Sicherheit

Fast-Ethernet-Firewall-Appliances

Mit Volldampf durch die Feuerwand

Firewalls schützen Unternehmensnetze effektiv gegen Gefahren von innen und außen — doch Sicherheit geht häufig zu Lasten der Performance. Mit welcher Geschwindigkeit aktuelle Firewall-Appliances heute eine gesicherte Kommunikation in Unternehmensnetzen realisieren können, musste eine Reihe von Firewall-Appliances der unterschiedlichen Leistungsklassen in unseren Real-World Labs an der FH Stralsund beweisen.

Für eine sichere aber nach wie vor performante Kommunikation zwischen einem internen Netzwerk – beispielsweise einen Unternehmensnetz – und einem externen Netzwerk – beispielsweise dem Internet oder aber auch anderen Segmenten des eigenen Unternehmensnetzes – sollen Firewalls sorgen. Technisch ist eine Firewall folglich eine aktive Netzwerkkomponente, wie ein Switch oder ein Router, die nicht nur die Kommunikation zwischen zwei Netzwerken oder Netzwerksegmenten ermöglichen soll, sondern zugleich eine Überwachungs- und Kontrollfunktion erfüllt, um das interne Netzwerk vor unerwünschtem Datenverkehr zu schützen. Auf der internen Seite handelt es sich zumeist um Ethernet-basierte Netze, extern können auch die unterschiedlichsten WAN-Verbindungen, wie ISDN, Mietleitungen, Datendirektverbindungen, Standleitungen oder X.25, angeschlossen sein. Platziert werden Firewalls in der Regel zwischen dem internen Netz und einem entsprechenden Remote-Access-System oder einer anderen aktiven Komponente, die die WAN- oder LAN-Anbindung ins externe Netz ermöglicht. Hierfür bieten Firewall-Appliances Fast-Ethernet- und – in der Highend-Klasse – auch Gigabit-Ethernet-Ports an. Manche Systeme stellen darüber hinaus auch WAN-Anschlüsse wie ISDN oder xDSL zur Verfügung. Häufig lässt sich über einen der LAN-Ports zusätzlich eine »demilitarisierte Zone«, kurz DMZ, einrichten, in der beispielsweise Web-Server stehen, die von außen erreichbar sein müssen.

Mit zunehmender Komplexität der heutigen Unternehmensnetze und in Anbetracht der Erkenntniss, dass das Gros der virtuellen Gefahren aus dem eigenen Unternehmensnetz und nicht aus dem Internet drohen, gehen Netzwerkdesigner mehr und mehr dazu über, auch das interne Unternehmensnetz in einzelne Segmente zu parzellieren, die gegeneinander durch Firewalls gesichert sind. Durch die Integration der Firewalls in das Unternehmensnetz muss nun aber nicht nur der Datenverkehr intern – extern, sondern auch ein Großteil des internen Datenverkehrs passieren. In Anbetracht der Datenmengen, der Qualitätsanforderungen in heutigen konvergenten Netzen und der Leistungsfähigkeit der übrigen Komponenten im Unternehmensnetz erhöht dieses Anwendungsszenario deutlich die Anforderungen an Firewall-Systeme im Hinblick auf Performance und Funktionalität. In Anbetracht dieser Situation machen auch Durchsatzraten im Gigabit-Bereich durchaus Sinn und die Implementierung von Gigabit-Ethernet-Technologie ist eine logische Konsequenz. Die Anforderungen an die Leistungsfähigkeit solcher Firewalls entsprechen logischerweise denen, die auch an andere Komponenten des Unternehmensnetzes gestellt werden.

Firewalls arbeiten auf den Ebenen 2 bis 7 des OSI-Referenzmodells. Funktional ist zwischen Paket-Filtern, Stateful-Inspection-Firewalls und Application-Gateways zu unterscheiden. Paket-Filter-Systeme lesen die ein- und ausgehenden Datenpakete auf den Ebenen 2 bis 4 und gleichen sie mit einer vorgegebenen Tabelle ab. Unerwünschte Daten werden so herausgefiltert. Stateful-Inspection-Firewalls sind gegenüber einfachen Paketfiltern »intelligenter« und arbeiten als zustandsabhängige Paket-Filter, die auch die Status- und Kontextinformationen der Kommunikationsverbindungen analysieren und protokollieren. Application-Level-Gateways oder -Proxys realisieren aufwändige Sicherheitsmechanismen über mehrere Schichten hinweg. Sie können die Netze physikalisch wie logisch entkoppeln und von jedem Benutzer Identifikation und Authentifikation prüfen. Komplexere Firewall-Systeme kombinieren in der Praxis häufig verschiedene Firewall-Konzepte in einer Lösung.

