

Sonderdruck für Netropol Digitale Systeme

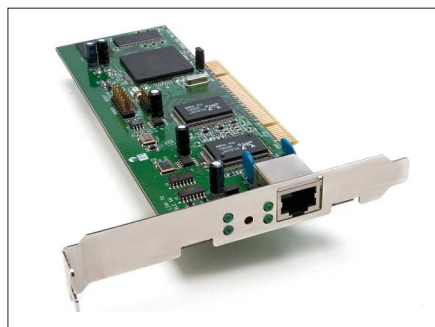
INTERNE FIREWALL SG635 VON CYBERGUARD IM TEST

Sicherheit zum Einstecken

Mit der SG635 von Cyberguard wandert die Firewall in den PC. Die PCI-Karte enthält ein speziell auf ihren Einsatz als Firewall abgestimmtes Linux im ROM. Neben dem Schutz vor Angriffen sind damit auch VPN-Tunnel, Proxy-Funktion und Intrusion Protection möglich.

Firewalls gibt es mit unterschiedlichen Kapazitäten und Funktionen, um sie an die Anforderungen des Unternehmens anzupassen. Eines haben sie jedoch immer gemeinsam: Es handelt sich um externe Lösungen, gleichgültig, ob man dafür eine Appliance oder einen dedizierten Computer heranzieht. Cyberguard weicht von diesem Konzept ab und packt die Firewall auf eine PCI-Karte zum Einstecken in den zu schützenden Computer. Auf der einen Seite kommt das der Sicherheit zu Gute: Man kann nicht einfach den Stecker ziehen und die Firewall aus dem Netzwerkpfad nehmen. Wer die Firewall vom Computer trennt, nimmt ihn komplett vom Netz. Dem gegenüber steht der größere Aufwand für die Installation und das zunächst ungewohnte Konzept bei der Konfiguration. Auf der Karte sind drei Ethernet-Chips untergebracht, die sich im Netzwerk auch mit drei getrennten Adressen bemerkbar machen. Im Router-Modus ist das eine IP-Adresse für den Host-Computer und zwei Adressen für das Gateway, einmal zum internen und einmal zum externen Netzwerk.

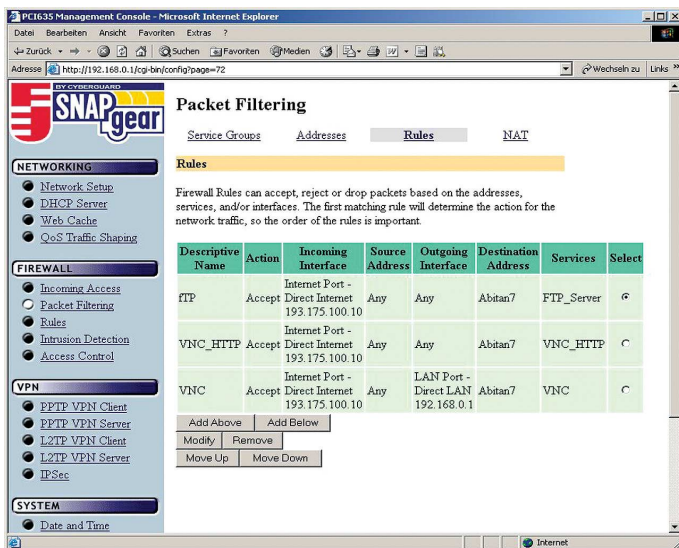
Obwohl es möglich ist, mit der SG635 den Internetzugang für ein LAN herzustellen, zielt Cyberguard mit der Einbau-Firewall auf den Schutz von Computern im Netzwerk ab. Im Normalfall sitzt die Firewall an der Schnittstelle zum Internet. Ist ein Angreifer daran vorbeigekommen, zum Beispiel, weil er von Innen Zugriff auf das Netzwerk hat, sind die Ressourcen ungeschützt. Mit einer SG635 verfügen Server über einen unabhängigen Schutzwall, der solchen Attacken vorbeugt. So kann die Karte Authentifizierung vor dem Zugriff



