Geruhsamer Brandschutz

Vergleichstest Security-Appliances, Teil 2 – Firewall und VPN bieten einen recht guten Schutz in modernen Netzen. Teils zu kurz kommen aber immer noch Performance und Quality-of-Service. Dies hat ein Vergleichstest der Real-World Labs von Network Computing ergeben.

Dafür, 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 heute zumeist mit Gigabit-Ethernet-Ports aus. Denn darin sind sich die Security-Hersteller zumindest in der Theorie einig: Security-Appliances sind aktive Netzwerkkomponenten, die ebenso wie LAN-Switches möglichst mit Wirespeed arbeiten sollen und nicht zum Flaschenhals werden.

REPORTCARD FIREWALL-PERFORMANCE UND -QoS

interaktiv unter www.networkcomputing.de

	Gewichtung in Prozent	Alcatel-Lucent VPN Firewall Brick 1200	Juniper SSG-550	Siemens 4YourSafety RX300S3	Stonesoft FW-5100	Phion netfence nf-850	Fortinet FortiGate 3600A	Clavister SG4250	Gateprotect X-Serie Enterprise Box	Zyxel ZyWALL 1050
FW-UDP-Durchsatz 64 Byte	20	4	3	3	2	2	3	2	2	1
FW-UDP-Durchsatz 512 Byte	20	5	5	5	4	4	4	4	4	2
FW-UDP-Durchsatz 1518 Byte	20	5	5	5	5	5	5	5	5	2
Latency 1518 Byte 50 % Last	5	5	5	5	5	5	5	5	5	4
Latency 1518 Byte 100 % Last	5	4	4	5	5	4	4	4	4	4
Portlimitierung	10	3	2	3	3	3	3	1	1	3
Datenpriorisierung	10	5	5	1	5	5	1	1	1	5
Bandbreitenlimitierung	5	2	3	3	3	3	2	1	1	2
Bandbreitengarantie	5	2	3	3	2	2	1	1	1	2
Gesamtergebnis	**100**	**4,25**	**4,05**	**3,80**	**3,75**	**3,70**	**3,40**	**2,95**	**2,95**	**2,40**
		B+	**B+**	**B**	**B-**	**B-**	**C+**	**C**	**C**	**D**

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

Max. Durchsatz	Latency	QoS
›/= 70 % = 5	‹ 1000 µs = 5	Σ ‹ 5% = 5
›/= 35 % = 4	›/= 1000 µs = 4	Σ ›/= 5% = 4
›/= 15 % = 3	›/= 10 000 µs = 3	Σ ›/= 10% = 3
›/= 5 % = 2	›/= 100 000 µs = 2	Σ ›/= 30% = 2
‹ 5 % = 1	›/= 1 000 000 µs = 1	Σ ›/= 50% = 1

Wie gut solche Systeme diese Anforderungen erfüllen, sollte ein Vergleichstest in unseren Real-World Labs an der FH Stralsund zeigen. Getestet haben wir Security-Appliances auf ihre Tauglichkeit für den performanten Schutz von konvergenten 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 jeweils 30 PC-Arbeitsplätzen sowie zwei Auslandsniederlassungen in New York und Hongkong mit jeweils 40 PC-Arbeitsplätzen.

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

Die Ausgangssituation

Die Network Computing Musterfirma möchte die verschiedenen Segmente 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.

Ethernet-Seurity-Appliances:

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

Folgende Testparameter sollten untersucht werden:

- Überprüfung der VPN- und HA-Funktionalität,
- Überprüfung der Datenpriorisierung und des Bandbreiten-Managements,
- Firewall- und VPN-Performance (Datendurchsatzraten)
- Packet-Loss,
- Latency sowie
- Jitter.

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

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

In unseren Tests haben wir die Aspekte Firewall- und VPN-Performance, Quality-of-

DAS TESTFELD

Fast-Ethernet-Appliances

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

ZUM THEMA

Vergleichtests Security-Appliances

- Theorieartikel: NWC 5-6 / 2007, S.16 ff.
- Test Teil 1, VPN-Performance: NWC 5-6 / 2007, S.20 ff.

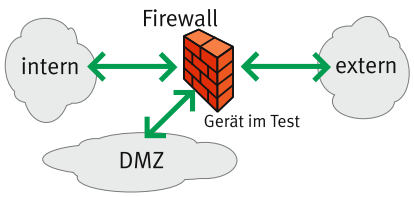
Service sowie Hochverfügbarkeit untersucht. In unserem zweiten, hiermit vorliegenden Testbericht stellen wir die Ergebnisse der Performance-Messungen im Firewall-Betrieb sowie unsere Tests zu den Themen Quality-of-Service und Hochverfügbarkeit dar. Die Ergebnisse unserer Performance-Messungen im VPN-Betrieb waren Thema des ersten Teils, der in Network Computing 5-6/2007 erschienen ist.

