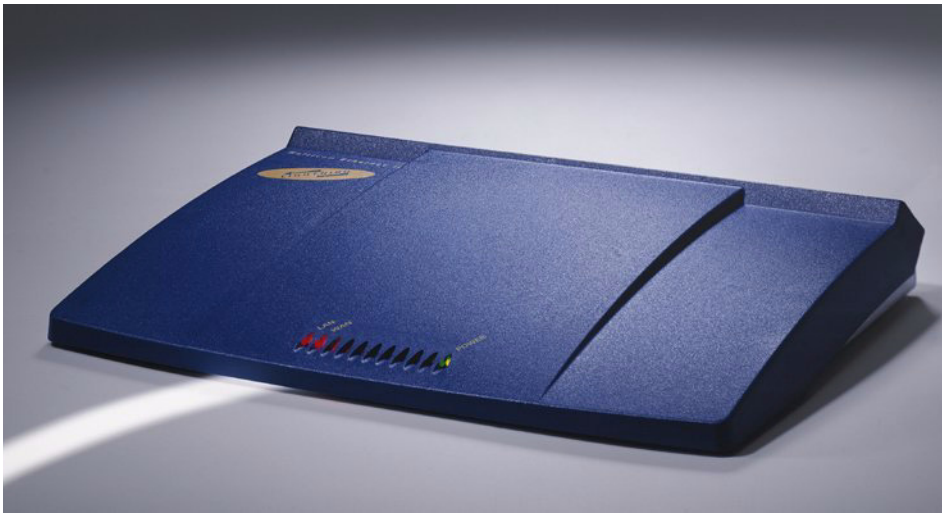
Lightning-Linux 3.7



Reference Manual

For Firmware 3.7 -11/1/04

LIGHTNING Instrumentation SA

Avenue des Boveresses 50
Lausanne, Vaud 1010
Switzerland
Phone +41.21.654.2000
Fax +41.21.654.2001
http://www.lightning.ch
info@lightning.ch

APLIWARE SA

rue du Grand-Pre 70
1222 Geneva 2
Switzerland
Phone +41.22.918.3610
Fax +41.22.918.3695
http://www.apliware.com
info@apliware.com

Copyright, Warranty, Liability

Copyright

Trademarks

Revisions

Warranty

LIGHNTING S.A. and APLIWARE S.A. warrants all hardware products of its manufacture to be free from defects in material and workmanship for 12 months from date of delivery. Upon prompt notification by the purchaser, LIGHNTING S.A. and APLIWARE S.A. will correct, within the warranty period, any defects in equipment of its manufacture either by repair at its factory or by supply of replacement parts to the purchaser.

LIGHNTING S.A. and APLIWARE S.A. must decide to its own satisfaction that the equipment is defective and has not developed malfunctions as a result of misuse, modification, or abnormal conditions of operation. Damages due to over voltage (e.g. lightning strokes) or wrong cabling on any interface are expressly excluded from the warranty. Opening the products also voids the warranty. LIGHNTING S.A. and APLIWARE S.A. assumes no liability for consequential damages, and its liability shall in no case exceed the original purchase price of the equipment.

The warranties set forth above are the sole warranties applicable to LIGHNTING S.A. and APLIWARE S.A. products. THE IMPLIED WARRANTY OF MERCHANTABILITY AND ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, ARE EXCLUDED.

Limitation of Liability

UNDER NO CIRCUMSTANCES, INCLUDING NEGLIGENCE, SHALL LIGHNTING S.A. AND APLIWARE S.A. BE LIABLE FOR LOSS OF USE, INTERRUPTION OF BUSINESS, OR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND (INCLUDING LOST PROFITS) REGARDLESS OF THE FORM OF ACTION WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT PRODUCT LIABILITY OR OTHERWISE, EVEN IF LIGHNTING S.A. AND APLIWARE S.A. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

In no event shall LIGHNTING S.A. and APLIWARE S.A. be liable for costs of procurement of substitute goods. The potential liability of LIGHNTING S.A. and APLIWARE S.A. arising out of this product is in any case limited to the purchase price paid to LIGHNTING S.A. and APLIWARE S.A. for its products.

Software and Documentation License

The software and documentation included in or with products of LIGHNTING S.A. and APLIWARE S.A. is subject to following licence.

Third-Party Software. A part of the software used within the MultiCom Ethernet series can be freely distributed under the terms of the GNU Public License and BSD copyright. However, some applications remain the property of their owners, and require their permission to redistribute. For a complete listing of the software used within the MultiCom Firewall, and the terms under which it can be distributed, refer to the LIGHTNING Web site at http://www.lightning.ch/ and to the Appendix on Additional Licenses and Copyrights.

Shareware and Freeware Software. Your MultiCom Companion CD contains shareware, freeware and other 3rd Party software not developed by LIGHNTING S.A. and APLIWARE S.A. Such software is neither warranteed or supported by LIGHNTING S.A. and APLIWARE S.A. and is not necessary to use LIGHNTING S.A. and APLIWARE S.A. products. If you wish to use it be sure to check that it meets your company's standards for reliability, security and useability. Please check with the developer of the software for any necessary information about the use or capabilities of such included software.

While all included software on this CD has been virus checked and tested LIGHNTING S.A. and APLIWARE S.A. does not provide any guarantees concerning these products. Be sure to use any virus protection that is required by your company before using the included software. If you go to a website of these software developers be sure to virus check any software that you download from them before using it as well.

LIGHNTING S.A. and APLIWARE S.A. cannot accept responsibility for any disruption, damage and/or loss to your data or computer system that may occur while using these programs. If you are unsure about what you are doing check with your network administrator before installing any software.

License. The software, on any media, including disk, read-only memory, and flash memory and the products related documentation are licensed to you by LIGHNTING S.A. and APLIWARE S.A.. You own the media on which the LIGHNTING S.A. and APLIWARE S.A. software is recorded, but LIGHNTING S.A. and APLIWARE S.A. and/or LIGHNTING S.A. and APLIWARE S.A.'s Licensor(s) retain title to the LIGHNTING S.A. and APLIWARE S.A. software and related documentation. The license allows you to use the LIGHNTING S.A. and APLIWARE S.A. software on a

single LIGHNTING S.A. and APLIWARE S.A. hardware product. In the case of software on disk, you are allowed to make one copy of LIGHNTING S.A. and APLIWARE S.A. software in machine-readable form for backup purposes only. You must reproduce on such copy the LIGHNTING S.A. and APLIWARE S.A. copyright notice and any other proprietary legends that were on the original copy of the disk containing LIGHNTING S.A. and APLIWARE S.A. software. You may also transfer all your license rights in the LIGHNTING S.A. and APLIWARE S.A. software, together with the associated hardware, the backup copy, the related documentation, and a copy of this license to another party, provided the other party reads and agrees to accept the terms and conditions of this license.

Restrictions. The LIGHNTING S.A. and APLIWARE S.A. software contains copyrighted materials, trade secrets, and other proprietary materials and in order to protect them you may not decompile, reverse engineer, disassemble, or otherwise reduce the LIGHNTING S.A. and APLIWARE S.A. software to a human-perceivable form. You may not modify, network, rent, lease, loan, distribute, or create derivative works based upon the LIGHNTING S.A. and APLIWARE S.A. software in whole or in part. You may not electronically transmit the LIGHNTING S.A. and APLIWARE S.A. software from one computer to another or over a network.

Termination. This license is effective until terminated. You may terminate this license at any time by destroying the LIGHNTING S.A. and APLIWARE S.A. software, the related hardware, related documentation and all copies thereof. The license will terminate immediately without notice from LIGHNTING S.A. and APLIWARE S.A. if you fail to comply with any provision of this license. Upon termination you must destroy the LIGHNTING S.A. and APLIWARE S.A. software, the related hardware, related documentation and all copies thereof.

Limited Warranty on Media. LIGHNTING S.A. and APLIWARE S.A. warrants the media on which the software is recorded as its hardware materials, and limits the liability as set for the hardware material.

Disclaimer of warranty on LIGHNTING S.A. and APLIWARE S.A. software. You expressly acknowledge and agree that use of the LIGHNTING S.A. and APLIWARE S.A. software is at your sole risk. The LIGHNTING S.A. and APLIWARE S.A. software and related documentation are provided "AS IS" and without warranty of any kind and LIGHNTING S.A. and

APLIWARE S.A. EXPRESSLY DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. LIGHNTING S.A. AND APLIWARE S.A. DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE LIGHNTING S.A. AND APLIWARE S.A. SOFTWARE WILL MEET YOUR REQUIREMENTS, OR THAT THE OPERATION OF THE LIGHNTING S.A. AND APLIWARE S.A. SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE LIGHNTING S.A. AND APLIWARE S.A. SOFTWARE WILL BE CORRECTED. FURTHERMORE, LIGHNTING S.A. AND APLIWARE S.A. DOES NOT WARRANT OR MAKE ANY REPRESENTATIONS REGARDING THE USE OR THE RESULTS OF THE USE OF THE LIGHNTING S.A. AND APLIWARE S.A. SOFTWARE OR RELATED DOCUMENTATION IN THE TERMS OF THEIR CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY LIGHNTING S.A. AND APLIWARE S.A. OR A LIGHNTING S.A. AND APLIWARE S.A.-AUTHORIZED REPRESENTATIVE SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY. SHOULD THE LIGHNTING S.A. AND APLIWARE S.A. SOFTWARE PROVE DEFECTIVE, YOU (AND NOT LIGHNTING S.A. AND APLIWARE S.A. OR A LIGHNTING S.A. AND APLIWARE S.A. AUTHORIZED REPRESENTATIVE) ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR, OR CORRECTION. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Limitation of Liability. Conforming to the general limitation of liability.

Controlling Law and Severability. This license shall be governed by and construded in accordance with the laws of Switzerland and Canton de Vaud, as applied to agreements entered into and to be performed entirely between Canton de Vaud residents. If for any reason a court of competent jurisdiction finds any provision of this license, or portions thereof, to be unenforceable, that provision of the license shall be enforced to the maximum extent permissible so as to effect the intent

of the parties, and the remainder of this license shall continue in full force and effect.

Complete agreement. The license constitutes the entire agreement between the parties with respect to the use of the LIGHNTING S.A. and APLIWARE S.A. software and related documentation, and supersedes all prior or contemporaneous understandings or agreements, written or oral, regarding such subject matter. No amendment to or modification of the License will be binding unless in writing and signed by a duly authorized representative of LIGHNTING S.A. and APLIWARE S.A..

Export

Some versions and options of LIGHNTING S.A. and APLIWARE S.A.'s Software and Hardware, including technical data, may be subject to Swiss, E.U., U.S. (including the U.S. Export Administration Act) or other countries export control laws, and their associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import Software and Hardware.

Table of Contents

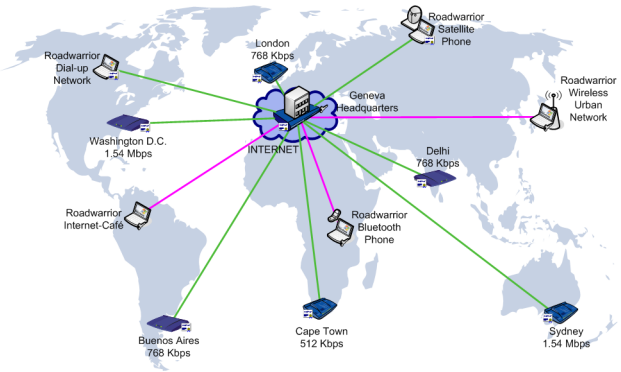
Contents

Chapter 1

Preface

This release of this manual was written to work with the current versions of the Lightning-Linux 3.7 for MultiCom Firewalls and the Configurator Software (version 3.7). If you are using different versions please check with your distributor or the LIGHTNING or APLIWARE websites for updated technical information.

For the latest release notes check the Lightning website at http://www.lightning.ch/support or http://www.apliware.com.



About This Manual

Putting together a solution to meet your networking needs is not always an easy task. Whether you are a seasoned professional or a new office network administrator you will find there are many networking possibilities you may have not have considered. This manual is designed to introduce you to all of the possible tasks of your new MultiCom Firewall and then walk you step-by-step through configuring the features you want. You will also find references “Recommended Reading and Free Software” on page 553, and a list of terms in the “Glossary” on page 575 to help you better understand the more advanced features of your firewall.

While every attempt has been made to explain the features and configuration steps of your new firewall you should have some basic experience in the following areas.

- familiarity with general computer usage
- understanding of basic networking (if not check out the technology overview sections at the end of this manual first.)
- connecting to a network (you still need to have a working connection to either the Internet or a local network: check with your local network administrator or Internet Service Provider for assistance in getting that connection up and running.)

Working with the Internet requires knowing many technical acronyms. Please refer to the “Glossary” on page 575 for short descriptions of many of these buzzwords and technologies.

Conventions

The following tables describe the typefaces and symbols used in this manual.

Table 1: Typography

Typography	Meaning
`Computer Output`	is data generally display or presented by the computer
`User Input`	is text or commands that you type, contrasted with onscreen computer output
`Button`	is the text on a button, used to describe what button to click
`Menu`	indicates the name of a menu or tab that takes you to specific options
`MENU` > `BUTTON`	describes which buttons to click and the order to click on them for a specific action to occur: for example `FILE` > `PRINT` says to click on the menu named “File” and then the Menu item named “Print”.

Table 2: Symbols

Symbol	Meaning
NOTE -	Notes describe particular features which require attention
CAUTION -	Cautions explains conditions that may cause unwanted results
TIP -	Tips offer useful suggestions

Safety Precautions

WARNING THERE ARE NO USER SERVICEABLE PARTS INSIDE THIS EQUIPMENT. SERVICE MUST BE PERFORMED BY QUALIFIED SERVICE PERSONNEL. **OPENING CASE VOIDS GUARANTEE**.

VORSICHT KEIN TEIL IM GEHÄUSE KANN VOM BENÜTZER SELBST REPARIERT WERDEN. BITTE WENDEN SIE SICH AN QUALIFIZIERTES WARTUNGSPERSONAL. **DAS ÖFFNEN DES GERÄTES FÜHRT ZUM VERLUST DER GARANTIE.**

ATTENTION CET APPAREIL NE CONTIENT AUCUN ELEMENT QUE L'UTILISATEUR PUISSE REPARER. CONFIEZ LA MAINTENANCE AU PERSONNEL TECHNIQUE QUALIFIE. **L'OUVERTURE DE L'APPAREIL ANNULE LA GARANTIE**.

Release History

For more up-to-date information be sure to check the LIGHTNING web site at http://www.lightning.ch/support.

LIGHTNING-Linux 3.7

- added IPSec Domain Name support for endpoints, (ideal for use with a Dynamic DNS service)
- added IPSec wizard on web interface
- added IPSec "Allow Subnets" feature to easily configure Roadwarrior connections
- added IPSec configurable Dead Peer Detection timeout and polling
- added IPSec event log output on webserver and Monitor software
- added Ability to start and stop individual tunnels (in Monitor, Configurator and CLI)
- added DHCP over IPSec with Proxy ARP to serve Roadwarriors a local IP (recommended to be used with SSH Sentinel)
- added High Availability option for many services including IPSec using the VRRP protocol
- added Quick Restore Button enhancement: choose to load the boot configuration, a custom emergency configuration, or the factory default configuration, with LED feedback.
- added MAC based SPI Filtering
- added New CLI commands for IPSec, date & time
- added Configuration import feature for exchanging configurations between different devices
- added CertIssuer software for managing IPSec PKI x.509 keys.

LIGHTNING-Linux 3.6

- added IPSec PKI x.509 Certificate Authority, External Certificate and Certificate Revocation list support
- added IPSec traffic discrimination support for protocol and ports
- added IPSec "Allow Subnets" feature to easily configure Roadwarrior

connections

- added IPSec configurable Dead Peer Detection timeout and polling
- added IPSec event log output on webserver and Monitor software
- added Ability to start and stop individual tunnels (in Monitor, Configurator and CLI)
- added DHCP over IPSec with Proxy ARP to serve Roadwarriors a local IP (recommended to be used with SSH Sentinel)
- added High Availability option for many services including IPSec using the VRRP protocol
- added Quick Restore Button enhancement: choose to load the boot configuration, a custom emergency configuration, or the factory default configuration, with LED feedback.
- added MAC based SPI Filtering
- added New CLI commands for IPSec, date & time
- added Configuration import feature for exchanging configurations between different devices
- added CertIssuer software for managing IPSec PKI x.509 keys.

LIGHTNING-Linux 3.5

- added SSH Port Forwarding VPN Option
- added IPSec Features: statistics, NAT Traversal, RoadWarrior Support, IKE key support for FQDN and email, Serpent encryption, SHA2 256 & SHA2 512 Authentication, Modp 2048, Modp 3072 & Modp 4096 Diffie-Hellman (DH) Groups, connection table, Dead Peer Detection
- removed IPSec Features: IDEA Encryption, Tiger192 & Ripemd160 Authentication, IKE data-size rekeying
- added Network Intrusion Detection System (Enterprise only)
- added Domain Name Server
- added CLI user management
- added Syslog notification of dropped SecureWall packets
- added support for Quick Restore config button
- added in-table editing with Configurator software
- added DSL support for Enterprise DSL

LIGHTNING-Linux 3.4.1

- fixed remote boot issue after upgrade

LIGHTNING-Linux 3.4

- added SSH v2 telnet access
- added GUI web interfaces
- added FTP server
- added NTP server
- added Dynamic DNS support
- added Ethernet parameter editing (MAC, MTU...)
- added Status messages to web interface
- added Easy Firewall to web interface
- added option to disable Proxy DNS cache
- added compatibility for new MultiCom products

LIGHTNING-Linux 3.3

- added IPSec manual keying
- added PPTP passthrough
- added PPPoE call management
- added DHCP/BootP relay
- added ARP Proxy
- added HTTPS
- added multimedia application support (H.323)
- activation of security led
- added compatibility for new MultiCom products

LIGHTNING-Linux 3.2.1

- added french online help for Configurator software
- bug fixes for new Configurator software
- added compatibility for new MultiCom products

LIGHTNING-Linux 3.2

- added IPSec VPN option
- added Internationalisation options (French, German, English)
- added PPTP for selected Broadband modems
- added Easy Firewall in Configurator software
- added additional administrative access accounts
- enhanced backward compatibility
- added Bootp/DHCP Relay
- enhanced Object Filtering in Configurator software

LIGHTNING-Linux 3.1

- added support for multi-sessions of PPP Over Ethernet (PPPoE)
- expanded PPPoE option support
- added PPPoE trace support via syslog
- added Easy-Setup configuration via web server
- added support for Routing Information Protocol (RIP) v2
- added object filtering options for managing filter parameters
- added command line interface (CLI) via console or telnet
- added support for load-sharing using NAT

LIGHTNING-Linux 3.0.1

- added support for PPP authentication over Ethernet (PPPoE)
- added support for SNMP v2 MIB (read-only)
- added support for proxy DNS

Advanced Configuration Software Requirements

For advanced configuration options you may install or run the Configurator Software from your MultiCom Companion CD. Below are the requirements to use this software.

- CD-ROM drive (if installing the Configuration software from CD-ROM)
- Mac OSX, Windows 98, ME, NT4.0, 2000, XP, 2003 or higher, Linux kernel 2.2 or higher, Solaris version 2 or higher

- Pentium CPU, PowerPC CPU or better
- SVGA monitor with at least 800x600 pixel display and 256 colors (more than 256 colors are recommended)
- 64MB of RAM,
- 40 MB of free hard disk space

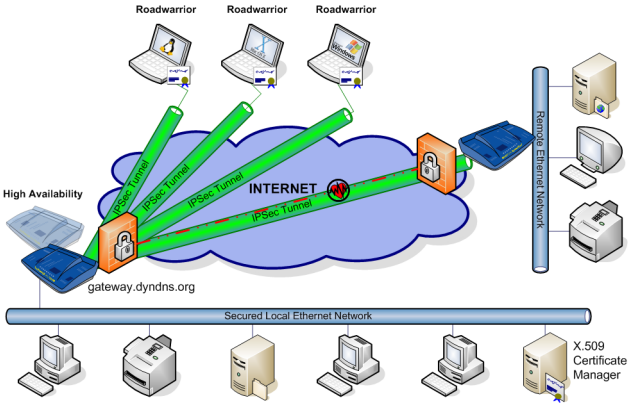
NOTE - The web interface of the MultiCom Firewall has an Easy Setup wizard for Internet and IPSec VPN connections.

LIGHTNING - Linux Features

Chapter 2

LIGHTNING-Linux Features

Your Lightning-Linux firmware offers tools to configure firewall security, manage your networked connections, to create paths for your data to travel through, monitor your network, and keep up to date with the latest networking enhancements.



Remember Easy Setup, Easy Firewall and Easy IPSec are available on the built-in web server to with the Configurator software is always available to quickly get you up and running and to keep your configuration simple.

NOTE — The term “Internet” is used to describe the network that you use the MultiCom Firewall to connect to. Because the MultiCom Firewall has NAT and VPN features you can also use it to connect to other remote computers or servers such as those at another office site. To keep things simple we will refer to the external or WAN network as the “Internet”.

MultiCom Firewall Features

Security

- Dual firewalls, using Stateful Packet Inspection (SPI) Filtering and/ or a NAT based Firewall on each interface to protect against External Intrusions, Denial of Service (DoS), Port Scanning, Spoofing Attacks and more
- URL Filtering to block or drop web connections based on URL or keywords.
- Intrusion Detection System (IDS) using SPI filtering & syslog
- Real time alerts and statistics using Syslog, SNMPv2, web-based Event Monitor, email and more
- Up to 10 separate user accounts with passwords and access rights
- Secure SSL (HTTPS) & SSHv1-2 (telnet CLI) for remote access & configuration
- DMZ interface support giving extra security for network servers (Ethernet III and Enterprise Ethernet only)

Internet Access

- Connect multiple computers and ethernet devices to the Internet using Internet Sharing using Network Address Translation (NAT)
- Easy Setup & Easy Firewall wizards via the web interface or the multi-platform Configurator software
- DNS Cache for faster Internet response
- Dynamic DNS supporting 9 different services for finding your computer even

if the IP address changes

- Multimedia (H.323, IRC, ICQ) and PPTP client pass through support with NAT
- DHCP server (up to 1,000 clients) for automatic IP configuration to clients or DHCP Relay on any Interface
- Ethernet parameter editing for MTU, MAC address, duplex and speed
- Integrated PPPoE client, for single or multiple concentrators (for ISP backup purposes)
- Network traffic round-robin load sharing using NAT
- Virtual IP address support for one or more IP addresses using ARP Proxy and Network Address Translation
- IP Port Redirection with NPAT Network Port & Address Translation
- Static and dynamic routing using RIP (V1 and v2)

Management

- Configurator software for configuring Virtual Private Networks, validating configurations, managing all features and firewall rules. Available for Windows, Macintosh, and Linux. With secured remote access.
- Monitor software to manage status and restart services like PPP, IPSec, VRRP, DHCP. Available for Windows, Macintosh, and Linux. With secured remote access.
- Configuration scheduling for up to 6 configuration files based on day, hour or minute.
- Telnet, console & ssh Command Line Interface (CLI) with powerful network tools like ping, traceroute name server lookup. Ideal for scriptable configuration changes using 3rd party software like CatTools for time based and centralized management
- Quick Restore Button with LED feedback to load boot config, emergency config (config 1), or the factory default configuration. Additional memory is available on each device to store up to 6 different configurations.
- Centralized time management using the Network Time Protocol
- Transfer configurations to and from the device using the File Transfer Protocol (FTP)
- Built-in Domain Name Server (DNS) to name local computers
- Multilingual with English, French and German built-in

- Upgradable flash memory

Software Add-on Options

- IPSec based Virtual Private Network (VPN) supporting Gateway, client and point-to-point modes. Preshared, Manual and PKI x.509 Keys for central management and 3rd party vendor compatibility. Support for multiple world-class encryption ciphers such as AES (Rijndael), CAST 128, Twofish, Blowfish, 3DES and more. Includes Dead Peer Detection (DPD), NAT Traversal, DHCP over IPSec, Traffic filtering, Domain Name endpoints, Connection testing support.
- SSH Port Forwarding VPN Gateway with public key or user based access, using SSH v1 and v2. With unique authentication for up to 10 users.
- High Availability using the VRRP protocol with authentication
- Network Intrusion Detection System (NIDS) using SNORT for Enterprise devices
- Network Monitoring Service for monitoring local and remote TCP servers.
- Certificate Manager software for generating, managing and deploying PKI x.509 keys, certificates and certification authorities. Available for Windows, Macintosh, and Linux.
- VPN Client software available

Network Hardware

- 10/100 Mbit/s multi-interface Switch for high-speed communication within your network (Ethernet III & Enterprise Ethernet only)
- 10/100 Mbit/s autosensing LAN interface for your Local network
- DSL annex A integrated modem (Enterprise DSL only)
- 802.11b WiFi with LAN Bridge (Enterprise WiFi only)

Options

Certain functionalities, such as IPSec VPN, SSH Port Forwarding VPN, High Availability or Network Monitoring are not immediately available in the standard firmware releases. These functions are called Options and need to be purchased and activated to be usable.

Activation of Options currently requires the user to install a unique key file (versions before 3.4 required a special firmware) containing the purchased options and then reboot the MultiCom Firewall. Currently the options are available IPSec VPN 2 tunnels, IPSec VPN 20 tunnels and unlimited IPSec VPN tunnel options.

- IPSec VPN 2 Tunnels
- IPSec VPN 20 Tunnels
- IPSec VPN unlimited Tunnels
- SSH Port Forwarding VPN 10 Users
- Network Intrusion Detection System (NIDS)
- High Availability (VRRP)
- Network Monitoring

Below are the requirements of this process:

- The option key or firmware is only valid on the machine for which it was purchased.
- For machines using a Lightning Linux older than 3.2, you must either first upgrade to the standard OS 3.2 and then apply the firmware with the option or upgrade to at least OS 3.4 and apply the option key.

Contact your distributor if you are interested in purchasing this option.

IPSec VPN Option

All existing MultiCom Firewalls offer Virtual Private Networks (VPN) using the IPSec protocol when the IPSec option is purchased. This is a powerful Secure Remote Access add-on to the standard MultiCom Firewall functionality. Using IPSec the MultiCom Firewall becomes a security gateway, securing data transfers between other IPSec capable devices or computers running IPSec software.

Simple IPSec configuration can be made using the web based wizard. Advanced IPSec configurations require the use of the Configurator software (included on the MultiCom Companion CDROM) in the Advanced Configuration mode. Refer to the Lightning-Linux Reference Manual for information on configuring this feature.

Optionally, the Certificate Manager can be purchased to manage and deploy PKI Digital Authentication Certificates for more complex IPSec configurations.

For more information or to purchasing this option contact your distributor.

SSH VPN Option

All existing MultiCom Firewalls offer Virtual Private Networks (VPN) using the SSH Port Forwarding protocol when the SSH option is purchased. This is a powerful Secure Remote Access add-on for the standard MultiCom Firewall functionality. Using SSH Port Forwarding the MultiCom Firewall also becomes a security gateway, securing data transfers between remote SSH software on a Macintosh, Windows, Linux, PDA or other computing platform.

All SSH Port Forwarding configurations require the use of the Configurator software (included on the MultiCom Companion CDROM) in the Advanced Configuration mode. Refer to the Lightning-Linux Reference Manual for information on configuring this feature.

For more information or to purchasing this option contact your distributor.

NIDS Option

All Enterprise model MultiCom Firewalls support the Network Intrusion Detection System using the SNORT engine when the NIDS option is purchased. NIDS watches all network traffic passing through the MultiCom Firewall and sends real-time syslog notification if network traffic is seen that matches the activated traffic signatures. This allows servers behind the Firewall such as web and file servers to be monitored for suspicious traffic.

All NIDS configurations require the use of the Configurator software (included on the MultiCom Companion CDROM) in the Advanced Configuration mode. Refer to the Lightning-Linux Reference Manual for information on configuring this feature.

For more information or to purchasing this option contact your distributor.

High Availability Option

All existing MultiCom Firewalls support High Availability using the Virtual Router Redundancy Protocol (VRRP) when the VRRP option is purchased. VRRP allows 1 or more additional MultiCom Firewalls to be configured into a redundant fail-safe backup in case of failure on the Master firewall. This High Availability does not require dynamic routing or router discovery protocols to be installed on local networking devices.

All VRRP configurations require the use of the Configurator software (included on the MultiCom Companion CDROM) in the Advanced Configuration mode. Refer to the Lightning-Linux Reference Manual for information on configuring this feature.

For more information or to purchasing this option contact your distributor.

Network Monitoring Option

All existing MultiCom Firewalls support Network Monitoring when the Network Monitoring Service (NMS) option is purchased. NMS allows the MultiCom Firewall to maintain a list of TCP ports on local and remote networks and regular intervals check if the connection is available and measure the delay time. The results of these status checks are written to the internal log, optionally can be emailed to selected email accounts, and is visible from the web interface and the Monitor software.

All NMS configurations require the use of the Configurator software (included on the MultiCom Companion CDROM) in the Advanced Configuration mode. Refer to the Lightning-Linux Reference Manual for information on configuring this feature.

For more information or to purchasing this option contact your distributor.

Feature Highlights

Network Security

With the IPSec or SSH encryption option, build Virtual Private Networks to secure your networking activity. See the Chapter “IPSec Virtual Private Network” on page 233.

Network Address Translation (NAT) allows your LAN or server to access the Internet while hiding its real network address on your network. See “Hide Internal Network Addresses with NAT” on page 362.

SPI Firewall filtering for controlled access to/from your network. Here you can pick the types of data that you want to block. General options include detection by source, destination, state, type, frequency, service port with even more advanced options. See “Filtering Data Packets” on page 194.

Protect against common hacker attempts by setting thresholds that refuse or log data when exceeded. See “Watch For Security Breaches” on page 390.

Use Object Filtering to quickly configure your own SPI Firewall filtering rules for traffic control, hacking attacks, access or custom logging. See “Filtering Objects” on page 200.

Advanced filtering allows you to carry this even further by picking options like TCP flags, burst levels or the connection state of the data. See “Advanced Filtering Parameters” on page 214.

Physically securing your firewall is as important as securing your data. The MultiCom Firewall has a Kensington Lock Slot built in. See “Physically Secure Your Router” on page 367.

Network Management

Allows multiple users to access the Internet simultaneously through a Single Internet User Account. See “Use One External IP Address for Multiple Computers” on page 391.

Secured Remote management is available using the Configurator software using HTTPS (3.3+), SSHv2 (3.4+) or IPSec connections (3.3+).

Dynamically assign IP address and firewall information using your Firewall’s built in DHCP server for Windows, Apple, Unix and Linux based computers.

Use a remote server to configure a local network with PPTP Passthrough or DHCP Relay (3.3+).

With PPPoE Call management, configure automatic, manual, or permanent PPPoE connections with your ISP (3.3+).

Centrally managed firewall configurations can be saved for backup or to email to a client or support. Search for all of your firewalls on your local network and allow management from one location. See “Backup Your Configuration” on page 350.

Access the web-server or Configurator software in French, English or German.

Multiple alternate configurations for your firewall, storing up to 6 configurations at once. See “Backup Your Configuration” on page 350.

Network Infrastructure

Use more than one IP address on any of the Firewall interfaces using NAT and Proxy ARP. See “Configure Virtual IP Addresses” on page 392.

Select which computers can access which remote (or Internet) services. See “Filtering” on page 210.

Static and dynamic routes (RIP v1 and 2) are easily configured. See “Routing Data Packets” on page 225.

Limit network traffic by type, source IP or network, direction or average throughput. See “Filter Unwanted Activity” on page 363.

Change IP requests transparently on your network, for instance redirect web traffic to a web proxy supporting transparent proxy or even redirect a request for one web server to another. See “NAT” on page 172.

Load sharing you can have IP data requests bounce between a group of mirrored servers, providing faster transparent service to your clients. See “Configure Load Sharing” on page 398.

Network Monitoring

Send alerts from your firewall to syslog servers across your network. Typical syslog alerts include failed logins, connection activity, packets blocked by the NAT Firewall or even customize your own messages. See “Syslog Messages” on page 304.

Be aware when suspicious activity is occurring using custom syslog logging options. By setting frequency limits to particular types of data packets, or other suspicious activity you can send syslog notification with customized comments about the activity. See “Filter Unwanted Activity” on page 363.

SNMP v2 support allows realtime statistics on important network functions of one or more MultiCom Firewalls. Information on traffic patterns, system uptime, routing tables, interface status and even remote connections are available using an SNMP browser. See “SNMP Polling” on page 343.

With the Configurator software you can securely communicate with remote MultiCom Firewall to check routing tables, interface status, DHCP services and more. See “Using the Configurator” on page 423.

Use the built in secured web server for common statistics when you need them. See “Web Server Status Reports” on page 330.

Keep up to date

Flash Memory upgrades allow you to keep your firewall up to date either locally or remotely with the latest networking technology firmware released by Lightning Instrumentation S.A. After you download a newer version of the firmware it is an easy process to then upgrade your firewall. Please check with your distributor about how to get the latest upgrade for your firewall. See “Updating Your Firmware” on page 352.

Chapter 3

Concepts

To help in understanding some of the technologies used in your MultiCom Firewall we have put together overviews of essential topics. For more detailed explanations please check the Recommended Reading section or RFC's on the subject you are interested in. The following subjects are discussed in this chapter.

- Options
- Scheduling
- Users
- Services
- Configuration Files

Options

Certain features, such as IPSec VPN, SSH Port Forwarding VPN, High Availability with VRRP, Network Monitoring and Network Intrusion Detection System are not immediately available in the standard firmware releases. These functions are called Options and need to be purchased and activated to be usable.

Activation of Options currently requires the user to install a unique key file (versions before 3.4 required a special firmware) containing the purchased options and then reboot the MultiCom Firewall.

Below are the requirements of this process:

- The option key or firmware is only valid on the machine for which it was purchased.
- For machines using a Lightning Linux older than 3.2, you must either first upgrade to the standard OS 3.2 and then apply the firmware with the option or upgrade to at least OS 3.4 and apply the option key.

Contact your distributor if you are interested in purchasing options for your for your MultiCom Firewall.

Scheduling

Up to six different configurations can be saved on the Secure Firewall and a scheduler allows the user to choose the days, hours and minutes of when to activate any of these six configurations.

The entire configuration can be changed such as filter rules, VPN access, routing, NAT... and whatever else that can be stored in a configuration file. Additionally, event logs can be scheduled to be sent to valid email accounts from the MultiCom Firewall. Some uses of Scheduling include:

- Rotating configurations allowing for changes based on daytime, nighttime, and weekends, for example URL Filtering
- For remote configurations, new configurations can be tested and automatically reset to a base configuration for guaranteed remote access
- Event Logs can be sent to 1 or more email addresses for remote monitoring
- Schedule VPN access availability
- Redirect incoming server traffic to different servers based on the time of day

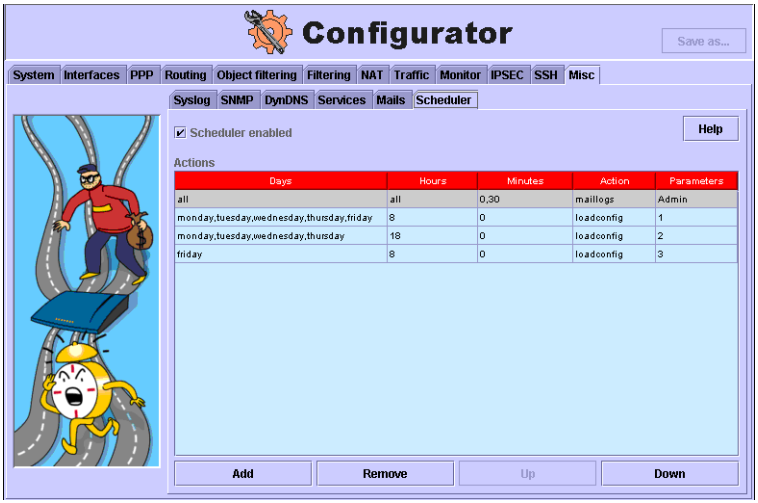
The timing is based on the real time of the system clock so 10 minutes is not 10 minutes from the time of saving the configuration but 10 minutes of the selected hour of the selected day. For example, to load a configuration every 10 minutes the timing should say Day=any, Hours=any, Minutes=0, 10, 20, 30, 40, 50.

Scheduling activity is reported in the Event Log and the Syslog messages.

Using Scheduling

The Configurator Software must be used

To configure Network Monitoring you first must have installed the Network Monitoring option key using the web interface of the MultiCom Firewall. This is available at http://10.0.0.1/tools/options/ where 10.0.0.1 is the IP address of the MultiCom Firewall. The rest of the configuration steps are as follows.



1. Open the Configurator software and connect to the MultiCom Firewall
2. Save the current configuration to a different memory position (the host name can be changed to show the difference between any 2 configurations)
3. Goto the MISC > SCHEDULER panel of the Configurator and check the Scheduler Enabled box
4. Click the Add button to add an action
5. Select the day, hour and minute when the configuration should be changed
6. Select the "loadconfig" action
7. Choose a the Config memory position from step 2 to load under the Parameters drop down box
8. Save the changes

CAUTION - The Scheduler settings are saved inside a configuration file. If you load a configuration (manually or with the scheduler), the new configuration may have a different schedule loaded with it. Be sure that if you have rotating configurations that each loaded configuration file has the Scheduler configuration that you want to use.

Users

Starting with Lightning-Linux version 3.2 it will be possible to configure multiple user accounts on the MultiCom Firewalls. Up to 10 different users can be configured with different usernames, passwords, administrative privileges and Command Line Interface (CLI) access. These Users will be allowed access to the MultiCom Firewall for configuration and data access purposes (from http, https, telnet, ssh, and ftp.) Additionally the Users are the accounts used to authenticate incoming SSH Port Forwarding users. These accounts are not related to PPPoE or PPTP accounts with an Internet Service Provider. The three different types of users are:

- Guest Users
- Configuration Users
- Privileged Users

Usernames must start with a lowercase letter and can be followed by lowercase letters or numbers. The usernames of “multicom” and “root” are not accepted. Viewing, editing, adding and deleting users can be done with both the Configurator software and from the built-in webserver of MultiCom Firewalls running Lightning-Linux 3.2 or greater.

NOTE - the default user “multicom” will disappear after the first Privileged user is added and will reappear if there are no more Privileged users configured.

This means that the first time you configure a Privileged user you will need to relogin as the new user since the default username “multicom” became disabled as soon as you saved the new Privileged name. It is not possible to edit the “multicom” user itself.

Guest Users

Guest users can only read a configuration but may not make changes to it. This allows them to check the status of a MultiCom Firewall or review the configuration but not to make changes, save or apply a configuration (it is not even possible to save the configuration to a computer file from the Configurator). The only change that a Guest user can make is to change their password

Configuration Users

Configuration Users can read and write the configuration of the MultiCom Firewalls but they cannot read or write the security keys used for IPSEC tunnels. Additionally, these users can create Guest users as well as edit their own passwords. The Configuration users can also save configurations to computer files from the Configurator software.

Privileged Users

Privileged users have access to all functionality of the MultiCom Firewalls. These users have all of the abilities of the previous users in addition to having read and write access to the IPSEC security keys, create and delete all other user accounts (but can only edit their own account), update the firmware.

User Rights

All users can use their username and password to login to the telnet, ftp, web servers as well as use the Configurator software to interact with MultiCom Firewalls. The following 2 tables summarize the rights of all user categories.

Table 1: Web Interaction Rights

Activities	Guest User	Configuration User	Privileged User
Easy Setup	no	yes	yes
Configuration	no	yes, restricted	yes
Status	yes	yes	yes
Configuration Tools	no	yes	yes
Users Configuration	no	yes, restricted	yes
Language Selection	yes	yes	yes
Firmware Upgrade	no	no	yes
Reboot	no	yes	yes

Table 2: CLI Interaction Rights

Commands	Guest User	Configuration User	Privileged User
loadconfig	yes	yes	yes
saveconfig	no	yes	yes
showconfig	yes	yes	yes
help	yes	yes	yes
info	yes	yes	yes
print	yes	yes	yes
go	yes	yes	yes
set	no	yes	yes
add	no	yes	yes
del	no	yes	yes
ping	yes	yes	yes
traceroute	yes	yes	yes
nslookup	yes	yes	yes
dhcpclient	no	yes	yes
reboot	no	yes	yes
exit	yes	yes	yes

CLI Access Rights

Starting in Lightning-Linux 3.5 it is possible to give users the right to access the CLI or not. This is useful when configuring users for SSH Port Forwarding VPN access. Previously all added users could access the CLI through a telnet session or serial cable.

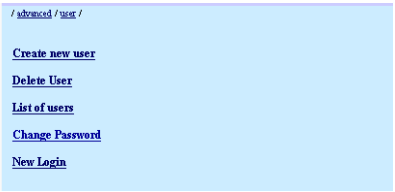
If you have the SSH Port Forwarding option, the MultiCom Firewall's user list is used to authenticate incoming VPN connections with the assigned password or private key. Only one user can log into the CLI at any time so it is possible that an incoming SSH Port Forwarding user might accidentally login to the CLI, blocking administrative users. If incoming SSH users do not need CLI access it is best to disable it in their User Rights table.

NOTE - User's without CLI access can still log into the HTTP or HTTPS interface of the MultiCom Firewall. It is recommended to give incoming SSH VPN users "Guest" privileges unless they are administrators of the firewall.

Configuring Users

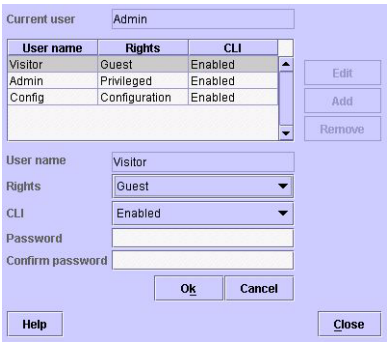
Using The Webserver

Users can be configured from the MultiCom Firewalls web server at http://10.0.0.1/advanced/user/ where “10.0.0.1” is the IP address of the MultiCom Firewall. The administrator can create, delete user accounts as well as change the password of the active account. It is not possible to change the passwords of other users without first logging in as that user or deleting the user and recreating the account.



Using The Configurator

Additionally, configuration of users is available from the Configurator software that is connected to a live configuration of a MultiCom Firewall. The button is in the Configurator text menu at Tools>User management and is shown below.



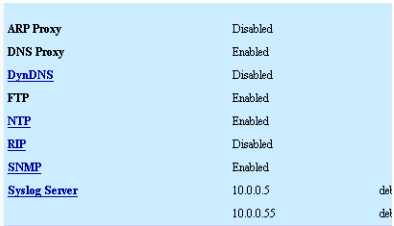
Using The CLI

Starting with Lightning-Linux 3.5 it is possible to configure users using the CLI interface (either with Telnet, SSH Telnet, or Serial console connection). The commands available are: deluser, listusers, adduser, and passwd. These commands are described with the other CLI commands in the “CLI Command Summary” on page 89.

Services

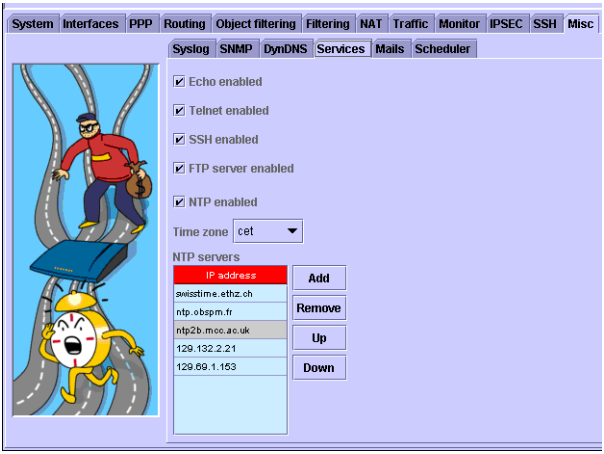
The MultiCom Firewall has many features that are called services. These are programs that run inside the MultiCom Firewall provide useful tasks to the connected networks. Many of these services are described in their own chapters. The easiest way to activate these services is to use the Configurator software to activate them. The status of these services can be viewed through the built-in web server’s status screen at http://10.0.0.1/status/services/ (where 10.0.0.1 is the IP address of the MultiCom Firewall.) These services are

- ARP Proxy (See “Proxy ARP” on page 188.)
- DNS Proxy (See “Proxy DNS” on page 148.)
- Dynamic DNS (See “Internet Dynamic DNS” on page 152.)
- Echo enabled (See below)
- FTP (See “FTP Access” on page 84.)
- NTP (See below)
- RIP (See “Dynamic Routing with RIP” on page 227.)
- SSH telnet (See “Accessing CLI With Telnet” on page 86.)
- SNMP (See “SNMP” on page 341.)
- Syslog (See “Syslog Messages” on page 304.)



Echo enabled

Starting with Lightning-Linux 3.4 it is possible to tell the MultiCom Firewall to not respond to the Configurator software search requests. Enabling this option allows the Configurator software to search for the MultiCom Firewall on a network. Disable this option if you do not want the MultiCom Firewall to be visible to searches by the Configurator. It is available for configuration at the MISC>Services panel of the Configurator software.



NTP

Starting with Lightning-Linux 3.4 the Configurator software can be used to configure the Network Time Protocol (NTP) service on the MultiCom Firewall. This service allows the firewall to query remote servers for the correct time (See RFC1305) and for clients on the local network (LAN) to query the MultiCom Firewall to receive this time.

One or more remote NTP servers can be queried for the current time. Once configured, LAN computers can be directed to the MultiCom Firewall to receive the most current time using 3rd Party software or the built in NTP client services of Windows XP. The MultiCom Firewall will regularly verify the current time with the remote servers. Any public NTP server can be queried by their IP address or URL Domain name. A list of public NTP servers can be found at http://www.eecis.udel.edu/~mills/ntp/servers.html.

Starting in Lightning-Linux 3.5 it is also possible to configure the Time Zone Adjustment to compensate for the geographical location of the MultiCom Firewall. Lightning-Linux 3.6 additionally offers the option of loading a timezone file for a particular region of the world. These files are stored in the zoneinfo directory of your Configurator installation or the MultiCom Companion CD.

Configuration Files

The MultiCom Firewalls contain 3 configuration files which are stored in Flash memory. All of these will need to be backed up to safeguard the complete configuration. The 2 areas which you cannot backup are the user lists and PKI keys and Certificates. These need to be stored separately. The 3 configuration files are:

- Device Configuration file
- Security Key File
- URL Filtering Rules

When the MultiCom Firewall boots (powers on) it executes the commands that it finds in the “boot configuration” file. There are also memory space to store up to 6 other device configuration files in the Flash memory but this is for storage only as the MultiCom Firewall will not use them when it boots. If the IPSec option is enabled, there is a second Security Configuration file that contains the Preshared and Manual keys as well as the x.509 key definitions used to make the VPN connections.

Although the use of the Configuration software is the recommended method for building and editing the configuration files of your MultiCom Firewall there are times when you may prefer to work with the raw configuration file itself.

- to see at a glance the entire configuration of the firewall
- to email it for support or remote editing
- to cut and paste features from other configurations
- to enter a configuration just by using the web server on the firewall
- to create large filtering tables in a spreadsheet program and cut and paste them into an actual configuration

Parts of a Configuration File

The configuration file is stored in a tree structure which contains all configuration parameters. These parameters describe the expected behavior of the firewall hardware and can be modified by the user.

Each section of the structure is a component that will have a beginning and ending announcement. These components are hierarchical and are used in the same order that they are entered in the file. For instance, in a list of filters, the ones on top are the ones that are checked first.

The configuration file also follows the MIB definition as shown from the Configurator software's TOOLS > Show MIB Tree menu. Sample configurations are also available on the MultiCom Companion CD and from the support website. The order of the statements is as follows:

> CAUTION - the order stated below is a summary. Lightning-Linux requires specific syntax to write commands in a text file. If you want to edit sections by hand it is recommended that you first make a similar configuration in the Configurator, save the configuration to your hard disk, and then edit it with a word processor.

```
begin config
  begin ip
    begin dns
      begin proxy
        begin local_address
    begin routing
      begin static
    begin filtering
      begin input
      begin forward
      begin output
      begin user
    begin nat
       max_connection_tracking
    begin syslog
      begin server
    begin snmp
      begin security
```

```
    begin filtering_objects
      network
      service
      action
      log
      begin network_list
      begin service_list
      table (of object filter rules)
    begin ftp
      begin server
    begin ntp
      begin server
    begin dyndns
      begin service
    begin mail
      being client
  begin interface
    begin Ethernet (interface LAN/WAN/DMZ/WLAN/DSL)
      begin bridge (for devices with WLAN)
        begin use
          begin ethernet
          begin bridge_atm (if ADSL interface)
        begin stp
      begin ip
        begin dhcp
          begin server or client
          relay
        begin vrrp
          begin virtual_address
          begin authentication
      begin arp
        begin proxy
          begin table
      begin settings
    begin ppp interface
      begin ip
        begin nat
          begin input
          begin output
      begin use (which physical interface to use PPP on)
```

```
      begin ethernet
    begin authentication
  begin dsl
    begin atm
        begin connection
          begin aal5
  begin wlan
    begin settings
    begin wep
    begin acl
begin routing
  begin ip
    begin rip
      begin neighbor
begin security
  begin ipsec
    begin filters
    begin connection
      begin remote_addr
      begin local_addr
      begin manual
        begin key
      begin ike
        begin ike_proposal
        begin sa_proposal
        begin pfs
        begin dpd
    begin ike_proposals
      begin ike
      begin sa
    begin contexts
    begin options
    begin dhcp
    begin proxy_arp
  begin access
    begin ssh
      begin server
        begin protocol
        begin authentication
  begin nids
```

```
    begin url_filtering
    begin monitor
      begin host
  begin timer
```

Default Configuration File

The default configuration of the MultiCom Firewall is loaded at the first boot of the MultiCom Firewall and when the config button is held down during power up.

This file can be edited directly on the MultiCom Firewall via the built-in web server at http://10.0.0.1/advanced/config/ (where 10.0.0.1 is the IP address of your MultiCom Firewall) or edited with the Configurator software. It is also possible to enter commands on-line from a telnet or serial connection (if supported by the hardware), however these commands are not automatically stored in the configuration file and their effect will be lost the next time the MultiCom Firewall reboots unless saved manually to one of the existing memory locations.

The current default configuration has the following characteristics:

- WAN configured as DHCP client
- LAN configured as DHCP server
- DMZ is disabled
- Internal firewall IP address/ netmask 10.0.0.1/255.0.0.0
- Internal clients served IP addresses from 10.0.0.17 to 10.0.2.254
- All outgoing connections use address of WAN interface as the source (NAT)
- Firewall enabled (external connections allowed only when a response to a request from the LAN)
- Proxy DNS is on
- SNMP and syslog messaging disabled

> NOTE - This configuration is used as a template when using the Easy Setup to make a basic configuration. When this happens the DHCP client on the WAN interface is replaced by either the PPPoE, PPTP or the Static settings you enter in Easy Setup.

See below for how this configuration looks when edited by a word processor.

Default Configuration File

```
# ************************************************************
# ************************************************************
# ***                                                      ***
# ***      Apliware Firewall Configuration File            ***
# ***                                                      ***
# ***      Date : 10/20/2004        Time : 00:08:36        ***
# ***      User : Privileged ( Privileged )                ***
# ***                                                      ***
# ***   Hardware Type    :          MultiCom SpeedSurf     ***
# ***   Serial Number    :           LI-MU11-CH-022518     ***
# ***   Firmware Version :                       3.7       ***
# ***   Option           :                   IPSEC20       ***
# ***   Option           :                   SSHDVPN       ***
# ***   Option           :                      VRRP       ***
# ***   Option           :                       NMS       ***
# ***                                                      ***
# ************************************************************
# ************************************************************

begin config
  begin ip
    begin dns
      mode = dynamic
    end dns
    begin filtering
      enabled = true
      begin forward[]
        protocol = tcp
        dport = 137
        to_interface = WAN
        object_key =
ANY;WAN_Interfaces.WAN_Network;NetBIOS_Services.NetBIOS_Name_Servic
e-TCP;DROP;;
      end forward
      begin forward[]
        protocol = udp
        dport = 137
        to_interface = WAN
        object_key =
ANY;WAN_Interfaces.WAN_Network;NetBIOS_Services.NetBIOS_Name_Servic
e-UDP;DROP;;
      end forward
      begin forward[]
        protocol = tcp
        dport = 138
        to_interface = WAN
```

```
        object_key =
ANY;WAN_Interfaces.WAN_Network;NetBIOS_Services.NetBIOS_Datagram_Se
rvice-TCP;DROP;;
      end forward
      begin forward[]
        protocol = udp
        dport = 138
        to_interface = WAN
        object_key =
ANY;WAN_Interfaces.WAN_Network;NetBIOS_Services.NetBIOS_Datagram_Se
rvice-UDP;DROP;;
      end forward
      begin forward[]
        protocol = tcp
        dport = 139
        to_interface = WAN
        object_key =
ANY;WAN_Interfaces.WAN_Network;NetBIOS_Services.NetBIOS_Session_Ser
vice-TCP;DROP;;
      end forward
      begin forward[]
        protocol = udp
        dport = 139
        to_interface = WAN
        object_key =
ANY;WAN_Interfaces.WAN_Network;NetBIOS_Services.NetBIOS_Session_Ser
vice-UDP;DROP;;
      end forward
      begin forward[]
        state = new,established,related
        action = accept
        from_interface = LAN
        object_key = LAN_Network;ANY;ANY;ACCEPT;;
      end forward
      begin forward[]
        state = established,related
        action = accept
        to_interface = LAN
        object_key = LAN_Network;ANY;ANY;ACCEPT;;
      end forward
      begin forward[]
        from_interface = WAN
        object_key = Drop*FromWAN
      end forward
    end filtering
    begin filtering_objects
      enabled = true
      begin table[]
```

```
      source = ANY
      destination = WAN_Interfaces
      service = NetBIOS_Services
      action = DROP
    end table
    begin table[]
      source = LAN_Network
      destination = ANY
      service = ANY
      action = ACCEPT
    end table
  end filtering_objects
end ip
begin interface
  begin ethernet[WAN]
    begin ip
      begin dhcp
        mode = client
        begin client
          begin request[]
          end request
          begin request[]
            name = broadcast-address
          end request
          begin request[]
            name = routers
            mode = require
          end request
          begin request[]
            name = domain-name
          end request
          begin request[]
            name = domain-name-servers
            mode = require
          end request
        end client
      end dhcp
      begin nat
        enabled = true
        securewall = true
        begin input[]
          protocol = tcp
          dport = 113
          mapping = internal
          to_port = 113
        end input
      end nat
    end ip
```

```
    end ethernet
    begin ethernet[LAN]
      begin ip
        address = 10.0.0.1
        netmask = 255.0.0.0
        begin dhcp
          mode = server
          begin server
            begin range[]
              from = 10.0.0.17
              to = 10.0.2.254
            end range
          end server
        end dhcp
      end ip
    end ethernet
  end interface
end config
```

Security Key File

This file is only generated when the IPSec option is installed and Preshared or Manual keys are created. Only Privileged Users can read and write to this file. For backup purposes this file should be copied to a floppy or disk drive.

This file can be edited directly on the MultiCom Firewall via the built-in web server at http://10.0.0.1/advanced/security/ (where 10.0.0.1 is the IP address of your MultiCom Firewall) or edited with the Configurator software. It is also possible to enter commands on-line from a telnet or serial connection (if supported by the hardware).

Sample Security Key File

```
# ********************************************************
# ********************************************************
# ***                                                  ***
# ***      Apliware Firewall Configuration File        ***
# ***                                                  ***
# ***      Date : 10/20/2004       Time : 16:21:16     ***
# ***      User : Admin ( Privileged )                 ***
# ***                                                  ***
# ***   Hardware Type    :       MultiCom Ethernet III  ***
# ***   Serial Number    :           LI-MU10-CH-020576  ***
# ***   Firmware Version :                        3.7   ***
# ***   Option           :                  IPSEC20    ***
# ***   Option           :                  SSHDVPN    ***
```

```
# ***   Option           :                          VRRP   ***
# ***   Option           :                           NMS   ***
# ***                                                      ***
# ************************************************************
# ************************************************************

begin security
  begin ipsec
    begin psk[]
      name = Home_Key
      secret = home
      local_id = isp.com
      remote_id = home@isp.com
      local_id_type = fqdn
      remote_id_type = e-mail
    end psk
    begin psk[]
      name = Office_Key
      secret = office
      local_id = 10.0.0.1
      remote_id = 192.168.0.2
    end psk
    begin psk[]
      name = firewall
      secret = firewall
    end psk
    begin psk[]
      name = secret
      secret = secret
    end psk
    begin x509[]
      name = Test2
     local_id = "CN=My Company Root, O=Apliware SA, OU=IT, L=Geneva,
C=CH"
      remote_id = "CN=VPN Gateway, O=My Company SA, OU=IT,
L=Neuchatel, C=CH"
    end x509
    begin x509[]
      name = ExternalCert
      client_certificate = PublicCertificate1
    end x509
    begin x509[]
      name = Roadwarrior
      local_id = "CN=Captain Haddock, O=Apliware SA, OU=Naval,
L=Brussels, C=BE, E=haddock@apliware.ch"
      remote_id = "CN=Tintin, O=Apliware SA, OU=Documentation,
L=Geneva, C=CH, E=tintin@apliware.ch"
    end x509
```

```
    begin manual[]
      name = Bank_Key
      cipher_algo = cast
      cipher_key_in = 11111111111111111111111111111111
      cipher_key_out = 22222222222222222222222222222222
      auth_key_in = 11111111111111111111111111111111
      auth_key_out = 22222222222222222222222222222222
    end manual
  end ipsec
  begin vrrp
    begin authentication_contexts[]
      name = "HighAvailability Key 1"
      type = pass
      key = 1234567890abcdef
    end authentication_contexts
    begin authentication_contexts[]
      name = "HighAvailability Key 2"
      key = 1234567890abcdef
    end authentication_contexts
  end vrrp
end security
```

URL Filtering Rules

This file contains the keywords and domain names that is used by the URL filtering service to block access to the matching web sites. Only Privileged Users can read and write to this file. For backup purposes this file should be copied to a floppy or disk drive.

This file can be edited directly on the MultiCom Firewall via the built-in web server at http://10.0.0.1/advanced/filters/ (where 10.0.0.1 is the IP address of your MultiCom Firewall) or edited with the Configurator software. It is also possible to enter commands on-line from a telnet or serial connection (if supported by the hardware).

> NOTE - The MultiCom Firewalls can support up to 100 keywords or domain names.

Sample Filtering Rules

```
action DROP
server apple.com
path trailers
path ipod
path games
```

```
action DROP
server bluewin.ch
path mail
path unterhaltung
path shopping
path /news/
path divertissements
path intrattenimento
action DROP
server google.com
path imghp
path nwshp
path froogle
action DROP
server yahoo.com
path adv
path promotions
action DROP
path sex
path liveadvert
path porn
path adserver
path casino
path xxx
```

Import Configuration

Starting in Configurator version 3.6 there is a new Import feature available from the Configuration menu. Import allows for exchanging configurations between different devices. This feature moves a configuration file from one MultiCom Firewall to another of a different model.

> CAUTION - this will replace the existing configuration with the imported one. It is not meant to import only a portion of another configuration.

If there are missing interfaces or features in the new devices then these portions of the configuration will not be imported (for instance ADSL, ISDN, WIFI, DMZ interfaces are not present in all devices.)

Option related portions of a configuration file (for example IPSec and SSH) will be imported only if the new configuration already supports these features. In this case you will need to open a configuration from the new device first because the default configuration for any device does not have any options activated.

The following standard portions of a configuration will be imported. If they do not exist in the configuration being imported then they will be deleted in the current configuration.

- System Hostname
- LAN interface configuration
- Routing configuration (including RIP)
- IP portions of the Configuration (DNS, Filtering, NAT, Syslog, SNMP, Filtering Objects, FTP, NTP, DynDNS, VRRP)
- Security configuration (not relating to options, as explained above)

Any existing configuration information in these areas will be overwritten by the imported configuration file.

Importing Partial Configuration

Importing only a portion (node) of a configuration file is possible with special preparation of the file to be imported and the imported portion will replace an existing component. The imported configuration must contain, in addition to the configuration data in MIB format, a variable (# set top_node) to define the access path to the node being imported.

Other variables can be defined and initialized by expressions containing constants, the references to nodes of the current MIB and functions calls. These variables can then be used in the imported configuration. This type of configuration with variables and functions is already used in the case of Configuration Wizards such as ' Requests DHCP client' and ' Filters standard'.

Below is an example based on the ' Filters standard' Wizard:

```
#
# set lan_address = /config/interface/ethernet[LAN]/ip/address
# set lan_netmask = /config/interface/ethernet[LAN]/ip/netmask
# set lan_subnet = subnet (netaddr (lan_address, lan_netmask), lan_netmask)
#
# set top_node = "/config/ip/filtering"
# set clear_node = top_node
#
begin filtering
  enabled = true
  input[] action = forward user_action = Spoofing_FWD-IN
```

```
  forward[] action = forward user_action = Spoofing_FWD-IN
  begin user[Spoofing_FWD-IN]
    filters[] source = 10.0.0.0/8 from_interface = WAN
    filters[] source = 127.0.0.0/8 from_interface = WAN
    filters[] source = 172.16.0.0/12 from_interface = WAN
    filters[] source = 192.168.0.0/16 from_interface = WAN
    filters[] destination = 255.255.255.255/32 action = return
    filters[] source = !<lan_subnet> from_interface = LAN
  end user
end filtering
```

The line ' # set lan_address =... ' creates the variable lan_address which will be initialized with the value of the node /config/interface/ethernet[LAN]/ip/address of the current configuration.

The line ' # set lan_subnet =... ' creates the variable lan_subnet which will be initialized by the result of the evaluation of the expression ' subnet (netaddr (lan_address, lan_netmask), lan_netmask) ', for example ' 10.0.0.0/8 '.

This variable is then used in the configuration in the line ' filters[ ] source =! < lan_subnet > from_interface = LAN ' where it will be substituted by its value.

Chapter 4

Interfaces

Your Multicom Firewall can have up to 3 types of physical interfaces for transmitting data - Ethernet Interfaces, PPP Interfaces, and a Serial Interface.

- Ethernet Interface
- Serial Interface
- Virtual PPP Interface
- ADSL Interface
- WLAN Interface
- Configuration of Interfaces

Ethernet Interfaces

10 Mbits/s Ethernet Interfaces

These Ethernet Interfaces will only communicate with other 10 Mbits/s interfaces. If this interface is to be connected to a faster network (using 100 Mbits/s for instance) a dual speed hub or switch will be needed.

The 10 Mbits/s interface is currently only the WAN interface and is always a non-crossed connection.

10/100 Mbits/s Auto-sensing Interfaces

Some of your Ethernet interfaces on the MultiCom Firewalls support speeds up to 100Mbits/s (typically the LAN and DMZ interface). These ports are actually auto-sensing ports that optionally allow you to connect 10Mbits/s or 100Mbits/s devices to them. The Ethernet interface will automatically detect the highest possible speed the connected device can communicate at and configure itself to the same (either 10Mbits/s or 100Mbits/s).

The Ethernet interfaces that are auto-sensing can also detect if your external Ethernet device is capable of operating at full or half duplex modes and will automatically configure itself to the fastest option. If there is a problem with the autosensing or you simply prefer to manually set the duplex and speed of the interface this can be done with firmware 3.4 or greater on the Interface>Ethernet panel.

NOTE - Products with "Switching hubs" have crossed interfaces on the hub (typically the LAN interfaces). Please refer to your User Manual to correctly identify these interfaces.

Switching Hub

The Ethernet III and Ethernet Enterprise have an expanded LAN interface. There are 4 10/100 mbps autosensing interfaces that are also a switching hub. This means that you can use your Ethernet III as a hub and connect directly up to 4 computers or Ethernet devices.

The switching hub functionality allows these devices to communicate with each other separately from other traffic happening at the LAN interfaces. For example Computer A and Computer B could communicate at 100mbps while connected to the switching hub at the same time as Computer C is using 10mbps Internet access.

The interfaces on the Switching Hubs are already crossed ethernet. Use a straight Ethernet cable to connect from the Switching Hub to a computer or a crossed Ethernet cable to connect to another hub.

MAC Addresses

The Media Access Control (MAC) is used to provide a basic form of identification for Ethernet interfaces which is independent of an IP address. The ARP address is made up of 6 hexadecimal numbers in the form 00:90:F4:00:27:29. The first 3 numbers identifies the manufacturer of the Ethernet device and the last 3 numbers is a unique number for each Ethernet interface.

In the above example the first 3 hexadecimal numbers 00:90:F4 is the identifier of Lightning Instrumentation SA Ethernet interfaces. The final 3 hexadecimal numbers is the unique identification for the particular Lightning product. In the MultiCom line of ISDN firewalls this number is the hexadecimal version of the serial number 10025. With the Ethernet series of firewalls you will have 2 or more ARP addresses, 1 for each of your Ethernet interfaces.

NOTE - MAC addresses can be changed in firmware versions 3.4 or later. This is often needed if you have registered a previous MAC address with your ISP and now want to change devices. This parameter is available under the Interface>Ethernet panel.

A list of common Ethernet devices can be found below. A complete listing can be found at http://www.normos.org/en/ieee.html.

Table 1: Common MAC identification

ARP identifier	
00:90:F4	Lightning Instrumentation
00:A0:C9	Intel Corporation
08:00:20	Sun Microsystems
08:00:09	Hewlett Packard
00:50:E4	Apple Computer, Inc.
00:B0:A4	Cisco
00:B0:D0	Dell Computer
00:C0:F0	Kingston Technology Corp.
00:20:AF	3Com

The Address Resolution Protocol (ARP) uses this information to match up an Ethernet interface with a corresponding IP address. You can use the Configurator Monitoring windows to see the MAC addresses of devices communicating with your firewall.

Serial Interfaces

Serial Interfaces

Some MultiCom Firewalls have a serial interface for console access via a serial connection (currently the MultiCom Ethernet III MultiCom SpeedSurf offer these interfaces.) Using the Serial cable that came with your MultiCom you can connect this interface to another computer's 9 pin serial interface for management or configuration purposes.

The console interface is identical to a telnet interface of the MultiCom Firewall except that it is always on and does not need a proper Ethernet configuration to communicate with the computer.

A user can connect to the Serial Interface using software such as HyperTerminal for Windows, ZTerm for Macintosh or another terminal emulator software. The typical settings are (please see the User Manual for the physical specifications of your particular MultiCom product.):

- Baud Rate: 9600 bits/s
- Data bits: 8
- Stop bits: 2
- Parity: none

The available commands can be found at "Command Line Interface" Section on page 86.

PPP Connections

PPP connections using PPPoE or PPTP encapsulation are different from physical Ethernet interfaces because they override the configuration of the Ethernet Interface they are used on. In the case of PPPoE, multiple PPP Connections can use the same Ethernet Interfaces at once. This means that you could have multiple IP addresses assigned to the same port were each one refers to a different PPPoE connection.

When a PPPoE connections is used on an Ethernet interface it disables any configurations on the specified physical Ethernet interface (such as options for DHCP or static IP address configuration and NAT.) Instead the user must

configure each PPPoE connection separately under the PPP panel of the Configurator. The PPP panel contains options for IP address configuration, default routes, and NAT.

When a PPTP connection is used on an Ethernet interface it has the same characteristics as above except that the IP Address and the Netmask of the specified interface is still active. This is because the PPTP of Lightning-Linux 3.2.x is designed to communicate with modems using this option but only works in conjunction with an existing IP address on the physical interface (usually in the 10.x.x.x range.)

After configuring PPP connections these connections will be available for use in the Routing and Filtering tables by the name the user has assigned to them. For more information on configuring PPP Connections see the “PPP Connections” Chapter on page 157.

ADSL Interfaces

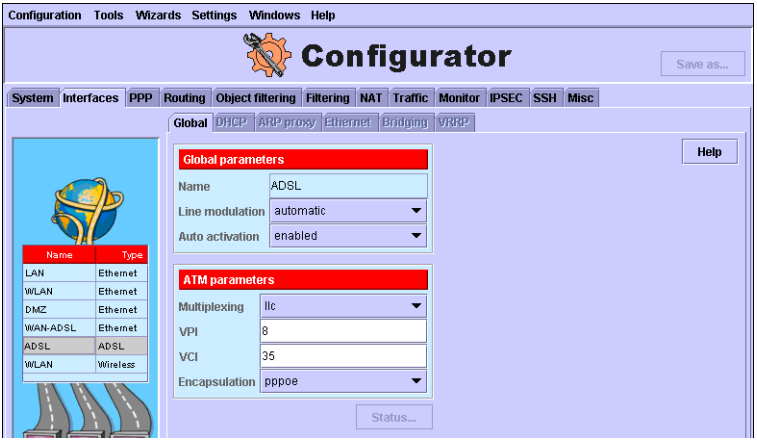
Some MultiCom Firewalls have an ADSL Modem interface (currently the Enterprise ADSL offers this interface.) The ADSL interface will have 2 configuration components, an ADSL Modem configuration and an Ethernet configuration.

ADSL Modem Interfaces

The Configurator software has a DSL interface panel that allows you to configure that interface with PPPoE, PPPoA or a Bridged Ethernet parameters. Set the ADSL parameters as requested by your ISP (Internet Service Provider). According to the selected encapsulation additional parameters will be requested.

The following parameters are available for configuration of an ADSL interface:

- Line Modulation
- Multiplexing
- VPI
- VCI
- Encapsulation



The Easy Setup wizard of the Configurator software or the Web interface will automatically detect this interface and allow quick configuration of the needed parameters.

Diagnostics and status information on this connection is available from the MultiCom web server at http://10.0.0.1/status/adsl/ or from the Interface tab of the Configurator software's Monitor window.

WLAN Interfaces

Some MultiCom Firewalls have a WLAN Modem interface (currently the Enterprise Wireless offers this interface.) The WLAN interface will have 2 configuration components, a Wireless configuration and an Ethernet configuration.

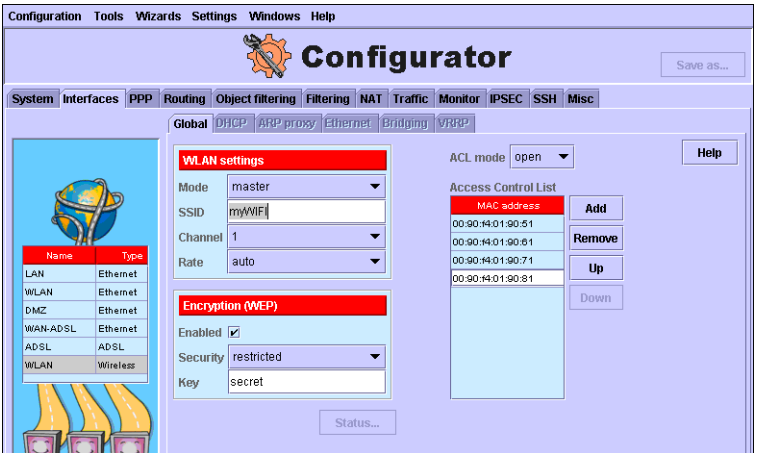
WLAN Wireless Interfaces

The Configurator software has a Wireless interface this panel allows you to configure that interface with Wireless local network (WLAN) parameters. Wireless networks can be configured in 3 possible modes:

- Managed: Another device is acting as the Access Point for the wireless network. All wireless devices must communicate through the Access Point.
- Ad-hoc: also called a peer-to-peer network, all wireless devices can

communicate with each other directly as long as the wireless device is within range of the signal

- Master: sets the MultiCom Firewall as the Access Point for the wireless network. This allows the MultiCom Firewall to distribute IP addresses and manage the wireless activity on the network. All wireless devices must communicate through the MultiCom Firewall. These other devices will be configured in Managed mode.



The Easy Setup wizard of the Configurator software or the Web interface will automatically detect this interface and allow quick configuration of the needed parameters.

Diagnostics and status information on this connection is available from the MultiCom web server at http://10.0.0.1/status/wlan/ or from the Interface tab of the Configurator software's Monitor window

WLAN Security

MultiCom Firewalls with wireless interfaces offer the following security features:

- SSID is not broadcast
- Access Control List based on MAC hardware addresses
- 40 or 104 bit based Wired Equivalent Privacy (WEP) encryption

- Optional use of IPSec tunnels over the WLAN
- Optional use of SSH Port Forwarding over the WLAN

WLAN Bridge To LAN

Starting in firmware 3.7 it is possible to activate a Bridge between the Wireless WiFi network and the LAN network. This allows the two networks to seem as one single network.

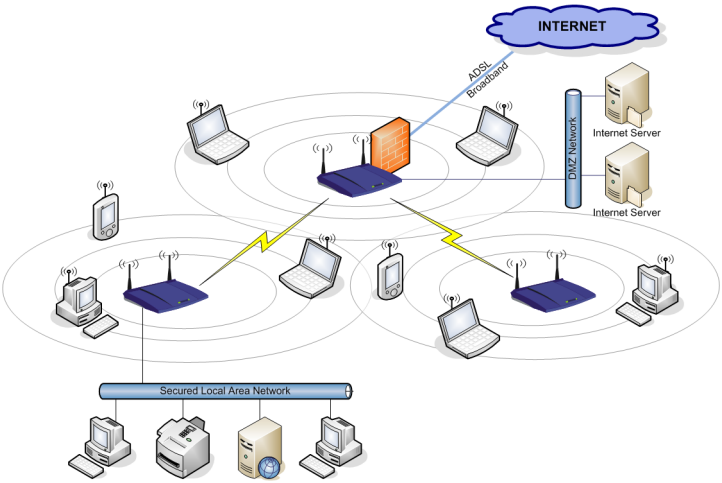


Table 2: Bridge parameters

MAC Ageing	the time in seconds during which a MAC address is valid. The range is from 10 seconds to 1,000,000 seconds, and the default value is 300 seconds. When no traffic has been received from this MAC address the address will be removed from the Forwarding Database
Garbage Collection	the interval in seconds that the MultiCom Firewall will check the Forwarding Database for expired entries. The default is 4 seconds.

This interface optionally supports the Spanning Tree Protocol (STP). STP should be used when 2 or more Bridges are connected to the same network. This protocol dynamically manages redundant paths to the bridged networks while eliminating loops in the bridged network topology.

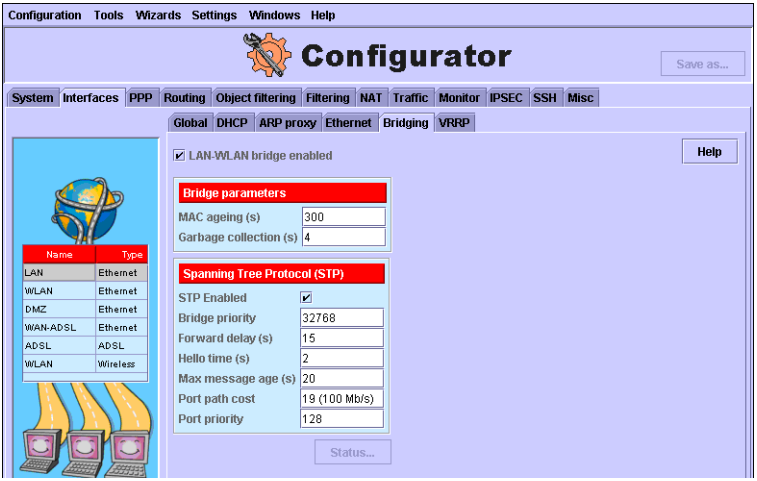
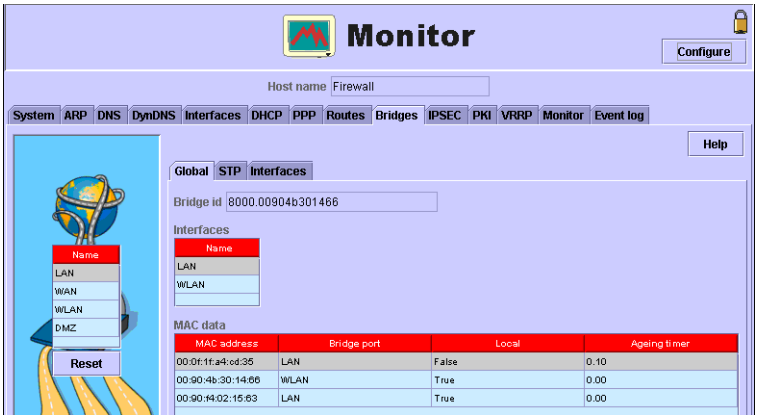


Table 3: STP parameters

Bridge Priority	the priority for this Bridge, the range is from 0 to 65,535 and the default is 32,768
Forward Delay	the time in seconds during which the Bridge is in the "listening & learning" state. The range is from 4 to 30 seconds, and the default value is 15 seconds.
Hello Time	the interval in seconds that the MultiCom Firewall will send a BPDU (Bridge Protocol Data Unit) configuration message. The range is from 1 to 10 seconds, and the default value is 2 seconds.
Max Message Age	the maximum time in seconds that the Bridge will wait to receive a BPDU configuration message. The range is from 6 to 40 seconds, and the default value is 20 seconds.
Port Path Cost	the cost to the subnetwork connected to a port for this Bridge, the range is from 0 to 65,535 and the default is 100. If the user does not choose a value it will be picked automatically based on the bandwidth of the connected port.
Port Priority	the priority for this port so the STP protocol can select a port if two or more ports have the same cost. The range is from 0 to 255, and the default value is 128.

Diagnostics and status information on Interface connections are available from the MultiCom web server at

http://10.0.0.1/advanced/status/interface/ethernet[LAN]/bridge/status/ or from the Interface tab of the Configurator software's Monitor window.



If the STP protocol is activated and port path costs are being used, the table below can be used as a reference for the recommended values of the port path costs.

Table 4: Spanning Tree Protocol Costs

Bandwidth	Value Suggested	Range Suggested	Range Limits
4 Mb/s	250	100-1000	1-65,535
10 Mb/s	100	50-600	1-65,535
16 Mb/s	62	40-40	1-65,535
100 Mb/s	19	10-60	1-65,535
1 Gb/s	4	3-10	1-65,535
10 Gb/s	2	1-5	1-65,535

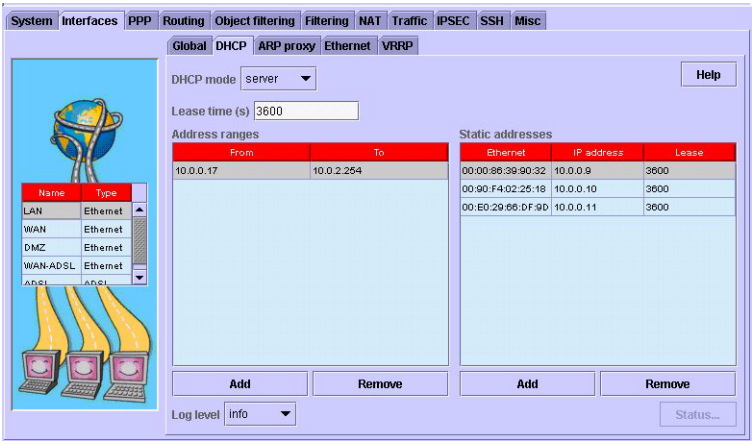
Interface Configuration

This window is where you will configure the general settings for each interface of your MultiCom Firewall. You have at least two Ethernet interfaces, your WAN link (to connect to your modem) and your LAN link (to connect to your local network or computer.) Some MultiCom Firewalls offer additional Ethernet interfaces like a multiple port LAN or a DMZ interface. Each interface configuration type will have different options to prepare the interface to communicate with the rest of your network. If you will be using a PPPoE or PPTP connection please refer to "Configuring PPP" on page 166.

Each Ethernet interface on your MultiCom Firewall can be configured as only one of the choices below.

- DHCP client
- DHCP server
- DHCP Relay
- static IP address
- PPPoE client
- PPTP client (also requires a static IP address of the selected interface)

You cannot mix these types of configurations on a single interface but with the last two choices (PPPoE and PPTP), the user can configure multiple connections such as multiple PPPoE connections on a single interface.

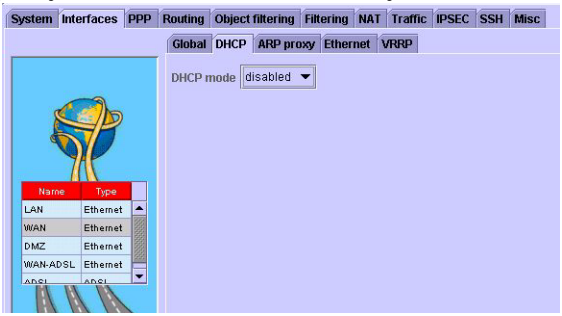


Your first screen in the Interface window is where you can manually set the IP address and netmask for the selected interface. While you will have one IP address for each Ethernet interface of your firewall you may not have to configure them all manually. For instance, if your Internet Service Provider is using a DHCP server you be automatically given an IP address for the WAN interface of the firewall.

CAUTION — the netmask for your WAN interface must be the same as the netmask for your Internet Service Provider (ISP) or you will not be able to communicate to the ISP. Check with your ISP support if you are unsure what to set it as.

Static IP Addressing

The other main option for configuring your firewall is to not use DHCP and instead manually set the IP parameters for the interface. You will need to identify the IP information of the LAN interface as well as adding a route in the routing table that says send everything through the firewall of the Internet Service Provider. The route is especially important because without the DHCP server adding it for you, your data would never travel beyond the MultiCom Firewall.



To set your computer to use static addressing (meaning each computer will manually be configured with all of the necessary information) you will need to set the LAN interface DHCP `Mode` to be `disabled`. You will also have to turn off the DHCP mode for the LAN interface. Finally, be sure that you have identified an IP address and subnet mask for the LAN interface.

Next, you will need to click on the `Routing` tab, click `Add`, and enter in the following line: `0.0.0.0/0` under the `Destination` and `x.x.x.x` where the x's are the IP address of your Internet Service Provider's firewall to the Internet. The “0.0.0.0/0” is the firewall's term for identifying all IP address destinations that are not specified somewhere else.

Additionally you will need to set each computer that will use the MultiCom Firewall as a firewall with the following parameters.

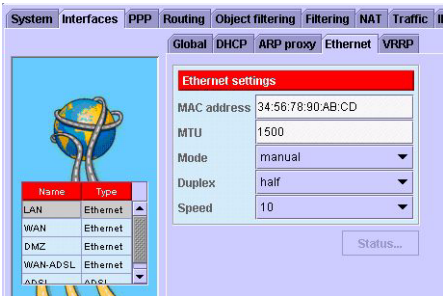
- give each computer its own unique IP address
- the same subnet mask as your local network
- the IP address for the MultiCom Firewall (if you use the Proxy DNS option of your MultiCom Firewall, otherwise you need the DNS IP addresses of your Internet Service Provider)
- the IP address of your MultiCom Firewall (the LAN interface IP address)

This information should already have been chosen by you earlier in this chapter. If not please do so now before continuing on to the next section.

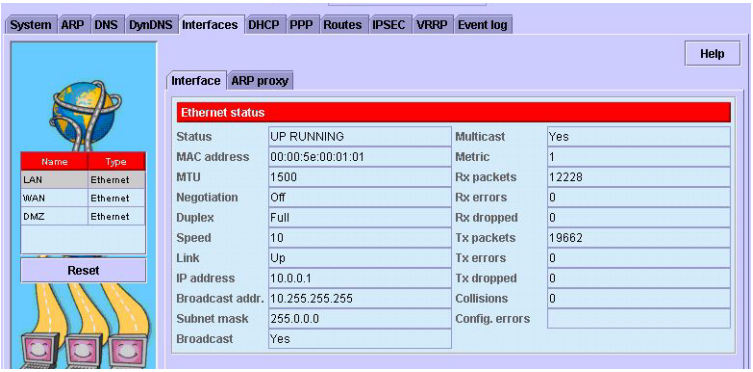
> NOTE — remember that manually setting your IP addresses means that every time you make a change to your Internet configuration you may need to make that change at each computer.

Ethernet Interface Parameters

With Lightning-Linux 3.4 or higher, it is possible to manually configure the Ethernet parameters such as MAC hardware address, MTU size of the packets, speed of the interface, and the duplex of the Ethernet interface. Unless you are told that you need to change these parameters it is best to leave the defaults.



Ethernet Interface Monitoring



Using the Monitoring window of the Configurator software you can access many useful statistics on the state of a particular Ethernet interface or PPP connection.

The Interface Monitor panel displays information about each physical interface of your MultiCom Firewall. This is the window where the user can see the MAC address of each hardware interface, the current IP configuration of the selected interface, the count of transmitted and received packets which successfully are processed by the interface, are dropped or cause errors.

NOTE - the switched LAN ports are reported as a single LAN interface for statistics and status

For more information on the statistics available from the Interface Monitor panel check the Monitor Panels Appendix.

Chapter 5

Configuration Choices

There are many ways to configure your MultiCom Firewall. The best one to use depends on the type of configuration that you wish to use. The following are the options for making a configuration.

- Using the built-in Web Server for Easy Setup, Easy Firewall, Easy IPSec and basic interface configuration
- Using the Configurator software for Easy Setup, Easy Firewall, Easy IPSec configurations
- Using the Configuration Software for Advanced Configuration
- Edit the text of the configuration file in a word processor and load it via the webserver, Configurator software, or FTP (Lightning-Linux 3.4 or higher)
- Using the CLI interface from a telnet, ssh telnet, or console connection

Installation of the Configurator software is described in the “Configurator Software Installation” Appendix on page 409.

Using The Built-In Web Server

Easy Configuration Wizards

By connecting to the web-server of the MultiCom Firewall it is possible to access the 3 Configuration Wizards:

- **Easy Setup** to make a simple Internet configuration and configure the LAN interface
- **Easy Firewall** to configure the NAT firewall, publish local servers onto the Internet and activate some Stateful Packet Inspection filtering
- **Easy IPSec** to build IPSec VPN tunnels, test the tunnels, and enable, disable and delete them.

make a simple Internet configuration using the Easy Setup menu. This menu walks the user through the steps needed to configure the WAN interface with a DHCP, PPP, PPTP or Static IP Address.

Additionally there is the option to configure the LAN interface IP address, whether to activate the built-in DHCP server to manage IP addresses on the Local Area Network (LAN) and the option to use the Easy-Firewall Wizard. Typically this menu is available at http://10.0.0.1/easysetup where 10.0.0.1 is the IP address of the LAN interface of your MultiCom Firewall.

> TIP - use https://<ip address of MultiCom> for secured remote configuration. See “HTTPS Secured Communication” on page 81.

After these configurations are saved and the MultiCom Firewall rebooted it will be using its new configuration.

Other Web Configurations

Using the web interface of the MultiCom Firewall it is also possible to configure the following features.

- Physical interface configurations (LAN, WAN, DMZ, ADSL, WIFI)
- URL Filtering rules
- Enable, disable or delete IPSec connections

- Users and user privileges
- Install and delete PKI keys, certificates and certificate revocation lists
- Configure the time and date
- Update the firmware
- Reboot the MultiCom Firewall
- Load Option keys
- Restore to factory defaults (deleting all option keys, security settings, user information and reloading the default configuration)

HTTPS Secured Communication

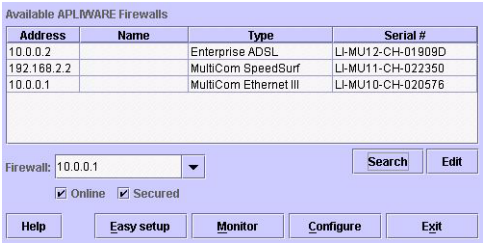
Starting with Lightning-Linux 3.3 it is possible to communicate with the MultiCom Firewall using encrypted communication. This is useful for remote secured configurations and is used by simply typing https://<IP address of MultiCom>. This communication is done using port 443.

Because the security certificate is not registered with your computer you will have to accept it manually when your web browser asks you. You will have the option to:

- make 1 time communication to an untrusted source (which will be remembered by your Internet browser until the browser is restarted)
- add this certificate to your list of trusted certificates (and future visits to the same IP address will immediately take place securely)

Once these formalities have taken place, all of the packets between the MultiCom Firewall and your web browser are encrypted. This does not encrypt packets that are going to the internal protected network or packets that are being redirected to other servers, only packets that are communicating directly with the MultiCom webserver. If you want to encrypt data going to the internal network please “IPSec Virtual Private Networks” Chapter on page 233.

To use the Configurator the “secured” button must be clicked when opening the access from the Main Screen. This is the default option whenever using the Configurator software.



After a secured connection is made the Configurator software will show a small closed lock in the upper right corner of the screen. If the lock is open then your communication between the Configurator and the MultiCom Firewall is not secured and someone on the intervening networks could use a network sniffer to capture the configuration details and user names and passwords.

CAUTION - HTTPS encrypted connections are only possible with Lightning-Linux 3.3 or higher. You will need to upgrade the MultiCom Firewall to this version or you will be limited to clear-text HTTP connections when configuring the remote Firewalls.

HTTPS Secured Connection

Non-Secured Connection

Using The Configurator Software

The Configurator Software can be run from the CDROM or installed to a computer. This software allows for advanced configuration of the MultiCom Firewall as well as monitoring the status of the Firewall. The Easy Setup can be started by clicking on the Easy Setup button of the Main Configurator screen. Additional Configuration Wizards can be accessed through the Wizards item of the menu bar. A list of configuration wizards is below.

- **Easy Setup** to make a simple Internet configuration and configure the LAN interface
- **Easy Firewall** to configure the NAT firewall, publish local servers onto the Internet and activate some Stateful Packet Inspection filtering
- **New IPSec Tunnel** to build IPSec VPN tunnels
- **DNS/ DHCP Entries** to set the DNS local addresses (IP address and hostname) and the DHCP server static environment (ethernet and IP addresses) and search the local network for active MAC hardware addresses
- **Remote Access** to allow remote access from the Internet to the MultiCom Firewall using HTTP, HTTPS, SSH
- **DHCP Client Requests** quickly configure an interface as a DHCP client
- **Standard Filters** quickly activate Stateful Packet Inspection rules for protection against Spoofing, Denial of Service, Bad TCP traffic.

