© Peps / PIXELIO

Schneller durch den Tunnel

Vergleichstest Security-Appliances – Spezialisierte Systeme mit Sicherheitsfunktionalität ermöglichen eine geschützte Kommunikation. Ein Test klärt, ob solche Systeme den Anforderungen von Unified-Communicatiions gewachsen sind.

Die Network Computing-Musterfirma möchte drei Niederlassungen mit rund 20 Arbeitsplätzen mit der Unternehmenszentrale und dem Internet verbinden. Geeignete, durchsatzstarke Security-Appliances sollen den Aufbau von VPNs ermöglichen. Für die Realisierung der klassischen Datenanbindung und gleichzeitige Nutzung von Real-Time-Applikationen wie VoIP oder Video-over-IP sollen die Systeme geeignete Priorisierungsmechanismen unterstützen. Ein Vergleichstest sollte die Produktauswahl unterstützen. Aus dem Testszenario ergeben sich folgende Anforderungen an die Teststellungen.

Ethernet-Appliance für die Zentrale:

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

Ethernet-Appliances für die Niederlassungen:

- Drei Appliances inklusive Zubehör und Dokumentation,
- VPN-Funktionalität (IPSec, SSL),
- Verschlüsselung nach AES mit 256 Bit,
- je Gerät mindestens zwei Ethernet-Ports (RJ45-Stecker),
- CoS-Mechanismen (Datenpriorisierung) sowie
- Bandbreitenmanagement (Bandbreitenlimitierung).

Folgende Testparameter wollten wir untersuchen:

- Überprüfung der VPN-Funktionalität,
- Überprüfung der Datenpriorisierung und des Bandbreiten-Managements,
- VPN-Performance: Datendurchsatzraten (unidirektional/bidirektional),
- Packet-Loss,
- Latency sowie
- Jitter.

Die gesamte Funktionalität sollte durch dokumentierte Konfigurationseinstellungen gewährleistet sein, so dass sie auch jedem Anwender zugänglich ist.

REPORTCARD SECURITY-APPLIANCES

	Gewichtung	Clavister SG3200 / SG50	Gateprotect GPX800 / GPA400	Securepoint RC 300 / RC 100
Firewall-Duchsatz	30%	5	5	5
VPN_Durchsatz	30%	5	5	5
Bandbreitenlimitierung	10%	5	4,5	4,5
CoS-Datenpriorisierung	10%	3	5	1
Bandbreitenlimitierung im VPN	10%	5	3	1
CoS-Datenpriorisierung im VPN	10%	5	1	1
	100%	**4,8**	**4,35**	**3,75**
		A +	**A -**	**B**

A› 4,3; B› 3,5; C› 2.5; D› 1,5; E‹1,5;

Die Bewertungen A bis C enthalten in ihren Bereichen + oder -; Gesamtergebnisse und gewichtete Ergebnisse basieren auf einer Skala von 0 bis 5.

network Computing Referenz

DAS TESTFELD

Zentrale
- Clavister SG3200
- Gateprotect GPX800
- Securepoint RC 300

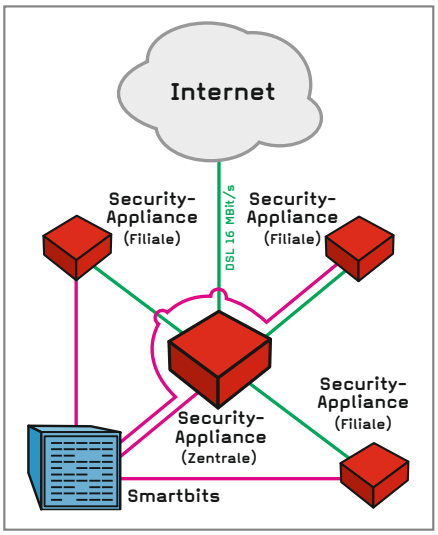
Niederlassungen
- Clavister SG50
- Gateprotect GPA400
- Securepoint RC 100

Die Topologie

In den Räumen der Unternehmenszentrale stehen alle zentralen Ressourcen des Musterunternehmens. Hier befinden sich die Server aber auch der zentrale Übergang ins Internet. Eine »große« Security-Appliance sollte hier für die notwendige Sicherheit aber auch die entsprechend performanten Verbindungen sorgen. Die LANs der drei externen Niederlassungen waren jeweils mit einer »kleinen« Security-Appliance abzusichern. Die Kommunikation der Niederlassungen mit der Zentrale, der Niederlassungen untereinander sowie aller Stellen mit dem Internet sollte zentral über die Infrastruktur der Unternehmenszentrale laufen. Die Verbindung von der Zentrale ins Internet erfolgte mit einer 16-MBit/s-Leitung. Die einzelnen Niederlassungen waren mit 4 MBit/s angebunden. Die Security-Appliances sollten die einzelnen Standorte mittels ihrer Firewall-Funktionalität absichern. Eine gesicherte Kommunikation zwischen den einzelnen Standorten sollte via VPN erfolgen.

