Schneller Brandschutz

Vergleichstest Security-Appliances, Teil 2 – Für einen durchsatzstarken Brandschutz im Netz sollen spezialisierte Gigabit-Ethernet-Systeme mit Firewall- und VPN-Funktionalität sorgen.

Eine sichere aber auch schnelle Kommunikation zwischen verschiedenen Netzen oder auch getrennten Segmenten eines Unternehmensnetzes sollen Security-Appliances ermöglichen. 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 Netzen 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 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 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 mit dem »Gigabit-Trend« 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.

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 droht, 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 entsprechende Systeme 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 im Gigabit-Bereich durchaus Sinn und die Implementierung von Gigabit-Ethernet-Technologie ist eine folgerichtige Konsequenz. Die Anforderungen an die Leistungsfähigkeit solcher Firewalls entsprechen logischerweise denen, die auch an andere Komponenten des Unternehmensnetzes, wie LAN-Switches, gestellt werden.

Schnelle Tunnel

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 Hardwarenäher realisiert sind und dann entsprechend leistungsfähiger sein können. Gerade für das Segment der Gigabit-Ethernet-Systeme hat sich gezeigt, dass möglichst viel Funktionalität in Hardware abgebildet werden sollte, damit die in vielen Szenarien geforderten Durchsatzleistungen erreicht werden können.

Inwieweit aktuelle Systeme den Performance-Anforderungen gewachsen sind, klärt der nachfolgende Testbericht unserer Real-World Labs an der FH Stralsund. Der Frage, wie viel Sicherheit die getesteten Systeme gewähren, klärt ein weiterer Artikel in einer der kommenden Ausgaben von Network Computing.

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