



STORMSHIELD



NETWORK SECURITY
STORMSHIELD

Technical Write Up
January 2020

1. About Stormshield

Stormshield, fully owned subsidiaries of Airbus Defense and Space Cybersecurity, offering innovative end-to-end security solutions both in France and worldwide to protect networks (Stormshield Network Security), workstations (Stormshield Endpoint Security) and data (Stormshield Data Security).

Stormshield is an expert in defense, cyber space and cyber security experts that dedicatedly provide solutions to highly sensitive organization like Defense, Government, and Finance institution sectors, etc.




1.1 Why choose Stormshield

Corporate networks grow more complex, e.g. the development of Wi-Fi connectivity within local networks or increasingly thorough segmentation of privileges and usage often as a result of compliance measures (ISO270X, PCI-DSS, etc.).

Stormshield is the only security vendor certified by both NATO and European Union (EU) in the market. It is the only vendor that does not compromise security by not revealing source code to any form of government body including National security agency (NSA), unlike other vendors that released which pose a danger of having backdoors.

In this context, it is a fundamental security requirement to restrict traffic on the network and to use solutions that can seamlessly apply filtering based on user identity.

1.2 Stormshield Certifications & Qualifications

	<p>Common Criteria Certifications</p>
<ul style="list-style-type: none"> • EAL 3+ / EAL 4+, granted by a European administration. • The EAL4+ certification for Stormshield products was awarded by two different European certifying organizations (France and Netherlands). 	
	<p>Standard Level Qualifications (ANSSI)</p>
<p>Stormshield Network Security has been qualified by French National Cybersecurity Agency – ANSSI, in its capacity as the national authority, and aware of the need for clarification for the market, helping companies and government authorities make a choice, by qualifying and certifying security solution. ANSSI qualification enforce a higher security check on top of the Common Criteria (CC) evaluation on the solution.</p>	
<ul style="list-style-type: none"> • Certifies that the product comply with the French security requirements. • The qualification process includes a detailed audit and review of the code related to encryption mechanisms • It guarantees organization a solution’s robustness has been tried and tested through various security test (Brute force, penetration test and etc.) • The tests are carried out under time and workload constraints (minimally 2 months or 25 to 35 man-days). • Source code has been audited and assured that it does not contain any form of backdoor. • Processes are recognized as trusted by a Member State of the European Union. 	
	<p>NATO Restricted Classification</p>
<ul style="list-style-type: none"> • NATO Restricted classification carried by a European certification body. 	



EU Restricted Classification

- EU Restricted Classification which certifies that the product has a sufficient level of confidence to protect sensitive data in the EU. The Stormshield products are the only firewall/UTM product to be referenced in the official catalog of the EU

2. Next-Generation UTM Firewall

Such segmentation, in addition to enabling the control of user access to each of the resources on the network, can offer some protection against external attacks. It also prevents the spread of viruses internally between departments.

Furthermore, if your business is subject to standards such as PCI-DSS, you are required to screen certain areas of your network. In many cases the installation of a firewall is a requirement to ensure compliance.

2.1 Windows Service Filter

Thanks to the feature that filters Windows services, you can closely manage how these services are used (Active Directory backup and restoration, IIS services, Microsoft Messenger, etc) on your network.

2.2 Availability

The optimization of network availability and connectivity is a fundamental requirement for every business and enterprise. Network failure is simply unacceptable as it can directly impact companies' business, affect sales and productivity, in addition to damaging image and credibility with customers and partners. Poor quality of service can also adversely affect employees' productivity.

2.3 Quality of Service (QoS)

Stormshield Network Security Quality of Service (QoS) feature helps to prevent network congestion and guarantees 100% reliable connectivity. Bandwidth management and traffic prioritization capabilities prevent denial of service attacks.

Certain protocols are particularly bandwidth hungry, leaving others with insufficient capacity. Video and audio codecs require a high-speed connection simply to function properly. There are also several protocols like Voice over IP that need a constant, uninterrupted connection. Last but not least, intelligent bandwidth management can contribute to preventing denial of service and other malicious attacks.

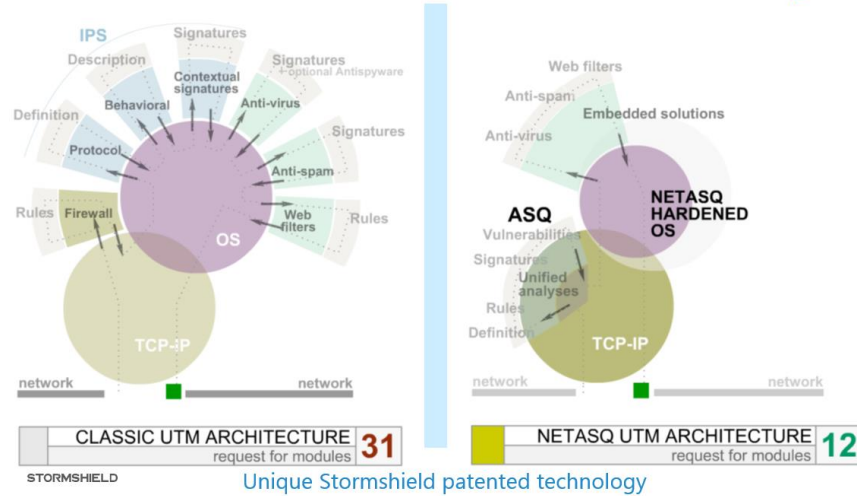
Also the IPS engine has several QoS mechanisms to protect against malicious hacking attempts. For example, the administrator can limit the amount of concurrent connections to avoid denial of service attacks.

