# Im Flaschenhals hängen geblieben

## Vergleichstest Security-Appliances Teil 2 – Gigabit-Ethernet-Security-Appliances bilden häufig den Flaschenhals in modernen Netzen. Dies hat ein Vergleichstest der Real-World Labs von Network Computing ergeben.

Dafür, dass Unternehmen weitgehend abgesichert ihren Geschäften nachgehen können, sollen Security-Appliances sorgen. Diese Appliances stellen Funktionalität wie Firewall, VPN oder auch IPS 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 Router, Switches und andere Systeme möglichst mit Wirespeed arbeiten sollen und nicht zum Flaschenhals wer-

**REPORTCARD** FIREWALL- UND VPN-PERFORMANCE

interaktiv unter www.networkcomputing.de

| | Gewichtung | Siemens YourSafety RX300 with Turbocard R55 HFA14 | Astaro Sun Fire V20z | Clavister SG-4230 | Pyramid BenHur² 80 X (künftig Collax Business Server) |
|---|---|---|---|---|---|
| Max. FW-Durchsatz 64 Byte | 8,33 | 3 | 2 | 2 | 2 |
| Max. FW-Durchsatz 512 Byte | 8,33 | 5 | 4 | 4 | 3 |
| Max. FW Durchsatz 1024 Byte | 8,33 | 5 | 5 | 4 | 4 |
| Max. FW-Durchsatz 64 Byte (Block) | 8,33 | 3 | 2 | 2 | 2 |
| Max. FW-Durchsatz 512 Byte (Block) | 8,33 | 5 | 4 | 4 | 3 |
| Max. FW-Durchsatz 1024 Byte (Block) | 8,33 | 5 | 5 | 4 | 4 |
| Max. VPN-Durchsatz 64 Byte unidirektional | 8,33 | 3 | 2 | 2 | 2 |
| Max. VPN-Durchsatz 512 Byte unidirektional | 8,33 | 5 | 3 | 4 | 3 |
| Max. VPN-Durchsatz 1024 Byte unidirektional | 8,33 | 5 | 3 | 4 | 3 |
| Max. VPN-Durchsatz 64 Byte bidirektional | 8,33 | 1 | 1 | 1 | 1 |
| Max. VPN-Durchsatz 512 Byte bidirektional | 8,33 | 5 | 2 | 2 | 2 |
| Max. VPN-Durchsatz 1024 Byte bidirektional | 8,33 | 5 | 3 | 3 | 3 |
| **Gesamtergebnis** | **100,00** | **4,17** | **3,00** | **3,00** | **2,67** |
| 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 - | Max. Durchsatz ›/= 700 MBit/s = 5 ›/= 350 MBit/s = 4 ›/= 150 MBit/s = 3 ›/= 40 MBit/s = 2 ‹ 40 MBit/s = 1 | B + | C | C | C - |
| Gesamtergebnisse und gewichtete Ergebnisse basieren auf einer Skala von 0 bis 5 | | | | | |

Siemens YourSafety RX300 with Turbocard R55 HFA14 – Der Testsieger lag in fast allen Durchsatzmessungen vor dem Mitbewerb.

## TESTFELD

### Firewall- und VPN-Systeme

**Fast-Ethernet-Appliances**

- Astaro Security Gateway 220
- Clavister SG-3150
- Funkwerk bintec VPN Access 250
- gateProtect Firewall Server v. 4.2.1
- Lucent VPN Firewall Brick 150
- OSST SecureGUARD for Microsoft ISA Server 2004 ISA110
- Rimapp RoadBLOCK CF401U
- Telcotech LiSS II secure gateway pro
- Zycel ZyWALL 5

**Gigabit-Ethernet-Appliances**

- Astaro Sun Fire V20z
- Clavister SG-4230
- Pyramid BenHur² 80 X (künftig Collax Business Server)
- Siemens 4YourSafety RX300 with Turbocard R55 HFA14

den dürfen. Wie gut solche Systeme diese Anforderungen erfüllen, sollte ein groß angelegter 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. Das Testfeld gruppiert sich in drei Bereiche: Gigabit-Ethernet-Systeme mit Firewall- und VPN-Funktionalität, Gigabit-Ethernet-Systeme mit Intrusion-Prevention-Technologie, auch Intrusion-Protection-Systeme genannt, und Fast-Ethernet-Appliances mit Firewall- und VPN-Funktionalität. Wie sich die Fast-Ethernet-Appliances im Test verhalten haben ist im ersten Teil dieses Vergleichstests, den wir im Network Computing Special 7/2005 veröffentlicht haben, nachzulesen. Die Ergebnisse der Gigabit-Ethernet-Tests steht im vorliegenden Artikel.

