Im Flaschenhals hängen geblieben

Vergleichstest Security-Appliances – Firewall und VPN bilden häufig den Flaschenhals in modernen Netzen. Dies hat ein Vergleichstest der Real-World Labs von Network Computing ergeben.

Noch nie war sie so wichtig wie heute, die IT-Sicherheit. Und dafür, dass Unternehmen auch 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 werden 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 steht im vorliegenden Artikel. Die Ergebnisse der Gigabit-Ethernet-Tests folgen dann in den kommenden Ausgaben von Network Computing.

Das erste Testfeld bildeten Astaros »Security Gateway 220«, »Clavister SG-3150«, »bintec VPN Access 250« von Funkwerk, der »gateProtect Firewall Server v. 4.2.1«, Lucents »VPN Firewall Brick 150«, »SecureGUARD for Microsoft ISA Server 2004 ISA110« von OSST, Rimapps »RoadBLOCK CF401U«, Telcotechs »LiSS II secure gateway pro« und die »ZyWALL 5« von Zycel.

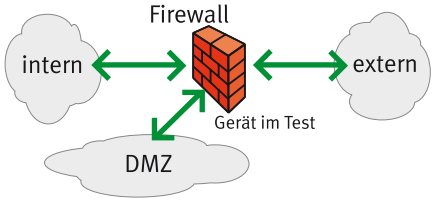
Firewall-UDP-Durchsatz

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.

Astaros Security-Gateway-220 erreichte einen maximalen Durchsatz von 67 MBit/s bei der Messung mit den 1518 Byte großen Frames. Waren die Pakete kleiner, ging die Performance weiter zurück. So schaffte das System bei der Messung mit 1024-Byte-Paketen noch 64 und bei 512-Byte-Paketen noch 57 MBit/s. Verwendeten wir die kleinsten 64-Byte-Pakete, dann brach die Durchsatzleistung des Astaro-Systems deutlich

Testaufbau Firewall-UDP-Durchsatz



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

ein, hier war noch ein maximaler Durchsatz von gerade mal 8 MBit/s möglich. Unter Volllast mit 64-Byte-Paketen machte die Security-Gateway-220 dann praktisch völlig »dicht«, 99,99 Prozent aller Daten gingen verloren. Mit den größeren Frames kam die Astaro-Appliance dann auch unter Volllast besser zurecht. So waren bei der Messung mit den größten Frames rund 60 MBit/s drin. Dabei hat das Gerät aber nicht alle Flows gleich behandelt. So schwankte der Frame-Loss bei der Messung mit 1518-Byte-Paketen beispielsweise zwischen rund 47 und gut 33 Prozent.

Clavisters SG-3150 schaffte immerhin bei den Messungen mit den großen Frames Wirespeed. Verwendeten wir 512-Byte-Pakete waren noch 88 MBit/s drin. Mit den 64-Byte-Paketen hatte dann auch das Clavister-System seine Probleme. Hier war noch ein UDP-Durchsatz von 32 MBit/s möglich. Unter Volllast ging der 512-Byte-Durchsatz dann auf rund 78 MBit/s zurück. Verwendeten wir die kleinsten Datenpakete, schaffte die SG-3150 noch maximal gut 18 MBit/s. Dabei ging es auch nicht allzu fair zu, so schwankte der Frame-Loss bei der Messung mit den 512-Byte-Paketen zwischen gut 11 und über 32 Prozent.

Funkwerks Bintec-VPN-Access-250 schaffte mit Ausnahme der Messung mit 64-Byte-Paketen durchgehend Wirespeed. Verwendeten wir die kleinsten Pakete, waren noch rund 37 MBit/s möglich. Und die standen auch unter Volllast noch zur Verfügung. Dabei behandelte die Bintec-Firewall die verschiedenen Flows sehr fair.

Telcotech LiSS II secure gateway pro

Gleichfalls Wirespeed erreichte auch der Gateprotect-Firewall-Server. Allerdings nur bei den Messungen mit 1518- und mit 1024-Byte-Frames. Bei der Messung mit 512-Byte-Paketen waren noch maximal fast 85 MBit/s möglich. Verwendeten wir dann wieder die kleinsten Datenrahmen, ging der maximal erreichbare Durchsatz auf 17 MBit/s zurück. Von diesen blieb unter Volllast aber nur noch gut 1 MBit/s übrig und auch die übrigen Durchsätze reduzierten sich unter Volllast. Unabhängig von den erreichbaren Durchsatzwerten behandelte der Gateprotect-Firewall-Server alle Flows recht fair.

Lucents VPN-Firewall-Brick-150 ähnelt hier in ihrem Leistungsverhalten dem Gateprotect-System. Wirespeed lag bei den Messungen mit 1518- und 1024-Byte-Paketen an. Mit kleineren Frames hatte auch die Brick-150 ihre Probleme. So waren bei der Messung mit 512-Byte-Paketen noch 93 MBit/s möglich. Waren die Frames nur 64 Byte groß, ging der maximal zu erreichende Durchsatz auf 27 MBit/s zurück. Unter Volllast mit 64-Byte-Paketen machte die Lucent-Appliance dann aber komplett dicht. Gerade mal 0,01 MBit/s Durchsatz waren noch messbar. Verwendeten wir 512-Byte-Pakete, schaffte die Brick-150 immerhin unter Volllast noch gut 88 MBit/s. Allerdings behandelte das Lucent-System die einzelnen Flows hierbei nicht allzu fair. Hier schwankte der Frame-Loss immerhin zwischen gut acht und fast 15 Prozent.

Gleichfalls Wirespeed schaffte der Secureguard-for-Microsoft-ISA-Server-2004 von OSST bei den Messungen mit den größten Frames. Mit kleineren Frames hatte dann auch das System von OSST deutliche Probleme. So betrug der maximal erreichbare Durchsatz bei der Messung mit 64-Byte-Paketen dann noch rund 8 MBit/s, die dann aber auch unter Volllast noch zur Verfügung standen. Unter Volllast zeigten sich schon bei der Messung mit 1024-Byte-Paketen deutliche Probleme. Der erzielbare Durchsatz belief sich im Durchschnitt auf rund 67 MBit/s pro Flow. Allerdings schwankten die Durchsätze zwischen den einzelnen Flows sehr stark. So betrug der Frame-Loss zwischen gut 4 und über 99 Prozent bei ein und der selben Messung.