Alcatel-Lucent VPN Firewall Brick 1200

Firewall-UDP-Durchsatz

In einer Messreihe haben wir den Firewall-UDP-Durchsatz ermittelt. Hierzu haben wir die jeweilige Appliance über drei Ports – intern, DMZ und extern – mit dem Smartbits-Lastgenerator/Analysator verbunden. Die Smartbits generierten dann Flows aus UDP-Paketen jeweils mit konstant 64, 256, 512, 1024 und 1518 Byte Größe und sendeten diese an alle drei Ports. Die Datenströme adressierten wir jeweils an die zwei »gegenüber« liegenden Ports der Appliance. Neben konstant großen Frame-Formaten haben wir dann noch einen Frame-Mix erzeugt und Real-World Traffic genannt. Dieser entspricht der gemessenen Verteilung der Frame-Formate im MCI-Backbone. Hier sind rund 50 Prozent aller Frames 64 Byte groß. Die übrigen 50 Prozent streuen über alle möglichen Frame-Formate. Die Belastung des Systems erfolgte multidirektional, das heißt alle drei Ports sendeten und empfingen gleichzeitig maximal mit Wirespeed.

Testaufbau Firewall-UDP-Durchsatz




Gateprotect X-Serie Enterprise Box

Gemessen haben wir Frame-Loss, Latency und Jitter. Die erzeugte Last beginnt bei einem Prozent und wird dann schrittweise erhöht. Aus den ermittelten Frame-Loss-Werten errechnen sich die Werte für den maximalen Durchsatz. Dieser ist der maximal mögliche Durchschnittswert aller Flows bei einem Frame-Loss von weniger als einem Prozent.

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

Alcatel-Lucents VPN-Firewall-Brick-1200 erreichte im multidirektionalen Betrieb mit 64-Byte-Paketen einen Durchsatz von 39 Prozent, was einem Durchsatz je Port und Senderichtung von 390 MBit/s entspricht. Auch wenn dieser Wert noch weit von der nominellen Leistungsgeschwindigkeit entfernt ist liegt die Brick hier deutlich vor dem Mitbewerb im Testfeld. Verwendeten wir das zweitgrößte Frame-Format, schaffte die Alcatel-Lucent-Appliance schon 85 Prozent des maximal möglichen Durchsatzes. Und mit noch größeren Datenrahmen lieferte das System durchgängig Leitungsgeschwindigkeit. Daran änderte sich auch nichts, als wir unseren Real-World Traffic verwendeten. Die Latency-Werte bei unseren Messungen mit halber Durchsatzleistung mit der VPN-Firewall-Brick-1200 lagen zwischen 129 und 204 µs. Bei voller Durchsatzleistung stieg die Latency dann auf Werte im vier- bis fünfstelligen Bereich an. Sie schwankten zwischen rund 5000 und 24 000 µs.

Clavisters SG4250 hatte – wie die übrigen Systeme im Test auch – größere Probleme mit den kleineren Datenrahmen als die Brick. Betrug das Frame-Format 64 Byte, schaffte die SG4250 einen Durchsatz von 9 Prozent. Mit steigender Frame-Größe vergrößerte sich auch die maximal mögliche Durchsatzleistung. So lagen bei 258-Byte-Frames 29 Prozent und bei 512-Byte-Frames 54 Prozent der Leistungsgeschwindigkeit an. Verwendeten wir noch größere Datenrahmen, war Wirespeed möglich. So konnten wir mit 1024-Byte-Paketen 98 Prozent und mit den größten Frames 100 Prozent Durchsatz messen. Mit Real-World Traffic schaffte die SG4250 49 Prozent der nominellen Leitungsgeschwindigkeit. Bei halber Durchsatzleistung verhielt sich die SG4250 vorbildlich. Hier blieben die Werte durchweg im zweistelligen Bereich. Unter voller Leistung erhöhten sich die Werte für die Latency deutlich. Sie betrugen dann zwischen rund 3600 µs im Betrieb mit den größten Frames und um die 50 000 µs in allen übrigen Fällen.

Fortinets Fortigate-3600A schaffte im Betrieb mit den kleinsten Frames einen Durchsatz von maximal 16 Prozent. Verwendeten wir größere Frames stieg auch hier der möglich Durchsatz kontinuierlich an. Mit maximal 71 Prozent Durchsatz bei der Messung mit den größten Frames konnte die Fortigate-3600A allerdings die nominelle Leitungsgeschwindigkeit nicht erreichen. Mit Real-World Traffic belastet erreichte die Fortigate-3600A eine Durchsatzleistung von 55 Prozent der Wirespeed. Arbeitete die Fortigate-3600A mit halber Durchsatzlast, so betrug die Latency zwischen 100 und 175 µs. Mit maximal möglichem Durchsatz erreichte die Fortinet-Appliance Latency-Werte zwischen gut 500 µs im Betrieb mit den kleinsten Frames und rund 3800 µs im Betrieb mit den größten Frames.