Das Testfeld der Gigabit-Ethernet-Firewall-und-VPN-Appliances bildeten Astaros auf Sun-Hardware basierende »Sun Fire V20z«, die »Clavister SG-4230«, die »Pyramid BenHur² 80 X«, die künftig als »Collax Business Server« gehandelt wird, sowie die mit der »Turbocard R55 HFA14« ausgestattete »Siemens 4YourSafety RX300«.

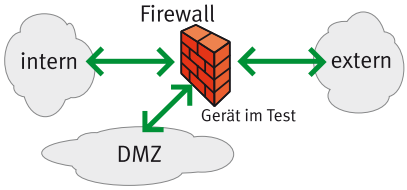
### Firewall-UDP-Durchsatz

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 multidirektional, das heißt alle drei Ports senden und empfangen gleichzeitig mit Wirespeed.

Gemessen werden 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 sechs Flows bei einem Frame-Loss von weniger als einem Prozent. Darüber hinaus bewerten wir hier das Verhalten der Systeme bei Volllast und die Fairness, mit der die verschiedenen Flows behandelt werden.

Gigabit-Ethernet-Wirespeed schaffte Astaros Sun-Fire-V20z in der ersten Messreihe bei der Messung mit den 1518-Byte-Frames. Ver-

Testaufbau Firewall-UDP-Durchsatz



**MEINUNG** SECURITY-APPLIANCES

**Dr. Dirk R. Glogau**

Ein Blick auf die technischen Daten und die Preise der Teststellungen zeigt, dass unser Testfeld recht heterogen ist. Der Grund hierfür liegt darin, dass es zu den Aufgaben der beteiligten Hersteller gehört, nach den Vorgaben unserer Ausschreibung das geeignete Testgerät auszuwählen. Manche Hersteller neigen dazu, hier mit Kanonen auf Spatzen zu schießen. Andere versuchen, um im Bildfeld zu bleiben, mit einer Wasserpistole Elefanten zu jagen. In realen Projekten sind beide Ansätze nicht im Sinne der Kunden. Denn die schiere Leistung überzeugt nicht, wenn der Preis unbezahlbar ist. Günstige Lösungen nützen aber auch nichts, wenn sie zum Flaschenhals werden. Die Auswahl der passenden Lösung sollten IT-Verantwortliche nicht unbedingt den Herstellern überlassen. Denn ob die auch auswählen, was ihr Kunde braucht, oder ob der Kunde unabhängig von den technischen Anforderungen bekommt, was er bereit ist zu bezahlen, ist fraglich.

wendeten wir kleinere Datenpakete, ging auch die Performance langsam zurück. Bei der Messung mit 1024-Byte-Frames schaffte das System immerhin noch eine Bandbreite von rund 933 MBit/s. Halbierten wir dann die Frame-Größe auf 512 Byte, reduzierte sich auch der Durchsatz bei Volllast auf 527 MBit/s. Bei der Messung mit den kleinsten Frames wechselte die Sun-Fire dann quasi ins Fast-Ethernet-Segment. Hier schaffte sie unter Volllast noch gut 65 MBit/s.

Clavister stellte ihre SG-4230 in einer »gedrosselten« Version zur Verfügung. Wie Clavister uns nach dem Test mitteilte, ist bei der SG-4230, der ersten Appliance der 4200-Serie, der Gesamtdurchsatz auf 1 GBit/s beschränkt. Das bedeutet bei dieser Messung einen theoretisch maximalen Durchsatz von 333 MBit/s. Über einen Lizenz-Key bietet Clavister ein Upgrade auf 2 GBit/s an, der das System dann zu einer SG-4250 macht. Die Messungen zeigen dann, dass diese Drosselung hier auch funktioniert. Zwischen 1518 Byte und 512 Byte betrug der Durchsatz auch unter Volllast je Senderichtung maximal 380 MBit/s. Verwendeten wir 64-Byte-Pakete, reduzierte sich der Durchsatz auf rund 80 MBit/s.

Pyramids Benhur²-80-X schaffte unter Volllast und mit dem größten Frame-Format einen Durchsatz von gut 655 MBit/s. Auch hier ging die Leistung dann mit dem Frame-Format zurück. Verwendeten wir 512-Byte-Pakete, schaffte die Benhur noch gut 290 MBit/s. Belasteten wir das System mit den kleinsten Frames, betrug der maximale Durchsatz unter Volllast noch rund 46 MBit/s.