Als deutlich standfester erwies sich die Roadblock-CF401U von Rimapp. Zwischen 1518 und 512 Byte stand durchgehend und auch

REPORTCARD FIREWALL- UND VPN-PERFORMANCE

interaktiv unter www.networkcomputing.de

	Gewichtung	Telcotech LiSS II secure gateway pro	Rimapp RoadBLOCK CF401U	Lucent VPN Firewall Brick 150	Gateprotect gateProtect Firewall Server v. 4.2.1	Funkwerk bintec VPN Access 250	Clavister SG-3150	Astaro Security Gateway 220	OSST SecureGUARD for Microsoft ISA Server 2004 ISA110	Zycel ZyWALL 5
Max. FW-Durchsatz 64 Byte	8,33	1	1	1	1	2	1	1	1	1
Max. FW-Durchsatz 512 Byte	8,33	5	5	5	4	5	4	2	1	1
Max. FW Durchsatz 1024 Byte	8,33	5	5	5	5	5	5	3	4	1
Max. FW-Durchsatz 64 Byte (Block)	8,33	1	1	1	1	2	1	1	1	1
Max. FW-Durchsatz 512 Byte (Block)	8,33	5	5	5	4	5	5	3	1	1
Max. FW-Durchsatz 1024 Byte (Block)	8,33	5	5	5	5	5	5	4	2	1
Max. VPN-Durchsatz 64 Byte unidirekt.	8,33	1	1	2	1	1	1	1	1	1
Max. VPN-Durchsatz 512 Byte unidirekt.	8,33	5	5	5	5	4	4	4	1	1
Max. VPN-Durchsatz 1024 Byte unidirek.	8,33	5	5	5	5	4	5	5	2	1
Max. VPN-Durchsatz 64 Byte bidirekt.	8,33	1	1	1	1	1	1	1	1	1
Max. VPN-Durchsatz 512 Byte bidirek.	8,33	4	2	2	2	2	2	1	1	1
Max. VPN-Durchsatz 1024 Byte bidirekt.	8,33	5	5	3	5	2	3	3	1	1
Gesamtergebnis	**100,00**	**3,58**	**3,42**	**3,33**	**3,25**	**3,17**	**3,08**	**2,42**	**1,42**	**1,00**
		B -	**C +**	**C +**	**C +**	**C**	**C**	**D**	**E**	**E**

A › 4,3; B › 3,5; C › 2.5; D › 1,5; E ‹ 1,5;
Die Bewertungen A bis C enthalten in ihren Bereichen + oder -;

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

gateProtect
Firewall Server v. 4.2.1

unter Volllast Wirespeed zur Verfügung. Bei der Messung mit den kleinsten Paketen ging der maximal erzielbare Durchsatz dann auf rund 25 MBit/s je Flow zurück. Unter Volllast blieben davon noch rund 15 Prozent übrig. Allerdings hat auch die Rimapp-Firewall die Flows nicht allzu fair behandelt. So schwankte der Frame-Loss bei der 64-Byte-Messung zwischen rund 70 und 98 Prozent.

Wie schon die Rimapp-Firewall hat auch Telcotechs Liss-II-Secure-Gateway-pro von 1518 bis zur Messung mit 512-Byte-Paketen durchgehend 100 MBit/s für alle Flows zur Verfügung gestellt. Bei der Messung mit 64-Byte-Frames ging der maximal erzielbare Durchsatz dann auf 13 MBit/s zurück. Unter Volllast blieben davon dann noch 0,01 MBit/s übrig.

Zycels Zywall 5 zeigte dagegen schon früh Probleme. So schaffte das System bei der Messung mit den größten Frames gerade mal 27 MBit/s. Mit abnehmenden Frame-Größen ging dann auch der erzielbare Maximaldurchsatz weiter zurück. So lagen bei der Messung mit 512-Byte Paketen noch 9 MBit/s an. Betrug das Frame-Format 64 Byte, waren gerade noch rund 1 MBit/s zu messen. Unter Volllast war das Zycel-System dann schnell überfordert. Hier lagen die Durchsatzwerte noch je nach Frame-Größe zwischen gut 23 und rund 0,6 MBit/s. Und auch mit der Fairness hat es die Zywall 5 nicht allzu genau genommen. So schwankte der Frame-Loss der einzelnen Flows bei der Messung mit den größten Datenrahmen zwischen rund 65 und über 83 Prozent.

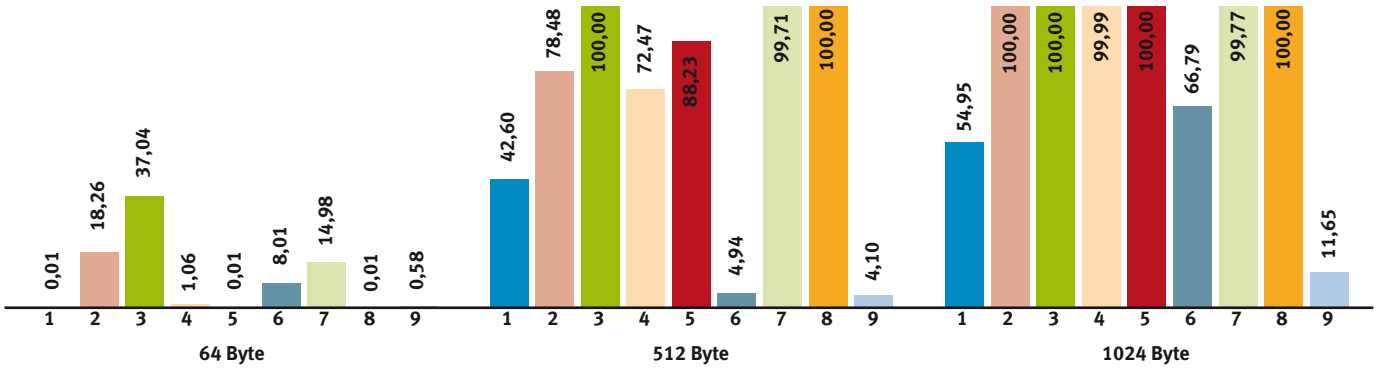
Firewall-UDP-Durchsatz mit zu blockendem Verkehr

In einer zweiten Messreihe haben wir dann 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 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.

