Aufbau der VPN-Tunnel erfolgt zwischen den beiden Appliances. Standardmäßig haben wir das VPN durch

TECHNISCHE DATEN FIREWALL- UND VPN-SYSTEME

	Alcatel-Lucent VPN Firewall Brick 1200	Clavister SG4250	Fortinet FortiGate 3600A	gateProtect Germany X-Serie Enterprise Box	Juniper Networks SSG-550	Phion Information Technologies netfence nf-850	Siemens IT Solutions and Services 4YourSafety RX300S3	Stonesoft FW-5100	ZyXEL ZyWALL 1050
Anzahl unabh. (nicht geswitchter) LAN-Ports									
Anzahl Gigabit-Ethernet-Ports	10	2+8 MiniGBIC	10	7	4 [15]	12	6	18	5 [13]
Anzahl Fast-Ethernet-Ports	0	4	k.A.	0	0-16	0	6 [9]	18 [10]	0
Anzahl WAN-Ports									
X.21	0	0	0	0	0-12	0	0	0	0
X.25	0	0	0	0	0	0	0	0	0
ISDN S_0	0	0	0	0	0	0 [4]	0	0	0
ISDN S_{2M}	0	0	0	0	0	0	0	0	0
xDSL	0	4	0	0	0	0-4	0	0	0
E1	0	0	0	0	0-12 T1, E1, E3	0-4	0	0	0
Hardware/Betriebssystem									
Prozessor (Typ), MHz	3.2 GHz	k.A.	Intel-based	2 x Intel-Xeon DC 2.8 GHz	3,4 GHz	Intel-Xeon, 2,8 GHz	Intel-Xeon (5130 Dual C.), 2 GHz	2 x Intel-Xeon quad C. E5345	Intel-Mobile 1,5 MHz
Arbeitsspeicher	1 GByte	k.A.	2 GByte	4096 MByte	1 GByte	2048 MByte	2 GByte	4096 MByte	512 MByte
Betriebssystem Name/Version	Inferno Version 9.1.219	Cl. CorePlus 8.80.00	FortiOS 3.0 (MR4)	Linux 2.6	ScreenOS 5.4	phion OS 3.6.0	Ch.P. Secure Platf. NGX R62	k.A.	ZLD
IPv6-Unterstützung für alle Firewall-Funktionen	○	○	●	○	○ [14]	○	●	k.A.	○
Firewall-Technik									
Stateful-Inspection-Firewall	●	●	●	●	●	●	●	●	●
Layer-7-Application-Gateway-Proxies	●	●	●	●	●	●	○	●	●
anpassbare Proxies	●	●	●	●	○	● [5]	○	●	○
Stateful-Inspection und Proxy kombiniert	●	●	●	●	○	●	○	●	●
transp. Firewallfunktionalität konfigurierbar	●	●	●	●	●	●	●	○	●
spezielle Firewall-ASICs integriert	○	●	●	○	○	○	○	○	○
Netzwerkproz. m. Firewall Teilfunktionen auf NIC	○	○	●	○	○	○	○	○	○
VPN-Protokolle									
L2TP	○	●	●	○	○	●	●	○	○
PPTP	○	●	●	●	○	●	○	○	○
Secure-Socket-Layer/TLS	○	○	●	●	○	● [6]	●	○	○
IPSec über X.509/IKE	●	●	●	●	●	●	●	●	●
Routing-Protokolle									
RIPv1	○	○	●	○	●	●	●	○	●
RIPv2	○	○	●	○	●	●	●	○	●
OSPF	○	●	●	○	●	●	●	○	●
BGP-4	k.A.	○	●	○	●	○	●	○	○
Cluster									
maximale Clustergröße (Zahl der Systeme)	○	2	4	○	2	2	8	16	2
Cluster über 3rd-Party-Software etabliert	○	○	○	○	○	○	○	○ [11]	○
Cluster über externen Load-Balancer-Switch	○	○	○	○	○	● [7]	●	○ [11]	○
Cluster über Netzwerk-Links etabliert	○	●	●	○	●	● [8]	●	●	○
Management	[1]								
Telnet	○	○	●	○	●	○	optional	●	●
rollenbasierte Verwaltung	●	●	●	●	● [2]	●	●	●	●
Auditing-fähig	○	●	●	●	●	●	●	●	○
SSH-Support für CLI	○	○	●	●	●	●	●	●	○
HTTP	○	○	●	○	●	○	●	○	●
HTTPS	○	○	●	○	●	○	●	○	●
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	●	●	●	●	● im Cluster	●	●	●	●
Schwellenwerte für Auslastung möglich	●	●	●	●	●	●	●	○	○
Logging-Daten und -Events									
per SNMP exportiert	●	●	●	●	●	●	●	●	●
per WELF-Format exportiert	●	●	●	○	○	○	○	○	○
an Syslog-Server exportieren	●	●	●	●	●	●	●	●	●
Events zentralisiert	●	●	●	○	● [2]	●	●	●	○
Event-Management korelliert einzelne Einträge	○	●	●	○	● [2]	●	●	●	○
Authentisierung/Autorisierung									
NT-Domain	●	●	●	●	○	●	●	●	●
TACACS/TACACS+	○	○	●	○	○ [14]	○	●	●	○
Radius	●	●	●	○	●	●	●	●	●
LDAP über TLS	●	○	●	○	○	●	●	●	●
X.509-digitale Zertifikate	●	●	●	○	●	●	●	●	●
Token-basierend	●	●	●	●	●	●	●	●	○
Sicherheitsfeatures									
DMZ	●	●	●	●	●	●	●	●	●
Intrusion-Detection/-Prevention	●	●	●	●	●	●	●	●	●
AAA-Support	●	●	●	●	●	●	●	●	●
DHCP	●	●	●	●	●	●	●	○ [12]	●
NAT-Support	●	●	●	●	●	●	●	●	●
Content-Filter	●	●	●	●	●	●	●	●	●
Virenscanner	●	●	●	●	●	●	●	○	○
Listenpreis in Euro für Teststellung zzgl. MwSt. *	46 969 **	50 400	78 950	6184	24 300 [3]	28 545	22 977	132 900	2999
Website	www.lucent.com/security	www.clavister.com	www.fortinet.com	www.gateprotect.de	www.juniper.net	www.phion.com	www.4ys.de	www.stonesoft.com	www.zyxel.de