To install the Configurator software please see the “Configurator Software Installation” Appendix on page 409.

Easy Setup

After starting the Configurator software from the CDROM or your hard drive you can select the MultiCom Firewall that you are going to configure and enter the Easy Setup panels. These panels give the same options as the Web-based Easy setup with 2 important additions:

1. When saving the configuration you can choose where to save the configuration (directly to the active or boot memory of the firewall, to a standby memory position on the firewall, and to a text file.
2. When finished with the Easy Setup portion of the configuration you can optionally take that configuration into the Advanced Configuration portion of

the Configurator software for adding additional options.

Advanced Configuration

The Advanced Configuration option of the Configurator software offers windows to configure all of the options of the MultiCom Firewall along with online help and error checking of the configuration file before it is saved to the MultiCom Firewall.

When saving the configuration you can choose where to save the configuration (directly to the active or boot memory of the firewall, to a standby memory position on the firewall, or to a text file.

Using The Configuration File

The built-in web server also allows direct access to the text of the configuration file using the MultiCom Config Tools menu. Under this menu one can directly edit in the web browser an existing configuration file being used or load a pre-existing configuration file from a hard drive or CD. Typically this menu is available at http://10.0.0.1/advanced/config/ where 10.0.0.1 is the IP address of the LAN interface of your MultiCom Firewall.

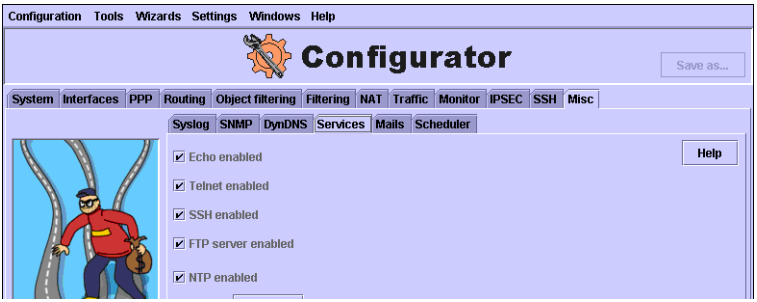
After these configurations are saved and the MultiCom Firewall rebooted it will be using its new configuration.

FTP Access

Starting with Lightning-Linux 3.4 and higher, it is possible to allows users to use the FTP protocol to retrieve or send configuration text files directly to the MultiCom Firewall. This feature can be activated in the Misc>Services panel of the Configurator software.

NOTE - If the SecureWall is activated or filtering rules are blocking access to the FTP ports then this access to the MultiCom Firewall will still be blocked.

To use the FTP protocol it is necessary to have FTP client software. There is a simple version available for free with the Windows operating system. Otherwise check the list of 3rd Party Software on your MultiCom Companion CDROM or in this manual to see other available software.



A sample FTP connection is shown below from a Windows 2000 Command Prompt. Using 3rd Party software may offer a more comfortable graphical interface.

```
D:\>ftp 10.0.0.1
Connected to 10.0.0.1.
220-=(<*>)=-.:. (( Welcome to PureFTPd 0.97.6 )) .:.-=(<*>)=-
220-You are user number 1 of 32255 allowed
220-Local time is now 14:16 and the load is 0.00. Server port: 21.
220 You will be disconnected after 15 minutes of inactivity.
User (10.0.0.1:(none)) : multicom
331 User multicom OK. Password required
Password :
230-User multicom has group access to: 100
230 OK. Current directory is / ftp> ls
200 PORT command successful
150 Connecting to port 3760
config
firmware
226 2 matches total
ftp : 18 octets reçus dans 0.00Secondes 18000.00Ko/sec.
ftp> cd config
250 OK. Current directory is /config
ftp> ls
200 PORT command successful
150 Connecting to port 3761
1
2
3
4
5
6
boot
226 7 matches total
```

```
ftp : 24 octets reçus dans 0.02Secondes 1.20Ko/sec.
ftp> get boot
200 PORT command successful
150-Connecting to port 3762
150 9.2 kbytes to download
226 File successfully transferred
ftp : 9451 octets reçus dans 0.00Secondes 9451000.00Ko/sec.
ftp> quit
221-Goodbye. You uploaded 0 and downloaded 10 kbytes.
221 Logout - CPU time spent: 0.180 seconds.
```

Command Line Interface

The Command Line Interface (CLI) provides an option for direct access to the configuration of Lightning-Linux via a common text-only interface. CLI access is available using a serial connection (if the device has a serial interface), telnet and SSH secured telnet.

Accessing CLI With Telnet

This functionality can be accessed by telnet, ssh telnet (Lightning-Linux 3.4 or higher) or a serial connection if your hardware offers this interface.

For serial connections follow the instructions in your User Manual to correctly configure the serial port of your workstation. You will also need a terminal emulator software such as HyperTerminal in Windows.

For telnet you will simply have to type “telnet x.x.x.x” where x.x.x.x is either the IP address of your firewall. Additionally you may need to enter in a valid user name and password if your firewall is configured to ask for it.

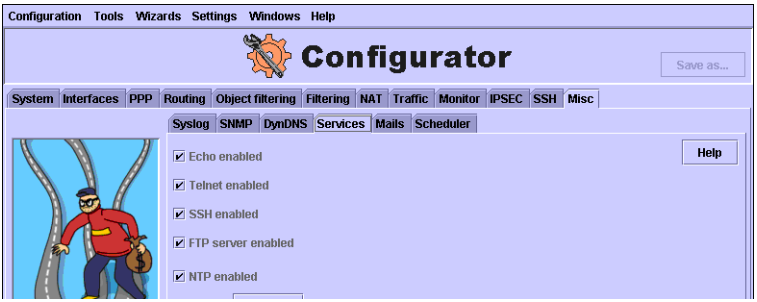
WARNING - All telnet data is transferred insecurely. Any usernames, passwords, or data you transmit or receive is be unencrypted. SSH can secure telnet connections and is recommended if you will be accessing the telnet service from the Internet.

Accessing CLI With SSH

SSH telnet can secure the telnet connection but requires an SSH client software (most linux and MacOSX systems include this software but Windows users should check the list of 3rd party software or the Internet for an SSH client). This allows the administrator to configure and troubleshoot a MultiCom Firewall remotely and securely.

Telnet and/ or SSH services can be enabled or disabled at the MISC>Services panel of the Configurator software. The user accounts for logging in to the Telnet or SSH services are the same accounts that have been created to configure the Multicom Firewall.

NOTE - This should not be confused with the SSH Virtual Private Networking option. The SSH VPN allows additional network traffic to be tunneled to the secured network using the SSH protocol and must be installed as an add-on option. By default the MultiCom Firewall supports only remote configuration by the SSH protocol.



Navigating the active configuration

Normally you will not be interacting with the configuration file itself. If you edit the configuration text file or use the CLI connection for working with the MultiCom Firewall you should know the basic structure of the configuration file.

Configuration as a Tree

The configuration is stored in a tree structure which contains all configuration parameters. These parameters describe the expected behavior of the firewall and can be modified by the user.

This tree structure is also used to hold the status parameters which give information about the current state of the firewall. These parameters can only be read by an authenticated user.

The configuration tree contains three types of nodes or branches:

• Structure: A node containing a fixed number of sub-nodes of any type. Each sub-node is identified by its name.

• Array: A node containing a variable number of sub-nodes, all of the same type (a structure). Each sub-node is identified by an array index. Array indexes can be strings, enumeration or integer.

• Leaf: A node without children (or sub-nodes) containing a configuration parameter value.

Paths

Since the commands of the CLI act on a given part of the configuration tree, they must specify a particular path in the tree. A path is a sequence of structure or array node names separated by spaces. To specify an entry in an array node, its name must be followed by an index entry. An index entry can be specified by appending the index to the array name between "[ ]" or by following the array name with the name of the index. Paths ending with an array name are paths to the array itself. Paths ending with an array name followed by an index are paths to a specific entry in the array.

Example 1: designating a path name

```
ip filtering input
```

is the path to the array of input filtering rules.

```
ip filtering input [0]
```

or

```
ip filtering input 0
```

is the path to the first filtering rule.

In order to avoid typing a complete path in each command, a working path can be specified. The path given in command is appended to the current working path to build the complete path on which the command must be applied. The current working path is displayed before the prompt ":".

Completion and history

Command and names in the path can be completed at any time with the <TAB> key. If only one completion is possible, the word is completed. If many completions are possible, a beep (char <BEL>) is sent. Typing <TAB> a second time displays all possible completions.

A history of 32 commands is available. Commands can be searched in the history with the <UP> and <DOWN> arrow keys and executed by typing the <ENTER> key.

CLI Command Summary

By typing "help" you will be given a list of possible commands that you can enter. These commands are context-sensitive and must be typed in without errors.

Below are the commands available in a telnet session with the MultiCom Firewall.

Table 1: CLI Added in LL 3.7+

Command	Description
mail	mail logs or a test message to selected email account
ipsec {test}	test the selected IPSec VPN connection

Table 2: CLI Added in LL 3.6+

Command	Description
backtrace	shows debug of last reboot
date	set date
eventdebug	activate and deactivate debug syslog messages
ipsec	initiate and terminate the selected IPSec connection
selectmode	choose to work with the device or security config file
time	set time
unset	unmodify a part of the configuration tree
vrrp	start and stop VRRP services

Table 3: CLI Commands LL 3.1+

Command	Description
add	to add an entry in an array
adduser	adds a new user to the firewall (3.5+)
del	to remove an entry from an array
deluser	delete a user from the firewall (3.5+)
dhcpclient	to restart the dhcp client
exit	exit telnet session
go	to change the current working path
help	help
info	to get the list of sub-nodes available from a node
listusers	list users on the firewall (3.5+)
loadconfig	to load a configuration from flash memory
nslookup	nslookup hostname
passwd	change a users password on the firewall (3.5+)
ping	use ICMP echo-request to check reachability of a host
ppp	to connect or disconnect a ppp site (3.5+)
print	to display a part of the configuration tree
reboot	reboot the firewall
saveconfig	to permanently save a configuration to the flash memory
set	to modify a part of the configuration tree
showconfig	show the content of an array or a structure in the command format

Command	Description
traceroute	use UDP packet with incremental TTL to determine the route to a host
unset	to unmodify a part of the configuration tree (3.5+)

Table 4: CLI Commands LL 3.0, 3.0.1 - Obselete List

Command	Description
add	add [path] index
applyconfig	applyconfig
cd	cd [path]
config	config
connect	connect
cp	[path] curr_index new_index
del	del [path] index
dhcpclient	dhcpclient {LAN|WAN|eth0|eth1} {renew|renewall}
exit	exit telnet session
help	help
info	info [path]
loadconfig	loadconfig [1][2][3][4][5][6][boot]
ls	ls [path]
mv	mv [path] old_index new_index
nslookup	nslookup hostname
ping	ping hostname
reboot	reboot
saveconfig	[1][2][3][4][5][6][boot]
set	set [path] value [path2 value2 ...]
status	status
traceroute	traceroute hostname

Configuration Commands - CLI

Add

LL Version

3.1+

Description

Add an entry in an array.

Syntax

```
add [path] index
```

Parameters

•path: Path to the array to which the entry must be added. The index must be specified.

•index: Index for the new entry.

Example 2: add command

```
/: add ip routing static 0
entry [0] added in ip routing static
/:
Adding entries using go:
/: go ip routing static
path set "to ip routing static"
/ip/routing/static: add 1
entry [1] added in ip routing static
/ip/routing/static: add 2
entry [2] added in ip routing static
/ip/routing/static: go root
path set to root
/:
```

Adduser

LL Version

3.5+

Description

Adds a new user to the firewall .

Syntax

```
adduser {guest|config|privileged} username password [nocli]
```

Parameters

•guest: sets "guest" rights level for the new user
•config: sets "config" rights level for the new user.
•privileged: sets "privileged" rights level for the new user.
•username: name of the new user.
•password: password of the new user.
•nocli: optionally disable CLI access for the new user.

Backtrace

LL Version

3.6+

Description

Shows debug output, date and time of the last system reboot.

Syntax

```
backtrace
```

Parameters

•none

Example 3: backtrace command

```
Config /: backtrace
Last backtrace saved :
14/10/2004 22:03:53
child died: caught signal SIGSEGV
code: 00000001, errno: 00000000, addr: 7070703C
NIP: 10184F68, LINK: 80000002, SP: 7FFFF4A0
Call backtrace: 102334D8 0FEEC7F4 100EC498 100295DC 100263B0
100261EC 100263E8 100262CC 10026420 100261EC 100263E8 100261EC
100263E8 100261EC 100263E8 10026110 10028F34 1005C030 10058970
10004328 10004124 100DF048 100040F8 100053A4 10002C08
 100044EC 100DB0F8 100DB4CC 100DB648 10004434 100032D0 0FE9A234
```

Date

LL Version

3.6+

Description

Set or view the system date of the MultiCom Firewall.

Syntax

date [dd/mm/yyyy]

Parameters

•dd: day as a number from 1-31
•mm: month as a number from 1-12
•yyyy: year

Del

LL Version

3.1+

Description

Delete an entry in an array.

Syntax

```
del [path] index
```

Parameters

•path: Path to an entry in an array. The index must be specified.
•index: Index of the entry to delete

Deluser

LL Version

3.5+

Description

Restart the DHCP client.

Syntax

```
deluser user
```

Parameters

•user: the username to be deleted.

DhcpClient

LL Version

3.1+

Description

Restart the DHCP client for the selected interface.

Syntax

```
dhcpclient {WAN|LAN|DMZ} {renew|renewall}
```

Parameters

•WAN|LAN|DMZ: the interface on which the DHCP client has to be restarted.

•renew: current leases are taken into account when restarting the client.

•renewall: all current leases are purged before restarting the client.

Eventdebug

LL Version

3.6+

Description

Activate and deactivate syslog debug messages.

Syntax

eventdebug {start|stop}

Parameters

•start: start sending debug syslog messages
•stop: stop sending debug syslog messages

Exit

LL Version

3.1+

Description

Closes the connection with the CLI if using telnet or SSH telnet.

Syntax

```
exit
```

Go

LL Version

3.1+

Description

Change the current working path

Syntax

```
go .. |/| path
```

Parameters

•path: List of node names specifying a path relative to the current path.

•..: Go to the path that was selected before the previous call to go.

•/: Go to the root of the configuration tree.

Example 4: go command

```
/: go ip routing
path set to "ip routing"
/ip/routing: go static
path set to "ip routing static"
/ip/routing/static: go ..
path set to "ip routing"
/ip/routing: go /
path set to root
/:
```

Help

LL Version

3.0

Description

Lists available commands in the CLI

Syntax

```
help
```

Info

LL Version

3.1+

Description

Display the list of sub-nodes available under the given node. Arrays are followed by “[ ]”, structure are followed by “{ }”.

Syntax

```
info [path]
```

Parameters

•path: Path to a node.

Example 5: info command

```
/: info ip routing
static[] status{}
/:
```

Ipsec

LL Version

3.6+

Description

Initiate, terminate and test the selected IPSec connection.

Syntax

ipsec {initiate|terminate|test} <connection>

Parameters

•initiate: attempt to initiate the selected IPSec connection

•terminate: terminate the selected IPSec connection

•test: choose the IPSec connection to be tested, the test must then be started and then asked to show the results.

•connection: name of the preconfigured IPSec connection

Example 6: ipsec command

```
Config /: ipsec
Usage: ipsec {initiate|terminate} <connection>
       ipsec test connection <connection>
       ipsec test {start|stop|show}

Available connections : Roadwarriors
, testPKI
, testPSK
Config /: ipsec test connection
Usage: ipsec {initiate|terminate} <connection>
       ipsec test connection <connection>
       ipsec test {start|stop|show}

Available connections : Roadwarriors
, testPKI
, testPSK
Config /: ipsec test connection testPKI
Config /: ipsec test start
Config /: ipsec test show
```

```
Test Connection : testPKI
Test Date : 02/01/2004 18:57:04

Connection to Remote Gateway :
Connected

IKE Phase 1 :
Starting IKE Phase I in Main Mode
NAT Traversal : no NAT detected
Invalid Certificate on Remote Gateway

Info phase 1:
Option on Remote Gateway : draft-ietf-ipsec-nat-t-ike-03
Option on Remote Gateway : Dead Peer Detection
Remote ID : CN=Tryphon Tournesol, O=Apliware SA, OU=R&D,
L=Geneva, C=CH, E=tourn
esol@apliware.ch

Error in IKE Phase I ...
[error because MultiCom had been off for more than 2 days and
the system time was not reset, hence certificates and
Certificate Revocation list was invalid]



Config /: ipsec test connection testPKI
Config /: ipsec test start
Config /: ipsec test show

Test Connection : testPKI
Test Date : 22/10/2004 12:24:06

Connection to Remote Gateway :
Connected

IKE Phase 1 :
Starting IKE Phase I in Main Mode
NAT Traversal : no NAT detected
IKE ISAKMP Established

Info phase 1:
```

```
Option on Remote Gateway : draft-ietf-ipsec-nat-t-ike-03
Option on Remote Gateway : Dead Peer Detection
Remote ID : CN=Tryphon Tournesol, O=Apliware SA, OU=R&D,
L=Geneva, C=CH, E=tourn
esol@apliware.ch

IKE Phase 2 :
Starting IKE Phase II in Quick Mode
IKE IPSec SA Established

Info phase 2:
Dead Peer Detection (DPD) Enabled on this connection

IPSec connection succeeded ...
[After update of system clock]
```

Listusers

LL Version

3.5+

Description

Lists configured users on the firewall and shows their privilieges.

Syntax

```
listusers
```

LoadConfig

LL Version

3.1+

Description

Load a configuration from the flash memory and apply it as the current configuration. The format of the ile to load is the standard 3.x format which represents the MIB structure.

Syntax

```
loadconfig 1|2|3|4|5|6|boot|empty|current
```

Parameters

•1 .. 6: Load the current configuration from the specified slot in flash memory.

•boot: Restore the boot configuration as current configuration.

•empty: Load an empty configuration.

•current: Load the configuration which is currently running.

Mail

LL Version

3.7+

Description

Mail logs or a test message to all email accounts or a selected email account.

Syntax

mail {logs|test} [client]

Parameters

•logs: Send event logs to all or selected email accounts.
•test: send email test message to all or selected email accounts
•client: select a valid email account to receive logs or tests

Example 7: mail command

```
Config /: mail logs
Config /: mail logs clients
Unknown client : clients
Current mail clients are :
Support, Admin
Config /: mail logs Admin


****email test message****
From: myname@bluemail.ch
Sent: Friday, 22. October 2004 14:28
To: support@apliware.ch
Subject: Test Mail


Test Mail

Date              : 22.10.2004 / 14:27:34
E-Mail Client     : Support

Hostname          : Firewall
```

```
Hardware Type    : MultiCom SpeedSurf
Serial Number    : LI-MU11-CH-022518
Firmware version : 3.7

****email log report****
From: myname@bluemail.ch
Sent: Friday, 22. October 2004 14:26
To: support@apliware.ch
Subject: Log


Date             : 22.10.2004 / 14:25:47
E-Mail Client    : Support

Hostname         : Firewall

Hardware Type    : MultiCom SpeedSurf
Serial Number    : LI-MU11-CH-022518
Firmware version : 3.7

Last Events History
===================
22/10/2004 13:57:58 , Service : ACCESS    , Info  : New CLI login
(Telnet) for user : Privileged.
22/10/2004 12:24:54 , Service : DYNDNS    , Info  : Successful
update of IP address.
22/10/2004 12:23:58 , Service : SYSTEM    , Info  : Time and Date
corrected.
02/01/2004 19:44:16 , Service : CONFIG    , Info  : New config
applied.
02/01/2004 19:44:16 , Service : CONFIG    , Info  : New config
received.
02/01/2004 19:41:10 , Service : CONFIG    , Info  : New config
applied.
02/01/2004 19:41:10 , Service : CONFIG    , Info  : New config
received.
02/01/2004 19:40:55 , Service : IPSEC     , Info  : Opening IPSec
tunnel to gateway 195.186.157.118 on connection testPKI
02/01/2004 19:40:55 , Service : IPSEC     , Info  : Opening IPSec
tunnel to gateway 195.70.14.20 on connection testPSK
02/01/2004 19:40:54 , Service : IPSEC     , Info  : Closing IPSec
tunnel to gateway 195.70.14.20 on connection testPSK
```

```
02/01/2004 19:40:54 , Service : IPSEC    , Info  : Closing IPSec
tunnel to gateway 195.186.157.118 on connection testPKI

02/01/2004 19:40:54 , Service : CONFIG    , Info  : New config
applied.

02/01/2004 19:40:51 , Service : CONFIG    , Info  : New config
received.

02/01/2004 18:54:16 , Service : ACCESS    , Info  : New CLI login
(Telnet) for user : Privileged.

02/01/2004 18:53:20 , Service : DYNDNS    , Info  : Successful
update of IP address.

02/01/2004 18:53:20 , Service : IPSEC    , Info  : Opening IPSec
tunnel to gateway 195.70.14.20 on connection testPSK

02/01/2004 18:53:20 , Service : IPSEC    , Info  : Opening IPSec
tunnel to gateway 195.186.157.118 on connection testPKI

02/01/2004 18:53:13 , Service : PPP      , Info  : Connected to
PPP Server on site PPPoE

02/01/2004 18:53:13 , Service : DNS       , Info  : New DNS
Servers received : 195.186.1.108 , 195.186.4.109

02/01/2004 18:53:05 , Service : IPSEC     , Info  : IPSec
Connection Roadwarriors not configured.

02/01/2004 18:53:05 , Service : IPSEC     , Info  : Could not
find a route to remote gateway ().

02/01/2004 18:53:03 , Service : IPSEC     , Info  : IPSec
Connection Roadwarriors not configured.

02/01/2004 18:53:03 , Service : IPSEC     , Info  : Could not
find a route to remote gateway ().

02/01/2004 18:53:03 , Service : IPSEC     , Info  : IPSec
Connection Roadwarriors not configured.

02/01/2004 18:53:03 , Service : IPSEC     , Info  : Could not
find a route to remote gateway ().

02/01/2004 18:53:02 , Service : IPSEC     , Info  : IPSec
Connection Roadwarriors not configured.

02/01/2004 18:53:02 , Service : IPSEC     , Info  : Could not
find a route to remote gateway ().

02/01/2004 18:53:02 , Service : IPSEC     , Info  : IPSec
Connection Roadwarriors not configured.

02/01/2004 18:53:02 , Service : IPSEC     , Info  : Could not
find a route to remote gateway ().

02/01/2004 18:53:02 , Service : IPSEC     , Info  : IPSec
Connection Roadwarriors not configured.

02/01/2004 18:53:02 , Service : IPSEC     , Info  : Could not
find a route to remote gateway ().

02/01/2004 18:53:02 , Service : IPSEC     , Info  : IPSec
Connection Roadwarriors not configured.

02/01/2004 18:53:02 , Service : IPSEC     , Info  : Could not
find a route to remote gateway ().

02/01/2004 18:53:01 , Service : CONFIG    , Info  : New config
applied.
```

```
02/01/2004 18:53:01 , Service : SSH      , Info  : Starting SSH
access.
02/01/2004 18:53:01 , Service : DYNDNS    , Info  : Starting
DynDNS.
02/01/2004 18:52:59 , Service : FILTER    , Info  : SecureWall
enabled
02/01/2004 18:52:59 , Service : IPSEC     , Info  : IPSec
Connection Roadwarriors not configured.
02/01/2004 18:52:59 , Service : IPSEC     , Info  : Could not
find a route to remote gateway ().
02/01/2004 18:52:56 , Service : IPSEC     , Info  : Starting
IPSec service.
02/01/2004 18:52:56 , Service : VRRP      , Info  : Starting
VRRPd process on interface LAN
02/01/2004 18:52:54 , Service : PPP       , Info  : MSS hack
installed.
02/01/2004 18:52:53 , Service : OPTIONS   , Info  : NMS Option
enabled.
02/01/2004 18:52:53 , Service : OPTIONS   , Info  : PayNET
Option enabled.
02/01/2004 18:52:53 , Service : OPTIONS   , Info  : VRRP
enabled.
02/01/2004 18:52:53 , Service : OPTIONS   , Info  : SSH VPN
enabled.
02/01/2004 18:52:53 , Service : OPTIONS   , Info  : IPSec
enabled ( 20 tunnels )
02/01/2004 18:52:53 , Service : CONFIG    , Info  : Configure
Ethernet interface WAN
02/01/2004 18:52:53 , Service : CONFIG    , Info  : Configure
Ethernet interface LAN
02/01/2004 18:52:53 , Service : CONFIG    , Info  : Starting
System ...
```

Nslookup

LL Version

3.1+

Description

Name server lookup of specified hostname.

Syntax

```
nslookup host
```

Parameters

•host: the hostname to be queried at the DNS server.

Passwd

LL Version

3.5+

Description

Changes a users password on the firewall.

Syntax

```
passwd [user] newpass
```

Parameters

•user: the username which will have it’s password changed.
•newpass: the new password for the selected user.

Ping

LL Version

3.1+

Description

Use ICMP echo-request to check reachability of a host.

Syntax

```
ping [-LRdnqrv] [-c count] [-i wait] [-p pattern] [-s
packetsize] [-t ttl] [-I interface address] host
```

Parameters

•-c count: Stop after sending (and receiving) count ECHO_RESPONSE packets.

•-d: Set the SO_DEBUG option on the socket being used.

•-i wait: Wait "wait#" seconds between sending each packet. The default is to wait for one second between each packet.

•-n: Numeric output only. No attempt will be made to lookup symbolic names for host addresses.

•-p pattern: You may specify up to 16 ``pad" bytes to fill out the packet you send. This is useful for diagnosing data-dependent problems in a network. For example, ``-p ff" will cause the sent packet to be filled with all ones.

•-q: Quiet output. Nothing is displayed except the summary lines at startup time and when finished.

•-R: Record route. Includes the RECORD_ROUTE option in the ECHO_REQUEST packet and displays the route buffer on returned packets. Note that the IP header is only large enough for nine such routes. Many hosts ignore or discard this option.

•-r: Bypass the normal routing tables and send directly to a host on an attached network. If the host is not on a directly-attached network, an error is returned.

•-s packetsize: Specifies the number of data bytes to be sent. The default is 56, which translates into 64 ICMP data bytes when combined with the 8 bytes of ICMP header data.

•-v: Verbose output. ICMP packets other than ECHO_RESPONSE that are

received are listed..

•-t ttl: The TTL value of an IP packet represents the maximum number of IP routers, that the packet can go through before being thrown away. The maximum possible value of this field is 255 with TCP traffic using 60.

•-L: Suppress loopback of multicast packets. This flag only applies if the ping destination is a multicast address.

•-I interface: specify the IP address of the interface to send the ping from.

•host: hostname or IP address of the computer to receive the ping request.

PPP

LL Version

3.5+

Description

Connect or disconnect a ppp site.

Syntax

```
ppp {PPPoE} {connect|disconnect}
```

Parameters

•PPPoE: the PPP connection name to be started or stopped.
•connect: attempt to connect the selected PPP connection.
•disconnect: disconnect the selected PPP connection.

Print

LL Version

3.1+

Description

Print the content of an array or a structure. If the specified node is a structure, print the content of each leaf in the structure. If the specified node is an array, print leaf sub-nodes of each entry in the array, one by line.

Syntax

print path

Parameters

•path: Path to the structure or array to display.

Example 8: print command

```
/: print ip dns static
domain: lightning.ch
primary: 193.5.2.143
secondary: 193.5.2.147
```

Reboot

LL Version

3.1+

Description

Reboot the firewall.

Syntax

```
reboot
```

SaveConfig

LL Version

3.1+

Description

Save the current configuration in the flash memory. The boot configuration is used when the firewall reboots and becomes the current configuration. The format of the configuration file is the standard 3.x format, namely it represents the MIB structure not the format as commands.

Syntax

```
saveconfig current | 1 | 2 | 3 | 4 | 5 | 6 | boot
```

Parameters

•1 .. 6: Save the current configuration in the specified slot in flash memory.

•boot: Save the current configuration in the specified slot in flash memory.

•current: Save the current configuration as the configuration to be used now.

Selectmode

LL Version

3.6+

Description

Choose to load the device or the security configuration.

Syntax

selectmode {CONFIG | SECURITY}

Parameters

•CONFIG: Choose to work with the device configuration information.

•SECURITY: Choose to work with the security configuration information.

Set

LL Version

3.1+

Description

Modify a set of parameter. All parameters are in the same structure.

Syntax

```
set [path] {leaf_name "=" value}
```

Parameters

•path: Path to the structure to modify. Can be omitted if the current context is a structure.

•leaf_name: Parameter to modify in the structure.

•value: Value to be set to the parameter.

Example 9: set command

Setting DNS mode.

```
/: set ip dns mode=static
ok
```

Configuring static DNS.

```
/: set ip dns static domain=lightning.ch primary=193.5.2.143
ok
```

ShowConfig

LL Version

3.1+

Description

Show the content of an array or a structure in the command format. The result can be used directly to type commands.

Syntax

```
showconfig [path]
```

Parameters

•path: Path to the array or to the structure to show. Can be omitted if the current context is an array or a structure.

Example 10: showconfig command

```
/: showconfig ip dns
set ip dns static domain=lightning.ch primary=192.168.16.143
secondary=192.168.16.144
/: showconfig ip routing
add ip routing static 0
set ip routing static 0 destination=192.168.18.0/24
firewall=0.0.0.0
metric=0
/: go ip filtering
path set to "ip filtering"
/ip/filtering: showconfig
set enabled=true
add forward 0
set forward 0 source=192.168.17.0/24 action=accept
add forward 1
set forward 1 destination=192.168.18.5/32 action=drop
```

Time

LL Version

3.6+

Description

Set or show system time on the MultiCom Firewall.

Syntax

time [hh:mm:ss]

Parameters

•hh: hour of the day in 24 hour format
•mm: minutes
•ss: seconds

Traceroute

LL Version

3.1+

Description

Use UDP packets with incremental TTL to determine the route to a host.

Syntax

```
traceroute [-dFInrvx] [-g gateway] [-i iface] [-f first_ttl] [-m
max_ttl] [ -p port] [-q nqueries] [-s src_addr] [-t tos] [-w
waittime] [-z pausemsecs] host [packetlen]
```

Parameters

•host: hostname or IP address of the computer that is the end point.

•-d: enable socket level debugging.

•-F: set the "don't fragment" bit.

•-I: use ICMP ECHO instead of UDP datagrams.

•-n: print hop addresses numerically rather than symbolically and numerically (saves a nameserver address-to-name lookup for each gateway found on the path).

•-r: bypass the normal routing tables and send directly to a host on an attached network. If the host is not on a directly-attached network, an error is returned. This option can be used to ping a local host through an interface that has no route through it.

•-v: verbose output. Received ICMP packets other than TIME_EXCEEDED and UNREACHABLEs are listed.

•-x: toggle ip checksums. Normally, this prevents traceroute from calculating ip checksums. In some cases, the operating system can overwrite parts of the outgoing packet but not recalculate the checksum (so in some cases the default is to not calculate checksums and using -x causes them to be calcualted). Note that checksums are usually required for the last hop when using ICMP ECHO probes (-I). So they are always calculated when using ICM.

•-g gateway: specify a loose source route gateway (8 maximum).

•-i iface: specify a network interface to obtain the source IP address for

outgoing probe packets. This is normally only useful on a multi-homed host. (See the -s flag for another way to do this.)

•-f first_ttl: set the initial time-to-live used in the first outgoing probe packet.

•-m max_ttl: set the max time-to-live (max number of hops) used in outgoing probe packets. The default is 30 hops (the same default used for TCP connections).

•-p port: set the base UDP port number used in probes (default is 33434). Traceroute hopes that nothing is listening on UDP ports base to base + nhops - 1 at the destination host (so an ICMP PORT_UNREACHABLE message will be returned to terminate the route tracing). If something is listening on a port in the default range, this option can be used to pick an unused port range.

•-q nqueries: number of probes sent at each ttl setting.

•-s source_addr: use the following IP address (which usually is given as an IP number, not a hostname) as the source address in outgoing probe packets. On multi-homed hosts (those with more than one IP address), this option can be used to force the source address to be something other than the IP address of the interface the probe packet is sent on. If the IP address is not one of this machine's interface addresses, an error is returned and nothing is sent. (See the -i flag for another way to do this.)

•-t tos: Set the type-of-service in probe packets to the following value (default zero). The value must be a decimal integer in the range 0 to 255. This option can be used to see if different types-of-service result in different paths. Not all values of TOS are legal or meaningful - see the IP spec for definitions. Useful values are probably `-t 16' (low delay) and `-t 8' (high throughput).

•-w waititme: Set the time (in seconds) to wait for a response to a probe (default 5 sec.).

•-s pausemsecs: pause between probes in milliseconds.

•packetlen: the default probe datagram length is 40 bytes, but this may be increased by specifying a packet length (in bytes) after the destination host name.

Unset

LL Version

3.5+

Description

Unmodify a part of the configuration tree.

Syntax

```
unset [path] leaf_name
```

Parameters

•path: Path to the structure to modify. Can be omitted if the current context is a structure.

•leaf_name: Parameter to modify in the structure.

Vrrp

LL Version

3.6+

Description

Start and stop VRRP services for the selected interface

Syntax

vrrp {<interface> | all} {start | stop}

Parameters

•interface: specify a valid interface to start or stop.

•all: start or stop VRRP services on all interfaces

•start: start VRRP services on the selected interface.

•stop: stop VRRP services on the selected interface.

Examples

Configuration as commands

An active configuration can be viewed as a sequence of commands with the `showconfig` command. An example of configuration as a sequence of commands is done below:

```
:/ showconfig
set ip dns mode=dynamic
set interface ethernet LAN ip address=10.0.0.1 netmask=255.0.0.0
set interface ethernet LAN dhcp mode=server
add interface ethernet LAN dhcp server range 0
set interface ethernet LAN dhcp server range 0 from=10.0.0.10
to=10.0.0.254
set interface ethernet WAN dhcp mode=client
add interface ethernet WAN dhcp client request 0
set interface ethernet WAN dhcp client request 0
name=subnet-mask
mode=require
add interface ethernet WAN dhcp client request 1
set interface ethernet WAN dhcp client request 1
name=domain-name
mode=require
add interface ethernet WAN dhcp client request 2
set interface etherent WAN dhcp client request 2
name=domain-name-server
mode=require
set interface ethernet WAN ip nat enabled=true securewall=true
add interface ethernet WAN ip nat input 0
set interface ethernet WAN ip nat input 0 protocol=tcp dport=80
mapping=internal to-port=80
```

Advanced Examples

Some advanced examples of commands are given in order to understand the configuration of the filtering and translation features.

The following commands allow to configure a filtering rule which accepts TCP packets going out eth0 if the source address stands in the specified source subnet.

```
/:set ip filtering enabled=true
/:add ip filtering forward 0
/:set ip filtering forward 0 protocol=tcp to_interface=eth0
source=192.168.17.0/24 action=accept
```

The commands below add a filtering rule which drop all incoming ICMP traffic with a destination set as the local processes of the firewall.

```
/:add ip filtering input 0
/:set ip filtering input 0 protocol=icmp
```

These commands go to the input filtering table and add a rule to deny incoming UDP traffic with a destination address which match the local subnet and where the destination port number is included in the range 0 to 1024.

```
/:go ip filtering forward
/ip/filtering/forward:add 0
/ip/filtering/forward:set 0 protocol=udp from_interface=eth1
destination=192.168.17.0/24 dport=0-1024 action=reject
reject_with=destination-unreachable
```

The command below enables the translation and adds a rule that redirects the incoming telnet packets to the firewall itself on port 23.

```
/:set interface ethernet[WAN] ip nat enabled=true
/:add interface ethernet[WAN] ip nat input 0
/:set interface ethernet[WAN] ip nat input 0 protocol=tcp
dport=23
mapping=internal to_port=23
```

The first command below changes the working directory to the MIB structure corresponding to the IP configuration of the interface WAN. The second command adds a translation rule which redirects the incoming TCP packets with a destination address equeal to the interface eth1 address and a destination port equal to 80. The incoming packets are redirected to the internal web server responding to the address 192.168.17.254 on port 8080.

```
/:go interface ethernet[WAN] ip
/interface/ethernet[WAN]/ip:add nat input 0
/interface/ethernet[WAN]/ip:set nat input 0 protocol=tcp
dport=80
to_address=192.168.17.254 dport=8080
```

The following command shows a filtering rule with some advanced parameters.

```
/:add ip filtering forward 0
/:set ip filtering forward 0 protocol=tcp from_interface=eth1
source=!10.0.0.0/8 sport=!0-1024 destination=192.168.17.0/24
dport=21 tcp_flags_mask=syn,ack,fin tcp_flags_value=syn
limit=1/s
limit_burst=3 action=accept
```

These rules are examples for adding translation rules in the global NAT table.

```
/:ip nat enabled=true
/:add ip nat table 0
/:set ip nat table 0 protocol=udp source=192.168.17.193/26
to_address=192.168.16.1
/:add ip nat table 1
/:set ip nat table 1 protocol=udp destination=192.168.16.1/32
dport=21 to_address=192.168.17.194 to_port=2121
type=destination
```

Other Useful CLI Examples

Below are a list of common activities a user might make on telnet or console connection to the MultiCom Firewall. For more information on the commands themselves please refer to the Reference Manual. Italicised text is sample output when available.

MULTICOM SERIAL NUMBER

```
info system hardware serial_number
serial_number = LI-MU7-CH-0200D2
```

SOFTWARE VERSION

```
info system software firmware
firmware = 3.4
```

LAN STATUS

```
info interface ethernet LAN status status
status = UP RUNNING
```

LAN IP ADDRESS

```
info interface ethernet LAN status ip_address
ip_address = 10.0.0.1
info interface ethernet LAN ip netmask
netmask = 255.0.0.0
```

LAN DHCP MODE

```
info interface ethernet LAN ip dhcp mode
mode = server
```

WAN STATUS

```
info interface ethernet WAN status status
status = UP RUNNING
```

WAN DHCP CLIENT STATUS

```
info interface ethernet WAN ip dhcp client status state
state = Assigned, Disabled, Fail, Try to get Address, Expire,
Rebind, Renew (all possible responses)
```

PPPoE STATUS

```
info interface ppp PPPoE status status
status = UP RUNNING
```

PPPoE IP ADDRESS

```
info interface ppp PPPoE status ip_address
ip_address = 212.147.17.76
```

PPPoE IPCP INFO

```
info interface ppp PPPoE ipcp status state
state = UP
```

```
state = DOWN
```

PPPoE LINK STATUS

```
info interface ppp PPPoE lcp status info
info = "" (which means everything is OK)
info = CHAP authentication failed
info = Timeout sending Config-Requests
info = Endpoint not connected
```

PPPoE DNS ASSIGNED SERVERS

```
info interface ppp PPPoE ipcp status primary
primary = 212.147.10.10
info interface ppp PPPoE ipcp status secondary
secondary = 212.147.0.1
```

AVAILABLE PPPoE SERVERS

```
info interface ppp PPPoE pppoe server_list
indexes: 0 1 2
info interface ppp PPPoE pppoe server_list 0
access_concentrator_name
access_concentrator_name = ipc-lsp690-r-lc-01
info interface ppp PPPoE pppoe server_list 0 service_name
service_name = Any
```

ARP ENTRIES

```
info arp status arp_entry
indexes: 0 1 2
info arp status arp_entry 0 hw_address
hw_address = 00:C0:F0:57:4A:6D
info arp status arp_entry 1 hw_address
hw_address = 00:C0:F0:4C:A7:90
```

DNS SERVERS USED

```
info ip dns status nameserver 0 ip
ip = 192.168.1.115
info ip dns status nameserver 1 ip
ip = 192.168.1.116
```

ENABLE IPSEC

```
set security ipsec enabled=true
saveconfig current
```

DISABLE IPSEC

```
set security ipsec enabled=false
saveconfig current
```

TURN ON SECUREWALL

```
set interface ethernet WAN ip nat securewall=true
saveconfig current
```

TURN OFF SECUREWALL

```
set interface ethernet WAN ip nat securewall=false
saveconfig current
```

ENABLE FILTERING

```
set ip filtering enabled=true
saveconfig current
```

ENABLE FILTERING OBJECTS

```
set ip filtering_objects enabled=true
saveconfig current
```

ENABLE DNS PROXY

```
set ip dns proxy enabled=true
saveconfig current
```

DISABLE DNS PROXY

```
set ip dns proxy enabled=false
saveconfig current
```

ENABLE RIP

```
set routing ip rip enabled=true
saveconfig current
```

DISABLE RIP

```
set routing ip rip enabled=false
saveconfig current
```

ENABLE FTP

```
set ip ftp server enabled=true
saveconfig current
```

DISABLE FTP

```
set ip ftp server enabled=false
saveconfig current
```

ADD SYSLOG SERVER at 10.0.0.2 (assumes there is no other Syslog Server in position 0)

```
add ip syslog server 0
set ip syslog server 0 address=10.0.0.2 level=debug
saveconfig current
```

DHCP

Chapter 6

Dynamic Host Configuration Protocol (DHCP)

DHCP servers store and distribute network information to DHCP clients on your local network. Network information such as firewalls, DNS servers and even the IP address and netmask settings for an entire network can be managed from a central DHCP server.

When a computer on a local network announces that it is a DHCP client and wants to be connected to your local network, it is the server that replies. The DHCP server will pick an IP address from a preset pool of addresses and assign this to the requesting client along with any other network information that has been asked for. Because the information is solely TCP/IP protocol related a single DHCP server can manage Microsoft Windows, Macintosh, Linux, Unix and any other device that has software allowing it to be a DHCP client.

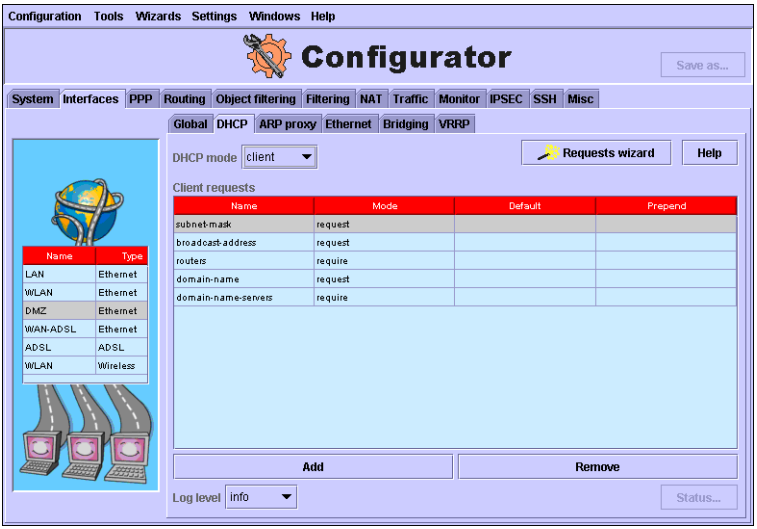
Along with the information that is required for network connectivity, the DHCP server sets a time limit for how long this information is good for. When the time limit has expired the DHCP client will request new information.

The options table contains the options sent by the DHCP server (normally is the ISP DHCP server). Those options tell servers to configure some TCP/IP parameters and services.

Not all of those options are interpreted (or applied). For example if the DNS on the firewall is configured in static mode, the DNS options received by the client are ignored.

DHCP Services Configuration

The Interface Window is also where you can configure DHCP services on your firewall. Click on the `DHCP` mode box under the `Interface>Global` window. Here you can set whether each interface is to be a DHCP client, DHCP server, DHCP relay or to have a static address. For instance if your Internet Service Provider is using a DHCP server you will probably want to use it to get an IP address and netmask for your WAN interface as well as the DNS information. This information is transferred automatically but you must have set the WAN interface as DHCP client. If your Internet Service Provider has a DHCP server then click on `WAN` in the interfaces box and choose client under the DHCP mode box.



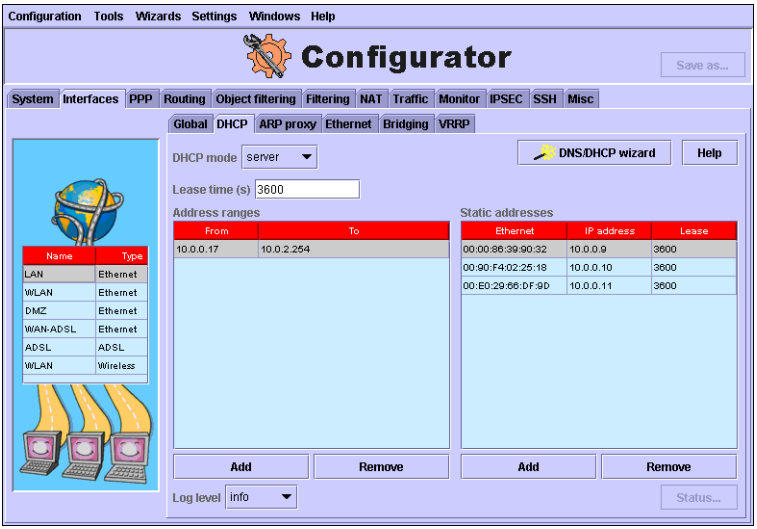
You have 3 different ways for preparing your firewall to interact with your network. Either it will act as a DHCP server and automatically give all of the necessary setup information to any computer plugged in to your network, you can configure the use of a remote DHCP server using DHCP relay, or you can choose the all manual route where every network device must manually be configured with the necessary settings to reach the firewall.

> TIP — If this is the first time you have set up a network we recommend you start using the MultiCom Firewall as a DHCP server. This is a very quick way to manage your network and when changes are made they will automatically be sent to your network.

LAN As A DHCP Server

While the firewall is set to act as the DHCP server on your LAN, it can automatically distribute most necessary information to the computers on your network you do need to tell it what range of IP addresses to distribute.

To use the MultiCom Firewall as a DHCP server start by going to the `Interfaces>Global` window and click on the `DHCP mode` box. Next choose the `LAN` interface in the interface box and then choose `server` in the `Mode` box.



The DHCP Server of the MultiCom Firewall can either randomly assign IP Addresses within a preselected range or static entries can be given out based on the MAC Address of different Ethernet devices on the network.

We recommend using a range between 10.0.0.17 and 10.0.2.254 since they are private addresses and will never be found on the Internet, however you may change this range to suit your needs.

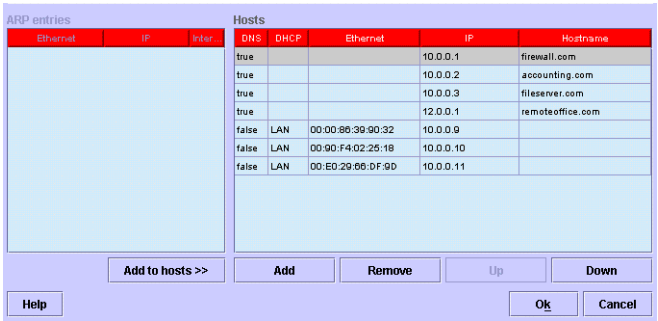
NOTE - Lightning-Linux allows you to have up to 1,000 DHCP clients per MultiCom Firewall. For instance if you have to 100 computers on your internal network you could set your IP address range to be 10.0.0.11 to 10.0.0.110.

This ensures that every computer on the local network that wants to connect to your firewall will be able to get its own IP address.

DHCP Static Addresses

It is possible to guarantee that the same computer requesting an IP address will always receive the same IP address. This is useful for servers or using the Local DNS service of the MultiCom Firewall.

The only way to uniquely identify a computer is by the MAC Hardware address of the Ethernet interface card. To quickly find the MAC Hardware address of a computer you can use the Configurator software's DNS/DHCP Wizard available under the Configurator's Wizard menu.



When the Configurator is connected to an online Firewall, active ARP/MAC hardware address entries are retrieved from the Firewall and can be used to build up new DNS/DHCP entries. Otherwise check the information that came with the network card of the device to find out how to retrieve the MAC Hardware address.

Starting with Lightning-Linux 3.5 it is possible for the DHCP range to contain IP addresses that are being used for static DHCP distribution.

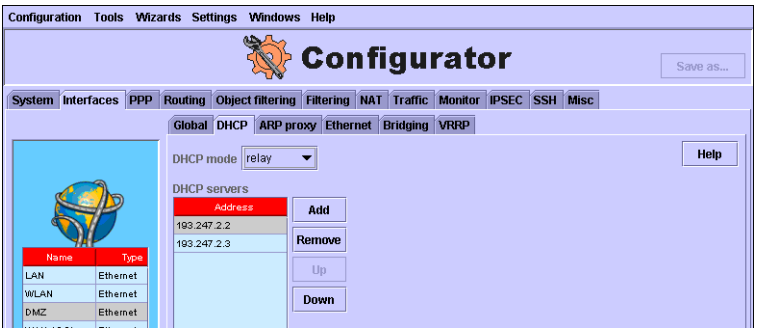
LAN As A DHCP Relay

The MultiCom Firewall can be configured to use a remote DHCP server to distribute IP configurations to the LAN. This may be preferable when the IP distributions are centralized on a remote server.

To use the MultiCom Firewall as a DHCP server start by going to the `Interfaces>Global` window and click on the `DHCP mode` box. Next choose the `LAN` interface in the interface box and then choose `relay` in the `Mode` box as shown in the screen below.

Simply add the IP Address or Addresses of the remote DHCP servers that will be managing the IP Address distribution. Requests from the LAN will be forwarded to this remote server and replies from the server will be passed on to the DHCP clients in the local network.

CAUTION - It is necessary that the remote DHCP server be configured correctly to manage these requests. For instance, it must give the IP Address of the LAN interface of the MultiCom Firewall as the default gateway for Internet access.



LAN Using Manual Configuration

When manually configuring your own DHCP services please consider the following 3 guidelines to avoid network communication problems. If you are using the automatic DHCP configurations for your LAN these guidelines are already being used and you should not need to change anything.

1. Make sure that none of the IP addresses overlap with static IP addresses (for instance your firewall is defaulted to 10.0.0.1 for the LAN interface so be sure there are no other devices on your network using 10.0.0.1). If you told the DHCP server that it could also distribute that number there will be two devices with the same network name.
2. We recommend IP addresses in the 10.0.0.0 range because they are private addresses that cannot be assigned on the Internet. If you choose other IP addresses you may be using an address from the Internet and if someone from your network wants to go to that Internet site they will instead go to someplace in your internal network.
3. The IP addresses that you choose must be in the same subnet range as specified by your interface connection. For example, if you have an IP address for the LAN interface of 10.0.0.1, with a subnet of 255.0.0.0 then you cannot use DHCP ranges of 192.5.0.1–192.5.0.100 because they do not start with the number 10 (instead they start with 192.)

DHCP Client Configuration

When an interface is configured as a DHCP client it can receive its IP parameters from a connected DHCP server. The default configuration of the MultiCom Firewall's WAN interface is to act as a DHCP client.

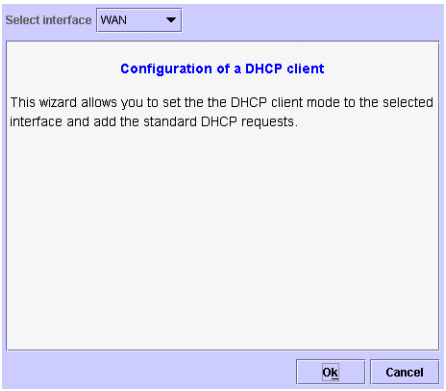
There are 5 DHCP requests that an interface of a MultiCom Firewall can request.

- subnet-mask
- broadcast-address
- routers
- domain-name
- domain-servers

Each request can be optional, required, and can have a default value and/ or a prepend. The default parameter is the value assigned unless otherwise given. The prepend is the TCP/IP configuration settings that the DHCP Client can use while waiting for a DHCP server to configure it

DHCP Client Request Wizard

This wizard allows the selected interface to be quickly configured with the most common DHCP requests. It is available in the Configurator software under the Wizard menu.



When the Wizard is activated the selected interface will be reconfigured as a DHCP client with the requests shown below:

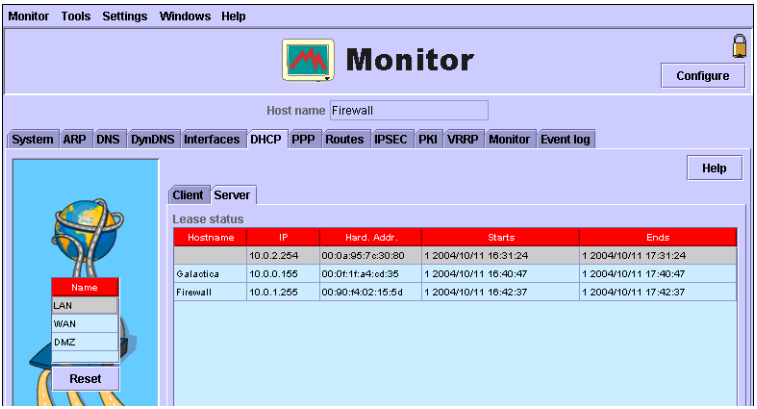
Table 1: Default DHCP client requests

subnet-mask	request
broadcast-address	request
routers	require
domain-name	request
domain-servers	require

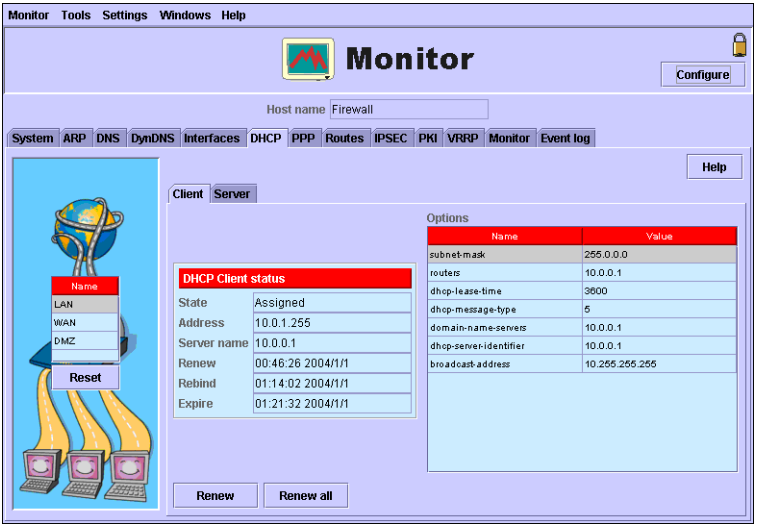
DHCP Monitoring

Using the Monitoring window of the Configurator software you can access useful DHCP information for each Ethernet interfaces configured as a DHCP server or client.

Below is the screenshot of the Monitor for a DHCP server. All of the DHCP clients that your MultiCom Firewall is managing from the selected interface will be shown. Additionally it will give you status messages for each DHCP client lease.



Below is the screenshot of the DHCP client monitor. All of the configured DHCP options on the selected Ethernet interfaces are shown if that interface is configured to be a DHCP client. Additionally it will give you status messages for each interface.



For more information on the statistics available from the DHCP Monitor panels check the Monitor Panels Appendix.

Chapter 7

DNS or Name Resolution

The DNS system is actually a huge distributed database spread over many servers on the Internet. This system keeps track of the names and IP addresses of public networks (much like a phone books keeps lists of names and their corresponding phone numbers.) If your local DNS server does not know the IP address that you are looking for it makes a request to the closest DNS server until either a server is found that knows the answer or the request times out.

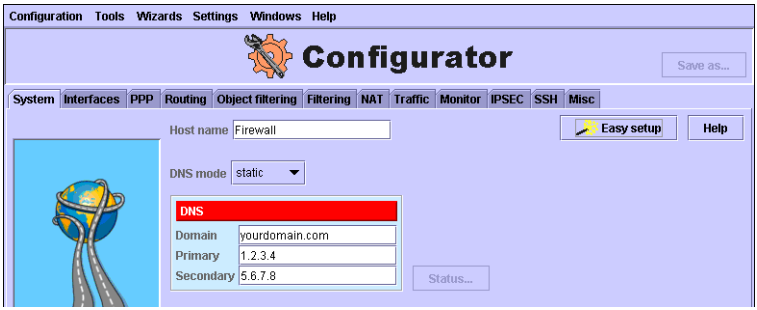
To use this service there must be some server accessible from your network that knows the website name and IP address to link it to. When you try to reach a computer using its “name” your computer makes a request to the nearest DNS server (which is part of a huge distributed database of network names and IP addresses) to see if it knows the IP address of the requested computer's name.

This service translates network names to IP Addresses (i.e. www.lightning.ch -> 193.247.134.2). These numeric IP addresses are required to send data over the Internet using but are often difficult to remember, especially when surfing the Internet or moving between many different sites. Using name resolution is very helpful because it is easier to remember a company or website's name instead of its IP address.

Global DNS

Global DNS information is configured statically or received dynamically through a protocol such as DHCP, PPPoE, or PPTP. This information is used by the DHCP server when it sends this DNS information to its DHCP clients on the LAN and by the proxy DNS server to redirect DNS requests to real DNS servers.

A static configuration requires that the IP addresses of the DHCP are entered into the configuration along with the domain name if used. This is done on the System Panel of the Configurator. This static information is not overwritten by DHCP or PPP dynamically assigned DNS information.



Dynamic configuration of Global DNS implies that information DNS information will be received through a protocol such as DHCP, PPPoE, or PPTP. For DHCP, received information (from the WAN interface's DHCP client for instance) is used by the proxy DNS or the DHCP server as in the case of a static configuration. For PPPoE, the problem becomes more complex. Because multiple PPPoE sites can be active simultaneously, it is possible to receive IP addresses for multiple DNS servers.

In the case where proxy DNS is disabled, the last PPPoE connection to receive DNS server information becomes the Global DNS servers to be used for resolving DNS queries. If this site looses connection, the PPPoE connection just before the site that lost connection which provides the Global DNS information. If a site is connected afterwards, it is this most recent site that supplies the Global DNS information. Another way to view this is that all of the PPPoE connections with DNS information form a list where the most recent connection is the one used as Global DNS. When that connection disappears it is the connection before it in the list that is used.

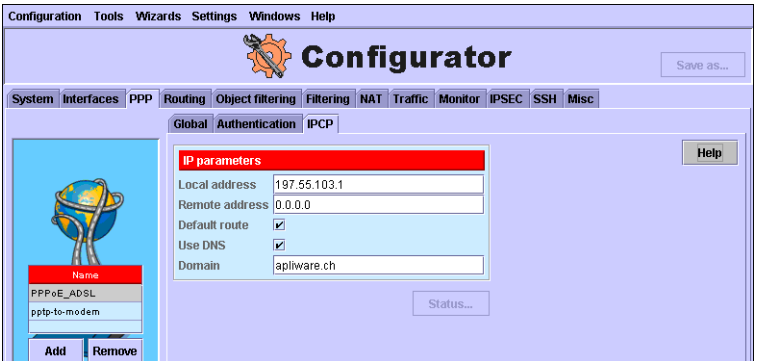
In the case where proxy DNS is active, one of the PPPoE connections provides the default DNS information while the others resolve DNS requests that match the Domain Name configured for each specific site. All other DNS queries with an unknown Domain Name will use the default DNS information.

If several sites do not have a configured Domain Name it is the last of these sites that provides the default DNS information. If all of the PPPoE connections have a configured Domain Name it is the last connected PPPoE connection which provides the default DNS information.

DNS and PPP connections

For a PPP connections it is possible to enable or disable the use of DNS information received from this site. Additionally it is possible to associate a Domain Name with the selected PPP connections (which is only usable if the Proxy DNS option is being used on the firewall.) When used together, PPP domain names and Proxy DNS, the firewall can redirect DNS requests to different servers according to the domain name forming part of the request.

For example, lightning.ch, lightning.net, and lightning.edu could all have separate PPP DNS servers assigned to them which would be used depending on which one was used in the request. Therefore the request for webserver.lightning.ch could use a different DNS server than the request for webserver.lightning.edu.



The DNS info received by the PPPoE sites can also change as it is given during the authentication process. It is not obligatory to assign a PPP connection a Domain Name. If no domain name is given and the Use DNS option is selected

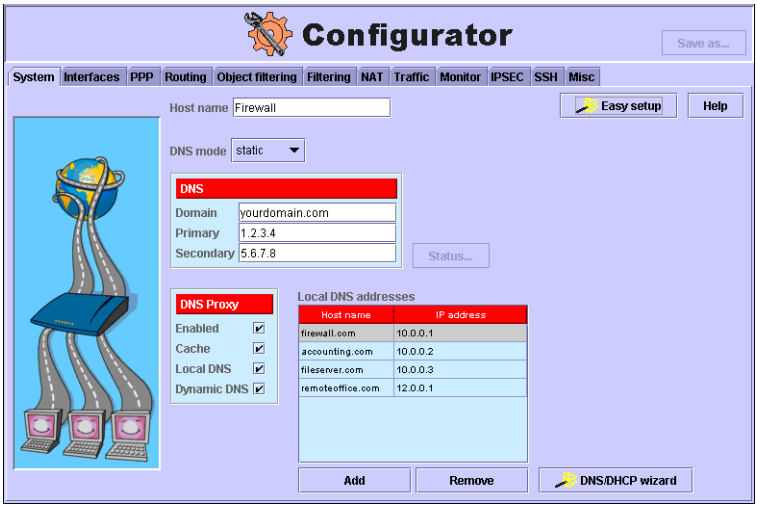
for the PPP connection then the DNS information received via the PPP connection is considered to be the default global DNS information for the firewall.

Multiple PPP connections using PPPoE, which have DNS servers associated to a Domain Name become a list that is used before the default DNS server. DNS requests will be checked to see if they contain a matching Domain Name that corresponds to a PPPoE site. If such a site is found, that site's DNS servers will be used to resolve the query. If no PPPoE site has a matching Domain name or there are no PPPoE sites then the query is sent to the firewall's Global (default) DNS server.

Proxy DNS

Proxy DNS allows computers on the local area network (LAN) to use the MultiCom Firewall as the DNS server. The MultiCom Firewall then checks it cache of recently used names and if it does not find the actual IP address the firewall forwards the request to a "real" DNS server.

This allows the use of different DNS services without having to change the configuration of each client workstation; only the firewall needs to receive the new IP addresses of the DNS servers and it will forward requests to the appropriate server.



When the proxy DNS is activated on the System panel of the Configurator, the DHCP server sends its clients the IP address of the interface on which the DHCP server is configured as the IP address for DNS. This global DNS is not associated with a particular Domain Name as can occur with PPPoE sites.

Different DNS servers can be identified by Domain name allow redirection to the appropriate DNS server. This feature is used particularly when Domain names are specified in PPPoE sites.

DNS Cache

When using the DNS Proxy of the MultiCom Firewall there is the additional option to use the DNS Cache. The cache is a list of recent DNS queries that allows the MultiCom Firewall to reply to matching requests without asking the information again from the main external DNS server. While in most cases this enhances and speeds up the Internet requests in some cases it may not be desirable.

With Lightning-Linux 3.4 or higher it is also possible to enable or disable the DNS cache used by the Proxy DNS service. This is useful when a DNS name might have a changed IP address due to the use of Dynamic DNS on the remote site. The cache of the MultiCom Firewall's Proxy DNS may not update fast enough to keep track of the latest IP address.

Local DNS Server

Starting in Lightning-Linux 3.5 there is a built-in DNS server. This service allows the administrator of the firewall to give personalized names to internal computers and aid in redirecting traffic (for instance to a local webserver) from the internet. There are 3 ways to add a name to a computer on your local network.

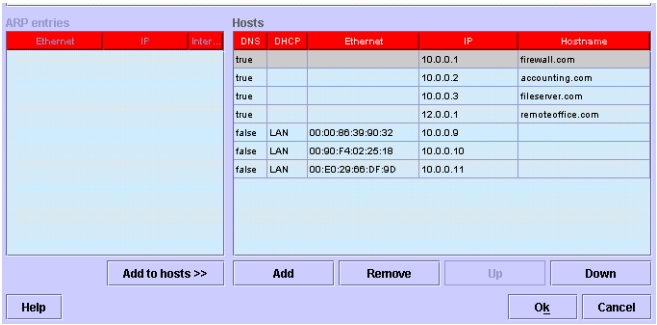
- DNS Wizard
- Manually Configure DNS with the Configurator's System panel
- Dynamically for DHCP clients

For example, by adding a Local DNS hostname of "mybusiness.com" and redirecting it to 10.0.0.2, any user on the LAN that is using the MultiCom's DNS server will receive 10.0.0.2 when they type in the name "http://mybusiness.com".

NOTE - The computers on the LAN must be using the MultiCom Firewall to receive their DNS information. If the LAN computers are configured to use the DNS servers of the ISP directly or another DNS server, then the MultiCom Firewall will not respond to those requests.

DNS Wizard

The DNS/DHCP wizard is available from the Wizard menu or the System panel button titled "DNS/DHCP Wizard" of the Configurator software.



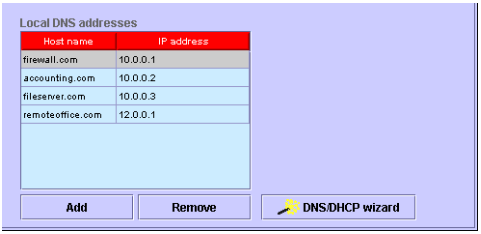
This wizard allows you to set the DNS local addresses (IP address and hostname) and the DHCP server static environment (ethernet and IP addresses) all at once. If the Configurator is online, current ARP entries are retrieved from the device and can be used to build up new DNS/DHCP entries. If the Configurator is offline, then you can either manually enter this information or add only a hostname that will resolve to the listed IP address.

Configuring static IP addresses to computers with DHCP allows them to still request regularly their DHCP information and to always receive the same IP address.

Local DNS must be enabled on the System panel of the Configurator and UDP port 53 must not be blocked for the networks using the MultiCom as a DNS proxy/server.

Manually Configure DNS

When manually configuring the DNS names of local computers or other network devices you can add a name to one IP address. You cannot add multiple names to the same IP address.



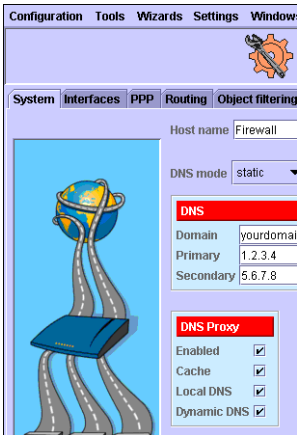
If the Configurator is offline, then you can either manually enter this information or add only a hostname that will resolve to the listed IP address.

> CAUTION - If the devices on your network are DHCP clients their IP address might change dynamically. To avoid this, use the DNS/DHCP wizard to assign fixed IP addresses to the MAC hardware address of each network device.
>
> Optionally, activate Dynamic DNS on the Configurator's System panel and the host name of the DHCP client will automatically be used as the network name, regardless if the IP address changes or not.

Local DNS must be enabled on the System panel of the Configurator and UDP port 53 must not be blocked for the networks using the MultiCom as a DNS proxy/server.

Local Dynamic DNS

Starting with firmware 3.7 it is possible for the DNS server of the MultiCom Firewall to automatically take the hostname of any DHCP client and add the name and assigned IP address to the DNS name list.



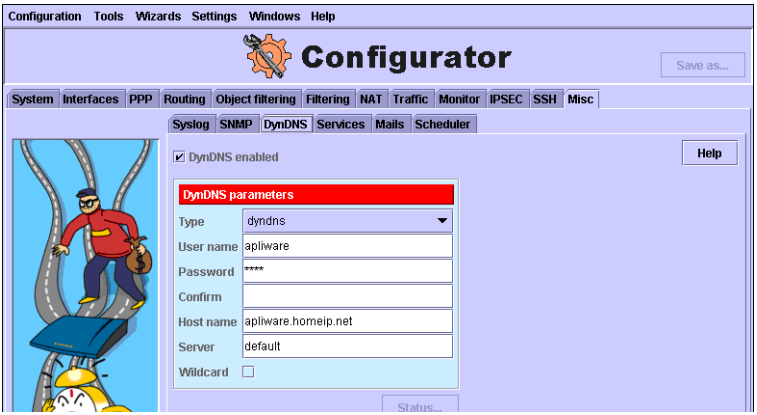
CAUTION - Each DHCP client must have a unique host name configured on the operating system. Optionally you can use the DNS/DHCP wizard instead to configure static DHCP assigned IP addresses and DNS names to each computer.

The LAN interface must be configured as a DHCP server and Local DNS and Dynamic DNS must be enabled on the System panel of the Configurator and UDP port 53 must not be blocked for the networks using the MultiCom as a DNS proxy/server.

Internet Dynamic DNS

With Lightning-Linux 3.4 and higher it is possible to configure the WAN interface to connect to one of many dynamic DNS server on the Internet where you already have an account. These services allow the MultiCom Firewall to receive an Internet name even if you do not have a static IP address from your ISP. Whenever your broadband connection is activated or receives a new IP address the dynamic DNS server will be contacted.

This allows for Internet users to easily find your MultiCom Firewall by the name that you have configured for it.



This is useful when the MultiCom Firewall does not have a fixed IP address but the user still wants to have a name on the Internet that the device can be found. When this service is configured the MultiCom Firewall will update the chosen dynamic DNS server with the current IP address of the WAN interface whenever it is changed.

Supported services include

- http://www.dyndns.org
- http://gnudip2.sourceforge.net/gnudip-www/
- http://hn.org/
- http://www.zoneedit.com/
- http://www.dhs.org/
- http://www.ods.org/
- http://www.dyns.cx/
- http://www.tzo.com/
- http://www.easydns.com/

NOTE - By default the MultiCom Firewall's Securewall will block all incoming traffic from the Internet. You must open holes in the Securewall to allow access to the MultiCom Firewall itself (for configuration or VPN tunnels) or to publish LAN servers on the Internet.

Configuring DNS

A typical Internet connection will require that you enter in your Internet Service Provider's name and address of its DNS server. Alternatively, your organization may maintain its own DNS server or DNS proxy which will resolve these name requests for you. With the MultiCom Firewalls you can configure DNS globally, or dynamically with 1 or more PPPoE sites. Additionally you can enable the firewall to be a Proxy DNS service for easier managing of DNS servers.

If you use a static DNS server you must supply to your firewall: your DNS Domain Name and a Primary and a Secondary DNS server. You may need to ask your Network Manager or your Internet Service Provider (Internet Service Provider) to obtain this information.

In many cases you don't need to configure the DNS, as this information can be obtained automatically when a connection is established. If you use Easy Setup to configure the firewall it will try to obtain this information automatically from your Internet Service Provider. In manual configuration you will need to configure from which site you wish to obtain the DNS information in one of the following screens.

Not using the DNS service will limit you to using only IP addresses to identify remote networks unless your system administrator has created an alternate service to provide name resolution.

Special DNS Activity

The Global DNS information (DNS primary and secondary servers as well as the configured Domain Name) is stored permanently to facilitate a special situation. It is possible that the MultiCom Firewall using dynamically assigned DNS servers may not receive DNS information before a DHCP server receives a demand for an IP configuration. In this case, the DHCP server sends the saved

DNS information from before the restart of the firewall. This information is saved only when the DNS information is modified and the DNS mode is set to Dynamic in the System panel of the Configurator.

If the DNS information has changed it would be necessary for the DHCP clients on the LAN to renew their DHCP configuration to retrieve the new DNS information. This problem is avoided when using the proxy DNS feature of the MultiCom Firewall. In this case the DNS information is always the interface of the DHCP server on the MultiCom Firewall.

The recommended configuration of DNS services is

- proxy DNS activated
- (if using multiple PPPoE sites) define one site without an associated Domain Name (this site would become the default DNS server)
- (if using multiple PPPoE sites) define the other sites using DNS with associated Domain Names

Chapter 8

PPP Connections

Point to Point Protocol (PPP) encapsulation over Ethernet is one of the ways for you to configure your MultiCom Firewall interfaces. Frequently Internet Service Providers who offer Broadband access will use PPP to manage and configure users connections.

PPP connections is a method similar to DHCP for managing network IP addresses. Whereas DHCP will simply assign any DHCP client plugging into a network an IP configuration, PPP connections requires a user to authenticate with a user name and password BEFORE any IP configuration is given.

These types of connections are popular with xDSL Internet Service Provider's (ISP) and is sometimes the only way they will let you connect to their network. Be sure to check if your ISP uses this service if you are unsure. The two types of PPP connections supported by the MultiCom Firewall are:

- PPPoE (PPP over Ethernet) specifications at RFC2516
- PPTP (Point to Point Tunneling Protocol) specifications at RFC2637

PPPoE Connections

A PPPoE (PPP over Ethernet) is very similar to PPP used for analog modems except that it occurs over Ethernet connections. After using an username and password for authentication the physical Interface of the MultiCom Firewall receives IP configuration information directly from the ISP (IP address, subnet mask, default gateway, DNS servers).

There are many options that can be used depending on what features are supported by your ISP or your account with the ISP. Some connections are closed after 30 minutes of inactivity, reset after 2 hours regardless of active use or no use, or charges may even accrue depending on the time the PPPoE connection is being used. Be sure to request a detailed explanation from your ISP which explains how they manage your PPPoE sessions.

Multiple PPPoE sessions can be opened to one or more destinations via a shared Ethernet interface, using one or more bridging modems. This type of connection requires that one or more PPPoE servers be available to support each PPP connection using PPPoE encapsulation. These servers may be offered by an ISP using hardware known as a Broadband Remote Access Server or Access Concentrator.

CAUTION - enabling PPPoE connections for an interface will disable the interface's other configuration settings such as DHCP, static IP and NAT configurations. If you want to use those modes or features later you will need to turn off the PPP feature for that specific interface. NAT configurations can be configured under the PPP connections NAT table.

Available Options

Below is a list of the possible options that can be configured with a PPPoE connection in the MultiCom Firewalls.

- Physical Interface to use on the Firewall (normally this is the WAN Interface)
- Username/ Password (in PAP or CHAP modes)
- IP Address
- DNS Server - primary and secondary (dynamically set if the use_dns parameter is activated)

- Default Firewall (dynamic if the default_route parameter is activated)
- Access Concentrator name
- Service Name
- Call Management and Idle Close Time
- TCP Frame size adaption

PPPoE Call Management

In Lightning-Linux 3.3 PPPoE Call Management has been added. This allows more control over the state and use of a PPPoE connection. There are now 3 types of PPPoE connections:

- Permanent (always on and the default mode)
- Dial_on_Demand (activated when any routable IP activity is passed to the selected interface)
- Manual (connection activated only by using the Configurator's Monitor window)

For the last 2 options it is possible to set an Idle Close Time in seconds. When this time passes without any routable IP activity occurring the connection is closed. Otherwise the connection is retried in intervals not lasting more than 64 seconds.

PPTP Connections

The Point-to-Point Tunneling protocol uses a version of GRE (Generic Routing Encapsulation) to transport PPP packets. This makes it possible to provide flow control and create tunnels used to transport packets inside the PPP encapsulation. The version implemented in Lightning-Linux 3.2 is only usable on local networks and not usable over routable networks like the Internet (however as of version 3.3 there is PPTP Passthrough available. It was implemented to connect to broadband modems that do not offer the bridge mode for PPPoE authentication. These broadband modems often offer a PPTP connection for use in the LAN and if so the MultiCom Firewall can connect to it.

If using the PPTP encapsulation the user will also need to know the IP address of the PPTP server as well (in most cases this is the IP address of the broadband modem on the LAN side). There can be only one PPTP connections per interface.

NOTE - In Lightning-Linux 3.3 PPTP passthrough has also been added for 1 or more clients on the LAN. This allows VPN's to be created between remote servers and individual computers on your local network. Currently this does not support remote requests to a PPTP server on your local network.

Special attention needs to be taken when using PPTP on the WAN interface. Using PPTP requires a pre-existing IP configuration for an Ethernet interface (typically the WAN interface) since the PPTP server is identified with an IP address. Some modems such as Alcatel modems default their broadband modem's IP address to 10.0.0.138 (this is the same IP range enabled on the LAN by default. While this configuration is available through the Easy-Setup on the webserver or Configurator software of Lightning-Linux 3.3 the steps below summarize how to do this manually.

To build a PPTP connection to the modem the user will need to reconfigure the broadband modem to use a different IP address or reconfigure the MultiCom Firewall as shown below...

1. configure the WAN interface to have an IP address of 10.0.0.1 with a subnet of 255.0.0.0 (this assumes that the PPTP modem is on this subnet, if you are not sure you must check the modem's manual or contact the manufacturer of that modem.)
2. change the LAN interface to another public range such as 192.168.0.1 with a subnet of 255.255.0.0
3. if using the DHCP server on the LAN reconfigure the range to 192.168.0.17 - 192.168.2.254
4. Configure and enable a PPP connection using PPTP encapsulation

Because the IP address is required on the WAN interface to communicate with PPTP server communication can arrive on both networks... the network physically assigned to the WAN interface (in this example 10.0.0.1) and through the PPTP configured interface.

CAUTION - enabling PPTP connections for an interface will disable the physical interface's NAT configuration settings. NAT configurations can be configured under the PPP connections NAT table.

Available Options

Below is a list of the possible options that can be configured with a PPTP connection in the MultiCom Firewalls.

- Physical Interface to use on the Firewall (normally this is the WAN Interface)
- Username/ Password (in PAP or CHAP modes)
- IP Address
- DNS Server - primary and secondary (dynamically set if the use_dns parameter is activated)
- Default Firewall (dynamic if the default_route parameter is activated)
- PPTP Server Address
- TCP Frame size adaption

PPTP Passthrough

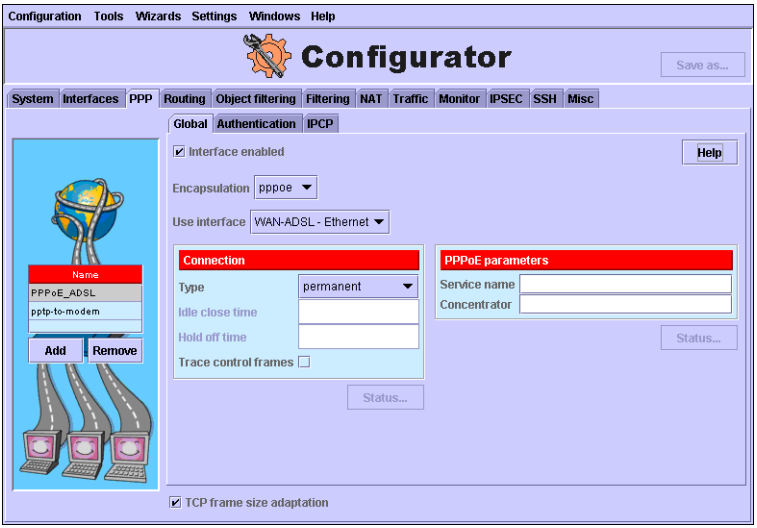
In Lightning-Linux 3.3 PPTP passthrough has also been added. This allows VPN's to be created between remote servers and one or more client computers on your local network. In this situation the MultiCom Firewall is not the PPTP client but passes PPTP requests on to the requested remote server.

This option may be used with Microsoft's PPTP VPN client which is built-in to many versions of Windows to communicate through the MultiCom Firewall to a remote PPTP server. Connections to an internal PPTP server from the WAN are not supported at this time.

PPP Connection Interface

Global PPP Settings

The Global PPP Panel of the Configurator offers access to the most commonly used parameters used to configure a PPPoE or PPTP connection. Each PPP connection can have its own NAT rules, DNS servers, and be used for routing and filtering.



While it is possible to assign PPPoE connections to one or more physical interfaces of the MultiCom Firewall, each PPPoE connection must be enabled to be active. Disabled interfaces are stored in the configuration file but are inactive.

> NOTE - It is possible to enable more than one PPPoE connections assigned to the same MultiCom Firewall Ethernet interface.

A username and password are required to make a PPP connection. If a PPTP connection is made the IP Address of the PPTP server is also required.

Optionally for PPPoE connections the user may configure the PPPoE Service Name and/ or Access Concentrator to be used by this site. This type of configuration is not always an option with your network or Internet Service

Provider. For example, this might be useful if 2 different ADSL modems were connected to the WAN interface. For the MultiCom Firewall to know which modem connection gets which set of username and password the user could identify specifically the Access Concentrator for each set of username and password.

Enabling the option to “Trace Control Frames” (disabled by default), generates debug information concerning the selected PPP connection. This information is sent via syslog messaging at the Debug Log Level (see the Chapter on Syslog messages) and are traces of the following protocols and activity:

- LCP (Link Control Protocol)
- IPCP (Internet Protocol Control Protocol)
- PAP (Password Authentication Protocol)
- CHAP (Challenge Handshake Authentication Protocol)

Only the control packets of these four protocols is sent as syslog messages. The fields forming part of the packet headings are decoded and posted in a readable form. The data part of the packet is not decoded and is posted in hexadecimal.

TCP Frame Size Adaption

TCP Frame Size Adaption is an option that is enabled by default. This forces the size of TCP packets to fit within the PPPoE interface. Some routers on the Internet can cause TCP communications to be dropped without this option set. More information about this problem can be found in RFC2923.

NOTE - Using "TCP frame size adaption" may block IPSec packets as IPSec will not allow you to change the data packet in this way.

When using PPPoE interfaces, packets (the pieces of data traveling over the Internet) have less space to carry data because some of the packet is being used to encapsulate Ethernet frames inside a PPPoE frame which itself is packaged into another Ethernet frame on the wire. With this fix enabled, all TCP SYN packets which seem to be a PPP packet set the MSS to 1452.

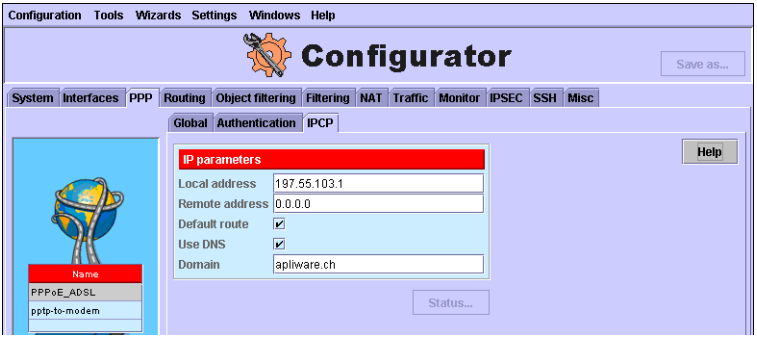
A data packet must fit within this smaller space to make it through the PPP interface or it will be dropped. There are 2 ways for the size of the packets to be agreed upon.

- AGREEMENT: when the TCP connection is initiated, both sides agree on the size of packet they will accept.
- DISCOVERY: the remote computer will try to discover the largest size of the packets it can send by sending a special discovery packet and wait until it hears an ICMP response saying that Fragmentation is Required.

With the AGREEMENT process, although both sides may find an packet size they can accept there may be routers in between them that only support even smaller sizes. Packets could be dropped here.

With the DISCOVERY process, the remote host (often a webserver) will be waiting to receive a "Fragmentation Required" ICMP packet to decide what size of packet to send. Some routers or firewalls may not send this message (being "anti-social"). Without this message the remote host will not send any further information and the remote site may appear to be down or broken.

Advanced PPP Settings



If you are using PPPoE or PPTP and your Internet Provider has given you a permanent IP address you can configure it on this screen. This will configure your MultiCom Firewall to always ask for the same IP address when it authenticates (your ISP must support this.)

You can also choose whether to use this PPP connection as the default route (typically a route to the Internet) or not on your firewall and if you want to use it as your source of DNS name resolution. When the PPPoE connection is ready to be used a default route is automatically added for it in the firewall's routing table.

If several PPPoE connections are established (remember there can be only one PPTP connection per interface), several default routes can be added to the routing table. In this case it is the last PPPoE site that was inserted into this list that will be used as the default route. To not include a PPPoE site as a possible default route be sure to disable the Default Route option in the site's IPCP panel of the Configurator.

Your final option is to assign a domain name for this specific PPP interface. This will be used to direct DNS traffic for the specified domain name to the DNS servers being used by the selected PPP connection.

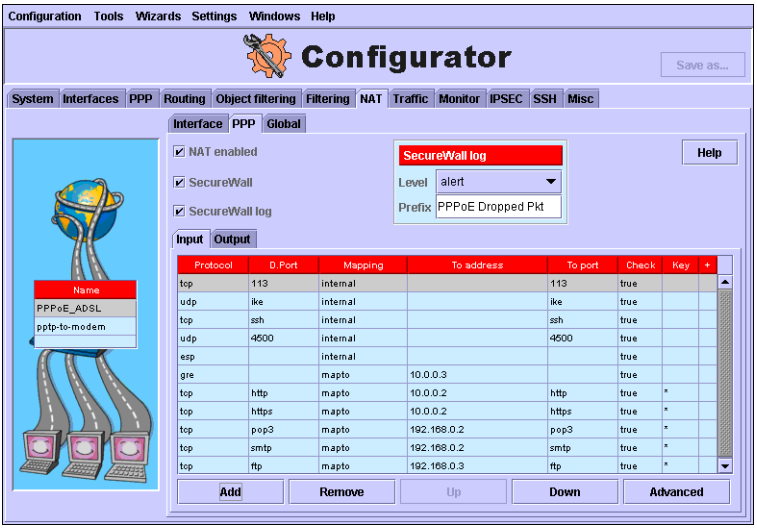
NOTE - these options are only good for the selected PPP connection and not for all PPP connections.

WARNING - Use caution when using multiple PPPoE sites for default routing or collecting DNS information. For example, when using multiple ADSL modems and sites, one modem may finish authentication before the other in a seemingly random order. It is the last site that authenticates that will typically be used for default routing or as a source of default DNS information.

NAT Using PPP Connections

The NAT panel of the Configurator has a PPP tab where Network Address Translation rules can be added that are used only for the selected PPP connection. It is configured the same as the Network Address Translation of Ethernet interfaces. The only difference is that these NAT settings are valid only for the selected PPP connection and always disables the physical Ethernet interface's NAT configuration if there was any. If you want to make NAT rules that are valid for more than one interface you will need to make the rules under the NAT > Global table and activate NAT on the interfaces which are to use those rules.

Please see the "NAT & PAT" Chapter on page 171 for an a full explanation on configuring and using Network Address Translation.



Configuring PPP

You will have the option of identifying more than one set of PPP connection and if they use PPPoE encapsulation any of these connections can be active at the same time. You can also use the others as a backup list or as alternate connections. However it is not possible to activate PPPoE and PPTP connections at the same time.

New PPPoE & PPTP Connections Defaults

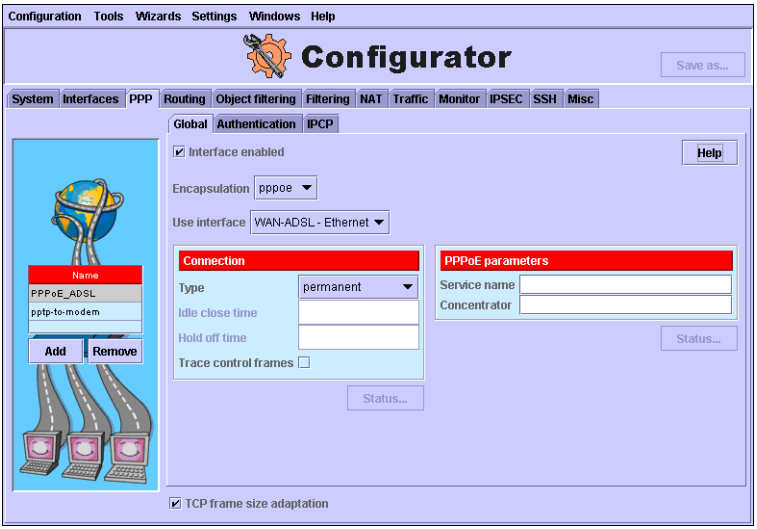
Below are the default settings for newly configured PPPoE and PPTP connections.

Table 1: Default settings for PPPoE and PPTP connections

Parameters	PPPoE	PPTP
Interface enabled	no	no
TCP framesize adaption	enabled	enabled
Default route	yes	yes
Use DNS	yes	yes
NAT	disabled	disabled
SecureWall	disabled	disabled
Trace control frames	disabled	disabled
Connection type	permanent	permanent

PPP Connection Configuration

Authentication with the Internet Service Provider is supported in both PAP and CHAP modes.



Now we will configure your WAN port to use PPPoE to connect to your Internet Service Provider (ISP) and hence to the Internet.

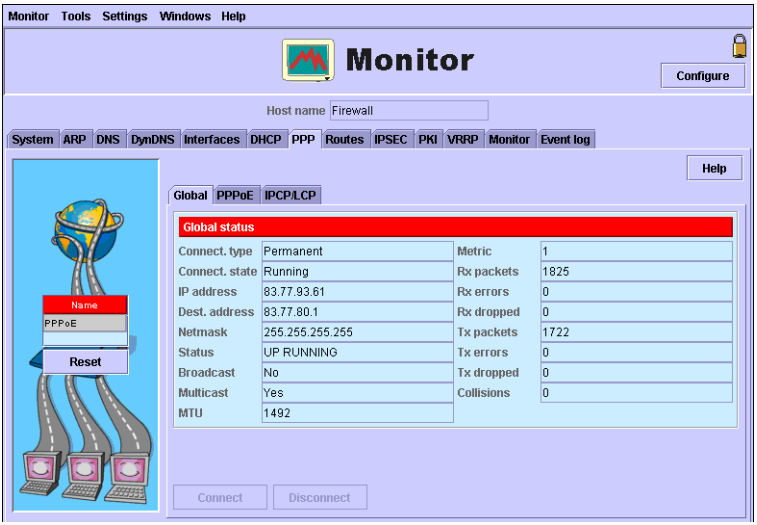
You will need to have your modem set as a bridge (please refer to the documentation that came with the modem or from your ISP for method to do this.) You will also need a username and password from your ISP. The following steps assumes that you have already opened the Configurator software.

