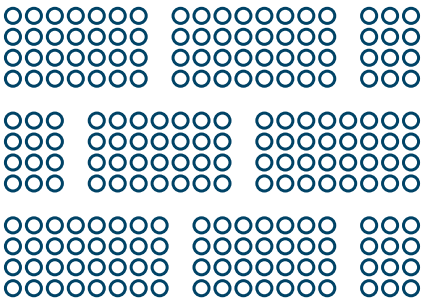
# Stonesoft Firewall/ VPN 5.6



## Firewall/VPN 5.6 Datasheet

Stonesoft Firewall/VPN is available as a physical appliance or a software or virtual solution.

**Tight integration from the ground up**
Stonesoft Firewall/VPN benefits from the many advantages of a built-in rather than a bolt-on approach to solution architecture. While other security vendors have acquired their functionality over the years, Stonesoft has built all of its network security functions from the ground up to ensure tight integration, better performance and seamless management.

**Unmatched availability, usability and serviceability**
High availability is at the core of the Stonesoft Firewall/VPN solution. Active clustering of up to 16 nodes provides great flexibility in situations where processing-intensive security applications such as deep inspection or VPNs require more performance. Transparent session failovers and support for running different hardware and software versions in the same cluster provide industry-leading system availability and serviceability without breaks. Through Stonesoft Multi-Link, high availability is also extended to cover network and IPsec VPN connections.

**Powerful management**
Stonesoft's award-winning Security Management Center is at the core of the Stonesoft Firewall/VPN solution. In addition to next-generation security and built-in high availability, users also have the ability to easily manage and/or monitor all security devices across their network – whether virtual, physical, hybrid or from another vendor.

**Advanced anti-evasion capabilities**
Stonesoft Firewall/VPN provides the industry's most advanced anti-evasion capabilities to protect against today's advanced threats and evasion techniques. It is the only security solution to protect against highly sophisticated and dynamic Advanced Evasion Techniques (AETs).

STONESOFT
A McAfee Group Company

# Stonesoft Firewall/VPN 5.6 Specifications

| GENERAL | |
|---|---|
| **Supported Platforms** | |
| Stonesoft Appliances | FW-315, 1035, 1301, 1302, 3202, 3206, 5206 appliances. See more details from appliance specific datasheets. |
| Software Appliance | X86-based systems. See more details from software appliance datasheet. 64-bit software can be used with 10 Gbps or higher licenses. 32-bit software can be used with all software licenses |
| Virtual Appliance | VMware ESX virtualization platforms. See more details from Virtual appliance datasheet |
| **Supported Roles** | Firewall/VPN (layer 3) |

| FEATURES | |
|---|---|
| **General** | IPv4 and IPv6 stateful and stateless packet filtering, circuit level firewall with TCP proxy and Protocol Agents |
| **Firewall protocol agents** | FTP, H.323, HTTP, HTTPS, IMAP4, MGCP, MS RPC, NetBios Datagram, Oracle SQL Net, POP3, RSH, SCCP, SIP, SMTP, SSH, SunRPC, TCP Proxy, TFTP, RTSP |
| **VPN** | |
| Protocols | IKEv1, IKEv2, and IPsec with IPv4 and IPv6 |
| Encryption | AES-128, AES-256, AES-GCM-128, AES-GCM-256, Blowfish, DES, 3DES* |
| Message Digest Algorithms | AES-XCBC-MAC, MD5, SHA-1, SHA-2-256, SHA-2-512 |
| Diffie-Hellman | DH group 1, 2, 5, 14, 19, 20, 21 |
| Authentication | RSA, DSS, ECDSA signatures with X.509 certificates, pre-shared keys, hybrid, XAUTH, EAP |
| Other | IPCOMP Deflate Compression<br>NAT-T<br>Dead Peer Detection<br>MOBIKE |
| Site-to-Site VPN | Policy-based VPN, Route-Based VPN (GRE, IP-IP, SIT)<br>Hub and spoke, full mesh, partial mesh topologies<br>Multi-Link fuzzy logic-based dynamic link selection<br>Multi-Link modes: load sharing, active/standby, link aggregation |
| Client-to-Gateway VPN | IPsec VPN client for Windows<br>Automatic configuration updates from gateway<br>Automatic failover with Multi-Link<br>Client security checks<br>Secure domain logon |
| **User Authentication** | Internal user database, LDAP, MS Active Directory, RADIUS, TACACS+, Stonesoft Authentication Server |
| **High Availability** | Active-active/active-standby firewall clustering for up to 16 nodes<br>Stateful failover (including VPN connections)<br>VRRP<br>Server load balancing<br>Link aggregation (802.3ad)<br>Link failure detection |
| **ISP Multihoming** | Multi-Link: High availability and load balancing between multiple ISPs including VPN connections, Multi-Link VPN link aggregation, QoS-based link selection |
| **IP Address Assignment** | Firewall Clusters: Static, IPv4, IPv6<br>Single Firewalls: static, DHCP, PPPoA, PPPoE, IPv4, static IPv6<br>Services: DHCP Server and DHCP relay for IPv4 |
| **Address Translation** | IPv4 , IPv6<br>Static NAT, source NAT with Port Address Translation (PAT), Destination NAT with PAT |
| **Routing** | Static IPv4 and IPv6 routes, policy-based routing, static multicast routing |
| **Dynamic routing** | IGMP proxy, RIPv2, OSPFv2, BGP, PIM-SM |
| **IPv6** | Dual stack IPv4/IPv6, ICMPv6, DNSv6 |
| **SIP** | Allows RTP media streams dynamically, NAT traversal, deep inspection, interoperability with RFC3261 compliant SIP devices |
| **CIS redirection** | HTTP, FTP, SMTP protocols redirection to Content Inspection Server (CIS) |

