

# Brandschutz im Einsatz



**Vergleichstest Security-Appliances – Firewall und VPN bieten einen recht guten Brandschutz in modernen Netzen. Manchmal kommt dabei aber die Performance zu kurz. Dies hat ein Vergleichstest der Real-World Labs von Network Computing ergeben.**

**D**a für, dass es in modernen Unternehmensnetzen gar nicht erst brennt, sollen Security-Appliances sorgen. Diese Appliances stellen Funktionalität wie Firewall und VPN aber auch weitere Security-Funktionalitäten 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, sondern die Hersteller ihre Systeme großzügig mit Fast- und 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 Fast- und Gigabit-Ethernet-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
- ◆ Backup-Rechenzentrum (Serverfarm, SAN, Administration, 5 PC-Arbeitsplätze).

Hinzu kommen vier Niederlassungen in Frankfurt, Berlin, München und Passau mit je-

weils 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 Niederlas-

## REPORTCARD FIREWALL- UND VPN-PERFORMANCE

interaktiv unter [www.networkcomputing.de](http://www.networkcomputing.de)

	Gewichtung	Clavister SG4205	Fortinet Fortigate 300A	Securepoint Security Appliance RC3	gateProtect Firewall Server 5.0 - Professional 2U Box	Lucent VPN Firewall Brick 50	Symantec SGS 1620
FW-Durchsatz 64 Byte unidirekt.	8,33	4	4	5	4	2	2
FW-Durchsatz 512 Byte unidirekt.	8,33	5	5	5	5	5	5
FW-Durchsatz 1518 Byte unidirekt.	8,33	5	5	5	5	5	5
FW-Durchsatz 64 Byte multidirekt.	8,33	2	2	3	1	1	1
FW-Durchsatz 512 Byte multidirekt.	8,33	5	5	5	5	3	4
FW-Durchsatz 1518 Byte multidirekt.	8,33	5	5	5	5	5	5
VPN-Durchsatz 64 Byte unidirekt.	8,33	3	2	2	2	1	1
VPN-Durchsatz 512 Byte unidirekt.	8,33	5	5	5	5	1	1
VPN-Durchsatz 1280 Byte unidirekt.	8,33	5	5	5	5	2	1
VPN-Durchsatz 64 Byte bidirekt.	8,33	2	1	1	1	1	1
VPN-Durchsatz 512 Byte bidirekt.	8,33	5	5	3	3	1	1
VPN-Durchsatz 1280 Byte bidirekt.	8,33	5	5	5	5	1	1
<b>Gesamtergebnis</b>	<b>100,00</b>	<b>4,25</b>	<b>4,08</b>	<b>4,08</b>	<b>3,83</b>	<b>2,33</b>	<b>2,33</b>
<small>A &gt; 4,3; B &gt; 3,5; C &gt; 2,5; D &gt; 1,5; E &lt; 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:                      &gt;/= 85 MBit/s = 5                      &gt;/= 65 MBit/s = 4                      &gt;/= 45 MBit/s = 3                      &gt;/= 25 MBit/s = 2                      &lt; 25 MBit/s = 1</small>		<b>B+</b>	<b>B+</b>	<b>B+</b>	<b>B</b>	<b>D</b>	<b>D</b>

**DAS TESTFELD****Fast-Ethernet-Appliances**

- ◆ Clavister SG4205
- ◆ Fortinet FGT 300A
- ◆ Gateprotect Firewall Server 5.0 – Professional 2U Box
- ◆ Lucent Brick 50
- ◆ Securepoint RC3
- ◆ Symantec Symantec Gateway Security 1620

sungen 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 seines 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.

Gigabit-Ethernet-Firewall- und VPN-Appliances:

- ◆ 2 Firewall- und VPN-Appliances inklusive Zubehör und Dokumentation,
- ◆ 1 VPN-Client (Windows-Software),
- ◆ IPSec-VPN,
- ◆ Verschlüsselung nach 3DES,
- ◆ Verschlüsselung nach AES mit 256 Bit,
- ◆ je Gerät mindestens 3 Gigabit-Ethernet-Ports (RJ45-Stecker),
- ◆ zusätzlicher Management-Port (Fast-Ethernet oder Gigabit-Ethernet mit RJ45-Stecker),
- ◆ Content-Security,
- ◆ High-Availability (HA),
- ◆ Datenpriorisierung,
- ◆ Bandbreiten-Management sowie
- ◆ IPS/IDS-Funktionalität.

Fast-Ethernet-Firewall- und VPN-Appliances:

- ◆ 2 Firewall- und VPN-Appliances inklusive Zubehör und Dokumentation,
- ◆ 1 VPN-Client (Windows-Software),
- ◆ IPSec-VPN,

- ◆ Verschlüsselung nach 3DES,
- ◆ AES-Verschlüsselung mit 256 Bit,
- ◆ je Gerät mindestens 3 Fast-Ethernet-Ports (RJ45-Stecker),
- ◆ zusätzlicher Management-Port (Fast-Ethernet mit RJ45-Stecker),
- ◆ Content-Security,
- ◆ High-Availability (HA),
- ◆ Datenpriorisierung,
- ◆ Bandbreiten-Management sowie
- ◆ IPS/IDS-Funktionalität.

Folgende Testparameter sollten untersucht werden:

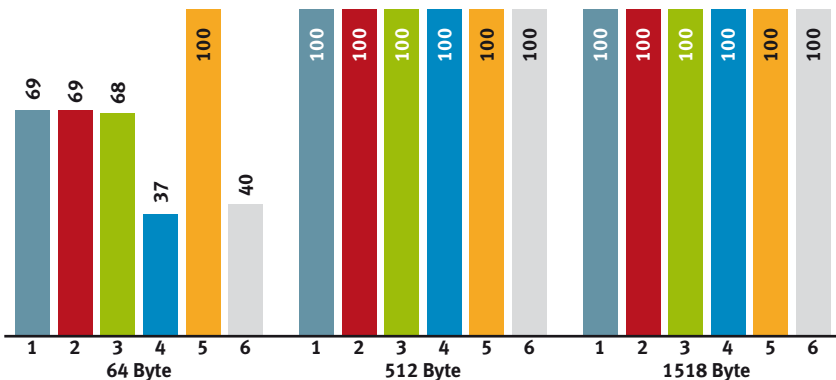
- ◆ Firewall-Performance: Datendurchsatzraten (unidirektional/bidirektional) im Firewall-Betrieb,
- ◆ VPN-Performance: Datendurchsatzraten (unidirektional/bidirektional) im VPN-Betrieb,
- ◆ Intrusion-Prevention-Funktionalität unter verschiedenen Belastungssituationen,

- ◆ Packet-Loss, Latency und - Jitter,
- ◆ Überprüfung der Firewall-, VPN- und HA-Funktionalität,
- ◆ Überprüfung der Content-Security- und Intrusion-Prevention-Funktionalität und
- ◆ Überprüfung der Datenpriorisierung und des Bandbreiten-Managements.

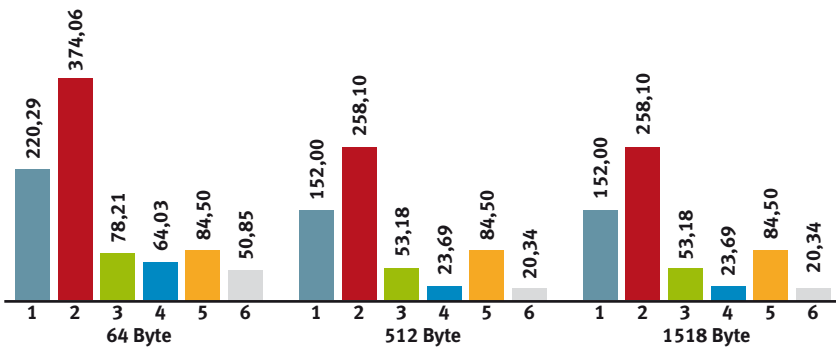
Die gesamte Funktionalität sollte durch dokumentierte Konfigurati-

— Anzeige —

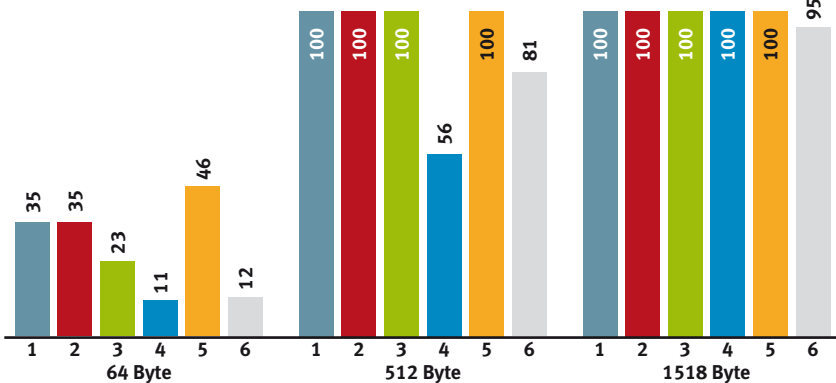
Messergebnisse FW unidirektional (Datendurchsatz in MBit/s)



