GIBRALTAR

Support-services and consulting

eSYS offers professional product support (e-mail and telephone) to all clients and partners of Gibraltar. Short reaction times, the proximity to our customers and the **direct contact to the developers of Gibraltar** are major factors of the success of Gibraltar.

By developing Gibraltar over the last years, we were able to generate an outstanding knowledge in all fields of network security. We provide this knowledge to our customers.

eSYS is a professional partner for:

- Planning and implementing security concepts
- Managed firewall services (permanent management and support of security solutions)
- Security audits (Black box, white box, penetration testing)
- Implementing individual security solutions on the basis of Gibraltar

About Gibraltar

Gibraltar was founded as an open source project in 1999 by Dr. Rene Mayrhofer. Since that time, Gibraltar has been used by over 5.000 companies, organisations, public facilities, private users, schools and universities. Through permanent product development and significant participation of the open source community, Gibraltar has been evolved to one of the leading security products.

Since 2003, Gibraltar has been developed in cooperation by Dr. Rene Mayrhofer and eSYS Information Systems GmbH in Austria. Gibraltar is being distributed in over 10 countries through a world wide partner network.

GIBRALTAR
Partnerinformation

KASPERSKY
ANTI-VIRUS

GIBRALTAR

Firewall rules

Firewall rules	Overview active rules	Additional interfaces	Port aliases	Port groups

Interface	Source address	Dest. address	Protocol	Source port	Dest. port	Action
1. int1 -> LOCAL	ANY	ANY	TCP	ANY	ftp	ACCEPT
2. int1 -> LOCAL	ANY	ANY	UDP	ANY	dns	ACCEPT
3. int1 -> LOCAL	ANY	ANY	TCP	ANY	8110	ACCEPT
4. int1 -> LOCAL	ANY	ANY	TCP	ANY	3128	ACCEPT
5. ANY -> LOCAL	ANY	ANY	ICMP	ANY	ANY	ACCEPT
6. ANY -> LOCAL	ANY	ANY	TCP	ANY	22	ACCEPT
7. ANY -> LOCAL	ANY	ANY	TCP	ANY	443	ACCEPT
	ANY	ANY	UDP	137:139	137:139	DROP
	ANY	ANY				ACCEPT
10. ANY -> LOCAL	ANY	ANY		ANY	ANY	
12. ANY -> ANY	ANY	ANY				
13. ANY -> ANY	ANY					
14. ANY -> ANY						

