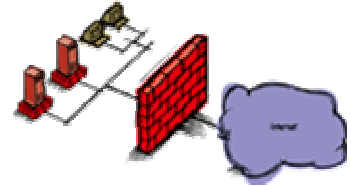


SKL Firewall v10.0 security and network firewall supports high traffic network infrastructures from small business, large enterprise and data centers. The v10.0 firewall has excellent pricing, high performance and ease of management. It has excellent expansion capabilities (depending on your hardware selection). SKL Firewall is a server made up of several network interfaces connected to different branches of different networks. Every interface allows the firewall to communicate with the zone the interface is connected to. A *zone* can be made up of one or more subnets or even all Internet. Every firewall interface can communicate with a zone. If a host belonging to the zone X wants to communicate with another host that belongs to the zone Y, it has to pass through the firewall.



Using SKL Firewall, it is possible to define the elements that can be a source or destination of a connection, assign them a name and then use the name to define the firewall rules via a web interface.

SKL Firewall now has implemented **Snort** and **Guardian** to give our clients a very powerful **Intrusion Detection System (IDS)**. An intrusion detection system is capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching, and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more.

Snort uses a flexible rules language to describe traffic that it should collect or pass, as well as a detection engine that utilizes a modular plug-in architecture. Snort has a real-time alerting capability as well, incorporating alerting mechanisms for syslog, a user specified file, a UNIX socket, or Win-Popup messages to Windows clients using Samba's smbclient. Snort has three primary uses. It can be used as a straight packet sniffer, like tcp-dump (1), a packet logger (useful for network traffic debugging, etc), or as a full blown network intrusion detection system.

Guardian is a security program which works in conjunction with Snort to automatically update firewall rules based on alerts generated by Snort. The updated firewall rules block all incoming data from the IP address of the attacking machine for any specified time. There is also logic in place which prevents blocking important machines, such as DNS servers, gateways, etc.

Virtual Private Network (VPN) is a network that is constructed by using public wires to connect nodes. For example, IPSEC, PPTP, MS-Chap and VTUND are systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption methods ranging from 0 – 1024k encryption along with other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

Spam Assassin is a mail filter which attempts to identify spam using text analysis and several internet-based real-time blacklists. Using its rule base, it uses a wide range of heuristic tests on mail headers and body text to identify "spam", also known as unsolicited commercial email. Once identified, the mail can then be optionally tagged as spam for later filtering using the user's own mail user-agent application. Spam Assassin typically differentiates successfully between spam and non-spam in between 95% and 99% of cases, depending on what kind of mail you receive.

Overall, the SKL Firewall will provide your company with the protection it needs for now and into the future. To find out more information please visit our website at www.sklservices.com or call us at 1-888-755-6864.



DATA SHEET

SKL FIREWALL v10.0

P.O Box 966, Alvin, TX 77512 281-756-9800 281-754-4436 fax www.sklservices.com

Management

- Command Line Utilities
- Intrusion Detection
- Spam filtering
- DNS
- My SQL
- Postgre SQL
- SMTP, POP3
- SNMP
- FTP
- SSHv2 Secure Telnet & FTP
- HTTP Server
- SSL/TLS RFC 2246

Security

- Secure Admin Access
- Centralized Authentication
- Traffic Management
- Read/Write and Read-Only Access Modes
- MDS Routing
- Authentication (RIPv2) RFC 1723
- SSH (secure Telnet & FTP)
- SSL/TLS (secure HTTP) RFC 2246
- S/Key(one time passwords) RFC 1760
- Access Control List
- Native IPSec (for non-firewall apps)
- DNS Client, NTP Client and Server

Internet Protocols

- IP RFC 791
- ICMP RFC 792
- ARP RFC 826
- ICMP Router Discovery (Server) RFC 1256
- CIDR RFC 1519
- Static Routes
- RIP RFC 1058
- RIP Version 2(with authentication)
- RFC 1723
- IPv6 core RFCs
- Multicast Tunnels
- IPv4 Router RFC 1812
- Boot/DHCP Relay
- Differentiated Services (EF) RFC2598
- Route Aggregation & Redistribution
- Un-numbered Interfaces

Performance

- Firewall Forwarding
- FW Connections
- VPN Connections

LAN Support

- 10/100 Mbps Ethernet
- 1000 BaseF Multi-mode Fiber (MMF)
- 1000 BaseT (1000 Mbps only)

WAN Support

- Frame Relay FRF1, RFC 1490
- HDLC Cisco

- PPP RFC 1661, 1662

Supported Standards

- IPSec (RFCs 2401-2411, 2451)
- GRE (RFCs 1701 & 1702) Generic Routing Encapsulation

System Indicators

- Power status on system
- Failure status on system
- Integrated 10/100 Ethernet port status
- Port status on network interface cards

Optional Hardware:

- Rack mount case 3U + (holds additional cards)
- 4 Port 10/100 Ethernet
- 2 Port Multi-mode Fiber
- 2 – 4 Port Copper Gigabit Ethernet

Software Specifications:

- Red Hat 9.0 Operating System
- SKL Firewall Code

Hardware Specifications:

- 2.4 GHz processor
- Integrated motherboard
- Rack mount (Std 1U Case)
- Tower Case optional
- 512K memory
- 20 GB enhanced IDE hard drive
- (2) 10/100 Network Cards Std