

# BizGuardian 3.3

Technical Evaluation

---

An NSS Group White Paper



First published December 2002 (V1.0)

Published by The NSS Group  
Oakwood House, Wennington, Cambridgeshire, PE28 2LX, England

Tel : +44 (0)1487 773307  
Fax : +44 (0)1487 773168  
E-mail : [info@NSS.co.uk](mailto:info@NSS.co.uk)  
Internet : <http://www.NSS.co.uk>

©1991-2002 The NSS Group

All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the authors. This report shall be treated at all times as a confidential and proprietary report for internal use only.

Please note that access to or use of this Report is conditioned on the following:

1. The information in this Report is subject to change by The NSS Group without notice.
2. The information in this Report is believed by The NSS Group to be accurate and reliable, but is not guaranteed. All use of and reliance on this Report are at your sole risk. The NSS Group is not liable or responsible for any damages, losses or expenses arising from any error or omission in this Report.
3. *NO WARRANTIES, EXPRESS OR IMPLIED ARE GIVEN BY THE NSS GROUP. ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT ARE DISCLAIMED AND EXCLUDED BY THE NSS GROUP. IN NO EVENT SHALL THE NSS GROUP BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES, OR FOR ANY LOSS OF PROFIT, REVENUE, DATA, COMPUTER PROGRAMS, OR OTHER ASSETS, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.*
4. This Report does not constitute an endorsement, recommendation or guarantee of any of the products (hardware or software) tested or the hardware and software used in testing the products. The testing does not guarantee that there are no errors or defects in the products, or that the products will meet your expectations, requirements, needs or specifications, or that they will operate without interruption.
5. This Report does not imply any endorsement, sponsorship, affiliation or verification by or with any companies mentioned in this report.
6. All trademarks, service marks, and trade names used in this Report are the trademarks, service marks, and trade names of their respective owners, and no endorsement of, sponsorship of, affiliation with, or involvement in, any of the testing, this Report or The NSS Group is implied, nor should it be inferred.

# TABLE OF CONTENTS

---

- INTRODUCTION ..... 1**
  - What Is A Firewall? ..... 1
  - Firewall Architectures ..... 2
    - Static Packet Filtering ..... 2
    - Dynamic Packet Filtering/Stateful Inspection ..... 3
    - Proxy Servers ..... 3
    - Which Architecture Is Best? ..... 4
  
- BIZGUARDIAN 3.3 ..... 5**
  - Platform & Architecture ..... 5
  - Installation ..... 6
  - Management ..... 8
  - Configuration ..... 9
  - Reporting ..... 14
  - Verdict ..... 16
  - Contact Details ..... 17

## TABLE OF FIGURES

---

- Figure 1 - BizGuardian: Advanced Tasks menu ..... 5
- Figure 2 - BizGuardian: Configuring network parameters ..... 6
- Figure 3 - BizGuardian: Status screen ..... 7
- Figure 4 - BizGuardian: Numerous Wizards are provided to simplify administration tasks ..... 8
- Figure 5 - BizGuardian: Defining security rules ..... 9
- Figure 6 - BizGuardian: Adding a security rule ..... 10
- Figure 7 - BizGuardian: Real-time status monitor ..... 12
- Figure 8 - BizGuardian: Viewing log entries ..... 14
- Figure 9 - BizGuardian: Viewing graphical reports ..... 15

## The NSS Group

---

The NSS Group is Europe's foremost independent network and security testing facility.

Based in Cambridgeshire, England, and with additional labs and conference centre in the South of France, The NSS Group offers a range of specialist IT, networking and security-related services to vendors and end-user organisations throughout Europe and the United States.

The Group consists of two wholly-owned subsidiaries :

- *NSS Network Testing Laboratories*
- *Network Security Services*

**NSS Network Testing Laboratories** are available to vendors and end-users for fully independent testing of networking, communications and security hardware and software.

NSS Network Testing Laboratories also operates certification schemes for vendors and certification bodies, and currently provides certification of firewalls, VPN's, crypto products and PKI products.

Output from the labs, including detailed research reports, articles and white papers on the latest network and security technologies, are made available free of charge on the NSS web site at <http://www.nss.co.uk>

**Network Security Services** provides a range of security-related services to vendors and end-users including security policy definition, IDS, firewall and VPN implementation, network security auditing and analysis, and penetration testing.

---

## INTRODUCTION

---

With the whole of the networking world moving toward inhabiting a single global village, we inevitably have to start thinking about locking our doors and bolting our windows. It has to be recognised that no computer system can ever be 100 per cent secure, but it has to be secure enough to deter the casual hacker – we don't want some spotty adolescent spiriting away our corporate secrets from his bedroom using nothing more than a cheap PC, a modem and a few lines of code downloaded from the "*Hackers 'R' Us*" Web site.