Denial of service attacks against an internal server can be prevented by limiting the number of concurrent connections. Stormshield Network Security appliances also fully support bandwidth protocols like TOS and DSCP. To ensure the highest possible level of bandwidth management, a policy rule decision can even be based on DSCP settings from another network device.



2.4 Intrusion Prevention (IPS)

Classic IPS Architecture vs Stormshield IPS Engine



Optimal efficiency is achieved by the IPS sharing synergies with other technologies. Integrating an IPS with an application firewall, user recognition or vulnerability audit enhances its relevance. An IPS system can lie at the heart of a multifunction firewall deployed at segmentation points. It can also operate in transparent mode without the need to modify an existing network infrastructure.

Stormshield is the first who invented real-time intrusion prevention system in 1998, Stormshield UTM firewall hardcoded the IPS and firewall into the kernel, making less context switching point, hence the performance quality will still remain even when modules are turn on. It combines several protocol and behavioral analysis technologies to offer zero-day protection, detecting and blocking most threats even before they are published.

Because the IPS function provides uniquely high levels of efficiency, it is reflected in performance measurements for all Stormshield Network Security products. Stormshield Network Security’s combination of technologies allows you to choose the most appropriate protection for each threat, rather than depending solely on signatures.

2.5 Zero-Day Protection

Zero-day protection eliminates the period of vulnerability for your enterprise. Protection is available, even when vulnerabilities are exploited before public notification. Every zero-day protection signature targets an abnormal behavior. The database is updated to enable immediate detection of new threats.

Network security is a race against time in which attacks are often one step ahead of defenses. Some attacks, known as zero-day exploits, spread before any official communication can be issued. Hackers take advantage of them before software companies or the world at large can be notified.

Stormshield Network Security’s intrusion prevention engine has been designed to maximize its zero-day protection capabilities. A number of complementary technologies are deployed:

- Protocol inspection
- Abnormal behavior detection
- Hidden interactive connection detection (e.g. C&C, Botnet)
- And proactive creation of contextual protection signatures

These 4 forms of analysis are effective because they don’t have to wait for a vulnerability to appear. The linchpin of Stormshield Network Security’s zero-day protection is protocol inspection.

Stormshield’s security watch teams anticipate future attacks by continuously adding new inspections for each protocol. Thus, the SIP voice protocol already incorporates various levels of protection against identity theft and denial of service. These effective analyses are activated on all appliances.



2.6 Real-Time Vulnerability Manager

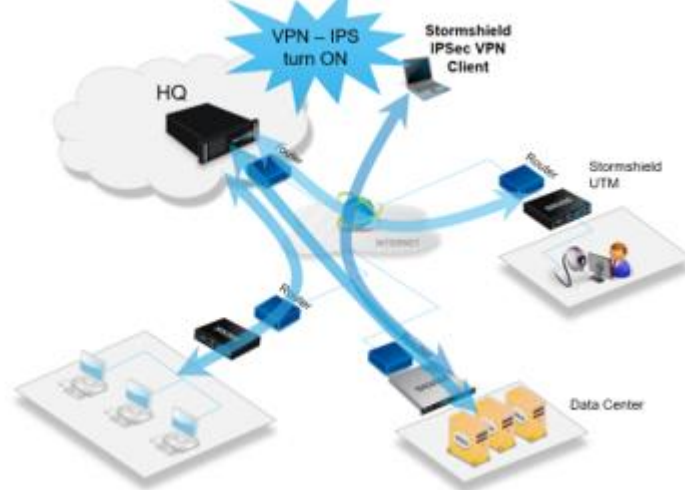
Stormshield Network Vulnerability Manager allows organization to stay ahead of new threats. To neutralize modern attacks that affect businesses of all sizes, conventional protection systems are no longer enough. The efficient and constant management of vulnerabilities is now necessary. Arm yourself with a simple and powerful vulnerability detection tool that leaves no Impact on your information system.

Based on data passing through the appliance, Stormshield Network Vulnerability Manager makes an inventory of operating systems, applications used and their vulnerabilities. This map provides you with constant visibility over your deployment. As soon as vulnerability appears on your network, you will be kept informed.

