Sicher im Flaschenhals

Vergleichstest Security-Appliances – Für die notwendige Sicherheit im Netz sorgen spezialisierte Systeme mit Firewall-, VPN- oder auch IPS-Funktionalität.

Eine sichere aber auch schnelle Kommunikation zwischen einem internen Netzwerk – beispielsweise einem Unternehmensnetz oder einem besonders zu schützenden Segment eines solchen – und einem externen Netzwerk – beispielsweise dem Internet aber auch anderen Segmenten des eigenen Unternehmensnetzes – sollen Security-Appliances ermöglichen. Solche Systeme vereinen Firewall, VPN und/oder IPS auf einer Hardware-Plattform.

Eine Security-Appliance ist eine aktive Netzwerkkomponente, wie ein Switch oder ein Router, die nicht nur die Kommunikation zwischen zwei Netzwerken oder Netzwerksegmenten ermöglicht, 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, xDSL, Mietleitungen, Datendirektverbindungen, Standleitungen oder X.25, angeschlossen sein. Platziert werden Security-Appliances 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 oder benachbarte LAN-Segment ermöglicht. Hierfür bieten solche Appliances heute Fast-Ethernet- und – in der Oberklasse – auch Gigabit-Ethernet-Ports an. Manche Systeme stellen darüber hinaus auch eigene 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 und innen erreichbar sein müssen.

Mit zunehmender Komplexität der heutigen Unternehmensnetze und in Anbetracht der Erkenntnisse, 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 Security-Appliances gesichert sind. Durch die Integration dieser Systeme in das Unternehmensnetz muss nun aber nicht nur der Datenverkehr intern – extern, sondern auch ein Großteil des internen Datenverkehrs das entsprechende System passieren. In Anbetracht der Datenmengen, der Qualitätsanforderungen in heutigen konvergenten Netzen mit ihren Voice- und Video-Applikationen 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 auch 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, wie LAN-Switches, gestellt werden.

Unabhängig vom individuellen Konzept arbeiten die Firewall-Systeme auf den Appliances generell 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 entkoppeln die Netzwerke physikalisch wie logisch und können beispielsweise von jedem Be-

nutzer Identifikation und Authentisierung 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-Funktionaltät.

Firewalls bestehen aus Hard- und Softwarekomponenten, die häufig von unterschiedlichen Herstellern stammen und individuell kombiniert werden. Bei den Security-Appliances, die Firewall-Funktionalität bieten, 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/Prevention 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. Um das Preis-Leistungverhältnis entsprechend zu würdigen haben wir darüber hinaus unseren Preis-Performance-Index ermittelt.

VPN inklusive

Neben der klassischen Firewall-Funktionalität gehört der Aufbau von VPNs zur Standardfunktionalität von Security-Appliances. Virtuelle private Netzwerke, neudeutsch Virtual-Private-Networks oder kurz VPN, sollen einer geschlossenen Gruppe von Rechnern eine geschützte Kommunikation über ein potentiell unsicheres Netz hinweg erlauben. Die logisch geschlossene Verbindung, auch VPN-Tunnel genannt, wird durch kryptografische Algorithmen realisiert, die die zu schützenden Datenströme verschlüsseln und an der Gegenstelle wieder entschlüsseln. Für diese Verschlüsselung gibt es eine ganze Reihe von Standards, wie DES, 3DES

oder AES. Über die Sicherheit solcher Verbindungen entscheidet wie bei anderen kryptografischen Verfahren auch nicht zuletzt die Länge der verwandten Schlüssel. Mechanismen wie Authentisierung und Autorisierung sorgen zusätzlich dafür, dass keine unerwünschten User in das private Netz eindringen. Technisch realisieren Unternehmen ein solches VPN, indem sie an den Übergangsstellen zwischen sicherem und unsicherem Netzwerk ein VPN-System installieren.

Die wesentliche Verschlüsselungsfunktionalität ist zumeist in Software abgebildet, was bedeutet, dass die Funktionalität sehr rechenintensiv ist und eine gute Performance eine entsprechend leistungsfähige Hardware voraussetzt. Es gibt aber auch VPN-Lösungen, die Hardware-näher realisiert sind und dann entsprechend leistungsfähiger sein können.