Quelle: Angaben der Hersteller

● = ja; ○ = nein; k.A. = keine Angabe; 1) = Kein direkter Login auf der FW Appliance möglich. Management ausschließlich über automatisch aufgebauten IPSec Tunnel vom zentralen Management System; 2) über Management-System; 3) 2xSSG-550 und 4 zusätzliche Gigabit-Module; 4) optional als Add-on erhältlich, nicht im Umfang der Teststellung enthalten; 5) generische Circuit-Level-Proxy-Funktion der FW, pro Regel einstellbar; 6) HTTPS-Emulation f. Site-to-Site VPN über Proxy; 7) für Active-active Modus; 8) Standard-Modus; 9) über GBit-Ports möglich; 10) Appliance hat insgesamt 18 10/100/1000-MBit/s-Ports; 11) integriert; 12) Relay ja; 13) Zone (LAN /WAN /DMZ) frei konfigurierbar; 14) ab Screen OS 6; 15) integriert + 0-4 als Module; *) Listenpreis = Zwei Appliances (Hard- und Software) inkl. Lizenzen für 100 User und vollständige Managementlösung; **) 1 Dollar = 0,74589 Euro, Stand 11.04.07

Alcatel-Lucent VPN Firewall Brick 1200

AES-256-Verschlüsselung realisiert. Die Belastung des VPN-Systems erfolgte erst uni- und dann bidirektional, das heißt beide Ports sendeten und empfingen gleichzeitig maximal mit Wirespeed.

In einer Variante der UDP-Durchsatzmessung, die wir hier »UDP-Mix« nennen, haben wir 50 Prozent der jeweiligen Gesamtlast verschlüsselt durch den VPN-Tunnel geschickt. Die übrigen 50 Prozent der Gesamtlast ging unverschlüsselt über die Leistung. Die gemessenen Durchsätze entsprechen der Gesamtleistung des Systems. Diese Variante haben wir bidirektional durchgeführt. Gemessen haben wir wieder Frame-Loss, Latency und Jitter. Die erzeugte Last beginnt bei einem Prozent und wird dann schrittweise erhöht. Aus den ermittelten Frame-Loss-Werten errechnen sich die Werte für den maximalen Durchsatz. Dieser ist der maximal mögliche Durchschnittswert aller Flows bei einem Frame-Loss von weniger als einem Prozent. Wichtig ist noch zu betonen, dass Gateprotect und Zyxel den UDP-Mix-Test nicht in dem vorgegebenen Szenario mit definierten Diensten außerhalb des VPN-Tunnels realisieren konnten. Als Alternative haben wir hier ein Szenario mit mehreren Netzen aufgebaut, wobei der unverschlüsselte Netzverkehr nur anhand der IP-Adressen festgelegt werden konnte.