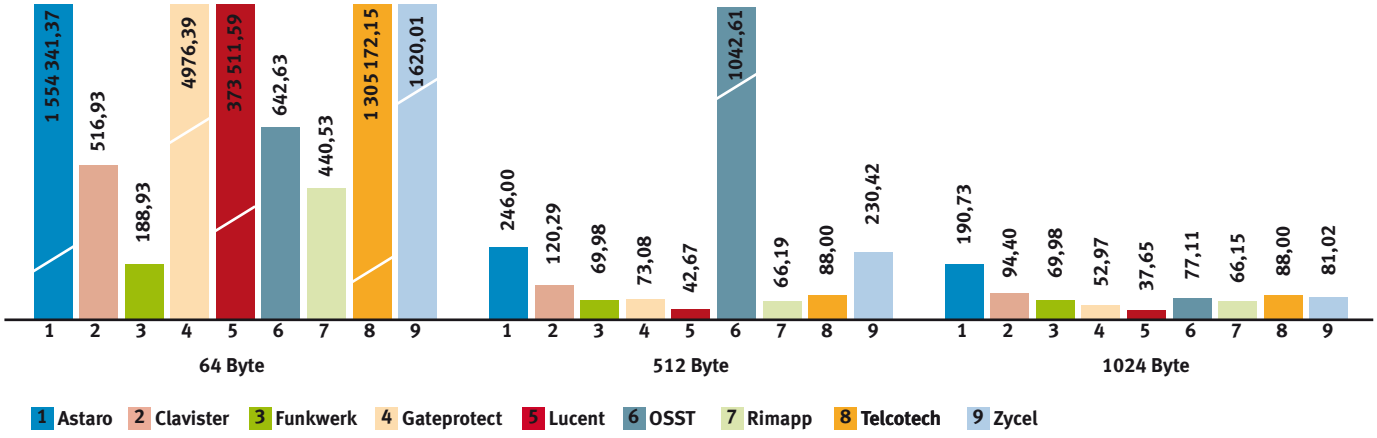
Astaros Security-Gateway-220 zeigte ein ähnliches Verhalten wie in der ersten Messreihe. Die maximal erzielbaren Durchsatzraten lagen hier zwischen 76 MBit/s bei den größten Frames und 8 MBit/s bei den kleinsten Frames. Unter Volllast lagen die Leistungswerte dann noch etwas tiefer. So betrug die Durchsatzrate schon bei der Messung mit den 1518-Byte-Frames nur rund 59 MBit/s. Verwendeten wir kleinere Frames, ging der Durchsatz weiter zurück. Bei der Messung mit Volllast und 64-Byte-Paketen lagen dann nur noch 0,01 MBit/s an. Dabei schwankten die Verlustraten zwischen den einzelnen Flows recht stark. So bewegt sich der Wert für den Frame-Loss bei der Messung mit den größten Frames zwischen gut 40 und 0 Prozent.

Clavisters SG-3150 schaffte bei den Messungen mit 1518- und mit 1024-Byte-Frames erneut Wirespeed. Betrug das Frame-Format 512 Byte, standen noch rund 96 MBit/s je Flow zur Verfügung. Bei der Messung mit den kleinsten Frames ging der maximale Durchsatz dann auf 33 MBit/s zurück. Unter Volllast blieben hiervon dann noch rund 20 MBit/s übrig. Dabei behan-

Messergebnisse Firewall Multi-Groups (Datendurchsatz in MBit/s)



Messergebnisse Firewall Multi-Groups (Preis/Performance-Index in Euro/MBit/s)



delte das System nicht alle Flows gleich fair. Die Werte für den Frame-Loss schwankten hier immerhin zwischen rund 72 und 85 Prozent. Unter Volllast schaffte die SG-3150 dann bei der Messung mit 512-Byte-Paketen noch einen Durchsatz von fast 92 Prozent je Flow. Zwischen den einzelnen Flows schwankten die Verlustraten dann aber auch wieder zwischen gut 19 und 0 Prozent.

Mit Ausnahme der Messung mit den kleinsten Frames bot die Bintec-VPN-Access-250 hier durchgehend Wirespeed. Verwendeten wir 64-Byte-Frames, stand noch eine Bandbreite von rund 40 MBit/s je Flow zur Verfügung, die sich auch durch Volllast nicht weiter verringen ließ. Das ist zwar auch noch weit von der theoretisch möglichen Wirespeed entfernt. Im Vergleich ist das aber mit Abstand der beste 64-Byte-Durchsatz im Testfeld, der darüber hinaus auch sehr fair auf alle Flows verteilt ist.

Wirespeed stellte auch Gateprotects Firewall-Server bei den Messungen mit 1518- und 1024-Byte-Paketen zur Verfügung. Waren die Frames 512 Byte groß, betrug die maximale Bandbreite je Flow noch 73 MBit/s. Unter Volllast blieben davon noch rund 68 MBit/s erhalten. Und bei der Messung mit den kleinsten Frames stand noch eine Bandbreite von 13 MBit/s zur Verfügung. Unter Volllast blieb davon dann noch knapp 1 MBit/s übrig. Insgesamt hat der Firewall-Server die Flows sehr fair behandelt und die Datenverluste gleichmäßig auf alle Flows verteilt.

Bis auf die Messung mit den kleinsten Frames stellte Lucents Brick-150 in dieser Disziplin Wirespeed zur Verfügung. Betrug das Frame-Format 64 Byte, dann war noch ein Maximaldurchsatz von 24 MBit/s möglich. Bei Volllast machte die Lucent-Firewall bei der Messung mit 64-Byte-Frames dann allerdings ganz dicht. Waren die Frames größer, konnten wir der Brick-150 in dieser Messreihe keine weiteren Schwächen nachweisen.

Deutliche Probleme hatte dagegen die OSST-Firewall. Schaffte sie in der ersten Messreihe noch bei den großen Frame-Formaten Wirespeed, so waren hier maximal 69 MBit/s bei 1518 Byte drin. Bei den kleinsten Frames schaffte die OSST-Box dann noch rund 8 MBit/s, die aber auch bei Volllast noch zur Verfügung standen. Unter Volllast schwankten die Durchsatzraten dann je nach Frame-Größe zwischen rund 80 und 8 MBit/s. Dabei verteilten sich die Datenverluste recht unfair zwischen den einzelnen Flows. So schwankten die Verlustraten bei der Messung mit den größten Frames zwischen rund 64 und 0 Prozent.

Rimapps Roadblock-CF401U überzeugte dagegen mit den gleichen Maximalwerten, die wir auch in der ersten Messreihe ermittelt hatten. Bei den kleinsten Frames waren maximal 25 MBit/s drin. Ansonsten lag durchgehend Wirespeed an.

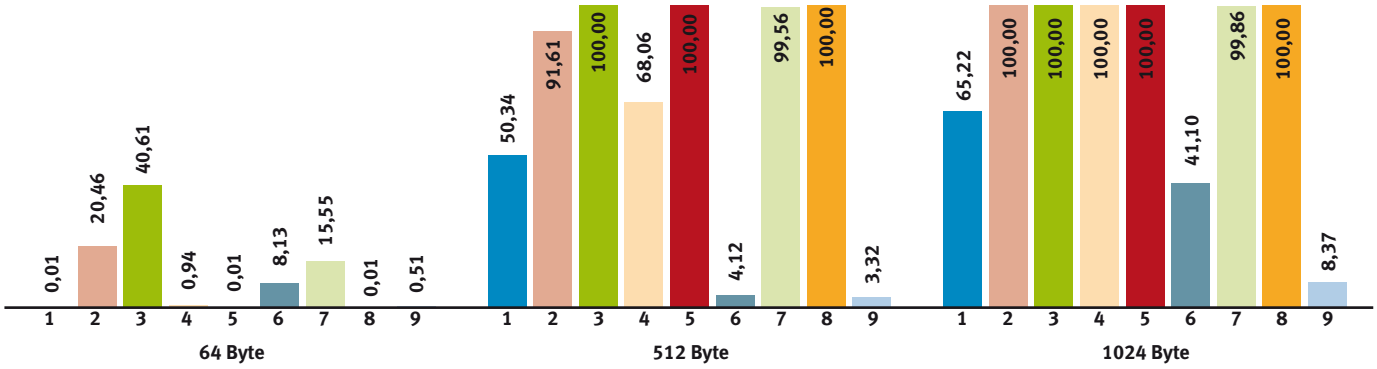
Unter Volllast mit 64-Byte-Paketen schaffte das System dann noch fast 16 MBit/s. Allerdings ließ hier dann auch die Fairness zu Wünschen übrig. So schwankten die Datenverluste zwischen den einzelnen Flows bei letztgenannter Messung zwischen 69 und fast 99 Prozent.