Juniper SSG-550

Gateprotects X-Serie-Enterprise-Box schaffte im Test mit den 64-Byte-Frames gerade mal 6 Prozent Durchsatzleistung. Mit größeren Frames kam sie dann deutlich besser zurecht. So waren bei der Messung mit 512-Byte-Frames 35 Prozent Durchsatz und bei der Messung mit 1024-Byte-Frames 70 Prozent Durchsatzleistung realisierbar. Betrug das Frame-Format 1518 Byte, erreichte die X-Serie-Enterprise-Box die nominelle Leitungsgeschwindigkeit. Arbeitete die X-Serie-Enterprise-Box mit halber Durchsatzleistung, so betrug die Latency zwischen rund 90 und 150 µs. Unter maximalem Durchsatz stieg die Latency auf Werte zwischen rund 5000 und 10 000 µs.

Junipers SSG-550 erreichte im Test mit den kleinsten Frames einen Durchsatz von 16 Prozent. Verwendeten wir größere Datenrahmen, stiegen die Durchsatzwerte zügig an. So schaffte das System schon mit 256-Byte-Paketen 54 und mit 512-Byte-Paketen 79 Prozent der Leitungsgeschwindigkeit. Praktisch Wirespeed erreichte die SSG-550 mit 1024-Byte-Frames, hier waren 98 Prozent Durchsatz zu messen. Mit den größten Frames schaffte auch die Juniper-Appliance dann volle 100 Prozent Durchsatz. Mit Real-World Traffic belastet kam die SSG-550 auf

85 Prozent Durchsatzleistung. In der Disziplin Latency erreichte die Juniper-Appliance mit halber Durchsatzleistung Latency-Werte zwischen gut 50 und 180 µs. Unter der jeweils maximal realisierbaren Last lag die Latency dann zwischen knapp 1300 und rund 4100 µs.

Auch Phions Netfence-nf-850 schwächelte, wenn es galt, 64-Byte-Pakete zu verarbeiten. Hier lag der maximale Durchsatz bei 12 Prozent. Mit größeren Frames kam die Netfence-nf-850 dann deutlich schneller voran. So schaffte sie bei der Messung mit 512-Byte-Paketen schon 63 Prozent der nominellen Leitungsgeschwindigkeit. Mit noch größeren Frames belastet erreichte die Phion-Appliance Wirespeed. Verwendeten wir unseren Real-World Traffic, lag der maximal erreichbare Datendurchsatz bei 65 Prozent der Leitungsgeschwindigkeit. Die Latency pendelte bei unseren Messungen mit der Netfence-nf-850 unter halber Last zwischen rund 100 und 140 µs. Arbeitete die Phion-Appliance mit maximal möglichem Durchsatz, stieg die Latency auf Werte zwischen gut 1800 und 4500 µs an.

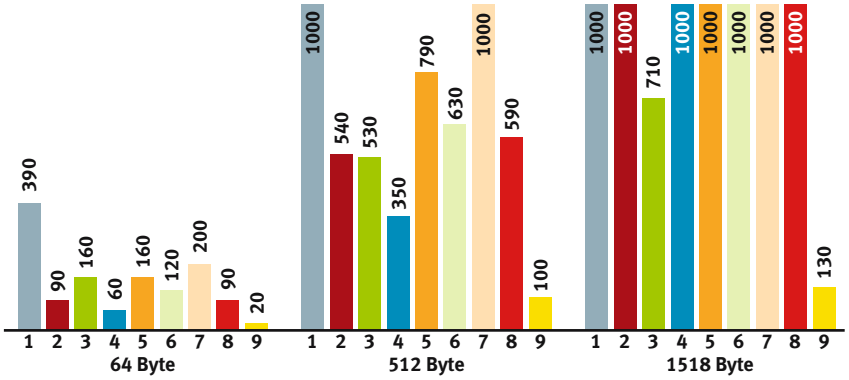
Siemens 4Yoursafety-RX300S3 erwies sich in der Disziplin Firewall-Performance als deutlich performanter als bei unseren VPN-Messungen. Schaffte die Siemens-Appliance mit den kleinsten Frames noch 20 Prozent Durchsatz, so stieg die Leistung mit dem Frame-Format deutlich an. Mit 256-Byte-Frames lag der Durchsatz bei 58 Prozent. Ab 512 Byte lieferte die 4Yoursafety-

