

Gemeinsam durch den Tunnel



Vergleichstest VPN-Appliances
– Für eine geschützte und zuverlässige Kommunikation zwischen Unternehmenszentrale und Niederlassungen sollen Security-Appliances mit VPN-Funktionalität sorgen.

Im Zeitalter von Unified-Communications müssen Security-Appliances eine ganze Reihe von Anforderungen erfüllen. Ihre Aufgabe lautet nicht nur, mit Hilfe von Verschlüsselungsmechanismen Daten gesichert von A nach B zu schieben. Durch die virtuellen Tunnel, die sie etablieren, laufen klassische Daten, aber auch beispielsweise IP-Telefongespräche oder IP-Videoübertragungen. Und diese Datenströme sind nicht nur schützenswert. Sie stellen auch anspruchsvolle Forderungen an die Qualität der Übertragung. Daher sind auch im VPN heute Mechanismen erforderlich, die für die notwendige »Quality-of-Service« sorgen. Hierzu zählen neben den notwendigen Durchsatzleistungen auch Mechanismen wie Datenpriorisierung oder Bandbreitenmanagement. In unseren Real-World Labs an der FH Stralsund wollten wir aktuelle VPN-Lösungen auf ihre Tauglichkeit für

den Einsatz in Unified-Communications-Umgebungen untersuchen. Für die Entwicklung des Test-Szenarios haben wir wieder auf unsere bewährte Network Computing-Musterfirma zurück gegriffen.

Das Testszenario

Unsere Network Computing-Musterfirma möchte die Unternehmenszentrale und verschiedene Niederlassungen untereinander sowie mit dem Internet verbinden. Geeignete, durchsatzstarke Security-Appliances sollen den Aufbau von VPNs ermöglichen. Um die störungsfreie Übertragung von Real-Time-Applikationen wie VoIP oder Video-over-IP zu gewährleisten sollen die Systeme die geeigneten »Quality-of-Service«-Mechanismen unterstützen. Daraus ergeben sich die folgenden Anforderungen an die Teststellungen.

Ethernet-Appliance für die Zentrale:

- ◆ Eine Appliance inklusive Zubehör und Dokumentation,
- ◆ VPN-Funktionalität wie IPSec oder SSL,
- ◆ Verschlüsselung nach AES mit 256 Bit,
- ◆ je Gerät mindestens vier Ethernet-Ports (RJ45-Stecker),
- ◆ CoS-Mechanismen (Datenpriorisierung) sowie
- ◆ Bandbreitenmanagement (Bandbreitenlimitierung, Bandbreitengarantie).

Ethernet-Appliances für die Niederlassungen:

- ◆ Drei Appliances inklusive Zubehör und Dokumentation,
- ◆ VPN-Funktionalität wie IPSec oder SSL,
- ◆ Verschlüsselung nach AES mit 256 Bit,

- ◆ je Gerät mindestens zwei Ethernet-Ports (RJ45-Stecker),
- ◆ CoS-Mechanismen (Datenpriorisierung) sowie
- ◆ Bandbreitenmanagement (Bandbreitenlimitierung, Bandbreitengarantie).

Folgende Testparameter sollten untersucht werden:

- ◆ Überprüfung der VPN-Funktionalität,
- ◆ Überprüfung der Datenpriorisierung und des Bandbreiten-Managements,
- ◆ VPN-Performance Datendurchsatz,
- ◆ Packet-Loss,
- ◆ Latency sowie
- ◆ Jitter.

Die gesamte Funktionalität musste durch dokumentierte Konfigurationseinstellungen gewährleistet sein, so dass sie auch jedem Anwender zugänglich ist. Um die Transparenz der Tests zu erhöhen sollten alle beteiligten Hersteller die im Test eingesetzte Firmware zur Verfügung stellen. Die Firmware wird nach Veröffentlichung auf der Webseite von Network Computing zusammen mit den Konfigurationsdaten zum Download zur Verfügung gestellt.

Unsere Testausschreibung haben wir dann wieder an die »Üblichen Verdächtigen«, also alle relevanten Hersteller in unserem Verteiler, gesandt. Das Testfeld bildeten letztendlich Clavister »SG12« und »SG3250«, Funkwerk »utm1500« und »utm2500«, Gateprotect »GPO 125« und »GPX 800«, Siemens »4YourSafety RX100S4« und »4YourSafety RX300S3« sowie Underground8 »Limes MF 150« und »Limes MF 500«.