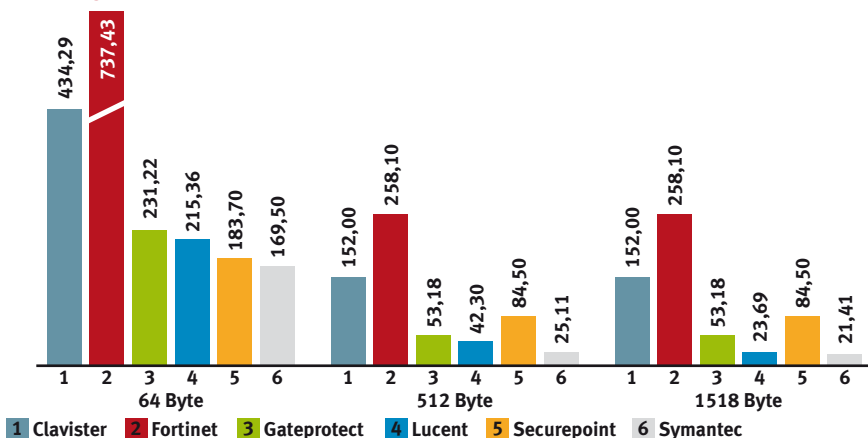
Messergebnisse FW unidirektional (Preis/Performance-Index in Euro/MBit/s)



Messergebnisse FW multidirektional (Datendurchsatz in MBit/s)



Messergebnisse FW multidirektional (Preis/Performance-Index in Euro/MBit/s)



onseinstellungen 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 gruppiert sich in zwei Bereiche: Gigabit-Ethernet-Systeme mit Firewall- und VPN-Funktionalität und Fast-Ethernet-Appliances mit Firewall- und VPN-Funktionalität. Wie sich die Fast-Ethernet-Appliances im Test verhalten haben steht im vorliegenden Artikel. Die Ergebnisse der Gigabit-Ethernet-Tests folgen dann in den kommenden Ausgaben von Network Computing. An den Vorbereitungen für einen Intrusion-Prevention-Vergleichstest arbeiten wir derzeit noch.

Das erste Testfeld im Vergleichstest Firewall- und VPN-Systeme bildeten die Fast-Ethernet-Systeme »Clavister SG4205«, »Fortinet FGT 300A«, »Gateprotect Firewall Server 5.0«, »Lucent Brick 50«, »Securepoint RC3« sowie »Symantec Gateway Security 1620«. Ein zweites Testfeld bilden Gigabit-Ethernet-Appliances von Clavister, Fortinet, Gateprotect, Juniper und Netasq. 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 Fast-Ethernet-Segment dar. Die weiteren Folgen unseres Security-Vergleichstests werden dann die Performance-Messungen im Gigabit-Ethernet-Umfeld sowie Quality-of-Service, Hochverfügbarkeit und Exploit-Erkennung zum Thema haben.

Firewall-UDP-Durchsatz

In unserer ersten Messreihe haben wir den UDP-Datendurchsatz im Firewall-Betrieb untersucht. Hierbei musste die jeweilige Firewall drei Netzsegmente gegeneinander abschotten: das interne Netz, das externe Netz und die DMZ. Um den Datenverkehr zwischen diesen drei Netzsegmenten zu simulieren, haben wir die zu testenden Systeme über drei Ports mit unserem Lastgenerator/Analysator Smartbits verbunden. Die Smartbits generierten dann Flows aus UDP-Paketen jeweils mit konstant 64, 512, 1024 und 1518 Byte Größe, die Last beginnt bei jeder Messung mit 10 Prozent und wird dann in 10-Prozent-Schritten bis auf 100 Prozent erhöht. Weitere Detail-Messungen haben wir dann in 1-Prozent-Schritten durchgeführt, um die Leistungsgrenzen exakt zu analysieren. Die Belastung der Systeme im Test ist in diesem Aufbau zunächst unidirektional, dann bidirektional und zuletzt multidirektional. Bei den unidirektionalen Messungen ging der Datenstrom vom LAN in Richtung DMZ. Bei den symmetrischen bidirektionalen Messungen haben wir eine entsprechende Kommunikation zwischen LAN und DMZ simuliert. Bei den asymmetrisch-bidirektionalen Messungen lief ein Datenstrom vom LAN ins WAN, der andere vom WAN in die DMZ. Im multidirektionalen Modus haben wir dann Kommunikationsflüsse zwischen LAN,

DMZ und WAN simuliert. Hierbei senden und empfangen alle drei Ports gleichzeitig.

Gemessen haben wir Frame-Loss, Latency und Jitter. Aus den ermittelten Frame-Loss-Werten errechnen sich die Werte für den maximalen Durchsatz, der unter optimalen Bedingungen möglich ist. Dieser ist der maximal erreichbare Durchschnittswert aller jeweils gemessenen Flows bei einem Frame-Loss von weniger als einem Prozent.

Als Variante der ersten Messreihe haben wir Firewall-UDP-Durchsatz mit NAT gemessen. Diese zweite Messreihe besteht aus drei Messungen: mit Source-NAT unidirektional vom LAN ins WAN, mit Destination-NAT unidirektional vom WAN in die DMZ sowie eine bidirektionale Kombination aus SNAT und DNAT mit Datenströmen vom LAN ins WAN sowie vom WAN in die DMZ.

Volle Leitungsgeschwindigkeit erreichte Clavisters SG4205 bei allen UDP-Durchsatzmessungen. Lediglich bei den Messungen mit einer Frame-Size von 64 Byte blieb diese Appliance hinter dem Sollwert zurück. Im unidirektionalen Betrieb mit dem kleinsten Frame-Format schaffte die SG4205 noch einen Durchsatz von 69 MBit/s. Im symmetrischen wie asymmetrischen bidirektionalen Betrieb mit 64-Byte-Frames ging die Performance dann auf 35 MBit/s zurück. Diese Durchsatzleistung konnte das System dann aber auch im multidirektio-

nalen Betrieb noch halten. Bei unseren Messungen mit NAT änderte sich an diesem Verhalten nichts.

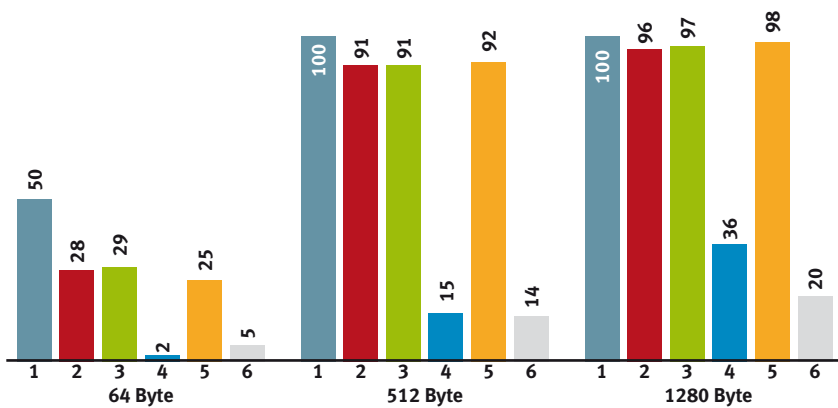
Fortinets FGT-300A glich in ihrem Verhalten dem System von Clavister wie ein Ei dem anderen. Auch die zweite Appliance im Feld arbeitete völlig unbeeindruckt mit Leitungsgeschwindigkeit, so lange wir nicht mit 64-Byte-Frames Last erzeugten. In diesem Fall konnten wir auch hier unidirektional Durchsätze von 69 MBit/s und bi- beziehungsweise multidirektional 35 MBit/s messen. Setzten wir zusätzlich noch NAT ein, änderte sich an den Messergebnissen im Prinzip nichts.

Auch Gateprotects Firewall Server 5.0-Appliance stellte klaglos ihre volle Bandbreite von 100 MBit/s zur Verfügung, sofern die Frames größer als 64 Byte waren. Und das unabhängig davon, ob sie uni-, bi- oder multidirektional arbeiten musste. Verwendeten wir das kleinste Frame-Format, lagen die Durchsatzwerte geringfügig unter denen der Systeme von Clavister und Fortinet. Im unidirektionalen Betrieb vermochte die

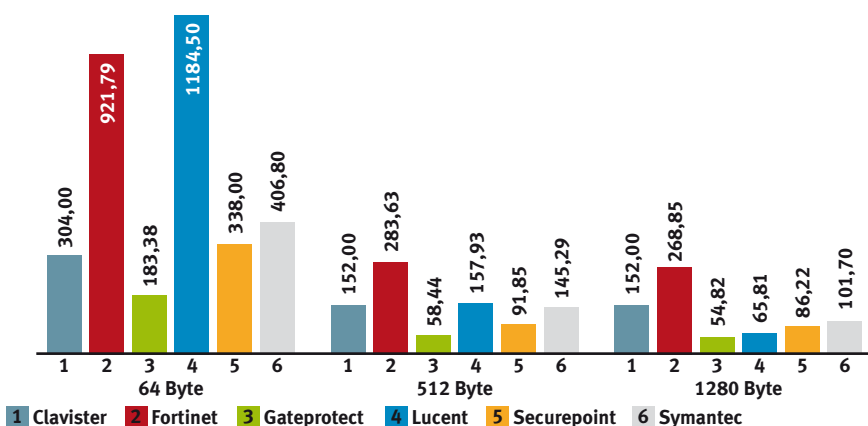
Clavister SG4205



Messergebnisse VPN unidirektional (Datendurchsatz in MBit/s)



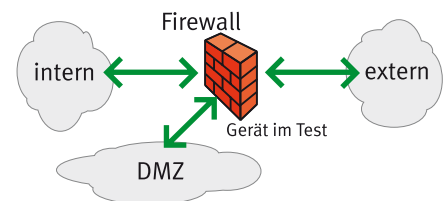
Messergebnisse VPN unidirektional (Preis/Performance-Index in Euro/MBit/s)



Firewall-Server-5.0-Appliance mit 68 MBit/s mit den genannten noch mitzuhalten. Im bidirektionalen Modus schaffte das Gateprotect-System dann noch 34 MBit/s. Maßen wir multidirektionalen Datenströmen, reduzierte sich der Durchsatz des Systems auf 23 MBit/s. Setzten wir zusätzlich noch NAT ein, erzielten wir praktisch die gleichen Resultate.