1. goto the PPP window of the Configurator
2. click the Add button under the Interfaces table and enter a name for this configuration
3. click Interface Enabled
4. under “Use interface”, click on WAN
5. click on the tab named “Authentication”
6. enter your Username and Password from your Internet Service Provider in the Local Authentication section of the window.

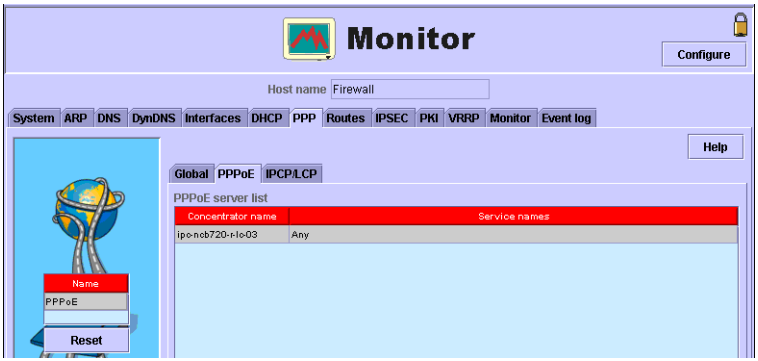
NOTE - If a PPPoE connection is closed by its’ remote server the firewall will periodically try to reinitiate the connection.

PPP Connection Monitoring

With Lightning-Linux 3.1 and later PPP statistics have been greatly improved. You now have three panels of data regarding your PPP connections.

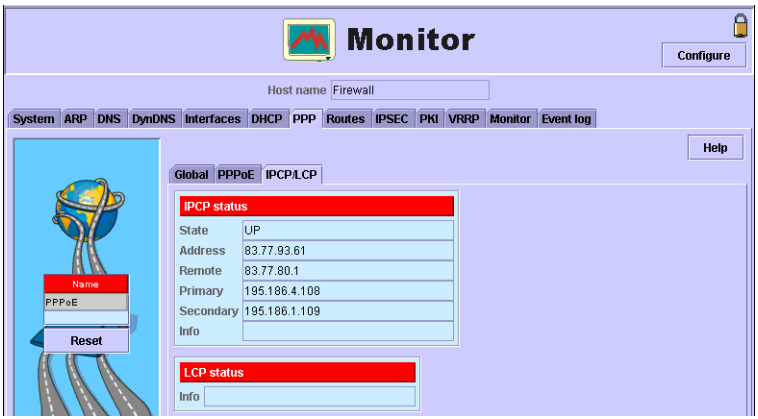


The PPP Global panel displays the status of the selected PPP connection but also display the current IP configuration of the selected interface, the count of transmitted and received packets which successfully are processed by the interface, are dropped or cause errors data statistics.



This PPPoE Server window displays the available PPPoE WAN Access concentrators and services that are available on the network attached to the MultiCom Firewall interface that is configured as a PPPoE interface. If no Concentrator is shown there is none available to give an IP configuration. If this is the case

1. check if you have not already received a configuration on the previous window
2. check that your modem is configured properly, and
3. check that your ISP is not experiencing difficulties.



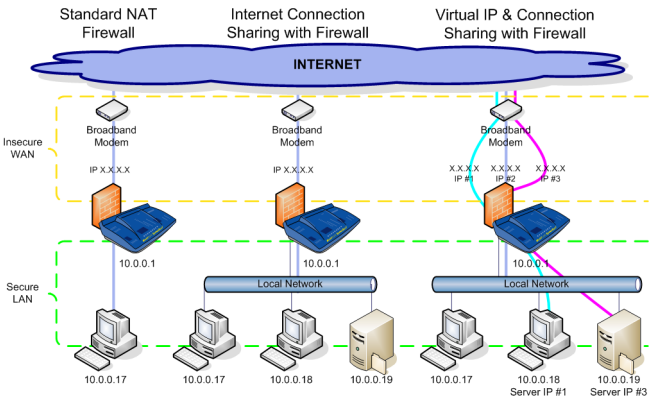
This IPCP/LCP window displays information about the PPPoE connection status for the selected PPP interface. Additionally, the LCP info field tells of any errors received from the remote server during an attempt to start a PPPoE session. If the error “endpoint not connected” appears there is no connected PPPoE server to give the Firewall an IP configuration (check the modem or contact the ISP). If the error “chap authentication failure” there is a problem with the username and password that was entered for this site.

For detailed descriptions of the PPPoE Monitors see the “PPP Monitor” Section on page 543.

NAT & PAT

Chapter 9

NAT stands for Network Address Translation, while PAT stands for Port Address Translation. Both processes change the IP header that tell a packet where to go but they each change a different part of the header. This is the technology that allows you to share your Internet connection, provides the first wall of protection for your network known as the SecureWall, and allows the use of more than one IP address.



IP Header Translation

NAT and PAT can be categorized together as IP Header Translations. They can change a portion of the IP header such as the IP address and port address of a private local webserver into legal external Internet address. You can disable IP Header Translations if you have your own internal range of legal IP addresses, and you would like to be visible "as is" from remote external sites. Starting with Lightning-Linux 3.3 you can disable IP Header Translations for selected IP addresses.

The most common use is to share a Single Internet User Account (SUA) where a single IP address can be used by a whole network, thus reducing the cost of Internet connection. Additionally, it is this technology that provides the first level of security for the MultiCom Firewall - SecureWall.

PAT

Port Address Translation (PAT) allows the translation of port numbers in the IP packet header. Because only TCP and UDP packets use port numbers only data traffic using these protocols are can use PAT. You can allow some services (like www, mail, new, telnet, ...) to be redirected to an internal machine (and optionally change the destination port as well).

TIP - Although you might redirect traffic using PAT, you will probably need either a static IP Address or be using Dynamic DNS for users to easily find you on the Internet. If your address changes dynamically, it will be difficult to find you on the Internet.

NAT

Network Address Translation (NAT) transparently changes IP addresses in TCP, UDP, GRE, ESP, AH or ICMP (using the ANY option) packets, allowing external access to internal machines. NAT can be activated on any Ethernet or PPP interface. These are the type of capabilities that you can expect from NAT...

- Mapping many addresses into one address
- Mapping many addresses to many addresses
- One to one mapping
- One to many mapping

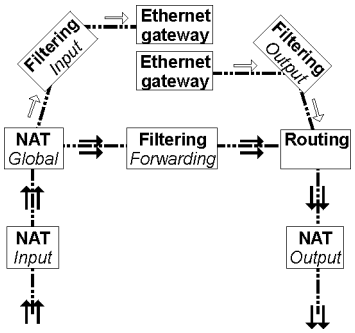
- Spoofing services

A domain with a set of private network addresses can be enabled to communicate with the external network by dynamically mapping to a set of global network addresses. Local nodes allowed to have simultaneous access to the external network are limited by the number of addresses in the global set. In addition, individual local addresses may be statically mapped to specific global addresses to ensure guaranteed access to the outside or to expose a local node for total access from the outside.

Static addresses are needed if you want to provide services like mail and web to the outside world. Indeed, if your address changes dynamically, it will be difficult to reach you from the Internet.

For each entry in the NAT table, you can specify the External IP Address that is used by NAT: either the address received dynamically from your Internet Service Provider, the global IP address of the MultiCom itself, or a static IP Address, and map this external address to an Internal IP Address.

CAUTION - be sure to take into account when the network address translation occurs in relation to other processes of the MultiCom Firewall.



Please refer to the above graphic to see the data flow through the MultiCom Firewall. For example, if you use NAT Input to change the destination of an IP address for a data packet then when it reaches filtering the filters will see the packet with the changed destination (and not the original destination that the

packet entered the firewall with.) Another example is that changes made with NAT Output happen after filtering and routing just as the packet is leaving the firewall. No further processes would affect it.

NAT Tables

There are 3 types of NAT tables that are used with the MultiCom Firewall. Using different tables allows you to create rules that target a specific IP address or port range.

Each physical interface can have its own NAT table (for instance the LAN, WAN or DMZ). If a PPP connection is used, the NAT tables of the physical interface is disabled.

For example, if you are using a PPPoE connection on your WAN interface, any NAT rules on the WAN interface are disabled and the PPPoE connection NAT rules are used instead. The LAN interface in this example still has active NAT rules, only rules of the physical interface using PPPoE is disabled.

NOTE - While each interface can only have one pair of Input and Output NAT tables, it is possible to have multiple PPPoE interfaces on a particular physical interface, each with its own NAT rules.

Interface or PPP NAT Input

The Interface or PPP NAT Input table controls Network Address Translation on data packets that come in on the specified interface. For example, using the LAN NAT Input table allows the user to make rules that only affect data packets arriving on the LAN interface. Rules in this table can use the “mapto” or “internal” NAT actions

Interface or PPP NAT Output

The Interface or PPP NAT Output table controls Network Address Translation on data packets that leave on the specified interface. For example, using the PPPoE NAT Output table allows the user to make rules that only affect data packets leaving on the PPPoE interface. Rules in this table can use the “mapto”, “masquerade” or “nomap” NAT actions.

CAUTION - when NAT is activated on an interface or PPP connection a default rule is added that masquerades all data leaving from that interface with the IP Address of that interface. If this is not desired you must add a NAT rule that specifies Mapping=Nomap for the packets that you do not want to be masqueraded.

Global NAT

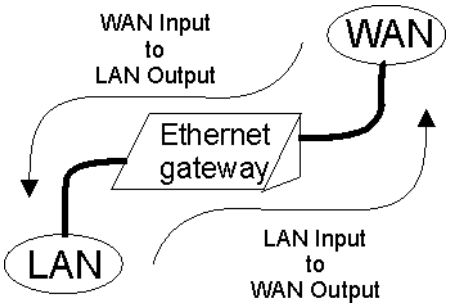
The Global NAT table controls Network Address Translation on all packets that interact with the MultiCom Firewall. An example of using this would be an office that wants to map their public IP address to an internal server an have external and internal users reach it with the public IP address. Rules in this table can use the “mapto”, “masquerade”, and “internal” NAT actions.

NAT In Action

When making Network/ Port address translations you must first decide

- Which packets to translate (identified by the IP address and/ or port address of the packet’s source or destination.)
- Which interface the rule is valid for (LAN, WAN, DMZ, a PPPoE site, or Globally.)
- Which direction the packet is moving in relation to the firewall interface or PPP connection - either Input (incoming to the interface) or Output (leaving from the interface.) Remember global NAT rules apply to packets moving in either direction.
- How to translate the packet. You can map the packet to another network or port address, you can redirect it internally to the firewall itself, you can masquerade the packet so it looks like it originated from the interface it exited from or you can choose NOT use NAT on selected packets.

The table that you use depends on the direction of the origin and destination of the traffic that you wish to affect. See the graphic below to see how the Input table is used for traffic arriving at an Interface and the Output table is for traffic leaving from the selected interface.



Input (data coming in on this interface)

1. mapto - replace the selected data's IP header with a different destination IP address or port.
2. internal - forward selected data to the firewall.

Output (data leaving from this interface)

1. mapto - replace the selected data's header with a different source IP address/ port
2. masquerade - all data leaving this interface has the source IP address replaced by the IP address of the interface the rule is set on.
3. nomap - data matching the description (IP Address/ port source or destination) can leave the MultiCom Firewall without receiving Network Address Translation (available in firmware 3.3 or higher)

For instance, if the MultiCom Firewall has a WAN IP address 192.0.0.10 and you want all information arriving at that IP address to be sent to a device on your network you would select mapto (on the WAN Incoming interface) and enter in the internal IP address of where you want it to go.

> CAUTION — Take care when translating port destinations as the remote servers need to be configured to listen at those ports. For example, sending external web requests with the destination port set at something other than 80 may cause it to fail to reach its destination.

Another option is to have the firewall check to see if the destination of the incoming data packet matches that of the interface it is arriving on. This is the same as entering the IP address of the interface being used, in the destination field. The option to do this in found at `Interfaces>NAT>Input` and is visible as a

check box. This is active by default but may be deactivated for the use of Virtual IP's where the WAN interface may be expecting traffic for more than 1 IP address.

NAT can also work with data packets coming from inside your network. For instance, if you wanted to redirect all internal news server requests to an internal news server you would instruct NAT to watch for all data packets going to port 119 (the port used by most Usenet news servers) and redirect those requests to the IP address of your internal news server.

CAUTION — NAT rules and Input NAT rules are the only way data can traverse the Firewall of the MultiCom Firewall. Once data has been allowed through by NAT it is up to the filtering rules to limit data access to NAT-enabled addresses since the Firewall will have let it through.

Common NAT Uses

Single Internet User Account

Sharing a single Internet Account works by changing the port number of all outgoing data requests, and logging them in an IP Translation table. Additionally, NAT will replacing the source address with the IP address assigned to the MultiCom Firewall by the Internet Service Provider. When a corresponding reply comes, the correct destination and port will be retrieved from the table (see below).

TIP - By default the NAT Connection Tracking table can track 2,048 simultaneous connections. If you have a heavy traffic load (popular web servers or many Internet users in the office) you may need to increase this.

This will hide all your local machines behind a single IP address and, since it records all outgoing requests, this allows to filter and record all unwanted incoming accesses, thus providing the SecureWall protection of your network against unsolicited accesses and hacker attacks from the Internet.

Single Internet User Account is activated by default in all Easy Setup configurations.

SecureWall

When NAT is activated on an interface a table is created of all outgoing traffic. This NAT Connection Tracking table is the basis of the SecureWall protection of the MultiCom Firewall. When the SecureWall is activated on an interface using NAT all incoming traffic is compared to the NAT Connection Tracking table to see if it is matching an outgoing request. If there is no match the packet is dropped.

Starting with Lightning-Linux 3.5, when the SecureWall drops a packet a syslog message can be sent to indicate that unrequested traffic has arrived at the selected interface. This message can have a customized syslog level and text (for instance "dropped packet").

With the SecureWall active (it is activated by default in all Easy Setup configurations) outgoing traffic is allowed to pass out of the selected interfaces but only exact responses to that traffic are allowed back in. This simple yet powerful feature protects your network from incoming attacks or hackers. To add additional security you can also activate the Stateful Packet Inspection (SPI).

Virtual IP

A popular use of NAT is to redirect multiple IP Addresses arriving at the WAN interface to different servers on the LAN or DMZ. Multiple IP Addresses are received from the ISP with one being assigned to the MultiCom Firewall and the others used as an IPSec gateway point or to access different servers (such as web, email, news, ftp or other services.) All traffic to the Virtual IP addresses can be redirected to an internal server or selected traffic.

You may also need to use the ARP Proxy to correctly configure access to the Virtual IP addresses.

CAUTION - when NAT is activated all outgoing traffic will receive the WAN's official IP address unless there are additional NAT rules changing this.

Load Sharing

One possible configuration of the NAT services allows you to redirect data randomly to a range of machines, otherwise known as load-sharing. Typically all of the servers will be mirrors of each other. This allows CPU intensive operations such as searches to be distributed over a group of servers.

This is useful when you want to share the workload over similar servers. One possibility would be a group of web servers that do lengthy searches for web users. Instead of only having one machine doing all of the work, it is possible to send the same request for searches to other duplicate servers.

For example a destination IP addresses can be mapped to 10.0.0.11-10.0.0.15 you have chosen five possible hosts 10.0.0.11, 10.0.0.12, 10.0.0.13, 10.0.0.14 and 10.0.0.15. This means that whenever a packet is to have the destination IP address translated it will always pick randomly between those five addresses, effectively sharing the load. This is also known as round-robin load sharing.

> TIP — This feature allows you to direct incoming traffic to multiple servers or redirect all of your traffic through a selected group of port addresses for security.

This can also be done with the port addresses, you choose a range of ports and those are the ones that are randomly chosen by the firewall to be put into the data's packet header.

When you tell the firewall to pick from a range of port addresses you are limiting your outgoing communication to that range and hence can plan your network security around communication within that range of ports.

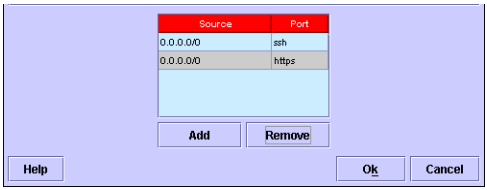
Remote Access

When the SecureWall is active it is not possible for remote access to the secured network or the MultiCom Firewall. In some cases it may be necessary to open a hole in the SecureWall for remote troubleshooting or updating. In this case the administrator has 2 options:

- Deactivate the SecureWall temporarily (least secure)
- Use the Remote Access Wizard to open an HTTPS or other port

Remote Access Wizard

This wizard allows the user to quickly open a hole in the SecureWall for remote administration. It is located in the Configurator software under the Wizard menu. When activated it will add entries to the NAT input table of the current WAN interface or WAN PPP site to allow remote users to configure MultiCom Firewall.



By clicking ADD the default suggests allowing access from anywhere in the Internet just to the WAN/PPP interface. This connection is secured by HTTPS and the incoming user still needs to authenticate with a valid username and password before they will have access to the MultiCom Firewall.

Access to the MultiCom Firewall can also be configured using the insecure HTTP or the SSH Telnet. If the user knows the IP address of the incoming remote access it is recommended to enter this IP address under the Source parameter with a "/32" at the end of it.

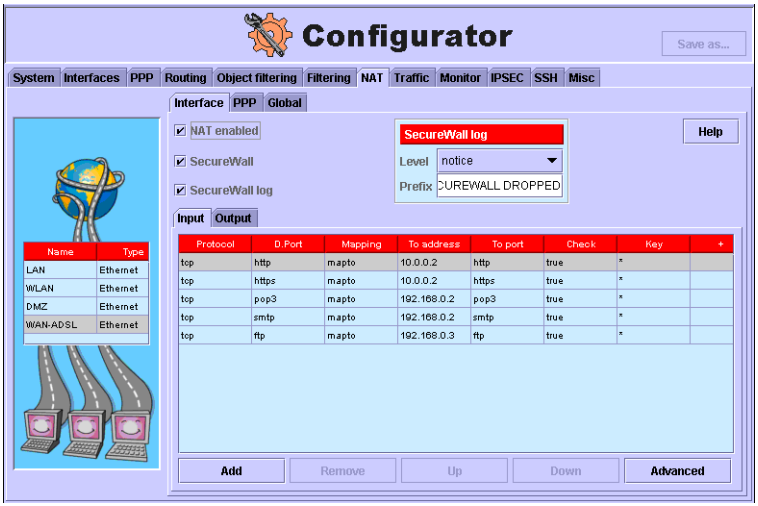
NOTE - filtering can also block the remote access. If there are problems connecting to the MultiCom Firewall then you may need to temporarily deactivate the Filtering.

Interface NAT

To reach these options go to the NAT Panel > Interface tab of the Configurator software, as shown below. Here you can choose which interfaces will have NAT activated, whether or not to use the SecureWall on interfaces using NAT, and if SecureWall is being used, whether or not to use the syslog notification of dropped packets.

Configuring NAT For Interfaces

By adding NAT Input rules to a specific interface you allow traffic to be allowed through the NAT firewall (if activated) and are translating only data packets that are arriving on this specific interface. This is especially useful if you need to make specific holes in the NAT firewall for external access such as for remote configuration or access to an internal server.



Normally if access was requested to the firewall from the Internet the firewall would refuse access (if enabled.) By using NAT rules access can be allowed through specific ports.

Below are the steps needed to configure remote access to your firewall when the firewall is enabled. This configuration is adding NAT access rules on the WAN interface to both telnet and web services but it could also be used with any PPPoE NAT interface.

1. goto the NAT panel of the Configurator
2. select the Interface tab
3. select the WAN interface
4. be sure to enable the NAT enabled and optionally the Securewall (firewall)
5. click the Add button under the Input table
6. under the Protocol column select TCP

7. under the D.Port column type 2000
8. under the Mapping column select “internal”
9. under the To port type 80
10. click the Add button under the Input table
11. under the Protocol column select TCP
12. under the D.Port column type 2323
13. under the Mapping column select internal
14. under the To port type 23

That is it, you can now save these rules to your MultiCom Firewall. The two above rules allows access to the web server and telnet server of the firewall.

Although Securewall would normally block all unrequested access from the Internet (WAN network), a request for port 2000 would not only be allowed through but also be mapped to the firewall via its port 80. This allows you to have remote access via port 2000 for remote configuration or monitoring of the firewall. In your web browser you could access the firewall with its IP address and ":2000" added to the end such as http://193.247.134.2:2000.

The access method for the telnet server is the same. Assuming your WAN IP address was 193.247.134.2 you could access the telnet server on the firewall by typing telnet 193.247.134.2:2323.

CAUTION - These open ports are effectively holes in your firewall that should be secured by either specifying the IP address they are allowed to be used from and/ or enabling additional filtering rules to block unwanted access.

Configuring Virtual IP

Common Virtual IP Decisions

To successfully configure Virtual IPs you will need to answer a few questions

- Are you only using the single IP Address that your WAN interface receives?
- Will both the WAN and LAN need to use the Virtual IP or simply the traffic arriving from the WAN?

- Do you need Proxy ARP?
- Will replies or other traffic from the LAN or DMZ servers need unique IP addresses or can it share the WAN IP address?

SINGLE IP ADDRESS: If you are only using a single IP Address you do not need Virtual IP addresses. All you need to do is redirect different services based on their port numbers to different servers on the LAN or DMZ. The easiest way to make this configuration is to use the Easy Firewall Wizard in the Configurator software. This is the quickest way to make the necessary rules (filtering and NAT) to redirect traffic to different servers on your LAN and DMZ. See "Easy Firewall Filter Panel" on page 400.

WAN AND/OR LAN ACCESS: If you are using multiple IP Addresses you have 2 choices to configure which IP traffic will receive the NAT redirection.

- WAN ONLY: Add those IP addresses to the NAT Interface WAN Input table. Click "advanced", deselect the "check destination" box and enter in the IP Address to be redirected and the internal IP address to receive the packets
- LAN and WAN: Just activate NAT on the LAN and WAN interface and enter in the redirection rule in the NAT > Global table. All data entering the LAN will look as though it is coming from the LAN interface of the MultiCom Firewall

If you wish to test your Virtual IP from the LAN interface you will need to activate NAT on the LAN interface and enter either a NAT Input rule on the LAN interface which is the same as exists on the NAT Input rule on the WAN interface OR, make NAT redirection rule in the Global Table for the Virtual IP Address.

USING PROXY ARP: If using more than 1 IP will you be using Proxy ARP unless the ISP add routes to their routing table (directing the other IP Addresses through the IP Address of the WAN interface of the MultiCom Firewall?)

When deciding whether or not to use Proxy ARP you need to know how your WAN Interface is configured.

If the WAN is using PPPoE, your provider simply adds another IP address to come into your account. Note that the WAN itself will officially be only one of these IP addresses and NAT will be needed to redirect the 2nd IP address to the correct location. Proxy ARP is not needed.

If the WAN is a Static IP Address or is using DHCP you will need to activate Proxy ARP to have the WAN interface respond to requests for 1 or more additional IP Addresses. Note that the WAN itself will officially be only one of these IP addresses and NAT rules will be needed to redirect the 2nd IP address to the correct location.

To activate Proxy ARP simply go to the WAN Interface window, select the ARP Proxy tab, activate Proxy ARP and select either dynamically generated Proxies (taken from the NAT Input table) or manually enter in the IP Addresses to receive Proxy ARP.

NOTE - if creating more than 1 Virtual IP Address and using Dynamic Proxy ARP your NAT rules must be in the NAT Interface Input table (usually the WAN). This automatically creates the PROXY ARP entries based on the NAT rules in the Interface Input table. Otherwise you will need to manually add IP Addresses to use Proxy ARP.

MAPPING OUTGOING TRAFFIC: If using more than 1 IP Address, will the packets leaving the internal servers (on the LAN or DMZ) need to identify themselves with their original IP Addresses or with one of the Virtual IP Addresses? By default the WAN interface with NAT activated will masquerade all traffic leaving on its interface. In many cases this is okay but some software uses the source IP address for authentication and when data arrives seemingly from another IP address (for instance the “Official” WAN IP address) the software may not accept the packet.

If this is not desired WAN Interface NAT Output rules will need to be added to either not map traffic from these servers (only useful if the LAN or DMZ servers have actual Internet IP Addresses) or be specifically masqueraded as the Virtual IP Address that they are pretending to be. For instance a "nomap" rule could turn off NAT for traffic from a particular server or the MISC NAT table can use "mapto" to change the source to the 2nd virtual IP address depending on which server on the LAN/ DMZ sent the packet.

Global NAT

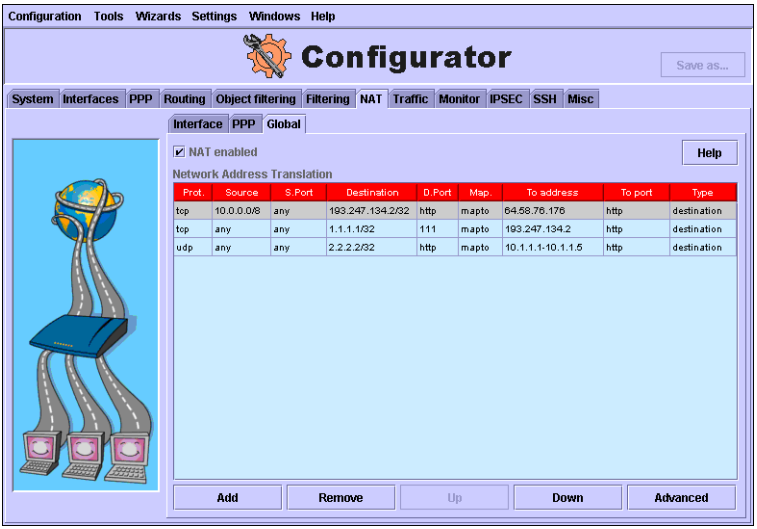
Network Address Translation remaps parts of the data packets header before passing it through the firewall. Data coming back in response to these translated responses, in turn are translated back so the original device can receive the response to its query. NAT can be applied to specific interfaces or globally (MISC Panel > NAT tab). Using NAT allows servers in your LAN to be accessed from the public network.

For example you could register 3 different IP addresses for three different companies but have them all served by the same Web server in your network.

By picking source and/ or destination information to qualify packets of information you can redirect them to the firewall, have the packets masquerade as though the MultiCom Firewall WAN, LAN, DMZ or PPPoE interfaces was the source of the data, or specify an IP address and /or port address to pretend the data was from or going to somewhere else.

Global NAT Settings

Global settings for NAT are found in the Configurator under `NAT>Global`. This NAT is almost the same as above except they apply to all data passing through the MultiCom Firewall to another network (such as the Internet). You have all of the options mapto/ masquerading/ and internal but when using mapto you get an additional option.

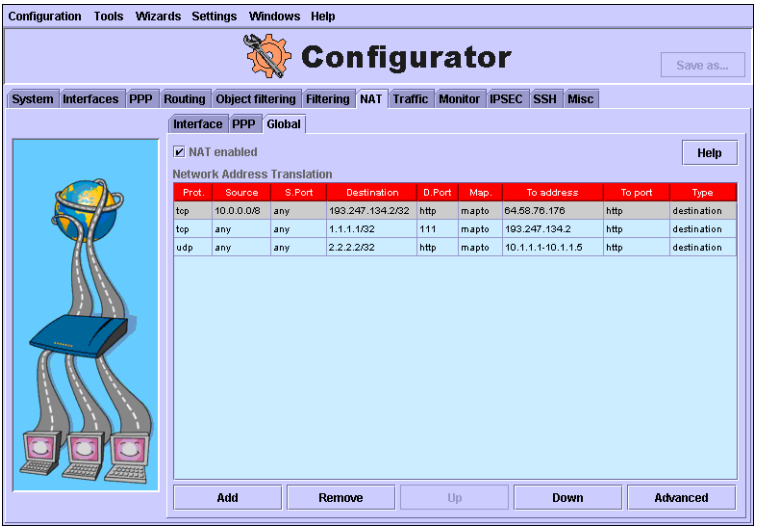


When using the global NAT setting and mapto you get to choose which part of the data header is to be translated. The choices for translating are source, destination and localsource.

NOTE — When you choose masquerade in the global NAT settings you are changing selected data to make it look as if it was sent from the port the data will leave the firewall from.

Configuring Global NAT

Global NAT rules offer a convenient way to redirect packets to other resources. This is also referred to as Port Mapping because you can choose specific ports to watch for packets and when found change the destination of where they are going to. This is helpful to hide commonly used port addresses from hackers, redirect web traffic through a proxy server or another website, and make remote computers appear to be on the same network as a local subnet.



By entering Global NAT rules you can translate any data packets that move through the firewall in either direction. One application of this is redirecting both internal and external visitors to a specified web server.

Below are the steps needed to configure network translation and port mapping for data moving through your firewall. In both cases you are redirecting data packets to somewhere other than where they were first sent to.

1. goto the NAT panel of the Configurator
2. select the Global tab
3. be sure to enable the NAT enabled button
4. click the Add button
5. under the Protocol column select TCP
6. under the source column type 10.0.0.0/8
7. under the Destination column type 193.247.134.2/32
8. under the D.Port column type 80
9. under the Mapping column select mapto
10. under the To address column type another website IP address (for example 64.58.76.176)
11. under the To port column type 80

12. under the Type column select destination
13. click the Add button again
14. under the Protocol column select TCP
15. under the Destination column type 1.1.1.1/32
16. under the D.Port column type 111
17. under the Mapping column select mapto
18. under the To address column type another website IP address (for example 193.247.134.2)
19. under the To port column type 80
20. under the Type column select destination

That is it, you can now save these rules to your MultiCom Firewall. The two above rules redirect access to web servers.

To test the first rule open your web browser and type in http://www.lightning.ch as the web page that you wish to open. Your computer should goto its DNS server and retrieve the 193.247.134.2 IP address for Lightning's website. Next your packet will be sent through the firewall with this IP address in the header.

When the firewall gets the packet it sees the 193.247.134.2 as matching one of its rules and instead redirects the packet to the specified IP address of another web server. Although you will see http://www.lightning.ch in your web browser you will see a different web page. This rule also only will translate for packets originating in the 10.0.0.0/8 network (by default your LAN network). This rule would not translate packets coming from the Internet.

The second rule makes up a fake web address and only redirects it when it matches the set port address for the destination. To test this rule, open your web browser and try going to the IP address http://1.1.1.1. You should not be able to find this. Next try going to the IP address http://1.1.1.1:111 (adding a specific port address). Now the MultiCom Firewall will see a packet matching its Global NAT rule and redirect it instead to port 80 of the IP address you specified.

Proxy ARP

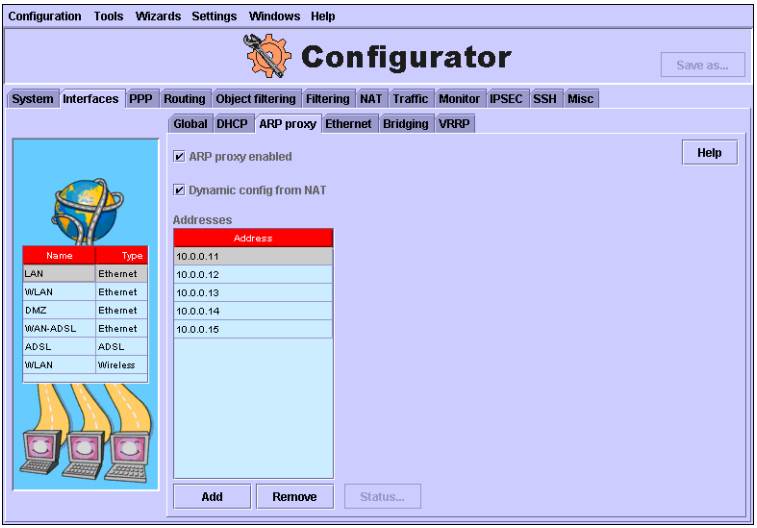
Starting with Lightning-Linux 3.3 Proxy ARP is available to assist with configuring Virtual IP addresses. When configured with an IP Address Proxy ARP acts as though it is that IP Address by responding to ARP requests.

This feature is typically used when a user receives more than one IP Address from their ISP. One of the addresses is given to the MultiCom Firewall and the other addresses are configured to be redirected to internal servers either on the LAN or DMZ networks of the MultiCom Firewall. Proxy ARP makes it seem like all of the IP Addresses are lined up on the same network when in fact only one IP Address is (the WAN interface for the firewall.)

Without Proxy ARP, it is still possible to use virtual IP Addresses but the ISP must add routes in their routing tables (which some ISP's may not be willing to do.) Proxy ARP is the recommended solution when creating Virtual IP Addresses.

Configuring Proxy ARP

Proxy ARP can be configured for any physical interface (PPP connections do not use Proxy ARP).



Available options include:

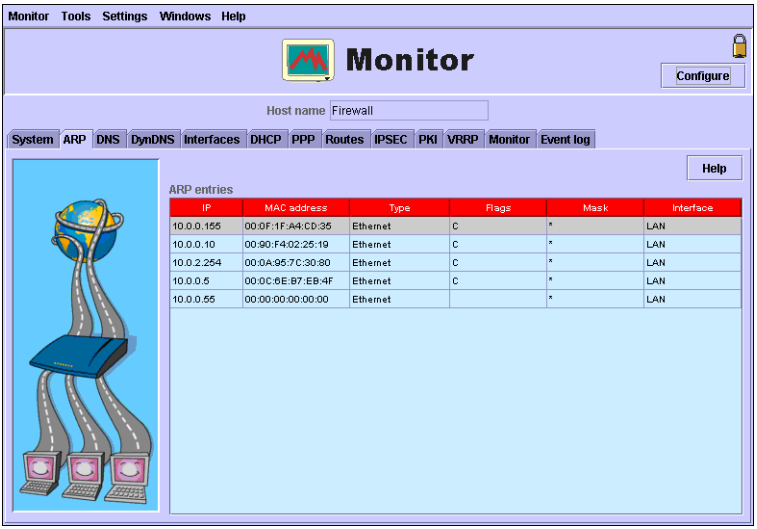
- enable/ disable Proxy ARP for the selected Interface
- dynamically create Proxy ARP by checking the NAT Input table for IP redirection rules on the selected interface

- manually enter Proxy ARP IP Addresses for the selected Interface

To use simply activate Proxy ARP (usually on the WAN interface) and either manually add the IP Addresses that will be proxied (that the MultiCom Firewall will pretend to be) or select “Dynamic config from NAT” and the rules will be created from your NAT Input table when you save your configuration to the MultiCom Firewall.

Monitoring Proxy ARP

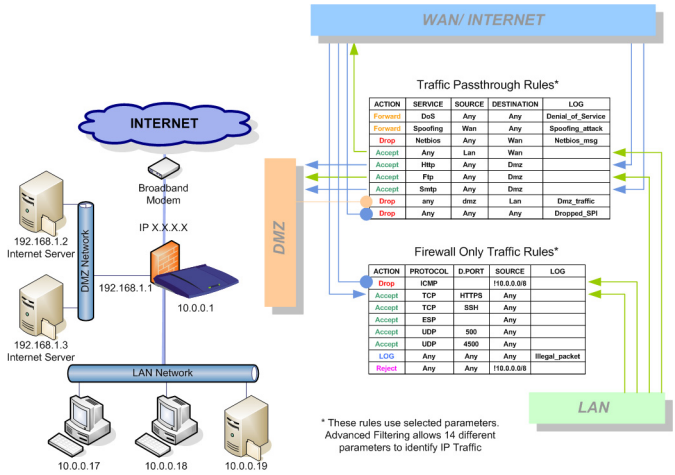
Using the 3.3 Configurator or later allows users to view the active Proxy ARP rules for each Physical Interface as shown below. For more information about this screen please see“ARP Proxy Monitor” on page 539.



Chapter 10

Stateful Packet Inspection

Stateful Packet Inspection - SPI is a rigorous method of controlling access to and through the MultiCom Firewall. This technology provides the second wall of protection for your network, the SPI Filtering Firewall or SPI Firewall. It can be used together with, or independently from the SecureWall.



Filtering Data Packets

Filtering is the act of matching each data packet against preset identifiers or flags and corresponding rules. The rules say what to do with the particular data packet when it matches the specified identifiers. These actions can be to accept, reject, drop, forward, or simply log the data packet as having arrived at the firewall.

Below are the common types of identifiers you can use to choose the data that is filtered...

- Source and/ or Destination IP Address
- Source and/ or Port Address
- Type of IP protocol
- Number of packets per second
- Related traffic

Rules are set in a hierarchy where the first rule the packet matches is the one that causes an action to occur. For instance, if the first rule that you used was to deny all data packets then every further rule would never get used since the first rule takes precedence.

> NOTE - A common mistake is to insert a rule for a type of data when actually an earlier rule denied it already. Be sure to take into account the previous rules when adding a new one.

Because there are many combinations possible it is a good idea to decide what you want to do first. Then you look for the identifiers that will always be associated with your goals.

- Does the type of data you want to filter or log only come in from the LAN or WAN port?
- Does the data use a specific port for communication?
- Does the data come from a specific machine with a static IP address?

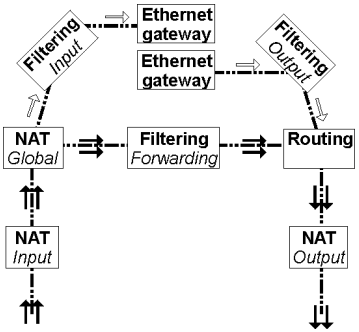
For instance if you wanted to only allow incoming web access you could make a rule such as

- allow incoming to port 80
- deny all incoming

The first rule allows in the data with a destination of port 80 — the common destination when looking for a web site server. The next rule says that if the data packet does not find a previous rule that it matches that it will be denied.

Packet Flow

Before you jump into the advanced configurations please spend a moment to familiarize yourself with the way data packets traverse the firewall (as seen in the graphic below). Changes made in a previous area of this path will become part of the identifier for later changes.



Also note how the change in origin and destination of a packet affects the order of services it will pass through.

Filtering Tables

There are 5 filtering tables that are used with the MultiCom Firewall. Each table has different characteristics from the others but each will use the same syntax for building filtering rules (except for the Object Filtering table which works with objects.)

Using different tables allows you to create rules that target a specific activity and saves in processing time by the firewall as data traffic are only affected by relevant rules.

Object Filtering

The Object Filtering table is a simple way to design filtering rules with your firewall. Rules are built using default or customized objects. These objects allow for quick rule building such as from LAN_Network to ANY Web_HTTP Allow. For more advanced functionality there are the 4 other Filtering tables.

Forward Filtering

The Forward Filtering table is used for rules which target all data that traverse the MultiCom Firewall, moving from one network to another. An example of this type of data activity is all interactions with the Internet - web browsing, file transfer, streaming media, telnet, email to name a few. Filtering rules in this table can affect this type of data.

Input Filtering

The Input Filtering table creates rules targeting data packets that are directed at the MultiCom Firewall itself. For example, accessing the built-in web server, telnet server or pinging an interface is considered data directed only at the firewall and not the networks around it.

Output Filtering

Output Filtering tables are used for rules which target data packets which leave from the MultiCom Firewall. For example, responses to pings, the monitoring data that is sent to the Configurator software, and the web server pages sent to a browser. Data that is from one of the connected networks is not considered in Output Filtering rules.

User Filtering

Filtering rules located in the User Filtering table are of a special sort. These are filtering groups contain one or more individual filtering rules and each group contains a unique name. These rules are not used unless a rule from the Input, Output or Forward Filtering tables sends a packet to a specific group.

This allows the user to simplify rule creation and not have all rules active at once. For example, one group of User Filter rules could be called “Drop Bad Data” and contain 50 rules. A user could then make a single rule in

each of the Input, Output and Forward tables saying that all data packets must first go through the “Drop Bad Data” group of rules before being accepted. Instead of 150 rules (50 in each table) the user would only program 53.

Additionally, if there was some special testing being done it would not be necessary to turn off all filtering to avoid these rules, just delete the rule in each of the 3 tables which uses it and the group “Drop Bad Data” will be unused but still exist in the configuration.

Standard Filters Wizard

This wizard allows you to set default filtering rules to your LIGHTNING Firewall and reject common attacks like IP spoofing and. User filter rules will be added for IP spoofing protection, Denial-of-Service, incorrect TCP flags, NetBIOS Traffic, Active FTP attempts, and Aureate spyware using port 1975.

WARNING - All existing filtering rules will be deleted! They will be replaced by the default filtering rules as described in the Reference Manual.

Note that forward filtering rules generated by the object filtering and the Easy Firewall will be automatically added

---

These rules will be accessible through Forward Filter and Input Filter rules. The added rules will use the "forward" action to redirect traffic through these rules. In all cases a syslog will be generated before traffic is dropped.

WARNING - the IP spoofing rules blocks traffic arriving on the WAN/PPP interface that says it was sent from the 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 subnets. This is okay for normal Internet security but if you are using the MultiCom Firewall inside a network or to make VPN’s to remote networks that use those subnets, you will have to disable them.

Using Ports

Because each IP address can be communicated to through more than 65,000 different ports (similar to channels on a radio where each IP address can receive over 65,000 channels)

Table 1: Commonly Used Ports Description

PORT	SERVICE	EXPLANATION
20, 21	FTP	FTP servers can be used to store and retrieve files anonymously, possibly to transfer illegal or pirated software.
22	Secure Shell	This is a known port to be used for secure shell communications. You can consider changing the port address for this service to make it less likely that hackers will be aware that you are running it. For the client it allows remote ssh access and for the server it allows incoming ssh access.
23	Telnet	Telnet services allow remote access to servers. Hackers may try to exploit this capability with stolen passwords or scanning attempts to recognize the services available.
25	SMTP Mail	SMTP mail services can be exploited as a relay point for spammers.
43	Whois	This service is used to request "whois" information about your computer
80	Web/ http Services	Unauthorized access to internal web servers can allow sensitive information to be seen (in the case of intranets), and possibly allow remote users to take advantage of weaknesses in the web server. Allowing outgoing web access can use bandwidth or encourage non business use of company resources.
110	POP3 Mail	Used when either you are serving POP services or you have users retrieving their email from a remote POP server (commonly an Internet Service Provider). As with many services there are vulnerabilities to using this service such as a crashed email server caused by sending to much information or illegal access to user name and passwords possibly opening holes for access.

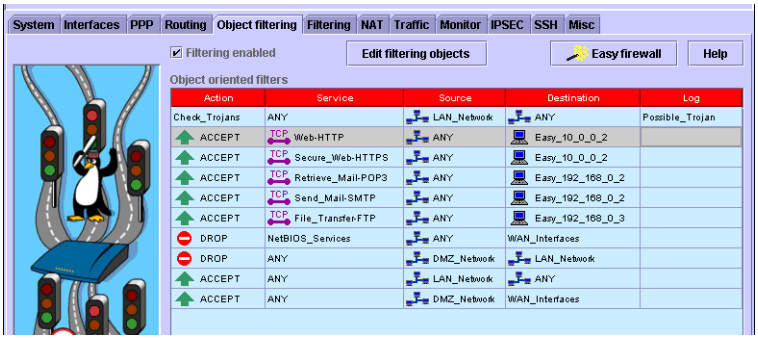
PORT	SERVICE	EXPLANATION
113	Identd Auth	This service is used to identify users of a TCP connection. While it offers information a hacker could exploit it is also used by numerous services such as mail, ftp, irc to assist in identifying the users. If you have users trying to access these services you will see incoming connection attempts on this port as the remote server tries to authenticate the user. Simply dropping incoming requests on these ports may cause slow connections as the remote server keeps trying to identify the user. Rejecting the request allows a message to be sent back to the remote server which prevents the above mentioned stalling.
119	Usenet News	If your news server is open to anyone then anyone can post, read anything in the groups. This access may allow undesirable visitors to use the service
123	Network Time Service	This service is used to spread the same time parameters throughout the network, often retrieved from a remote, central time source.
143	IMAP4 Mail	This mail service has similar vulnerabilities to the POP3 service. Crashes of an email server could be caused by sending to much information, possibly opening holes for illegal access.
443	SecureWeb/ https Services	If you want your users to be able to use this service then this port must be left open for the https secure sites to work correctly.
2049	NFS	This is the port that the NFS program runs on. It is generally used for LAN purposes and opening it up to the Internet could risk hacker attacks.
4000	Internet Chat	This is another chatting service frequently referred to as ICQ.
6000+	Xwindows	This is the port that an X windows server begins opening for each remote X window session that is requested. Unless you need this service to be opened over a remote connection consider blocking port 6000 or at least consider identifying which IP addresses can have this access.
6667	Internet Relay Chat	This service allows users to utilize the IRC chatting often used on the Internet.

PORT	SERVICE	EXPLANATION
ICMP	Ping	While this service is very useful for identifying whether a computer is working or not remote pings can be used in denial of service attacks and/ or discover IP addresses of your network.
ICMP	Traceroute	While useful for gauging the speed and accessibility of different routes it can be used to flood networks with messages. Denying traceroutes to your internal computers may be a security consideration.
ICMP	Destination Unreachable	These messages are used to say a remote system is unreachable and to negotiate acceptable fragment size of data communication. Be careful if you wish to disable this message as other services frequently use it.

Filtering Objects

Starting with Lightning-Linux 3.1 it is now possible to design advanced filtering rules within a simple table. Using predefined objects (networks, services, actions and logging rules) you can quickly build a customized firewall to protect your network.

The Configurator software comes with some predefined objects such as your LAN, WAN or DMZ network. Additionally there are a list of commonly used Internet services available for you to configure. You also have the option of defining your own custom objects which will be saved with your config file to the MultiCom Firewall.



Filter Object Overview

To configure filtering you must make rules which identify IP packets and the identify the action to occur when such a packet is found. The identity of the packet is based on certain parameters found in all IP packets. The action will be to accept or reject the particular IP packet that matches the recorded identity.

Object Filtering uses the following objects categories to create filtering rules.

- **source**: specify the source of the IP traffic
- **destination**: specify the destination of the IP traffic
- **service**: specify the service to be filtered
- **action**: specify the action to be undertaken for the identified IP traffic
- **log**: specify a custom log message to occur at the same time as the action

Building Object Filter Rules

To use make custom Object Filtering rules the user will need to open the Configurator software and select the Object filtering panel. A rule is defined by selecting from the object categories. Rules are traversed from the top down so if the first rule was to drop all IP packets then any following rules would be ignored.

By moving rules up or down in the Object filtering table the order can be changed by the user.

Table 2: Object Filtering Sample

Source	Destination	Service	Action	Log
LAN_Network	WAN_Network	Web-HTTP	ACCEPT	
LAN_Network	WAN_Network	Retrieve_Mail-POP3	ACCEPT	
*ANY	ANY	ANY	DROP	

*This final rule is *automatically* added to the end of generated Object Filter rules. This means that if the IP packet has gone through the above rules and not been accepted it will be dropped.

With rules as shown above you have just limited your entire LAN network to only use web browsing and retrieving email. Any other type of service request would be dropped.

The Configurator takes these rules and enters them into the Filter Forward rules table, always starting after any existing rules in that table. This means that if you already have rules in the Filter Forward table the Object Filter rules will be added after them. These Object Filter rules are identified with an "*" in the Obj field of the Forward Filter table. These rules are regenerated when a configuration is Applied.

For each of these events you can also add a customized syslog message to be sent when any of your Object Filtering rules is activated.

NOTE - Be sure to enable the Object Filtering enabled button when you want to use these rules.

Customizing Available Objects

While there are default objects available, additional objects in these categories can be defined by the user.

New objects are created in a separate table for each category of objects. Each object is distinguished by a unique name to identify the customized parameters entered by the user. It is this name that is used to when configuring object filtering rules.

All of the objects and rules being used in a given configuration are stored directly in the configuration file. This means that a remote administrator can simply load the configuration and have all of the objects available, even the ones that are not being used.

Network Objects

Network Objects make it possible to represent a network IP address, IP subnet, or a particular machine (host) on an IP network. This object is typically a user's computer, a network's subnet, a network server, or other device like a networked printer or hard disk. Object filtering allows users to filter data coming from or going to these objects or their subnets. The following parameters are used to define a Network Object.

- **Name**: used to identify a particular Network Object or list
- **Subnet**: represents an IP address and a subnet mask of a machine or network
- **Interface_Network**: represents a network being connected to a specific

interface on the MultiCom Firewall.

Predefined Network Objects

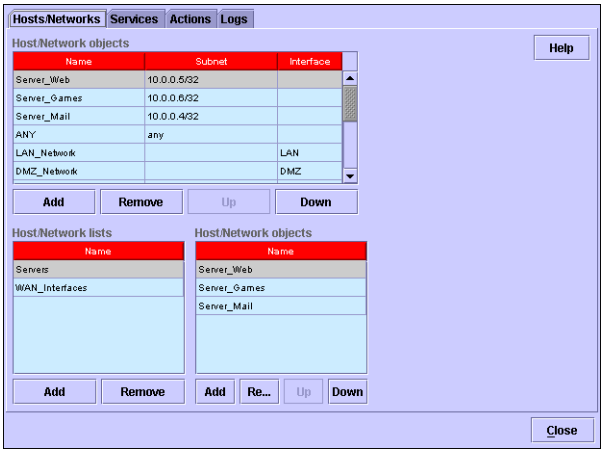
There are some predefined Network Objects that are available in default configurations. These objects can be modified.

Table 3: Predefined Network Objects

Name	Subnet	Interface_Network
ANY	0.0.0.0/0	
WAN_Network		WAN
LAN_Network		LAN
DMZ_Network		DMZ

Building Network Objects

It is possible to build new Network Objects in a configuration file with the Configurator software. After clicking on the Edit filtering objects button of the Object filtering panel select the Hosts/ Networks tab.



The Name attribute is a character string limited to 32 characters. The allowed characters are alphanumerical (ABC...def...123...) and the special characters “_” and “-”.

The Subnet attribute is a pair of values made up of an IP address and a subnet mask. The IP address is in the “dotted quad notation”, for example 192.168.1.0. The subnet mask can be either in the same notation or in CIDR format (number of masked bits from 1 to 32). The pair are separated by a “/”. A complete entry could look like 192.168.1.0/255.0.0.0 or 192.168.1.0/24. If no subnet is given the IP address is assumed to correspond with a single machine and will be given a netmask of 255.255.255.255 or in CIDR format /32.

The Interface_Network attribute is the name of an interface (LAN, WAN, DMZ) or an existing PPP site. One predefined object, ANY, is used to associate with any IP address, i.e. all of the Internet without distinction.

NOTE - If you select an interface in a Network Object, you cannot select a subnet mask as it will be the subnet mask in use by that interface.

Service Objects

A Service Object represents a service which corresponds directly with TCP/ UDP port number. Such services like http web browsing, email pop3 and others are available as defaults but the user may define other services. This object is used to identify IP packets going to or coming from this port number. Additionally, this category is also used to identify types of ICMP packets. The following parameters are used to define a Service Object.

- **Name**: used to identify a particular Service Object or list
- **Protocol**: associates a particular protocol (TCP, UDP, or ICMP) to the service object
- **Port**: represents the TCP or UDP port corresponding to the service to be filtered, not available when configuring an ICMP service
- **ICMP type**: allows the configuration of different ICMP types

Predefined Service Objects

There are some predefined Service Objects that are available in default configurations. These objects can be modified.

Table 4: Predefined Service Objects

Name	Port/ ICMP_Type	Protocol
ANY	0-65,635	ANY
Web-HTTP	80	TCP
Secure_Web-HTTPS	443	TCP
File_Transfer-FTP	21	TCP
Secure_Shell-SSH	22	TCP
Telnet	23	TCP
Domain_Name_System-DNS	53	UDP
Send_Mail-SMTP	25	TCP
Retrieve_Mail-POP3	110	TCP
Internet_Message_Access-IMAP	143	TCP
News-NNTP	119	TCP
Network_Management-SNMP	161	UDP
Ping-Echo_Request	8	ICMP
Ping-Echo_Reply	0	ICMP
NetBISOS_Name_Service-TCP	137	TCP
NetBISOS_Name_Service-UDP	137	UDP
NetBIOS_Datagram_Service-TCP	138	TCP
NetBIOS_Datagram_Service-UDP	138	UDP
NetBIOS_Session_Service-TCP	139	TCP
NetBIOS_Session_Service-UDP	139	UDP
NetBIOS_Services	137-139	TCP,UDP

There are also some predefined ICMP types. These cannot be changed.

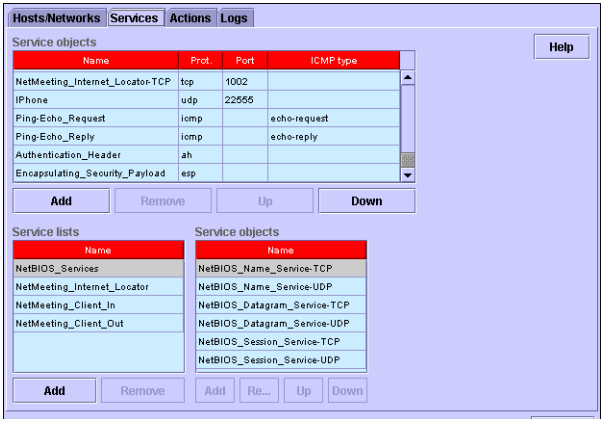
Echo reply (0)

Destination unreachable (3)

Echo request (8)

Building Service Objects

It is possible to build new Service Objects in a configuration file with the Configurator software. After clicking on the Edit filtering objects button of the Object filtering panel select the Services tab.



The Name attribute is a character string limited to 32 characters. The allowed characters are alphanumerical (ABC...def...123...) and the special characters “_” and “-”.

The Protocol attribute is can accept TCP, UDP or ICMP to designate the type of protocol being used by the filtered IP packet. Additionally there is an ANY option that instructs the filtering rule to not take into account what protocol the IP packet is using.

The Port attribute is only valid when the selected protocol is TCP or UDP. It can be a single number in the range of 0-65,535 or it can be a range of numbers separated by a “-”, for example 10-100 would be all ports between 10 and 100, including 10 and 100.

The ICMP_Type attribute is only available when the ICMP protocol is also selected. and allows you to pick from the list of predefined ICMP types.

Action Objects

An Action Object represents the action to be carried out on an IP packet that matches the filter rule. The following parameters are used to define an Action Object.

- **Name**: used to identify a particular Action Object
- **Action**: represents the action to occur with the packet, to Accept the packet into the network or Drop it without a response, or to Forward it to a predefined User Filter

- **Limit**: allows limiting of the number of IP packets accepted or rejected by the rule
- **Connection_Tracking**: allows the activation or deactivation of filtering of the IP packets according to the state of the connection
- **Allow_Related_Connection**: allows the activation or deactivation of filtering of the IP packets in relation to an existing connection

Predefined Action Objects

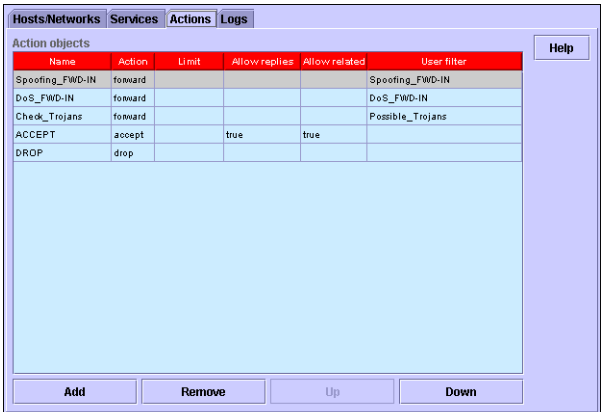
There are some predefined Action Objects that are available in default configurations. These objects can be modified.

Table 5: Predefined Action Objects

Name	Action	Limit	Connection _Tracking	Allow_Related_ Connection
Accept	ACCEPT	-	TRUE	TRUE
Drop	DROP	-		

Building Action Objects

It is possible to build new Action Objects in a configuration file with the Configurator software. After clicking on the Edit filtering objects button of the Object filtering panel select the Actions tab.



The Name attribute is a character string limited to 32 characters. The allowed characters are alphanumerics (ABC...def...123...) and the special characters “_” and “-”.

The Action attribute has three options: Accept, Drop, or Forward the filtered IP packet. In the case of forwarding the user must also select the User Filter table of rules to forward the packet to.

The Limit attribute is defined with a number of packages to be limited, a "/" and a time selection of seconds, minutes, hours or days. For example a definition of 10/h means 10 per hour. Optionally, this attribute can be left empty which implies that there is no limit on the number of accepted or dropped IP packets.

Connection_Tracking and Allow_Related_Connection attributes allow only a true or false value. They are available options when the protocol type is TCP or UDP and the Action is ACCEPT.

Log Objects

The Log Objects allow for notification by syslog messages each time the associated filtering rule is activated. By customizing the messages the user's syslog reports can contain specific text helping to find or track particular activity at the firewall. The syslog service must be configured to send syslog messages to a specified IP address if the messages are to actually be sent. The following parameters are used to define a Log Object.

- Name: used to identify a particular Action Object or list
- Level: is the level of the associated syslog message
- Limit: allows limiting of the number of syslog messages sent by the corresponding rule
- Prefix: a custom description which will be added to the beginning of the syslog message

Predefined Log Objects

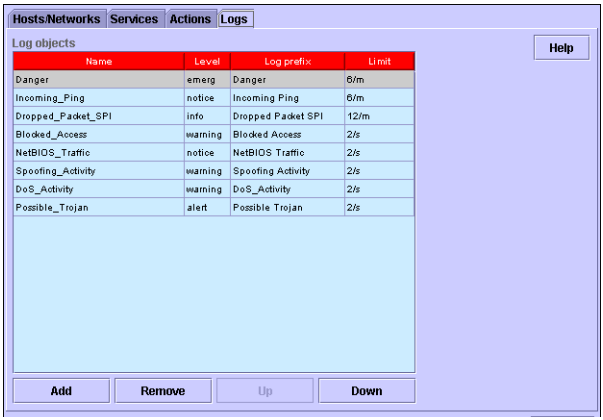
There are some predefined Action Objects that are available in default configurations. These objects can be modified.

Table 6: Predefined Log Objects

Name	Level	Limit	Prefix
Alert	Alert	1/ hour	
Warning	Warning	-	

Building Log Objects

It is possible to build new Log Objects in a configuration file with the Configurator software. After clicking on the Edit filtering objects button of the Object filtering panel select the Logs tab.



The Name attribute is a character string limited to 32 characters. The allowed characters are alphanumerical (ABC...def...123...) and the special characters “_” and “-”.

The Level attribute sets the Syslog level of notification for the filtered event. The options available are Debug, Info, Notice, Warning, Err, Crit, Alert, Emerg. These levels allow the user to assign a level of importance to the message.

The Limit attribute is defined with a number of packages to be limited, a “/” and a time selection of seconds, minutes, hours or days. For example a definition of 10/h means 10 per hour. Optionally, this attribute can be left empty which implies that there is no limit on the number of accepted or dropped IP packets.

The Log Prefix attribute is a customized character string of up to 28 characters long. This allows the user to enter a unique message to help identify or track the associated filtering event. For example, “Ping from the Internet”, “URGENT call Admin at ext 12”, “Attempted Access Blocked Web” are all possible custom messages that will be appended to the beginning of the syslog message.

Filtering Parameters

There are many advanced filtering capabilities included with your MultiCom Firewall. With these capabilities you will be able to customize your firewall and networking traffic to meet your specific needs. Below are some of the many IP identifiers you can use to match data packets with corresponding actions.

General Filtering Options

- source IP Address and netmask
- destination IP address and netmask
- port number or range of port numbers
- TCP/UDP/ICMP/ESP/AH/GRE protocols or all but the selected protocol
- filter action

Advanced Filtering Options

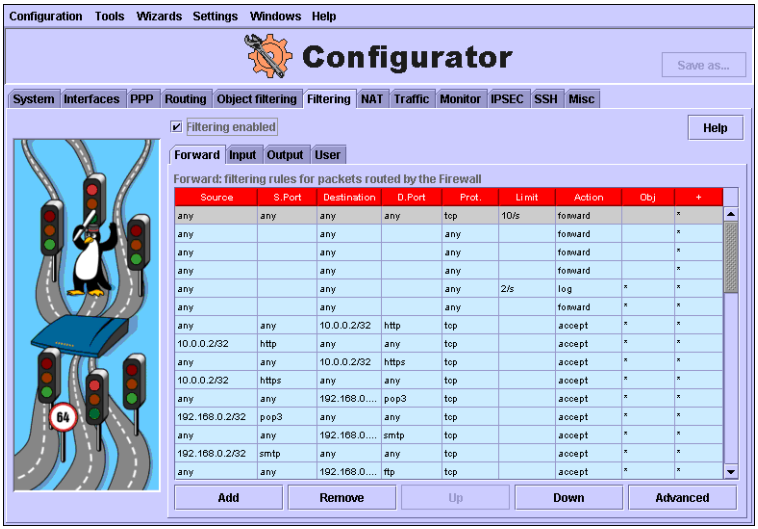
- which interface the packet arrived on
- TCP TCP options and flags
- tracked packet state information (established, new, related, invalid)
- ICMP packet type
- limit dataflow and burst levels

After identifying the data packets with the above choices you can choose an action to occur to each matching packet. These actions are to drop/ reject/ log/ forward/ return or accept the matching packets passing through the firewall.

Stateful Packet Inspection creates a table of packet types and associated actions. Every packet going through the firewall is matched sequentially against every entry of the table until a matching entry is found. The entries in the list are tested in descending order. Once an entry is found, the packet is either allowed through the firewall, rejected, dropped, forwarded or logged according to the action specified in the entry. If no matching entry is found, the packet is accepted.

If IP translation is in place, the filter is applied on the untranslated packet, i.e. before translation on outgoing packets and after reverse translation on incoming packets. See the graphic at the beginning of this chapter for the processes that traffic takes when passing through the MultiCom Firewall.

General Filtering Parameters



Click the Add button to add the current filter entry at the beginning of the list. The Remove button allows to remove the currently selected entry from the list. You can reorder the entries in the list with the Up and Down buttons to specify in which order the entries are processed.

Source and Destination

The source address and destination address are given as IP addresses in the `Source` and `Destination` fields. When both the `Source` and `Destination` fields are left empty, the entry matches any IP address. You can specify specific IP Addresses with netmasks to group large numbers of IP addresses. For instance 10.0.0.0/8 is all addresses from 10.0.0.0 to 10.255.255.255. Please read the “IP Subnetting” Section on page 525 for more information.

Ports

The Port field allows to specify the source port and the destination port of the packet as well as a range of ports. Leave this field empty or select the ANY value if all port values must match the entry. To specify a range of ports simply type X-Y where X is the lower end of ports to watch for and Y specifies the upper end of ports to watch for.

Protocol

Select the IP protocol to which the entry applies in the Protocol field. You can choose TCP, UDP, ICMP, ESP, AH, GRE or all of them. You can also select a port name with "!" before it. This "!" specifies any protocol but the one mentioned. For example !TCP means any protocol but TCP.

Limit

The limit field allows you to specify the maximum average number of matches per defined time period that will trigger the corresponding action to occur. This throughput limit is measured in frames (or packets) per second, minute, hour or per day. As long as packets matching all other parameters in the same rule as the limit and is within that limited time period then the action specified occurs on those packets.

For instance, you can specify that all web traffic (destination port 80) from a particular computer (source IP address) is accepted to a limit of 50/sec, which if exceeded will pass the packet to a second rule that causes the packets to be rejected. Now when the specified computer tried to use too much bandwidth its requests are rejected at the firewall, effectively slowing down the access so other users can also use the network.

In the advanced filtering settings you can configure this with more detail by selecting which interface these limits apply too you can limit traffic flows leaving (from the LAN port) or entering your network (from the WAN port). This prevents traffic from congesting your network or can be used to identify possible hacking attempts against your network.

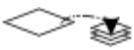
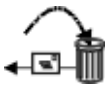
By using limits and filters you can shape IP traffic according to its type or limit overall throughput (such as limiting warnings of network flooding or slowing traffic to a set frame rate to a remote destination can support.)

CAUTION — While Ethernet packets can be as big as 1.5kb each this is the maximum limit only. Some programs, such as telnet for instance may send a separate packet for each character that you type hence your limits may have unexpected results such as blocking people who type too fast.

Consider either limiting communications that will probably use the full size such as ftp or web traffic if you want to limit their throughput. Otherwise checking frequency (packets per second) can allow you to set warnings or logs against possible Denial of Service attacks.

Actions

Table 7: Filter Actions

 drop — no notification	 forward — send to specified filter library
 reject — drop with ICMP notification	 return — return from library to main filters
 log — message to syslog server	 accept — let the data come in

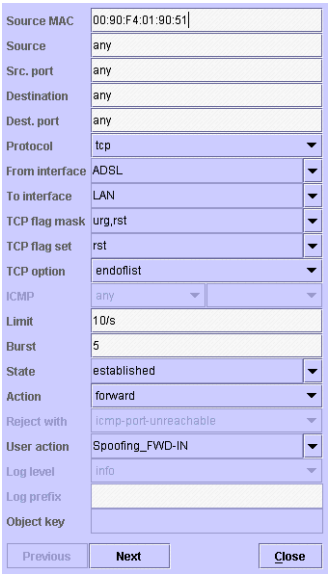
You must then choose an action for packets matching this entry: either drop/ reject/ accept/ forward/ log. Dropped data packets are discarded without any notice back to the sender, rejected packets also discard data packets but a message is sent back to the source IP address saying the packet was indeed rejected. Allow immediately allows the packet to pass through the firewall. Forwarding actually passes the data packet through the specified filter or filters in the filter library and if it has not found a matching rule there it is returned to the main filtering list.

It is possible to send a syslog notification on every possible filtering rule, for intrusion detection or statistical purpose. The syslog service must be configured to send syslog messages to a specified IP address if the

messages are to actually be sent. Using the LOG action does not accept or drop/ reject a packet. Once the syslog message has been sent the packet will continue down the list of filters to search for a matching rule.

Advanced Filtering Parameters

After having started a new filtering rule you can click on the advanced button to access the advanced filtering options. This gives you many more parameters with which you can identify your data traffic.



By identifying which interface the data arrived on (LAN or WAN) you are able to segment data coming from the WAN or LAN parts of your network. This allows you to focus certain rules based on the source of the data packets.

With TCP flag mask you identify which flag components to be watching for urg, ack, psh, rst, syn, fin or any combination of them. These flags are typically used in the setting up and closing down of TCP connections and are either on or off in the arriving data packet.

The TCP flag set is where you set which masked TCP flags (the ones you were watching) need to be set or active to cause the action of the filter to occur. For example you could say watch syn, psh, and urg and then set TCP flag set to activate when the syn flag was not set and psh and urg flags were set. When this type of packet is found the action chosen for the rule will be applied to that packet.

CAUTION — Be sure to only choose set flags that were also chosen above in the TCP flag mask field, otherwise you will be waiting for something that would never be watched.

Consider the TCP flag masks as the fields to watch and the TCP flag sets as the particular sequence that needs to occur. Also, setting TCP flag filters is a very advanced option, be sure to test your configuration to be sure it acts the way you want it to.

Identifying TCP TCP options such as no check, end of list, no operation, maximum segment size, window scale factor, and time stamp allows you very detailed tagging of the packets traversing the firewall. You may also use the "!" to specify all options but the selected one as in "!nocheck" which means any TCP option but "nocheck".

With the advanced filtering you can specify the exact type of ICMP data packet to trigger an action. This messaging protocol is frequently used to identify network errors, congestion as well as supporting the popular "ping" activity.

An optional filtering identifier that works in tandem with the "limit" parameter. Burst specifies the maximum burst of data packets allowed in the traffic flow before the associated limit parameter takes affect. The value is X where X equals the number of packets to match the associated rule before the limiting takes effect. By default this number is 5. This can help allow the typical bursty Ethernet traffic get through when a limit might otherwise block too much traffic.

By entering information on the packet connection state such as whether it is new, established, related or invalid you can specify identification of data packets that are related to a particular connection type.

When you choose to reject a packet matching your rules you have the option of picking which type of ICMP message to use to notify the sender that the requested activity is rejected. The types of replies that you can send are:

Table 8: Packet rejection messages

icmp-port-unreachable	PROTO=ICMP TYPE=3 CODE=3
icmp-net-unreachable	PROTO=ICMP TYPE=3 CODE=0
icmp-host-unreachable	PROTO=ICMP TYPE=3 CODE=1
icmp-proto-unreachable	PROTO=ICMP TYPE=3 CODE=2
icmp-net-prohibited	PROTO=ICMP TYPE=3 CODE=9
icmp-host-prohibited	PROTO=ICMP TYPE=3 CODE=10
tcp-reset	PROTO=TCP ACK RST URGP=0

The default reply of icmp-port-unreachable will be sufficient for most network needs.

When you have chosen forwarding as the action for your filter you will also need to enter in the filter in the user library that you want to send the packet through. You can enter the name of this group of filters under the User Action field.

Finally, if you have chosen to log data as the action for your filter you can optionally choose the priority level of the message and/ or a comment line to identify the reason this syslog message was generated.

Connection State Filtering

The Stateful Packet Inspection (SPI) of the MultiCom Firewalls keeps track the connections going through the firewall and assigns each packets a state. These states are.

- NEW - a packet which creates a new connection.
- ESTABLISHED - a packet which belongs to an existing connection (i.e. which is a reply to an accepted request, or an outgoing packet on a connection which has seen replies.)
- RELATED - a packet which is related to, but not part of, an existing connection such as some ftp data connections or some ICMP errors.
- INVALID - a packet which could not be identified for some reason such as running out of memory or ICMP errors which do not correspond to known connections.

It is often easier to work with the states of connections in place of trying to manage which TCP flags are being used to identify the connection.

ICMP messages do not use connections as part of their protocol. For common ICMP traffic refer to the table below to see what state the data will be marked as when it reaches the firewall.

Table 9: Connection States of Common ICMP Traffic

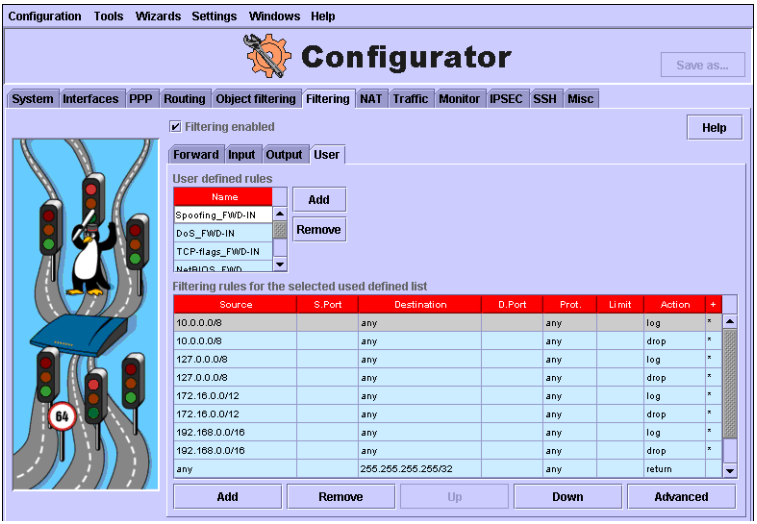
NEW	ESTABLISHED	RELATED
Echo_Request	Echo_Reply	Dest_Unreach
Timestamp_Request	Timestamp_Reply	Source_Quench
Info_Request	Info_Reply	Time_Exceeded
Address_Mask_Request	Address_Mask_Reply	ParameterProb
		Redirect

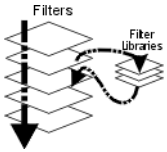
UDP is also a connectionless protocol but in some cases the data packets will react in a connection like manner in which case they will be assigned states. For instance when a workstation requests DNS information via a UDP packet to port 53 the request is tagged as a NEW state and the reply from the DNS server is tagged as ESTABLISHED.

Filtering User Library

The filtering library is where you can store groups of filters that you may not want always activated or that only specific types of data should traverse. The commands are the same as for the previous filtering options except for the following exceptions.

- There is a name for the group of filtering rules.
- Data is only sent to a group when a forwarding filter rule has the action of forward and uses the name of the group of filtering rules.
- There is an additional action called return which immediately returns the data packet to the main forwarding filter table so that it can continue through other filters.
- If there is no matching entry found that either drops, accepts or returns the data packet, it will be returned to the forwarding filter table so it can continue through other filters.





This feature allows you to store sets of filters for logging, limiting, accepting or denying specific types of data that are only activated when you want. To globally activate those rules you could simply put in a filtering rule in the Forward panel that sends all data through the specified filter library, after which it could continue through your other filters.

Filtering Samples

The sample rules below are described in detail to give an example of how different parameters can be used to achieve different filtering functionality.

Limiting Example

Table 10: Limit rule for syslog message

D.Port	Protocol	Limit	Burst	Action	Log Level Prefix
80	tcp	6/h	5	log	Notice:Web Traffic

This example shows how the limit parameter and burst parameter affect the actions they are associated with. The first 5 packets with a destination port of 80 will activate this rule when the burst parameter is set to 5. After this it will be 10 minutes before another packet with a destination port of 80 will be activate this rule due to the limit parameter being set at 6 per hour (1 every 10 minutes).

For every 10 minutes that go by without a packet whose destination port is 80, 1 of the burst counters will be regained. If 50 minutes go by and no packets are found with a destination port of 80 then the entire burst parameter of 5 is restored and 50 minutes would be considered the recharge time.

NOTE - you cannot create a rule with a recharge time greater than 59 hours. For example if you set a limit of 1/d then the burst rate would have to be 1 or 2 because a burst rate of 3 would give a total recharge time of 72 hours (more than the maximum time.)

NetBIOS

The Net_BIOS filtering rules was designed to block sensitive NetBIOS data from moving into other networks (this is a Windows protocol that sends information about devices to the network so users can use Network Neighborhood to find local computers and resources.) The ICMP sample filtering rules describes sample possibilities of a single filter rule and the different results possible.

Table 11: Net_BIOS filtering rules

S.Port	D.Port	Protocol	Limit	Action	Log Level Prefix
137-139		udp	1/h	log	Notice:NetBIOS traffic
137-139		udp		drop	
	137-139	udp	1/h	log	Notice:NetBIOS traffic
	137-139	udp		drop	
137-139		tcp	1/h	log	Notice:NetBIOS traffic
137-139		tcp		drop	
	137-139	tcp	1/h	log	Notice:NetBIOS traffic
	137-139	tcp		drop	

The Net_BIOS filtering rules are actually included in the default configuration under the name NetBIOS_FWD. It is used by a single rule in the Filter Forwarding table that sends all packets passing through the firewall through this set of rules. If a packet did not match any of these NetBIOS rules it would be sent back to the filtering table that had forwarded it to continue through any other filters.

NetBIOS broadcast traffic is either coming from or going to ports 137-139. Because of this it was necessary to write 2 rules, 1 for all data coming from these ports and another for all data going to these ports. Additionally NetBIOS traffic can be either TCP or UDP so it was necessary to double the existing rules, 1 set for TCP and 1 set for UDP. It was not possible to choose ANY protocol or !ICMP (any but ICMP) because those options do not allow you to choose port addresses.

Finally this demonstration wanted to show when the rules were being used (i.e. when this traffic was occurring). To accomplish this each rule has a matching LOG rule which instead of dropping a packet generates a Syslog message at the Notice level. A custom text message is attached to the generated Syslog message to help identify what rule caused it to be sent.

Because a lot of this traffic could be occurring on a network it was also necessary to limit these messages from being generated too often. A limit of 1/hour was chosen so that not more than 1 message per hour would be generated for each rule using the Log Action.

ICMP and Filter Tables

Table 12: ICMP sample filtering rules

#	Proto	Action	Type	From	State	Source	Table
1	ICMP	drop					input
2	ICMP	drop	echo_request				input
3	ICMP	drop	echo_request	WAN			input
4	ICMP	drop	echo_request			!10.0.0.0/8	input
5	ICMP	drop					output
6	ICMP	drop				!10.0.0.0/8	output
7	ICMP	drop					forward
8	ICMP	drop			new	!10.0.0.0/8	forward
9	ICMP	drop			related	!10.0.0.0/8	forward
10	ICMP	drop			established	!10.0.0.0/8	forward

These rules were designed to block ICMP traffic, specifically ping information from either coming from the firewall or going through it. Each rule has a change made to it that will affect the ICMP traffic it will block. Below are summaries of these affects for each line in the table above.

Filter Rule Samples

1. Rule 1 drops all ICMP traffic that is directed at any of the firewall's interfaces (LAN, WAN, DMZ, PPPoE sites). Pings and other ICMP traffic can still pass through the firewall going to the other attached networks.
2. Rule 2 drops only ICMP echo requests (requests to respond to a ping) that are directed at any of the firewall's interfaces. Other ICMP requests can reach the firewall and it can respond to them. Pings and other ICMP traffic can still pass through the firewall going to the other attached networks.
3. Rule 3 simply activates the same rule as Rule 2 but only when the ICMP echo request arrived at the WAN interface. Pings made to the other interfaces of the firewall (LAN, DMZ, PPPoE sites) would be responded to.
4. Rule 4 says to drop all ICMP echo requests that are not coming from the 10.0.0.0/8 network. Assuming that the 10.0.0.0/8 network was your LAN network (this is activated by default) you allow workstations on the LAN to ping the firewall but any other network (such as from the Internet) would not receive a response to their ping. Other ICMP requests can reach the firewall and it can respond to them. Pings and other ICMP traffic can still pass through the firewall going to the other attached networks.

5. Rule 5 changes the table which has the filtering rule to drop all ICMP traffic. The Filtering Output table blocks data originating from the firewall such as the response to a ping request. The firewall would still receive the ICMP echo request (and any other ICMP messages) and generate an ICMP response but the response itself is what gets dropped. This would not be useful to block Denial of Service like attacks as the firewall would still be receiving the many pings and using its processing time to reply. Pings and other ICMP traffic can still pass through the firewall going to the other attached networks.
6. Rule 6 is the same as Rule 5 except it allows responses to ICMP messages that arrived from the 10.0.0.0/8 network. The rule says to drop all ICMP traffic being sent from the firewall directly except when the source is on the 10.0.0.0/8 network - the LAN interface is by default 10.0.0.1/8 so an ICMP message from that interface would be allowed.
7. Rule 7 does not say anything about ICMP traffic to or from the firewall but instead drops ICMP traffic that is moving from one network to another through the firewall. So the LAN could not send a ping to the Internet (WAN) or the DMZ but anyone could send a ping or other ICMP message to any interface on the firewall itself.
8. Rule 8 makes a slight change to Rule 7. All ICMP traffic passing through the firewall with the IP state of NEW is blocked except those originating from the 10.0.0.0/8 network. Responses to ping or other ICMP requests that originated from the 10.0.0.0/8 network will be allowed to travel back through the firewall but all other ICMP messages will be dropped u(nless of course they are destined to or from the firewall itself.)

   The filtering rules can keep track of the state of a connection which make this rule different from the others. A NEW state is a packet which creates a new connection. In this case all ICMP traffic which is requesting a ping from a network connected to the firewall would be considered a new packet and the responses would be considered part of an established connection. Since the NEW packet is blocked there will not be a response for the firewall to expect. Without the NEW state option all ICMP traffic would be blocked unless it's origin was from the 10.0.0.0/8 network. That is fine for outgoing ping queries but the responses from the remote networks will not be from the 10.0.0.0/8 network and would have been blocked.
9. Rule 9 drops all ICMP traffic passing through the firewall that are RELATED to but not a part an existing connection, such as some ICMP errors. This allows a direct response to a ping from the 10.0.0.0/8 network because the response to the ping is considered to be ESTABLISHED (because it is a reply to an accepted request) instead of RELATED. Since

only the RELATED packets were being dropped that did not originate from 10.0.0.0/8 the valid response was allowed back through. The original ping request was allowed because it was made from the 10.0.0.0/8 network (the default LAN interface network.).

10. Rule 10 will drop all ICMP traffic which is considered ESTABLISHED but that did not originate from the 10.0.0.0/8 network. This will allow a ping request from the 10.0.0.0/8 network to go to networks attached to the firewall (the Internet for instance if it is connected to the WAN interface) but would not allow a response back as it would be considered related. Other ICMP traffic that was not considered RELATED (not requested) would be allowed through however. Of course ICMP traffic directly to or from the firewall are still allowed as the rule is in the Filter Forwarding table and not in the Filter Input or Filter Output tables.

Routing

Chapter 11

Static Routing

Routing is when data traffic is redirected according to the destination IP address of the packet. For instance, you want to reach the Internet from your office - each device your data travels through needs to know where to forward the data so that it will arrive at the right place. A simple set of rules would identify your office network data (and not let it go to your Internet Service Provider) and every other packet with different destination could be forwarded to your Internet Service Provider.

Routing is the process of assisting data packets to get from their source to their destination. These destinations and/or firewalls can be edited with the included Configurator software in the Routing panel.

Data packets that are searching for their destination are pointed in the right direction by the firewall. To identify these routes, information describing the data pathways are stored in a routing table. Common information in this table include

- Destination IP address and subnet mask
- Firewall IP address
- Interface to reach the firewall (physical or PPPoE)

- Metric or number of firewalls the data packet will travel over to reach its destination

By using the destination IP address and subnet mask you can specify a whole range of addresses that will use a particular firewall device to get to a remote network. Because a firewall must have at least 2 Ethernet interfaces it is also important to identify on which interface the firewall is reachable.

Metrics can be used for more advanced analysis of routing paths such as identifying which is the shortest to a given destination.

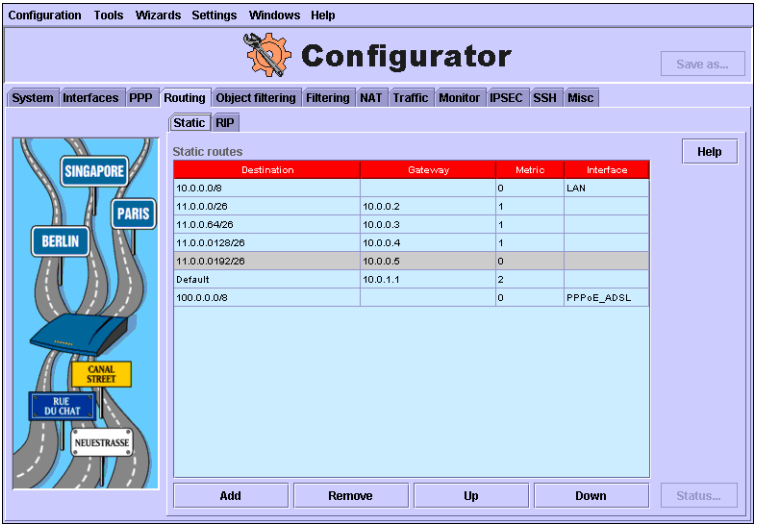
Routing, when possible, is very useful in Wide-Area Networks (WANs), where communication cost is an important factor, because it drastically reduces the number of broadcast packets that bridges would forward. Additionally selected addresses can be assigned to different gateways to better manage data flow. For example one could direct a specified web server backup data to use the firewall on an serial line and have the email server backup data via an ISDN telephone line. One of the most common routing selections is to send all Internet data requests through the user's Internet Service Provider.

IP routing tables can be maintained in two ways:

1. Statically, where the routing information is manually entered by the system administrator.
2. Dynamically, where the routing information is automatically passed between routing devices using a routing protocol.

Your firewall, in its current release, only supports static routing tables. Since network re-configuration is under the control of the network manager, the use of static routing tables increases security. Another advantage of using static routing over dynamic routing is the reduction of traffic.

Static Routing Configuration



This feature allows you to designate certain paths for data to travel. For instance, you will need a route for all of your Internet requests from your network to reach the Internet through your Internet Service Provider (if your Internet Service Provider is using DHCP servers to configure your account then this route will be entered automatically for you.) Another common use is if your MultiCom Firewall is in front of another firewall and needs to be forwarding packets to the other firewall to reach your LAN.

The data packets are told where to go based on the destination address of each packet. In the Routing panel you can enter in the static routes that tell data packets what IP address they need to go to reach their destination.

The Metric command allows the network administrator to keep track about which routes offer the quickest access to a given destination.

Dynamic Routing with RIP

The Routing Information Protocol (RIP) allows groups of firewalls to dynamically update their routing tables according to the state of the firewalls and routers they interact with. This is done by sending out regular UDP

announcements from each firewall using RIP. These announcements contain all known routes and a metric defining the distance to reach the known network (this metric is the number of firewalls that must be passed through to reach the given network.)

firewalls that are configured to receive these announcements compare the incoming routing table to its own. If the incoming announcement contains a route to a destination that has a shorter distance it replaces the existing route. This process maintains the best possible routes to each network.

There are two versions of the RIP protocol being used by Lightning-Linux. Version 1 or RIPv1 is the widely implemented first version of this protocol. Version 2 or RIPv2 has added enhancements which may be better suited to modern networks.

The following sections will provide a summary of these 2 versions if RIP but for more detailed information refer to RFC1058 (RIPv1) or RFC1723 (RIPv2).

NOTE - RIPv1 or v2 is not available over PPPoE sites used on the MultiCom Firewalls.

RIPv1

RIPv1 is an easily configured protocol that is widely used to manage dynamic routing tables. Every 30 seconds RIPv1 enabled firewalls will advertise all of the network routes it knows. This advertisement is a UDP or group of UDP packets that is sent to the IP broadcast address of each selected Ethernet interface. Each UDP packet contains up to 25 destination networks and the metric count of how many firewalls it takes to reach the specified network.

When a RIPv1 enabled firewall receives this packet it adds 1 to each metric and then compares the routes against its own table of routes. If the incoming route has a smaller metric then the existing route it will replace the existing route.

To add stability to this process, RIP will only count metrics between 1-15, 16 or higher are considered unreachable. This rule limits your dynamic network to not more than 15 hops or firewalls in your network. Additionally, Lightning-Linux uses the split horizons method for limiting broadcasts. This blocks advertisements of routes from going back out the Ethernet interface that they arrived on.

NOTE - subnetworks are only advertised in RIPv1 when interfaces are on different subnetworks of the same network number. Otherwise these routes are summarized. If you need to be updating subnetworks on a more detailed basis consider using RIPv2.

The final method of managing stability is to decide when a route is unreachable. If a specified route has not been heard from for 180 seconds then the route is marked as invalid.

RIPv2

RIPv2 offers enhancements to RIPv1 such as multicasting, VLSM (variable length subject masking), classless interdomain routing and authentication (not currently supported with Lightning-Linux.)

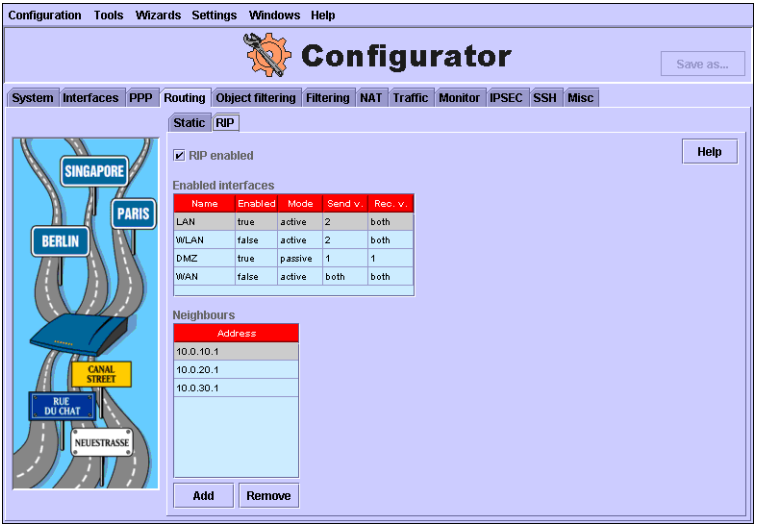
Routing UDP announcements are also sent every 30 seconds but always to the multicast IP address of 224.0.0.9. This lessens the network overhead being used by this protocol as compared with RIPv1 and allows them both to operate simultaneously.

CAUTION - Be sure to allow traffic for this IP address when configuring your security rules.

Each route being advertised by the RIPv2 enabled firewall will have its subnet attached to it (as opposed to route summarization that occurs in RIPv1).

Dynamic Routing Configuration w/RIP

Using the Advanced Configuration screen of the Configurator software you have access to the Dynamic Routing options of your Lightning-Linux device. Here you can enable or disable RIP v1 and/ or v2 for each Ethernet interface. You can also decide whether to send and/ or receive RIP broadcasts.

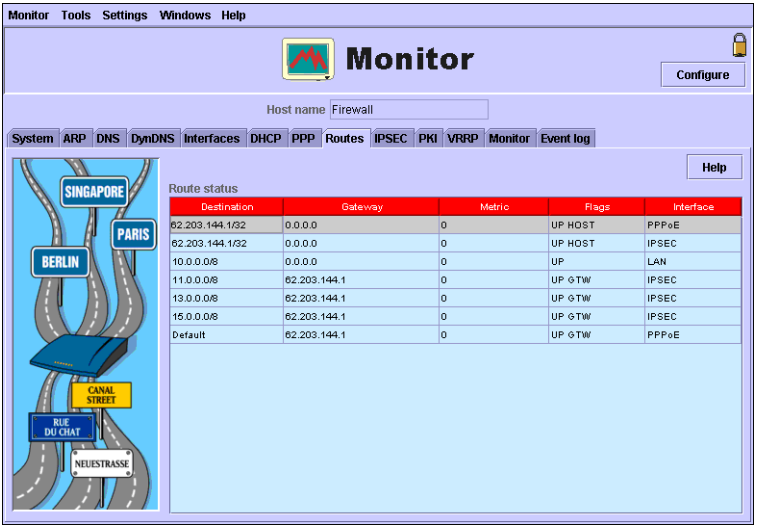


The Neighbors table is for listing nearby routers that do not understand multicast. Listing the IP address of the neighbor routers here establishes a direct link between routers, allowing the network administrator to specify the listed router as a RIP neighbor.

Routing Monitoring

The Monitoring window of the Configurator software has a table of all routes being maintained by your MultiCom Firewall. This table includes each routes firewall, metric, status flag and the Ethernet or PPP connection it is using. You can also see the active routing table by using the webserver of the MultiCom Firewall at http://10.0.0.1/advanced/status/ip/routing/status/route/, where 10.0.0.1 is the IP address of the LAN interface on the MultiCom Firewall.

If you have the IPSec option installed there may be special routes available when IPSec is activated. These are the routes to reach the other end of VPN tunnels.



