



User Manual

Gibraltar Firewall - release 2.6

Gibraltar Firewall

© 2008 by eSYS Informationssysteme GmbH

All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Printed: Juli 2008 in Attnang-Puchheim, AUSTRIA

Publisher

eSYS Informationssysteme GmbH

Managing Editor

Thomas Mayrhofer

Technical Editors

Dipl.-Ing. Richard Leitner

Mag. Andreas Wöckl

Manuel Hofer

Special thanks to: Univ.-Prof. Dr. Rene Mayrhofer

Table of Contents

Vorwort	0
Part I Introduction	1
1 Gibraltar - Development	1
2 Gibraltar - Features	1
Part II Firewall basics	5
1 Firewall	5
2 Network Address Translation (NAT)	6
3 Proxy services	6
4 Virtual Private Networks (VPN)	7
Part III Hardware requirements	7
Part IV Installation	8
Part V Licensing	8
Part VI The webinterface	9
Part VII Practical examples	10
1 ADSL	12
2 Internet-Gateway	15
3 Firewall und DMZ	17
4 IPSec VPN	22
5 Active Directory	26
6 Proxy Server	29
7 Traffic Shaping Citrix and VOIP bridged	31
8 Traffic Shaping Citrix and VOIP with VPN	36
9 Traffic Shaping VoIP	41
10 Traffic Shaping Web Traffic	44
Part VIII Configuration	45
1 License information	47
2 System configuration	49
System - General settings	50
Syslogs	51
Search the syslog	51
Configure hard disk	52
Heartbeat	52
Block Login Attempts	52
Active Connections	53
3 Monitoring	53
System	53
Mail	54

Interfaces	54
Traffic accounting	54
Traffic shaping	55
Troubleshooting	55
4 Services	55
5 Network	57
Network	57
DNS	58
Network interface.....	58
Routing	59
Connection test.....	60
Definitions	61
Host/Net aliases.....	61
Host/Net groups.....	61
Services	61
Additional interfaces.....	62
Dial-In	62
Dial-in via phone.....	62
Dial-in detail view.....	63
ADSL PPTP.....	63
ADSL PPTP detail view.....	64
ADSL PPP over ATM.....	64
ADSL PPP detail view.....	65
ADSL PPP over Ethernet.....	65
ADSL PPP over Ethernet detail view.....	66
Bridging	66
VLAN	67
DHCP server	67
DHCP - general settings.....	68
DHCP - configuration.....	68
DHCP leases.....	68
DHCP relay.....	68
Dynamic DNS.....	69
6 Firewall-rules	69
Firewall rules	69
Overview active rules	71
Firewall - Extended Settings	71
Firewall rules - Default	72
Firewall rules - Advanced	73
Firewall rules - Advanced P2P	74
7 NAT	74
NAT rules	75
Overview active rules	76
NAT Rule details	76
8 User	78
User management settings	78
LDAP Settings	80
Freeradius Accounting	82
9 Mail	83
Mail	83
Mail - General settings.....	83
Relay outgoing.....	84
Relay incoming.....	85
Common checks.....	85
SMTP Authentication.....	86
AntiSpam	86
AntiSpam (1).....	86

AntiSpam (2).....	87
Blacklists and Whitelists.....	88
Language Restrictions.....	88
Update rules.....	89
AntiVirus	89
10 VPN	89
Open VPN	90
General settings.....	90
Extended settings.....	90
Status	91
IPSec	91
IPSec - General settings.....	91
Tunnel	91
Tunnel - Default.....	92
Tunnel - Advanced.....	93
Watchdog.....	93
PPTP	94
General Settings.....	94
PPTP - Extended Settings.....	94
L2TP	94
L2TP-General settings.....	95
Certificates	95
Certificate Revocation List.....	96
Generate host certificate.....	96
Generate client certificate.....	96
SSL	97
SSL VPN	97
11 Proxy server	98
HTTP proxy	98
General settings.....	98
Proxy cache.....	99
Authentication.....	99
Content filter.....	99
Exceptions.....	100
PureSight Content Scanner.....	100
POP3 proxy	101
General settings.....	101
Rename attachments.....	102
FTP proxy	103
Outgoing.....	103
Incoming.....	103
Anonymization	104
Anon Proxy.....	104
Anonymizer.....	104
Freenet.....	105
12 Snort IDS	105
General	105
Output Modules	106
Update Snort Rules	106
Snort Rules	106
13 Traffic shaping	106
General settings	107
Interface groups	107
Classification	107
Classification Group	108
Traffic shaping rules	108
Traffic shaping rules - Detail	108
Overview active rules	109

14	Captive Portal	109
15	Configuration management	110
	General settings	110
	Save config	110
Part IX	Support	110
Part X	Update	111
1	Version info	111
2	Online update	111
3	Upload CF image	111
4	Remove updated files and Rollback	112
	Index	113

1 Introduction

1.1 Gibraltar - Development

We are glad to have you as customer of a Gibraltar Security Gateway or the Gibraltar Security Software.

Gibraltar is available in the following options:

- **Gibraltar Software:** a hardware irrespective software-solution
- **Gibraltar Security Gateway:** Gibraltar pre-installed on a Hardware Appliance

This manual guides you through the configuration of Gibraltar and should provide you with a directory for administrators. If this is the first firewall you are about to set-up and configure, you may want to read the chapter [Practical Examples](#). You'll find a lot of step-by-step instructions for common scopes in this chapter. These examples are perfect to just start with configuring your Gibraltar.

You can also find an current and up-to-date version of this manual on our website www.gibraltar.at, and also as online-help in the webinterface of Gibraltar (GibAdmin)

If you have any questions or suggestions pertaining to this manual, please send a Mail to support@gibraltar.at

1.2 Gibraltar - Features

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.

System and Management

- Hardened OS-Kernel based Debian Linux
- Read Only Boot media: USB, CD-ROM
- Conventional Boot media's: Compact Flash, Hard disk
- Languages: German, English
- Management: Remote via a web-based Configuration tool (SSL) or Remote Login (SSH)
- Simple Configuration Management
- User management: LDAP (local and extern), Active Directory
- Automatic Software-Update-Service
- High-Availability: Hot-Standby
- Detailed logging and interactive analysis

Interfaces

- Scalable number of network interfaces
- Scalable number of IP addresses on each network interface.
- Ethernet 10/100/1000: static or dynamic IP addresses
- ADSL (PPTP, PPPoATM, PPPoE), ISDN
- VLAN's

- Bridging
- Graphical traffic analysis

Firewall and Packetfilter

- Stateful Packet Inspection Firewall
- Support of all popular network protocols (protocol pass through: PPTP, FTP, H.323, IRC)
- Flexible Paket filter: Interface, MAC address, IP address, port, service, etc.
- Protection of DoS/Flood attacks.
- Limitation of Peer-2-Peer Services (P2P)
- Dynamic and static address translation: Network Address Translation (NAT), Port Address Translation (PAT)
- Load Balancing
- Transparent Layer 2 Firewalling (Bridged Mode)
- Randomized IP Sequencing
- Gezielte TTL Manipulation

Web Filter

- Proxy-Server (transparent)
- Caching-Proxy
- Authentification: LDAP (local and extern), Active Directory
- Blocking of websites after dynamic categorization (content filtering)
- User defined and server-based blocklists for URL's and Domains.
- Examination on dangerous content (Cookies, ActiveX, JavaScript)
- Detailed logging and interactive analysis

E-Mail Filter

- Virusfilter: protocols SMTP and POP3
- Spamfilter: protocols SMTP and POP3
- Filtering of undesirable E-Mail-Attachments
- Graphical Analysis
- Image- and PDF-spam-detection
- Deleting, marking or isolation of Spam-Mails
- Detection of Phishing-Mails
- SMTP-E-Mail-Encryption (TLS)
- Self-learning trainable Filter (Bayes-Filter)
- Sender Policy Framework (SPF)
- Blacklisting (RBL) and Hashreview (Razor, DCC)
- Rulebased Review (SpamAssassin) with automatic Update
- Review of RFC-Compliance
- Delaying of Bulk-Mails (tar pit)

Virtual Private Networks Gateway (VPN)

- Site-to-Site VPN: IPSec
- Client-VPN: IPSec, OpenVPN, L2TP, PPTP
- Clientless SSL VPN: Mit Windows XP/2000, MAC OS, Linux
- Unlimited number of tunnels and Clients
- NAT Traversal
- IPSec encryption: AES, 3DES, Blowfish, Twofish, CAST, Serpent
- IPSec authentication: PSK and X.509 certificates
- Perfect Forward Secrecy (PFS)

- certificate management

Traffic Shaping and Bandwidthmanagement

- Incoming and Outgoing Traffic
- Pre- and user- defined Traffic-classes, for example: VOIP, Citrix, RDP..
- Minimal guaranteed and maximal bandwidth per class
- VPN-bandwidthmanagement (IPSec)
- Splitting of general bandwidth: IP-addresses of Subnets
- Graphical analysis

Captive Portal

- Browser-based authentication to (WLAN-) Hotspots
- Automatic redirect to login-mask
- Authentication: LDAP (local and extern), Active Directory, external RADIUS-server
- Simultaneous public and private network services
- Logging of traffic and connection times
- Flexible user-right-management

Anonymity

- Anonymity of selected network traffic
- Provides anonym internet browsing
- JAP Anonymity-Proxy
- TOR Anonymity Network
- Freenet HTTP - Portal

Additional Services

- Dynamical DNS
- DHCP Server
- Secure DNS Resolver
- SSL Wrapper for selected TCP services
- Transparent FTP-Virus-scanning

#####

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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!

2 Firewall basics

2.1 Firewall

Configuring a firewall like Gibraltar correctly needs extensive knowledge about the functionality of a computer network and the techniques used by it. Only a firewall that is configured correctly enhances the security. This is the reason for explaining the most important basics and some essential terms at this point of the manual. A detailed explanation of all techniques would go beyond the scope of this manual. Some recommendable books and links can be found in the appendix.

A firewall is a security component of a computer network which allows or denies traffic using a defined rule set (policy). The aim of using a firewall is to divide different network segments based on their different states of trust. A typical situation for using a firewall is to control the traffic between a local area network (LAN) and the Internet.

Types of Firewalls

Generally firewalls are divided up into network firewalls and personal firewalls. A network firewall is a dedicated device that separates two networks or two network segments. The firewall controls the traffic between these network segments in this case. To divide the traffic of the different network segments the firewall has more than one network interface - one for each network segment. A personal firewall is a software that is installed at the computer that should be saved. It only secures the computer which it is installed on.

Gibraltar is a network firewall and can optionally be used at an existing hardware or at Gibraltar Security Gateways that can be purchased at the online shop at <http://www.gibraltar.at>.

There are different ways a firewall uses to divide wanted traffic from not allowed traffic. The most important component is the packet filter.

Packet Filter

A packet filter is a software that filters incoming and outgoing traffic using predefined rules. It uses different information that is provided by each data packet. Common criteria are:

- network protocol
- source and destination address
- source and destination port

The administrator defines a special set of rules (firewall rules, policy) to specify what should be done with the incoming and outgoing packets. Generally the packet can be forwarded to another network (**ACCEPT**), can be ignored (**DENY**), can be sent back with an addition why it is sent back (**REJECT**), or can create a new entry in the syslog (**LOG**). The packet filter is the core of each firewall and therefore it is very important to configure it very responsibly and attentively.

Gibraltar uses the principle: **"If it is not allowed, it is denied!"**. This means that by default Gibraltar blocks all traffic except some special kind of packets to reach the web interface or to check basic network connections (ping). The administrator of Gibraltar opens the ports to allow traffic passing Gibraltar.

Stateful Packet Inspection

Stateful inspection is an extended form of packet filtering. A simple packet filter checks each packet for its own and decides for each separate packet using the information in it if it is forwarded or if it should be blocked. Stateful packet inspection recognizes a logical stream of packets that is

opened by each connection and decides for all the packets assigned to this connection if they are allowed or if they are not. An additional filter criteria is the state of each packet depending on its situation within the logical stream (new, established, ..). This option can also be used to allow all answering packets to a specific connection automatically. This possibility eases the configuration of the filter rules and reduces the number of rules needed.

2.2 Network Address Translation (NAT)

Network address translation (NAT) is a collective term for processes that replace address information within network packets - automatically and fully transparent. NAT is a key feature of a router or firewall. It hides the internal structure of a network and allows using only one public IP address for a whole network of computers. This is both an advantage in security and a necessity because of the shortage of IPv4 addresses.

There are two different kinds of NAT:

- **Source NAT (SNAT):** Outgoing traffic is masqueraded by a fixed IP address (a public IP address for example).
- **Destination NAT (DNAT):** Incoming traffic is forwarded to a special internal network address. DNAT can be used to forward requests to a web address at the external interface to an internal web server that runs the web site.

Special cases of NAT are:

- **Masquerading:** Outgoing traffic is masqueraded with a dynamic IP address.
- **Redirection:** Incoming traffic is redirected to another port on the router where a special service listens. The destination address is not changed in this case.

2.3 Proxy services

A proxy server as the name implies acts as a replacement for another computer. It takes over the requests from a client for a web page for example and starts the requests instead of the clients. So the client is hidden for the server. The proxy server additionally can filter for viruses or unwanted content. It can also make the requested sites faster.

In simplest cases the proxy only forwards information. The user does not recognize the existence of it when it runs in transparent mode. The proxy - in most cases a http proxy - only controls the communication between the web browser (client) and the web server. Main functionalities are:

- **Cache:** The proxy saves the sites that are visited by a user in a cache. When the same site is requested by another user it is fetched from the cache and not from the web page directly again. This functionality fastens the requests and decreases the load at the net.
- **Filter:** The proxy allows filtering the visited sites for viruses or unwanted content. This can only be done because the proxy can put the single packets together to a whole http packet. It understands the traffic passing. The proxy is situated at the application level of the ISO/OSI layers model. Filtering can only be done by a proxy.
- **Access control:** A proxy can be used to control the access to separate sites or the whole Internet to single users or groups of users.

There are proxy servers for several Internet services. The following proxies are part of the Gibraltar firewall software:

- **HTTP proxy:** Acts as sub-agent and checks for viruses and unwanted content (only with separate licenses).
- **SMTP proxy:** Checks email traffic between mail servers. Allows checks for viruses and unsolicited bulk emails (spam) - also called Mail Relay.
- **POP3 proxy:** Checks emails traffic that is fetched by the client from a POP3 server. Allows checks for viruses and spam.
- **FTP proxy:** Checks ftp traffic for viruses (only with separate license).

Transparent Proxy

A proxy is called transparent if the client does not need to change anything at his client to use the proxy. Additionally it is not possible to bypass the proxy. Requests to the special port (e.g. HTTP proxy to port 80) are redirected to the port where the proxy listens. The user has no possibility to bypass the proxy. All proxies within the Gibraltar software can be run in transparent mode.

2.4 Virtual Private Networks (VPN)

A VPN (virtual private network) is a net that uses the public Internet to transport private data from one point to another. It allows to send confidential information over a insecure network. The members of a VPN can change information as if they were in a LAN. The connection is encrypted.

There are four different types of VPN; two of them are implemented in Gibraltar:

- **Site-to-Site:** Connection of two networks by VPN gateways on both sites. These gateways establish a permanent VPN connection that can be used by all clients behind the gateways to reach the opposite network. This kind of VPN is used to connect different headquarters of a company. Gibraltar uses IPSec for Site-to-Site VPN connections.
- **Site-to-End:** Connection of an external worker with the headquarter. The computer or laptop of the employee starts the VPN tunnel to connect his computer to the VPN gateway of his company. Using this connection allows the employee to work as if he were in the office. Gibraltar offers different possibilities for this kind of VPN.

Passwords, public keys, or digital certificates ensure the authentication of the VPN end points. To increase the security the traffic that comes through into the network via VPN should be filtered by the packet filter. This additional configuration makes the forwarding of worms or Trojans more difficult.

3 Hardware requirements

In case you bought a Gibraltar Security Gateway, you will find the software pre-installed on your appliance.

An additional way is to download the software-version of Gibraltar, which is a Live-CD-System, bootable and running from CD. Using a Hard Disk with your Live-CD-System is not necessary but you can, in most cases this depends on your requirements.

For running Gibraltar as a Live-CD-System you will in any case need 2 network interface cards and...

Recommended:

- PC Pentium (\geq 600 MHz)
- \geq 256 MB RAM
- bootable CD-ROM 32x or better
- HDD for bigger log files and email relaying (SMTP proxy)
- USB storage media
- 2 x 100 MBit/s network adapter (best tested: 3COM, Intel or Realtek chip set)

Compatibility:

- Network adapter: all PCI based 10/100 or 1000 MBit/s
- Modem: AT standard
- USB modem: ACM standard (not tested)
- DSL modem: Alcatel USB Speedtouch or any Ethernet modem

4 Installation

You have the following possibilities to purchase Gibraltar:

- You buy a complete Gibraltar package from one of the authorized Gibraltar partners.
- You download an image from our homepage and order a license key at the online portal.

Purchase from a partner

If you purchased Gibraltar from one of the authorized Gibraltar partners or resellers, you got Gibraltar within scope of delivery on a CD-ROM enclosed. If you put this CD into the computer you want to use for Gibraltar, the system boots completely from CD, and starts Gibraltar as far as you have selected the CD-ROM as first boot device in the BIOS.

Download the Gibraltar Image

After downloading the ISO image from the Gibraltar homepage you have to create a bootable CD. That process should not allegorise a major problem. Therefore you have to start your programme for burning CDs and choose an option for creating CDs by burning an ISO image. You find this option in every burning software. In case that you do not find the option, check the manual of your software. With this option you create a bootable Gibraltar CD which starts the computer you use for Gibraltar afterwards. Pay attention to the settings of the BIOS concerning the bootdevices. This CD behaves the same way as a CD you purchase from one of our partners. You can order the license key at our homepage <http://www.gibraltar.at> and we will send it to you via e-mail.

Access to GibADMIN

After starting Gibraltar you can perform the necessary settings with **GibADMIN**. Therefore Gibraltar has assigned itself an IP address (10.0.0.1); so you can reach **GibADMIN** via HTTPS at this address. Presupposed you have a computer in the same network segment (e.g: 10.0.0.50) you can immediately start your web browser and reach **GibADMIN** via <https://10.0.0.1>. If you do not have a computer in the network segment 10.0.0.0/24, install a suitable IP address (e.g. 10.0.0.50) at any computer from which you would like to reach **GibADMIN**. Afterwards you can modify the IP address of Gibraltar so that you can use your common IP addresses. If you don't know exactly, which of your computers' network interface was recognised first and thus has the IP address 10.0.0.1, please try your several network interfaces to find out. Plug the network cable to another network interface in case that you can't connect to the **GibADMIN**. Gibraltar assigns an IP address to every network interface, whereas the first recognised one gets the IP address 10.0.0.1, the second one 10.0.1.1, the third one 10.0.2.1 a.s.o. It goes on like that unless an address is already assigned in the network and can be reached by Gibraltar. While configuring Gibraltar it it's necessary to install your personal license file (by uploading via **GibADMIN**). Thereby the installation becomes complete and you can use the whole periphery of Gibraltar and take the support.

