STORMSHIELD

UNIFIED THREAT MANAGEMENT SOLUTIONS AND NEXT-GENERATION FIREWALLS

NETWORK SECURITY

NETWORK SECURITY | ENDPOINT SECURITY | DATA SECURITY
VISION

FUTURE-READY SECURITY
A security solution represents several years’ investment. That’s why Stormshield Network Security products give you the modularity and features you need to stay ahead of a fast-changing information technology landscape.

SEAMLESS SECURITY
In our “bring your own everything” world, it is becoming increasingly difficult to impose constraints on users while at the same time striving to be agile and in sync with current technology and trends. For security to be effective, it needs to be seamless for both users and administrators.

COLLABORATIVE SECURITY
Faced with today’s threats – which routinely bypass conventional protection systems – a new approach to security is needed.

Stormshield Network Security solutions are based on the concept of “Multi-layer Collaborative Security.” This holistic model relies on active collaboration between our different solutions’ security engines and represents the future of information system defense in depth.

TRUSTED SECURITY
Stormshield delivers trusted technologies that are certified to the highest levels in Europe (EU RESTRICTED, NATO RESTRICTED, EAL4+, ANSSI QUALIFICATION). These certifications and qualifications guarantee that the strategic information of even the most sensitive companies and organizations is properly protected.
Many organizations are shifting to the Cloud to streamline their IT infrastructure, to take advantage of technologies that significantly reduce total cost of ownership (TCO), to simplify use, and to make it both easier to upgrade and to ensure rapid restoration after an incident.

Stormshield Network Security's virtual appliances support this shift by providing the same level of protection and the same broad array of capabilities as its physical products.

Companies need to deploy a virtual, cloud-based infrastructure in a secure and controlled manner. This is why all of the Stormshield Network Security solutions’ capabilities are included in the Stormshield Network Cloud UTM application, made for Amazon Web Services environments.

- Effective protection of servers, web services, and virtual applications on an Amazon Web Services Cloud
- Simplified implementation through the Amazon Web Services Marketplace
KEEP YOUR ORGANIZATION RUNNING
The Stormshield Network Security appliances installed in sensitive and limited-technology areas provide peace of mind to organizations of all sizes.

The range as a whole includes all of the protection technology needed to resist even the most sophisticated attacks.

Stormshield Network Security’s intrusion prevention system (IPS) combines reactive target databases and proactive analysis to detect both known and unknown attacks.

PROTECT YOUR INTERNET USE
The Internet is an essential source of information and applications, but it’s important to control the way it is used.

With the advanced filter and service quality management features, you can define desired Internet use and analyze websites visited, including sites that are encrypted or that use Web 2.0 technology.

CONNECT WITH YOUR EMPLOYEES
Changing behaviors, increasing organizational complexity, and competitive pressures require that companies and their employees become more agile. Mobility, remote work, and the professional use of personal mobile devices are also new factors that you need to be able to handle with peace of mind.

With the virtual private network (IPSec and SSL VPN), employees have secure access to the company’s resources, no matter where they are and what device they’re using. The SSL VPN is particularly well-adapted to a BYOD environment.

SAVE TIME
Configuring security equipment is a critical step that needs to be both simple and thorough. Stormshield Network Security products’ administrative interface was designed to be both user-friendly and intuitive to help you secure your company quickly and avoid errors.

MANAGE VULNERABILITIES
Server and workstation vulnerabilities are like an open door to the advanced threats that are trying to infiltrate your information system. Stormshield has the only technology that effectively detects network and application vulnerabilities built into a firewall/UTM solution: the Stormshield Network Vulnerability Manager.

By analyzing network traffic, obsolete or vulnerable applications installed on workstations and servers are detected in real-time and targeted protective actions can be launched with a single click.

