

# SG720

## VPN/Firewall/Load Balancer



The SnapGear™ model SG720 is the flagship of the SnapGear family of firewall/VPN appliances. With multi-megabit throughput, three fast Ethernet ports and two additional gigabit ports standard, the ICSA-certified SG720 is an excellent solution for branch offices of large organizations, as well as central offices of small to mid-sized enterprises (SME).

The SnapGear SG720 provides central site VPN, firewall and session load balancing capabilities with the capacity to securely connect hundreds of mobile and remote employees. The SNORT-based Intrusion Detection System (IDS) adds an extra security layer by detecting attacks and alerting administrators so that counter measures can be implemented quickly before the network is compromised.

With its rich feature set and rack-optimized form factor, the SG720 is a compelling enterprise-class firewall solution at a mid-market price.

### Recommended For:

- Mid to large-sized enterprise branch offices requiring a fully integrated firewall/VPN/IDS solution
- Sites needing an ICSA-certified stateful inspection firewall supporting xDSL, T-1, T-3, OC-1 & OC-3 network configurations
- Mid-sized, multi-site networks needing a central VPN appliance to connect branch offices and mobile workers
- Sites requiring a DMZ or the capability to segment a network into separate workgroup or departmental security zones
- High bandwidth Internet and remote intranet environments

### Flexible Network Configuration with Bandwidth Optimization

The SnapGear SG720 supports three 10/100 Fast Ethernet (FE) segments and two 10/100/1000 Gigabit Ethernet segments. Central and remote networks can connect to the Internet through a variety of broadband (ADSL, SHDSL and cable) or dedicated high-speed copper (T-1, T-2, fractional T-3 and full T-3) or fiber circuits (OC-1 to OC-3).

The SG720 improves available Internet bandwidth and connection uptime by providing traffic load balancing across dual WAN links while an embedded Web proxy cache, based on Squid, further accelerates Web page downloads. This makes the SG720 an excellent solution for organizations that are power Web users or have many remote offices accessing corporate intranets. Bandwidth can be further optimized through traffic shaping controls. Customers wishing to protect against access to inappropriate Web material can purchase an URL content filtering (UCF) subscription service. This works in conjunction with the URL proxy embedded in the SG720 to increase productivity and available bandwidth. The combination supports blocking, monitoring, rating and optional reporting without the need for an on-site URL database.

### Fully Integrated Intrusion Detection System Assures Maximum Security

Although all SnapGear firewall/VPN appliances defend against Denial of Service and other common attacks, the SG720 raises the bar by detecting "suspicious" activity before it escalates into a full-blown network intrusion.

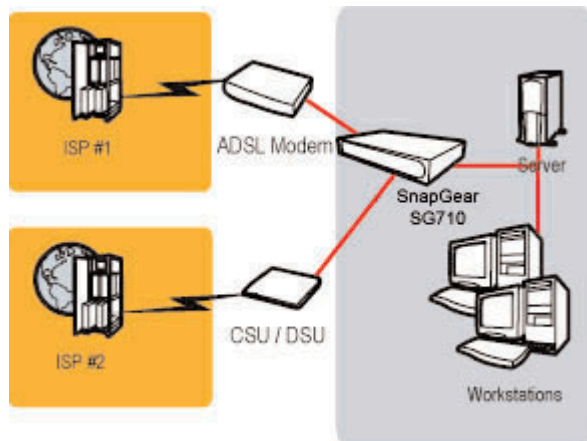
### Web Cache for Rapid Web Response Time

The SG720 incorporates a powerful Web proxy cache to improve Web page response time and reduce link loads. Designed to integrate seamlessly with upstream proxy caches provided by ISPs, the SG720 allows complete tuning of the service using the management console GUI and command-line interface.

### Failover and Load Balancing

Increase uptime and boost performance by connecting separate ports on the SG720 to two different Internet providers, and then combining these into a single "virtualized" high performance connection. A network outage on either link will automatically switch traffic to the operational link via the built-in link failover features. The resulting network redundancy makes it possible to reduce by half the number of security appliances required to protect a network while preserving maximum throughput and uptime. The traffic load-balancing feature also boosts the performance of Web transfers and the stability of a company network connected by DSL to the Internet.

# SG720



## Demilitarized Zones (DMZ)

Administrators can improve on-site and remote employee productivity without compromising security by creating DMZs that segment the network into private and public security zones. Typically, the private network will be used to secure "internal" data while the DMZ permits access to e-mail servers, Web servers, and other "public" applications and content.

## Specifications:

IPsec VPN  
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

SSH server & client  
Pass-through mode also  
MPPE 40 to 128-bit RC4 encryption  
PAP/CHAP/MS CHAPv2 authentication  
L2TP & GRE tunnelling extensions  
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 set-up 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  
RAS (dial-in)  
Failover/high availability  
Dial on demand  
RIP, RIPv2  
BGP, OSPF  
SSL/HTTPS web management

Failover  
Load balancing  
Intrusion Detection System (IDS) based on Snort Web proxy  
Cache/Accelerator based on Squid  
Status LEDs  
Three 10/100BaseT FE ports (All configurable for DMZ, LAN, WAN...)  
Two 10/100/1000 GbE ports (All configurable for DMZ, LAN, WAN...)  
Serial ports - one (console, dial-in, or dial-on-demand)  
Cryptographic acceleration  
Memory - 256Mb Flash, 256Mb RAM  
Real-time clock  
Intel Xscale IXP465 Processor  
Power - Mains AC (100 - 240 Volts)  
Weight - 4lb (2 Kg)  
Dimensions - 19" rack unit, 1RU  
Operating temperature 0C to 40C  
Storage temperature -20C to 70C  
Humidity 5 to 95%, non-condensing  
Certification - Office Use  
RoHS Compliant  
Warranty - 1 year\* in base product with 3 years available  
\*Except where required to be 2 years by law

## Features:

- 1RU rack mount case for server room/wiring closet
- Secure IPsec VPN with DES, 3DES and AES
- IDS for proactive detection and mitigation of network threats
- Session load balancing and Web proxy cache to optimise Internet traffic
- DMZ support to implement a public server infrastructure
- Unrestricted, unlimited user license
- No third-party client software required
- Web console for configuration and management
- Central management with Global Command Center