Brandschutz im Einsatz

Nachtest »FortiGate 1000A FA2« – Firewall und VPN bieten einen recht effektiven Brandschutz in modernen Netzen. Wie gut sich das Gigabit-Ethernet-System von Fortinet im Real-World-Labs-Test bewährt, hat ein Nachtest ergeben.

DAS TESTFELD

Gigabit-Ethernet-Appliances
- Fortinet FortiGate 1000A FA2

(Nachtest in der vorliegenden Ausgabe)
- Clavister SG4205
- Gateprotect Firewall Server 5.0 – Professional 4U Enterprise Box
- Juniper ISG-2000
- Netasq F2000

(Vergleichstest in NWC 7-8 2006, S. 18 ff.)

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

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

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

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

Testszenario und die Anforderungen der Network Computing-Musterfirma haben wir in Network Computing 7-8 2006 ab Seite 18 detailliert dargestellt.

Das erste Testfeld im Vergleichstest Firewall- und VPN-Systeme bildeten die Fast-Ethernet-Systeme »Clavister SG4205«, »Fortinet FGT 300A«, »Gateprotect Enterprise«, »Lucent Brick 50«, »Securepoint RC3« sowie »Symantec Gateway Security 1620«. Wie sich diese Systeme im Performance-Test verhalten haben, steht in Network Computing 5-6 2006. Das zweite Testfeld bildeten die Gigabit-Ethernet-Appliances »Clavister SG4205«, »Gateprotect Firewall Server 5.0 – Professional 4U Enterprise Box«, »Juniper ISG-2000« und »Netasq F2000«. Die Performance-Testergebnisse dieser Systeme haben wir in Network Computing 7-8 2006 dargestellt. In einem Nachtest haben wir nun Fortinets »FortiGate 1000A FA2« nach unserem standardisierten Testverfahren untersucht.

REPORTCARD FIREWALL- UND VPN-PERFORMANCE

interaktiv unter **www.networkcomputing.de**

Alle Messergebnisse finden Sie unter: **www.networkcomputing.de/nwc_downloads/fw_vpn_gigabit_ethernet_06_2.zip**

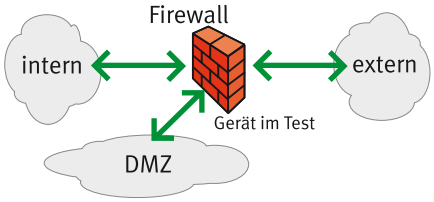
	Gewichtung	Juniper Networks ISG-2000	Fortinet FortiGate 1000A FA2	Clavister SG4205	Gateprotect Firewall-Server-5.0 – Professional-4U Enterprise-Box	Netasq F2000
FW-Durchsatz 64 Byte unidirekt.	8,33	5	5	3	3	2
FW-Durchsatz 512 Byte unidirekt.	8,33	5	5	5	5	4
FW-Durchsatz 1518 Byte unidirekt.	8,33	5	5	5	5	5
FW-Durchsatz 64 Byte multidirekt.	8,33	4	3	2	2	1
FW-Durchsatz 512 Byte multidirekt.	8,33	5	4	4	4	3
FW-Durchsatz 1518 Byte multidirekt.	8,33	5	5	4	4	3
VPN-Durchsatz 64 Byte unidirekt.	8,33	4	2	2	2	1
VPN-Durchsatz 512 Byte unidirekt.	8,33	5	4	4	3	2
VPN-Durchsatz 1280 Byte unidirekt.	8,33	5	4	4	3	3
VPN-Durchsatz 64 Byte bidirekt.	8,33	3	2	1	1	1
VPN-Durchsatz 512 Byte bidirekt.	8,33	5	3	3	2	2
VPN-Durchsatz 1280 Byte bidirekt.	8,33	5	3	4	2	2
Gesamtergebnis	**100,00**	**4,67**	**3,75**	**3,42**	**3,00**	**2,42**
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: ›/= 700 MBit/s = 5 ›/= 350 MBit/s = 4 ›/= 150 MBit/s = 3 ›/= 50 MBit/s = 2 ‹ 50 MBit/s = 1		**A**	**B-**	**C+**	**C**	**D**

