Schnelle Torwächter

Vergleichstest UTM Teil 1 – 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 ersten drei Probanden im Test verhalten haben, steht im vorliegenden Artikel. Teil 2 des Tests folgt dann in der nächsten Ausgabe von Network Computing.

Clavisters SG3210 ist das kleinste System der Clavister-Security-Gateway-3200-Serie. Als Basis dient eine Hardware-Plattform mit sechs Gigabit-Ethernet-Ports. Die einzelnen Modelle unterscheiden sich nach Leistung und Kapazität voneinander. Alle Produkte beinhalten zudem die gleichen Security- und Connectivity-Features, darunter Firewalling, VPN, Intrusion-Detection und -Prevention, Anti-Virus, Anti-Spam, Content-Filtering, High-Availability-Clustering oder Traffic-Management.

Das Clavister-System soll noch nie da gewesene Investment-Protection bieten, basierend auf der Fähigkeit, Performance und Funktionalität durch die Nutzung digitaler Lizenzvergabe auszuweiten. ITK-Verantwortliche können so zwischen Systemanforderungen und finanziellen Ressourcen wählen, ohne dabei für die Zukunft Kompromisse bei der benötigten Performance und Funktionalität einzugehen, so Clavister. Die SG3210 hat nach Herstellerangaben einen auf 350 MBit/s limitierten Datendurchsatz. Über ein Lizenzkey-Upgrade soll es aber möglich sein, das System auf einen Durchsatz von 1000 MBit/s aufzurüsten, ohne dabei die Hardware zu tauschen.

Als Unified-Threat-Management-System ist Funkwerks Packetalarm-UTM2500 eine Kombination aus Firewall, Netzwerk-Intrusion-Prevention-System und Gateway-Virenscanner. Die Box bietet darüber hinaus ein komplettes VPN-Gateway, einen Spamfilter, einen Content-Filter und ein Application-Level-Gateway. Hochverfügbarkeit und Quality-of-Service runden die Feature-Liste ab. Das System ist wahlweise für bis zu 250 User oder unlimitiert erhältlich. Für die Benutzer-Authentifizierung sowohl inband als auch out-of-band stehen neben statischen Listen auch Schnittstellen zu Radius und LDAP zur Verfügung. Außerdem verfügt die Packetalarm-UTM über einen eigenen Zertifikatsserver, um den Umgang mit Zertifikaten zu vereinfachen.

Das Funkwerk-UTM-System soll nach Herstellerangaben in der Regel am Gateway zum Internet eingesetzt werden. Hier kontrolliert es in Echtzeit den ein- und ausgehenden Datenverkehr. Durch seine aufeinander abgestimmten Komponenten soll es Viren, netzwerkbasierte Würmer, dateibasierte Würmer, Trojaner, Spam, Policy-Verletzungen, DoS-Angriffe, Backdoors und andere Hackerangriffe erkennen und verhindern. Somit soll die Packetalarm-UTM-Box die komplette Gateway-Sicherheit abdecken. Die Packetalarm-UTM2500 unterstützt SSL-VPNs. Die Anzahl der VPN-Verbindungen ist softwareseitig nicht limitiert, der dazugehörige SSL-VPN-Client für Windows-Betriebssysteme ist kostenlos. Die Konfiguration des SSL-VPN-Clients erfolgt über eine Konfigurationsdatei, die der Anwender entweder direkt im UTM-System herunterladen kann oder vom Administrator erhält.

Die Gateprotect-Appliance GPX-800 wurde nach Herstellerangaben insbesondere für Netzwerke mit einem erhöhten Anspruch an die Ausfallsicherheit ausgelegt. Gateprotect positioniert die Appliance für Unternehmen mit bis zu 500 Mitarbeitern. Die GPX-800 verfügt über einen aktiv/passiven HA-Modus sowie über redundante Server-Festplatten. Diese Kombination von Redundanz sowie hochwertiger Hardware soll für eine besonders hohe Ausfallsicherheit sorgen. Von den Features her soll die Appliance alle Anforderungen in großen und komplexen Netzwerken abdecken.