Firewall-Durchsatz

Zunächst wollten wir wissen, wie viel Durchsatz die Appliances im Firewall-Betrieb schaffen. Dazu haben wir die verschiedenen Geräte für die Zentrale einzeln einer Zangenmessung unterzogen. Hierzu haben wir mit unserem Lastgenerator/Analysator Smartbits Datenströme generiert und so einen Fully-Meshed-Betrieb zwischen dem LAN und der DMZ der Zentrale und dem Internet simuliert. Zum Einsatz kamen Gigabit-Ethernet-Ports.



Topologie des VPN-Tests

Clavisters SG 3200 erreichte bei dieser Messung einen Gesamtdurchsatz von 390 MBit/s. Gateprotects GPX800 lag mit 1320 MBit/s noch

Clavister SG3200

Clavister SG50

deutlich höher. Und Securepoints RC-300 schaffte volle 1500 MBit/s.

In einer zweiten Messreihe haben wir dann die Performance für die Niederlassungsgeräte ermittelt. Dabei haben wir bidirektionalen Datenverkehr zwischen LAN und WAN simuliert. Hierzu haben wir wieder unseren Lastgenerator/Analysator Smartbits eingesetzt. Clavisters drei SG50 erreichten maximale Durchsatzraten von 134 bis 136 MBit/s. Gateprotects GPA400 lagen zwischen 106 und 108 MBit/s. Securepoints RC 100 lagen mit 102 bis 106 MBit/s praktisch gleich auf.

Auch wenn die Firewall-Performance in keinem der Fälle die Leitungsgeschwindigkeit annähernd erreichte lagen die möglichen Durchsatzwerte doch in Regionen, die klar machen, dass im vorliegenden Einsatz-Szenario keine Engpässe entstehen sollten.

VPN-Durchsatz

Thema des zweiten Tests war der VPN-Durchsatz. Zunächst haben wir den Datendurchsatz zwischen dem LAN der Zentrale und den drei LANs der Niederlassungen ermittelt. Hierzu haben wir bidirektionale Datenströme zwischen der Appliance für die Zentrale und nacheinander den drei baugleichen Appliances der drei Niederlassungen erzeugt und die maximale Durchsatzrate gemessen.

Clavisters Teststellung kam hier auf Durchsatzraten zwischen 20 und 22 MBit/s. Gateprotects Appliances lagen mit 18 MBit/s knapp dahinter. Securepoints Teststellung war mit 36 MBit/s klar schneller.

Gateprotect GPX800

Dann haben wir gleichzeitig Daten von allen drei Niederlassungen an das LAN der Zentrale gesendet und den Gesamtdurchsatz dieser unidirektionalen Datenströme ermittelt.

Clavisters Testaufbau kam hierbei auf einen Gesamtdurchsatz von 63 MBit/s. Gateprotects Lösung erreichte einen Gesamtdurchsatz von 15 MBit/s. Securepoints Teststellung lag mit 99 MBit/s deutlich höher. Dann haben wir Datenströme von allen drei Niederlassungen an die jeweils zwei anderen gesendet. Auf Grund der Netzwerktopologie mussten alle diese Datenströme über die Appliance der Zentrale geleitet werden.

Clavisters Teststellung schaffte hierbei einen Gesamtdurchsatz von 72 MBit/s. Gateprotects Lösung war auch bei dieser Messung mit 30 MBit/s langsamer. Securepoints Appliances schafften einen kumulierten Durchsatz von 108 MBit/s.

Gateprotect GPA400

Auch wenn der VPN-Durchsatztest deutliche Unterschiede zwischen den Teststellungen zutage gefördert hat sind doch auch die Durchsatzwerte der langsamsten Appliances für das bestehende Szenario noch völlig ausreichend. Der Flaschenhals ist und bleibt das WAN selbst.

Bandbreitenlimitierung

Im nächsten Test haben wir die Bandbreitenlimitierung auf korrekte Funktion getestet. Dabei haben wir zunächst Datenströme aus dem LAN der Zentrale ins Internet gesendet. Die Bandbreite haben wir auf 16 MBit/s festgesetzt. Dann haben wir aus dem LAN der Niederlassung Datenströme ins Internet gesendet und die Bandbreite auf 4 MBit/s begrenzt.