The worrying trends in computer-related crime continue. According to the *2002 CSI/FBI Computer Crime and Security Survey*:

- *Ninety percent of respondents (primarily large corporations and government agencies) detected computer security breaches within the last twelve months.*
- *Eighty percent acknowledged financial losses due to computer breaches.*
- *For the fifth year in a row, more respondents (74%) cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (33%).*
- *Forty percent detected system penetration from the outside.*
- *Forty percent detected denial of service attacks.*

This is even more worrying than it sounds, since most experts agree that the majority of break-ins go undetected. For example, attacks by the Defence Information Systems Agency (DISA) on 9,000 US Department of Defence computer systems had an 88 per cent success rate but were detected by less than one in twenty of the target organisations. Of those organisations, only five per cent actually reacted to the attack (*Source: NCSA*).

The first step in securing our networks is not to rush out and buy the best firewall or encryption software we can find, however. Instead, some thought and effort should be put into developing a comprehensive, yet manageable, corporate security policy. This needs to cover everything from anti-virus protection to business recovery strategy. It should cover network access, password policy, authentication methods and how and when encryption should be employed. It should also cover physical security aspects too, such as building access, shredding of sensitive documents, and physical security of PC's and file servers.

When it comes to implementing the security policy, one of the major tools available to the network administrator is the firewall.

---

### What Is A Firewall?

---

There are a number of definitions of the firewall, but perhaps the simplest is "*a mechanism used to protect a trusted network from an untrusted network*". A firewall is a system, or group of systems that enforces an access control policy between two networks, and thus should be viewed as an *implementation of policy*.

The bottom line, therefore, is that a firewall is only as good as the Security Policy it supports. However, it is also true to say that a completely secure firewall is not always transparent to the user, and this can often lead to problems of users trying to circumvent the corporate security policy to get around some unpopular restriction imposed by the firewall.

In addition to providing protection from outside attacks, many firewalls today can present just a single IP address to the outside world (known as Network Address Translation, or NAT), thus hiding the real structure of the corporate network from prying eyes. They will also usually provide full auditing and reporting facilities.

One thing to bear in mind right from the outset is that a firewall is not simply for protecting a corporate network from unauthorised external access via the Internet, it can also be used internally to prevent unauthorised access to a particular subnet, workgroup or LAN *within* a corporate network.

Although the CSI/FBI figures identify the Internet connection as the most common source of attack, 33 per cent of respondents still identify the internal network as the point of origin. Thus, for example, if the Research & Development department has its own server, it could be protected – along with the department's workstations – behind a firewall, whilst still allowing them to remain a part of the corporate-wide network.

One caveat here, however. Be aware that there are still firewalls on the market today that struggle to provide wire speed throughput even at 100Mbps, let alone Gigabit speeds. Whilst this is not always an issue when the firewall is sitting in front of a slow Internet link, it can cause some serious bottlenecks if you try to put it on a Gigabit backbone!

With recent advances in processing speeds and multi-processor implementations we are now seeing dedicated appliances that can provide wire speed throughput on a Fast Ethernet network with a proxy server architecture, and even higher speeds when configured as stateful inspection devices. Some vendors are even claiming wire speed on Gigabit networks, although many organisations may prefer to opt for careful network design and load balancing across multiple firewall devices to improve resilience and achieve good performance at higher network speeds.

## Firewall Architectures

---

When looking at today's firewall products, there are three main architectures currently in use :

### Static Packet Filtering

Working at the Network Layer of the OSI stack, packet filters make simple deny or permit choices depending on the source/destination network address and port number contained within the packet, determined by a number of rules defined by the administrator.

Packet filtering is fast, transparent (no changes are required at the client), flexible and cheap (most routers will provide packet filtering capabilities, pure packet filter firewalls do not require powerful hardware on which to run). However, packet filter firewalls are traditionally difficult to configure and provide relatively poor logging capabilities, and straight packet filtering devices are few and far between today.

## Dynamic Packet Filtering/Stateful Inspection

Touted by some as the “third generation” of firewall architectures, this is really just an extension of the basic packet filtering architecture employed by most routers.

Stateful Inspection occurs at the MAC or Network Layer, thus making it fast and preventing suspect packets from travelling up the protocol stack. Unlike static packet filtering, however, Stateful Inspection is capable of making its decisions based on **all** the data in the packet (corresponding to **all** the levels of the OSI stack), although it is rare that all seven layers are examined in any great depth in practice.

The *state* of the connection is monitored at all times (hence *Stateful* Inspection), allowing the actions of the firewall to vary based on the administrator-defined rules and the state of previous conversations. In effect, the firewall is capable of remembering the state of each ongoing conversation across it and dynamically modifying the packet filter rules to suit (hence *Dynamic Packet Filtering*), thus allowing it to more effectively determine which inbound packets are part of an existing session and which are “rogue” packets.

## Proxy Servers

A Proxy Server firewall acts as an intermediary for user requests, setting up a second connection to the desired resource either at the application layer (an *application level gateway*) or at the session or transport layer (a *circuit level gateway*).

A strong application proxy works at all seven layers of the OSI model, performing such tasks as verifying the RFC-required three-way handshake, and ensuring that protocol header lengths meet with RFC guidelines, thus eliminating an entire class of buffer overrun attacks. Proxy code actually “stands in” for both client and server operations, relaying valid requests between the trusted and untrusted networks via the proxies. Unlike Packet Filter and Stateful Inspection firewalls, a direct connection is never allowed between the two networks.