Phion netfence nf-850

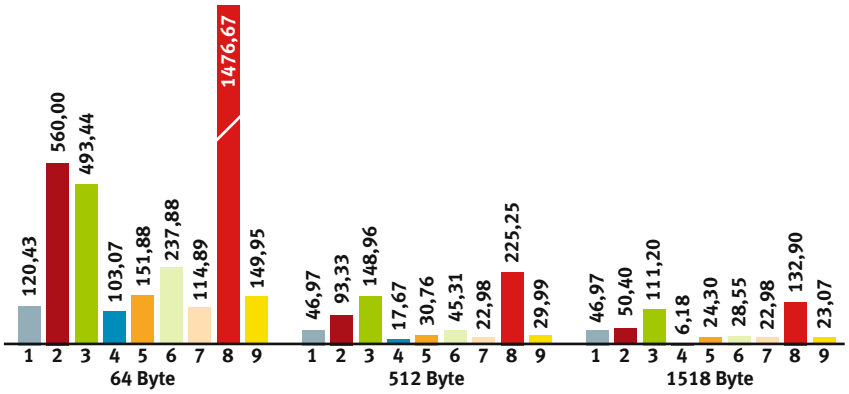
RX300S3 durchgängig Leitungsgeschwindigkeit. Die für die Siemens-Appliance ermittelten Latency-Werte unter halber Last variieren zwischen 75 und rund 170 µs. Arbeitete die 4Yoursafety-RX300S3 mit den maximal möglichen Durchsatzleitungen, lag die Latency bei der Messung mit den kleinsten Frames bei über 5600 µs. Verwendeten wir größere Frame-Formate, pendelte der Latency-Wert zwischen rund 450 und 960 µs.

Stonesofts FW-5100 schaffte bei unserer Messung mit den kleinsten Frames einen maximalen Durchsatz von 9 Prozent der nominellen Leitungsgeschwindigkeit. Mit dem Frame-Format stiegen auch hier wieder die Durchsätze deutlich an. So schaffte die FW-5100 mit 512-Byte-Frames bereits 59 Prozent. Ab 1024 Byte erreichte auch die Stonesoft-Appliance Leitungsgeschwindigkeit. Mit Real-World Traffic lag der Durchsatz der FW-5100 bei 53 Prozent. Dabei blieben die Latency-Werte im moderaten dreistelligen Bereich.

Messergebnisse FW-UDP multidirektional (Datendurchsatz in MBit/s)



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



Zyxels Zywall-1050 erreichte bei der Messung mit den kleinsten Frames maximal 2 Prozent Durchsatzleistung. Mit 256-Byte-Frames waren dann 7 Prozent der Leitungsgeschwindigkeit drin. Ihren maximalen Durchsatz erreichte die Zywall-1050 mit 13 Prozent bei der Messung mit den größten Frames. Mit Real-World Traffic schaffte die Zywall-1050 9 Prozent Durchsatz. Bei halber Durchsatzleistung schwankte dabei die Latency zwischen rund 800 und 1000 µs. Bei voller Leistung stieg die Latency dann auf Werte zwischen 2000 und 4500 µs an.

Die Latency-Werte im Vergleich

Auf Grund der vorhandenen Messdaten haben wir zwei Kennwerte herausgegriffen, die die gemessenen Latency-Werte vergleichbarer machen sollen. Dazu haben wir die gemessene Latency in Relation zur Durchsatzleistung gesetzt. Die Werte für die Messungen mit den größten Frames haben wir hier ausgewählt, weil sieben von neun Appliances hier Wirespeed lieferten. Somit konnten wir bis auf zwei Ausnahmen auf Grund der Messdaten die exakte Latency einer konstant gesetzten Durchsatzrate zuordnen.

Für unsere Messungen mit 50 Prozent Wirespeed und 1518-Byte-Paketen reicht die Spanne zwischen 85 µs bei Clavister bis zu 236 µs für Stonesoft. Die Werte für Fortinet und Zyxel sind hier nicht exakt bestimmbar, weil diese beiden Systeme die Leitungsgeschwindigkeit nicht realisieren konnten und die Latency-Werte daher für geringere Durchsatzwerte ermittelt wurden. Bei 100 Prozent Wirespeed variiert die Latency zwischen 611 µs für Siemens bis zu 8195 µs für Alcatel-Lucent. Auch wenn hier signifikante Unterschiede bestehen, bewegen sich die Messwerte maximal im einstelligen Millisekundenbereich und sind somit insgesamt unkritisch.

