

Die Firewall oder das Chinesisch in der Datenübertragung

Diejenigen, die Daten übertragen müssen oder wollen, werden mit mindestens zwei Problemen konfrontiert: Viren und unerlaubter Zutritt durch Dritte. Für die Lösung des ersten Problems gibt es eine Auswahl an Softwareprogrammen. Der unerlaubte Zutritt lässt sich damit nicht lösen, zu diesem Zweck gibt es Firewalls. Kurz und gut, man besorgt sich entsprechende Dokumentationen – und versteht oft nur noch Chinesisch. Das Beispiel Firewall Serie SnapGear soll auch für Laien etwas Licht ins Dunkel bringen.

Von Robert George Kroese *

Was ist eine Firewall?

Als Firewall bezeichnet man ein organisatorisches und technisches Konzept zur Trennung von Netzbereichen, dessen korrekte Umsetzung und dauerhafte Pflege. Es handelt sich um ein Stück Hardware, das zwei oder mehr physisch getrennte Netzbereiche verbindet.

Wer braucht eine Firewall?

Bei vielen Unternehmen – unabhängig von der Grösse – arbeitet der Aussendienstmitarbeiter von seiner Wohnung aus (SOHO). Die grosse Kosteneinsparung (kein Arbeitsplatz im Büro, kürzere Anfahrtswege zur Kundschaft), hat dieses Modell für diese Berufsgattung populär gemacht. In Zukunft ist zu erwarten, dass dieses Modell auf Personen, die nicht physisch in der «Zentrale» anwesend sein müssen, ausgedehnt wird.

Technisch gesehen bringt dies die Notwendigkeit einer Anbindung der PCs vom Mitarbeiter an das Netzwerk der «Zentrale» mit sich, damit beide Parteien immer «up-to-date» sind. Normalerweise wird die Datenübertragung über das Internet erfolgen. Die Gefahr des unerlaubten Zugriffs durch Dritte (Industriespionage!) erfordert den Einsatz von Firewalls nicht nur auf der Seite des Servers in der «Zentrale», sondern auch auf der Seite des SOHO-Mitarbeiters. Firewalls sind normalerweise recht kostspielige Geräte. Die Kosten bei der Reihe «SnapGear» sind dagegen erstaunlich tief, wenn man bedenkt, welch vorbeugende Wirkung damit erreicht wird.

Gerätebeschreibung und Übersetzung

Dieser Artikel ist primär an die Entscheidungspersonen (Verkaufsleitung, Marketingleitung) gerichtet, bei denen es

an spezifischen Kenntnissen des Fachchinesischen mangelt. Damit der Kopf-runter/Kopf-rauf-Effekt eines Glossars entfällt, ist die «Übersetzung» hinzugefügt.

Snapgear ist eine integrierte Hard-/Software-Lösung, welche auf dem führenden Betriebssystem für **Embedded Devices** (integrierte Geräte), dem uClinux, basiert. Durch den Einsatz bewährter **Open-Source-Technologie** (Software, deren Quellcode erhältlich ist, was aber nicht heissen muss, dass die Software kostenlos ist) bietet SnapGear ein hohes Mass an Stabilität, Robustheit und Benutzerfreundlichkeit.

Die Geräte bieten neben dem Anschluss über ein normales **Modem/ISDN-TA** (Integrated Services Digital Network Terminal Adapter) via serielle Schnittstelle auch Kabelmodem, **ADSL**- (Asynchronous Digital Subscriber Line = Breitbandanschluss über Kupferleitung) und **Ethernetanschluss** (Netzwerk im Büro).



Für kleine Büros und Heimnetzwerke: SnapGear LITE



Für mittlere Büros und grössere Heimnetzwerke, mehr Durchsatz speziell bei VPN (siehe oben): SnapGear SOHO+

Für mittlere und grössere Büros mit speziellem Crypto-Accelerator für VPN-Verbindungen bis 4 MBit/s: SnapGear PRO



Für kleine Büros und Heimnetzwerke inkl. 4-Port-100-MBit/s-Switch: SnapGear LITE+

Im Notfall kann so bei einem Ausfall des Breitbandanschlusses über Wählleitung weiter mit dem Internet gearbeitet werden.