It is important to note that the application proxy actually builds a new datagram from scratch, only copying known acceptable commands to the new datagram before forwarding it to the server behind the firewall. The datagram that enters the firewall from the outside is thus not the datagram that is delivered to the server, and thus the proxy effectively breaks the client server model (but in a “good way”).

With other technologies such as packet filtering there is still a direct connection between the client and server, albeit one that is monitored closely for abnormalities in a Stateful Inspection architecture. However, the nature of the direct connection does still provide the means for attackers to either hide data in unused datagram headers or to bury dangerous commands within the data area. This is simply not an issue with Proxy Servers.

The penalties paid for this level of security, however, are performance (Proxy Server firewalls have large processor and memory requirements in order to support many simultaneous users), and flexibility (since the introduction of new Internet applications and protocols can often involve significant delays while new proxies are developed to support them).

Once again, recent advances in processor speeds and SMP platforms are beginning to provide effective arguments against the performance criticism in well-designed systems, whilst the provision of “generic” proxies can allow unsupported protocols to be handled by the firewall.

### **Which Architecture Is Best?**

Whilst static packet filtering alone is usually confined to the router these days and not considered strong enough for enterprise class firewall devices, the differences between the remaining two architectures are negligible in most real world environments.

True proxy servers are undoubtedly the safest, but can impose a severe overhead in heavily loaded networks if not designed properly. Dynamic packet filtering is definitely faster, though most of the high-end firewalls are hybrids these days, incorporating elements of all three architectures and, arguably, the “best of all worlds”.

One final consideration is the underlying operating system. Good firewall code will not help if the OS on which the firewall is running is itself not secured. Whilst a dedicated firewall OS could be considered the best solution to this problem, general purpose operating systems can offer a secure platform providing they are “hardened” sufficiently before the firewall is installed.

However, at the end of the day, it is just as important to ensure that you have a comprehensive security policy in place and that your firewall is configured and managed effectively, as it is to have a firewall in the first place.

After all, a badly configured firewall could lead to a false sense of security – and that could be worse than leaving yourself unprotected.

## BIZGUARDIAN 3.3

BizGuardian is a combined Internet firewall and VPN product developed by Firewall Security Solutions Inc.(FSS) of Calgary, Canada. Currently, it is offered as a software-only solution for small to medium sized businesses, and is designed to be both inexpensive and easy to install and configure, whilst still offering an extensive feature list.

### Platform & Architecture

BizGuardian is currently a software-only product, designed to be installed on a wide range of low-cost PC hardware. Two versions are available – firewall only, and firewall plus VPN option.

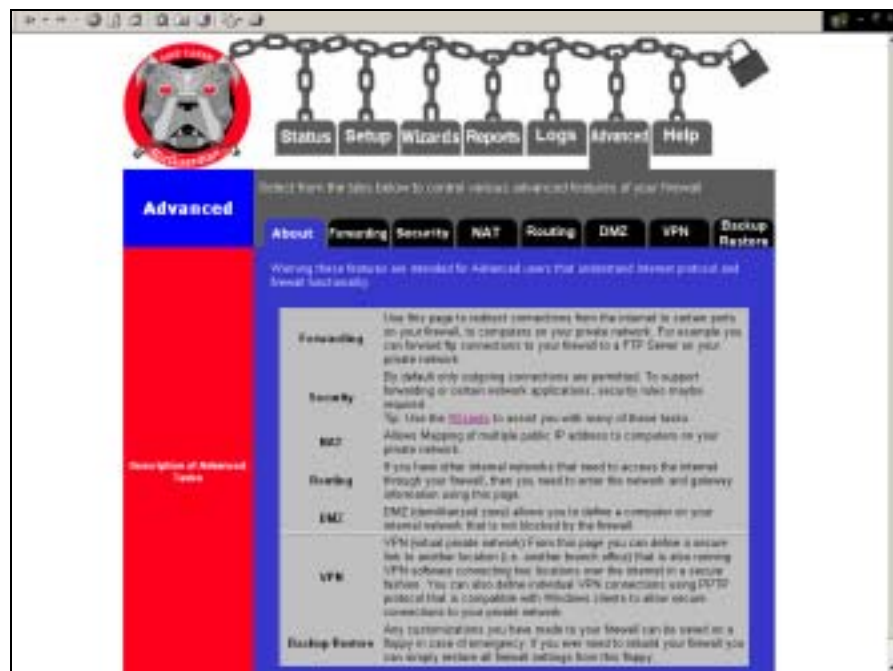


Figure 1 - BizGuardian: Advanced Tasks menu

The architecture is based on a hardened FreeBSD 4.6 kernel with the firewall and VPN features fully integrated into an easily downloadable package. Functionality for both the firewall and VPN are integrated into the kernel, providing high levels of performance and security. The firewall offers both stateful inspection and Network Address Translation (NAT) capabilities.

As you would expect, the FreeBSD kernel has been stripped down and hardened, removing all unnecessary and potentially insecure services. Further performance and security tweaks have been made by FSS under the banner of their proprietary “LoMax” technology, and the company claims advanced capabilities such as packet rate limiting and DoS pattern matching.