ATTENTION: If the IP address 10.0.0.1 is already used, Gibraltar will search in ascending order until the next available address is found (10.0.0.2, 10.0.0.3, ...).

Why does Gibraltar not start from CD although the CD-ROM is the first boot device?

If your computer does not start Gibraltar you either did not correctly implement the settings in the BIOS, or your computer is not able to start from CD. This can happen with older models. In case that you have checked your BIOS settings and you have ensured that the first boot device is the CD-ROM, but you still can not boot from CD, get the information how to install Gibraltar with boot disks at our homepage <http://www.gibraltar.at>.

5 Licensing

Gibraltar convinces with a unique price-performance ratio. By the large use of OpenSource components and the energetic support of the Debian Community we are able to offer Gibraltar as a professional security product for a very favorable price.

Gibraltar can be bought at the online-shop on our website and of course at one of our Gibraltar partners or resellers. You can get a complete and up-to-date Price list from the manufacturer or

from one of the authorized Gibraltar partners or resellers.

For using a Gibraltar there is a valid activation license. Without a valid license you won't be able to access the Gibraltar-Webinterface and routing won't be done by Gibraltar unless there is no valid license uploaded.

For private users who want to use Gibraltar and his in copyright matters protected tools, there is a free way of licensing up to 5 users.

What are the requirements for using Gibraltar?

Gibraltar is Operating System and Application in one, that means that you need the following components to run Gibraltar:

- **Gibraltar Software:** the ISO-Image is free for download available at our website.
- **Gibraltar license file:** must be acquired. Free for private users.
- **Optional:** License file for anti virus support via Kaspersky Antivirus.
- **Optional:** License file for Content filtering powered by Puresight TM*

Where do I get a Gibraltar license?

- **Private license:** just send an informally e-mail with your name to office@gibraltar.at. The private license is valid up to 5 computers/devices with a IP, in your network.
- **Test license:** a 30 day testing license can be requested at the [Gibraltar Website](#). You will receive the license (in a few minutes) via e-mail.
- **Regular license:** a regular license can be bought at the [Gibraltar Website](#) or via e-mail to the manufacturer.
- **Reduced licenses:** for schools and universities and/or Non profit organizations: plz contact office@gibraltar.at

Gibraltar Security Gateway:

Gibraltar Security Gateways are shipped pre-installed and with a valid license on it. You just need to plug in power and network to your Gibraltar Security Gateway, and you can immediately start configuring.

* Trademark of PureSight Technologies Ltd.

6 The webinterface

After starting Gibraltar from CD you can access **GibADMIN** via web browser (e.g: Microsoft Internet Explorer or Netscape Navigator). By initiation the network interface card gets assigned a standard IP address (https://10.0.0.1), over which the **GibADMIN** is accessible. Therefore you have to put your computer, with which you want to configure Gibraltar into the same network area as Gibraltar. That means to change your IP address, if your network doesn't work with IP address area 10.0.0.0/24 anyway. Assign an IP address (e.g.: 10.0.0.5) to your computer, whereas the last number is variable, if there already exists a computer with the IP address 10.0.0.5 in your network.



NOTE: It can take a few seconds, until the www server of GibADMIN is fully functional.

GibADMIN is separated into the following parts:

- **Title:** In the orange title line you can find the number of your current version of Gibraltar. In the right section of the title the language selection and a few links are located.
 - **Update license:** This link leads you to a form, where you can upload your Gibraltar or Kaspersky license.
 - **Support:** This link leads you to a page from where you can send a message to our support. Fill out every field and try to give an exact description of your problem, so that our support can retrace the problem as fast as possible.
 - **Update:** This link compares your version of Gibraltar with the currently available version. If an update is available you can get it on the Gibraltar homepage (<http://www.gibraltar.at>) if you have purchased a valid license.
 - **Help:** This link leads you to our online help where you can get information about the use of Gibraltar.
 - **Quick-Save:** Click this button to save the current configuration at the default save target with just one click. The default save target you have to set in the module [Configuration management](#) before.
 - **Logout:** This link quits your session with **GibADMIN**.
 - **Language selection:** To change the language, select a language in the select box and confirm with the button **Go!**. After actuating this button the whole **GibADMIN** will be displayed in the favoured language.
- **Main menu:** On the left section you see the main menu where the modules of **GibADMIN** are displayed as links. After clicking such a link you can configure this module in the content section in the middle of **GibADMIN**.
- **Content section:** The content section, the right section, contains the configuration forms of the separate modules. After starting you will come upon the login form primarily. Depending on choice out of the main menu you will be lead to the accordant configuration module.

At the beginning of each **GibADMIN** session the login-desktop will be displayed. You will be asked to enter your username and the accordant password. By first registration put the user "root" therefor and ignore the password. You only have to click **login** to apply for Gibraltar. The first step should be to specify a password for the user "root". The button for changing the password is situated in the menu **System**.

The screenshot shows a browser window titled "Login". Inside the window, there is a form with a "Login" label. Below the label, there are two input fields: "User:" with the text "root" entered, and "Password:". At the bottom of the form, there is a "Login" button.

NOTE: In the title bar of the browser window you can see the host name of the firewall you are configuring actually. So you are able to differentiate between several browser windows when you are dealing with more than one Gibraltar.

7 Practical examples

Hereafter some different, exemplary scenarios are described, in which Gibraltar could be applied as firewall. These are minimum configurations, that should help the network administrator to understand the functionality of Gibraltar. The following instructions can be executed point by point and do not require any knowledge in configuring Gibraltar.

Scenario 1 - ADSL-PPTP Dial-In and DHCP

In this scenario we will configure Gibraltar on a computer which is connected to the Internet by an ADSL-PPTP Internet connection. The public IP address is assigned dynamically. Gibraltar will be configured as gateway of a small local network. The hosts in the internal network will receive their

IP addresses from Gibraltar which will assign the addresses via DHCP. The users of the internal network can use all services of the Internet. There should be no possibility to access the internal network from the outside.

Scenario 2 - Internet Gateway with a static public IP address

This scenario shows the configuration of Gibraltar as an Internet gateway with a static public IP address. Gibraltar should protect the internal network and allow all clients to use any Internet services. The internal network must not be accessible from the Internet. **This scenario is the base of configuring Gibraltar for the most broadband Internet connections.**

Scenario 3 - Internet gateway and usage of a DMZ

In this scenario we will configure Gibraltar to deal with three networks. The internal network will be connected with the Internet through the firewall. The webserver and the mailserver are located in a demilitarized zone (DMZ). The DMZ is a network that is separated from both - internal network and from Internet.

Scenario 4 - Configuring a VPN tunnel between two Gibraltar firewalls

This scenario shows how to connect two Gibraltar firewalls via a IPSec-VPN over the Internet to access the computers at the other side of the tunnel. Additionally it shows the usage of the PPTP VPN service to connect a external worker to the local network. The local Gibraltar LDAP server does the user management.

Scenario 5 - Using Microsoft Active Directory Service and OpenVPN for accessing the network from outside

This scenario shows the connection of Gibraltar to an internal Microsoft Active Directory service. Some of the AD users should be able to use special services with their standard logon username and password. The administrator allows the usage of the special services by defining permissions in the AD security groups. Configuration of OpenVPN for external access of the network.

Scenario 6 - Configuring Gibraltar as application level proxy for http, ftp, and pop3

This scenario shows the usage of Gibraltar as security gateway to protect the internal network from the Internet. Some services are offered as proxy services to avoid direct access of the clients to the Internet. A http proxy to cache the visited sites and optionally filter them for viruses. A ftp proxy to hide the internal network infrastructure from others or to avoid direct access to an internal ftp server from outside. A pop3 proxy that fetches the emails from the external pop3 account and filters them for spam and viruses before they are forwarded to the client.

Scenario 7 - Gibraltar as traffic shaper for Citrix and VoIP bridged

Configuration of Gibraltar as a transparent traffic shaper that can be activated without changing the current network infrastructure. This scenario shows how to ensure the usage of 70 per cent of the bandwidth for the Citrix terminal sessions (protocol ICA). The other services get only 80 per cent of the bandwidth because of latency reasons. To avoid failures and problems it is only allowed to use max. 95 per cent of the bandwidth.

Scenario 8 - Gibraltar as traffic shaper for Citrix and VoIP with VPN

In this scenario we will configure 3 Gibaltars that are connected via IPSEC-VPN. As we are using Citrix Terminalservices we also have to guarantee a minimum of 35 % for the ICA traffic. We also have to guarantee a minimum of 35 % of the traffic for Voice over IP.

Scenario 9 - Gibraltar managing the bandwidth for VoIP

Configuration of Gibraltar as bandwidth manager to ensure a minimal bandwidth for usage with

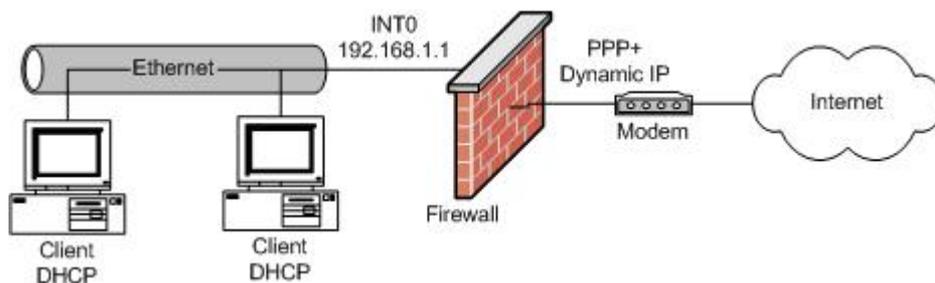
VoIP. The internal telephone system must get a minimum of 1 MBit, if the bandwidth of the Internet connection has 2 MBit up- and download. To avoid failures and problems it is only allowed to use max. 95 per cent of the bandwidth.

Scenario 10 - Gibraltar managing the bandwidth for web traffic

Configuring the Gibraltar Firewall to ensure a minimal bandwidth for web traffic (http, https). Additional a minimal bandwidth for fetching the emails via pop3 is configured.

7.1 ADSL

In this scenario we will configure Gibraltar on a computer which is connected to the Internet via ADSL PPTP. The public IP address is assigned dynamically. Gibraltar will be configured as the gateway of a small local network. The hosts in the internal network will receive their IP addresses via DHCP. The users of the internal network can use all services of the Internet. There should be no access to the internal network from the outside.



System Requirements

Computer with two compatible network interfaces or a Gibraltar Security Gateway and an ADSL PPTP modem.

Note: All stated values are only examples. You have to adapt these values to your individual needs.

Installation of Gibraltar

Please install Gibraltar as described in chapter [Installation](#).

[System configuration](#)

First you must set general system settings.

1. Choose **System** in the main menu.
2. Choose the card **General settings**.
3. **System name:** Enter the desired name of the system in this text field (e.g. "gibraltar").
4. **Domain:** Enter the name of the domain, Gibraltar should be integrated in, in this text field (e.g. "gibraltar.at").
5. **Time zone:** Choose the time zone in which you are running Gibraltar.
6. **Mail of Admin:** Enter the e-mail address of the administrator in this text field. You will receive system messages from Gibraltar on this email address.
7. **Save:** Click this button to save the changes.

[Network settings - Network interface cards](#)

Set the IP addresses of the network interface cards of the Gibraltar firewall. Both the external and the internal network interface get static IP addresses. The external IP address is used for connecting to the ADSL modem of the ISP.

1. Choose **Network** in the main menu.

2. Choose the tab of the interface **eth0**.
3. **Interface:** Enter the name of the network interface card in this text field (e.g. "int0" to be able to define the network card for the intranet explicitly).
4. **Start automatically:** Mark this checkbox to start the network interface automatically, when Gibraltar boots.
5. **IP address:** Choose the option field **static** to allocate the IP address for this network interface statically.
6. **Static IPs:** Change the IP address in the text field **IP address/netmask** ([CIDR-notation](#): e.g. 192.168.0.1/24) to the IP address you intend for Gibraltar.
7. **Save:** Confirm your changes with clicking the button **Save**.
8. Choose the tab of the interface **eth1**.
9. **Interface:** Enter the name of the NIC in this text field (e.g. "ext0" to identify the NIC as external network clearly).
10. **Start automatically:** Mark this checkbox to start the network interface automatically when Gibraltar boots.
11. **IP address:** Choose the option field **static** to allocate the IP address for this NIC statically.
12. **Static IPs:** Change the IP address in the text field **IP address/netmask** to the IP address your ISP told you to connect to the ADSL modem ([CIDR Notation](#): e.g. 10.0.0.140/24).
13. **Save:** Confirm your changes with clicking the button **Save**.

ATTENTION: By changing the IP address on the network card which you use for access to Gibraltar, the connection is interrupted. Please adapt the IP address on your work station computer as well.

Connect your ADSL modem with the interface ext0 of Gibraltar now.

[Network settings - Routing](#)

You do not have to set a configuration on this card, because the settings for the standard route are done with configuring the modem. Please read the information of your ISP carefully. There are many different possibilities to configure ADSL modems correctly.

[Dial-in via PPTP](#)

This section defines the settings for the ADSL PPTP connection. The Gibraltar starts a PPTP connection to the modem to start connecting to the Internet. You need the information you got from your ISP for your ADSL connection.

1. Choose **Network** in the main menu.
2. Choose **Dial-in** in the sub menu.
3. Choose the card **ADSL PPTP**.
4. **Add connection:** Click this button to add a new connection. You will be forwarded to a [detail form](#).
5. **Name:** Enter the name for this connection in this text field. You need the name to identify the connection in the overview of the card **ADSL PPTP**. Therefore the chosen name has to be unique (also from ADSL connections).
6. **IP address of modem:** Please enter here the internal IP address of your modem (e.g. 10.0.0.138).
7. **User name:** Enter the user name your provider set for you in this text field.
8. **Password** and **Password (confirmation):** Enter the password your provider set for you in these text fields.
9. **Start automatically:** Mark this checkbox to start the connection automatically when Gibraltar boots.
10. **Default route:** Mark this checkbox to use this connection as the default route.
11. Set the other options as you are told by your provider or as you need for your personal situation.
12. **Save:** Confirm your changes with clicking the button **Save**.
13. **Start connection** : Click this button to build up the connection to your provider by your modem. If you activate **Dial on demand** the connection will be built up automatically as soon as the client demands an Internet provider.

Firewall rules

This section shows the configuration of the firewall rules. The client computers in the local network get unrestricted access to the Internet. Gibraltar is used as DNS server for the client computers. Therefore we must allow DNS requests from the internal network to Gibraltar.

1. Choose **Firewall** in the main menu.
2. Choose the tab **Firewall rules**.
3. **Interface:** Choose the value "int0" for the network interface card (or the name of your network interface card) from the select box **incoming** and the value "ppp+" for your modem from the select box **outgoing**. Click the button **Go!**. **GibADMIN** now displays all filter rules for the packets that come from the network card "int0" and go to the modem "ppp+". We want to allow all requests in this direction.
4. **Add Rule:** Click this button to add a new rule for this direction ("int0 -> ppp+"). You will be forwarded to a [detail form](#).
5. **Source address:** Choose ANY from the drop down field to allow all source addresses.
6. **Destination address:** Choose ANY from the drop down field to allow all destination addresses.
7. **Comment:** Enter any comment you like. You do not need to configure the other fields for our configuration aim.
8. **Target:** Choose ACCEPT to allow all matching packets.
9. **Save:** Confirm your changes with clicking the button **Save**.
10. **Incoming:** Choose the value "int0".
11. **Outgoing:** Choose the value "local".
12. **Go!:** Click this button, to get displayed the filter rules that handle packets that come from the internal network and are determined locally for the firewall.
13. **Source address:** Choose ANY from the drop down field to allow all source addresses.
14. **Destination address:** Choose ANY from the drop down field to allow all destination addresses.
15. **Service:** Choose "dns" to allow DNS inquiries to the firewall.
16. **Save:** Confirm your changes with clicking the button **Save**.

NAT rules

The outgoing network traffic must be masqueraded with the external IP address.

1. Choose **NAT** in the main menu.
2. Choose the track "outgoing ppp+" from the select box on the tab **NAT rules**, because all packets that leave the firewall via modem have to be disguised with the public IP address.
3. **Add rule:** Click this button to add a new rule. You will be forwarded to a [detail form](#).
4. **Source IP address:** Enter the network address 192.168.0.0/24, because all packets that come from the internal network and leave the firewall via modem have to be altered.
5. **Target:** Choose the value MASQUERADE from this select box because we get the public IP address dynamically and so we can not disguise it with a fix IP address. If you choose MASQUERADE you are not allowed to enter a value in the textfield **--to**.
6. **Save:** Confirm your changes with clicking the button **Save**.

DHCP-Server

Configure the DHCP server for the local network.

1. Choose **Network** in the main menu.
2. Choose **DHCP server** in the sub menu.
3. Choose the card **General settings**.
4. **Domain:** Enter the domain, the DHCP clients should be allocated to in this text field.
5. **Save:** Confirm your changes with clicking the button **Save**.
6. Choose the tab **int0**.
7. **Activate DHCP:** Mark this checkbox to activate DHCP for this network interface.
8. **IP address:** Choose the IP address from the select box by which dynamic IP addresses

- should be allocated (192.168.0.1).
9. **IP-range:** Click the button **Add range** to add a new IP-range.
 10. **From IP:** Enter the first IP address, that should be assigned dynamically in this text field (192.168.0.10).
 11. **To IP:** Enter the last IP address that should be assigned dynamically in this text field (192.168.0.20). Therewith IP addresses from 192.168.0.10 to 192.168.0.20 will be assigned to clients dynamically.
 12. **DNS Server:** Click the button **Add server** to add a DNS server.
 13. **IP address:** Enter the IP address of your DNS server in this text field. As Gibraltar is configured as a DNS server, you can enter 192.168.0.1.
 14. **Router:** Click the button **Add router** to add a router.
 15. **IP address:** Enter the IP address of your router in this text field in the element group Router. As you have configured Gibraltar as a router you can enter 192.168.0.1.
 16. **Save:** Confirm your changes with clicking the button **Save**.

Services

Activate the service DHCP server to start it automatically at boot time or start it right now.

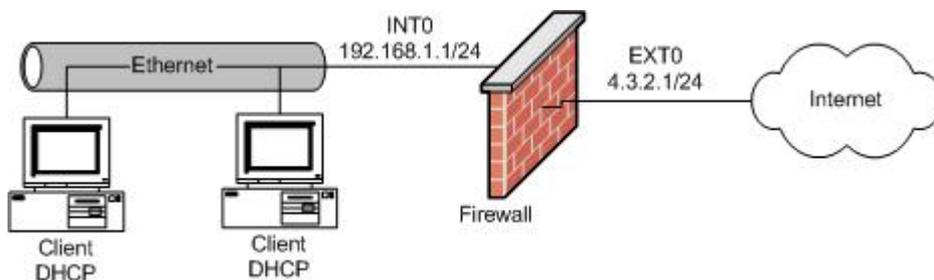
1. Choose **Services** in the main menu.
2. **Available services:** Select the option **On** next to **DHCP server**. Thus the DHCP server will be started automatically, when Gibraltar reboots.
3. **Save:** Confirm your changes with clicking the button **Save**.
4. **Start service** : Click this button next to **DHCP server**, if the DHCP server is not started yet. Thereby the service will start. The state will change to **(started)** and the button to **Stop service** .

