

Comparison of SmoothWall Corporate Server Version 3.0 and Express Version 2.0



Corporate Server was developed as a commercially supported version of the extremely popular SmoothWall Open Source firewall now known as SmoothWall Express. The bulk of the Corporate Server code remains licensed under the General Public Licence, new code written specifically for Corporate Server has in general been licensed under a proprietary licence. However a number of elements originally developed for Corporate Server Versions 1.0 and 2.0 have since been introduced into Version 2.0 of GPL SmoothWall and re-licensed under the GPL.

Corporate Server is aimed at commercial users who require the guaranteed post-sale support provided by SmoothWall Limited and its worldwide network of Resellers. A large number of extra features have been introduced into Corporate Server to make it more suitable for commercial users with more demanding requirements, where it may be protecting networks with hundreds of user computers and servers. Corporate Server was designed as a modular system allowing customers to add extra functions like server hosting support (SmoothHost), VPN Gateway (SmoothTunnel), Web Content Filtering (SmoothGuardian) and Internet (Service) Access Control (SmoothRule). The latest add-on module known as SmoothTraffic adds Bandwidth Management (QoS) features.

Corporate Server Version 3.0 Enhancements over Express Version 2.0:

- SCSI Support (common chipsets from Adaptec, Future Domain, Symbios, Advansys and BusLogic)
- Multiple Sub-Net support on the Green (Protected) Network (Single NIC)
- PPTP Forwarding, allowing SmoothWall to protect a Microsoft VPN Server
- Static DNS Name Facility (Hosts File Maintenance)
- Option to display Error Messages in a Pop-Up Window
- Identification string (name for the Corporate Server) displayed in title bar
- New Traffic Statistics Page
- Simplified yet more powerful Port Forwarding configuration
- Drop-down lists provided for the most commonly used TCP/IP Services/Ports
- Fail-over (manual) to alternative Internet Connection (eg Ethernet to PPP/ISDN))
- Serial Console Support (from a VT100 terminal program running on an RS232 connected PC)
- Un-interruptable Power Supply (UPS) support
- SNORT Intrusion Detection System (IDS) allows Rule/Signature update and rule enable/disable
- Remote Syslog support (send log files to a remote logging system)
- Comment Field per entry in the Port Forward, DMZ Pinhole and all other lists
- Multi-Port NIC Support (Intel EtherExpress Pro100S dual port, 3Com dual port and DLink DE580 4 port)
- Restrict Admin/SSH access to Corporate Server to specified Local or Remote IP Addresses
- Create list of domains not to be cached by the Web Proxy Server
- Option to configure the DHCP Server to only support static address assignments
- Administration Users with limited access to Log Viewers, VPN configuration etc.
- Additional traffic graphs
- Diagnostics file generation
- Enhanced Graphical User Interface with improved "GO" Navigation

Virtual Private Network (SmoothTunnel and SmoothNode Modules)

SmoothWall GPL provides very basic Virtual Private Network (VPN) facilities using Shared Secret (PSK, Pre-Shared Key) authentication. GPL does not support dynamic IP addresses as provided by most ISPs. Likewise Road Warriors using Microsoft Windows™ IPsec VPN clients cannot connect to GPL SmoothWall.

The SmoothTunnel VPN Gateway module has addressed all of the above issues and more. Offering a rich set of VPN facilities, including:

- Dynamic IP address support
- The ability to connect to a SmoothTunnel gateway identified by a dynamic DNS name
- Manage individual VPN tunnels
- Road Warrior Support
- x509 Certificate Authentication (the industry norm, far stronger and essential for Road Warriors)
- NAT Traversal (NAT-T) option for a VPN tunnel to use UDP instead of Protocol 50. This allows VPN traffic at the remote end of the VPN tunnel (eg SmoothNode or Road Warrior) to pass through a router or other communications device running Network Address Translation (NAT).

- AES (Rijndael), Twofish, Blowfish, and CAST encryption algorithms in addition to existing 3DES

SmoothTunnel can produce self-signed x509 certificates to avoid the normal costs associated with the lease or purchase of certificates. The SmoothNode module supports a single VPN tunnel where for example remote (branch) offices need a VPN connection to head office.

Server Hosting Support / Multiple Public IP Addresses on Red Interface (SmoothHost Module)

Corporate Server's SmoothHost module allows multiple public IP addresses to be configured on the Red (Internet) interface. These IP addresses are configured to port forward to private IP address of servers within the De-Militarized Zone (DMZ) or the Green (Local) network. Several hundred IP addresses can be configured in this way, thus allowing Corporate Server to protect multiple Web or Mail Servers etc. Enhancements introduced in Version 3.0 of SmoothHost include:

- Map internal IP/network addresses to public IP addresses, so that web servers etc. can respond on specific IP addresses rather than on the Corporate Server default Red IP address
- Support for PPP based Subnets
- Handle multiple Subnets on the same physical (Red) interface
- Support dial-up PPP connections (ISDN, analogue modem etc.) as well as Ethernet
- Can access a DMZ server by its External (Public) IP address from the Local (Green) network

Web Content Filtering (SmoothGuardian Module)

SmoothGuardian is built on the DansGuardian open source content filtering software. DansGuardian blocks objectionable content using a URL/IP/domain blocklist, MIME/PICS code checking and most important of all, the dynamic word and phrase analysis of the received web pages. As matches are made against lists of objectionable words and phrases a points count is incremented until a user configurable threshold is reached, whereupon the page is blocked. SmoothGuardian:

- Introduces a simple to use GUI to configure the powerful DansGuardian features
- Configure blocking by category (eg pornography, violence, news etc.)
- URL/IP/Domain blocklist is updated weekly by SmoothWall Limited
- Override standard SmoothWall supplied blocklist with additions/deletions and whitelist facility
- Multiple filter rules groups so that different users can be subjected to different filtering rules
- Report generation facility (eg user activity, analysis of attempts to access blocked pages etc.)

Internet Access Control (SmoothRule Module)

By default SmoothWall blocks all incoming traffic that did not result from a local network request (ie it rejects all unsolicited messages) and allows all outgoing traffic. To restrict which Internet services users can access requires changing SmoothWall's IPTables rule set; something requiring considerable knowledge. SmoothRule provides a simple browser based facility that uses drop-down list boxes to select services to be blocked or enabled, so you don't have to be a Linux expert to customise your firewall.

Bandwidth Management /Quality of Service (SmoothTraffic Module)

Linux provides powerful Quality of Service features but they are complex to understand and configure. SmoothTraffic provides a simple GUI to:

- Limit bandwidth utilisation by IP/network address to ensure equitable provision of bandwidth amongst users
- Prioritise traffic by protocol (port); typically used to ensure that interactive traffic such as web browsing, SSH and VoIP get the bandwidth they need to function properly.
- Control total bandwidth utilisation so that queuing and prioritisation is performed by SmoothWall rather than by the upstream networking equipment over which users have no control. This is particularly important with DSL which is typically optimised for file downloads rather than interactive traffic.

SmoothWall Limited
Regent House
Skinner Lane
Leeds. LS7 1AX. UK

Tel: +44-(0)870-1999500
Fax: +44-(0)870-1991399
Email: sales@smoothwall.net
www.smoothwall.net