

# Snapgear SG580

Wednesday, 12 September 2007

A robust network security solution that unifies layers of defense and response mechanisms with centralized management can provide increased protection against blended threats. The SnapGear<sup>®</sup> model SG580 is a feature-rich, compact, network security appliance, which consolidates firewall, sophisticated intrusion-prevention, secure VPN access, anti-SPAM, and Web content filtering on a single device. This reduces the complexity of network security deployments while lowering administration and maintenance requirements. The SG580 is well suited to protecting central offices of small to mid-sized enterprises as well as branch offices of large enterprises. It enables offices to easily and safely connect their network of desktops, notebooks, 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 SG580 provides connectivity and security features normally found only in enterprise-class solutions. With the inclusion of five Fast Ethernet ports, link fail-over and Internet session load balancing as well as multiple security zones (VLANs), the SG580 can be deployed in a myriad of environments.

Should the primary broadband connection fail, the SG580 can fail over to a secondary link. Internet traffic can be balanced between links, increasing bandwidth for faster web page delivery and more concurrent downloads. Should there be a complete broadband failure, the built-in dial-up connection can be invoked automatically. To further enhance web performance and reduce WAN bandwidth, the SG580 has a built-in Web proxy cache. Recommended for: •SME and large branch offices•Suitable for ADSL, Cable and T1 to T3 circuits •Central VPN for small multi-site networks  
•Suitable for use as a VPN concentrator leveraging VPN offloading•Networks with mobile and remote workers•Complementary VPN end-point for Secure Computing enterprise appliances (Sidewinder)

The SnapGear SG580 provides layers of network protection. A powerful stateful-inspection firewall, service-based intrusion detection and prevention, and advanced Internet connection sharing protect the branch-office network from the Internet.

An intrusion detection system adds an extra security layer by detecting suspicious activity through a database of thousands of attack signatures. It can alert an administrator so that countermeasures can be implemented quickly before the network is compromised. It can also be configured to respond by adjusting the firewall automatically and refusing the connection, effectively preventing intrusions. Finally, the SG580 also provides security policy enforcement across the network by probing desktops and servers in an attempt to identify vulnerable network services. Systems that are deemed vulnerable are blocked from Internet access or access to other security zones. This reduces the possibility of staff spreading viruses, worms and Trojans.

The SG580 provides default physical security zones (DMZ, Guest and LAN) on separate Ethernet segments. The DMZ segment can be used for publicly accessible servers (e-mail, file download); the Guest segment enables mobile staff or visitors to have general Internet access only, while the LAN segment connects the entire office network. These can be reconfigured to create three departmental security zones or other custom configurations. If only one WAN connection is required the other can be configured as a fourth security zone. Complete flexibility was a primary goal of the SG580.

A remote office network can safely become part of a central office network, since the SG580 is also a cost-effective VPN appliance. The SG580 includes industry-standard secure VPN access methods (IPsec, PPTP, L2TP) with hardware-accelerated encryption. It is complementary to the SG720 and Sidewinder line of appliances for VPN deployments at mid- to large-sized branch offices and head offices. Mobile and remote workers can also gain access to the central location across the Internet by having similar security configurations using an SG300 device or through VPN client software – and all appliances can be managed by Secure Computing's Global Command Center.

## Features

- Full IPsec, PPTP & L2TP VPN client and server
- Link fail-over & load balancing
- Intrusion detection and prevention
- DMZ, Guest and LAN security zones
- Web console for configuration and management
- Central management with Global Command Center
- Fully interoperable with Sidewinder appliances and other standards-based security devices Specifications

## 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 endpoints
- 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
- MPPE 40 to 128-bit RC4 encryption
- PAP/CHAP/MS CHAPv2 authentication
- L2TP & GRE tunneling extensions

#### Firewall

- Dynamic stateful inspection firewall
- ICSA-certified
- NAT - static and dynamic
- NAT/PAT - port forwarding
- Connection sharing
- Intrusion Protection (Snort)
- Security Policy Enforcement (Nessus)
- Web proxy cache based on Squid

#### Network

- Traffic shaping (QoS)
- IP aliases
- DHCP - client and server
- PPPoE (for ADSL support)
- Bridging (802.1d)
- RIP, RIPv2, BGP, OSPF
- RAS (dial-in)
- Dial on demand
- Fail-over / high availability
- Traffic Load Balancing
- DNS enhanced caching, masquerading, proxy, multiple DNS server proxying
- SIP Proxy
- URL filtering subscriptions available (Webwasher)
- Anti-SPAM subscriptions available (TrustedSource)

#### Management

- Logging (local and remote)
- NTP client and server
- Web management
- CLI (Telnet) management
- Initial setup via either static IP address or dynamic IP address (DHCP client)
- Administration user accounts
- RADIUS / TACACS+

#### Hardware

- Status LEDs
- WAN port - 1x10/100BaseT

- LAN ports - 4x10/100BaseT
- WAN2, DMZ, Guest, LAN
- Serial ports - 1 (dial-in, or dial-on-demand)
- Memory - 16MB Flash, 64MB RAM
- Real time clock
- Power - 5V 1.5A
- Weight - 1lb (500g)
- Dimensions - 6.5"x4.5"x1" (168mmx115mmx26mm)
- 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

Other Snapgear models and links: SG300

SG560

SG565

SG580

SG720

SG640