GIBRALTAR SECURITY GATEWAY
Unified Threat Management by Gibraltar

FW-7870

eSYS@AT
www.esys.at

Unified Threat Management by Gibraltar

Gibraltar Security Gateways provide a comprehensive and competitive protection against a multitude of current security risks and threats. They combine several important security applications into one product and provide for secure connections in your network. Gibraltar is either available preinstalled on five different hardware appliances or just as a software release.
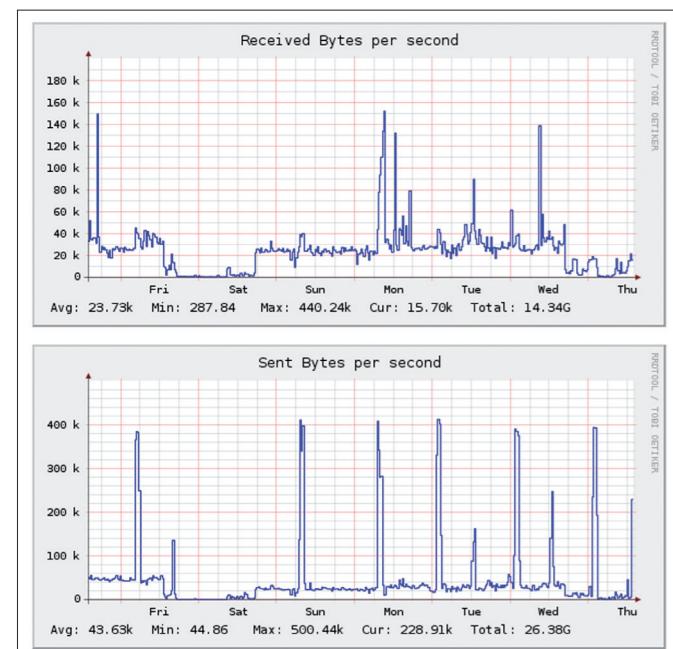
Figure: Monitoring of incoming and outgoing data
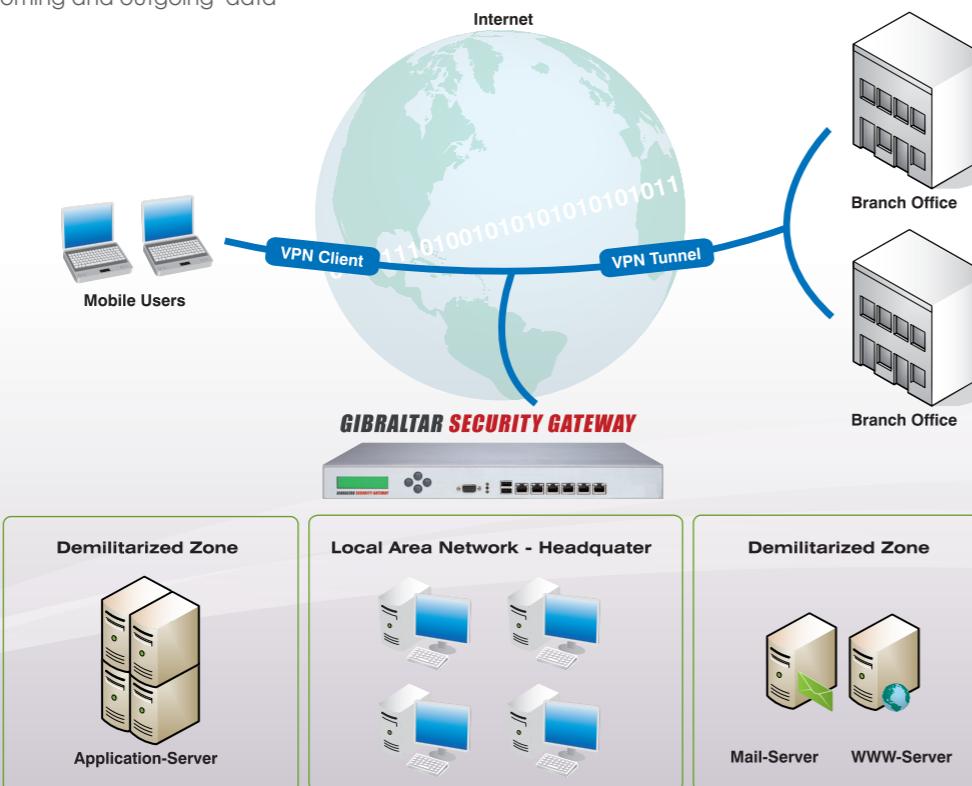
Firewall

The Gibraltar Firewall inspects and secures overall network and Internet traffic and provides for secure connections. The Gibraltar dynamic packet filter (Stateful Packet Inspection) and several application level proxy servers guarantee highest available security for all prevalent network protocols.

Proxy Server

Several proxy servers provide for high performance and additional security. The integrated e-mail proxy is able to check all e-mails against spam and viruses. The transparent Web proxy enables a restrictive management of the private Web usage of all employees.

Anonymisation-Gateway

Internet providers and companies are legally bound to monitor all network traffic. Thus, it is possible to identify and track sensitive data about companies and their customer and supplier relationships. Gibraltar is able to make selected network traffic anonymous. This means, that not even Internet providers are able to track down traffic to the originating server or user. By using Gibraltar anonymisation service, it is possible to both observe law and assure anonymity.

System
- Specially hardened Linux kernel
- Write-protected boot media: USB and CD-ROM
- Conventional boot media: CF and HDD
- Languages: German and English
- Remote configuration: web based configuration tool (SSL) or remote login (SSH)
- Easy configuration management
- Automatic Software Update Service
- Stateful high availability: Hot standby firewall

Network Interfaces
- Arbitrary number of network interfaces
- Ethernet 10/100/1000 MBit/s: static or dynamic IP addresses, virtual IP addresses
- DSL (Ethernet and USB), cable, modem
- VLAN

Firewall
- Stateful Packet Inspection Firewall
- Support of all popular network protocols
- Flexible packet filter: interface, MAC address, IP address, port, service, ...
- Protection from DoS/Flood attacks
- Limitation of peer-2-peer services (P2P) and instant messaging services
- Dynamic and static address translation (NAT)
- Load balancing: port address translation (PAT)
- Transparent firewalling (bridged mode)
- Randomized IP Sequencing
- TTL manipulation
- Protocol Pass Through: PPTP, FTP, H.323, IRC

