STORMSHIELD

MOBILITY & INTERCONNECTIVITY

Features

SECURITY OF INFORMATION TECHNOLOGIES

Frequent changes to the structure of enterprise workforces mean that many are moving away from the traditional model of a single site where all the employees are physically based. Telecommuting, increasingly mobile sales forces and the dispersal of employees over multiple sites make it inevitable for network infrastructures and IT systems to change and adapt.

Mobile and interconnect solutions must be implemented to support the use of laptops, tablets and smartphones. To be effective, remote workers must be able to access all types of information, even when it is confidential. Secure access is therefore an absolute requirement.

Virtual private networking technology has become the answer to the corporate need for interconnectivity and mobility. IPSec VPN functions are embedded in Stormshield Network Security appliances, allowing corporations to link up multiple sites in total security. Nomad workers or telecommuters would then be able to log on to their corporate network via Stormshield's IPSec VPN client. Using an IPSec VPN guarantees the highest level of security as our appliances' source code for this feature has been audited to meet the requirements of the most sensitive organizations.

To be effective, remote workers must be able to access all types of information.

Stormshield Network Security appliances also support SSL VPN, a convenient and secure solution for remote access. A simple browser or a lightweight agent allows users to access the network from any device (PC, tablet, smartphone running Android, IOS, Windows, etc). Unlike a dedicated SSL VPN solution located within a DMZ, integration within the Stormshield Network Security appliance guarantees that all VPN traffic will be scanned.

Both technologies are complementary and the administrator can define profiles on a per-user basis to ensure access is restricted only to authorized personnel. Combining both VPN technologies allows the administrator to choose the most appropriate technology to manage both mobility within the enterprise and interconnectivity between sites.

IPSec VPN

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.

Geographically distributed enterprises with a number of branch offices also need to offer secure communications between sites and share centrally hosted content and resources. However, security must not affect network availability, which is vital to customers.

IPSec delivers real interoperability and a host of other benefits. As an Internet Engineering Task Force (IETF) standard, it has been widely adopted by vendors. An independent standard offers unparalleled flexibility. Users may choose the encryption and authentication algorithms that are best suited to their requirements and a key length compliant with local legislation and appropriate to their need for confidentiality.

Stormshield's VPN client enables the establishment of secure remote connections via IPSec VPN tunnels. Installed on remote devices, the client works in association with the IPSec VPN gateway functions integral to the Stormshield Network Security operating system. The presence of IPSec at the network layer delivers encryption, connection integrity and control of access via unsecured channels. This guarantees customer confidentiality and authenticity of data streams.

A COMPREHENSIVE, REAL-TIME SCAN OF THE DATA STREAM

The Stormshield VPN solution goes one step further. Once all the above criteria have been met, the Stormshield Intrusion Prevention Engine will conduct a comprehensive, real-time scan of the data stream across the secured tunnel. This prevents infected remote hosts from spreading malicious software or advanced attacks on the corporate network.

This is one of the reasons why our customers have adopted Stormshield VPN solutions and benefit at the same time from the unparalleled intrusion prevention features delivered by the IPS engine.

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.

FLEXIBLE IMPLEMENTATION

Stormshield Network Security appliances contain a VPN module which can create VPN tunnels either between VPN gateways (firewall to firewall) or between a VPN gateway and a VPN client installed on a remote device.

OPTIMAL SECURITY ON ANY NETWORK CONFIGURATION

A Hub & Spoke architecture means that Stormshield can guarantee failsafe security. Traffic can be analyzed at the central site (the "hub") as it arrives, either from multiple sites or from roaming connections (the "spokes"). As all Internet traffic is analyzed by the central site, the possibility of a roaming device getting infected by malicious web traffic is therefore eliminated.

OPTIMAL SECURITY REGARDLESS OF THE AUTHENTICATION METHOD

A number of authentication methods are offered to facilitate the setup of IPSec VPN tunnels: pre-shared keys, X509 certificates and even X-Auth.

EASE OF INSTALLATION AT NO INCREMENTAL COST

Stormshield's VPN client has a configuration wizard to enable rapid implementation of VPN tunnels. This makes it a particularly profitable solution for integrators. Configurations are stored in a single file, making deployment of the VPN Client as easy as copying a file to a directory.

SSL VPN

Connection devices for roaming networks now range from portable PCs, tablets and smartphones to public computers. Network managers must respond flexibly to support a variety of access methods, without losing sight of the need to continue guaranteeing the highest levels of security and confidentiality. When they need to access resources on the corporate network, nomad users usually have no choice but to log on to unsecured networks on which they might not be able to use IPSec (Wi-Fi networks in hotels, restaurants, airports, etc). SSL VPN is a key technology in this respect.

Stormshield Network Security solutions are designed to deliver roaming access without compromising your security. Connections crossing this VPN tunnel are secured by the native intrusion prevention technology integral to all Stormshield Network Security appliances.

- Ability to connect from any device with a web browser or a lightweight agent
- Perfectly adapted to BYOD environments (available for Windows, iOS and Android devices)
- Full access to internal resources
- Delivers exceptional security levels
- Personal configuration
- Security for all users
- Protection for all data streams

Stormshield's SSL VPN supports two access modes: one allows users to access web applications such as web mail and intranet servers through a simple web browser while the other provides full access to office networks, similar to a local connection. Full access is granted using a lightweight agent available on Windows (Stormshield Network SSL VPN agent), on Android or iOS (with a standard OpenVPN Connect agent). This helps to provide any BYOD device with a remote access.

Stormshield Network SSL VPN and OpenVPN Connect agents can be downloaded directly from the appliance and the configuration of the Stormshield Network SSL VPN agent can be deployed simply and centrally.

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