Cyberguard SG635: klein, aber mit komplettem Linux onboard

verlangen oder nur über VPN-Tunnel mit der Außenwelt kommunizieren. Die Firewall von Cyberguard ist weitgehend unabhängig vom Betriebssystem und lässt sich in Windows- und Linux-Servern einbauen. Völlige Unabhängigkeit wie bei einer Appliance erreicht man damit allerdings nicht. Einschränkungen in der Leistungsfähigkeit (verglichen mit externen Lösungen) konnten wir im Test hingegen nicht feststellen. Der Hersteller gibt einen Durchsatz von 95 MBit/s für die Firewall an, ein Hitachi SH-4 Prozessor mit 240 MHz Taktfrequenz und die für ein Embedded Linux üppige Ausstattung mit 64 MByte RAM sorgten für flottes Arbeiten, auch bei mehreren parallelen VPN-Verbindungen.

GROSSER FUNKTIONSUMFANG Beschränkt sich eine externe Firewall in dieser Preisklasse meist nur auf einen Paketfilter und eventuell noch einen VPN-Server, bietet Cyberguard deutlich mehr. In der SG635 findet ein Squid Proxy-Server genauso Platz wie ein DNS-Proxy. NTP (Network Time Protocol) und DHCP sind mit Server und Client implementiert. Zusätzlich leistet die Karte QoS-Traffic-Shaping mit Bandbreitenkontrolle und Priorisierung. Das Thema VPN wird für LLTP und L2TP, jeweils mit Server und Client, sowie mit IPsec (Initiate/Terminate) abgedeckt. Darüber hinaus hat sich Cyberguard viel Mühe mit dem Einbau von IDS-Funktionen gegeben. Ein IDB-(Intrusion Detection and Blocking-)System kann auf Wunsch zu neugierige Anfragen auf frei wählbaren Ports erkennen und blockieren. Für größere Systeme, bei denen mehrere, verteilte Instanzen nach Attacken suchen,



Die Firewall blockt standardmäßig jeden Zugriff auf den Host ab

ist eine komplette Snort-Implementation vorhanden, die allerdings einen zentralen Datenbankserver für die Ausgabe der Ergebnisse benötigt. Das IDB-System schreibt seine Meldungen in das System-Log, das per E-Mail oder Syslog-Protokoll an eine Managementkonsole verteilt werden kann. Im Test schlug IDB wie erwartet bei Scans durch Nessus Alarm, selbst als der Probe Level von Nessus auf "unauffällig" gestellt war. Das Ergebnis der Firewall war sehr gut. Offen wurden nur die Ports gemeldet, die wir vorher explizit freigegeben hatten, zum Beispiel VNC für die Fernsteuerung. Andere Netzwerkdienste wie die VPN-Server zeigten nach Außen zwar ihre Präsenz, blockten weitere Zugriffe jedoch zuverlässig ab. Dabei profitiert die SG635 von ihrer "alles zu" Strategie. Der Administrator muss die benötigten Dienste vorher freigeben, im Grundzustand verbietet die Firewall jeden Zugriff. Wie bei den meisten Firewalls erwartet die SG635 zunächst vom Administrator, Dienste, Hosts und Netzwerke zu definieren, die er in den Regeln zusammenstellen kann. Die gebräuchlichsten Einträge wie HTTP, FTP, DNS und Ähnliches sind schon vorgegeben, individuelle Anwendungen wie VNC können frei über die Angabe der Ports definiert werden. Durch das Zusammenspiel mit NAT (Network Address Translation) kommt jedoch eine Komplikation dazu. Im Routing-Modus ist der IP-Adressbereich des Hosts ein anderer als der des LAN, an dem der Host eigentlich eingesteckt ist. Darum müssen Zu-

griffsregeln in der Firewall auch eine Entsprechung in der NAT-Tabelle finden. Zum Glück nimmt eine Hilfsfunktion dem Administrator die Arbeit ab. Definiert er zuerst die NAT-Regel, erzeugt sie auf Wunsch einen passenden Firewall-Eintrag.