MEET YOUR COMPLIANCE COMMITMENTS
Stormshield Network Security products are a key part of ensuring compliance with standards, regulations, and norms for limiting access (PCI-DSS, ISO 27001, Data Protection Act, etc.).
### Hardware solution specifications

<table>
<thead>
<tr>
<th></th>
<th>Small businesses, Agencies, Subsidiaries</th>
<th>Medium-sized organizations, Agencies</th>
<th>Large organizations, Datacenters</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SN150</td>
<td>SN200</td>
<td>SN300</td>
</tr>
<tr>
<td><strong>PERFORMANCE</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall (UDP 1518 bytes)</td>
<td>400 Mbps</td>
<td>600 Mbps</td>
<td>800 Mbps</td>
</tr>
<tr>
<td>IPS (UDP 1518 bytes)</td>
<td>200 Mbps</td>
<td>600 Mbps</td>
<td>800 Mbps</td>
</tr>
<tr>
<td>IPS (1 Mb HTTP)</td>
<td>150 Mbps</td>
<td>600 Mbps</td>
<td>800 Mbps</td>
</tr>
<tr>
<td>Anti-virus</td>
<td>55 Mbps</td>
<td>165 Mbps</td>
<td>200 Mbps</td>
</tr>
<tr>
<td><strong>NETWORK CONNECTIVITY</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Max concurrent sessions</td>
<td>30,000</td>
<td>75,000</td>
<td>150,000</td>
</tr>
<tr>
<td>No. of new sessions per sec.</td>
<td>2,500</td>
<td>15,000</td>
<td>18,000</td>
</tr>
<tr>
<td><strong>VPN</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPSec (AES128 – SHA1)</td>
<td>100 Mbps</td>
<td>250 Mbps</td>
<td>400 Mbps</td>
</tr>
<tr>
<td>Max IPSec VPN tunnels</td>
<td>25</td>
<td>50</td>
<td>100</td>
</tr>
<tr>
<td>No. of concurrent VPN SSL clients</td>
<td>5</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td><strong>HARDWARE</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Redundancy (SSD, Power Supply)</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Local storage</td>
<td>SD Card**</td>
<td>SD Card**</td>
<td>320 GB</td>
</tr>
<tr>
<td>Size</td>
<td>&lt;0.5U - 19&quot;</td>
<td>0.5U - 19&quot;</td>
<td>0.5U - 19&quot;</td>
</tr>
</tbody>
</table>

### Monitoring

Firewall/IPS/IDS mode, User ID-based Firewall, Application Firewall, Microsoft Services Firewall, Detection and monitoring of mobile device use, Application inventory [optional], Vulnerability detection [optional], Filtering by location [countries, continents], URL Filtering [built-in database or Cloud mode], Transparent authentication [SSO Agent Active Directory, SLL, SPNEGO], Multi-user authentication with cookies [Citrix-TSE], Invited authentication mode, hourly programming by rule.

### Threat protection

Intrusion prevention, Protocol analysis, Application inspection, Protection against denials of service (DoS), Protection against SQL injections, Protection against Cross Site Scripting [XSS], Protection against malicious Web 2.0 code and scripts, Trojan horse detection, Interactive connection detection [Botnets, Command & Control], Protection against data theft, Advanced fragmentation management, Automatic quarantine in the event of attack, Anti-spam and anti-phishing tools: reputation analysis – heuristics engine, Built-in anti-virus [HTTP, SMTP, POP3, FTP], unknown malware detection with sandboxing, SSL decoding and inspection, VoIP protection [SIP], Collaborative security, Dynamic Host reputation, IP reputation.

### Data exchange confidentiality

Site-to-site or roaming IPSec VPN, Remote SSL VPN access in multi-OS [Windows, Android, iOS, etc.] tunnel mode, Centrally configured SSL VPN Agent [Windows], Android/Phone IPSec VPN support.