Astaro Sun Fire V20z

Als deutlich leistungsfähiger erwies sich die mit Turbocard ausgestattete 4Yoursafety-RX300 von Siemens. Bei der Messung mit den größten Frames schaffte sie immerhin rund 913 MBit/s. Verkleinerten sich die Frames, stieg ihr Leistungsvermögen im Gegensatz zu den anderen Appliances noch etwas an. So waren bei der Messung mit 1024 Byte-Frames 935 MBit/s und bei der Messung mit 512 Byte-Frames sogar 971 MBit/s möglich. Bei der Messung mit den kleinsten Datenpaketen schaffte die 4Yoursafety-RX300 noch maximal rund 350 MBit/s. Unter Volllast blieben davon noch 290 MBit/s übrig.

## Firewall-UDP-Durchsatz mit zu blockendem Verkehr

In einer zweiten Messreihe haben wir dann den Firewall-UDP-Durchsatz mit zu blockendem Verkehr gemessen. Aufbau und Durchführung der Messung waren dabei wie schon in der ersten Messreihe. Allerdings musste die Firewall zusätzlich den Datenstrom vom externen zum internen Netz zu 100 Prozent blocken, was auch allen Systemen im Testfeld fehlerfrei gelungen ist. Alle anderen Flows sollte das jeweilige System im Test möglichst ungehindert passieren lassen. Gemessen werden wie oben Frame-Loss, Latency und Jitter. Aus den ermittelten Frame-Loss-Werten errechnen sich die Werte für

Clavister SG-4230

den maximalen Durchsatz. Dieser ist der maximal mögliche Durchschnittswert aller Flows mit Ausnahme der zu blockenden bei einem Frame-Loss von kleiner 1 Prozent. Dann haben wir wie oben das Verhalten der Systeme bei Volllast und die Fairness, mit der die verschiedenen Flows behandelt werden, untersucht.

Wie schon bei der ersten Messreihe schaffte auch bei unserer zweiten Messreihe Astaros Sun-Fire-V20z als einziges System im Testfeld Gigabit-Ethernet-Wirespeed. Ohne Einschränkungen gilt das aber nur für die größten verwendeten Frames. Schickten wir 1024 Byte große Frames durch das System, waren es immer noch über 992 MBit/s. Halbierten wir die Paketgröße auf 512 Byte, reduzierte sich der Durchsatz unter Volllast auf gut 577 MBit/s. Klare Schwierigkeiten hatte das Astaro-System dann wieder mit den kleinsten Datenrahmen. Hier war unter Volllast noch ein Durchsatz von rund 79 MBit/s möglich.

Clavisters gedrosselte SG-4230 schaffte in dieser Messreihe Durchsätze bei Volllast zwischen 453 und 461 MBit/s. Mit den kleinsten Frames im Test hatte dann auch die SG-4230 wieder Probleme. Hier konnten wir einen maximalen Durchsatz bei Volllast von gut 85 MBit/s messen.

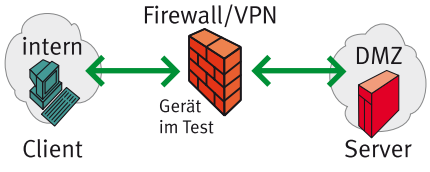
Pyramids Benhur erreichte in dieser Messreihe unter optimalen Bedingungen und bei Verwendung der größten Frames einen Durchsatz von rund 710 MBit/s. Unter Volllast blieben davon noch 638 MBit/s erhalten. Wurden kleinere Frames verwendet, ging auch hier wieder die Leistung zurück. So stand bei der Messung mit 1024-Byte-Paketen noch eine Bandbreite unter Volllast von 561 MBit/s zur Verfügung. Betrug die Frame-Größe 512 Byte, waren noch rund 288 MBit/s je Flow möglich. Die kleinsten Frames im Test reduzierten die Bandbreite dann auf rund 45 MBit/s.

Siemens 4YourSafety-RX300 lag bei allen Messungen mit Ausnahme der mit den kleinsten Frames durchweg bei Volllast-Werten von über 900 MBit/s. Ihren Bestwert erreichte das System bei der Messung mit 512-Byte-Frames. Hier standen 968 MBit/s an Bandbreite je Flow zur Verfügung. Bei der Messung mit 64-Byte-Paketen waren dann noch 297 MBit/s möglich.

## Firewall-TCP-Messungen

In unserer dritten Messreihe haben wir die Connection-Setup-Rate und die Connection-Capacity 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 dieser Performance-Messung baut die Messtechnik Verbindungen durch die Firewall auf und generiert Datenströme. Dabei geht der Hauptdatenstrom vom

