THE LIGHTNING FLASH

A VISION OF A NETWORKED WORLD ISSUE 4/2001

Secure Gateways

LIGHTNING now integrates high-end functions in its new gateways !

Thanks to its new LIGHTNING-Linux embedded system, Lightning focuses its new product range to Secure Internet Access Gateway Appliances. Lightning is known for its secure routers.

The new LIGHTNING-Linux embedded system allows Lightning to now integrate high-end functions into its products, in addition to the core routing capabilities. These functions make the new Lightning Ethernet III a true Gateway with integrated router, extended firewall and broadband Internet access functions.

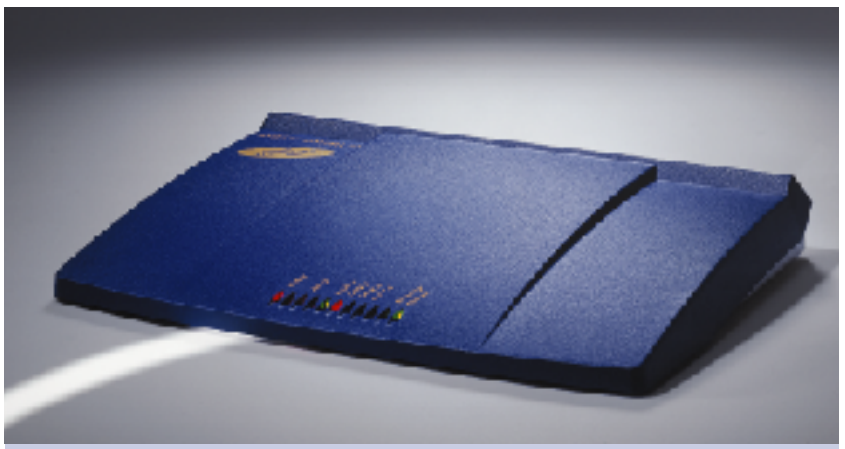
This issue of THE LIGHTNING-FLASH presents the new MultiCom Ethernet III, the main highlights of the secure firewall now integrated in the new MultiCom Ethernet family, and the unique Lightning configuration tools.

Dr. B. Brunner
Managing Director

CONTENTS :

MultiCom Ethernet III
New Firewall and NAT Open
Source contribution
Automatic Configuration
Lightning News

Corporate-class unlimited firewall gateway for SMEs



MultiCom Ethernet III: the new 3-port firewall gateway

LIGHTNING introduces the MultiCom Ethernet III firewall gateway. This new development of LIGHTNING brings the security of large enterprise firewalls, combined with broadband Internet gateway functions, into an easy to install, secure and affordable solution for the small and medium-sized businesses.

With the expansion of the Internet, the protection of the sensitive company data stored on the computers connected to the internal LAN network has become of paramount importance.

The demand for easy to use, secure and affordable firewall solutions has exploded, especially for permanent broadband Internet connections.

LIGHTNING's response to this demand is the MultiCom Ethernet III, which has three distinct Ethernet ports and an integrated 4-port 10/100 Mbit/s Ethernet switching hub, allowing to connect PCs directly in small environments. Gateway functions for ADSL, CATV, WLL and WLAN Internet access modems are also included.

The MultiCom Ethernet family

The MultiCom Ethernet III extends the family of the MultiCom Ethernet II, which has two Ethernet ports. These two devices are the first ones of the MultiCom Ethernet series, a new range of Gateway appliances. These gateways include, in addition to the router and firewall functions, Network Address Translation (NAT), Single Internet User Access, and PPPoE. This features-combination allows accessing the Internet from your entire network with just one IP address.