Application-Level-Gateways oder -Proxys analysieren den Inhalt der Datenströme, nicht nur wie Paket-Filter- und Stateful-Inspection-Firewalls die Header der Datenpakete, was zur Folge hat, dass ihr Rechenaufwand deutlich größer ist und das Mehr an Sicherheit zu Lasten der Performance geht. Das bedeutet, dass für die gleiche Performance – beispielsweise Fast-Ethernet-Wirespeed – eine deutlich leistungsfähigere Hardware erforderlich ist. Um unsere Tests trotzdem fair und vergleichbar zu halten, haben wir an alle Teststellungen die gleichen Anforderungen gestellt und ein Standard-Rule-Set definiert, das die Hersteller zunächst konfigurieren mussten. Dieses Rule-Set erforderte lediglich eine Paket-Filter- und Stateful-Inspection-Funktionaltät.

Firewalls bestehen aus Hard- und Softwarekomponenten, die häufig von unterschiedlichen

Report-Card /interaktiv unter www.networkcomputing.de

Firewall-Performance

Max. Durchsatz	Gewichtung	Netscreen NS 204 Appliance	Watchguard Firebox Vclass V80	Telco Tech LiSS II secure gateway	Siemens/ Check Point Four your safety RX 100
512 Byte unidirektional	20%	5	5	5	5
512 Byte bidirektional	20%	5	5	3	2
1518 Byte unidirektional	20%	5	5	5	5
1518 Byte bidirektional	20%	5	5	5	5
64 Byte unidirektional	10%	2	1	1	1
64 Byte bidirektional	10%	1	1	1	1
Gesamtergebnis	**100%**	**4,3**	**4,2**	**3,8**	**3,6**
A>=4,3 B>=3,5 C>=2,5 D>=1,5 E<1,5 Die Bewertungen A bis C beinhalten in ihren Bereichen + oder -; Gesamtergebnisse und gewichtete Ergebnisse basieren auf einer Skala von 0 bis 5.		**A-**	**B+**	**B**	**B-**

Bewertungsschlüssel für maximalen Datendurchsatz: > 95 MBit/s = 5, > 90 MBit/s = 4, > 80 MBit/s = 3, > 70 MBit/s = 2, </= 70 MBit/s = 1

Info

Das Testfeld

Gruppe 1: Fast-Ethernet-Appliances
- NetScreen NS-204 Appliance
- Siemens/Check Point Four your safety RX 100 / VPN1 Pro Express
- TELCO TECH LiSS II secure gateway
- WatchGuard Firebox Vclass V80

Gruppe 2: Gigabit-Ethernet-Appliances
- Enterasys, XSR 3150/3250
- GeNUA GeNUGate Enterprise
- Nokia/Check Point IP 740 Check Point NG with Application Intelligence
- Pyramid Computer BenHur II
- Siemens/Check Point Four your safety RX 300 mit Corrent Turbo Card / VPN-1 pro
- Stonesoft StoneGate
- Symantec Gateway Security Appliance

Herstellern stammen und individuell kombiniert werden. Bei den sogenannten Firewall-Appliances handelt es sich um Komplettlösungen, die in den unterschiedlichsten Leistungsklassen angeboten werden und für die unterschiedlichsten Einsatzszenarien gedacht sind. Neben der Firewall-Funktionalität integrieren die Hersteller weitere Funktionalität in die Boxen, so dass immer mehr universelle Security-Appliances angeboten werden, die neben der Firewall-Funktionalität Virtual-Private-Networks, Intrusion-Detection und andere Security- und Kommunikationsfunktionen integrieren. Andererseits verleihen die Hersteller der »klassischen« aktiven Komponenten, wie Switches oder Routern, diesen zunehmend Firewall- und andere Security-Funktionalität, so dass insgesamt derzeit ein recht heterogenes Feld von Systemen auf dem Markt ist.

Die Hersteller teilen die verschiedenen Firewall-Appliances in Leistungsklassen ein, die für die entsprechenden Anwendungsszenarien entwickelt werden und sich deutlich in Leistungsvermögen und Preis unterscheiden. Die preisgünstigsten Geräte bilden die Gruppe der Small-Office/Home-Office-Systeme. Dann folgt das breite und heterogene Feld der Mittelklasse, häufig neudeutsch Medium-Business genannt. Die leistungsfähigen Highend-Systeme bilden dann die Enterprise- und Carrier-Klasse. Das Feld der in unseren Labs befindlichen Firewall-Appliances haben wir dagegen schlicht nach den vorhandenen LAN-Ports in Fast-Ethernet- und Gigabit-Ethernet-Systeme eingeteilt.

Das Real-World-Labs-Test-Szenario

Gegenstand unseres ersten diesjährigen Firewall-Vergleichstests, den wir in unseren Real-World Labs an der FH Stralsund durchführten, war die Performance, die solche Systeme derzeit zur Verfügung stellen. Wir wollten wissen, wie stark die Firewall-Funktionalität die Leistungsfähigkeit der reinen Hardware vermindert, beziehungsweise ob die heute verfügbaren Systeme sichere Verbindungen mit Wirespeed ermöglichen. Darüber hinaus interessierte uns, wie viel gesicherten Datenverkehr der IT-Verantwortliche derzeit für sein Budget erhält.