DAS TESTFELD

Appliances für die Niederlassungen

- ◆ Clavister SG12
- ◆ Funkwerk utm1500
- ◆ Gateprotect GPO 125
- ◆ Siemens 4YourSafety RX100S4
- ◆ Underground8 Limes MF 150

Appliances für die Zentrale

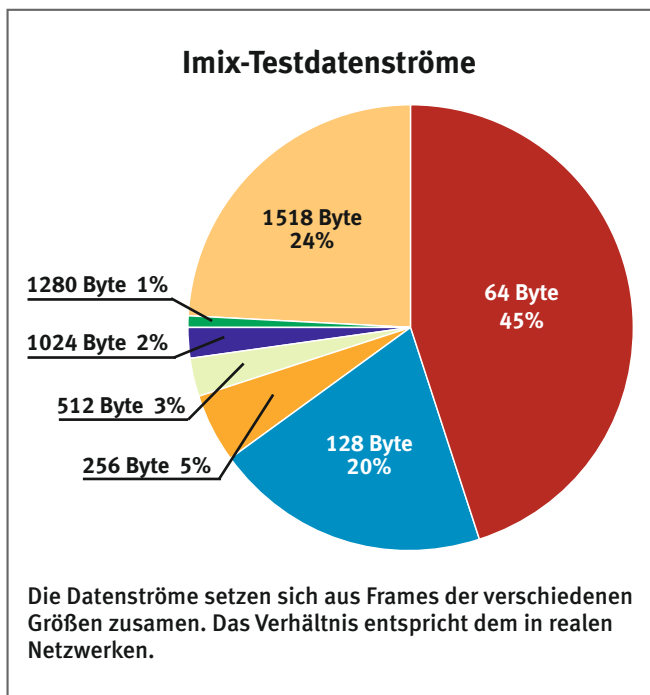
- ◆ Clavister SG3250
- ◆ Funkwerk utm2500
- ◆ Gateprotect GPX 800
- ◆ Siemens 4YourSafety RX300S3
- ◆ Underground8 Limes MF 500

Die Testreihen

Für unsere Messungen haben wir die drei Niederlassungs-Appliances sternförmig mit der Appliance der Zentrale verbunden. Der gesamte Datenverkehr – auch zwischen den einzelnen Niederlassungen – läuft bei einer solchen Topologie grundsätzlich über das System der Zentrale. Eine solche Infrastruktur erhöht zwar die Gesamtdatenlast zum Teil, hat aber verschiedene Vorteile in Sachen System-Management und IT-Sicherheit. Aus diesem Grund ist dieser Aufbau in der Realität häufig anzutreffen. An Stelle der Systeme in den lokalen Netzen der drei Niederlassungen und der Zentrale sendete und empfing der Lastgenerator und Analysator Smartbits von Spirent die entsprechenden Datenströme. Zwischen den einzelnen Appliances bauten wir die VPN-Kanäle auf, durch die wir die Testdatenströme sendeten.