Die Latency haben wir in µs gemessen und den jeweiligen Mittelwert gebildet. Wir haben dabei für jede Teststellung die Latency bei 50 und bei 100 Prozent des jeweils möglichen Durchsatzes ermittelt. Die G.114-Empfehlung der ITU-T besagt, dass für eine gute Sprachqualität maximal 150 ms oder 150 000 µs als einseitige Verzögerung auftreten dürfen. Dabei sollte aber nicht aus den Augen verloren werden, dass sich dieser Wert auf die gesamte Strecke zwischen zwei Endgeräten beziehungsweise Kommunikationspartnern und nicht auf einzelne Komponenten bezieht. Für diese sollte er deutlich geringer sein, da sich die Latency der gesamten Strecke entsprechend aufaddiert.

Fortinet FortiGate 3600A

Alcatel-Lucents VPN-Firewall-Brick-1200 schaffte im unidirektionalen VPN-Betrieb mit 64-Byte-Paketen einen maximalen Durchsatz von rund 25 Prozent oder 250 MBit/s. Auch wenn dieser Wert meilenweit von der Leitungsgeschwindigkeit von einem GBit/s entfernt ist legt Alcatel-Lucent hiermit die Messlatte recht hoch. Im direkten Vergleich mit den anderen Systemen im Testfeld konnte keine andere Teststellung diesen Wert erreichen. Mit den nächstgrößeren Frames kam die Brick dann auf deutlich mehr Durchsatz. Hier waren schon 67 Prozent drin. Mit wachsendem Frame-Format stiegen die Durchsätze der Brick weiter an. Verwendeten wir 512-Byte-Pakete, lagen bereits 90 Prozent der Leitungsgeschwindigkeit an. Und mit dem größten Frame-Format waren dann immerhin 96 Prozent Durchsatz möglich. Mit unserem Real-World-Traffic lag der maximale Durchsatz dann bei 87 Prozent.

Der Wechsel in den bidirektionalen Betrieb reduzierte die Durchsatzleistung je Senderichtung um rund 50 Prozent. So waren hier zwischen 12 und 60 Prozent der nominellen Leitungsgeschwindigkeit möglich. Dabei galt auch hier, dass kleine Paketgrößen und somit eine höhere Anzahl der zu transportierenden Datenpakete sich entsprechend negativ auf die Durchsatzleistung auswirkte. Mit Real-World-Traffic kam die Brick dann bidirektional noch auf rund 41 Prozent Durchsatzleistung. Im UDP-Mix-Betrieb lagen die möglichen Durchsätze mit Werten zwischen 24 und 82 Prozent dann wieder ähnlich wie die im unidirektionalen Modus.

Clavister SG4250

Die Werte für die Latency betrugen bei unseren Messungen mit unidirektionalem Datenverkehr und halber Durchsatzleitung zwischen 420 und 500 µs, wobei die Latency-Werte mit wachsendem Frame-Format anstiegen. Bei maximalem Durchsatz stieg die durchschnittliche Latency dann deutlich an. Hier betrug sie über 32 000 µs bei der Messung mit den kleinsten Paketen. Mit gut 2000 µs erreichte die Brick dann bei unserer Messung mit 256-Byte-Paketen ihren Bestwert für den Betrieb mit vollem Durchsatz. Mit weiter steigenden Frame-Größen stieg dann auch die Latency wieder an, um bei der Messung mit den größten Frames wieder über 13 000 µs zu erreichen. Im bidirektionalen Modus mit halber Durchsatzleistung betrug die Latency ebenfalls zwischen 420 und 500 µs. Bei voller Durchsatzleistung erhöhten sich die Latency-

Werte dagegen deutlich. Sie schwankten hier zwischen gut 32 000 und 9000 µs.

Clavisters SG4250 hatte schon im unidirektionalen Betrieb mehr Probleme mit kleinen Frames als die Brick. Verwendeten wir 64-Byte-Frames, betrug der maximal mögliche Durchsatz 7 Prozent der nominellen Leitungsgeschwindigkeit. Mit 256-Byte-Frames lagen schon rund 25 Prozent Durchsatz an. Mit steigender Frame-Größe stiegen auch hier die Durchsatz-

Gateprotect X-Serie Enterprise Box

leitungen weiter an. So erreichte das Clavister-System dann im unidirektionalen Betrieb mit den 1280-Byte-Frames einen maximalen Durchsatz von immerhin 73 Prozent. Das ist nach Alcatel-Lucent das zweitbeste Ergebnis. Der Wechsel in den bidirektionalen Betrieb reduzierte auch bei der SG4250 die Leistung um rund die Hälfte. Hier waren zwischen 4 Prozent Durchsatz mit den kleinsten Frames und 36 Prozent Durchsatz mit den größten Frames möglich. Mit Real-World-Traffic erreichte die SG4250 unidirektional 38 und bidirektional 19 Prozent der nominalen Leitungsgeschwindigkeit. Wechselten wir in den UDP-Mix-Betrieb, ähnelte das Ergebnis wieder dem der Messungen im unidirektionalen Modus. Hier waren zwischen 6 und 69 Prozent der nominellen Leitungsgeschwindigkeit drin.