Für die Ausschreibung unseres Vergleichstests haben wir ein Unternehmen unterstellt, das sein heterogenes, konvergentes Netzwerk sowie eine eigenständige DMZ am Unternehmensstandort hochperformant untereinander sowie mit dem Internet verbinden will. Eine geeignete, durchsatzstarke Firewall-Appliance sollte für die notwendige Sicherheit und Performance sorgen. Zugleich sollte die Appliance den Aufbau eines VPNs zu einer entfernten Niederlassung ermöglichen, die mit einem baugleichen Gerät ausgestattet werden soll.

Daraus ergaben sich folgende Anforderungen an die Teststellungen:
- 2 Firewall- und VPN-Appliances inklusive Zubehör und Dokumentation,
- IPSec-VPN mit IKE,
- Verschlüsselung nach 3DES,
- je Gerät mindestens 3 Fast-Ethernet-Ports oder
- 2 Gigabit-Ethernet- und 1 Fast-Ethernet-Port.

Messen wollten wir die Firewall-Performance, also die unidirektionalen und bidirektionalen Datendurchsatzraten im Firewall-Betrieb, die Datenverlustraten, Latency sowie Jitter unter Last. Als Test-Equipment dienten die Lastgeneratoren und -analysatoren Smartbits 6000B von Spirent Communications mit den aktuellen Applikationen Smartflow und Websuite-Firewall.

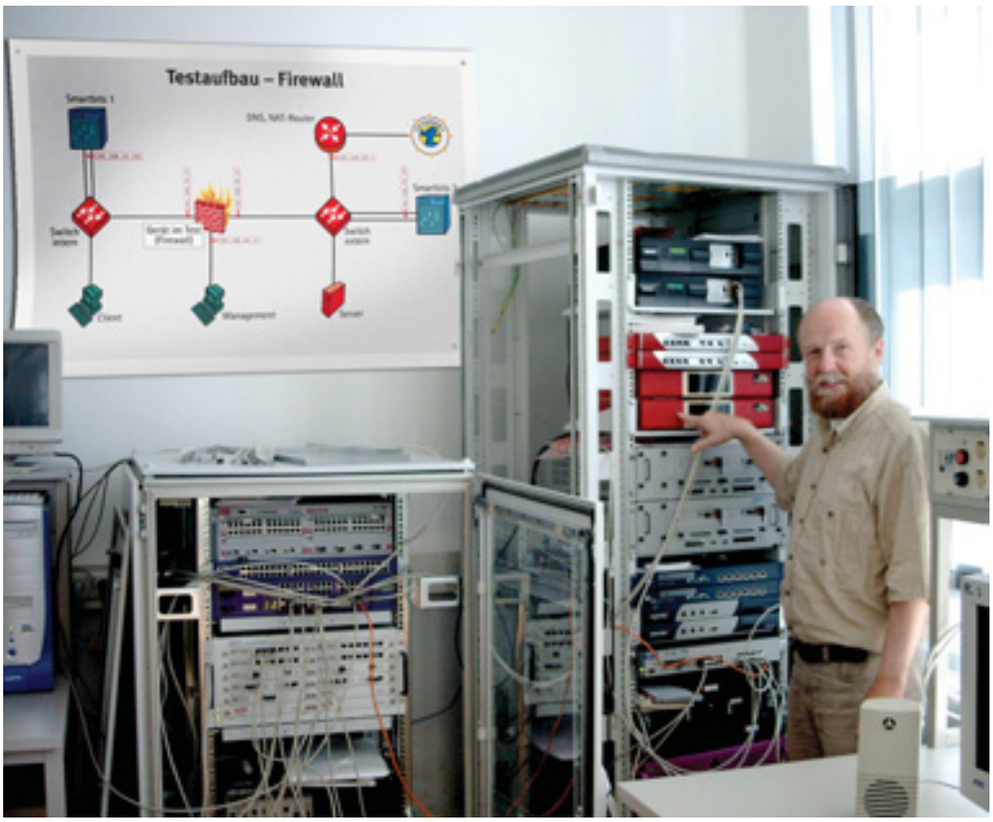
In einer Ausschreibung haben wir dann alle einschlägigen Hersteller von Security-Appliances eingeladen, uns eine entsprechende Teststellung zur Verfügung zu stellen und ihr System in unserem Vergleichstest in unseren Labs an der FH Stralsund zu begleiten. Jedem Hersteller standen unsere Labs exklusiv für einen Tag zur Verfügung. Insgesamt gingen elf Hersteller mit ihren Teststellungen an den Start. Die Gruppe Gruppe 1 der Fast-Ethernet-Appliances bildeten »NetScreen NS-204 Appliance«, Siemens »Four your safety RX 100« mit Check Points »VPN1 Pro Express«, Telco Techs »LiSS II secure gateway« sowie Watchguards »Firebox Vclass V80«. Die übrigen Hersteller zogen es vor, gleich Gigabit-Ethernet-Maschinen ins Rennen zu schicken. Zur Gruppe der Gigabit-Ethernet-Systeme gehören Enterasys »XSR 3150/3250«, Genuas »GeNUGate Enterprise«, Nokias »IP 740« mit Check Points »NG with Application Intelligence«, Pyramids »BenHur II« sowie Siemens »Four your safety RX 300« mit »Corrent Turbo Card« und Check Points »VPN-1 pro«. Das Testfeld vervollständigten Stonesofts »StoneGate« sowie Symantecs »Gateway Security Appliance«. Wie sich die Fast-Ethernet-Appliances in unserem Test verhielten, steht im hier vorliegenden Testbericht. Die Veröffentlichung der Ergebnisse der Gigabit-Ethernet-Appliances ist für die Ausgabe 18/03 der Network Computing vorgesehen.