Größere Probleme mit kleinen Frames müssen wir der Brick-50 bescheinigen. Lucent Appliance schaffte bei unserer unidirektionalen Messung mit 64-Byte-Frames gerade 37 MBit/s. Wechselten wir auf bidirektionalen Betrieb, waren gerade noch 15 MBit/s im symmetrischen und 18 MBit/s im asymmetrischen Modus möglich. Im multidirektionalen Betrieb mit 64-Byte-Frames schaffte die Brick-50 dann noch 11 MBit/s. Mit größeren Frame-Formaten kam auch das Lucent-System deutlich besser zurecht. So schaffte es bei den unidirektionalen Messungen mit größeren Frames durchgängig Leitungsgeschwindigkeit. Im bidirektionalen Modus war die Performance-Schwäche dann noch et-

Testaufbau Firewall-UDP-Durchsatz



was ausgeprägter. So erreichte die Brick-50 bei der Messung mit bidirektional symmetrischen Datenströmen und 512-Byte-Paketen 79 MBit/s. Bidirektional asymmetrisch waren es dann 89 MBit/s. Den größten Stress hatte die Lucent-Firewall bei unserer Messung mit multidirektionalen Datenströmen. Verwendeten wir 512-Byte-Pakete, waren noch 56 MBit/s drin, bei der Messung mit 1024-Byte-Paketen schaffte das System 88 MByte/s. Bei allen übrigen Messungen lieferte die Brick-50 dann auch Leitungsgeschwindigkeit. Musste die Brick-50 zusätzlich noch die Adressen via NAT verarbeiten, ließ die Durchsatzleistung insbesondere bei der Verarbeitung kleinerer Pakete noch weiter nach.

Securepoints RC3 schaffte in unseren UDP-Firewall-Durchsatzmessungen mit Abstand die besten Performance-Werte. So ist die RC3 das einzige System im Test, das bei den unidirektionalen Messungen ausnahmslos Leitungsgeschwindigkeit zur Verfügung stellte. Und auch

TECHNISCHE DATEN

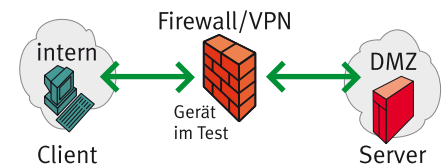
FIREWALL- UND VPN-SYSTEME

	Clavister SG4205	Fortinet FortiGate 300A	gateProtect Firewall Server 5.0 - Professional 2U Box	Lucent VPN Firewall Brick 50	Securepoint Security Appliance RC3	Symantec SGS 1620
Anzahl unabh. (nicht geschwichteter) LAN-Ports						
Anzahl Gigabit-Ethernet-Ports	2 <sup>2)</sup>	2	1	0	0	3
Anzahl Fast-Ethernet-Ports	4	4	4	3	6	0
Anzahl WAN-Ports						
X.21	0	0	0	0	0	0
X.25	0	0	0	0	0	0
ISDN <sub>50</sub>	0	0	0	0	0	0
ISDN <sub>52M</sub>	0	0	0	0	0	0
xDSL	4	0	2	0	1	0
E1	0	0	0	0	0	2
Hardware/Betriebssystem						
Prozessor (Typ), Taktrate	k.A.	Celeron, 2GHz	P4, 2,4 GHz	MMD Geode, 466MHz	P4, 3GHz	k.A.
Arbeitsspeicher in MByte	k.A.	512	1024	64	1024	k.A.
Betriebssystem Name/Version	Clavister OS v. 8.6.02	FortiOS 3.0	Debian Linux Kern. (2.4.31)	Inferno version 9.0.187	Securepoint Linux	Linux, gehärtet
IPv6-Unterstützung für alle FW-Funktionen	○	○	○	○	○	○
Firewall-Technik						
Stateful-Inspection-Firewall	●	●	●	●	●	●
Layer-7-Application-Gateway-Proxies	●	●	●	●	●	●
anpassbare Proxies	●	●	●	●	●	●
Stateful-Inspection und Proxy kombiniert	●	●	●	●	●	●
transparente FW-Funktionalität konfigurierbar	●	○	○	○	○	○
spezielle Firewall-ASICs integriert	●	●	○	○	○	○
Netzwerkprozessor mit FW 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)	2	16	0	0	4	2
Cluster über 3rd-Party-Software etabliert	○	○	○	○	○	○
Cluster über externen Load-Balancer-Switch	○	○	○	○	○	○
Cluster über Netzwerk-Links etabliert	●	●	○	○	○	●
Management						
Telnet	○	●	○	○	○	○
rollenbasierte Verwaltung	○	●	○	○	○	○
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	●	●	○	○	○	○
Schwellenwerte für Auslastung möglich	●	●	○	○	○	○
Logging-Daten und -Events						
per SNMP exportiert	○	●	○	○	○	○
per WELF-Format exportiert	○	●	○	○	○	○
an Syslog-Server exportieren	○	●	○	○	○	○
Events zentralisiert	●	●	○	○	○	○
Event-Management korreliert einzelne Einträge	●	●	○	○	○	○
Authentisierung/Autorisierung						
NT-Domain	○	○	○	○	○	○
TACACS+/TACACS+	○	○	○	○	○	○
Radius	○	○	○	○	○	○
LDAP über TLS	○	○	○	○	○	○
X.509-digitale Zertifikate	○	○	○	○	○	○
Token-basierend	○	○	○	○	○	○
Sicherheitsfeatures						
DMZ	●	●	●	●	●	●
Intrusion-Detection-/Prevention	●	●	○	○	○	○
AAA-Support	●	●	○	○	○	○
DHCP	●	●	○	○	○	○
NAT-Support	●	●	○	○	○	○
Content-Filter	○	○	○	○	○	○
Virens Scanner	○	○	○	○	○	○
Listenpreis in Euro für Teststellung zzgl. MwSt. <sup>1)</sup>	15 200	25 810	5 318	2 369 <sup>3)</sup>	8 450	2 034 <sup>4)</sup>
Website	www.clavister.de	www.fortinet.com	www.gateprotect.de	www.lucent.com/security	www.securepoint.de	www.symantec.de

bei den bidirektionalen Messungen, schaffte die Securepoint-Appliance bei der Messung mit 64-Byte-Paketen immer noch 74 beziehungsweise 76 MBit/s. Bei größeren Frames war auch hier durchgehend Leitungsgeschwindigkeit möglich. Erst bei unserer Messung mit multidirektionalen Datenströmen und 64-Byte-Paketen ging die Durchsatzleistung der RC3 deutlicher zurück. Hier waren noch 46 MBit/s möglich. Verwendeten wir größere Frames, kam das System auch hier auf volle Leitungsgeschwindigkeit. Auch die Messungen mit NAT gaben kein anderes Bild von der RC3 ab.

Symantecs Gateway-Security-1620 ähnelte dagegen in ihrer Leistungscharakteristik dem System von Lucent. So waren schon bei der unidirektionalen Messung mit 64-Byte-Frames lediglich 40 MBit/s möglich. Wechselten wir auf bidirektionalen Betrieb, halbierte sich die Leistung auf rund 20 beziehungsweise 23 MBit/s. Im multidirektionalen Betrieb schaffte die Gateway-Security-1620 dann bei einer Frame-Größe von 64 Byte noch 12 MBit/s. Mit größeren Frame-Formaten kam dann auch die Symantec-Appliance deutlich besser zurecht. So schaffte sie bei allen uni- wie bidirektionalen Messungen mit

Testaufbau Firewall-TCP-Messung



größeren Frames durchweg Leitungsgeschwindigkeit. Unsere Messungen mit multidirektionalen Datenströmen und größeren Frames brachten die Gateway-Security-1620 dann erneut an ihre Grenzen, hier lagen je nach Frame-Format die möglichen Durchsätze zwischen 81 und 95 MBit/s. Der Betrieb mit NAT reduzierte dann die Durchsatzleistungen noch weiter.

Firewall-TCP-Messungen

In unserer dritten Messreihe haben wir die Connection-Setup-Rate, die Connection-Capacity sowie den maximal erreichbaren Durchsatz in MBit/s im Firewall-Betrieb gemessen. Die Connection-Setup-Rate gibt an, wie viele Verbindungen das System maximal pro Sekunde aufbauen kann. Die Connection-Capacity ist das Maß dafür, wie viele Verbindungen das System maximal gleichzeitig halten kann.