INSTALLATION MIT HÜRDEN

Normalerweise sitzt eine Firewall am Rand des Netzwerks und stellt die Schnittstelle zum Internet dar. Die Aufteilung ist klar: An einem Port wird das externe Netzwerk angeschlossen, zum Beispiel über ein DSL-Modem. An einem anderen Port liegt das interne LAN, die Firewall kümmert sich um das Routing zwischen den beiden. Weil die SG635 nur einen Netzwerkanschluss hat, aber trotzdem diese Trennung vornimmt, muss sie das intern erledigen. Dazu gibt es drei Netzwerkadressen, die der Wizard nicht eindeutig beschreibt. Der LAN-Port bezeichnet das virtuell interne Netzwerk der Karte, in dem der Host angeschlossen ist, zum Beispiel 192.168.10.1. Der Host benötigt darüber hinaus eine weitere IP-Adresse aus diesem Bereich. Sie taucht nicht in der Konfigurationsoberfläche auf, sondern wird an die Netzwerkkarte gebunden, die der Treiber im Host einrichtet. Für unser Beispiel kann dies 192.168.10.2 sein. Die dritte Adresse ist der Internet-Port, der jedoch schlicht das physikalische, lokale Netzwerk bezeichnet, an dem der Host angeschlossen ist. Je nach Konfiguration ist das eine völlig andere IP-Adresse als 193.175.100.10. Wer auf die Routing-Funktion verzichten will, kann das nach der Erstinstallation über die Auswahl eines Bridge-Modus tun. Dabei agiert die Firewall-Karte als transparenter Filter mit nur zwei IP-Adressen aus dem gleichen Bereich, einer internen und einer externen.

Die Installation ist einfach, wenn man das Konzept einmal verstanden und die Begriffsdefinitionen zugeordnet hat. Lei-

der hilft die mitgelieferte Dokumentation dabei kein bisschen. Ein DIN-A4-Faltblatt mit acht Seiten erklärt reichlich wenig; das auf der CD enthaltene, ausführliche Manual bezieht sich auf alle Firewalls von Cyberguard, in der Mehrzahl externe Appliances. Die Übereinstimmung mit der SG635 ist minimal, das Handbuch größtenteils unbrauchbar. Ebenfalls unverständlich: Das dringend benötigte NAT wird im Router-Modus nicht automatisch eingeschaltet und taucht nicht im Wizard auf. Wer die Funktion im Netzwerk-Setup, Unterpunkt „Advanced“ findet, muss schon eine Weile mit dem Gerät zugebracht haben.

Einmal eingerichtet zeigt sich die Firewall jedoch von ihrer besten Seite und funktioniert problemlos. Die VPN-Server sind einfach zu konfigurieren und arbeiteten mit den meisten Clients zusammen. Im Test wurden Verbindungen zu anderen Routern über das Internet und DynDNS aufgebaut sowie der Standard-Windows-VPN-Client verwendet. Angenehm ist, dass auch dynamische Adressen als Endpunkte gewählt werden können, eine statische IP ist nicht nötig. Die Benutzerverwaltung kann ein externen Tacacs+ oder Radius-Server abwickeln, in kleinen Netzwerken genügt die eingebaute lokale Verwaltung der SG635. Leider synchronisiert die Karte die Benutzer-Accounts weder zwischen LLTP, IPsec und L2TP noch mit der allgemeinen Benutzerverwaltung für das Management der Karte über den Browser. Der Admin muss die Nutzer jeweils separat anlegen. Standardbenutzer ist root, das Kennwort lautet "default". Die Daten finden sich zwar im Beiblatt, könnten aber durchaus deutlicher sichtbar gemacht werden.

Mit der SG635 kann man einen Host im Netzwerk absichern, das steht außer Frage. Der Funktionsumfang ist riesig, die Arbeit mit der Benutzeroberfläche nach den Anfangsschwierigkeiten kein Problem. Die SG635 kann in Netzwerken, in denen wichtige Host-Rechner explizit geschützt werden sollen, einen wertvollen Beitrag zur Sicherheit leisten. Die Karte kostet zirka 359 Euro.

(Elmar Török/mw)

Info: Netropol
Tel: 040/4325000
Web: www.cyberguard.com