

# Snapgear SG560U

Thursday, 11 June 2009

The SnapGear® SG560U model is a feature-rich, compact, network security device, which is well suited to protecting small branch offices of mid-sized enterprises. It is also a great choice for cost-effectively protecting satellite offices, gas stations and restaurants, as well as SCADA installations. The SG560U enables remote office networks to easily connect their PCs and servers to the Internet via broadband (ADSL, cable, SHDSL, T-1 and T-2 circuits, etc.) or narrow-band (modem or ISDN). The SG560 provides connectivity and security features normally found 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, the SG560U can be deployed in a myriad of environments.

Should the primary broadband connection fail, the SG560 can fail over to a second broadband link, ensuring uninterrupted service. Internet traffic can also be load balanced between links, increasing bandwidth for web surfing. And if there is a complete broadband failure, the SG560 can automatically restore Internet connectivity with a dial-up connections. Recommended for: • Networks with mobile and remote workers • Complementary VPN endpoint for Secure Computing TSP and Classic Family appliances • Branch office VPN endpoint • Suitable for routing ADSL and Cable up to T1, DS1 and E1 • Central VPN for small multi-site networks • Suitable for VPN up to approximately 30Mbps (broadband and LAN-to-LAN) • Small branch offices • Integrated USB Port and support for 3G Wireless Modems

A powerful stateful-inspection firewall, service-based intrusion detection blocking and advanced Internet connection sharing protect the branch office network from the Internet. The SG560 provides three security zones (DMZ, Guest, and LAN) on separate Ethernet segments. These have appropriate default security policies. The DMZ segment can be used for publicly accessible servers (e-mail, file download etc.) the Guest segment enables mobile staff or visitors to have general Internet access only, while the LAN segment connects the entire office network. These security zones can be reconfigured as required. For example, if only one WAN connection is in use, the other can be configured as a fourth security zone.

The SnapGear SG560U is also a cost-effective VPN endpoint device that can safely connect a remote office to a central office network using secure, industry-standard VPN access methods (IPSec, PPTP, L2TP) with hardware-accelerated encryption.

The SnapGear SG560 is complementary to the SG720 firewall/VPN appliance for mid- to large-scale branch office to head office VPN deployments. For small multi-site VPN deployments, the SG560 provides a cost-effective head office solution thanks to its encryption acceleration and expanded internal resources. In this deployment scenario, an SG300 will typically be installed as the VPN endpoint device at the remote office locations. Mobile and remote workers can also gain access to the central location across the Internet by using an SG300 device or using VPN client software.

## Features

- Steel casing for SME environments
- IPSec, L2TP & PPTP VPN client and server
- Link fail -over & load balancing
- Fully interoperable with CyberGuard appliances and other standards-based security devices
- DMZ, Guest and LAN security zones
- No per-user licensing or restrictions
- Web management console
- No third-party client software required
- Central management with Global Command Center 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
- 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
- Anti-intrusion Network
- Traffic shaping (QoS)
- IP aliases
- DHCP - client and server
- PPPoE (for ADSL support)
- Bridging (802.1d)
- RIP, RIPv2
- RAS (dial-in)
- Dial on demand
- Fail-over / high availability (req v3.0 firmware)
- 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 set-up 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 - 8MB Flash, 16MB 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

Other Snapgear models and links: SG300

SG560  
SG565  
SG580  
SG720  
SG640