Firewall-TCP-Messungen

In einer weiteren 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 jeweilige 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 vom WAN ins LAN sowie von der DMZ ins WAN. Die generierte Last ähnelt insgesamt einer bidirektionalen Smartbits-Messung mit größeren UDP-Paketen. Die jeweilige Appliance wurde an die Messtechnik, den Spirent Avalanche und Reflector, angeschlossen. Als Frame-Formate haben wir hier 256, 512, 1024, 1280 und 1518 Byte verwendet. Die Messtechnik simuliert so die Kommunikation zwischen Client-Systemen im internen Netz sowie Rechnern in der

LATENCY BEI 50 % WIRESPEED MIT 1518 BYTE

Alcatel-Lucent	VPN-Firewall-Brick-1200	204 µs
Clavister	SG4250	85 µs
Fortinet	Fortigate-3600A	› 175 µs
Gateprotect	X-Serie-Enterprise-Box	147 µs
Juniper	SSG-550	164 µs
Phion	Netfence-nf-850	142 µs
Siemens	4Yoursafety-RX300S3	167 µs
Stonesoft	FW-5100	236 µs
Zyxel	Zywall-1050	› 2056 µs

LATENCY BEI 100 % WIRESPEED MIT 1518 BYTE

Alcatel-Lucent	VPN-Firewall-Brick-1200	8195 µs
Clavister	SG4250	3633 µs
Fortinet	Fortigate-3600A	› 3798 µs
Gateprotect	X-Serie-Enterprise-Box	5579 µs
Juniper	SSG-550	2749 µs
Phion	Netfence-nf-850	4479 µs
Siemens	4Yoursafety-RX300S3	611 µs
Stonesoft	FW-5100	670 µs
Zyxel	Zywall-1050	› 2055 µs

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 Messwerte hier nicht weiter ein.

Alcatel-Lucents VPN-Firewall-Brick-1200 erreichte eine Connection-Setup-Rate von 47 000, die Connection-Capacity schaffte mit über 2 033 000 Verbindungen das Hardware-Limit unserer Messtechnik. Clavisters SG4250 schöpfte mit einer Connection-Setup-Rate die Leistungsfähigkeit der Messtechnik voll aus. Die maximal mögliche Connection-Capacity betrug dabei rund 1 346 000 Verbindungen. Fortinets Fortigate-3600A schaffte eine Connection-Setup-Rate von 44 000 und eine Connection-Capacity von gut 940 000. Dabei überschrieb das Fortinet-System wie schon im Vorjahrestest alte Verbindungen durch neue, obwohl das Limit auf 800 000 gesetzt war.

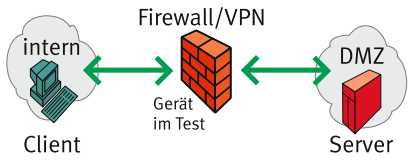
Gateprotects X-Serie-Enterprise-Box vermochte 42 000 Verbindungen pro Sekunde aufzubauen und mit einer Connection-Capacity von rund 2 033 000 Verbindungen erreichte auch diese Appliance die Grenzen der Messtechnik. Junipers SSG-550 lag mit einer Connection-Setup-Rate von 43 000 etwas über dem System von Gateprotect. Allerdings konnte das System »lediglich« 128 000 Verbindungen gleichzeitig offen halten. Phions Netfence-nf-850 schaffte dagegen eine Connection-Capacity von 237 000. Allerdings konnte das System »nur« 19 000 Verbindungen pro Sekunde aufbauen.

Fortinet FortiGate 3600A

Siemens 4Yoursafety-RX300S3 reizte unsere Messtechnik in der Disziplin Connection-Setup-Rate mit 50 000 Verbindungen voll aus. Die Connection-Capacity blieb dagegen mit rund 1 118 000 hinter den Möglichkeiten der Messtechnik zurück. Stonesofts FW-5100

schaffte es hingegen als einziger Hersteller, mit beiden Parametern die Grenzen der Messtechnik voll auszuloten. Zyxels Zywall-1050 lag dagegen in den Connection-Disziplinen am hinteren Ende des Feldes. Die Zywall-1050 baute 15 000 Verbindungen in der Sekunde auf und erreichte eine Kapazität von 131 000 Verbindungen.

Testaufbau Firewall-TCP-Messung



Auch hier zeigen sich signifikante Unterschiede in der Leistungsfähigkeit der getesteten Systeme. Insgesamt bewegen sich die Appliances aber in einem Bereich, der die Anforderungen in den meisten Einsatz-Szenarien vollständig erfüllen sollten.

Quality-of-Service

In einer weiteren Messreihe haben wir die implementierten Bandbreitenmanagement-Mechanismen untersucht. In der Disziplin »Portlimit« haben wir die Bandbreite des WAN-Ports auf 10 MBit/s limitiert und den Port mit 40 MBit/s belastet. Gemessen haben wir dann die Verlustraten in Prozent. Diese Ergebnisse haben wir dann mit dem errechneten Sollwert verglichen und die Abweichung bestimmt. Diese Messung haben wir wieder nacheinander mit den Frame-Größen 64, 256, 512, 1024 und 1518 Byte durchgeführt.