In der Latency mit halber Durchsatzleistung blieben die Ergebnisse im dreistelligen Bereich. Im unidirektionalen Betrieb lagen hier die Messwerte zwischen rund 100 und gut 200, im bidirektionalen Betrieb zwischen gut 100 und fast 600 µs. Bei voller Durchsatzleistung gingen die Latency-Werte dagegen in den sechsstelligen Bereich. Unidirektional schwankte die Latency zwischen rund 150 000 und über 400 000 µs. Bidirektional lagen die Werte mit rund 350 000 bis 540 000 noch etwas höher.

Fortinets Fortigate-3600A schaffte unidirektional mit den kleinsten Datenpaketen einen Durchsatz von 12 Prozent der Leitungsgeschwindigkeit. Verwendeten wir 256-Byte-Pakete, stieg der mögliche Durchsatz auf 41 Prozent. Mit wachsenden Frame-Formaten stieg auch der Durchsatz weiter an. Mit den 1280-Byte-Paketen waren so 67 Prozent der Leitungsgeschwindigkeit möglich. Der Wechsel auf bidirektionalen Betrieb halbierte auch hier die mögliche Leistung. Hier lagen zwischen 7 und 33 Prozent Durchsatz an. Im Betrieb mit Real-World-Traffic erreichte die Fortigate-3600A maximal unidirektional 53 beziehungsweise bidirektional 26

Juniper SSG-550

Prozent Durchsatz. Im UDP-Mix-Betrieb waren zwischen 14 Prozent mit den kleinsten Frames und 59 Prozent mit den größten Frames möglich.

Ebenfalls dreistellige Latency-Werte zeigte die Fortigate-3600A im Betrieb mit halber Durchsatzleistung. Hier lagen unidirektional zwischen gut 120 und 230 sowie bidirektional zwischen 200 und 270 µs an. Bei voller Durchsatzleistung der Fortigate-3600A waren dann vierstellige Latency-Werte zu messen. Im unidirektionalen Betrieb schwankte sie zwischen gut 2000 und fast 4000 µs. Bidirektional kam die Fortinet-Appliance auf Werte zwischen 2400 und 4700 µs.

Gateprotects X-Serie-Enterprise-Box blieb in den gemessen Durchsätzen ein Stück hinter dem Feld der allerdings auch deutlich teureren Appliances zurück. So schaffte das Gateprotect-System im unidirektionalen Betrieb mit den kleinsten Frames noch 2 Prozent der nominellen Leitungsgeschwindigkeit. Mit 256-Byte-Paketen waren dann 5 Prozent möglich. Die höchste Durchsatzleistung schaffte die X-Serie-Enterprise-Box mit den größten Paketen. Hier lagen dann 13 Prozent Durchsatz an. Der Wechsel in den bidirektionalen Modus halbierte auch hier die mögliche Leistung je Senderichtung. Hier waren also noch zwischen 1 und 7 Prozent Durchsatz drin. Im UDP-Mix-Betrieb lagen die

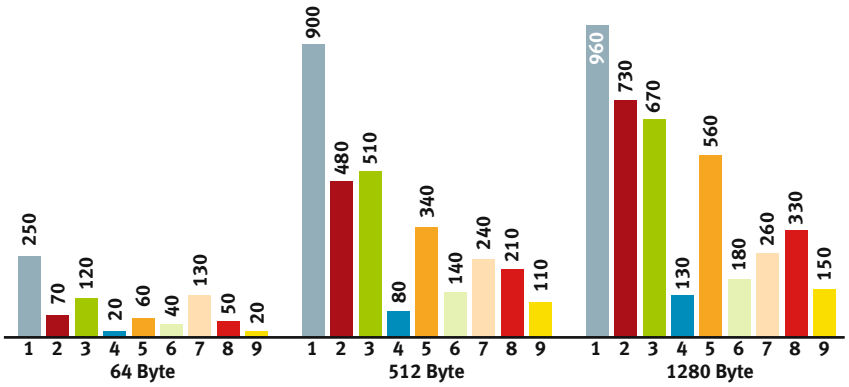
Phion netfence nf-850

Durchsätze dann zwischen 3 Prozent mit den kleinsten Frames und 15 Prozent mit den größten Frames.