Save config

1. Save your configuration on an USB-stick or to the HDD.

7.2 Internet-Gateway

Configuration of Gibraltar as a gateway to the Internet with a static public IP address. Gibraltar should protect the internal network and allow all clients to use any Internet services. There should be no access to the internal network from the outside. This scenario can be used as base configuration for most of the common broadband connections.



System Requirements

Computer with two compatible network interfaces or a Gibraltar Security Gateway. Broadband Internet connection with a static IP address (e.g. XDSL).

Note: All stated values are only examples. You have to adapt these values to your individual needs.

Installation of Gibraltar

Please install Gibraltar as described in chapter [Installation](#).

[System configuration](#)

System configuration as described in [Scenario 1](#).

[Network settings - Network interface cards](#)

Set the IP addresses of the network interface cards of the Gibraltar firewall. Both the external and the internal network interface get static IP addresses.

1. Choose **Network** in the main menu.
2. Choose the tab of the interface **eth0**.
3. **Interface:** Enter the name of the network interface card in this text field (e.g. "int0" to be able to define the network card for the intranet explicitly).
4. **Start automatically:** Mark this checkbox to start the network interface automatically, when Gibraltar boots.
5. **IP address:** Choose the option field **static** to allocate the IP address for this network interface statically.
6. **Static IPs:** Change the IP address in the text field **IP address/netmask** ([CIDR-notation](#): e.g. 192.168.0.1/24) to the IP address you intend for Gibraltar.
7. **Save:** Confirm your changes with clicking the button **Save**.
8. Choose the tab of the interface **eth1**.
9. **Interface:** Enter the name of the NIC in this text field (e.g. "ext0" to identify the NIC as external network clearly).
10. **Start automatically:** Mark this checkbox to start the network interface automatically when Gibraltar boots.
11. **IP address:** Choose the option field **static** to allocate the IP address for this NIC statically.
12. **Static IPs:** Change the IP address in the text field **IP address/netmask** to the IP address your ISP told you to connect to the ADSL modem ([CIDR Notation](#): e.g. 4.3.2.1/30).
13. **Save:** Confirm your changes with clicking the button **Save**.

ATTENTION: By changing the IP address on the network card which you use for access to Gibraltar, the connection is interrupted. Please adapt the IP address on your work station computer as well.

[Network settings - Routing](#)

Configuration of the default route (standard gateway).

1. Choose **Network** in the main menu.
2. Choose the card **Routing**.
3. **Default route:** Enter the default route in this text field. You get the value for the default route from your provider.
4. **Save:** Confirm your changes with clicking the button **Save**.

[Firewall rules](#)

This section shows the configuration of the firewall rules. The client computers in the local network get unrestricted access to the Internet. Gibraltar is used as DNS server for the client computers. Therefore we must allow DNS requests from the internal network to Gibraltar.

1. Choose **Firewall** in the main menu.
2. **Interface:** Choose the value "int0" from the select box **incoming** for the internal network interface and the value "ext0" from the select box **outgoing** for the external network interface. Click the button **Go!**. **GibADMIN** now displays all filter rules for the packets that come from the network interface "int0" and go to the network interface "ext0". We want to allow all requests in this direction.
3. **Add rule:** Click this button to add a new rule for this direction ("int0 -> ext0"). You will be

- forwarded to a [detail form](#).
4. **Source:** Choose ANY from the selection box to allow all source addresses.
 5. **Destination:** Choose ANY from the selection box to allow all destination addresses.
 6. **Comment:** Enter a comment about the rule. You do not have to configure the other fields in this case.
 7. **Save:** Confirm your changes with clicking the button **Save**.
 8. **Incoming:** Choose the value "int0".
 9. **Outgoing:** Choose the value "local".
 10. **Go!:** Click this button. Now GibADMIN displays all filter rules for the packets that come from "int0" and are determined locally for the firewall.
 11. **Source:** Choose ANY from the selection box to allow all source addresses.
 12. **Destination:** Choose ANY from the selection box to allow all destination addresses.
 13. **Service:** Choose "dns" to allow DNS requests to Gibraltar.
 14. **Save:** Confirm your changes with clicking the button **Save**.

NAT rules

The outgoing network traffic must be masqueraded with the external IP address.

1. Choose **NAT** in the main menu.
2. **Track:** Choose "outgoing ext0" from the selective list on the card **NAT rules**, because all packets that leave the firewall via network interface "ext0" have to be disguised with the public IP address.
3. **Add rule:** Click this button to add a new rule. You will be redirected to a [detail form](#).
4. **Source IP address:** Enter the value 192.168.0.0/24 because all packets that come from the internal network and leave the firewall by the external network interface card have to be disguised.
5. **Target:** Choose the value "SNAT" from this select box, because the source IP address has to be disguised with your fix, public IP address.
6. **--to:** Enter your public IP address you got from your provider (e.g. 4.3.2.1). Thereby all packets that go from the internal network to outside are disguised with this IP address.
7. **Save:** Confirm your changes with clicking the button **Save**.

DHCP server

DHCP server settings as described in [scenario 1](#).

Services

Activate the service DHCP server as shown in [scenario 1](#).

Save config

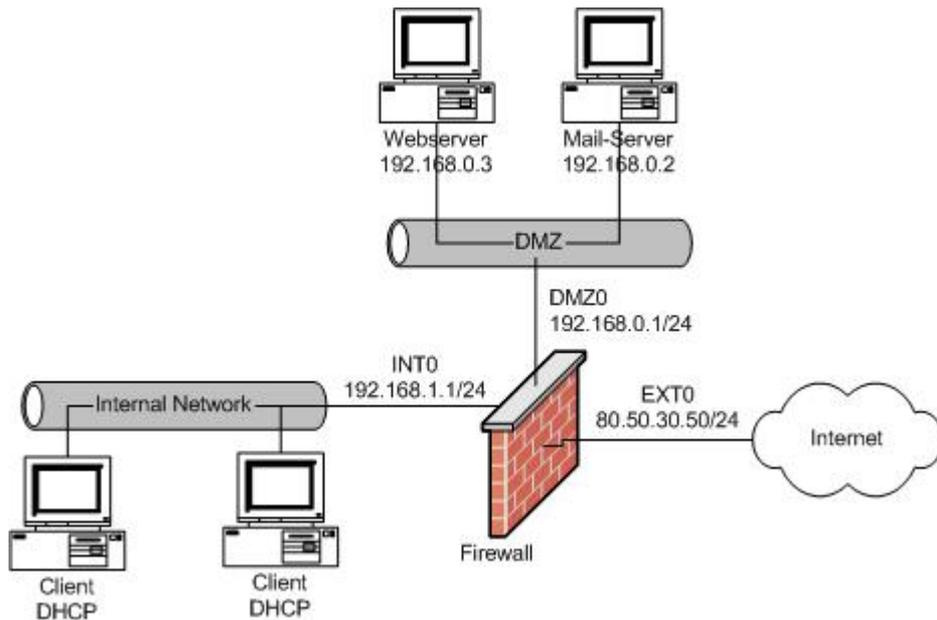
1. Save your configuration on an USB-stick or to the HDD.

With these settings your Gibraltar firewall is configured and the client computers should have unrestricted access to the Internet.

7.3 Firewall und DMZ

Configuration of Gibraltar as gateway to the Internet and definition of a DMZ (demilitarized zone). A webserver and a mailserver are located in a demilitarized zone (DMZ). The firewall needs three network interfaces with the following names:

- **int0** for the internal network
- **dmz0** for the DMZ
- **ext0** for the Internet



System Requirements

Computer with three compatible network interface cards or a Gibraltar Security Gateway.
Broadband Internet connection.

Note: All stated values are only examples. You have to adapt these values to your individual needs.

Installation of Gibraltar

Please install Gibraltar as described in chapter [Installation](#).

[System configuration](#)

System configuration as described in [Scenario 1](#).

[Network settings - Network interface cards](#)

1. Choose **Network** in the main menu.
2. Choose the tab of the interface **eth0**.
3. **Interface:** Enter in this text field the desired name of the network interface card (e.g. "ext0" for the network interface card to the Internet).
4. **Start automatically:** Mark this checkbox to start the network interface automatically when Gibraltar boots.
5. **IP address:** Choose the option field **static** to allocate the IP address for this network interface statically.
6. **Static IPs:** Change the IP address in the text field **IP address/netmask** to the IP address you intend for Gibraltar ([CIDR-notation](#) e.g. 80.50.30.50/24).
7. **Save:** Confirm your changes with clicking the button **Save**.
8. Choose the tab of the interface **eth1**.
9. **Interface:** Enter the name you want for this network interface in this text field (e.g. "int0" for the network interface to the internal network)
10. **Start automatically:** Mark this checkbox to start the network interface card automatically when Gibraltar boots.
11. **IP address:** Choose the option field **static** to allocate the IP address for this network interface card statically.
12. **Static IPs:** Change the IP address in the text field **IP address/netmask** to the IP address you intend for Gibraltar ([CIDR-notation](#) e.g. 192.168.1.1/24).
13. **Save:** Confirm your changes with clicking the button **Save**.

14. Choose the tab of the interface **eth2**.
15. **Interface:** Enter the name you want for this network interface in this text field (e.g. "dmz0" for the network interface that involves the DMZ).
16. **Start automatically:** Mark this checkbox to start the network interface card automatically when Gibraltar boots.
17. **IP address:** Choose the option field **static** to allocate the IP address for this network interface card statically.
18. **Static IPs:** Change the IP address in the text field **IP address/netmask** to the IP address you intend for Gibraltar ([CIDR-notation](#) e.g. 192.168.0.1/24).
19. **Save:** Confirm your changes with clicking the button **Save**.

Now the internal network covers the network address area 192.168.1.0/24 and the DMZ covers the network address area 192.168.0.0/24. Therefore you have to configure the routing so that you can reach the Internet and the DMZ via the firewall.

ATTENTION: By changing the IP address on the network card which you use for access to Gibraltar, the connection is interrupted. Please adapt the IP address on your work station computer as well.

[Network settings - Routing](#)

1. Choose **Network** in the main menu.
2. Choose the tab **Routing**.
3. **Default route:** Enter the standard route you get from your provider in this textfield. All packets that are not determined for other networks will be forwarded to this IP address.
4. **Save:** Confirm your changes with clicking the button **Save**.

Now we have to set the filter rules to allow the packets the way to the Internet or to the server. The default policy is that no traffic can pass the firewall. Only packets that you allow explicitly can pass the firewall. We want to allow the traffic from the internal network to the Internet. Our employees should also be able to get the e-mails from the mailservers in the DMZ via POP3. Furthermore they are allowed to use the webserver.

[Firewall rules](#)

1. Choose **Firewall** in the main menu.
2. Choose the tab **Firewall rules**.
3. **Incoming:** Choose the value "int0" from this select box.
4. **Outgoing:** Choose the value "ext0" from this select box.
5. **Go!:** Click this button to show the rules for packets that are determined to go the way "int0 -> ext0".
6. **Add rule:** Click this button to add a new rule that allows packets from the internal network to the Internet. The browser will redirect you to a [detail form](#).
7. **Service:** Choose ANY from the select box.
8. **Source:** Choose ANY from the selection box to allow all source addresses.
6. **Destination:** Choose ANY from the selection box to allow all destination addresses.
9. **Save:** Keep the default settings of the rule to allow all packets from the internal network to the Internet. Click the button **Save**.
10. **Incoming:** Leave the value of the incoming interface at "int0".
11. **Outgoing:** Choose the value "dmz0" from this select box.
12. **Go!:** Click this button to show the rules for packets that go the way "int0" -> "dmz0".
13. **Add Rule:** Click this button to add a new rule that allows packets from "int0" to "dmz0".
14. **Service:** Choose the value "pop3".
16. **Source:** Choose ANY from the selection box to allow all source addresses.
17. **Destination:** Choose ANY from the selection box to allow all destination addresses.
18. **Save:** Leave all fields in the default settings in the following detail form.
19. **Add another rule:** Click this button to add a further rule.
20. **Service:** Choose the value "http".
21. **Source:** Choose ANY from the selection box to allow all source addresses.
22. **Destination:** Choose ANY from the selection box to allow all destination addresses.
23. **Save:** Confirm your changes with clicking the button **Save**. So you can request your mails on

the mailserv in the DMZ from the internal network and also access the webserver in the DMZ.

The firewall acts as a mail relay that relays the incoming mails via SMTP to the mailserv in the DMZ. Therefore you have to allow SMTP packets to pass the firewall.

1. Choose **Firewall** in the main menu.
2. Choose the tab **Firewall rules**.
3. **Incoming:** Choose "ext0" as incoming interface.
4. **Outgoing:** Choose "local" as outgoing interface.
5. **Go!:** Click this button to show the rules for packets that come from outside ("ext0") to the firewall.
6. **Add Rule:** Click this button to add a new rule. The browser will redirect you to a [detail form](#).
7. **Service:** Choose the value "smtp".
8. **Source:** Choose ANY from the selection box to allow all source addresses.
9. **Destination:** Choose ANY from the selection box to allow all destination addresses.
10. **Target:** This selection box keeps its value ("ACCEPT").
11. **Save:** Confirm your changes with clicking the button **Save**.

To send e-mails via Gibraltar, also the SMTP port from the internal network to the firewall has to be accessible.

Repeat the prior operation with the incoming interface "int0" and the outgoing interface "local". Additionally restrict the source IP address to the ones of the internal network by entering 192.168.1.0/24 in the textfield Source IP address.

DNS requests to the local DNS server on Gibraltar should also be possible. Add a rule for the incoming interface "int0" and the outgoing interface "local" as well as for the incoming interface "dmz0" and the outgoing interface "local" that allows packets for the service "dns".

The mail server in the DMZ sends emails to the SMTP server on Gibraltar. So you have to add a rule for the incoming interface "dmz0" to the outgoing interface "local" that allows TCP packets on the service "smtp".

For the correct forwarding of the packets in the Internet, the internal addresses have to be masqueraded with the public IP address as source IP address, when they go through the firewall (NAT).

Also inquiries to the HTTP port (80) of the firewall have to be forwarded to the webserver in the DMZ. This settings are done in the NAT module.

[NAT - rules](#)

1. Choose **NAT** in the main menu.
2. Choose the card **NAT rules**.
3. **Track:** Choose "outgoing ext0" from this select box, because all packets that leave the firewall via modem have to be masqueraded with the public IP address.
4. **Add rule:** Click this button to add a NAT rule. The browser will redirect to a [detail form](#).
5. **Source IP address:** Enter the value 192.168.1.0/24 because all packets that come from the internal network and leave the firewall via "ext0" have to be masqueraded with a new source IP address.
6. **Target:** Leave the value "SNAT" in this select box because the source IP address should be masqueraded with public IP address we know.
7. **--to:** Enter the new source IP address (in our case: 80.50.30.50).
8. **Save:** Confirm your changes with clicking the button **Save**.

Repeat this operation for the source IP address 192.168.0.0/24 because also packets from the DMZ have to be masqueraded.

To relay requests from the port 80 of the firewall to the webserver in the DMZ we have to do the following settings:

1. Choose **NAT** in the main menu.
2. Choose the tab **NAT rules**.
3. **Track:** Choose "incoming ext0" from this select box to masquerade the outgoing packets.

4. **Add rule:** Click this button to add a new NAT rule. The browser will redirect to a [detail form](#).
5. **Dest. IP address:** Enter the value 80.50.30.50 in this text field as the inquiries arrive at the IP address of the firewall.
6. **Service:** Choose the value "http" from the selection box.
7. **Target:** Leave the value "DNAT" because the destination address has to be changed.
8. **--to:** Enter the new destination IP (in our case: 192.168.0.3).
9. **Save:** Confirm your changes with clicking the button **Save**.

Now the destination IP address of HTTP packets has changed to the address of the WWW server (192.168.0.3). In order that the packets arrive at the WWW server, we have to add a packet filter rule in the module Firewall. This rule will allow HTTP packets to get into the DMZ from outside.

1. Choose **Firewall** in the main menu.
2. Choose the tab **Firewall rules**.
3. **Incoming:** Choose the value "ext0" from this select box.
4. **Outgoing:** Choose the value "dmz0" from this select box.
5. **Go!:** Click this button to show the rules for packets that go the way "ext0" -> "dmz0".
6. **Add Rule:** Click this button to add a new rule. The browser will redirect to a [detail form](#) where you can configure the rule.
7. **Dest. IP address:** Enter the IP address of the webserver in this text field (192.168.0.3).
8. **Service:** Choose the value "http".
9. **Target:** Leave the value "ACCEPT".
10. **Save:** Confirm your changes with clicking the button **Save**.

[Configuration of the mail relaying](#)

The mail relay receives e-mails and relays them to your mail server in the DMZ. Therefore the mail server cannot be accessed directly from the Internet and thus it is more secured from attacks. To forward incoming e-mails to the internal e-mail server, please act as follows:

1. Choose **Mail** in the main menu.
2. Choose the tab **Relay incoming**.
3. **Managed Domains:** Enter the domains you administrate on your mail servers in this element group.
4. **Add server:** Click this button to add a server to this list.
5. **Domain:** Enter the name of the domain you want to administrate in this text field (e.g. "esys.at").
6. **Mailserver IP address:** Enter the IP address of the mail server that manages the mails for the stated domain (e.g. 192.168.0.2).
7. **Save:** Confirm your changes with clicking the button **Save**.
8. Choose the tab **General settings**.
9. **Activate virus and spam checks:** Activate this option to check your e-mails for viruses and spam.
10. **Scan e-mails for:** Activate the domain you want to check for viruses and spam.
11. **Save:** Confirm your changes with clicking the button **Save**.

To adjust the settings for the mail relay to outside, please act as follows:

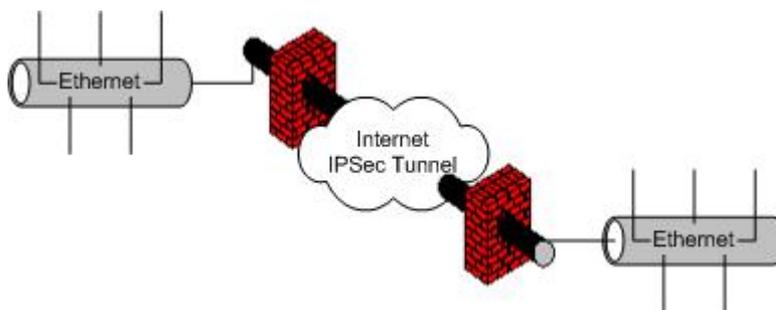
1. Choose **Mail** in the main menu.
2. Choose the tab **Relay outgoing**.
3. **Local networks:** Click the button **Add network address** to add a new network address. All networks in this list are allowed to send e-mails. Keep the setting 127.0.0.1/8 because Gibraltar also sends e-mails to the administrator.
4. **Network address:** Enter the value 192.168.1.0/24 to allow your clients from the internal network to send e-mails. Enter furthermore the value 192.168.0.0/24, because e-mails are also sent from the DMZ .
5. **Save:** Confirm your changes with clicking the button **Save**.