Proxyservices
- Deep packet inspection (application level filter)
- Secure SMTP relay: secure relaying of e-mails, attachment blocking, block lists, virus protection by Kaspersky, spam protection
- Transparent http proxy: no client configuration necessary, block lists for URLs and domains, virus protection by Kaspersky
- User authentification: user list, Active-Directory, LDAP
- Content caching: caching of web contents to improve web performance
- Content scanning: virus protection, check for dangerous contents (Cookies, ActiveX, JavaScript)
- FTP proxy: outgoing, incoming, virus protection by Kaspersky
- Transparent POP3 proxy: virus protection, spam protection, attachment blocking

Virtual Private Networks Gateway
- L2TP and IPSec VPN Server, PPTP
- Clientless VPN with Windows XP/2000, MAC OS, Linux
- VPN Client for NT/98/2000/XP/2003
- Unlimited number of tunnels and VPN clients
- NAT Traversal
- Encryption: AES, 3DES, Blowfish, Twofish, CAST, Serpent
- Authentification: PSK and X.509 certificates
- Perfect Forward Secrecy (PFS)

Spam protection
- Combination of ten different detection methods
- Deletion, marking or isolation of spam e-mails
- Detection of phising e-mails
- SMTP e-mail encryption (TLS)
- Self learning and adaptive filter (Bayes filter)
- Sender Policy Framework (SPF)
- Black lists (RBL) and hash check (Razor, DCC)
- Rule based filter (SpamAssassin)
- Check for RFC conformity
- Deceleration of Bulk mails (tar pit)

Antivirus protection
- Check of e-mail, downloads, web pages and FTP
- Powered by Kaspersky Labs

Traffic Shaper (QoS)
- Effective and flexible bandwith management
- Class based traffic shaping
- Prioritisation of network traffic

Monitoring
- Extensive logging
- Graphic and text based web and e-mail reports

Anonymisation
- Anonymisation of network traffic
- Supports anonymous web surfing
- JAP anonymisation proxy
- TOR anonymity network
- Freenet http - Portal

Additional services
- Dynamic DNS
- DHCP Server
- Secure DNS Resolver
- SSL wrapper for arbitrary services

Secure, convenient, powerful

Gibraltar Security Gateways offer a unique cost/performance ratio and a very simple and flexible administration. For schools and universities, Gibraltar offers very special conditions. Feel free to ask for academic licenses.

Scalability and reliability through simple hardware replacement

The software release of Gibraltar can be operated on all common hardware platforms. This makes Gibraltar unbeaten in scalability. Hardware replacement is very easy and can be achieved during a couple of minutes.

Secure and simple management by Read-only technology

Gibraltar starts and runs fully off physically write protected media. For this reason, a time-consuming and insecure hard disk installation is not necessary. On the contrary, read-only operation of Gibraltar leads to a significant improvement of security, since it is not possible for potential attackers to permanently reside on the system. System configuration can be archived alternatively on hard disk, USB media, floppy disk or e-mail.

Pure flexibility on the console

For the sophisticated administrator, Gibraltar offers a maximum of flexibility and functionality by using the system console. Nothing is impossible if you are approaching Gibraltar on the console. Gibraltar can be configured both on the console and with the easy-to-use Web based configuration tool. Linux experts will be highly surprised what Gibraltar offers beneath the surface.

Comfortable with easy configuration system

Gibraltar can be installed and configured with an easy to use Web based configuration tool. A detailed online help and many useful configuration scenarios assist the firewall administrator. However, if there are some questions left, Gibraltar offers professional telephone and e-mail support.
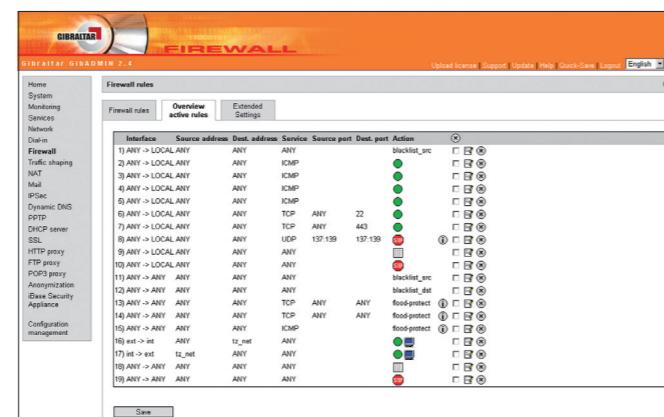
Figure: Screenshot of the Web based configuration tool

Unbeatable in cost/performance ratio through open source development

Gibraltar is based on an accurately hardened Debian/GNU Linux and solely uses proved and tested open source components. Except for the Web based configuration tool, all Gibraltar source codes are permanently published and can be reviewed and tested by open source community. In return, privately using Gibraltar is cost-free.