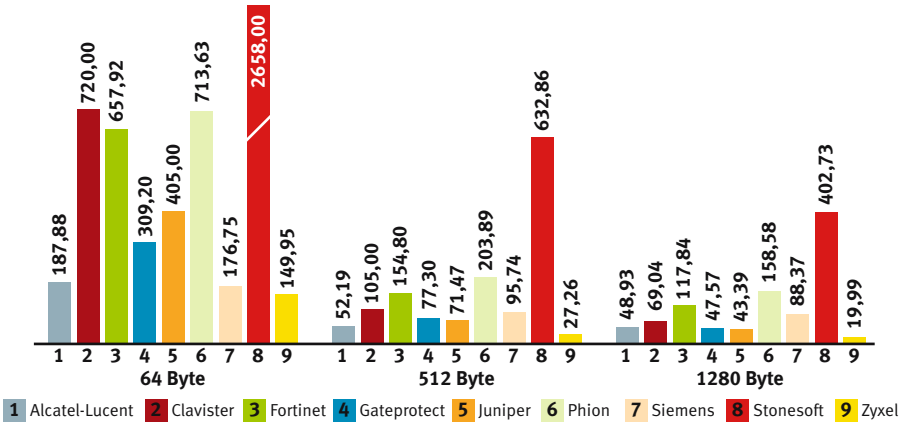
Die Latency-Werte mit halber Durchsatzleistung blieben bei unseren Messungen mit der X-Serie-Enterprise-Box durchweg im dreistelligen Bereich und schwankten unidirektional zwischen rund 200 und 550 µs sowie bidirektional zwischen 230 und gut 400 µs. Unter Volllast waren die Latency-Werte dann fünf- bis sechsstellig. Im unidirektionalen Betrieb schwankten sie zwischen 15 000 und 45 000 µs. Bidirektional waren Werte zwischen rund 70 000 und 165 000 µs zu messen.

Junipers SSG-550 schaffte im unidirektionalen Betrieb mit den kleinsten Frames einen Durchsatz von 6 Prozent der Leitungsgeschwindigkeit. Betrug die Frame-Größe 256 Byte, waren 19 Prozent möglich. Ihren Bestwert erreich-

Messergebnisse VPN-UDP unidirektional (Datendurchsatz in MBit/s)



Messergebnisse VPN-UDP unidirektional (Preis/Performance-Index in Euro/MBit/s)



te auch die SSG-550 bei der Messung mit den größten Frames. Hier schaffte sie 56 Prozent. Der Wechsel in den bidirektionalen Betrieb halbierte auch im Fall der Juniper-Box die möglichen Durchsätze je Senderichtung. So lagen hier die Werte zwischen 3 Prozent mit den kleinsten und

Siemens 4YourSafety RX300S3

28 Prozent mit den größten Frames. Im UDP-Mix-Betrieb schaffte die SSG-550 zwischen 5 und 46 Prozent Durchsatz. Auch hier stiegen die möglichen Durchsätze wieder mit dem Frame-Format an. Mit unserem Real-World-Traffic erreichte die Juniper-Appliance unidirektional 29, bidirektional 15 und im UDP-Mix-Betrieb 24 Prozent Durchsatz.

Mit halber Durchsatzleistung erreichte die Juniper-SSG-550 unidirektional Latency-Werte zwischen rund 370 und 600 µs. Bidirektional stigen diese Werte auf rund 470 bis 1000 µs. Unter maximaler Leistung stiegen diese Werte dann auf vier- bis fünfstellige Zahlen an. So schwankten die Latency-Mittelwerte im unidirektionalen Betrieb dann zwischen rund 5400 und 12 300 µs. Im bidirektionalen Betrieb kam die SSG-550 dann auf eine Latency zwischen rund 12 000 und über 27 000 µs.

Phions Netfence-nf-850 erreichte im unidirektionalen Betrieb mit 64-Byte-Frames eine maximalen Durchsatz von 4 Prozent der nominalen Leitungsgeschwindigkeit. Mit 256-Byte-Frames stieg dieser Wert auf 10, mit 512-Byte-Frames auf 14 Prozent. Maximal war ein Durchsatz von 18 Prozent möglich. Dieser war bei der Messung mit den größten Frames möglich. Der Wechsel in den bidirektionalen Betrieb halbierte auch bei der Phion-Appliance die je Senderichtung möglichen Durchsätze. Im UDP-Mix-Betrieb waren dann Durchsätze zwischen 4 und 17 Prozent möglich. Mit unserem Real-World-Traffic schaffte die Netfence-nf-850 maximal 13 Prozent unidirektional, 12 Prozent mit Mixed-UDP und 6 Prozent bidirektional.

Stonesoft FW-5100

Die Latency-Werte stiegen bei den Messungen des Phion-Systems mit dem Durchsatz an. Im unidirektionalen Betrieb mit halber Durchsatzleistung lagen die Latency-Mittelwerte für die verschiedenen Frame-Formate zwischen 140 und rund 3000 µs. Im bidirektionalen Betrieb mit halber Leistung waren dann Mittelwerte zwischen gut 160 und 360 µs festzustellen. Mit voller Leistung stiegen die Latency-Werte dann im unidirektionalen Betrieb auf Werte zwischen gut 8000 und über 16 000 µs an. Bidirektional schwankten die Mittelwerte für die Latency zwischen rund 32 000 und 59 000 µs.

