




STORMSHIELD

WEB PROTECTION

Features

SECURITY OF INFORMATION TECHNOLOGIES



The web today has become an indispensable tool for running a business, and is as such a favorite attack vector for hackers. Injecting malicious code into a compromised website, redirecting users to bogus and potentially infected websites or tricking users into downloading malware are just a few examples of the threats your organization faces if you do not have a defense system that is able to monitor users' web browsing and inspect the contents thereof. Furthermore, any inappropriate use of the internet in your organization may end up being your liability.

Stormshield Network Extended Web Control

Monitor how your users surf the internet on your corporate network and optimize your bandwidth consumption by deploying an efficient and best-of-breed URL filtering solution.

Stormshield Network Security proposes a cloud-based solution for the advanced monitoring of web browsing, allowing you to stay ahead of threats and protect your infrastructure. Setting up a solution to monitor web browsing will allow you to meet the following needs:

OPTIMIZATION OF BANDWIDTH CONSUMPTION

Watching video content or visiting websites that are not work-related can up the amount of bandwidth that your internet access consumes. Monitoring your corporate users' web browsing and controlling which websites to authorize ensure the optimal use of your bandwidth.

COMPREHENSIVE MONITORING OF WEB BROWSING

More than 65 categories provide a rich URL filter feature. You can therefore configure your security policy as finely as possible according to the departments in your company. For example, the marketing department may access social networks whereas other services will not be allowed to do so, thereby ensuring better productivity. Furthermore, the use of time slots allows creating flexibility in the URL filter policy at certain times of the day, making it possible for you to meet employees' requirements.

PREVENTION OF WEB-BASED THREATS

There is no longer a need to prove how widespread the use of the internet has become. The number of websites online has increased by 5000% in 12 years and 60% of these sites are less than 2 years old. Incidentally, they are the resources that cybercriminals prefer for launching attacks. Even though 87% of attacks originate from malicious URLs, they can also affect reputed websites. The right security solution therefore needs in-depth and continuous knowledge about the web traffic in order to guarantee that your company's users surf safely.

Benefits:

- Prevention of all web-based threats
- Employee productivity
- High granularity of URL categories
- Advanced features available on the whole Stormshield Network Security range
- Protection of the corporate image

.....



PROTECT YOUR LEGAL INTERESTS

In some countries, CEOs may be held criminally liable for users on their networks visiting illicit websites. A granular URL policy makes it possible to prevent visiting such sites. Stormshield Network Security Extended Web Control enables organizations to block specific websites, without interfering with employee access to appropriate sites and their day-to-day work.

Every Stormshield Network Security appliance includes an integrated URL filter which identifies and classifies millions of websites. A range of data sources are regularly scanned in order to update the URL database using a processing algorithm.

PROTECTION AGAINST MALICIOUS EMBEDDED CODE

Web browsers have become complex applications that are able to interpret JavaScript code in cloud-hosted applications. This complexity comes at a price. Every year, the major browsers on the market fall prey to security flaws that can allow the execution of malicious code on targeted workstations.

Thanks to its expertise in application recognition technology, Stormshield's Next-Generation firewalls do not only allow or block applications. Stormshield Network Security's technology also protects you from attacks encapsulated in these complex application traffic packets.

For example, JavaScript code in web-based applications is inspected in real time by the application intrusion prevention engine. Many attack and escape techniques are recognized and the detection of attacks is not restricted to known attacks. Abnormal application behavior is isolated and malicious code is deleted without disrupting legitimate browsing. And thanks to SSL traffic inspection, no code injection or malicious program can be hidden within encrypted protocols and your network perimeter will be fully protected.


Antispyware & Antiphishing

The internet brings with it new security risks such as spyware and phishing, which enable criminal attacks on company networks and private individuals. Bodies such as the Anti-Phishing Working Group which monitor such illegal activity believe that the incidence of attacks will only grow and become increasingly sophisticated.

Malicious software is often installed via freely distributed applications, videos or animations which are willingly downloaded. They remain undetected by the user and are extremely persistent. Information gathered in this way may be used for advertising targeted specifically at the user. The consequences of stolen credit card details are obvious and can be much more dangerous.

Spyware programs collect personal information, and can take control of the user's computer. They do this by installing software onto the user's computer without their knowledge, redirecting web browser activity.

.....



Phishing is criminally fraudulent activity. Sensitive information including usernames, passwords and credit card details are obtained by impersonating a known and trustworthy organization, such as a bank, and using standard emails to request personal data. Phishing is now developing further to take advantage of SMS and VoIP communications.

The development of the intrusion prevention engine is based on more than 10 years of research from 2 companies that specialize in security (Arkoon and Netasq). The engine incorporates the latest technologies and uses a number of different analyses to deliver enhanced levels of security. It also includes a choice of embedded antivirus solutions; a choice of either ClamAV® or Stormshield's custom-designed Kaspersky® solution.

Stormshield Network Security provides multi-level protection against spyware and other malware applications for your users through a combination of antispam, contextual signatures and web filtering. When delinquent applications are detected, an alarm alerts the administrator who can then clean the infected machine. The most stringent levels of security are guaranteed by automatically updating spyware and malware lists in addition to antivirus databases.

Antispam analysis determines the deceptive techniques used by offenders and identifies phishing.

.....

ABOUT

Arkoon and Netasq, fully owned subsidiaries of Airbus Defence and Space CyberSecurity, run the Stormshield brand and offer 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).

All trademarks are the property of their respective companies.



STORMSHIELD

Phone

+33 9 69 32 96 29

The cost of a call may vary according to the country you are calling from and your telecoms operator.

WWW.STORMSHIELD.EU

Netasq

Parc Scientifique Haute Borne - Parc Horizon, Bat 6, Avenue de l'Horizon 59650 Villeneuve d'Ascq - FRANCE

Arkoon & Netasq © Copyright 2014