Telcotechs Liss-II bot mit Ausnahme der Messung mit den kleinsten Frames durchgehend Wirespeed. Betrug das Frame-Format 64 Byte, schaffte das System noch einen maximalen Durchsatz von 13 MBit/s, von dem unter Volllast nur noch 0,01 MBit/s übrig bleibt. Abgesehen von dieser deutlichen 64-Byte-Schwäche arbeitete die Liss-II hier völlig unauffällig und korrekt.

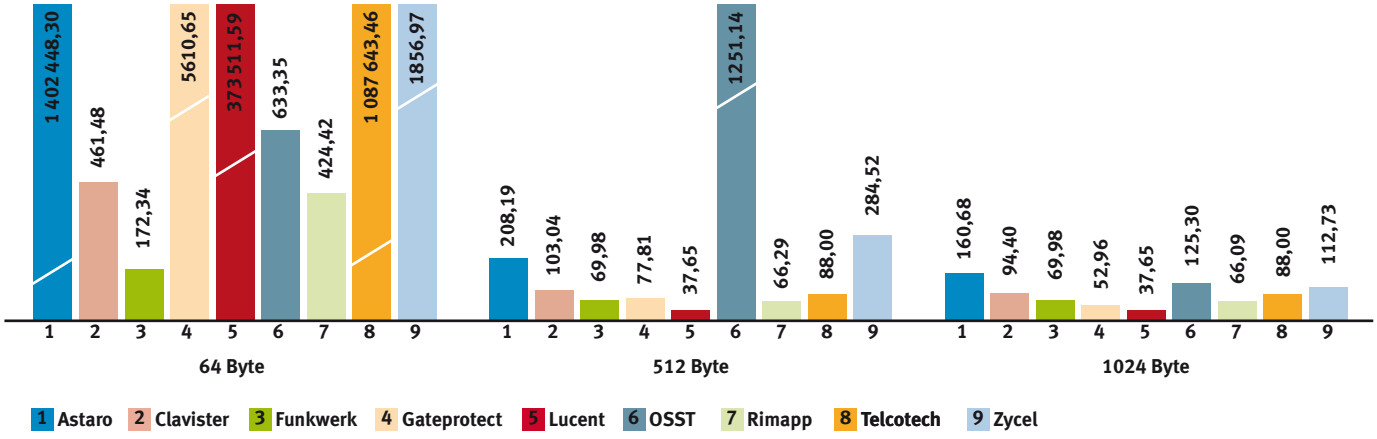
Funkwerk bintec
VPN Access 250

Zycels Zywall 5 zeigte sich auch in dieser zweiten Messreihe als überfordert. Betrug die Frame-Größe 1518 Byte, schaffte das System eine maximale Bandbreite von 25 MBit/s je Flow. Mit abnehmender Frame-Größe wurden die möglichen Bandbreiten dann immer geringer. Bei der Messung mit 64-Byte-Frames betrug der maximale

Messergebnisse Firewall Block (Datendurchsatz in MBit/s)



Messergebnisse Firewall Block (Preis/Performance-Index in Euro/MBit/s)



Clavister SG-3150

Durchsatz noch rund 1 MBit/s. Unter Volllast verschlechterten sich die Performance-Werte dann auch für die größeren Frame-Formate noch. So betrug der Durchsatz bei der Messung mit den größten Frames noch gut 9,3 MBit/s je Flow. Dabei schwankten die Werte für die einzelnen Flows auch noch, so betrug der Frame-Loss je Flow bei der letztgenannten Messung zwischen gut 84 und über 92 Prozent.

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 Performance-Messung baut die Messtechnik Verbindungen durch die Firewall auf und generiert Datenströme. Dabei geht der Hauptdatenstrom vom Reflector zum Avalanche. Die generierte Last ähnelt insgesamt einer unidirektionalen Smartbits-Messung mit großen UDP-Paketen. Daher sind die Messergebnisse relativ gut. Die jeweilige Appliance wird über zwei Ports 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 und Servern in der DMZ und protokolliert das Verhalten der Appliance.

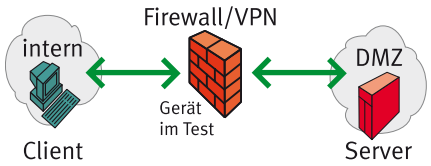
Astaros Security-Gateway-220 erreichte eine Connection-Setup-Rate von 8000 und eine Connection-Capacity von 432 369. Die gemessenen Durchsatzwerte lagen zwischen 96,3 MBit/s bei den 1518 Byte großen und 93,68 MBit/s bei den 512 Byte großen Frames.

Clavisters SG-3150 vermochte sogar 15 000 Sessions pro Sekunde aufzubauen. Mit einer Connection-Capacity von 126 210 liegt sie zwar deutlich unter dem Astaro-System, bietet aber absolut immer noch eine hohe Zahl an möglichen Verbindungen. Der maximal erreichbare Durchsatz liegt zwischen 96,23 und 93,67 MBit/s und erreicht somit fast die gleichen Werte wie Astaro.

Die Bintec-VPN-Access-250 schaffte eine Connection-Setup-Rate von 5000. Die Connection-Capacity des Funkwerk-Systems lag bei vergleichsweise geringen 16 734 Verbindungen. In der Durchsatzmessung vermochte die Bintec-Appliance mit Astaro und Clavister gleichzuziehen. Sie kam hier auf Werte zwischen 96,35 und 93,7 MBit/s.

