Schnelle Torwächter

Vergleichstest UTM Teil 2 – Aktuelle Security-Appliances bieten einen umfangreichen Schutz für moderne ITK-Netze. In den Real-World Labs musste eine Auswahl an UTM-Lösungen zeigen, wie performant sie für die notwendige Sicherheit sorgen kann.

UTM-Appliances sind die digitalen Torwächter für moderne Unternehmen. Hinter dem Begriff Unified-Threat-Management steht der Anspruch, einen universellen Schutz gegen alle relevanten Bedrohungen aus dem Netz zu bieten. Folglich vereint eine solche Box Funktionalitäten wie Firewall, VPN, IDS/IPS, Anti-Virus, Content-Filter oder Anti-Spam. Im Zeitalter von Unified-Communications sollen diese digitalen Torwächter natürlich die notwendigen Bandbreiten zur Verfügung stellen und auch Quality-of-Service bieten.

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

Den Vergleichstest haben wir wie gewohnt ausgeschrieben und alle Hersteller und Anbieter zur Teilnahme eingeladen. Das Testfeld bildeten letztendlich Clavisters »SG3210«, Funkwerks »packetalarm UTM2500«, Gateprotects »GPX 800«, Securepoints »RC300«, Telco Techs »LiSS 3000« sowie Zyxels »ZyWALL USG-300«. Wie sich die drei letztgenannten Probanden im Test verhalten haben, steht im vorliegenden Artikel. Teil 1 des Tests haben wir in Ausgabe 10 von Network Computing veröffentlicht.

Securepoints RC300 ist eine IT-Security-Appliance für kleine und mittlere Unternehmen mit bis zu 100 Anwendern. Sie soll sich mit ihrem 19-Zoll-Format in professionelle Rechenzentrumsumgebungen einfügen. Securepoint möchte mit der Lösung die vollständige Network-, Web- und Mail-Sicherheit mittels einer intuitiv bedienbaren Benutzerschnittstelle integrieren und vor aktuellen Internet-Gefahren schützen. Der Hersteller empfiehlt eine User-Anzahl von 50 bis 100 und nennt selbst einen möglichen Firewall-Durchsatz von 400 MBits/s und einen VPN-Durchsatz von 195 MBit/s. Die Liste der Features ist lang. So verfügt die Appliance über eine Stateful-Inspection-Firewall, eine Application-Layer-Firewall, Virenscanner, Spam-Filter, Content-Filter, VPN-Gateway, Intrusion-Detection/Prevention und Bonding/Trunking. Funktionen wie Quality-of-Service, Authentisierung, SIP-, VoIP- und VNC-Support, Multi-Path-Routing, Hochverfügbarkeit, X509-Zertifikatsserver sowie Reporting- und Logserver vervollständigen die Feature-Liste des »All-in-One-Systems«.

Telco Techs Liss-3000 soll sich nach Angaben des Herstellers problemlos in nahezu jede IT-Umgebung integrieren und sich durch Performance, Multifunktionalität und universelle Einsatzmöglichkeiten auszeichnen. Auch die Liss-3000 vereint zahlreiche Funktionen in einer Box. Hierzu gehören ein zentrales IP-Gateway, eine mehrstufige Firewall, VPN-Gateway, Proxy-Server für Antivirus, Spam und Content-Filter. Als Highlights des 19-Zoll-Geräts nennt der Hersteller Policy-Based-Routing, Bridging/Routing, umfangreiche Diagnosemöglichkeiten und das zentrale Management.