Die neue »eGUI«-Technologie von Gateprotect soll sich durch ihre ergonomische Orientierung am Bearbeitungsprozess auszeichnen. Besondere Features sind die Extended-User-Authentication, VPN-Gateway msSL mit X.509 Zertifikaten und IPSec, Traffic-Shaping und QoS, Hochverfügbarkeit und HTTP-Scan. Sie kann auch in verschlüsselten HTTPs-Verbin-

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

dungen den Datenverkehr auf Viren und andere Schadsoftware scannen. Hierfür wird auf der Firewall der Datenstrom entschlüsselt, analysiert und, wenn keine Viren gefunden wurden, anschließend verschlüsselt wieder versandt.

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

Als UTM-System ist Funkwerks Packetalarm-UTM 2500 eine Kombination aus Firewall, IPS und Gateway-Virenscanner.

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 zehn Prozent 100 MBit/s entsprechen 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. Bei allen Messungen mit den Appliances war von Anfang an die gesamte UTM-Funktionalität mit Ausnahme der QoS-Datenpriorisierung aktiviert. Clavisters SG3210 schaffte bei unseren Messungen mit allen Frame-Formaten einen nach unserer Definition maximalen Bruttodurchsatz von 30 Prozent oder 300 MBit/s. Einzige Ausnahme war der Betrieb mit ausschließlich 64 Byte großen Datenpaketen. In diesem Fall waren noch 200 MBit/s drin.

Funkwerks Packetalarm-UTM2500 schaffte ebenfalls einen maximalen Durchsatz von 300 MBit/s. Allerdings war diese Leistung nur mit den beiden größten Frame-Formaten realisierbar. Bei der Messung mit dem Fame-Format 512 Byte lagen dann noch Durchsatzraten von 200 MBit/s an. Im Betrieb mit 256 Byte kleinen Frames waren dann noch 100 MBit/s möglich. Datenströme aus 64-Byte-Paketen drückten den Durchsatz auf unter 100 MBit/s.

Gateprotects GPX-800 schaffte bei den Messungen mit den drei großen Frame-Formaten 100 Prozent und somit Gigabit-Ethernet-Leitungsgeschwindigkeit. Verwendeten wir 256-Byte-Pakete, waren noch 600 MBit/s brutto drin.

TECHNISCHE DATEN FIREWALL/VPN-APPLIANCES *

	Clavister SG3210	Funkwerk UTM 2500	Gateprotect GPX 800
Anzahl unabhängiger (nicht geswitchter) LAN-Ports			
Anzahl Gigabit-Ethernet-Ports	6	6	10
Anzahl Fast-Ethernet-Ports	0	0	0
Anzahl WAN-Ports			
X.21	0	0	0
X.25	0	0	0
ISDN $_{S0}$	0	0	1
ISDN $_{S2M}$	0	0	1
xDSL	6	Ein Ethernet-Port verwendbar	bis zu 6
E1	0	0	0
Hardware/Betriebssystem			
Prozessor (Typ), MHz	k.A.	Intel	Xeon Dual Core 1.86 GHz
Arbeitsspeicher in MByte	k.A.	1024	2048
Betriebssystem Name/Version	Clavister CorePlus 8.90.05	Linux-basiert	Debian 4.0
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)	2	2	8
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	Kaspersky	Kaspersky	●
Website	www.clavister.com	www.funkwerk-ec.de	www.gateprotect.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)

Waren die Frame 64 Byte klein, dann schaffte das Gerät einen Durchsatz von 200 MBit/s brutto.

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, mit 1024-Byte-Paketen auf 20 µs. Mit den größten Frames erhöhte sich die Latency auf 28 µs.

Clavisters SG3210 erreichte bei dieser Messung Latency-Werte zwischen 34 und 114 µs. Dabei lag der niedrigste Werte bei der Messung mit 512-Byte-Paketen an. Die höchste Latency erreichte die Clavister-Teststellung bei der Messung mit den kleinsten Paketen. Bei den größten Frames betrug die Latency 70 µs.

Funkwerks Packetalarm-UTM2500 erreichte bei unserer Messung von 10 Prozent Last mit 256-Byte-Paketen eine Latency von 56 µs. Mit zunehmender Frame-Größe stieg dann hier die Latency auch moderat an, so dass die Funkwerk-Teststellung bei der Messung mit den größten Frames eine Latency von 110 µs erreichte.