Testaufbau Firewall-TCP-Messung



## TECHNISCHE DATEN FIREWALL- UND VPN-SYSTEME

| | Astaro Sun Fire V20z | Clavister SG-4230 | Pyramid BenHur² 80 X (künftig Collax Business Server) | Siemens YourSafety RX300 with Turbocard R55 HFA14 |
|---|---|---|---|---|
| Anzahl unabhängiger (nicht geswitchter) LAN-Ports | | | | |
| Anzahl Gigabit-Ethernet-Ports | 4 | 2 + 8 Mini Gbic | 6 | 5 |
| Anzahl Fast-Ethernet-Ports | | 4 | 0 | 0 |
| Anzahl WAN-Ports | | | | |
| PPPoE auf LAN-Port(s) | 4 | 4 | 6 | 1 |
| X.21 | 0 | 0 | 0 | 0 |
| X.25 | 0 | 0 | 0 | 0 |
| ISDN $S_0$ | 0 | 0 | 0 | 0 |
| ISDN $S_{2M}$ | 0 | 0 | 0 | 0 |
| xDSL | 0 | 4 | 0 | 0 |
| E1 | 0 | 0 | 0 | 0 |
| Sonstige | 0 | 0 | 0 | 0 |
| Hardware/Betriebssystem | | | | |
| Prozessor (Typ), MHz | Dual-Opteron 2,4Ghz | k.A. | Intel P4, 3,6 MHz | Intel Xeon 3,0 GHZ 1MB/800 Mhz |
| Arbeitsspeicher in MByte | 4096 | k.A. | 1024 | 512 (bis zu 4 GB maximal) |
| Betriebssystem Name/Version | Astaro Security Linux V5.2 | Clavister OS v.8.5 | Pynix / BenHur² 2.0.20 | Check Point Secure Platform R55 HFA14 |
| IPv6-Unterstützung für alle Firewall-Funktionen | ○ | ○ | ○ | ● |
| Firewall-Technik | | | | |
| Stateful-Inspection-Firewall | ● | ● | ● | ● |
| Layer-7-Application-Gateway-Proxies | ● | ● | ● | ● |
| anpassbare Proxies | ● | ● | ● | ○ |
| Stateful-Inspection und Proxy kombiniert | ● | ● | ● | ● |
| transparente Firewallfunktionalität konfigurierbar | ● | ● | ○ | ● |
| spezielle Firewall-ASICs integriert | ○ | ○ | ○ | ● |
| Netzwerkprozessor mit Firewall Teilfunktionen 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) | k.A. | 2 | 1 | 8 |
| Cluster über 3-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/S | ● | ○ | ● | ● |
| automatische Synchronisierung im Cluster | ○ | ● | ○ | ● |
| Synchronisierung über multiple Pfade möglich | ○ | ● | ○ | ● |
| Out-Band-Management | ● | ● | ○ | ● |
| Monitoring | | | | |
| CPU überwacht | ● | ● | ● | ● |
| Speicherauslastung gemessen | ● | ● | ● | ● |
| Port-Auslastung gemessen | ● | ● | ○ | ● |
| Synchronisierung überwacht | ● | ● | ○ | ● |
| die Firewall-Software wird überwacht | ● | ● | ○ | ● |
| Schwellenwerte für Auslastung möglich | ○ | ● | ● | ○ |
| Logging-Daten und -Events | | | | |
| per SNMP exportiert | ● | ○ | ○ | ● |
| per WELF-Format exportiert | ○ | ○ | ○ | ○ |
| an Syslog-Server exportieren | ● | ● | ● | ● |
| Events zentralisiert | ● | ● | ● | ● |
| Event-Management korelliert einzelne Einträge | ○ | ● | ● | ● |
| Authentisierung/Autorisierung | | | | |
| NT-Domain | ● | ● | ● | ● |
| TACACS/TACACS+ | ○ | ○ | ○ | ● |
| Radius | ● | ● | ○ | ● |
| LDAP über TLS | ○ | ○ | ● | ● |
| X.509-digitale Zertifkate | ● | ● | ● | ● |
| Token-basierend | ● | ● | ○ | ● |
| Sicherheitsfeatures | | | | |
| DMZ | ● | ● | ● | ● |
| Intrusion-Detection/-Prevention | ● | ● | ○ | ● |
| AAA-Support | ● | ○ | ○ | ● |
| DHCP | ● | ● | ● | ● |
| NAT-Support | ● | ● | ● | ● |
| Content-Filter | ● | ● | ● | ○ |
| Virenscanner | ● | ○ | ● | ○ |
| Listenpreis in Euro für Teststellung* ohne MwSt. | 19 240 | 33 600 | 5980 | 55 500 |
| Website | www.astaro.de | www.clavister.de | www.ben-hur.de | www.4ys.de |

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

*Quelle: Angaben der Hersteller*

Reflector zum Avalanche. Die generierte Last ähnelt insgesamt einer unidirektionalen Smartbits-Messung mit großen UDP-Paketen. Daher ist die Gesamtlast für das System verhältnismäßig gering und die Messergebnisse fallen entsprechend relativ gut aus. Die jeweilige Appliance wird über zwei Ports an die Messtechnik, den Avalanche und Reflector von Spirent, 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 und Servern in der DMZ und protokolliert das Verhalten der Appliance.