Bei der Zywall-USG-300 handelt es sich nach Herstellerangaben um ein Unified-Security-Gateway, das umfassende, maßgeschneiderte Sicherheitsfunktionen auf Unternehmensniveau für kleine und mittelgroße Unternehmen bieten soll. Integriert ist sowohl IPSec-VPN als auch SSL-VPN. Einen weiteren Vorteil sieht der Hersteller in der Integration einer benutzerfreundlichen Zugriffssteuerung, die gegen eingehenden und ausgehenden Traffic und zum Schutz der Netzwerkressourcen eingesetzt werden kann. Die USG-300 soll in der Lage sein, Multi-Layer-Schutz für sicherheitskritische Unternehmensfelder zu bieten. Mit einem integrierten Sicherheits-Co-Prozessor soll die USG-300 in der Lage sein, auch bei hoher Netzwerkbelastung »unerschütterliche und zuverlässige Performance« zu bieten. Zusätzlich soll das IDP-Feature schädliche Angriffe erkennen und notwendige Maßnahmen gegen bösartige oder verdäch-

DAS TESTFELD

Teil 1

- Clavister SG3210
- Funkwerk packetalarm UTM2500
- Gateprotect GPX 800

Teil 2

- SecurePoint RC300
- Telco Tech LiSS 3000 System
- Zyxel ZyWALL USG-300

Telco Techs Liss-3000 soll sich in nahezu jede IT-Umgebung integrieren und sich durch Performance und Multifunktionalität auszeichnen.

tige Aktivitäten treffen. Die signaturbasierte IDP-Engine ist in der Lage, Protokoll- oder Traffic-Anomalien zu erkennen und durch den Abgleich von Verhaltensmustern vor bösartigen Angriffen auf Anwendungsebene zu schützen.

UDP-Durchsatz

In unserer ersten Messreihe haben wir den UDP-Datendurchsatz im UTM-Betrieb untersucht. Hierbei muss die jeweilige Appliance das interne Netz gegen das externe Netz abschotten. Um den Datenverkehr zwischen diesen Netzen zu simulieren, haben wir die zu testenden Systeme über zwei Ports mit unserem Lastgenerator/Analysator Smartbits verbunden. Die Smartbits generierten dann Flows aus UDP-Paketen jeweils mit konstant 64, 256, 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. Bei 100 Prozent liegt dann eine Bruttodurchsatzrate von 1 GBit/s vor. Der realisierbare Nutzdatendurchsatz ist natürlich entsprechend geringer und hängt unter anderem von den verwendeten Frame-Formaten ab. Weitere Detail-Messungen haben wir dann bei Bedarf in 1-Prozent-Schritten durchgeführt, um die Leistungsgrenzen näher zu analysieren. Die Belastung der Systeme im Test ist in diesem Aufbau

Securepoints RC300 ist eine IT-Security-Appliance für kleine und mittlere Unternehmen mit bis zu 100 Anwendern.

unidirektional. Bei den Messungen ging der Datenstrom vom WAN in Richtung LAN.

Gemessen haben wir Frame-Loss und Latency. 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. Da ein Prozent 100 MBit/s entspricht erreicht hier eine Teststellung eine nominale Durchsatzleistung von beispielsweise 300 MBit/s, wenn 400 MBit/s nicht ohne entsprechend hohe Datenverluste darstellbar sind.

Um Referenzwerte für den Vergleich zu erhalten, haben wir zuerst den Testaufbau ohne zwischengeschaltete Appliance getestet. Dann haben wir die entsprechend konfigurierten Systeme nacheinander den entsprechenden Zangenmessungen unterzogen. Bei diesen Referenzmessungen ohne UTM-Appliance ereichte der Testaufbau bei allen Frame-Formaten einen Durchsatz von 100 Prozent oder brutto 1 GBit/s. Dabei war von Anfang an die gesamte UTM-Funktionalität mit Ausnahme der QoS-Datenpriorisierung aktiviert.

Securepoints RC300 schaffte mit den Frame-Formaten zwischen 512 und 1518 MBit/s volle Leitungsgeschwindigkeit, also 1 GBit/s Brutto-Datendurchsatz. Mit kleineren Frames ging dann die Durchsatzrate moderat zurück. Betrug das verwendete Frame-Format 256 Byte, schaffte die RC300 noch einen Durchsatz von 800 MBit/s. Waren die Frames 64 Byte klein, war noch eine Durchsatzrate von 200 MBit/s realisierbar.