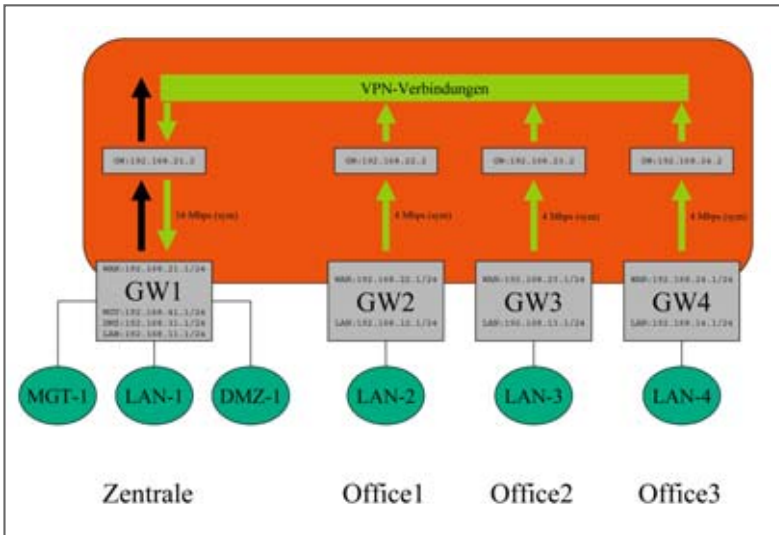
Bidirektionale Imix-Performance

In der ersten Testreihe haben wir ein VPN zwischen »Office 1« und der Zentrale aufgebaut. Dann haben wir in beiden Richtungen gleichzeitig Datenströme gesendet und so den maximal möglichen bidirektionalen Datendurchsatz ermittelt. Als Frame-Formate haben wir eine Imix genannte Mischung aus allen Frame-Größen verwendet, die den Lastmustern realer Umgebungen entspricht.



Dieser Performance-Test ermittelt die Leistungsgrenzen der Niederlassungs-Appliances, die von ihrer Hardware-Ausstattung her natürlich nicht so leistungsfähig sind, wie die Systeme für die Unternehmenszentrale. In unserem Testszenario sind wir davon ausgegangen, dass die maximale Bandbreite der WAN-Verbindung zwischen Office 1 und Zentrale 4 MBit/s im Up- wie im Download beträgt. Gemessen haben wir den maximal möglichen Durchsatz im VPN.

Clavisters Teststellung erreichte einen Durchsatz je Senderichtung von 12 MBit/s. Bidirektional waren daher 24 MBit/s möglich. Funkwerk schaffte mit 22 beziehungsweise 44 MBit/s noch höhere Durchsätze. Gateprotect lag mit 2 mal 17 MBit/s knapp darunter. Und underground8 schaffte bidirektional 46 MBit/s. Eine Leistungsklasse für sich war die Siemens-Teststellung. Sie verfügte über Gigabit-Ethernet-Interfaces und kam bidirektional auf einen VPN-Nutzdatendurchsatz von 220 MBit/s. Ausgehend von unserer Testanforderung erwiesen sich aber alle Teststellungen in unserer ersten Testreihe als mehr als ausreichend.



Die Topologie des Tesaufbaus

Multidirektionale Imix-Performance

In unserer zweiten Testreihe haben wir die möglichen Datendurchsätze »fully meshed« zwischen den drei Niederlassungen und der Zentrale ermittelt. Die multidirektionalen Datenströme setzten sich wieder aus den unterschiedlichen Frame-Formaten im Imix-Verhältnis zusammen. Die drei Niederlassungen bauten zur Zentrale hin jeweils einen Tunnel auf. Durch diese drei Tunnel hinweg sendeten wir multidirektionalen Datenverkehr zwischen der Zentrale und den Niederlassungen hin und her. Dabei sendete die Appliance in der Zentrale an Office 1 bis 3. Die drei Niederlassungs-Systeme sendeten an die Zentrale sowie an die jeweils beiden übrigen Niederlassungen. Je Tunnel ergab das drei Datenströme. Auf diese Weise haben wir den möglichen Gesamtdurchsatz für das Unternehmensnetzwerk ermittelt.

Clavisters Teststellung kam hierbei auf 72 MBit/s. Funkwerk und Gateprotect ermöglichten jeweils einen Gesamtdurchsatz von 102 MBit/s. Underground8 schaffte 132 MBit/s und Siemens kam auf 180 MBit/s. Dass Siemens im Gegensatz zu den anderen Herstellern die Durchsatzleistung gegenüber der ersten Testreihe nicht steigern konnte liegt daran, dass hier die Limits des Systems für die Zentrale erreicht waren. Insgesamt lagen aber alle Teststellungen auch hier deutlich über den Anforderungen unseres Testszenarios.

Bandbreitenmanagement im Upstream

Unsere dritte Testreihe setzt sich aus drei Messungen zusammen. Im ersten Test haben wir die Limitierung der Bandbreite untersucht. Hier bauten wir ein VPN zwischen unserer Zentrale und dem Office 1 auf. Die Datenströme sollten unidirektional von Office 1 an die Zentrale gesendet werden. Dabei sollte die Bandbreite auf 4 MBit/s begrenzt sein, da mehr Daten über unsere WAN-Verbindung nicht gesendet werden können.