[Save config](#)

1. Save your configuration on an USB-stick or to HDD.

7.4 IPSec VPN

Configuration of two Gibraltar Firewalls to connect two networks via an IPSec VPN tunnel. Additionally this scenario shows the configuration of PPTP to connect external workers with the LAN. The local Gibraltar LDAP server does the user administration.



System Requirements

Computer with two compatible network interfaces or two Gibraltar Security Gateways. Broadband Internet connection with static public IP addresses.

Note: All stated values are only examples. You have to adapt these values to your individual needs.

Installation of Gibraltar

Please install Gibraltar as described in chapter [Installation](#).

[System configuration](#)

System configuration as described in [Scenario 1](#).

[Network settings - Network interface cards](#)

Network and routing configuration as described in [Scenario 2](#)

ATTENTION: By changing the IP address on the network card which you use for access to Gibraltar, the connection is interrupted. Please adapt the IP address on your work station computer as well.

[Set default route](#)

1. Choose the tab **Routing**.
2. **Default route:** Enter the default route in this textfield. You get the value for the default route from your provider. All packets, that are not determined to be forwarded to other networks will be forwarded to this address.
3. **Save:** Confirm your changes with clicking the button **Save**.

[Firewall rules](#)

Firewall rules as described in [Scenario 2](#)

[NAT rules](#)

NAT rules as described in [Scenario 2](#)

[Connect a remote computer with the internal network via PPTP](#)

1. Choose **VPN** in the main menu.
2. Choose **PPTP**.
3. Choose the tab **General settings**.
4. **Local IP (with netmask)**: Enter the IP address with which the remote computer contacts the internal network. This IP address has to be in the internal network (e.g. 192.168.1.100/24). Please also indicate a netmask.
5. **Remote IP from**: Enter the first IP address of a range of IP addresses. A remote user will get assigned an IP address of this range (e.g: 192.168.1.211).
6. **Remote IP to**: Enter the last IP address of the range of IP addresses. A remote user will get assigned an IP address of this range (e.g: 192.168.1.220). Because of setting the range 192.168.1.211 - 192.168.1.220, 10 IP addresses can be used for remote users.
7. **Domain**: Enter the domain the remote user should be assigned to in this textfield.
8. **DNS server**: Enter the DNS server. By default this is Gibraltar.
9. **WINS server**: Enter the WINS server, the remote user should use (you can also leave this field blank).
10. **Save**: Confirm your changes with clicking the button **Save**.

[PPTP remote user](#)

1. Choose **User** in the main menu.
2. You will be forwarded automatically to the tab **LDAP Settings**.
3. Choose **local OpenLDAP** in the drop down field and start the LDAP service at the same tab afterwards.
4. Choose the tab **User**.
5. Add a new user by setting username and password and activate the checkbox **VPN**.
6. **Save**: Confirm your changes with clicking the button **Save**.

[Setting filter rules for the PPTP access](#)

1. Choose **Firewall** in the main menu.
2. Choose the tab **Firewall rules**.
3. **Incoming**: Choose "ext0" as incoming interface.
4. **Outgoing**: Choose "local" as outgoing interface.
5. **Go!**: Click this button to get displayed all filter rules for the packets that come from "ext0" and go to "local".
6. **Add Rule**: Click this button to add a new rule.
7. **Service**: Choose the value "pptp".
8. **Source**: Choose ANY from the selection box to allow all source addresses.
9. **Destination**: Choose ANY from the selection box to allow all destination addresses.
10. **Save**: Confirm your changes with clicking the button **Save**.

To allow the remote users to connect to the network behind the firewall you have to define additional rules. These rules have to forward the data traffic from the PPTP dial-in to the internal network.

1. Choose the tab **Firewall rules**.
2. **Incoming**: Choose "ppp+" as incoming interface.
3. **Outgoing**: Choose "int0" as outgoing interface.
4. **Go!**: Click this button to get displayed all filter rules for the packets that come from "ppp+" and go to "int0".
5. **Add Rule**: Click this button to add a new rule.
6. **Source**: Choose ANY from the selection box to allow all source addresses.
7. **Destination**: Choose ANY from the selection box to allow all destination addresses.
8. **Service**: Choose ANY from the selection box.
9. **Save**: Confirm your changes with clicking the button **Save**.

Starting the PPTP server

1. Choose **Services** in the main menu.
2. **Available services:** Select the option **On** next to **PPTP**. The PPTP server will be started automatically when Gibraltar boots.
3. **Save:** Confirm your changes with clicking the button **Save**.
4. **Start service** : Click this button next to **PPTP**, if the PPTP server is not started. Thereby the service will be started. The state will change to **(started)** and the button to **Stop service** .

Thereby the access via PPTP is set and the remote user can log in to the internal network with his registration data.

For the setting of the IPsec tunnel we use two Gibraltar firewalls ("gibraltar1" and "gibraltar2").

Starting the IPsec service

1. Choose **Services** in the main menu.
2. **Available services:** Select the option **On** next to **IPsec**. The IPsec service will be started automatically when Gibraltar boots.
3. **Save:** Confirm your changes with clicking the button **Save**.
4. **Start service** : Click this button next to **IPsec**, if the IPsec service is not started. Thereby the service will be started. The state will change to **(started)** and the button to **Stop service** .

IPsec

1. Choose **IPsec** in the main menu.
2. Choose the tab **General settings**.
3. **Activate for IPsec:** Activate the checkboxes of the network interface cards, on which you want IPsec to be activated (e.g "ext0").
4. **Save:** Confirm your changes with clicking the button **Save**.

Download certificate

To disclose the certificate at the remote station, you have to download it and upload it at your remote firewall. Therefore we use the Gibraltar firewalls "gibraltar1" and "gibraltar2".

1. Choose **VPN** in the main menu of "gibraltar1".
2. Choose **Certificates** in the sub menu.
3. **Host certificates:** In this element group the self-created certificates and the uploaded certificates from the remote firewalls are shown.
4. **Download certificate** : Click this button to download the certificate ("gibraltar.pem"). You have to enter a storage-destination. Change the name of the certificate, so that thereafter you can definitively identify it as a certificate of this firewall (e.g. "gibraltar1Cert.pem"). Afterwards you have to upload this certificate at the remote computer.
5. Change to the other firewall "gibraltar2", log in and upload the certificate "gibraltar1Cert" in the element group **Host certificates**.
6. Download the certificate "gibraltar.pem" from the firewall "gibraltar2" and upload it at the firewall "gibraltar1" in the element group **Host certificates** after you renamed it (e.g. "gibraltar2Cert").

Therewith every firewall has the certificate of the remote station now, and you can start to configure the tunnels.

Configure an IPsec tunnel

1. Choose **VPN** in the main menu of "gibraltar1".
2. Choose **IPSec** in the sub menu.
3. Choose the tab **Tunnel**.
4. **Add Tunnel:** Click this button to add a new tunnel.
5. **Name:** Enter a name for the tunnel (e.g. "gib1Tunnel").
6. **State after start:** Choose the state the tunnel should have after a restart of the IPSec service (e.g. "(standby)").
7. **Local IP:** Choose the IP address of "gibraltar1" through which the tunnel should go. Note that only those IP addresses of the network interface cards can be chosen which were activated for IPSec in the card **General settings**. If you want to connect two locations, you should take the public IP address.
8. **Local subnet:** Enter the local subnet here if it should be accessible over the IPSec tunnel.
9. **Local certificate:** Choose the certificate you created before ("gibraltar1Cert").
10. **Remote IP address:** Enter the IP address of the remote firewall (the public IP address of "gibraltar2").
11. **Remote Subnet:** Enter the subnet of the remote network if you want it to be accessible over the tunnel.
12. **Authorization:** Choose a variant for authorization (in this case X.509). Choose the certificate of the remote firewall in the select box ("gibraltar2Cert").
13. **Save:** Click this button to save the changes. You will be redirected to the overview.
14. Change to firewall "gibraltar2" and create a tunnel "gib2Tunnel" that ends in the IP address of the firewall "gibraltar1".

Starting/Stopping the IPSec tunnel

1. **Starting IPSec tunnel** : Click this button to start the tunnel if the current state is **(deactivated)** or **(standby)**.
2. **Activate IPSec tunnel (standby mode)** : Click this button to set the tunnel to the standby mode if the current state is **(deactivated)**.
3. **Stopping IPSec tunnel (standby mode)** : Click this button to set the tunnel to the standby mode if the current state is **(started)**.
4. **Deactivate IPSec tunnel** : Click this button to deactivate the IPSec tunnel, if the current state is **(standby)** or **(started)**.

Setting filter rules for the IPSec tunnel

To allow the remote users to reach the network behind the firewall you have to set additionally filter rules for the IPSec tunnel. These rules forward the traffic from the IPSec tunnel to the internal network (FORWARDING rules).

1. Choose **Firewall** in the main menu.
2. Choose the tab **Firewall rules**.
3. **Incoming:** Choose "ipsec0" as incoming interface.
4. **Outgoing:** Choose "int0" as outgoing interface.
5. **Go!:** Click this button to get displayed all filter rules for the packets that come from "ipsec0" and go to "int0".
6. **Add Rule:** Click this button to add a new rule.
7. **Service:** Choose ANY from the selection box.
8. **Source:** Choose ANY from the selection box to allow all source addresses.
9. **Destination:** Choose ANY from the selection box to allow all destination addresses.
10. **Save:** Confirm your changes with clicking the button **Save**.
11. **Incoming:** Choose "int0" as incoming interface.
12. **Outgoing:** Choose "ipsec0" as outgoing interface.
13. **Go!:** Click this button to get displayed all filter rules for the packets that come from "int0" and go to "ipsec0".
14. **Add Rule:** Click this button to add a new rule.
15. **Service:** Choose ANY from the selection box.
16. **Source:** Choose ANY from the selection box to allow all source addresses.

17. **Destination:** Choose ANY from the selection box to allow all destination addresses.
18. **Save:** Confirm your changes with clicking the button **Save**.

[Save config](#)

1. Save your configuration on an USB-stick.

7.5 Active Directory

Configuration of Gibraltar in combination with a Microsoft Windows Active Directory. Some of the Active Directory users should be able to use some special services by using their common username and password. Active Directory Organisational Units can manage the access to those services. Configuration of OpenVPN for remote access.

- **HTTP-Proxy** to secure HTTP traffic
- **SMTP authentication** to allow external users to send emails by using the Gibraltar firewall
- **OpenVPN** for secure remote access to the LAN

The Active Directory domain is configured as follows:

- Domain name "**company.local**"
- Organisational unit for the user communicating with Gibraltar:
company.local/company/Users
- Login name of the AD user: "**gibuser**"
- OU for the groups to handle the access to specific services:
company.local/company/Groups
- A domain local group "**dl_http**" in the OU "company.local/company/Groups" to handle the access to the http proxy.
- A domain local group "**dl_smtp**" in the OU "company.local/company/Groups" to handle the access to the smtp authentication.
- A domain local group "**dl_vpn**" in the OU "company.local/company/Groups" to handle the access to the usage of VPN.
- Internal network: **192.168.0.0/24**
- External IP: **1.1.1.1**

Note: All stated values are only examples. You have to adapt these values to your individual needs.

System Requirements

Computer with two compatible network interfaces or Gibraltar Security Gateway.

Installation of Gibraltar

Please install Gibraltar as described in chapter [Installation](#).

[System configuration](#)

System configuration as described in [Scenario 1](#).

[Network settings - Network interface cards](#)

Network and routing configuration as described in [Scenario 2](#)

ATTENTION: By changing the IP address on the network card which you use for access to Gibraltar, the connection is interrupted. Please adapt the IP address on your work station computer as well.

[Firewall rules](#)

Firewall rules as described in [Scenario 2](#)

[NAT rules](#)

NAT rules as described in [Scenario 2](#)

Integration into Microsofts Active Directory

The Gibraltar firewall must be integrated into the Active Directory to allow the usage of the common Windows Logins. Please follow the steps below:

1. Choose **User** in the main menu.
2. You will be forwarded automatically to the tab **LDAP Settings**.
3. **Server**: Choose "Active Directory"
4. **IP Domaincontroller**: Enter the IP address of the domain controller.
5. **AD user**: Enter name of the AD user ("gibuser"). This user does **not** need administrator privileges because she is only needed for communication with the AD.
6. **AD user password**: Enter the password of the user "gibuser" and confirm it in the next text field.
7. **Organizational Unit AD users**: Enter the OU of the AD user ("ou=users,ou=company").
8. **Organizational Unit AD Groups**: Enter the OU of the AD groups ("ou=groups,ou=company").
9. **Domain**: Enter the FQDN of the internal Windows domain ("company.local").
10. **Save**: Confirm your changes with clicking the button **Save**.
11. **Enter Domain**: Click this button to enter the Active Directory Domain.
12. **Domain Administrator**: Enter the name of a Windows Domain Administrator to join the domain.
13. **Password**: Enter the password of the Domain Administrator.
14. **Enter Domain**: Click this button to enter the Active Directory Domain.
15. **Select AD groups**: Click this button to select the Active directory groups that handle the access to the specified services. All groups within the OU "ou=groups,ou=company" are listed.
16. **VPN Group**: Choose the group "dl_vpn".
17. **HTTP-Proxy Group**: Choose the group "dl_http".
18. **Mail Group**: Choose the group "dl_mail".
19. **Save**: Confirm your changes with clicking the button **Save**.
20. Add the users to the specified groups by using the Active Directory Snap-In at the Windows Domain Controller.

[HTTP-Proxy](#)

1. Choose **Proxy Server** in the main menu.
2. Choose **HTTP Proxy** in the sub menu.
3. Choose the tab **Proxy Cache**.
4. **RAM for proxy (in MB)**: This value defines the usage of RAM for caching objects. Do not change it, if you are not sure what consequences it will have. The RAM for proxy caching cannot be used by other services.
5. **Maximum size of an object (in KB)**: This value limits the size of the objects stored into the cache.
6. **Use disk cache**: Activate this checkbox if you are using a HDD and if you want to use the disk cache.
7. **Size of disk cache (in MB)**: Enter the size of the disk cache you want to be reserved for caching objects.
8. **Save**: Confirm your changes with clicking the button **Save**.
9. Choose the tab **Authentication**.
10. **Authentication method**: Choose the value "Authentication via LDAP".
11. **Save**: Confirm your changes with clicking the button **Save**.
12. Choose the tab **Content Filter**.
13. **Kaspersky Anti-Virus**: Activate this checkbox if you want to check your HTTP traffic and you bought a Kaspersky license key.

14. **Save**: Confirm your changes with clicking the button **Save**.
15. Add a new firewall rule to allow the traffic on TCP-port 3128 from incoming int to outgoing LOCAL.
16. Start the service **HTTP-Proxy** at the module **services** and change the value of starting the service automatically if you want.

Note: The HTTP-Proxy must be configured at the Internet browsers of the clients. Otherwise it will not be used. Group policies are the best method to publish these settings. The users can now connect to the Internet by using their common login information.

Mail Authentication

1. Choose **Mail** at the main menu.
2. Choose the tab **SMTP user authentication**.
3. **Use Authentication**: Activate the checkbox to use the authentication.
4. **Save**: Confirm your changes with clicking the button **Save**.
5. Add a new firewall rule to allow traffic at TCP port 25 from incoming ext to outgoing LOCAL. This rule allows sending mails from external to the mail relay at the firewall.
6. Start the service Mailserver to activate the settings and change the automatic start method to "On" if you want to start the service after rebooting.

Configure the mail clients of your users to use the Gibraltar SMTP service for sending mails now. Please be aware that you must configure a secure connection (SSL). "Extended account options" at MS Outlook Express for example.

Creating a Client Certificate

OpenVPN uses client certificates for user authentication. These certificates should be stored to the Active Directory. Therefore you must set privileges for the scheme for the user "gibuser". Login to the Domain Controller as Scheme Administrator and enter the following line:

```
dscls ou=Users,ou=company,dc=company,dc=local /I:S /G "company\gibuser:RPWP;userPKCS12;user"
```

Follow the lines below to create a client certificate:

1. Choose **VPN** at the main menu.
2. Choose **Certificate** at the sub menu.
3. **Generate client cert**: Click this button to generate a new client certificate.
4. Fill in reasonable values into the text fields and choose the **owner** out of the drop down list of the Active Directory users. Note the password, because the user will need it to start the remote connection via OpenVPN.
5. Save the new certificate to your desktop.

Configuring the OpenVPN service

1. Choose VPN at the main menu.
2. Choose OpenVPN at the sub menu.
3. Listen on IP: Choose your public IP address out of the list ("1.1.1.1").
4. Routed networks: Enter the internal network(s) address which should be reachable through the VPN tunnel ("192.168.0.0/24").
5. **Save**: Confirm your changes with clicking the button **Save**.
6. Add a new firewall rule to allow traffic from incoming **tun+** (virtual interface used by OpenVPN) to outgoing **int**.
7. Start the Service **OpenVPN** at the module **Services**.

Installing the Windows Client

To use OpenVPN with Microsoft Windows Clients you must install a client software which can be downloaded at <http://openvpn.se/>.

After booting Windows you can see a small icon on the right side beside the clock of your task bar.

Follow the steps below to configure your OpenVPN client software correctly.

1. Copy the downloaded certificate to the directory "C:\Program files\openvpn\config".
2. Choose **VPN** at the main menu.
3. Choose **OpenVPN** at the sub menu.
4. **Download client config:** Click this button to download the client configuration file client.ovpn and save it to the same directory as the certificate.
5. Start the OpenVPN connection by using the right button of your mouse and enter the password you chose at the creation of your certificate.

When the connection is started the remote user can access the resources in the local area network.

Active Directory Groups

Now you can add new users to the specific groups to allow access to the services. For example add "user1" to the group "dl_http" to allow the HTTP-Proxy.

NOTE: To increase the performance the authentication data is cached at the Gibraltar firewall. If you remove a user from a group, the new settings will be active after an hour. Restart the HTTP Proxy service to speed up this settings.