Der Firewall-Server von Gateprotect erreichte eine Connection-Setup-Rate von 8000 und konnte so mit Astaro mithalten. Die maximale

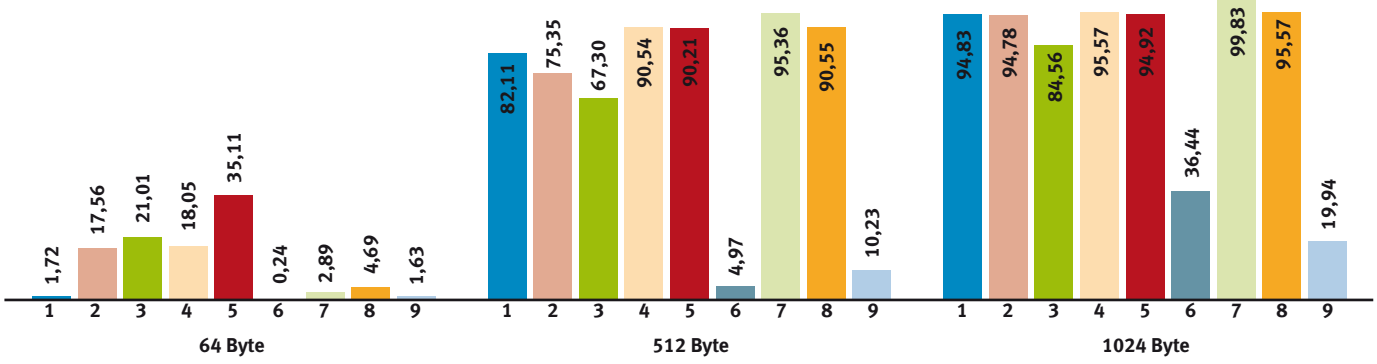
Testaufbau Firewall-TCP-Messung



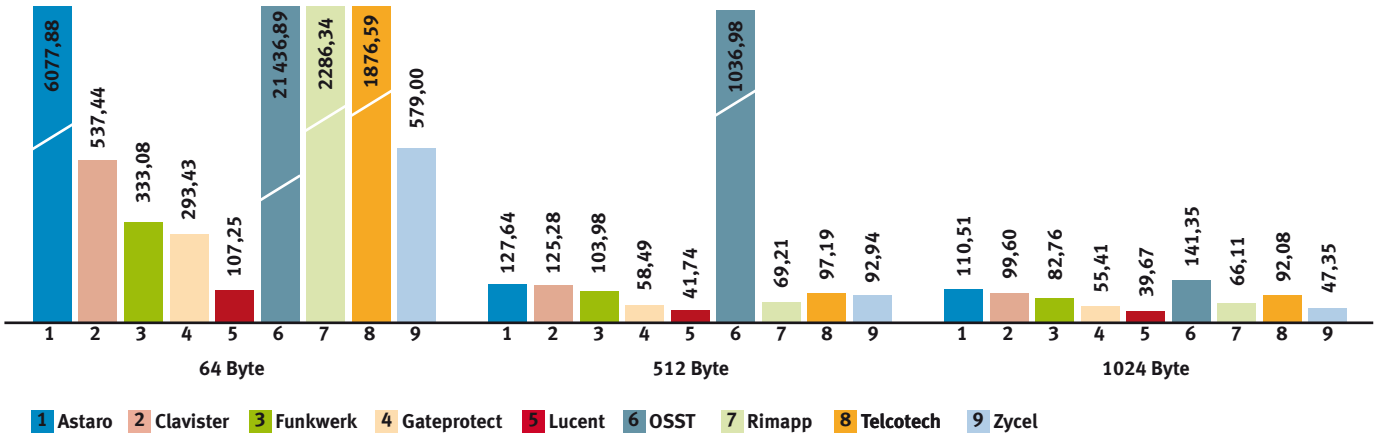
Connection-Capacity lag dagegen bei »nur« 64 416. In der Disziplin Durchsatz herrscht dagegen Gleichstand. Das Gateprotect-System schaffte je nach Frame-Format zwischen 96,36 und 93,67 MBit/s.

Lucents Brick-150 vermochte 10 000 Connections pro Sekunde aufzubauen und maximal 195 709 Verbindungen gleichzeitig zu halten. Im Durchsatz konnte das Lucent-System mit dem übrigen Mitbewerb mithalten. Die Brick erreichte

Messergebnisse VPN unidirektional (Datendurchsatz in MBit/s)



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



Astaro Security Gateway 220

hier Bandbreiten zwischen 96,3 und 93 MBit/s. Mit einer Connection-Setup-Rate von 3000 fällt OSST hinter dem Feld zurück. Die Connection-Capacity lag dagegen bei 236 270 Verbindungen, also noch über der Leistung des Lucent-Systems. Im Durchsatz konnte das OSST-System dagegen mit dem Feld mithalten; es schaffte Werte zwischen 96,26 und 93,6 MBit/s.

Rimapps Roadblock-CF401U liegt mit einer Connection-Setup-Rate von 9000 im Mittelfeld. Die Connection-Capacity von 627 778 Verbindungen ist dagegen der höchste Messwert in dieser Disziplin in unserem Testfeld. Und auch beim Durchsatz vermochte Rimapp dem Feld zu folgen. Das Rimapp-System erreichte Durchsatzwerte zwischen 95,87 und 93,2 MBit/s.

Telcotechs Liss-II erreichte mit einer Connection-Setup-Rate von 11 000 einen guten zweiten Platz im Testfeld. Mit einer Connection-Capacity von 130 912 liegt sie dagegen hinter dem Testfeld. In der Durchsatzmessung konnte die Liss-II dagegen mit dem Feld mithalten. Sie schaffte Werte zwischen 96,3 und 93,68 MBit/s.

Dass Zycels Zywall 5 gegenüber dem Testfeld zurück fällt, zeigen auch die TCP-Messwerte. Die Zywall erreichte eine Connection-Setup-Rate von 500 Sessions pro Sekunde und eine Connection-Capacity von 5999. Bei den Durchsatzmessungen blieb das System als einziges im Testfeld deutlich unter 90 MBit/s. Die Werte schwanken zwischen 49,47 und 21,43 MBit/s.

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 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 den Teststellungen von OSST und Rimapp erforderlich war. Die Belastung des VPN-Systems erfolgte erst uni- und dann bidirektional, das heißt beide Ports sendeten und empfingen gleichzeitig maximal mit Wirespeed.