Auch Telco Techs Liss-3000 schaffte Leitungsgeschwindigkeit – so lange die Frames zwischen konstant 512 und 1518 Byte groß waren. Mit 256 Byte großen Frames schaffte die Liss dann noch einen Durchsatz von 600 MBit/s. Und der Betrieb mit den kleinsten Frames reduzierte die Durchsatzraten auf 200 MBit/s.

Deutlich mehr Probleme mit dem Durchsatz hatte Zyxels Zywall-USG-300. Mit den größten Frames war hier ein Durchsatz von 100 MBit/s dar-

www.networkcomputing.de ...

Ergänzende Beiträge zu Unified-Threat-Management (UTM):

TESTS

Vergleichstests:

VPN-Appliances für die Zentrale beziehungsweise Niederlassungen von Clavister, Funkwerk, Gateprotect, Siemens und Underground8
... /test-vpn-systeme-gemeinsam-durch-den-tunnel/

Fünf Datenbank-Extrusion-Prevention-Systeme von Crossroads System, Guardium, Imperva, Pyn Logic und RippleTech, um Datenbanken zu schützen
... /dringeblieben-oder-ich-schiesse/

Einzeltests:

Unified-Threat-Management-System »Firebox Peak X8500e«
... /first-look-test-unified-threat-management-system-firebox-peak-x8500e/

Astaro-Firewall 7.3 zündet Nachbrenner
... /aus-dem-testlabor-astaro-firewall-73-zuendet-nachbrenner/

GRUNDLAGEN

Virtual-Appliance von Gateprotect bietet Schutz für Vmware-Plattformen
... /virtual-appliance-von-gateprotect-bietet-schutz-fuer-vmware-plattformen/

Vereint im Tunnel -- Faktoren, die den Einsatz von VPN-Appliances in einem Netzwerk beeinflussen
... /vereint-im-tunnel/

Datendiebstahl stoppen -- Einführung in Datenbank-Extrusion-Prevention-Systeme
... /rauchende-colts/

MEINUNG

Unified-Threat-Management-Appliances anstatt Firewalls, Teil 1 und 2
.../thema-der-woche-unified-threat-management-teil-1/
.../thema-der-woche-unified-threat-management-teil-2/