This window shows you the currently active routes on your MultiCom Firewall. Routes are entered automatically for each subnet of a physical interface or PPP connection on the MultiCom Firewall. Additionally routes can be added statically by using the Configurator software or dynamically by enabling the RIP listener on selected interfaces.

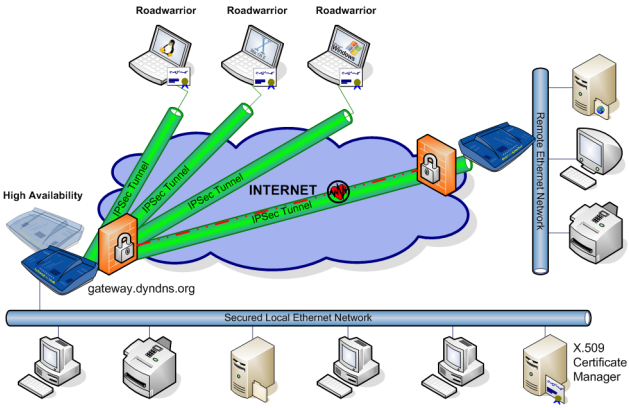
For more information on the statistics available from the Routing Monitor panel check the Monitor Panels Appendix.

Chapter 12

IPSec Virtual Private Network

Introduction

Lightning-Linux 3.2 and above support building Virtual Private Networking (VPN) using the MultiCom Firewalls with add-on options. Starting with version 3.5 SSH VPNs are also offered. With the IPSec VPN option users receive world-class protection for their sensitive data communications.



- Transport Encryption (for remote access)
- Tunnel Encryption (for encrypted Virtual Private Networks)
- Authentication w/o Encryption

Because IPSec is an international standards for security you are able to create secured connections with other networking equipment or software such as Linux users of FreeS/WAN, Checkpoint Firewalls, Cisco Routers and many other products supporting the IPSec and SSH specifications.

Lightning-Linux offers many special features that may not be found in all IPSec implementations. Below is a table of the different IPSec features with the firmware versions they are supported.

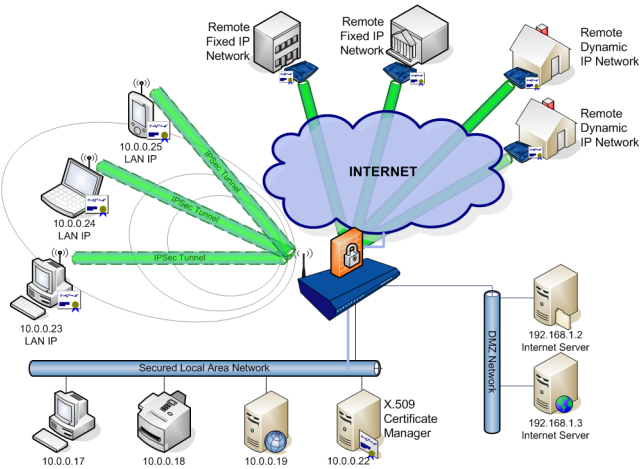
Table 1: IPSec Feature List

Feature/ Version	3.0	3.1	3.2	3.3	3.4	3.5	3.6	3.7
IPSec			x	x	x	x	x	x
Perfect Forward Secrecy			x	x	x	x	x	x
IDEA Cipher			x	x	x			
Manual Key support				x	x	x	x	x
Syslog debug						x	x	x
AES Cipher						x	x	x
Dead Peer Detection						x	x	x
IKE PSK email/FQDN IF						x	x	x
NAT Traversal						x	x	x
Roadwarrior Support						x	x	x
Serpent Cipher						x	x	x
Allow Subnet							x	x
DHCP over IPSec							x	x
High Availability Option							x	x
IPSec Traffic Filtering							x	x
IPSec with ARP Proxy							x	x
PKI Certificate Support							x	x
Connection Testing								x
Domain Name for endpoint								x
Web based wizard								x

IPSec Configuration Scenarios

With the IPSec option the MultiCom Firewall offers many VPN possibilities:

- Configure incoming Road Warriors
- Encrypted “tunneled” communication between 2 or more private subnets over the Internet
- Encrypted “transport” communication where the MultiCom Firewall is the endpoint, useful for remote configuration or SNMP/Syslog management
- Encrypted communication in the LAN between the MultiCom Firewall and a computer running IPSec client software (for instance to protect wireless data)
- Configure multiple connection rules based on various destinations or for different users
- Secured communications over wireless networks
- Communicate securely with other IPSec capable networking devices such as CheckPoint, Cisco PIX, Windows 2000/XP, SSH Sentinel



All scenarios offer a choice of many world-class encryption algorithms to protect your data and with support for NAT traversal, optionally at the same time as normal Internet traffic. Firmware 3.5 adds an IPSec Tunnel Wizard to make setting up a VPN quick and simple.

Be sure to check the IPSec FAQ available at http://www.lightning.ch/support and see the example configurations also on that site.

IPSec Protocol

IPSec Protocol Suite

IPSec is a suite of protocols designed by the Internet Engineering Task Force (IETF) to protect IP communication. Working on the network level, IPSec provides authentication, encryption, and integrity services for data packets and streams. This can be done either between 2 machines (transport mode) or 2 networks (tunnel mode)

IPSec uses three protocols to provide these services:

- Authentication Header (AH) offers data packet verification of the sender and that the packet has not been tampered with RFC2402
- Encapsulating Security Payload (ESP) offers encrypting and additional authentication services RFC2406
- Internet Key Exchange (IKE) negotiates the parameters needed to build a secured connection RFC2409 (usually using UDP for transport)

Using these protocols IPSec builds secured communication links by first establishing the communication parameters between any two or more hosts. The pre-selection of these parameters is entered into customized Security Associations (SA) which designate various algorithms for authentication and encryption, keys required as well as connection lifetimes for a specified communication link.

The keys can either be negotiated manually or, using IKE, the keys are negotiated automatically. IKE offers two mechanisms for automatic negotiation.

- Preshared Keys (PSK): where the same key is installed on each of the two entities involved in the encrypted communication link.
- Public Key Infrastructure (PKI): where certificates and public keys are exchanged using RSA and DSA.

> NOTE - The IPSec option of Lightning-Linux 3.2 will only negotiate keys using the IKE protocol and Preshared Keys (PSK). Lightning-Linux 3.3 or higher is required to use manual key negotiation and PKI negotiation is not supported at this time.

After the connection parameters have been agreed upon by IKE, data can transfer over those connections being encrypted, authenticated, and decrypted according to the options configured in the SA controlling that connection. The data packets are transported at this time via the AH or ESP protocols.

Many other details about functionality of IPSec can be found at the website for Internet Draft documents: http://www.ietf.org/ids.by.wg/ipsec.html.

MultiCom IPSec

The IPSec for the MultiCom Firewall offers selected features of the available protocol suite. More features are constantly being added so be sure to check back for updates and frequently asked questions at http://www.lightning.ch/.

VPN Firewall - with the IPSec option, each network interface on the MultiCom Firewall has the potential to act as an IPSec gateway.

VPN Client - Lightning Instrumentation also offers software clients (currently for the Windows operating systems).

Features

- Network encryption support for Rijndael (AES), Serpent, Twofish, Blowfish, CAST128, 3DES
- IP Compression: deflate, LZS
- IPSec modes: transport mode, tunnel mode
- IKE authentication: PSK, Manual Key, PKI certificates
- IKE modes: main mode, aggressive mode
- Certificates: support for X.509v3, CRLv2
- Centralized policy management
- Multi-layer security policy support
- Default IPSec response
- PMTU optimization
- Pre-IPSec packet filtering
- NAT Traversal
- Dead Peer Detection (DPD)
- DHCP over IPSec
- Security association (SA) statistics display

MultiCom Client Software

Lightning Instrumentation S.A. also offers client software for the Windows operating system.

Requirements

- Pentium 100 MHz processor or better
- 32 MB for Windows 9x, 64 MB for Windows NT/2000/XP
- 10 MBytes of free disk space
- TCP/IP network protocol

Features

Below are the features included with the MultiCom IPSec client software.

- All required IPSec + IKE protocol standards supported
- Network encryption support for Rijndael (AES), Twofish, Blowfish, CAST, 3DES, DES
- IP Compression: deflate
- IPSec modes: transport mode, tunnel mode
- IKE authentication: certificates, PSK
- IKE modes: main mode, aggressive mode
- Certificates: support for X.509v3, CRLv2
- Certificate online enrollment: SCEP, PKIX CMP, PKCS#7/#10 file, CAPIv2
- Certificate status: CRL distribution point extension
- Directory support: LDAP
- Centralized policy management: SPRP (proprietary), SPSL policy language parser
- Multi-layer security policy support
- Post- and pre-IPSec packet filtering
- Default IPSec response
- Support for self-signed certificates
- Security association (SA) statistics display
- NAT Traversal

- PMTU optimization
- Auditing
- PCSC/PKCS#15 smart card support (Setec, Miotec and Schlumberger cards)

IKE Key Negotiation

In the first phase of VPN process the IKE protocol builds the connections over which encrypted and/ or authenticated data will travel. Negotiation occurs over UDP port 500 between the two hosts attempting to build a secured connection.

CAUTION - Do not forget that if you are using NAT on the WAN Interface that there should be a rule to direct UDP 500 IKE key negotiations to the MultiCom Firewall. See “Making An IPSec VPN Connection” on page 264..

The parameters being negotiated are:

- mode: main
- authentication hashes: MD5, SHA1, SHA2 256 & SHA2 512
- authentication type: PSK, RSA, DSA (PSK only is supported in OS3.2-3.5)
- encryption ciphers: Rijndael (AES), Serpent, Twofish, Blowfish, CAST128, 3DES, DES
- key group: defines the group which is used by the algorithm Diffie-Hellman for the exchange of keys - Modp768, Modp1024, Modp1536, Modp 2048, Modp 3072 & Modp 4096
- lifetime of key negotiation (after which a new key negotiation occurs)
- datasize: the traffic in megabytes before renegotiation of keys (removed in 3.5)

In this first phase two firewalls set up an agreement between the two firewalls (also known as an ISAKMP SA) over which the IPSec SA (which does the packet authentication and/ or encryption) will be negotiated. Once this two-way negotiation has been completed multiple IPSec SA’s can be negotiated over it.

IPSec SA Negotiation

In the second phase of the VPN process Security Association are negotiated, after successful IKE negotiation. This negotiation has the similar parameters as the IKE negotiation plus some additional ones:

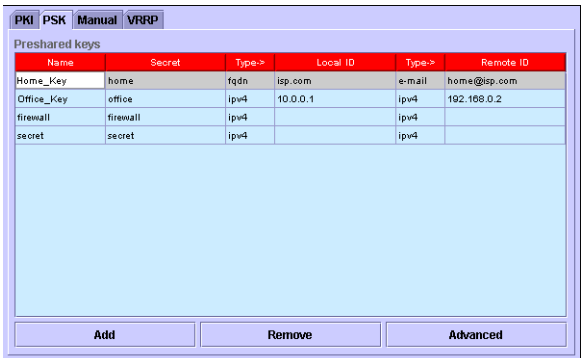
- protection: pick the AH or ESP protocol for encapsulating data packets
- hmacs authentication: algorithms - hmac-md5-96 and hmac-sha-96
- compression: LZS or deflate
- perfect forward secrecy (PFS): enabled or not enabled

After the IKE negotiation has successfully authenticated with the second firewall and agreed on how to communicate the IPSec SA's are negotiated as unidirectional links, one going in each direction (using different keys in each direction for added security). This negotiation is done in pairs so that traffic in both directions is possible. Once this is successfully completed data will be authenticated and/ or encrypted according to the options chosen in the SA and data secured communication is possible.

Preshared Key

When using IKE key negotiation Preshared keys (PSK) will be used to authenticate the connection. The PSK is a text based secret password that must be known on both sides of the IPSec connection if communication is to be allowed. The Preshared key should be carefully chosen.

The keys are managed using the Configurator software by clicking on the IPSec tab and then the "Privileged security parameters" button.



There are 5 parameters to each PSK.

Table 2: PSK parameters

Name	a name that the Preshared key can be referred to
Secret	the secret password of the key
Type	if using the optional ID's, choose ipv4, fqdn, or email
Local ID	the information used to identify the local host
Remote ID	the information used to identify the remote host

Using ID is not required but it is an optional level of security used during phase 1 of the protocol IKE and used by the associated Preshared Key to identify each side of the IPSec connection. The types of ID are as follows: IPV4 is an IP address, FQDN is a domain name, and email is an email address. If not being used these fields can be left blank.

This information will be saved in the Security Configuration file of the MultiCom Firewall and only be accessible by users with the "Privileged" rights.

Roadwarrior Configuration

When using IKE Key Negotiation it is possible to make Roadwarrior configurations. A Roadwarrior is a user on the Internet who wants to make a VPN secured connection to the central site but their IP address is not known in advance of the connection. For example, a user with a dialup connection at home or who is travelling in a different city and connects through their local Internet provider for that city or their hotel will receive different IP addresses each time they connect. The user can be using another MultiCom Firewall, 3rd party IPSec device, or IPSec client software.

The Roadwarrior will have an IPSec configuration with an unknown Local Gateway and the IPSec Server will have an IPSec configuration with an unknown Remote Gateway. When traffic is attempted for the remote network the MultiCom Firewall will attempt to build the IPSec connection. If successful a route for this new connection will be built using the current

As soon as the configuration is saved and traffic is sent to the remote, hidden subnet the MultiCom will try and build the IPSec channel. This will create a Virtual Private Network between 2 subnets with the MultiCom Firewall's encapsulating the packets into new packets that can

travel between the 2 Firewalls. Status of the connection can be seen at the MultiCom webserver, with the Monitor portion of the Configurator software or from syslog messages.

WARNING - Due to the unknown IP address of the Roadwarrior, it is impossible for the IPSec Gateway to open a tunnel to them. For all Roadwarrior connections the Roadwarrior must initiate the connection.

Current Roadwarrior configurations are only available when using Lightning-Linux 3.5, IKE IPSec key negotiation and when using the same Preshared Key for all incoming Roadwarriors. Remote subnets must also be identified (although the actual IPSec gateway points do not need to be identified) for correct routing to take place.

Check the Samples section for example parameters to use with the IPSec Tunnel Wizard. If the Roadwarrior user is behind a NAT firewall please see “NAT Traversal” on page 254.

PKI x.509 Certificates

Starting in firmware 3.6 MultiCom Firewalls with the IPSec option support the use of PKI x.509 certificates to authenticate both sides of an IPSec connection (in addition to Preshared Keys (PSK)). The x.509 Certificates are digitally signed and encrypted files generated and managed by a Certificate Authority software such as the CertIssuer software for MultiCom Firewalls.

Both Preshared Keys and x.509 Certificates can be managed by MultiCom Firewall users that have Privileged Rights. This user can open the Privileged Security Parameters window.

CAUTION - PKI x509 keys are the recommended way to secure an IPSec connection. If you use a Preshared key be sure to pick a random name that cannot be guessed.

Loading PKI Certificates

The certificates are files directly installed into the MultiCom Firewall using the web interface or the Certificate Manager software. Certificate status and information is visible from the web interface, Monitor software

or from the Certificate Manager software. To load the actual x.509 Certificates into the MultiCom Firewall the user with Privileged user rights must access the web interface of the firewall at http://10.0.0.1/advanced/security/pki/ where 10.0.0.1 is the IP address of the firewall. Optionally, the Certificate Manager software allows the creation , management and deployment of PKI Certificates to MultiCom Firewalls.

After installation of certificates and keys into the MultiCom Firewall the Configurator's PKI Certificate Management Window is used to give unique names to external public certificates or sets of identification rules. These unique names are used in the IKE section of each configured IPSec connection.

Using PKI Certificates

There are 2 ways to use PKI x.509 certificates:

1. A CA Certificate is created and distributed to each MultiCom device. Additionally, a Public Certificate/ Private Key Pair is created uniquely describing each device and is signed by the CA for authenticity. Each Key Pair will be installed into its own MultiCom device.
2. Each device has its own 3rd party CA installed (from another company for example) and its own Public Certificate/ Private Key Pair (signed by its own CA). Each device wanting to connect to the MultiCom device must load its Public Key into the External Trusted Clients portion of the MultiCom Firewall.

If everyone uses the same CA (#1) then configuration is easier because a certificate does not need to be installed for each external client. Additionally, multiple external clients, each using their own unique key, can use the same IPSec connection. Requirements for using the same CA Certificate in each device are:

- Load the same CA Certificate into each Firewall or IPSec Client software
- Load a unique Public Certificate/ Private Key Pair into each Firewall or IPSec Client software
- Create a unique name with Local ID and Remote ID rules to authenticate with the CA Certificate.

Optionally, identification rules can be created using the CA Certificate parameters, for instance this connection is for Sales keys only, or for keys from Italy only (as identified by the key). This is recommended for RoadWarrior connections.

Using different CA's (#2) is useful for providing access to users outside the organization however only one key can be used for each configured IPSec connection. For each external client the administrator must:

- Load the external client's Public Certificate into the External Trusted Clients list of the MultiCom Firewall
- Load the MultiCom Firewall's Public Certificate into the external client's External Trusted Clients list
- Create a unique name for their Public Certificate using the Configurator software

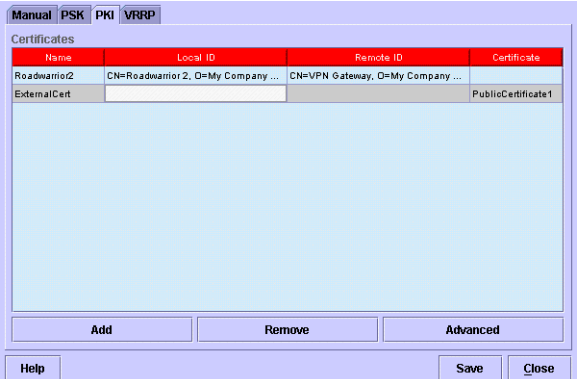
---

NOTE - if using 3rd party software to generate PKI keys for the MultiCom Firewall they must be in the Openssl format to be loaded into the MultiCom Firewall. The CertIssuer and Certificate Manager software are available for creating, managing and deploying PKI Certificates.

Creating Certificate Names And Rules

In both cases described above the MultiCom Configurator is used to give unique names to a group of identification rules or public certificates. These unique names will appear in the PKI Authentication box so that they can be used for the selected IPSec connection. All devices or software clients should have a CA Certificate installed and a key pair made of a public certificate and private key for each device.

The keys are managed using the Configurator software by clicking on the IPSec tab and then the "Privileged security parameters" button and choosing the PKI tab.



This panel is where you can name, edit, add or delete links to the PKI x.509 external client certificates installed on the MultiCom Firewall. These links (also called PKI contexts) can be used when negotiating a secured VPN connection. All certificates listed here are available to use on the IKE Panel to authenticate the selected IPSec connection. Be sure that these keys match the local and remote IPSec device/ firewall's Public Certificates.

Each entry in this table will have a unique name and one of the following

- Identification Rules for the Local ID and Remote ID of the installed CA Certificate
- a selected Public Certificate of an installed External Trusted Client certificate. No identification rules can be used with External Trusted Clients.

Identification Rules are only used when the same CA Certificate is installed on both sides of an IPSec connection. These rules identify the subjects of the Public Certificate of both sides (local and remote) of an IPSec connection. If a user with a certificate wants to connect to the MultiCom Firewall their Public Certificate that they use must match these Identification Rules. The subjects available to identify the key are:

- CN: Common Name
- O: Organization.
- OU: Organizational Unit
- L: Locality

- C: Country using its 2 letter country code in capital letters
- E: Email address

An IPSec tunnel to a single client might have fixed Identification Rules looking like this example:

> WARNING - Identification Rules must use EXACT syntax and each of the 5 values must be included. These rules are only valid on Public Certificates signed by the CA Certificate installed in the MultiCom Firewall.

Table 3: MultiCom VPN Gateway

Local ID:	CN=VPN Server, O=My Company SA, OU=IT, L=Neuchatel, C=CH, E=vpn@my.com
Remote ID:	CN=Mr Roadwarrior, O=My Company SA, OU=Sales, L=Neuchatel, C=CH, E=road@my.com

Table 4: Remote VPN User

Local ID:	CN=Mr Roadwarrior, O=My Company SA, OU=Sales, L=Neuchatel, C=CH, E=road@my.com
Remote ID:	CN=VPN Server, O=My Company SA, OU=IT, L=Neuchatel, C=CH, E=vpn@my.com

Optionally the VPN Gateway could use * in place of an actual value to allow any value in the Certificate's subject field to be allowed. This allows for easy grouping of users into categories and to allow many users to use the same IPSec connection, for instance many Roadwarriors from the same or different departments.

To allow multiple users only the VPN Gateway device needs to be changed and only the Remote ID portion of the Identification Rule. An example allowing all incoming users possessing a Public Certificate signed by the CA is below.

Table 5: MultiCom VPN Gateway

Local ID:	CN=VPN Server, O=My Company SA, OU=IT, L=Neuchatel, C=CH, E=vpn@my.com
Remote ID:	CN=*, O=*, OU=*, L=*, C=*, E=*

To group only users from the Sales department you could group the users like the following example.

Table 6: MultiCom VPN Gateway

Local ID:	CN=VPN Server, O=My Company SA, OU=IT, L=Neuchatel, C=CH, E=vpn@my.com
Remote ID:	CN=*, O=*, OU=Sales, L=*, C=*, E=*

CAUTION - Multiple users are subject to the limitations of the MultiCom Firewall option key that is installed. For example, if a 2 channel IPSec option key is installed only 2 users can be connected at the same time.

These links are stored in memory on the MultiCom Firewall as a second configuration called the Security Configuration. There is only one Security Configuration on a MultiCom Firewall and it can be accessed using the MultiCom Firewall's webserver at http://10.0.0.1/advanced/security/ where 10.0.0.1 is the IP address of the MultiCom Firewall.

NOTE - Only a user with Privileged rights can read, edit or save the Security Configuration.

TIP - Be sure to save a copy of your Security Configuration file in case of emergency.

The real x.509 certificates can be managed by MultiCom Firewall users that have Privileged Rights. To delete or load x.509 certificates the MultiCom Firewall the user must access the web interface of the firewall at http://10.0.0.1/advanced/security/pki/ where 10.0.0.1 is the IP address of the firewall or use the Certificate Manager software.

Certification Revocation List

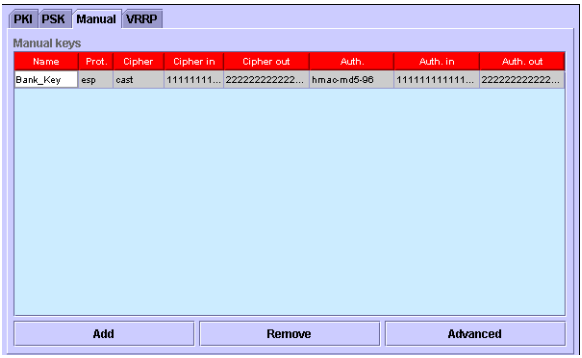
A Certificate Revocation List (CRL) can be created to list the public keys of devices that should no longer be allowed to access an IPSec tunnel. For instance, if everyone in the sales department has a public/ private key pair and salesperson A looses his laptop, the administrator can simply load salesperson A's public certificate into the Certificate Revocation List to block access for that laptop without having to reissue new certificates to the entire sales force.

This list is created by your Certificate Authority software (such as CertIssuer or the Certificate Manager for MultiCom Firewalls) and can be entered into the MultiCom Firewall at http://10.0.0.1/advanced/security/pki/crl/ .

Manual Key Negotiation

IPSec connections can also be configured using Manual Keying (often used for compatibility with 3rd Party IPSec Devices.) This option skips all of the IKE negotiation and instead every packet that is to be sent to another encrypted IPSec endpoint (the remote MultiCom Firewall for instance) will be encrypted.

The keys are managed using the Configurator software by clicking on the IPSec tab and then the "Privileged security parameters" button and choosing the Manual tab.



The parameters being configured are:

- Protection: AH or ESP
- SPI In and Out: an index number between 256 and 32767
- Key Protocol: AH or ESP
- Encryption Ciphers: Rijndael (AES), IDEA, Twofish, Blowfish, CAST128, 3DES, DES, None
- HMAC Authentication: either hmac-md5-96 or hmac-sha1-96
- Cipher In and Out: hexadecimal number which meets the minimum key size for the selected encryption cipher
- Authentication Key: a 4 digit hexadecimal number

When In and Out parameters exist the In parameter of the local MultiCom Firewall must match the Out parameter of the remote MultiCom Firewall.

General Components

IPSec Mode

There are 2 modes to choose from: Transport Mode or Tunnel Mode. You use Transport mode when the MultiCom Firewall is the endpoint of an encrypted flow of data. This means that you cannot use this mode when you are trying to gain full access to a subnet hidden behind the MultiCom Firewall with IPSec enabled. Tunnel Mode is used when configuring secured access through the MultiCom Firewall into a subnet behind it.

IKE Mode

There are 2 modes to choose from: Main Mode or Aggressive Mode. The Main Mode is required by the RFCs while the Aggressive Mode is an option. While the Aggressive mode may authenticate faster it is not considered as secure as Main Mode. The Main Mode provides identity protection for the hosts initiating the IPSec connection over 6 IKE packets. When using Aggressive mode it provides no identity protection and is compressed into 3 IKE packets.

Authentication Hashes

Hash algorithms compute a short digest/ summary of a longer message. Users can choose the authentication hash algorithm for authenticating IKE keys. It is possible to make a list of multiple algorithms and then the order of the algorithms in the list defines their priority during negotiation. The first algorithm in the list is used if the distant endpoint supports it. If the remote endpoint does not support it, the following algorithm in the list is tried, until there are no more options on the list to choose. Choosing ALL selects all of the algorithms in the order shown.

Table 7: Authentication Hashes

md5	Message Digest Algorithm 5 is a 128 bit cryptographic hash, see RFC1321
sha1	Secure Hash Algorithm version one is a 160 bit cryptographic hash, developed by the NSA and part of the U.S. Digital Signature Standard (DSS), more info at http://www.itl.nist.gov/fipspubs/fip180-1.htm
tiger192	192 bit cryptographic hash, more info at http://www.cs.technion.ac.il/~biham/Reports/Tiger/ (supported until 3.5)
ripemd160	160 bit cryptographic hash, more information at http://www.esat.kuleuven.ac.be/~bosselae/ripemd160.html (supported until 3.5)

Authentication Type

Lightning-Linux 3.2 and above uses Preshared Keys (PSK) for authenticating between 2 different endpoints of an IPSEC VPN. This means that the same key is installed on both endpoints of the VPN link or tunnel, for example if there is one MultiCom Firewall in Geneva and another in Seattle communicating from the Internet, they both must have the same key installed for the IPSEC VPN to be built.

Compression

Compression options are chosen by the user from those provided. It is possible to make a list of multiple algorithms and then the order of the algorithms in the list defines their priority during negotiation. The first algorithm in the list is used if the distant endpoint supports it. If the remote endpoint does not support it, the following algorithm in the list is tried, until there are no more options on the list to choose. Choosing ALL selects all of the algorithms in the order shown and selecting DISABLED turns off the compression option for the selected Security Association (SA).

Encryption Ciphers

These algorithms are how data is actually encrypted. Both sides must support the same algorithms to function.

For IKE key configurations it is possible to make a list of multiple algorithms and then the order of the algorithms in the list defines their priority during negotiation. The first algorithm in the list is used if the distant endpoint supports it. If the remote endpoint does not support it, the following algorithm in the list is tried, until there are no more options on the list to choose. Choosing ALL selects all of the algorithms in the order shown.

For Manual key configurations a key must be manually created that is equal to or larger than the minimum key size and equal to or smaller than the maximum key size. The Configurator software shows a Manual key size in bits when you click on the “Advanced” button on the Manual Key Input Window.

Table 8: Encryption Block Ciphers

Rijndael	variable block size and key length of 128, 192, or 256 bits, proposed as the new U.S. Advanced Encryption Standard (AES) in October 2000.
Serpent	is a 128-bit block cipher designed by Ross Anderson, Eli Biham and Lars Knudsen
IDEA	fixed block size of 64-bit with key length of 128 bits, recommended by the International Standards Organization (ISO), International Telecommunications Union (ITU), and the Swiss Telebanking Security Standard (available in firmware 3.3-3.5)
Twofish	fixed block size of 128 bits and key length up to 256 bits, designed by Bruce Schneier (MultiCom Firewall supports only 128 bits)
Blowfish	fixed block size of 64 bits and key length of 40 to 448 bits, designed by Bruce Schneier
CAST128	block size of 64 bits and key length of 128 bits
3DES	block size of 64 bits and key length of 192 bits
DES	block size of 64 bits and key length of 64 bits

HMACS authentication

The Hashed Message-Authentication Code is a complex hash used by the IPSec SA to authenticate the integrity of data packets. By using both a hashing algorithm (MD5 or SHA) on the packet’s data and a key it not only tells if a data packet has been changed but also if the sender knew the HMAC key.

It is possible to make a list of multiple algorithms and then the order of the algorithms in the list defines their priority during negotiation. The first algorithm in the list is used if the distant endpoint supports it. If the remote endpoint does not support it, the following algorithm in the list is tried, until there are no more options on the list to choose. Choosing ALL selects all of the algorithms in the order shown.

IKE Key Group

When negotiating a VPN connection or tunnel both endpoints must decide on which keys to use to encrypt the data. These keys are based on the private keys of each party and additional random data. The IKE Key Group identifies how many pool bits to use. More bits creates larger numbers which are consequently harder to break and provide more security. This option selects the group which is used by the Diffie-Hellman algorithm for the exchange of keys.

Table 9: Key Groups

modp768	modular exponentiation group with 768 bits
modp1024	modular exponentiation group with 1024 bits
modp1536	modular exponentiation group with 1536 bits
modp2048	modular exponentiation group with 2048 bits
modp3072	modular exponentiation group with 3072 bits
modp4096	modular exponentiation group with 4096 bits

Lifespan

The number of minutes or the datasize in megabytes that can pass before renegotiation of keys is required for an IKE proposal or SA proposal. Shorter lifespans increase the security of the connection because the keys are exchanged more frequently. However more frequent key exchanges will use more bandwidth for the negotiation and use more processor power. Be sure that when interacting with 3rd Party IPSec implementations that they support the same frequency of renegotiations that you set here.

Path Maximum Transfer Unit (PMTU)

This option tells the MultiCom Firewall to discover the maximum transfer unit (MTU) size that can be used through all of the links in the VPN connection before fragmentation will occur. Enabling this will avoid data

fragmentation because the MultiCom Firewall will use the discovered MTU and assure that all packets will be the correct size. In firmware 3.5+ this is automatically enabled.

Perfect Forward Secrecy

When enabled, Perfect Forward Secrecy (PFS) ensures that new key negotiations are not related to previous keys. This means that if someone obtains your short-term authentication keys they can not use them to read data they had previously received or to deduce other keys. To read ongoing data they would have to successfully attack your system to regain keys each time they are renegotiated. Disabling this option is allows faster but less secure encryption.

Protection

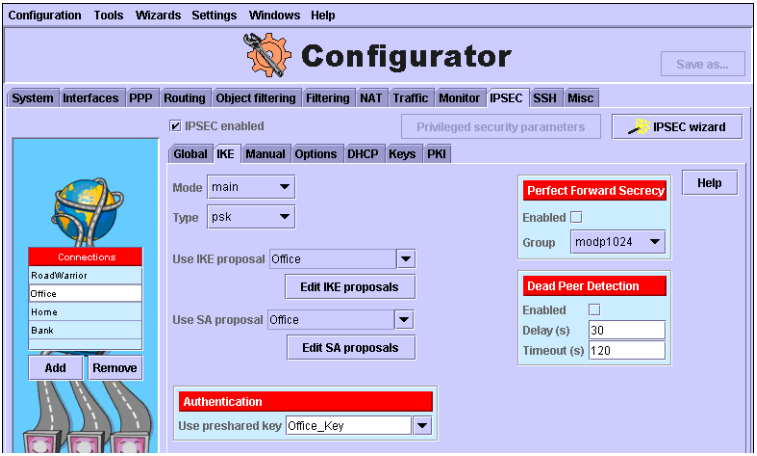
Users can choose to use either the authentication of the AH protocol or the authentication and encryption features of the ESP protocol. If you want to encrypt your data you must choose ESP. Using AH only verifies that the data packet came from a particular machine and that it was not altered in transit

Special Features

Dead Peer Detection

Starting in firmware 3.5 IPSec users of IKE can optionally activate Dead Peer Detection (DPD). DPD uses IPSec traffic patterns to limit the number of IKE messages sent and close broken tunnels. This feature is based on IETF draft: "A Traffic-Based Method of Detecting Dead IKE Peers" (draft-ietf-ipsec-dpd-02.txt).

When an IPSec connection is unexpectedly broken, due to routing issues, reboot of the client or server, IPSec does not normally know that a problem has occurred. SA's will remain until their lifetimes have expired. Dead Peer Detection can close the IPSec tunnel in this case, conserving resources and allowing the tunnel to wait for reactivation due to traffic. When DPD has closed a tunnel, the MultiCom IPSec monitoring will show that the tunnel is not established.

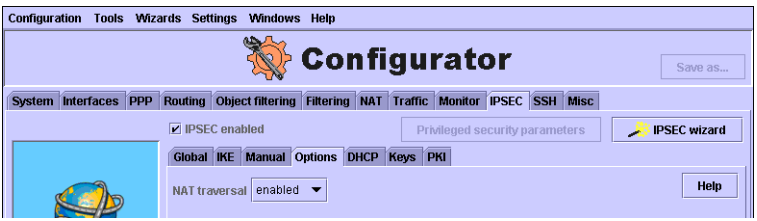


Both the server and the client must have this activated to work. By default every 2 minutes there will be an exchange of messages over the IPSec channel to verify that both sides are available. Success leaves the tunnel active and a failure will close the tunnel until reactivated due to traffic.

NOTE - Starting in firmware 3.6 this timeout and the delay can be edited in the IPSec > IKE tab for the selected IPSec connection.

NAT Traversal

Starting in firmware 3.5 IPSec offers the possibility for incoming clients to be behind a NAT firewall. Previous firmware versions did not support this option. In the Configurator software's IPSec > Option window there is the option to enable or disable this feature.



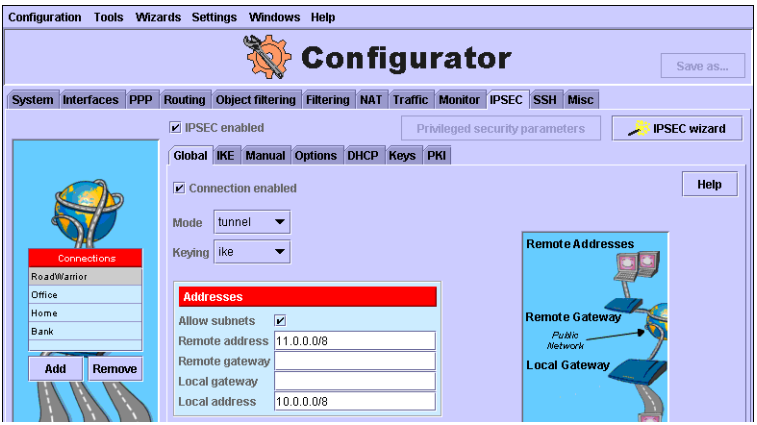
When enabled, the MultiCom Firewall allows IPSec clients behind a NAT device to build an IPSec connection that is encapsulated in UDP packets. There are some minimum requirements to use NAT traversal.

- IPSec connections must use Tunnel mode
- Remote subnets must be identified
- Roadwarrior connections must use the same PSK (and not Manual keys)

NAT-T support is based on IETF drafts: “Negotiation of NAT-Traversal in the IKE” (draft-ietf-ipsec-nat-t-ike-01-04) and “UDP Encapsulation of IPSec Packets” (draft-ietf-ipsec-udp-encaps-01-04). After IKE authentication (UDP 500) encrypted traffic will be encapsulated in UDP packets with a source and destination of port 4500.

Allow Subnets

Starting in firmware 3.6 IPSec tunnel can be configured with multiple remote IP addresses that are within the same subnet. This means that 1 connection can be used for multiple incoming roadwarriors with each road warrior having a different virtual IP address.



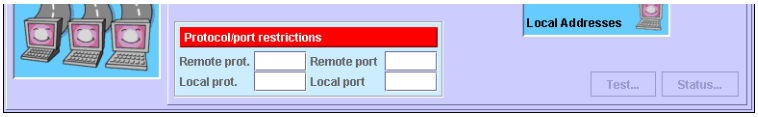
If you are using Preshared keys on this connection then everyone must have the same preshared key. However if you are using the same CA Certificate on both sides you can configure wildcards "*" in identifiers for the keys to allow multiple people with their own keys to access via a single IPSec connection.

For example, using PKI certificates allows you to allow all users in the sales department to have road warrior access using a single IPSec rule. Of course the incoming tunnels will be refused if they pass the limit of your IPSec option, 2, 20 or 200 channels.

This feature is activated in the IPSec Global panel when a roadwarrior configuration is being used (a configuration where the Remote Gateway is unknown).

Protocol/ Port Restrictions

Starting in firmware 3.6 IPSec offers the possibility to limit traffic on IPSec connections to a particular protocol and or port number (for TCP and UDP traffic). In the Configurator software's IPSec > Global tab there is the option use this feature for the selected IPSec connection.



- Remote Protocol & Port
- Local Protocol & Port

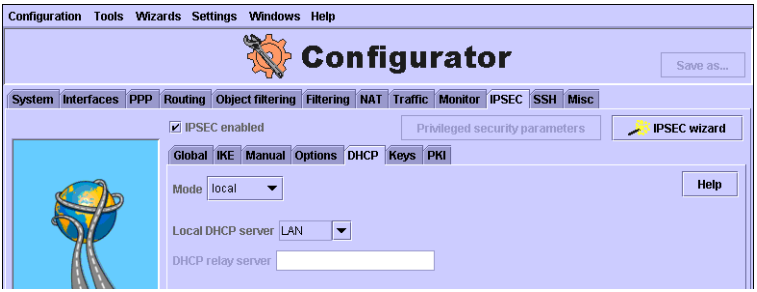
A protocol can be specified for use by the remote and/ or local side of the IPSec connection. Right click with the mouse over this field to see all options or enter 0 for ANY protocol, 1 for ICMP, 6 for TCP, or 17 for UDP. The default is any protocol is allowed.

A port that can be specified for use by the remote and/ or local side of the IPSec connection. Either enter the port number or right click with the mouse over this field to see some common ports. The default is any port is allowed.

If a protocol or port is listed then only that type of traffic is allowed to travel within the tunnel.

DHCP Over IPSec

Starting in firmware 3.6 incoming IPsec clients can ask for an IP address from a DHCP server on the MultiCom firewall or from another DHCP server using the "relay" feature. IPsec client software capable of requesting a DHCP address (such as SSH Sentinel) can now receive a local IP address.

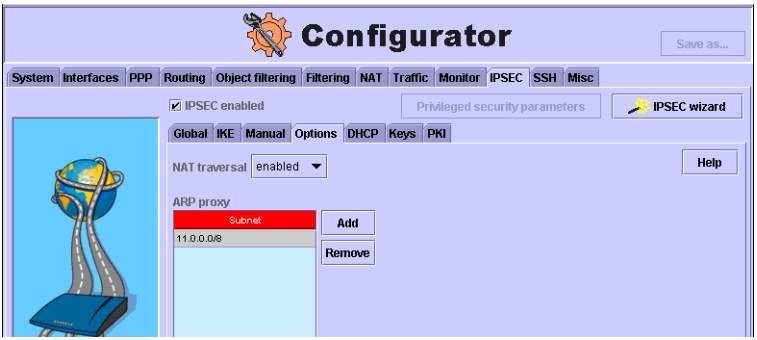


This feature is activated in the IPSec DHCP panel. A local interface with an already activated DHCP server or a remote DHCP server (identified with an IP address in the Relay field). Optionally these IPSec clients can appear to be on the local LAN by additionally using ARP Proxy.

NOTE - The IPSec client hardware or software must be capable of requesting a DHCP address over IPSec if it is wants to use this feature. Currently another MultiCom Firewall cannot receive a DHCP address.

IPSec With ARP Proxy

Starting in firmware 3.6 incoming IPsec connections can appear to be on the local network. This is meant to be used together with the IPSec DHCP feature allowing distribution of the IP addresses to a remote IPSec client by the DHCP server of the MultiCom FIrewall.



This feature is activated in the IPSec Option panel. A single IP addresses or entire subnets can be entered to allow the remote clients appear to be on the LAN.

IPSec Filters

This option was discontinued in firmware 3.5.

IPSec with MultiCom Firewalls has 2 special filtering options:

- Allow unprotected traffic
- Accept config from LAN

Allowing unprotected traffic made it possible for the MultiCom Firewall to send and respond to unencrypted traffic (such as normal Internet traffic) on all interfaces, otherwise only encrypted traffic is allowed to be sent or received.

If this is disabled the following option to “Accept config from LAN” is available. Enabling this option allows the MultiCom Firewall to be configured from the LAN on port 80 (HTTP) or port 443 (HTTPS) but if it is disabled and the “Allow unprotected traffic” is also disabled, then further configuration is not possible unless the computer attempting the configuration access has a software IPSec client installed.

Monitoring IPSec Connections

IPSec connections can be monitored in the following ways:

- using the Webserver
- using the Monitor portion of the Configurator software
- using syslog

Using the Webserver

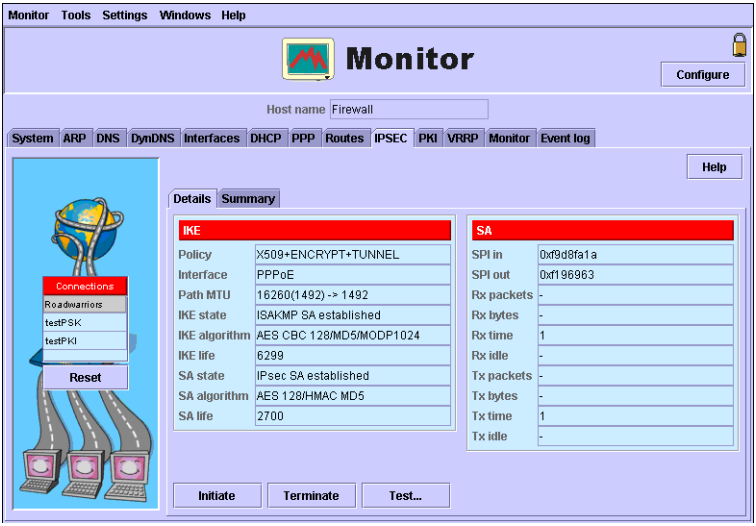
The MultiCom Firewall offers statistics on each IPSec connection as well as a table of connections and their state. A summary of all connections and their status is available at the web address of http://10.0.0.1/status/ipsec/.

Each connection's status is available at the web address http://10.0.0.1/advanced/status/security/ipsec/connection/. On this page is a list of all configured connections and by clicking on a connection and then the word Status the Administrator can access the status of both IKE and SA portions of an IPSec secured connection.

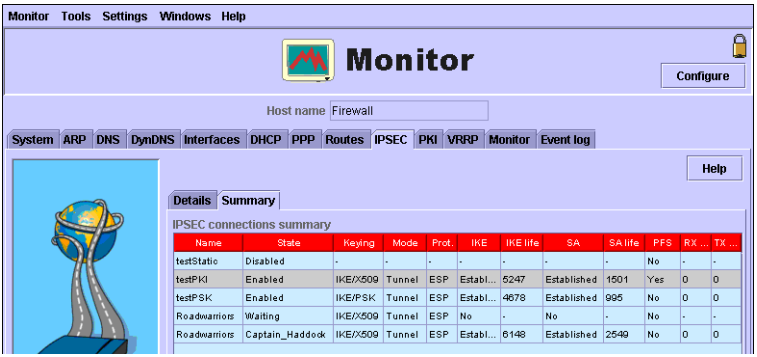
Using the Monitor

The Monitor portion of the Configurator software offers statistics on each IPSec connection as well as a table of connections and their state. Each connection's status is available at the IPSec > Details tab of the Configurator. A list of connections is available on the left.

Each connection can be initiated, terminated or tested from this interface.



A summary of all connections and their status is available at the IPSec > Summary tab of the Configurator.



Using Syslog

When Syslog messaging is activated on the MultiCom Firewall, messages will be generated during normal IPSec activity. This information is very useful for troubleshooting or for keeping a log of connection successes and failures. Sample messages are in the Chapter on SNMP & Syslog.

Connection Testing

IPSec connections can be tested to verify parameters are correctly configured on both sides of the IPSec VPN. Connection testing can be done

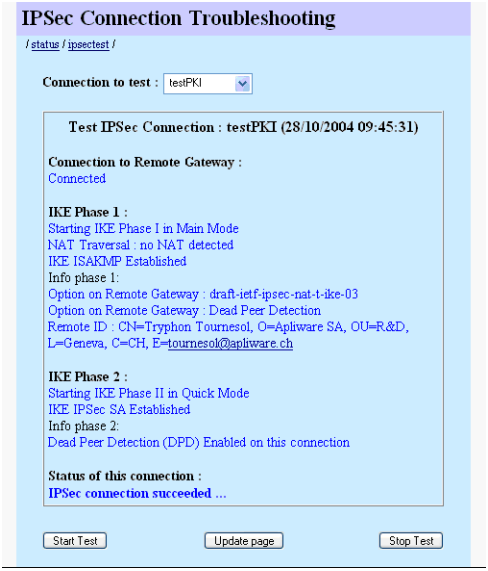
- using the Webserver
- using the Monitor portion of the Configurator software
- using CLI (telnet, SSH, or serial interface)

Using the Webserver

The MultiCom Firewall can test each enabled IPSec connection from the webserver interface. This test page is available at the web address of http://10.0.0.1/status/ipsectest/.

Select an IPSec connection from the drop down list and click the START TEST button. The page will refresh but because the test may take a long time it is possible to update the page with whatever status has been discovered or to stop the test.

Assuming everything has been correctly configured the test should look as follows.

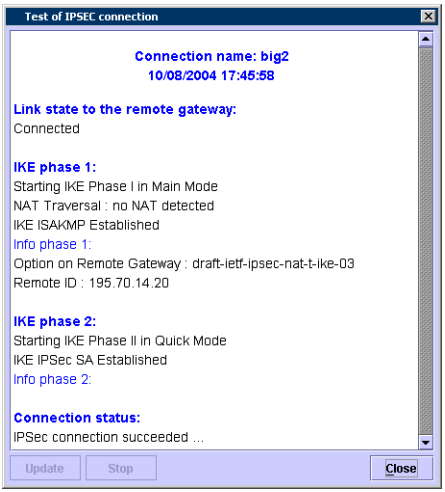


Using the Configurator

The Configurator software can test IPSec connections by clicking on the TEST button of the IPSEC > GLOBAL panel. The Monitor portion of the Configurator software can also test IPSec connections by clicking on the TEST button of the IPSEC > DETAILS panel.

Select an IPSec connection from the list and click the TEST button. The test will start but because the test may take a long time it is possible to update the window with whatever status has been discovered or to stop the test.

Assuming everything has been correctly configured the test should look as follows.



Using the CLI

After logging into the MultiCom Firewall's CLI interface (through Telnet, SSH secured telnet, or a serial interface if your MultiCom Firewall has a serial interface), it is possible to test a selected connection. More details about this command can be found at the command "Ipsec" on page 104.

An example of using this command is below.

Config /: ipsec

```
Usage: ipsec {initiate|terminate} <connection>
       ipsec test connection <connection>
       ipsec test {start|stop|show}

Available connections : Roadwarriors
, testPKI
, testPSK
```

```
Config /: ipsec test connection
Usage: ipsec {initiate|terminate} <connection>
       ipsec test connection <connection>
       ipsec test {start|stop|show}

Available connections : Roadwarriors
, testPKI
, testPSK
Config /: ipsec test connection testPKI
Config /: ipsec test start
Config /: ipsec test show

Test Connection : testPKI
Test Date : 02/01/2004 18:57:04

Connection to Remote Gateway :
Connected

IKE Phase 1 :
Starting IKE Phase I in Main Mode
NAT Traversal : no NAT detected
Invalid Certificate on Remote Gateway

Info phase 1:
Option on Remote Gateway : draft-ietf-ipsec-nat-t-ike-03
Option on Remote Gateway : Dead Peer Detection
Remote ID : CN=Tryphon Tournesol, O=Apliware SA, OU=R&D, L=Geneva,
C=CH, E=tourn
esol@apliware.ch

Error in IKE Phase I ...
[error because MultiCom had been off for more than 2 days and the
system time was not reset, hence certificates and Certificate
Revocation list was invalid]



Config /: ipsec test connection testPKI
Config /: ipsec test start
Config /: ipsec test show

Test Connection : testPKI
```

```
Test Date : 22/10/2004 12:24:06

Connection to Remote Gateway :
Connected

IKE Phase 1 :
Starting IKE Phase I in Main Mode
NAT Traversal : no NAT detected
IKE ISAKMP Established

Info phase 1:
Option on Remote Gateway : draft-ietf-ipsec-nat-t-ike-03
Option on Remote Gateway : Dead Peer Detection
Remote ID : CN=Tryphon Tournesol, O=Apliware SA, OU=R&D, L=Geneva,
C=CH, E=tourn
esol@apliware.ch

IKE Phase 2 :
Starting IKE Phase II in Quick Mode
IKE IPSec SA Established

Info phase 2:
Dead Peer Detection (DPD) Enabled on this connection

IPSec connection succeeded ...
[After update of system clock]
```

Making An IPSec VPN Connection

There are many choices to make an IPSec encrypted connection. Each side must have the same configuration except that the endpoints will be inverted (for instance the remote gateway of Side A will say Side B's IP address and the remote gateway of Side B will say Side A's IP address.)

Quick configurations for tunnel mode can be made using the IPSec Tunnel Wizard. Optionally, to build a VPN connection without the wizard you will need to be sure that IKE/SA Associations match, the keys match, and that the endpoints are configured correctly.

IPSec Tunnel Wizard

Starting in firmware 3.7 there is an IPSec Tunnel Wizard available in the Configurator software which allows quick and simple configuration of an IPSec VPN in Tunnel mode, using Preshared keys. This wizard is also available in the Configurator software starting in version 3.5.

Using the Web Interface

The web interface of the MultiCom Firewall has an IPSec wizard that can quickly create and test IPSec tunnels without having to use the Configurator software. It is designed for the enduser connecting to a fixed IP or dynamic IP VPN gateway. Configuration for incoming dynamic IP's (roadwarriors or mobile users) should be done using the Configurator software.

To use the IPSec Tunnel Wizard, simply go to the first screen and follow the intstructions to Find, Authenticate, and Test and save the IPSec connection. The IPSec Tunnel Wizard is available at http://10.0.0.1/easyipsec/ where 10.0.0.1 is the IP address of the MultiCom Firewall.

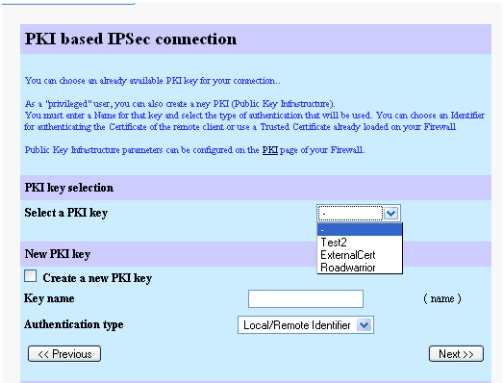
NOTE - if PKI Certificates are chosen the actual certificates must be already loaded into the MultiCom Firewall before using the IPSec Tunnel Wizard.

After describing how to reach the remote IPSec secured network and choosing the authentication type (Preshared Key or PKI Certificate) the next screens will allow the user to configure the authentication details. Below is the screen for the use of Preshared keys. Simply choose an existing Preshared key or, if the user has "Privileged" rights, create a new one.

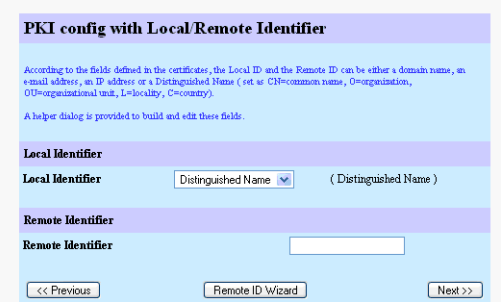
If the user has chosen an existing PKI context then the IPSec Tunnel Wizard is over and the new IPSec connection can be saved and tested.

NOTE - Preshared Keys created with the IPSec Tunnel Wizard do not have remote or local IDs. This is accepted by the MultiCom Firewalls by default but not all 3rd party IPsec gateways accept preshared keys without these IDs. If you must add IDs then you will have to use the Configurator software.

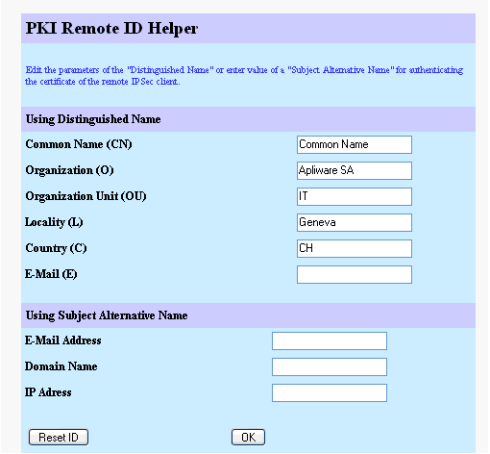
Below is the screen for the use of PKI Certificates. Simply choose an existing PKI context or create a new one. NOTE - the actual PKI Certificates cannot be entered here, only the PKI contexts (or key summaries) can be added.



If the user has choosen to create a new PKI context for authentication the next page will offer a field to either type in the context or a button to start the Remote ID Wizard to create a context. If the user has chosen an existing PKI context then the IPSec Tunnel Wizard is over and the new IPSec connection can be saved and tested.



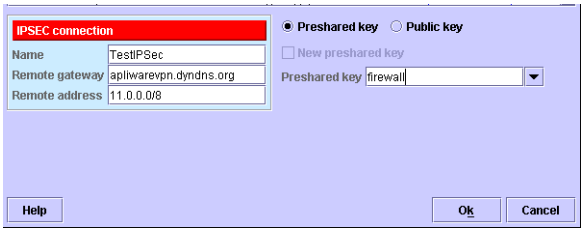
The Remote ID Wizard is shown below. After finishing the choice of the Remote ID for the PKI Certificate, the IPSec Tunnel Wizard is over and the new IPSec connection can be saved and tested.



Using the Configurator

The wizard is available in the Configurator software under the Wizard menu item.

NOTE - You must be connected to a MultiCom Firewall with the IPSec option for this wizard to be available. Additionally you must login using a username with Configuration or Privileged rights. Configuration level users can only choose from pre-existing Preshared Keys.



Using the IPSec Tunnel Wizard only requires the following information

- Name for the IPSec Tunnel
- The IP Address of the remote gateway as seen from the Internet
- The hidden, remote network's IP address (or subnet, for example

11.0.0.0/8)

•Select from either an existing Preshared Key or make a new one (creation of a new Preshared key is only possible for users with Privileged rights).

•Click OK

The Wizard will add a new IPSec connection with the chosen name to the configuration of the MultiCom Firewall. Additionally it will add NAT SecureWall rules to allow incoming IKE (UDP 500) and ESP traffic. Finally it will enable IPSec. The IPSec tunnel that is created will have an undefined Local Gateway which means that whatever IP address that is received by the MultiCom Firewall will be used to build the IPSec connection.

As soon as the configuration is saved and traffic is sent to the remote, hidden subnet the MultiCom will try and build the IPSec channel. For instance trying to ping IP address 11.0.0.1 would now cause the MultiCom Firewall to try to build the remote connection. Status of the connection can be seen at the MultiCom webserver, with the Monitor portion of the Configurator software or from syslog messages.

Check the Samples section for example parameters to use with the IPSec Tunnel Wizard.

IPSec Configuration Requirements

Matching Keys

In both cases you will need to make either a preshared key or a manual key which matches the remote Firewall's key for the selected VPN connection. Both types of keys can be configured using the Configurator software's "Privileged security parameters" which must be the same on both computers. This button is available in the IPSec window of the Configurator software.

NOTE - Manual keys have an added layer of complexity where you can specify different keys for data coming in and data going out of the Firewall. Be sure that if these values are different that the incoming key values for Side A matches the outgoing key values for Side B.

Matching IPSec Mode

For the selected connection verify that both sides are using the same IKE mode, either “transport” or “tunnel” mode. This option is under the IPSec>Global panel for the Configurator software.

IKE/SA Associations

All of the IKE/ SA Association parameters must match to make a successful VPN connection. For testing a new connection we recommend that you use the preset default connections that allow for all possible IKE/SA connections. Later, you may wish to limit this to a specific combination of these variables for increased security. These options can be set under the IPSEC>IKE panel.

Access Through SecureWall

Starting in Lightning-Linux 3.5, users of IPSec connections and the SecureWall must add the following rules for incoming IPSec traffic on the Interface connected to the Internet (either the WAN or PPP interface).

- UDP port 500 should be mapped to internal for IKE data
- UDP port 4500 should be mapped to internal NAT-Traversal data
- ESP Protocol traffic should be mapped to internal when using ESP
- AH Protocol traffic should be mapped to internal (only for users of IPSec who have chosen to use the AH protocol.)

Samples

There are 6 general types of IPSec configurations to be made with the MultiCom Firewall. Additional sample configurations are available at the support website.

- IPSec Tunnel Wizard for Roadwarriors
- IPSec Tunnel Wizard with fixed IP addresses
- Tunnel Mode using a Preshared Key (PSK)
- Tunnel Mode using a Manual Key
- Transport Mode using a Preshared Key (PSK)
- Transport Mode using a Manual Key

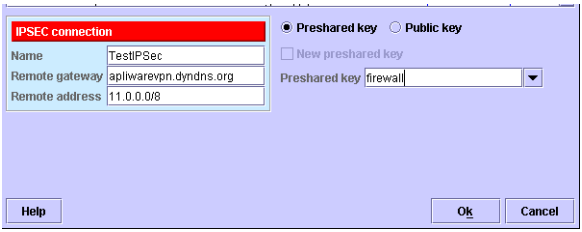
Using PSK requires a known key in both configurations and NAT rules to redirect IKE activity. After the Authentication with IKE (using UDP or TCP) all other data is encrypted between the two endpoints (between the two MultiCom Firewalls.)

Using Manual Keys skips the IKE activity and immediately communicates using encrypted packets. However the configuration of the keys must be manually entered on both Firewalls or communication cannot take place. Configuring this is more complex than the configuration for PSK.

Below are the tables showing the parameters necessary to make a Tunnel connection, using both a preshared key and a manual key.

Tunnel Using IPSec Wizard

The IPSec Tunnel Wizard is the quickest way to make IPSec tunnels. Connect to a MultiCom Firewall with the IPSec option using the Configurator software. Login using a username with Privileged rights (users with Configuration rights can only use pre-existing IPSec keys.) To reach the wizard you must go to the Wizard menu of the Configurator software and choose New "IPSec Tunnel".



The Wizard will add a new IPSec connection with the chosen name to the configuration of the MultiCom Firewall. Additionally it will add NAT SecureWall rules to allow incoming IKE (UDP 500) and ESP traffic. Finally it will enable IPSec. Data traffic over the Internet between the 2 MultiCom Firewalls will be encrypted and traffic from the LAN to the Internet will not be encrypted.

As soon as the configuration is saved and traffic is sent to the remote, hidden subnet the MultiCom will try and build the IPSec channel. Status of the connection can be seen at the MultiCom webserver, with the Monitor portion of the Configurator software or from syslog messages.

NOTE - Due to the unknown IP address of the Roadwarrior, it is impossible for the IPSec Gateway to open a tunnel to them. For all Roadwarrior connections the Roadwarrior must initiate the connection.

Table 10: IPSec Tunnel Wizard for Roadwarriors

	Local MultiCom	Remote MultiCom
IPSec Connection Parameters		
Name	Roadwarrior	Roadwarrior
Remote Gateway	a.a.a.a	
Remote Address	192.168.0.0/24	10.0.0.0/8
Local Address	10.0.0.0/8	192.168.0.0/24
Local Gateway		a.a.a.a
WAN IP Address	unknown	a.a.a.a
Preshared Key		
New Preshared Key	checked	checked
Name	Roadwarrior	Roadwarrior
Secret	mykey	mykey

Since you will need the Remote MultiCom's IP address to ask for a connection you might as well use it in the Remote MultiCom's configuration. After clicking OK from the wizard, goto the IPSec > Global table of the Remote MultiCom and enter in its known IP address as the Local Gateway parameter.

If the Local MultiCom is behind a NAT firewall you can optionally goto the IPSec > Options table of both MultiComs and "enable" NAT Traversal.

Table 11: IPSec Tunnel Wizard for fixed IP addresses

	Local MultiCom	Remote MultiCom
IPSec Connection Parameters		
Name	Roadwarrior	Roadwarrior
Remote Gateway	a.a.a.a	b.b.b.b
Remote Address	192.168.0.0/24	10.0.0.0/8
Local Address	10.0.0.0/8	192.168.0.0/24
Local Gateway	b.b.b.b	a.a.a.a
WAN IP Address	b.b.b.b	a.a.a.a
Preshared Key		
New Preshared Key	checked	checked
Name	Roadwarrior	Roadwarrior
Secret	mykey	mykey

The IPSec Tunnel Wizard will do everything but enter in the Local Gateway IP addresses. After clicking OK from the wizard, goto the IPSec > Global table of the MultiComs and enter in their fixed IP address as the Local Gateway parameter.

If the Local MultiCom is behind a NAT firewall you can optionally goto the IPSec > Options table of both MultiComs and "enable" NAT Traversal.

Tunnel Connection

This type of connection will create VPN between 2 subnets with the MultiCom Firewall's encapsulating the packets into new packets that can travel between the 2 Firewalls. This allows 2 private subnets that could not normally communicate over the Internet to not only communicate but to be encrypted at the same time.

Data traffic over the Internet between the 2 MultiCom Firewalls will be encrypted and traffic from the LAN to the Internet will not be encrypted.

NOTE - Previous users of Lightning-Linux 3.3 - 3.4.1 may have been using NOMAP rules to reach the remote IPSec secured subnet. These rules are no longer necessary in firmware 3.5 and should be deleted.

With Lightning-Linux 3.2.1 it was required to make 2 tunnels on each Firewall because NAT occurs on each packet before it gets encrypted by IPSec. This is no longer required starting in firmware 3.3.

Table 12: IPSec Tunnel using PSK and IKE

	Local MultiCom	Remote MultiCom
IPSec Connection Parameters		
Mode	Tunnel	Tunnel
Keying	IKE	IKE
Remote Address	192.168.0.0/24	10.0.0.0/8
Local Address	10.0.0.0/8	192.168.0.0/24
Remote Gateway	a.a.a.a	b.b.b.b
Local Gateway	b.b.b.b	a.a.a.a
WAN IP Address	b.b.b.b	a.a.a.a
LAN Interface IP Address	10.0.0.1/8	192.168.0.1/24
NAT Traversal	Enabled	Enabled
WAN/PPP NAT Rule		
NAT	Enabled	Enabled
SecureWall	Enabled	Enabled
WAN Interface Input NAT Rule	Rule #1	
Protocol	UDP	UDP
Destination Port	500	500
Mapping	Internal	Internal
To Port	500	500
	Rule #2	
Protocol	ESP	ESP
Mapping	Internal	Internal
IKE Key Parameters		
IKE Mode	Main	Main
IKE Type	PSK	PSK
IKE Proposal	Default	Default
SA Proposal	Default	Default
Preshared Key (PSK) Name	Lightning	Lightning
Preshared Key (PSK) Secret	lightning	lightning
Preshared Key (PSK) Local ID	<blank>	<blank>
Preshared Key (PSK) Remote ID	<blank>	<blank>

Table 13: IPSec Tunnel using Manual Key

	Local MultiCom	Remote MultiCom
IPSec Connection Parameters		
Mode	Tunnel	Tunnel
Keying	Manual	Manual
Remote Address	192.168.0.0/24	10.0.0.0/8
Local Address	10.0.0.0/8	192.168.0.0/24
Remote Gateway	a.a.a.a	b.b.b.b
Local Gateway	b.b.b.b	a.a.a.a
WAN IP Address	b.b.b.b	a.a.a.a
LAN Interface IP Address	10.0.0.1/8	192.168.0.1/24
NAT Traversal	Enabled	Enabled
WAN/PPP NAT Rule		
NAT	Enabled	Enabled
SecureWall	Enabled	Enabled
WAN Interface Input NAT Rule		
Protocol	ESP	ESP
Mapping	Internal	Internal
Manual Key Parameters		
Manual Protection	ESP	ESP
SPI In	256	32767
SPI Out	32767	256
Manual Key Name	Manual	Manual
Manual Key Protocol	ESP	ESP
Manual Key Cipher	Rijndael	Rijndael
Manual Key Cipher In (128 bit)	1111111111111 1111111111111 111111	222222222222222 222222222222222 22
Manual Key Cipher Out (128 bit)	2222222222222 2222222222222 222222	111111111111111 111111111111111 11
Manual Key Authentication	Hmac-md5-96	Hmac-md5-96
Auth In	3333	4444
Auth Out	4444	3333

Transport Mode Using PSK

This type of connection will create VPN between 2 MultiCom Firewalls where the encrypted data request is expected to end at the remote MultiCom Firewall (and not a protected subnet behind the MultiCom Firewall.) The primary use of this is to access the MultiCom Firewall for configuration. Additionally, access to the internal protected networks is limited.

This would be useful to access the MultiCom firewall for administration, firmware update, transmitting Syslog or SNMP messages.

Below are the tables showing the parameters necessary to make a Transport connection, using both a preshared key and a manual key.

Table 14: IPSec Transport using PSK and IKE

	Local MultiCom	Remote MultiCom
IPSec Connection Parameters		
Mode	Transport	Transport
Keying	IKE	IKE
Remote Address	a.a.a.a	b.b.b.b
Local Address	b.b.b.b	a.a.a.a
WAN IP Address	b.b.b.b	a.a.a.a
NAT Traversal	Enabled	Enabled
WAN/PPP NAT Rule		
NAT	Enabled	Enabled
SecureWall	Enabled	Enabled
WAN Interface Input NAT Rule	Rule #1	
Protocol	UDP	UDP
Destination Port	500	500
Mapping	Internal	Internal
To Port	500	500
	Rule #2	
Protocol	ESP	ESP
Mapping	Internal	Internal
IKE Key Parameters		
IKE Mode	Main	Main
IKE Type	PSK	PSK
IKE Proposal	Default	Default
SA Proposal	Default	Default
Preshared Key (PSK) Name	Lightning	Lightning
Preshared Key (PSK) Secret	lightning	lightning
Preshared Key (PSK) Local ID	<blank>	<blank>
Preshared Key (PSK) Remote ID	<blank>	<blank>

Table 15: IPSec Transport using Manual Key

	Local MultiCom	Remote MultiCom
IPSec Connection Parameters		
Mode	Transport	Transport
Keying	Manual	Manual
Remote Address	a.a.a.a	b.b.b.b
Local Address	b.b.b.b	a.a.a.a
WAN IP Address	b.b.b.b	a.a.a.a
NAT Traversal	Enabled	Enabled
WAN/PPP NAT Rule		
NAT	Enabled	Enabled
SecureWall	Enabled	Enabled
WAN Interface Input NAT Rule		
Protocol	ESP	ESP
Mapping	Internal	Internal
Manual Key Parameters		
Manual Protection	ESP	ESP
SPI In	256	32767
SPI Out	32767	256
Manual Key Name	Manual	Manual
Manual Key Protocol	ESP	ESP
Manual Key Cipher	Rijndael	Rijndael
Manual Key Cipher In (128 bit)	11111111111111 11111111111111 1111	222222222222222 222222222222222 22
Manual Key Cipher Out (128 bit)	22222222222222 22222222222222 2222	111111111111111 111111111111111 11
Manual Key Authentication	Hmac-md5-96	Hmac-md5-96
Auth In	3333	4444
Auth Out	4444	3333

IPSec Frequently Asked Questions

What is the difference between tunnel or transport mode?

You use Transport mode when the MultiCom Firewall is the endpoint of an encrypted flow of data. This means that you cannot use this mode when you are trying to gain full access to a subnet hidden behind the MultiCom Firewall with IPSec enabled.

You will use Tunnel Mode when configuring access through the MultiCom Firewall into a subnet behind it.

WARNING - Be sure to have configured both endpoints of the encrypted connection to use the same mode.

What is the order of activity for the IPSec process?

Incoming data packets pass through the following processes when arriving at an interface of the MultiCom Firewall:

1.SecureWall

2.NAT

3.IPSec

4.Filtering

5.Routing

Remember that the first packets in the IKE authentication are unencrypted and must be able to access the MultiCom Firewall via UDP port 500 or an encrypted connection cannot be built.

Can I use filtering with IPSec?

Yes, but note that in the above description that IPSec packets using AH/ ESP are decrypted before they reach the Filtering level and so requests to see these 2 protocols will fail since the packet is AH/ESP portion of the packet is removed. However, once the incoming IPSec connection has been authenticated the packets can be filtered.

Does the MultiCom Firewall support NAT Traversal

No. If NAT is being used on other devices between the MultiCom Firewall and the Internet the IPSec connection will not work. The ESP packets are

changed and hence the authentication portion of the IPSec protocol will fail. The MultiCom Firewall with NAT enabled must be an endpoint for the encrypted packets. If you do not enable NAT then the ESP packets will be routed without a problem based on their IP header.

How do I close unused encrypted connections?

The available processes for this are disabling IPSec on the MultiCom Firewall and resaving the configuration, turning off or rebooting the MultiCom Firewall, or setting the connection lifetime to a small enough number to close unused connections within the time frame desired.

After the SA lifetime or IKE lifetime expires, if no traffic is sent, an IKE information packet is sent to tell that the connection will be closed (no new key is generated). Optionally activate the Dead Peer Detection for IKE. Every 2 minutes a query will take place between the 2 sides of the connection and if there is no response the connection is closed.

Do MultiCom Firewalls support dynamic user authentication?

No, tunnels are built based on IP addresses and preconfigured encryption options. There are currently no links to the likes of Radius, SecureID or other authentication services other than already provided by IPSec's preshared key solution (PSK).

You can of course configure different IPSec connections for different users and assign each connection different IP addresses and preshared keys.

Can I use FQDN (name of a website) to identify the endpoint of a tunnel?

Not at this time. Currently you can only use IP addresses, IP ranges, IP subnets, or identify any IP traffic using “0.0.0.0/0”.

How do I troubleshoot an encrypted connection that is not working?

The first thing to do is to verify if basic Ethernet connectivity is possible.

1. Check the status of the IPSec connection on the Webserver or Monitor portion of the Configurator. It is recommended to be running syslog also for the best diagnostics.
2. Turn off IPSec and test basic network connectivity. You must be sure that your packets can arrive in an unencrypted state to their destination before you can attempt to encrypt them (routing, NAT, filtering...)
3. Verify IPSec parameters are matching for IKE, SA, preshared keys (value

and IDs)

4. Verify IP addresses are assigned correctly for endpoints and protected subnets
5. If using NAT with SecureWall, verify the UDP port 500 and the ESP protocol is mapped to INTERNAL
6. If using filtering, be sure that you have not filtered the traffic that is coming through the channels, try disabling the filtering to see if the data can traverse the IPSec tunnel
7. Verify that other encrypted connections are not using the same IP addresses or subnets
8. Try the connections without IPSec options such as compression, Path Maximum Transfer Unit, Perfect Forward Secrecy

How can I be sure my data is being encrypted?

connect a hub (not a switch) to the WAN interface and also connect a 3rd computer running IP sniffing software such as Ethereal to watch the actual data packets traversing the Ethernet.

How can I reconfigure my MultiCom Firewall if I have forgotten the username or password?

If you have lost your username and/ or password to the MultiCom Firewall there is no backdoor for you to get access again to the existing configuration and IPSec keys. You can reset the MultiCom Firewall into default mode by holding down the Config button on the back of the device during a reboot but all configuration and keys will be lost.

NOTE - Configuration and keys are only lost if you write the default configuration to the boot memory. You can temporarily load the default settings to make tests of network connectivity but you must NOT save any configuration to the boot memory.

Will the MultiCom Firewall work with wireless networks?

Using the IPSec option of a MultiCom Firewall will work over Wireless networks and often provides stronger security than available with the wireless hardware. By installing the IPSec client software on the wireless workstation and connecting to an encrypted LAN endpoint data can be transmitted over the wireless network encrypted with the user's selected algorithm.

How long does it take to build an IPSec connection?

About 1 second assuming that there is already an existing Ethernet connection. If you must make a connection with a Modem to an external network than the time it takes to connect is of course added to the time to build an IPSec connection.

How can I turn off IPSec if I have made a an error in the configuration?

You can connect to the MultiCom Firewall using the console connection (available in the Ethernet III, SpeedSurf, and Enterprise). The following commands will enable or disable the IPSec functionality.

TURN ON IPSEC

set security ipsec enabled=true

saveconfig current

TURN OFF IPSEC

set security ipsec enabled=false

saveconfig current

How does my encrypted data look on the Internet?

Below are the packet sniffer results when watching a computer sending email with and without IPSec. Without IPSec, the final destination is known, usernames and passwords are visible and in fact all of the contents of the email are visible as well. Packets below are NOT encrypted.

No. Source Destination Protocol Info

1 10.0.2.254 222.1.1.1 TCP 4199 > smtp [SYN]

2 222.1.1.1 10.0.2.254 TCP smtp > 4199 [SYN, ACK]

3 10.0.2.254 222.1.1.1 TCP 4199 > smtp [ACK]

4 222.1.1.1 10.0.2.254 SMTP Response: 220 mailserver.me.com SMTP

5 10.0.2.254 222.1.1.1 SMTP Command: HELO mycomputer

6 222.1.1.1 10.0.2.254 TCP smtp > 4199 [ACK]

7 222.1.1.1 10.0.2.254 SMTP Response: 250 mailserver.mycompany.com

8 10.0.2.254 222.1.1.1 SMTP Command: MAIL FROM: <shawn.giese@lightning.ch>

When the message is encrypted using IPSec, it is impossible to know the contents of the data packets or, in many cases, even where those packets are

going. Notice that all descriptions of the packets are gone and replaced by the ESP protocol. Anyone watching this traffic will not know if the data is accessing a database, email, internal web services. Below are packets using IPSec encryption when sending the same email message as above. The first 9 packets are the IKE Key exchange that takes place during the building of an IPSec encrypted connection using IKE.

No.	Source	Destination	Protocol	Info
1	10.0.2.254	10.0.0.1	ISAKMP	Identity Protection (Main Mode)
2	10.0.0.1	10.0.2.254	ISAKMP	Identity Protection (Main Mode)
3	10.0.2.254	10.0.0.1	ISAKMP	Identity Protection (Main Mode)
4	10.0.0.1	10.0.2.254	ISAKMP	Identity Protection (Main Mode)
5	10.0.2.254	10.0.0.1	ISAKMP	Identity Protection (Main Mode)
6	10.0.0.1	10.0.2.254	ISAKMP	Identity Protection (Main Mode)
7	10.0.2.254	10.0.0.1	ISAKMP	Quick Mode
8	10.0.0.1	10.0.2.254	ISAKMP	Quick Mode
9	10.0.2.254	10.0.0.1	ISAKMP	Quick Mode
10	10.0.2.254	10.0.0.1	ESP	ESP (SPI=0xa6d4b946)
11	10.0.2.254	10.0.0.1	ESP	ESP (SPI=0xa6d4b946)
12	10.0.0.1	10.0.2.254	ESP	ESP (SPI=0xef1015de)
13	10.0.2.254	10.0.0.1	ESP	ESP (SPI=0xa6d4b946)
14	10.0.0.1	10.0.2.254	ESP	ESP (SPI=0xef1015de)
15	10.0.2.254	10.0.0.1	ESP	ESP (SPI=0xa6d4b946)
16	10.0.0.1	10.0.2.254	ESP	ESP (SPI=0xef1015de)

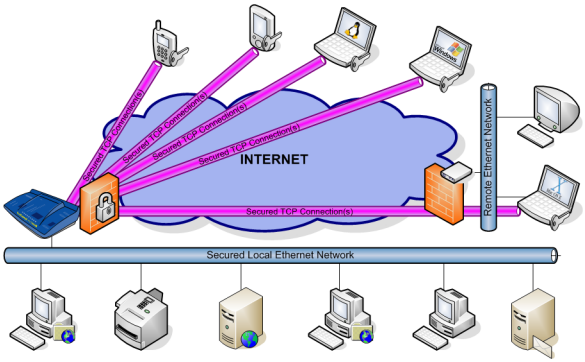
Chapter 13

SSH Virtual Private Network

Introduction

Starting with version 3.5 SSH based VPNs are offered for all MultiCom Firewalls as an add-on option. The following features are available with the SSH VPN option.

- TCP Port Forwarding VPN
- TCP Gateway Ports VPN
- Authentication with username/ password
- Authentication with username/ public key



Because SSH is an international security standard you are able to create secured connections with other networking equipment or software such as SSH Secure Shell, PuTTY and many other products supporting the SSH specifications.

SSH Configuration Scenarios

With the SSH option the MultiCom Firewall offers many configuration possibilities:

- Secured remote management of a MultiCom Firewall using SSH secured CLI access (included for free with Lightning-Linux 3.4+)
- Configure incoming Road Warriors
- Encrypted TCP port communication between a client and server over the Internet (Remote Desktop, POP3, IMAP, SMTP, HTTP, HTTPS, Telnet, VNC...)
- Configure multiple access for different users, optionally with RSA & DSA public key management
- Communicate securely with other SSH capable networking devices or software such as SSH SecureShell, PuTTY and more

All scenarios offer a choice of many world-class encryption algorithms to protect your data and with support for NAT traversal, optionally at the same time as normal Internet traffic. Be sure to check the 3.x FAQ available at http://www.lightning.ch/support.

SSH Virtual Private Networks

SSH Protocol

The SSH protocol offers secure remote login and data transfer over the Internet or any IP based network. Working on the network level, SSH provides authentication and strong encryption services for data packets and streams. Because you are validating public keys you are assured that the receiver of your authentication information is correct. Additionally, SSH Port Forwarding protects against eavesdroppers and session hijacking.

The SSH protocol consists of 3 major components:

- Transport layer protocol (SSH Transport Layer Protocol, secsh-transport) for authentication of the MultiCom Firewall.

- User authentication protocol (SSH Authentication Protocol, secsh-userauth) for authentication of the incoming user.
- Connection protocol (SSH Connection Protocol, secsh-connect) for combining multiple channels into a single, multiplexed encrypted tunnel.

SSH offers its services to authenticated users on TCP port 22 (optionally can be changed). After authentication it is the client that selects from available encryption option, asks for particular ports to be forwarded, and possibly also has CLI access (similar to a telnet access) if allowed. Secure authentication using SSH is provided by

- RSA Host public key (optionally DSA with SSH v2) to identify the MultiCom Firewall.
- RSA Client public key (optionally DSA with SSH v2) to identify the incoming user.
- Username and password verification against registered users of the MultiCom Firewall

Using these protocols SSH builds secured communication links by first establishing the authentication parameters between any two hosts.

NOTE - changing the SSH port in the SSHVPN panel also affects normal SSH CLI port use.

After the connection parameters have been agreed upon, data can transfer over those connections being encrypted, authenticated, and decrypted. The data packets are transported at this time over TCP port 22 by default.

Many other details about functionality of the SSH protocol can be found at the website for Internet Draft documents: http://www.ietf.org/ids.by.wg/secsh.html.

MultiCom SSH

The SSH for the MultiCom Firewall offers selected features of the available protocol suite. More features are constantly being added so be sure to check back for updates and frequently asked questions at http://www.lightning.ch/.

VPN Firewall - with the SSH option, each network interface on the MultiCom Firewall has the potential to act as an SSH gateway.

NOTE - The MultiCom SSH implementation only offers the server portion of the SSH secured connection. To use this you must use software or hardware to provide the client side of the connection. See the list below for suggested software clients.

Features

- Network encryption support for Rijndael (AES128, 192, 256), Blowfish, CAST128, Arcfour, 3DES
- Custom port usage (default TCP 22)
- Authentication and Banner message
- Port Forwarding
- Gateway Ports
- SSH Protocol version 1 and 2
- Compression
- RSA & DSA Public Key Management
- NAT Traversal

Client Software

There are numerous sources of 3rd party software that support SSH CLI access and/ or SSH Port Forwarding.

- SSH Secure Shell (Windows) http://www.ssh.com
- PuTTY (Windows) http://www.chiark.greenend.org.uk/~sgtatham/putty/
- Cygwin (Windows) http://www.cygwin.com/
- MacSSH (MacOS9) http://pro.wanadoo.fr/chombier/
- Open SSH (MacOSX, Linux, Unix) http://www.openssh.com/
- PockeTTY (WinCE) http://www.dejavusoftware.com/pocketty/index.html
- MochaTelnet (PalmOS) http://www.mochasoft.dk/palm.html#palmtelnet
- Nokia 9200 series http://www.f-secure.com/wireless/symbian/nokia-ssh.shtml
- Other SSH Client software can be found at http://www.freessh.org/other.html

SSH Version 1

This first version of SSH uses the asymmetric cryptography algorithm RSA (Rivest-Shamir-Adleman) for key negotiation with only 3DES and Blowfish ciphers to encrypt the data. SSH v1 uses a simple CRC for data integrity.

This version of SSH may be needed to support older software/ hardware. The MultiCom Firewall can be configured to support only v1, v1 & v2 or only v2. Whenever possible it is recommended to use only SSH v2.

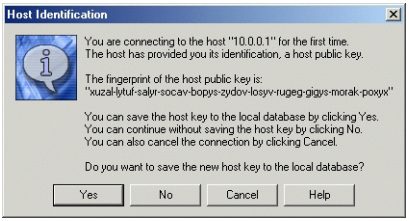
SSH Version 2

The second version of SSH uses the asymmetric DSA (Digital Signature Algorithm) and DiffieHellman algorithms in addition to RSA for key negotiation. Additionally v2 offers support for more ciphers than v1(Rijndael (AES128, 192, 256), Blowfish, CAST128, Arcfour, and 3DES ciphers) and uses a real HMAC algorithm for enhanced data integrity control.

It is recommended to use v2 whenever possible.

Authentication

The SSH protocol is designed to verify first the host and then the incoming clients by using public keys and optionally passwords. When an external client wants to make a secure connection it first retrieves the public key from the MultiCom Firewall itself to validate the MultiCom is the correct SSHVPN gateway and another server is not being used to impersonate it.



Once the client software or user verifies that the MultiCom Firewall is correct (and optionally saves it to an internal file so that future verifications at this level can be automated).

After MultiCom Firewall is validated as the SSH host the incoming client can be validated in one of following ways:

- Username & Password
- Username only (without password)
- Username and a public key

After the client authenticates it can ask for services such as port forwarding, compression, access to the CLI interface of the MultiCom Firewall and pick the cipher to be used for transferring data. If the MultiCom Firewall is configured to offer these services to the user they will be allowed, otherwise, disabled SSH services will be refused.

Username And Password

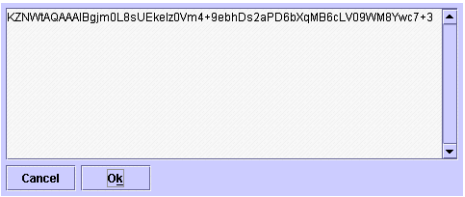
When the "Passwords" option of the SSH panel is enabled then usernames with passwords on the MultiCom Firewall may access the MultiCom as an SSH client. A maximum of 10 different usernames and passwords can be configured.

Username Only

When the "Empty passwords" option is enabled, users on the MultiCom Firewall that do not have passwords may access the MultiCom as an SSH client. Users with passwords will not be allowed even if they enter nothing for their password.

Username And A Public Key

When the "Public keys" option is enabled then usernames with a valid public key (RSA or DSA for v2 or only RSA for v1) can be used as to authenticate the user. User's public keys can be stored in the MultiCom Firewall. Depending on the Client software being used, the key of the user may need to be validated at the time of use.



The client software must generate the Public Key for the incoming user.

Configuring An SSH VPN

Enabling the SSH server on the MultiCom Firewall can be quickly done on the Configurator's tab for SSH (this window is only available after installation of the SSH option.)

The administrator of the MultiCom Firewall chooses which services to allow incoming users to request and the incoming client has the responsibility to ask for the services and authentication to use.

For example, enabling all of the options allows the incoming client to decide how to authenticate, with a username & password, with just a username, or with a public key. Choosing Protocol version 1+2 allows the incoming client to choose which version of SSH to use.

CAUTION - Only one user can log into the CLI interface at one time. For multiple users to have access through SSH be sure that they are configured to request tunnels only and disable CLI access in the User Management of the MultiCom Firewall.

Optionally a Banner Text can be entered in the SSH panel. The text contents of this field are sent to the remote user before authentication is allowed. The Welcome Text will normally be shown only after a successful client authentication (if the client software supports receiving this message.)

Port Forwarding

Allows data to be forwarded through an authenticated SSH connection. Responses to this data flow will be redirected back through the SSH connection. If at any time the SSH connection stops the Port Forwarding will also stop. If the MultiCom Firewall is configured to accept Port Forwarding requests an authenticated client can request 1 or more ports on their computer to be redirected through the SSH connection.

Port Forwarding has two general options:

- Port Forwarding: from the local SSH client to a remote server through the MultiCom Firewall
- Gateway: ports on the Remote MultiCom Firewall are opened and redirected to the local SSH client.

The first option is the most common. The SSH client software will open ports on the computer it is running on and redirect any data received on those ports to a remote machine. For instance, using Port Forwarding to redirect packets arriving on port TCP 80 (of the SSH client machine) to a webserver on the secured network protected by the MultiCom Firewall. If the a user on the SSH client computer directs a web browser to http://127.0.0.1 they will arrive instead at the remote machine, with the data between the SSH client and the remote MultiCom Firewall being secured. Common ports that might use SSH Port Forwarding for secured connections:

Table 1: Common ports to redirect over SSH

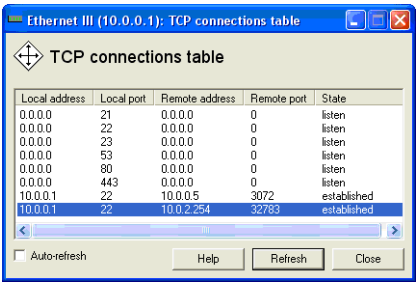
Protocol	TCP Port
Remote Desktop	3389
Email POP3	110
Email SMTP	25
Email IMAP	143
HTTP	80
Telnet	23
VNC	5900
Rsync	873

Most SSH client software offer the option to allow this tunnel to be used either only by the computer running the SSH client software or by any computer connected to the same network as the computer running the SSH client software.

Using the Gateway option of SSH Port Forwarding is less common. That is when you want to open ports on the remote MultiCom Firewall and redirect the traffic arriving there to a port on the computer running the SSH client. This might be used for instance when it is the server running the SSH client and wanting to offer its services to clients behind a MultiCom Firewall.

Monitoring SSH Connections

The easiest way to monitor an SSH connection is to activate SNMP in the MultiCom Firewall and use an SNMP browser to see which computers are connected to the SSH VPN Port (by default TCP port 22).



The example above uses the Router IP Console from http://www.innerdive.com/ to browse the TCP connections of an Ethernet III and see two computers that have established active SSH connections to it on port TCP 22.

Chapter 14

Traffic Control

Introduction

MultiCom Firewalls support 2 different types of traffic control URL Filtering and a Network Intrusion Detection System (NIDS). These controls are used along with the dual firewalls to limit outgoing traffic or to monitor incoming traffic.

All MultiCom Firewalls support URL filtering. The NIDS functionality is an add-on option that can be purchased.

URL Filtering

URL filtering on the MultiCom Firewall allows Internet browser traffic to be blocked or logged based on the domain name of the final destination. A maximum of 100 rules can be added that either DROP traffic or BLOCK traffic and send a predefined message to the requesting web browser.

Keywords can be entered in the URL filtering rules that cause matching HTTP traffic to be blocked or dropped. The keyword will be blocked if it is found anywhere in the URL of a web request, including web form requests. Dropping a site with a matching keyword will simply make the browser timeout and appear

as an error. Blocking the site with a matching keyword will send the user instead to a page with personalized text telling them that the site is blocked, this text can be customized.

CAUTION - URL filtering rules are not saved as part of the Configuration file. To save the URL filtering keywords and rules you must either download the list from the web interface at http://10.0.0.1/advanced/filters/ .

Optionally goto the TRAFFIC > URL FILTERING panel of the Configurator software and click the "Edit URL Filtering Rules" button. In the URL Rules Filtering window there is a FILE > SAVE option from the menu.

URL Filter Rules

A maximum of 100 rules can be added that either BLOCK traffic (and send a predefined message to the requesting web browser), or DROP traffic. Accepted characters to spell the URL are defined in RFC1738 (Uniform Resources Locators (URL) specification): 0-9, A-Z, a-z, $ - . + ! * ’ ( ) ,

Entering in the full web site name will block traffic to that website, for example "www.mysite.com" will drop or block all traffic to that site. Optionally you can enter in keywords that will be searched for in the URL. For instance entering "sex" will block URL’s such as www.someplace.com/sex, www.somplace.com/sextant, www.someplace.com/sex.php as well as block www.sex.com.

CAUTION - keywords will not block access to the same websites if the IP address is used since the keyword is not visible in a web request like http://198.133.219.25. To block the actual IP address either enter "198.133.219.25" as a keyword or use SPI filtering.

Per host filtering can be used to block specific parts of only a particular website. This is used to block access to certain Intranet servers by keyword but allow traffic to other sites that use the same keyword. The per host filtering is not for choosing which hosts on the LAN that will be blocked. For example, if the host

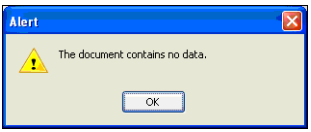
parameter is www.someplace.com, the action is DROP, and the URL is "support", HTTP traffic to www.someplace.com/support will be blocked but www.elsewhere.com/support would still be allowed.

