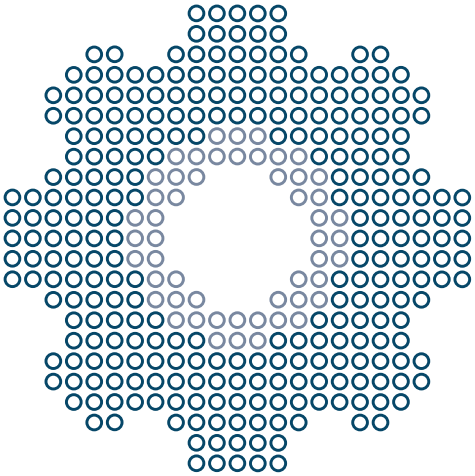

# Stonesoft Next Generation Firewall 5.6

## Stonesoft Next Generation Firewall Datasheet

- One unified software core -based design for all network security controls
- One adaptive, affordable solution for all environments
- One integrated Security Management Center
- One dynamic, contextually-aware solution

STONESOFT
A McAfee Group Company

# The Stonesoft NGFW is designed to solve the challenges that IT departments face when choosing a network security solution:

## One solution with multiple product roles

The Stonesoft NGFW can be configured to fill any needed network security product role: a traditional or next generation Firewall/VPN (NGFW), traditional or next generation intrusion prevention systems (IPS/NGIPS), Layer 2 firewall, or UTM solution.

## One unified software core

The Stonesoft NGFW is available as a physical appliance, software solution, or virtual appliance. Virtualization is supported in two ways. Virtual Appliance enables installing the NGFW solution into a virtual machine environment whereas with Virtual Engines multiple NGFW configurations may be deployed into one physical appliance. All options are software-based and receive new features and updates automatically. The solution has been designed from the ground up to offer significant performance advantages and ease of use compared with traditional multifunction products.

## One Management Center

The Security Management Center provides comprehensive contextual and situational awareness and visibility of users and applications. Administrators also have the ability to manage and/or monitor all security devices across their network – whether virtual, physical, hybrid or from another vendor.

## Self customization

The Stonesoft NGFW lets administrators choose, self-configure and change platform, capacity, security controls and features on the fly and without extra fees or new contracts.

## Anti-evasion capabilities

The Stonesoft NGFW provides the industry's most advanced anti-evasion capabilities to protect against today's advanced threats and evasion techniques.

# Stonesoft NGFW 5.6 Specifications

## GENERAL

| | |
|---|---|
| **Supported Platforms** | |
| Stonesoft Appliances | MIL-320, 1035, 1065, 1402, 3202, 3206, 5206 appliances. See more details from appliance specific datasheets. |
| Software Appliance | X86-based systems. See more details from software appliance datasheet. |
| Virtual Appliance | VMware ESX virtualization platforms. See more details from Virtual appliance datasheet. |
| **Supported Roles** | Firewall/VPN (layer 3), IPS/IDS (layer 2), Layer 2 Firewall |
| **Virtual Engines** | Virtualization to separate logical engines with separate interfaces, addressing, routing and policies |

## FIREWALL/VPN-SPECIFIC FUNCTIONALITY

| | |
|---|---|
| **General** | Stateful and stateless packet filtering, circuit-level firewall with TCP proxy protocol agent |
| **Firewall Protocol Agents** | FTP, H.323, HTTP, HTTPS, IMAP4, MGCP, MS RPC, NetBios Datagram, Oracle SQL Net, POP3, RSH, RTSP, SCCP, SIP, SMTP, SSH, SunRPC, TCP Proxy, TFTP |
| **VPN** | |
| Protocols | IKEv1, IKEv2, and IPsec with IPv4 and IPv6v6 |
| 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+ |
| **High Availability** | Active-active/active-standby firewall clustering 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** | FW clusters: Static, IPv4, IPv6<br>FW single nodes: 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) |
| **Antivirus (subscription required)** | |
| Scanned protocols | HTTP, HTTPS, POP3,IMAP, SMTP |
| Engine | File-based, local signature database, automatic real-time updates |
| **Antispam (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 |

## IPS AND LAYER 2 FIREWALL-SPECIFIC FUNCTIONALITY

| | |
|---|---|
| General | Stateless packet filtering for Ethernet protocols (Dix/IEEE)<br>Stateful packet filtering for IP protocols<br>Logical Interface matching for VLANs and physical interfaces<br>MAC address filtering |
| High Availability | Layer 2 Firewall clustering (active-passive)<br>IDS clustering (active-active / active-passive)<br>IPS serial clustering (active-active)<br>Fail-open interface support (IPS role)<br>Dynamic inspection overload handling (IPS role) |

| GENERAL FUNCTIONALITY (ALL ROLES) | |
|---|---|
| **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>Concurrent session limiting<br>Policy-based TCP MSS rewrite |
| **Inspection** | |
| 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), GRE, IP-in-IP, IPv6 encapsulation |
| Protocol-Specific Inspection | DNS, FTP, HTTP, IMAP, IMAPS, SMTP, SSH, NBT, SMB, SMB2, MSRPC, POP3, POP3S, SIP, TFTP, HTTPS |
| Protocol-Independent Fingerprinting | Any TCP / UDP protocol |
| Evasion and Anomaly Detection | Multi-layer traffic normalization<br>Vulnerability-based fingerprints<br>Fully upgradable software-based inspection engine<br>Evasion and anomaly logging |
| Custom Fingerprinting | 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 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, redirect |
| Traffic Recording | Automatic traffic recordings / excerpts from misuse situations |
| Updates | Automatic dynamic updates through Security Management Center (SMC)<br>Current coverage of over 3000 protected vulnerabilities |
| **Web Filtering (subscription required)** | |
| Protocols | HTTP, HTTPS |
| Engine | Webroot category-based URL filtering, Blacklist / whitelist |
| Database | Over 280 million top level domains and sub pages (billions of URLs)<br>Support for over 43 languages<br>82 Categories |
| **Management and Monitoring** | |
| Centralized Management | Enterprise-level centralized management, logging and reporting system. See more details from Security Management Center datasheet |
| SNMP monitoring | SNMPv1, SNMPv2c, and SNMPv3 |
| Traffic capturing | 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, certification, IKEv2, and IPv6 |
| **ICSA Labs** | Network IPS, Network Firewall, IPv6, High Availability, USGv6 |
| **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.

** Firewall/VPN role only

**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