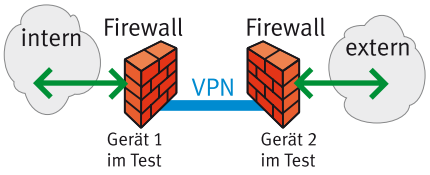
Bei der Messung der Connection-Setup-Rate haben sich keine nennenswerten Unterschiede zwischen den vier Systemen im Test ergeben. Die Appliances von Astaro, Pyramid und Siemens konnten mit 25 000 Connections pro Sekunde punkten. Clavister liegt mit 24 000 Connections pro Sekunde nur knapp dahinter.

In der Disziplin Connection-Capacity unterschieden sich die Systeme dann deutlicher. Astaros Sun-Fire-V20z erreichte mit 1 009 598 Connections den Spitzenwert im Testfeld. Der zweite Platz geht mit 513 293 an die Clavister-SG-4230. Deutlich weniger aber absolut immer noch recht viele Connections schafften Pyramid-Benhur mit 172 031 und Siemens 4YourSafety-RX300 mit 130 897.

### VPN-UDP-Durchsatz

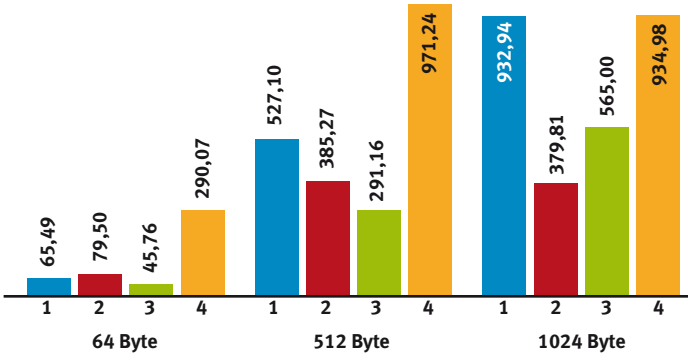
In unserer vierten Messreihe haben wir den VPN-UDP-Durchsatz ermittelt. Hierzu haben wir zwei identische Appliances miteinander verbunden. Dann haben wir den Smartbits-Lastgenerator/Analysator über jeweils einen Port an beide Appliances angeschlossen, so dass wir erneut eine Zangenmessung durchführen konnten. Die Smartbits generierten dann Flows aus UDP-Paketen jeweils mit konstant 64, 512 und 1024

Testaufbau VPN-UDP-Durchsatz

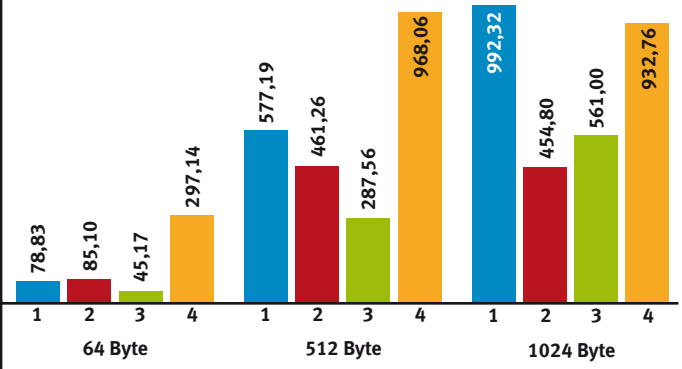



Byte Größe. Die Last beginnt auch hier wieder mit 10 Prozent und wird dann in 10-Prozent-Schritten bis auf 100 Prozent erhöht. Der Aufbau des VPNs erfolgt zwischen den beiden Appliances. Standardmäßig wurde das VPN durch AES-256-Verschlüsselung realisiert. War das Testgerät entgegen unserer Anforderungen dazu nicht in der Lage, haben wir das VPN mit 3DES-Verschlüsselung realisiert, was bei der Teststellung von Siemens erforderlich war. Die Belastung des VPN-Systems erfolgte erst uni- und dann bidirektional, das heißt beide Ports sendeten und

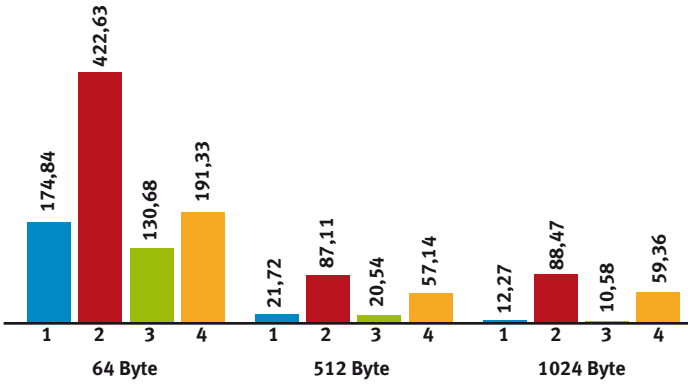
**Messergebnisse Firewall Multi-Groups**
**Datendurchsatz in MBit/s**