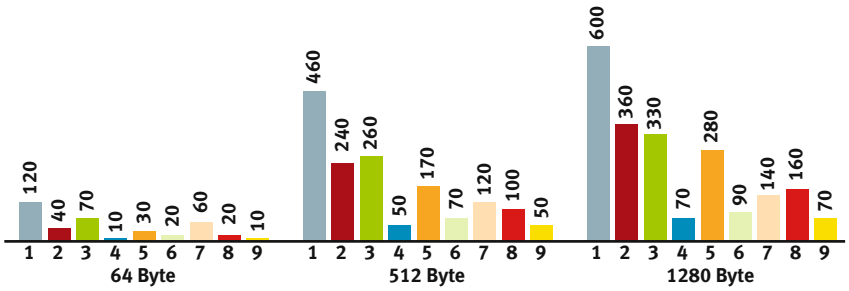
Siemens 4YourSafety-RX300S3 erreichte mit 13 Prozent bei unserer Messung im unidirektionalen Betrieb mit den kleinsten Datenpaketen nach Alcatel-Lucent und knapp vor Fortinet den zweitbesten Wert in dieser Disziplin. Bei ansteigenden Frame-Formaten vermochte die Appliance mit der Check-Point-Software allerdings nicht, mit den beiden anderen Konkurrenten mitzuhalten. Maximal erreichte sie einen Durchsatz von 26 Prozent bei der Messung mit den größten Frames. Der Wechsel in den bidirektionalen Betrieb halbierte dann noch fast die möglichen Durchsätze je Senderichtung. Hier lagen je nach Frame-Format zwischen 6 und 14 Prozent Durchsatzleitung an. Im UDP-Mix-Betrieb schaffte die Siemens-Appliance dann zwischen 11 Prozent mit den kleinsten Frames und 27 Prozent mit den größten Frames.

Die Latency-Mittelwerte mit halber Durchsatzleistung schwankten unidirektional zwischen rund 130 und 250 µs. Bidirektional betrugen sie zwischen rund 130 und 270 µs. Unter Volllast stiegen die Latency-Mittelwerte auch hier bis in den fünfstelligen Bereich an. Unidirektional bewegten sie sich zwischen rund 3900 und fast 30 000 µs. Im bidirektionalen Betrieb schwankten sie zwischen rund 10 000 und über 33 000 µs.

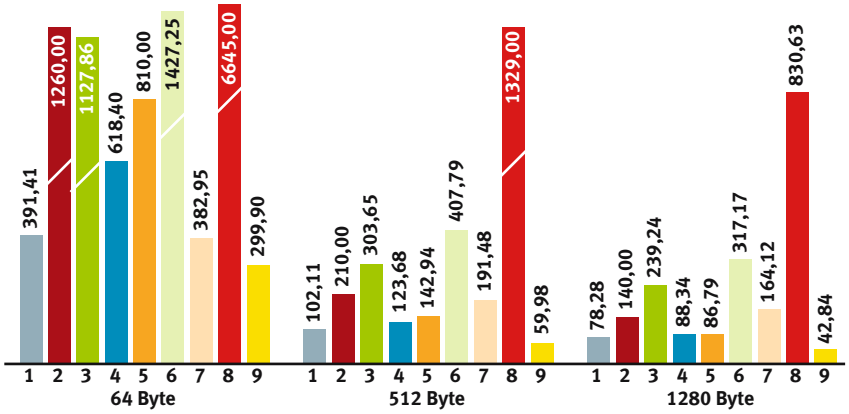
Stonesofts FW-5100 leitete im unidirektionalen Betrieb mit 64-Byte-Paketen maximal 5 Prozent des theoretischen Maximums an Daten weiter. Mit dem Frame-Format stiegen auch hier die Durchsätze. Ihre Maximalleistung erreichte die FW-5100 bei der Messung mit den größten Datenrahmen mit 33 Prozent. Der Wechsel auf den bidirektionalen Betrieb halbierte auch hier die Durchsatzleistung je Senderichtung. So waren hier zwischen 2 und 16 Prozent Durchsatz realisierbar. Im UDP-Mix-Betrieb konnten wir dagegen zwischen 4 Prozent mit den kleinsten Frames und 35 Prozent mit den größten Frames messen. Mit unserem Real-World-Traffic belastet schaffte die Stonesoft-Appliance 19 Prozent Durchsatz unidirektional und 9 Prozent Durchsatz bidirektional.

