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
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, HTTP, HTTPS, IMAP4, MGCP, MS RPC, MS SQL, NTLM, Oracle, Oracle Net, POP3, RSH, RTP, 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, NAT-T, Dead Peer Detection, MOBIKE |

### Site-to-Site VPN

Policy-based VPN, Route-Based VPN (GRE, IP-IP, SIT)

### Client-to-Gateway VPN

IPsec VPN client for Windows, Automatic configuration updates from gateway, Automatic failover with Multi-Link, Client security checks, Secure domain logon

### User Authentication

Internal user database, LDAP, MS Active Directory, RADIUS, TACACS+

### High Availability

Active-active/active-passive firewall clustering up to 16 nodes, Stateful failover (including VPN connections), VRRP, Server load balancing, Link aggregation (802.3ad), 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, FW single nodes: static, DHCP, PPPoA, PPPoE, IPv4, static IPv6, Services: DHCP Server and DHCP relay for IPv4

## Address translation

IPv4, IPv6, 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, 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

## Antispam (subscription required)

Scanned protocols: SMTP

## IPS AND LAYER 2 FIREWALL-SPECIFIC FUNCTIONALITY

### General

Stateless packet filtering for Ethernet protocols (DIX/IEEE), Stateful packet filtering for IP protocols, Logical Interface matching for VLANs and physical interfaces, MAC address filtering

### High Availability

Layer 2 Firewall clustering (active-passive), IDS clustering (active-active / active-passive), IPS serial clustering (active-active), Fail-open interface support (IPS role), Dynamic inspection overload handling (IPS role)
<table>
<thead>
<tr>
<th>General Functionality (All Roles)</th>
<th>Traffic Recording</th>
<th>Updates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encapsulation</td>
<td>Automatic traffic recordings / excerpts from misuse situations</td>
<td>Automatic dynamic updates through Security Management Center (SMC)</td>
</tr>
<tr>
<td>Access Control</td>
<td>Web Filtering (subscription required)</td>
<td></td>
</tr>
<tr>
<td>Advanced Access Control</td>
<td>Protocols HTTP, HTTPS</td>
<td></td>
</tr>
<tr>
<td>Traffic Management and QoS</td>
<td>Engine Webroot category-based URL filtering, Blacklist / whitelist</td>
<td></td>
</tr>
<tr>
<td>Web Filtering</td>
<td>Database Over 280 million top level domains and sub pages (billions of URLs) Support for over 43 languages 82 Categories</td>
<td></td>
</tr>
<tr>
<td>Management and Monitoring</td>
<td>SNMP monitoring SNMPv1, SNMPv2c, and SNMPv3</td>
<td></td>
</tr>
<tr>
<td>Traffic capturing</td>
<td>Traffic capturing Console tcpdump, remote capture through SMC</td>
<td></td>
</tr>
<tr>
<td>High security management</td>
<td>High security management communication 256-bit security strength in engine – management communication</td>
<td></td>
</tr>
<tr>
<td>PLATFORM CERTIFICATIONS</td>
<td><strong>VPN Consortium</strong> VPNC interoperability certified: Basic, AES, certification, IKEv2, and IPv6</td>
<td></td>
</tr>
<tr>
<td>ICSA Labs</td>
<td><strong>ICSAs Labs</strong> Network IPS, Network Firewall, IPv6, High Availability, USGv6</td>
<td></td>
</tr>
<tr>
<td>VMware</td>
<td><strong>VMware</strong> Virtual appliance VMware ready certified</td>
<td></td>
</tr>
<tr>
<td>RSA</td>
<td><strong>RSA</strong> Secured by RSA certified with RSA SecureID and RSA enVision</td>
<td></td>
</tr>
<tr>
<td>Arcsight</td>
<td><strong>Arcsight</strong> Common Event Log format (CEF) certified</td>
<td></td>
</tr>
<tr>
<td>Q1Labs</td>
<td><strong>Q1Labs</strong> Log Event Enhanced Format (CEF) certified</td>
<td></td>
</tr>
<tr>
<td>Microsoft</td>
<td><strong>Microsoft</strong> IPSec VPN client certified for Windows Vista, Compatible with Windows 7</td>
<td></td>
</tr>
</tbody>
</table>

**Blocking methods**
- Direct blocking, connection reset, blacklisting (local and distributed), HTML response, redirect

**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

* Supported encryption algorithms depend on used license.
** Firewall/VPN role only