Durchsatzraten und Datenverlustverhalten

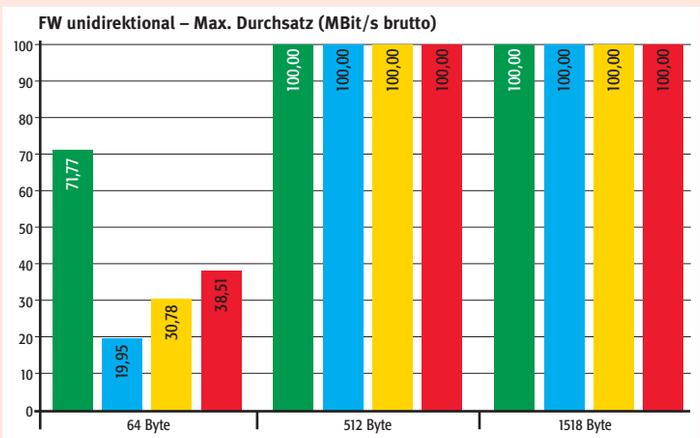
Zur Messung der maximal möglichen Durchsatzraten sowie des lastabhängigen Datenrahmenverlustverhaltens haben wir mit Hilfe der Spirent-Smartbits-Lastgeneratoren/Analysatoren die Firewall-Appliances mit unidirektionalem und bidirektionalem Datenverkehr mit verschieden Framegrößen belas-

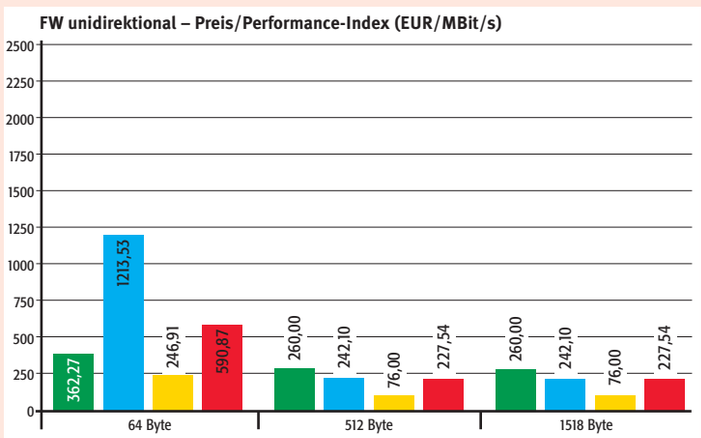
tet. Die Messung der maximalen Durchsatzraten ermittelt den jeweiligen optimalen Durchsatz bei einer für das System idealen Inputrate, zeigt also die maximale Leistungsfähigkeit der Appliance unter optimalen Bedingungen. Die Messung des Datenrahmenverlustverhaltens in Abhängigkeit zur Input-Last zeigt das Verhalten der jeweiligen Appliance unter variierenden Lastbedingungen. Arbeitet eine so getestete Firewall-Appliance mit Wirespeed, so verliert sie unter keinen Umständen Datenrahmen, da die Geräte mit maximal 100 Prozent Last belastet wurden und wir somit keine Überlastsituationen provoziert haben. Erreicht das jeweilige System im Test Wirespeed, dann bedeutet das für den Durchsatzratentest eine maximale zu messende Rate von 100 Prozent oder im Fall des hier vorliegenden Tests 100 MBit/s.

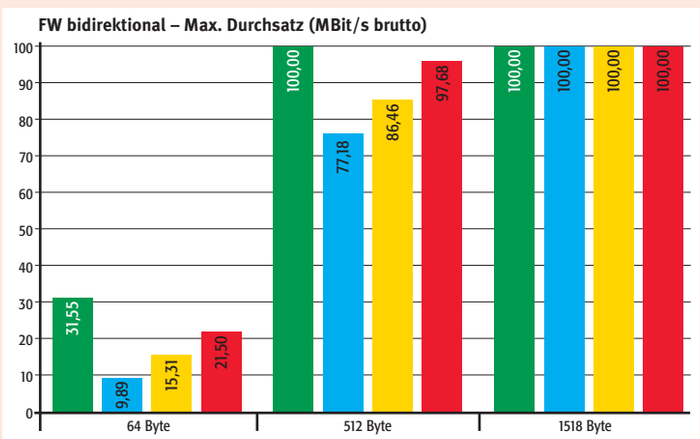
Die Auswirkungen gegenüber Wirespeed reduzierter Durchsatzraten und damit verbundener Datenverluste bei entsprechender Last sind natürlich in realen Unternehmensnetzen abhängig von einer ganzen Reihe von Faktoren – wie den eingesetzten Applikationen oder der Gesamtauslastung des Netzwerks. Generell gilt, dass klassische Datenanwendungen weniger anfällig für entsprechende Engpässe im Netz sind, als moderne konvergente Anwendungen, wie Voice- oder Video-over-IP. Für eine Beurteilung der Testergebnisse für die Praxis ist auch eine Einschätzung wichtig, mit welchen Da-