Gateprotects GPX-800 schaffte bei unserer Messung mit den kleinsten Frames dagegen auch den geringsten Latency-Wert von 32 µs. Mit zunehmender Frame-Größe stieg dann auch der Messwert für die Latency moderat an und erreichte bei der Messung mit den größten Frames eine Latency von 88 µs.

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.

Clavisters SG3210 kam bei diesem Verfahren auf einen Durchsatz von 380 MBit/s. Die Latency betrug bei dieser Leistung 154 µs. Funkwerks Packetalarm-UTM2500 erreichte in dieser Disziplin einen Durchsatz von 370 MBit/s. Dabei lag die Latency bei 279 µs. Und Gateprotects GPX-800 schaffte das volle GBit/s mit einem Latency-Wert von 299 µs.

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

Die Appliance GPX-800 hat Gateprotect für Netze mit einem erhöhten Anspruch an die Ausfallsicherheit ausgelegt.

normalen Download, bei dem in Upload-Richtung kleine Frames mit den entsprechenden Requests und in Download-Richtung automatisch die größtmöglichen Frames verwendet 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.

Clavisters SG3210 schaffte hier 282 098 beziehungsweise 290 297 Transaktionen und einen maximalen Durchsatz von 360 MBit/s. Funkwerks Packetalarm-UTM2500 erreichte 57 339 und 214 710 Transaktionen und 211 MBit/s beziehungsweise 270 MBit/s. Allerdings konnte die Messung nicht fehlerfrei durch laufen, da die Connection-Capacity nicht ausreichte und ab der Hälfte des Testdurchlaufes keine neuen TCP-Verbindungen mehr aufgebaut werden konnten. Gateprotects GPX-800 erreichte einen Wert von 758 010 Transaktionen und einen maximalen Durchsatz von 960 MBit/s, also auch hier quasi Leitungsgeschwindigkeit.

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.

Clavisters SG3210 schaffte hier 89 749 Transaktionen und erreichte einen Durchsatz von 115 MBit/s. Funkwerks Packetalarm-UTM2500 schaffte hier 5240 Transaktion und einen Durchsatz von 6 MBit/s. Gateprotects GPX-800 erreichte hier 9260 Transaktionen und einen Durchsatz von 11 MBit/s.

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.

Clavisters SG3210 kam hierbei auf eine Latency von rund 70 µs. Griffen zusätzlich die simulierten HTTP-User auf das Netz zu, stieg die Latency auf 400 µs. Funkwerks Packetalarm-UTM2500 kam auf eine Latency von 110 µs für UDP und mit zusätzlichem HTTP-Traffic erhöhte sich die Latency auf 150 µs. Gateprotects GPX-800 erreichte eine Latency ohne HTTP-Last von rund 100 und mit von rund 115 µs.

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.

Über ein Lizenzkey-Upgrade läßt sich Clavisters SG3210 auf 1000 MBit/s aufrüsten, ohne dabei die Hardware zu tauschen.

Bei Clavisters SG3210 waren praktisch keine Unterschiede zwischen den unterschiedlich priorisierten Datenströmen feststellbar. Beide kamen auf eine Latency von rund 380 µs. Funkwerks Packetalarm-UTM2500 erzeugte beim Transport der hoch priorisierten Datenströme eine Latency von 160 µs. Die niedrig priorisierten Datenströme transportierte das System dagegen mit einer Verzögerung von 280 µs. Gateprotects GPX-800 kam bei der gleichen Messung mit hoch priorisierten Datenströmen auf eine Latency von 120 µs. Die niedrig priorisierten Daten hatten dagegen eine Latency von 325 µs.

Fazit

Die Hersteller der UTM-Appliances haben sich viel vorgenommen. Ihre digitalen Torwächter müssen die Daten, die möglichst in Leitungsgeschwindigkeit und mit der gewünschten Übertragungsqualität an ihrem Ziel ankommen sollen, genauestens untersuchen. – Das sollen sie möglichst gründlich machen, aber auch ohne nennenswerte Bearbeitungszeiten zu benötigen. 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 Communications 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 Firewall-Konfiguration und -Funktion jeweils vor den einzelnen Testläufen überprüft.