Easy updates and professional support

With the Gibraltar UpToDate-Service you stay permanently up to date. Software updates will be downloaded and installed fully automated. New releases of Gibraltar can be installed using the web based configuration tool (Gibraltar Security Appliances) or replacing the system CD (Software release).

The professional telephone and e-mail support guarantees a trouble free installation and smooth operation of Gibraltar. Gibraltar support means you will get direct support from Gibraltar developers. These guys are real security pros and will find a solution for each of your problems. Give us a test!

Antivirus Gateway

The *Gibraltar Antivirus-Gateway powered by Kaspersky Labs* inspects all e-mails, Web downloads and FTP data transfers for computer viruses. Additionally the Antivirus Gateway includes an effective protection against phishing e-mails and spyware.
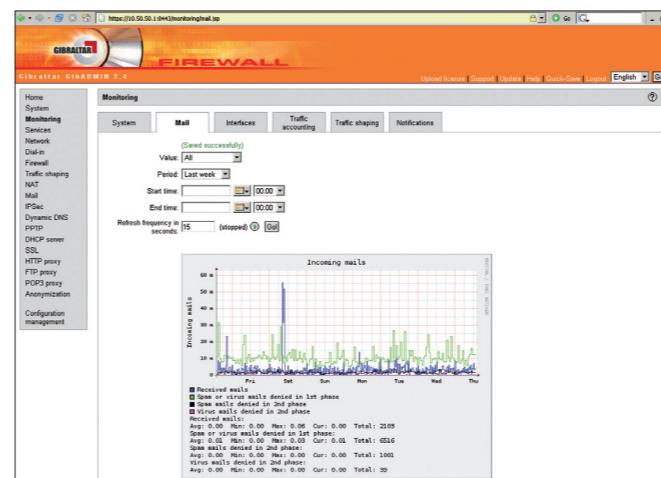
Figure: Screenshot of the mail monitor

Bandwidth management

Gibraltar bandwidth management makes it possible to prioritise and to regulate overall network traffic. Time-critical applications like VoIP (Voice over IP) and all kind of terminal server protocols receive the minimum bandwidth they require. The built-in monitoring feature makes it possible to permanently observe the shaped traffic.

Spam filter

The Gibraltar mail filter reliably identifies and deals with unsolicited e-mails. This will raise the productivity of your employees. By using the Gibraltar spam filter it is possible to reduce the number of unrequested e-mails by over 99 per cent.

Virtual private network gateway

The Gibraltar VPN server securely connects all company sites and branch offices over potentially insecure networks. It also provides encrypted and secured remote access to the company network for your field staff.
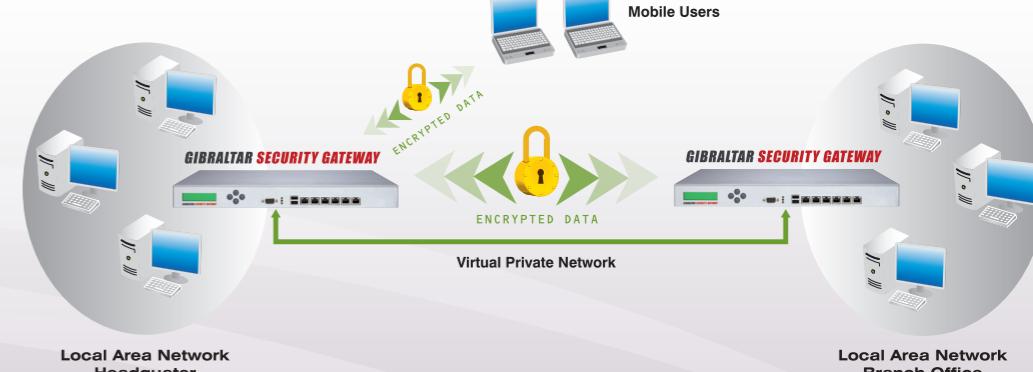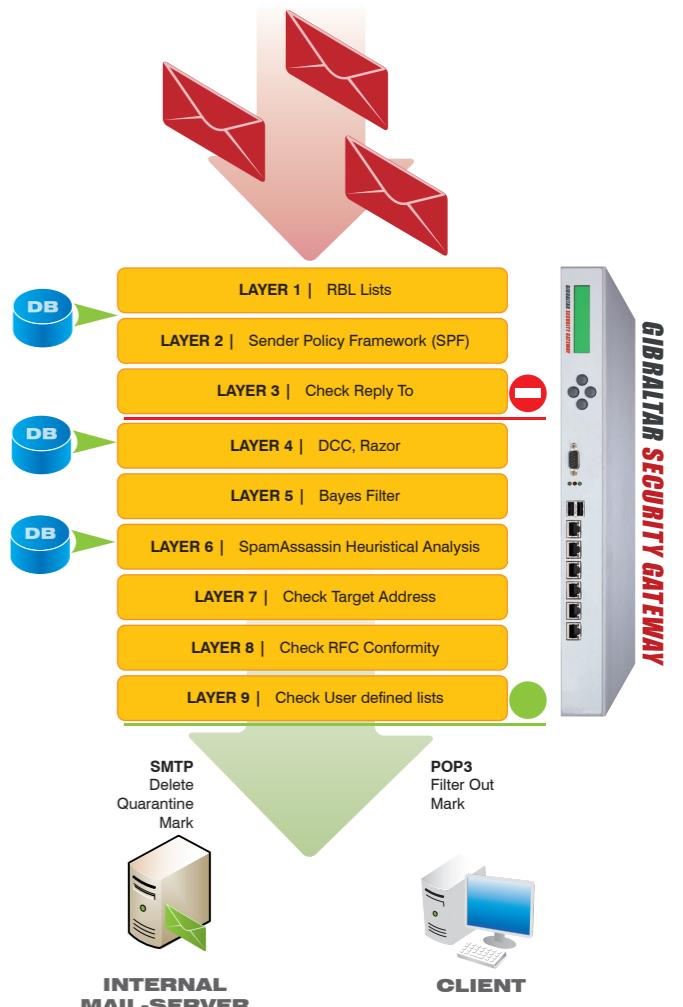
Figure: The different layers of the spam filter