Alcatel-Lucents VPN-Firewall-Brick-1200 arbeitete insbesondere mit den kleinsten Frames nicht sehr präzise. Hier wich sie um 19 Prozentpunkte vom Sollwert ab. Die Abweichungen von den Sollwerten bei den Messungen mit den übrigen Frame-Formaten waren deutlich geringer. Insgesamt addierten sich die Abweichungen für alle Frame-Formate auf 26 Prozent auf. Clavisters SG4250 arbeitete deutlich unpräziser als die Brick. Sie wich alleine bei der Messung mit den kleinsten Frames schon um 39 Prozent vom Sollwert ab. Mit zunehmender Frame-Größe arbeitete dann auch die SG4250 genauer. In der Summe kam sie auf 60 Prozent Abweichung von den Sollwerten.

Fortinets Fortigate-3600A arbeitete in dieser Disziplin am präzisesten. Die Abweichungen von den Sollwerten schwankten zwischen 7 Prozent bei der Messung mit 64-Byte-Frames und 1 Prozent bei der Messung mit 512-Byte-Frames. Insgesamt kam die Fortigate-3600A auf einen kumulierten Wert von 14 Prozent Abweichung. Gateprotects X-Serie-Enterprise-Box unterstützte die geforderten Quality-of-Service-Mechanismen nicht, obwohl sie diese Funktionalität nach Herstellerangaben prinzipiell beherrschen sollte. Grund dafür war offensichtlich, dass sich nicht das richtige und aktuelle Modul für das Bandbreitenmanagement auf der Firewall befand.

Auch Junipers SSG-550 hatte in erster Linie Probleme mit den kleinsten Frames. Hier wich sie um 22 Prozent von den Sollwerten ab. Mit größeren Frames arbeitete auch dieses System genauer. Insgesamt summierten sich die Abweichungen auf 31 Prozent. Phions Netfence-nf-850 wich bei der Messung mit 64-Byte-Frames um 18 Prozent vom Sollwert ab. Insgesamt kam die Netfence auf eine kumulierte Abweichung von 26 Prozent.

Siemens 4Yoursafety-RX300S3 wich bei der Messung mit den kleinsten Datenrahmen um 13 Prozent vom Sollwert ab. In der Summe kam sie auf 25 Prozent. Stonesofts FW-5100 verhielt sich ähnlich wie das Siemens-System. Sie wich um 12 Prozentpunkte bei der Messung mit 64-Byte-Frames vom Sollwert ab und summierte eine Gesamtabweichung von 19 Prozent. Zyxels Zywall-1050 kam auf eine Gesamtabweichung von den Sollwerten von 29 Prozent. Davon entfielen allein auf die Messung mit den kleinsten Frames 19 Prozent.

In der Disziplin »Bandbreitenlimit« haben wir die maximalen Bandbreiten für vier verschiedene Prioritäten im Verhältnis von 4 zu 3 zu 2 zu 1 festgelegt und die Abweichungen in der höchsten Priorität von den Sollwerten ermittelt. Diese Messung haben wir wieder nacheinander mit den Frame-Größen 64, 256, 512, 1024 und 1518 Byte durchgeführt.

Alcatel-Lucents VPN-Firewall-Brick-1200 arbeitete im Modus Bandbreitenlimit unpräziser als im vorhergehenden. Sie wich allein bei der Messung mit den kleinsten Frames um 17 Prozent vom Soll ab. Insgesamt addieren sich die Abweichungen auf 40 Prozent auf. Clavisters SG4250 hatte hier deutliche Probleme. So wich die SG4250 alleine bei der Messung mit den kleinsten Datenrahmen schon um 48 Prozent ab. Aber auch mit den anderen Frame-Formaten arbeitete das System nicht sehr genau. Insgesamt summierten sich so 110 Prozentpunkte.

Stonesoft FW-5100

Fortinets Fortigate-3600A wich bei der Messung mit den 64-Byte-Frames um 16 Prozent vom Sollwert ab. Insgesamt kam sie auf eine kumulierte Abweichung von 37 Prozent. Junipers SSG-550 hielt sich schon präziser an die Vorgaben. Sie kam hier insgesamt auf eine Abweichung von 12 Prozentpunkten. Phions Netfence-nf-850 hatte bei diesen Messungen die Nase noch ein Stück weiter vorne. Sie arbeitete auch mit den kleinsten Frames recht präzise. Insgesamt kam die Netfence-nf-850 auf eine kumulierte Abweichung von 11 Prozent.

Siemens 4YourSafety RX300S3

Siemens 4Yoursafety-RX300S3 arbeitete nicht ganz so präzise und erreichte eine kumulierte Abweichung von den Sollwerten von 15 Prozent. Stonesofts FW-5100 wich zwar im Betrieb mit den kleinsten Frames schon um 9 Prozent vom Sollwert ab. Mit allen anderen Frame-Formaten kam sie dafür aber sehr gut zurecht. So kam sie insgesamt auf eine Abweichung von 13 Prozent. Zyxels Zywall-1050 hatte dagegen die meisten Probleme mit den größten Frames. Hier wich sie schon alleine um 14 Prozent vom Soll ab. Insgesamt addierten sich bei der Zywall-1050 die Abweichungen auf 31 Prozentpunkte.

