

# Snapgear SG640

Wednesday, 12 September 2007

## Integrated Firewall/VPN/IDS on a PCI Card Protects Desktops and Critical Servers

The SnapGear® model SG640 is a cost-effective firewall/VPN/IDS solution packaged on a PCI card. By offloading all firewall, VPN, and IDS processing from the host computer, the SG640 ensures high performance and throughput with the convenience of remote management and simplified installation. Unlike "co-processing" products, the SG640 is an advanced, self-contained multi-tasking stateful firewall, VPN, and IDS appliance. It includes a RISC processor and two Ethernet interfaces for host and LAN communications. The SG640 packs the power of a firewall, VPN and IDS solution while eliminating the cabling, space and power requirements of an external appliance PDAs, web and applications servers to the Internet via business- and consumer-grade broadband, dedicated circuits from T-1 to T-3 or narrow-band connections (modem/ISDN). The SnapGear SG640 provides connectivity and security features normally found only in enterprise-class solutions.

Recommended for: • Security-conscious businesses that wish to deploy a defense-in-depth security strategy • Data Centers with Web and Application Server Farms • Environments where the integrity of the host server operating environment cannot be controlled or trusted • Organizations seeking to demonstrate compliance with regulatory requirements concerning privacy and access to personal information • A co-location/Web hosting center Embedded distributed firewalls offer external and internal protection

The SnapGear SG640 is a cost-effective, VPN Firewall PCI card that offloads all firewall and VPN processing from the host computer to the card yielding greater performance, higher security, remote management, and simplified installation. Unlike "co-processing" products on the market, the SG640 is an advanced self-contained VPN and stateful firewall multi-tasking appliance. It contains a RISC processor, encryption accelerator for IPsec VPN traffic and two Ethernet NICs for host and LAN communications. As it presents a normal Ethernet interface to the LAN, it also eliminates the cabling, space and power issues associated with external firewall appliances.

While perimeter firewalls are the first line of external defense, they cannot see activity behind them and cannot defend against internal threats. The SG640 fulfills this role, protecting the host and complementing the existing perimeter firewall. Many SG640 adapters can be installed throughout an organization providing a robust distributed firewall that operates even when the host systems are down or entirely unresponsive. These can be managed through the SnapGear Central Management System (CMS) running on a management station on the network. Protects against external and internal intruders

While most firewall products focus on external intruders, the SG640 adapter card can also protect from internal intruders whether intentional or not. It has been estimated that 90% of security violations are internal, not external. The US military is also pursuing research into distributed embedded firewalls as the best line of defence against intrusion. The SG640 can be configured to enable every desktop user to have their access to the general LAN and critical servers significantly restricted. Therefore every host and network service that a user is authorized to utilize is allowed while any other actions are blocked. It therefore provides access separation, which can be along departmental lines such as sales department, e-commerce, finance, customer records, etc. This can be useful in providing isolation between access to credit card details, personal information, payment history, etc. Increasingly this is becoming obligatory for e-commerce, electronic health records (e.g. HIPAA) and other privacy sensitive applications. Protect Hosts on your DMZ or in your DataCenter

Often web, e-mail and download servers are made publicly accessible through the Internet on a network that has less stringent security than the private internal network. Although these servers can be accessed across the hostile Internet, they can be protected against attack by installing a SG640 in each system. The same can be applied to critical hosts within a data center in your enterprise, a hosting provider or ASP (Application Service Provider). Host-based without suffering from 'software firewall' vulnerabilities

The SG640 also eliminates the problems with software firewalls that run on the host operating system, which is most vulnerable to attack. The SG640 places a hardware firewall as close to the host system as possible without suffering from host vulnerabilities. It is also tamperproof as it is internal to the system and can only be configured by the system administrator. The SG640 can be configured to enforce strict access filters per system and draws from the fine pedigree of all SnapGear embedded Linux based security appliances. Features

- Dynamic stateful firewall, IPsec VPN, and IDS packaged on a PCI card to secure desktop and server systems
- Full PPTP VPN client and server
- Unrestricted, unlimited user license
- Web console for configuration and management
- No per-user licensing or restrictions
- Fully interoperable with Secure Computing Corporation appliances and other standards-based security devices
- No third-party client software required

- Central management with Global Command Center (bridge mode not available for central management) Specifications

- ICSA-certified dynamic firewall

#### Routing

- DHCP - client and server
- PPPoE (for ADSL support)
- NAT - static and dynamic
- NAPT/PAT - port forwarding
- Connection sharing
- Anti-intrusion
- Logging (local and remote)
- Traffic shaping (QoS)
- IP aliases
- NTP client and server
- Web management
- CLI (Telnet) management
- Initial setup via either static IP address or dynamic IP address (DHCP client)
- Bridging (802.1d)
- Administration user accounts
- RADIUS/TACACS+
- DNS enhanced caching, masquerading, proxy, multiple DNS server proxying
- RIP, RIPv2
- Throughput: Please reference the SnapGear Product overview for performance data
- Status LEDs
- Network port - 1x10/100BaseT
- Memory - 16Mb Flash, 64Mb RAM
- Real time clock
- Power - powered by PCI slot
- Operating temperature 0C to 40C
- Storage temperature -20C to 70C
- Humidity 0 to 95%, non-condensing
- Certification - home and office
- Warranty - 1 year\*
- Extended 3 year Warranty Available
- \*Except where required to be 2 years by law Supported Platforms:
- Any PCI-based host, independent of host operating system
- Tested platforms include:
- Windows 2000 server and client
- Windows 2003 server
- Windows XP
- Linux

- VPN - IPSec
- VPNC-certified interoperability
- Peer-to-peer (initiate and terminate)
- ESP and AH payloads
- Supports aggressive mode
- Dead peer detection
- Compression (deflate/gzip type algorithm)
- DES 56-bit, 3DES 168-bit, AES 256-bit encryption
- Hashes HMAC - MD5 and SHA-1 authentication
- IKE/ISAKMP Diffie-Hellman key exchange
- Diffie-Hellman Groups (1,2,5) and Oakley Groups (14,15,16) to 4096-bits
- X.509 certificates DER, PEM formats
- Pre-shared secrets
- Dynamic IP address end-points
- Dynamic DNS IPsec support
- Authentication up to 2048-bit for RSA key signatures
- Multiple subnets
- NAT traversal
- VPN - L2TP
- IPsec config Wizard
- L2TP over IPsec
- Autonomous L2TP
- Client: NAT, default route via L2TP

- Server: specify client IP address range
- VPN - PPTP
- v2 client and server
- Pass-through mode also
- PAP/CHAP/MS CHAPv2 authentication
- L2TP & GRE tunneling extensions

Other Snapgear models and links: SG300

SG560

SG565

SG580

SG720

SG640