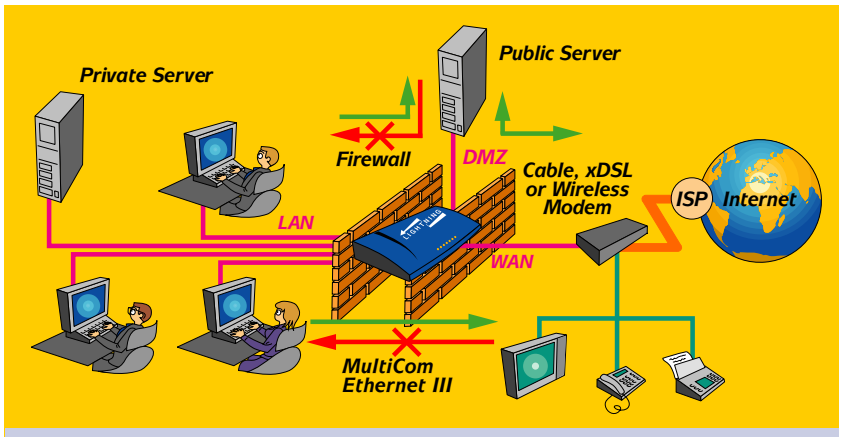
In the near future an IPSec option will allow you to build a Virtual Private Network (VPN) and to transfer data between your locations over the Internet in a secure manner using strong encryption algorithms.

Switching hub included

The LAN port has an integrated switching hub with four interfaces (10/100Mbit/s). This allows connecting directly up to four PCs, meaning a simple installation for small businesses or home offices. The WAN 10Mbit/s Ethernet port offers broadband access via ADSL, cable or wireless modems. A console port has been added to allow local management of configuration facilities. Internally a Real Time Clock (RTC) with a 2 day backup has been built to keep all traces of the different events that have happened even if you have no more power supply.

Firewall with DMZ

The three integrated ports allow companies to divide their network into publicly accessible and protected zones with a single device: Sensitive company data resides securely in the Intranet, inaccessible for outsiders. All publicly relevant web-site content and e-mail servers can be stored protected on a separate server in the “demilitarised zone” (DMZ) using the third 10/100Mbit/s Ethernet port. This assures absolute protection for the



MultiCom Ethernet III: the new 3-port firewall gateway

Intranet data. Unwanted access, for example by hackers, can only get as far as the DMZ, if at all.

The MultiCom Ethernet III can act as a three-way single-direction firewall gateway (see figure): Intranet (LAN) can access the Internet (WAN), while the Internet cannot access the LAN, but only specifically allowed services of servers connected to the third Ethernet port (demilitarized zone, DMZ). The DMZ can send data to the WAN, but cannot access the LAN directly. The information on the DMZ however can be accessed from the LAN.

The integrated stateful firewall can send syslog messages reporting particular events of your secure connection. Specific internal user's Internet access can be blocked with filtering. Further firewall functions are described in the next article.

Wireless applications

The MultiCom Ethernet III can be used to select data to be transferred over wireless LANs and thus filter according to freely configurable criteria. This enables the use of Wireless Ethernet 802.11 for Internet access in a city network by simply inserting the device between the LAN and the wireless modem. In contrast to conventional wireless LAN data transmission, Ethernet III data transmission is filtered and forwarded to the correct network site. This offers an interesting alternative for companies who connect their local networks on large corporate sites or in cities with wireless communication. Another nice application is to separate your LAN into 2 sub-LANs to have even more security locally.

LIGHTNING-Linux

Last but not least, the new device harnesses the power of the Linux-Kernel 2.4 in LIGHTNING-Linux. With future firmware releases you have access to the most up-to-date and reliable functions. Another benefit of the LIGHTNING-Linux system are the time-saving Easy Configuration tools.

Remote management

As a member of the popular MultiCom family, the MultiCom Ethernet Series can be remotely managed and remotely configured through standard interfaces, including Web, telnet, SNMP and a multi-platform configurator. Thanks to built-in Flash memory new firmwares can be upgraded even over the Internet without losing your own configuration file.

The MultiCom Ethernet III, with its six Ethernet connections, powerful firewall capabilities and complete broadband Internet access functions is the ideal firewall gateway for small and medium sized enterprises, as well as extended home offices.

The new MultiCom Ethernet gateways with firmware 3.0.1 are packed with new features, thanks to the latest 2.4 Linux kernel. This includes a very strong stateful firewall with Traffic Shaping, as well as interesting new Network Address Translation features like Load Balancing and Transparent Redirection. This article explains these new features and their benefits.

New Firewall and NAT features in MultiCom Ethernet Series

Stateful Inspection

The new firewall is a powerful stateful packet filter that is able to track all existing connections and not only single independent packets, like expensive enterprise-level firewalls. It does detailed header inspection of each packet, including protocol, source and destination (addresses or ports or interfaces), TCP flags, TCP options, ICMP type and connection state.