Bei der TCP-Performance-Messung baut die Messtechnik Verbindungen durch die Firewall auf und generiert Datenströme. Bei der unidirektionalen Messung geht der Hauptdatenstrom vom Reflector zum Avalanche. Bei der bidirektionalen Messung laufen die Datenströme

Quelle: Angaben der Hersteller

● = ja; ○ = nein; k.A. = keine Angabe; 1) = 2 Appliances (Hardware- und Software) inkl. Lizenzen für 100 User u. vollst. Management-Lösung; 2) plus 8 MiniGBIC; 3) Sonderpreis bis 30.6.2006; 4) inklusive Lizenz für 3 Monate;

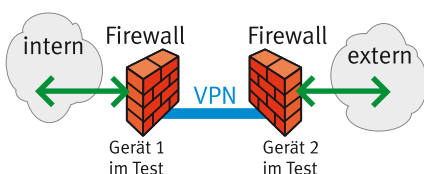


Fortinet FortiGate 300A

vom WAN ins LAN sowie von der DMZ ins WAN. Die generierte Last ähnelt insgesamt einer uni- beziehungsweise bidirektionalen Smartbits-Messung mit größeren UDP-Paketten. Die jeweilige Appliance wird an die Messtechnik, den Spirent Avalanche und Reflector, angeschlossen. Als Frame-Formate haben wir hier 512, 1024 und 1518 Byte verwendet. Die Messtechnik simuliert so die Kommunikation zwischen Client-Systemen im internen Netzwerk sowie Rechnern in der DMZ und im externen Netz und protokolliert das Verhalten der Appliance. Da die Ergebnisse der TCP-Durchsatzmessungen gegenüber den UDP-Durchsatzmessungen keine signifikanten Abweichungen zeigten, gehen wir auf die einzelnen Messergebnisse hier nicht weiter ein.

Clavisters SG4205 schaffte den Aufbau von 16 000 Verbindungen pro Sekunde und erreichte eine Connection-Capacity von 127 000 Sessions. Fortinets FGT-300A konnte bei der Connection-Setup-Rate mithalten und erreichte ebenfalls den Wert von 16 000 Verbindungen pro Sekunde. Bei der Messung der Connection-Capacity gab es ein technisches Problem, da das System wie wir vermuteten in einen Fail-over-Modus wechselte. Nach GUI-Statistik waren aber rund 500 000 Verbindungen möglich. Fortinet erklärt das Verhalten ihres Systems folgendermaßen: Die FGT wurde mit TCP Sessions »geladen«. Auf der Fortigate blieb der maximale Session-Count bei rund 500 000 stehen, auf dem Avalanche-Generator wurden jedoch rund 1,5 Millionen Sessions gezählt. Das System verhält sich so, dass von den bestehenden Sessions die am wenigsten aktiven gedroppt werden. Zu keinem Zeitpunkt gehen Pakete »stateless« durch die FGT. Durch dieses Verhalten soll gewährleistet werden, dass die Box aktiv bleibt beziehungsweise Services überwiegend zur Verfügung bleiben.

#### Testaufbau VPN-UDP-Durchsatz



Auch Gateprotects Firewall-Server-5.0-Appliance baute 16 000 Verbindungen pro Sekunde auf. Insgesamt vermochte sie 65 000 Verbindungen gleichzeitig zu halten. Lucent's Brick-50 bleibt dagegen bei der Messung der Connection-Setup-Rate unter der Messgrenze von 1000 Sessions. Als Connection-Capacity konnten wir dagegen einen Wert von immerhin 26 000 Sessions ermitteln.

Securepoints RC3 erreichte mit 19 000 Verbindungen das beste Ergebnis in der Disziplin Connection-Setup-Rate und setzte mit einer Connection-Capacity 1 048 000 Verbindungen einen Höchstwert im Testfeld. Symantecs Gateway-Security-1620 blieb dagegen mit einer Setup-Rate von 6000 Verbindungen und einer Connection-Capacity von 49 000 hinter dem Feld zurück.



Securepoint Security Appliance RC3b

#### VPN-UDP-Durchsatz

In einer weiteren 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-Paketten jeweils mit konstant 64, 512, 1024 und 1280 Byte Größe. Die Last beginnt auch hier wieder mit 10 Prozent und wird dann in 10-Prozent-Schritten bis auf 100 Prozent erhöht. Der Aufbau der VPN-Tunnel erfolgt zwischen den beiden Appliances. Standardmäßig haben wir das VPN durch AES-256-Verschlüsselung realisiert. Die Belastung des VPN-Systems erfolgte erst uni- und dann bidirektional, das heißt beide Ports sendeten und empfangen gleichzeitig maximal mit Wirespeed.



gateProtect  
Firewall Server 5.0 – Professional 2U Box



Lucent VPN Firewall Brick 50

In einer Variante der UDP-Durchsatzmessung, die wir hier »Mix UDP« nennen, haben wir 50 Prozent der jeweiligen Gesamtlast verschlüsselt durch den VPN Tunnel geschickt. Die übrigen 50 Prozent der Gesamtlast gingen unverschlüsselt über die Leitung. Die gemessenen Durchsätze entsprechen der Gesamtleistung des Systems. Auch diese Variante haben wir unidirektional und bidirektional durchgeführt. Gemessen haben wir wieder Frame-Loss, Latency und Jitter. 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 kleiner 1 Prozent.

Auch bei unseren VPN-Performance-Messungen legte Clavisters SG4205 die Messlatte recht hoch an. So schaffte die Appliance bei unserer Messung mit 64 Byte-Paketen immerhin 50 MBit/s. Verwendeten wir größere Frames, so

erreichte die SG4205 bei unseren unidirektionalen Messungen durchweg Leistungsgeschwindigkeit. Im bidirektionalen Betrieb reduzierten sich die möglichen Durchsätze dann durchgehend. Führten wir die Messung mit 64-Byte-Frames durch, dann schaffte das System noch 28 MByte/s. Bei größeren Frames lagen die möglichen Durchsatzraten zwischen 91 und 93 MByte/s. Im Mix-UDP-Modus waren die möglichen Durchsatzraten dann messbar höher. Hier konnten wir unidirektional zwischen 66 und 98 MBit/s und bidirektional zwischen 32 und 97 MBit/s messen.

Fortinets FGT-300A lag in dieser Disziplin ein Stück hinter Clavister zurück. So schaffte die FGT-300A bei der unidirektionalen Messung mit 64-Byte-Paketen einen Durchsatz von 28 MBit/s. Nicht ganz Leitungsgeschwindigkeit erreichte das Fortinet-System auch bei den Messungen mit größeren Frames. Hier lagen die

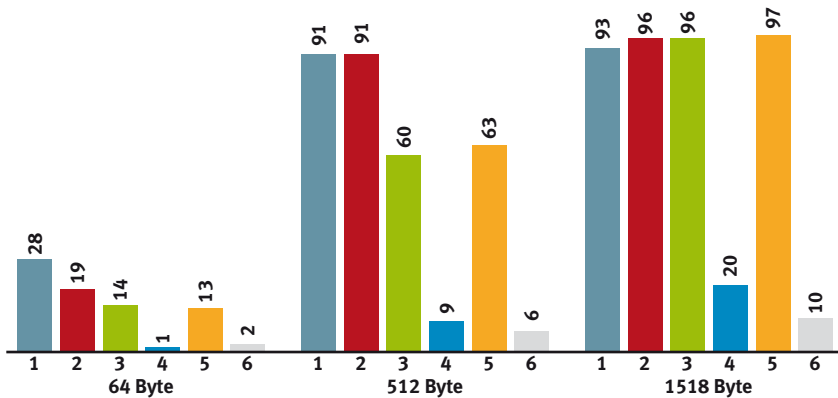
Werte zwischen 91 und 96 MBit/s. Im bidirektionalen Betrieb mit 64-Byte-Paketen erreichte die FGT-300A noch 19 MBit/s. Bei den Messungen mit größeren Frames schwankten die Durchsatzraten zwischen 91 und 96 MBit/s. Im Mix-UDP-Modus verhielt sich die FGT-300A nicht deutlich anders als im UDP-VPN-Modus.

Gateprotects Firewall-Server-5.0-Appliance lieferte sich bei den unidirektionalen Messungen ein Kopf-an-Kopf-Rennen mit Fortinets FGT-300A. Hier schwankten die Durchsätze je nach Frame-Format zwischen 29 und 97 MBit/s. Im bidirektionalen VPN-Betrieb blieb die Firewall-Server-5.0-Appliance dann hinter der FGT-300A zurück. So schaffte sie hier mit 54-Byte-Frames einen Durchsatz von 14 MBit/s. Bei der Messung mit 512-Byte-Frames erreichte sie 60 MBit/s und bei den noch größeren Frame-Formaten lagen dann Durchsätze von 86 beziehungsweise 96 MBit/s an. Im Mix-UDP-Modus verhielt sich die Gateprotect-Appliance dann ähnlich wie das Fortinet-System.