In der Disziplin »Bandbreitengarantie« haben wir die maximalen Bandbreiten für vier verschiedene Prioritäten im Verhältnis von 4 zu 3 zu 2 zu 1 festgelegt und die Abweichungen in der höchsten Priorität von den Sollwerten ermittelt. Diese Messung haben wir wieder nacheinander mit den Frame-Größen 64, 256, 512, 1024 und 1518 Byte durchgeführt.

Alcatel-Lucents VPN-Firewall-Brick-1200 arbeitete im Betrieb mit Bandbreitengarantie praktisch genauso wie mit Bandbreitenlimit. Insgesamt wich sie um 39 Prozent vom Soll ab. Clavisters SG4250 hatte hier deutlich weniger Probleme mit den kleinen Frames als im vorhergehenden Test. Insgesamt kam sie aber auch hier noch auf 70 Prozent Abweichung von den Sollwerten. Fortinets Fortigate-3600A stellte diese Funktionalität nicht zur Verfügung.

Junipers SSG-550 arbeitete mit Bandbreitengarantie insbesondere im Bereich der größeren Frames unpräziser als im vorhergehenden Test. Sie sammelte insgesamt 24 Prozentpunkte an Abweichungen an. Auch Phions Netfence-nf-850 hatte hier mehr Probleme, sich an die Sollwerte zu halten. So wich sie schon alleine im Betrieb mit den kleinsten Frames um 22 Prozent vom Sollwert ab. Mit größeren Frames kam sie deutlich besser zurecht, so dass sich die Werte für die Abweichungen insgesamt auf 30 Prozent summierten.

Siemens 4Yoursafety-RX300S3 wich schon im Betrieb mit den kleinsten Frames alleine um 12 Prozent vom Sollwert ab. Insgesamt addierten sich die Sollwert-Abweichungen hier auf 26 Prozent. Stonesofts FW-5100 arbeitete hier noch etwas unpräziser als die Siemens-Appliance. So war schon bei der Messung mit den kleinsten Frames eine Abweichung vom Soll von 17 Prozent festzustellen. Über alle Frame-Formate hinweg addierten sich die Abweichungen dann auf 42 Prozent auf. Zyxels Zywall-1050 arbeitete mit

DAS TESTVERFAHREN

Als Lastgenerator/Analysator haben wir in unseren Real-World Labs den bekannten »Smartbits 6000C Traffic Generator/Analyser« von Spirent eingesetzt. Das in dieser Konfiguration rund 250 000 Euro teuere Gerät war mit der Software »Smartflow« ausgestattet und mit 24 Gigabit-Ethernet-Fibre/Kupfer-Ports bestückt. Alle Ports arbeiten im Full-Duplex-Modus und können somit gleichzeitig Last mit Wirespeed generieren und analysieren. Für die TCP-Messungen haben wir dann »Avalanche« und »Reflector« von Spirent verwendet. Bei allen Messungen handelt es sich um Zangenmessungen, bei denen entsprechende Datenströme generiert und analysiert werden.

Um vergleichbare, gültige und aussagefähige Ergebnisse zu erzielen, haben wir im Vorfeld die Einstellungen der Security-Appliances festgelegt und ein für alle Firewall-Tests verbindliches Standard-Rule-Set vorgegeben. Für die korrekte Konfiguration haben wir gemeinsam mit den Ingenieuren des jeweiligen Herstellers gesorgt, die ihr eigenes System im Test begleitet haben.

Die einzelnen Netzsegmente haben wir über Gigabit-Ethernet-Switches realisiert. Diese Systeme leisteten in den den einzelnen Tests vorhergehenden Kontrollmessungen volle Wirespeed und sind aus diesem Grund in Hinsicht auf das Datenrahmenverlustverhalten des Testaufbaus vollständig transparent. Die geringe Latency der Systeme wurde entsprechend berücksichtigt. Mit Hilfe von drei Linux-Intel-PC-Clients in den einzelnen Netzsegmenten haben wir die korrekte Firewall-Konfiguration und -Funktion jeweils vor den einzelnen Testläufen überprüft.

Clavister SG4250

Bandbreitengarantie praktisch genauso wie zuvor mit Bandbreitenlimit. Die kumulierte Abweichung von den Sollwerten beträgt hier 30 Prozent.