Benefit: corporate enterprise-class security for small and medium enterprises

External Intrusion Prevention

By keeping track of all outgoing connections, our firewall allows only replies to established connections, thus preventing any external access to the internal network (even when not using NAT). While authorized access can be silently logged, unauthorized connections can be directly reported to a Security Manager.

Benefit: protects from break-ins and WinNuke attacks

Intrusion Detection

The firewall has a simple detection scheme of intrusion attempts using its advanced logging feature: each type of packet can generate a different Syslog message, with specific security level and text prefix. In combination with the traffic shaping, this allows logging of only the first packet of an attack, resulting in shorter and more useful logs or to log only very frequent traffic (like Port Scanning or DoS attacks). It can also be used for simple statistical usage reporting.

Benefit: you are not only protected, you are also warned about potential hacker attack attempts

Port Scanning

Many hacking or security advising programs, such as nmap, Satan and Nessus, check all TCP and UDP ports of a machine, to detect potential weaknesses and identify the Operating System used by the computer. This allows dangerous system-specific attacks.

The LIGHTNING firewall is able to allow incoming requests only for selected authorized services and discard any mal-

formed packet, typically used in those attacks.

Benefit: protects from sophisticated attacks

Spoofing attacks

Since hacking is considered a crime, many hackers hide their real identity. This is done by forging the IP header to make it look like it comes from a different IP address than the real one. The LIGHTNING firewall can guarantee that the source address of outgoing packets has not been forged by a malicious internal user, thus preventing spoofing attacks originating at your site and avoiding external complaints for allowing such activities. IP Spoofing can also be used to gain access to servers by tricking it into thinking that the request comes from inside a trusted network. The LIGHTNING firewall can also forbid external packets from using internal trusted addresses, to prevent this attack. This unauthorized traffic can generate Syslog messages to alert the Security Manager that an attack attempt is underway.

Benefit: avoids hacker attacks and complaints from external companies

Traffic Shaping

This feature allows limiting the throughput of a specific connection. For instance, you can limit the FTP traffic, to reserve bandwidth to Web requests. Now when a computer tries to use too much FTP bandwidth, its requests are rejected by the MultiCom, effectively slowing down its access, so that other users can also use the network.

This feature 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.

Benefit: more efficient use of your bandwidth

Misuse of Internet Connection

Internal users can be prevented from using specific services (i.e. IRC or Napster) or reaching specific hosts. Users can be grouped by subnets to receive different levels of service. This can be linked with bandwidth limitation to limit the amount of bandwidth a single person or group can get from a costly WAN connection.

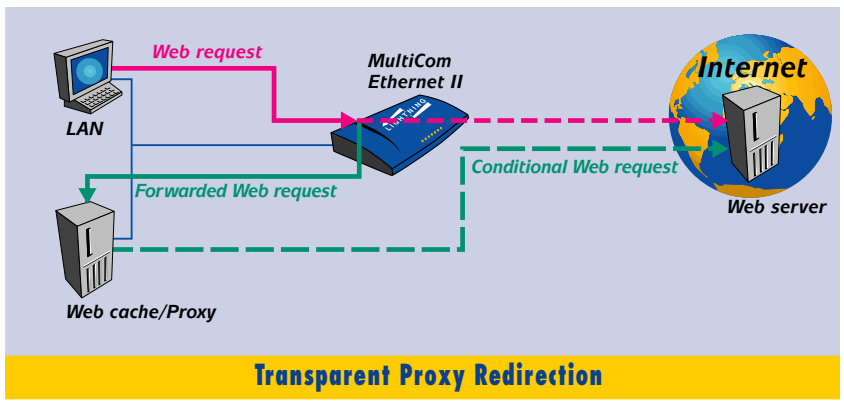
Benefit: reduce Internet costs, increase productivity

Unlimited corporate-class firewall

Denial of Service

Most DoS attacks can be avoided by rejecting malformed packets and using bandwidth limitations. This includes the infamous Ping of Death, the UDP diagnostic port attack, SYN flood attacks, Smurf, Nestea, Bonk, LAND, Teardrop…

Benefit: avoids disrupting vital e-commerce servers



Transparent Proxy Redirection

Transparent Redirection

The address translation can transparently and forcibly redirect outgoing Web (or FTP) requests to a local proxy/cache, to avoid unneeded traffic on the WAN.