Neben bewährten Firewall-Technologien wie **statefull packet inspection** (der IP-Stack der Firewall merkt sich, welche Anfragen aus dem internen Netz ans Internet gingen, und kann so kontrollieren, ob eingehende Pakete eine Antwort auf eine gestellte Anfrage darstellen oder «uneingeladen» eintreffen) und **masquerading** (wird bei NAT erklärt) bieten die SnapGear-Geräte auch **IDS-Funktionalität** (Intrusion Detection System = System zur Erkennung von Angriffen und/oder Einbrüchen), **VPN-Verbindungen** (Virtual Private Network = transparente Verbindung zwischen zwei sicheren Netzwerken über ein unsicheres Medium, z. B. Internet, mit jedem IPSec-kompatiblen Endpunkt; IPSec = IETF-Standard für ein standardisiertes VPN-Protokoll, welches von allen namhaften Herstellern unterstützt wird) sowie Microsoft **PPTP-Verbindungen** (Microsoft Point-to-Point Tunneling Protocol, ebenfalls ein VPN-Protokoll, welches jedoch nur von Microsoft verwendet wird und nicht über die gleichen Stärken wie IPSec verfügt, es wird aber standardmässig von allen Microsoft-Produkten unterstützt). Die IPSec-Verbindungen können dabei mit **DES** (Digital Encryption Standard, einer der weitest verbreiteten Verschlüsselungsalgorithmen, jedoch heute

relativ leicht zu knacken und daher eher veraltet; Schlüssellänge 56 Bit) oder **3DES** (sprich tripple-Des = wie DES, jedoch mit dreimal längerem Schlüssel = 168 Bit) hergestellt werden.

Die **masquerade/Nat-Funktion** (Network Address Translation) impliziert heutzutage automatisch auch **PAT** (Port Address Translation). Diese Technik sorgt dafür, dass hunderte von Anwendern über eine einzige öffentliche IP-Adresse Zugriff aufs Internet haben; masquerade = NAT, die Linux Implementation von NAT/PAT wird masquerade genannt), sorgt dafür, dass eine unbegrenzte Anzahl Benutzer über die SnapGear-Firewall das Internet über einen einzelnen Modem- oder Breitband-Anschluss nutzen können.

Einfache Konfiguration

Die Konfiguration ist innert weniger Minuten zu bewerkstelligen und wird nach dem Setzen der IP-Adresse über ein mitgeliefertes Windows-Programm komplett über den integrierten Webserver vervollständigt. Die Konfiguration der SnapGear Firewall Appliances kann durch Herunter- bzw. Heraufladen eines ca. 2 kB grossen Textfiles auf einfachste Weise gesichert bzw. zurückgesichert werden. Updates werden mittels Mausklick von einem Windows-Rechner eingespült; kein mühsames Verbinden über eine serielle Schnittstelle und Eingabe von kryptischen Upload-Befehlen, das Up-date-

Programm sucht sogar selbstständig nach dem «upzudatenden» SnapGear-Firewall im Netz.

Nochmals Chinesisch

Der integrierte **DHCP-Server** (Dynamic Host Configuration Protocol, teilt Rechnern dynamisch eine IP-Adresse zu) und der **DNS-Forwarder-Server** (DNS = Domain Name System, das System welches es uns erlaubt, im Internet Namen statt Nummern als Adressen zu verwenden; DNS-Forwarder = kein eigener DNS-Server, sondern einfach eine Weiterleitung an einen bestimmten DNS-Server) sorgen bei den angeschlossenen Rechnern dafür, dass die Konfiguration auf ein Minimum beschränkt wird.

Ein weiteres Highlight stellt die **Traffic Shaping** (Verkehrspriorisierung) dar: Damit kann der Benutzer verschiedenen Applikationen verschiedene Prioritäten bei der Übermittlung zuweisen, sodass z. B. Mails nur mit der Bandbreite versendet werden, welche vom Websurfen übrig bleibt, sodass die Webzugriffe immer mit maximaler Geschwindigkeit laufen, während Mails nur während den Zeiten versendet werden, in denen kein Webpaket ansteht.

*Robert George Kroese ist Inhaber der IMC Industrial Marketing Consultancy

IMC Industrial Marketing Consultancy
5276 Wil AG
Tel. 062 867 20 50
imc@industrial-marketing.ch
www.industrial-marketing.ch