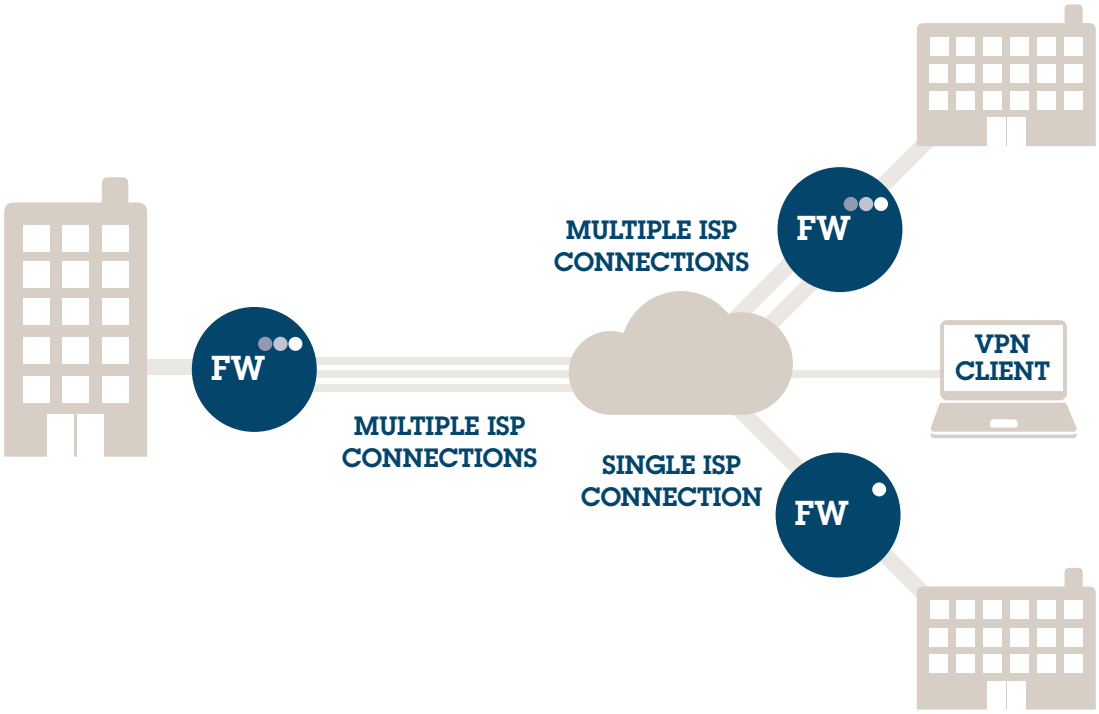
* Supported encryption algorithms depend on used license