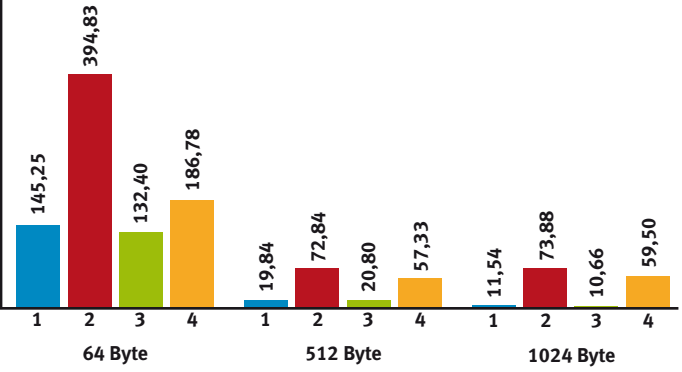

**Messergebnisse Firewall Block**
**Datendurchsatz in MBit/s**




**Preis/Performance-Index in Euro/MBit/s**




**Preis/Performance-Index in Euro/MBit/s**






empfingen gleichzeitig maximal mit Wirespeed.

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. Darüber hinaus bewerten wir hier das Verhalten der Systeme bei Volllast und im bidirektionalen Modus die Fairness, mit der die verschiedenen Flows behandelt werden.

Dass die VPN-Verschlüsselung sehr rechenintensiv ist, zeigt schon ein erster Blick auf die Messergebnisse. Astaros Sun-Fire-V20z schaffte bei der Messung mit den kleinen 64-Byte-Frames unter Volllast einen unidirektionalen Durchsatz von gut 46 MBit/s. Bidirektional waren noch je Flow-Richtung rund 26 MBit/s möglich. Mit größeren Datenpaketen kam die Astaro-Appliance dann etwas besser zurecht. So waren bei der Messung mit 512 Byte unidirektional gut 214 MBit/s möglich, davon blieben im bidirektionalen Modus noch 112 MBit/s übrig. Und auch bei der Messung mit den größten Frames blieb die Sun-Fire weit von Wirespeed entfernt. Hier waren rund 310 MBit/s unidirektional und gut 157 MBit/s bidirektional das Maximum.

Etwas besser kam die Clavister-SG-4230 mit den kleinsten Frames im unidirektionalen Modus zurecht, hier schaffte sie rund 73 MBit/s. Im bidirektionalen Betrieb blieben davon aber nur noch knapp 22 MBit/s bei Volllast übrig. Deutlich besser sah es dann wieder bei den Messungen mit größeren Frames aus. Unidirektional waren mit 512-Byte-Paketen 454 MBit/s und mit 1025 Byte-Paketen 680 MBit/s möglich. Im bidirektionalen Betrieb reduzierten sich diese Werte dann aber um deutlich mehr als 50 Prozent. Bei diesen Messungen schaffte die SG-4230 noch 140 beziehungsweise 212 MBit/s.

Pyramids Benhur ähnelte in seinem Leistungsverhalten bei diesen Messungen dem großen Astaro-System. Bei den Messungen mit den kleinsten Frames waren unter Volllast rund 44 MBit/s unidirektional und gut 23 MBit/s bidirektional möglich. Bei den Messungen mit den

mittelgroßen Datenpaketen realisierte das Pyramid-System 214 MBit/s unidirektional und 114 MBit/s bidirektional. Bei der Messung mit den größten Frames war auch hier noch etwas mehr Durchsatz drin. So schaffte der Kommunikationsserver dann rund 329 MBit/s unidirektional und 175 MBit/s bidirektional.

Auch die mit der Turbocard-R55-HFA14 ausgestattete 4Yoursafety-RX300 von Siemens hatte ihre Probleme mit kleinen Frames. Sie war übrigens das einzige System im Gigabit-Ethernet-Testfeld, das auf 3DES-Verschlüsselung ausweichen musste. Die 4Yoursafety-RX300 schaffte bei unserer Messung mit 64-Byte-Paketen 187 MBit/s unidirektional und nur noch 24 MBit/s im bidirektionalen Betrieb. Verwendeten wir größere Frames, kam das Siemens-Gerät schnell in andere Leistungsregionen. So waren bei unseren Messungen unidirektional wie auch bidirektional Durchsätze unter Vollast von rund 920 MBit/s möglich.