TECHNISCHE DATEN UTM-APPLIANCES *

	Securepoint 2007nx	Telco Tech LiSS 3000 series	ZyXEL ZyWALL USG-300
Anzahl unabhängiger (nicht geswitchter) LAN-Ports			
Anzahl Gigabit-Ethernet-Ports	6	6	7 (frei definierbar)
Anzahl Fast-Ethernet-Ports	0	6 über Gigabit-Ports	0
Anzahl WAN-Ports			
X.21	0	0	0
X.25	0	0	0
ISDN $_{S0}$	0	max. 1	0
ISDN $_{S2M}$	0	0	0
xDSL	0	max. 4	0
E1	0	0	0
Hardware/Betriebssystem			
Prozessor (Typ), MHz	Intel Core2Duo 2,2 Ghz E4500	Intel Core2Duo 2400 MHz	Freescale 8349E
Arbeitsspeicher in MByte	1024	512	256
Betriebssystem Name/Version	Securepoint OS Build 5651	Linux	ZLD
IPv6-Unterstützung für alle Firewall-Funktionen	○	●	○
Firewall-Technik			
Stateful-Inspection-Firewall	●	●	●
Layer-7-Application-Gateway-Proxies	●	●	●
anpassbare Proxies	●	●	○
Stateful-Inspection und Proxy kombiniert	●	●	○
transparente Firewallfunktionalität konfigurierbar	○	●	●
spezielle Firewall-ASICs integriert	○	○	●
Netzwerkprozessor mit Firewall Teilfunktionen auf NIC	○	○	○
VPN-Protokolle			
L2TP	●	○	●
PPTP	●	○	○
Secure-Socket-Layer/TLS	●	○	●
IPSec über X.509/IKE	●	●	●
Routing-Protokolle			
RIPv1	○	○	●
RIPv2	○	○	●
OSPF	○	○	●
BGP-4	○	○	○
Cluster			
Maximale Clustergröße (Zahl der Systeme)	Unlimitiert	16	○
Cluster über 3rd-Party-Software etabliert	○	○	○
Cluster über externen Load-Balancer-Switch	●	●	○
Cluster über Netzwerk-Links etabliert	●	●	○
Management			
Telnet	○	○	●
rollenbasierte Verwaltung	●	●	●
Auditing-fähig	●	○	●
SSH-Support für CLI	●	○	●
HTTP	○	○	●
HTTPS	○	●	●
automatische Synchronisierung im Cluster	○	○	○
Synchronisierung über multiple Pfade möglich	○	○	○
Out-Band-Management	●	●	●
Monitoring			
CPU überwacht	●	●	●
Speicherauslastung gemessen	○	●	●
Port-Auslastung gemessen	○	●	●
Synchronisierung überwacht	○	○	●
die Firewall-Software wird überwacht	●	●	●
Schwellenwerte für Auslastung möglich	●	●	○
Logging-Daten und -Events			
per SNMP exportiert	○	●	●
per WELF-Format exportiert	○	○	○
an Syslog-Server exportieren	●	●	●
Events zentralisiert	●	●	●
Event-Management korelliert einzelne Einträge	●	●	○
Authentisierung/Autorisierung			
NT-Domain	○	●	●
TACACS/TACACS+	○	○	○
Radius	●	○	●
LDAP über TLS	●	○	●
X.509-digitale Zertifkate	●	●	●
Token-basierend	○	○	●
Sicherheitsfeatures			
DMZ	●	●	●
Intrusion-Detection/-Prevention	●	●	●
AAA-Support	○	○	●
DHCP	●	●	●
NAT-Support	●	●	●
Content-Filter	●	●	●
Virenscanner	Clam AntiVirus	Avira Antivir	Kaspersky
Website	www.securepoint.de	www.telco-tech.de	www.zyxel.de

Quelle: Angaben der Hersteller

● = ja; ○ = nein; k.A. = keine Angabe;

* Die Tabelle beschreibt die Ausstattung der getesteten Geräte (optionale Ausstattung und Funktionen sind für viele Appliances zusätzlich erhältlich)

stellbar. Verwendeten wir kleinere Frames, lag der mögliche Durchsatz durchgängig unter 100 MBit/s.

UDP-Latency

Für den gleichen Testaufbau oben haben wir dann als nächstes die Werte für die Latency ermittelt. Dabei haben wir eine konstante Durchsatzgeschwindigkeit von 100 MBit/s erzeugt. Auch diese Messung haben wir zunächst ohne Appliance ermittelt. Die Werte für die Latency betrugen bei den beiden kleinsten Frame-Formaten 7 µs. Mit 512-Byte-Paketen stieg die Latency auf 12 µs, mit 1024-Byte-Paketen auf 20 µs. Mit den größten Frames erhöhte sich die Latency auf 28 µs.

Securepoints RC300 erreichte Latency-Werte, die zwischen 36 und 83 µs lagen. Dabei erreichte die Appliance die niedrigste Latency im Betrieb mit dem kleinsten Frame-Format. Mit dem Frame-Format stieg dann auch die Latency kontinuierlich an, um mit den größten Frames auch die höchste Latency von 83 µs zu erreichen.

Telco Techs Liss-3000 kam bei unseren Latency-Messungen auf Werte zwischen 33 und 98 µs. Wie schon bei dem Securepoint-System lagen die niedrigsten Werte bei den Messungen mit den kleinsten Frames an und stiegen dann kontinuierlich mit dem Frame-Format.