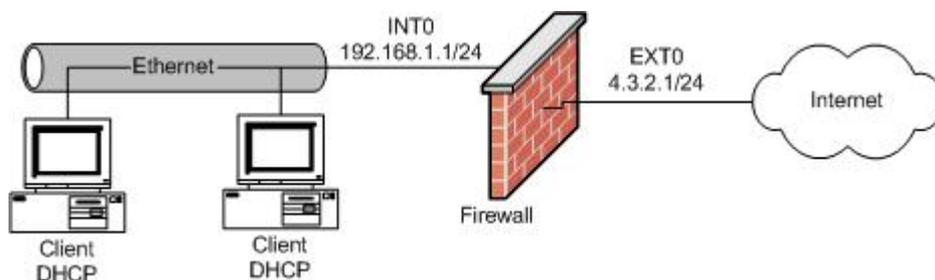
Saving configuration

1. Save the configuration to your default storage destination and save a backup to a USB stick.

7.6 Proxy Server

In this scenario we will configure Gibraltar on a computer with two network interface cards. One of them is used for the Internet connection, the other one is used for the connection to the internal network. Gibraltar should protect the internal network and allow all clients to use any Internet services. The internal network must not be accessible from the Internet. Furthermore proxy-servers should be installed. An HTTP proxy, to cache queried homepages on the hard disk and therewith make an anew query faster. An FTP proxy, to either receive inquiries from the internal network and therewith veil the topology or to receive inquiries from outside and pass them on to an internal FTP server. Also a POP3 proxy has to be configured, that takes on queries of clients in the internal network and checks the answer mails for viruses and spam when it fetches them from the external pigeon hole.

Note: This scenario shows a simple configuration of the services. For detailed information, please consult the specific modules.



Note: All shown values are only examples. You must adapt these values to your individual needs.

System Requirements

Computer with two compatible network interfaces or Gibraltar Security Gateway.

Installation of Gibraltar

Please install Gibraltar as described in chapter [Installation](#).

[System configuration](#)

System configuration as described in [Scenario 1](#).

[System configuration - hard disk](#)

1. Choose **System** in the main menu.
2. Choose the tab **Configure hard disk**.
3. **Use hard disk:** Choose from the selection field the hard disk you want to use as cache for the HTTP proxy.
4. **Save:** Click this button to save the changes.

[Network settings - Network interface cards](#)

Network and routing configuration as described in [Scenario 2](#)

ATTENTION: By changing the IP address on the network card which you use for access to Gibraltar, the connection is interrupted. Please adapt the IP address on your work station computer as well.

[Firewall rules](#)

Firewall rules as described in [Scenario 2](#)

[NAT rules](#)

NAT rules as described in [Scenario 2](#)

[DHCP server](#)

DHCP server settings as described in [Scenario 1](#)

[HTTP proxy configuration](#)

1. Choose Proxy Server in the main menu.
2. Choose **HTTP proxy** in the sub menu.
3. Choose the tab **General settings**.
4. Mark your internal interface in the element group **Allow transparent proxying**. Thereby all inquiries from the internal network to port 80 are redirected to port 3128 (or to the port defined in the textfield **Port**), where the HTTP proxy listens.
5. **Save:** Click this button to save your changes.
6. Choose the card **Proxy cache**.
7. **Main storage for proxy (in MB):** Indicate, how much of the main storage should be available for the proxy cache. This part of the main storage is blocked for the other services thereby. Leave the value 4.
8. **Maximum size of the object (in KB):** This value indicates the size, objects of homepages can have at most, to be stored in the cache. If an object exceeds this value, it won't be stored in the cache for a further request.
9. **Use cache on hard disk:** Mark this checkbox, if you integrated a hard disk in the module **System** and if you want to use this hard disk as cache for the HTTP proxy also.
10. **Size of disk cache (in MB):** In the case, that you marked the checkbox **Use cache on hard disk**, you can enter the disk space of the hard disk you want to use for the HTTP proxy in this textfield.
11. **Save:** Click this button to save your changes.
12. Choose the card **Content filter**.
13. **Kaspersky Anti-Virus:** Mark this checkbox to activate the Kaspersky Anti-Virus scanner, if you purchased a Kaspersky for Gibraltar license.
14. **Save:** Click this button to save your changes.

15. Afterwards start the **HTTP proxy** in the module **Services** to activate the settings.

FTP proxy configuration:

In this scenario we will configure the FTP proxy to protect an internal FTP server from dangers of outside. The FTP proxy takes on inquiries from outside, fetches the inquired data from the internal FTP server and relays them to the inquirer from outside by itself.

1. Choose **FTP proxy** in the main menu.
2. Choose the tab **General settings**.
3. **Direction:** Mark the option field **incoming** and click the button **Go!**.
4. **Destination FTP server:** Enter in this textfield the IP address of your internal FTP server to which access from outside should be directed.
5. **Destination FTP port:** Enter the port on which the FTP server offers the FTP services. By default you can leave the value 21 (default FTP port).
6. **Transfer mode:** Choose the transfer mode you want to use. If you leave the mode Client, the transfer mode of the client will be used.
7. **Save:** Click this button to save your changes.
8. Afterwards start the **FTP proxy** in the module **Services** to activate the settings.

POP3 proxy:

1. Choose **POP3 proxy** in the main menu.
2. Choose the tab **General settings**.
3. Here you can change settings to your special needs. Yet the default settings are a good basis.
4. **Save:** Click this button to save your changes.
5. Choose the tab **Rename attachments**.
6. **Rename attachments:** Mark this checkbox if you want the file extensions listed in the element group below to be renamed when you receive them as attachment.
7. **Save:** Click this button to save your changes.
8. Afterwards start the **POP3 proxy** in the module **Services** to activate the settings.

Save config

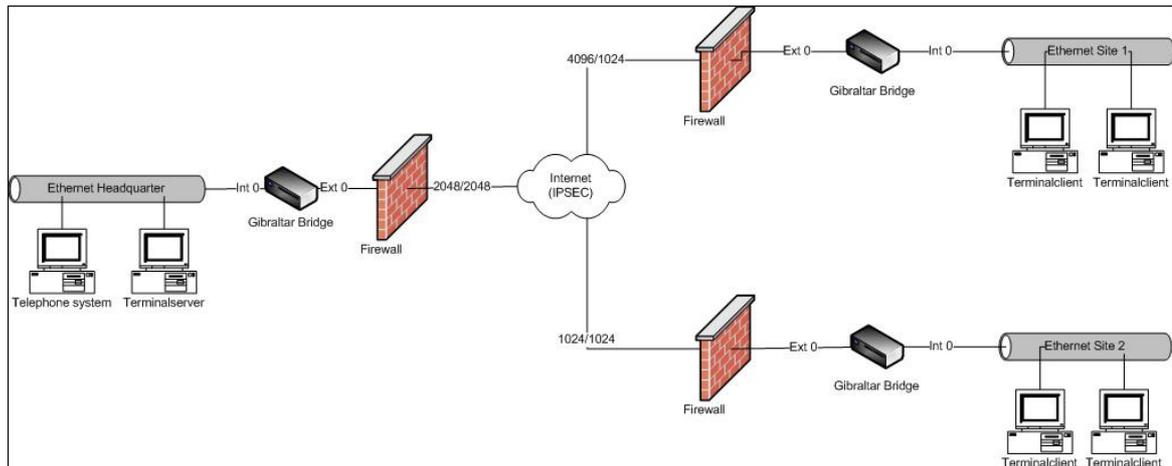
1. Save your configuration.

7.7 Traffic Shaping Citrix and VOIP bridged

In this scenario we will configure Gibraltar on a transparent traffic shaper on a computer, which is equipped with two network interface cards. Both network interface cards are combined to a bridge therefore, to make the transparent mode possible. The destination of this scenario is to provide a Citrix terminalserver surrounding for the critical corporate protocol ICA of minimum 35 % of the available bandwidth. We also have to guarantee a minimum of 35 % of the traffic for Voice over Ip. Because of latency the rest traffic only gets a maximum of 75 % of the total bandwidth. This is a must have if you do not have a provider that supports the QoS based on TOS bits (most providers don't). Furthermore only 95 % of the total bandwidth may be used to ensure a optimal functionality. The following initial situation is given:

- Headquarter with 2048/2048 (down,up) internet bandwidth (192.168.0.0/24), IP telephone system: 192.168.0.100
- Site 1 with 4096/1024 internet bandwidth (192.168.1.0/24), IP telephone system: 192.168.1.100
- Site 2 with 1024/1024 internet bandwidth (192.168.2.0/24), IP telephone system: 192.168.2.100

The sites are already connected with a third party product over a secure IPSec tunnel with the headquarter.



System Requirements

A computer with two compatible network interface cards or a Gibraltar Security Gateway.

Configuration Headquarter

Installation of Gibraltar

Please install Gibraltar as described in chapter [Installation](#).

[System configuration](#)

System configuration as described in [Scenario 1](#).

[Network settings - Network interface cards](#)

1. Choose **Network** in the main menu.
2. Choose the tab of the interface **eth1**.
3. **Interface:** Enter the desired name of this network interface (e.g. "int0" so that you can definitely identify the network interface for the internal network).
4. **Start automatically:** Mark this checkbox to start the network interface automatically when Gibraltar boots.
5. **Save:** Confirm your changes with clicking the button **Save**.
6. Choose the tab of the interface **eth0**.
7. **Interface:** Enter the desired name of this network interface (e.g. "ext0" so that you can definitely identify the network interface for the external network area).
8. **Start automatically:** Mark this checkbox to start the network interface automatically, when Gibraltar boots.
9. **Save:** Confirm your changes with clicking the button **Save**.
10. Choose the index card **Bridging**.
11. **Interface:** Allocate a name for the bridge (e.g. "myBridge")
12. **Static IPs:** Alter the IP address in the textfield **IP address/netmask** to the IP address you intend for Gibraltar ([CIDR-Notation](#): e.g. 192.168.1.1/24). You can continue the configuration over this address of the bridge later.
13. **Bridged Interfaces:** Choose the interfaces "int0" and "ext0".
14. **Save:** Confirm your changes with clicking the button **Save** to generate the bridge.

ATTENTION: By changing the IP address on the network card which you use for access to Gibraltar, the connection is interrupted. Please adapt the IP address on your work station computer as well.

[Firewall rules](#)

1. Choose **Firewall** in the main menu.
2. **Interface:** Choose the value "int0 bridged" from the select box **incoming** for the internal network interface and the value "ext0 bridged" from the select box **outgoing** for the external network interface. Click the button **Go!** **GibADMIN** now displays all filter rules for the packets that come from the network interface "int0" and go to the network interface "ext0".
3. **Add Rule:** Click this button to add a new rule in this range ("int0 -> ext0"). The browser will redirect to a [detail form](#)
4. **Source address:** Choose ANY from the selection box to allow all appropriate resource addresses.
5. **Destination address:** Choose ANY from the selection box to allow all destination addresses.
7. **Comment:** Enter a comment about the rule. You can leave the other fields blank in this case.
8. **Save:** Confirm your changes with clicking the button **Save**.

Add another rule from incoming "ext0 bridged" to outgoing "int0 bridged" with the same settings.

IMPORTANT: You have to place Gibraltar now that the internal interface is attached to the switch for the internal LAN and that the external interface leads directly to the router (contingently with a crossbred cable). Gibraltar is now in transparent mode and able to regulate the traffic from the internal network to the external network.

Now a service has to be designed for defining the shaping rules. The definition has to occur with the ICA source ports because the rules have to be defined for the headquarter.

Network - Definitions

1. Choose **Network** in the main menu.
2. Choose **Definitions** in the sub menu.
3. Choose the index card **Host/Net Aliases**.
4. Define one host/net alias for the site 1 and one for the site 2 (e.g.net1 - 192.168.1.0/24 and net2 - 192.168.2.0/24).
5. Define one host for the host/net alias "voip" for the telephone system 192.168.0.100
6. **Save:** Confirm your changes with clicking the button **Save**.

The following steps are necessary to be able to manage the total bandwidth:

- Definition of the bandwidth of each interface
- Classifying the traffic to assign it to the shaping rules
- Creating the shaping rules for the regulation

Traffic shaping

1. Choose **Traffic shaping** in the main menu.
2. Choose the tab **General Settings**.
3. **Bandwidths:** Define the value "2048" for the interface "ext0" for the upload and the download.
4. **Save:** Confirm your changes with clicking the button **Save**.
5. Choose the tab **Classification**.
6. **Add classification:** Click this button for adding a new classification for the ICA source ports.
7. **Name:** Enter a name for the new classification (e.g. "icaSource").
8. **Source address, Destination address:** Select the value ANY from the select boxes.
9. **Service:** Select the value "ica_source" from the select box.
10. **TOS:** Select the value "Minimize Delay".
11. **Save:** Confirm your changes with clicking the button **Save**.
12. **Cancel:** Click this button to get back to the overview.
13. **Add classification:** Click this button for adding a new classification for the ICA destination ports.
14. **Name:** Enter a name for the new classification (e.g. "icaDest").
15. **Source address, Destination address:** Select the value ANY from the select boxes.
16. **Service:** Select the value "ica_destination" from the select box.
17. **TOS:** Select the value "Minimize Delay".

18. **Save:** Confirm your changes with clicking the button **Save**.
19. **Cancel:** Click this button to get back to the overview.
20. **Add classification:** Click this button for adding a new classification for the source packets of the telephone system.
21. **Name:** Enter a name for the new classification (e.g. "voipSource").
22. **Source address:** Select the value "voip" from the select boxes.
23. **Destination address:** Select the value "voip" from the select boxes.
24. **TOS:** Select the value "Minimize Delay".
25. **Save:** Confirm your changes with clicking the button **Save**.
26. **Cancel:** Click this button to get back to the overview.
27. **Add classification:** Click this button for adding a new classification for the destination packets of the telephone system.
28. **Name:** Enter a name for the new classification (e.g. "voipDest").
29. **Source address:** Select the value "ANY" from the select boxes.
30. **Destination address:** Select the value "voip" from the select boxes.
31. **TOS:** Select the value "Minimize Delay".
32. **Save:** Confirm your changes with clicking the button **Save**.
33. **Cancel:** Click this button to get back to the overview.
34. **Add classification:** Click this button for adding a new classification for ICMP. ICMP should be managed by default for error diagnosis.
35. **Name:** Enter a name for the new classification (e.g. "icmp").
36. **Source address, Destination address:** Select the value ANY from the select boxes.
37. **Service:** Select the value "CUSTOM" from the select box.
38. **Protocoll:** Select the value "ICMP".
39. **TOS:** Select the value "Minimize Delay".
40. **Save:** Confirm your changes with clicking the button **Save**.
41. **Cancel:** Click this button to get back to the overview.
42. **Add classification:** Click this button for adding a new classification for the remaining traffic.
43. **Name:** Enter a name for the new classification (e.g. "rest").
44. **Source address, Destination address:** Select the value ANY from the select boxes.
45. **Save:** Confirm your changes with clicking the button **Save**.

ICMP and ICA traffic will be joined to a group "ica". We also join both voip classifications to a group as those groups has to get regulated as a whole.

1. Choose the tab **Classification Group**.
2. **Add group:** Click this button to add a new classification group containing "icaSource", "icaDest" and "icmp".
3. **Name:** Enter a name for the group (e.g. "ica").
4. **Add member:** Choose the members "icaSource", "icaDest", and "icmp".
5. **Save:** Confirm your changes with clicking the button **Save**.
6. **Cancel:** Click this button to get back to the overview.
7. **Add group:** Click this button to add a new classification group containing "voipSource" and "voipDest".
8. **Name:** Enter a name for the group (e.g. "ica").
9. **Add member:** Choose "voipSource" and "voipDest".
10. **Save:** Confirm your changes with clicking the button **Save**.

To finish the configuration you must set the rules for the two external offices. These rules are responsible for the regulation of the bandwidth. First we will regulate the upload of the headquarter - this is the track "outgoing ext0".

1. Choose the tab **Traffic shaping rules**.
2. **Track:** Choose "outgoing ext0". Gibraltar now takes the predefined upload bandwidth of the track "ext0". This traffic represents the upload of the headquarter.
3. **Add rule:** Click this button to add a new rule.
4. **Name:** Enter a name for the new rule (e.g. "ruleNet1").
5. **Add member:** Click this button to add classifications or classification groups.
6. Choose the classification group "ica" and set the values "360" for Min and "1024" for Max.
7. Choose the classification group "voip" and set the values "360" for Min and "1024" for

- Max.
8. Choose the classification "rest" and set the values "250" for Min and "768" for Max.
 9. **Save:** Confirm your changes with clicking the button **Save**.
 10. Choose the tab **Advanced**.
 11. **Destination address:** Choose the definition "net1", because this rule should only be valid for this destination net.
 12. **Bandwidth (kbit) for nets:** Choose the value "1024" as we only want to provide a maximum of 1024kbit for this net. All traffic that goes the way: headquarter->site1 is not allowed to exceed the maximum of 1024kbit.
 13. **Save:** Confirm your changes with clicking the button **Save**.
 14. **Cancel:** Click this button to return to the overview.
 15. **Add rule:** Click this button to add a new rule.
 16. **Name:** Enter a name for the new rule (e.g. "ruleNet2").
 17. **Add member:** Click this button to add classifications or classification groups.
 18. Choose the classification group "ica" and set the values "360" for Min and "1024" for Max.
 19. Choose the classification group "voip" and set the values "360" for Min and "1024" for Max.
 20. Choose the classification "other" and set the values "250" for Min and "768" for Max.
 21. **Save:** Confirm your changes with clicking the button **Save**.
 22. Choose the tab **Advanced**.
 23. **Destination address:** Choose the definition "net2", because this rule should only be valid for this destination net.
 24. **Bandwidth (kbit) for nets:** Choose the value "1024" as we only want to provide a maximum of 1024kbit for this net. All traffic that goes the way: headquarter->site1 is not allowed to exceed the maximum of 1024kbit.
 25. **Save:** Confirm your changes with clicking the button **Save**.

Note:

To regulate all traffic in the headquarter it is also essential to limit the download traffic. If we do not regulate this traffic it could be possible that a download into the headquarter blocks the upload packets of the sites.

1. Choose the tab **Traffic shaping rules**.
2. **Track:** Choose "incoming int0". Gibraltar now takes the predefined download bandwidth of the track "ext0". This traffic represents the download of the headquarter.
3. **Add rule:** Click this button to add a new rule.
4. **Name:** Enter a name for the new rule (e.g. "ruleDownload").
5. **Add member:** Click this button to add classifications or classification groups.
6. Choose the classification group "ica" and set the values "716" for Min and "2048" for Max.
7. Choose the classification group "voip" and set the values "716" for Min and "2048" for Max.
8. Choose the classification "rest" and set the values "500" for Min and "1536" for Max.
9. **Save:** Confirm your changes with clicking the button **Save**.

As we do not want to regulate a net with download shaping it is not necessary to define a target net on the "advanced" tab.

Save config

1. The configuration has to be saved on an USB-stick or harddisc.

The traffic is regulated on the basis of the different bandwidths in both sites now. A printjob, that usually passes an ICA-flow, would not cause a problem any more. To control the outgoing traffic of the sites, the following configurations are necessary:

Traffic shaping (site 1)

1. Choose **Traffic shaping** in the main menu.
2. Choose the tab **General Settings**.
3. **Bandwidths:** Define the values "1024" and "4096" for the up and the download bandwidth of this site.