Pyramid BenHur² 80 X – künftig Collax Business Server

Und bei den Messungen mit den größten Frames schaffte die RX300 fast 960 MBit/s – wohlgemerkt im unidirektionalen wie auch im bidirektionalen Betrieb.

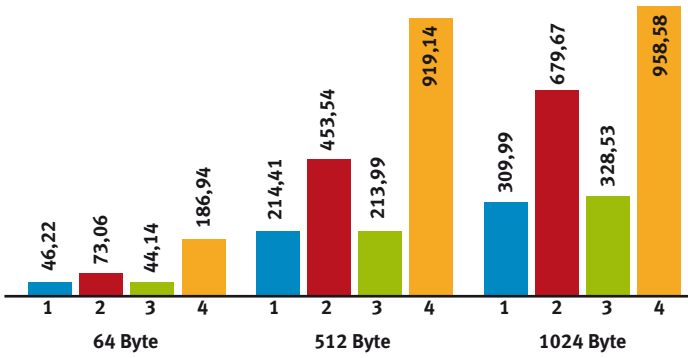
## Fazit

Eine Klasse für sich im Testfeld ist die mit der Turbocard-R55-HFA14 ausgestattete 4Yoursafety-RX300 von Siemens. Dies gilt sowohl im Leistungsvermögen als auch im Preis. Sie zeigt in ihrem Leistungsverhalten eindrucksvoll, dass hohe Durchsätze auch bi- oder multidirektional möglich sind, wenn der Hersteller nicht an Hardware und Rechenpower spart. Deutliche Probleme hatte aber auch dieses Highend-System bei unseren Messungen mit den kleinsten Frames.

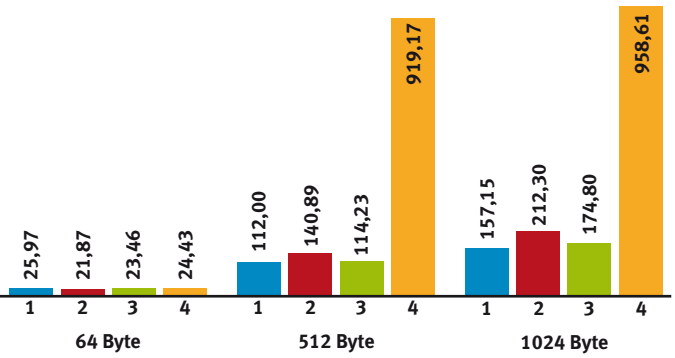
Astaros Sun-Fire-V20z und Clavisters SG-4230 bilden das Mittelfeld im Gigabit-Ethernet-Segment. Beide mochten insbesondere keine kleinen Datenpakete. Dabei war die Clavister-Appliance auf einen Gesamtdurchsatz von 1 GBit/s gedrosselt. Die doppelte Leistung gibt es dann für mehr Geld. Bei unseren Messungen mit kleinen Datenrahmen im Firewall-Betrieb und bei unseren VPN-Durchsatzmessungen blieb die SG-4230 aber auch deutlich unter diesem Gesamtdurchsatz. Wie viel das Upgrade dann noch bringen würde ist Spekulation.

Pyramids im Testfeld letztplatzierte Benhur, die künftig als Collax-Business-Server Karriere machen soll, hat sich in diesem Umfeld trotz allem recht gut geschlagen. Nicht um

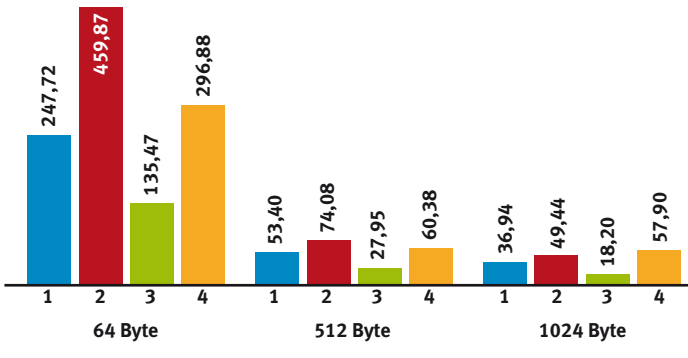
**Messergebnisse VPN unidirektional**
**Datendurchsatz in MBit/s**



