Rundum geschützt

Vergleichstest Security-Appliances – Für eine effiziente Absicherung der Unternehmens-IT sollen spezielle Systeme mit Firewall- und VPN-Funktionalität sorgen.

Die schnelle und zugleich sichere Kommunikation zwischen verschiedenen Netzwerken oder auch getrennten Segmenten eines Unternehmensnetzes ermöglichen Security-Appliances. Solche Systeme vereinen Firewall, VPN sowie diverse weitere Funktionalität 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 erlaubt. Sie erfüllt vielmehr zugleich eine Überwachungs- und Kontrollfunktion, um das interne Netz vor unerwünschtem Datenverkehr zu schützen.

Auf der »internen« Seite handelt es sich zumeist um auf Ethernet basierende Netze, »extern« können neben Ethernet-Netzen 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 abzusichernden Netz oder Netzsegment und einem entsprechenden Remote-Access-System oder einer anderen aktiven Komponente. Diese ermöglichen die WAN- oder LAN-Anbindung ins externe Netz oder ins benachbarte LAN-Segment. Hierfür bieten solche Appliances heute Fast-Ethernet- und mit dem Adapter-Preisverfall zunehmend 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 sollen.

Doch die Komplexität der Unternehmensnetze nimmt zu, und das Gros der virtuellen Gefahren aus droht dem eigenen Unternehmensnetz, und nicht aus dem Internet. Deshalb gehen Netzwerkdesigner mehr und mehr dazu über, auch das interne Web in einzelne Segmente zu parzellieren, die gegeneinander durch Security-Appliances gesichert werden. Wegen der Integration dieser Systeme in das Unternehmensnetz muss nun aber nicht nur der Datenverkehr intern – extern, sondern auch ein Großteil des internen Datenverkehrs entsprechende Systeme passieren.

In heutigen konvergenten Netzen sind nicht nur die Datenmengen riesig. Auch die Qualitätsstandards der Voice- und Video-Applikationen und die Leistungsfähigkeit der übrigen Komponenten beanspruchen die Firewall-Systeme, was Performance und Funktionalität anbelangt. In Anbetracht dieser Situation sind auch Durchsatzraten auch im Gigabit-Bereich durchaus sinnvoll, und die Implementierung der Gigabit-Ethernet-Technologie ist eine logische Konsequenz. Die Anforderungen an das Leistungsvermögen solcher Firewalls entsprechen also 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 Paketfiltern, Stateful-Inspection-Firewalls und Application-Gateways zu unterscheiden. Paketfiltersysteme lesen die ein- und ausgehenden Datenpakete auf den Ebenen 2 bis 4 und gleichen sie mit einer vorgegebenen Tabelle ab. Unerwünschte Daten werden so eliminiert. Stateful-Inspection-Firewalls sind im Vergleich zu einfachen Paketfiltern »intelligenter« und arbeiten zustandsabhängig. Sie analysieren und protokollieren auch die Status- und Kontextinformationen der Kommunikationsverbindungen.

Application-Level-Gateways oder -Proxys realisieren aufwändige Sicherheitsmechanismen über mehrere Schichten hinweg. Sie entkoppeln die Netzwerke physikalisch wie logisch und können beispielsweise von jedem Benutzer 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, und nicht nur wie Paketfilter- und Stateful-Inspection-Firewalls die Header der Datenpakete. Das hat zur Folge, dass ihr Rechenaufwand deutlich größer ist und das Mehr an Sicherheit zu Lasten der Performance gehen kann. Für die glei-

che Performance – beispielsweise Fast-Ethernet-Leitungsgeschwindigkeit – ist also eine erheblich leistungsfähigere Hardware notwendig. Um unsere Tests trotzdem fair und vergleichbar zu halten, haben wir an alle Teststellungen die gleichen Maßstäbe gelegt und ein Standard-Rule-Set definiert, das die Hersteller zunächst konfigurieren mussten.

Firewalls bestehen aus Hard- und Softwarekomponenten, die häufig von unterschiedlichen Herstellern stammen und individuell kombiniert werden. Bei den Security-Appliances, die Firewall- und VPN-Funktionalität bieten, handelt es sich um Komplettlösungen, die in den unterschiedlichsten Leistungsklassen angeboten werden und für die unterschiedlichsten Einsatzszenarien gedacht sind. Neben der Firewall packen die Hersteller weitere Funktionalität in die Boxen, so dass immer mehr universelle Security-Appliances angeboten werden, die darüber hinaus Virtual-Private-Networks, Intrusion-Detection/Prevention und andere Security- und Kommunikationsfunktionen integrieren. Andererseits verleihen die Produzenten der »klassischen« aktiven Komponenten wie Switches oder Router diesen zunehmend Firewall- und andere Security-Eigenschaften. So ist insgesamt derzeit ein recht heterogenes Feld von Systemen auf dem Markt.