4. **Save:** Confirm your changes with clicking the button **Save**.
5. Now define the same classifications as in the headquarter!
6. Choose the tab **Traffic shaping rules**.
7. **Track:** Choose "outgoing ext0". Gibraltar now takes the predefined upload bandwidth of the track "ext0". This traffic represents the upload of the site1.
8. **Add rule:** Click this button to add a new rule.
9. **Name:** Enter a name for the new rule (e.g. "ruleHeadquarter").
10. **Add member:** Click this button to add classifications or classification groups.
11. Choose the classification group "ica" and set the values "360" for Min and "1024" for Max.
12. Choose the classification group "voip" and set the values "360" for Min and "1024" for Max.
13. Choose the classification "rest" and set the values "250" for Min and "768" for Max.
14. **Save:** Confirm your changes with clicking the button **Save**.
15. **Cancel:** Click this button to return to the overview.

It is also necessary to limit the download traffic in the sites. Do the following to achieve this goal:

1. Choose the tab **Traffic shaping rules**.
2. **Track:** Choose "incoming ext0". Gibraltar now takes the predefined download bandwidth of the track "ext0". This traffic represents the download of the site1.
3. **Add rule:** Click this button to add a new rule.
4. **Name:** Enter a name for the new rule (e.g. "ruleDownload").
5. **Add member:** Click this button to add classifications or classification groups.
6. Choose the classification group "ica" and set the values "360" for Min and "1024" for Max.
7. Choose the classification group "voip" and set the values "360" for Min and "1024" for Max.
8. Choose the classification "rest" and set the values "2000" for Min and "3072" for Max.
9. **Save:** Confirm your changes with clicking the button **Save**.
10. **Cancel:** Click this button to return to the overview.

Note:

We do not have to give the Voip or Ica-traffic a maximum of 4096 in this szenario as the maximum that comes from the headquarter is 1024kbit. The most important thing is the limitation to 75% of the rest traffic to provide a buffer for Voice over IP and ICA.

Complete the configuration for site 2 with the bandwidth value of 1024 for upload and download. Therewith you control the traffic at both sites and avoid to affect your ICA-sessions through to big printjobs or video streams. A graphical reporting of the regulation of bandwidths you can find in the module [Monitoring](#).

Save config

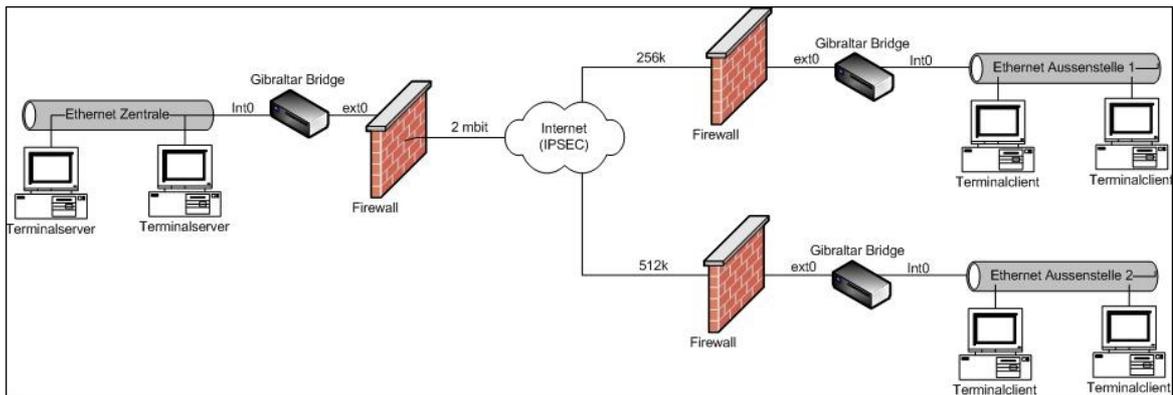
1. Save your configuration on an USB-stick or harddisc.

7.8 Traffic Shaping Citrix and VOIP with VPN

In this scenario we will configure 3 Gibraltors that are connected via IPSEC-VPN. As we are using Citrix Terminalservices we also have to guarantee a minimum of 35 % for the ICA traffic.

We also have to guarantee a minimum of 35 % of the traffic for Voice over Ip. Because of latency the rest traffic only gets a maximum of 75 % of the total bandwidth. This is a must have if you do not have a provider that supports the QoS based on TOS bits (most providers don't). Furthermore only 95 % of the total bandwidth may be used to ensure a optimal functionality. The following initial situation is given:

- Headquarter with 4096/2048 (down,up) internet bandwidth (192.168.0.0/24), IP telephone system: 192.168.0.100
- Site 1 with 4096/1024 internet bandwidth (192.168.1.0/24), IP telephone system: 192.168.1.100
- Site 2 with 1024/1024 internet bandwidth (192.168.2.0/24), IP telephone system: 192.168.2.100



System Requirements

A computer with two compatible network interface cards or a Gibraltar Security Gateway.

IPSEC-VPN

Configure the IPSEC connections as described in [Scenario 4](#).

Network - Definitions

1. Choose **Network** in the main menu.
2. Choose **Definitions** in the sub menu.
3. Choose the index card **Host/Net Aliases**.
4. Define one host/net alias for the site 1 and one for the site 2 (e.g. net1 - 192.168.1.0/24 and net2 - 192.168.2.0/24).
5. Define one host for the host/net alias "voip" for the telephone system 192.168.0.100.
6. **Save**: Confirm your changes with clicking the button **Save**.

The following steps are necessary to be able to manage the total bandwidth:

- Definition of the bandwidth of each interface
- Classifying the traffic to assign it to the shaping rules
- Creating the shaping rules for the regulation

Traffic shaping

1. Choose **Traffic shaping** in the main menu.
2. Choose the tab **General Settings**.
3. **Bandwidths**: Define the value "2048" for the interface "ext0" for the upload and "4096" for the download.
4. Define the value "2048" for the interface "int0" for the download and "4096" for the upload.
5. **Save**: Confirm your changes with clicking the button **Save**.

Note: When using IPSEC we have to take care for some special constructions when implementing traffic shaping. If we would implement on the basis of the track "ext0", Gibraltar could only analyse ESP encrypted packets and therefore not regulate Ica or Voip. Gibraltar only can "see" the decrypted packets on the internal interface "int0". As Gibraltar always uses the upload bandwidth for outgoing tracks we have to swap the upload and download bandwidth for the internal interface "int0".

"outgoing int0" = download of the headquarter -> packets that go from the external interface to the internal interface.

"incoming int0" = upload of the headquarter -> packets that go from the internal interface to the external interface.

6. Choose the tab **Classification**.
7. **Add classification:** Click this button for adding a new classification for the ICA source ports.
8. **Name:** Enter a name for the new classification (e.g. "icaSource").
9. **Source address, Destination address:** Select the value ANY from the select boxes.
10. **Service:** Select the value "ica_source" from the select box.
11. **TOS:** Select the value "Minimize Delay".
12. **Save:** Confirm your changes with clicking the button **Save**.
13. **Cancel:** Click this button to get back to the overview.
14. **Add classification:** Click this button for adding a new classification for the ICA destination ports.
15. **Name:** Enter a name for the new classification (e.g. "icaDest").
16. **Source address, Destination address:** Select the value ANY from the select boxes.
17. **Service:** Select the value "ica_destination" from the select box.
18. **TOS:** Select the value "Minimize Delay".
19. **Save:** Confirm your changes with clicking the button **Save**.
20. **Cancel:** Click this button to get back to the overview.
21. **Add classification:** Click this button for adding a new classification for the source packets of the telephone system.
22. **Name:** Enter a name for the new classification (e.g. "voipSource").
23. **Source address:** Select the value "voip" from the select boxes.
24. **Destination address:** Select the value "voip" from the select boxes.
25. **TOS:** Select the value "Minimize Delay".
26. **Save:** Confirm your changes with clicking the button **Save**.
27. **Cancel:** Click this button to get back to the overview.
28. **Add classification:** Click this button for adding a new classification for the destination packets of the telephone system.
29. **Name:** Enter a name for the new classification (e.g. "voipDest").
30. **Source address:** Select the value "ANY" from the select boxes.
31. **Destination address:** Select the value "voip" from the select boxes.
32. **TOS:** Select the value "Minimize Delay".
33. **Save:** Confirm your changes with clicking the button **Save**.
34. **Cancel:** Click this button to get back to the overview.
35. **Add classification:** Click this button for adding a new classification for ICMP. ICMP should be managed by default for error diagnosis.
36. **Name:** Enter a name for the new classification (e.g. "icmp").
37. **Source address, Destination address:** Select the value ANY from the select boxes.
38. **Service:** Select the value "CUSTOM" from the select box.
39. **Protocoll:** Select the value "ICMP".
40. **TOS:** Select the value "Minimize Delay".
41. **Save:** Confirm your changes with clicking the button **Save**.
42. **Cancel:** Click this button to get back to the overview.
43. **Add classification:** Click this button for adding a new classification for the remaining traffic.
44. **Name:** Enter a name for the new classification (e.g. "rest").
45. **Source address, Destination address:** Select the value ANY from the select boxes.
46. **Save:** Confirm your changes with clicking the button **Save**.

ICMP and ICA traffic will be joined to a group "ica". We also join both voip classifications to a group as those groups has to get regulated as a whole.

1. Choose the tab **Classification Group**.
2. **Add group:** Click this button to add a new classification group containing "icaSource", "icaDest" and "icmp".
3. **Name:** Enter a name for the group (e.g. "ica").
4. **Add member:** Choose the members "icaSource", "icaDest", and "icmp".
5. **Save:** Confirm your changes with clicking the button **Save**.
6. **Cancel:** Click this button to get back to the overview.
7. **Add group:** Click this button to add a new classification group containing "voipSource"

and "voipDest".

8. **Name:** Enter a name for the group (e.g. "ica").
9. **Add member:** Choose "voipSource" and "voipDest".
10. **Save:** Confirm your changes with clicking the button **Save**.

To finish the configuration you must set the rules for the two external offices. These rules are responsible for the regulation of the bandwidth. First we will regulate the upload of the headquarter - this is the track "incoming int0" from the point of view of the Gibraltar.

1. Choose the tab **Traffic shaping rules**.
2. **Track:** Choose "incoming int0". Gibraltar now takes the predefined download bandwidth of the track "int0". This traffic represents the upload of the headquarter.
3. **Add rule:** Click this button to add a new rule.
4. **Name:** Enter a name for the new rule (e.g. "ruleNet1").
5. **Add member:** Click this button to add classifications or classification groups.
6. Choose the classification group "ica" and set the values "360" for Min and "1024" for Max.
7. Choose the classification group "voip" and set the values "360" for Min and "1024" for Max.
8. Choose the classification "rest" and set the values "250" for Min and "768" for Max.
9. **Save:** Confirm your changes with clicking the button **Save**.
10. Choose the tab **Advanced**.
11. **Destination address:** Choose the definition "net1", because this rule should only be valid for this destination net.
12. **Bandwidth (kbit) for nets:** Choose the value "1024" as we only want to provide a maximum of 1024kbit for this net. All traffic that goes the way: headquarter->site1 is not allowed to exceed the maximum of 1024kbit.
13. **Save:** Confirm your changes with clicking the button **Save**.
14. **Cancel:** Click this button to return to the overview.
15. **Add rule:** Click this button to add a new rule.
16. **Name:** Enter a name for the new rule (e.g. "ruleNet2").
17. **Add member:** Click this button to add classifications or classification groups.
18. Choose the classification group "ica" and set the values "360" for Min and "1024" for Max.
19. Choose the classification group "voip" and set the values "360" for Min and "1024" for Max.
20. Choose the classification "other" and set the values "250" for Min and "768" for Max.
21. **Save:** Confirm your changes with clicking the button **Save**.
22. Choose the tab **Advanced**.
23. **Destination address:** Choose the definition "net2", because this rule should only be valid for this destination net.
24. **Bandwidth (kbit) for nets:** Choose the value "1024" as we only want to provide a maximum of 1024kbit for this net. All traffic that goes the way: headquarter->site1 is not allowed to exceed the maximum of 1024kbit.
25. **Save:** Confirm your changes with clicking the button **Save**.

Note:

To regulate all traffic in the headquarter it is also essential to limit the download traffic. If we do not regulate this traffic it could be possible that a download into the headquarter blocks the upload packets of the sites.

1. Choose the tab **Traffic shaping rules**.
2. **Track:** Choose track "outgoing int0". Gibraltar now takes the predefined upload bandwidth of the track "int0". This traffic represents the download of the headquarter.
3. **Add rule:** Click this button to add a new rule.
4. **Name:** Enter a name for the new rule (e.g. "ruleDownload").
5. **Add member:** Click this button to add classifications or classification groups.
6. Choose the classification group "ica" and set the values "716" for Min and "2048" for Max.
7. Choose the classification group "voip" and set the values "716" for Min and "2048" for Max.
8. Choose the classification "rest" and set the values "500" for Min and "1536" for Max.
9. **Save:** Confirm your changes with clicking the button **Save**.

As we do not want to regulate a net with download shaping it is not necessary to define a target net on the "advanced" tab.

Special construction: Gibraltar also as mail relay or HTTP proxy

If you are using Gibraltar also as a mail relay or HTTP proxy in this scenario you have the following situation: With the rules "outgoing int" and "incoming int" we are able to regulate the upload and download traffic from and to the internal net. Gibraltar as a proxy or mail relay of course also "produces" upload and download traffic that is not regulated up to now in this case. Do the following if this scenario occurs:

1. Choose the tab **Classification**.
2. **Add classification:** Click this button to add a new classification for IPSEC as it is the aim to provide a maximum of 100% for the IPSEC traffic as Ica and Voip-packets are encapsulated in IPSEC.
3. **Name:** Enter a name for the classification (e.g. "ipsec")
4. **Source address, Destination address:** Select the value ANY from the select boxes.
5. **Service:** Choose the value "ipsec" from the select box.
6. **Save:** Confirm your changes with clicking the button **Save**.
7. **Cancel:** Click this button to return to the overview.
8. : Click this button to place the classification "ipsec" before the classification rest!
9. **Save:** Confirm your changes with clicking the button **Save**
10. Choose the tab **Traffic shaping rules**.
11. **Track:** Choose the track "incoming ext0". Gibraltar now takes the predefined download bandwidth of the track "ext0". This traffic represents the download of the headquarter.
12. **Add rule:** Click this button to add a new rule.
13. **Name:** Enter a name for the new rule (e.g. "limitGibDownload").
14. **Add member:** Click this button to add classifications and classification groups.
15. Choose the classification group "ipsec" and set the values "2864" for Min and "4096" for Max.
16. Choose the classification "rest" and set the values "1000" for Min and "3072" for Max.
17. **Save:** Confirm your changes with clicking the button **Save**.
18. Choose the tab **Traffic shaping rules**.
19. **Track:** Choose the track "outgoing ext0". Gibraltar now takes the predefined upload bandwidth of the track "ext0". This traffic represents the upload of the headquarter.
20. **Add rule:** Click this button to add a new rule.
21. **Name:** Enter a name for the new rule (e.g. "limitGibUpload").
22. **Add member:** Click this button to add classifications and classification groups.
23. Choose the classification group "ipsec" and set the values "720" for Min and "1024" for Max.
24. Choose the classification "rest" and set the values "250" for Min and "768" for Max.
25. **Save:** Confirm your changes with clicking the button **Save**.

Now we arrived that

[Save config](#)

1. The configuration has to be saved on an USB-stick or harddisc.

The traffic is regulated on the basis of the different bandwidths in both sites now. A printjob, that usually passes an ICA-flow, would not cause a problem any more. To control the outgoing traffic of the sites, the following configurations are necessary:

[Traffic shaping \(site 1\)](#)

1. Choose **Traffic shaping** in the main menu.
2. Choose the tab **General Settings**.
3. **Bandwidths:** Define the values "1024" and "4096" for the up and the download bandwidth of this site.
4. Define the value "1024" for the interface "int0" for the download and "4096" for the upload.
5. **Save:** Confirm your changes with clicking the button **Save**.

6. Now define the same classifications as in the headquarter!
7. Choose the tab **Traffic shaping rules**.
8. **Track:** Choose "outgoing ext0". Gibraltar now takes the predefined upload bandwidth of the track "ext0". This traffic represents the upload of the site1.
9. **Add rule:** Click this button to add a new rule.
10. **Name:** Enter a name for the new rule (e.g. "ruleHeadquarter").
11. **Add member:** Click this button to add classifications or classification groups.
12. Choose the classification group "ica" and set the values "360" for Min and "1024" for Max.
13. Choose the classification group "voip" and set the values "360" for Min and "1024" for Max.
14. Choose the classification "rest" and set the values "250" for Min and "768" for Max.
15. **Save:** Confirm your changes with clicking the button **Save**.
16. **Cancel:** Click this button to return to the overview.

It is also necessary to limit the download traffic in the sites. Do the following to achieve this goal:

1. Choose the tab **Traffic shaping rules**.
2. **Track:** Choose "outgoing int0". Gibraltar now takes the predefined upload bandwidth of the track "int0". This traffic represents the download of the site1.
3. **Add rule:** Click this button to add a new rule.
4. **Name:** Enter a name for the new rule (e.g. "ruleDownload").
5. **Add member:** Click this button to add classifications or classification groups.
6. Choose the classification group "ica" and set the values "360" for Min and "1024" for Max.
7. Choose the classification group "voip" and set the values "360" for Min and "1024" for Max.
8. Choose the classification "rest" and set the values "2000" for Min and "3072" for Max.
9. **Save:** Confirm your changes with clicking the button **Save**.
10. **Cancel:** Click this button to return to the overview.

Note:

We do not have to give the Voip or Ica-traffic a maximum of 4096 in this szenario as the maximum that comes from the headquarter is 1024kbit. The most important thing is the limitation to 75% of the rest traffic to provide a buffer for Voice over IP and ICA.

Complete the configuration for site 2 with the bandwidth value of 1024 for upload and download. Therewith you control the traffic at both sites and avoid to affect your ICA-sessions through to big printjobs or video streams. A graphical reporting of the regulation of bandwidths you can find in the module [Monitoring](#).