LAYER 1	RBL Lists
LAYER 2	Sender Policy Framework (SPF)
LAYER 3	Check Reply To
LAYER 4	DCC, Razor
LAYER 5	Bayes Filter
LAYER 6	SpamAssassin Heuristical Analysis
LAYER 7	Check Target Address
LAYER 8	Check RFC Conformity
LAYER 9	Check User defined lists

SMTP
Delete
Quarantine
Mark

POP3
Filter Out
Mark

INTERNAL MAIL-SERVER

CLIENT

Figure: VPN networks

Mobile Users

GIBRALTAR SECURITY GATEWAY   ENCRYPTED DATA   GIBRALTAR SECURITY GATEWAY

ENCRYPTED DATA

Virtual Private Network

Local Area Network Headquater

Local Area Network Branch Office

Gibraltar Security Gateway Appliances

	GSG1000	GSG1200	GSG2800	GSG3400	GSG6800
Form Factor		1U Rack Mount	1U Rack Mount	1U Rack Mount	2U Rack Mount
Dimension	225 x 156 x 35 mm	426 x 270 x 44,4 mm	426 x 391 x 44,4 mm	426 x 495 x 44,4 mm	426 x 550 x 88,8 mm
Weight	2 kg	6 kg	5 kg	9 kg	14 kg
Performance Data					
Users	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Firewall throughput					
VPN throughput					
VPN tunnels					
Concurrent connections					
Policies	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Hardware specification					
Main memory	256 MB	512 MB	512 MB	1024 MB	2048 MB
Processor	1 GHz VIA	1,2 GHz Mobile Celeron	P4 2,8 GHz	P4 3,4 GHz	P4 Xeon
Hard disc	Optional 40 GB IDE	40 GB IDE	80 GB SATA	80 GB SATA	2 x 80 GB SATA
10/100	4 (LAN Bypass)	4 (LAN Bypass)	-	(4/8)	-
10/100/1000	-	-	6 (LAN Bypass)	(4/8)	(4/8/12)
USB	2 x USB 2.0	2 x USB 2.0	2 x USB 2.0	1 x USB 2.0	1 x USB 2.0
RS232	1 x DB9	1 x DB9	1 x DB9	1 x DB9	-
AC voltage	100 - 240 V	90 - 264 V	90 - 264 V	90 - 264 V	90 - 264 V
Frequency	50 - 60 Hz	47 - 63 Hz	47 - 63 Hz	47 - 63 Hz	47 - 63 Hz
Power supply	20 W Power Adapter	ATX 220 W	ATX 220 W	300 W Auto Switching	1+1 Redundant 460 W
Operating temperature	0 - 40° C	0 - 40° C	0 - 40° C	0 - 40° C	0 - 40° C
Certification	CE, FCC	CE, FCC	CE, FCC	CE, FCC	CE, FCC