Benefit: no client proxy configuration needed, better use of the Internet connection

Load Balancing

External requests to a single address can be redirected to multiple internal addresses, with a Least Recently Used algorithm (i.e. for a Web server farm). This allows sharing the load between multiple machines.

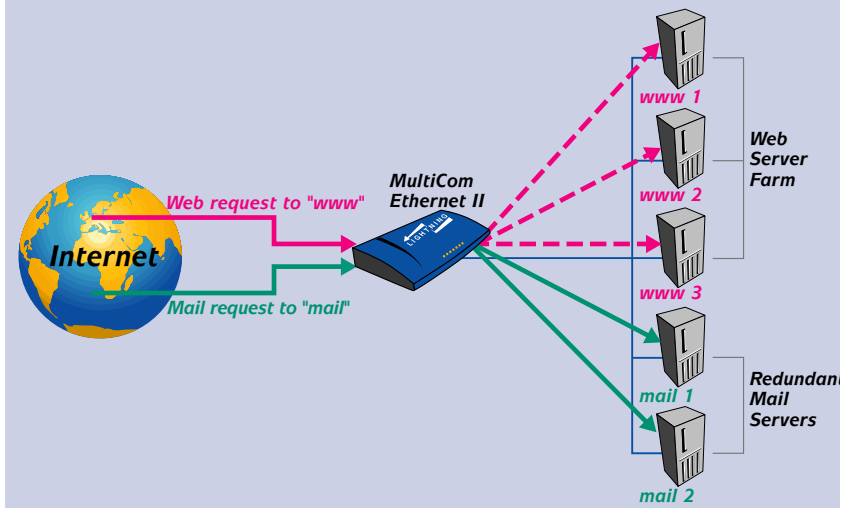
Benefit: avoids expensive dedicated load-sharing devices

Easy Configuration

The MultiCom comes with a default set of useful filtering rules, to prevent Port Scanning, External Intrusion, IP spoofing and Denial of Service attacks.

The bundled multi-platform configurator lets you graphically configure and monitor the MultiCom under Windows, MacOS and Linux. You can easily edit and create filtering rules, especially when using the predefined rules.

Benefit: automatic expert security for your entire network



Load Balancing

LIGHTNING's contribution to the Open-Source community

With the completion of its own Linux distribution, LIGHTNING-Linux, LIGHTNING is available for professional collaboration on customized projects as well as offering direct licensing of the LIGHTNING-Linux development platform and administration system. LIGHTNING-Linux is based on the very latest Linux kernel version 2.4, providing complete libraries with POSIX compliant APIs. Current projects take advantage of the advanced routing and gateway functionality of Linux. The Open-Source modifications are available on LIGHTNING's Web site at: http://www.lightning.ch/opensource/ along with an announcement list and an email for enquiries (opensource@lightning.ch).

NEW DISTRIBUTORS :

Finland
Ascom Fintel Oy
Rälssitie 7 A
01510 Vantaa
Phone: +358 90 870 3711
Fax: +358 90 870 3755
Web: www.ascom.fi

Greece
CPI S.A.
348 Messogion Ave.
153 41 Ag. Paraskevi
Phone: +30 65 45 802-5
Fax: +30 65 45 805
Web: www.cpi.gr

India
Zoom Technologies (India) Pv Ltd
C-Block Pent House - Banjara Kiran - RD
No 12 Banjara Hills
500034 Hyderabad
Phone: +91 40 339 4150
Fax: +91 40 33 18 770
Web: www.zoomgroup.com

Portugal
Mitrol S.A.
Rua de Diu, 6A
2685 Prior Velho
Phone: +351 219 407 390
Fax: +351 219 407 399
Web: www.mitrol.pt

United Kingdom
EDGE Technologies (Europe) Limited
1210 Parkview - Arlington Business Park
RG7 4TY Theale, Berkshire
Phone: +44 118 965 77 43
Fax: +44 1189 860 422
Web: www.edgetechnologies.co.uk

NEW PARTNERS IN GERMANY :

