STORMSHIELD

PROTECTING YOUR MAILBOXES

Features

SECURITY OF INFORMATION TECHNOLOGIES

In 2013, 50% of businesses would have experienced a virus infection by e-mail. Electronic mail remains one of the preferred vectors for introducing and spreading malicious programs within an information system.

Indeed, just simply sending an e-mail, whether it has a specific target or is sent to a wide group of recipients, allows a malicious user to very easily reach its targets by playing on their curiosity. The flourishing use of personal mobile terminals without the corporation's protection or supervision to access its IT resources poses an additional risk.

90% of the e-mails received today turn out to be spam. Deleting these irrelevant and sometimes malicious messages to prevent congestion in mail servers, maintain employee productivity and protect the information system has become a real challenge.

> 90% of the e-mails received today turn out to be spam.

An adapted response to the protection of electronic mail lies in the antivirus and antispam engines on Stormshield Network Security solutions.

Antivirus

EVOLVING THREATS

The social network boom, the upload of web 2.0 content by internet users and the use of personal terminals in the professional context have opened new avenues for cybercrime. Attackers are using increasingly sophisticated malicious content to achieve their goals.

Malicious code is designed to become less easily detectable by conventional protection systems. Since malicious content can hold up your information system, you will need to deploy advanced protection solutions that have what it takes to handle this type of threat.

MOBILITY AND NEW USER HABITS

The emergence of mobile devices has led to new ways of using the corporate network. A growing number of employees now use their personal terminals – often poorly or not protected – to log on to the company's information system.

These devices have become the favorite target of cybercrime, since they are not supervised by security teams and escape their control most of the time.

To keep up the all-round protection of the network against the malware that may be lurking on these devices, what is needed is the installation of an antivirus solution placed directly in the path of network traffic.

PERIPHERAL PROTECTION

Rather frequently, the antivirus solutions deployed on workstations and servers are part of the problem on a section of the whole fleet: a neglected or failed installation, an inactive agent, an outdated antivirus database, wrong configuration, etc. Such a situation can endanger your information system if a complementary malware protection solution is not implemented on your network filter devices.

The antivirus technology on Stormshield Network Security appliances is always equipped with the latest signature updates. Applying an antivirus inspection on the traffic of all devices connected to the network, it does not require the deployment of any agent. As such, mobile terminals that log on to the internal mail system also benefit from protection against threats that spread by e-mail.

Benefits:

- Recognized antivirus and antispam solutions
- Peripheral protection, even devices without a local antivirus are protected
- Protection from re-infection by preventing propagation
- Protection against sophisticated malicious content
- 99% of undesirable messages detected

Antispam

Spam and malicious e-mail cost millions of dollars in lost productivity, slow down company networks and waste the time of network administrators. E-mail is now an essential business tool for most companies.

However, with spam accounting for 90% of all e-mail messages, it is important to have a solution that addresses this problem while ensuring that legitimate messages are delivered to the intended recipient.

OPTIMAL PERFORMANCE

Stormshield Network Security's unique architecture combines two technologies to create a highly effective double barrier to protect against spam. DNS-based blacklists use reputation analysis to identify spam senders and enable your network administrator to create blocking lists to combat them.

Stormshield Network Security allocates a 'confidence index' to each blacklisting server, allowing your administrator to choose which to interrogate. A whitelist of legitimate e-mail servers is updated daily to reduce the likelihood of false positives and ensure that legitimate messages arrive safely.

Stormshield Network Security's powerful engine heuristically examines message headers and content, using empirical rule and semantic analysis, detecting counter-measures employed by spam senders and even analyzing HTML code. Any new category of spam, including image spam, will be detected.

ISP tests have shown that analytical engine from Stormshield Network Security blocks up to 99% of unwanted mail, without affecting legitimate messages. Crucially, these multiple levels of analysis are performed in parallel to offer maximum efficiency without affecting performance.

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).

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