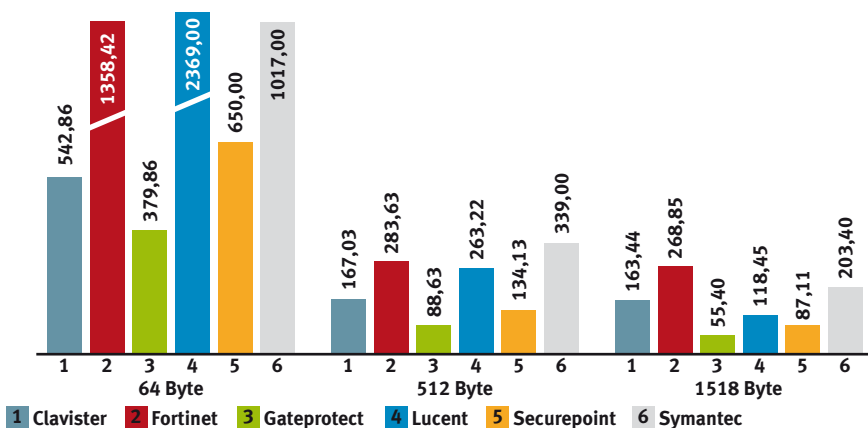
Lucent's Brick-50 lag in den gemessenen Durchsätzen deutlich hinter den oben genannten Systemen zurück. So schaffte sie im unidirektionalen VPN-Betrieb mit den kleinsten Frames gerade mal 2 MBit/s. Verwendeten wir größere Frame-Formate, waren auch hier höhere Durchsatzraten drin. Ein Maximum von 36 MBit/s im Betrieb mit den größten Frames bleibt aber deutlich von der gewünschten Leitungsgeschwindigkeit zurück. Im bidirektionalen Betrieb halbierten sich die Durchsatzwerte dann noch, so dass je nach Frame-Format Durchsätze zwischen 1 und 20 MBit/s möglich waren. Im Mix-UDP-Modus waren dann höhere Durchsätze möglich. Die Messwerte schwanken hier zwischen 4 und 64 MBit/s im unidirektionalen und zwischen 3 und 36 MBit/s im bidirektionalen Betrieb.

Securepoints RC3 kam dagegen der Leitungsgeschwindigkeit deutlich näher. Schaffte das System unidirektional mit 64 Byte-Frames noch 25 MBit/s, so stiegen die Durchsatzraten bei unseren Messungen mit größeren Frames auf Werte zwischen 92 und 98 MBit/s an. Langsamer wurde auch die RC3 im bidirektionalen Betrieb. So standen hier bei der Messung mit 64-Byte-Frames noch 13 MBit/s an Bandbreite zur Verfügung. Bei den Messungen mit größeren Frames schwankten die Ergebnisse zwischen 63 und 97 MBit/s. Im Mix-UDP-Modus war dann auch die RC3 tendentiell etwas schneller. So erreichte sie im bidirektionalen Betrieb je nach verwendetem Frame-Format Ergebnisse zwischen 21 und 100 MBit/s.

Messergebnisse VPN bidirektional (Datendurchsatz in MBit/s)



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



## DAS TESTVERFAHREN

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 teure Gerät war mit der Software »Smartflow« 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. 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 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 Firewall-Konfiguration und -Funktion jeweils vor den einzelnen Testläufen überprüft.

**Alle Messergebnisse finden Sie im Internet unter:**  
[www.networkcomputing.de/nwc\\_downloads/fw\\_vpn\\_fast\\_ethernet\\_o6.zip](http://www.networkcomputing.de/nwc_downloads/fw_vpn_fast_ethernet_o6.zip)



Symantec SGS 1620

Symantecs Gateway-Security-1620 ähnelte in ihrem Leistungsverhalten dem System von Lucent. So schaffte das System im unidirektionalen Betrieb Durchsätze zwischen 5 und 20 MBit/s. Bidirektional blieben davon dann noch zwischen 2 und 10 MBit/s übrig, wobei die Performance auch hier mit dem Frame-Format anstieg. Im Mix-UDP-Modus verdoppelten sich die möglichen Durchsätze, wobei absolut auch im günstigsten Fall nicht mehr als 37 MBit/s möglich waren.

### Fazit

Leitungsgeschwindigkeit ist immer noch keine Selbstverständlichkeit für Security-Appliances. Dabei treten Bandbreitenengpässe in erster Linie dort auf, wo entsprechende Rechenarbeit zu leisten ist. So bleiben alle Systeme insbesondere im VPN-Betrieb mit kleinen Frames deutlich hinter der geforderten Leitungsgeschwindigkeit zurück. Deutliche Unterschiede in ihrem Durchsatzverhalten zeigen aber auch die einzelnen Appliances untereinander. Für die Anforderungen unserer Musterfirma unterdimensioniert waren die Teststellungen von Lucent und Symantec. Die

se Systeme lagen auch preislich unter den Geräten des Mitbewerbs, die durchsatzstärker arbeiteten. Für unsere Anforderungen recht ordentliche Datendurchsätze zeigten die besser platzierten, teureren Systeme, die in ihrem Leistungsverhalten recht dicht beieinander lagen. Dabei zeigt der Test eindeutig, dass die Preise der Appliances in einem direkten Verhältnis zur Leistungsfähigkeit der Systeme stehen. Performance erfordert leistungsfähige Hardware- und die hat ihren Preis.

Für die Beurteilung einer Security-Apliance ist das Durchsatzverhalten aber nur ein Kriterium. Gefordert hatten wir auch Merkmale wie Daten-Priorisierung, Bandbreitenmanagement, Hochverfügbarkeit und – natürlich – die eigentlichen Schutzfunktionen. Wie sich die Gigabit-Ethernet-Systeme in Sachen Performance und alle Systeme im Testfeld in Sachen 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](mailto:dg@networkcomputing.de)

**DAS TESTFELD**

**Gigabit-Ethernet-Appliances**

- ◆ Clavister SG4205
- ◆ Gateprotect Firewall Server 5.0 – Professional 4U Enterprise Box
- ◆ Juniper ISG-2000
- ◆ Netasq F2000

**Fast-Ethernet-Appliances**

(Testbericht in NWC 5-6 2006, S. 20 ff.)

- ◆ Clavister SG4205
- ◆ Fortinet FGT 300A
- ◆ Gateprotect Enterprise
- ◆ Lucent Brick 50
- ◆ Securepoint RC3
- ◆ Symantec Gateway Security 1620

# Brandschutz im Einsatz



**Vergleichstest Security-Appliances, Teil 2 – Firewall und VPN bieten einen recht guten Brandschutz in modernen Netzen. Zu kurz kommt dabei aber immer noch die Performance. Dies hat ein Vergleichstest der Real-World Labs ergeben.**

**D**afür, dass es in modernen Unternehmensnetzen gar nicht erst brennt sollen Security-Appliances sorgen. Diese Appliances stellen Funktionalität wie Firewall und VPN aber auch weitere Security-Funktionalitäten 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 großzügig mit Fast- und 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 Fast- und Gigabit-Ethernet-Security-Appliances auf ihre Tauglichkeit für den performanten Schutz von Unternehmensnetzen und deren einzelnen Segmenten.



**REPORTCARD** FIREWALL- UND VPN-PERFORMANCE

interaktiv unter [www.networkcomputing.de](http://www.networkcomputing.de)

Alle Messergebnisse finden Sie unter: [www.networkcomputing.de/nwc\\_downloads/fw\\_vpn\\_gigabit\\_ethernet\\_o6.zip](http://www.networkcomputing.de/nwc_downloads/fw_vpn_gigabit_ethernet_o6.zip)

	Gewichtung	Juniper Networks ISG-2000	Clavister SG4205	Gateprotect Firewall-Server-5.0 – Professional-4U Enterprise-Box	Netasq F2000
FW-Durchsatz 64 Byte unidirekt.	8,33	5	3	3	2
FW-Durchsatz 512 Byte unidirekt.	8,33	5	5	5	4
FW-Durchsatz 1518 Byte unidirekt.	8,33	5	5	5	5
FW-Durchsatz 64 Byte multidirekt.	8,33	4	2	2	1
FW-Durchsatz 512 Byte multidirekt.	8,33	5	4	4	3
FW-Durchsatz 1518 Byte multidirekt.	8,33	5	4	4	3
VPN-Durchsatz 64 Byte unidirekt.	8,33	4	2	2	1
VPN-Durchsatz 512 Byte unidirekt.	8,33	5	4	3	2
VPN-Durchsatz 1280 Byte unidirekt.	8,33	5	4	3	3
VPN-Durchsatz 64 Byte bidirekt.	8,33	3	1	1	1
VPN-Durchsatz 512 Byte bidirekt.	8,33	5	3	2	2
VPN-Durchsatz 1280 Byte bidirekt.	8,33	5	4	2	2
<b>Gesamtergebnis</b>	<b>100,00</b>	<b>4,67</b>	<b>3,42</b>	<b>3,00</b>	<b>2,42</b>
<small>A &gt; 4,3; B &gt; 3,5; C &gt; 2,5; D &gt; 1,5; E &lt; 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: &gt;/= 700 MBit/s = 5 &gt;/= 350 MBit/s = 4 &gt;/= 150 MBit/s = 3 &gt;/= 40 MBit/s = 2 &lt; 40 MBit/s = 1</small>		<b>A</b> 	<b>C+</b>	<b>C</b> 	<b>D</b>

**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

- ◆ Backup-Rechenzentrum (Serverfarm, SAN, Administration, 5 PC-Arbeitsplätze).
- ◆ High-Avalibility (HA),
- ◆ Datenpriorisierung,
- ◆ Bandbreiten-Management sowie
- ◆ IPS/IDS-Funktionalität.
- ◆ IPSec-VPN,
- ◆ Verschlüsselung nach 3DES,
- ◆ Verschlüsselung nach AES mit 256 Bit,
- ◆ je Gerät mindestens 3 Fast-Ethernet-Ports (RJ45-Stecker),
- ◆ Bandbreiten-Management sowie
- ◆ IPS/IDS-Funktionalität.
- ◆ Firewall-Performance: Datendurchsatzraten (unidirektional/bidirektional) im Firewall-Betrieb,
- ◆ VPN-Performance: Datendurchsatzraten (unidirektional/bidirektional) im VPN-Betrieb,

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.