Mit Ausnahme der Teststellung von Underground8 war diese Limitierung bei allen Teststellungen darstellbar. Allerdings waren die Ergebnisse bei allen Teststellungen abhängig von den verwendeten Frame-Formaten und zum Teil auch von den Eingangslasten. Je nach willkürlich gewählter Konstellation sah die eine oder andere Teststellung besser oder schlechter aus, so dass hier keine klare Rangreihenfolge dargestellt werden kann.

Im zweiten Test unserer dritten Testreihe haben wir Strict-Priority gefordert. Es galt, vier Prioritäten unter DSCP 0x20/0x60/0xA0/0xE0 beziehungsweise optional UDP 10/20/30/40 einzurichten und grundsätzlich die Daten der niedrigen zu Gunsten der Daten der höheren Prioritäten zu verwerfen. Die Datenströme haben wir unidirektional von Office 1 an die Zentrale gesendet. In vier Lastschritten haben wir dann mit 4, 5, 33, 8 und 16 MBit/s gesendet und so eine maximal vierfache Überlast generiert, da das Office-System maximal 4 MBit/s an die große Appliance schicken konnte. Die Bandbreitenlimitierung war dabei noch eingeschaltet, sie diente als Grundlage dafür, dass die Geräte eine Priorisierung vornehmen mussten. Genau deshalb ist eine genaue Limitierung wichtig. Die notwendigen Datenverluste sollten dann zu Lasten der jeweils niedrigsten Priorität gehen. Das bedeutet bei 25 Prozent Frame-Loss Totalverlust der niedrigsten Priorität, bei 50 Prozent Frame-Loss Verlust der beiden niedrigen Prioritäten und bei 75 Prozent Frame-Loss Verlust aller Prioritäten bis auf die höchste.

Mit der Siemens-Teststellung war dieses Verhalten abbildbar. Allerdings ging das nur mittels entsprechender Konfiguration der WFQ-Funktionalität, die eigentlich nicht für Strict-Priority, sondern für das Weighted-Fair-Queuing gedacht ist. Die Funkwerk-Teststellung beherrschte diesen Mechanismus, wenn wir fest Frame-Formate von 512 Byte verwendeten. Nutzen wir Imix-Datenströme, kam es zu ungenauen Messergebnissen. Auch bei Clavister gab es Abhängigkeiten des Verhaltens im Zusam-

menhang mit der Frame-Size. Die Teststellung von Gateprotect arbeitete inkonsistent und das System von Underground8 ließ sich nicht von seiner Aufgabe überzeugen.

In einem dritten Test wollten wir dann den verschiedenen Prioritäten Bandbreitengarantien von jeweils 0,5 MBit/s einräumen. Die Daten der höchsten Priorität sollten so lange frei von Verlusten bleiben, wie dies möglich ist. Diese Aufgabe war mit keiner der fünf Teststellungen erfüllbar. Die Gründe hierfür liegen soweit nachvollziehbar teils im Design, teils in Produktschwächen. So waren große Schwankungen in den Messergebnissen in Abhängigkeit von den Frame-Formaten feststellbar.

Bandbreitenlimitierung

In unserer vierten Testreihe haben wir dann die großen Appliances für die Zentrale in einer Zangenmessung untersucht. Das jeweilige System sollte mit maximaler Leistung ins Internet senden aber dabei die 16 MBit/s-WAN-Anbindung