Zyxels Zywall-USG-300 kam bei der Messung mit den größten Frames auf eine Latency von 345 µs. Verwendeten wir kleinere Frames, lag die Latency durchweg bei rund 33 ms. Die deutliche Erhöhung der Latency ist hier darauf zurückzuführen, dass das System an seiner Leistungsgrenze war und die Pufferspeicher sich entsprechend füllten.

Optimaler UDP-Durchsatz und Latency

Wir haben dann die gleiche Messung mit 1-Prozent-Schritten und dem größten Frame-Format durchgeführt und so die maximal erreichbare Durchsatzleistung sowie die damit verbundene Latency ermittelt. Die Referenzmessung ohne Appliance ergab 100 Prozent oder 1 GBit/s und eine Latency von 28 µs.

Securepoints RC300 erreichte bei diesem Test volle Leitungsgeschwindigkeit. Die Latency betrug dabei rund 280 µs. Wire-Speed erreichte hierbei auch Telco Techs Liss-3000. Die Latency betrug dabei rund 11 ms. Zyxels Zywall-USG-300 schaffte in diesem Test einen maximalen Durchsatz von 11 MBit/s bei einer Latency von gut 20 ms.

TCP-Performance

Bei der TCP-Performance-Messung baut die Messtechnik Verbindungen durch die Appliance auf und generiert Datenströme. Bei der Messung geht der Hauptdatenstrom als Download vom Reflector zum Avalanche. Die generierte Last ähnelt insgesamt einer unidirektionalen Smartbits-Messung mit größeren UDP-Paketen. Die jeweilige Appliance ist mit der

Messtechnik, dem Avalanche und Reflector von Spirent, angeschlossen. Es handelt sich hierbei um einen normalen Download, bei dem in Upload-Richtung kleine Frames mit den entsprechenden Requests und in Download-Richtung automatisch die größtmöglichen Frames gesendet werden. Frame-Formate werden also nicht explizit eingestellt. Die Messtechnik simuliert so die Kommunikation zwischen Client-Systemen im internen Netzwerk sowie Rechnern im externen Netz und protokolliert das Verhalten der Appliance. Auch hier war von Anfang an die gesamte UTM-Funktionalität außer der QoS-Priorisierung aktiv. Allerdings ging hier der TCP-Verkehr am HTTP-Proxy vorbei.

Wir haben so zunächst 100 User simuliert, die jeweils einen beziehungsweise zehn Requests je 10 000 Byte pro TCP-Connection starten. Auch diese Messung haben wir zunächst mit dem Testaufbau ohne dazwischen geschaltete Appliance durchgeführt und dann die Leistungswerte der einzelnen Teststellungen ermittelt. Der Testaufbau selbst kam auf 696 993 beziehungsweise 773 260 Transaktionen und 948 beziehungsweise 970 MBit/s.

Securepoints RC300 schaffte hierbei 687 035 beziehungsweise 772 200 Transaktionen und Durchsätze von 900 beziehungsweise 970 MBit/s. Telco Techs Liss-3000 kam auf 32 179 und 321 790 Transaktionen. Der maximale Durchsatz konnte hierbei nicht ermittelt werden, da die maximale Connection-Capacity nicht ausreichte. Zyxels Zywall-USG-300 kam hier auf 21 444 beziehungsweise 61 410 Transaktionen und Durchsatzwerte von 27 sowie 77 MBit/s.

TCP-Durchsatz mit URL-Filter und Antivirus

Als nächstes wollten wir wissen, welche Durchsatzleistungen die Appliances ermöglichen, wenn der HTTP-Verkehr mit dem URL- und Antivirus-Filter analysiert wird. Wir haben 100 User simuliert, die jeweils zehn Requests je 10 000 Byte pro TCP-Connection starten.