With Stormshield Network Vulnerability Manager, you can respond more quickly to internal requests relating to the compliance of your information system. You will be able to anticipate audits and thereby demonstrate the added value of your assets.

2.7 IPsec VPN

MILITARY GRADE IPSEC VPN TUNNELS



Organizations that adopt a remote working policy need to ensure service continuity, while protecting network resources at the same time. Access needs to be managed according to the company's security policies to prevent malware from being introduced into the network through unsecured channels. Providing employees with flexible remote access to the company network has long been a requirement. This practice is now a fact of life, no matter how much mobility is viewed as a threat by network managers.

Stormshield is recognized for its military grade IPsec VPN because of Diffie-Hellman implementation (e.g.768-bits min to max 8192-bits) , which provides high level of crypto tool and mechanism that support secure communication.

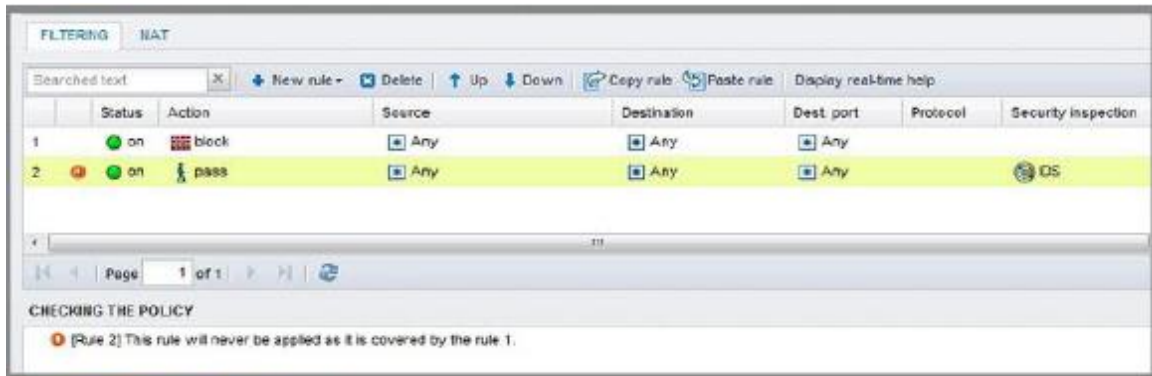
Stormshield IPsec VPN tunnel is able to turn on IPS within the tunnel. If there is a man in the middle attack, or someone trying to tap/ intercept the VPN, Stormshield IPS is able to detect, block and drop the traffic. Stormshield is the only firewall vendor that able to block this man-in-middle attack.

2.8 Trusted Encryption Technology

The IPsec VPN module on Stormshield Network Security appliances, certified and approved by European authorities, provides the highest level of trust on the market. It has undergone tests specifically to protect the sensitive data of the European Union and NATO. Using AES algorithms, the VPN module is configured to offer the most robust encryption.



2.9 Real Time Error checks



Stormshield is the first in its market to introduce a new security feature - REAL TIME SECURITY POLICY ENFORCEMENT that allows the Security Managers to further reduce mistakes while implementing rules and policies to their network.

Every error in a security policy is a potential loophole. Real-Time help is provided in the Stormshield Security Policy, informing the administrator whenever errors are detected. In addition, it greatly reduces IT deployment time, allowing them to narrow down the mistakes which save up a lot of time deployment firewall.

2.10 Reputation

With the new Dynamic Host Reputation feature, it is now possible to adjust a reputation derived from the score of a particular host or the average score of your entire environment thanks to monitoring curves.

When host reputation scores are defined as a filter criterion, your security policy can be adjusted dynamically and effortlessly. For example, you will be able to prevent hosts with undesirable reputations from accessing parts of your network or the whole network.

Geolocation

Stormshield Network Security continues to optimize the use of the filter policy. In addition to resources (hosts), users, services and applications as well as time periods, you can now filter traffic by country or continent as well.

It is the granularity offered by this approach that sets us apart from our competitors. For some of them, countries and continents have to be managed in a separate dedicated panel which would involve a configuration that applies to all filter rules.

With Stormshield Network Security, restrictions on connections can be defined to or from a certain country rule by rule.

2.11 Reports and Logs

Stormshield provides a comprehensive report, highly customizable to user preferences. Stormshield Network Activity Reports present "Top 10" reports in the categories of **Web, Security, Viruses, Vulnerabilities and Spam**. As such, the administrator will be able to view how the internet access is used, which attacks the firewall has blocked as well as the vulnerable hosts on his corporate network. Many interactive features allow the administrator to directly fine-tune the firewall's configuration. Activity reports also allow the administrator to read logs (made easy with views by types of alarms, connections, web logs, etc) generated by appliance and stored locally. Advanced filters allow these logs to be thoroughly analyzed.

- End of Document -