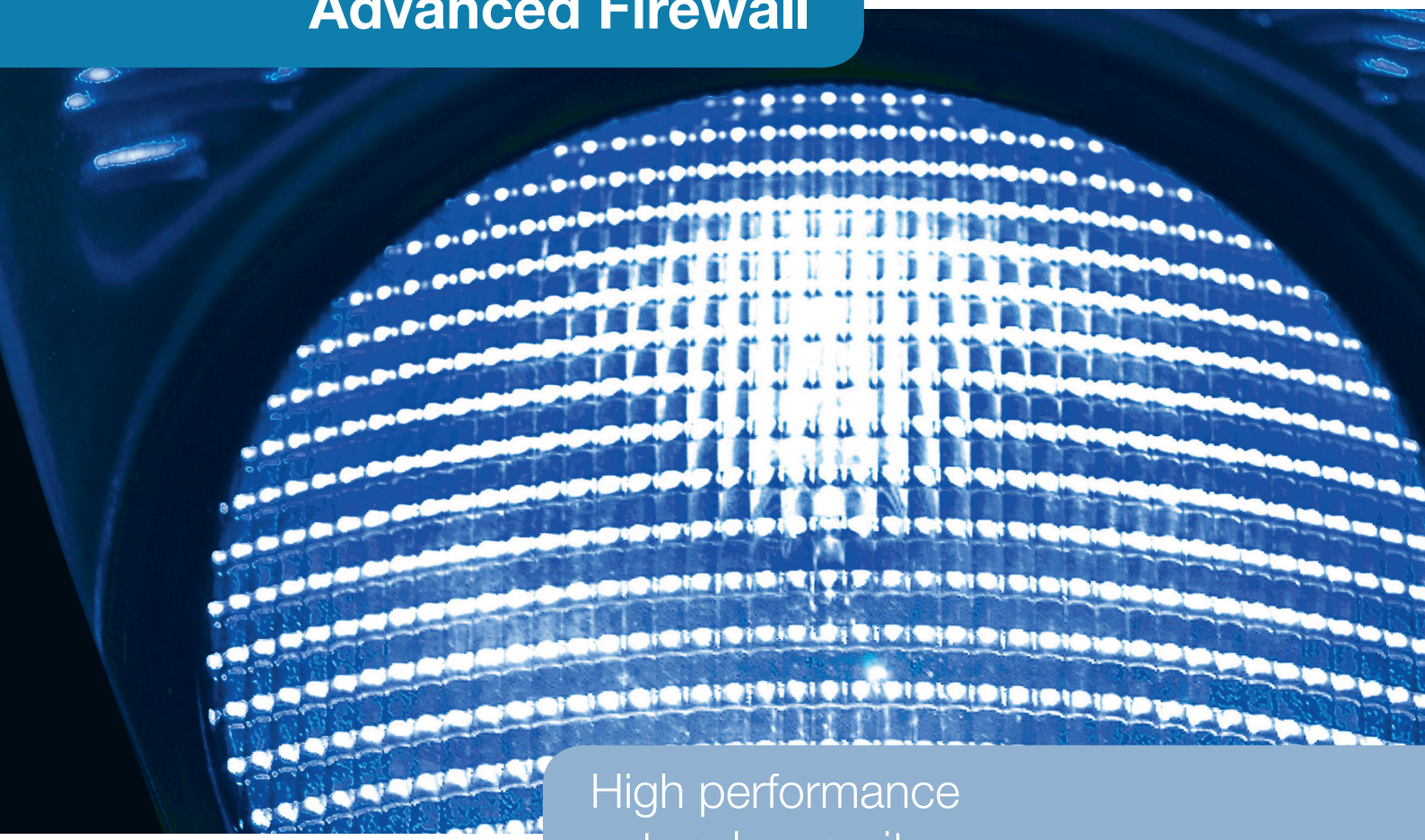
smoothwall®
Web Filtering + Security

Advanced Firewall



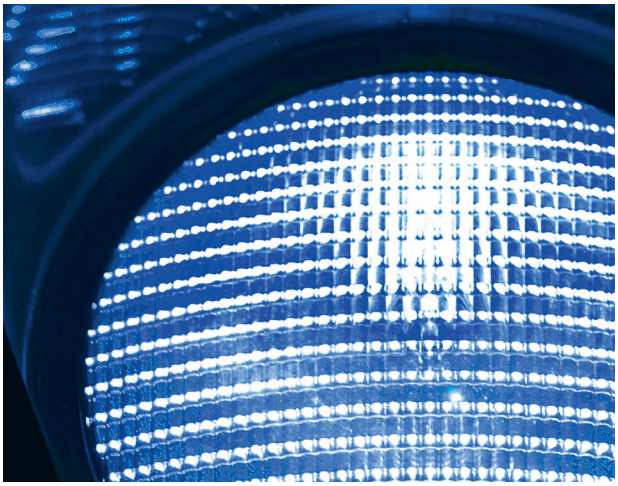
High performance network security

Protect and secure networks, prevent unauthorised access and block the spread of viruses and other malicious code.

- **Perimeter Firewall**
  Block threats at the network boundary
- **Internal Firewall**
  Control access by segregating networks into zones
- **Intrusion Detection System**
  Strategically defend against external attacks
- **Integrated VPN Gateway**
  Provide secure connectivity for remote/wireless users

Advanced Firewall

Advanced, robust and flexible network security



Smoothwall firewalls combine the functions of perimeter and internal firewalls to provide robust, advanced and scalable protection. Outbound filtering and a built-in VPN gateway allow a flexible and secure level of control over all network and Internet access.

Smoothwall firewalls are available in a range of software and hardware appliances. They can also be combined with other add-on modules (Web Content Filtering, Email Security, Anti-Spam & Bandwidth Management) to form a complete Unified Threat Management solution. For more information please see individual product datasheets or discuss with a technical representative.

* Only available on certain products.

External Attack Defence

A variety of methods are used to protect private local networks and servers from external attack. All unauthorised traffic is blocked and incoming data is analysed for threats using a sophisticated Intrusion Detection System. **Stateful Packet Inspection** is used to ensure that all packets that are part of a complete legitimate sequence and **Deep Packet Inspection** technology ensures that the traffic patterns of port agile software, such as Peer-to-Peer networks, are detected and blocked, before they eat into your bandwidth.

Security through Segregation