Mit der halben Durchsatzleistung belastet blieben die Latency-Mittelwerte für die einzelnen Frame-Formate im moderaten dreistelligen Bereich. So waren im unidirektionalen Betrieb zwischen rund 120 und gut 200 µs, im bidirektionalen Betrieb zwischen 116 und 214 µs zu messen. Arbeitete die FW-5100 dagegen mit voller Durchsatzleistung, stiegen die Latency-Mit-

Messergebnisse VPN-UDP bidirektional (Datendurchsatz in MBit/s)



Messergebnisse VPN-UDP bidirektional (Preis/Performance-Index in Euro/MBit/s)



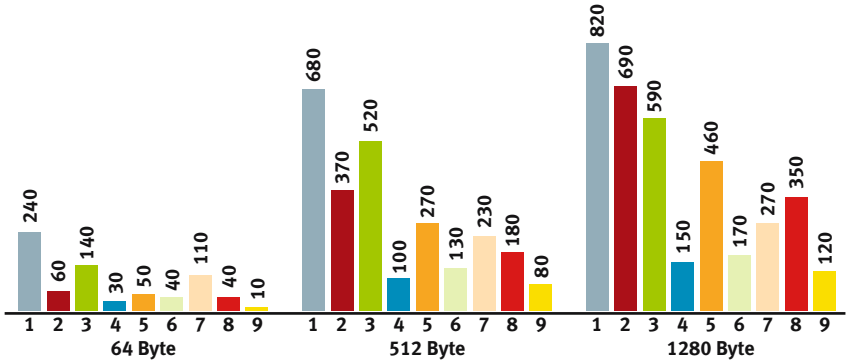
Zyxel ZyWALL 1050

telwerte geradezu dramatisch an. So betrugen sie im unidirektionalen Modus zwischen gut 1 und 10 Millionen µs. Das sind 1 bis 10 Sekunden. Bidirektional stiegen diese Werte noch weiter auf rund 2,8 bis über 10 Sekunden.

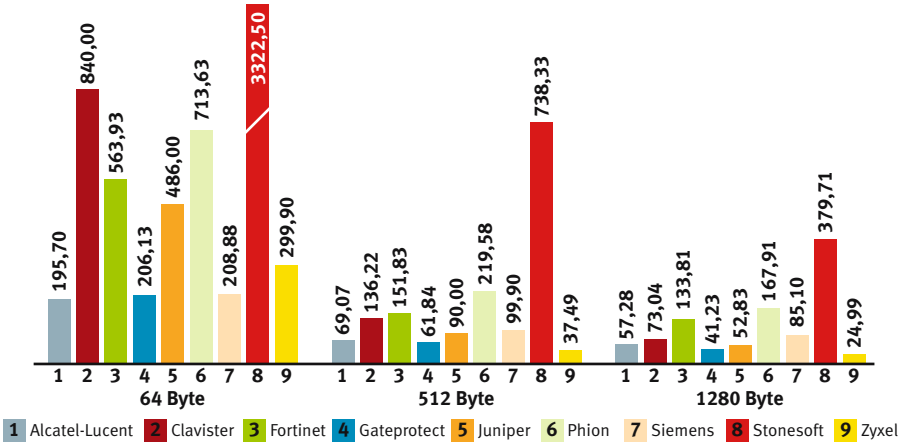
Das mit Abstand preisgünstigste System im Testfeld, Zyxels Zywall-1050, schaffte im unidirektionalen Betrieb mit den kleinsten Frames einen Durchsatz von 2 Prozent. Mit größeren Frames kam dann auch diese Appliance zunehmend besser zurecht. Ihren maximalen Durchsatz erreichte das System dann mit 15 Prozent bei der Messung mit den größten Frames. Der Wechsel in den bidirektionalen Betrieb bedeutete auch für die Zywall-1050 die Halbierung der Durchsätze je Senderichtung. Die Durchsätze betrugen hier also dann zwischen 1 und 7 Prozent der theoretischen Leitungsgeschwindigkeit. Im UDP-Mix-Betrieb waren dann wieder Durchsätze zwischen 1 und 12 Prozent realisierbar. Mit Real-World-Traffic erreichte die Zywall-1050 einen unidirektionalen Durchsatz von 9 und einen bidirektionalen Durchsatz von 4 Prozent.

Schon bei halber Durchsatzleistung lagen die gemessenen Latency-Werte durchweg im vierstelligen Bereich. So schwankten sie im unidirektionalen Betrieb zwischen gut 1400 und fast 3000 µs. Im bidirektionalen Modus lagen die Latency-Mittelwerte dann zwischen gut 1400 bis 2000 µs. Arbeitete die Zyxel-Appliance mit maximalem Durchsatz, stiegen auch hier die Mittelwerte für die Latency deutlich an. So betrugen sie im unidirektionalen Betrieb zwischen rund 6400 und 17 800 µs. Arbeitete die Zywall-1050 im bidirektionalen Modus mit maximaler Geschwindigkeit, stiegen die Latency-Mittelwerte sogar auf 16 500 bis 89 000 µs an.