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

Firewall-UDP-Durchsatz

In unserer ersten Messreihe haben wir den UDP-Datendurchsatz im Firewall-Betrieb untersucht. Hierbei muss 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

Testaufbau Firewall-UDP-Durchsatz



Smartbits generierten dann Flows aus UDP-Paketen jeweils mit konstant 64, 512, 1024 und 1518 Byte Größe, die Last beginnt bei jeder Messung mit 10 Prozent und wird dann in 10-Prozent-Schritten bis auf 100 Prozent erhöht. Weitere Detail-Messungen haben wir dann in 1-Prozent-Schritten durchgeführt, um die Leistungsgrenzen exakt zu analysieren. Die Belastung der Systeme im Test ist in diesem Aufbau zunächst unidirektional, dann bidirektional und zuletzt multidirektional. Bei den unidirektionalen Messungen ging der Datenstrom vom LAN in Richtung DMZ. Bei den symmetrischen bidirektionalen Messungen haben wir eine entsprechende Kommunikation zwischen LAN und DMZ simuliert. Bei den asymmetrisch-bidirektionalen Messungen lief ein Datenstrom vom LAN ins WAN, der andere vom WAN in die DMZ. Im multidirektionalen Modus haben wir dann Kommunikationsflüsse zwischen LAN, DMZ und WAN simuliert. Hierbei senden und empfangen alle drei Ports gleichzeitig.

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

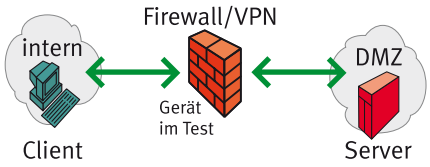
Volle Leitungsgeschwindigkeit erreichte die Fortigate-1000A-FA2 bei unseren Messungen mit unidirektionalem UDP-Durchsatz. Und zwar bei allen Messungen unabhängig vom Frame-Format. Und auch im symmetrischen bidirektionalen UDP-Betrieb lieferte das Fortinet-System durchweg Wirespeed. An ihre Leistungsgrenzen kam dann die Fortinet-Appliance bei unseren asymmetrischen bidirektionalen und bei den multidirektionalen Messungen. Das Durchsatzmaximum lag in beiden Betriebsarten bei 840 MBit/s. Dieses Ergebnis erzielten wir jeweils mit dem größten Frame-Format. Mit kleiner werdenden Frames und einer damit einhergehenden wachsenden Anzahl der zu verarbeitenden Frames sank dann der Durchsatz weiter ab. Waren die Frames 1024 Byte groß, maßen wir jeweils 780 MBit/s. Im Betrieb mit 512 Byte-Frames waren noch 640 MBit/s drin und bei den Messungen mit 64-Byte-Frames reduzierten sich die möglichen Durchsätze auf 170 MBit/s.

Firewall-TCP-Messungen

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

Bei der TCP-Performance-Messung baut die Messtechnik Verbindungen durch die Firewall auf und generiert Datenströme. Bei der unidirektionalen Messung geht der Hauptdatenstrom vom Reflector zum Avalanche. Bei der bidirektionalen Messung laufen die Datenströme vom WAN ins LAN sowie von der DMZ ins WAN. Die generierte Last ähnelt insgesamt einer uni- beziehungsweise bidirektionalen Smartbits-Messung mit größeren UDP-Paketen. Die jeweilige Appliance wird an die Messtechnik, den Spirent Avalanche und Reflector, angeschlossen. Als Frame-Formate haben wir hier 512, 1024 und 1518 Byte verwendet. Die Messtechnik simuliert so die Kommunikation zwischen Client-Systemen im internen Netzwerk sowie Rechnern in der DMZ sowie im externen Netz und protokolliert das Verhalten der Appliance. Da die Ergebnisse der TCP-Durchsatzmes-

Testaufbau Firewall-TCP-Messung



sungen gegenüber den UDP-Durchsatzmessungen keine signifikanten Abweichungen zeigten, gehen wir auf die einzelnen Messergebnisse hier nicht weiter ein.