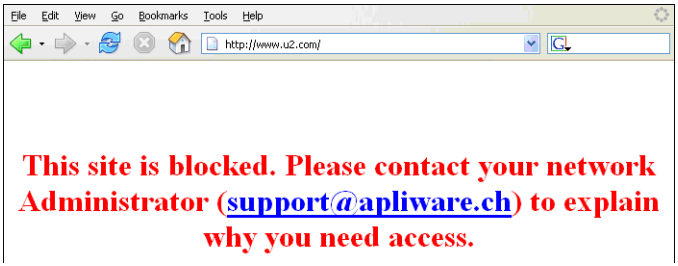
HTTPS traffic can only be blocked according to its domain name or IP address. This is because the rest of the packet is encrypted and the Multicom Firewall does not see anything more than the domain name or the IP address of the traffic request.

Some web traffic use TCP ports other than port 80. If websites such as http://www.apliware.ch:8080 (using port 8080 instead of port 80), then the HTTP(80) only feature should be disabled. Non-HTTP traffic like FTP, telnet, SSH will not be blocked. To block this traffic use the SPI filtering rules.

URL Filter Notifications

Web users will see either a timeout message if the URL filter rule DROPs the traffic or the customized message if the URL filter rule BLOCKs the traffic.





In all cases an Event Log and Syslog message will be generated describing which activity was used, the IP address of who was trying to reach it, the date and the time.

Event logs can be viewed in the Monitor portion of the Configurator, from the Web Interface or received as emails using the Scheduler to send log reports. Sample Event Log messages are below.

```
29/10/2004 19:40:50 FILTER  HTTP request from 10.0.1.100 has been
dropped
29/10/2004 19:34:56 FILTER HTTP request from 10.0.1.100 has been
blocked (2x)
```

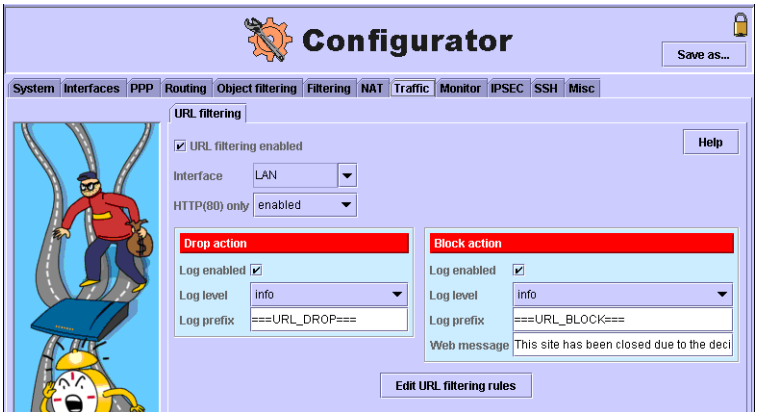
Syslog notifications can only be sent when the syslog service is activated, a valid IP address has been given to receive the syslog messages and a syslog software is running at the selected IP address to receive the syslog messages. These settings can be configured on the MISC > SYSLOG panel. Example Syslog messages are below.

```
kernel: url_blocked:IN=eth1 OUT=ppp0 SRC=10.0.0.75 DST=144.85.15.72
LEN=376 TOS=0x00 PREC=0x00 TTL=127 ID= 43562DF PROTO=TCP SPT=3649
DPT= 80 WINDOW=64240 RES=0x00 ACKPSH URGP= 0
kernel: url_dropped:IN=eth1 OUT=ppp0 SRC=10.0.0.75
DST=198.133.219.25 LEN=518 TOS=0x00 PREC=0x00 TTL=127 ID= 43661DF
PROTO=TCP SPT=3651 DPT= 80 WINDOW=64440 RES=0x00 ACKPSH URGP= 0
```

TIP - if using Syslog messages it can be easier to find a URL filtering message among the many other possible messages by giving it a prefix such as ===URL_BLOCK===.

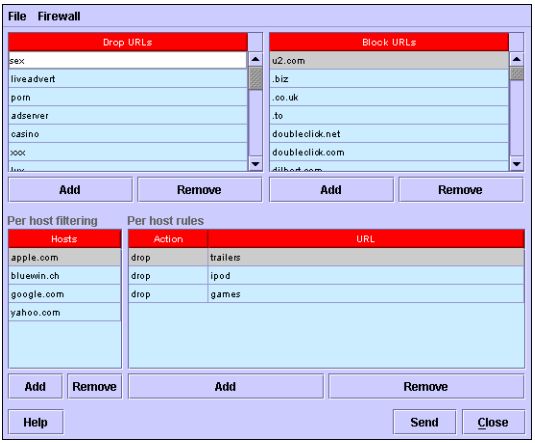
Using URL Filtering

URL Filtering rules can be configured using the Configurator software or by directly accessing the URL filter page of the MultiCom Firewall webserver.



1. Open the Configurator software and connect to the MultiCom Firewall

2. Goto the TRAFFIC > URL FILTERING panel of the Configurator
3. Check the box for URL Filtering enabled
4. Select the LAN interface to block traffic originating from the LAN network
5. Check "log enabled" for both Drop and Block actions
6. Select a syslog Log Level for both Drop and Block actions
7. Add a personalized log prefix for both Drop and Block actions
8. Optionally enter a Blocked site message such as "This site is blocked. Please contact your network Administrator (support@apliware.ch) to explain why you need access."
9. Click the "Edit URL Filtering Rules" button to edit the keywords

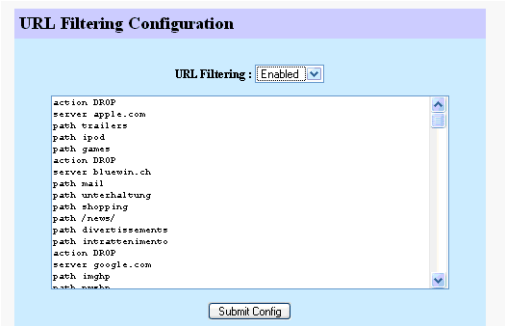


Next you will need to configure keyword lists that you wish will be used to identify traffic that should be blocked.

1. Finish the steps above to activate the URL Filtering functionality
2. Add keywords to either the drop or block list
3. Click the "Send" button to send these keywords to the Secure Firewall
4. Save the configuration to the MultiCom Firewall
5. After saving the configuration to the MultiCom Firewall, try accessing a website with the keyword from a web browser on the LAN network

URL Filter List Web Page

The URL filter lists can also be accessed and enabled from the web browser at http://10.0.0.1/advanced/filters/ where 10.0.0.1 is the IP address of the MultiCom Firewall.



Editing the URL Filter rules as a text files require you to use the exact syntax as seen above. It is recommended that you first make the rules with the Configurator software and use the same syntax as the Configurator creates.

Network Intrusion Detection System

Lightning-Linux 3.5 and above offer a Network Intrusion Detection System (NIDS) based on the well known SNORT engine as an add-on option. NIDS scans all network traffic passing through the MultiCom Firewall and sends real-time syslog notification if network activity is seen that matches the activated traffic signatures. This option allows Network Administrators to identify possible attacks.

This allows workstations and servers behind the Firewall such as web and file servers to be monitored for suspicious traffic.

NOTE - This option is currently only available with the Enterprise models of MultiCom Firewalls.

Features

When activated, the Network Intrusion Detection System will scan and decode all network traffic passing through the MultiCom Firewall. Each data packet is compared to a list of suspicious network activity and traffic patterns.

When using the NIDS option the following signature categories are available to scan network traffic:

- Access
- Attacks
- Databases
- Email
- Files
- Info
- Multimedia
- Services
- Web

More information on the SNORT engine can be found at http://www.snort.org .

Complete rules descriptions can be downloaded at http://www.snort.org/dl/rules/ .

NIDS Configuration Scenarios

With the NIDS option the MultiCom Firewall can monitor traffic for the following types of activities:

- Identify known attacks and probes directed at internal servers (for instance a port scan or Denial of Service attack)
- Identify common network and high bandwidth traffic such as multimedia and Peer-to-Peer traffic
- Scan incoming email for potential viruses
- Identify potentially dangerous network activity on the network

Access

Rules for remote services (rsh, rlogin), shell code exploits, attempts to access telnet without passwords.

Table 1: NIDS Access Rules

Rules	Description
rservices.rules	remote services (rsh, rlogin)
shellcode.rules	shellcode exploits, +
telnet.rules	telnet exploits and access to accounts

Attacks

Rules for identifying machines on the network that have been compromised, traffic that should not be appearing on any network, well known backdoor exploits, denial and distributed denial of service attacks, well known exploits, network scanners such as port scanning, ip mapping and various application scanners, finding other IDS on the network.

Table 2: NIDS Attack Rules

Rules	Description
attack-response.rules	signatures of a possibly compromised network machine
bad-traffic.rules	traffic that should never be seen on a network
backdoor.rules	signatures well known back door exploits
dos.rules	signatures of Denial of Service attacks
ddos.rules	signatures of Distributed Denial of Service attacks
exploit.rules	miscellaneous well-known exploits
scan.rules	network scanner detection (port scanning, ip mapping, and various application scanners)
other-ids.rules	detection of other IDS software running on the network

Databases

Rules for SQL database exploits, dangerous Oracle traffic, and dangerous MySQL traffic.

Table 3: NIDS Database Rules

Rules	Description
sql.rules	known attacks against SQL servers
oracle.rules	unusual and potentially dangerous Oracle server traffic
mysql.rules	unusual and potentially dangerous MySQL server traffic

E-mail

Rules for attacks against mail servers (sendmail, etc...), POP2 and POP3attacks, dangerous IMAP traffic, detection of some well known viruses in email.

Table 4: NIDS E-mail Rules

Rules	Description
smtp.rules	known attacks against mail servers (Sendmail, etc...)
pop2.rules	known attacks against pop2 mail servers
pop3.rules	known attacks against pop3 mail servers
imap.rules	known attacks against imap mail serves
virus.rules	possible virus attachments

Files

Rules for FTP attacks, NetBIOS access, malicious files distributed by TFTP and generic TFTP GET and PUT on the network.

Table 5: NIDS File Rules

Rules	Description
ftp.rules	known attacks against ftp file servers
netbios.rules	signatures for netbios activity
tftp.rules	possibly dangerous uses of TFTP

Info

Rules for generic network traffic (HTTP, telnet, FTP), standard (OS pings, routing, etc...) and potentially bad (such as redirect host) ICMP traffic, diverse traffic.

Table 6: NIDS Info Rules

Rules	Description
info.rules	signatures for general network traffic
icmp.rules	scan for potentially bad ICMP traffic
icmp-info.rules	signatures for standard ICMP traffic
misc.rules	signatures for miscellaneous network traffic

Multimedia

Rules for detection of multimedia traffic (sound and video for Quicktime, Windows Media, Shoutcast, Icecast, Audio Galaxy), Xserver traffic, Peer-to-Peer traffic (Gnutella, Napster, Kazaa, Morpheus), chat software (ICQ, MSN, IRC, AIM).

Table 7: NIDS Multimedia Rules

Rules	Description
multimedia.rules	signatures of streaming multimedia
x11.rules	x11 traffic
p2p.rules	signatures of known P2P activity
chat.rules	signatures of various chat programs

Services

Rules for detecting dangerous DNS traffic, FINGER traffic, NNTP server attacks, interesting RPC messages, and dangerous SNMP access.

Table 8: NIDS Service Rules

Rules	Description
dns.rules	signatures of dangerous DNS traffic
finger.rules	detection of "finger" network traffic
nntp.rules	signatures of known NNTP attacks
rpc.rules	detection of interesting RPC traffic
snmp.rules	signatures of dangerous SNMP traffic

Web

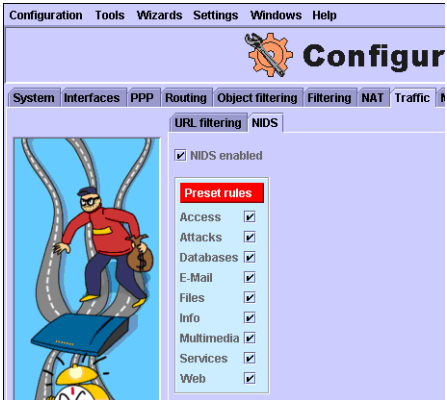
Rules for web server exploits, CGI attacks, web client attacks, Cold Fusion server attacks, Frontpage attacks, IIS server attacks, diverse web attacks, and PHP site attacks.

Table 9: NIDS Web Rules

Rules	Description
web-attacks.rules	signatures of common exploits against web servers
web-cgi.rules	signatures of common CGI attacks
web-client.rules	signatures of attacks against and from web users
web-coldfusion.rules	signatures of attacks against ColdFusion servers
web-frontpage.rules	signatures of attacks against Frontpage software
web-iis.rules	signatures of attacks against IIS servers
web-misc.rules	signatures of potentially dangerous web traffic
web-php.rules	signatures of attacks against sites using PHP

Configuring NIDS

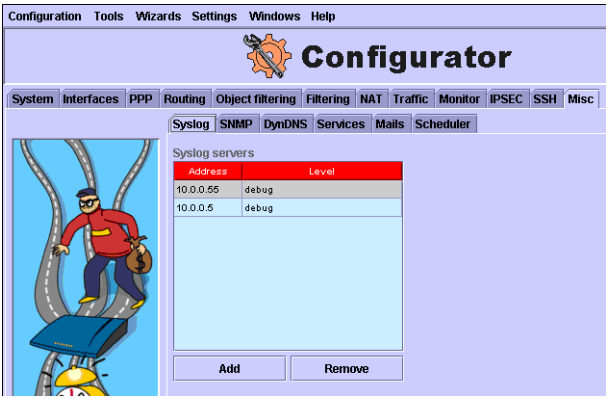
The NIDS option is very simple to use. Simply goto the Configurator window, activate NIDS ENABLED, and select which category of rules signatures you want to use for traffic scanning and save the configuration.



When network activity is detected that matches one of the signature rules a syslog message will be generated and sent to the selected Syslog clients.

Monitoring NIDS Activity

The Syslog service must be activated in the MISC tab of the Configurator software for Syslog messages to be sent. All NIDS notifications will be sent out at the INFO level of Syslog notification to all of the Syslog clients listed in the MISC > Syslog tab of the Configurator.



Below are a list of sample NIDS notifications that could be received as a syslog message.

Network Intrusion Detection Services (NIDS)

2003-06-27 09:47:01Auth.Info10.0.0.1snort[269]: [1:0:0] www.microsoft.com , URL Connection Stopped [Classification: Firewall URL Filtering configuration] [Priority: 1]: {TCP} 10.0.0.55:2510 -> 144.85.15.72:80

2003-06-27 09:47:15Auth.Info10.0.0.1snort[269]: [1:0:0] www.microsoft.com , URL Blocked [Classification: Firewall URL Filtering configuration] [Priority: 1]: {TCP} 10.0.0.55:2513 -> 193.247.134.2:80

2003-06-27 09:47:15Auth.Info10.0.0.1snort[269]: [111:8:1] (spp_stream4) STEALTH ACTIVITY (FIN scan) detection {TCP} 193.247.134.2:61 -> 10.0.0.55:2513

2003-05-13 11:09:08Auth.Info10.0.0.1snort[166]: [1:620:2] SCAN Proxy (8080) attempt [Classification: Attempted Information Leak] [Priority: 2]: {TCP} 208.41.189.170:3024 -> 62.203.39.140:8080

2003-05-13 19:44:58Auth.Info10.0.0.1snort[166]: [1:615:3] SCAN SOCKS Proxy attempt [Classification: Attempted Information Leak] [Priority: 2]: {TCP} 208.2.18.99:4178 -> 62.203.103.92:1080

2003-05-13 11:09:07Auth.Info10.0.0.1snort[166]: [1:618:2] SCAN Squid Proxy attempt [Classification: Attempted Information Leak] [Priority: 2]: {TCP} 208.41.189.170:2949 -> 62.203.39.140:3128

2003-04-04 14:29:21Auth.Info192.168.0.8snort[223]: [1:1545:4] DOS cisco attempt [Classification: Web Application Attack] [Priority: 1]: {TCP} 192.168.0.5:1613 -> 192.168.0.8:80

2003-04-04 14:29:20Auth.Info192.168.0.8snort[223]: [1:1425:6] WEB-PHP content-disposition [Classification: Web Application Attack] [Priority: 1]: {TCP} 192.168.0.5:1613 -> 192.168.0.8:80

2003-03-18 16:43:33Auth.Info10.0.0.1snort[202]: [1:1634:5] POP3 PASS overflow attempt [Classification: Attempted Administrator Privilege Gain] [Priority: 1]: {TCP} 10.0.0.5:1053 -> 80.86.193.49:110

2003-03-18 16:43:33Auth.Info10.0.0.1snort[202]: [1:1866:4] POP3 USER overflow attempt [Classification: Attempted Administrator Privilege Gain] [Priority: 1]: {TCP} 10.0.0.5:1053 -> 80.86.193.49:110

2003-03-18 16:41:23Auth.Info10.0.0.1snort[93]: [1:401:4] ICMP Destination Unreachable (Network Unreachable) [Classification: Misc activity] [Priority: 3]: {ICMP} 10.0.0.1 -> 10.0.0.5

2003-03-18 16:41:36Auth.Info10.0.0.1snort[93]: [1:1411:3] SNMP public access udp [Classification: Attempted Information Leak] [Priority: 2]: {UDP} 10.0.0.5:1030 -> 193.5.2.50:161

2003-03-14 15:35:07Auth.Info10.0.0.1snort[489]: [1:384:4] ICMP PING [Classification: Misc activity] [Priority: 3]: {ICMP} 10.0.0.5 -> 10.0.0.1

2003-03-14 15:35:07Auth.Info10.0.0.1snort[489]: [1:408:4] ICMP Echo Reply [Classification: Misc activity] [Priority: 3]: {ICMP} 10.0.0.1 -> 10.0.0.5

2003-03-14 15:21:00Auth.Info10.0.0.1snort[93]: [1:382:4] ICMP PING Windows [Classification: Misc activity] [Priority: 3]: {ICMP} 10.0.0.5 -> 10.0.0.1

2003-05-12 17:04:45Auth.Info10.0.0.1snort[166]: [1:469:1] ICMP PING NMAP [Classification: Attempted Information Leak] [Priority: 2]: {ICMP} 62.134.77.168 -> 213.3.68.237

2003-05-13 15:55:41Auth.Info10.0.0.1snort[166]: [1:499:3] ICMP Large ICMP Packet [Classification: Potentially Bad Traffic] [Priority: 2]: {ICMP} 195.186.0.98 -> 195.186.194.190

2003-05-14 15:12:47Auth.Info10.0.0.1snort[166]: [1:474:1] ICMP superscan echo [Classification: Attempted Information Leak] [Priority: 2]: {ICMP} 217.84.251.248 -> 62.202.69.61

2003-05-12 18:00:23Auth.Info10.0.0.1snort[166]: [1:449:4] ICMP Time-To-Live Exceeded in Transit [Classification: Misc activity] [Priority: 3]: {ICMP} 219.93.216.162 -> 10.0.0.5

2003-05-12 14:09:11Auth.Info10.0.0.1snort[164]: [1:1432:3] P2P GNUTella GET [Classification: Misc activity] [Priority: 3]: {TCP} 10.0.0.5:4855 -> 67.9.98.30:3605

2003-05-12 16:11:04Auth.Info10.0.0.1snort[180]: [1:556:4] P2P Outbound GNUTella client request [Classification: Misc activity] [Priority: 3]: {TCP} 62.203.68.58:3131 -> 24.209.129.42:6347

2003-05-13 02:30:49Auth.Info10.0.0.1snort[166]: [1:1699:2] P2P Fastrack (kazaa/morpheus) traffic [Classification: Generic Protocol Command Decode] [Priority: 3]: {TCP} 62.203.39.140:2123 -> 65.71.41.232:1214

2003-05-13 14:39:02Auth.Info10.0.0.1snort[166]: [1:1841:2] WEB-CLIENT javascript URL host spoofing attempt [Classification: Attempted User Privilege Gain] [Priority: 1]: {TCP} 129.33.21.40:80 -> 195.186.194.190:1499

2003-05-12 15:19:55Auth.Info10.0.0.1snort[180]: [1:1149:9] WEB-CGI count.cgi access [Classification: access to a potentially vulnerable web application] [Priority: 2]: {TCP} 62.203.68.58:2319 -> 209.130.129.232:80

2003-05-12 15:41:49Auth.Info10.0.0.1snort[180]: [1:1091:6] WEB-MISC ICQ Webfront HTTP DOS [Classification: Web Application Attack] [Priority: 1]: {TCP} 62.203.68.58:2645 -> 209.73.225.7:80

2003-05-12 15:44:21Auth.Info10.0.0.1snort[180]: [1:1767:3] WEB-MISC search.dll access [Classification: access to a potentially vulnerable web application] [Priority: 2]: {TCP} 62.203.68.58:2692 -> 66.135.194.135:80

2003-05-12 16:24:33Auth.Info10.0.0.1snort[166]: [1:1560:4] WEB-MISC /doc/ access [Classification: access to a potentially vulnerable web application] [Priority: 2]: {TCP} 62.203.39.140:1209 -> 216.185.87.221:80

2003-05-13 08:21:10Auth.Info10.0.0.1snort[166]: [1:1260:6] WEB-MISC long basic authorization string [Classification: Attempted Denial of Service] [Priority: 2]: {TCP} 62.203.39.140:3897 -> 216.127.72.105:80

2003-05-12 16:04:10Auth.Info10.0.0.1snort[180]: [1:1997:1] WEB-PHP read_body.php access attempt [Classification: access to a potentially vulnerable web application] [Priority: 2]: {TCP} 62.203.68.58:2973 -> 216.127.72.105:80

2003-05-13 08:11:31Auth.Info10.0.0.1snort[166]: [1:1425:6] WEB-PHP content-disposition [Classification: Web Application Attack] [Priority: 1]: {TCP} 62.203.39.140:3293 -> 216.127.72.105:80

2003-05-12 16:03:53Auth.Info10.0.0.1snort[180]: [1:895:5] WEB-CGI redirect access [Classification: Attempted Information Leak] [Priority: 2]: {TCP} 62.203.68.58:2987 -> 216.127.72.105:80

2003-05-12 17:41:12Auth.Info10.0.0.1snort[166]: [1:1243:8] WEB-IIS ISAPI .ida attempt [Classification: Web Application Attack] [Priority: 1]: {TCP} 213.3.185.60:1445 -> 213.3.68.237:80

2003-05-12 20:56:15Auth.Info10.0.0.1snort[166]: [1:1256:7] WEB-IIS CodeRed v2 root.exe access [Classification: Web Application Attack] [Priority: 1]: {TCP} 202.111.185.3:2677 -> 213.3.68.237:80

2003-05-12 20:56:24Auth.Info10.0.0.1snort[166]: [1:1945:1] WEB-IIS unicode directory traversal attempt [Classification: Web Application Attack] [Priority: 1]: {TCP} 202.111.185.3:2931 -> 213.3.68.237:80

2003-05-12 20:56:22Auth.Info10.0.0.1snort[166]: [1:1288:5] WEB-FRONTPAGE /_vti_bin/ access [Classification: access to a potentially vulnerable web application] [Priority: 2]: {TCP} 202.111.185.3:2888 -> 213.3.68.237:80

2003-05-12 22:31:09Auth.Info10.0.0.1snort[166]: [1:1301:4] WEB-MISC admin.php access [Classification: Attempted Information Leak] [Priority: 2]: {TCP} 62.203.39.140:4824 -> 216.127.72.105:80

2003-05-12 22:31:26Auth.Info10.0.0.1snort[166]: [1:882:4] WEB-CGI calendar access [Classification: Attempted Information Leak] [Priority: 2]: {TCP} 62.203.39.140:4847 ->

212.67.195.50:80

2003-05-13 14:23:56Auth.Info10.0.0.1snort[166]: [1:1478:3] WEB-CGI swc access [Classification: Attempted Information Leak] [Priority: 2]: {TCP} 195.186.194.190:1118 -> 205.141.213.7:80

2003-05-13 14:23:57Auth.Info10.0.0.1snort[166]: [1:1390:3] SHELLCODE x86 inc ebx NOOP [Classification: Executable code was detected] [Priority: 1]: {TCP} 64.37.137.83:80 -> 195.186.194.190:1113

2003-05-14 08:23:54Auth.Info10.0.0.1snort[166]: [1:1394:3] SHELLCODE x86 NOOP [Classification: Executable code was detected] [Priority: 1]: {TCP} 212.243.221.200:80 -> 195.186.128.25:1139

2003-05-13 14:24:36Auth.Info10.0.0.1snort[166]: [1:853:6] WEB-CGI wrap access [Classification: Attempted Information Leak] [Priority: 2]: {TCP} 195.186.194.190:1125 -> 205.141.213.7:80

2003-05-12 16:49:36Auth.Info10.0.0.1snort[166]: [1:2003:2] MS-SQL Worm propagation attempt [Classification: Misc Attack] [Priority: 2]: {UDP} 61.48.17.3:1425 ->

62.203.39.140:1434

Chapter 15

High Availability

Introduction

Lightning-Linux 3.6 and above supports High Availability using the Virtual Router Redundancy Protocol (VRRP) as an add-on option. VRRP allows 1 or more additional MultiCom Firewalls to be configured into a redundant fail-safe backup in case of failure on the Master firewall.

This High Availability does not require dynamic routing or router discovery protocols to be installed on local networking devices.

VRRP Configuration Scenarios

With the High Availability option the MultiCom Firewall the following services can be sustained in case of a Firewall device failure:

- IPSec secured remote access services
- Routing services, allowing uninterrupted IP traffic
- DNS services
- SSH services
- NTP services

VRRP Protocol

The Virtual Routing Redundancy Protocol (VRRP) is an election process that automatically assigns and maintains networking services in a "virtual firewall" that resides in a VRRP enabled MultiCom Firewall. This means that 2 or more MultiCom Firewalls can be in charge of a virtual firewall which provides services to a connected network. If one of the devices fails another will take over the responsibility of running the virtual firewall.

When using the VRRP option the following services are available to configure the virtual firewall:

- Address Owner: the actual address of a physical interface, this is the firewall that always takes control when it is available
- Router ID: a number between 1 and 255 to specify groups of backup firewalls
- Priority: a priority set between 1 and 254, this number is used to choose which firewall will be used to replace a failed Master firewall
- Advertisement: the interval time in seconds between polling the connected VRRP devices for the status of each device
- Authentication: optionally use authentication between each VRRP device
- Virtual IP Addresses: the virtual IP addresses that are being protected with High Availability

Switching to the Backup firewall will take about 3-5 seconds. If there are more than one Backup firewall the one with the highest Priority value is chosen. When a firewall with a higher priority is available it will become the new Master firewall. When the firewall that is the owner of the IP addresses is available it will always take control from any other Master firewalls.

More information on the VRRP protocol can be found in RFC 2338.

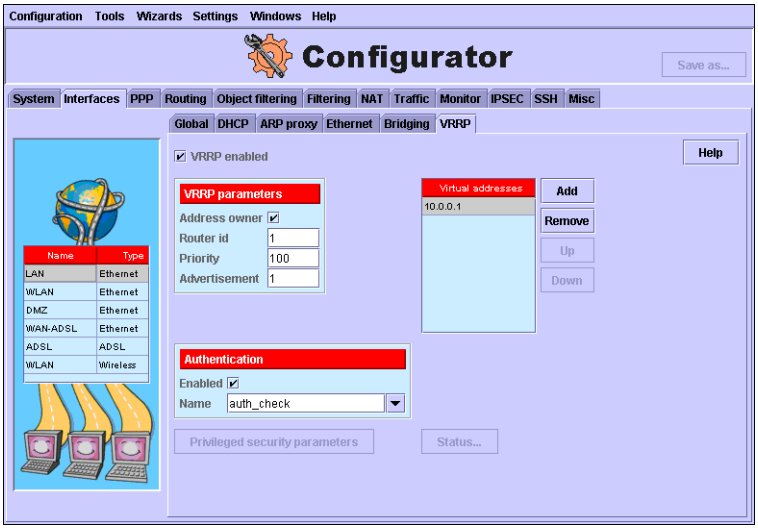
Configuring VRRP

There are 2 ways to configure VRRP for a subnet:

1. **With Owner IP Address**: One firewall is designated the Owner of the IP address with 1 or more additional firewalls configured as Backup firewalls. The protected IP address must be the real IP address of the selected interface.
2. **Without Owner IP Address**: A virtual IP address is chosen that normally is

not being used on the subnet. Each VRRP Backup firewall is configured to protect the virtual IP address. Because there is no Owner each VRRP backup firewall must have a different Priority level which is used to decide which firewall is the current Master firewall.

The Master firewall is the firewall that currently controls the protected IP address (this is usually the Owner unless the Owner is not available). When the Master firewall fails or is not responsive a Backup firewall is chosen through an election process to become the new Master firewall.



Networking activity such as routing will change automatically. VPN connections such as IPSec or SSH Port Forwarding will be disconnected and VPN clients will need to be reconnected.

TIP - If an IPSec connection is created between 2 MultiCom Firewall's, Dead Peer Detection (DPD) can be used to make an automatic switch of services in about 20 seconds (configuring DPD with a delay of 5 seconds and a timeout of 10 seconds.)

Each VRRP enabled firewall will still retain its unique IP address for its own interfaces which can be used to reach firewall for configuration or monitoring. Multicast packets are used to make advertisements in the group 224.0.0.0.18/32.

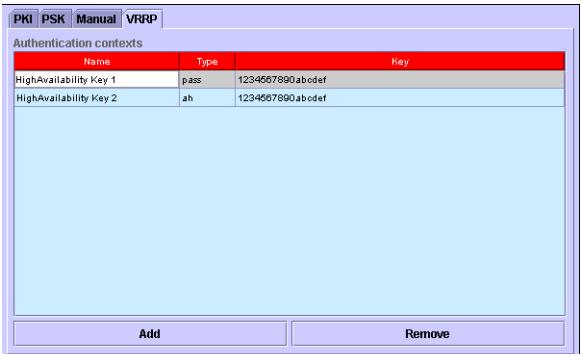
The VRRP IP address will be responded to with a new virtual MAC hardware address such as 00-00-5e-00-01-xx where xx is the hexadecimal value of the Router ID.

> WARNING - During the backup process, the backup firewall will use the virtual MAC hardware address to respond to IP requests of the VRRP IP address and its own physical interface. This means that after the original firewall is restored the backup firewall will be unreachable with its own IP address until your computer's ARP table is cleared either manually or automatically.

Authentication

Authentication options for VRRP include no authentication, a simple password, or strong authentication using Authentication Headers (AH). The authentication must match between all Backup and Master firewalls.

To enter in new authentication keys click on the Privileged Security Parameters button and select the VRRP tab.

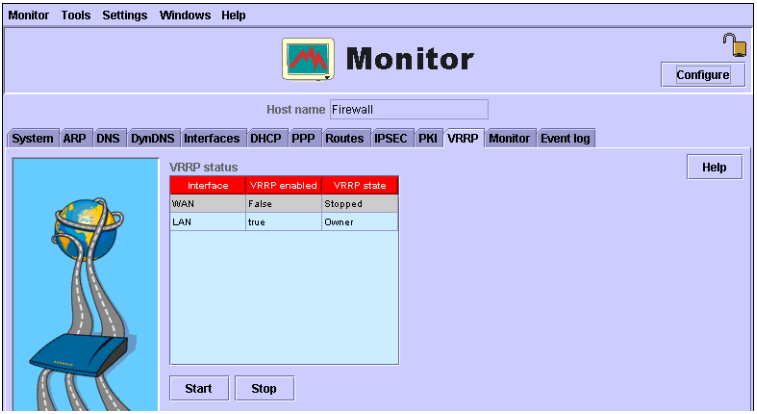


This window will allow you to create keys that can be selected in the main VRRP window. Each each keys can use either a simple password or use the strong authentication using Authentication Headers (AH).

These keys will be saved in the Security Configuration file of the MultiCom Firewall.

Monitoring VRRP

Diagnostics and status information on VRRP are available from the MultiCom web server at http://10.0.0.1/vrrp/ or from the VRRP tab of the Configurator software's Monitor window. Additionally, when VRRP activity occurs on the network Syslog messages are generated using the real IP address of the VRRP firewall.



Requirements And Limitations

Some requirements and limitations of the VRRP option on MultiCom Firewalls are listed below.

- VRRP on the MultiCom Firewalls only works with other MultiCom Firewalls using VRRP.
- If VPN options are being used the security configuration and keys must be the same on all backup firewalls and the master firewall.
- VRRP Firewall groups must have matching Authentication values and be able to communicate with Multicast packets in 224.0.0.0.18/32. A group is defined as all VRRP firewalls that have the same Router ID number and are protecting the same IP address.
- Router IDs and their protected IP addresses must stay together as a group. The group can be configured on multiple MultiCom Firewalls but the same Router ID number must protect the same IP address or addresses. If

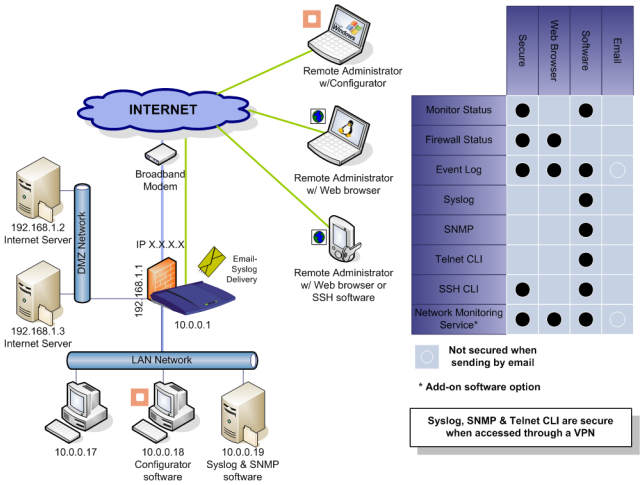
additional groups of VRRP firewalls are used on the same subnet then the Router IDs and protected IP addresses must be different.

- One VRRP device can have multiple VRRP interfaces but they must use different Router IDs and protect different IP addresses. For example the LAN interface can be protecting its IP address as a the network default gateway at the same time that the WAN interface is protecting its IP address as a VPN gateway.
- VRRP can only be configured on physical Ethernet interfaces with a static IP address.

Chapter 16

Alerts & Diagnostics

MultiCom Firewalls offer many ways to monitor the status of the MultiCom Firewall and the surrounding networks. Errors and logs can also be scheduled to be sent at regular intervals using the Email or Syslog features.



Status and diagnostics can be viewed using the following features:

- Network Monitoring Service (add on option)
- Event Log
- Monitor Software Diagnostics
- Webserver Status Pages
- Email Messages
- Syslog Messages
- SNMP Polling
- Command Line Interface Status

MultiCom Firewalls can optionally send alerts telling the status and activity of certain processes on the Firewall. Syslog and Email Messages provides this functionality. Email messages can be sent to different SMTP email accounts with the latest event logs or error reports.

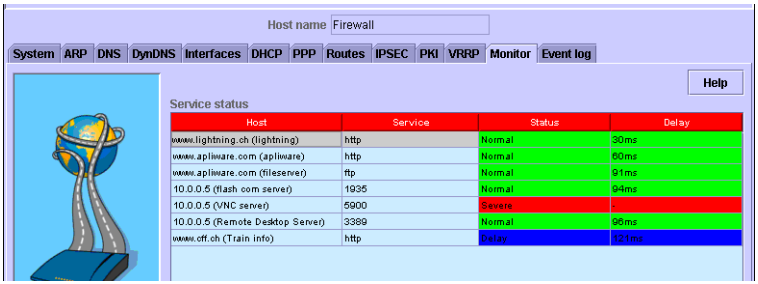
SNMP allowing SNMP browser software to read status information from the Firewall and Syslog messages send messages to selected Syslog servers.

Please see “Using Syslog Messages” on page 306 for more information on Syslog features.

Network Monitoring

When the Network Monitoring Service Option has been installed into any MultiCom Firewall it becomes possible to monitor the status of network devices and services with the Firewall.

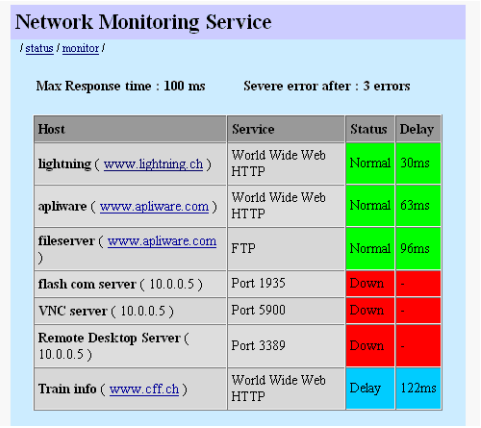
The Network Monitoring Service allows the MultiCom Firewall to regularly check TCP services on local and remote networks. At predefined intervals the MultiCom will attempt to connect to each service in the "Hosts" list. Notification by email, event log or syslog can be sent if there are errors, severe errors, or delays.



The status of the network monitoring services can also be viewed in the following places:

- Monitoring panel of the Monitor software (part of the Configurator software)
- Received as syslog messages
- Event log panel of the web interface of the MultiCom Firewall
- Event log panel of the Monitor software
- Received as email when valid email accounts are configured

Viewing the Event logs through the MultiCom Firewall's web server requires an Internet Browser and a valid username and password to access the MultiCom Firewall. This can be done securely using the HTTPS interface or within an SSH or IPSec VPN tunnel.



Syslog notifications can only be sent when the syslog service is activated, a valid IP address has been given to receive the syslog messages and a syslog software is running at the selected IP address to receive the syslog messages. These settings can be configured on the MISC > SYSLOG panel. Example Syslog messages are below.

```
08-04-2004 23:41:56 Daemon.Notice 10.0.0.10 Admind[96]: NMS: Delay
on host 10.0.0.1 , service FTP
08-04-2004 23:41:56 Daemon.Notice 10.0.0.10 Admind[96]: NMS: Delay
on host www.apliware.com , service World Wide Web HTTP
2004-08-04 18:32:37 Daemon.Notice 10.0.0.10 Admind[96]: NMS: Severe
error on host 10.0.0.55 , service Port 3300
2004-08-04 18:32:37 Daemon.Notice 10.0.0.10 Admind[96]: NMS: Severe
error on host 10.0.0.55 , service Port 1935
```

Event logs can be viewed in the Monitor portion of the Configurator, from the Web Interface or received as emails using the Scheduler. Sample Event Log messages are below.

```
04/08/2004 23:41:56   NMS   Delay on host 10.0.0.1 , service FTP
04/08/2004 23:41:56   NMS   Delay on host www.apliware.com , service
World Wide Web HTTP
04/08/2004 23:22:13   NMS   Severe error on host 10.0.0.55 , service
Port 3300
04/08/2004 23:22:13   NMS   Severe error on host 10.0.0.55 , service
Port 1935
```

Emails notifications can only be sent when emails are enabled and there are valid email recipients. These settings can be configured on the MISC > MAILS panel. An example email is below.

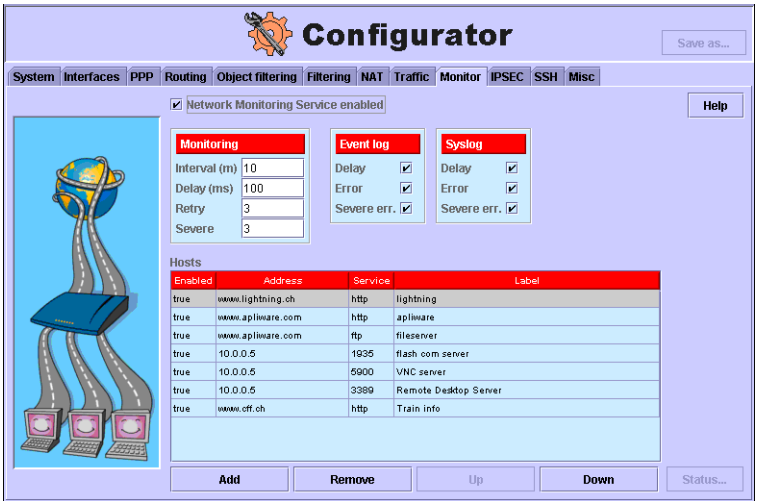
```
From: Firewall@bluewin.ch
Sent: Friday, August 20, 2004 3:00 PM
To: support@mycompany.ch
Subject: Error


ERROR : Severe error on host 10.0.0.55 , service Port 1935
============================================================

Date             : 29/10/2004 11:42:56
E-Mail Client    : shawn

Hostname         : Firewall

Hardware Type    : MultiCom Ethernet III
Serial Number    : LI-MU10-CH-020576
Firmware version : 3.7
```

```
Last Events History
===================
21/08/2004 08:00:29 , Service : NMS        , Error : Severe error on
host 10.0.0.55 , service Port 1935
```

Configuring Network Monitoring

To configure Network Monitoring you first must have installed the Network Monitoring option key using the web interface of the MultiCom Firewall. This is available at http://10.0.0.1/tools/options/ where 10.0.0.1 is the IP address of the MultiCom Firewall. The rest of the configuration steps are as follows.

1. Open the Configurator software and connect to the MultiCom Firewall
2. Goto the Monitor panel of the Configurator software
3. Check the box for Network Monitoring Service enabled
4. Add a host IP address or FQDN (such as someplace.com) that has a TCP Service to be checked
5. Select the port number of the service to check (right click the mouse to see a list of services)
6. Add a personalized label to this check.



Event Log

The MultiCom Firewall keeps an internal log of system events and errors. This log is automatically generated by the Firewall and will contain the following information.

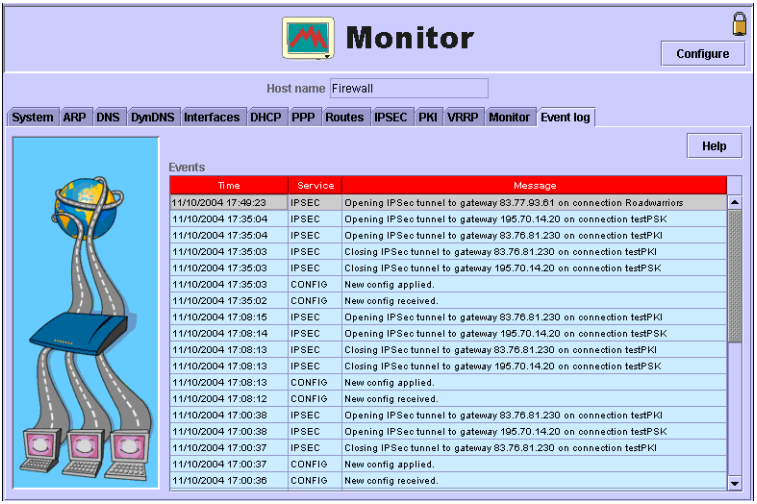
- System startup information
- Login activity and errors
- Service errors (such as DNS, NTP, FTP and others)
- Network monitoring errors or delays
- Scheduling activity
- IPSec activity
- PPP activity
- DHCP activity

NOTE - The most detailed status logs for the MultiCom Firewall are available by activating the Syslog functionality. Due to the size of these messages they are not stored on the Multicom Firewall itself and require an external software to receive and optionally store these messages. This can be found in the Syslog section below.

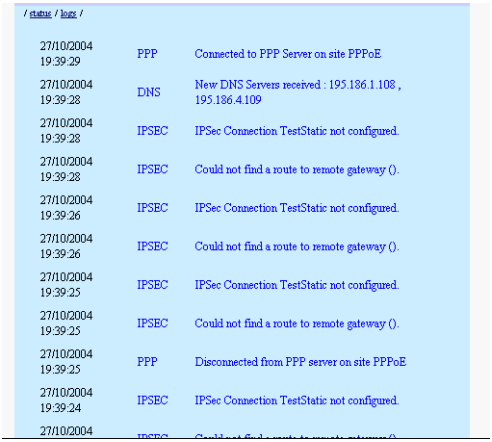
Viewing Event Logs

Event logs can be viewed in the Monitor portion of the Configurator, from the Web Interface or received as emails using the Scheduler.

Viewing the Event logs through Monitor portion of the Configurator requires an network access to the MultiCom Firewall, a computer to run the Configurator software (directly from the CDROM or installed on the computer's hard drive) and a valid username and password to access the MultiCom Firewall. This can be done securely using the HTTPS interface or within an SSH or IPSec VPN tunnel.



Viewing the Event logs through the MultiCom Firewall's web server requires an Internet Browser and a valid username and password to access the MultiCom Firewall. This can be done securely using the HTTPS interface or within an SSH or IPSec VPN tunnel.



Event logs can be sent at regular intervals by configuring the Scheduler and adding valid email accounts to the MultiCom Firewall. An email will be sent from the MultiCom Firewall to the configured accounts. An example email is below.

```
From: Firewall@bluewin.ch
Sent: Friday, August 20, 2004 3:00 PM
To: support@mycompany.ch
Subject: Log


Date              : 20.09.2004 / 15:00:06
E-Mail Client     : support

Hostname          : FirewallGeneva

Hardware Type     : MultiCom SpeedSurf
Serial Number     : LI-MU11-CH-022518
Firmware version : 3.7

Last Events History
===================
20/08/2004 15:00:06 , Service : TIMER      , Info  : Send Logs E-mail
20/08/2004 14:59:51 , Service : FILTER     , Info  : HTTP request from
10.0.0.55 has been blocked
20/08/2004 14:10:09 , Service : NMS        , Info  : Delay on host
10.0.0.5 , service Port 1935
20/08/2004 14:10:09 , Service : NMS        , Info  : Delay on host
www.apliware.com , service World Wide Web HTTP


20/08/2004 14:10:09 , Service : NMS        , Info  : Delay on host
www.lightning.ch , service World Wide Web HTTP


20/08/2004 14:05:05 , Service : TIMER      , Info  : Send Logs E-mail
20/08/2004 14:00:10 , Service : NMS        , Info  : Delay on host
10.0.0.5 , service Port 1935
20/08/2004 14:00:10 , Service : NMS        , Info  : Delay on host
www.apliware.com , service World Wide Web HTTP


20/08/2004 14:00:10 , Service : NMS        , Info  : Delay on host
www.lightning.ch , service World Wide Web HTTP


20/08/2004 14:00:05 , Service : TIMER      , Info  : Send Logs E-mail
(5x)
20/08/2004 11:34:09 , Service : SYSTEM     , Info  : Time/Date
adjusted by NTP
```

```
20/08/2004 11:30:44 , Service : DYNDNS    , Info  : Successful update
of IP address.
20/08/2004 11:30:41 , Service : IPSEC     , Info  : Opening IPSec
tunnel to gateway 62.202.66.217 on connection gostan
20/08/2004 11:30:38 , Service : DNS       , Info  : New DNS Servers
received : 195.186.1.108 , 195.186.4.109
20/08/2004 11:30:33 , Service : PPP       , Info  : Connected to PPP
Server on site PPPoE
20/08/2004 11:30:28 , Service : IPSEC     , Info  : Opening IPSec
tunnel to gateway 195.70.14.20 on connection big2
20/08/2004 11:30:27 , Service : DHCP      , Info  : Configuration
changes for DHCP Server.
20/08/2004 11:30:27 , Service : CONFIG    , Info  : New config
applied.
20/08/2004 11:30:26 , Service : SSH       , Info  : Starting SSH
access.
20/08/2004 11:30:26 , Service : DYNDNS    , Info  : Starting DynDNS.
20/08/2004 11:30:20 , Service : FILTER    , Info  : SecureWall
enabled
20/08/2004 11:30:16 , Service : IPSEC     , Info  : Starting IPSec
service.
20/08/2004 11:30:15 , Service : SNMP      , Info  : Starting SNMP.
20/08/2004 11:30:15 , Service : FTP       , Info  : Starting FTP
Server.
20/08/2004 11:30:15 , Service : DHCP      , Info  : Starting DHCP
Server.
20/08/2004 11:30:12 , Service : PPP       , Info  : MSS hack
installed.
20/08/2004 11:30:10 , Service : OPTIONS   , Info  : NMS Option
enabled.
20/08/2004 11:30:10 , Service : OPTIONS   , Info  : PayNET Option
enabled.
20/08/2004 11:30:10 , Service : OPTIONS   , Info  : VRRP enabled.
20/08/2004 11:30:10 , Service : OPTIONS   , Info  : SSH VPN enabled.
20/08/2004 11:30:10 , Service : OPTIONS   , Info  : IPSec enabled (
20 tunnels )
20/08/2004 11:30:10 , Service : CONFIG    , Info  : Configure
Ethernet interface WAN
20/08/2004 11:30:10 , Service : CONFIG    , Info  : Configure
Ethernet interface LAN
20/08/2004 11:30:10 , Service : CONFIG    , Info  : Starting System
...
End of log
```

Diagnostics with the Monitor

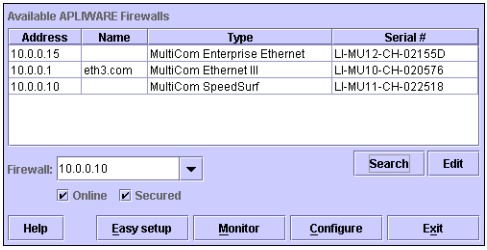
The Configurator software for your MultiCom Firewall includes detailed monitoring windows. These diagnostic utilities give you the current state of your firewall whether it is on a local or remote network.

> CAUTION - when accessing remote MultiCom Firewalls on the Internet it is recommended to always use the Configurator in "Secured" mode to protect the information exchanges.

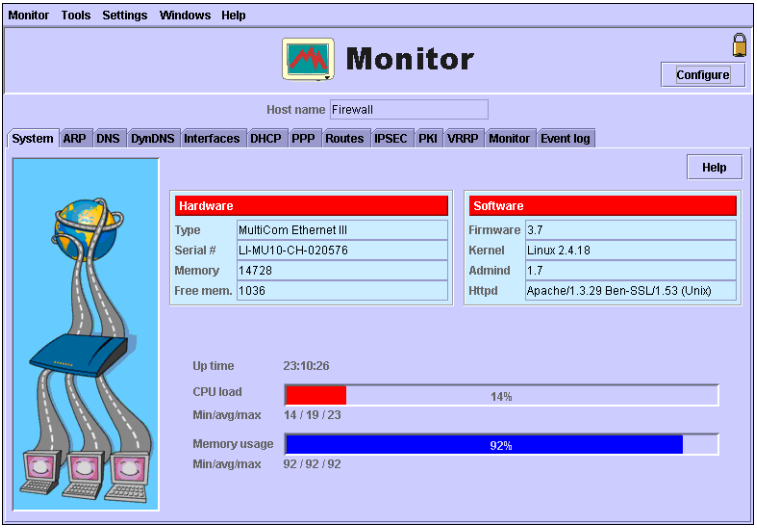
With the monitoring options you will be able to get information on the System status, ARP tables, DNS, each interface, DHCP services, installed routes and more.

Optionally you could also have a syslog server set to listen for info level announcements from the MultiCom Firewall and watch for alerts, warnings, notices and other information.

1. To reach the monitoring screens of the Configurator you will need to first start the Configurator from CD, hard disk or a remote drive. (see the section on Starting Easy Setup or Installing the Configuration Software if you need assistance in starting the Configurator).



2. Click search to search for the MultiCom Firewall on your local network or just enter the IP address of the firewall you wish to monitor
3. Be sure "Online" and "Secured" buttons are checked and click on the Monitor button
4. You should now have arrived at the screen titled Monitor. Depending on what sort of diagnostics you are looking for, go to the appropriate screen.



You should now have arrived at the screen titled Monitor. Depending on what sort of diagnostics you are looking for, go to the appropriate screen. Screenshots of all of the screens can be found in the "Monitor Panels" Appendix on page 529.

Panels	Available Information
System	General information about the hardware, firmware and work load of your MultiCom Firewall.
ARP	The currently active ARP table in the firewall
DNS	The currently active DNS servers for the firewall
Dynamic DNS	The current status of a Dynamic DNS configuration if one exists
Interfaces	Status of each interface port (LAN/WAN), identifying information, and data traffic reports
DHCP	Client Window— shows all of the configuration data received from a DHCP server Server Window — shows currently assigned IP addresses and their lease times.
PPP	Describes current status of PPPoE interfaces if they are active
Routes	The currently active routes in your firewall
Event Log	Events being generated by the MultiCom Firewall

Webserver Status Reports

By using a web browser you can get status information of ARP and routing tables, interfaces, memory and CPU loads, uptime and more. You just type in the IP address of the MultiCom Firewall's LAN or WAN interface, enter any necessary user names and passwords, and can browse the firewall's status. You can also print this information out using your web browser's print functions.

Starting in Lightning-Linux 3.4 the webserver provides direct status information of the Firewall, services, interfaces, and logged events. To see all of the web servers status screens see "Status Firewall" on page 476.

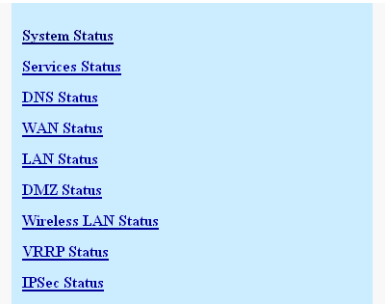


Table 1: Common web server diagnostics pages for LL 3.0-3.3

Description	url address to enter into a web browser
MultiCom Serial number	http://10.0.0.1/config/system/hardware/
Software version	http://10.0.0.1/config/system/software/
LAN status	http://10.0.0.1/config/interface/ethernet[LAN]/status/
LAN DHCP server leases	http://10.0.0.1/config/interface/ethernet[LAN]/ip/dhcp/server/status/leases/
WAN status	http://10.0.0.1/config/interface/ethernet[WAN]/status/
WAN DHCP client status	http://10.0.0.1/config/interface/ethernet[WAN]/ip/dhcp/client/status/
PPPoE status	http://10.0.0.1/config/interface/ppp[PPPoE]/status/
PPPoE IP status	http://10.0.0.1/config/interface/ppp[PPPoE]/ipcp/status/
PPPoE Link status	http://10.0.0.1/config/interface/ppp[PPPoE]/lcp/status/
Available PPPoE servers	http://10.0.0.1/config/interface/ppp[PPPoE]/pppoe/server_list/
PPTP Status	http://10.0.0.1/config/interface/ppp[PPTP]/status/
PPTP Link status	http://10.0.0.1/config/interface/ppp[PPTP]/lcp/status/
ARP entries	http://10.0.0.1/config/arp/status/arp_entry/
DNS servers used	http://10.0.0.1/config/ip/dns/status/nameserver/

Using the above links will help you to find where a problem may be in versions of Lightning-Linux 3.1-3.3. For example, if you have checked the WAN status or the PPPoE status and they both have IP addresses assigned to them they are functioning normally and your problem is probably somewhere else.

Email Messages

Multiple email accounts can be configured to receive errors or logs. Internal service errors and event logs can be sent to one or more email addresses. Errors are sent automatically to configured email accounts but sending event logs must be configured in the Configurator's MISC > Schedule panel.

Emails can be sent for the following activities.

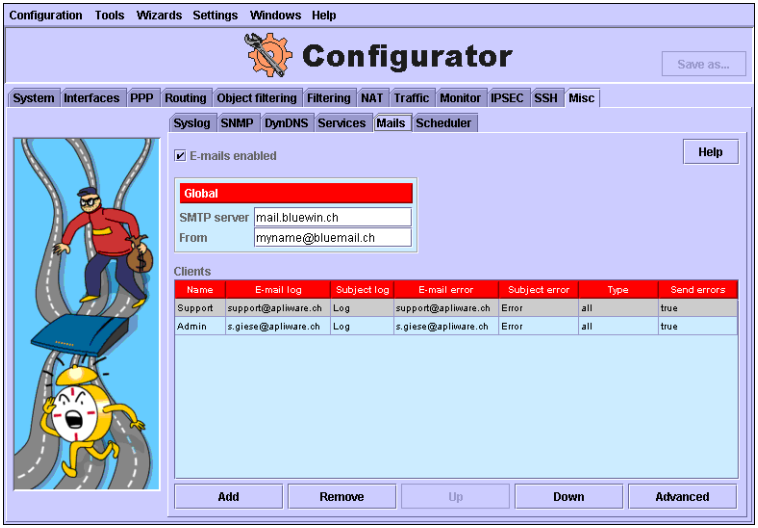
- Service errors for all or selected internal service errors
- URL filtering for blocked or dropped traffic
- Network monitoring errors or delays, when the network monitoring option is installed.

- Event logs when configured in the Scheduler

A valid SMTP email server must be reachable by the MultiCom Firewall and this server must accept emails sent from the MultiCom Firewall using the configured From address.

Configuring Email Messages

Emails can now be sent to 1 or more configured email accounts to notify of errors or to send Event logs. The Scheduler can also identify when to send email logs and to whom.



To configure Email Notification:

1. Open the Configurator software and connect to the MultiCom Firewall
2. Goto the MISC > MAILS panel of the Configurator
3. Check the box for E-mails enabled
4. Enter an SMTP server such as "mail.bluewin.ch"
5. Enter in a complete from address such as Firewall@mydomain.com
6. Add 1 or more email "clients" that can receive email logs or error messages. The clients need a personalized name to be referenced by the Secure Firewall

as well as the actual email address of the "client" such as support@apliware.ch.

7. Optionally change the subjects for the email message. The subject can be the same for log and error emails or they can be different.

NOTE - Email configuration can be tested from the CLI interface with the command "mail test <client>" where <client> is the personalized name of the email client/user or trying to login to the MultiCom Firewall with an invalid account.

CAUTION - Be sure that you are not blocking TCP packets on port 25 from the firewall since this is the port used to send email.

Example Email Error Message

```
From: Firewall@bluewin.ch
Sent: Friday, August 20, 2004 3:00 PM
To: support@mycompany.ch
Subject: Log


ERROR : Could not resolve Gateway Address someplace.com for
connection test2
================================================================
=========

Date              : 29/10/2004 11:42:56
E-Mail Client     : shawn

Hostname          : Firewall

Hardware Type     : MultiCom Ethernet III
Serial Number     : LI-MU10-CH-020576
Firmware version : 3.7

Last Events History
===================
29/10/2004 11:42:56 , Service : IPSEC     , Error : Could not resolve
Gateway Address someplace.com for connection test2
29/10/2004 11:39:42 , Service : PPP       , Info  : Connected to PPP
Server on site PPPoE
29/10/2004 11:39:42 , Service : DNS       , Info  : New DNS Servers
received : 195.186.4.108 , 195.186.1.109
```

Syslog Messages

Syslog messages are used to log events from a networking device. These messages are generated by a syslog client which sends them to a syslog server for further processing. The Configurator software offers a simple Syslog server to receive messages but 3rd party software offers additional processing such as time stamping, saving to a database or text file, analysis, forwarding to email/ fax.

There are 2 types of Syslog messages being sent from the MultiCom Firewall:

- Automated messages from the MultiCom describing status and activity occurring on the firewall itself
- Customized messages that were added as filtering rules, which are triggered when the corresponding filter rule is activated

Each Syslog message will have a name of the sending software component, a level of priority from 0–7, and use UDP port 514 on the MultiCom Firewall

The software components generating messages will be from one of the following sources.

`Kernel` - sends customized messages that were configured in your filtering table, major software events, DSL modem activation, SecureWall dropped packets

`Daemon` - sends error messages, service activity (PPP, DHCP), notifications of telnet session closure, reception and application of new configuration files

`Auth` - sends login information for failures and successful telnet logins

`System0` - sends IPSec information

`Syslog` - sends syslog service activity

Priority levels have been given names to help differentiate the type of message. When making a customized syslog message the priority can be manually set to the desired level.

Table 2: Syslog Priority Table

Log Level	Priority
0	Emergency
1	Alert
2	Critical
3	Error
4	Warning
5	Notice
6	Info
7	Debug

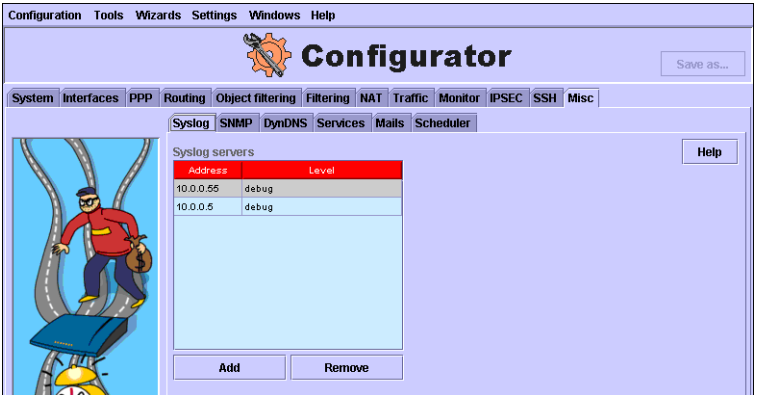
CAUTION — While these messages do not have any error correction (meaning if there is no one there to receive them they will simply disappear), they do take up processing time for your firewall. If you notice that the CPU load is excessively high, check to be sure you do not have too many syslog messages being generated.

Syslog Configuration

To configure Syslog services you simply have to type in the IP address of the computer that is going to receive the messages and select which level of messages to send to this computer. This computer can be on any connected network.

Goto the Misc>Syslog panel of the Configurator software and select where to send syslog data by entering the IP address of a computer with a syslog server program listening. Along with the IP address you can designate what level of priority reports that will be sent to the particular IP address. Because the UDP packets used by the syslog system do not verify a connection the packets will be sent whether or not there is a program running at the selected IP address to receive the messages.

The screenshot below shows the Syslog Panel of the Configuration Software.



Using Syslog Messages

It is important to be aware of activities occurring with your firewall. Enabling Syslog reporting in your MultiCom Firewall (under the MISC panel > Syslog tab in the Configurator software) allows your firewall to tell you when certain activities are occurring at the firewall. This information may also be requested by Technical Support in case of any problems.

By default the Syslog client inside the MultiCom Firewall will generate the following messages.

- service activity (PPP, DHCP, Dynamic DNS)
- Telnet logins, attempted logins and disconnections
- Startup of the firewall
- Configuration save errors
- IPSec activity

Optional messages can occur for the following activities.

- PPP Trace control frames (using the PPP > Global table for any selected PPP connection)
- Packets dropped by the SecureWall (using the SecureWall log in the NAT tables)
- Customized Filtering activity (using the LOG action for any filter rule with an optional comment/ prefix)

Depending on the features of your Syslog Server software you can have emails or pager messages automatically sent according to predefined emergency levels. Some software can also have logging information sent to a database and run daily, weekly, or monthly reports.

Among the types of information that can get reported are: failed login attempts, when filtering rules are triggered, Firewall break-in attempts, telnet or DHCP activity.

> CAUTION — Setting a high-level of syslog notices to be sent to a remote Syslog Server will cause many Internet connections and may increase your phone bill. In this case consider installing a syslog server on your LAN.

Sample Syslog Messages

There are many different parameters being reported depending on the reason for the message and its type. Some sample outputs are below.

SecureWall Message

```
2003-07-03 12:38:51Kernel.Warning10.0.0.1kernel: Dropped Packet:IN=ppp0 OUT=
MAC= SRC=202.168.224.62 DST=62.203.0.147 LEN=78 TOS=0x00 PREC=0x00
TTL=114 ID=19527 PROTO=UDP SPT=64559 DPT=137 LEN=58
```

TCP Filter Message

```
07-06-2003 11:51:22 Kernel.Emerg 192.168.63.3 kernel: webstuff IN=eth1 OUT=
MAC=00:90:f4:01:00:0a:00:80:ad:90:d4:5d:08:00 SRC=193.5.2.178 DST=192.168.63.3
LEN=40 TOS=0x00 PREC=0x00 TTL=127 ID=34046 DF PROTO=TCP SPT=4421
DPT=80 WINDOW=8591 RES=0x00 ACK URGP=0
```

UDP Filter Message

```
07-06-2003 11:32:26 Kernel.Notice 192.168.63.3 udpflooding IN=eth1 OUT=
MAC=00:90:f4:01:00:0a:00:80:ad:90:d4:5d:08:00 SRC=193.5.2.178 DST=192.168.63.3
LEN=1028 TOS=0x00 PREC=0x00 TTL=127 ID=13820 PROTO=UDP SPT=4272
DPT=100 LEN=1008
```

ICMP Filter Message

```
07-06-2003 11:53:55 Kernel.Info 192.168.63.3 kernel: icmpechorequest IN=eth1 OUT=
MAC=00:90:f4:01:00:0a:00:80:ad:90:d4:5d:08:00 SRC=192.168.63.1 DST=192.168.63.3
LEN=84 TOS=0x00 PREC=0x00 TTL=64 ID=44654 PROTO=ICMP TYPE=8 CODE=0
ID=13366 SEQ=256
```

System Restart

```
07-06-2003 11:07:46 Syslog.Info 192.168.63.3 syslogd 1.3-3: restart
```

Telnet Login Success

07-06-2003 10:58:56 Auth.Info 192.168.63.3 login: LOGIN ON s0 BY MultiCom FROM 192.168.63.1

Telnet Logout

07-06-2003 10:59:19 Daemon.Warning 192.168.63.3 inetd[48]: pid 61: exit status 1

Failed Login

07-06-2003 11:04:24 Auth.Notice 192.168.63.3 login: LOGIN FAILURE FROM 192.168.63.1, badperson

Attempted save of a bad Configuration

07-06-2003 10:33:15 Daemon.Alert 192.168.63.3 Admind[50]: Error while saving data to flash memory.

DHCP Activity

07-06-2003 13:28:17 Daemon.Info 192.168.63.3 dhcpd: DHCPDISCOVER from 00:50:e4:da:5f:4e via eth0

07-06-2003 13:28:18 Daemon.Info 192.168.63.3 dhcpd: DHCPOFFER on 192.168.63.10 to 00:50:e4:da:5f:4e via eth0

07-06-2003 13:28:18 Daemon.Info 192.168.63.3 dhcpd: DHCPREQUEST for 192.168.63.10 from 00:50:e4:da:5f:4e via eth0

07-06-2003 13:28:18 Daemon.Info 192.168.63.3 dhcpd: DHCPACK on 192.168.63.10 from 00:50:e4:da:5f:4e via eth0

PPPoE Connection

06-14-2003 23:09:51 Daemon.Notice 10.0.0.1 pppd[83]: secondary DNS address 195.186.1.111

06-14-2003 23:09:51 Daemon.Notice 10.0.0.1 pppd[83]: primary DNS address 195.186.1.110

06-14-2003 23:09:51 Daemon.Notice 10.0.0.1 pppd[83]: remote IP address 213.3.144.1

06-14-2003 23:09:51 Daemon.Notice 10.0.0.1 pppd[83]: local IP address 213.3.147.160

06-14-2003 23:09:51 Daemon.Error 10.0.0.1 pppd[83]: Couldn't increase MRU to 1500

06-14-2003 23:09:49 Daemon.Notice 10.0.0.1 pppd[83]: Connect: ppp0 <--> eth1

06-14-2003 23:09:49 Daemon.Info 10.0.0.1 pppd[83]: Using interface ppp0

06-14-2003 23:09:49 Daemon.Info 10.0.0.1 pppd[83]: Connecting PPPoE socket: 00:03:e3:5d:f3:07 11c9 eth1 0x1004dac0

06-14-2003 23:09:49 Daemon.Info 10.0.0.1 pppd[83]: Got connection: 11c9

06-14-2003 23:09:49 Daemon.Info 10.0.0.1 pppd[83]: HOST_UNIQ successful match

06-14-2003 23:09:49 Daemon.Info 10.0.0.1 pppd[83]: HOST_UNIQ successful match

06-14-2003 23:09:11 Daemon.Info 10.0.0.1 pppd[83]: Sending PADI

06-14-2003 23:09:11 Daemon.Notice 10.0.0.1 pppd[83]: pppd 2.4.0 started by root, uid 0

06-14-2003 23:09:11 Daemon.Info 10.0.0.1 pppd[83]: PPPoE Plugin Initialized

06-14-2003 23:09:11 Daemon.Info 10.0.0.1 pppd[83]: Plugin /lib/pppoe.so loaded.

PPPoE Disconnect

06-14-2003 23:13:27 Daemon.Info 10.0.0.1 pppd[83]: Exit.

06-14-2003 23:13:27 Daemon.Warning 10.0.0.1 pppd[83]: Doing disconnect

06-14-2003 23:13:27 Daemon.Error 10.0.0.1 pppd[83]: Couldn't release PPP unit: Inappropriate ioctl for device

06-14-2003 23:13:27 Daemon.Info 10.0.0.1 pppd[83]: Sent 54 bytes, received 114 bytes.

06-14-2003 23:13:27 Daemon.Info 10.0.0.1 pppd[83]: Connect time 3.6 minutes.

06-14-200323:13:27 Daemon.Notice 10.0.0.1 pppd[83]: Connection terminated.

No PPPoE Server

06-14-2003 23:20:53 Daemon.Error 10.0.0.1 pppd[163]: Couldn't get channel number: Transport endpoint is not connected

Failed PPPoE Authentication

06-14-2003 23:27:23 Daemon.Info 10.0.0.1 pppd[179]: Remote message: Authentication failure

06-14-2003 23:27:23 Daemon.Error 10.0.0.1 pppd[179]: CHAP authentication failed

PPPoE Trace Control Frames

07-05-2003 11:05:58 Daemon.Debug 10.0.0.1 pppd[121]: sent [LCP ConfReq id=0x1 <mru 1492> <magic 0xe47b6260>]

07-05-2003 11:05:58 Daemon.Debug 10.0.0.1 pppd[121]: rcvd [LCP ConfNak id=0x1 <mru 1500>] 05 06 e4 7b 62 60 62 60 88 88 88 88 88 88 88 88 88 88 88 88 88 88 88 88 88 88

07-05-2003 11:05:58 Daemon.Debug 10.0.0.1 pppd[121]: sent [LCP ConfReq id=0x2 <magic 0xe47b6260>]

07-05-2003 11:05:58 Daemon.Debug 10.0.0.1 pppd[121]: rcvd [LCP ConfAck id=0x2 <magic 0xe47b6260>] 62 60 88 88 88 88 88 88 88 88 88 88 88 88 88 88 88 88 88 88 88 88

07-05-2003 11:06:00 Daemon.Debug 10.0.0.1 pppd[121]: rcvd [LCP ConfReq id=0x9a <auth chap MD5> <magic 0x271f88db>] ee 8a bb 16 d9 2f 2f 2f 0d 0a 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f

07-05-2003 11:06:00 Daemon.Debug 10.0.0.1 pppd[121]: sent [LCP ConfAck id=0x9a <auth chap MD5> <magic 0x271f88db>]

07-05-2003 11:06:00 Daemon.Debug 10.0.0.1 pppd[121]: sent [LCP EchoReq id=0x0 magic=0xe47b6260]

07-05-2003 11:06:00 Daemon.Debug 10.0.0.1 pppd[121]: rcvd [CHAP Challenge id=0x64 <2fcf93f8be98570c83394fc75d01fb40>, name = "ipc-lsp690-r-lc-01"]

07-05-2003 11:06:00 Daemon.Debug 10.0.0.1 pppd[121]: sent [CHAP Response id=0x64 <fc18d7cb6a404e428fed0e8a51d59edf>, name = "ls.fami.lightning@coppernet.ch"]

07-05-2003 11:06:00 Daemon.Debug 10.0.0.1 pppd[121]: rcvd [LCP EchoRep id=0x0 magic=0x271f88db] 88 88 88 88 88 88 88 88 88 88 88 88 88 88 88 88 88 88 88 88 88 88

07-05-2003 11:06:02 Daemon.Debug 10.0.0.1 pppd[121]: rcvd [CHAP Success id=0x64 ""] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

07-05-2003 11:06:02 Daemon.Debug 10.0.0.1 pppd[121]: sent [IPCP ConfReq id=0x1

<addr 0.0.0.0> <ms-dns1 0.0.0.0> <ms-dns3 0.0.0.0>]

07-05-2003 11:06:02 Daemon.Debug 10.0.0.1 pppd[121]: rcvd [IPCP ConfReq id=0x1 <addr 212.147.11.245>] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

07-05-2003 11:06:02 Daemon.Debug 10.0.0.1 pppd[121]: sent [IPCP ConfAck id=0x1 <addr 212.147.11.245>]

07-05-2003 11:06:02 Daemon.Debug 10.0.0.1 pppd[121]: rcvd [IPCP ConfNak id=0x1 <addr 212.147.17.18> <ms-dns1 212.147.10.10> <ms-dns3 212.147.0.1>] 00 00 00 00
07-05-2003 11:06:02 Daemon.Debug 10.0.0.1 pppd[121]: sent [IPCP ConfReq id=0x2 <addr 212.147.17.18> <ms-dns1 212.147.10.10> <ms-dns3 212.147.0.1>]

07-05-2003 11:06:02 Daemon.Debug 10.0.0.1 pppd[121]: rcvd [IPCP ConfAck id=0x2 <addr 212.147.17.18> <ms-dns1 212.147.10.10> <ms-dns3 212.147.0.1>] 00 00 00 00

IPSec Activity

07-15-200314:55:01System0.Warning10.0.0.1pluto[584]: Starting Pluto (FreeS/WAN Version super-freeswan-1.99.7)

07-15-200314:55:01System0.Warning10.0.0.1pluto[584]: including X.509 patch with traffic selectors (Version 0.9.28)

07-15-200314:55:01System0.Warning10.0.0.1pluto[584]: including NAT-Traversal patch (Version 0.5a) [disabled]

07-15-200314:55:01System0.Warning10.0.0.1pluto[584]: ike_alg_register_enc(): Activating OAKLEY_AES_CBC: Ok (ret=0)

07-15-200314:55:01System0.Warning10.0.0.1pluto[584]: ike_alg_register_enc(): Activating OAKLEY_BLOWFISH_CBC: Ok (ret=0)

07-15-200314:55:01System0.Warning10.0.0.1pluto[584]: ike_alg_register_enc(): Activating OAKLEY_CAST_CBC: Ok (ret=0)

07-15-200314:55:01System0.Warning10.0.0.1pluto[584]: ike_alg_register_enc(): Activating OAKLEY_SERPENT_CBC: Ok (ret=0)

07-15-200314:55:01System0.Warning10.0.0.1pluto[584]: ike_alg_register_hash(): Activating OAKLEY_SHA2_256: Ok (ret=0)

07-15-200314:55:01System0.Warning10.0.0.1pluto[584]: ike_alg_register_hash(): hash alg=6 has ctx_size=216 > hash_ctx=212

07-15-200314:55:01System0.Warning10.0.0.1pluto[584]: ike_alg_register_hash(): Activating OAKLEY_SHA2_256: FAILED (ret=-75)

07-15-200314:55:01System0.Warning10.0.0.1pluto[584]: ike_alg_register_enc(): Activating OAKLEY_TWOFISH_CBC: Ok (ret=0)

07-15-200314:55:01System0.Warning10.0.0.1pluto[584]: ike_alg_register_enc(): Activating OAKLEY_SSH_PRIVATE_65289: Ok (ret=0)

07-15-200314:55:01System0.Warning10.0.0.1pluto[584]: Could not change to directory '/etc/ipsec.d/cacerts'

07-15-200314:55:01System0.Warning10.0.0.1pluto[584]: Could not change to directory '/etc/ipsec.d/crls'

07-15-200314:55:01System0.Warning10.0.0.1pluto[584]: OpenPGP certificate file '/etc/pgpcert.pgp' not found

07-15-200314:55:01System0.Debug10.0.0.1pluto[584]: | from whack: got --esp=aes128-md5-96!

07-15-200314:55:01System0.Debug10.0.0.1pluto[584]: | from whack: got --ike=aes128-sha-modp1024!

07-15-200314:55:01System0.Warning10.0.0.1pluto[584]: added connection description "roadwarrior"

07-15-200314:55:01System0.Warning10.0.0.1pluto[584]: listening for IKE messages

07-15-200314:55:01System0.Warning10.0.0.1pluto[584]: adding interface ipsec0/ppp0 62.202.93.44

07-15-200314:55:01System0.Warning10.0.0.1pluto[584]: loading secrets from "/etc/ipsec.secrets"

07-15-200314:55:01System0.Warning10.0.0.1pluto[584]: "roadwarrior": cannot route Road Warrior template

SNMP

What is SNMP

SNMP (Simple Network Management Protocol) is a network management protocol. It allows a managing station to consult information tables and counters belonging to a network station through an SNMP agent. These counters and tables are located in a Management Information Base (MIB), which is organized as a tree of data.

There are two versions of SNMP, version 1 (SNMPv1) and version 2 (SNMPv2). The version 2 is a superset of version 1, adding mainly security, in the form of authentication and encryption, and information sharing, in the form of the manager-to-manager MIB.

The current firmware implements an SNMPv2 agent for read-only access.

Both SNMP and the MIB are defined in RFC's (Request for comments) as follows.

RFC 1155, 1156, 1157	SNMP version 1
RFC 1212, 1213	MIB-II
RFC 1441 to 1452	SNMP version 2

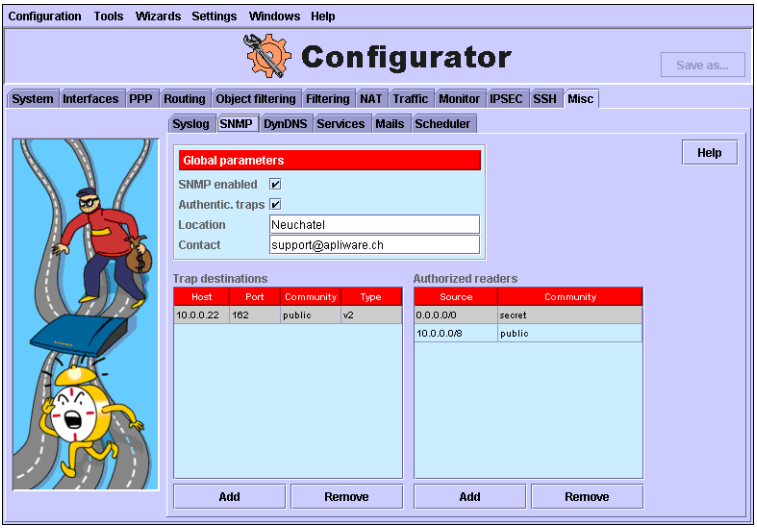
Please refer to the different RFC's described above for more detailed information on SNMP and the behavior of an SNMP agent.

To be able to access the SNMP agent with a manager (remote access software to read the SNMP data) you need to have a community name, which is a sort of password. While the default community name “public” is good for testing it is widely known you may prefer to change it to a more secure name.

Some examples of the information that you can receive from the MultiCom Firewall are found below. To retrieve this information you will need to have SNMP software and have configured the MultiCom Firewall to report and allow you to read the requested data.

- Hostname and Linux firmware version
- Uptime
- Customizable location and contact information
- detailed information on each Ethernet interface
- detailed IP/UDP/ICMP packet statistics
- connection state for ports on the MultiCom Firewall and IP address of who is using that port
- statistics on SNMP data requests
- route and ARP data stored on the MultiCom Firewall

SNMP Configuration



To enable SNMP you must SNMP access is enabled in your MultiCom Firewall firewall (under the MISC panel > SNMP tab in the Configurator software) to allow specific IP addresses to read this data.

1. enable SNMP using the Configurator software (under the MISC panel > SNMP tab)
2. enter the IP address of the authorized reader and the community name they will use to read the SNMP data. The default of 0.0.0.0 will allow anyone to read SNMP variables from your MultiCom Firewall.

> CAUTION - simply enabling the SNMP is not enough to access the SNMP information, be sure that you have also entered in the IP address of who can read the data and a community name.

SNMP Polling

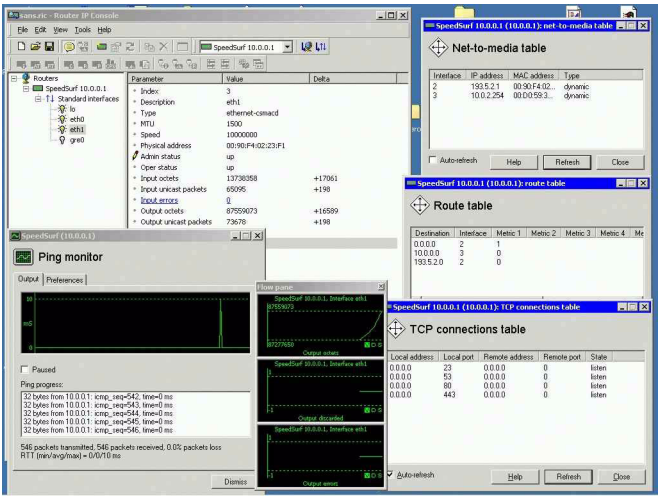
Your MultiCom Firewall offers Simple Network Management Protocol (SNMP) v2 for tracking important operating statistics of the firewall. This data is stored into a table called a Management Information Base (MIB). You can use SNMP management software to poll this MIB for the latest SNMP information the device has available.

The SNMP MIB inside the MultiCom Firewall will generate the following information.

- Hostname and Linux firmware version
- Uptime
- Customizable location and contact information
- detailed information on each Ethernet interface
- detailed IP/UDP/ICMP packet statistics
- connection state for ports on the MultiCom Firewall and IP address of who is using that port
- statistics on SNMP data requests
- route and ARP data stored on the MultiCom Firewall

Samples of the SNMP output available from your MultiCom Firewall can be found in the SNMP Variables Appendix. You can find more information on the variables designed for SNMP version 2 in RFC1213.

Third party software such as Router IP Console by Innerdive (http://www.innerdive.com/products/ric/) or Active SNMP from CSCare (http://www.cscare.com/activesnmp) can be used to regularly make reports on the status of the MultiCom Firewall.



Some statistics that you may find useful to watch on a regular basis however are:

Table 3: Useful SNMP variables

SNMP Variable	Description
tcpCurrentEstab	live TCP connections
tcp ConnTable	See which IP Addresses are connecting to the Gateway directly (for http, telnet, ftp access)
icmpOutEchoReps	ICMP responses to Pings
sysUptime	System uptime
ifOutErrors	Wan errors, possibly the link is down
ifOperStatus	Current operational status of an interface
ipOutNoRoutes	IP datagrams discarded because no route could be found
ipNetToMediaTable	IP Address Translation table
icmpInDestUnreachs	# of ICMP Destination Unreachable messages received
udpNoPorts	number of received UDP datagrams for which there was no application

Telnet/ Console Status Reports

By logging into the Firewall's telnet or console interface (check your User's Manual to see if your firewall has a console interface) you can run the "status" command to get a single text output of the entire firewalls system status report.

You can then cut and paste that to an email file or print it out for review. This is nice if you do not want to open the web browsing port to your firewall or if you run telnet scripting utilities (such as the Expect software for Linux and Windows) for reports or configurations.

Table 4: Common telnet/ console diagnostics commands

Description	Commands	Sample output
MultiCom Serial number	/: info system hardware serial_number	serial_number = LI-MU7-CH-0200D2
Software version	/: info system software firmware	firmware = 3.1
LAN status	/: info interface ethernet LAN status status	status = UP RUNNING
LAN IP Address	/: info interface ethernet LAN status ip_address	ip_address = 10.0.0.1
	/: info interface ethernet LAN ip netmask	netmask = 255.0.0.0
LAN DHCP Mode	/: info interface ethernet LAN ip dhcp mode	mode = server

Description	Commands	Sample output
LAN DHCP server leases	/: info interface ethernet LAN ip dhcp server status leases	indexes: 0 1 2 3
	/: info interface ethernet LAN ip dhcp server status leases 0 ip	ip = 10.0.0.17
	/: info interface ethernet LAN ip dhcp server status leases 0 hw_address	hw_address = 00:c0:f0:4c:a7:90
	/: info interface ethernet LAN ip dhcp server status leases 0 starts	starts = 4 2001/06/28 13:24:06
	/: info interface ethernet LAN ip dhcp server status leases 0 ends	ends = 4 2001/06/28 14:24:06
	/: info interface ethernet LAN ip dhcp server status leases 0 hostname	hostname = "NT-workstation"
WAN status	/: info interface ethernet WAN status status	status = UP RUNNING
WAN DHCP client status	/: info interface ethernet WAN ip dhcp client status state	state = Assigned
PPPoE status	/: info interface ppp PPPoE status status	status = UP RUNNING
PPPoE IP address	/: info interface ppp PPPoE status ip_address	ip_address = 212.147.17.76
PPPoE IPCP info	/: info interface ppp PPPoE ipcp status state	state = UP state = DOWN
PPPoE Link status	/: info interface ppp PPPoE lcp status info	info = "" info = CHAP authentication failed info = Timeout sending Config-Requests info = Endpoint not connected
PPPoE DNS assigned servers	/: info interface ppp PPPoE ipcp status primary	primary = 212.147.10.10
	/: info interface ppp PPPoE ipcp status secondary	secondary = 212.147.0.1
Available PPPoE servers	/: info interface ppp PPPoE pppoe server_list	indexes: 0 1 2

Description	Commands	Sample output
	/: info interface ppp PPPoE pppoe server_list 0 access_concentrator_name	access_concentrator_ name = ipc-lsp690-r-lc-01
	/: info interface ppp PPPoE pppoe server_list 0 service_name	service_name = Any
ARP entries	/: info arp status arp_entry	indexes: 0 1 2
	/: info arp status arp_entry 0 hw_address	hw_address = 00:C0:F0:57:4A:6D
	/: info arp status arp_entry 1 hw_address	hw_address = 00:C0:F0:4C:A7:90
DNS servers used	/: info ip dns status nameserver 0 ip	ip = 192.168.1.115
	/: info ip dns status nameserver 1 ip	ip = 192.168.1.116

Chapter 17

Maintenance

While basic security is enabled as soon as you plug your MultiCom Firewall firewall between your modem and your network, a well running network requires regular maintenance. A poorly maintained network may suffer from network performance loss or worse such as network failure (especially when you need it most.)

Any number of factors can affect the way your network runs — new software installations, misconfigurations of hardware, and even electromagnetic interference can all cause serious changes in the way data travels through your network.

Just as with any emergency, preparation will minimize the effect on your business and peace-of mind. Your MultiCom Firewall has been equipped with numerous tools to assist in your maintenance needs.

- Checking System Status
  —Using the Configurator software
  —Using the built-in web server
  —Using shell commands to directly log into the firewall
- Configuration
  —Backup the Configuration

—Restoring the Configuration

- Keep up to date

—update the firmware

—read about current networking exploits

Backup Your Configuration

It is important to maintain a backup of your configuration file in case of emergencies. This can easily be done with the MultiCom Firewall built-in webserver or the included Configurator software package.

Using the Webserver

1. Start web browser software and go to http://10.0.0.1/advanced/config/current.cfg where 10.0.0.1 is the IP Address of the MultiCom Firewall.
2. Enter in the name you want to save the configuration backup under and the directory location.
3. Click Ok. If you use IPSec or High Availability (VRRP) authentication then continue to the next step. Otherwise you are done with the backup.
4. Start web browser software and go to http://10.0.0.1/advanced/security/security.cfg where 10.0.0.1 is the IP Address of the MultiCom Firewall.
5. Enter in the name you want to save the configuration backup under and the directory location.
6. Click Ok. You are now done with the backup.

The file saved is a text file that you can save to a floppy or attach to an email.

NOTE - The URL Filtering rules are not part of the 2 above configuration files. If you wish to backup the URL Filtering rules you must go to http://10.0.0.1/advanced/filters/ and cut and paste the rules into a text file. It is possible to save these rules directly as a file when using the Configurator software.

Using the Configurator

1. Start the Configurator software
2. Either enter in the IP address of your MultiCom Firewall or click on the Search button to search your local network for it.
3. Click `Configure`
4. Simply click on the File menu > Save As > and select To File.
5. Enter in the name you want to save the configuration backup under and the directory location.
6. Click Ok

The file saved is a text file that you can save to a floppy or attach to an email.

Restoring A Configuration

When you need to restore a saved configuration file to your MultiCom Firewall firewall you will use the built in web server or the included Configurator software.

During the application of a new configuration or while an MultiCom Firewall is loading a new configuration during bootup the routing table is blocked. This allows all of the rules to be loaded before activation of the firewall.

Using the Webserver

1. Start web browser software and go to http://10.0.0.1/advanced/config/upload/ where 10.0.0.1 is the IP Address of the MultiCom Firewall.
2. Enter the directory and name where the saved configuration file resides. Optionally use the Browse... button to search for the file on your hard disk.
3. Click Submit Values. You are now finished unless you have a Security Configuration file to reload with IPSec and/ or High Availability authentication values.
4. Start web browser software and go to http://10.0.0.1/advanced/security/upload/ where 10.0.0.1 is the IP Address of the MultiCom Firewall.
5. Enter the directory and name where the saved configuration file resides. Optionally use the Browse... button to search for the file on your hard disk.
6. Click Submit Values. You are now finished.

NOTE - The URL Filtering rules are not part of the 2 above configuration files. If you wish to reload the URL Filtering rules you must go to http://10.0.0.1/advanced/filters/ and cut and paste the rules from a text file.

Using the Configurator

1. Start the Configurator software
2. Click `Configure`
3. Click on File menu > Load From > and select Local File.
4. Enter the directory and name where the saved configuration file resides. Optionally use the Browse... button to search for the file on your hard disk.
5. Click Ok
6. Click on File menu > Save As > and select To firewall.
7. Enter in the IP address of the MultiCom Firewall that you will be saving to.
8. Make sure Current Config is selected in the Download to... option
9. Click Ok

NOTE - During the application of a new configuration or while an MultiCom Firewall is loading a new configuration during bootup the routing table is blocked. This allows all of the rules to be loaded before activation of the firewall.

Updating Your Firmware

Because your MultiCom Firewall has been equipped with flash memory it is possible for you to update it with a newer operating system (also known as firmware) than was available when you purchased it.

NOTE — Contact your distributor or check the Lightning web site for notifications on the latest firmware. Additional charges may apply.