Often ignored, the threat from within can be greater than from external hackers. Segregate local networks and DeMilitarised Zones (DMZs) into multiple physically separate zones to protect mission critical systems and confidential information from accidental access, inquisitive users or malicious interference.

Internet Access Control

Outbound (egress) filtering rules put you in control of exactly what Internet services and ports users can access, significantly decreasing the risk of external threats. Integration with User Authentication systems (such as Microsoft Active Directory®) also allows access to be controlled based on **authenticated** user identity rather than **assumed** identity derived from a computer's IP address.

VPN Gateway

Site-to-site (inter office) VPN connectivity is supported, alongside **SSL VPN** and **Secure Remote Access** for mobile users, home workers and wireless (WiFi) connections. Several hundred VPN tunnels can be configured if necessary, distributed across multiple Internet connections.

Load Balancing*

Multiple Internet connections can be used more efficiently and resiliently by load-balancing both outgoing and incoming traffic across two or more connections. High priority traffic can be separated using protocol specific routing and in the event of an ISP/connection failure, all traffic is automatically re-routed to an alternate ISP/connection.

Unified Threat Management

Smoothwall firewalls can be extended to form full Unified Threat Management (UTM) solutions, which combine multiple security functions on a single UTM appliance at the network perimeter. Smoothwall offers both software and hardware-based UTM appliances; for further information please refer to the Unified Threat Management brochure.

Smoothwall
1 John Charles Way
Leeds LS12 6QA
United Kingdom

+44 (0)800 5 999 040 UK
+44 (0)870 1 999 500 International
sales@smoothwall.net
www.smoothwall.net

05 | 2011