Fortinets Fortigate-1000A-FA2 erreichte eine Connection-Setup-Rate von 44 000 Verbindungen pro Sekunde. Damit lag sie knapp hinter der Clavister-Lösung, die in unserem Vergleichstest mit unserer Messtechnik voll mithalten konnte. Die Messung der Connection-Capacity ergab einen im Vergleich recht hohen Wert von 1 100 000 Verbindungen. Allerdings verwarf die Fortigate-1000A bei diesen Messungen einzelne bereits bestehende oder auch neue Verbindungen.

Diese Verhaltensweise ist vom Hersteller so gewollt. Fortinet argumentiert folgendermaßen: Verwirft man bestehende Verbindungen, kann es passieren, dass »gute« Sessions verworfen werden. Diese könnten dann aber auch wieder neu etabliert werden. Verwirft man neue Sessions, kann dies einem klassischen DoS gleichkommen, da man einen Service – eine neue Verbindung – auf Systeme hinter der Firewall »denied«. Der positive Askpekt wäre, dass bestehende Sessions erhalten bleiben – nun kann man nicht davon ausgehen, dass alle diese »gut« sind und so ließe sich mit einer großen Anzahl »Zombie-Sessions« der Schutzmechanismus quasi dazu auszunützen, Services hinter der Firewall zu blockieren.

Fortinet hat sich für den reinen Stateful-Handling-Betrieb entschieden, da in der Praxis die Verfügbarkeit eines Dienstes meist höher wiegt als eine »Störung« (Unterbruch der TCP-Session).

Einen erweiterten Schutz bietet nach Angaben des Herstellers das integrierte Intrusion-Prevention-System beziehungsweise der »Anomalie-Teil« dessen. Hier sollen intelligentere Algorithmen zum Tragen kommen. Zum einen können pro Host/Netz oder global eigene Werte für TCP-Sessions definiert werden. – Ebenso wie die »max connections« von einer Quelle. Bei Erreichen dieser Werte sollen umfangreichere Maß-

Fortinet FortiGate 1000A FA2

nahmen greifen, um bestmöglich festzustellen, was »gute« oder »schlechte« Verbindungen sind. Dies hat als Ergebnis, dass bei einer Session-Überlast beziehungsweise für den definierten Grenzbereich bestehende aber auch neue Sessions verworfen werden können.

VPN-UDP-Durchsatz

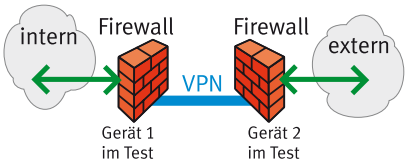
In einer weiteren Messreihe haben wir den VPN-UDP-Durchsatz ermittelt. Hierzu haben wir zwei identische Appliances miteinander verbunden. Dann haben wir den Smartbits-Lastgenerator/Analysator über jeweils einen Port an beide Appliances angeschlossen, so dass wir erneut ein Zangenmessung durchführen konnten. Die Smartbits generierten dann Flows aus UDP-Paketen jeweils mit konstant 64, 512, 1024 und 1280 Byte Größe. Die Last beginnt auch hier wieder mit 10 Prozent und wird dann in 10-Prozent-Schritten bis auf 100 Prozent erhöht. Der Aufbau der VPN-Tunnel erfolgt zwischen den beiden Appliances. Standardmäßig haben wir das VPN durch AES-256-Verschlüsselung realisiert. Die Belastung des VPN-Systems erfolgte erst uni- und dann bidirektional, das heißt beide Ports sendeten und empfingen gleichzeitig maximal mit Wirespeed.