BizGuardian is designed for either cable modem or DSL connections and is currently optimised for up to 8000 simultaneous connections. During testing, however, we found that it could handle beyond this, providing the connection rates were kept to reasonable levels.

Even when number of connections and connection rates far exceeded expected levels for this product, BizGuardian performance degraded in a graceful manner, never failing or succumbing to Denial of Service conditions. Despite the low price, therefore (starting at \$150 for a four-user license), the product is clearly designed to handle typical small-to-medium enterprise environments.

In addition to the basic firewall and VPN features, the latest version of BizGuardian also offers integrated Web cache, content filtering and Intrusion Detection capabilities. These are all useful features in a firewall of this type, but are sensibly switched off by default when the firewall is first installed.

## Installation

---

Installation is designed to be as foolproof as possible, the entire package being delivered and installed via the Internet.



Figure 2 - BizGuardian: Configuring network parameters

BizGuardian is not a "personal firewall" product, and so – as with any firewall – a dedicated hardware platform is required. Any suitable Pentium-class PC platform can be used, as long as it has a minimum specification of 133MHz processor, 32MB of memory, two PCI network cards (or one, if the external interface is a modem), 500MB IDE Hard drive and floppy drive. FSS recommends that an average small business with less than 20 users will run happily on a Pentium 166MHz or faster, and for sites over 20 users or with a 1.5Mbs link or faster, a 300MHz PC should be used.

More memory and disk space may also be required if the Web caching feature is to be used. No CD-Rom drive is required, and a keyboard and monitor are only required during the installation process.



## Management

Administration of BizGuardian is accomplished using a standard Web Browser – no client software or java applications are required on the administrator’s workstation.

The admin interface is entirely graphical and reasonably intuitive. Wizards are used throughout the product in an attempt make it as easy as possible for the inexperienced to configure, and yet there are still “advanced” screens available to provide a more direct means of configuration for those who are confident in their abilities.

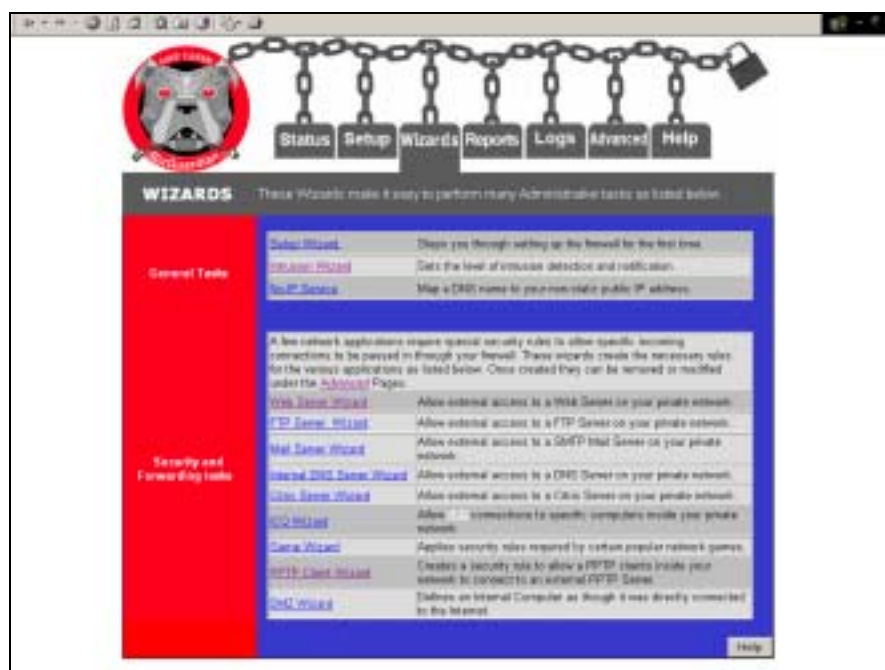


Figure 4 - BizGuardian: Numerous Wizards are provided to simplify administration tasks

If there are multiple BizGuardian firewalls on the same network, it is possible to manage them all from a single interface. Note, however, that each admin session can only establish a direct one-to-one relationship with any firewall – it is not possible to configure firewall policies centrally and then apply those across a number of firewalls in a single operation.

FSS is nothing if not responsive, however, and between producing the first draft of this report and publishing the final version, the company has already provided a means to transfer configuration parameters between firewalls via the built-in backup and restore capability (unfortunately we were not able to test this feature in time for publication).

A simple user name and password combination is used to provide authentication for the firewall administrator to each firewall under his control, but the link between admin PC and firewall is not secured. The latest release does now provide the option to restrict administrative access to one or more specific IP addresses (or to completely disable the Web administrative access) which is be a sensible precaution given the ease of access from any Web browser.

Initially, administrative access is restricted to the internal interface only, but it is possible to use the VPN (if the VPN option has been purchased) to provide a secure connection for administration across the Internet. We would still, however, prefer to see a secure connection between client and firewall for admin access, even on the internal network.

## Configuration

After authenticating to the firewall via a Web browser, the administrator is presented with the initial status screen, and a number of tabs provide intuitive access to all the functions necessary to configure and manage the firewall.