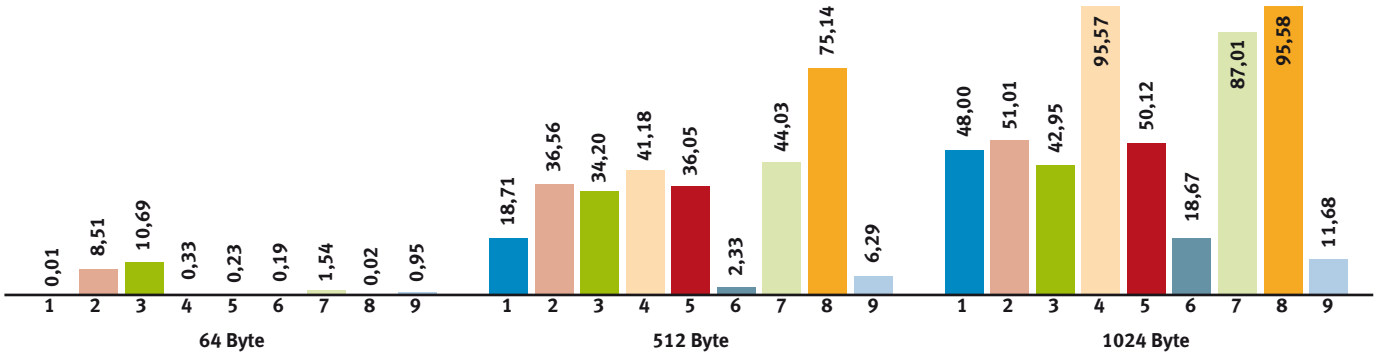
Gemessen haben wir wieder Frame-Loss, Latency und Jitter. Aus den ermittelten Frame-Loss-Werten errechnen sich die Werte für den maximalen Durchsatz. Dieser ist der maximal mögliche Durchschnittswert aller Flows bei einem Frame-Loss von kleiner 1 Prozent. Darüber hinaus bewerten wir hier das Verhalten der Systeme bei Volllast und im bidirektionalen Modus

Zycel ZyWALL 5

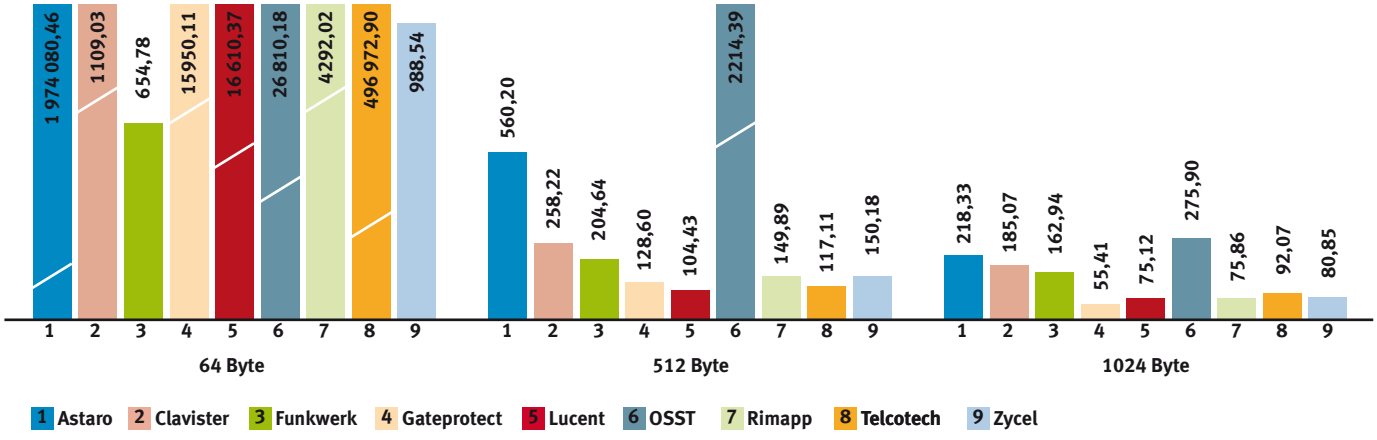
die Fairness, mit der die verschiedenen Flows behandelt werden.

Mit 95 MBit/s verfehlt Astaros Security-Gateway-220 bei der unidirektionalen Messung mit 1024-Byte-Paketen nur knapp die Wirespeed. Bei der Messung mit 512 Byte großen Paketen schaffte das System dann noch 85 MBit/s. Schwierigkeiten hatte das Astaro-System dann wieder mit

Messergebnisse VPN bidirektional (Datendurchsatz in MBit/s)



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



TECHNISCHE DATEN FIREWALL- UND VPN-SYSTEME

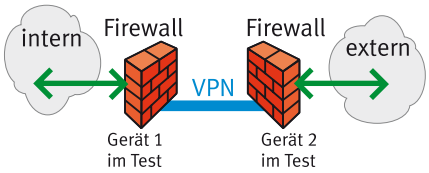
	Astaro Security Gateway 220	Clavister SG-3150	Funkwerk bintec VPN Access 250	Gateprotect gateProtect Firewall Server v. 4.2.1	Lucent VPN Firewall Brick 150	OSST SecureGUARD for Microsoft ISA Server 2004 ISA110	Rimapp RoadBLOCK CF401U	Telcotech LiSS II secure gateway pro	Zycel ZyWALL 5
Anzahl unabhängiger (nicht geswitchter) LAN-Ports									
Anzahl Gigabit-Ethernet-Ports	0	0	0	0	0	0	2	0	0
Anzahl Fast-Ethernet-Ports	8	6	3	5	4	3	2	6	4
Anzahl WAN-Ports									
X.21	0	0	0	0	0	0	k.A.	0	0
X.25	0	0	0	0	0	0	k.A.	0	0
ISDN S0	0	0	1	0	0	0	k.A.	0	0
ISDN S2M	0	0	0	0	0	0	k.A.	0	0
xDSL	0	6	0	0	0	0	k.A.	0	0
E1	0	0	0	0	0	0	k.A.	0	0
Hardware/Betriebssystem									
Prozessor (Typ), MHz	Intel P 3, 1,2 Ghz	k.A.	IBM PCC 750 FX, 733MHz	Intel P4 2,8GHz	Celeron 650MHz	Intel P4, 2 GHz	Intel P 4, 3.4MHz	Intel P 4, 3,06 GHz	Intel, 266MHz
Arbeitsspeicher in MByte	512	k.A.	64	1024	128	512 MN	2048	512	32
Betriebssystem Name/Version	Astaro Security Linux V5.2	Clavister OS v.8.5	BOSS	Linux 2.4.29	Inferno OS	Windows 2003 SP1	Win 2003 Server Appl. Edition	gehärtetes Linux/L52X0-v2.14.6	ZyNOS v3.64
IPv6-Unterstützung für alle Firewall-Funktionen	○	k.A.	○	○	○	k.A.	●	○	○
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	○	○	○	○	○	○	k.A.	○	○
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	k.A.	0	2	32	32	16	1
Cluster über 3-Party-Software etabliert	○	○	○	○	○	●	●	○	○
Cluster über externen Load-Balancer-Switch	●	○	●	○	○	●	●	●	●
Cluster über Netzwerk-Links etabliert	○	●	k.A.	○	●	k.A.	k.A.	○	○
Management									
Telnet	○	○	●	○	○	●	●	○	●
rollenbasierte Verwaltung	○	●	●	●	●	●	●	●	○
Auditing-fähig	●	●	●	○	●	●	●	●	○
SSH-Support für CLI	●	○	●	●	○	○	○	○	●
HTTP/S	●	○	●/○	○	○	●	●	●	●
automatische Synchronisierung im Cluster	○	●	○	○	●	●	●	○	○
Synchronisierung über multiple Pfade möglich	○	●	○	○	●	●	●	○	○
Out-Band-Management	●	●	●	○	○	○	○	●	●
Monitoring									
CPU überwacht	●	●	●	○	●	●	●	●	●
Speicherauslastung gemessen	●	●	●	●	●	●	●	●	●
Port-Auslastung gemessen	●	●	●	●	●	●	●	○	○
Synchronisierung überwacht	●	●	○	○	●	●	●	●	○
die Firewall-Software wird überwacht	●	●	k.A.	●	●	●	●	●	○
Schwellenwerte für Auslastung möglich	○	●	●	○	●	●	●	○	○
Logging-Daten und -Events									
per SNMP exportiert	●	○	●	○	●	●	●	○	●
per WELF-Format exportiert	○	○	○	○	●	k.A.	k.A.	○	○
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.	10 480	9440	6998	5296	ca. 3765	5150	6600	8800	944
Website	www.astaro.de	www.clavister.de	www.funkwerk-ec.com	www.gateprotect.de	www.lucent.com/security	www.secureguard.at/isaserver	www.rimapp.com	www.liss.de	www.zyxel.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*