In einer Variante der UDP-Durchsatzmessung, die wir hier »Mix UDP« nennen, haben wir 50 Prozent der jeweiligen Gesamtlast verschlüsselt durch den VPN Tunnel geschickt. Die übrigen 50 Prozent der Gesamtlast ging unverschlüsselt über die Leitung. Die gemessenen Durchsätze entsprechen der Gesamtleistung des Systems. Auch diese Variante haben wir unidirektional und bidirektional durchgeführt. Gemessen haben wir wieder Frame-Loss, Latency und Jitter. Aus den ermittelten Frame-Loss-Werten errechnen sich die Werte für den maximalen Durchsatz. Dieser ist der maximal mögliche Durchschnittswert aller Flows bei einem Frame-Loss von kleiner 1 Prozent.

Fortinets Fortigate-1000A-FA2 erreichte bei unseren VPN-Messungen keine Leitungsgeschwindigkeit mehr. Das ist aber auch bei unserem vorhergehenden Vergleichstest schon keiner der Appliances gelungen. Im unidirektionalen Betrieb mit AES256-Verschlüsselung schaffte die Fortigate bei unserer Messung mit den größten Frames eine Durchsatz von 580 MBit/s. Verwendeten wir 1024-Byte-Pakete, ging der Durchsatz auf 560 MBit/s zurück. Bei der Verwendung von 512-Byte-Frames waren dann noch 460 MBit/s möglich. Und die kleinsten Frames reduzierten den möglichen Durchsatz auf 110 MBit/s. Der Wechsel auf bidirektionalen VPN-Betrieb halbierte dann auch die möglichen Durchsätze. So schaffte die Appliance in dieser Disziplin noch je nach Frame-Format zwischen 290 und 50 MBit/s.

Im Mix-UDP-Betrieb mit AES256-Verschlüsselung waren dann auch bei der Fortigate wieder höhere Durchsatzraten möglich. In der unidirektionalen Betriebsart schwankten die Durchsätze zwischen 990 und 930 MBit/s. Lediglich bei der Verwendung der kleinsten Frames reduzierte sich der mögliche Datendurchsatz auf 230 MBit/s. Der Wechsel auf den bidirektionalen Betrieb reduzierte dann auch im Mix-UDP-Betrieb die möglichen Durchsätze deutlich. Verwendeten wir 64-Byte-Frames, waren hier noch 110 MBit/s möglich. Bei den größeren Frame-Formaten erreichte die Fortigate Durchsatzraten zwischen 460 und 600 MBit/s.

Testaufbau VPN-UDP-Durchsatz



Fazit

Auch unser Nachtest hat gezeigt, dass Leitungsgeschwindigkeit in der Klasse der Gigabit-Ethernet-Geräte immer noch keine Selbstverständlichkeit ist. Dabei treten Bandbreitenengpässe in erster Linie dort auf, wo entsprechende Rechenarbeit zu leisten ist. So bleiben alle getesteten Systeme insbesondere im VPN-Betrieb mit kleinen Frames deutlich hinter der geforderten Leitungsgeschwindigkeit zurück. Klare Unterschiede in ihrem Durchsatzverhalten zeigen aber auch die einzelnen Appliances untereinander. Dabei zeigt der Test eindeutig, dass die Preise der Appliances in einem direkten Verhältnis zur Leistungsfähigkeit der Systeme stehen. Performance erfordert leistungsfähige Hardware – und die hat ihren Preis. Letztendlich vermochte Fortinet aber im Preis-Leistungsverhältnis zu punkten. Schneller als die Fortigate war im Testfeld nur die bald doppelt so teuere Juniper-Appliance. Und das etwa gleich teuere Clavister-System war in machen Disziplinen etwas langsamer. Auch wenn die Systeme von Clavister und Fortinet keine Welten trennen, reicht es für einen wenn auch kleinen Preis-Leistungsvorsprung und somit für unsere Preis-Leistungs-Auszeichnung.

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

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

DAS TESTVERFAHREN

Als Lastgenerator/Analysator haben wir in unseren Real-World Labs den bekannten »Smartbits 6000B Traffic Generator/Analyser« von Spirent eingesetzt. Das in dieser Konfiguration gut 250 000 Euro 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.