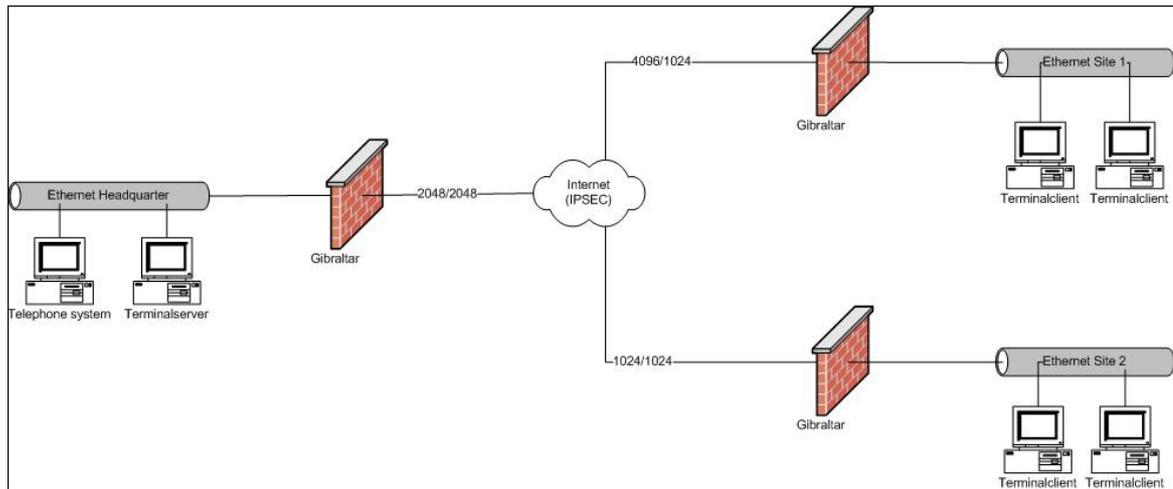
Save config

1. Save your configuration on an USB-stick or harddiscs.

7.9 Traffic Shaping VoIP

This scenario shows the configuration of Gibraltar to secure a minimum bandwidth for a internal VoIP telephone system having the IP 192.168.0.40.

The aim of this scenario is to ensure a minimum bandwidth of 1 MBit for the telephone system. The internet connection has a bandwidth of 2 MBit both - up- and download. Because of latency the rest traffic only gets a maximum of 75 % of the total bandwidth. This is a must have if you do not have a provider that supports the QoS based on TOS bits (most providers don't). Furthermore only 95 % of the total bandwidth may be used to ensure a optimal functionality.



System Requirements

A computer with two compatible network interface cards or a Gibraltar Security Gateway.

Installation of Gibraltar

Please install Gibraltar as described in chapter [Installation](#).

System configuration

System configuration as described in [Scenario 1](#).

Network settings - Network interface cards

Network and routing configuration as described in [Scenario 2](#).

ATTENTION: By changing the IP address on the network card which you use for access to Gibraltar, the connection is interrupted. Please adapt the IP address on your work station computer as well.

Firewall rules

Firewall rules as described in [Scenario 2](#).

Network - Definitions

1. Choose **Network** in the main menu.
2. Choose **Definitions** in the sub menu.
3. Choose the index card **Host/Net Aliases**.
4. Define a host/net alias named "voipHost" with the IP address 192.168.0.40.
5. **Save:** Confirm your changes with clicking the button **Save**.

The following steps are necessary to be able to manage the total bandwidth:

- Definition of the bandwidth of each interface
- Classifying the traffic to assign it to the shaping rules
- Creating the shaping rules for the regulation

Traffic shaping

1. Choose **Traffic shaping** in the main menu.
2. Choose the tab **General Settings**.
3. **Bandwidths:** Define the value "2048" for the interface "ext0" for the download and 1024 for the upload.

4. **Save:** Confirm your changes with clicking the button **Save**.
5. Choose the tab **Classification**.
6. **Add classification:** Click this button for adding a new classification for the source address of the telephone system.
7. **Name:** Enter a name for the new classification (e.g. "voipSource").
8. **Source address:** Select the value "voipHost".
9. **Destination address:** Select the value "ANY".
10. **TOS:** Select the value "Minimize Delay".
11. **Save:** Confirm your changes with clicking the button **Save**.
12. **Add classification:** Click this button for adding a new classification for the destination address of the telephone system.
13. **Name:** Enter a name for the new classification (e.g. "voipDest").
14. **Source address:** Select the value "ANY".
15. **Destination address:** Select the value "voipHost".
16. **TOS:** Select the value "Minimize Delay".
17. **Save:** Confirm your changes with clicking the button **Save**.
18. **Add classification:** Click this button for adding a new classification for ICMP. ICMP should be managed by default for error diagnosis.
19. **Name:** Enter a name for the new classification (e.g. "icmp").
20. **Service:** Select the value "CUSTOM" from the select box.
21. **Protocoll:** Select the value "ICMP".
22. **Save:** Confirm your changes with clicking the button **Save**.
23. **Add classification:** Click this button for adding a new classification for the remaining traffic.
24. **Name:** Enter a name for the new classification (e.g. "rest").
25. **Source address, Destination address:** Select the value ANY from the select boxes.
26. **Save:** Confirm your changes with clicking the button **Save**.

ICMP and VoIP traffic will be joined to a group "highPrio". This group should always be observed as a whole to ease troubleshooting.

1. Choose the tab **Classification Group**.
2. **Add group:** Click this button to add a new classification group.
3. **Name:** Enter a name for the group (e.g. "highPrio").
4. **Add member:** Choose the members "voipSource", "voipDest", and "icmp".
5. **Save:** Confirm your changes with clicking the button **Save**.

Now you must create the shaping rules for the minimum bandwidth:

1. Choose the tab **Traffic shaping rules**.
2. **Track:** Choose "incoming ext0" to manage incoming traffic to the internal network.
3. **Add rule:** Click this button to add a new rule.
4. **Name:** Enter a name for the new rule (e.g. "ruleDownload").
5. **Add member:** Click this button to add classifications or classification groups.
6. Choose the classification group "highPrio" and set the values "1024" for Min and "2048" for Max.
7. **Add member:** Click this button to add classifications or classification groups.
8. Choose the classification group "rest" and set the values "800" for Min and "2048" for Max.
9. **Save:** Confirm your changes with clicking the button **Save**.
10. **Add rule:** Click this button to add a new rule.
11. **Track:** Choose "outgoing ext0" to manage outgoing traffic.
12. **Name:** Enter a name for the new rule (e.g. "ruleUpload").
13. **Add member:** Click this button to add classifications or classification groups.
14. Choose the classification group "highPrio" and set the values "512" for Min and "1024" for Max.
15. **Add member:** Click this button to add classifications or classification groups.
16. Choose the classification group "highPrio" and set the values "450" for Min and "1024" for Max.
17. **Save:** Confirm your changes with clicking the button **Save**.

[Save config](#)

1. Save your configuration on an USB-stick or harddisc.

The above configuration ensures a minimal bandwidth of 1 MBit for your telephone system. If you notice some troubles during your telephone calls, adapt the values for the "rest" classification down to a lower one. A detailed reporting of your bandwidth management can be seen at [Monitoring](#).

7.10 Traffic Shaping Web Traffic

Configuring the Gibraltar Firewall to ensure a minimal bandwidth for web traffic (http, https). Additional a minimal bandwidth for fetching the emails via pop3 is configured. These services will get a minimal bandwidth of 1024 kbit. The whole bandwidth of the line is 2048 kbit (up- and download). As those services are not latency critical it is not necessary to limit the rest traffic to 75% of the maximum bandwidth.

System Requirements

A computer with two compatible network interface cards or a Gibraltar Security Gateway.

Installation of Gibraltar

Please install Gibraltar as described in chapter [Installation](#).

[System configuration](#)

System configuration as described in [Scenario 1](#).

[Network settings - Network interface cards](#)

Network and routing configuration as described in [Scenario 2](#).

ATTENTION: By changing the IP address on the network card which you use for access to Gibraltar, the connection is interrupted. Please adapt the IP address on your work station computer as well.

[Firewall rules](#)

Firewall rules as described in [Scenario 2](#).

[Traffic shaping](#)

1. Choose **Traffic shaping** in the main menu.
2. Choose the tab **General Settings**.
3. **Bandwidths:** Define the value "2048" for the interface "ext0" for the upload and the download
4. **Save:** Confirm your changes with clicking the button **Save**.
5. Choose the tab **Classification**.
6. **Add classification:** Click this button for adding a new classification for the web traffic.
7. **Name:** Enter a name for the new classification (e.g. "web").
8. **Source address:** Select the value "ANY".
9. **Destination address:** Select the value "ANY".
10. **Service:** Select the value "web".
11. **Save:** Confirm your changes with clicking the button **Save**.
12. **Add classification:** Click this button for adding a new classification for the pop3 traffic.
13. **Name:** Enter a name for the new classification (e.g. "pop3").
14. **Source address:** Select the value "ANY".
15. **Destination address:** Select the value "ANY".
16. **Service:** Select the value "pop3".

17. **Save:** Confirm your changes with clicking the button **Save**.

Now we have to create a group to put the services together.

1. Choose the tab **Classification Group**.
2. **Add group:** Click this button to add a new classification group.
3. **Name:** Enter a name for the group (e.g. "groupWeb").
4. **Add member:** Choose the members "web" and "pop3".
5. **Save:** Confirm your changes with clicking the button **Save**.

Now you must create the shaping rules for the minimum bandwidth:

1. Choose the tab **Traffic shaping rules**.
2. **Track:** Choose "incoming ext0" to manage incoming traffic to the internal network.
3. **Add rule:** Click this button to add a new rule.
4. **Name:** Enter a name for the new rule (e.g. "groupWeb").
5. **Add member:** Click this button to add classifications or classification groups.
6. Choose the classification group "groupWeb" and set the values "1024" for Min and "2048" for Max.
7. **Save:** Confirm your changes with clicking the button **Save**.

Now you have defined a minimum bandwidth for the services HTTP, POP3 and HTTPS.

[Save config](#)

1. Save your configuration on an USB-stick or on a harddisc.

8 Configuration

Before you start configuring Gibraltar with **GibADMIN** we will give you a quick overview about the user interface. While configuring Gibraltar, avoid using the **Forward** and the **Back** button of the browser. Nevertheless, if you use the buttons you will get a suitable message in **GibADMIN**.

Link

A link indicates a navigation to another page in **GibADMIN** and acts the same way as a link to another HTML page. Links can be found e.g. on the left side in the main menu.

Buttons

After clicking a button, a command is executed in the background; it e.g. stores the changes you made in the form. It is also possible to be redirected to another page by clicking a button (like a link). It is very important that you confirm any changes you made in a form by clicking a button so that the data can be saved permanently. The following buttons are available in **GibADMIN**:

-  This button is located in the title of each module. By clicking such a button you get a context help for the form you are currently working on.
-  This button is mostly located in an element group. You can move a row upwards in an element group. You find this option only in lists in which the ranking is important. After moving the row you have to click the button **Save** to store the settings.
-  This button is mostly located in an element group. You can move a row downwards in an element group. You find this button only in lists in which the ranking is important. After moving the row you have to click the button **Save** to store the settings.
-  This button is used for deleting of entries in lists. By clicking the button the entry in the labeled row gets deleted. Take care that only with clicking **Save** the entries get permanently deleted and the configuration file will be rewritten.
-  With this button you can alter into a detail mode for configuration. By clicking this button the labeled entry of the detail mode for configuration will be opened where you can alter configurations.

-  This button makes it possible to insert a new entry into the list below the selected entry. You find this button only in lists in which the ranking is important.
-  This button is only used to show a personal comment for a list entry. If you move the mouse cursor above this button the information is shown in a yellow box. You can not click this button.
-  This button is used to start services, devices or something else. You only see this button if the service or the device is stopped or in standby mode.
-  This button is used to stop services, devices or something else. You only see this button if the service or the device is started or in standby mode.
-  This button is used to change to the standby mode. An IPSec tunnel can be in standby mode if it is waiting for a start of the connection.
-  By clicking this button a form for sending mails will be opened.
-  This button is used to download a file. Before storing the file you have to give a path for the storage.

Textfield

You have to make entries in a textfield to perform a certain configuration. Textfields are used if the entries can not be selected from a select box or another option. Every entry in a textfield is checked so that the value fits in a predefined context. For example if we have a field that should contain an IP address you are only allowed to put values like a.b.c.d, where a, b, c and d have to be between 0 and 255. If **GibADMIN** checks that you inserted a wrong value, a suitable error message is displayed and points at the textfield that caused the error.

Select Box

In a select box you can select a value out of a predefined range of values. This is possible if the values have been reduced unto some few predefined values.

Checkbox

A checkbox offers the possibility to choose between two states. That are decisions like yes/no or activated/deactivated. The checkbox is activated if a tick is in the checkbox. You can change the state by clicking the left mouse button on the checkbox.

Option field

Option fields are used when more possibilities are available from which only one can be selected. The current selected option field is marked with a black dot.

Element group

An element group is a kind of representation in **GibADMIN**, which allows to represent identical elements in a table. For every element in a list, a row will be created. Some register cards allow to configure the elements in the element group or to go to a detail form by clicking a button. In some element groups it's possible to delete more than one entry at the same time. If there appears a

delete symbol  in the heading line of the element group, you can delete several entries at once by marking the checkboxes in the rows you want to delete and afterwards clicking the button

Delete marked entries  in the heading line.

CIDR - Classless Inter-Domain Routing

GibADMIN uses the CIDR notation to enter IP addresses in conjunction with the subnet mask. A CIDR address includes the standard 32-bit IP address and also information of how many bits are used for the network prefix. For example, in the CIDR address 192.168.0.1/24, the "/24" indicates the first 24 bits are used to identify the unique network leaving the remaining bits to identify the specific host. The last valid address of this network is consequently 192.168.0.254/24. The CIDR block - this is the slash with the number - can have values from "/13" to "/27".

Some examples:

CIDR block	# Equivalent Class C	# of Host Addresses
/27	1/8 of a Class C	32

/25	1/2 of a Class C	128
/24	1 Class C	256
/16	256 Class C	65536
/13	2048 Class C	524288

255.255.0.0 corresponding /16
255.255.255.0 corresponding /24
255.255.255.192 corresponding /26

8.1 License information

To use the Gibraltar firewall a valid license key is needed. You get your license file when purchasing Gibraltar. When you purchase a Gibraltar Security Gateway the license file is already uploaded.

The MAC addresses of the licensed network interface cards are encoded into the license file. Therefore this license file is only valid at the hardware with the MAC addresses within it.

NOTE: You can send us additional MAC addresses of a backup device so that we can also encode these MAC addresses to the license file when you purchase Gibraltar. The license file is valid for the main device as well as for the backup device. It is not necessary to buy a separate license for the backup device.

ATTENTION: If you must replace the current hardware because of a failure and you do not have a valid license for the backup hardware, you can get a temporary license directly with the **GibADMIN**. This temporary license is valid for 10 days and is generated automatically. It must be replaced with a new, valid license within the 10 days.

The license file

How you get the license file:

- When you purchase Gibraltar: Via email directly at the manufacturer or at a authorized partner or reseller.
- When you purchase a Gibraltar Security Gateway: The license is already pre-installed by the manufacturer.
- Test license: You can get a test license that is valid for 30 days directly from Gibraltar web site.
- Private license: A free license for private use can be ordered by sending a informal email to license@gibraltar.at. This license is only valid for 5 network devices behind the firewall.

The name of the license file contains some information that can be parsed into the following parts. An example for the name of a license file is `gib_2_4_6543_CompanyX_GS50Y1_22_07_2008.key`:

- Gibraltar version: `gib_2_4`
- License number: `6543`
- Name of the licensee: `CompanyX`
- Product: `GS50` (Gibraltar Software 50)
- Valid to: `22.7.2008`

Installation of the license file

If you are accessing **GibADMIN** for the first time you have to upload the license file.

1. **License file:** Choose **Choose...** and select your license file (license.key).
2. **Gibraltar license:** Choose this option if you want to upload a license for the Gibraltar Firewall.
3. **Kaspersky license:** Choose this option if you want to upload a license for the Kaspersky anti virus scanner.
4. **Puresight license:** Choose this option if you want to upload a license for the Puresight Content Scanner.
5. **Upload:** Choose this button to upload the license file to Gibraltar.

6. **MAC addresses:** In this list the MAC addresses of all network interface cards included in the computer are shown. This information is needed, to order a valid license.
7. **Puresight Network ID:** This ID is needed to purchase a license file for the Puresight Content Scanner.

License information ⓘ

License data

License file:

Gibraltar license
 Kaspersky license
 PureSight license

MAC addresses: 00:03:2d:08:fd:47
00:03:2d:08:fd:46
00:03:2d:08:fd:45
00:03:2d:08:fd:44

PureSight Network ID: BENA957X-PCRT3C26-RFDWY3B1-4VHZN49W

After you have uploaded your license file successfully, you are redirected to the login form.

1. **User:** Enter the user name "root".
2. **Password:** Enter the password for user "root". When you login the first time, the password is empty.
3. **Login:** Choose this button to login into Gibraltar.

After successful login, your license information will be displayed.

License information ?

License data

License number: 3

License owner: Richard Leitner

Email: leitner@esys.at

Purchased at: Wed Oct 06 15:49:25 CEST 2004

Valid to: Sun Dec 05 14:49:25 CET 2004

Number of licenses: 1

Valid for version: 2.0.11d

Kaspersky license: Expiration date: 03-11-2005

Number of VPN tunnels: 10 + 1 (Tunnel, Roadwarrior)

Number of VPN users: 10

Valid for these MAC addresses: 00:40:95:30:c2:1b
00:00:21:d7:27:ea
00:05:5d:7b:18:12



8.2 System configuration

In the module **System** you can make basic settings of Gibraltar.

- **General settings:** System name, local time, time zone, email address of the administrator, default language, automatic updates, port where the GibADMIN listens for requests
- **Syslogs:** Show the system log and search within it.
- **Hard disk:** Integration of a hard disk.
- **Heartbeat:** Configuration of the high availability solution Heartbeat
- **Block Login Attempts**
- **Active Connections:** Lists all currently active connections with the firewall.

System configuration ?

General settings
Syslogs
Search the syslog
Configure HDD
High availability
Block Login Attempts
Active Connections

System name: esys-firewall

Domain:

Local time: Tue Mar 4 21:58:54 CET 2008 Reset time

Local time in UTC: Tue Mar 4 20:58:54 UTC 2008

Time zone:

Email of admin: separate the addresses with comma

Activate admin email: Interval admin email: hour(s)

Default language:

Enable automatic update: Every day at

Webinterface port:

Uptime: 3 d 8 h 00 min

Reboot
Shutdown

Save
Change password

8.2.1 System - General settings

The following settings can be made here:

- **System name:** host name of the Gibraltar firewall
- **Domain:** network domain (e.g. example.com); if you do not have your own public domain, enter "local".

NOTE: Host name and domain together are the "fully qualified domain name" (FQDN) of Gibraltar. This FQDN should be resolvable via DNS to ensure the correct sending of the administrator email addresses sent by Gibraltar itself. Many mail servers and spam filters use techniques to avoid getting emails from mail servers that do not have a resolvable FQDN. Please create a separate DNS A-Record for your Gibraltar firewall.

- **Local time:** The current system time. Press the button "Reset time" to synchronize Gibraltar with time servers in the Internet. Before you can do this Gibraltar must be connected to the Internet correctly. Please finish the configuration of the network settings first.
- **Local time in UTC:** Time in UTC (Universal Time Coordinated).
- **Time zone:** Selection of your time zone.
- **Email of admin:** The email address of the administrator. Gibraltar sends reports and error messages to this email address. Separate more than one email address by commas.
- **Activate admin mail:** Deactivate this check box if you do not want to get any status information from Gibraltar.
- **Interval admin mail:** Interval for the sending of status information mails.
- **Default language:** Set the language that should GibADMIN start with.
- **Enable automatic update:** Activate the automatic update mechanism of the Gibraltar firewall. The Gibraltar developers offer patches and security updates at their web servers. If you activate this option, Gibraltar downloads and installs them automatically. The interval for checking for new updates can be set aside.
- **Webinterface port:** Port to access the GibADMIN. If you do not want to access the web interface at the TCP port 443, you can change this option.
- **Uptime:** Shows how long Gibraltar is running without any disruption.