Rules control traffic flow in both directions. However, by default, all outgoing traffic is allowed and any returning packets for the outgoing connection are permitted to travel back to the originator of the connection. Therefore most applications will work fine through the firewall without any special configuration. Custom rules are required for permitting inbound traffic to services within the private network, or for applying restrictions to outbound traffic (preventing the use of Telnet whilst allowing the more secure SSH, for example).



Figure 5 - BizGuardian: Defining security rules

The most important and useful tab for the novice administrator is the *Wizard* tab, which provides access to a number of wizards that can be used to configure the most common settings and services.

The Setup Wizard guides the administrator through the initial configuration of IP addresses, DNS servers, default gateway and whether or not a DHCP server is running on the internal interface. Other wizards are provided to set the level of intrusion detection and notification, configure external access to key internal servers such as Web, mail, FTP, Citrix and DNS, configure PPTP client access through the firewall, provide access to selected network games through the firewall, and configure a “DMZ” server.

This latter Wizard could be quite misleading for some administrators, since it implies the use of a secure subnet on which can be installed one or more public-facing servers. BizGuardian does not actually support a third DMZ interface, however, and so all the DMZ Wizard does is to open a hole through the firewall directly to an internal server. At least FSS has now added a suitably dire warning as to just how dangerous this can be.

In fact, most of the Wizards are geared towards creating “holes” through the firewall to various internal hosts, and this highlights one of the dilemmas facing software developers – how do you make a firewall easy to use and perfectly secure? The answer is, of course, that you can’t. There is no substitute for experience and hand crafting of the firewall rules, and the easy-to-use Wizards in BizGuardian can do much to encourage the adoption of an insecure policy. It is all well and good, for example, making it easy to provide external access to an FTP server on the internal network, but should that server ever be compromised there would be nothing the firewall could do to prevent an attacker wreaking havoc on the internal – supposedly protected – network. Some of the administrators that make up the exact target market for a product such as BizGuardian may not realise this.



Figure 6 - BizGuardian: Adding a security rule

If BizGuardian is to provide Wizards of this nature, it would be far better to support the use of a third – true DMZ – network interface, and to have the Wizards provide access to that subnet only. This would leave the internal network fully protected unless an administrator who knows what he is doing chooses to expose it in a controlled manner via the *Advanced* rules pages.

To place this in perspective, it should be remembered that it is possible for **any** administrator to misconfigure **any** firewall, easily opening a security hole wide enough through which to drive the *Hacker Express*.

At least BizGuardian tries to minimise the possibility of serious error by implementing Wizards to cover most of the more common operations – we simply feel it could go one step further to make things even more secure by implementing a true DMZ interface (FSS has informed us that it will now be implementing this facility in the next release - version 3.4).

For those who prefer not to use the wizards, or who wish to view or refine the various rules created by the wizards, the *Advanced* tab is the place to go. Here, a number of “sub-tabs” provide access to various advanced administrative functions such as:

- **Forwarding** – *This page can be used to redirect connections from the Internet to certain ports on the firewall, and then on to computers on the private network. For example, FTP connections to the firewall can be forwarded to a FTP Server on the private network. It is transparent to the users on the internet that the FTP server is actually running on another computer within the private network.*

*BizGuardian also supports basic load balancing capabilities via the Server Pooling option. By specifying more than one Private Network destination address, the firewall will distribute inbound connections to a particular port in a round-robin fashion to all the addresses that are specified.*

- **Security** – *Security rules can either Allow or Deny specified traffic. When a packet is denied is it basically dropped and the potential attacker does not learn any information about the firewall or network behind it. To the attacker the firewall “stealths” any ports not permitted.*

*By default all outgoing connections are permitted, along with inbound replies to established outbound connections. The Security page allows the administrator to define packet filter rules that examine the protocol along with source and destination IP addresses and ports in order to determine which packets are allowed to pass through the firewall. Each rule can be set to Allow or Deny, and can be logged to the intrusion log file whenever a rule is matched (no other logging or alerting option is available).*

*It is also possible to reorder rules (they are checked in the order they are defined on the Security page), modify them, delete them, or mark them active or inactive from this screen. Some of the BizGuardian Wizards create security rules automatically to accomplish the Wizard task. Any Security rule created this way will indicate in the comment field that they were created by a Wizard.*

- **NAT** – *Allows Mapping of multiple public IP address to computers on the private network. This would allow the administrator to publish a second external address which is then automatically forwarded to an internal Web or FTP server, for example.*
- **Routing** – *This page allows the administrator to define static routes. All that is required is the target network address (in CIDR format) and the required gateway.*
- **DMZ** – *The DMZ (DeMilitarised Zone) allows the administrator to define a computer on the internal network that is not blocked by the firewall. A true third DMZ subnet is not supported via this option, however.*

- **VPN** – The IPSEC-compliant VPN (Virtual Private Network) is an extra cost option that allows the administrator to define a secure link to another location (i.e. another branch office) that is also running VPN software. It is also possible to define individual VPN connections using the PPTP protocol to allow secure connections from individual remote clients through to the private network.
- **Backup/Restore** – All configuration changes that have been made to a firewall can be saved to a floppy disk in case of emergency. If it is ever necessary to rebuild the firewall, these settings can simply be restored from this floppy once the BizGuardian software has been installed.