Appliances für die Niederlassungen



Clavister SG12



Funkwerk utm1500



Gateprotect GPO 125



Siemens 4YourSafety RX100S4



Underground8 Limes MF 100

TECHNISCHE DATEN

VPN-APPLIANCES FÜR NIEDERLASSUNGEN UND ZENTRALE *

	Appliances für die Niederlassungen					Appliances für die Zentrale				
	Clavister SG12	Funkwerk UTM 1500	Gateprotect GPO 125	Siemens 4YourSafety RX100S4	Underground8 Limes MF 150	Clavister SG3250	Funkwerk UTM 2500	Gateprotect GPX 800	Siemens 4YourSafety RX300S3	Underground8 Limes MF 500
Anzahl unabh. (nicht geswitchter) LAN-Ports	0	0	0	4	0	6	6	8	6	4
Anzahl Gigabit-Ethernet-Ports	3	4	3	0	4	0	0	0	0	0
Anzahl Fast-Ethernet-Ports										
Anzahl WAN-Ports										
X.21	0	0	0	0	0	0	0	0	0	0
X.25	0	0	0	0	0	0	0	0	0	0
ISDN _{S0}	0	0	0	0	0	0	0	0	0	0
ISDN _{S2M}	0	0	0	0	0	0	0	0	0	0
xDSL	3	0	3	0	0	6	0	4	0	0
E1	0	0	0	0	0	0	0	0	0	0
Hardware/Betriebssystem										
Prozessor (Typ), GHz	k.A.	Pentium M 1,2 GHz	Via 1 GHz	Xeon 3040 DC 1,86 GHz	Celeron 2 GHz	k.A.	Pentium 4 2,8 GHz	Xeon 1,86 GHz	Xeon 5335 QC 2,00 GHz	Pentium 4 3,4GHz
Arbeitsspeicher in MByte	k.A.	512	512	1024	1024	k.A.	1024	2048	2048	4096
Betriebssystem Name/Version	Clavister CorePlus 8.90.00	Funkwerk PASOS	Debian 4.0	Check Point Sec.Platform NGX R65	Limes OS / 71	Clavister Core Plus 8.90.00	Funkwerk PASOS	Debian 4.0	Check Point Sec.Platform NGX R65	Limes OS / 71
IPv6-Unterstützung für alle Firewall-Funkt.	○	○	○	●	○	○	○	○	●	○
Firewall-Technik										
Stateful-Inspection-Firewall	●	●	●	○	●	●	●	●	●	●
Layer-7-Application-Gateway-Proxies	●	●	●	○	●	●	●	○	○	●
anpassbare Proxies	●	●	●	○	●	●	●	○	○	●
Stateful-Inspection und Proxy kombiniert	●	○	●	○	●	●	●	○	○	●
transp. Firewallfunktionalität konfigurierbar	●	○	●	○	●	●	●	○	○	●
spezielle Firewall-ASICs integriert	○	○	○	○	○	○	○	○	○	○
Proz. 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)	0	2	0	8	2	2	2	0	8	2
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	○	○	○	○	○	○	○	○	○	○
Synchr. 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 korreliert einz. Einträge	○	○	○	○	○	○	○	○	○	○
Authentisierung/Autorisierung										
NT-Domain	○	○	○	○	○	○	○	○	○	○
TACACS/TACACS+	○	○	○	○	○	○	○	○	○	○
Radius	○	○	○	○	○	○	○	○	○	○
LDAP über TLS	○	○	○	○	○	○	○	○	○	○
X.509-digitale Zertifikate	○	○	○	○	○	○	○	○	○	○
Token-basierend	○	○	○	○	○	○	○	○	○	○
Sicherheitsfeatures										
DMZ	○	○	○	○	○	○	○	○	○	○
Intrusion-Detection/-Prevention	○	○	○	○	○	○	○	○	○	○
AAA-Support	○	○	○	○	○	○	○	○	○	○
DHCP	○	○	○	○	○	○	○	○	○	○
NAT-Support	○	○	○	○	○	○	○	○	○	○
Content-Filter	○	○	○	○	○	○	○	○	○	○
Virens Scanner	○	○	○	○	○	○	○	○	○	○
Listenpreis in Euro für Teststellung zzgl. MwSt. (**)	495	1099	2605	6528	1490	9995	5999	4305	13741	5490
Website	www.clavister.com	www.funkwerk-ec.com/utm	www.gateprotect.de	www.siemens.de/it-solutions/4ys	www.underground8.com	www.clavister.com	www.funkwerk-ec.com/utm	www.gateprotect.de	www.siemens.de/it-solutions/4ys	www.underground8.com

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)

** Eine Appliance (Hard- und Software) inkl. Lizenzen für 100 User und vollständiger Managementlösung

nach draußen nicht überlasten. Daher sollte eine Bandbreitenlimitierung auf 16 MBit/s eingerichtet werden.