| | |
|---|---|
| **Anti-Virus (subscription required)** | |
| Scanned protocols | HTTP, HTTPS, POP3,IMAP, SMTP |
| Engine | File-based, local signature database, automatic real-time updates |
| **Anti-Spam (subscription required)** | |
| Scanned protocols | SMTP |
| Engine | Scoring-based spam detection |
| Filtering methods | Customizable email envelope/header/content matching<br>Local Antispoofing and relay<br>Honeypot filtering<br>SPF/MX record matching<br>DNS based blacklists |
| **Web Filtering (subscription required)** | |
| Protocols | HTTP, HTTPS |
| Engine | Webroot category-based URL filtering, blacklist / whitelist |
| Database | Over 280 million top level domains and subpages (billions of URLs)<br>Support for over 43 languages<br>82 Categories |
| **Virtual Engines** | FW/VPN virtualization to separate logical engines with separate interfaces, addressing, routing and policies** |
| **Encapsulation** | Ethernet, 802.1q VLAN, PPPoA, PPPoE |
| **Access control** | IPv4 and IPv6<br>Tunneled IP<br>IP-in-IP<br>IPV6 encapsulation<br>GRE |
| **Advanced Access Control** | Interface Zones<br>Time<br>TLS information<br>Domain Names<br>User information<br>Applications |
| **Traffic Management and QoS** | Policy-based traffic shaping<br>Guaranteed / maximum / bandwidth prioritization<br>Differentiated Services Code Point (DSCP) matching / marking<br>Policy-based concurrent session limiting<br>Policy-based TCP MSS rewrite |
| **Inspection** | |
| Basic Inspection | DNS, HTTP, HTTPS, IMAP, IMAPS, POP3, POP3S, SIP, SMTP |
| Full Inspection with Add-On License | All supported protocols listed below |
| Dynamic Context Detection | Protocol<br>Application<br>File type (Flash, GIF, JPEG, MPEG, OLE, PDF, PNG, RIFF, RTF, text file, binary file) |
| Protocol Normalization | Full protocol normalization for Ethernet, IPv4, IPv6, ICMP, UDP, TCP, DNS, FTP, HTTP, IMAP, IMAPS, SMTP, SSH, NBT, SMB, SMB2, MSRPC, POP3, POP3S, SIP, TFTP, HTTPS (SSL/TLS) |
| Protocol-Specific Fingerprint Inspection | DNS, FTP, HTTP, HTTPS, IMAP, IMAPS, MSRPC, NBT, POP3, POP3S, SIP, SMB, SMB2, SMTP, SSH, TFTP |
| Protocol-Independent Fingerprint Inspection | Any TCP / UDP protocol |
| Evasion and Anomaly Detection | Multi-layer traffic normalization<br>Vulnerability-based fingerprints<br>Exploit-based fingerprints<br>Fully upgradable software-based inspection engine<br>Evasion and anomaly logging |
| Custom Fingerprint Inspection | Protocol-independent fingerprint matching<br>Regular expression-based fingerprint language<br>Snort® signature converter<br>Custom Application fingerprinting |
| TLS Inspection | HTTPS client and server stream decryption and inspection<br>TLS certificate validity checks<br>Certificate domain name-based exemption list |

| | |
|---|---|
| Correlation | Local correlation, Log Server correlation |
| DoS/DDoS protection | SYN/UDP flood detection<br>Concurrent connection limiting, interface-based log compression |
| Reconnaissance | TCP/UDP/ICMP scan, stealth and slow scan detection in IPv4 and IPv6 |
| Blocking Methods | Direct blocking, connection reset, blacklisting (local and distributed), HTML response, HTTP redirect |
| Traffic Recording | Automatic traffic recordings / excerpts from misuse situation |
| Updates | Automatic dynamic updates through Security Management Center (SMC) |
| **Management and Monitoring** | |
| Centralized Management | Enterprise-level centralized management, logging and reporting system. See more details from the Security Management Center datasheet. |
| SNMP Monitoring | SNMPv1, SNMPv2c, and SNMPv3 |
| Traffic Capture | Console tcpdump, remote capture through SMC |
| High security management communication | 256-bit security strength in engine – management communication |

| **PLATFORM CERTIFICATIONS** | |
|---|---|
| **VPN Consortium** | VPNC interoperability certified: Basic, AES, certificate, IKEv2 and IPv6 |
| **ICSA Labs** | Network Firewall, IPv6, USGv6, High Availability |
| **NSS Labs Tested** | Next Generation Firewall |
| **VMware** | Virtual appliance VMware ready certified |
| **RSA** | Secured by RSA certified with RSA SecureID and RSA enVision |
| **Arcsight** | Common Event Log format (CEF) certified |
| **Q1Labs** | Log Event Enhanced Format (LEEF) certified |
| **Microsoft** | IPsec VPN client certified for Windows Vista, Compatible with Windows 7 |

* Supported encryption algorithms depend on used license.
** Virtual Engines requires NGFW capable hardware and licensing




**Stonesoft Corporation International Headquarters**
Itälahdenkatu 22A FI-00210 Helsinki, Finland
tel. +358 9 4767 11 | fax. +358 9 4767 1349
www.stonesoft.com

STONESOFT
A McAfee Group Company

**Stonesoft Inc Americas Headquarters**
1050 Crown Pointe Parkway, Suite 900
Atlanta, GA 30338, USA
tel. +1 866 869 4075 | fax. +1 770 668 1131