

● FIREWALL/VPN APPLIANCE

CyberGuard SG710



PRICE £1,460 exc VAT

BASIC WARRANTY 1yr RTB

INTERNET www.cyberguard.com

SUPPLIER CyberGuard Corporation 01344 382550

VERDICT A modest hardware specification, but CyberGuard still delivers top-notch firewall and VPN facilities, plus useful Internet load-balancing and failover support.

The majority of vendors try to pack as many features as possible into their firewall appliances, but CyberGuard focuses on the key security issues to avoid spreading itself too thin. Consequently, the top-of-the-range SG710 delivers solid firewall protection, intrusion detection and blocking, plus some of the best VPN capabilities we've seen from an SME security appliance.

In a direct comparison with SonicWALL's PRO 3060 (see issue 113, p172), CyberGuard comes out wanting in the hardware department. All components are embedded on the sparse motherboard and comprise a simple Intel network processor and a small portion of memory, while the Linux kernel has been embedded onto a 32MB DiskOnChip module. It fares much better for network connection options, as ten Fast Ethernet ports are up for grabs. The SG710 incorporates two Fast Ethernet switches, each looking after four ports. Ideally, the first group is used for LAN connections, but all support LAN, WAN and DMZ functions. A separate pair is provided for Internet access only, and with two separate links configured you can implement load balancing across them or keep one to the side as a backup link if the primary connection goes down. Further options include a serial port that accepts a PSTN or ISDN



Bandwidth management is available via Quality and Type of Service settings.

modem, which can be used for dial-in remote access or as a primary or failover Internet link.

The firewall defaults to blocking unsolicited inbound connection attempts. New rules may be added to the default rules or used instead of them, and all can be placed in order of priority. VPN support doesn't get any better, as the SG710 can manage PPTP, L2TP, IPSec and GRE VPNs. The manual devotes almost half of its pages to assisting the configuration of these features and includes plenty of help for setting up clients on Windows 98 right through to XP.

Intrusion detection and prevention is handled by Snort, which comes preconfigured with plenty of rules, leaving little to do other than enable this feature. Snort can send its report logs to a remote MySQL database. The traffic shaping function will come in handy too, as once you've entered upstream and downstream speeds the appliance can automatically apply preconfigured QoS (Quality of Service) parameters to Internet traffic. Alternatively, custom ToS (Type of Service) traffic

shaping may be applied to a range of services, including POP3, SMTP and HTTPS. These were easy to set up and had three priorities for each service. A web cache is provided, and if local memory is insufficient the SG710 can employ a remote network share for caching web pages.

Internet access controls are extensive. Black-and-white lists of source and destination IP addresses as well as websites can be enforced, and user authentication is required as well.

Applying policies to groups of IP addresses allows access to be permitted or denied to multiple services, and NASL (Nessus Attack Scripting Language) scripts may be used to scan for vulnerabilities.

CyberGuard doesn't provide any help with NASL, but you're able to access the appliance's setup files directly from the browser and add your own instructions. Web content category filtering rounds off this package nicely. The Cerberian service is available as an option, and once a licence key has been entered at the browser you can select more than 50 content category filters and view reports on user activity.

The SG710 is easy to set up and use, offers a fine range of features at a great price. Overall, a top choice for SMEs looking for a security appliance that focuses on the key areas of firewalling, IDS and, in particular, VPNs.

DAVE MITCHELL

PC PRO RATINGS	
PERFORMANCE	★★★★★
FEATURES & DESIGN	★★★★★
VALUE FOR MONEY	★★★★★
OVERALL	★★★★★
SPECIFICATIONS 1U rack appliance; 533MHz Intel IXP425 network processor; 128MB PC133 SDRAM; 32MB M-Systems DiskOnChip Millennium Plus; SafeNet SafeXcel-1141 VPN accelerator chip; 10 x 10/100BaseTX ports; 9-pin serial port; NAT/SPI firewall; 1,000 IPSec VPN tunnels; IPSec/GRE; PPTP/L2TP VPN client and server; supports HTTPS, NAT, DHCP, PPPoE, all TCP/IP OSes; IDS; web browser management.	