The *Status* page provides a useful real-time monitoring capability that provides instant access to information such as which services are running on the firewall, how much traffic has passed through the firewall, how many packets have been rejected, and how many intrusions have been logged.

Real-time graphical displays provide indications of CPU utilisation, network load, memory usage, active connections and top users of network bandwidth.

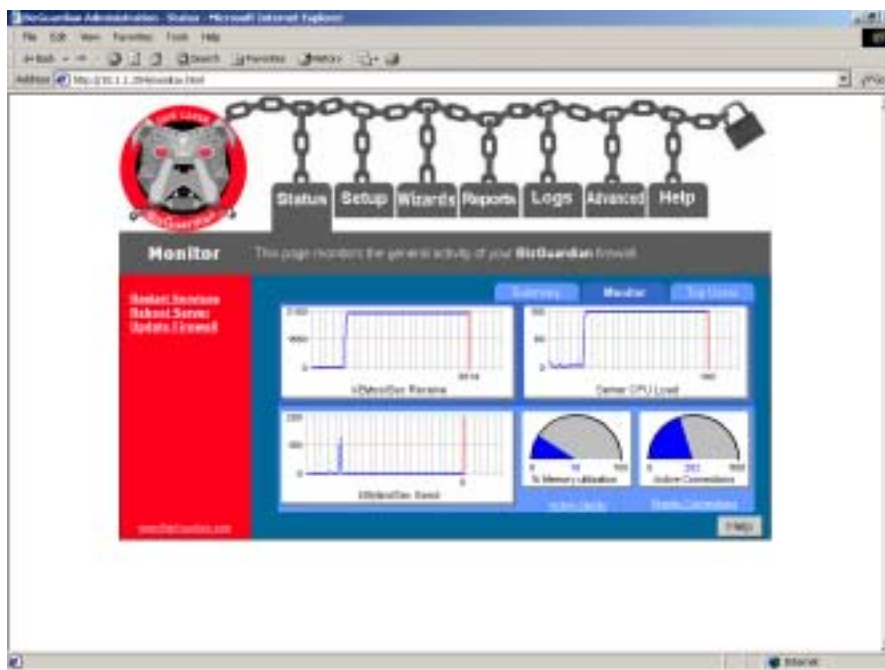


Figure 7 - BizGuardian: Real-time status monitor

Other services are integrated into the firewall, including:

- **DNS Cache** – This provides a DNS resolution service which can be used as the primary DNS server for all internal hosts. A DNS Cache can reduce the amount of Internet traffic required for name lookups thanks to the local store of recently-accessed DNS names. Using the local DNS service, it is also possible to map hosts and domains differently inside the private network to how they would resolve outside the firewall.

- **DHCP Server** – Dynamic Host Configuration protocol (DHCP) allows IP addresses (and other IP configuration information, such as default route and DNS servers) to be assigned to hosts dynamically each time they attach to the network. For sites with no existing DHCP server, BizGuardian provides this on the internal interface.
- **WINS Server** – A Windows Internet Name Service (WINS) Server maintains a database that maps the IP addresses of WINS clients to their computer (or NetBIOS) name. For sites with no existing WINS server, BizGuardian provides one – this can help when using PPTP or VPN services.
- **Web Cache** – The Web Cache is designed to reduce the amount of Internet traffic – whilst increasing performance for local hosts – by storing a number of recently-accessed Web pages on the local hard drive of the firewall. If those pages are accessed again by other internal hosts, they are served from the firewall's cache rather than from the original Web server on the Internet. The BizGuardian Web cache (based on Squid) can be configured to act as a Web proxy server, or as a transparent cache. Enabling the Web Cache also provides much more extensive Web access logging capabilities than the standard Connection log, since the Web Cache records the complete URL accessed.
- **Content Filtering** – Once enabled, the Content Blocking feature uses Client Classes and Content Blocking lists to restrict access to certain Web sites. Client Classes define group of workstations, time ranges and a selection of Pass and Block lists that are used to determine if access to a particular Web page is allowed.

A number of Pass/Block lists are provided as part of the package categorising sites into groups such as Adult, Violence, Gambling, Drugs, Hacking, and so on. Weekly updates to these built-in lists are provided free of charge, and it is possible to create custom lists from scratch if required (perhaps to keep employees away from local job hunting or sports sites). If a match is found, the user is presented with an information page telling them why access to that site has been blocked and who to contact in case of query.

- **Intrusion Detection** – The built-in Intrusion Detection System (IDS) is based on version 1.8.7 of Snort, and is designed to analyse traffic arriving at the external interface for known attack patterns. If any suspicious activity is observed it is recorded in the Intrusion Detection log file, and e-mail alerts can be raised automatically should the number of intrusion attempts exceed a pre-defined level.