### Network - Integration

IPv6, NAT, PAT, transparent mode [bridge]/routed/hybrid, Dynamic routing [RIP, OSPF, BGP], Internal or external multi-level PKI management, Multi-domain directories [including internal LDAP], Explicit proxy, Policy Based Routing [PBR], Service quality management, DHCP client/relay/server, Client NTP, Proxy-cache DNS, Proxy-cache HTTP, High Availability, WAN connection redundancy, LACP Management, Spanning tree management [RSTP/MSTP], IETF/Netflow.

### Management

Web management interface, Object-oriented security policy, Real-time configuration support, Firewall rule use counters, More than 15 installation assistants, Global/local security policy, Built-in log analysis and reporting tools, Interactive and personalization reports, UDP/TCP/TLS syslog trace reporting, SNMP Agent v1, v2, v3, Automated backup of settings, external storage [optional].

### Virtual solution specifications

<table>
<thead>
<tr>
<th>CHARACTERISTICS</th>
<th>V50</th>
<th>V100</th>
<th>V200</th>
<th>V500</th>
<th>VU</th>
<th>V5S</th>
<th>V510</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protected IP addresses</td>
<td>50</td>
<td>100</td>
<td>200</td>
<td>500</td>
<td>Unlimited</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Protected virtual machines</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Unlimited</td>
<td>5</td>
</tr>
<tr>
<td>Vulnerability manager</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Concurrent connections</td>
<td>100,000</td>
<td>200,000</td>
<td>400,000</td>
<td>600,000</td>
<td>3,000,000</td>
<td>1,000,000</td>
<td>2,000,000</td>
</tr>
<tr>
<td>Max. No. of Vlan</td>
<td>128</td>
<td>128</td>
<td>128</td>
<td>128</td>
<td>512</td>
<td>512</td>
<td>512</td>
</tr>
<tr>
<td>Max. No. of IPSec VPN tunnels</td>
<td>100</td>
<td>500</td>
<td>1,000</td>
<td>1,000</td>
<td>10,000</td>
<td>10,000</td>
<td>10,000</td>
</tr>
<tr>
<td>No. of concurrent VPN SSL clients</td>
<td>20</td>
<td>35</td>
<td>70</td>
<td>125</td>
<td>500</td>
<td>500</td>
<td>500</td>
</tr>
</tbody>
</table>

* Performance is measured in a laboratory under ideal conditions for version 3.0. Results may vary based on testing conditions and the version of the software.

** Optional
Stormshield is a wholly-owned Airbus Defense and Space subsidiary that provides innovative end-to-end security solutions for protecting networks (Stormshield Network Security), workstations (Stormshield Endpoint Security) and data (Stormshield Data Security).

CLOUD SERVICES

CLOUD BACKUP
Automated backup of settings

With this free service, you can automatically save the most recent settings on your Stormshield Network Security appliances to Stormshield's Cloud infrastructure or one of your own servers. You can easily recover and restore your previous settings if you reboot or change your hardware, or in the event of an error.

CLOUD UPDATE
Automatic updates

The Cloud Update service automatically updates:
- Contextual signatures for the intrusion prevention system
- Applications
- The vulnerability database
- URL filtering databases
- Anti-virus signatures
- RBL servers and anti-spam approved lists
- Minor and major versions

SERVICES

SERVICE PACKS
A prolonged period of security equipment downtime can have catastrophic consequences for your company’s business. Stormshield has four simple and clear security service packs that include hardware maintenance for your product.

TECHNICAL SUPPORT

Via your partner, you have access to our multi-lingual technical support teams. These teams are based at our offices, next to the R&D teams, for better and closer collaboration. For you, this means direct access to developers’ expertise.

TRAINING

Training is provided by Stormshield or by one of our certified and authorized partners. Our Administrator and Expert programs provide you with a sound understanding of our products. These training programs include several practical exercises and result in a certification that is recognized throughout the market.

STORMSHIELD

Version 4.0 - Copyright Stormshield 2017

WWW.STORMSHIELD.EU