Upgrading the firmware on your MultiCom Firewall requires you to access the web server on the firewall. Your configuration files will remain untouched however the factory default configuration may change (this configuration is accessed when rebooting the Firewall while holding down the config button.)

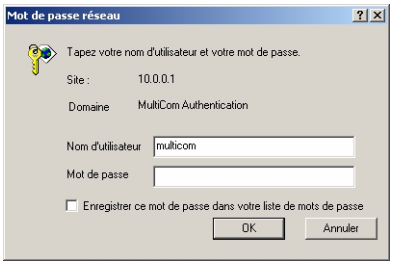
Your MultiCom Firewall will reboot and be offline for up to 5 minutes during the upgrade process. Be sure that your network can afford to be without Internet access for at least 5 minutes and that there are no important data transfers occurring during this time.

CAUTION - Please note, that if the power is interrupted during the upgrade process your MultiCom Firewall could become unusable and require repairs from your local distributor. Continue at your own risk.

To install the latest firmware follow the steps below.

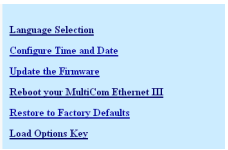
NOTE - hitting refresh during the upgrade process can cause the web browser to restart the upgrade process. If you want to check the status of the MultiCom Firewall during an upgrade check the LED lights or click the HOME button on the left menu.

1. Download the latest firmware to your computer
2. Access the MultiCom Firewall web server. Simply type in the IP Address of the MultiCom Firewall into an Internet browser which is connected to the same network as the MultiCom (usually this is the LAN interface).
3. Type in your username and password (by default the username is "multicom" and there is no password.)

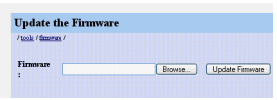


4. Select `Toolbox` (or MultiCom Tools in firmware versions before 3.4)

5. Select `Update the Firmware`

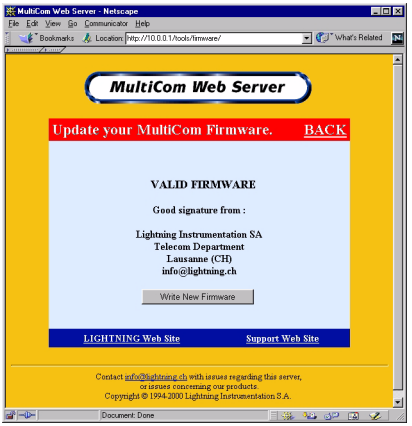


6. Type in the location of the new firmware file or click `Browse` to find the file on your hard disk. If you use `Browse` you may need to choose “All Files (*.*) in the Type: box if you cannot see the firmware.



7. Select `Update Firmware` after you have selected the firmware file to update with.
8. The Web server will verify that the firmware is indeed valid before writing it to the device. If it is valid you will see the button `Write New Firmware`, press this button. Otherwise you are asked to reload the firmware.

   If the web server gives you an error or does nothing then try using a different web browser or check with your distributor for another copy of the firmware.



NOTE - this step is skipped in firmware versions 3.1 and higher. If the firmware is good you will jump to step 9 and write the new firmware. If the firmware is bad your router will reboot with the previous firmware.

9. The MultiCom Firewall now begins the process of erasing the old firmware and writing the new firmware. Wait for the MultiCom Firewall to reboot with the new firmware upgrade. The lights on the front of the device will change colors during the upgrade process and will stop blinking after the MultiCom Firewall has rebooted.

WARNING - While the firmware upgrade is being written do not interrupt the power to the MultiCom Firewall!

10. You are finished. Verify that your new version of Lightning-Linux firmware is currently installed in your MultiCom Firewall. In your web browser go to http://10.0.0.1/config/system/software/ where 10.0.0.1 is the IP Address of your MultiCom Firewall.

LED Status During Upgrade

Starting with Lightning-Linux 3.1 the leds on the front of your MultiCom Firewall indicate the status of the firmware upgrade according to the table below.

Table 1: LED Status during upgrade

Status	Description
Checking the validity of the firmware	All of the leds are lit green except the power led which is blinking green and black.
Erasing existing flash memory	All of the leds are lit green except the power led which is blinking orange and black.
Writing the new firmware into the flash memory	All of the leds are lit green except the power led which is blinking orange and green.
Error while erasing the existing flash memory	All of the leds are blinking red and orange.
Error while writing the new firmware to flash memory	All of the leds are blinking red and black.

Troubleshooting Firmware Upgrade

If power is interrupted during the flash upgrade process the existing firmware could become corrupted. Normally this will be evident because the lights are frozen every time you reboot the MultiCom Firewall and it will not respond to normal networking activity. To recover from this please contact your local distributor. If after a reboot you have the same firmware version that was previously installed then there was a problem with the firmware upgrade. Try reinstalling it again, rebooting the MultiCom Firewall into the default configuration and then try reinstalling again, download or contact your distributor for another copy of the firmware.

Remember that you will need to upgrade the Configurator software to the same version of the firmware that you just installed.

Chapter 18

Network Security

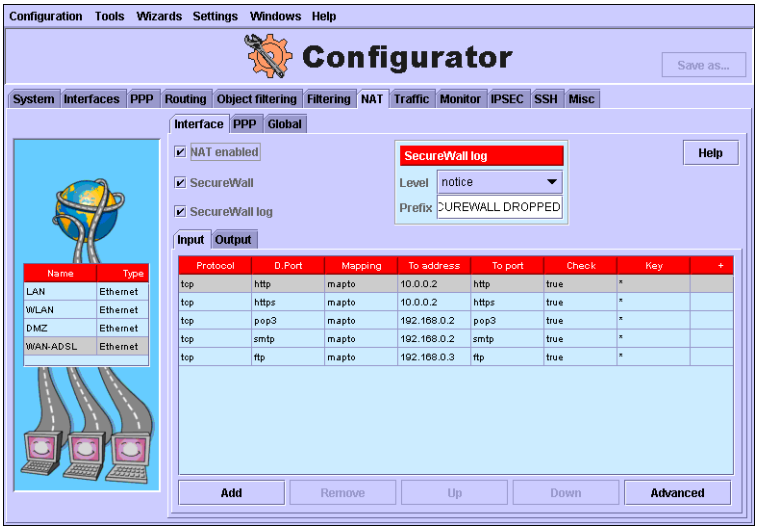
Security on the Internet is of great concern to most users. No one wants a hacker changing their web sites let alone getting access to personal or confidential information stored on local computers. Your MultiCom Firewall comes with special features to protect your internal network from hackers or other malicious people trying to get access to your network.

- Username and password for firewall access
- Built-in Firewall (NAT)
- Easy-Firewall Wizard
- Advanced logging via syslog and SNMP v.2
- Using NAT to hide internal network addresses
- Stateful packet filtering Firewall
- Bandwidth limitations
- Physical security with Kensington lock

Along with disallowing access you also want to protect against hackers using your computer or network to make attacks on others. Tricking your network to flood another with useless data, storing illegal software on your ftp sites and remotely controlling your computer are types of unauthorized use that you need to protect against.

Enabling the Firewall

There is a built-in NAT firewall capability that is included with your MultiCom Firewall. No data is allowed through the firewall unless it has either been requested or a filter/ NAT rule allows it through. You can easily activate it for each interface by using the Configurator software.



1. Open the Configurator's `Configure` button
2. Go to the `Interface` window and click on the `NAT` panel
3. Select the interface you want to turn on the Firewall for
4. Click on `NAT Enabled` and `Secure Wall`
5. Save the configuration to the firewall or click the `Save` button

That is all there is to starting the Firewall. You do not need to reboot anything as long as you click the `Save` button or save the configuration to the `CURRENT CONFIG` space on your MultiCom Firewall.

CAUTION - Some network services may not work correctly with the Firewall activated. This is because certain services such as H.323 video connections require the remote server to open random

connections into your network. This is the same type of access the Firewall is protecting you from - random or unknown external connections into your network.

Please check with your software vendor for different ways to configure such software to work through firewalls.

Using Easy-Firewall

When making an Easy Setup configuration from the Configurator software or by choosing Wizards > Easy Firewall from the Advanced Configurator window you can have access to a 3-step wizard that helps configure NAT and Filtering rules.

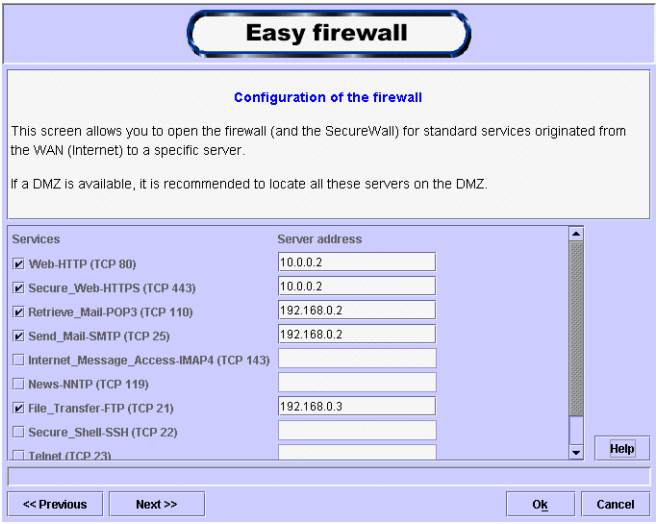
The first Panel allows the activation of Filtering and offers the option to activate the NetBIOS filters. This wizard add NAT and Filtering rules to an existing configuration however it is recommended to start without existing NAT/ Filtering rules and add them after using the Easy Firewall Wizard.

When this panel is disabled, the filtering system does not perform any traffic control. However if the SecureWall is active on the WAN interface it does act as a firewall (with all traffic coming from the WAN being dropped unless it is in response to a demand from the LAN.)

When the Filtering is enabled on this window 4 rules are activated:

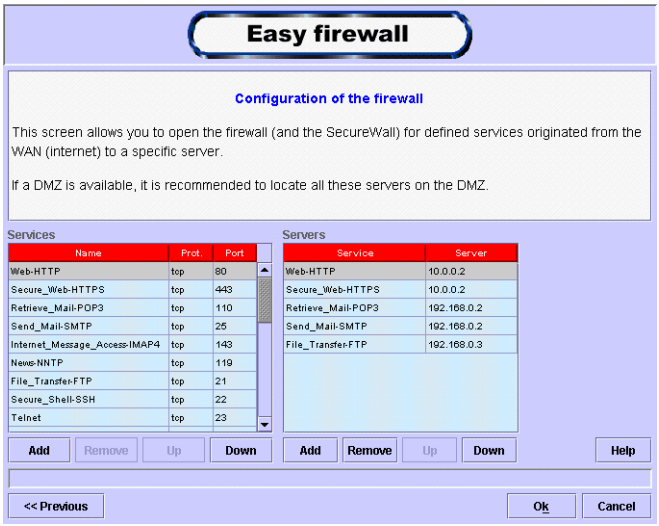
- The SecureWall on the WAN interface is activated
- All traffic originating from the WAN to the LAN/DMZ is dropped
- All traffic originating from the DMZ to the LAN is also dropped
- Only requests originating from the LAN to the FDMZ/ WAN and from the DMZ to the WAN and their related responses are allowed to go through the firewall.

The second window enables access to specific servers on the LAN or DMZ. Service requests that arrive at the WAN interface of the MultiCom Firewall will be allowed into the network and redirected to the specified IP address on the LAN or DMZ.



Simply select the service that you want to redirect internally and supply the IP Address where the server will be available to respond.

The 3rd and final window allows customized services to be added to the Easy Firewall Wizard. Added services can be redirected to internal servers.



Logging network activity

What you log depends on your goal in the administration of your network security. Because creating a syslog message is a possible filtering action you are able to decide exactly what type of data packet that you want to be notified about. When using this along with 3rd party Syslog software you are able to create logs of activity traversing your network through the MultiCom Firewall.

Because you are using filtering rules to create the Syslog message you can identify packets based on their source/ destination IP address and/ or port number, their frequency, TCP flags and options, ICMP types and even its state.

Regularly checked logs can help you not only be aware of the types of traffic that traverse your network but often give indications of attempts to breach your network security.

Below are some suggestions of commonly logged parameters that can indicate illegal access attempts to your network.

- WAN data packets that are claiming to come from inside your network (IP source address spoofing)

- WAN, incoming and outgoing traffic that are trying to reach the Class A, B, and C private network addresses. These addresses are not supposed to be used on the Internet. External, incoming traffic that reports its source as from a Class A, B, and C private network address. These addresses are not supposed to be reachable on the Internet.
- WAN, incoming traffic that claims to be from 127.0.0.1. This address should never be the source of information from the Internet.
- WAN, incoming broadcast traffic. Messages sent to broadcast address 0 are usually attempts to identify your operating system.
- WAN, incoming or outgoing multicast, anycast, or broadcast traffic. This should normally not be seen on the Internet side.
- Requests coming in on the restricted, unprivileged ports to show attempts at reaching those services such as x windows.
- WAN access attempts to unavailable TCP privileged ports shows possible external scans or access attempts.
- WAN, incoming attempts to unavailable UDP privileged ports. These are not normally contacted and may indicate a hacking attempt.

Sometimes hackers will simply run scans of your servers/ firewalls to see what services are being refused (hence identifying which services may be running on your network.)

Hide LAN IP Addresses with NAT

One of the big features of Network Address Translation is that you can keep secret the IP addresses of your internal network. This information is kept at the firewall where the IP address and port address of the sending computer is temporarily replaced with the IP address of the Firewall's WAN port and a random port address. When the remote computer replies with information to the firewall, those packets are forwarded to the original IP address of the computer that first made the request for information.

You can use this functionality in reverse also. For instance, you might consider changing the internal server port addresses to less commonly used ports, maybe changing the web server from listening at port 80 to listening at port 8000. The NAT service can be told to send all web requests for a particular server to port 8000 on a particular internal server.

These types of configurations are done transparently to the external and internal user but allows the system administrator great flexibility in managing the IP addresses of internal Ethernet servers and devices.

Filter Unwanted Activity

There are many ways to plan a firewall security. One method is to consider blocking all traffic and then decide what to allow through. While this method will offer the most security you will also need to know many details about your network, what protocols it uses and how it communicates over the network.

For normal Internet use you may not want to be too restrictive in setting certain services (particularly ftp). Since users will may be looking for software or data they may not know ahead of time where they will find it and hence need to be able to ftp from numerous locations and not a specific location. Be sure to consider how your network users interact with the network to avoid blocking services or features they may need.

Recommended filters for typical Internet access security

- Net Bios traffic, incoming and outgoing traffic on port 137-139
- Block WAN, incoming packets with an internal network address
- Block WAN, outgoing packets with an IP source different from your internal net address
- Block WAN, incoming packets to net 0 or 255.255.255.255
- Block WAN, incoming source and destination of 10/8, 127/8, 172.16/12, 192.168/16 and LAN outgoing destinations of the same.
- Block WAN, incoming all UDP packets less than 900 unless for a specific service
- Block WAN, incoming ICMP fragments (pings sending too large of ICMP packets)

Below is a list of common services and the types of considerations you need to make regarding their access into and from your network. Many of these services are defined at the software client computer (such as the specific IP address of your remote email server.) The more details you can provide about these to the firewall the more secure your network will be.

Keep in mind, however, that making your firewall very restrictive means that whenever a change occurs at the IP level you will have to make the corresponding changes to the firewall configuration (for instance if you are only allowing email from a particular IP POP server on the Internet and then, due to a system change the POP server now has another address you may need to reconfigure your firewall to take into account the change.

Service Options

Below are a list of common services and the types of questions you should be asking yourself when you want to use them. If you are not going to use a service then you should definitely not allow access to that port from the LAN or WAN. When you do decide to leave the port open remember that you can allow, forward, reject, log or drop data packets that are traversing your firewall.

If a specific computer needs a service that opens up questionable ports consider limiting that type of communication only when coming from or going to that specific computer.

Table 1: Port Based Services Options

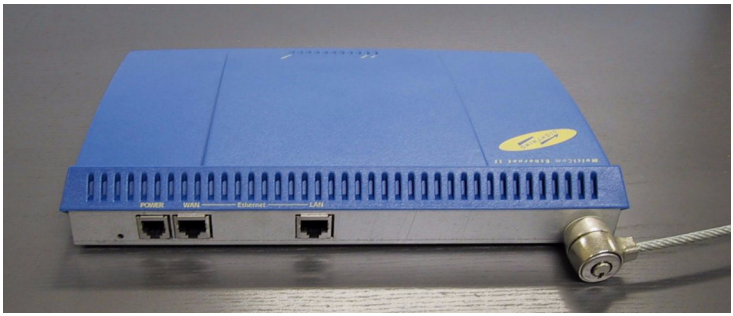
Services (Port)	Options
AUTH (113)	Allow incoming identd requests Reject incoming identd requests Drop identd requests
Finger (79)	Allow outgoing finger requests to remote networks Allow incoming finger requests to your network
FTP services (20, 21)	Allow access to an external FTP server • using active mode • using passive mode • using either mode IP addresses of remote server to access Allow incoming activity to an internal FTP server • using active mode • using passive mode • using either mode IP address of the internal FTP server
ICMP Destination Unreachable	Deny outgoing Destination Unreachable messages Only allow for fragmentation requests
ICMP Ping	Deny incoming ping requests from external users IP address of the ping requests to accept from external users Deny external ping requests to remote computers
ICMP Traceroute	Deny incoming traceroute requests IP address of external computers allowed to make traceroute requests Deny outgoing traceroute requests
ICQ (4000)	Allow outgoing ICQ chats Allow incoming ICQ chats
IMAP (143)	Allow outgoing requests to remote IMAP servers IP address of remote IMAP server Allow incoming IMAP requests from remote users IP address of internal IMAP server IP address of external clients to the internal IMAP server
IRC (6667)	Allow outgoing IRC chats Allow incoming IRC chats

Services (Port)	Options
Multimedia	Pick the protocols to use Will it support multicast Will it support unicast Will it only use TCP Will it only use HTTP IP address for remote content servers IP address for internal content servers
NFS (2049)	Deny incoming connections to your internal NFS servers
NTP (123)	Allow clients to use port 123 Allow clients to use unprivileged ports (an option for ntupdate only) IP address of external time server IP address of local time server
POP3 (110)	Allow external access to POP server (if client) IP address of external POP server (if client) Allow internal POP server (if server) IP addresses of clients of internal POP server (if server)
Secure Web/ https (443)	Allow access to external secure web sites Allow access to internal secure web servers
SMTP (25)	IP address of the remote server you are using (if client) IP addresses of your clients (if server)
SSH (22)	Allow ssh outgoing access of remote servers Allow ssh incoming access of an internal server Select lowest available port to use (between 513-1023)
Telnet (23)	Allow access to remote telnet servers IP addresses of remote telnet servers Allow access to internal telnet servers IP address of internal telnet servers
Usenet (119)	IP addresses of external Usenet server (if client) IP address of internal Usenet server (if server)
Web Proxies	Allow access to an external web proxy server Redirect all web traffic to a web proxy server IP address of the web server Port number the web server is listening on
Web/ http (80)	Allow outgoing web requests Allow incoming web requests IP address of internal web server IP address of allowed external servers IP address of clients of internal web server

Services (Port)	Options
Whois (43)	Allow whois outgoing requests Allow whois incoming requests
X Windows (6000)	Allow external requests to open an X Windows session IP addresses of external X Window clients

Physically Secure Your Firewall

Securing your firewall is as important as securing the data that passes through it. The added security of a physical lock increases your protection from theft. To assist in this your MultiCom Firewall has a built in Kensington Lock Slot. This slot is a small hole on the right side of the back of your MultiCom Firewall.



Locks, such as seen in the above image, are available from the Kensington Technology Group at http://www.kensington.com. Check with Kensington or your local computer store for there latest locks that work with the Kensington Lock Slot (also known as the Kensington Security Slot).

Chapter 19

Troubleshooting

When you are running a network (whether one computer connected directly to the Internet or many) it is possible that problems can come up. Maybe the network is giving you slow responses, some devices or computers are not reachable, you are reaching the wrong computer or your filters do not seem to be working. This chapter will help you fix some common networking issues.

To correctly fix the problem the source of it must be found. In networking this is especially true because the problem may not necessarily point you toward the answer (for instance a bad DNS server would stop you from reaching web addresses but not if you only used the IP address.)

There are two questions you must always check...

1. Were the instructions followed correctly?
2. Has anything recently changed before the problem occurred? (for instance are you using new network drivers, new workstation on the network...)

If these two questions do not help you find the problem then it is time to do some troubleshooting with the firewall itself.

Basic Things To Check

Always check that your cabling and basic connections are functioning correctly for the ports you are using. If there is a problem moving your data back and forth at this level then higher level troubleshooting will be ineffective.

- Are the cables correct (crossed cable versus straight cable.)
- Are the interface lights (LAN, WAN, DMZ) on the firewall green when the cables are plugged into your ethernet card/interface or xDSL, cable or wireless modems?
- Are the lights on the hub or ethernet interface of the device green where the firewall cable is plugged in.

These answers must be yes before you do any more in-depth troubleshooting. If there are problems here and you are using a hub, be sure to verify that you are not using the uplink port. Otherwise try verifying the ethernet device is functioning correctly and try switching the ethernet cable to one that you know is good.

If all of the physical connections are good (as tested above) the next steps is to verify that you can:

1. from your computer, communicate with the LAN interface of the MultiCom Firewall
2. from the MultiCom Firewall, communicate with your ISP
3. from your computer, communicate with the Internet

TIP - A simple troubleshooting step is to reboot the MultiCom Firewall and try again. If all else fails, reset the Firewall into the default mode as described in the “Resetting the Default Configuration” Section on page 386. Then reconfigure it using the Easy-Setup.

After checking these basic issues please continue to the Common Network Problems on the next page which describe some common problems that may occur on your Local Network.

Finally, look at the sections below that corresponds to the type of connection that your ISP uses - DHCP, PPPoE, PPTP. These sections will explain common problems on the Remote Network that connects you to your ISP and the Internet. If you are still having problems consider calling technical support.

Common Local Network Problems

Please look over these common reasons for networking problems. Additionally, please check the section below relating specifically to your type of connection (DHCP, PPPoE, PPTP, Static IP addresses.)

Once you know that your cabling is okay it is time to ask some more detailed questions.

- Is the modem working? (check the diagnostics that came with the modem, maybe you can check LED displays or communicate directly with the modem)
- Is TCP/IP installed on your computer? (if you can ping 127.0.0.1 in a telnet window/ DOS window TCP is installed)
- Is the firewall reachable? (using the ping command for instance in a telnet window/ DOS window and try PING 10.0.0.1 where 10.0.0.1 is the IP Address of your MultiCom Firewall's LAN interface.) Sometimes a Filter or recent configuration change can block access to the Firewall.
- Did you try using an IP address (such as http://193.247.134.2) to reach a web site. If it does then your DNS is not reachable and you should check with your Internet Service Provider.
- Is there another DHCP server on your Local Network in addition to the one on the MultiCom Firewall? If so you can only have one so you must disable one of them.
- Were you using an analogue modem before connecting the Broadband modem? Maybe you forgot to change the Internet Options of Windows. Be sure that under the Control Panels>Internet Connections>Connections the "Never dial a connection" is activated or your computer will keep trying to use the modem.
- If you are using more than one Ethernet card on your computer be sure that you do not have more than one default route.
- Are there other devices on your network using the same IP Address as the MultiCom Firewall's LAN interface (10.0.0.1) the IP Addresses being given by the Firewall's DHCP server?
- If you are using a Static IP on your Local Network make sure that each of your workstations are configured to be on the same subnet as the MultiCom Firewall and use the Firewall as their default Gateway.

DHCP Troubleshooting

DHCP To The Internet

With DHCP configured for your WAN interface your MultiCom Firewall sends out discovery packets looking for a DHCP server to give it an IP configuration. If a DHCP server is not found then the WAN interface is not enabled (i.e. you cannot reach the Internet.)

Some common connection problems are...

- DHCP is not being used by your Internet Service Provider
- your cabling is incorrect
- your modem is not configured as a bridge
- you changed the time on the MultiCom Firewall but did not reboot
- your WAN and LAN interfaces are using the same IP address range

To check the status of your WAN interface using DHCP visit the WAN DHCP client status web page using the web server diagnostic pages (found at “Diagnostics With The Web Server” on page 380.) Also be sure to check the IP configuration received by your workstations and that the firewall IP address received is the IP address of your MultiCom Firewall (the default setting is 10.0.0.1).

Table 1: WAN DHCP client status states

State of the interface	Possible problem
Disabled	DHCP is not enabled for this interface.
Expired	The existing IP configuration has expired without it being renewed. Check that firewall was rebooted after changing the time.
Trying to get address	The firewall is in the process of trying to get an IP configuration from the Internet Service Provider.
Failed	The attempt to contact a DHCP server failed, check all troubleshooting steps.
Assigned	The DHCP interface is functioning correctly.
Rebind	Normal DHCP activity, check back soon to see if the state is Assigned or Failed.
Renew	Normal DHCP activity, check back soon to see if the state is Assigned or Failed.

DHCP is not being used by your Internet

Service Provider

Verify that your Internet Service Provider uses DHCP to configure your connection to them. Other possible connections may be PPPoE or a static IP configuration.

State: Trying to get address or State: failed or State: Assigned or State: Expired

Your cabling is incorrect

Be sure that the WAN interface light on your MultiCom Firewall is green. If it is not you either have the wrong cable, a faulty cable or the broadband modem is not plugged in. Try switching cables and verify that the modem is indeed turned on.

Your modem is not configured as a bridge

Your broadband modem must be configured as a bridge for you to connect directly to your Internet Service Provider. Verify with the instruction manual of your modem that it is indeed configured as a bridge. If the two above steps are not showing a problem this may be your problem.

You changed the time on your firewall but did not reboot.

The default date of your MultiCom Firewall is January 1970. DHCP works on a lease system where IP configurations are good for a specified amount of time. When the original lease runs out your MultiCom Firewall will attempt to renew its IP configuration information but will erroneously report that the IP configuration has expired (since the current date is now more then 30 years in the future.) The easiest fix for this is to reboot the MultiCom Firewall and it will make a fresh request using the new time.

Your WAN and LAN interfaces are using the same IP address range

This will normally only happen office to office connections since the default IP range of 10.0.x.x for your LAN network is never used on the Internet. Check that the WAN network is not assigning address in the 10.0.x.x range

and if it is change either the LAN or the WAN network so that one of them uses a different range of IP addresses. For example, reconfigure your LAN address range to be from 192.168.0.2-192.168.0.100.

DHCP On Your Local Network

Using DHCP on to manage your own network's IP addresses makes administration convenient. The most common problem is that a device is unable to receive an IP configuration from the DHCP server (normally your MultiCom Firewall. Below are some reasons this might happen.

- your workstations are not configured as DHCP clients
- there are not enough IP addresses for your computers
- there is another DHCP server on your network
- there is another device on your network with the same IP address as your firewall
- you changed the time on the MultiCom Firewall but did not reboot

Be sure to check the LAN DHCP server leases page to see what IP addresses have been assigned and their status. These require using the web server diagnostic pages found at "Diagnostics With The Web Server" on page 380.

Your workstations are not configured as DHCP clients

Check that each workstation is configured as a DHCP client. For some operating systems setting this configuration requires you to reboot your workstation. Please refer to the section on Configuring your Computers or to the manuals that came with your computer for instructions on configuring this setting.

There are not enough IP addresses for your computers

The default setting of the MultiCom Firewalls allows for up to 1,000 DHCP clients. If you either need more than this or have customized your settings please refer to the Lightning-Linux manual for more information.

There is another DHCP server on your

network

If you are sure that your workstations are configured as DHCP clients and they are receiving IP configuration information check the LAN DHCP server leases page to see if those computer names or IP addresses show up there. If they do not then you may have another DHCP server on your network giving out configurations. Check with your Computer Administrator to see if this is the case.

Only one DHCP server is allowed on your local network. If there is another one in place you need to decide to use the built-in one of the MultiCom Firewall or your other server.

There is another device on your network with the same IP address as your firewall

Your MultiCom Firewall has a default IP address of 10.0.0.1 on the LAN interface. You cannot have another ethernet device on your network with this same IP address. Consider changing the other devices IP address or change the IP address of your MultiCom Firewall.

You changed the time on your firewall but did not reboot.

The default date of your MultiCom Firewall is January 1970. DHCP works on a lease system where IP configurations are good for a specified amount of time. When the original lease runs out your MultiCom Firewall will attempt to renew its IP configuration information but will erroneously report that the IP configuration has expired (since the current date is now more then 30 years in the future.) The easiest fix for this is to reboot the MultiCom Firewall and it will make a fresh request using the new time.

PPPoE Troubleshooting

If you are using a PPPoE connection there are a few specific troubleshooting steps for you to try. These require using the web server diagnostic pages found at “Diagnostics With The Web Server” on page 380. Common problems that can block your Internet connection include...

- incorrect password

- PPPoE server (ISP) not available
- some web sites are not available

Incorrect Password

If you have typed in an incorrect username or password you will not be able to open a PPPoE Internet connection with your Internet Service Provider.

To check if this is the case visit the PPPoE Link status page on your firewall. You will see the error message “CHAP authentication failed”. This means that a connection to the ISP is possible but that the username and password you have entered is incorrect.

Verify your username and password is correct and/ or contact your Internet Service Provider.

PPPoE Server (ISP) Not Available

If your cabling is incorrect, the modem is not functioning/ configured properly or the xDSL line is not functioning you will not be able to reach your ISP’s PPPoE server to correctly use their services.

To check that this connection is available or not visit the PPPoE Link status page on your firewall. If you see the error message “Endpoint not connected” that means there is no available connection to the ISP.

Check that your cables are connected properly (all interface lights are green on your modem and MultiCom Firewall), and that the modem is configured to act as a bridge. Finally if these are OK, contact your Internet Service Provider to verify the line is connected properly.

Some Web Sites Are Not Available

In some cases certain web sites will not be available when using PPPoE connections. Using PPPoE over the Internet requires that data packets of a certain size move over the Ethernet connection. Usually this process is done by the remote web server using a discovery process to discover the best size of data packets to use. Sometimes Internet routers between you and the web page you are trying to reach do not support this process and the data is dropped by these routers.

When this problem is happening, normally small packets will move back and forth fine but large data packets (often occurring during file transfer, web page reception, and media streaming) will not reach your computer. This problem will be evident in the following ways

Table 2: PPPoE Frame Size Symptoms

Web Page/ HTTP	your browser will seem to connect but no data or web page comes back
FTP	you can login into a web server but cannot use dir (ls) of directories with a lot of files and cannot transfer large files
Telnet	you can log into a telnet server but any action which sends your computer a lot of text will hang the connection
Email (POP3)	you can often log into the remote email server and even receive small messages of a few lines but larger emails or long lists of emails will not transfer to your computer
Real Player or Microsoft Media Player	when using TCP or HTTP options to make a connection the connection will start but then stops saying the network is busy or it is rebuffering (however using UDP works fine)
Ping	usually pinging the remote host will work fine but this requires that you have ping software on your computer to test with

The easiest fix for this problem is to enable the TCP Frame Size Adaption option under your PPPoE configuration. To do this go back through the Easy Setup you used to configure your firewall and select “enable” by the question asking if you want to use TCP Frame Size Adaption. This sends the correct size of packet to use automatically to remote web servers using TCP.

You can try communicating with your Internet Service provider but the problem may be out of their control as the router causing the problem can be half way around the world.

More information about this can be found in RFC2923 “TCP Problems with Path MTU Discovery”

Other Sources Of DSL Information

DSL Reports at http://www.dslreports.com/

PPTP Troubleshooting

If you are using a PPTP connection there are a few specific troubleshooting steps for you to try. These require using the web server diagnostic pages found at “Diagnostics With The Web Server” on page 380. Common problems that can block your Internet connection include...

- incorrect password
- PPTP server (ISP) not available
- incorrect IP configuration of WAN or LAN

Incorrect Password

If you have typed in an incorrect username or password you will not be able to open a PPTP Internet connection with your Internet Service Provider.

To check if this is the case visit the PPP Link (LCP) status page on your firewall. You will see the error message “CHAP authentication failed”. This means that a connection to the ISP is possible but that the username and password you have entered is incorrect.

Verify your username and password is correct and/ or contact your Internet Service Provider.

PPTP Server Not Available

If your cabling is incorrect, the modem is not functioning/ configured properly, the xDSL line is not functioning, or the IP Address of the WAN interface is not in the same subnet as the Broadband Modem you will not be able to reach your Broadband Modem’s PPTP server to correctly receive the IP configuration to communicate with the ISP.

To check that this connection is available or not visit the PPTP status page on your firewall. If you see the error message

- “Connection refused” means the IP address that was given for the PPTP Server is refusing to allow an PPTP connection.

- “Connection timed out” means there is no response from the remote IP Address when a request is made to open a PPTP tunnel.

Check that your cables are connected properly (all interface lights are green on your modem and MultiCom Firewall), and that the modem is configured to act as a bridge. Finally if these are OK, contact your Internet Service Provider to verify the line is connected properly.

Incorrect IP configuration of WAN or LAN

If the IP Address of the WAN interface is not in the same subnet as the Broadband Modem you will not be able to reach your Broadband Modem's PPTP server to correctly receive the IP configuration to communicate with the ISP.

To check that this connection is available or not visit the PPTP status page on your firewall. If you see the error message

- "No route to host" means the WAN Interface is configured for a different subnet than the IP address that was given for the PPTP Server.

Error Messages

The MultiCom Firewall has 6 methods for informing you what is happening and if something is wrong.

- LED light messages
- Webserver Status pages
- Telnet Status requests
- Monitor Software Status pages
- Email Messages
- Syslog messages
- SNMP messages

LED Light Messages

The LED lights on the front of your MultiCom Firewall are designed to give you a quick update on the current status of your firewall. Some of the things you can find out from your Interface LED lights (labeled LAN, WAN or DMZ) are

- If an ethernet interface is properly connected (a solid green light)
- If an interface is not connected (a solid red light)

- If data is traversing the interface (when the active port blinks orange, data is traveling through that interface)
- If there are collisions occurring on the firewall (the light red)

Starting with Lightning-Linux 3.3 the Security LED is also functional and will show:

- If SecureWall is activated (a solid green light)
- If SecureWall is deactivated but Filtering is activated (a solid orange light)
- If both SecureWall and Filtering are deactivated (a solid red light)

Diagnostics With The Web Server

By using a web browser you can get status information of ARP and routing tables, interfaces, memory and CPU loads, uptime and more. You just type in the IP address of the firewalls LAN or WAN interface, enter any necessary user names and passwords, and can browse the firewalls status. You can print this information out using your web browser's print functions.

Below are some of the direct web links to commonly used diagnostic information. The following examples use the firewall's default IP address of 10.0.0.1. If your firewall is using a different IP address use that in place of the 10.0.0.1.

Starting in Lightning-Linux 3.4 the webserver provides direct status information of the Firewall, services, interfaces, and logged events. Simply go to the web interface using a web browser and select the STATUS link. This page is shown below.

All of the web servers status screens are shown in the Web Server Screens Appendix in the Reference Manual.

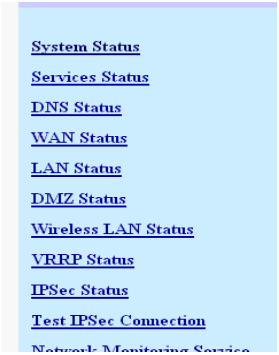


Table 3: Common web server diagnostics pages for firmware 3.0-3.3

MultiCom Serial number	http://10.0.0.1/config/system/hardware/
Software version	http://10.0.0.1/config/system/software/
LAN status	http://10.0.0.1/config/interface/ethernet[LAN]/status/
LAN DHCP server leases	http://10.0.0.1/config/interface/ethernet[LAN]/ip/dhcp/server/status/leases/
WAN status	http://10.0.0.1/config/interface/ethernet[WAN]/status/
WAN DHCP client status	http://10.0.0.1/config/interface/ethernet[WAN]/ip/dhcp/client/status/
PPPoE status	http://10.0.0.1/config/interface/ppp[PPPoE]/status/
PPPoE IP status	http://10.0.0.1/config/interface/ppp[PPPoE]/ipcp/status/
PPPoE Link status	http://10.0.0.1/config/interface/ppp[PPPoE]/lcp/status/
Available PPPoE servers	http://10.0.0.1/config/interface/ppp[PPPoE]/pppoe/server_list/
PPTP Status	http://10.0.0.1/config/interface/ppp[PPTP]/status/
PPTP Link status	http://10.0.0.1/config/interface/ppp[PPTP]/lcp/status/
ARP entries	http://10.0.0.1/config/arp/status/arp_entry/
DNS servers used	http://10.0.0.1/config/ip/dns/status/nameserver/

Using the above links will help you to find where a problem may be. For example, if you have checked the WAN status or the PPPoE status and they both have IP addresses assigned to them they are functioning normally and your problem is probably somewhere else.

Diagnostics with Telnet/ Console

By logging into the Firewall's telnet, SSH telnet or console interface (check your User's Manual to see if your firewall has a console interface) you can run the "status" command to get a single text output of the entire firewalls system status report.

You can then cut and paste that to an email file or print it out for review. This is nice if you do not want to open the web browsing port to your firewall or if you run telnet scripting utilities (such as the Expect software for Linux and Windows) for reports or configurations.

Table 4: Common telnet/ console diagnostics

Description	Commands	Sample output
last error causing reboot	/: backtrace	only available in 3.5+
MultiCom Serial number	/: info system hardware serial_number	serial_number = LI-MU7-CH-0200D2
Software version	/: info system software firmware	firmware = 3.1
LAN status	/: info interface ethernet LAN status status	status = UP RUNNING
LAN IP Address	/: info interface ethernet LAN status ip_address	ip_address = 10.0.0.1
	/: info interface ethernet LAN ip netmask	netmask = 255.0.0.0
LAN DHCP Mode	/: info interface ethernet LAN ip dhcp mode	mode = server
LAN DHCP server leases	/: info interface ethernet LAN ip dhcp server status leases	indexes: 0 1 2 3
	/: info interface ethernet LAN ip dhcp server status leases 0 ip	ip = 10.0.0.17
	/: info interface ethernet LAN ip dhcp server status leases 0 hw_address	hw_address = 00:c0:f0:4c:a7:90
	/: info interface ethernet LAN ip dhcp server status leases 0 starts	starts = 4 2001/06/28 13:24:06
	/: info interface ethernet LAN ip dhcp server status leases 0 ends	ends = 4 2001/06/28 14:24:06
	/: info interface ethernet LAN ip dhcp server status leases 0 hostname	hostname = "NT-workstation"
WAN status	/: info interface ethernet WAN status status	status = UP RUNNING
WAN DHCP client status	/: info interface ethernet WAN ip dhcp client status state	state = Assigned
PPPoE status	/: info interface ppp PPPoE status status	status = UP RUNNING
PPPoE IP address	/: info interface ppp PPPoE status ip_address	ip_address = 212.147.17.76

Description	Commands	Sample output
PPPoE IPCP info	/: info interface ppp PPPoE ipcp status state	state = UP state = DOWN
PPPoE Link status	/: info interface ppp PPPoE lcp status info	info = "" info = CHAP authentication failed info = Timeout sending Config-Requests info = Endpoint not connected
PPPoE DNS assigned servers	/: info interface ppp PPPoE ipcp status primary	primary = 212.147.10.10
	/: info interface ppp PPPoE ipcp status secondary	secondary = 212.147.0.1
Available PPPoE servers	/: info interface ppp PPPoE pppoe server_list	indexes: 0 1 2
	/: info interface ppp PPPoE pppoe server_list 0 access_concentrator_name	access_concentrator_name = ipc-lsp690-r-lc-01
	/: info interface ppp PPPoE pppoe server_list 0 service_name	service_name = Any
ARP entries	/: info arp status arp_entry	indexes: 0 1 2
	/: info arp status arp_entry 0 hw_address	hw_address = 00:C0:F0:57:4A:6D
	/: info arp status arp_entry 1 hw_address	hw_address = 00:C0:F0:4C:A7:90
DNS servers used	/: info ip dns status nameserver 0 ip	ip = 192.168.1.115
	/: info ip dns status nameserver 1 ip	ip = 192.168.1.116

The console interface is useful if you may have blocked your Ethernet interface access or think there may be a problem with your Ethernet network (your computer's Ethernet interface, a hub/ switch, cabling). Simply configure your workstations serial port according to the Console Configuration in the Hardware Specification chapter and plug in the serial cable to your MultiCom Firewall and workstation's 9pin serial port. This gives direct access to the firewall.

Table 5: Common telnet/ console commands

Description	Commands
ENABLE IPSEC	set security ipsec enabled=true saveconfig current
DISABLE IPSEC	set security ipsec enabled=false saveconfig current
ENABLE SECUREWALL	set interface ethernet WAN ip nat securewall=true saveconfig current
DISABLE SECUREWALL	set interface ethernet WAN ip nat securewall=false saveconfig current
ENABLE FILTERING	set ip filtering enabled=true saveconfig current
DISABLE FILTERING	set ip filtering enabled=false saveconfig current
ENABLE FILTERING OBJECTS	set ip filtering_objects enabled=true saveconfig current
DISABLE FILTERING OBJECTS	set ip filtering_objects enabled=false saveconfig current
ENABLE DNS PROXY	set ip dns proxy enabled=true saveconfig current
DISABLE DNS PROXY	set ip dns proxy enabled=false saveconfig current
ENABLE RIP	set routing ip rip enabled=true saveconfig current
DISABLE RIP	set routing ip rip enabled=false saveconfig current
ENABLE FTP	set ip ftp server enabled=true saveconfig current
DISABLE FTP	set ip ftp server enabled=false saveconfig current
ADD SYSLOG SERVER	add ip syslog server 0 set ip syslog server 0 address=10.0.0.2 level=debug saveconfig current
ENABLE SYSLOG DEBUG OUTPUT	eventdebug start
DISABLE SYSLOG DEBUG OUTPUT	eventdebug stop
ENABLE SSH	set security access ssh enabled=true saveconfig current
DISABLE SSH	set security access ssh enabled=true saveconfig current

Description	Commands
REBOOT	reboot
ENABLE TELNET	set security access telnet enabled=true saveconfig current
DISABLE TELNET	set security access telnet enabled=false saveconfig current
RENEW DHCP CLIENT ON WAN	dhcpclient WAN renew

Monitor Software

You can optionally load the Configurator software for even more diagnostic information. While this software is running you can see live statistics on the MultiCom Firewall. Please see the section on “Diagnostics with the Monitor” on page 328 for more information.

Email Messages

Email messages can be configured to send Service errors for all or selected internal service errors to one or more email addresses. See the section “Email Messages” on page 331.

Syslog Messages

Syslog messages can be configured to be sent from the firewall to a syslog server. Please refer to the section “Syslog Messages” on page 304 if you wish to use this functionality.

Some common, Syslog messages are

- Telnet logins and logouts
- Failed and successful attempts to save a configuration file to the firewall
- Failed logins
- DHCP activity
- PPPoE activity
- PPTP activity
- Startup of firewall

SNMP Messages

SNMP responses can be configured to be sent from the firewall to a SNMP client software. Please refer to the section “SNMP” on page 341 if you wish to use this functionality.

Configurator messages

The Configurator has a log window that lists successful activity and errors as they come up. These error messages will explain what has gone wrong and will help identify what is causing the problem. The information in this window can be cut and paste for printing or emailing.

To see the Log window click on the Tools Menu and select the Show Log command.

The error messages from the Configurator allow you to cut and paste the text in most operating systems. Check with your operating system for it’s method of cutting and pasting text into different windows.

Shell messages

Shell messages are messages that occur during a telnet or console session to your firewall. These messages are in response to a command that has been issued in a telnet session such as to try pinging an external source, getting statistics on a parameter or interface, or moving from directory to directory in the firewall itself. For more information on Shell commands see

Reloading The Default Configuration

If you think that a configuration is preventing you from accessing the firewall you may want to restore the default configuration of the firewall and start with a fresh configuration file.

This may be useful if you have configured your firewall in such a way that it is inaccessible (accidentally typing in the wrong IP address or if you have moved the firewall to a different network). When you want to restore the default configuration for your MultiCom Firewall you need only to follow these steps.

For firmware 3.6+

1. Leave the MultiCom Firewall powered on
2. Hold down the config button in the back, using a ballpoint pen if available, until the front LED lights change to RED. This will load the factory default configuration.
3. Optionally holding the config button down until the LEDs are ORANGE will load the last saved boot config or holding the config button down until the LEDs are GREEN will load the configuration in memory position 1.

NOTE - Resetting the default configuration this way does not erase your user accounts. To load the default configuration with the default "multicom" user account you will need to follow the instructions for **For firmware 3.0-3.4.1** below.

For firmware 3.5+

1. Leave the MultiCom Firewall powered on
2. Hold down the config button in the back, using a ballpoint pen if available, for 6 or more seconds will load the default configuration. (holding the config button down for 3 seconds will load the boot config.)

For firmware 3.0-3.4.1

1. Power off the MultiCom Firewall.
2. While holding down the config button in the back (using a ballpoint pen if available), turn on the MultiCom Firewall.
3. Wait for the firewall to finish booting up; this is when the LAN and WAN light remain either a steady green or red and the rest of the LEDs have stopped blinking.

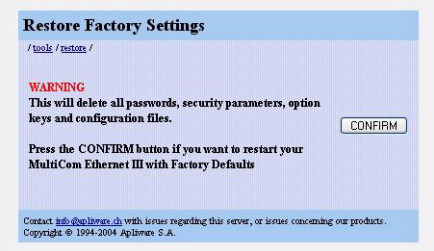
The default configuration is then loaded up into the current memory location of the MultiCom Firewall. Configurations, users, and option keys that were stored in the firewall prior to the reset are still saved in the memory of the firewall.

CAUTION - This configuration is temporary and unless you save it to the Boot Memory location on the firewall, your original configuration will return after a reboot.

Factory Reset Option

To completely reset the firewall you will need to goto the webserver of the MultiCom Firewall and select the Restore Factory Settings option in the Toolbox. The direct link to this page is: http://10.0.0.1/ tools/restore/.

This option will delete all passwords, security parameters, configuration files and options like SSH or IPSec. If you cannot reach the MultiCom Firewall on a network you may first have to load the default configuration as described above.



Chapter 20

How To ...

While there are indeed many capabilities of your MultiCom Firewall sometimes finding how to do something can be time consuming. To assist you in handling common tasks we have put together step by step instructions for configuring your MultiCom Firewall for certain features.

Each of the instructions assumes that you have opened the Configurator software and are at the advanced window. Remember that you can run the Configurator software from a CD or from an installation on your computer. Additionally you can use the Configurator when it is not connected to the firewall and save the changes to a text file for later uploading or emailing.

- Watch for security breaches
- Use one external IP address for multiple computers
- Configuring more than one external IP address
- Use one IP address for one computer
- Setup a testing environment
- Configure load sharing
- Copy between configurations

Watch For Security Breaches

One of the best ways to monitor security is to set up a Syslog server somewhere on your local or remote network and have your MultiCom Firewall notify it whenever strange activity occurs. Of course you will have to be the one defining strange behavior. Check the chapter on Security Configurations for suggestions on activity to log. Remember anything that you can filter you can log to the Syslog server.

To do this you will need to

- identify a Syslog server
- setup customized message events (i.e. filters with the logging option set)
- analyze your messages at the Syslog server

To identify your Syslog server that will receive your messages

1. go to the Misc>Syslog panel
2. enter in the IP address of the remote Syslog server
3. set the highest level of reports to send to this server (debug sending everything and emerg sending the least messages — those tagged as emergencies.)
4. click on Configuration>Save to save this configuration to the Current Config and/or Boot Config location on your MultiCom Firewall

To customize your own Syslog messages

1. go to the Filtering>Forwarding panel (though you could also choose Input, Output or User)
2. click on the enable filtering
3. click add and then advanced
4. define a type of data to watch for (for example maybe all outgoing TCP web connections, choose TCP under protocols and select destination port 80)
5. under Action choose log
6. under Log Level choose a priority level for your message (from 8 different options)
7. under Log Prefix optionally add a comment to identify the message more clearly, such as “webtraffic”
8. close the Advanced Filtering Window
9. click on Configuration>Save to save this configuration to the Current Config

and/or Boot Config location on your MultiCom Firewall.

> CAUTION — be sure that the priority level of your custom Syslog message is within the range you specified in the first step or else it will never be sent from the firewall.

Finally, depending on what features your Syslog server has available you can analyze the types and/ or frequency of your messages, you can look for key phrases (the ones you identified in the Log Prefix box), or maybe forward selected messages to a database, an email program, fax or pager.

Use One IP Address For Multiple Computers

Using one external IP address for many users is commonly called SUA or Single User Account. This is often used when the user has multiple computers that they want to access the Internet but only want to use one phone number or Internet Service Provider (ISP) and go through one modem. As far as the ISP is concerned they are only giving out one IP address.

Using NAT features you actually have all of your workstation Internet requests masquerading as if they were all coming from the same machine (in this case the MultiCom Firewall's WAN interface.) This IP address is typically an actual IP address that can be reached from anywhere on the Internet but it can change if the ISP assigns IP addresses dynamically, such as each time you logon to the ISP. The IP address can also be assigned statically so everyone will always knows how to get back to you (for example a business that has a publicly registered IP address).

To activate this functionality.

1. go to the NAT panel
2. select the Interface tab
3. select WAN Interface
4. click on NAT enabled
5. click on Configuration>Save to save this configuration to the Current Config and/or Boot Config location on your MultiCom Firewall

Now all data leaving through your WAN port will have their source IP address replaced by that of the WAN port and hence be allowed through your Internet Service Provider.

TIP — You can also specify specific groups of IP addresses, data protocols, or even destinations if you want to limit those computers using this access route.

Configure Virtual IP Addresses

Using NAT allows you to configure more than 1 external IP address to reach or leave your internal network. Two reasons why you would want to do this are...

- You have more than one publicly known IP address and want them to be routed into your network
- You have multiple outgoing connections and want to have different groups of users using different ones

When you have more than one publicly known IP address that will be coming through your WAN link you need to tell those data packets where to go. You can select the incoming data by choosing the destination IP address and/ or the destination port and redirecting the data to another server on the LAN or DMZ.

One example is given below but a more detailed description of this functionality is in the Section “Configuring Virtual IP” on page 182. Additional samples are on the CDROM (\Lightning_Software\Version_3.x\Configuration_Examples) or on the support website.

To setup multiple incoming IP addresses and map all of the incoming traffic from the WAN interface for the specified IP address to an internal server.

1. go to the NAT panel
2. click on the Interface tab
3. click on NAT enabled
4. click on WAN interface
5. click on NAT enabled
6. on the Input table click add
7. on the Input table click advanced

8. uncheck the “Check dest.” field
9. under Destination enter in the IP address that is to be added as a Virtual IP
10. under Map choose mapto
11. under To Address and Port enter in the internal (LAN or DMZ) destination for those data packets
12. repeat steps 6-11 for each additional Virtual IP address to be added
13. click on Configuration>Save to save this configuration to the Current Config and/or Boot Config location on your MultiCom Firewall

Preparing for source based routing

For preparing for source based routing (if you have additional bridges or routers capable of directing traffic based on its source IP address,) over multiple outgoing connections you will still use NAT but in a different way. Some organizations may have an series or group of Ethernet modems... some working on serial lines, some on analog and some on digital. Since these modems all have different speeds and costs associated with their use a system administrator may desire to route different types of data through different devices. With NAT you can select the source or the destination as the deciding factor in which device the data can travel on. Some options to consider are.

- source IP address — use this to identify groups of users to direct through a particular device
- destination IP address — to select which end points get which connection (for instance the company email servers maybe get to use the faster connections).
- destination Port address — allows you to redirect the data based on the type of service they are using, for instance port 80 for web access.

Once you have decided how you want to direct your data you will.

1. go to the NAT>Global panel
2. click on NAT enabled
3. click add
4. describe which data to be assigned a specific IP by entering in the descriptions as decided above in either the source, destination, or destination port fields
5. under Map choose “mapto”
6. under To Address and Port enter in the IP address of the device that will

become the source IP of the specified data

7. verify that the Type field says “source” so that the translation is done to the source section of the IP packet
8. click on Configuration>Save to save this configuration to the Current Config and/or Boot Config location on your MultiCom Firewall

Now all of the identified data will leave the MultiCom Firewall with the specified source address.

Use One IP Address For One Computer

This is the default configuration of the MultiCom Firewall. To help configure this quickly you can use the Easy Setup of the built-in webserver or the Configurator software. All traffic from the LAN will by default go through the WAN interface and share the IP address assigned to the WAN interface by the ISP. There are still have a couple choices.

- Do you want to manually assign the Ethernet information on each computer on your LAN network or have DHCP do it?
- Do you manually set the WAN IP address parameters or does your Internet Service Provider to do it with DHCP or PPPoE?

LAN: The benefit of having DHCP manage the computer(s) on the LAN is that changes and networking updates can happen more quickly and with less hassle. In some situations however, managing everything by hand is preferred to keep compatibility with older devices, software limitations or it is just a preference of the network administrator. By default the DHCP server is activated on the LAN interface.

WAN: By default the MultiCom Firewall will act as a DHCP client on the WAN side and a DHCP server on the LAN side (with the LAN interface being assigned the IP address of 10.0.0.1.) This means that if your modem is set up as a DHCP server and your computer is set up as a DHCP client you can just place the MultiCom Firewall in between them and have all of your data routed through correctly without any configuration.

To configure a PPPoE, PPTP or Static IP configuration for the WAN interface you will be using the Easy Setup of the MultiCom Firewall’s web server. These screens are shown on Section “Easy Setup” on page 445

Configuring the WAN interface with Easy Setup.

1. in a web browser enter the IP address of the MultiCom Firewall's LAN interface (by default this is 10.0.0.1)
2. when requested enter in the Username and Password to access the MultiCom Firewall (by default the username is "multicom" and there is no password
3. click `Easy Setup` in the menu on the left
4. click the "next" button
5. under Connection Type choose `static, PPPoE, or PPTP` as instructed by your ISP and click the "Next" button
6. enter in the WAN configuration parameters as given by your ISP (if you do not have the answer to these questions contact your ISP) and click the "Next" button
7. here you can change the LAN parameters if desired, it is usually best to not change the defaults
8. click the "Next" button when you are finished
9. the Lightning Firewall Filters window allows configuration of the default filters, click "Next"
10. the Firewall Host Mapping allows you to open holes in your firewall to allow traffic to specific servers on your network, click "Next"
11. click `Apply Configuration or Apply Configuration and Save as Boot` to save directly to your firewall

Now all of your LAN computers will receive an IP configuration from the MultiCom Firewall and send its traffic through the WAN interface to reach other networks (like the Internet).

CAUTION — If you change the LAN IP address, as soon as you activate the new IP address for the LAN link (immediately if you sent it to Current Config or after a reboot if you sent the change to Boot config) you will need to give the browser software the new IP address.

If you were accessing your firewall as a DHCP client the moment you activate the new IP address for the LAN interface your DHCP configuration will have become outdated. In this case it would be easiest (depending on your operating system) to drop your old DHCP information and ask for a new one.

Setup A Testing Environment

There are many considerations when setting up your own firewall testing environment. An ideal test environment would be having either 2 computers or one computer with two Ethernet interface cards. This allows you full observation of all data moving through the MultiCom Firewall. If you can do this you will probably want to configure the WAN port with a static IP address since there will be no modem or Internet Service Provider to assign it.

Depending on what features you will want to use you could test the following capabilities...

- Test that Syslog messages are arriving correctly
- Try to get past your filtering rules
- Watch for network address translations in the IP header
- Verify that you can reach DNS servers
- Access the firewall remotely
- Test user security

Using Syslog Reports

Enabling Syslog from the start will be helpful. There is a simple syslog server included with the Configurator software package under the menu item Tools>Syslog. While Syslog reporting relatively easy to set up (run a server on a machine and configure the firewall to send Syslog messages to that machines IP address) you may want to test out the receiving capabilities itself of the Syslog server. A product like Kiwi Enterprises Syslog Generator is a good way to test that your Syslog server is reachable.

To test the logging capability of filtering rules you can either try to access a service/ computer that was filtered or set the logging option to notify when that type of connection was attempted. Easy types of services to test could be telnet, ftp, or web access but another good service is ping. You could also try port scans and flooding through or of the firewall itself.

Be sure to try blocking and accepting packets through the firewall.

Packet Filter Testing

To test the filtering you can either try to access a service/ computer that was filtered or set the logging option to notify when that type of connection was attempted. Easy types of services to test could be telnet, ftp, or web access but another good service is ping. Be sure to try blocking and accepting packets through the firewall.

NOTE — Remember that filtering rules for incoming and outgoing are rules that affect packets going to the firewall specifically or originating from the firewall. For filtering data that moves through the firewall from one network to another use the Filter Forwarding panel.

Verify NAT Changes

Since network address translation will change the IP address or port address in the destination or source location of each TCP header you will probably want to have packet sniffers on at least one side if not both of your firewall. This will allow you to see data packets after they have traversed your firewall and you can clearly see any changes to the header of the data packet. For Windows NT servers you could use Network Monitor and for Linux you could use tcpdump or sniffit to capture packets traversing your network.

Testing DHCP Services

By setting one of your LAN computers to be a DHCP client and one of the ports on your MultiCom Firewall as a DHCP server you can test the ability of your firewall to configure TCP interfaces. Try dropping and asking again for a DHCP configuration from the client computer. Additionally, if you have a syslog server activated you will see numerous messages about the DHCP activity that the firewall is working with.

Verify DNS Access

To test if you are able to reach your Domain Name Servers you can try pinging or accessing a website on the other side of the firewall by using the full name of the remote computer, for example www.lightning.ch instead of 193.247.134.2. For this test you may want to actually be connected to your Internet Service Provider as it will be easy to see if you can reach Internet websites by their names (and hence show that the DNS servers are working correctly.

Remote access of the firewall

As long as you can access the Firewall's web server you can use the Configurator software. The software uses the port 80 to talk with the firewall. Try typing in the IP address of your firewall, preferably when it is not directly connected to your workstation.

For example, you could have the firewall connected to a second Ethernet interface port on a Linux workstation and want to reach it from a Windows machine connected to the first Ethernet interface port of the Linux workstation. Of course you will need to identify the Linux workstation as the firewall and not have filters blocking access to port 80.

User security

Your MultiCom Firewall has user security built in that will limit access at all points. After setting a user name and password try accessing the firewall via telnet, a web browser, and with the Configurator to verify that the security has been set correctly.

Configure Load Sharing

Configuring this is similar to configuring NAT redirection of data packets. However, instead of sending the data packets to one IP address, the destination is actually a range of IP addresses. A mapped destination of 10.0.0.10 - 10.0.0.15 would send packets randomly to any of the six specified IP addresses.

Once you have decided the range of possible destinations to direct data to you will.

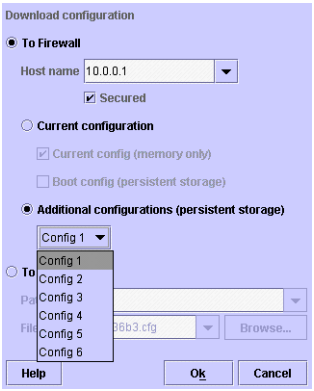
1. go to the NAT>Global panel
2. click on NAT enabled
3. click add

4. enter in the description of the data to be routed such the source or destination IP addresses or ports
5. under Map choose “mapto”
6. under To Address and Port enter in the range of IP addresses that will receive the data identified in step 4
7. under Type select destination to show that you want to change the destination portion of the IP packet identified in step 4
8. click on Configuration>Save to save this configuration to the Current Config and/or Boot Config location on your MultiCom Firewall

Uploading Or Saving Your Configuration File

Now that you have finished configuring the settings for your MultiCom Firewall firewall you need to either upload it into the firewall or save it for later uploading. If you are directly connected to your firewall you can simply click on the `Save` button to immediately apply the new configuration to your firewall. Otherwise you can save it to one of the 6 different memory locations on the firewall itself or to a file on your hard disk.

To upload the configuration to a memory location on your firewall follow the directions below.



1. click on `Configuration` > `Save`

2. select the `To firewall` option
3. enter in the IP address of your firewall (the default is 10.0.0.1) in the `Host name` box.
4. select one of the memory locations numbered Config 1 through 6
5. click on `OK`

> NOTE — You may optionally save to the Current config location on your MultiCom Firewall for your changes to take effect immediately without rebooting. Clicking on the `Save` button will also save to the Current config location.
>
> Remember that changes to the Current config are not saved however and that after a reboot they will be replaced by the contents of the Boot config.

To save the configuration to a file on your computer or floppy disk follow the directions below.

1. click on `Configuration` > `Save` to save to a local file
2. verify the directory you are saving to is correct, if not click `Browse` and choose the location of where you want to save your configuration
3. enter in the file name that you will save this configuration under
4. click on `OK`

> NOTE — You can use this same program to later open a saved configuration from either a firewall or a file.

Copy Between Configurations

It is possible to copy components of a configuration between configurations. Because the configurations are stored in text files you can open them in your favorite text editor and cut and paste sections to other configurations. You can also use a spreadsheet program or database to generate the text for long series on information.

For instance, the “The Configuration File” Section on page 50 shows a detailed configuration with filters logging requests to open connections to common TCP services. If you wanted to incorporate these filter rules into another config you could simply open up either two configurations in a text editor and cut and paste the parts you want.

Additionally, the Configurator software that comes with your MultiCom Firewall firewall has a text editor built in which you can directly copy information into.

> CAUTION - When cutting and pasting information into a configuration file you must be sure to follow the MultiCom Firewall format. For instance you cannot simply copy a group of filtering rules into the beginning of a configuration file and expect the MultiCom Firewall to know when and where you wanted them used.
>
> Consider copying information to similar areas of another configuration, such as copying User library filters to other User library sections.

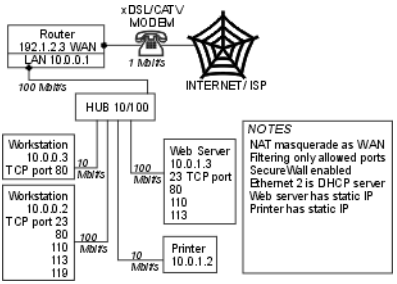
Such manipulation of your configuration should only be done by advanced users familiar with the format used by your MultiCom Firewall. If there is a problem with the configuration file the Configurator software will tell you that a parameter is incorrect.

Diagram Your Network

Designing a network diagram helps in planning your network layout and in future troubleshooting. The following sample shows a simple format that you may wish to follow. These are the goals of a well designed Network diagram

- Identification of network devices
- Identification of network access points or interfaces
- Identification of data communication methods (i.e. TCP ports)
- Clear pathways links to other devices
- Description of the network link (speed, encrypted, leased line...)

Figure 1: Sample Network Diagram



There are many software packages that can help you build/ manage your network plan such as tkined, HP Openview, Microsoft VISIO, KIVIO and others.

In many cases however, a custom design like the one shown above can be a very good building point for your specific and customized needs.

Appendix A

Frequently Asked Questions

Below are a collection of frequently asked questions of the MultiCom Firewall. For a more up to date FAQ list be sure to check the LIGHTNING web site at http://www.lightning.ch.

Frequently Asked Questions

What will a power outage do?

1. Without power no data will be able to go through the firewall. If you have saved your config to the memory of the firewall (such as the config boot location) then it will still be there when you boot up again. If your changes were only made in the config current location then your changes are erased and you will need to load them from a backup copy.
2. However, after 2 day without power your MultiCom Firewall will forget what the date is and reset itself back to January 1970. You would need to rest the date to the current time.

Can I back up my configuration?

3. Yes, you can save your configuration to a text file. Refer to the section on saving your configuration

My changed configuration disappeared after a reboot, what happened?

4. If you only save a configuration to the Current Config memory location in your firewall it is only temporary and will be erased after a reboot. This is useful for tests and quick changes. Be sure to always backup your config changes to a text file and/or keep a copy in one of the permanent memory locations in the firewall.

After making changes to the configuration I cannot reach the firewall any more.

5. Since you communicate with the firewall via an Ethernet connection it is possible to accidentally filter all traffic or route it incorrectly and hence block your own access to the firewall. In that case you will need to reboot the firewall into the default configuration and either edit your saved configuration or make a new one.

What is the default configuration of the firewall?

6. The while the default setting may be changed by your distributor or Internet To see the default configuration installed in the Ethernet firewall see the Concepts Chapter of the Lightning-Linux Reference Manual.

Why do some network services seem very slow after I have applied filtering?

7. Be sure to have read the chapter on filtering data and that you understand how your software communicates with remote servers. In particular port 113 is often used to verify if a communication link is valid and if all external packets are being dropped instead of rejected (allowing a message to be sent back to the remote server) the software keeps waiting for a response, eventually timing out.

How do I know what ports are being used?

8. The best place is to check with the manufacturer of the software that you are using. Consider using network monitoring software such as network monitor for Windows NT Server or the free software Ethereal at http://www.ethereal.com/ to track usage over a general amount of time and identify ports and addresses that are commonly being used.
9. Another option is to set the filters on your Ethernet firewall to log all types of TCP and/or UDP data. Your Syslog server will receive messages reporting all network traffic and you can then study the output for common usage types.

Can I use the firewall as a bridge?

10. The Ethernet firewall is not designed to be used as a bridge at this time.

What is the order that data goes through the firewall?

11. Data comes into an interface as Input and is subject to Input NAT rules for

the particular interface

12. Data is subject to filtering rules* (in the Filtering Forward Panel)
13. Data is subject to routing rules
14. Data goes out an Interface as Output and is subject to Output NAT rules for the particular interface
15. *data going directly to the firewall (telnet for example) use the Filtering Input panel and data leaving directly from the firewall (syslog message for example) uses the Filtering Output panel

How can I filter any thing but a certain address?

16. In the filtering source window you have the option of adding a ! before the IP address or Port number. For instance if you selected !10.0.0.1 you are selecting every IP address but 10.0.0.1. The same reaction occurs for ports such as !1000–2000 means all ports except those between 1000 and 2000.

If I log a packet will it continue through the filtering rules or will it be dropped?

17. Logging a packet in the filtering rules table does not stop it from going through other rules which in turn could drop, accept or use any other available action on them.

What is a connection and how does it affect my filtering rules?

18. Because data packets are necessarily small they may not contain all of the information that was requested in a data transaction (such as downloading a web page). When the first packet is allowed through you are actually saying that traffic related to this connection should be allowed through until its completion.

What is the IP address of my firewall?

19. Devices do not have IP addresses, only their interfaces. In that sense there are two IP addresses that will reach you firewall, the one on the LAN side and the one on the WAN side. If you have a DMZ, Wireless, DSL or multi-PPPoE configurations, your MultiCom can be reached by IP addresses assigned to those interfaces.

Do routing rules take place before or after IP addresses have been translated by NAT?

20. Routing takes place after IP network address translation, unless Output NAT rules are being used. Any Output NAT rules change the data after routing.

What happens if I turn off the SecureWall Firewall?

21. When the SecureWall Firewall is enabled for an interface all incoming data-packets must have a matching NAT rule to allow them into the network,

either through the internal Connection Tracking table (which keeps track of all outgoing requests to the Internet for data) or a fixed rule for services like Virtual IP or Port Mapping to an internal computer or server. When the SecureWall Firewall is turned off then data can come through with or without matching a NAT rule and it is up to the Stateful Packet Inspection Firewall to turn away data packets that you do not want.

If I use NAT to map a range of ports or IP addresses how does it choose?

22. Choosing ranges of port numbers or IP addresses tells NAT to randomly choose a number in this range to use for its mapping. This is also known as Round-Robin load-sharing.

Is it possible to assign more than 1 IP address to the WAN interface?

23. You can use NAT to have the Ethernet firewall accept data packets for an IP address other than the one assigned to the WAN interface. ARP requests to the WAN interface are only replied to when the requested IP address is the one assigned to the WAN interface or if the ARP Proxy is configured to respond to a chosen IP address. Otherwise no ARP replies will occur for the other IP addresses using NAT. Check the Virtual IP section of the Reference Manual.

If I am using NAT to redirect WAN data to an internal server can I also redirect LAN requests?

24. Yes, you can redirect LAN and WAN data to the same server when you enter in a NAT rule in the NAT Global panel and activate NAT on the LAN interface. This is a common use when redirecting HTTP (web) traffic to a publicly known IP address for users on the LAN... allowing them to use the same IP address as the external or WAN users. Activating NAT on the LAN interface will however make all traffic seem to originate from the LAN interface itself and so possibly cause problems with any statistics logs you are keeping. In this case it might be better to use the DNS server on the LAN instead of activating NAT.

Can I reset the connection for my WAN port on the Ethernet firewall

25. For a static configuration you simply use the Web Interface to access and change the WAN settings. For a DHCP client setting on an interface you need to telnet into the Ethernet firewall and enter `dhcpclient WAN renew`. And for a PPPoE configuration you open the Monitor window of the Configurator software, goto the PPP window and select the PPPoE interface you are using, and then click the RESET button on the screen. Of course you

could always simply reboot the device to reset all services.

Appendix A

Configurator Software Installation

This chapter will explain the configuration steps necessary to get your MultiCom Firewall up and running for most local network situations. This includes installing the configuration software, configuring to connect to your Internet Service Provider through your existing xDSL, cable or wireless modem, and configuring your computers to access the MultiCom Firewall.

> TIP - Users with firmware 3.1 or greater can always use the Easy Setup on the web server of the MultiCom Firewall to configure a quick and simple WAN and LAN connection

There are 3 ways to use the Configurator software for advanced configuration and monitoring of the MultiCom Firewall.

- Running the software from the Companion CD
- Installing the software to your computer and then use without the CD
- Copy the software from the Companion CD to your computer

Starting Easy Setup From The CD

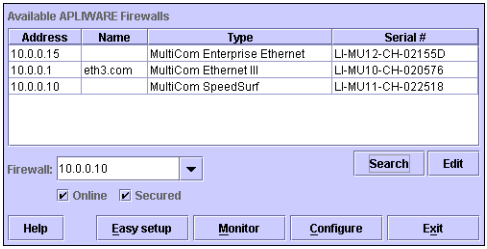
You will only be needing to read this section if your Internet Service Provider is not offering a DHCP server but you still want your LAN to be auto-configured by a DHCP server on the Ethernet Series. With the information from the previous section you will need to start the Configurator software and manually enter in that data.

While you can install the Configurator software onto your computer, these instructions will have you start the Configurator program from the Companion CD that was included with your packaging.

CAUTION — You must be using a computer that either is set as a DHCP Client or has a static IP Address (in the 10.x.x.x range) and a netmask of 255.0.0.0. Otherwise you will not be able to find the MultiCom Firewall.

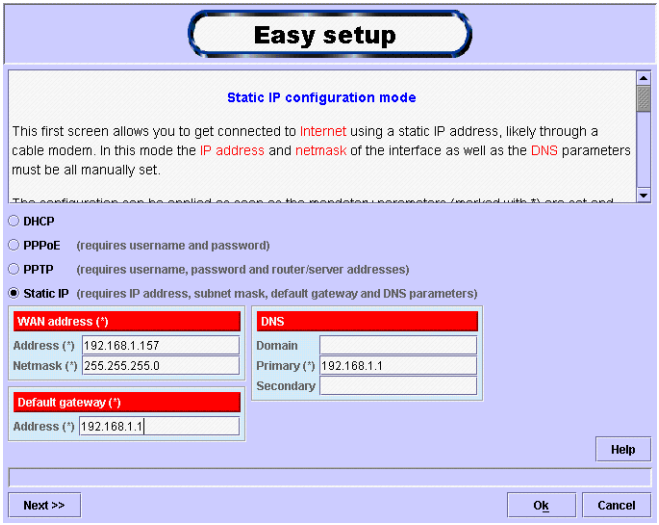
NOTE — If you wish to upload these settings or otherwise communicate directly with the MultiCom Firewall you will have to have TCP/IP installed already onto a computer with either a static IP address (in the 10.x.x.x range) and a subnet mask of 255.0.0.0.

1. To run the Configuration utility insert the Companion CD into your CD-ROM drive. The starting web page should automatically start on a Windows or Macintosh computer but you will not be using it to start the Configurator.
2. Next access your CD-ROM drive and select from one of the following files to start the Configurator (choose according to the type of operating system you will be running this software on.) To select the file simply double click on it.
   - `configwin.bat`
   - `configmac`
   - `configlinux`
3. When the Main window appears click on `Search` to search your network or directly type in the IP address directly of the LAN port of your Ethernet Series (by default this address is 10.0.0.1). Then click on `Easy Setup`.

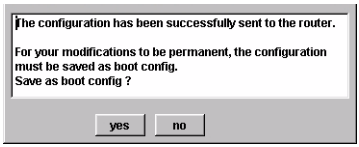


4. If asked enter in the Username and Password required to access the MultiCom Firewall and click `OK`.(by default the Username is “multicom” and there is no password but the Configurator software will automatically use this password for you.)

5. Click on the `Static IP` button to begin entering the information that you recorded above.

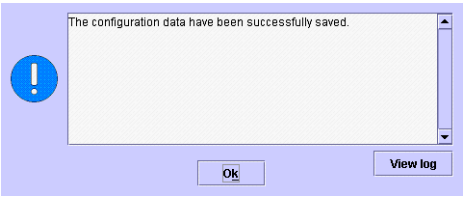


6. Enter in the WAN IP address that your MultiCom Firewall will be known as by your Internet Service Provider.
7. Enter in the netmask that will be used between the Internet Service Provider and the MultiCom Firewall.
8. Enter in the gateway address (otherwise known as the IP address of the Internet Service Provider's firewall).
9. Optionally enter in your local domain name. (This will become the default suffix used for networking activity.)
10. Enter in the IP addresses of your Internet Service Provider's Primary and Secondary DNS servers and then click `ok`.
11. Clicking `ok` will automatically upload the changes to your MultiCom Firewall. These changes however are not permanent unless you choose `yes` to the following screen.



NOTE — Choosing `yes` saves the configuration changes you have made so that when the Ethernet Series is rebooted your changes will still be there. If you choose `no` then these changes will be deleted the next time you reboot your MultiCom Firewall.

12. When the configuration has been successfully saved as the boot config you will see the following screen.



That is all there is to the Quick Start. You do not need to reboot your MultiCom Firewall for the changes to take affect but you may need to reboot your computer workstations that are going to begin using the firewall. After rebooting your computers that use DHCP clients they will be assigned addresses and other necessary information to reach the modem through the Ethernet Series.

TIP — If your operating system has the option to clear and renew DHCP information (such as the winipcfg panel of Windows 98) you can use this to get the necessary IP information from the Ethernet Series without rebooting the computer.

Installing The Configuration Software

Installing the Configuration software for your MultiCom Firewall requires that you have your Companion CD and a CD-ROM drive on your computer. Once the software has been installed on your hard drive you can run the software directly from the hard drive that it is stored on, without the use of the Companion CD.

CAUTION — Some operating systems (Windows NT, Unix, Linux) often have strict controls about installing software. Special privileges may need to be assigned to you for software installation to be successful. Check with your system administrator for the accepted method.

NOTE — The Configurator software is only for configuring your MultiCom Firewall. You do not need this software to be running to use the firewall, only to configure it.

In all cases please close and exit all other programs running on your operating system before inserting the MultiCom Companion CD.

The following instructions are specific to the type of computer you have — either a Windows 95, 98, NT, 2000 machine, a Macintosh with OS 9 or greater, Linux with kernel 2.2 or greater or a version of the Unix operating system. Go to the following section that describes your operating system to continue.

Configuration Software Requirements

For advanced configuration options you may install the Configurator Software from your MultiCom Companion CD. Below are the requirements to use this software.

- CD-ROM drive (if installing the Configuration software from CD-ROM)
- Mac OS 8.5 or higher, Windows 98 or higher, Windows NT 4.0 or higher, Linux kernel 2.2 or higher, Solaris version 2 or higher
- Pentium CPU, PowerPC CPU or better
- SVGA monitor with at least 800x600 pixel display and 256 colors (more than 256 colors are recommended)
- 64MB of RAM,
- 10 MB of free hard disk space

Additionally the Configurator installer for Linux and MacOS does not install any Java runtime (however it is installed for Windows). If either of these operating systems does not have an existing Java runtime (also known as JRE) the user will need to download and install it.

The current Java Runtime for Linux can be found at http://java.sun.com/j2se/1.3/jre/ and the current Java Runtime for Macintosh can be found at http://www.apple.com/java/. Running the Configurator from the MultiCom Companion CD does not require a separate Java Runtime for Windows or Linux machines because a Java Runtime is already installed on the CD.

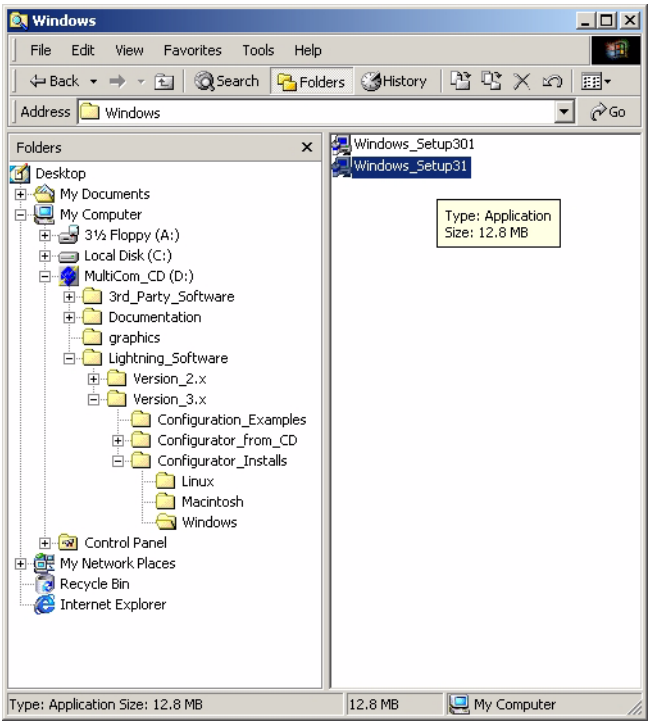
Windows

After inserting the Companion CD into your CD-ROM drive you can access it installation command by double clicking on `MY COMPUTER`. You should see all of the drives now connected to your Windows computer. Select the one that says `MultiCom_CD` and using the RIGHT mouse button click on it. A menu will appear and you will click on with either button on the word Explore.

NOTE - if your web browser opens instead of the menu then you have clicked on the icon with the left button instead of the right button.

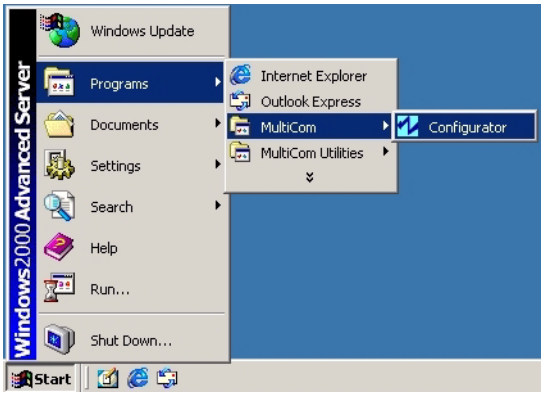
Install From CD

You should now have a list of the directories and files on your Companion CD. Go to the installation file named Windows_Setup31.exe located at Lightning_Software > Version_3.x > Configurator_Installs > Windows. Double click on this file to begin the installation process.



Please follow the instructions that appear on your screen to complete the installation of the Configurator.

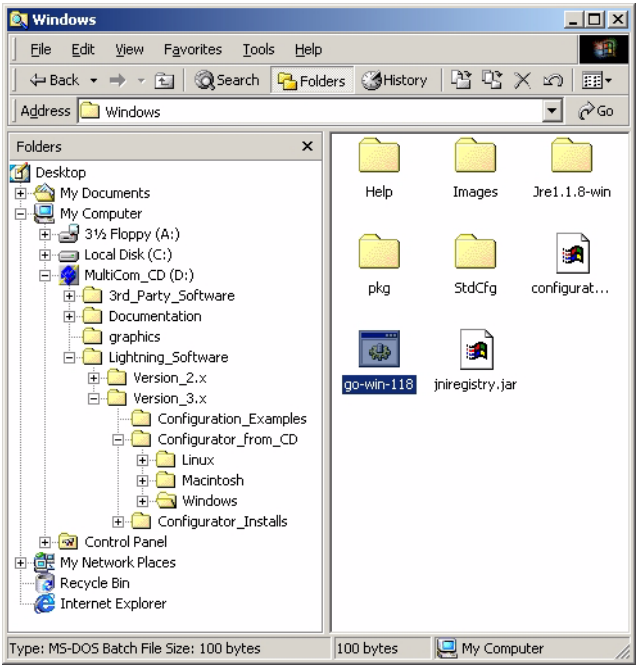
Once the installation has finished, start the software by clicking on your Windows `Start` menu, select Programs, select Lightning Firewall (or the custom subdirectory you chose during installation), and click on Configurator.



Now that the installation is finished you will not need the CD to run the Configurator software. Please remove the CD now and continue on to “Using the Configurator” Section on page 423.

Copy From CD

If you wish to install the Configurator to your Windows hard drive simply drag the folder containing the Configurator software to your hard disk. It is located in the following directory Lightning_Software > Version_3.x > Configurator_from_CD > Windows.

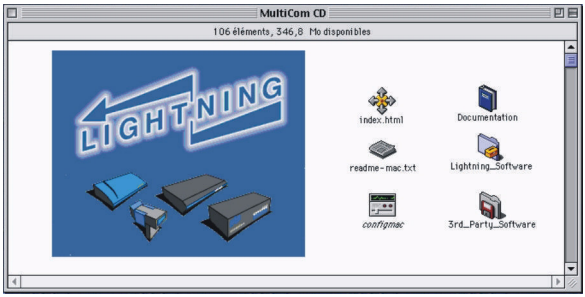


To start the Configurator, simply double click on the icon go-win-118.

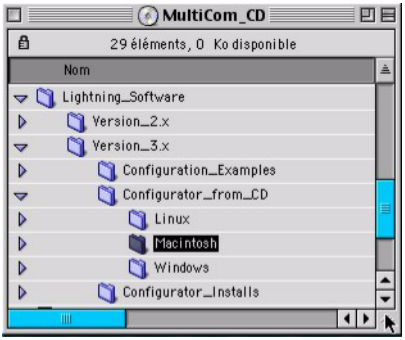
Macintosh

After inserting the Companion CD into your CD-ROM drive you will see it appear on the Desktop above the name `MultiCom_CD`. Double click on the CD.

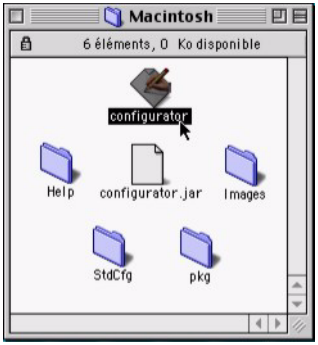
You should now have a list of the directories and files on your Companion CD. Please find `configmac` in the list (with an icon of a lightning bolt) and double click on that file to start the Configurator.



If you wish to install the Configurator to your Macintosh hard drive simply drag the folder containing the Configurator software to your hard disk. It is located in the following directory Lightning_Software > Version_3.x > Configurator_from_CD > Macintosh.



Once this directory is copied to your hard disk you can start the software by going to the directory you copied and double clicking on the icon named `Configurator`.



Now that the installation is finished you will not need the CD to run the Configurator software. Please remove the CD now and continue on to “Using the Configurator” Section on page 423.

Linux

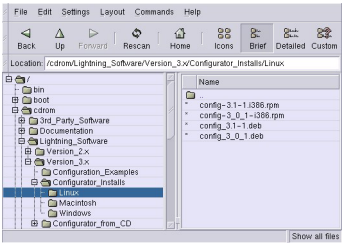
There are 2 options to installing the Configurator software on to a computer running Linux. You may either use your existing Java runtime installation by installing the .rpm or .deb file into your system or you can simply copy the entire folder from the CD-ROM.

> CAUTION - copying the entire folder to a computer running Linux will require nearly 40MB of free space on your hard disk.

Mounting a CD onto a Linux system could be done in many different ways depending on the distribution you have installed. Check with your system administrator for the preferred method of using your CD-ROM drive. In many cases you can mount your CD with the command `mount –t iso9660 –r /dev/cdrom /cdrom` (where /cdrom is the directory you use to mount the CD.)

Install From CD

Once the CD is mounted you will need to access the directory where the CD-ROM is mounted. Again the actual method for doing this will vary depending on your distribution but if you are in a terminal window you should be able to type `cd /cdrom` (using the above location that as an example). Finally, to get a list of the files on the cd type `ls`. If this has given you a list of files your CDROM has been mounted correctly. Next goto the directory with the installation files for the Configurator by typing the command `cd /Lightning_Software/Version_3.x/Configurator_Installs/Linux`.



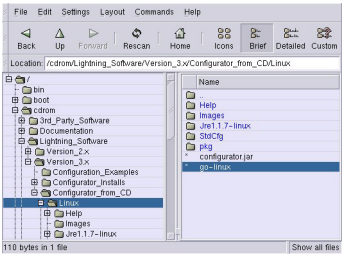
You should now be able to install either the Debian (the file with .deb) or Redhat (the file with .rpm) distribution depending on which version of Linux you are use.

The Debian command to install the Configurator is “dpkg -i config_3.1-1.deb” and the Redhat command to install the Configurator is “rpm -i config-3.1-1.rpm”. Once the Configurator has been installed you can run it by executing the command “multicom_configurator.”

Now that the installation is finished you will not need the CD to run the Configurator software, it is known as “multicom-configurator”. Please remove the CD now and continue on to “Using the Configurator” Section on page 423.

Copy From CD

If you wish to install the Configurator to your Linux hard drive simply drag the folder containing the Configurator software to your hard disk. It is located in the following directory Lightning_Software > Version_3.x > Configurator_from_CD > Linux.



Once this directory is copied to your hard disk you can start the software by going to the directory you copied and executing or double clicking on the file named `go-linux`.

Manual Configuration With Java

The JRE scripts of some Java runtimes are not well written. These JRE scripts build the CLASSPATH needed to run Java applications but it is not EXPORTED. In this case the Configurator will not start and the error "java\lang\Thread class not found" will be displayed (if the standard and error outputs were not redirected to the null device in the multicom_configurator script). To fix this situation, add the line "export CLASSPATH" to the JRE script after setting the CLASSPATH variable.

NOTE — on some Linux configurations you may find the Configurator window partially beyond your viewable area on your screen. Simply hold down the Alt key on the keyboard as you drag the window to a better viewing position.

Using The Configurator

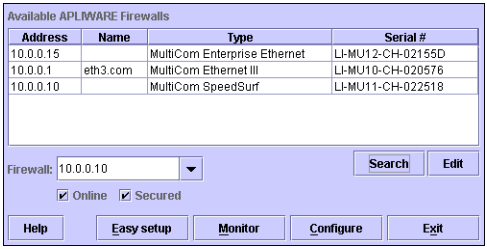
The Configurator software distributed with your MultiCom Firewall has been designed to be very robust and detailed. With it you will be making a configuration file that, when loaded into the firewall, will tell it how to interact with data passing through it or trying to pass through it. While many options are available you will now configure your firewall in a way suitable for your local network. If you would like to walk through a configuration tutorial please read the "Configuration Tutorial" Chapter on page 507.

To properly configure your firewall we will be using the information that you have written in the Pre-Configuration Checklist. Please be sure that you have filled in that information now before continuing.

For the following explanation we assume that you will be directly connected to your firewall, but you could also save the configuration file to your hard disk and upload it at a later time. Saving the configuration settings to a file does not require that you be connected to the firewall.

The Main Screen

The first screen that you will see is the Main window. Here you have five options to get started.



- Search for all connected MultiCom Firewall firewalls on your network or manually type in the IP address (10.0.0.1 is the default IP address for your MultiCom Firewall.)
- The Easy Setup button is for a quick configuration
- The MONITOR button is for diagnostic information on the MultiCom Firewall firewall at the selected IP address (please see the “Monitor Panels” Appendix on page 529 for descriptions of the screens available.)
- The Configure button is to access the Advanced Configuration mode for the most detailed setup options.
- The Help button is to access the online help for the MultiCom Firewall firewall.

> NOTE - If you want to immediately load the currently used configuration file of the selected MultiCom Firewall be sure that you have checked the “Online” box. Otherwise you will load a default configuration file.

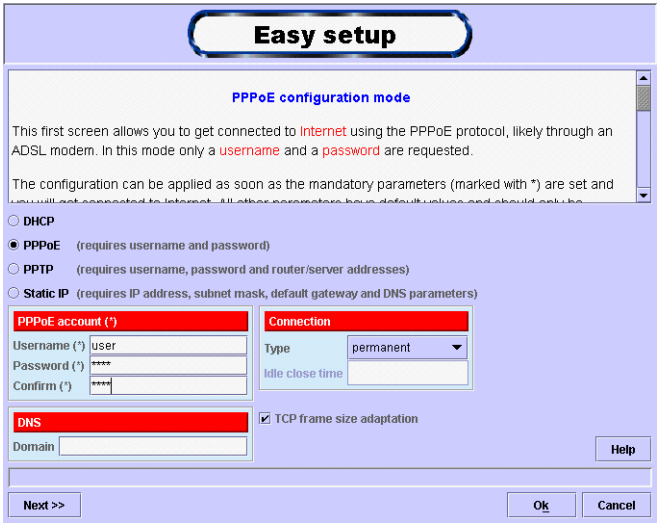
If you have already plugged everything in you can select search now to find your firewall on the local network.

Your firewall should appear as 10.0.0.1 unless you or your distributor changed the default. It should now appear in the Available firewalls window. Double click on this now.

CAUTION — Remember that you must be using a computer that either is set as a DHCP Client or has a static IP Address (in the 10.x.x.x range, for example 10.0.0.2) and a subnet mask of 255.0.0.0. Otherwise you will not be able to communicate with the MultiCom Firewall in its default settings.

Using Easy Setup

To configure basic Internet (or remote network) access with the default configuration of the MultiCom Firewall you use the Easy Setup window. Start Easy Setup by clicking the Easy Setup button on the Main screen. The following window will appear.