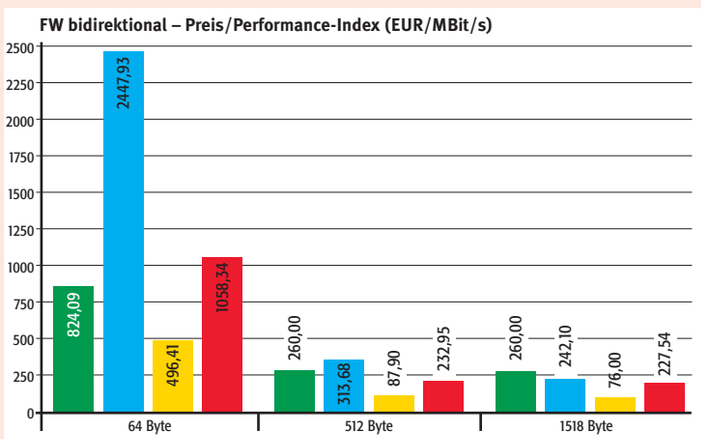


Messergebnisse









Netscreen, Netsreen-NS 204 Appliance
Siemens/Check Point, Four your safety RX 100
Telco Tech, LiSS II secure gateway
Watchguard, Firebox Vclass V80

tenrahmengrößen zu rechnen ist. Bei klassischen Dateitransfers arbeitet das Netzwerk mit möglichst großen Rahmen. Bei Echtzeit-Applikationen teilt sich das Feld. Video-Übertragungen nutzen ähnlich den Dateitransfers relativ große Datenrahmen. Messungen mit Ethernet-LAN-Phones in unseren Real-World Labs haben beispielsweise ergeben, dass diese Voice-over-IP-Lösung die Sprache mit konstant großen Rahmen von 534 Byte überträgt. Noch deutlich kürzere Rahmen sind beispielsweise bei der TCP-Signalisierung mit 64 Byte zu messen. Für die Sprachdatenübertragung wie auch für andere echtzeitfähige Applikationen ist das Datenverlustverhalten von entscheidender Bedeutung. Ab 5 Prozent Verlust ist je nach Voice-over-IP-Codec mit deutlicher Verschlechterung der Sprachqualität zu rechnen, 10 Prozent führen zu einer massiven Beeinträchtigung, ab 20 Prozent Datenverlust ist die IP-Telefonie definitiv nicht mehr möglich. So verringert sich der R-Wert für die Sprachqualität gemäß E-Modell nach ITU G.107 schon bei 10 Prozent Datenverlust um je nach Codec 25 bis weit über 40 Punkte, also Werte, die massive Probleme im Telefoniebereich sehr wahrscheinlich machen.

Netscreens NS-204-Appliance erreichte bei den Messungen mit 64-Byte-Paketen eine maximale Durchsatzrate von rund 72 Prozent unidirektional und von rund 32 Prozent bidirektional. Bis 70 Prozent Eingangslast verlor die NS-204 bei unidirektionalem Datenverkehr keine Datenrahmen. Bis 100 Prozent Eingangslast stiegen die Verlustraten dann bis auf rund 29 Prozent an. Bei der Messung mit bidirektionalem Datenverkehr und 64-Byte-Paketen traten deutliche Datenverlustraten bereits ab 40 Prozent Eingangslast auf, um Spitzenwerte bei 100 Prozent Last in beiden Richtungen von rund 70 Prozent zu erreichen. Bei den Messungen mit größeren Datenrahmen arbeitete Netscreens NS-204-Appliance praktisch mit Wirespeed.

Siemens Four-your-safety-RX-100, ein System, das mit Check Points »VPN1 Pro Express«-Software ausgeliefert wird, zeigte noch größere Probleme mit kleinen Datenrahmen als das Netscreen-Gerät. So erreichte das Fast-Ethernet-System von Siemens in der unidirektionalen Kommunikation mit 64-Byte-Paketen maximal knapp 20 Prozent Durchsatz. In den bidirektinalen Messungen schaffte es nur rund 10 Prozent maximalen Datendurchsatz. Entsprechend gestaltet sich auch der Verlauf der Frame-Loss-Kurven. Bei der unidirektionalen Messung mit 64 Byte schnellte hier der Rahmenverlust bereits bei 30 Prozent Input auf über 55 Prozent Frame-Loss hoch, um dann kontinuierlich bis zum praktischen Vollverlust bei 50 Prozent Last anzusteigen. Bidirektional erreichte die Frameloss-Rate schon bei 20 Prozent Last gut 82 Prozent Frame-Loss, um dann ab 30 Prozent Input praktisch keine Datenrahmen mehr passieren zu lassen. Bei den Messungen mit größeren Datenrahmen und einer unidirektionalen Kommunikation arbeitete das Siemens/Check Point-System dagegen mit Wirespeed. Mehr Probleme bereitete Four-your-safety-RX-100 dagegen der bidirektionale Datenverkehr. Hier betrug die maximale Datendurchsatzrate auch bei der Messung mit 512-Byte-Paketen gut 77 Prozent. In der Frame-Loss-Statistik bedeutet das einen Datenverlust bei 100 Prozent Last von fast 30 Prozent. Erste nennenswerte Verluste sind