Securepoints RC300 schaffte hierbei 31 790 Transaktionen bei einem Durchsatz von 43 MBit/s. Telco Techs Liss-3000 kam auf 10 585 Transaktionen und einen Durchsatz von 12,5 MBit/s. Zyxels Zywall-USG-300 lag mit 9117 Transaktionen und 9 MBit/s knapp dahinter.

UDP-Latency bei HTTP-Durchsatz

Dann wollten wir wissen, wie sich die Teststellungen bei einem Mix aus UDP-Datenströmen und HTTP-Durchsatz verhalten. Dazu generierten wir mit den Smartbits 1 MBit/s UDP-Datenlast. Zusätzlich simulierten wir mit dem Avalanche den Zugriff von 100 Usern.

Securepoints RC300 kam bei der Messung mit der Grundlast auf eine Latency von 83 µs. Griffen zusätzlich zur Grundlast noch die simulierten HTTP-User auf das System zu, betrug die Latency 108 µs. Telco Techs Liss-3000 kam auf eine Latency von 100 µs mit der Grundlast und auf 150 µs mit dem zusätzlichen HTTP-Traffic. Zyxels Zywall-USG-300 erreichte eine Latency von 190 µs mit der Grundlast und von 250 µs mit den zusätzlich simulierten HTTP-Usern.

Bei der Zywall-USG-300 handelt es sich um ein Unified-Security-Gateway, das umfassende, maßgeschneiderte Sicherheitsfunktionen bieten soll.

UDP-Latency mit Datenpriorisierung

In der letzten Testreihe haben wir untersucht, inwieweit die Datenpriorisierung Einfluss auf die Latency-Werte hat. Dabei haben wir niedrig und hoch priorisierte UDP-Datenströme von jeweils 1 MBit/s gesendet und zugleich wieder die Zugriffe von 100 Usern simuliert.

Securepoints RC300 und Telco Techs Liss-3000 boten keine Möglichkeit, eine Datenpriorisierung zu konfigurieren. Zyxels Zywall-USG-300 gestattete dies. Allerdings zeigten die Latency-Messwerte für die beiden Prioritäten keine Unterschiede. Sowohl für die hoch als auch für die niedrig priorisierten Datenströme konnten wir eine Latency von 250 µs messen.

Fazit

UTM-Appliances müssen sich widersprechende Anforderungen erfüllen. Auf der einen Seite müssen sie die Daten, die sie an das interne, zu schützende Netz weiter leiten, möglichst genau untersuchen. Auf der anderen Seite sollen sie aber möglichst mit Leitungsgeschwindigkeit arbeiten und keine störenden Latency-Werte produzieren. Bei solchen Anforderungen sind Kompromisse unvermeidbar. Die vorliegenden Testergebnisse haben gezeigt, dass die Systeme den Datentransport mit gewissen Einschränkungen durchaus beherrschen. Wie sicher sie wirklich sind und welche Kompromisse die Hersteller zu Gunsten der übrigen Funktionalität eingehen, werden wir im kommenden Frühjahr in einem neuen erweiterten Testverfahren prüfen.

Dipl.-Ing. Thomas Rottenau,
dg@networkcomputing.de

TESTVERFAHREN FIREWALL/VPN-APPLIANCES

Als Lastgenerator und Analysator haben wir in unseren Real-World Labs einen »Smartbits 6000C Traffic Generator/Analysor« von Spirent Comminications eingesetzt. Das System ist mit der Software »SmartFlow« ausgestattet und mit 24 Gigabit-Ethernet-Kupfer-Ports bestückt. Alle Ports können softwareseitig als Lastgeneratorausgang und/oder als Analysatoreingang eingesetzt werden. 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 UTM-Appliances festgelegt und ein für alle 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 realisiert. Diese Systeme leisteten in den den einzelnen Tests vorhergehenden Kontrollmessungen volle Leitungsgeschwindigkeit 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 Konfiguration und -Funktion jeweils vor den einzelnen Testläufen überprüft.