The Easy Setup window allows for fast configuration of your MultiCom Firewall firewall's WAN interface using DHCP, PPPoE or a static configuration. Your next choice depends on how your Internet Service Provider offers to connect you to the Internet.

DHCP Configuration from the Internet Service Provider

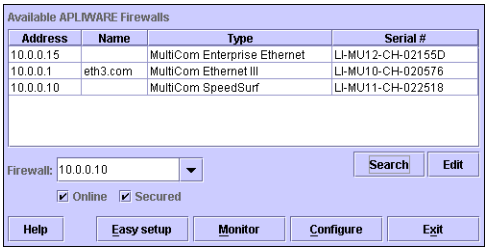
If your Internet Service Provider connects you using a DHCP server you will not have to configure any parameters with Easy Setup because this is the default mode of the MultiCom Firewall. During the bootup of your firewall in its default mode it will automatically search for the DHCP server and configure itself with everything needed to reach the Internet Service Provider.

Optionally you can indeed open the Easy Setup window, select the DHCP option and click the OK button to apply your changes.

PPPoE Configuration from the Internet Service Provider

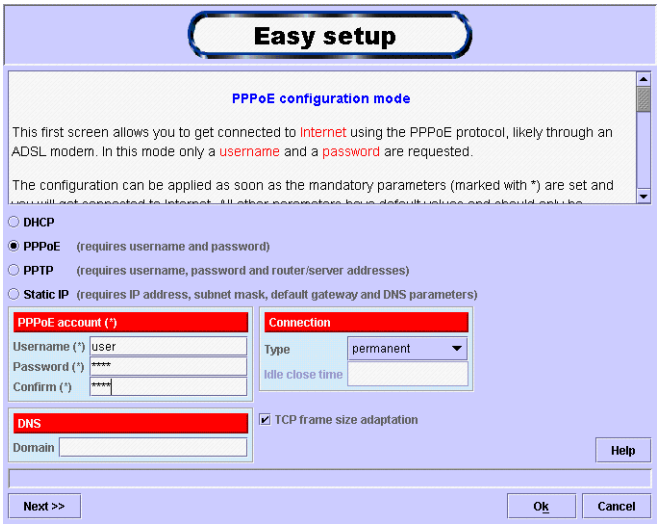
If your Internet Service Provider connects you using a PPPoE server you need to click the PPPoE option in the Easy Setup Window (see the window above). This window only requires a username and password to access your Internet Service Provider (ISP). This information is available from your ISP. Below are the steps necessary to configure a PPPoE connection.

1. When the Main window appears click on `Easy Setup` to open that window. Be sure that you have either selected a firewall that was found on the network or have typed in the IP address of the firewall you are going to configure (10.0.0.1 is the default IP address for your MultiCom Firewall firewall.)



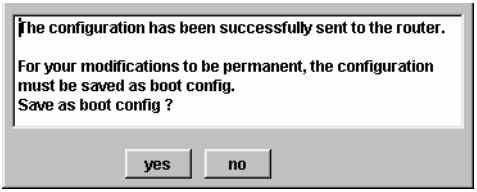
2. If asked, enter in the Username and Password required to access the MultiCom Firewall and click `OK`. (by default the Username is “multicom” and there is no password but the Configurator software will automatically use this password for you.)

3. Click on the PPPoE button to see the places to enter in your username and password.



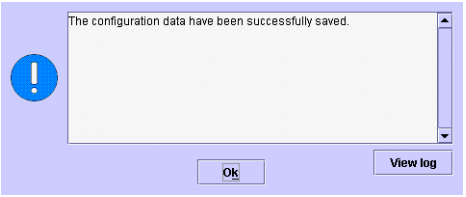
4. Enter in the username that your Internet Service Provider gave to you.
5. Enter in the password that your Internet Service Provider gave to you.
6. Optionally enter in your local domain name. (This will become the default suffix used for networking activity.)
7. Optionally enable the TCP Frame Size Adaption as a troubleshooting step if you are having problems connecting to your Internet Service Provider.
8. Click ok
9. Clicking ok will automatically upload and activate the changes to your MultiCom Firewall. These changes however are not permanent unless you

choose `yes` to the following screen.



NOTE — Choosing `yes` saves the configuration changes you have made so that when the MultiCom Firewall is rebooted your changes will still be there. If you choose `no` then these changes will be deleted the next time you reboot your MultiCom Firewall.

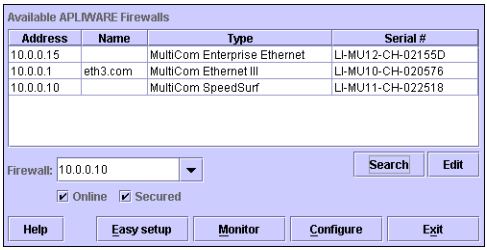
10. When the configuration has been successfully saved as the boot config you will see the following screen. Clicking the OK button will close the Easy Setup.



Static Configuration from the Internet Service Provider

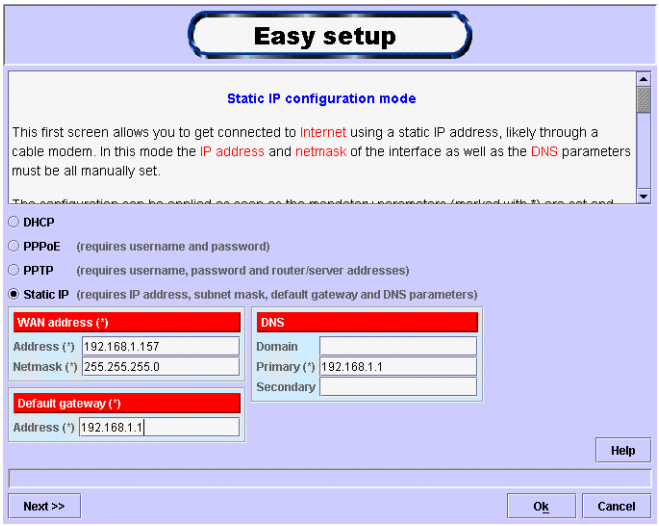
In some cases your Internet Service Provider will have you configure all of the necessary information manually. This is common when you are assigned a static IP address that will not change. The needed configuration information is available from your Internet Service Provider. Below are the steps necessary to configure a Static connection.

1. When the Main window appears click on `Easy Setup` to open that window. Be sure that you have either selected a firewall that was found on the network or have typed in the IP address of the firewall you are going to configure (10.0.0.1 is the default IP address for your MultiCom Firewall firewall.)

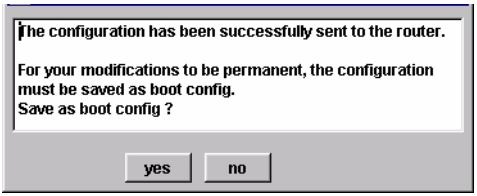


2. If asked enter in the Username and Password required to access the MultiCom Firewall and click `OK`.(by default the Username is “multicom” and there is no password but the Configurator software will automatically use this password for you.)

3. Click on the `Static IP` button to begin entering the information that you recorded above.

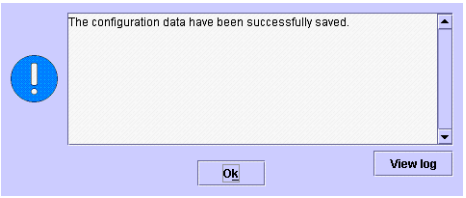


4. Enter in the WAN IP Address that your MultiCom Firewall will be known as by your Internet Service Provider.
5. Enter in the WAN netmask that will be used between the Internet Service Provider and the MultiCom Firewall.
6. Enter in the default gateway address (otherwise known as the IP address of the Internet Service Provider's firewall).
7. Optionally enter in your local domain name. (This will become the default suffix used for networking activity.)
8. Enter in the IP addresses of your Internet Service Provider's Primary and Secondary DNS servers and then click `ok`.
9. Clicking `ok` will automatically upload the changes to your MultiCom Firewall firewall. These changes however are not permanent unless you choose `yes` to the following screen.



NOTE — Choosing `yes` saves the configuration changes you have made so that when the MultiCom Firewall is rebooted your changes will still be there. If you choose `no` then these changes will be deleted the next time you reboot your MultiCom Firewall.

10. When the configuration has been successfully saved as the boot config you will see the following screen. Clicking the OK button will close the Easy Setup.



Configuring Your Computers

Now that your MultiCom Firewall is configured you have to set up your computers to access it. There are two general paths for you to follow.

- Set each computer as a DHCP client to receive all necessary information from the MultiCom Firewall each time you boot up your computer on the local network.
- Manually choose IP addresses for each computer on your network and enter in the IP address of the MultiCom Firewall as the firewall for trying to reach the Internet.

To process to enter these settings into your computer varies depending on your operating system. If you do not see your operating system represented in the following sections please refer to your computer's user's manual for explanations on configuring your network settings.

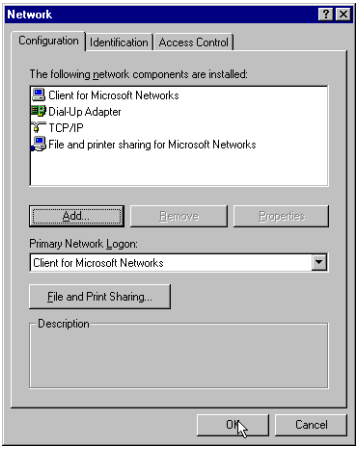
Windows

Windows 9x

To reach the network control on a Windows 95, 98 machine click on `START` > `Parameters` > `Control Panel` > `Network Settings`.

In your networking window you should be in the Configuration panel. Here you will see the network devices (such as your ethernet card/interface) and the protocols installed for each device.

Find the setting the says `TCP/IP -> (the name of your ethernet card)` or just `TCP/IP` and double click on it to open the properties window.



NOTE — if you have scrolled down to the bottom of the list and do not see either TCP/IP or the name of your ethernet card/interface then they are not installed in your computer. Please check the instructions that came with your ethernet card/interface to install that now.

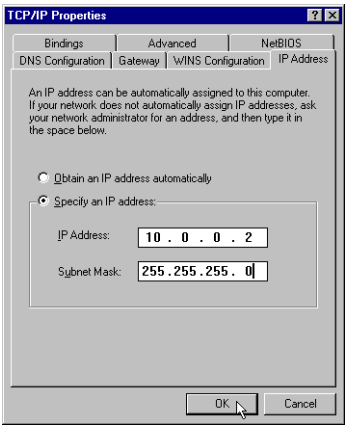
To set your computer as a DHCP Client

1. choose the IP Address tab
2. click on `Obtain IP address automatically`.
3. click on `OK`

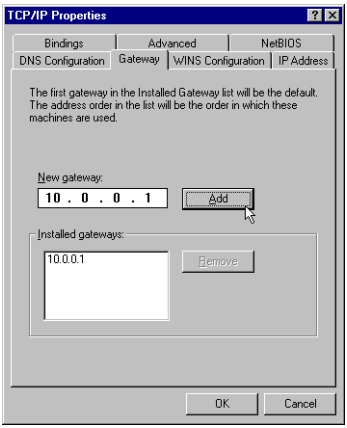
4. click on OK
5. follow the onscreen instructions (which will probably have you reboot your computer)
6. if you have the option to select a DNS server choose Obtain DNS automatically.

To manually set your computer's IP address

1. choose the IP address tab
2. choose specify an IP address
3. enter the IP address and Netmask for your computer (the Netmask should be the same as is configured for the LAN interface of the MultiCom Firewall)
4. choose the Gateway tab
5. Under New Gateway, enter in the IP address of your MultiCom Firewall's LAN interface and click add
6. click on OK to close and save the properties window
7. click on OK to close and apply the network controls for your computer
8. follow the onscreen instructions (which will probably have you reboot your computer)



Windows IP Address Panel



Windows Gateway Panel

Now you are finished configuring your Windows computer to access your MultiCom Firewall. Please continue onto the next section to test your that everything is set up correctly.

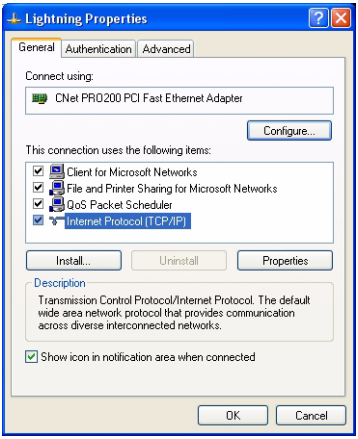
Windows 2000 or XP

To reach the network control on a Windows 2000 or XP machine click on `START` > `Control Panel` > `Network Connections`.

Right click on your network card and select “Properties.”

In your Properties window you should see the protocols and services installed for the selected network device.

Find the setting the says `Internet Protocol (TCP/IP)` and double click on it to open the properties window.



NOTE — if you have scrolled down to the bottom of the list and do not see either TCP/IP or the name of your ethernet card/interface then they are not installed in your computer. Please check the instructions that came with your ethernet card/interface to install that now.

To set your computer as a DHCP Client

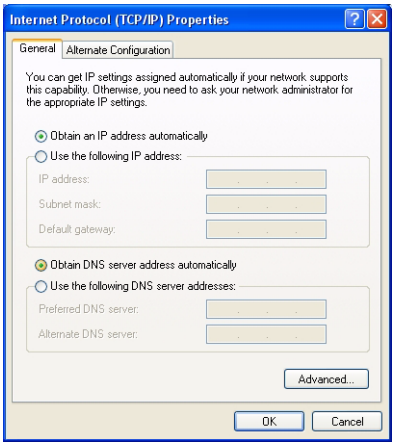
1. choose the `General` tab
2. click on `Obtain IP address automatically`.
3. click on `Obtain DNS server address automatically`
4. click on `OK`
5. follow the onscreen instructions (which might ask you to reboot your computer)

To manually set your computer's IP address

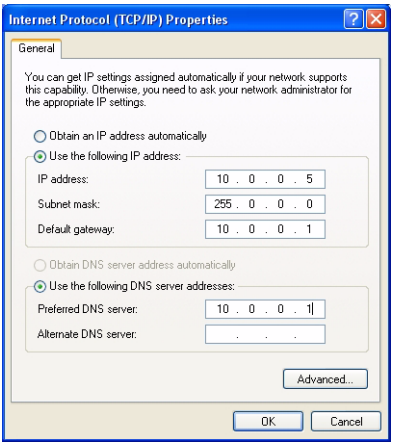
1.choose the `General` tab

2.click on `Use the following IP address`

3. enter the IP address, Subnet mask, and Default gateway. Be sure that the Subnet Mask and Default gateway match the settings of the MultiCom Firewall's LAN interface.
4. click on `Use the following DNS server addresses`
5. Under `Preferred DNS server`, enter in the IP address of your MultiCom Firewall's LAN interface or the Primary DNS server of your ISP
6. Under `Alternate DNS server`, leave it blank or enter the Secondary DNS server of your ISP
7. click on `OK`
8. follow the onscreen instructions (which might ask you to reboot your computer)



Ethernet DHCP Client



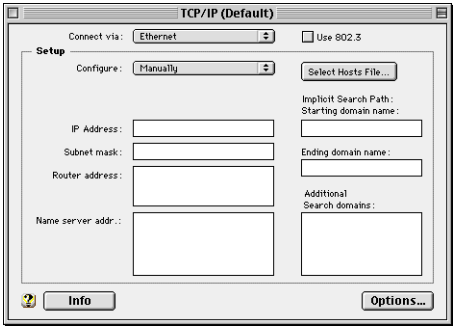
Ethernet Static IP Address

Now you are finished configuring your Windows computer to access your MultiCom Firewall. Please continue onto the next section to test your that everything is set up correctly.

Macintosh

To reach the network control panel on your Macintosh you need to choose on your `Apple Menu` > `Control Panels` > `TCP/IP Panel`. This is where you will find the options to set your Macintosh to use a DHCP server on the network or to use static IP addressing.

These instructions use MacOS9. If you do not see a TCP/IP control panel or are using an earlier version of the MacOS software please check the documentation that came with your Macintosh Operating system for instructions on how to load TCP/IP protocols into your computer.



To set your computer as a DHCP client

1. under `Configure` select "`Using DHCP`"
2. close the TCP/IP panel
3. choose "`Save`" when asked if you want to save your changes

To manually set your computer's IP address

1. under `Configure` select "`Manually`"
2. enter the IP address for your computer in the `IP address` field
3. enter your network mask in the `Network mask` field
4. enter your firewall IP address (the IP address of your MultiCom Firewall's LAN interface) in the `firewall address` field
5. enter the DNS server IP addresses in the `Name server addr` field
6. enter your local domain (if you have one) in the `Starting domain name` field
7. close the TCP/IP panel
8. choose "`Save`" when asked if you want to save your changes

Linux

Configuring the network settings for your Linux-based computer will depend on the type of graphical interface and distribution that you have. Be sure you've installed the TCP/IP options when you installed your version of Linux. Otherwise please refer to the documentation that came with your system for the method of configuring your particular networking options.

The following instructions were used on the Debian distribution by editing the configuration file at `/etc/network`

For configuration of the Ethernet interface to use DHCP services

```
iface eth0 inet dhcp
```

To manually set the IP address of the interface card

```
iface eth0 inet static

address 10.0.0.200

netmask 255.0.0.0

broadcast 10.0.0.255

firewall 10.0.0.1
```

Testing Your Configuration

The process of communication to the Internet works as follows when your MultiCom Firewall and workstation computers are configured properly.

1. Your computer makes a request to reach the Internet or a service from the Internet.
2. This request is sent to the network through your Ethernet interface.
3. Your Ethernet interface forwards this information to the MultiCom Firewall firewall
4. Your MultiCom Firewall takes this information and forwards it to your modem
5. your modem, unless already connected will dial your Internet Service Provider, authenticate your user name and password and then send information request to the Internet

The information that you requested will follow the same route back to reach your computer. In most cases you will either get the information that you received, get a response that it was not found, or because of network congestion be told that your request has timed-out and was dropped.

To test that your connections are working correctly you can open your preferred Internet browser (Netscape Navigator or Microsoft's Internet Explorer) and type in a web address.

NOTE — please hit the refresh page on your browser to be sure that you are getting information from the Internet directly instead of from a web page saved to your hard disk.

Unless your modem is already connected it will make the phone call now and retrieve the information that your computer requested. If you are able to reach the Internet then everything is working properly. If you have problems first check that everything is plugged in, go over this chapter again, check the Troubleshooting chapter, and finally consider calling the Technical Support of where you purchased your MultiCom Firewall from.

Don't forget to register your MultiCom Firewall and consider reading up on the more advanced options available.

CAUTION — A request to the Internet may be made without your being aware of it. These requests could inadvertently open your network connection and cause you additional phone. Check the Troubleshooting chapter for more information on Internet connections

For more detailed testing suggestions for your configuration and firewall check the How To.. section on “Testing the Router” on page 396.

Testing security

Here are some web sites that offer free security scanning of your Internet connection. There are many such sites available on the Internet.

http://www.dslreports.com/scan

http://www.securetips.com/tools/portscan.asp

http://www.hackerwhacker.com/

http://scan.sygatetech.com/

http://security1.norton.com/us/intro.asp

http://www.mcafeeasap.com/asp_subscribe/trial_cc.asp

Testing connection speed

Here are some web sites that offer free bandwidth tests of your Internet connection. There are many such sites available on the Internet.

http://www.zdnet.co.uk/misc/band-test/speedtest50.html

http://www.testmyspeed.com/internationalspeedtests.htm

http://www.dslreports.com/stest

http://www.gibroadband.com/speedtest.asp

http://bandwidthplace.com/speedtest/

http://www.itzalist.com/com/cable-speed-test.html

Fine Tuning Your Configuration

The default configuration that you have just set up enables the basic features of your MultiCom Firewall. For more advanced features please refer to the following chapters “How To ...” on page 389, “Security Configurations” on page 357 or “System Maintenance” on page 349.

Registering Your firewall

Registering your firewall allows you to keep up to date with the latest developments for your product. Additionally registration takes away the burden of keeping proofs of purchase (for upgrades or repairs) as our database will take care of that for you. Now is a good time to do it while you have your receipts and serial number readily available.

For online registration go to http://www.lightning.ch/register.html

Appendix D

Web Server Screens

The built-in web server provides quick access to many features of your MultiCom Firewall. If the SecureWall or Stateful Filtering are not blocking access you can reach these screens from any interface using http or the secured https.

The webserver allows the authorized visitor to:

- Use the Easy-Setup configuration (for DHCP, PPPoE, PPTP, or Static IP)
- Use the Easy IPSec for quickly configuring and testing IPSec connections
- Configure the LAN, WAN, DMZ, and Easy Firewall
- Upgrade the firmware or add IPSec VPN options
- View, edit add and delete user names and passwords
- Edit, download and upload your configuration or IPSec security file
- View the status of the Firewall, services, interfaces, and logged events
- View the status of the Network Monitoring Service and IPSec connections
- Reboot the MultiCom Firewall
- Restore the factory defaults
- Configure time, date and language on the MultiCom Firewall
- Edit, download and upload the URL Filtering rules file

To access all Configuration options you must use the Configurator software or access the CLI interface through Telnet, SSH Secured Telnet or the serial interface (if your Multicom Firewall has a serial interface).

Additional status messages can be received by email, syslog, snmp, or by using the Monitoring screen of the Configurator software.

Navigation Menu

This menu is found on the left side of the webpage. It provides access to the different categories of web pages available on the MultiCom Firewall and is available in different languages. This menu is available in all of the other web pages.

Home:	the Web Main page
Easy Setup:	access point for the Easy-Setup configuration tools
IPSec:	configuration wizard for IPSec connections
WAN:	WAN interface settings page
LAN:	LAN interface settings page
DMZ:	DMZ interface settings page (if the device has a DMZ interface)
WLAN:	Wireless interface settings page
Firewall:	access point for web based Firewall configuration tools
Toolbox:	access point for other tools
Status:	access point for system diagnostic screens
Advanced:	access point to advanced parameters

Web Main Window

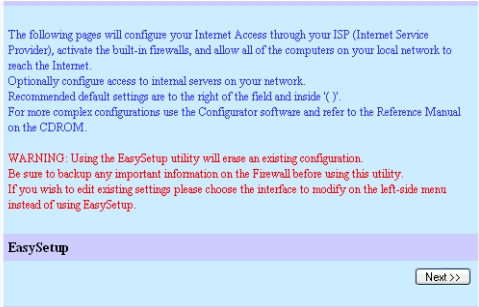
The Main Menu shows you the options you can access on your MultiCom Firewall via the built-in web server. The serial number, hardware model and firmware version is shown.

Easy Setup:	access point for the Easy-Setup configuration tools
Registration:	link to the registration page

Easy Setup

Easy Setup Menu Page

The Main Menu shows you the options you the 3 Easy Setup options for configuring the MultiCom Firewall - DHCP, PPPoE, and Static IP.

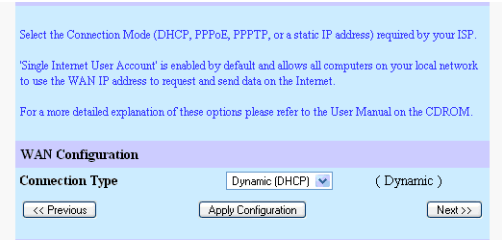


Next:	start the Easy Setup

WAN Setup Web

The WAN Setup page allows the user to configure the settings of the MultiCom Firewall's WAN interface without the use of the Configurator software. After setting the WAN choice as instructed by your ISP you can then choose to accept the default settings for your LAN or to customize them as needed.

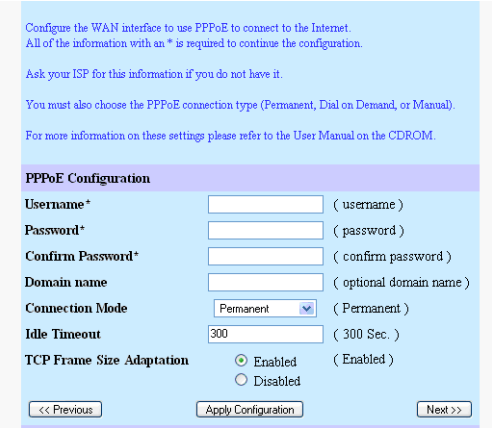
By default the connection type of the WAN interface is DHCP which sets your WAN port to automatically configure itself as a DHCP client (receiving its IP configuration from your ISP). Optionally you can also select PPPoE, PPTP, or a static IP configuration. Be sure to check with your ISP if you have questions about the type of WAN connection they support.



Connection Type:	configure the WAN interface as a static IP interface or, DHCP, PPPoE, PPTP client
Hostname:	optionally give a name to the MultiCom Firewall
Single Internet User Account:	currently not available
Previous:	go back to the previous page
Reset Values:	reset the default values
Next:	continue to the next configuration screen

WAN PPPoE Web

If the WAN Setup page has chosen PPPoE for the connection type this is the next visible window. PPPoE web parameters are configured for your WAN port to use a username and password to make a connection to your ISP. You can then click Next and choose to accept the default settings for your LAN or to customize them as needed. Be sure to check with your ISP if you have questions about the type of WAN connection they support.



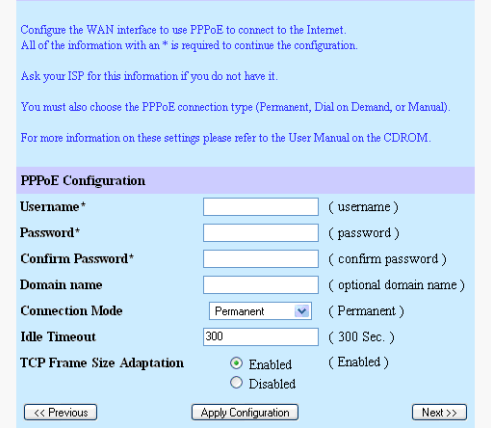
Username:	this is the username used to connect with your Internet Service Provider
Password:	this is the password used to connect with your Internet Service Provider
Confirm:	reenter your password to verify it was entered correctly
Domain:	this is the domain name of the LAN the firewall is connected to, for example lightning.ch
Connection Type:	for PPPoE connections, choose the type of connection: Permanent (connection is always maintained), dial on demand (connection made when activity is requested on the selected interface, and closed after idle close time passes), or manual (all connections are opened from the Monitor screen for the selected PPP interface)
Idle Close Time:	the time in seconds before a “dial on demand” or ”manual” PPPoE connection is closed due to a lack of data traffic

TCP frame size adaption:	this enables or disables the MTU adaption. This is normally disabled and is an advanced troubleshooting option.
Previous:	go back to the previous page
Reset Values:	reset the default values
Next:	continue to the next configuration screen

WAN PPTP Web

If the WAN Setup page has chosen PPTP for the connection type this is the next visible window. PPPoE web parameters are configured for your WAN port to use a username and password to make a connection to your ISP. You can then click Next and choose to accept the default settings for your LAN or to customize them as needed.

Be sure to check with your ISP if you have questions about the type of WAN connection they support. Because using PPTP also configures your WAN interface be 10.0.0.1/255.0.0.0 and changes the LAN interface to 192.168.1.1/255.255.255.0.

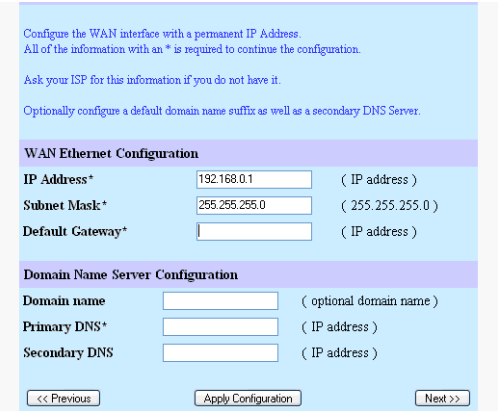


Username:	this is the username used to connect with your Internet Service Provider
Password:	this is the password used to connect with your Internet Service Provider
Confirm:	reenter your password to verify it was entered correctly
Domain Name:	this is the domain name of the LAN the firewall is connected to, for example lightning.ch
PPTP Server IP Address:	This is the IP address of your PPTP server, typically the default is 10.0.0.138 for known modems offering PPTP configuration

WAN IP Address	This is the IP address of the WAN interface that is connected to the Broadband modem. The default of 10.0.0.1 is good for most cases.
Subnet Mask:	This is the netmask of the WAN interface that is connected to the Broadband modem. The default of 255.0.0.0 is good for most cases.
Previous:	go back to the previous page
Reset Values:	reset the default values
Next:	continue to the next configuration screen

WAN Static IP Web

This is how the WAN Option panel looks after the Static IP option has been clicked. It shows you the parameters needed to manually configure the WAN interface with a Static IP. If your ISP has told you to manually configure your WAN interface this is where you will enter in the information that they send you. Be sure to check with your ISP if you have questions about the type of WAN connection they support. You can then click Next and either accept the default settings for your LAN or to customize them as needed.

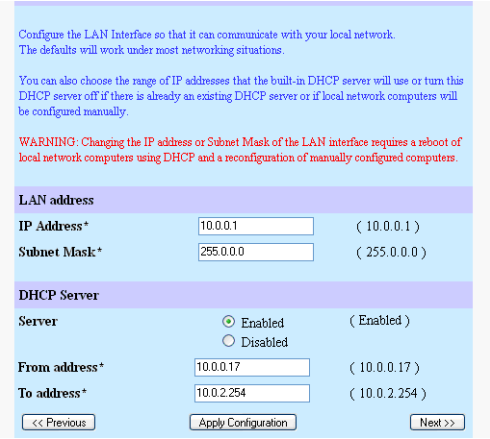


Address:	where you set the IP address for the WAN port
Netmask:	where you set the netmask for the WAN port
Firewall Address:	the IP address of the device to forward outgoing data to (usually your Internet Service Provider)
Domain:	this is the domain name of the LAN the firewall is connected to, for example lightning.ch
Primary DNS:	this is the Primary IP address of the DNS server for the firewall to use
Secondary DNS:	this is the backup IP address of a DNS server for the firewall to use
LAN Address:	configure the LAN interface static IP address
LAN Netmask:	configure the LAN interface netmask
LAN DHCP server:	enable LAN interface be a DHCP server
From address:	this is the start of a range of IP addresses to be offered DHCP clients on your network

To address:	this is the end of a range of IP addresses to be offered DHCP clients on your network
Previous:	go back to the previous page
Reset Values:	reset the default values
Next:	continue to the next configuration screen

LAN Setup Web

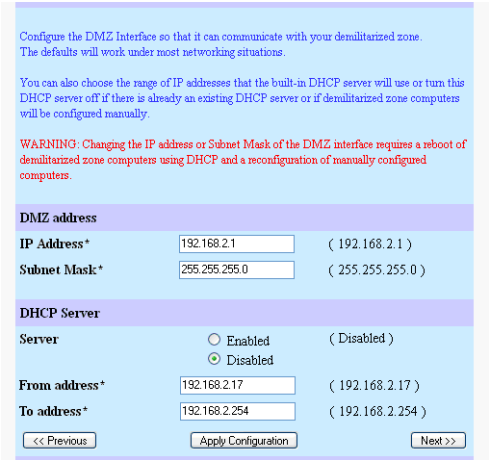
The LAN Setup web page allows you to configure your LAN interface with an IP configuration. Here you either accept the default LAN IP Address or give it a different IP Address. Additionally you can allow your MultiCom Firewall to manage your internal network with DHCP or disable this DHCP administration. Be sure that the range of addresses for the DHCP server is within the subnet you have identified for the LAN address.



IP Address:	where you set the IP address for the LAN port
Subnet Mask:	where you set the netmask for the WAN port
Server:	enable LAN interface be a DHCP server
From address:	this is the start of a range of IP addresses to be offered DHCP clients on your network
To address:	this is the end of a range of IP addresses to be offered DHCP clients on your network
Previous:	go back to the previous page
Reset Values:	reset the default values
Next:	continue to the next configuration screen

DMZ Setup Web

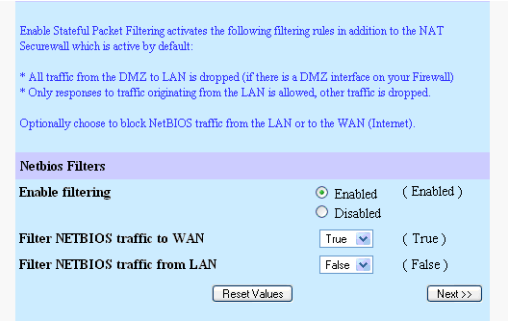
This page is for devices which have a DMZ interface. If there is no DMZ interface then this panel will not be available. Here you either accept the default DMZ IP Address, give it a different IP Address or disable it by simply entering 0.0.0.0 in both the Address and Netmask fields. If this interface is available it is the recommended to place external servers on this network to better protect your LAN network. Optionally enable the DHCP server for the DMZ network as well. Be sure that the range of addresses for the DHCP server is within the subnet you have identified for the DMZ address.



IP Address:	where you set the IP address for the WAN port
Subnet Mask:	where you set the netmask for the WAN port
Server:	enable DMZ interface be a DHCP server
From address:	this is the start of a range of IP addresses to be offered DHCP clients on your network
To address:	this is the end of a range of IP addresses to be offered DHCP clients on your network
Previous:	go back to the previous page
Reset Values:	reset the default values
Next:	continue to the next configuration screen

Firewall Filter Configuration

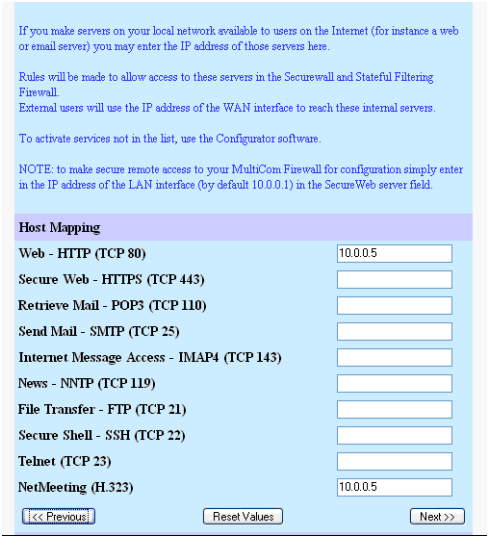
By default, all web-based configurations have the SecureWall (NAT-based Firewall which blocks all unrequested packets on the WAN) activated by default. Here you additionally activate the filtering Firewall. This Firewall blocks the outgoing NetBIOS traffic and/ or continues with more detailed Filtering and NAT customizations (by clicking the Next button.)



Enable Filtering:	enable Filtering rules for the current configuration
Filter NetBIOS traffic to WAN:	discards NetBIOS traffic to the WAN interface
Filter NetBIOS traffic from LAN:	discards NetBIOS traffic from the LAN interface
Reset Values:	reset the default values
Next:	continue to the next configuration screen

Firewall Host Configuration

This page configures standard accesses from the Internet/WAN to specific internal servers. By selecting from the listed services and identifying the IP Address to allow access towards, a user can allow access through the NAT-based Securewall and Filtering Firewall from the WAN interface.



Services:	enable packet traffic for the listed services
Server address:	select the IP Address of the server corresponding to the type of service checked to the left of this box
Previous:	go back to the previous page
Reset Values:	reset the default values
Next:	continue to the next configuration screen

Save Configuration Web

This window is available when saving configurations. The user can make configurations immediately active (saving to the current config,) to the boot config (which will become the active config after the next reboot,) to one of six different inactive memory locations and finally to a file for later use or email attachment.

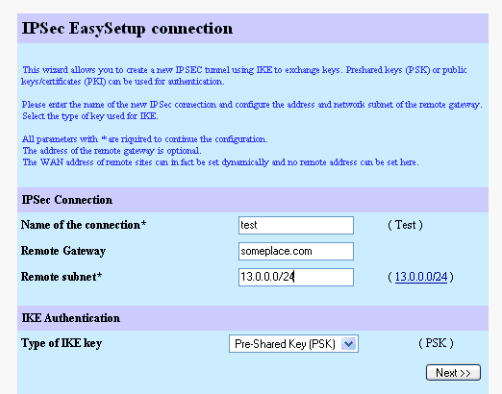
Apply Config:	make changes immediately available but only temporary
Apply Config and Save as Boot Config:	make changes immediately available and permanent
Previous:	go back to the previous page

IPSec

Easy IPSec Setup Page

Quickly configure the network IP and authentication parameters needed to make an IPSec connection. This window is only available when the IPSec option is installed in the MultiCom Firewall and the user has "Privileged" access rights.

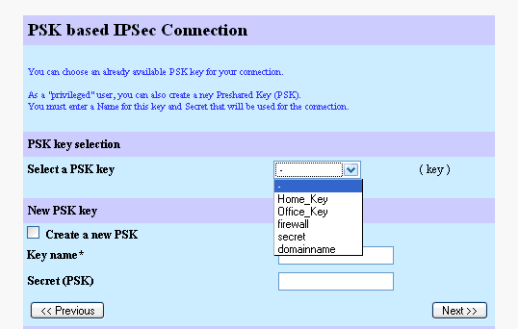
Additional information on configuring IPSec connections can be found in the “IPSec Virtual Private Network” Chapter on page 233.



Name of the connection:	give a unique name to the new IPSec connection
Remote Gateway:	enter the Domain Name or IP address of the remote gateway
Remote Subnet:	enter the remote network IP and subnet. This is the network that will be accessed using this IPSec connection
Type of IKE Key:	select from Preshared key or a PKI Certificate
Next:	continue to the Authentication configuration for this IPSec connection

PSK Configuration Page

If the previous page has chosen to use a Preshared key to authenticate the IPSec connection this page will offer a choice of pre-existing preshared keys. If the user has the "privileged" user rights they will also be given the option of creating a new Preshared key.



Select a key:	select an existing Preshared Key
Create a new PSK:	check this box to create a new Preshared key
Key name:	give a unique name to the new key, it is recommended to use a name that is not the same as the actual secret
Secret (PSK):	enter the "secret" that will be used to authenticate this IPSec connection. It is recommended to choose a long and random string of characters to be sure that this "secret" cannot be guessed.
Previous:	return to the previous configuration screen
Next:	continue to the next configuration screen

PKI Configuration Page

If the previous page has chosen to use a PKI Key to authenticate the IPSec connection this page will offer a choice of pre-existing PKI keys. If the user has the "privileged" user rights they will also be given the option of creating a new PKI key.

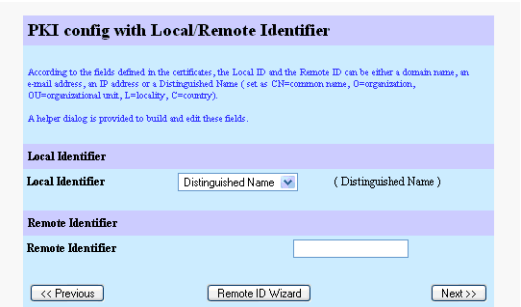
NOTE - this page is only identifying the PKI Contexts. A PKI Key and/or Certificate must be installed using the web interface of the MultiCom Firewall or the Certificate Manager software. The web interface is available at http://10.0.0.1/advanced/security/pki/ where 10.0.0.1 is the IP address of the MultiCom Firewall.

Select a PKI key:	select an existing PKI key
Create a new PKI key:	check this box to create a new PKI key
Key name:	give a unique name to the new key
Authentication type:	choose how to authenticate with this PKI key. You can choose an Identifier for authenticating the Certificate of the remote client or use a Trusted Certificate already loaded on your Firewall.
Previous:	return to the previous configuration screen
Next:	continue to the next configuration screen

PKI Identifier Page

If the PKI Authentication type is Local/Remote Identifier then ID's must be created for the local and remote portion of the IPSec connection. According to the fields defined in the certificates, the Local ID and the Remote ID can be either a domain name, an e-mail address, an IP address or a Distinguished Name (set as CN=common name, O=organization, OU=organizational unit, L=locality, C=country).

The Remote ID Wizard is provided to build and edit these fields.

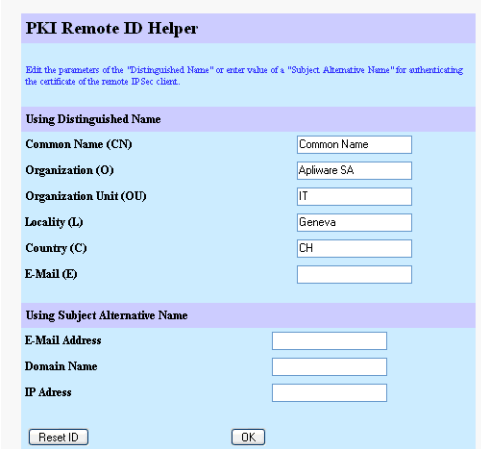


Local Identifier:	choose the local ID based on the installed certificate
Remote Identifier:	enter in the remote ID in the format CN=common name, O=organization, OU=organizational unit, L=locality, C=country, E=email
Remote ID Wizard:	get values of the remote ID from the wizard
Previous:	return to the previous configuration screen
Next:	continue to the next configuration screen

PKI Identifier Helper Page

The Remote ID Wizard will bring up this window, offering the values of the preinstalled PKI Certificate. Either use or edit the values for "Using Distinguished Name" or enter value of a "Subject Alternative Name" for authenticating the certificate of the remote IPSec client.

NOTE - These values must match those of the installed PKI Certificate. Check the Remote PKI Certificate to be sure that the values match.



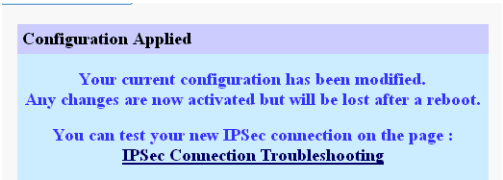
Common Name (CN):	value of the Distinguished name of the PKI Certificate
Organization (O):	value of the Distinguished name of the PKI Certificate
Organization Unit (OU):	value of the Distinguished name of the PKI Certificate
Locality (L):	value of the Distinguished name of the PKI Certificate
Country (C):	value of the Distinguished name of the PKI Certificate
E-Mail (E):	value of the Distinguished name of the PKI Certificate
E-Mail Address:	value of the Alternative Subject Name of the PKI Certificate

Domain Name:	value of the Alternative Subject Name of the PKI Certificate
IP Address:	value of the Alternative Subject Name of the PKI Certificate
Reset ID:	reload the ID of the preinstalled PKI Certificate
OK:	finish using the Remote ID wizard

IPSec Configuration Applied Page

After making the configuration changes the configuration file of the MultiCom Firewall is updated with the new IPSec connection. If the configuration was APPLIED then it will be available for immediate use. If the configuration was APPLIED and SAVED AS BOOT CONFIG then the changes will be immediately available and will be retained even after a system reboot.

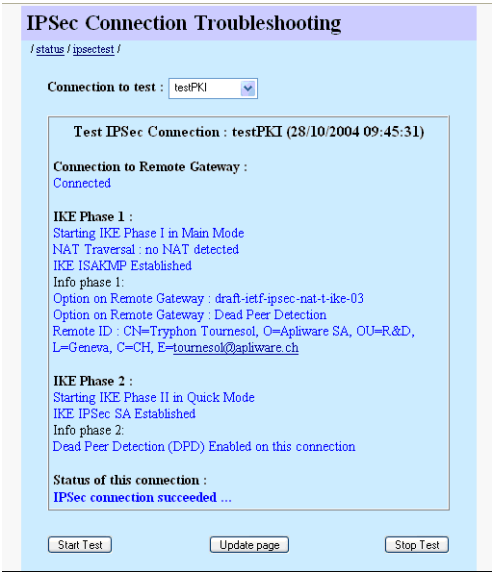
NOTE - it is recommended to make changes temporary until they have been tested. This allows a simple reboot to reset the MultiCom Firewall



IPSec Connection Troubleshooting:	optionally goto the IPSec Connection Testing page to test the new connection.

IPSec Connection Test Page

IPSec connections can be tested from the web interface of the MultiCom Firewall. Any enabled IPSec connection can be tested. The test web page is available at http://10.0.0.1/status/ipsectest/ and the page to enable or disable an IPSec connection is at http://10.0.0.1/advanced/ipsec/. In each case 10.0.0.1 is the IP address of the MultiCom Firewall.



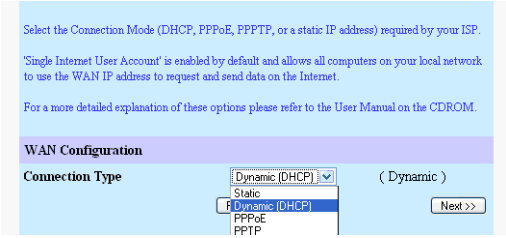
Connection to test:	choose an enabled IPSec connection to test
Start test:	click this button to start an IPSec connection test
Update page:	IPSec connection tests can take some time to finish, click this button to update the current status of the IPSec connection test even if the test is not finished.
Stop test:	stop the current IPSec connection test

Configure Interface/ Firewall

WAN Configuration

The WAN Configuration page allows the user to configure the settings of the MultiCom Firewall's WAN interface without the use of the Configurator software. After setting the WAN choice as instructed by your ISP you can then choose to accept the default settings for your LAN or to customize them as needed.

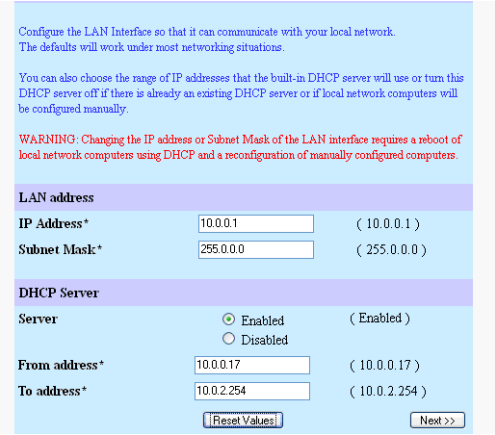
By default the connection type of the WAN interface is DHCP which sets your WAN port to automatically configure itself as a DHCP client (receiving its IP configuration from your ISP). Optionally you can also select PPPoE, PPTP, or a static IP configuration. Be sure to check with your ISP if you have questions about the type of WAN connection they support.



Connection Type:	configure the WAN interface as a static IP interface or, DHCP, PPPoE, PPTP client
Hostname:	optionally give a name to the MultiCom Firewall
Single Internet User Account:	currently not available
Previous:	go back to the previous page
Reset Values:	reset the default values
Next:	continue to the next configuration screen

LAN Configuration

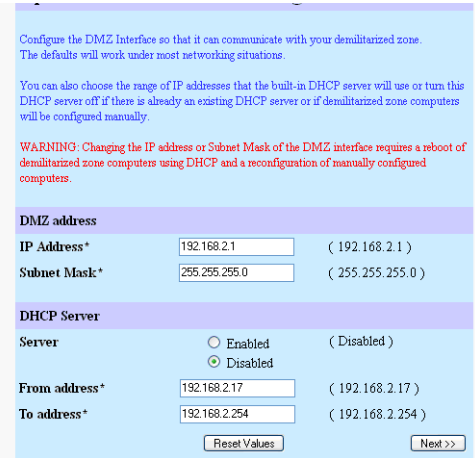
The LAN Configuration web page allows you to configure your LAN interface with an IP configuration. Here you either accept the default LAN IP Address or give it a different IP Address. Additionally you can allow your MultiCom Firewall to manage your internal network with DHCP or disable this DHCP administration. Be sure that the range of addresses for the DHCP server is within the subnet you have identified for the LAN address.



IP Address:	where you set the IP address for the LAN port
Subnet Mask:	where you set the netmask for the WAN port
Server:	enable LAN interface be a DHCP server
From address:	this is the start of a range of IP addresses to be offered DHCP clients on your network
To address:	this is the end of a range of IP addresses to be offered DHCP clients on your network
Previous:	go back to the previous page
Reset Values:	reset the default values
Next:	continue to the next configuration screen

DMZ Configuration

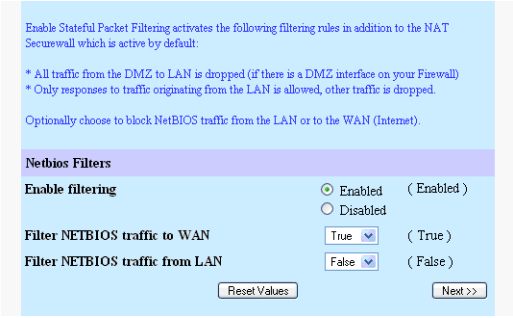
This page is for devices which have a DMZ interface. If there is no DMZ interface then this panel will not be available. Here you either accept the default DMZ IP Address, give it a different IP Address or disable it by simply entering 0.0.0.0 in both the Address and Netmask fields. If this interface is available it is the recommended to place external servers on this network to better protect your LAN network. Optionally enable the DHCP server for the DMZ network as well. Be sure that the range of addresses for the DHCP server is within the subnet you have identified for the DMZ address.



IP Address:	where you set the IP address for the WAN port
Subnet Mask:	where you set the netmask for the WAN port
Server:	enable DMZ interface be a DHCP server
From address:	this is the start of a range of IP addresses to be offered DHCP clients on your network
To address:	this is the end of a range of IP addresses to be offered DHCP clients on your network
Previous:	go back to the previous page
Reset Values:	reset the default values
Next:	continue to the next configuration screen

Firewall Filter Configuration

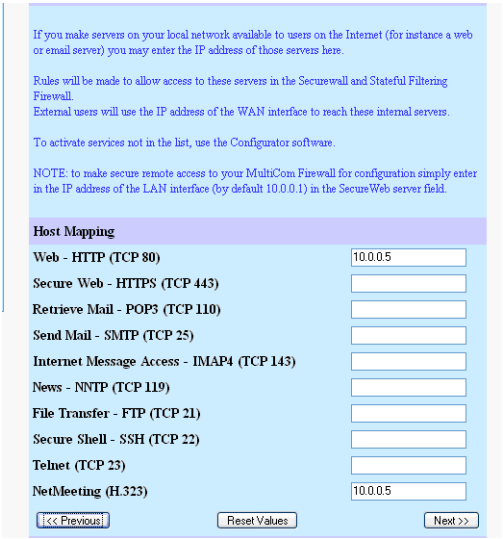
By default, all web-based configurations have the SecureWall (NAT-based Firewall which blocks all unrequested packets on the WAN) activated by default. Here you additionally activate the filtering Firewall. This Firewall blocks the outgoing NetBIOS traffic and/ or continues with more detailed Filtering and NAT customizations (by clicking the Next button.)



Enable Filtering:	enable Filtering rules for the current configuration
Filter NetBIOS traffic to WAN:	discards NetBIOS traffic to the WAN interface
Filter NetBIOS traffic from LAN:	discards NetBIOS traffic from the LAN interface
Previous:	go back to the previous page
Reset Values:	reset the default values
Next:	continue to the next configuration screen

Firewall Host Configuration

This page configures standard accesses from the Internet/WAN to specific internal servers. By selecting from the listed services and identifying the IP Address to allow access towards, a user can allow access through the NAT-based Securewall and Filtering Firewall from the WAN interface.



Services:	enable packet traffic for the listed services
Server address:	select the IP Address of the server corresponding to the type of service checked to the left of this box
Previous:	go back to the previous page
Reset Values:	reset the default values
Next:	continue to the next configuration screen

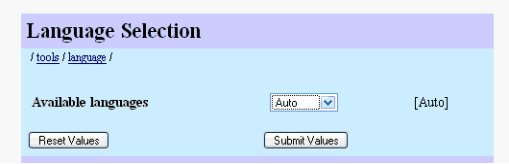
Web Toolbox

The MultiCom Tools menu offers access to many useful utilities directly from your web browser. Please note that some security configurations (notably the built in firewall) will block access to this page, at least from the WAN interface port.

Language Selections:	click here to change the language that the MultiCom Firewall uses for its webserver pages
Configuration Time and Date:	click here to changing the time and date on the firewall
Update the Firmware:	click here to upgrade your firewall's firmware
Reboot your MultiCom Firewall	click here to reboot your MultiCom Firewall
Restore to Factory Defaults:	click here to erase the existing configuration, security configuration and option keys
Load Options Key:	click here to load Option key to activate additional features

Web Language Selection

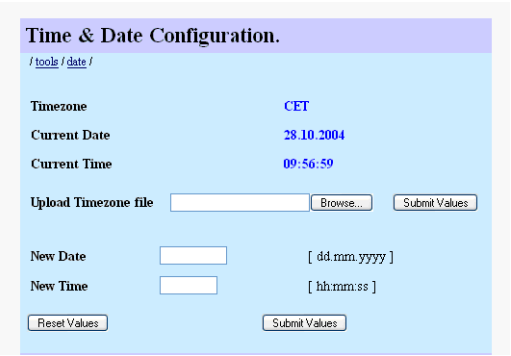
The Web User Configuration Page is where you change the user name and password that has access to configure the firewall.



Available languages:	shows you the current username that is activated
Reset Values:	reset the default values
Submit values:	click here to submit the changes you have made

Time & Date Configuration

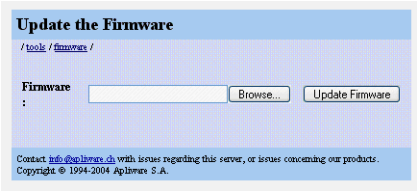
The Time & Date Controls page is where you can change the date and time as it is recorded inside the MultiCom Firewall. This information is also used when configuring DHCP lease times.



Current Date:	shows you the current date being used by the firewall
Current Time:	shows you the current time being used by the firewall
Upload Timezone File:	optionally upload a timezone file identifying the city in which the MultiCom Firewall is being used.
New Date:	enter in the new date in this field [dd.mm.yyyy]
New Time:	enter the new time in this field [hh.mm.ss]
Reset Values:	reset the default values
Submit Values	click here to submit the changes you have made

Firmware Update

The Web Firmware Page is where you enter the name of the new firmware that you wish to load into your firewall. You will need to have already downloaded this firmware and saved it to your hard drive. Check the MultiCom Support website for information on the latest firmware versions available http://www.lightning.ch/support.



Firmware:	enter in the name of the new firmware that you wish to load
Browse...:	click here to browse your hard disk for the new firmware that you wish to load
Update Firmware:	click here to update the new firmware after you have entered in the name of the file to upload

Load Options Key

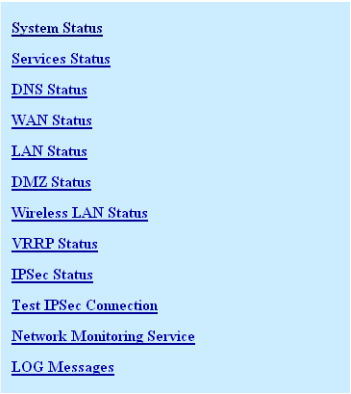
The Load Options Page asks where the options key file is stored. After showing the MultiCom where the file and clicking OK, the new options will be activated in the MultiCom. The new options should be visible in the Status > System window.

Firmware:	enter in the name of the new firmware that you wish to load
Browse...:	click here to browse your hard disk for the new firmware that you wish to load
Update Options Key:	click here to update the new firmware after you have entered in the name of the file to upload, this will erase the previous key.

Status Firewall

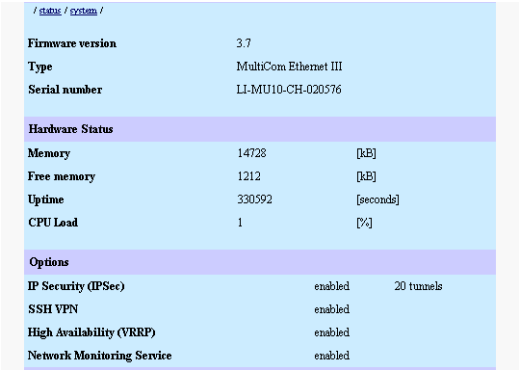
The Status Firewall Page shows a list of status reports available for the MultiCom Firewall. There are status reports for the overall system, the software services running on the Firewall, each physical interface (for the Ethernet III the switched LAN is reported as a single interface), and status log messages generated during the normal usage of the MultiCom Firewall. Each window is described below.

- System Status
- Services Status
- WAN Status
- LAN Status
- DMZ Status (if available on the selected Firewall)
- Wireless LAN Status (if available on the selected Firewall)
- DSL Status (if available on the selected Firewall)
- High Availability (VRRP) Status (if available on the selected Firewall)
- IPSec Status (if available on the selected Firewall)
- IPSec Connection Test (if available on the selected Firewall)
- Network Monitoring Service Status (if available on the selected Firewall)
- Event LOG Messages



System Status

The System Status Page is where you get see the installed Firmware version, hardware type, Serial number, and any options that are installed. Additionally there are statistics concerning the device... uptime, CPU load, and memory. You must refresh the browser window to have these last statistics updated.



/ status / system /

Firmware version	3.7		
Type	MultiCom Ethernet III		
Serial number	LI-MU10-CH-020576		
Hardware Status			
Memory	14728	[kB]	
Free memory	1212	[kB]	
Uptime	330592	[seconds]	
CPU Load	1	[%]	
Options			
IP Security (IPSec)		enabled	20 tunnels
SSH VPN		enabled	
High Availability (VRRP)		enabled	
Network Monitoring Service		enabled	

Previous:	go back to the previous page

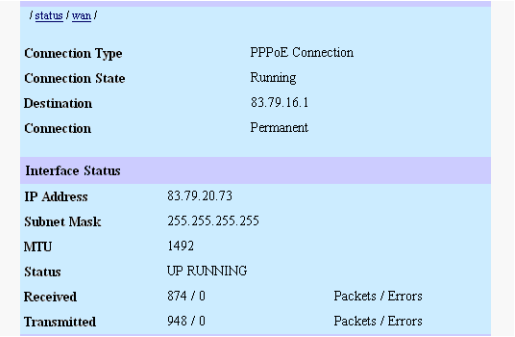
Service Status

The Service Status Page shows which software services are active on the MultiCom Firewall. Configuration of these options is done through the Advanced Configurator software. Note that even though these options may be activated, NAT or Stateful Packet Filtering configurations can possibly be blocking access to these services.

Previous:	go back to the previous page

WAN Status

The WAN Status Page shows the current configured status of the WAN interface. Information available is the connection type (PPPoE, PPTP, DHCP Client or Static IP), status and configuration of the Ethernet parameters of the interface, and the DNS configuration.

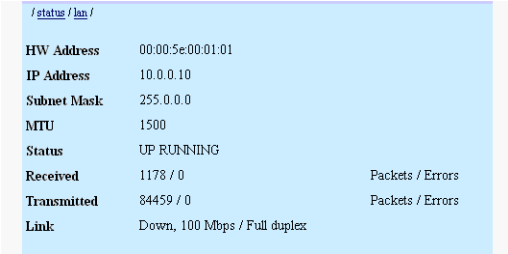


Previous:	go back to the previous page

LAN Status

The LAN Status Page shows the current configured status of the LAN interface. Information available is the MAC Address, status and configuration of the Ethernet parameters of the interface, and the DHCP Server configuration (if enabled,) with a link to active DHCP leases.

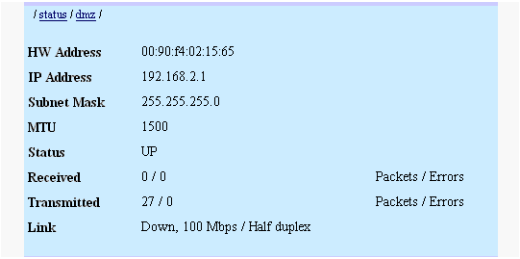
Note: for the Ethernet III or Ethernet Enterprise the switched LAN is reported as a single interface.



Previous:	go back to the previous page

DMZ Status

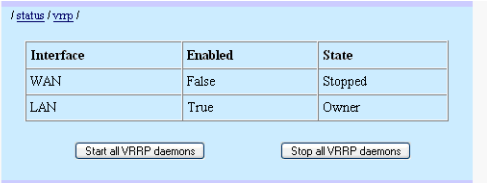
The DMZ Status Page is available on devices with a DMZ interface and shows the current configured status of the interface. Information available is the MAC Address, status and configuration of the Ethernet parameters of the interface, and the DHCP Server configuration (if enabled,) with a link to active DHCP leases.



Previous:	go back to the previous page

High Availability Status

This page shows which interfaces High Availability is enabled for, the status for each interface, and allows the starting and stopping of all High Availability services. The Configurator software must be used to configure the use of High Availability.

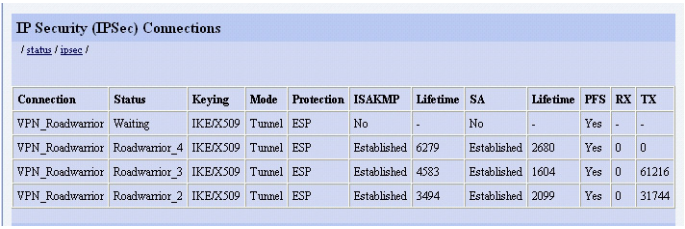


Start all VRRP daemons:	start the High Availability configuration
Stop all VRRP daemons:	stop the High Availability configuration

IPSec Status

When IPSec has been installed and configured, this page shows the status of each IPSec connection. If a Roadwarrior connection has been configured all Roadwarriors using that connection will also be shown.

If PKI Certificates are being used to authenticate the IPSec connections then the Common Name of the certificate is used to identify the tunnel. See the "IPSec Virtual Private Network" Chapter on page 233 for more information on each of the parameters shown in this table.



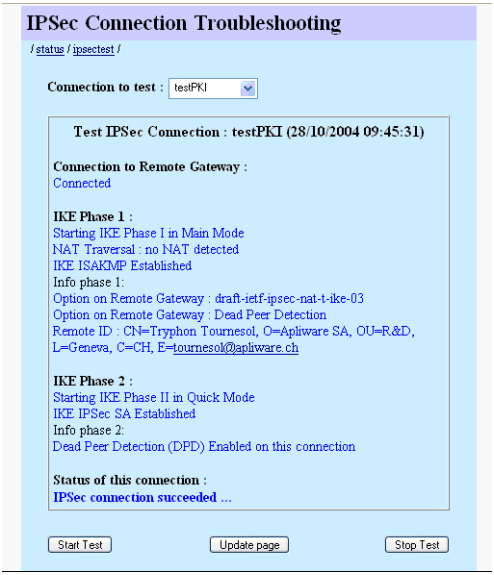
IP Security (IPSec) Connections

/ status / ipsec /

Connection	Status	Keying	Mode	Protection	ISAKMP	Lifetime	SA	Lifetime	PFS	RX	TX
VPN_Roadwarrior	Waiting	IKE/X509	Tunnel	ESP	No	-	No	-	Yes	-	-
VPN_Roadwarrior	Roadwarrior_4	IKE/X509	Tunnel	ESP	Established	6279	Established	2680	Yes	0	0
VPN_Roadwarrior	Roadwarrior_3	IKE/X509	Tunnel	ESP	Established	4583	Established	1604	Yes	0	61216
VPN_Roadwarrior	Roadwarrior_2	IKE/X509	Tunnel	ESP	Established	3494	Established	2099	Yes	0	31744

IPSec Connection Test Page

IPSec connections can be tested from the web interface of the MultiCom Firewall. Any enabled IPSec connection can be tested. The test web page is available at http://10.0.0.1/status/ipsectest/ and the page to enable or disable an IPSec connection is at http://10.0.0.1/advanced/ipsec/. In each case 10.0.0.1 is the IP address of the MultiCom Firewall.



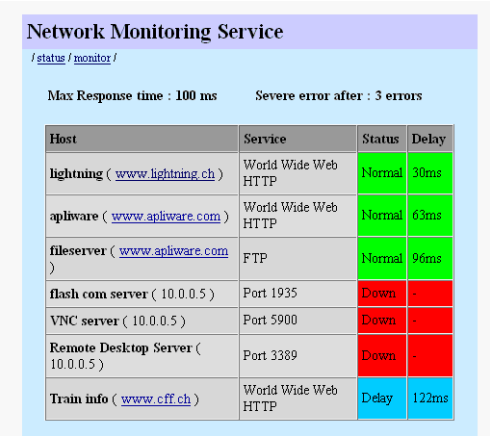
Connection to test:	choose an enabled IPSec connection to test
Start test:	click this button to start an IPSec connection test
Update page:	IPSec connection tests can take some time to finish, click this button to update the current status of the IPSec connection test even if the test is not finished.
Stop test:	stop the current IPSec connection test

Network Monitoring Service

When the Network Monitoring Option is activated this page will show the status and delay of each listed service host. The list of service hosts is configured using the Configurator software or through the web interface of the MultiCom Firewall.

The web page is at http://10.0.0.1/status/monitor/ where 10.0.0.1 is the IP address of the MultiCom Firewall. This information is also available from the Monitor screens of the Configurator software.

The Network Monitoring option must be installed for this monitor panel to become available. For more information about Network Monitoring please see the Section “Network Monitoring” on page 320.



Network Monitoring Service

/ status / monitor /

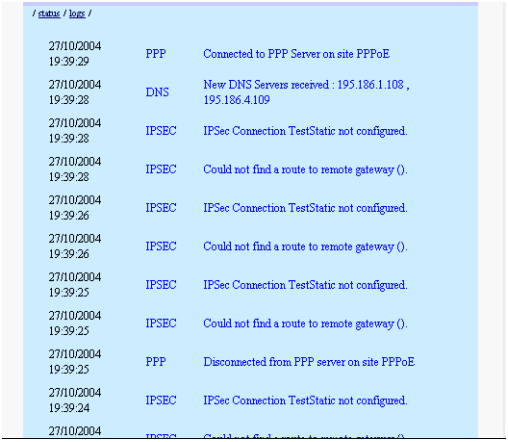
Max Response time : 100 ms Severe error after : 3 errors

Host	Service	Status	Delay
lightning (www.lightning.ch)	World Wide Web HTTP	Normal	30ms
apliware (www.apliware.com)	World Wide Web HTTP	Normal	63ms
fileserver (www.apliware.com)	FTP	Normal	96ms
flash com server (10.0.0.5)	Port 1935	Down	-
VNC server (10.0.0.5)	Port 5900	Down	-
Remote Desktop Server (10.0.0.5)	Port 3389	Down	-
Train info (www.cff.ch)	World Wide Web HTTP	Delay	122ms

Previous:	go back to the previous page

Log Messages

The Log Messages Page is where you see messages generated during the normal usage of the MultiCom Firewall. This includes software services which start or stop, authentication errors, when a new configuration is applied, changes to the DHCP services and more.

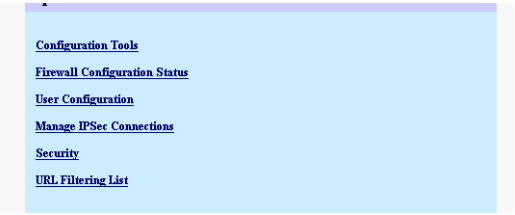


Previous:	go back to the previous page

Web Advanced

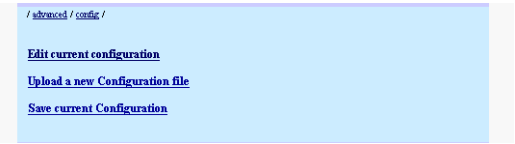
The Web Advanced Page is where you have access to the advanced interactive features of the MultiCom Firewall.

- Configuration Tools (for editing, uploading and saving a configuration file)
- Firewall Configuration Status (detailed statistics on every configurable parameter of the MultiCom Firewall)
- User Configuration (for changing a login or creating, deleting, editing a user account)
- Security (for editing, uploading and saving an IPSec Security configuration file)
- URL Filtering (for editing, uploading and saving URL Filter rules file)



Configuration Tools

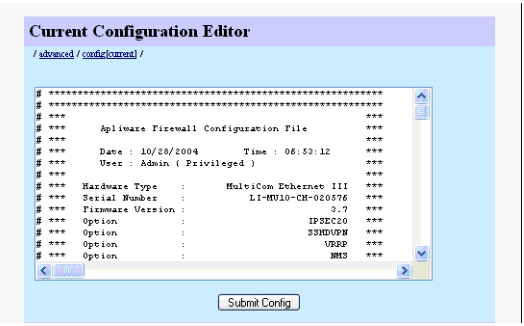
The Configuration Tools page is where you can edit, upload or save the current configuration on the MultiCom Firewall.



Edit current configuration:	clicking here opens a window for editing the current configuration file
Upload a new Configuration file:	clicking here allows you to enter the filename of an existing configuration file on your hard disk
Save current Configuration:	clicking here allows you to download and save the current configuration file to your hard disk

Configuration Edit

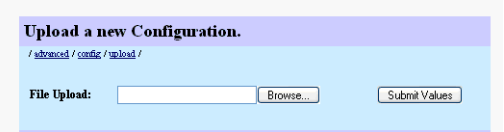
The Configuration Edit page is where you can edit the current configuration and save it as the Boot Configuration.



Submit Config:	clicking here error checks the configuration and then presents the option to write in the Boot Config memory location. To make this configuration active you will need to reboot the MultiCom Firewall.

Configuration Upload

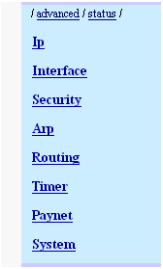
The Configuration Upload page is where you can upload a configuration from your computer's hard disk to the MultiCom Firewall.



Browse:	clicking here to search for existing configuration file on your hard disk
Submit Values:	clicking here sends the selected configuration file to the MultiCom Firewall, error checks the configuration and then presents the option to write in the Boot Config memory location. To make this configuration active you will need to reboot the MultiCom Firewall.

Firewall Configuration Status

The Advanced Firewall Configuration Status Page gives you detailed statistics on every configurable parameter of the MultiCom Firewall. These pages are read only.



IP:	information on most software services in the MultiCom Firewall in addition to filtering and NAT
Interface:	information about Ethernet and PPP interfaces
Security:	information concerning the IPSec configuration and access services like SSH and telnet
Arp:	ARP table entries for MultiCom Firewall showing recently connected local IP addresses and their MAC hardware address
Routing:	shows the RIP routing configuration
System:	shows system configuration and status concerning Lightning-Linux, the MultiCom Firewall and IPSec

User Configuration

The User Configuration Page is where you change the active user logged into the MultiCom Firewall, and also create, edit or delete another user account. It is available to privileged users to edit, add, or remove User Accounts from the authentication list of the MultiCom Firewall. You cannot make blank user names, use the name “root”, or change the “multicom” user account.

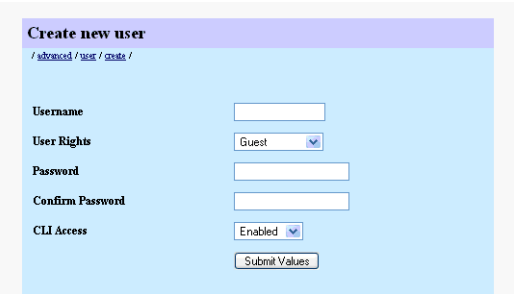
Create new user:	add a new User
Delete user:	remove the selected User
List of users:	show a list of all configured users
Change password:	type in the new password for active user
New login:	login in to the MultiCom Firewall as a different user

Create New User

The Create New User Page is where you add user names and passwords for new users that will have access to configure the firewall.

NOTE - when the first “privileged” user is added the “multicom” account is automatically deleted. This means that the current session of the Configurator will not be able to make any other changes until the user goes to the Change Login window and logs in as the new privileged user.

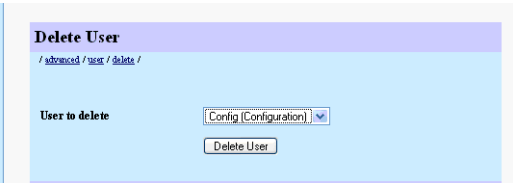
Optionally the Configurator window can be closed and reopened and the user will be asked to authenticate again before being allowed to see or change the configuration files of the MultiCom Firewall.



Username:	the name of the new user of the MultiCom Firewall
User Rights:	these are the assigned rights of a User of the Firewall, options available - Guest, Configuration, Privileged
Password:	the masked password of a User
Confirm Password:	retype the new password to be sure you did not make a mistake
CLI Access:	choose to allow this user CLI access to the MultiCom Firewall or not. Since there can be only one user logged into the CLI interface it is a good idea to disable this access for users who do not need it, for example SSH VPN users.
Submit Values:	send the changes to the firewall which will activate them for all new sessions

User Delete

The User Delete Page is where you delete a selected user name.



User to delete:	select a user to delete
Delete user:	push this button to delete the names user

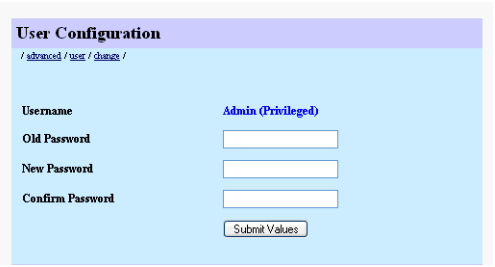
User List

The User List Page is where you can see a list of users that have access to configure the firewall. Additionally it shows the name of the currently logged in user.

Current User:	shows you the current username that is logged into the MultiCom Firewall
User List:	lists all users configured to access the MultiCom Firewall

Change Password

The Change Password Page is where you change the password of the current user.



Username:	shows you the current username that is activated
Old Password:	type in the old password for the current user
New Password:	type in the new password for the current user
Confirm Password:	retype the new password to be sure you did not make a mistake
Submit Values:	send the changes to the firewall which will activate them for all new sessions

New Login Window

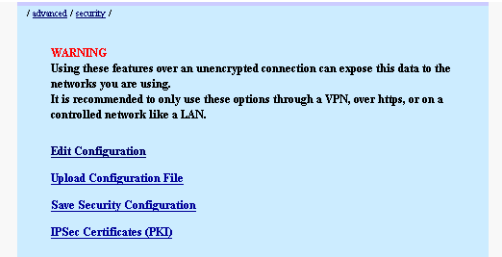
The New Login Window appears the first time you try to login to the web server of the MultiCom Firewall. You can either use the default user ”multicom” with no password or if that has been changed, use any valid username and password. The exact form and options on this window may change depending on the Operating system and Internet browser software that you use to access the MultiCom Firewall from.

Optionally, it is possible to logout of the MultiCom Firewall and login again under a different user account. This is available under the Advanced > User Configuration page of the webserver, http://10.0.0.1/advanced/user/login/.

Username:	type in a valid username
Password:	type in the valid password for the above named user
Remember my password:	if this option is available it allows your Internet browser software to remember the last username and password
OK:	send the username and password to the MultiCom Firewall for authentication, if the username and password is valid then access will be permitted
Cancel:	cancel the attempt to login in to the MultiCom Firewall

Security Configuration

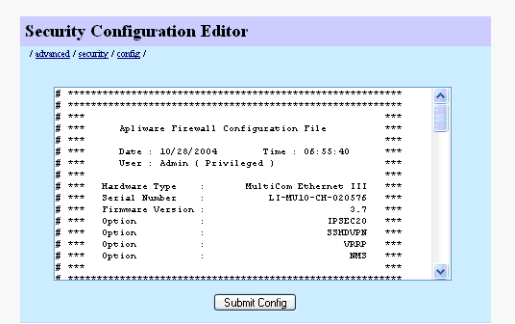
The Security Configuration Page is where you configure the IPSec Security Preshared and Manual keys. The user can directly edit the current keys, upload a new configuration from the hard disk or download a copy of the existing IPSec keys for backup.



Edit Configuration:	edit the existing IPSec key file on the MultiCom Firewall
Upload Configuration File:	load a new Security Configuration file from hard disk
Save Security Configuration:	save the current Security Configuration to hard disk
IPSec Certificates (PKI)	add and remove certificates from the MultiCom Firewall and load the Certificate Revocation list here

Security Edit

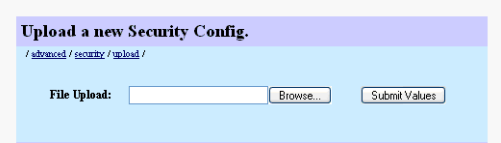
The Security Edit Page is where you directly edit the IPSec Security Preshared and Manual keys on a MultiCom Firewall.



Submit Config:	clicking here error checks the security configuration and then saves it to the MultiCom Firewall.

Security Upload

The Security Upload Page is where you can upload a configuration from your computer's hard disk to the MultiCom Firewall.

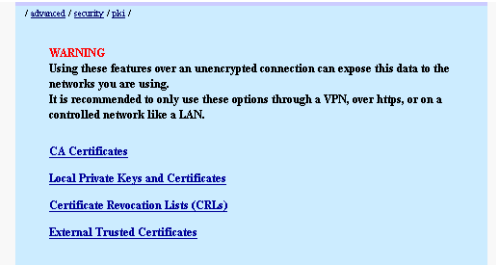


Browse:	clicking here to search for existing configuration file on your hard disk
Submit Values:	clicking here sends the selected configuration file to the MultiCom Firewall, error checks the configuration and then presents the option to write in the Boot Config memory location. To make this configuration active you will need to reboot the MultiCom Firewall.

IPSec PKI Certificates Configuration

Managing PKI Certificates can be done using the web browser interface of the MultiCom Firewall or with the Certificate Manager software. IPSec connections do not require PKI Certificates and can be done simple with a Preshared key. PKI Certificates can be used for added security and for large distributions of authentication information.

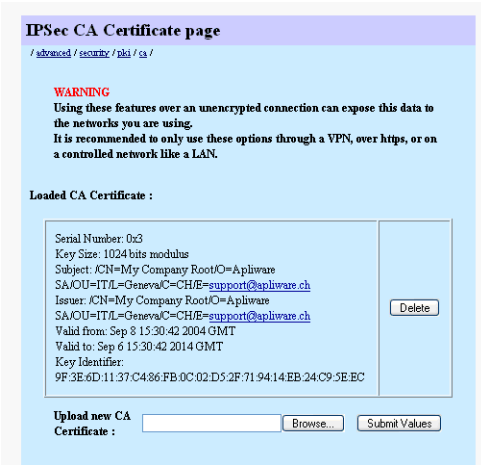
This menu is available at http://10.0.0.1/advanced/security/pki where 10.0.0.1 is the IP address of the MultiCom Firewall.



CA Certificates:	load or delete an existing PKI CA Certificate
Local Private Keys and Certificates:	load or delete a private and public key to identify the MultiCom Firewall
Certificate Revocation Lists (CRLs):	load or delete a Certificate Revocation List to identify invalid PKI Certificates
External Trusted Certificates	load or delete 1 or more External Trusted Certificates to use to authenticate IPSec connections

CA Certificates

This page shows any installed CA Certificate and gives the option to delete it or load a new one.



Delete:	delete the selected CA Certificate
Upload new CA Certificate:	enter the name and path location of a new CA Certificate
Browse:	browse a connected file system to find a new CA Certificate
Submit Values:	clicking this button will start loading the new CA Certificate

Private Keys And Certificates

This page shows any installed Private Keys and Certificate and gives the option to delete them or load a new ones.

Delete:	delete the selected Private Key or Certificate
Change Private Key:	enter the name and path location of a new CA Certificate
Change Public Key:	enter the name and path location of a new CA Certificate
Browse:	browse a connected fleshiest to find a new Private Key or Certificate
Submit Values:	clicking this button will start loading the new Private Key or Certificate

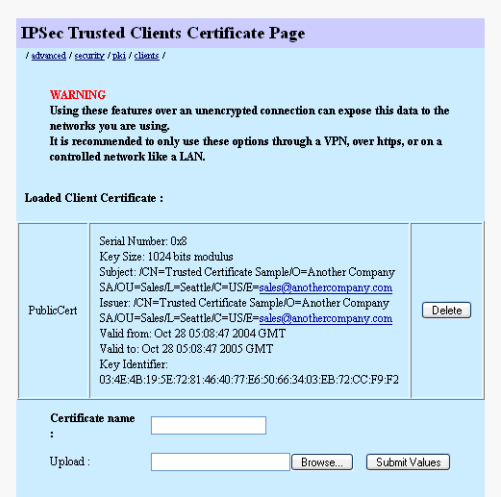
Certificate Revocation List

This page shows any installed Certificate Revocation List (CRL) and gives the option to delete it or load a new one.

Delete:	delete the selected CRL
Upload new CRL:	enter the name and path location of a new CRL
Browse:	browse a connected fleshiest to find a new CA Certificate
Submit Values:	clicking this button will start loading the new CA Certificate

External Trusted Certificates

This page shows any installed External Trusted Certificates and gives the option to delete them or load a new ones.



Delete:	delete the selected Trusted Certificate
Certificate Name:	enter a name for the new Trusted Certificate
Upload:	enter the name and path location of a new Trusted Certificate
Browse:	browse a connected fleshiest to find a new Trusted Certificate
Submit Values:	clicking this button will start loading the new Trusted Certificate

URL Filtering

URL Filtering rules can be entered using the web interface of the MultiCom Firewall or by using the Configurator Software. Using the web interface requires the use of the correct syntax. The correct syntax is automatically generated when using the Configurator software.

Additionally it is possible to enable or disable the URL Filtering feature.

URL Filtering:	enable or disable URL Filtering
Submit config:	submit the changes to the MultiCom Firewall

Appendix E

Configuration Tutorial

This configuration tutorial will setup a sample configuration file and explain how it interacts with the LAN and data packets moving through it. It is important that you already know what services you want to use from your firewall before you start configuring it. The steps to enter the configuration are relatively simple but deciding what is necessary for your specific needs require some advance planning. For assistance in beginning to plan your network needs see the "Forms" Appendix on page 517.

What we will do is set the WAN interface to be a DHCP client that will ask for its IP configuration either from your Internet Service Provider or a remote device. Then we will continue by setting the LAN interface as a DHCP server itself so the rest of the LAN can be automatically configured with all of the information needed. We will here add a static address of a printer so it will be "known" by the LAN interface and not be interfered with.

Next we will configure some filters to watch for activity that we want to be aware of and block off some unused IP addresses. Then a quick addition of a syslog server for reporting purposes and configuring NAT to redirect all incoming web requests to a specific computer.

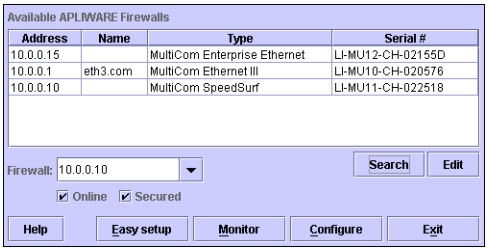
Finally we will save the changes and close the Configurator.

NOTE - This walk through assumes that you already have computers configured to use TCP/IP and that you have started the Configurator software (either from the CD or from an installed directory on your computer.) If this is not the case please refer to the Getting Started chapter first.

Accessing The Firewall

We will assume that you will be connecting through the LAN port as the WAN port is already defaulted to be a DHCP client and does not have an IP address until one is assigned. Remember that the LAN port is defaulted 10.0.0.1 with a subnetmask of 255.0.0.0.

Open the Main window of the Configurator software. To open the Configurator you can either open using the same method as the last step in “Installing The Configuration Software” on page 414.

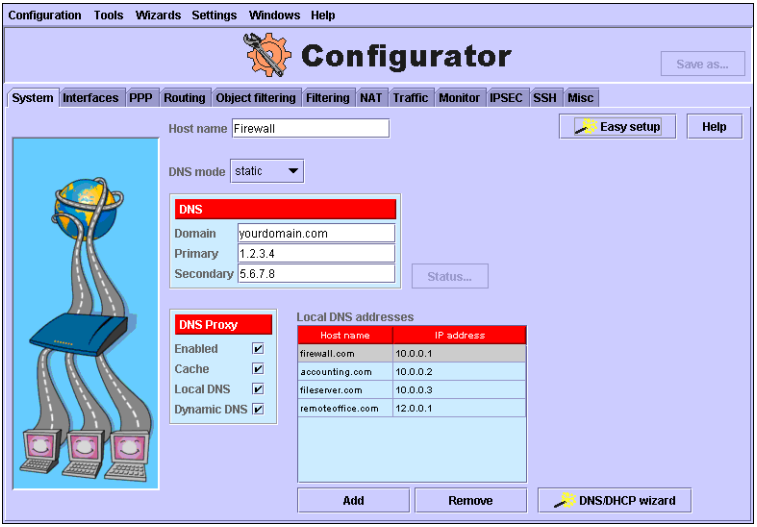


You can also start the Configurator directly from the MultiCom Companion CD. Insert your MultiCom Companion CD and access it via your operating system (Windows, Macintosh or Linux for example.) On a Microsoft Windows computer run configpc to start the Configurator. On a Linux computer run configlinux to start the Configurator. On a Macintosh computer there should be a Configurator Folder on the CD, open that folder and run the Start Configurator icon.

Configuring The Interfaces

This is where we will configure the information of each interface and the DHCP services

1. In the Main window click on `Configure` to open an empty configuration and start you in the System Window



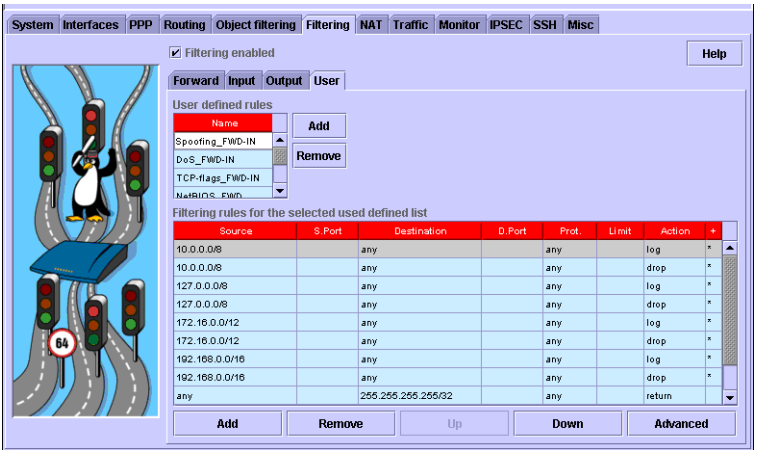
2. Click in the DNS `Mode` box and choose `dynamic`
3. Click on the `Interfaces` tab
4. Select `LAN` under the list of possible interfaces
5. Enter `10.0.0.1` in the `IP Address` field
6. Enter `255.0.0.0` in the `Netmask` field
7. Under the `DHCP Mode` field select `server`
8. Click on the `Add` button under `Address Ranges` section
9. Under the `From` field of address ranges enter `10.0.0.10`
10. Under the `To` field of address ranges enter `10.0.0.100`
11. Click on the `Add` button under the `Static Addresses` section
12. Under the `Ethernet` field enter in `00:12:34:56:78:9A`

13. Under the `IP Address` field enter in `10.0.1.20`
14. Now click on the Wizards option in the top menu and select DHCP client requests
15. In the Select Interface window select WAN
16. Click OK

Configuring Filters

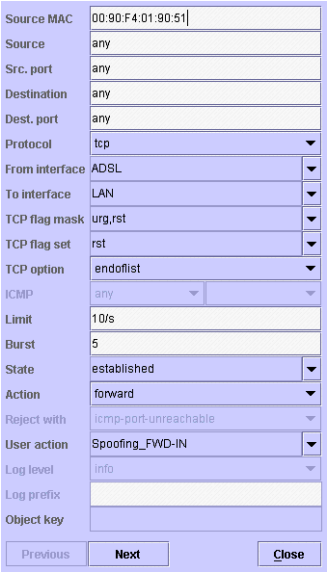
We will configure a logging of ICMP packets that are exceeding a preset limit and also setting an upper limit where we will start dropping those packets. ICMP packets passing through the firewall at the rate of 25 or less per second are automatically accepted. ICMP packets coming at a rate of 100 or less are logged and then accepted. Finally, ICMP packets coming at faster than 100 per second are dropped.

These filter rules will be stored in the filter library and accessed by another entry from the Filtering Forward panel.



1. Click on the `Filtering` tab > `User` tab
2. Click `Filtering Enabled` if it is not already enabled
3. Under `User Filters` click `Add`
4. At the blinking cursor enter `packet_logging` as the name

5. Under the User Filtering table click `Add`
6. Now click `Advanced`

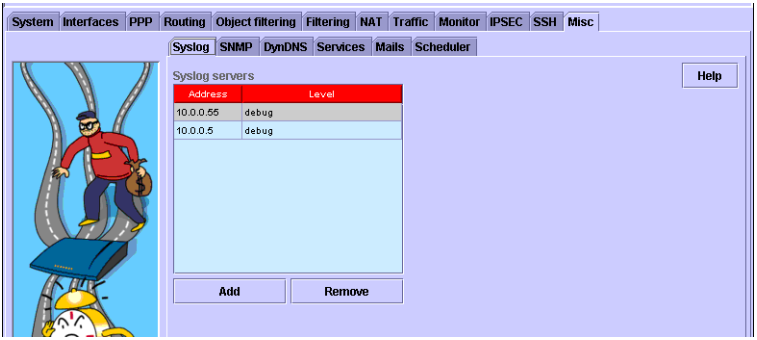


7. In the `Action` box select `log`
8. In the `Log Level` box select `warning`
9. Type `high packet rate`
10. Close the Advanced Filtering window
11. Under the User Filtering table click `Add` again
12. In the `Action` box select `accept`
13. Next click on the `Filtering>Forward` window
14. Click `Add`
15. In the `Protocol` box select `ICMP`
16. In the `Limit` field type 25/s
17. In the `Action` box select `accept`
18. Click `Add`
19. Now click `Advanced`
20. In the `Protocol` box select `ICMP`

21. In the `Limit` field type 100/s
22. In the `Action` box select `forward`
23. In the `User Action` field enter `packet_logging`
24. Close the Advanced Filtering window
25. Click `Add`
26. In the `Protocol` box select `ICMP`
27. Under `Action` click `drop` (unless there is a rule allowing the data through the filtering rules will drop it.)