Die Hersteller teilen die verschiedenen Security-Appliances in Leistungsklassen ein, die für die entsprechenden Anwendungsszenarien entwickelt werden und sich deutlich in Leistungsvermögen und Preis voneinander unterscheiden. Die preisgünstigsten Geräte bilden die Gruppe der Small-Office/Home-Office-Systeme. Dann folgt das breite und bunte Mittelfeld, häufig neudeutsch Medium-Business genannt. Die Highend-Systeme stellen dann die Carrier- und Enterprise-Klasse. Wegen des Preisverfalls der Gigabit-Ethernet-Adapter sind inzwischen fast alle aktuellen Systeme unabhängig von der Leistung mit Gigabit-Ethernet-Adaptern ausgestattet. Eine Unterscheidung zwischen Fast- und Gigabit-Ethernet-Systemen ist daher nicht mehr sinnvoll möglich.

Die Geräte, welche die beteiligten Hersteller auf Grund unserer Testspezifikation auswählen, unterscheiden sich zumeist in der Leistungsfähigkeit und Preisgestaltung voneinander. Um das Preis-Leistungs-Verhältnis entsprechend zu würdigen, haben wir daher wieder unseren Preis-Performance-Index ermittelt. Dieser zeigt, wie viel Leistung der IT-Verantwortliche heute für sein Geld bekommt.

VPN inklusive

Neben der klassischen Firewall-Funktionalität gehört der Aufbau von VPNs zur Standardfunktionalität von Security-Appliances. Virtual-Private-Networks oder kurz VPN sollen einer geschlossenen Gruppe von Rechnern eine geschützte Kommunikation über ein potenziell unsicheres Netz hinweg erlauben. Die Verbindung, auch VPN-Tunnel genannt, wird durch kryptographische Algorithmen realisiert, welche die zu schützenden Datenströme ver- und an der Gegenstelle wieder entschlüsseln. Dafür gibt es eine ganze Reihe von Standards wie DES, 3DES oder AES. Über die Sicherheit solcher Verbindungen entscheidet wie bei anderen kryptographischen 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 erreichen 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. Das bedeutet, dass die Funktionalität sehr rechenintensiv ist. Eine gute Performance setzt also eine entsprechend leistungsfähige Hardware voraus. Es gibt aber auch VPN-Lösungen, die Hardware-näher realisiert sind und dann entsprechend mehr Power bringen.

Real-World Labs zum Anfassen

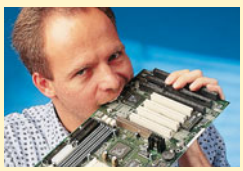
Illusion oder wirkliche Hardware

Virtuelle Maschinen eignen sich nicht nur für Testinstallationen oder Demo-Setups. Viele Standarddienste und Server-Applikationen lassen sich konsolidiert auf wenigen physischen Servern abbilden und produktiv nutzen. Die Technologie für virtuelle Umgebungen steckt bereits in den Server-CPUs; fehlt nur noch die passende Software, um die Dienste der virtuellen Maschinen umzusetzen. Der Marktführer Vmware sieht sich einer ganzen Reihe neuer VM-Lösungen gegenüber. Diese neuen Applikationen gehen stellenweise ganz eigene Wege, um aus einzelnen physischen Servern konsolidierte Plattformen für viele virtuelle Maschinen zu machen.

Die Real-World Labs beobachten den Virtualisierungstrend bereits seit Jahren und haben das Gros der verfügbaren Lösungen näher unter die Lupe genommen. Jetzt können Sie sich selbst ein Bild vom Stand der Technik machen. Network Computing verfrachtet Teile der Laborinfrastruktur in ein mobiles Rack und zeigt die laufenden Tests auf der Technology-Tour. Darunter finden sich Maschinen mit Vmware-ESX ebenso wie Virtuozzo, der MS Virtual-Server oder die freien Lösungen wie Xen und Virtual-Box.

Und weil es im mobilen Labor so schön virtuell zugeht, nimmt Network Computing gleich passende SAN-Lösungen mit Fibre-Channel und iSCSI mit, die dazu bestens passen.

Mehr hierzu gibt es auf der Technology Tour zu sehen.



Andreas Stolzenberger,
Stellvertr. Chefredakteur
Network Computing

Mitte	Süd
24.04.07 Frankfurt	**08.05.07** München
26.04.07 Oberhausen	**10.05.07** Stuttgart

Besuchen Sie uns auf der Technology-Tour
www.networkcomputing.de/technology-tour

Für die Beurteilung des Verhaltens der Systeme im Test, 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 Bereich der mittelgroßen und kleinen Frames. 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 er 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 ist bei der IP-Sprachübertragung davon auszugehen, 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.

50 Prozent der Datenrahmen sind 64 Byte groß

Die Analyse der Verteilung der Frame-Größen, 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 sinkt 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 in der Telefonie sehr wahrscheinlich machen. Auf Grund ihrer Bedeutung für die Übertragungsqualität haben wir daher das Datenrahmen-Verlustverhalten 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 Haus 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 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 ist daher auch für Security-Appliances wichtig, die in entsprechenden Netzen zum Einsatz kommen.

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