den kleinen 64-Byte-Paketen. Hier waren maximal 14 MBit/s möglich. Unter Volllast schrumpfte diese Bandbereite dann auf ganze 1,72 MBit/s zusammen. Verwendeten wir die größeren Frames, blieb das Gerät auch bei Volllast stabil und schaffte rund 95 beziehungsweise gut 82 MBit/s. Bidirektional gingen die pro Flow erreichbaren Bandbreiten dann weiter zurück. So waren hier bei Verwendung des größten Frame-Formats noch maximal 71, beim mittleren Format 48 und bei den kleinen Frames noch 8 MBit/s möglich. Unter Volllast reduzierten sich die Durchsätze dann auf 48 beziehungsweise rund 19 MBit/s für die großen und die mittleren Frames. Bei der bidirektionalen Messung mit 64-Byte-Frames machte die Astaro dann praktisch ganz dicht. Hier war noch ein Durchsatz von 0,01 MBit/s messbar. Signifikante Unterschiede in der Fairness gab es zwischen den beiden Senderichtungen im bidirektionalen Betrieb nicht. Beiden Flows standen praktisch die gleichen Bandbreiten zur Verfügung.

Unidirektional und mit den großen Frames machte auch die Clavister-SG-3150 eine gute Figur und verfehlte die Wirespeed nur knapp. Auch

Testaufbau VPN-UDP-Durchsatz



sie erreichte hier einen maximalen Durchsatz von 95 MBit/s. Bei den mittelgroßen Frames reichte es dann im unidirektionalen Betrieb noch für 76 MBit/s. Sendeten wir 64-Byte-Frames schaffte das System noch einen maximalen Durchsatz von 17 MBit/s. Diese Bandbreiten standen dann aber auch noch bei Volllast zur Verfügung. Im bidirektionalen Betrieb halbierten sich die möglichen Durchsätze nahezu. Standen bei der Messung mit den 1024-Byte Frames noch maximal 52 MBit/s zur Verfügung, so reduzierten sich die Werte bei 512-Byte-Paketen auf 37 MBit/s und bei 64-Byte-Paketen auf 8 MBit/s. Diese Durchsätze waren dann aber auch noch bei Volllast realisierbar. Bei der Beurteilung der Fairness fällt eine Benachteiligung der Senderichtung intern – remote auf. So war hier bei der Messung mit den großen Frames ein Frame-Loss von fast 52 Prozent zu messen, in der Gegenrichtung betrug der Frame-Loss dagegen nur gut 46 Prozent.

Etwas hinter dem Hauptfeld lag die Bintec-VPN-Access-250 von Funkwerk. Unidirektional schaffte sie mit den größten Frames einen Durchsatz von 85 MBit/s. Bei der gleichen Messung mit 512-Byte-Paketen stand dann noch eine Bandbreite von 67 MBit/s zur Verfügung. Verwendeten wir die kleinsten Pakete, reduzierte sich die Bandbreite auf 21 MBit/s. Diese Bandbreiten standen dann aber auch noch bei Volllast zur Verfügung. Im bidirektionalen Betrieb reduzierte sich dann die verfügbare Bandbreite je Flow um ganze 50 Prozent, was eine maximale Bandbreite von 43 MBit/s bei den größten und von 10 MBit/s bei den kleinsten Frames bedeutet. Auch diese Bandbreiten waren unter Volllast noch nutzbar. Weiterhin hat die Bintec-Appliance die verfügbare Bandbreite im bidirektionalen Betrieb immer sehr fair zwischen beiden Flows aufgeteilt.

Nahezu Wirespeed erreichte Gateprotects Firewall-Server bei der unidirektionalen Messung mit den größten Flows, hier stand eine Bandbreite von 96 MBit/s zur Verfügung. Verwendeten wir 512-Byte-Frames, reduzierte sich die Bandbreite auf 91 MBit/s. Probleme hatte dann auch das Gateprotect-System mit den 64-Byte-Paketen. Hier ging die Bandbreite auf 26 MBit/s zurück. Im bidirektionalen Betrieb schaffte der Firewall-Server bei der Messung mit den 1024-Byte-Frames gleichfalls 96 MBit/s. Verwendeten wir die 512-Byte-Pakete, reduzierte sich die Bandbreite auf 66 MBit/s je Flow. Und als wir die Messung mit 64-Byte-Paketen wiederholten waren nur noch 13 MBit/s möglich. Unter Volllast und mit 64-Byte-Paketen verringerte sich die Bandbreite dann nochmals, hier waren unidirektional noch rund 18 und bidirektional nur noch 0,33 MBit/s je Flow möglich.

