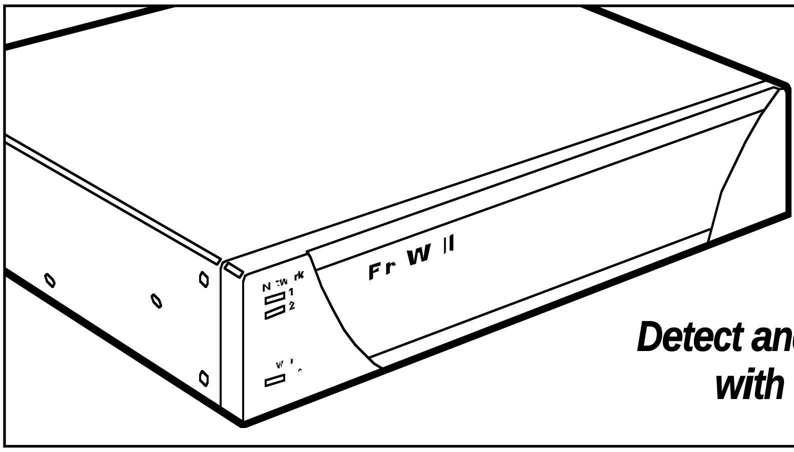
BLACK BOX®
NETWORK SERVICES

Black Box Network Services • 464 Basingstoke Road • Reading, Berkshire, RG2 0BG • Tech Support: 0118 965 6000 • **www.blackbox.co.uk • e-mail: techhelp@blackbox.co.uk**

BLACK BOX® FIREWALL



Detect and prevent attacks in real-time with this upgradable firewall.

Key Features

- ***Stateful inspection firewall that detects 70 types of attack.***
- ***Can also be used as a broadband router.***
- ***VPN capabilities make it ideal for teleworkers.***
- ***Ideal for applications with up to 50 users.***
- ***56-bit VPN encryption. Upgrade to 128 bits also available.***
- ***Keeps logs of all attempted attacks.***
- ***DMZ protection for Web or FTP servers.***
- ***Ports autosense 10 and 100 Mbps.***
- ***Includes 1 free year of software updates.***

If your business or organisation is like most others today, you depend on the Internet to streamline your operations and communications. But, of course, this route can expose your network to intrusion or hacking.

The full-featured BLACK BOX® FireWall provides you with the power, flexibility, and high-level security you need to not only protect your network's users but leverage your Web-based approach.

This hardware/software firewall helps to protect small- to medium-sized organisations (with up to 50 users) from outside intrusions. It's ideal for small or home office (SOHO) uses or applications where you need to protect an exchange of data between central and branch offices or traveling co-workers, whether it's via an intranet or your Web servers.

With its bandwidth-management capabilities, the firewall can be used to split your network users into groups and allocate bandwidth where it's needed most. You even get a statistical breakdown of how it's been used by each host.

Connect users through the firewall's autosensing 10-/100-Mbps Ethernet ports. Depending on the firewall licence you buy, you can use two or three of the connections. Just plug your Internet connection into one port on the BLACK BOX® FireWall and an Ethernet switch into another, and then use the third port to connect your FTP or Web server and keep it protected within a ”demilitarised zone” (DMZ) that stands independent of the rest of your network.

The firewall supports up to 5000 simultaneous sessions. For the first year that you own the firewall, updates for all the newest break-in methods that it protects against are free. After that, there's a charge (which Black Box offers as Upgrade Extensions of one or two years).

Multilayer detection

The ASQ (Active Security Qualification) of the BLACK BOX® FireWall detects up to 70 forms of attacks in real-time, whether they're context, non-context, or application-level attacks. Many competing SOHO firewalls fall short in this category, and many higher-end firewalls only offer protection against 30 types of attacks.

The firewall's multilayer ASQ technology examines data passing through it, groups it, and compares it to its global knowledge base to determine if it's safe. It does this by performing four types of inspections:

- Packet format analysis
- Connection analysis
- Global context analysis, and
- Data applications program analysis.

With the *packet format analysis* method, the firewall rejects packets that could be used to generate hacking in some systems by means of a knownattacks base. This analysis enables the firewall to manage attacks with no context.

The BLACK BOX® FireWall uses the *connection analysis method* to better apply security policies at the filtering level by, for example, suppressing the opening of temporary ports for return packets. By analysing connection content, the firewall can detect specific types of hacking and their context. Through this method, you can use the firewall to assemble logs with accurate and pertinent statistics that aid in traffic management.