Eine exakte Limitierung war mit keinem der getesteten Systeme möglich. Dabei war das Verhalten der Systeme von den verwendeten Frame-Formaten abhängig. Mit großen Formaten kamen die Systeme vergleichsweise gut zurecht. Verwendeten wir kleinere Formate, stieg das Limit in der Regel auf Werte an die 20 MBit/s an. Dabei war das Verhalten des Clavister-Systems lastabhängig. Und die Lösung von Underground8 arbeitete auch hier nicht korrekt.

Bandbreitenmanagement im Downstream

Unsere fünfte Testreihe entspricht der dritten. Allerdings musste nun die Appliance der Zentrale unidirektional an Office 1 senden. Da die WAN-Anbindung von Office 1 eine Bandbreite von 4 MBit/s haben sollte, sollte die Zentrale maximal mit dieser Leistung an Office 1 senden. Die restlichen 12 MBit/s an WAN-Bandbreite, die der Zentrale in unserem Szenario zur Verfügung steht, sollte für den unidirektionalen Datentransfer ins Internet zur Verfügung stehen. In einem ersten Test sollten die Bandbreiten entsprechend diesen Vorgaben limitiert werden, um eine Überlastung der WAN-Verbindung zu vermeiden.

Die Teststellungen von Clavister, Gateprotect und Siemens erfüllten diese Vorgaben weitgehend, wenn auch nicht ganz präzise. Das System von Funkwerk arbeitete hier inkonsistent und die Underground8-Teststellung bot nicht genügend Klassen in ihrer Klassenhierarchie.

Im zweiten Test unserer fünften Testreihe galt es wieder wie in der dritten Testreihe oben vier Prioritäten zu unterscheiden und gemäß den Regeln der Strict-Priority bei entsprechenden Überlasten zu verwerfen. Bei der Siemens-Teststellung war dieses Verhalten durch den Umweg über die WFQ-Funktionalität möglich. Auch Gateprotect arbeitete weitgehend korrekt. Clavister realisierte das geforderte Verhalten, hatte aber Probleme mit den 1518 Byte großen Frames, die anscheinend nicht durch den Tunnel kamen. Funkwerk und Underground8 waren hier aus oben genannten Gründen nicht sinnvoll einsetzbar.

Im dritten Test wollten wir dann wie oben den verschiedenen Prioritäten Bandbreitengarantien von jeweils 0,5 MBit/s einräumen. Die Daten der höchsten Priorität sollten so lange frei von Verlusten bleiben, wie dies technisch möglich ist. Bei Clavister funktionierte designbedingt die Priorisierung nicht zusammen mit der Bandbreitengarantie. Bei Funkwerk war die gewünschte Funktionalität nicht über das GUI abzubilden. Die Gateprotect-Lösung ermöglichte es nicht, Bandbreitengarantien für Unterklassen einzurichten. Die Siemens-Teststellung lieferte hier dann auch keine Priorisierung mehr. Und bei Underground8 gab es wie gesagt nicht genügend Klassen.

Bandbreitenmanagement mit Strict-Priority

In unserer sechsten und letzten Testreihe haben die Appliances von Office 1 und von Office 2 Datenströme der höchsten Priorität an die Appliance der Zentrale gesendet. Gleichzeitig haben wir einen Datenstrom mit der maximalen Portgeschwindigkeit, also 100 beziehungsweise 1000 MBit/s, von der DMZ an das LAN der Zentrale gesendet. Gemäß den Strict-Priority-Regeln sollte die Appliance der Zentrale die Daten der beiden Niederlassungen unbeschadet passieren lassen und so viele Daten aus der DMZ wie notwendig verwerfen.

Funkwerk, Gateprotect und Siemens haben diesen Test erfolgreich absolviert. Clavister arbeitete bis 50 MBit/s Last korrekt, dann waren anscheinend die Grenzen der Queue erreicht. Mit dem System von Underground8 war keine QoS-Priorisierung auf LAN-Interfaces möglich.

Fazit

Was in Broschüren und auf Datenblättern so einfach aussieht hat sich in unseren Real-World Labs als sehr anspruchsvoll erwiesen. Grundsätzlich sind alle Systeme im Testfeld für das geplante Szenario mehr oder weniger einsetzbar. Allerdings ist es notwendig, das Verhalten der einzelnen Kandidaten genau zu kennen.