Messergebnisse VPN-UDP-Mix bidirektional (Datendurchsatz in MBit/s)



Messergebnisse VPN-UDP-Mix bidirektional (Preis/Performance-Index in Euro/MBit/s)



Fazit

Es ist eigentlich ein ganz alter Hut: Die kryptografische Ver- und Entschlüsselung ist ein rechenaufwändiges Verfahren. Und um so sicherer das Verfahren ist, um so aufwändiger ist es auch. Der aktuelle Test hat gezeigt, dass diese Regel immer noch gilt. Und er hat gezeigt, dass Hard- und Software der Security-Appliances

DAS TESTVERFAHREN

Als Lastgenerator/Analysator haben wir in unseren Real-World Labs den bekannten »Smartbits 6000C Traffic Generator/Analyser« von Spirent eingesetzt. Das in dieser Konfiguration rund 250 000 Euro teuere Gerät war mit der Software »Smartflow« ausgestattet und mit 24 Gigabit-Ethernet-Fibre/Kupfer-Ports bestückt. Alle Ports arbeiten im Full-Duplex-Modus und können somit gleichzeitig Last mit Wirespeed generieren und analysieren. Für die TCP-Messungen haben wir dann »Avalanche« und »Reflector« von Spirent verwendet. Bei allen Messungen handelt es sich um Zangenmessungen, bei denen entsprechende Datenströme generiert und analysiert werden.
Um vergleichbare, gültige und aussagefähige Ergebnisse zu erzielen, haben wir im Vorfeld die Einstellungen der Security-Appliances festgelegt und ein für alle Firewall-Tests verbindliches Standard-Rule-Set vorgegeben. Für die korrekte Konfiguration haben wir gemeinsam mit den Ingenieuren des jeweiligen Herstellers gesorgt, die ihr eigenes System im Test begleitet haben.
Die einzelnen Netzsegmente haben wir über Gigabit-Ethernet-Switches 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. Die geringe Latency der Systeme wurde entsprechend berücksichtigt. Mit Hilfe von drei Linux-Intel-PC-Clients in den einzelnen Netzsegmenten haben wir die korrekte Firewall-Konfiguration und -Funktion jeweils vor den einzelnen Testläufen überprüft.

nicht mit der Entwicklung der LAN-Adapter Schritt halten konnten. So liegen realistischerweise zu erwartende Datendurchsätze aktueller Security-Appliances deutlich unter der Nennleistung der zur Verfügung gestellten Gigabit-Ethernet-Adapter. Und das gilt auch für Teststellungen, deren Listenpreise denen von respektablen Limousinen oder rassigen Sportwagen entspricht. Vergleichsweise günstigere Appliances bewegen sich – Gigabit-Ethernet-Adapter hin oder her – von der Leistung eher im Fast-Ethernet-Bereich. Und auch Highend-Systeme tun sich schwer, die Netzwerkbandbreite auch nur zu 50 Prozent auszuschöpfen.

IT-Verantwortliche tun gut daran, auch dieses Leistungspotential nicht voll auszureizen. Denn die Ausnutzung der nutzbaren Kapazität wird mit erhöhten Latency-Werten bestraft. Wann diese anfangen kritisch zu werden, hängt natürlich nicht von den Eigenschaften eines einzelnen Systems ab, sondern von der gesamten Strecke, die ein Signal durchläuft. Bei der Verdoppelung der genutzten Bandbreite steigt in einigen Fällen die Latenz um den Faktor 10 oder gar 100 und mehr. Dieses Verhalten macht es wahrscheinlich, dass es zu Problemen mit Real-Time-Applikationen wie Voice- oder Video-over-IP kommt.

Bis die Hersteller ihre Systeme performanter gemacht haben hilft folglich nur eine intelligente Strategie, die dafür sorgt, dass es im Netz erst gar nicht eng wird. Hier ist sicherlich auch ein geeignetes Bandbreitenmanagement und eine wirkungsvolle Quality-of-Service erforderlich.

Für die Beurteilung einer Security-Appliance ist das VPN-Durchsatzverhalten aber nur ein Kriterium. Gefordert hatten wir auch Merkmale wie Daten-Priorisierung, Bandbreitenmanagement, Hochverfügbarkeit und – natürlich – die eigentlichen Schutzfunktionen. Wie sich die Security-Appliances in Sachen Firewall-Performance und Quality-of-Service sowie Sicherheit in unseren Labs verhalten haben, steht in den kommenden Ausgaben von Network Computing.

Dipl.-Ing. Thomas Rottenau,
Prof. Dr. Bernhard G. Stütz,
dg@networkcomputing.de