Features

Firewall-Teststellungen

	Netscreen NS-204	Siemens / Check Point Four your safety RX 100 / VPN1 Pro Express	TELCO TECH LiSS II secure gateway	Watchguard Firebox Vclass V80
Anz. unabhäng. (nicht geswitchter) LAN-Ports				
Anz. Gigabit-Ethernet-Ports	0	1	0	0
Anz. Fast-Ethernet-Ports	4	3	6	4
Anz. WAN-Ports				
PPoE auf LAN-Port(s)	1	1	1	1, auf Public
X.21	0	0	0	0
X.25	0	0	0	0
ISDN S0	0	0	0	0
ISDN S2M	0	0	0	0
xDSL	0	1	0	0
E1	0	1	0	0
Sonstige (Angabe Typ)	0	0	0	0
Hardware/Betriebssystem				
Prozessor (Typ)	keine Angabe	Celeron P4, 2 GHz	Pentium 4, 3.06 GHz	Asic mit vier RISC CPUs
Arbeitsspeicher in MByte	keine Angabe	256	512	256
Betriebssystem Name/Version	ScreenOS 4.0.1r8	Red Hat Linux 7.3 gehärtet	gehärteter Linux-Kernel	gehärteter Linux-Kernel
Firewall-Technik				
Stateful-Inspection-Firewall	●	●	●	●
Layer-7-Application-Gateway-Proxies	○	●	●	●
anpassbare Proxies	○	●	●	●
Stateful-Inspection und Proxy kombiniert	○	●	●	●
Transp. Firewallfunktionalität konfigurierbar	●	●	●	●
spezielle Firewall-ASICs integriert	●	○	○	●
Netzprozessor mit Firewall Teilfunkt. auf NIC	○	○	○	○
VPN-Protokolle				
L2TP	●	●	○	○
PPTP	○	○	○	○
Secure-Socket-Layer/TLS	○	●	○	○
IPSEC über X.509/IKE	●	●	●	●
Routing-Protokolle				
RIPv1	○	●	○	●
RIPv2	●	●	○	●
OSPF	●	●	○	●
BGP-4	●	○	○	optional
Cluster				
Maximale Clustergröße (Zahl der Systeme)	2	8	beliebig	2
Cluster über 3-Party-Software etabliert	○	●	○	○
Cluster über externen Load-Balancer-Switch	○	●	●	●
Cluster über Netzwerk-Links etabliert	●	●	○	○ , zwei dedizierte Ports
Management				
Telnet	●	●	○	●
Rollen-basierte Verwaltung	●	●	●	●
Auditingfähig	●	●	○	keine Angabe
SSH-Support für CLI	●	●	○	●
HTTP/S	●	●	● , HTTPS	● , HTTPS
Automatische Synchronisierung im Cluster	●	●	●	●
Synchronisierung über multiple Pfade möglich	●	●	●	● , über beide HA Ports
Out-Band-Management	●	●	●	●
Monitoring				
CPU überwacht	●	●	●	●
Speicherauslastung gemessen	●	●	●	●
Port-Auslastung gemessen	●	●	in Vorbereitung	●
Synchronisierung überwacht	●	●	●	●
Die Firewall-Software wird überwacht	●	●	●	●
Schwellenwerte für Auslastung möglich	●	●	○	●
Logging-Daten und -Events				
per SNMP exportiert	●	●	○	●
per WELF-Format exportiert	○	○	○	○
an Syslog-Server exportieren	●	●	●	●
Events zentralisier	●	●	●	●
Event-Management korelliert einzelne Einträge	●	●	○	●
Authentisierung/Autorisierung				
NT-Domain	● , über Radius	●	in Vorbereitung	● , über Radius
TACACS/TACACS+	○	●	○	○
Radius	●	●	○	●
LDAP über TLS	●	●	in Vorbereitung	○
X.509-digitale Zertifkate	●	●	○	●
Token-basierend	●	●	○	●
Sicherheitsfeatures				
DMZ	●	●	●	●
Intrusion-Detection	in Vorbereitung	●	●	●
AAA-Support	●	●	●	○
DHCP	●	○	●	●
NAT-Support	●	●	●	●
Content-Filter	in Vorbereitung	● ,Drittanbieter	●	●
Virenscanner	in Vorbereitung	● ,Drittanbieter	optional	○
Website	www.netscreen.com	www.4ys.de, www.checkpoint.com	www.telco-tech.de, www.liss.de	www.watchguard.com
Listenpreis in Euro für Teststellung zzgl. MwSt. (*)	26 000	24 210	7600	24 800 Dollar

● = ja; ○ = nein; * 2 Appliances (Hard- und Software) inkl. Lizenzen für mindestens 100 User und vollständige Managementlösung

hier bei 80 Prozent Last mit gut 3 Prozent Frame-Loss zu verzeichnen. Bei der Messung mit 1518-Byte-Paketen war dann auch hier die Welt wieder in Ordnung.