Global context analysis goes one step further. It's what makes the ASQ technology truly powerful. With it, the BLACK BOX® FireWall meticulously examines all activity on the network so you can detect "developed" attacks—attacks with context.

You can also monitor data in transit and prohibit access to specific Web sites, mask SMTP banners, monitor certain FTP actions, prohibit the relaying of e-mail, and more. The firewall does this by using a *data applications program analysis* that authorises protocols and verifies the consistency of your data applications. Even better, it does all this without severely affecting the rate of your data flow.

Intuitive configuration

ASQ technology not only gives the BLACK BOX® FireWall its sophisticated detection and protections capabilities, but it also provides powerful tools to assist you with its configuration and maintenance.

Configuring the firewall is easy and intuitive. It comes with a management tool that simplifies the setup process. Once the firewall is installed, you can configure it in three easy steps, all of which can be done through a user-friendly Windows® based GUI application that's included with the firewall.

First, you configure your network parameters for the interfaces and default router; then, configure all connected objects (including user workstations and external networks and services) by dividing them into groups; and, lastly, configure the filtering rules for users and services, as well as groups of users and services.

Access to the firewall's settings is password-protected, and all exchanges between the administration console and the device are encrypted in 128-bit TSL.

You also get a reporting tool—a real bonus, since many other firewall manufacturers offer this only as an add-on accessory, which inflates the total cost. With the BLACK BOX® FireWall's integrated reporting functions, you can compile detailed reports based on the firewall's logs.

Routing capabilities, too

You also get a broadband router in the same box. With Asymmetrical Digital Subscriber Line (ADSL) routing capabilities built in, the firewall doubles in most cases as a DSL router. When you open your network to the Internet via ADSL technology, the firewall safeguards and manages the connections to your public servers.

In addition to data routing, the BLACK BOX® FireWall enables you to establish dialup access redundancy and perform address translation. The firewall is compatible with standard ADSL Point-to-Point Tunneling Protocol (PPTP) and (Point-to-Point Protocol over Ethernet (PPPoE) and is typically used alongside an ADSL modem (because the BLACK BOX® FireWall *cannot* be used as a DSL modem.).

Use to establish VPNs

You can also use the BLACK BOX® FireWall to set up virtual private networks (VPNs), so you can distribute your organisation's resources in an efficient yet secure way by using a Web-based infrastructure. This way, you can avoid the expense of providing dedicated lines to each user in the communications network.

The firewall ensures privacy by tunneling communications while it checks VPN traffic and actively prevents attacks launched through VPN tunnels.

With IPSec VPN features, the BLACK BOX® FireWall encrypts communications and sends them through multialgorithm VPNs. All numbering takes place at the network level, which means no information (except for IP addresses of the origin and destination firewall) is visible in the public area.

To configure the firewall for VPN, just identify the linkups and their properties, such as whether each is a machine or network, their origin and destination, and the protocols involved. The VPN component then automatically numbers and/or authenticates according to the IPSec standard the communications you've defined. Encrypt as you like either the exchanges between two networks or just between specified user machines.

The BLACK BOX® FireWall supports five encryption methods: DES, 3DES, Blowfish, Cast128, and AES. These provide you with the highest throughput and security. The firewall also offers full compatibility with any other IPSec compliant device.

Compliance with the IPSec standard makes the firewall a highly flexible device that's compatible with many existing products. That's because the standard works entirely independent of encryption and authentication algorithms. You can choose numbering and authentication algorithms that best suit your level of confidentiality.