Setting Syslog Reporting

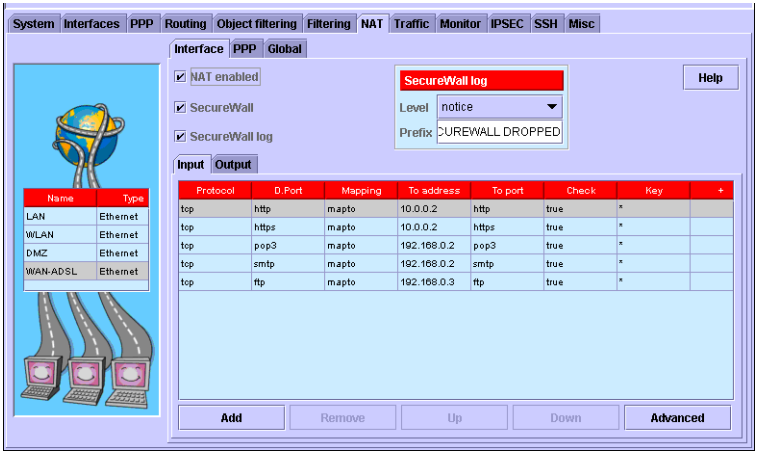
For the syslog messages to be read you will need a syslog server program running on a computer with a static IP address. This configuration will send all warning level Syslog messages and above to the computer at IP address 10.0.0.22.



1. Click on the `Misc` tag to go to the `Syslog` configuration window
2. Click `Add`
3. Enter in `10.0.0.22` in the address field
4. Under the Level field select `warning`

Setting NAT

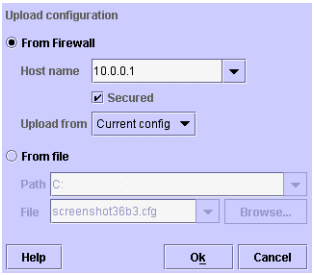
Next we will set all incoming WAN requests for web services at port 80 to be forwarded to an internal computer that is running a webserver but at a special port (a port other than the default of 80).



1. Click on `NAT>Interfaces` to reach the NAT configuration window
2. Select `WAN` under the list of available interfaces
3. Click `NAT` enabled if it is not already enabled
4. Under the `Input` table click `Add`
5. Under `Protocol` select `TCP`
6. Under `DPort` select `80` for the standard http request port
7. Under `Map` be sure that `mapto` is selected
8. Under `To Address` enter the `10.0.0.210`(the static IP of a possible internal web server)
9. Under `To Port` enter `8080` (a slight variation of the standard port 80, the web server needs to be configured to listen on this port)

Saving The New Configuration

Finally we will save the configuration to a file. If you were making these changes while connected directly to the firewall you can click the `Apply` button to immediately activate your changes on your firewall.



1. Click on the `Configuration` menu option and choose `Save As`
2. Be sure that `To File` is selected
3. Enter in a path to save your configuration file to (in the `Path` field) or click browse to help find a folder to save to
4. Enter `finished` into the `File` field (which will become the name of the new configuration file.)
5. Click `OK`

CAUTION — Remember that configurations saved to the Current Config memory location will not be saved after reboot. While this might be fine for testing you may want to have a backup saved to a text file or to one of the other memory locations on the MultiCom Firewall.

TIP — If you are going to be making changes to your configuration file you might consider having your first step to make a backup of the existing configuration to either a file or one of the 6 memory locations in the firewall in case you need to restore it.

That is it. You have successfully created and saved a configuration file for your MultiCom Firewall. If any error messages came up while you were saving the file check them for clues as to where you may have incorrectly typed one of the steps.

Appendix F

Forms

Configuration Checklist

The Configuration checklist is a place for you to keep track of your vital network connection information. If you do not write it here be sure to have this information in your files somewhere in case of emergencies.

In cases where your Internet Service Provider is using DHCP to configure your network connection you do not need to fill in the section for Manual WAN Configuration. This information will be given automatically to your MultiCom Firewall and in fact may change later by your Internet Service Provider.

Planning Worksheets

These are some simple worksheets to help you in planning out your configuration of the MultiCom Firewall. In most cases your configurations will be a series of rules which apply either NAT or Filtering actions to your packets.

If you will be creating many rules consider taking the headers from the following forms and creating a spreadsheet to accommodate your additional rules.

Configuration Checklist

Table 1: Configuration Checklist

	Configuration Questions	Your Choices
Default LAN Configuration	IP Address of the MultiCom Firewall LAN interface	10.0.0.1
	Subnet Mask of your network	255.0.0.0
	Will you use DHCP on your LAN?	Yes
	IP address range for your internal network	10.0.0.17 - 10.0.2.254
	User name to configure the MultiCom Firewall	multicom
	Password to configure the MultiCom Firewall	(there is no password set by default)
Your LAN Configuration	IP Address of the MultiCom Firewall LAN interface	
	Subnet Mask of your network	
	Will you use DHCP on your LAN?	
	IP address range for your internal network	
	User name to configure the MultiCom Firewall	
	Password to configure the MultiCom Firewall	
Manual WAN Configuration	IP address assigned to you by your Internet Service Provider	
	IP netmask used by your Internet Service Provider	
	Default gateway of your Internet Service Provider	
	The domain name of your Internet Service Provider or yours	
	Primary IP address of the DNS of your Internet Service Provider	
	Secondary DNS IP Address of your Internet Service Provider	

Planning NAT Rules

Network Address Translation Rules							
Interface	Direction	Protocol	Source:Port	Destination:Port	Action	To:Port	Change
any WAN LAN PPPoE	any Input Output	any TCP UDP ICMP			Mapto Masquerade Internal		source destination localsource

Planning Filtering Rules

Filtering Rules										
Type	Interface	Proto	Source Port	Destination Port	TCP Flag	TCP Option*	TCP Limit	TCP state	Action	Special
Forward User/ name Input Output	any WAN LAN	any TCP UDP ICMP			any urg ack psh rst fin			any new established related invalid	drop accept reject forward log	Reject w/ type of ICMP Forward to which user filter Log level/ custom
* TCP Options: A-endoflist, B-nooperation, C-maximumsegmentsize, D-windowscalefactor, E-timestamp										

Security Checklist

Table 2: Security Checklist

	Configuration Questions	Your Choice
Basic, Level 1	Have you changed the default username and password to access the firewall?	
	Have you activated the NAT firewall on your WAN interface? (also known as SecureWall)	
	Have you activated the standard filtering protection - DoS, Spoofing, TCP-flags with the Standard Filter Wizard?	
	Did you save your configuration in the boot memory?	
	Did you make a backup of your active configuration file?	
Medium, Level 2	Have you disabled unused interfaces?	
	Have you activated filtering rules to limit the services you want to allow through the firewall?	
	Have you remapped the firewalls web server, telnet, ftp services with NAT for the LAN and/or WAN to different ports?	
	Have you added non-privileged users to be sure other users do not change important information?	
	Have you limited which IP addresses will be translated through the firewall with NAT?	
Maximum, Level 3	Have you limited which IP addresses can administer the firewall with filtering rules?	
	Have you added a logging rule for each of your filtering rules to know when they are activated?	
	If using remote administration, have you blocked access to http and telnet and instead only allow access to https and SSH telnet?	
	Have you blocked or limited pings to the firewall?	
	Have you limited SNMP statistic reading from a specific network or IP address and changed the default community address?	
	Have you enabled syslog reports to a particular IP address for record keeping and loaded a Syslog client?	
	Are you using the latest firmware?	

Appendix A

Internet Protocols

Using Internet Protocols

What is an IP Address

An IP address (or IP number) is a 32 bit number that uniquely identifies a host on the Internet, typically written as four decimal bytes separated by dots. For example: `193.5.2.1`.With each data packet there are two of these numbers attached, one to say where the data came from and one to say where the data is going to.

To the computer, 32 bits means 32 positions that are either turned on or are turned off. To make things simpler these 32 bits are broken into 4 pieces, each one being called octets (having 8 bits per octet) or also bytes. For example, the IP address 192.247.134.2 would look like this in computer binary language 11000000 11110111 10000110 00000010 with each 1 or 0 taking one of the 32 locations for the IP address.

1st octet								2nd octet								3rd octet								4th octet							
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
1	1	0	0	0	0	0	0	1	1	1	1	0	1	1	1	1	0	0	0	0	1	1	0	0	0	0	0	0	0	1	0
$2^7+2^6=128+64=$								$2^7+2^6+2^5+2^4+2^2+2^1+2^0=$								$2^7+2^2+2^1=128+4+2=$								$2^1=$							
								$128+64+32+16+4+1=$																									
192								247								134								2							

This layout is especially important when we start talking about subnetting using CIDR.

IP Network Classes

The first, fixed, part of the address is known as an IP Network, or the network part of the address. The last part (i.e. x) is known as the host address or host part of the address.

The IP standard defines five main classes of IP Networks:

Class A networks: the first byte is fixed (0xxxxxxx) by the registration authority and the company is free to assign the last three bytes (e.g. `32.x.x.x`). Class A networks must be in the range `1.x.x.x` to `126.x.x.x`.

Class B networks: the first two bytes are fixed (10xxxxxx) by the authority and the company may set the last two bytes (e.g. `128.172.x.x`). Class B networks must be in the range `128.0.x.x` to `191.255.x.x`.

Class C networks: the first three bytes are fixed (110xxxxx) by the authority and the company may set the last byte (e.g. `193.172.38.x`). Class C networks must be in the range `192.0.0.x` to `223.255.255.x`.

Class D networks: the first four bytes are fixed (1110xxxx) by the authority and is reserved for IP multicasting. Class D networks must be in the range `224.0.0.x` to `239.255.255.x`.

Class E networks: the first four bytes are fixed (1111xxxx) by the authority and is reserved for experimental purposes. Class E networks must be in the range `240.0.0.x` to `255.255.255.x`.

For example a C class network would have the first 24 bits of an address already used to identify it to the Internet. This would take the form of 110nnnnn nnnnnnnn nnnnnnnn hhhhhhhh where the n's are used to identify the network and the h's are the space left for the owner of the address to use as they want (to identify other publicly known computers to act as web servers for instance.)

Private IP Addresses

There are 3 groups of IP addresses that are not used on the Internet. These private IP address ranges are often used for private networks, such as a home or office network where not every computer has a unique IP address visible from the Internet.

Table 1: Private IP Addres3ses

IP Address Range	IP Range with CIDR notation
10.0.0.0 - 10.255.255.255	10.0.0.0/8
172.16.0.0 - 172.31.255.255	172.16.0.0/12
192.168.0.0 - 192.168.255.255	192.168.0.0/16

More information about these addresses can be found in RFC1918.

IP Subnetting

Once a company has reserved an official IP Network number, it is free to assign the host part of the address as it wishes. The simplest way of doing so is to assign the first host the address 1, the second host the address 2 and so on. However, as the number of hosts grows, it will become necessary to assign the addresses in a more structured manner. This is known as IP subnetting.

IP subnetting consists of sub-dividing the host part of the address into two parts, the subnet part and a (smaller) host part. Instead of the IP address being made up of 2 pieces (network address / host address) the “host” section was further subdivided making the IP address into three components (network address / subnet mask / host address.) The subnet mask tells the computer how many bits to use for the special subnet and how many are left over for the host or computer identification. Now the firewalls can find the needed network using both the official network address and the locally maintained subnet mask.

These IP subnets are typically assigned to individual physical networks (e.g. Ethernet or Token- Rings) but can also be used to simply organize the network in a smoother fashion — creating smaller routing tables and lessening network congestion.

One example might be a business with a single IP address that wants to divide its different departments into different subnets. With subnets they do not all get the same broadcasts and the computers will know when to forward information to a firewall instead of just throwing out the message to anyone on the network who is listening. Both of these results lessens needless network congestion.

Another example is a company that has reserved the IP Network `128.190.x.x`. It might decide to use the third byte (i.e. the first x) as the subnet number and the last byte as the host part of the address. The company has two buildings, each with it's own Ethernet network. The two networks are linked together by an IP

firewall. Hosts in the first building could be assigned addresses of the form `128.190.1.x` and hosts in the second building `128.190.2.x`. This makes the configuration of the IP firewall much simpler.

Making Subnet Masks

There are a two questions you should be asking yourself before beginning to use subnet masks.

1. How many subnets do you want or will want in the near future?
2. How many hosts will be on the largest subnet?

In the above example, the subnet part of the address was the third byte and the host part was the last byte. Put a different way, of the 16 available bits, the upper eight were assigned to the subnet part and the lower eight to the host part. It is possible to choose a different boundary between the two. For example, it is possible to assign the upper 4 bits to the subnet part and the lower 12 bits to the host part. This allows for 16 (2 to the 4th power) different IP subnets, each containing a maximum of 4096 (2 to the 12th power) machines.

If the math starts to get to you there are actually a few subnet calculators available on the Internet and you can check the following table to identify the subnet that you need.

Table 2: Subnet Masks

Number of Subnets	Class C — users/ subnet	Class B — users/ subnet	Class A— users/ subnet	Subnet Mask
2	62	16,382	4,194,301	192
8	30	8,190	2,097,150	224
16	14	4,094	1,048,574	240
32	6	2,046	524,286	248
64	2	1,022	262,142	252
128	0	510	131,070	254
256	0	254	65,534	255

The boundary between the subnet part and the host part of the address is specified by a Subnet Mask. The mask has the bits set to 1 for the network and subnet parts of the address and 0 for the host part. It is up to the system administrator to decide the size of the subnet mask.

In the above example, where the third byte is the subnet part, the subnet mask is `255.255.255.0`. In the case where there are only 4 bits for the subnet part, the mask would be `255.255.240.0`.

Classless Inter-Domain Routing

While subnetting assisted the network administrators in managing their networks more efficiently there was still a problem with more and more networks being connected to the Internet. The class based system of A, B and C was not robust enough to support all of the new growth and yet another method of identifying networks was needed.

This new method of assigning subnet is called CIDR (for Classless Inter-Domain Routing) or supernetting and has a slash appended to the end of an IP address with the number (0–32). This number is the number of bits to be used for the network portion of the address. This allows for a more efficient distribution of IP addresses as well as providing a mechanism for supporting the route aggregation

For example, if you wanted to make separate static routes for groups of IP addresses you could identify them easily with CIDR.

For reference refer to the earlier diagram on IP addresses. If you had an address like 10.0.0.0/8 (pronounced 10.0.0.0 “slash” 8 or even 10 “slash” 8) you would count over 8 bit spaces and know to the left of that would be the portion of the IP address to say which network it was on and to the right of that was the host information. In this instance the notation 10.0.0.0/8 is all IP address from 10.0.0.0 to 10.255.255.255.

This type of notation is very useful for identifying specific groups of IP addresses for NAT, filtering or routing. The table below shows some ways to use CIDR notation to group IP addresses. Notice that

Table 3: Sample IP grouping with CIDR

IP Net Address	CIDR prefix	Hosts	Range	Broadcast
10.0.0.0	/24	254	10.0.0.1 - 10.0.0.254	10.0.0.255
10.0.1.0	/24	254	10.0.1.1 - 10.0.1.254	10.0.1.255
10.0.2.0	/24	254	10.0.2.1 - 10.0.2.254	10.0.2.255
10.0.3.0	/24	254	10.0.3.1 - 10.0.3.254	10.0.3.255
10.0.0.0	/25	126	10.0.0.1 - 10.0.0.126	10.0.0.127
10.0.0.128	/25	126	10.0.0.129 - 10.0.0.254	10.0.0.255
10.0.1.0	/25	126	10.0.1.1 - 10.0.1.126	10.0.1.127
10.0.1.128	/25	126	10.0.1.129 - 10.0.1.254	10.0.1.255
10.0.0.0	/26	62	10.0.0.1 - 10.0.0.62	10.0.0.63
10.0.0.64	/26	62	10.0.0.65 - 10.0.0.126	10.0.0.127
10.0.0.128	/26	62	10.0.0.129 - 10.0.0.190	10.0.0.191
10.0.0.192	/26	62	10.0.0.193 - 10.0.0.254	10.0.0.255

Notice how in the above table that different size of CIDR prefixes breaks the IP subnet into different size groups of addresses. The host range is the number of IP hosts that can be used in the subnet. It corresponds to the table below except that for each network 1 host IP address is removed to identify the network and 1 host IP address is removed to identify the broadcast address for that subnet.

The following table shows you the corresponding CIDR notation for a subnet mask and the number of IP hosts supported on each subnet.

Table 4: CIDR and Subnet mask comparisons

CIDR	Subnet Mask	Number of IP hosts
/1	128.0.0.0	2,048 million
/2	192.0.0.0	1,024 million
/3	224.0.0.0	512 million
/4	240.0.0.0	256 million
/5	248.0.0.0	128 million
/6	252.0.0.0	64 million
/7	254.0.0.0	32 million
/8	255.0.0.0	16 million
/9	255.128.0.0	8 million
/10	255.192.0.0	4 million
/11	255.224.0.0	2 million
/12	255.240.0.0	1,024 thousand
/13	255.248.0.0	512 thousand
/14	255.252.0.0	256 thousand
/15	255.254.0.0	128 thousand
/16	255.255.0.0	64 thousand
/17	255.255.128.0	32 thousand
/18	255.255.192.0	16 thousand
/19	255.255.224.0	8 thousand
/20	255.255.240.0	4 thousand
/21	255.255.248.0	2 thousand
/22	255.255.252.0	1,024
/23	255.255.254.0	512
/24	255.255.255.0	256
/25	255.255.255.128	128
/26	255.255.255.192	64
/27	255.255.255.224	32
/28	255.255.255.240	16
/29	255.255.255.248	8
/30	255.255.255.252	4
/31	255.255.255.254	2
/32	255.255.255.255	1

For more specific information on translating your network addresses into the CIDR format please check RFC1878 for more information.

IP Broadcasts

IP Broadcasts are sent to a group of machines. The number of machines that a broadcast reaches depends on the type of the broadcast. There are three types of broadcast:

Network broadcasts

3. These broadcasts are sent to all hosts in the IP Network. These addresses have all the bits in the subnet and host parts of the address set to 1. The above example network has the network broadcast address `128.190.255.255`.

Subnet broadcasts

4. Subnet broadcasts are sent to all hosts in the same subnet. The host part of the address has all its bits set to 1. In the above example, the subnet in the first building would have the subnet broadcast address of `128.190.1.255`.

Cable broadcasts

5. These broadcasts are received by all hosts on the local physical network. The address is `255.255.255.255`.

Using TCP

TCP/IP stands for Transmission Control Protocol and Internet Protocol. Together these two agreed upon standards allow computers to communicate with one another around the world. While IP defines the standard to move data packets through a network, TCP works at a higher level by setting up a connection between 2 computers for the transfer of data and includes error checking to be sure all of the data received is all of the data that was sent.

To communicate between devices or computers, each device must have an IP address through which it can be reached. These addresses define the individual host computer, the class of the network it is attached to and in the case of broadcast messages, identifies who will get the message. Additionally, there are numerous flags, options, and other numbers for special features that are stored in the TCP/IP header.

Using UDP

UDP stands for User Datagram protocol. Unlike TCP, UDP is a connectionless protocol. It will be used to broadcast and receive such messages but there is not a guarantee that it will reach its destination. This may be seen used to send syslog messages, send SNMP traps and sometimes in media streaming over the Internet.

Like the TCP protocol, it also uses port addresses to identify the destination of the packet.

Using ICMP

ICMP stands for Internet Control Message Protocol. While they are not designed to guarantee arrival at their destination, they will often contain important messages relating to network errors, congestion or timeouts, and echoes (used by the ping command.)

Table 5: Common ICMP messages

echo-reply (used by ping)	a reply from a device saying the device is accessible
destination-unreachable (any TCP/UDP traffic)	a data packet is not able to reach its destination
source-quench	a firewall may not have the buffer space to store the data packet or a host may be receiving data packets too fast
redirect (common routing activity)	when there is a shorter path to a firewall for a data packet this message may be sent from another firewall to the device
echo-request	a request to a device to reply that it is accessible
firewall-advertisement	periodic multicasts from a firewall so that the hosts can know which firewalls are available
firewall-solicitation	a solicitation by device for firewalls on the attached multicast link to advertise that they are there (instead of waiting for the periodic advertisements)
time_exceeded (used by traceroute)	a data packet was not able to be delivered before expiring
parameter-problem	when there is a problem with an entry in the IP header of the data packet

timestamp-request	a request to a device to put a received timestamp on the included data packet and return it
timestamp-reply	a reply from a device with the original data packet and a received timestamp
address-mask-request	a request to a device to return the address mask of the network it is on
address-mask-reply	a reply from a device saying the address mask of the network it is on

Appendix G

SNMP Variables

Below is a list of common SNMP v2 variables, and their description. Please refer to the “Status and Diagnostics” Chapter on page 319. For a more detailed description of these variables please see RFC1907.

NOTE - The text in **bold** in the Variable column is the name of the variable and the text that is not bold in the Variable column is sample output data.

Table 1: SNMP variables

Variable	Description
sysDescr.0: Linux MultiCom 2.4.0 #1 Wed Jan 24 17:04:03 MET 2001 ppc	A textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software. It is mandatory that this only contain printable ASCII characters.
sysObjectID.0: enterprises.2021.250.10	The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining `what kind of box' is being managed. For example, if vendor `Flintstones, Inc.' was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its `Fred firewall'.
sysUpTime.0: 3 d, 1 h, 58 m, 7.27 s	The time (in hundredths of a second) since the network management portion of the system was last re-initialized.
sysContact.0: support@lightning.ch	The textual identification of the contact person for this managed node, together with information on how to contact this person.
sysName.0: Ethernet_II	An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name.
sysLocation.0: Lausanne	The physical location of this node (e.g., `telephone closet, 3rd floor').
sysORLastChange.0: 0 d, 0 h, 0 m, 0.8 s	The value of sysUpTime at the time of the most recent change in state or value of any instance of sysORID.
sysORID.1: mib-2.31	An authoritative identification of a capabilities statement with respect to various MIB modules supported by the local SNMPv2 entity acting in an agent role.
sysORID.2: snmpMIB	
sysORID.3: mib-2.49	
sysORID.4: ip	
sysORID.5: mib-2.50	

Variable	Description
sysORID.6: snmpModules.16.2.2.1	
sysORID.7: snmpModules.10.3.1.1	
sysORID.8: snmpModules.11.3.1.1	
sysORID.9: snmpModules.15.2.1.1	
sysORDescr.1: The MIB module to describe generic objects for network interface sub-layers	A textual description of the capabilities identified by the corresponding instance of sysORID.
sysORDescr.2: The MIB module for SNMPv2 entities	
sysORDescr.3: The MIB module for managing TCP implementations	
sysORDescr.4: The MIB module for managing IP and ICMP implementations	
sysORDescr.5: The MIB module for managing UDP implementations	
sysORDescr.6: View-based Access Control Model for SNMP.	
sysORDescr.7: The SNMP Management Architecture MIB.	
sysORDescr.8: The MIB for Message Processing and Dispatching.	
sysORDescr.9: The management information definitions for the SNMP User-based Security Model.	
sysORUpTime.1: 0 d, 0 h, 0 m, 0.11 s	The value of sysUpTime at the time this conceptual row was last instanciated.

Variable	Description
sysORUpTime.2: 0 d, 0 h, 0 m, 0.11 s	
sysORUpTime.3: 0 d, 0 h, 0 m, 0.12 s	
sysORUpTime.4: 0 d, 0 h, 0 m, 0.12 s	
sysORUpTime.5: 0 d, 0 h, 0 m, 0.12 s	
sysORUpTime.6: 0 d, 0 h, 0 m, 0.12 s	
sysORUpTime.7: 0 d, 0 h, 0 m, 0.12 s	
sysORUpTime.8: 0 d, 0 h, 0 m, 0.12 s	
sysORUpTime.9: 0 d, 0 h, 0 m, 0.12 s	
ifNumber.0: 4	The number of network interfaces (regardless of their current state) present on this system.
ifIndex.1: 1	A unique value for each interface. Its value ranges between 1 and the value of ifNumber. The value for each interface must remain constant at least from one re-initialization of the entity's network management system to the next re- initialization.
ifIndex.2: 2	
ifIndex.3: 3	
ifIndex.4: 4	
ifDescr.1: lo0	A textual string containing information about the interface. This string should include the name of the manufacturer, the product name and the version of the hardware interface.
ifDescr.2: eth0	
ifDescr.3: eth1	
ifDescr.4: ppp0	
ifType.1: softwareLoopback(24)	The type of interface, distinguished according to the physical/link protocol(s) immediately `below' the network layer in the protocol stack.
ifType.2: ethernet-csmacd(6)	
ifType.3: ethernet-csmacd(6)	

Variable	Description
ifType.4: ppp(23)	
ifMtu.1: 3904	The size of the largest datagram which can be sent/received on the interface, specified in octets. For interfaces that are used for transmitting network datagrams, this is the size of the largest network datagram that can be sent on the interface.
ifMtu.2: 1500	
ifMtu.3: 1500	
ifMtu.4: 1492	
ifSpeed.1: 10000000	An estimate of the interface's current bandwidth in bits per second. For interfaces which do not vary in bandwidth or for those where no accurate estimation can be made, this object should contain the nominal bandwidth.
ifSpeed.2: 10000000	
ifSpeed.3: 10000000	
ifSpeed.4: 0	
ifPhysAddress.1:	The interface's address at the protocol layer immediately `below' the network layer in the protocol stack. For interfaces which do not have such an address (e.g., a serial line), this object should contain an octet string of zero length.
ifPhysAddress.2: 00:90:F4:02:00:D3	
ifPhysAddress.3: 00:90:F4:02:00:D2	
ifPhysAddress.4:	
ifAdminStatus.1: up(1)	The desired state of the interface. The testing(3) state indicates that no operational packets can be passed.
ifAdminStatus.2: up(1)	
ifAdminStatus.3: up(1)	
ifAdminStatus.4: up(1)	
ifOperStatus.1: up(1)	The current operational state of the interface. The testing(3) state indicates that no operational packets can be passed.
ifOperStatus.2: up(1)	
ifOperStatus.3: up(1)	
ifOperStatus.4: up(1)	
ifInOctets.1: 2363413	The total number of octets received on the interface, including framing characters.

Variable	Description
ifInOctets.2: 0	
ifInOctets.3: 4407148	
ifInOctets.4: 2955158	
ifInUcastPkts.1: 23835	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
ifInUcastPkts.2: 67647	
ifInUcastPkts.3: 10384	
ifInUcastPkts.4: 6438	
ifInErrors.1: 0	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
ifInErrors.2: 0	
ifInErrors.3: 0	
ifInErrors.4: 0	
ifOutOctets.1: 2363413	The total number of octets transmitted out of the interface, including framing characters.
ifOutOctets.2: 0	
ifOutOctets.3: 2226188	
ifOutOctets.4: 467858	
ifOutUcastPkts.1: 23835	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
ifOutUcastPkts.2: 60012	
ifOutUcastPkts.3: 50856	
ifOutUcastPkts.4: 5329	
ifOutDiscards.1: 0	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
ifOutDiscards.2: 0	
ifOutDiscards.3: 0	
ifOutDiscards.4: 0	
ifOutErrors.1: 0	The number of outbound packets that could not be transmitted because of errors.
ifOutErrors.2: 0	
ifOutErrors.3: 0	

Variable	Description
ifOutErrors.4: 0	
ifOutQLen.1: 0	The length of the output packet queue (in packets).
ifOutQLen.2: 0	
ifOutQLen.3: 0	
ifOutQLen.4: 0	
ifSpecific.1: 0.0	A reference to MIB definitions specific to the particular media being used to realize the interface. For example, if the interface is realized by an ethernet, then the value of this object refers to a document defining objects specific to ethernet. If this information is not present, its value should be set to the OBJECT IDENTIFIER { 0 0 }, which is a syntatically valid object identifier, and any conformant implementation of ASN.1 and BER must be able to generate and recognize this value.
ifSpecific.2: 0.0	
ifSpecific.3: 0.0	
ifSpecific.4: 0.0	
atPhysAddress.1.1.17.0.0.10: 00:10:A4:D0:71:93	The media-dependent `physical' address. Setting this object to a null string (one of zero length) has the effect of invaliding the corresponding entry in the atTable object. That is, it effectively dissasociates the interface identified with said entry from the mapping identified with said entry. It is an implementation-specific matter as to whether the agent removes an invalidated entry from the table. Accordingly, management stations must be prepared to receive tabular information from agents that corresponds to entries not currently in use. Proper interpretation of such entries requires examination of the relevant atPhysAddress object.
atNetAddress.1.1.17.0.0.10: 17.0.0.10	The NetworkAddress (e.g., the IP address) corresponding to the media-dependent `physical' address.
ipForwarding.0: forwarding(1)	The indication of whether this entity is acting as an IP firewall in respect to the forwarding of datagrams received by, but not addressed to, this entity. IP firewalls forward datagrams. IP hosts do not (except those source-routed via the host). Note that for some managed nodes, this object may take on only a subset of the values possible. Accordingly, it is appropriate for an agent to return a `badValue' response if a management station attempts to change this object to an inappropriate value.

Variable	Description
ipDefaultTTL.0: 64	The default value inserted into the Time-To-Live field of the IP header of datagrams originated at this entity, whenever a TTL value is not supplied by the transport layer protocol.
ipInReceives.0: 100794	The total number of input datagrams received from interfaces, including those received in error.
ipInHdrErrors.0: 0	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.
ipInAddrErrors.0: 0	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., 0.0.0.0) and addresses of unsupported Classes (e.g., Class E). For entities which are not IP Firewalls and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
ipForwDatagrams.0: 10252	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Firewalls, this counter will include only those packets which were Source-Routed via this entity, and the Source- Route option processing was successful.
ipInUnknownProtos.0: 0	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
ipInDiscards.0: 0	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
ipInDelivers.0: 57908	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
ipOutRequests.0: 89437	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.

Variable	Description
ipOutDiscards.0: 0	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
ipOutNoRoutes.0: 0	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams which meet this `no-route' criterion. Note that this includes any datagarms which a host cannot route because all of its default firewalls are down.
ipReasmTimeout.0: 0	The maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity.
ipReasmReqds.0: 0	The number of IP fragments received which needed to be reassembled at this entity.
ipReasmOKs.0: 0	The number of IP datagrams successfully re-assembled.
ipReasmFails.0: 0	The number of failures detected by the IP re- assembly algorithm (for whatever reason: timed out, errors, etc). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC815) can lose track of the number of fragments by combining them as they are received.
ipFragOKs.0: 0	The number of IP datagrams that have been successfully fragmented at this entity.
ipFragFails.0: 3	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, e.g., because their Don't Fragment flag was set.
ipFragCreates.0: 0	The number of IP datagram fragments that have been generated as a result of fragmentation at this entity.
ipAdEntAddr.0.0.0.0: 0.0.0.0	The IP address to which this entry's addressing information pertains.
ipAdEntAddr.10.0.0.1: 10.0.0.1	
ipAdEntAddr.127.0.0.1: 127.0.0.1	
ipAdEntAddr.212.147.17.39: 212.147.17.39	

Variable	Description
ipAdEntIfIndex.0.0.0.0: 3	The index value which uniquely identifies the interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex.
ipAdEntIfIndex.10.0.0.1: 2	
ipAdEntIfIndex.127.0.0.1: 1	
ipAdEntIfIndex.212.147.17.39: 4	
ipAdEntNetMask.0.0.0.0 : 0.0.0.0	The subnet mask associated with the IP address of this entry. The value of the mask is an IP address with all the network bits set to 1 and all the hosts bits set to 0.
ipAdEntNetMask.10.0.0.1: 255.0.0.0	
ipAdEntNetMask.127.0.0.1: 255.0.0.0	
ipAdEntNetMask.212.147.17.39: 255.255.255.255	
ipAdEntBcastAddr.0.0.0.0: 0	The value of the least-significant bit in the IP broadcast address used for sending datagrams on the (logical) interface associated with the IP address of this entry. For example, when the Internet standard all-ones broadcast address is used, the value will be 1. This value applies to both the subnet and network broadcasts addresses used by the entity on this (logical) interface.
ipAdEntBcastAddr.10.0.0.1: 1	
ipAdEntBcastAddr.127.0.0.1: 0	
ipAdEntBcastAddr.212.147.17.39: 0	
ipRouteDest.0.0.0.0: 0.0.0.0	The destination IP address of this route. An entry with a value of 0.0.0.0 is considered a default route. Multiple routes to a single destination can appear in the table, but access to such multiple entries is dependent on the table- access mechanisms defined by the network management protocol in use.
ipRouteDest.10.0.0.0: 10.0.0.0	
ipRouteDest.212.147.11.245: 212.147.11.245	

Variable	Description
ipRouteIfIndex.0.0.0.0: 4	The index value which uniquely identifies the local interface through which the next hop of this route should be reached. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex.
ipRouteIfIndex.10.0.0.0: 2	
ipRouteIfIndex.212.147.11.245: 4	
ipRouteMetric1.0.0.0.0: 1	The primary routing metric for this route. The semantics of this metric are determined by the routing-protocol specified in the route's ipRouteProto value. If this metric is not used, its value should be set to -1.
ipRouteMetric1.10.0.0.0: 0	
ipRouteMetric1.212.147.11.245: 0	
ipRouteNextHop.0.0.0.0: 212.147.11.245	The IP address of the next hop of this route. (In the case of a route bound to an interface which is realized via a broadcast media, the value of this field is the agent's IP address on that interface.)
ipRouteNextHop.10.0.0.0: 0.0.0.0	
ipRouteNextHop.212.147.11.245: 0.0.0.0	
ipRouteType.0.0.0.0: indirect(4)	The type of route. Note that the values direct(3) and indirect(4) refer to the notion of direct and indirect routing in the IP architecture. Setting this object to the value invalid(2) has the effect of invalidating the corresponding entry in the ipRouteTable object. That is, it effectively dissasociates the destination identified with said entry from the route identified with said entry. It is an implementation-specific matter as to whether the agent removes an invalidated entry from the table. Accordingly, management stations must be prepared to receive tabular information from agents that corresponds to entries not currently in use. Proper interpretation of such entries requires examination of the relevant ipRouteType object.
ipRouteType.10.0.0.0: direct(3)	

Variable	Description
ipRouteType.212.147.11.245: direct(3)	
ipRouteProto.0.0.0.0: local(2)	The routing mechanism via which this route was learned. Inclusion of values for firewall routing protocols is not intended to imply that hosts should support those protocols.
ipRouteProto.10.0.0.0: local(2)	
ipRouteProto.212.147.11.245: local(2)	
ipRouteMask.0.0.0.0: 0.0.0.0	Indicate the mask to be logical-ANDed with the destination address before being compared to the value in the ipRouteDest field. For those systems that do not support arbitrary subnet masks, an agent constructs the value of the ipRouteMask by determining whether the value of the correspondent ipRouteDest field belong to a class-A, B, or C network, and then using one of: mask network 255.0.0.0 class-A 255.255.0.0 class-B 255.255.255.0 class-C If the value of the ipRouteDest is 0.0.0.0 (a default route), then the mask value is also 0.0.0.0. It should be noted that all IP routing subsystems implicitly use this mechanism.
ipRouteMask.10.0.0.0: 255.0.0.0	
ipRouteMask.212.147.11.245: 255.255.255.255	
ipRouteInfo.0.0.0.0: 0.0	A reference to MIB definitions specific to the particular routing protocol which is responsible for this route, as determined by the value specified in the route's ipRouteProto value. If this information is not present, its value should be set to the OBJECT IDENTIFIER { 0 0 }, which is a syntatically valid object identifier, and any conformant implementation of ASN.1 and BER must be able to generate and recognize this value.
ipRouteInfo.10.0.0.0: 0.0	
ipRouteInfo.212.147.11.245: 0.0	
ipNetToMediaPhysAddress.1.17.0.0.10: 00:10:A4:D0:71:93	The media-dependent `physical' address
ipNetToMediaNetAddress.1.17.0.0.10: 17.0.0.10	The IpAddress corresponding to the media- dependent `physical' address.

Variable	Description
ipNetToMediaType.1.17.0.0.10: dynamic(3)	The type of mapping. Setting this object to the value invalid(2) has the effect of invalidating the corresponding entry in the ipNetToMediaTable. That is, it effectively dissasociates the interface identified with said entry from the mapping identified with said entry. It is an implementation-specific matter as to whether the agent removes an invalidated entry from the table. Accordingly, management stations must be prepared to receive tabular information from agents that corresponds to entries not currently in use. Proper interpretation of such entries requires examination of the relevant ipNetToMediaType object.
icmpInMsgs.0: 24058	The total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmpInErrors.
icmpInErrors.0: 0	The number of ICMP messages which the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).
icmpInDestUnreachs.0: 24054	The number of ICMP Destination Unreachable messages received.
icmpInTimeExcds.0: 0	The number of ICMP Time Exceeded messages received.
icmpInParmProbs.0: 0	The number of ICMP Parameter Problem messages received.
icmpInSrcQuenchs.0: 0	The number of ICMP Source Quench messages received.
icmpInRedirects.0: 0	The number of ICMP Redirect messages received.
icmpInEchos.0: 4	The number of ICMP Echo (request) messages received.
icmpInEchoReps.0: 0	The number of ICMP Echo Reply messages received.
icmpInTimestamps.0: 0	The number of ICMP Timestamp (request) messages received.
icmpInTimestampReps.0: 0	The number of ICMP Timestamp Reply messages received.
icmpInAddrMasks.0: 0	The number of ICMP Address Mask Request messages received.
icmpInAddrMaskReps.0: 0	The number of ICMP Address Mask Reply messages received.
icmpOutMsgs.0: 23897	The total number of ICMP messages which this entity attempted to send. Note that this counter includes all those counted by icmpOutErrors.

Variable	Description
icmpOutErrors.0: 0	The number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.
icmpOutDestUnreachs.0: 23892	The number of ICMP Destination Unreachable messages sent.
icmpOutTimeExcds.0: 1	The number of ICMP Time Exceeded messages sent.
icmpOutParmProbs.0: 0	The number of ICMP Parameter Problem messages sent.
icmpOutSrcQuenchs.0: 0	The number of ICMP Source Quench messages sent.
icmpOutRedirects.0: 0	The number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
icmpOutEchos.0: 0	The number of ICMP Echo (request) messages sent.
icmpOutEchoReps.0: 4	The number of ICMP Echo Reply messages sent.
icmpOutTimestamps.0: 0	The number of ICMP Timestamp (request) messages sent.
icmpOutTimestampReps.0: 0	The number of ICMP Timestamp Reply messages sent.
icmpOutAddrMasks.0: 0	The number of ICMP Address Mask Request messages sent.
icmpOutAddrMaskReps.0: 0	The number of ICMP Address Mask Reply messages sent.
tcpRtoAlgorithm.0: other(1)	The algorithm used to determine the timeout value used for retransmitting unacknowledged octets.
tcpRtoMin.0: 0	The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the LBOUND quantity described in RFC793.

Variable	Description
tcpRtoMax.0: 0	The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the UBOUND quantity described in RFC793.
tcpMaxConn.0: 0	The limit on the total number of TCP connections the entity can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.
tcpActiveOpens.0: 0	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
tcpPassiveOpens.0: 0	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
tcpCurrEstab.0: 0	The number of TCP connections for which the current state is either ESTABLISHED or CLOSE- WAIT.
tcpInSegs.0: 27447	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
tcpOutSegs.0: 27442	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
tcpRetransSegs.0: 0	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
tcpConnState.0.0.0.0.23.0.0.0.0: listen(2)	The state of this TCP connection. The only value which may be set by a management station is deleteTCB(12). Accordingly, it is appropriate for an agent to return a `badValue' response if a management station attempts to set this object to any other value. If a management station sets this object to the value deleteTCB(12), then this has the effect of deleting the TCB (as defined in RFC793) of the corresponding connection on the managed node, resulting in immediate termination of the connection. As an implementation-specific option, a RST segment may be sent from the managed node to the other TCP endpoint (note however that RST segments are not sent reliably).

Variable	Description
tcpConnState.0.0.0.0.53.0.0.0.0.0: listen(2)	
tcpConnState.0.0.0.0.80.0.0.0.0.0: listen(2)	
tcpConnLocalAddress.0.0.0.0.23.0.0.0.0.0: 0.0.0.0	The local IP address for this TCP connection. In the case of a connection in the listen state which is willing to accept connections for any IP interface associated with the node, the value 0.0.0.0 is used.
tcpConnLocalAddress.0.0.0.0.53.0.0.0.0.0: 0.0.0.0	
tcpConnLocalAddress.0.0.0.0.80.0.0.0.0.0: 0.0.0.0	
tcpConnLocalAddress.212.147.17.39.80.193.5.2.183.3121: 212.147.17.39	
tcpConnLocalPort.0.0.0.0.23.0.0.0.0.0: 23	The local port number for this TCP connection.
tcpConnLocalPort.0.0.0.0.53.0.0.0.0.0: 53	
tcpConnLocalPort.0.0.0.0.80.0.0.0.0.0: 80	
tcpConnLocalPort.212.147.17.39.80.193.5.2.183.3121: 80	
tcpConnRemAddress.0.0.0.0.23.0.0.0.0.0: 0.0.0.0	The remote IP address for this TCP connection.
tcpConnRemAddress.0.0.0.0.53.0.0.0.0.0: 0.0.0.0	
tcpConnRemAddress.0.0.0.0.80.0.0.0.0.0: 0.0.0.0	
tcpConnRemAddress.212.147.17.39.80.193.5.2.183.3121: 193.5.2.183	
tcpConnRemPort.0.0.0.0.23.0.0.0.0.0: 0	The remote port number for this TCP connection.
tcpConnRemPort.0.0.0.0.53.0.0.0.0.0: 0	
tcpConnRemPort.0.0.0.0.80.0.0.0.0.0: 0	

Variable	Description
tcpConnRemPort.212.147.17.39.80.193.5.2.183.3121: 3121	
udpInDatagrams.0: 6894	The total number of UDP datagrams delivered to UDP users.
udpNoPorts.0: 51	The total number of received UDP datagrams for which there was no application at the destination port.
udpInErrors.0: 0	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
udpOutDatagrams.0: 38205	The total number of UDP datagrams sent from this entity.
udpLocalAddress.0.0.0.0.7: 0.0.0.0	The local IP address for this UDP listener. In the case of a UDP listener which is willing to accept datagrams for any IP interface associated with the node, the value 0.0.0.0 is used.
udpLocalAddress.0.0.0.0.53: 0.0.0.0	
udpLocalAddress.0.0.0.0.67: 0.0.0.0	
udpLocalAddress.0.0.0.0.161: 0.0.0.0	
udpLocalAddress.0.0.0.0.514: 0.0.0.0	
udpLocalAddress.0.0.0.0.2048: 0.0.0.0	
udpLocalAddress.0.0.0.0.2049: 0.0.0.0	
udpLocalAddress.0.0.0.0.2051: 0.0.0.0	
udpLocalPort.0.0.0.0.7: 7	The local port number for this UDP listener.
udpLocalPort.0.0.0.0.53: 53	
udpLocalPort.0.0.0.0.67: 67	
udpLocalPort.0.0.0.0.161: 161	
udpLocalPort.0.0.0.0.514: 514	
udpLocalPort.0.0.0.0.2048: 2048	

Variable	Description
udpLocalPort.0.0.0.0.2049: 2049	
udpLocalPort.0.0.0.0.2051: 2051	
snmpInPkts.0: 5188	The total number of Messages delivered to the SNMP entity from the transport service.
snmpOutPkts.0: 3919	The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service.
snmpInBadVersions.0: 0	The total number of SNMP Messages which were delivered to the SNMP protocol entity and were for an unsupported SNMP version.
snmpInBadCommunityNames.0: 0	The total number of SNMP Messages delivered to the SNMP protocol entity which used a SNMP community name not known to said entity.
snmpInBadCommunityUses.0: 0	The total number of SNMP Messages delivered to the SNMP protocol entity which represented an SNMP operation which was not allowed by the SNMP community named in the Message.
snmpInASNParseErrs.0: 0	The total number of ASN.1 or BER errors encountered by the SNMP protocol entity when decoding received SNMP Messages.
snmpInTooBigs.0: 0	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is `tooBig'.
snmpInNoSuchNames.0: 0	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is `noSuchName'.
snmpInBadValues.0: 0	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is `badValue'.
snmpInReadOnlys.0: 0	The total number valid SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is `readOnly'. It should be noted that it is a protocol error to generate an SNMP PDU which contains the value `readOnly' in the error-status field, as such this object is provided as a means of detecting incorrect implementations of the SNMP.
snmpInGenErrs.0: 0	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is `genErr'.

Variable	Description
snmpInTotalReqVars.0: 4360	The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.
snmpInTotalSetVars.0: 0	The total number of MIB objects which have been altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs.
snmpInGetRequests.0: 111	The total number of SNMP Get-Request PDUs which have been accepted and processed by the SNMP protocol entity.
snmpInGetNexts.0: 3822	The total number of SNMP Get-Next PDUs which have been accepted and processed by the SNMP protocol entity.
snmpInSetRequests.0: 0	The total number of SNMP Set-Request PDUs which have been accepted and processed by the SNMP protocol entity.
snmpInGetResponses.0: 0	The total number of SNMP Get-Response PDUs which have been accepted and processed by the SNMP protocol entity.
snmpInTraps.0: 0	The total number of SNMP Trap PDUs which have been accepted and processed by the SNMP protocol entity.
snmpOutTooBigs.0: 0	The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field is `tooBig.'
snmpOutNoSuchNames.0: 0	The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status is `noSuchName'.
snmpOutBadValues.0: 0	The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field is `badValue'.
snmpOutGenErrs.0: 0	The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field is `genErr'.
snmpOutGetRequests.0: 0	The total number of SNMP Get-Request PDUs which have been generated by the SNMP protocol entity.
snmpOutGetNexts.0: 0	The total number of SNMP Get-Next PDUs which have been generated by the SNMP protocol entity.
snmpOutSetRequests.0: 0	The total number of SNMP Set-Request PDUs which have been generated by the SNMP protocol entity.
snmpOutGetResponses.0: 3943	The total number of SNMP Get-Response PDUs which have been generated by the SNMP protocol entity.

Variable	Description
snmpOutTraps.0: 0	The total number of SNMP Trap PDUs which have been generated by the SNMP protocol entity.
snmpEnableAuthenTraps.0: enabled(1)	Indicates whether the SNMP agent process is permitted to generate authentication-failure traps. The value of this object overrides any configuration information; as such, it provides a means whereby all authentication-failure traps may be disabled. Note that it is strongly recommended that this object be stored in non-volatile memory so that it remains constant between re-initializations of the network management system.

Appendix H

Recommended Reading and Free Software

While every effort has been made to assure that this manual has described the features of your new MultiCom Firewall you may wish to further your understanding on different networking topics. To assist you we have composed the following list of reading materials and software.

The software was either shareware or freeware when this manual was written but this may have changed by the time you get a chance to consider using them. Additionally Lightning makes no warranty of any kind regarding the use of these products, they are included solely as either possible learning tools or utilities. If you have concerns about the programs requirements please contact the respective manufacturer.

PPP Recommended Reading

Carlson J., “PPP Design and Debugging”, Addison Wesley, December 1997.

Simpson W., "The Point-to-Point Protocol (PPP)", RFC1661, Daydreamer, July 1994.

Perkins, D., "Requirements for an Internet Standard Point-to-Point Protocol", RFC1547, Carnegie Mellon University, December 1993.

Reynolds, J., and Postel, J., "Assigned Numbers", STD 2, RFC1340, USC/Information Sciences Institute, July 1992.

DNS Recommended Reading

Mockapetris P., "Domain Implementation and Specification", RFC1035, ISI, November 1987.

Paul Albitz & Cricket Liu, "DNS and BIND, 2nd Edition", O'Reilly, December 1996.

Cobb S., "PPP Internet Protocol Control Protocol Extensions for Name Server Addresses", RFC1877, Microsoft, December 1995.

Network Security Recommended Reading

Zwicky E., Cooper S., Chapman D., “Building Internet Firewalls”, O’Reilly, June 2000.

Strebe M., Perkins C., “Firewalls 24seven”, Sybex, 2000.

“Maximum Linux Security”, SAMS, September 1999.

Other Recommended Reading

Barrett, D., “SSH, The Secure Shell: The Definitive Guide”, O'Reilly, 2001.

Bates, R., “Broadband Telecommunications Handbook”, Computing McGraw-Hill, 2000.

Maxwell, K., “Residential Broadband: An Insider’s Guide to the Battle for the Last Mile”, John Wiley & Sons, 1999.

Software, Shareware and Freeware

The folllowing software is either included on your MultiCom Companion CD or is mentioned here as a possible solution for your tests and troubleshooting. LIGHTNING Instrumentation assumes no responsibility for the use, maintenance or damage these software products may cause. Please refer to the software's authors for support and any other information you may need.

Please check the author's web sites for the latest information on these software packages.

General Utilities

Adobe Acorbat 5.1 (document reader) at http://www.adobe.com

Apache (web server) at http://www.apache.org

Internet Explorer 6 (web browser) at http://www.microsoft.com/ie

MP Commander 2 (configuration utility) at http://www.lightning.ch

Netscape 7 (web browser) at http://www.netscape.com

Opera 7 (web browser) at http://www.opera.com

Windows

Active SNMP at http://www.cscare.com/activesnmp/

Adaware (spyware removal) at http://www.lavasoftusa.com/

Ethereal (network protocol analyzer) at http://www.ethereal.com/

Expander (file compression) at http://www.aladdinsys.com/

Expect (telnet, ftp automation) at http://expect.nist.gov/

Eyeball Chat (video conferencing) at http://www.eyeball.com/

FileZilla (FTP client and server) at http://filezilla.sourceforge.net/

Hermes email server (free email server) at http://www.alixoft.com/

Kiwi Syslog Daemon at http://www.kiwi-enterprises.com/

Kiwi Syslog CatTools (remote control) at http://www.kiwi-enterprises.com/

NetMeeting (video conferencing) at http://www.microsoft.com/netmeeting/

NetStat Live at http://www.analogx.com/contents/download/network.htm

NetTime (time synchronization client) at http://nettime.sourceforge.net/

NetView Scanner at http://www.rawlogic.com
Nmap for Windows (port scanning) at http://sourceforge.net/projects/nmapwin
Proxomitron (web filter) at http://www.proxomitron.org/
PuTTY (ssh telnet) at http://www.chiark.greenend.org.uk/~sgtatham/putty/
OpenSSH for Windows at http://www.networksimplicity.com/openssh/
Ping-O-Meter at http://www.obesearmadillo.com
RealVNC (visual remote control) at http://www.realvnc.com/
Router IP Console (SNMP and Syslog tracking) at http://www.innerdive.com/
Servers Alive (network monitoring program) at http://www.woodstone.nu/salive/
SmartFTP at http://www.smartftp.com/
What's UP (network management software) at http://www.ipswitch.com
Winzip (file compression) at http://www.winzip.com/
602PRO LAN Suite (email server) at http://www.software602.com/

Macintosh

AGNetTools at http://www.aggroup.com/products/agnettools
AppTN4MP lite beta
BBBdir Lite 4.6 at http://web.barebones.com/free/free.html
Better Telnet 2.0 (FAT)at http://www.cstone.net/~rbraun/mac/telnet/
Expander at http://www.aladdinsys.com/
Fetch FTP at http://fetchsoftworks.com
Interarchie (FTP client) at http://www.stairways.com/
IPNetMonitor at http://www.sustworks.com/site/prod_ipmonitor.html
Mac NetLogger 0.96b8 at http://www.laffeycomputer.com/
MacSSH (ssh telnet) at http://pro.wanadoo.fr/chombier/
MacTelnet 3.0 at http://www.mactelnet.com
NCSA Telnet 2.6 at http://www.ncsa.uiuc.edu/SDG/Software/MacTelnet/Docs
OTTool at http://www.neon.com/
PortSniffer PPC 2.0 at http://www.zdnet.com
PortSniffer 68K at http://www.zdnet.com
SLog 2.5a1 at http://www.macdownload.com
Socket Sifter at http://www.ekimsw.com/socketsifter/

Transmit 1.5 (FAT) at http://www.panic.com/transmit/
TrashScan 1.0.3 at http://www.zdnet.com
VNC (visual remote control) at http://www.uk.research.att.com/vnc/
What Route at http://crash.ihug.co.nz/~bryanc/readme.html

Linux

Cheops at http://www.marko.net/cheops/
Ethereal at http://www.ethereal.com/
Expander at http://www.aladdinsys.com/
Expect at http://expect.nist.gov/
IP Traffic at http://cebu.mozcom.com/riker/iptraf/
Knoppix (Linux on a bootable CD) at http://www.knoppix.net/
Nessus at http://www.nessus.org/
Netstatpl at http://freshmeat.net
Net-tools at http://freshmeat.net
NMAP at http://www.insecure.org/nmap/
RealVNC (visual remote control) at http://www.realvnc.com/
Sniffit at http://reptile.rug.ac.be/~coder/sniffit/sniffit.html
Tcpdump at http://www.tcpdump.org/
Tkined (Scotty) at http://wwwsnmp.cs.utwente.nl/~schoenw/scotty

Web Site Links

CERT Coordination Center http://www.cert.org/index.html
Hacking Exposed http://www.hackingexposed.com/
SANS Institue Online http://www.sans.org/
Protocols.Com http://www.protocols.com/
Hacker Whacker http://hackerwhacker.com/
WebTrends http://www.webtrends.net/
Internet Assigned Numbers Authority http://www.iana.org

Appendix I

LIGHTNING Instrumentation SA

LIGHTNING Instrumentation SA manufacturers a complete line of other Internet Security products.

Other LIGHTNING Solutions

The full range of Lightning products can be found at http://www.lightning.ch. Below is a summary of selected networking and telecommunications products.

Table 1: Other solutions from LIGHTNING

Pocket MultiCom: 1 Ethernet, 1 ISDN BRI	The Pocket MultiCom, the smallest firewall in the world for mobile users, SOHO home offices, and smaller companies can serve any number of computers. It is also the first and only pocket firewall including 128 bit key encryption.
MultiCom Access IV: 1 Ethernet, 4 ISDN BRI	The MultiCom Access IV delivers fully secure network connectivity for remote workgroups and single remote users.
MultiCom Backup IV: 1 Ethernet, 4 ISDN BRI, 2 Leased Lines	The MultiCom Backup IV, the solution for secure high-speed backup and remote access.

MultiCom Classic IV: 1 Ethernet, 2 ISDN BRI, 2 Leased Lines	The MultiCom Classic IV is ideal for linking remote workgroups to a corporation wide network via leased lines with integrated Backup and Overflow over ISDN.
MultiCom Serial IV: 1 Ethernet, 2 Leased Lines	The MultiCom Serial IV delivers fast and secure network connectivity through synchronous leased lines.
MultiCom LAN Access Center: 1 Ethernet, up to 12 ISDN BRI or 2 ISDN PRI, 2 Leased Lines	The MultiCom LAN Access Center meets the requirements of large enterprises and Internet Service Providers, which require extensibility. This modular multi-protocol firewall manages up to 2 PRI and 2 Leased Lines.

Appendix J

Additional Licenses and Copyrights

Third-Party Software. A part of the software used within the MultiCom Ethernet series can be freely distributed under the terms of the GNU Public License and BSD copyright. However, some applications remain the property of their owners, and require their permission to redistribute. For a complete listing of the software used within the MultiCom Firewall, and the terms under which it can be distributed, refer to the LIGHTNING Web site at http://www.lightning.ch/.

GNU General Public License

GNU General Public License

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or dInternet Providerlay an

announcement including an appropriate copyright notice and a
notice that there is no warranty (or else, saying that you provide
a warranty) and that users may redistribute the program under
these conditions, and telling the user how to view a copy of this
License. (Exception: if the Program itself is interactive but
does not normally print such an announcement, your work based on
the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If
identifiable sections of that work are not derived from the Program,
and can be reasonably considered independent and separate works in
themselves, then this License, and its terms, do not apply to those
sections when you distribute them as separate works. But when you
distribute the same sections as part of a whole which is a work based
on the Program, the distribution of the whole must be on the terms of
this License, whose permissions for other licensees extend to the
entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest
your rights to work written entirely by you; rather, the intent is to
exercise the right to control the distribution of derivative or
collective works based on the Program.

In addition, mere aggregation of another work not based on the Program
with the Program (or with a work based on the Program) on a volume of
a storage or distribution medium does not bring the other work under
the scope of this License.

3. You may copy and distribute the Program (or a work based on it,
under Section 2) in object code or executable form under the terms of
Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable
source code, which must be distributed under the terms of Sections
1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three
years, to give any third party, for a charge no more than your
cost of physically performing source distribution, a complete
machine-readable copy of the corresponding source code, to be
distributed under the terms of Sections 1 and 2 above on a medium
customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer
to distribute corresponding source code. (This alternative is
allowed only for noncommercial distribution and only if you
received the program in object code or executable form with such

an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or

otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of

this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

BSD Copyright

BSD Copyright:

This product includes software developed by the University of California, Berkeley and its contributors:
Copyright (c) 1980-1998 Regents of the University of California. All rights reserved.

```
/*
 * Copyright (c) 1980-1998 Regents of the University of California.
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
```

Apache License

Apache License

The MultiCom Ethernet series include software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/).

OpenSSL License

OpenSSL License

```
/* ====================================================================
 * Copyright (c) 1998-2000 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must dInternet Providerlay the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
```

```
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*

*/
```

Original SSLeay License

```
Original SSLeay License
-----------------------

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
```

```
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
*    notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in the
*    documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*    must dInternet Providerlay the following acknowledgement:
*    "This product includes cryptographic software written by
*     Eric Young (eay@cryptsoft.com)"
*    The word 'cryptographic' can be left out if the rouines from the library
*    being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
*    the apps directory (application code) you must include an acknowledgement:
*    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS" AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed.  i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]

*/
```

TCPD License

```
TCPD LICENSE
------------

/*
```

```
* Copyright (c) 1998 Kazunori Fujiwara <fujiwara@rcac.tdi.co.jp>
* All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in the
*    documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*    must dInternet Providerlay the following acknowledgement:
*      This product includes software developed by Kazunori Fujiwara,
*      Polish Linux Distribution Team and its contributors.
* 4. Neither the name of the author nor the names of its contributors
*    may be used to endorse or promote products derived from this software
*    without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED.  IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.

*/
```

Login License

```
LOGIN LICENSE
-------------

/*
 * Copyright 1989 - 1994, Julianne Frances Haugh
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright
```

```
*    notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in the
*    documentation and/or other materials provided with the distribution.
* 3. Neither the name of Julianne F. Haugh nor the names of its contributors
*    may be used to endorse or promote products derived from this software
*    without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY JULIE HAUGH AND CONTRIBUTORS ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED.  IN NO EVENT SHALL JULIE HAUGH OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*/
```

Cryptix General License

Cryptix General License

Copyright (c) 1995, 1996, 1997, 1998, 1999, 2000 The Cryptix Foundation Limited. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE CRYPTIX FOUNDATION LIMITED AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE CRYPTIX FOUNDATION LIMITED OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR

BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

PureTls License

This package is a SSLv3/TLS implementation written by Eric Rescorla <ekr\@rtfm.com> and licensed by Claymore Systems, Inc.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
   This product includes software developed by Claymore Systems, Inc.
4. Neither the name of Claymore Systems, Inc. nor the name of Eric Rescorla may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Glossary

This is the glossary of terms relating to the usage of your MultiCom Firewall. Other terms relating to Internet Security can be found in RFC2828.

100Base-T

A networking standard (IEEE 802.3u) that allows for data transfer rates of up to 100 megabits per second between 2 or more devices. It is also referred to as Fast Ethernet. This standard frequently uses the same cable connectors (RJ45) as does its slower counterpart 10Base-T.

10Base-T

A networking standard that allows for data transfer rates of up to 10 megabits per second between 2 or more devices. It is also referred to as twisted pair ethernet because it uses twisted pairs of cable. The standard cable for the 10Base-T standard uses an RJ45 connector.

Action

The activity to occur when a specified data packet matches a filtering table entry. When configuring filtering you describe a type of data packet to watch for and then the “action” that is to occur to it when found.

The actions available are

drop	discarding the data packet as if it had never received it
accept	allow the data packet to pass
reject	like drop but sending out an ICMP message to the source that the data arrived but was rejected
forward	redirects a data packet to a local port
log	make a syslog report on the detection of the data packet
return	return to a previous set of rules (only available from the filter user library).

AH

Authentication Header can be part of an IP packet header that can ensure the integrity of the data and the IP header itself. It does not encrypt the data however.

See RFC2402.

ARP

The Address Resolution Protocol is used by TCP/IP to convert an IP address into a DLC or MAC address of a network interface. Whenever network traffic is made the first step is for the computer to make an ARP request to find the correct network interface to send the packet to.

See RFC826.

ARP Proxy

The Proxy of the Address Resolution Protocol is used by a network interface to pretend that it is in fact one or more different interfaces. After responding to an ARP request for the IP address that is being proxied, the remote device will send the IP packet to the ARP Proxy for further processing. This process can allow multiple IP addresses to receive traffic as if they were directly connected to the Internet when in fact they are hidden behind a network firewall.

Authentication

The process of identifying oneself over a network. This is commonly done by entering a user name and secret password to receive access to a network or networked device. A very common form of authentication is when you identify yourself to your Internet Service Provider to have access to the Internet.

Bandwidth

Describes how much data you can reach per second. An analogy could be the width of a pipe and how much water can come through per second. There are many factors that affect this speed so if you are unsure what speed you should be able to reach the Internet you should check with your Internet Service Provider.

Bridge

A device that connects to networks at a low level of connectivity. They will not modify, analyze or route packets that move over them. Many xDSL, Cable or wireless modems will be configured to act as a bridge allowing the Internet Service Provider to directly assign addresses to the customers computers.

Broadcast

When the same message or data packet is sent to a group of machines. This information may have many purposes such as simply announcing that a new device is on the network, saying that a device is still connected to the network, to providing a way for the backup power supply to send a message to everyone that it will be turning itself off due to a power outage.

The number of machines that a broadcast reaches depends on the type of the broadcast — network broadcast (where subnet and host parts of an IP address are set to 255 as in 128.190.255.255), subnet broadcast (where only the host part of the IP address is set to 255 as in 128.190.1.255, or a cable broadcast where all hosts on the local physical network are targeted to receive a message with the IP address of 255.255.255.255.

Burst

An optional filtering identifier that works in tandem with the “limit” parameter. Burst specifies the maximum burst of data packets allowed in the traffic flow before the associated limit parameter takes affect. The value is X where X equals the number of packets to match the associated rule before the limiting takes effect. By default this number is 5.

It is an extra identifier to help account for irregular network traffic (network overloads or faulty equipment) that might otherwise get blocked by the limit command.

Cable

The enclosure that holds your network wiring which has connectors such as RJ45 on both sides. The use of the cable can change depending on the layout of the wires at the end points. For example a straight through cable has the same wires

in the same connector locations at both ends of the cable. A crossed wire cable however has, as its name suggests, a pair of crossed wires ending in a different order at one end than on the other end.

Be sure you are using the right cable for your desired connection.

Cable Modems

These modems connect you to high speed Internet-access using cable TV lines. Since you are connecting to your TV line you will use coaxial cables between the modem and your cable TV interface. The modem should have an ethernet interface on it to communicate with your internal network. Speeds are possible up to 2 Mbps depending on your service provider.

CATV

The high speed Internet-access technology uses cable TV lines to connect the user's home to the Internet.

Client

Part of a client-server architecture. The client is the software which presents information to the user and often allows for interaction with that data as well. This information is retrieved from a server which will actually do the work of preparing the information for the client.

An example of this is an email program where the program on your computer is the client and the computer that you connect to (to retrieve your email) is the server.

Compression

The action of transforming data into files of smaller sizes. While in a small size the data can be transmitted faster over network media and then uncompressed on the other side.

Connection State

A TCP identifier found in the header of a TCP data packet. Below are the 4 IP packet states that filtering rules can be set to watch for.

New - A packet which creates a new connection.

Established - A packet which belongs to an existing connection (i.e. which is a reply to an accepted request, or an outgoing packet on a connection which has seen replies.)

Related - A packet which is related to, but NOT part of, an existing connection, such as an ICMP error or some ftp data connections.

Invalid - A packet which could not be identified for some reason such as running out of memory, ICMP errors which do not correspond to known connections.

Crossed Cable

An RJ45 ethernet cable that allows you to connect to network devices together without needing a hub in between them. For instance you might use this cable if you chose to connect your router directly to your computer or laptop. MultiCom crossed cables are blue or have a blue tape around them.

This cable is useful when you need to do direct testing and configurations of a network device and do not have a hub nearby.

Denial of Service

Also known as DoS, is a type of network attack where the attacker floods a known firewall or server with packets, thereby degrading network performance and possibly crashing the software that is receiving those packets.

Destination

The IP address of the firewall or host to which the data packet should be sent.

DHCP

Dynamic Host Configuration Protocol simplifies network administration by assigning IP addresses and other configurations from a central DHCP server. This information is given out to DHCP Clients that request it, usually for a preset period of time before a new request must be made.

See RFC1531

DHCP Client

A computer or device configured to receive its IP address, subnet mask, broadcast address, firewall address, domain name and DNS servers necessary to operate on the network. The client also receives a lease time after which it must ask the DHCP server if it can still have this information or if there is a new configuration that should be used instead.

DHCP Server

A computer configured with IP addresses to manage as well as other data necessary for a networked device to operate on the network. It responds to requests by DHCP clients who ask for this information. Many networks use this as a convenient way to manage many computers from one place.

DNS

Domain Name Servers are the phone books of the Internet. Just as people have trouble memorizing everyone's phone number they wish to call the same problem exists with the Internet. Having the DNS numbers of your Internet Service Provider allows you to move about the Internet with names like www.lightning.ch instead of 206.201.2.233. This number will take the form of x.x.x.x where x's are numbers between 0 and 255.

See RFC1035.

Domain

A virtual group of computers and devices that share a common administrative purpose. For instance, the domain mynetwork.com will cover everyone's computer in the “mynetwork” company. These computers may be in the same LAN or be located around the world in different offices.

Aside from administratively keeping a group of computers together, using a domain tells your router that there is network that can be reached internally, and that it may not need to connect to the Internet to reach a computer or web address ending in that name.

Download

To copy data (such as a file) from a remote source to a local destination. Usually referred to as the action of the recipient when taking the data. When you copy a file from the Internet to your computer you are downloading the data to your computer.

Duplex

Duplex identifies the possibility that the Ethernet interface can both send and receive data. Full-duplex means the interface can both send and receive at the same time while half-duplex means that the data can only go in one direction at a time.

EPROM

See Flash Memory

ESP

Encapsulated Security Payload is an IP packet that is transporting encrypted data. This is the type of Packet that the MultiCom Firewalls use to transfer IPSec protected data.

See RFC2406

Ethernet

A networking specification that identifies how the data is to travel. This term is sometimes used interchangeably with “LAN” to identify the local network.

Filter

The process of matching IP packet header information of incoming packets to a list of rules and corresponding actions. Either a matching entry is found and the specified action implemented or the packet is rejected because it did not match any of the table entries.

This table is stored on the router and the IP packets are checked by going sequentially down the table entries. When two entries identify the same type of packet (for instance, having two entries for all web data) the first one found in the table will be used.

Filter Forward

The filtering table used to list rules affecting IP packets that pass through the firewall from one network to another.

Filter Input

The filtering table used to list rules affecting IP packets that only arrive at one of the firewall’s interfaces and is not meant to be passed any further. For example accessing the built in webserver or a ping to the firewall itself.

Filter Forward

The filtering table used to list rules affecting IP packets that originate from the firewall. For example responses to pings of the firewall’s interfaces and responses to remote configuration requests by telnet or the webserver.

Filter User

The filtering table used to group lists of rules that are only used when packets are sent to the s.

Firewall

A hardware device or software program used to prevent unauthorized access to your computer or network. These walls are usually used at points where the network is vulnerable to the general public or hacker attempts to gain access. These firewalls examine all data packets that pass through it and search them for characteristics that match pre-defined access rules.

There is a built-in firewall capability in the MultiCom Firewall. When it is enabled all incoming data is denied unless there is a mapping rule in the NAT table for the interface it is active on. For instance, if the Firewall was enabled for the WAN interface, no data would be allowed through it unless it matched a rule in the NAT table for that interface.)

Typically this capability is enabled along with a single rule in the WAN outgoing interface that masquerades all data as if it had originated from the WAN port itself. What this does is limit communication to only be allowed in response to a request from the internal LAN.

Firmware

The basic software and data that is written to the read-only memory (ROM) of your router. This data is written to the Flash memory which is protected from power outages and reboots of the device. If your firewall has damaged firmware it will not know how to manage any activity.

Higher version numbers often contain additional functionality. Please check the Lightning Instrumentation website at http://www.lightning.ch/support for information on the most recent version available.

Flag

A TCP identifier found in the header of a TCP data packet.

Common types include.

URG	Urgent Pointer field significant
ACK	Acknowledgment field significant
PSH	Push Function, indicating that this segment contains data that must be pushed through to the receiving user
RST	Reset the connection
SYN	Synchronize sequence numbers (packets used to request a TCP connection)
FIN	No more data from sender announcement

Flash Memory

This is a type of memory that has similarities to both RAM and ROM. Its similarity to RAM is that it can be modified on-line. It acts like ROM in respect that it retains its contents even if the MultiCom is turned off.

In your MultiCom, it is used to store both the firmware and the configuration. Unlike a ROM memory, it is possible to install a new release of the firmware and store it in the Flash memory of your MultiCom.

Fragment

When a data is too large to fit into one packet it can be divided into multiple packets (also fragments). Typically the header information such as source port, destination port, ICMP type is only stored in the start of the packet (i.e. the first packet).

This is a problem since a rule filtering a source port (for instance port 80) will always fail when a fragment data packet is inspected because the source port was not in the header (except for the first data packet which had all of the required information.)

Freeware

This is software that is given away free by the author. The author still retains the copyright however so you cannot resell or alter the software without first obtaining permission from the author.

FTP

File Transfer Protocol creates a virtual connection over TCP/IP which allows file sharing. For example an FTP client (your computer) asks an FTP server (a remote computer with files you want) for permission to transfer files. You will often need a login ID and password to access the FTP server though many servers have a guest account under the login ID “anonymous” and password of the users email address.

See RFC959.

Firewall

The networking hardware device that links two different networks. Usually this device (such as a router) will be identified with an IP address. To reach the other network your computer must know the IP address of the firewall so it can send the information through it to the remote network.

G.DMT

Discrete Multitone Technology is a DSL line modulation standard. Sometimes referred to as “full rate” ADSL.

G.Lite

Also referred to as “DSL Lite”, “Universal DSL”, or “splitterless ADSL”, is a SDSL Line Modulation Standard. It requires no filters or splitters and supports speeds up to 1.5 Mbps download and 512Kbps upload.

Hacker

While a hacker means an amateur programmer it increasingly is recognized as meaning a person trying to get unauthorized access to your computer or network with the purpose of causing damage, stealing or manipulating information.

Host Name

A name that is used to identify and IP address in a way more user-friendly than a set of numbers alone. While host names are easier to remember they rely upon some method to translate the name into an IP address (such as using DNS.) Because of this it may be easier to use just the IP address when troubleshooting connectivity problems.

Hub

A physical device that contains multiple ethernet ports which allows devices on different network segments (or cables) to communicate. Data packets that reach the hub are copied to all of the other ports it is connected to.

Please note that not all hubs can communicate at the same speed. Some hubs work only at 10Base-T speeds or 100Base-T speeds while some can support mixed speeds together. Be sure the hub matches your needs and existing hardware.

ICMP

Internet Control Message Protocol messages are typically messages relating to network errors, congestion, timeouts of data packets and echoes (used by the ping command) by a device on the network. These messages are sent in the IP header and are often sent by a firewall on the path the data packet was traveling.

See RFC792, and RFC1256 for more information on router advertisement and solicitation.

IKE

Internet Key Exchange (formerly called the ISAKMP/Oakley key exchange) negotiates the parameters needed to build a secured connection with IPSec. This occurs using TCP or UDP port 500. After a successful key exchange encrypted data can travel between the two points.

See RFC2407, RFC2408, RFC2409.

Interface

This is the physical port on the back of your ethernet device. There are many possible interfaces depending on your model of MultiCom Firewall, the LAN (also known as the local area network), the WAN (also known as wide area

network), the DMZ (demilitarized zone). It is through these physical connections that the Internet device is connected to your network and/ or your xDSL, cable or wireless modem.

Internet

The global, decentralized network connecting computers. Many of these computers are connected 24 hours a day to provide services such as web sites, retail stores, databases of information, email services and more. Individuals can access the Internet through an Internet Service Provider (Internet Service Provider).

Internet Service Provider

Internet Service Providers are the companies that manage your Internet connection. Frequently they will have a local phone number for you to call with your modem which will give you access to the whole Internet, email and other services they may offer.

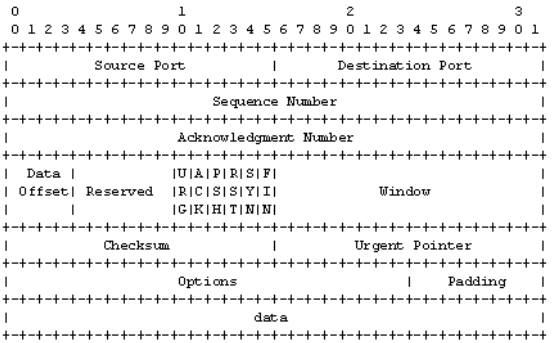
IP Address

A 32–bit number broken up into 4 octets and used to identify a computer on a TCP/IP network. This address takes the form of x.x.x.x where each x is an octet (a number from 0–255). It is these addresses that identifies computers and web sites on the Internet as well.

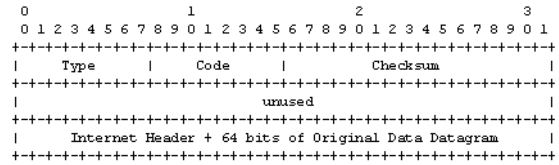
IP Header

The section of a data packet that is reserved for identifying information. Such information could be the source IP address, the destination IP address, and other information describing the type of data that the data packet carries. For examples of different headers please see below.

TCP Header



ICMP Header



IP Protocol

A format that specifies how data is transmitted between two or more devices or software. It is important to have devices using the same protocol such as assuring that your network printer and network computer both use TCP/IP.

Some common protocols are TCP, UDP and ICMP.

See RFC791 and RFC2411

IPSec

IPSec is a suite protocols designed by the Internet Engineering Task Force (IETF) to protect IP communication. Working on the network level, IPSec provides authentication, encryption, and integrity services for data packets and streams. This can be done either between 2 machines (transport mode) or 2 networks (tunnel mode)

IPSec can use three protocols to provide these services: Authentication Header (AH), Encapsulating Security Payload (ESP), Internet Key Exchange (IKE).

See RFC2401.

Kernel

This is the kernel or operating system corresponding to the release of the Linux Operating System. Lightning-Linux is the operating system that runs the MultiCom Firewall. Because it is a customized version of Linux, each version of Lightning Linux will have its corresponding Linux kernel that was integrated into the current version. This is visible in the first screen of the Monitor software.

LAN

Local Area Network is the interconnection of computers and network devices in a relatively small group. This group can be the computers in your home or the computers in your office building as compared to a remote network (WAN) that you may connect to through the phone company or satellite uplinks. LAN are typically differentiated by the media/ cabling connecting the devices, the protocols being run over the media and the layout or topology of the media.

Lease

The amount of time that a DHCP client can keep the configuration information that it was given by a DHCP server. When this time has expired the DHCP client must again ask for configuration information.

Limit

A definition to specify the maximum average number of matches to allow during the defined time frame. This parameter can take the form of X/s, X/m, X/h, or X/d where X is the number of packets and s=seconds, m=minute, h=hour, and d=hour. Traffic less than the limit activates the corresponding action. Traffic flow greater than this rate causes the corresponding filtering action to be skipped for all exceeding data packets UNLESS you specify burst sizes.

This is a filtering option where other types of tags can be used to identify types of data along with a limited throughput and actions such as dropping or rejecting can be specified.

LLC

Logical Link Control is one of 2 different methods for encapsulating data over a DSL connection. Sometimes it is also known as LLC/SNAP (Logical Link Control/ Sub-Network Access Protocol.) The other method is VC-Mux.

Login

A part of authenticating so that the computer or network will know who you are. This is often used with a secret password to identify users correctly.

MAC Address

Media Access Control addresses are unique addresses assigned to each ethernet interface such as found on an ethernet card in a networked computer. It is made up of 12 hexadecimal digits in the form such as 12:34:56:78:9A:BC, 123456789ABC, or 123456–789ABC. The first 6 digits is the identifying code of the manufacturer of the device.

Metric

The number of routers between one IP address and another. This field allows you to keep track of and manage routes according to the distance between any two computers. Note: this is a manually entered field and will not be computed for you.

MIB

Management Information Base is a database in the shape of a tree of objects. Each object is in fact a parameter which has specific settings or grouping of other subheadings. For instance under an object heading of ethernet interface may be information for the IP address of that interface, the netmask, or if DHCP is on or off.

The MIB in your router is where you will be making changes to the way your router works. You can enter your changes with the Configurator software or with line commands via a telnet connection directly to your router.

Modem

The acronym fro modulator-demodulator device that converts digital data from your computer to analog data that can be transmitted over your telephone line. This analog data is in turn converted back into digital data at the other end of the phone line.

MTU

The maximum transmission unit (MTU) is the largest size packet (or frame) that can be sent through a connected network. Ethernet networks can use up to 1500 MTU while interfaces configured to use PPPoE can have a maximum MTU of 1492.

NAT

Network Address Translation is done on a device resting between 2 or more networks (for instance between the WAN and the LAN). IP packets arriving or leaving can have their source or destination changed to a different IP address.

For example, incoming NAT allows you to store a publicly registered IP addresses at the router and link it (or them) to other IP addresses in the LAN. Outgoing NAT changes the source address of packets leaving the device (from the LAN to the Internet) so that the responses to the packets can find there way back. This allows more than one computer to share a single IP address on the Internet.

The added benefit of NAT is that it keeps a list of who asked for what information to the Internet and when data is trying to enter your own network it is compared against the list to be sure that someone has asked for it. If no one has the data is rejected and a report is sent to the Syslog server.

See RFC1631

NetBIOS

Network Basic Input Output System is a set of basic network functions that can be used on a LAN. Most frequently these ports are used by computers running Microsoft Windows software.

The data is used to identify names of shared objects and other computers but due to their frequency this data traffic may inadvertently open dial up connections. In this case it may be useful to disable the spreading of this data past the MultiCom Firewall.

Netmask

Also known as subnet mask, is a 32–bit number that separates the network and host portions of an IP address. The form looks like an appendage to a device's IP address such as 1.2.3.4/24 (meaning a 24–bit sized netmask for device 1.2.3.4) or as an IP address x.x.x.x such as 255.255.255.0 (also a 24–bit sized netmask). It is frequently used to divide a larger network into smaller, virtual networks.

Network

A group of computers connected together to share data. This group can be the computers in your home or the computers in your office building as compared to a remote network (WAN) that you may connect to through the phone company or satellite uplinks.

Networks are typically differentiated by the media/ cabling connecting the devices, the protocols being run over the media and the layout or topology of the media.

Octet

An 8-bit number. This number is often in binary as 00001111 or decimal 15. The range of numbers an octet can be is from 00000000–11111111 in binary or 0 – 255 in decimal form.

Packet

Also known as a datagram or frame is the envelope that data travels within over your network. Each of these envelopes can have different identifying information on them such as the source IP address, the destination IP address, error checking information, sequence numbers and more. Additionally packets can be of different sizes as well. Data that is too large to be fit into one packet of data will be broken down into a series of packets before being sent across the network.

PAT

Port Address Translation allows you to redirect internal or external data traveling via ports to specific locations. For instance you want everyone using Internet newsgroups (port 113) to be redirected to your internal news-server. All external web requests (typically on port 80) could also be directed to your web server inside your company. This redirection can also be to different ports. To redirect IP addresses you would use NAT.

See the technology overview section on PAT for a more detailed explanation on what it can do for you.

Ping

The Packet Internet Groper is a software utility used to verify if a remote device is accessible over a network. After the remote device is identified by either its IP address or its domain name the program or utility will send a small data packet to that device and wait to hear a reply. This reply uses the ICMP Echo function and will also usually include a time stamp identifying how long the packet exchange took.

Port

While people are getting more familiar with the IP addresses used on the Internet few people realize that for each different address there are over 65,000 channels over which the data can travel. Fortunately most communication takes place over preset channels (such as channel 80 for reaching for a web page.)

Some software makes use of random channels so if you want to filter data by the port address it is important that you know which ports are being used by which software on your network.

Port Scan

A network attack where the attacker tries to gain information about software running on servers or workstations. The attacker attempts to make access with every available TCP port on a computer and by analyzing the result the attacker can then focus their attack on the specific software.

PPP

The Point-to-Point Protocol provides a standard method for transporting IP data packets over point-to-point links (such as a link from a home computer to the Internet via an Internet Service Provider). This simple link between two network devices allows data packet transport between the two devices in full-duplex simultaneous bidirectional operation.

See RFC1661.

PPPoE

The Point-to-Point Protocol over Ethernet (PPPoE) encapsulates IP data packets over point-to-point links (such as a link from a home computer to the Internet via an Internet Service Provider). This link is authenticated with a username and password and then PPP communication can take place between two network devices (your router and your Internet Service Provider firewall).

See RFC2516.

PPTP

The Point-to-Point Tunneling protocol uses a version of GRE (Generic Routing Encapsulation) to transport PPP packets. A username, password and IP address of the PPTP server is required to receive IP address parameters. This is frequently used by Microsoft Windows as a way of creating Virtual Private Networks. See the chapter on PPP in the reference manual for more information.

Proxy DNS

A device which pretends to be a DNS server but actually forwards all DNS requests to a remote server is called a Proxy DNS. For instance, clients on a local network will make DNS requests to a Proxy DNS device which in turn forwards those requests to the appropriate external DNS server. Frequently there is a cache that keeps a list of frequently requested names so that the responses from the local network can be replied to quickly.

Reboot

Rebooting is when your router is powered off and then turned back on again. This happens either when your remove the power connection to the device or your local power supply is interrupted (a blackout for example.) After reboot the device will check to be sure all of the hardware is working correctly and then load in the “Boot Config”. Any changes that were made to the “Current Config” will have been erased after the reboot.

RFC

Request For Comments are documents that define standards on the Internet. They are a good resource when you need detailed information on a particular aspect of your network. Fortunately there are many databases of these documents such as at http://www.normos.org, http://www.faqs.org/rfcs/, http://www.cis.ohio-state.edu/hypertext/information/rfc.html, http://www.freesoft.org/CIE/RFC/

RIP

The Routing Information Protocol (RIP) allows groups of firewalls to dynamically update their routing tables according to the state of the firewalls or routers they interact with. By dynamically updating available routes a network can compensate when one router fails by sending data through another route. More information on this protocol is described in the chapter on Routing in the Reference manual.

RJ45

Registered Jack 45 is a commonly used eight-wire connector or cable that connects computers, routers, printers onto a ethernet based LAN.

Router

A device that connects networks and directs the traffic of data packets across them. The router uses the IP address of a data packet to decide where it should go (whether to send it out towards a remote network or to leave the data packet on the local side.) Because the router limits what data can leave the network it reduces unnecessary traffic over networks.

By keeping a table of IP addresses and the remote location that they should be forwarded to, the router is able to distribute data in the most efficient manner. The routing table can either be maintained statically (where the routes are manually entered) or dynamically (when routing devices pass information automatically between themselves.)

Shareware

Software that is freely distributable to friends or colleagues but which the author asks a small fee (also called registering the software) if you decide to regularly use the program. In some cases additional features are available when you register the program. Some shareware have built in time limits after which you must register or the program will not operate.

Shell

Or console is the text based window giving you direct access to your router. This window is accessible when using a telnet client to reach the telnet server built into the router. From this window you can enter commands that change your the configuration of your router or that return data on the status or history of activity within your router.

Source

The IP address of the firewall or host that composes the data packet.

Spoofing

A network attack when the attacker tries to send packets into a network by changing the source IP address to be that of a known network. Often this is done by saying the packet is from the LAN network but it arrives on the WAN and asks for permission to get in. A properly configured firewall will protect against this sort of access.

Spyware

A piece of software or Internet browser plug-in that makes unrequested contacts to the Internet to share information. For example, software that contacts the manufacturers web site each time the program is used, possibly even sending data about the computer it is running on. Although this is not necessarily a network attack it is a program that communicates to other programs without the user being aware of it. Possibly sensitive data could be communicated remotely as well.

Straight Cable

An RJ45 ethernet cable that connects network devices together through a hub. This will not allow you to connect network devices directly to each other, for that situation you would use a crossed wire cable.

Subnet

Dividing an TCP/IP network into smaller, equally sized logical networks. By using what used to be the host part of an IP address a network can seem to be many smaller networks lessening network traffic caused by broadcasts for instance.

See RFC950

Syslog Message

These messages are generated by the MultiCom Firewall for the following reasons: system events, custom filtering rules, DHCP trace activity, PPP trace activity. For more information see the chapter on Syslog messages in the Reference Manual.

Syslog Server

A software that collects and stores system events (syslog) messages. Syslog messages are sent to this server and stored for later reviewing. Some Syslog servers provide additional utilities such as sending pages or emails to administrators.

System Administrator

Or network manager is the individual or group of people responsible for supporting your office or company network. They maintain security, configurations, and upgrades for your computers so the network works for everyone. Sometimes certain functions of If you do not know certain configurations for your network they will probably know the answer. In some firms making changes to your computer or connecting devices to it first requires the permission of the System Administrator.

T1.413

An ANSI industry standard for full-rate DSL Line Modulation.

TCP

The Transmission Control Protocol actually establishes a connection between two hosts as though they were directly connected. By checking for errors and keeping track of which order the data packets should be in TCP provides for reliable data transmissions and interactions. If a data packet is lost or damaged during transit it is TCP that asks for that data packet to be retransmitted.

See RFC793.

TCP Option

A very technical variable in the TCP header. Filtering for these markers should be for advanced users only. RFC1323 describes the last two options in more detail.

Common types include:

end of list	when the end of the options would not otherwise coincide with the end of the TCP header
no operation	may be used between options, for example, to align the beginning of a subsequent option on a word boundary
maximum segment size	communicates the maximum receive segment size at the TCP which sends this segment
window scale factor	an option that allows the TCP packets to identify data windows larger than 65K bytes
timestamp	an option that allows time stamping from a virtual clock to allow accurate measurements of round-trip time between sending a segment and receiving an acknowledgement for it

TCP/IP

Transmission Control Protocol/ Internet Protocol is actually two separate protocols used to transmit data over a network. The Internet Protocol is used to move data packets (also known as datagrams) around the network or Internet but in a one way method.

The Transmission Control Protocol actually establishes a connection between two hosts as though they were directly connected. By checking for errors and keeping track of which order the data packets should be in TCP provides for reliable data transmissions and interactions. If a data packet is lost or damaged during transit it is TCP that asks for that data packet to be retransmitted.

See RFC793.

Telnet

Is a program that runs on your computer and allows you to connect to a telnet server on your network in a text based window. You will often need a login ID and password to access the telnet server but once you are logged in you can use commands as though you were typing them directly into the telnet server (even if the server or device is around the world, though that may make communication a little slower.)

Your router contains a telnet server to allow you remote control access to run commands or get reports. The telnet program is sometimes referred to as a terminal emulator.

See RFC854.

Threshold

Setting a level of throughput or activity is called setting the threshold. This number identifies a frequency or size of data that, when exceeded, cause an action to occur.

Trigger

The activity that causes an action to occur. By setting filtering rules and their corresponding actions you are setting a trigger. When the specified data packet is found by the router the action is triggered.

Trojan horse

A type of network attack that relies on a software program getting inside of the secured network, for example as an email attachment. This program can either open communication to a remote host or allow incoming communication by acting as a server itself, listening on a relatively unknown tcp or udp port.

UDP

User Datagram Protocol is similar to TCP/IP but unlike TCP it does not provide error recovery methods if the message was not received correctly. Because it is essentially a one way method of sending data it is primarily used to broadcast messages over a network.

See RFC768.

Uplink Port

Many hubs will have one uplink port where you can attach a cable to another hub to share interfaces. If this is the only port available on your hub you can indeed use it but you will need to connect a crossed cable to use it.

Upload

To copy data (such as a file) from a local source to a remote destination. Usually referred to as the action of the recipient when putting or sending data to another device or computer. When you copy a configuration file from your computer to your router you are uploading the data to your router.

URL

The Uniform Resource Locator is the global format to access documents and resources on the Internet. A URL uses three parts to reach a specified resource or file. The first part of the address describes the protocol to be used (such as http or ftp), the second part identifies the IP address or domain name of where the desired resource is located (www.mycompany.com). Finally the name of the resource or file is added. A complete url to reach a web page may look like this http://www.mycompany.com/storefront.html.

Users

User accounts on the MultiCom Firewall allows up to 10 different users to be configured with usernames, passwords and administrative privileges. These Users will be allowed access to the MultiCom Firewall for configuration and data access purposes (from http, https, telnet, ssh, and ftp.) These accounts are not related to PPPoE or PPTP accounts.

VC

Virtual Circuit Multiplexing is one of 2 different methods for encapsulating data over a DSL connection. The other method is LLC.

WAN

Wide Area Network is the interconnection of LAN's over phone lines, satellite links or other communication services. The WAN of a global company encompasses all of their LANs but more specifically the devices that connect them such as routers and switches as compared to a LAN which focuses on the network right up to the workstation. The largest WAN is the Internet.

Web Server

A computer or device that serves web pages. The web server is typically reached through a browser by either its IP address (http://10.0.0.1 is the default address of your routers web server) or domain name such as http://www.somecomputer.com. The pages of the web server may be read only or interactive.

xDSL

Digital Subscriber Lines such as ADSL, SDSL, HDSL are collectively referred to as xDSL. It is a high-speed networking technology allowing connection to the Internet from your home or office. Data rates for downloading information will be from 1.5 to 9 Mbps and uploading information from 16 to 640 Kbps depending on your service provider.

xDSL Modem

These modems are required to connect you to high speed Internet-access using Digital Subscriber lines. Since you are connecting through your phone line you will probably use a phone cable between the modem and your telephone wall interface. The modem should have an ethernet interface on it to communicate with your internal network. Data rates for downloading information will be from 1.5 to 9 Mbps and uploading information from 16 to 640 Kbps depending on your service provider.

INDEX

A

B

C

D

E

F

H

I

K

L

M

N

O

P

R

S

T

U

V

W