Telco Techs Liss-II erreichte bei den 64-Byte-Messungen unidirektional einen maximalen Durchsatz von gut 30 Prozent. Ein Blick in die entsprechende Datenverlustkurve zeigt, dass die Appliance schon bei 40 Prozent Eingangslast auf Datenverlustraten von über 30 beziehungsweise über 40 Prozent kommt. Die höchsten Verluste von praktisch 100 Prozent erlitt das System bei einem Input von 70 Prozent, um dann bei noch höheren Lasten wieder etwas besser zu arbeiten. Bei Volllast betrug die Datenverlustrate aber immer noch über 90 Prozent. Bei den bidirektionalen Messungen kam die Liss-II gleichfalls auf einen maximalen Datendurchsatz von gut 30 Prozent. Im Frame-Loss-Verhalten sind hier bereits gut 35 Prozent Verlust bei 20 Prozent Last zu verzeichnen, ab 40 Prozent Last bildet sich dann ein Plateau nahe einer Verlustrate von fast 100 Prozent. Bei den Messungen mit größeren Datenrahmen leistete sich die Liss-II dann keine Schwächen und arbeitete mit Wirespeed.

Auch Watchguards Firebox-Vclass-V80 zeigte Probleme mit den kleinen Datenrahmen. So betrug hier der maximal erreichbare unidirektionale Datendurchsatz rund 39 Prozent. Bidirektional kam die Firebox dann noch auf 21,5 Prozent. Die entstandenen Datenverluste bei 100 Prozent Input sind entsprechend. So erreichte das Watchguard-System unidirektional Verluste von rund 65 und bidirektional von rund 84 Prozent. Nennenswerte Verluste stellten sich hier schon bei 40 Prozent Last mit gut 4 Prozent und bei 50 Prozent Last von über 23 Prozent ein. Bei der bidirektionalen Messung mit 64-Byte-Paketen verlor das Watchguard-System bereits in beiden Richtungen bei 30 Prozent Input rund 30 Prozent der Daten. Die Kurve der Verlustraten steigt dann kontinuierlich an, um ihr Maximum bei 100 Prozent Last zu erreichen. Eine geringere, aber nicht unbedeutende Schwäche zeigte sich dann noch bei den bidirektionalen Messungen mit 512-Byte-Paketen. Hier kam die Watchguard-Appliance zwar immerhin auf einen maximalen Datendurchsatz von rund 98 Prozent. Allerdings erlaubte sie sich bei Volllast eine Verlustrate von immerhin gut 17 Prozent im Mittelwert. Genauer betrachtet verliert die Firebox bei der bidirektionalen Kommunikation gut ein Drittel aller von extern kommenden Daten. Die Verlustrate beträgt in der Gegenrichtung bei der selben Messung lediglich rund 1,5 Prozent. Bei den übrigen Messungen arbeitete die Firebox mit Wirespeed.

Fazit

Probleme hatten alle vier im Testfeld befindlichen Systeme mit 64-Byte-Datenpaketen. Am stärksten brach hier der Newcomer von Siemens/Check Point ein, der lediglich einen maximalen Durchsatz von unidirektional rund 20 und bidirektional rund 10 Prozent erreichte. Aber auch die Systeme von Telco Tech und Watchguard zeigten hier mit Ergebnissen im Durchsatz-Test in der 30-Prozent-Klasse deutliche Probleme. Mit maximalen Durchsatzwerten von rund 72 Prozent unidirektional und 32 Prozent bidirektional konnte Netsceen die Mitbewerber in der 64-Byte-Klasse klar distanzieren.

Deutliche, wenn auch gegenüber der 64-Byte-Messreihe geringere Schwächen zeigten die Firewalls von Siemens/Check Point, Telco Tech und Watchguard bei der bidirektionalen Messreihe mit 512-Byte-Paketen, wobei die beiden erstgenannten immerhin Frame-Loss-Raten zwischen 24 und 29 Prozent erreichten und die Firebox eine massive asymmetrische Schwäche zeigte. Weitgehend unauffällig arbeiteten die Systeme dann in den Tests mit den 1518-Byte großen Datenrahmen.