Clavisters Teststellung kam auf exakt 16 beziehungsweise 4 MBit/s. Für die Appliances von Gateprotect und Securepoint ermittelten wir Durchsätze von 17 und 4 MBit/s.

CoS-Datenpriorisierung

Dann haben wir Datenströme in vier verschiedenen Prioritäten vom LAN der Zentrale ins WAN gesendet. Auf Grund des Lastmusters sollte die entsprechend belastete Appliance die Datenströme der höchsten Priorität auf alle Fälle verlustfrei übermitteln.

Securepoint RC 300

Clavisters Teststellung verlor 50 Prozent der Daten in der höchsten Priorität, obwohl dies theoretisch nicht erforderlich gewesen wäre. Gateprotects Teststellung beherrschte diese Disziplin dagegen fehlerfrei. Die Appliances von Securepoint erlaubten es nicht, die Datenpriorisierung in Verbindung mit der Bandbreitenlimitierung zu konfigurieren.

Den gleichen Test wiederholten wir mit dem Unterschied, dass die Datenströme nun aus dem Niederlassungs-LAN via Zentrale und WAN gesendet wurden.

In diesem Szenario arbeitete Clavisters Teststellung fehlerfrei. Die Appliances von Gateprotect erfüllten auch diese Aufgabe korrekt. Securepoints Geräte ließen sich auch hier nicht wie erforderlich konfigurieren.

Bandbreitenlimitierung im VPN

Im nächsten Test haben wir dann die Bandbreiten im VPN auf 4 MBit/s je Niederlassung limitiert. Für die Appliance der Zentrale galt ein Limit von 12 MBit/s. Dann haben wir Datenströme aus der Zentrale zugleich an alle drei Niederlassungen gesendet. In einer zweiten Messung haben wir Datenströme vom LAN der Zentrale an das LAN der Niederlassung 1 gesendet. In

Securepoint RC 100

einer dritten Messung gingen die Datenströme vom LAN der Niederlassung an das LAN der Zentrale. mClavisters Appliances beherrschten diese Disziplin perfekt. Sendete die Zentrale an alle drei Niederlassungen, betrug der Datendurchsatz wie konfiguriert 12 MBit/s. Kommunizierte die Zentrale mit einer Niederlassung, betrug der Datendurchsatz wie vorgesehen 4 MBit/s. Bei der Gateprotect-Teststellung musste die Priorisierung für einen Dienst festgelegt werden. So war es möglich die Bandbreite in der ersten Messung auf 11 MBit/s zu reduzieren. Dann gab es Probleme mit der Konfiguration der für die nächste Messung notwendigen Bandbreitenlimitierung. Ähnliche Probleme gab es auch bei der Messung mit der Securepoint-Teststellung. Auch hier war es nicht möglich, die erforderliche hierarchische Bandbreitenlimitierung vorzunehmen.

CoS-Datenpriorisierung im VPN

Danach haben wir Datenströme in vier verschiedenen Prioritäten via VPN vom LAN der Zentrale ins WAN gesendet. Auf Grund des Lastmusters sollte die entsprechend belastete Appliance die Datenströme der höchsten Priorität auf alle Fälle verlustfrei übermitteln.

Clavisters Teststellung beherrschte auch diese Disziplin fehlerfrei und leistete sich keine Datenverluste in der höchsten Priorität. Bei der Gateprotect-Teststellung gab es dagegen wieder Probleme mit der Konfiguration. Und auch mit der Teststellung von Securepoint war dieser Modus nicht darstellbar.

Fazit

Der Flaschenhals war bei unserem Testaufbau nicht die Security-Appliance, sondern das WAN selbst. Was die reine Performance angeht zweigten sich die Teststellungen als mehr als ausreichend leistungsfähig. Komplizierter wurde es dagegen, wenn wir Bandbreitenmanagement, Datenpriorisierung und VPN sinnvoll kombinieren wollten. Nur Clavister beherrschte diese Kombination vollständig, wenn auch mit kleinen Einschränkungen bei der Datenpriorisierung unter höherer Last. Hier haben die anderen Hersteller ihre Hausaufgaben noch nicht vollständig erledigt, da nicht alle geplanten Szenarien konfiguriert werden konnten.

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

TESTVERFAHREN

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. Verwendet haben wir Datenströme im Imix-Format. Diese setzen sich aus Frames aller möglichen Größen zusammen und entsprechen der Zusammensetzung realer Umgebungen. Die Performance- und Class-of-Service-Eigenschaften der Systeme im Testfeld haben wir in verschiedenen Testreihen gemäß RFC 2544 gemessen.