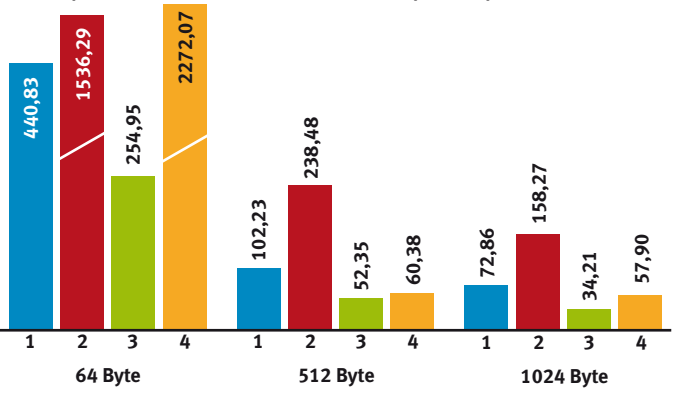

**Messergebnisse VPN bidirektional**
**Datendurchsatz in MBit/s**




**Preis/Performance-Index in Euro/MBit/s**




**Preis/Performance-Index in Euro/MBit/s**




1 Astaro 2 Clavister 3 Pyramid 4 Siemens

## 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 teuere 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 begleiten konnten.
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 und beeinträchtigten unsere Messergebnisse nicht. Mit Hilfe von drei Linux-Intel-PCs in den einzelnen Netzsegmenten unseres Testaufbaus haben wir die korrekte Firewall-Konfiguration und -Funktion jeweils vor den einzelnen Testläufen überprüft.

Klassen vom Mittelfeld entfernt, bietet Benhur ein konkurrenzlos günstiges Preis-Leistungsverhältnis und viel Funktionalität, deren Beurteilung nicht zur Aufgabenstellung dieses Tests gehörte.

Das noch recht moderate Abschneiden der meisten Gigabit-Ethernet-Appliances in unserer Report-Card sollte aber generell nicht darüber hinweg täuschen, dass alle Systeme mehr oder weniger stark ausgeprägt ihr Ziel verfehlten. Auch wenn alle Testgeräte viele Connections aufbauen und halten können nutzt das nicht viel, wenn sie die anvisierten Bandbreiten nicht durchgängig für alle Frame-Formate bieten können. Früher oder später wird jede Security-Appliance zum Flaschenhals. Spätestens wenn es gilt, im Firewall- oder VPN-Betrieb viele kleine Frames unter hoher Last bi- oder gar multidirektional zu verarbeiten, ist die theoretische Wirespeed und somit der Anspruch der Hersteller, Security-Appliances als transparente aktive Netzwerkkomponenten einzubinden, meist um Lichtjahre entfernt.

Generell gilt, dass die Security-Appliances umso stärker schwächelten, um so mehr Rechenarbeit sie leisten mussten. UDP-Ströme aus 64-Byte-Frames überforderten praktisch alle Systeme sowohl im Firewall- als auch im VPN-Betrieb. Aber auch größere Pakete wurden bei weitem nicht immer in Wirespeed verarbeitet. Häufig reduziert sich der Durchsatz pro Flow dann noch mal deutlich, wenn die Systeme vom unidirektionalen auf bi- oder multidirektionalen Betrieb umschalten. Hier rächt sich, dass die einzelnen Flows sich gemeinsame Ressourcen teilen müssen. Mehr Durchsatzleistung ist nur möglich, wenn die Hersteller den Geräten eine aufwändigere Hardware spendieren.

Zur verbreiteten Performance-Schwäche kommt hinzu, dass Priorisierungsmechanismen in aktuellen Security-Appliances wenn überhaupt nur sehr rudimentär implementiert sind. Das macht den Einsatz in modernen Netzwerken, die Daten, Voice-over-IP und Video-over-IP zugleich transportieren sollen, problematisch. Schafft eine Security-Appliance keine Wirespeed und unterstützt sie auch die Priorisierungsmechanismen nicht ausreichend, dann ist die Integration der IP-Telefonie nicht machbar. Manche IT-Verantwortliche leiten daher die Sprachanwendungen um die Security-Systeme herum und riskieren so ein neues, unkalkulierbares Sicherheitsloch.

Der Grund für die schlechte Performance aktueller Security-Appliances liegt darin, dass die Hersteller viel Funktionalität letztendlich in Software abbilden und die zu Grunde liegende Hardware dann häufig schlicht überlastet ist. So lange die Hersteller ihre Systeme nicht wirklich leistungsstark auslegen, ist es für einen reibungslosen Netzwerkbetrieb unerlässlich, dafür zu sorgen, dass die Systeme gar nicht erst an ihre Grenzen gelangen. Dies setzt die genaue Kenntnis der Leistungsfähigkeit der eingesetzten Systeme und der Lasten im Netz voraus. Nur dann ist ein intelligentes Bandbreitenmanagement möglich, das hilft, Performance-Probleme und somit Störungen im Netz zu vermeiden. Voraussetzung dafür ist aber, dass die Systeme auch ein entsprechendes Bandbreitenmanagement unterstützen. Dieser Frage werden wir in unseren Labs weiter nachgehen.

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