Three levels of intrusion reporting can be set from **Highest** (logs probes, service attacks, intrusion attempts, virus footprints), through **Medium** (logs service attacks, most intrusion attempts, virus footprints), to **None** (Intrusion Detection logging and notification disabled). It is also possible to provide IP addresses of hosts that should be excluded from IDS logging.

At present, the rule set is fixed, and cannot be changed by the administrator (future versions will allow custom modification of the rule set). Rules are updated regularly by FSS and can be applied to each firewall via the Update Firewall feature.

- **SNMP Agent** – This provides the ability for a management system to monitor remotely the performance counters and general health of a BizGuardian firewall. It also sends traps/alerts to the central management console whenever a significant firewall event occurs, such as an intrusion alert, or a firewall startup/shutdown.

All of these can be configured and administered via the admin interface and, more importantly, they can all be disabled if not required.

Alerting capabilities within BizGuardian are adequate. General alerts (intrusion attempts, etc.) can be e-mailed to an administrator when they reach a specified threshold, though it is not possible to set a different alert condition or frequency on a per-rule basis. Alerts that indicate potential known viruses immediately trigger an e-mail alert. Alerts can also be sent via SNMP traps to a central management console, where third party monitoring software could be used to more sophisticated alert handling if required.

## Reporting

There are six basic log files available in BizGuardian:

- **Intrusion Log** – This file monitors events from two components of the system: the Intrusion Detection knowledge module and the Security rule module. The intrusion module will record events such as known network intrusion footprints and port scanning attempts. The security rule module records entries whenever packets are blocked or passed with logging enabled on the rule.

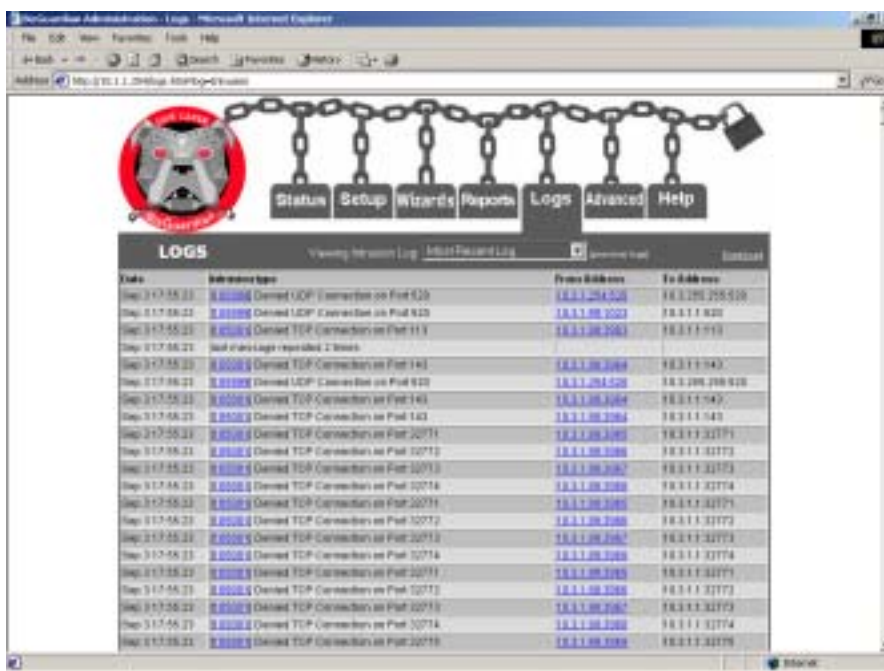


Figure 8 - BizGuardian: Viewing log entries

- **Connection Log** – Any outgoing connections are recorded in this log file. The date, source IP address, destination domain name and the destination port are all recorded.

- **Services Log** – Anytime the firewall services or the server itself are restarted an entry is recorded here. The Services log also audits information about Web Administrator Logins, PPTP VPN client logins and license conditions.
- **System Logs** – This log contains any Unix operating system events
- **Web Blocking** – This file contains details of all attempted accesses to prohibited Web sites.
- **Web Cache** – This file contains detailed information of all Web sites visited by all workstations protected by the firewall.

While viewing each log file a drop down list appears at the top of the log page to allow selection of archived logs. For each of the log files the administrator can specify the maximum size of the file (in Kbytes), before a new file is created, as well as the number of versions of the log files to retain. By default the log files are archived when they reach over 100KB in size and seven versions of the log files are retained.

When viewing the log files, it is possible to download each of them into CSV (comma separated value) files suitable for importing into Microsoft Excel for further analysis. The files can only be downloaded to a local drive on the firewall itself, however, and not pulled back to the admin console.