In der Disziplin »Datenpriorisierung« haben wir vier Prioritäten festgelegt, zwei Eingangsports mit Volllast belegt und die Datenströme an einen Ausgangsport adressiert. Da der entsprechende Ausgangsport mit 200 Prozent Last konfrontiert war sollte er gemäß den Regeln des Strict-Priority-Mechanismus die Daten der beiden niedrigen Prioritäten verwerfen und die der beiden hohen Prioritäten ungehindert passieren lassen. Gemessen haben wir die Datenverlustraten in der höchsten Priorität. Diese Messung haben wir wieder nacheinander mit den Frame-Größen 64, 256, 512, 1024 und 1518 Byte durchgeführt.

Alcatel-Lucents VPN-Firewall-Brick-1200, Junipers SSG-550, Phions Netfence-nf-850, Stonesofts FW-5100 und Zyxels Zywall-1050 arbeiteten absolut korrekt und leisteten sich keinerlei Datenverluste in der höchsten Priorität. Clavisters SG4250 hatte dagegen deutliche Probleme, die höchste Priorität von Datenverlusten frei zu halten. So lagen die Verlustraten zwischen 13 Prozent bei der Messung mit den größten Frames und 34 Prozent bei der Messung mit den 256 Byte großen Frames. Der kumulierte Datenverlust über alle fünf Messungen betrug 120 Prozent in der höchsten Priorität.

Fortinets Fortigate-3600A unterstützte die Datenpriorisierung nicht, daher waren hier keine entsprechenden Messungen möglich. Siemens 4Yoursafety-RX300S3 verlor insgesamt noch mehr Daten, als das System von Clavister. Bei der Messung mit den kleinsten Frames kam die Siemens-Appliance noch auf 9 Prozent Frame-Loss. Im Betrieb mit den größeren

Zyxel ZyWALL 1050

Frame-Formaten lagen die Verlustraten dann zwischen 43 und 48 Prozent. So kam die 4Yoursafety-RX300S3 auf einen kumulierten Datenverlust von 195 Prozent.

Hochverfügbarkeit

Im Hochverfügbarkeitstest haben wir jeweils zwei identische Appliances parallel geschaltet und dann im laufenden Betrieb unter Last den Ausfall eines der beiden Systeme erzwungen. Über die Messung der Datenverlustraten konnten wir dann die Umschaltzeit ermitteln. Da diese Zeit abhängig vom Polling-Intervall und vom willkürlichen Zeitpunkt des Ausfalls ist können die Werte für ein und die selbe Appliance stark schwanken. Um aussagekräftige Ergebnisse für die einzelnen Systeme zu erhalten, wäre daher eine häufige Wiederholung dieses Vorgangs erforderlich. Daraus könnte dann ein statistisch signifikantes Ergebnis generiert werden. Die Zeit für ein solches Verfahren hatten wir leider nicht. Daher können die Ergebnisse hier sinnvollerweise nur allgemein dargestellt werden.

Die stichprobenweise ermittelten Umschaltzeiten schwankten zwischen 1 und 7,5 Sekunden. Dabei lag der Mittelwert bei gut 4 Sekunden. Es ist also klar, dass diese Zeitspanne sich in der Praxis äußerst störend auf Echtzeitapplikationen wie Voice- oder Video-over-IP geschweige denn auf Produktionssteuerungssysteme auswirken würde.

Fazit

Im Zeitalter von Triple-Play haben sich die Anforderungen an Security-Appliances gewandelt. Nicht nur Sicherheit und Performance sind heute gefragt, sondern auch Echtzeitfähigkeit. Und die Hersteller haben reagiert und implementieren nicht nur praktisch durchgängig die sich zum kostengünstigen Standard entwickelnden Gigabit-Ethernet-Ports, sondern auch Quality-of-Service-Mechanismen. Damit sind aber noch lange nicht alle Probleme beseitigt. Der vorliegende Test hat gezeigt, dass die Hersteller einige ihrer Hausaufgaben bereits gemacht haben. Auf ihren Lorbeeren ausruhen sollten sie sich aber nicht. Alle Systeme im Testfeld haben durchaus noch Potential für Verbesserungen. Ein wirklich reibungsloser Einsatz der aktuell getesteten Appliances setzt voraus, dass sich die IT-Verantwortlichen sowohl mit den Eigenschaften der entsprechenden Systeme als auch mit dem gesamten Geschehen in ihrem ganzen Netzwerk auskennen.

Der vorliegende Test hat auch gezeigt, dass nicht immer das teuerste System das beste ist. So haben Juniper und Siemens im Preis-Leistungs-Segment eindeutig die Nase vorn. Alcatel-Lucent konnte auch den zweiten Teil unseres Vergleichstests für sich entscheiden und geht somit als Gesamtsieger durchs Ziel. Die Systeme von Gateprotect und Zyxel lagen nicht nur in ihrem Leistungsvermögen, sondern auch in der Preisklasse deutlich hinter beziehungsweise unter dem Testfeld. Die genannten Hersteller haben ihre Teilnahme wohl eher olympisch gesehen: Dabei sein ist alles.

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