Dass die Firewall-Appliances im Bereich der kleinsten Pakete und bei größeren Paketen bei bidirektionalem Datenverkehr als erstes schwächeln, war zu erwarten, da sie hier deutlich mehr Header lesen und Rechenarbeit leisten müssen, als bei großen Paketen. Richtig problematisch würde der Einsatz mehr oder weniger aller Systeme im Testfeld, wenn große Datenmengen mit kleinen Paketen zu erwarten wären, was aber in den wenigsten Fällen eintrifft. Für Anwendungen mit großen Datenrahmen, wie den meisten klassischen Datenanwendungen oder der Übertragung von Video-Streams sind weniger Probleme zu erwarten. Soll aber beispielsweise ein größeres Call-Center mit Voice-over-IP durch eine Firewall hindurch telefonieren, dann ist der IT-Verantwortliche gut beraten, wenn er für die Performance seiner Firewall ohne vorhergehende Analysen, Lastprognosen und fundierte Tests keinesfalls Wirespeed unterstellt.

Als performantestes System im Testfeld der Fast-Ethernet-Firewall-Appliances hat sich auf alle Fälle die Netscreen-Lösung erwiesen. In Anbetracht der Tatsache, dass Netscreen, Siemens und Watchguard auch preislich in einer Liga spielen, führt Netscreen das Testfeld unangefochten an. Die Preise in der Feature-Tabelle geben die aktuellen Listenpreise für unsere vollständige Teststellung – also zwei Systeme inklusive Hard- und Software, Client-Lizenzen für mindestens 100 User sowie die vollständige Managementlösung – wieder, im »wirklichen Leben« kann das Preisgefüge von diesen Angaben durchaus abweichen. So sind die Netscreen-Systeme im noch laufenden Monat zu einem Sonderpreis auf dem Markt erhältlich. Welche Preise zu erzielen sind, ist letztendlich Sache einer guten Einkaufsabteilung. Erstaunlich gut hat sich Telco Techs Liss-II im Umfeld der deutlich teueren Mitbewerber geschlagen. In Anbetracht ihres gegenüber den übrigen Systemen günstigeren Preises verdient sie die Preis-Leistungs-Empfehlung.

Dipl.-Ing. Thomas Rottenau,
Prof. Dr. Bernhard G. Stütz, [dg]

Info

So testete Network Computing

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 2.20.005.1« sowie »Websuite Firewall 2.10.001« ausgestattet und mit 24 Fast-Ethernet-Porst sowie vier Kupfer- und fünf Multimode-LWL-Gigabit-Ethernet-Ports bestückt. Alle Ports arbeiten wahlweise im Half- oder Full-Duplex-Modus und können somit gleichzeitig Last mit Wirespeed generieren und analysieren.

Um vergleichbare, gültige und aussagefähige Ergebnisse zu erzielen, haben wir im Vorfeld die Einstellungen der Firewalls 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.

Zur Ermittlung von Frameloss, Latency und Jitter haben wir mit dem Smartbits-Lastgenerator/Analysator Datenströme generiert und diese unidirektional und bidirektional mit verschiedenen Paketgrößen gesendet. Die Eingangslast haben wir in 10-Prozent-Schritten von 10 bis auf 100 Prozent erhöht. Lagen die ermittelten Performance-Werte unter 10 Prozent oder tauchten weitere Unregelmäßigkeiten auf, haben wir weitere Detail-Messungen gemacht, um das Problem zu analysieren. Den maximalem Durchsatz haben wir mit einem speziellen Mess-Algorithmus der Smartbits ermittelt, in dem der Lastgenerator alternierende Lasten erzeugt, die sich in kleiner werdenden Intervallen dem optimalen Input nähern, bis sie der maximalen Last entsprechen, die gerade noch ohne nennenswerte Datenverluste möglich ist. Nacheinander haben wir für beide Messreihen Datenströme mit konstanten Rahmengrößen von 64, 512 und 1518 Byte erzeugt. Die Messungen erfolgten mit einer Matching-Rule am Anfang und einem längeren Rule-Set mit Matching-Rule am Ende.

Nacheinander haben wir drei Firewall-Testreihen durchgeführt. In der ersten und zweiten Testreihe haben wir unidirektional von intern nach extern gesendet und jeweils einen beziehungsweise zehn UDP-Ports adressiert und entsprechend viele Streams erzeugt. In der dritten Testreihe haben wir dann mit bidirektionalem Datenverkehr gearbeitet. Der Smartbits-Lastgenerator/Analysator hat die empfangenen Datenströme auf die eingestellten Parameter hin untersucht und die Ergebnisse gesichert.

In zwei weiteren Messreihen haben wir die maximale Connection-Capacity sowie die maximale Connection-Setup-Rate ermittelt und weitere TCP-spezifische Messungen durchgeführt, über deren Ergebnisse wir in einer der folgenden Ausgaben von Network Computing berichten werden. Die Perfomance-Messungen haben wir ausschließlich mit UDP-Paketen durchgeführt, weil sich hierbei im Gegensatz zu TCP-Datenströmen Eigenschaften des Protokolls wie Retransmisson nicht auswirken. TCP-Datenströme haben wir dann für die Messungen der Connection-Setup-Rate und Connection-Capacity verwendet.