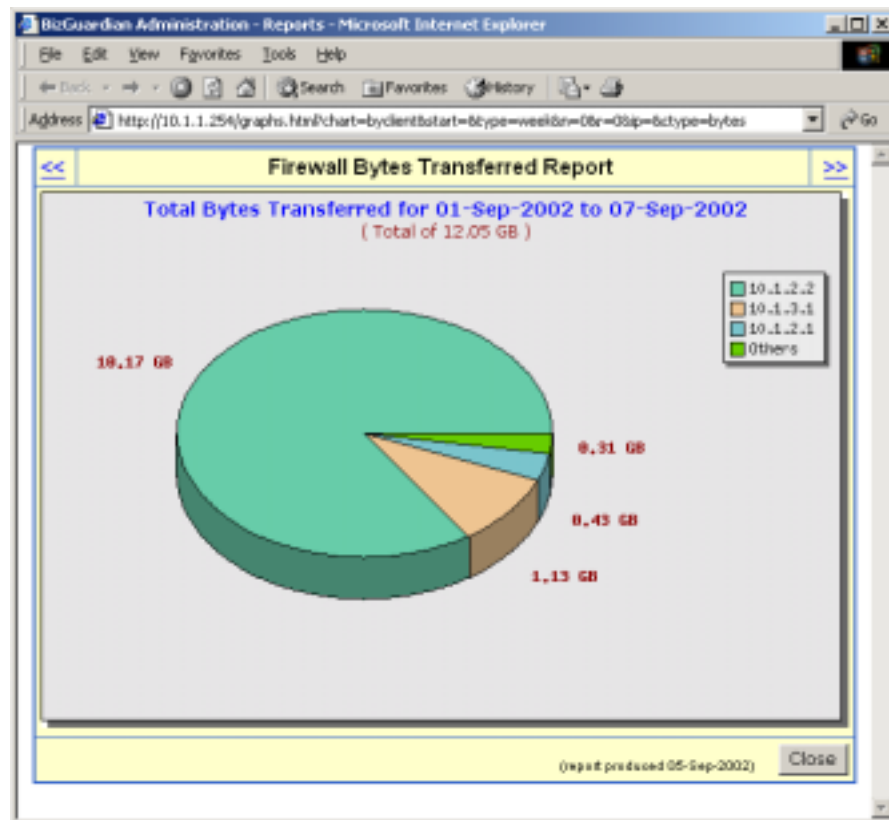


Figure 9 - BizGuardian: Viewing graphical reports

In addition to the basic log file output, BizGuardian also provides a number of graphical and text based traffic summary reports which are available via the *Reports* tab.

These include:

- *Total bytes transferred*
- *Average bytes per second*
- *Top ten clients (bytes transferred)*
- *Top ten clients (average bytes)*
- *Bytes transferred per client*
- *Web cache statistics*
- *Web cache top sites*

Once the report type has been selected, a time period can be specified, and the report can be run against all clients or a specific IP address. Not an extensive range of selection criteria or report types, perhaps, but this is more than some high-end firewalls provide from their management interfaces, and so BizGuardian is to be congratulated on including this functionality in an entry-level product.

## Verdict

---

At a level of pricing that starts at just \$150 for a four user license, many people may mistake BizGuardian for a personal firewall product at first glance. Nothing could be further from the truth, however.

The use of the FreeBSD platform with kernel-level stateful packet filtering and VPN capabilities provides a solid platform on which FSS has developed a number of custom, proprietary modifications to improve both performance and reliability. In our tests, BizGuardian survived all our penetration attempts and exceeded the performance specifications claimed by its developers.

Even when we pushed it beyond its claimed limits, performance degraded gracefully and reliably, quickly recovering when the test load was removed. FSS has designed this primarily product to protect networks connected to the Internet via cable modems, ADSL modems, ISDN TAs and similar devices. Even on a low-specification PC (as provided for testing) we found it handled that level of load with ease, and believe that it could handle far more given a suitably powerful hardware platform.

The installation was extremely straightforward, and the graphical management interface was very easy and intuitive to use. It provided a very effective Wizard-based approach for the novice administrator, and yet retained enough low-level control to keep the more experienced hands happy. The only real omission with which we could raise issue was the lack of support for a third network card to provide a true DMZ network. That aside, the range of features was very impressive, with a number of additional services such as DNS, DHCP, WINS, Intrusion Detection, Web cache and content blocking all integrated with the firewall should they be required.

This might not be the firewall you choose to protect a multi-million dollar network with thousands of PCs, but it is more than adequate to handle anything that may be thrown at it in its intended market. The excellent support (we found the company to be extremely responsive to both problems and general suggestions for improvements) gives it a huge advantage over the so-called "free" firewalls that appear to provide similar levels of functionality.

The low cost and ability to reuse existing older hardware that the average small company might have lying around also makes it a very cost-effective solution all round.

Well worth a look.

## **Contact Details**

---

**Company:** Firewall Security Solutions Inc.

**Internet:** [www.bizguardian.com](http://www.bizguardian.com)

**E-mail:** [sales@bizguardian.com](mailto:sales@bizguardian.com)

**Address:**

Suite 1650 734 7 Avenue SW,  
Calgary, Alberta T2P 3P8

**Tel:** +1 (403) 266-5895

**Fax:** +1 (403) 269-2287

**UK Office:**

**Internet:** [www.bizguardian.co.uk](http://www.bizguardian.co.uk)

**E-mail:** [uksales@bizguardian.co.uk](mailto:uksales@bizguardian.co.uk)

**Address:**

BizGuardian Ltd  
Suite 55  
Gateway House  
Northgate Street  
Chester, CH1 2HR

**Tel:** +44 (0)8701 614241

**Fax:** +44 (0)8701 614339