Germany
INC GmbH
Friedrichstrasse 20
D-63225 Langen
Phone: +49 6103 201 20 0
Fax: +49 6103 201 20 40
Web: http://www.inc-gmbh.de

terra link Internet Marketing GmbH
Merkurring 116
D-22143 Hamburg
Phone: +49 40 646 680 111
Fax: +49 40 648 680 120
Web: http://www.terralink.de

CALENDAR OF EVENTS

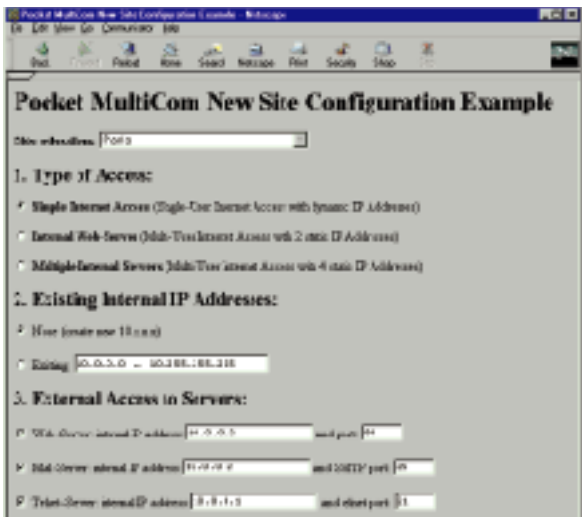
CeBIT 2001
Hannover
Hall 11 Stand D 09
22 - 28 March 2001

CommunicAsia 2001
Singapore
Hall 6 Stand D3-07
19 - 22 June 2001

Networld+Interop 2001
Paris
Stand M91
18 - 20 September 2001

Automatic Configuration of LIGHTNING Gateways

The automatic configuration of LIGHTNING MultiCom gateways allows Internet Service Providers (ISPs) to offer their clients additional services such as remote installation, maintenance and upgrade of the devices. Using MultiCom gateways in a bundle with an ISP is therefore of great advantage, for the end-user as well as for the ISP.



Before going out to the client, the MultiCom device is provided with an ISP specific configuration, which allows for automatic access to the registration server of the ISP.

The end-user only needs to connect the two color-coded cables between the gateway, the Internet-link and the PC. Furthermore he only needs to start-up any Web browser (Netscape or MS Internet Explorer) and to fill-in the URL of the ISP's registration server.

To be registered at the provider, the user enters the information required by the provider, such as his name, billing address, type of Internet access, his username, password, email name etc. to the registration server. His input will be transferred from the registration server to the configuration server who gathers all information in a configuration file, transfers it to the gateway and reconfigures the gateway. The client is now able to use his personalized Internet access without actually having configured the gateway himself.

A great advantage of this process is its platform-independence. The automatic configuration via registration server works with Microsoft Windows, Linux or Apple Macintosh, and is extremely easy and virtually maintenance- and support-free. Once the gateway is installed at the client's location, the end-user does not have to worry about the configuration, the management or the upgrade of his gateway.

France Telecom

France Telecom is successfully using LIGHTNING's MultiCom devices for the french national school Education project and guarantees its clients an easy configuration without needing the support of technical specialists. Thus LIGHTNING products received the "Scolagora" approval stamp.

Scol@gora matériel

New Resources at LIGHTNING's Website

While LIGHTNING's development labs are building new technologies, other departments of LIGHTNING have made these technologies easily accessible. For our German speaking clients LIGHTNING has a new website http://www.lightning-ag.de. This website not only has all of the German information but also offers an online discussion forum for users with questions.

LIGHTNING also has made numerous additions to the main website at http://www.lightning.ch. For example… in the Support section:

- **A new FAQ for firmware 2.6.1, and a new download and explanation page for software**
- **A new Reference Manual for the upcoming 2.6.2 firmware**
- **A new White Paper on firewalling with the LIGHTNING-Linux 3.0.1 firmware**

THE LIGHTNING FLASH
Issue 4/2001
Editor: Dr. B. Brunner, Managing Director
LIGHTNING Instrumentation SA

The LIGHTNING Flash is published twice a year for LIGHTNING Instrumentations SA,

Av. des Boveresses 50 - 1010 Lausanne - Switzerland
Phone +41 21 654 2000 - Fax +41 21 654 2001
Internet: www.lightning.ch
Email: info@lightning.ch

http://www.lightning.ch