Fast-Ethernet-Firewall und VPN-Appliances:

- ◆ 2 Firewall- und VPN-Appliances inklusive Zubehör und Dokumentation,
- ◆ 1 VPN-Client (Windows-Software),

- ◆ zusätzlicher Management-Port (Fast-Ethernet mit RJ45-Stecker),
- ◆ Content-Security,
- ◆ High-Avalibility (HA),
- ◆ Datenpriorisierung,

— Anzeige —

## Die Ausgangssituation

Die Network Computing Musterfirma möchte die verschiedenen Segmente seines heterogenen, konvergenten Netzwerks sowie eine eigenständige DMZ am Unternehmensstandort hochperformant untereinander sowie mit dem Intranet 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.

Gigabit-Ethernet-Firewall und VPN-Appliances:

- ◆ 2 Firewall- und VPN-Appliances inklusive Zubehör und Dokumentation,
- ◆ 1 VPN-Client (Windows-Software),
- ◆ IPSec-VPN,
- ◆ Verschlüsselung nach 3DES,
- ◆ Verschlüsselung nach AES mit 256 Bit,
- ◆ je Gerät mindestens 3 Gigabit-Ethernet-Ports (RJ45-Stecker),
- ◆ zusätzlicher Management-Port (Fast-Ethernet oder Gigabit-Ethernet mit RJ45-Stecker),
- ◆ Content-Security,

TECHNISCHE DATEN

FIREWALL- UND VPN-SYSTEME

	Clavister SG4205	Gateprotect Firewall-Server-5.0-Professional-4U-Enterprise-Box	Juniper Networks ISG-2000	Netasq F2000
Anzahl unabh. (nicht geschwächter) LAN-Ports				
Anzahl Gigabit-Ethernet-Ports	2 + 8 MiniGBIC	4	6	12
Anzahl Fast-Ethernet-Ports	4	9	0	12
Anzahl WAN-Ports				
X.21	0	0	0	0
X.25	0	0	0	0
ISDN S0	0	0	0	0
ISDN S2M	0	0	0	0
xDSL	4	3	0	0
E1	0	0	0	0
Hardware/Betriebssystem				
Prozessor (Typ), MHz	k.A.	AMD Opteron 2,8 Ghz	8 x Power PC CPU 1 Ghz	Intel Xeon 2,4 Ghz
Arbeitsspeicher in MByte	k.A.	2048	7000	1024
Betriebssystem Name/Version	Clavister OS v. 8.6.02	Debian Linux Kernel (2.4.31)	Screen OS 5.0	NS.BSD 6.1
IPv6-Unterstützung für alle Firewall-Funktionen	○	○	●	○
Firewall-Technik				
Stateful-Inspection-Firewall	●	●	●	●
Layer-7-Application-Gateway-Proxies	●	●	●	●
anpassbare Proxies	●	●	●	●
Stateful-Inspection und Proxy kombiniert	●	○	●	●
transparente FW-Funktionalität konfigurierbar	●	○	●	○
spezielle Firewall-ASICs integriert	○	○	○	○
Netzwerkprozessor mit FW 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)	2	0	2	2
Cluster über 3rd-Party-Software etabliert	○	○	○	○
Cluster über externen Load-Balancer-Switch	○	○	○	○
Cluster über Netzwerk-Links etabliert	●	○	●	○
Management				
Telnet	○	○	●	○
rollenbasierte Verwaltung	●	●	●	●
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	●	○	●	●
Schwellenwerte für Auslastung möglich	●	●	●	●
Logging-Daten und -Events				
per SNMP exportiert	●	○	●	●
per WELF-Format exportiert	○	○	●	●
an Syslog-Server exportieren	●	○	●	●
Events zentralisiert	●	○	●	●
Event-Management korreliert einzelne Einträge	●	○	○	○
Authentisierung/Autorisierung				
NT-Domain	●	○	●	●
TACACS/TACACS+	○	○	○	○
RADIUS	●	●	●	●
LDAP über TLS	○	○	●	●
X.509-digitale Zertifikate	●	○	●	●
Token-basierend	●	○	●	●
Sicherheitsfeatures				
DMZ	●	●	●	●
Intrusion-Detection/-Prevention	●	●	●	●
AAA-Support	●	○	●	●
DHCP	●	○	●	●
NAT-Support	●	○	○	●
Content-Filter	●	●	○	●
Virens Scanner	○	●	○	●
Listenpreis in Euro für Teststellung zzgl. MwSt. <sup>1)</sup>	48 000	8993	87 000	18 500
Website	www.clavister.de	www.gateprotect.de	www.juniper.net	www.netasq.com

Quelle: Angaben der Hersteller

● = ja; ○ = nein; k.A. = keine Angabe; 1) = 2 Appliances (Hardware- und Software) inkl. Lizenzen für 100 User u. vollst. Management-Lösung;

- ◆ Intrusion-Prevention-Funktionalität unter verschiedenen Belastungssituationen,
- ◆ Packet-Loss, Latency und - Jitter,
- ◆ Überprüfung der Firewall-, VPN- und HA-Funktionalität,
- ◆ Überprüfung der Content-Security- und Intrusion-Prevention-Funktionalität und
- ◆ Überprüfung der Datenpriorisierung und des Bandbreiten-Managements.

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 gruppiert sich in zwei Bereiche: Gigabit-Ethernet-Systeme mit Firewall- und VPN-Funktionalität und Fast-Ethernet-Appliances mit Firewall- und VPN-Funktionalität. Wie sich die Gigabit-Ethernet-Systeme in der Disziplin Performance verhalten haben, steht im vorliegenden Artikel. Die Ergebnisse des Fast-Ethernet-Performance-Tests haben wir im ersten Teil dieses Tests in NWC 5-6 2006, S. 20 ff. veröffentlicht.

Das erste Testfeld im Vergleichstest Firewall- und VPN-Systeme bildeten die Fast-Ethernet-Systeme »Clavister SG4205«, »Fortinet FGT 300A«, »Gateprotect Enterprise«, »Lucent Brick 50«, »Securepoint RC3« sowie »Symantec Gateway Security 1620«. Das zweite Testfeld bildeten die Gigabit-Ethernet-Appliances »Clavister SG4205«, »Gateprotect Firewall Server 5.0 – Professional 4U Enterprise Box«, »Juniper ISG-2000« und »Netasq F2000«. Die Performance-Testergebnisse dieser Systeme beschreiben wir im vorliegenden Artikel.

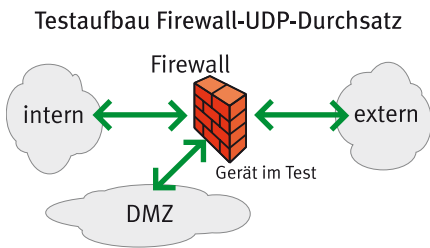
In unseren Tests haben wir generell die Aspekte Firewall- und VPN-Performance, Quality-of-Service, Hochverfügbarkeit und Exploit-Erkennung untersucht. Wie sich die Fast- wie auch die Gigabit-Ethernet-Appliances in den Disziplinen Quality-of-Service, Hochverfügbarkeit und Exploit-Erkennung bewährt haben, steht dann in einer der kommenden Ausgaben von Network Computing.

### Firewall-UDP-Durchsatz

In unserer ersten Messreihe haben wir den UDP-Datendurchsatz im Firewall-Betrieb untersucht. Hierbei musste die jeweilige Firewall drei Netzsegmente gegeneinander abschotten: das interne Netz, das externe Netz und die DMZ. Um den Datenverkehr zwischen diesen drei Netzsegmenten zu simulieren, haben wir die zu testenden Systeme über drei Ports mit unserem Lastgenerator/Analysator Smartbits verbunden. Die Smartbits generierten dann Flows aus UDP-Paketen jeweils mit konstant 64, 512, 1024 und 1518 Byte Größe, die Last beginnt bei jeder Messung mit 10 Prozent und wird dann in 10-Prozent-Schritten bis auf 100 Prozent erhöht. Weitere Detail-Messungen haben wir dann in 1-Prozent-Schritten durchgeführt, um die Leistungsgrenzen exakt zu analysieren. Die Be-

lastung der Systeme im Test ist in diesem Aufbau zunächst unidirektional, dann bidirektional und zuletzt multidirektional. Bei den unidirektionalen Messungen ging der Datenstrom vom LAN in Richtung DMZ. Bei den symmetrischen bidirektionalen Messungen haben wir eine entsprechende Kommunikation zwischen LAN und DMZ simuliert. Bei den asymmetrisch-bidirektionalen Messungen lief ein Datenstrom vom LAN ins WAN, der andere vom WAN in die DMZ. Im multidirektionalen Modus haben wir dann Kommunikationsflüsse zwischen LAN, DMZ und WAN simuliert. Hierbei senden und empfangen alle drei Ports gleichzeitig.