Auch Lucents VPN-Firewall-Brick-150 kam unidirektional und mit größeren Frames recht gut zurecht. So schaffte die Brick-150 bei der Messung mit 1024-Byte-Paketen einen Durchsatz von 95 MBit/s, verwendeten wir 512-Byte-Pakete, betrug die Bandbreite noch 91 MBit/s. Bei den kleinsten Frames reduzierte sich die Bandbreite dann auf 37 MBit/s. Diese Bandbreiten standen dann auch noch unter Volllast zur Verfügung. Der Wechsel in den bidirektionalen Betrieb reduzierte deutlich die verfügbaren Bandbreiten je Flow. Bei der Messung mit den größten Frames betrug die maximale Bandbreite noch 64 MBit/s, verwendeten wir 512-Byte-Frames, standen noch 51 MBit/s zur Verfügung und bei den kleinsten Frames verringerte sich die Bandbreite je Flow auf 17 MBit/s. Davon blieben unter Volllast dann nur noch 0,23 MBit/s übrig. Und auch bei den Messungen mit den größeren Frames verringerte sich die Bandbreite unter Volllast weiter. Waren die Frames 1024 Byte groß, blieb hier eine Bandbreite von gut 50 MBit/s übrig. Mit 51 MBit/s erreichte die OSST-Appliance bei der unidirektionalen Messung mit den größten Frames ihren Bestwert. Verwendeten wir die 512-Byte-Pakete, schaffte das System noch 26 MBit/s und bei den kleinsten Frames standen noch 3 MBit/s Bandbreite zur Verfügung. Davon blieben dann unter Volllast noch 0,24 MBit/s übrig. Aber auch bei den Messungen mit den größeren Frames reduzierte sich die mögliche Bandbreite unter Volllast weiter. So schaffte das OSST-System bei der Messung mit den größten Frames noch gut 36 MBit/s. Der Wechsel in den bidirektionalen Betrieb reduzierte die verfügbare Bandbreite je Flow noch einmal deutlich. So waren noch maximale Bandbreiten von 25 MBit/s bei den größten Frames und 2 MBit/s bei Verwendung der kleinsten Frames möglich. Unter Volllast blieben davon noch rund 19 beziehungsweise 0,2 MBit/s je Flow übrig. Mit der Fairness hat es das OSST-System dann auch nicht

OSST SecureGUARD for Microsoft ISA Server 2004 ISA110

besonders genau genommen. So betrug der Frame-Loss im bidirektionalen Modus bei der Messung mit den 1024-Byte-Frames für den Flow intern – remote 63,47 Prozent, in der Gegenrichtung verlor das System zugleich 99,2 Prozent aller Daten.

Volle Wirespeed erreichte die Rimapp-Roadblock-CF401U bei der unidirektionalen Messung mit den 1024-Byte-Frames. Verwendeten wir 512-Byte-Frames, reduzierte sich die maximale Bandbreite auf 86 MBit/s und bei der Messung mit den 64-Byte-Paketen waren noch 21 MBit/s möglich. Unter Volllast blieben davon dann noch rund 3 MBit/s übrig. Haben wir größere Frames

MEINUNG SECURITY-APPLIANCES

Prof. Dr. Bernhard G. Stütz

Zwischen den Performance-Aussagen der Hersteller, den Ansprüchen ihrer Kunden und dem wirklichen Potential aktueller Security-Appliances liegen vielfach Welten. Die Vermutung liegt nahe, dass die Hersteller derzeit nicht in der Lage sind, wirklich leistungsfähige Hardware für das Geld zu bieten, das ihre Kunden bereit sind zu zahlen. Denn eines ist klar: Den wirtschaftlichen Druck, der auf der gesamten Branche liegt, sollte man nicht unterschätzen. Wenn aber die Produkte nicht halten, was ihre eigenen Hersteller versprechen und deren Kunden verlangen, bringt das die Branche auch nicht weiter. Das Rennen werden künftig die Hersteller – und deren Kunden – machen, die es schaffen, zu einem guten Preis-Leistungsverhältnis wirklich leistungsfähige Hardware auf den Markt zu bringen.

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 250000 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 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.

verwendet, kam die Rimapp-Roadblock auch bei Volllast deutlich besser zurecht. So schaffte sie bei der Messung mit 512-Byte-Paketen gut 95 MBit/s. Der Wechsel auf bidirektionalen Betrieb reduzierte auch hier die möglichen Bandbreiten. So standen bei der Messung mit den größten Frames noch 80 MBit/s je Flow zur Verfügung. Verwendeten wir 512-Byte-Pakete, schaffte das System noch 44 MBit/s und bei der Messung mit den kleinsten Frames betrug der maximal möglich Durchsatz 8 MBit/s. Unter Volllast reduzierte sich dann bei der Messung mit den kleinsten Frames der Durchsatz bis auf gut 1,5 MBit/s. Deutliche Probleme hatte das Rimapp-System mit der Fairness. So betrug der Frameloss bei der Messung mit 512-Byte-Paketen für den Flow intern – remote rund 19 Prozent, in der Gegenrichtung gingen zugleich gut 93 Prozent aller Daten verloren.

Wirespeed verfehlte Telcotechs Liss-II bei der uni- wie der bidirektionalen Messung mit den 1024-Byte-Paketen mit 96 MBit/s nur knapp. Waren die Frames 512 Byte groß, schaffte das System noch 91 MBit/s uni- und 90 MBit/s bidirektional je Flow. Erst bei den Messungen mit den kleinsten Frames war ein deutlicher Unterschied zwischen dem uni- und dem bidirektionalen Betrieb feststellbar. Hier stehen sich die Maximalbandbreiten von 26 MBit/s für unidirektional und 14 MBit/s für bidirektional gegenüber. Unter Volllast reduzierten sich die Durchsätze bei den Messungen mit den kleinsten Frames dann noch mal. Hier waren unidirektional noch rund 4,7 und bidirektional nur noch 0,02 MBit/s möglich. Bei den Volllastmessungen mit größeren Frames hielt sich die Liss-II deutlich besser. So schaffte sie bidirektional mit 512-Byte-Paketen je Flow gut 75 MBit/s. Und bei der Messung mit den größten Frames blieb der Durchsatz je Flow bei rund 96 MBit/s.

Zycels Zywall 5 erwies sich auch in unserem VPN-Szenario als unterdimensioniert. So schaffte sie unidirektional bei der Messung mit den größten Frames gerade 22 MBit/s. Bidirektional stand noch eine Bandbreite von 12 MBit/s zur Verfügung. Bei den Messungen mit 512-Byte-Paketen waren dann noch 11 beziehungsweise 6 MBit/s möglich. Verwendeten wir die kleinsten Flows, gingen gerade noch rund 1 MBit/s je Flow über die Leitungen. Unter Volllast hat sich an diesen Bandbreiten dann auch nichts wesentliches mehr geändert.

Fazit

Das noch recht moderate Abschneiden der meisten Fast-Ethernet-Appliances in unserer Report-Card sollte 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 bidirektional 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. Insgesamt vermochte sich Telchotech mit ihrer Liss-II wenn auch relativ knapp vor dem Feld durchzusetzen und die Auszeichnung »Referenz« zu gewinnen. Hervorzuheben ist noch Lucent, deren Brick-150 durch ihren günstigen Preis und ihren recht guten dritten Platz zu überzeugen, was ihr die »Preis-Leistungs-Empfehlung« sichert. Schließlich kostet diese Lösung nur knapp halb so viel, wie die erstplatzierte. Die letztplatzierte Zyxel-Zywall 5 war dagegen für unser Szenario schlicht unterdimensioniert und spielt auch preislich in einer anderen Liga als das übrige Testfeld. Für andere Einsatzzwecke kann sie durchaus eine attraktive Wahl sein.

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 performant 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 Stö-

Lucent VPN Firewall Brick 150

rungen 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