Clavisters Teststellung zeigte, dass damit Limitierung, Priorisierung sowie Bandbreitengarantien realisierbar sind. Gleiches gilt für die Hierarchien von Pipes. Designbedingt sind aber Priorisierung und Bandbreitengarantie nicht kombiniert einsetzbar. Dabei waren die Messergebnisse stark lastabhängig.

Auch Funkwerks Teststellung funktioniert, hat aber ihre Eigenheiten. So erhielten wir teilweise inkonsistente Ergebnisse. Dabei läuft die QoS-Funktionalität auf einem externen Interface, nicht auf dem IPsec-Interface. Der QoS-Test ohne IPsec über das WAN-Interface lief einwandfrei. Das Testszenario des dritten Tests in der fünften Testreihe war über das GUI nicht abzubilden.

Auch mit der Teststellung von Gateprotect waren Limitierung und Priorisierung realisierbar. Die Ergebnisse waren aber nicht immer konsistent und reproduzierbar. Eine Garantie für die einzelnen Prioritäten kann mit der Lösung von Gateprotect nicht abgebildet werden, sondern nur für die übergeordnete Hauptklasse.

Die Lösung von Siemens mit der Checkpoint-Software erwies sich als sehr performant, war

aber wohl für unser Testszenario etwas überdimensioniert. Eine direkte Priorisierung ermöglicht sie nicht. Statt dessen war der Umweg über die Gewichtung der Dienste nach WFQ erforderlich. Arbeiteten wir hier mit Bandbreitengarantien, war keine »WFQ-Priorisierung« mehr möglich.

Mit der Teststellung von Underground8 war es nicht möglich, vier Klassen abzubilden, da nur drei fest eingestellt waren. Eine Priorisierung der Klassen war im Test nicht möglich. Die Einstellungen der Bandbreitenparameter »min/max« erwies sich als quasi auswirkunglos. Eine vollständige Abbildung des Testszenarios war daher nicht möglich.

Generell hat sich gezeigt, dass bei den aktuellen getesteten Systemen viele Möglichkeiten und unterschiedliche Konzepte vorhanden sind, um Bandbreitenmanagement und QoS abzubilden. Dies geschieht mit, ohne oder mit bedingter Priorität und Garantien. Lediglich die Bandbreitenlimitierung scheint relativ einfach realisierbar. Die Genauigkeit, mit der die Systeme arbeiteten, hing aber vom Netzwerkverkehr, den durchschnittlichen Paketgrößen und den auftretenden Lasten ab. Nicht immer war eine Klassifizierung über DSCP möglich. Alternativ muss diese dann aufwendig über Portnummern konfiguriert werden. Praktisch bei jedem Hersteller war ein Austesten der Konfiguration mit wiederholten Messungen notwendig, um das erwartete Verhalten zu erreichen. Grundsätzlich gilt, dass die geforderte Technologie im Prinzip vor-

Appliances für die Zentrale



Clavister SG3250



Funkwerk utm2500



Gateprotect GPX 800



Siemens 4YourSafety RX300S3



Underground8 Limes MF 500

TESTVERFAHREN VPN-APPLIANCES

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 teure 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. 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. 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 einzelnen Tests vorhergehenden Kontrollmessungen volle Leitungsgeschwindigkeit 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 VPN-Konfiguration und -Funktion jeweils vor den einzelnen Testläufen überprüft.



handen ist. Das Gros der Systeme auf dem Markt basiert ohnehin auf Linux und in Linux sind alle notwendigen Funktionalitäten sauber abgebildet. Probleme entstehen einerseits durch Einschränkungen seitens der Hardware und andererseits durch die GUIs. Die im Testszenario gewünschte Konfiguration erwies sich als nicht trivial. So hat bei keinem System im Test die Konfiguration ad hoc funktioniert, und das trotz Betreuung der Systeme durch Experten der Hersteller selbst. Unser Vergleichstest hat gezeigt, dass das gewünschte sichere Unified-Communications-Szenario technisch realisierbar ist. Die Anpassung an die individuellen Gegebenheiten ist allerdings sehr anspruchsvoll. Sie erfordert umfangreiches Produktwissen wie auch die messtechnische Überprüfung der Einstellungen im Labor und Probebetrieb.

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