Gemessen haben wir Frame-Loss, Latency und Jitter. Aus den ermittelten Frame-Loss-Werten errechnen sich die Werte für den maximalen Durchsatz, der unter optimalen Bedingungen möglich ist. Dieser ist der maximal erreichbare Durchschnittswert aller jeweils gemessenen

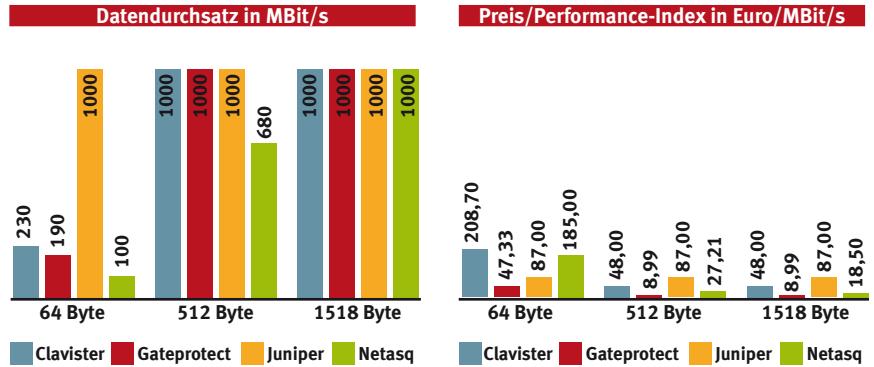


Flows bei einem Frame-Loss von weniger als einem Prozent.

Als Variante der ersten Messreihe haben wir Firewall-UDP-Durchsatz mit NAT gemessen. Diese zweite Messreihe besteht aus drei Messungen: mit Source-NAT unidirektional vom LAN ins WAN, mit Destination-NAT unidirektional vom WAN in die DMZ sowie eine bidirektionale Kombination aus SNAT und DNAT mit Datenströmen vom LAN ins WAN sowie vom WAN in die DMZ.

Volle Leitungsgeschwindigkeit erreichte Clavisters SG4205 bei unserer Messung mit unidi-

### Messergebnisse Firewall unidirektional



rektionalem UDP-Durchsatz so lange wir Frames verwendeten, die größer als 64 Byte waren. Bei der Messung mit den kleinsten Frames ging schon hier der maximal mögliche Durchsatz auf 230 MBit/s zurück. Im bidirektionalen Betrieb kam die Clavister-Appliance dann noch etwas schneller an ihre Grenzen. Hier waren schon bei einer Frame-Größe von 512 Byte nur noch 710 MBit/s und bei Verwendung der kleinsten Frames lediglich 120 MBit/s möglich. Dabei waren die Messwerte für den symmetrischen und für den asymmetrischen Betrieb praktisch identisch. Im multidirektionalen Betrieb war Leitungsgeschwindigkeit dann nur noch bei der Messung mit den 1518 Byte großen Frames drin. Schon bei der Verwendung von

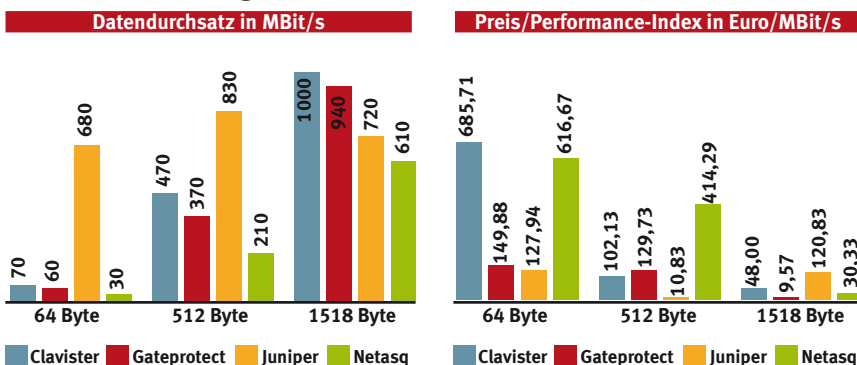
1024-Byte-Frames ging der Durchsatz auf 850 MBit/s zurück. Verwendeten wir die kleinsten Frames, bremste die SG4205 dann auf 70 MBit/s herunter.

Gateprotects Firewall-Server 5.0 in der Professional-4U-Enterprise-Box-Version ähnelte in seinem Verhalten sehr dem Clavister-System. Leitungsgeschwindigkeit schaffte auch diese Box im unidirektionalen Betrieb durchgängig mit Ausnahme der Messung mit 64-Byte-Frames. Hier waren dann noch 190 MBit/s möglich. Im bidirektionalen Betrieb traten auch hier schon Datenverluste bei unserer Messung mit 512-Byte-Frames auf. Bei dieser Messung schaffte der Firewall-Server einen Durchsatz von 580 MBit/s. Bei größeren Frames war auch im bidi-



Juniper Networks ISG-2000

### Messergebnisse Firewall multidirektional



rektonalen Betrieb noch Leitungsgeschwindigkeit möglich. Diese erreicht das Gateprotect-System dann im multidirektionalen Betrieb nicht mehr. Verwendeten wir hierbei die größten Frames, schaffte der Firewall-Server maximal 940 MBit/s. mit abnehmender Frame-Größe gingen die Durchsätze dann bis auf 60 MBit/s zurück.

Mehr Dampf als die Systeme von Clavister und Gateprotect hatte dann Junipers ISG-2000. Bei den uni- wie bidirektionalen Messungen lieferte diese Appliance unabhängig von der Frame-Größe durchgängig Wirespeed. Erst im multidirektionalen Betrieb geriet auch die Juniper-Appliance an ihre Grenzen. Hier schwankten die maximal erreichbaren Durchsätze zwi-



Clavister SG4205

schen 830 und 680 MBit/s. Dabei standen die maximal erreichbaren Durchsätze nicht in einem direkten Verhältnis zum verwendeten Frame-Format und somit zur Anzahl der zu verarbeitenden Datenrahmen pro Zeiteinheit.

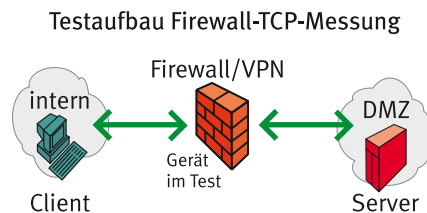
Netsqs F2000 kam dagegen schon recht schnell an ihre Grenzen. So erreichte sie Leitungsgeschwindigkeit im unidirektionalen Modus nur bei den Messungen mit 1518 und 1024 Byte großen Frames. Verwendeten wir 512 Byte große Frames, waren noch 680 MBit/s möglich. Bei den kleinsten Frames bremste die F2000 dann auf 100 MBit/s herunter. Im bidirektionalen Betrieb gingen dann die Durchsätze weiter zurück. Leitungsgeschwindigkeit schaffte die Netasq-Appliance nicht mehr. Hier lagen die erreichbaren Durchsätze je nach Frame-Format zwischen 920 beziehungsweise 940 und 50 MBit/s, wobei die erzielbaren Durchsätze mit der Frame-Größe abnahmen. Im multidirektionalen Betrieb ergab sich ein ähnliches Bild. Allerdings schaffte die F2000 hier nur noch Durchsätze zwischen 610 und 30 MBit/s.

**Firewall-TCP-Messungen**

In unserer dritten Messreihe haben wir die Connection-Setup-Rate, die Connection-Capacity sowie den maximal erreichbaren Durchsatz in MBit/s im Firewall-Betrieb gemessen. Die Connection-Setup-Rate gibt an, wie viele Verbindungen das System maximal pro Sekunde aufbauen kann. Die Connection-Capacity ist das Maß dafür, wie viele Ver-

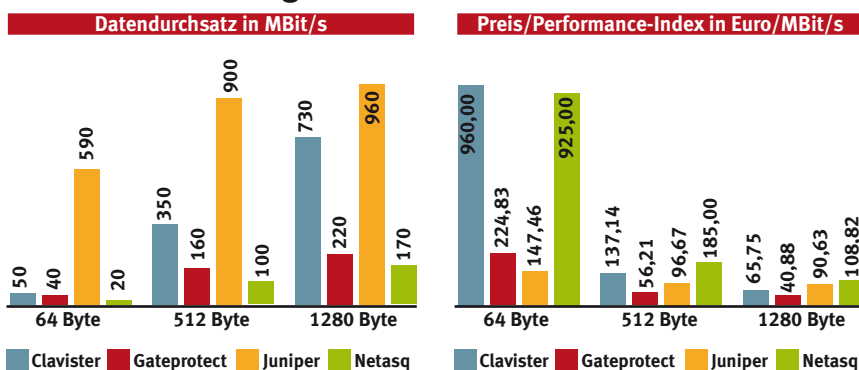
bindungen das System maximal gleichzeitig halten kann.

Bei der TCP-Performance-Messung baut die Messtechnik Verbindungen durch die Firewall auf und generiert Datenströme. Bei der unidirektionalen Messung geht der Hauptdatenstrom vom Reflector zum Avalanche. Bei der bidirektionalen Messung laufen die Da-



tenströme vom WAN ins LAN sowie von der DMZ ins WAN. Die generierte Last ähnelt insgesamt einer uni- beziehungsweise bidirektionalen Smartbits-Messung mit größeren UDP-Paketen. Die jeweilige Appliance an die Messtechnik, den Spirent Avalanche und Reflector, angeschlossen. Als Frame-Formate haben wir hier 512, 1024 und 1518 Byte verwendet. Die Messtechnik simuliert so die Kommunikation zwischen Client-Systemen im internen Netzwerk sowie Rechnern in der DMZ sowie

**Messergebnisse VPN unidirektional**



im externen Netz und protokolliert das Verhalten der Appliance. Da die Ergebnisse der TCP-Durchsatzmessungen gegenüber den UDP-Durchsatzmessungen keine signifikanten Abweichungen zeigten, gehen wir auf die einzelnen Messergebnisse hier nicht weiter ein.

