



Xnet Solutions

SN600 Product Data Sheet

(1.0)

<http://www.Xnet.com.pk/>

The SN600 hardware firewall is an ultra-high performance, high

security answer to the needs of the large sized network or ISP. As you connect to the Internet you become exposed to increasing numbers of threats. A high speed, broadband, connection enables hackers and worms easy access to your internal network. A firewall is required to keep these threats out. The SN600 can also restrict the users of your internal LAN in the services they can access on the Internet.

We are able to customise the SN600 to your needs. If you need Giga ports, Fibre-optic or wireless connectivity, have heavy encryption needs or anything else that is difficult or excessively expensive for others, let us know. We can do it.

SN600 Technical Specifications¹:

- Rackmount 2U profile;
- Dimensions: 17inch front x 3 inch height x 13 inch depth;
- Network Interfaces: 6 x 100/1000 Ethernet adaptors;
- CPU: 2GHz 64bit Processor;
- Memory: 1GB RAM, 128MB Flash;
- Chassis 100% Aluminium.

Xnet SN600 firewalls have following capabilities and features of traditionally expensive firewalls at a lower cost, including:

- Web interface (supports SSL, you may also change the port);
- Serial console interface for recovery;
- 802.1Q VLAN support;
- Stateful packet filtering including block/reject/pass rules;
- DMZ including ARP spoofing to allow a fully functional server access to the Internet;
- NAT/PAT (including 1:1, incoming and outgoing);
- SNMP client allows graphs of traffic to be generated remotely;
- Logging to a remote syslog server for detailed realtime and historical analysis;

¹ Note that specifications are subject to change without notice.

- DHCP client, PPPoE and PPTP support on the WAN interface;
- IPsec VPN tunnels (IKE; with support for mobile clients);
- PPTP VPN (with RADIUS server support);
- Static routes setup;
- DHCP server for the LAN and DMZ interfaces;
- Caching DNS forwarder;
- SVG based traffic grapher;
- Bandwidth management;
 - Multiple pipes, with multiple queues in each pipe;
 - Rule based filtering allows traffic shaping on source, destination IP address or port or packet flags;
- Firmware upgrade through the web browser;
- Configuration backup/restore;
- Host/network aliases for administrative ease.