Auswirkungen von Datenverlusten

Für die Beurteilung des Verhaltens der Systeme im Testfeld, die wir mit Datenströmen bestehend aus den unterschiedlichsten Frame-Formaten belastet haben, ist es von besonderem Interesse, zu betrachten, welche Lasten und Frame-Größen in realen Netzen vorkommen. Bei klassischen Dateitransfers arbeitet das Netzwerk mit möglichst großen Datenrahmen. Bei Echtzeit-Applikationen teilt sich das Feld. Video-Übertragungen nutzen ähnlich den Dateitransfers relativ große Datenrahmen. Voice-over-IP bewegt sich dagegen im Mittelfeld. Messungen mit Ethernet-LAN-Phones der ersten Generation in unseren Real-World Labs haben beispielsweise ergeben, dass diese Voice-over-IP-Lösung die Sprache mit konstant großen Rahmen von 534 Byte überträgt, ein aktuelles SIP-Phone überträgt 214 Byte große Rahmen. Aktuelle Lösungen überlassen es dem IT-Verantwortlichen selbst festzulegen, mit welchen Frame-Größen die Systeme arbeiten sollen. Dabei sollte der IT-Verantwortliche berücksichtigen, dass der Paketierungs-Delay mit kleiner werdenden Datenrahmen kleiner wird. Dagegen wächst der Overhead, der zu Lasten der Nutzdatenperformance geht, je kleiner die verwendeten Pakete sind. Generell kann man bei der IP-Sprachübertragung davon ausgehen, dass kleine Frames verwendet werden. Die meisten Web-Anwendungen nutzen mittelgroße Datenrahmen. Die kleinstmöglichen Frames von 64 Byte sind dagegen beispielsweise bei den TCP-Bestätigungspaketen oder interaktiven Anwendungen wie Terminalsitzungen zu messen.

Die Analyse der Verteilung der Framegrößen, die für das NCI-Backbone dokumentiert ist, sowie die Ergebnisse der Analyse typischer Business-DSL-Links haben ergeben, dass rund 50 Prozent aller Datenrahmen in realen Netzwerken 64 Byte groß sind. Die übrigen rund 50 Prozent der zu transportierenden Datenrahmen streuen über alle Rahmengrößen von 128 bis 1518 Byte. Für die Übertragung von Real-Time-Applikationen ist zunächst das Datenverlustverhalten von entscheidender Bedeutung. Für Voice-over-IP gilt beispielsweise: Ab 5 Prozent Verlust ist je nach Codec mit deutlicher Verschlechterung der Übertragungsqualität zu rechnen, 10 Prozent führen zu einer massiven Beeinträchtigung, ab 20 Prozent Datenverlust ist beispielsweise die 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. Auf Grund ihrer Bedeutung für die Übertragungsqualität haben wir daher das Datenrahmenverlustverhalten als K.O.-Kriterium für unsere Tests definiert. Die Parameter Latency und Jitter sind dann für die genauere Diagnose und weitere Analyse im Einzelfall wichtig. Sind jedoch die Datenverlustraten von Hause aus schon zu hoch beziehungsweise die maximal möglichen Durchsätze zu gering, können gute Werte für Latency und Jitter die Sprachqualität auch nicht mehr retten. Dafür, dass es zu solchen massiven Datenverlusten im Ethernet-LAN erst gar nicht kommt, sollen entsprechend gut funktionierende Priorisierungsmechanismen sorgen. Bei entsprechender Überlast im Netz sind Datenverluste unvermeidbar, jedoch sollen sie durch die Priorisierungsmechanismen in der Regel auf nicht echtzeitfähige Applikationen verlagert werden. Arbeitet diese Priorisierung nicht ausreichend, kommt es auch im Bereich der höher priorisierten Daten zu unerwünschten Verlusten. Dieses Priorisierungsverhalten wird Thema eines unserer nächsten Firewall- und VPN-Tests sein.

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