Clavisters SG4205 konnte bei unseren Messungen der Connection-Setup-Rate und der Connection-Capacity voll mit unserer Messtechnik mithalten. Die gemessenen Ergebnisse entsprechen daher dem Hardware-Limit unserer Smartbits. Die SG4205 vermochte mindestens 45 000 Verbindungen pro Sekunde aufzubauen und mindestens 2 200 000 Verbindungen gleichzeitig zu halten.

Die drei anderen Appliances im Gigabit-Ethernet-Testfeld blieben dagegen mehr oder



Gateprotect Firewall-Server-5.0 – Professional-4U Enterprise-Box

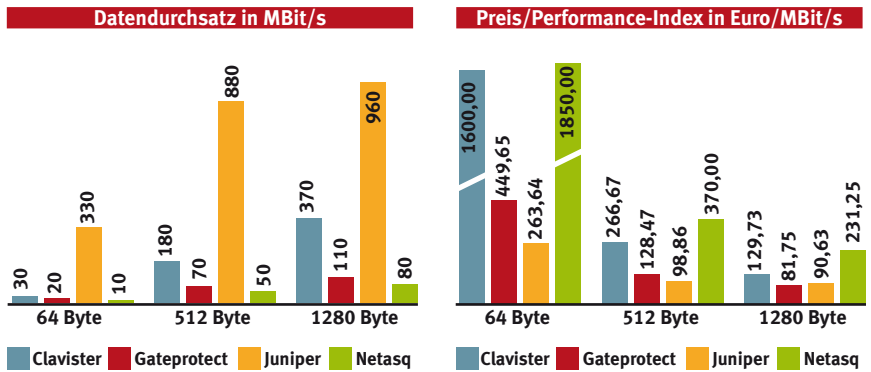
weniger deutlich hinter der Performance unserer Messtechnik zurück. So erreichte der Gateprotect-Firewall-Server eine Connection-Setup-Rate von 36 000 Sessions und eine Connection-Capacity von 524 000 Verbindungen. Junipers ISG-2000 baute »nur« maximal 10 000 Verbindungen pro Sekunde auf. Dieser Wert ist zwar der schlechteste im Gigabit-Ethernet-Testfeld aber absolut immer noch unbedenklich. Gleichzeitig halten konnte die ISG-2000 dann immer-

hin 1 048 000 Verbindungen. Netasqs F2000 lag mit einer Connection-Capacity von 22 000 und einer Connection-Setup-Rate von 1 850 000 Verbindungen im Mittelfeld.

**VPN-UDP-Durchsatz**

In einer weiteren Messreihe haben wir den VPN-UDP-Durchsatz ermittelt. Hierzu haben wir zwei identische Appliances miteinander verbunden. Dann haben wir den Smartbits-Lastgene-

**Messergebnisse VPN bidirektional**



rator/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, 512, 1024 und 1280 Byte Größe. Die Last beginnt auch hier wieder mit 10 Prozent und wird dann in 10-Prozent-Schritten bis auf 100 Prozent erhöht. Der Aufbau der VPN-Tunnel erfolgt zwischen den beiden Appliances. Standardmäßig haben wir das VPN durch 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 »Mix UDP« 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. Auch diese Variante haben wir unidirektional und bidirektional durchgeführt. Gemessen haben wir wieder Frame-Loss, Latency und Jitter. 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 kleiner 1 Prozent.

Bei unseren VPN-Messungen erreichten alle Systeme im Testfeld die Leitungsgeschwindigkeit nicht mehr. So schaffte Clavisters SG4205 im unidirektionalen Betrieb mit den 1280 Byte großen Frames einen Durchsatz von 730 MBit/s. Mit kleiner werdenden Frames ging dann auch die Durchsatzleistung weiter zurück, So konnten wir bei der Messung mit 512-Byte-Frames noch einen Durchsatz von 350 MBit/s und bei der Messung mit den kleinsten Frames noch einen Durchsatz von 50 MBit/s messen. Im bidirektionalen Betrieb halbierten sich die Datendurchsätze dann. Hier waren je nach verwendetem Frame-Format zwischen 370 und 30 MBit/s möglich.

Im Mix-UDP-Modus verhielt sich die SG4205 im Prinzip genauso wie bei den vorhergehenden VPN-Messungen. Allerdings lagen die erzielbaren Durchsätze noch ein Stück höher. So erreich-

**DAS TESTVERFAHREN**

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 teure Gerät war mit der Software »Smartflow« 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. 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 Configuration haben wir gemeinsam mit den Ingenieuren des jeweiligen Herstellers gesorgt, die ihr eigenes System im Test begleitet haben. Die einzelnen Netzsegmente haben wir über LAN-Switches vom Typ »Extreme Networks Summit 48si« realisiert. Diese Systeme leisteten in 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 Firewall-Configuration und -Funktion jeweils vor den einzelnen Testläufen überprüft.



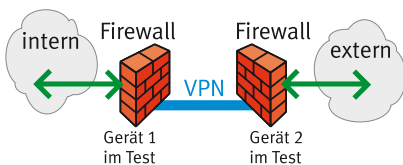
Netasq F2000

te die Clavister-Appliance hier im unidirektionalen Betrieb zwischen 980 und 90 MBit/s. Bei unseren Messungen mit bidirektionalen Datenströmen reduzierte sich der Datendurchsatz dann wieder deutlich. Hier waren noch zwischen 490 und 30 MBit/s realisierbar.

Gateprotects Firewall-Server erwies sich bei unseren VPN-Messungen als deutlich leistungsschwächer als das Clavister-System. So schaffte der Firewall-Server im unidirektionalen Betrieb zwischen 220 MBit/s mit den größten Frames und 40 MBit/s mit den kleinsten Frames. Auch hier halbierten sich die je Senderichtung möglichen Durchsätze noch mal mit der Umstellung auf den bidirektionalen Betrieb. Hier konnten wir noch Durchsätze zwischen 110 und 20 MBit/s messen.

Im Mix-UDP-Betrieb konnte auch Gateprotects Firewall-Server wieder spürbar höhere Durchsatzraten erzielen. Unidirektional wa-

#### Testaufbau VPN-UDP-Durchsatz



ren hier zwischen 410 und 70 MBit/s möglich. Bidirektional blieben davon je Senderichtung noch zwischen 200 und 30 MBit/s übrig.

Junipers ISG-2000 erwies sich bei unseren Messungen mit AES256-Verschlüsselung als performantestes System im Testfeld. So schaffte die ISG-2000 im unidirektionalen Betrieb mit 1280-Byte-Frames einen Durchsatz von 960 MBit/s. Mit den kleinsten Frames waren dann noch immerhin 590 MBit/s drin. Im bidirektionalen Betrieb war die Juniper-Appliance praktisch genauso leistungsfähig wie im unidirektionalen Betrieb. Auch hier schaffte die ISG-2000 mit den größten Frames einen

Durchsatz von 960 MBit/s pro Senderichtung. Erst bei der Messung mit den kleinsten Frames schaffte die ISG-2000 im bidirektionalen Modus weniger Durchsatz je Senderichtung als im unidirektionalen Betrieb. Hier waren noch maximal 330 MBit/s möglich.

Im Mix-UDP-Betrieb war auch hier noch etwas mehr Performance feststellbar. Allerdings schaffte die Juniper-Box auch hier keine echte Leistungsgeschwindigkeit. Dafür kam sie aber bei den Messungen mit den kleinsten Frames auf noch etwas besser Werte: 750 MBit/s im unidirektionalen und 400 MBit/s im bidirektionalen Betrieb waren drin.

Netasqs F2000 erwies sich dagegen bei unseren VPN-Performance-Messungen als das durchsatzschwächste System im Gigabit-Ethernet-Testfeld. Im unidirektionalen Betrieb schaffte die Box bei unserer Messung mit den größten Frames gerade 170 MBit/s. Verwendeten wir die kleinsten Frames, blieb eine Bandbreite von 20 MBit/s übrig. Der Wechsel in den bidirektionalen Modus halbierte die verfügbaren Bandbreiten je Senderichtung zusätzlich. Hier standen also nur noch zwischen 80 und 10 MBit/s an Durchsatzleistung zur Verfügung.

Mit dem Mix-UDP-Betrieb kam die F2000 dann schon besser zurecht. Hier lagen bei den unidirektionalen Messungen zwischen 290 und 30 MBit/s an. Bidirektional reduzierten sich auch die Durchsätze auf Werte zwischen 140 und 10 MBit/s.

#### Fazit

Leitungsgeschwindigkeit ist auch und gerade in der Klasse der Gigabit-Ethernet-Geräte immer noch keine Selbstverständlichkeit. Dabei treten Bandbreitenengpässe in erster Linie dort auf, wo entsprechende Rechenarbeit zu leisten ist. So bleiben alle Systeme insbesondere im VPN-Betrieb mit kleinen Frames deutlich hinter der geforderten Leitungsgeschwindigkeit zurück. Klare Unterschiede in ihrem Durchsatzverhalten zeigen aber auch die einzelnen Appliances untereinander. Dabei zeigt der Test eindeutig, dass die Preise der Appliances in einem direkten Verhältnis zur Leistungsfähigkeit der Systeme stehen. Performance erfordert leistungsfähige Hardware – und die hat ihren Preis.

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

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