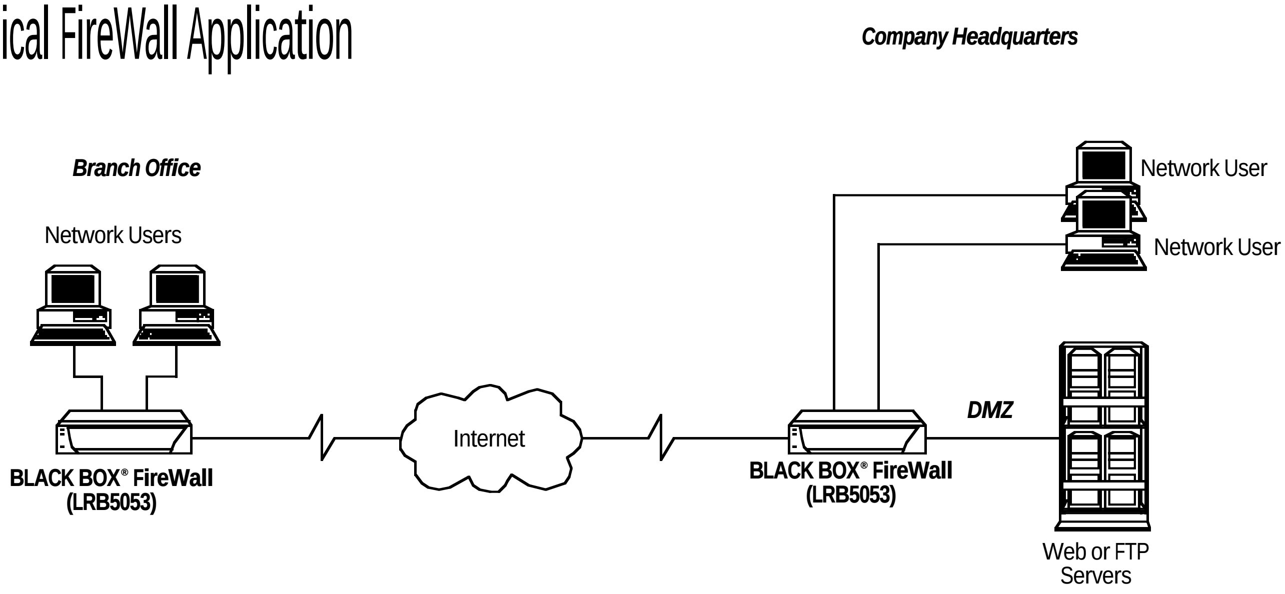
The standard BLACK BOX® FireWall offers 56-bit VPN encryption. For even more security, you can upgrade to 128 bits as an option.

Advanced filtering options

As an option, you can add URL filtering to the BLACK BOX® FireWall. This feature, which gives you a way to enforce a controlled Web-access policy on your network, enables you to manage and supervise the rights and restrictions of users when they log onto the Internet. You can define 10 profiles of URL filtering by the origin, the URL group, and the activity—all without having a subscription to the list of URLs.

By examining a log file dedicated to your Web connections, you can glean information on URLs and pages visited, duration of connections, volume of data transmitted, and more. And, for each user, you can choose the categories of Web sites they can and cannot enter. This level of control not only helps you ensure productivity and control bandwidth, but it can also keep users from engaging in Internet activity that's illegal or serves the basis for legal action against your company or organisation.

A Typical FireWall Application



Keep your server safe from attack by placing it within a DMZ.

Specifications

Filtering: Dynamic mode; from Physical to Application levels; in and out of interface; IP addresses; protocols including IP, TCP, UDP, ICMP, GRE, GMP; services including e-mail, FTP, http; context management filtering by connections and/or packets; time/day scheduling; configuration

Memory: 32 MB RAM, 65 MB Flash

Protocols: IP, ARP, TCP, UDP, ICMP, HTTP, IPsec, PPTP/PPPoE

VPN: PPTP management (40- and 128-bit MPPE); IPsec remote access management; IPsec gateways management; Manual, preshared key (PDK), or PKI management; IPsec UDP tunneling; DES, 3DES, BlowFish, CAST, or AES algorithms; Remote VPN client

Connectors: Ethernet: (3) RJ-45; Console Port: (1) DB9

Indicators: LEDs: (1) Power, (1) Network Activity

Power: 85–264 VAC, 50–60 Hz, autosensing

Size: 1.75"H x 9.5"W x 8.5"D (4.4 x 24.1 x 21.6 cm)

Weight: 4.4 lb. (2 kg)

Ordering Information

ITEM	CODE
BLACK BOX® FireWall	LRB5053
You'll also need Licence Keys for your firewall application.	
Licence Keys	
2 Ports, 25 Users	LRB5053-LK2/25
2 Ports, Unlimited Users	LRB5053-LK2/UNL
3 Ports, Unlimited Users	LRB5053-LK3/UNL
You may also need…	
56-Bit to 128-Bit VPN Upgrade	LRB5053-LK-VPN
URL Filtering	LRB5053-LK-URL
2-Port Update Extension, 1 Year	LRB5053-LK2-UPD-1
2-Port Update Extension, 2 Years	LRB5053-LK2-UPD-2
3-Port Update Extension, 1 Year	LRB5053-LK3-UPD-1
3-Port Update Extension, 2 Years	LRB5053-LK3-UPD-2