Change Port for access to webinterface

The web interface for Gibraltar (GibADMIN) is accessible at port 443 (HTTPS) by default. If you already use this port to run a secure website you can change the port of Gibraltar administration to another port (e.g. 8443).

After changing the access port, the web server of GibADMIN restarts, and you cannot access the GibADMIN at the usual port.

ATTENTION: It can take some time, until the web server is restarted for the web interface. You cannot access the GibADMIN during the restart.

Reboot: Reboots the Gibraltar firewall. You must acknowledge the reboot.

Shutdown: Shuts down the Gibraltar firewall. You must acknowledge the shutdown.

ATTENTION: With restarting or shutting down the system, GibADMIN goes offline. You can continue configuring Gibraltar via GibADMIN after a complete reboot of the system.

Changing the password

1. Choose **System** in the main menu.
2. Choose the card **General settings**.
3. **Change password**: Click this button to get redirected to an other form where you have to enter the new password twice. If the password does not match, an error message will be displayed.
4. **Save**: Confirm your changes with clicking the button **Save**. You have to enter the new password now to login again.

8.2.2 Syslogs

The syslog file records all relevant events for Gibraltar. The syslog is a important file to get information about the behaviour of the Gibraltar firewall. Examples for entries in the syslog:

- Dropped packets
- Starting and stopping of services/daemons
- Error messages

The following settings can be done here:

- **Number of logs**: Number of lines of the syslog that are shown at the GibADMIN.
- **Refresh frequency in seconds**: rate of actualization when the automatic refresh is activated.

Start refresh : Click this button to start the auto refresh .

Stop refresh : Click this button to stop the auto refresh.

ATTENTION: Do not choose an interval < 5 sec because stopping the refreshes could be very difficult.

- **IP of the external syslog server**: Enter the IP address of a syslog server that is running to get the syslogs from Gibraltar.
- **Allow syslog entries from other computers**: Activate this checkbox if you want to use Gibraltar as a syslog server for other computers. Note: you must add a firewall rule to accept packets from the UDP port 514 from the designated interface to LOCAL.

8.2.3 Search the syslog

Allows searching within the syslog file. Enter the text to search for in the text field and press Start. All lines containing the text to search for are shown below.

8.2.4 Configure hard disk

Before using a hard disk with Gibraltar the disk must be integrated into the system first. Basically the Gibraltar firewall works without hard disk. Some of the services need a hard disk to work properly (e.g. Proxy server). Only IDE or SATA hard disks can be used here.

WARNING: When you use a hard disk for Gibraltar, all files on this hard disk are deleted!

1. Choose **System** in the main menu.
2. Choose the card **Configure HDD**.
3. Choose from the selection field **Use hard disk** the hard disk, you want to use for Gibraltar. You can identify the right hard disk by the shown size. Note, that the chosen hard disk gets formatted, and all stored files will be deleted.
4. Click the button **Save** to format the chosen hard disk and prepare it for Gibraltar.
5. In the security inquiry afterwards, click the button **Yes**, if you are absolutely sure that by formatting the hard disk no important files get lost. Thereby the hard disk gets formatted. This can take a few minutes.
6. Afterwards Gibraltar has to be restarted, so that the hard disk can be embedded into the data system correctly. Before that, the configuration has to be stored. Therefore choose **Configuration management** from the main menu.
7. Choose the card **Save configuration**.
8. Choose your storage medium and click the button **Save**.
9. Choose **System** in the main menu.
10. Choose the button **Restart**, to reboot Gibraltar.
11. Click the button **Yes** to start the rebooting. Afterwards you loose the connection to the **GibADMIN**. You can login into the **GibADMIN** again after a few minutes, when Gibraltar finished the starting, in the usual way.

8.2.5 Heartbeat

The high availability service Heartbeat allows the usage of two Gibraltar firewalls in a failsafe mode. One Gibraltar is the main firewall (master), the other one is the backup firewall (slave). Both firewalls are connected at one port. If the master fails, the slave takes all the services and allows to work without any disruption.

Find a current and detailed description to configure Heartbeat at the Gibraltar web site www.gibraltar.at or ask our support team.

8.2.6 Block Login Attempts

This option avoids brute force attacks to SSH or the GibADMIN. The intruders cannot try more than the given number of passwords until their IP address is blocked.

1. Choose **System** in the main menu.
2. Choose the card **Block Login Attempts**.
3. **Check window:** Enter the number of seconds Gibraltar should count the login attempts. If you enter 30 seconds here Gibraltar counts the numbers of logins within this time interval.
4. **Amount of login attempts within check window:** Enter the number of login attempts that must be reached to block further login attempts. The login attempts must be within the check window to be counted for the blocking.
5. **Duration of blocking login attempts (in seconds):** If the number of login attempts is reached, the IP address is blocked for the number of seconds that is entered here.
6. **Save:** Confirm your changes by clicking the button **Save**.

8.2.7 Active Connections

Here you can see the currently active connections to Gibraltar.

You can see the following information in this overview:

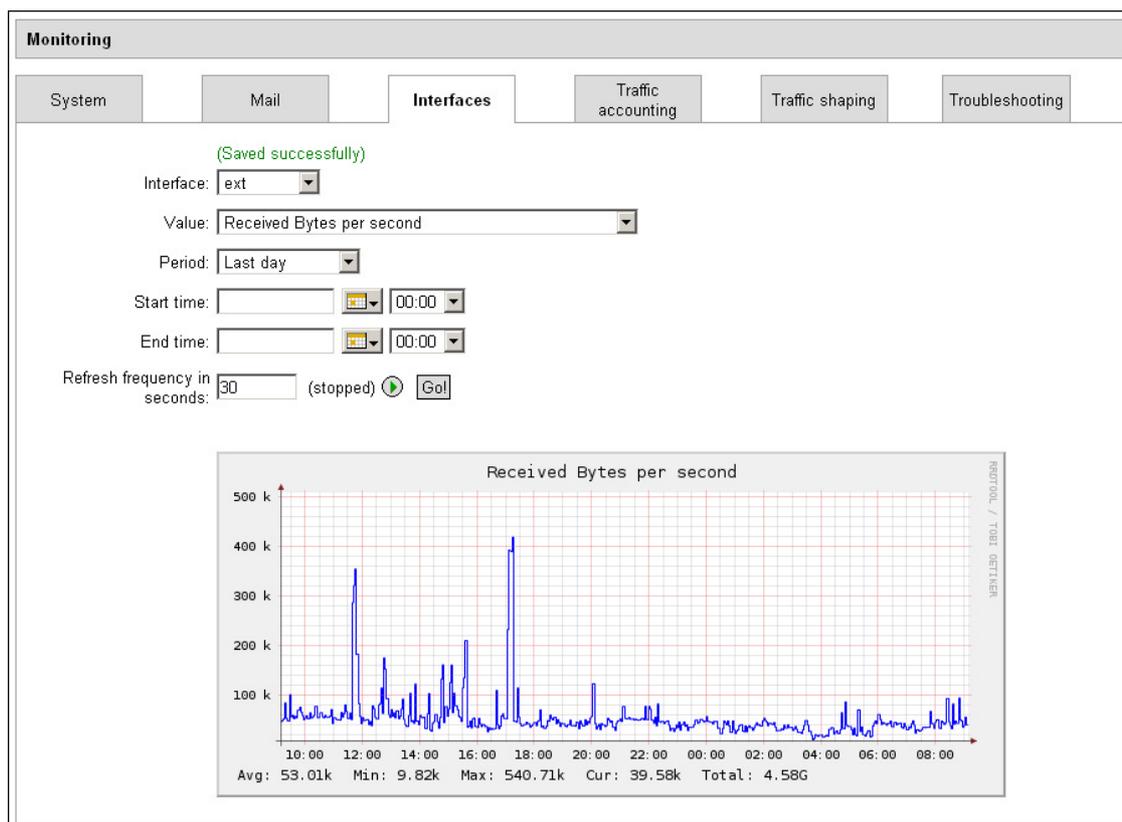
- **Source IP address:** The source IP of the packet.
- **Dest. IP address:** The destination IP of the packet.
- **Protocol:** Network protocol of the connection.
- **Source port**
- **Dest. port**
- **Time:** Time until the connection is closed automatically when not used.
- **State:** Current state

8.3 Monitoring

The module Monitoring offers some graphical reports to see what is happening at the Gibraltar Firewall.

The following overviews can be made:

- System reporting (CPU, memory)
- Mail reporting (incoming and outgoing mails)
- Interface reporting (received bytes, sent bytes)
- Traffic accounting (ad hoc defined monitoring-rules)
- Traffic shaping (inspection of the shaping-classes)



8.3.1 System

Shows information about your system (CPU load, memory usage).

- **Value:** Choose the category which you want to chart (CPU or memory)
- **Period:** Specify the period of reporting (choose CUSTOM to define a specific period)
- **Start time:** Insert date and time for the point of start of your reporting.

- **End time:** Insert date and time for the point of ending of your reporting.
- **Refresh frequency in seconds:** Enter a refresh frequency to periodically refresh your screen. A status beside the description field displays if the updating has yet been started or not.
- **Go!:** Click this button to generate the graph.

8.3.2 Mail

Shows information about incoming and outgoing E-Mails.

- **Value:** Choose the category which you want to chart (incoming or outgoing emails)
- **Period:** Specify the period of reporting (choose CUSTOM to define a specific period)
- **Start time:** Insert date and time for the point of start of your reporting.
- **End time:** Insert date and time for the point of ending of your reporting.
- **Refresh frequency in seconds:** Enter a refresh frequency to periodically refresh your screen. A status beside the description field displays if the updating has yet been started or not.
- **Go!:** Click this button to generate the graph.

8.3.3 Interfaces

Shows information about the traffic passing your network interfaces.

- **Interface:** Network interface card to chart
- **Value:** Choose the category which you want to chart
- **Period:** Specify the period of reporting (choose CUSTOM to define a specific period)
- **Start time:** Insert date and time for the point of start of your reporting.
- **End time:** Insert date and time for the point of ending of your reporting.
- **Refresh frequency in seconds:** Enter a refresh frequency to periodically refresh your screen. A status beside the description field displays if the updating has yet been started or not.
- **Go!:** Click this button to generate the graph.

8.3.4 Traffic accounting

Shows the charts for the rule you defined at **Traffic accounting**. You get a detailed reporting about your network traffic by creating monitoring rules at the Module [Firewall](#). You can create these monitoring rules for each filter rule of the packet filter and use them to analyze your network traffic.

This feature offers you e.g. the possibility to record the traffic to your web server. Therefore activate the check box at the firewall rule definition that allows traffic to the web server passing the firewall.

- **Select rule:** Choose the rule you activated monitoring for.
- **Value:** Choose the category which you want to chart (CPU or memory)
- **Period:** Specify the period of reporting (choose CUSTOM to define a specific period)
- **Start time:** Insert date and time for the point of start of your reporting.
- **End time:** Insert date and time for the point of ending of your reporting.
- **Refresh frequency in seconds:** Enter a refresh frequency to periodically refresh your screen. A status beside the description field displays if the updating has yet been started or not.
- **Go!:** Click this button to generate the graph.

8.3.5 Traffic shaping

Shows reports about the traffic shaping rules (bandwidth management). The configuration of such traffic shaping classes is described at the module [Traffic shaping](#). These charts should ensure a perfect configuration of bandwidth management and traffic shaping.

- **Track:** Choose the interface which the shaping rules were created for.
- **Shaping rule:** Choose the specific shaping rule to create charts for.
- **Value:** Choose the category which you want to chart (CPU or memory)
- **Period:** Specify the period of reporting (choose CUSTOM to define a specific period)
- **Start time:** Insert date and time for the point of start of your reporting.
- **End time:** Insert date and time for the point of ending of your reporting.
- **Refresh frequency in seconds:** Enter a refresh frequency to periodically refresh your screen. A status beside the description field displays if the updating has yet been started or not.
- **Go!:** Click this button to generate the graph.

8.3.6 Troubleshooting

In some situation the monitoring service stops working correctly and cannot be restarted or does not show charts.

To fix this state of failure you can press one of the buttons to re-initialize the monitoring service:

- **Re-Initialization:** Tries to re-initialize the monitoring service. Recorded data will not be deleted. If this action does not solve the problem you must delete the databases containing the recorded values.
- **Remove databases:** Deletes the recorded data and re-initializes the monitoring service.
- **Fix bug at Interfaces:** Deletes all recorded data of the traffic of each network interface. This button must be used after updating from release 2.4.1 to 2.5.

8.4 Services

Many features of the Gibraltar firewall depend on starting a specific service. Most of these features are additional services that are not essential for the basic functionality of the Gibraltar firewall. Therefore they are deactivated by default. If you need one of these additional features, start the specific service here.

Each of these services can be started, stopped, or restarted.

The following actions concerning services are available:

- **Start a service**
- **Stop a service**
- **Automatically start a service at boot time**

Description of the services:

- **Anon Anonymizer: Anon-Proxy:** Activates the HTTP anonymization solution Anon-Proxy
- **Block Login Attempts:** Activates the check for unauthorized login attempts
- **Captive Portal:** This feature is a hot-spot service that allows managing Internet connectivity by defining separate users. The duration of connection and the download volume can also be regulated.
- **DHCP relay:** Activates the forwarding of DHCP requests across the firewall.
- **DHCP server:** Activates the DHCP server of the firewall.
- **Dynamic DNS:** Use this feature if you do not have a static IP and if you want connect to the firewall anyway.
- **Freenet:** Activates the integrated anonymization software freenet.

- FTP proxy (incoming): FTP proxy for connections to an internal FTP server
- FTP proxy (outgoing): FTP proxy for connections to an external FTP server
- High availability: High availability service heartbeat to configure a second hardware in hot-standby
- HTTP proxy: Optionally transparent HTTP proxy
- IDS: Intrusion Detection System Snort
- IPSec: Service to manage IPSec/VPN tunnels
- Kaspersky anti virus: Checks HTTP, FTP and SMTP traffic with the Kaspersky AntiVirus software
- L2TP: Service to manage L2TP/IPSec VPN connections
- LDAP server: Integrated LDAP directory server to manage users for different services.
- Mail server: Activates the integrated mail relay that forwards incoming SMTP traffic to an internal mail server and optionally checks for spam or viruses
- Monitoring: Activates the service monitoring.
- OpenVPN: Activates the service OpenVPN to connect external workers via VPN with your office.
- POP3 proxy: Activates the POP3 proxy service.
- PPTP server: Activates the PPTP VPN solution to connect external workers via PPTP.
- PureSight Content Scanner: Activates the content checks of HTTP traffic using PureSight's CSDK.
- SMTP Content Scanner: Service that checks SMTP traffic passed through the firewall by the mail relay for viruses and spam.
- SSL Tunnel: Service to create SSL tunnels terminating at the firewall.
- SSL-VPN: Activates the SSL VPN service.
- Tor Anonymizer: Starts the anonymization service Tor.

ATTENTION: In certain cases, starting a service can fail and an error message will be displayed. For example you can not start the DHCP server if you have not activated any interface for DHCP.

ATTENTION: To check your mails for viruses and spam you must start the SMTP Content Scanner in the module Services.

Service settings

Services

Available services:

Name	Start automatically	State
Anon Anonymizer	<input type="radio"/> On <input checked="" type="radio"/> Off	(stopped)
Block Login Attempts	<input checked="" type="radio"/> On <input type="radio"/> Off	(started)
Captive Portal	<input type="radio"/> On <input checked="" type="radio"/> Off	(stopped)
DHCP relay	<input type="radio"/> On <input checked="" type="radio"/> Off	(stopped)
DHCP server	<input type="radio"/> On <input checked="" type="radio"/> Off	(stopped)
Dynamic DNS	<input type="radio"/> On <input checked="" type="radio"/> Off	(stopped)
Freenet	<input type="radio"/> On <input checked="" type="radio"/> Off	(stopped)
FTP proxy (incoming)	<input type="radio"/> On <input checked="" type="radio"/> Off	(stopped)
FTP proxy (outgoing)	<input type="radio"/> On <input checked="" type="radio"/> Off	(stopped)
High availability	<input checked="" type="radio"/> On <input type="radio"/> Off	(started)
HTTP proxy	<input checked="" type="radio"/> On <input type="radio"/> Off	(started)
IPSec	<input checked="" type="radio"/> On <input type="radio"/> Off	(started)
Kaspersky anti virus	<input checked="" type="radio"/> On <input type="radio"/> Off	(started)
L2TP	<input type="radio"/> On <input checked="" type="radio"/> Off	(stopped)
LDAP Server	<input checked="" type="radio"/> On <input type="radio"/> Off	(started)
Mail server	<input checked="" type="radio"/> On <input type="radio"/> Off	(started)
Monitoring	<input checked="" type="radio"/> On <input type="radio"/> Off	(started)
OpenVPN	<input checked="" type="radio"/> On <input type="radio"/> Off	(started)
POP3 proxy	<input type="radio"/> On <input checked="" type="radio"/> Off	(stopped)
PPTP server	<input checked="" type="radio"/> On <input type="radio"/> Off	(started)
PureSight Content Scanner	<input type="radio"/> On <input checked="" type="radio"/> Off	(stopped)
SMTP content scanner	<input checked="" type="radio"/> On <input type="radio"/> Off	(started)
SSL Tunnel	<input type="radio"/> On <input checked="" type="radio"/> Off	(stopped)
SSL-VPN	<input checked="" type="radio"/> On <input type="radio"/> Off	(started)
Tor Anonymizer	<input type="radio"/> On <input checked="" type="radio"/> Off	(stopped)

8.5 Network

8.5.1 Network

The module **Network** offers the following register cards.

- Internal and external DNS servers
- Network devices with addresses
- Routing
- Perform connection test
- Definition of host, or net aliases, groups and services to ease the generation of firewall rules
- Bridging
- VLAN definitions
- DHCP server
- dynamic DNS

The number of cards in this module depends on the number of network devices of Gibraltar. For each network device a register card is generated.

8.5.1.1 DNS

By adding external DNS servers Gibraltar forwards DNS request to these servers and does not use the root DNS servers to resolve DNS requests. Additionally you can add separate DNS servers for specific domains (for example internal Microsoft Windows DNS servers). With inserting the domain and the IP address of the DNS server the DNS requests get forwarded to the correct internal DNS server.

1. Choose **Network** in the main menu.
2. Choose the card **DNS**.
3. **External DNS Servers:** Enter here the IP addresses of the external DNS servers your provider offers to you. If you do not enter any DNS servers here, the root DNS servers will be used for resolving DNS names.
4. **Internal DNS Servers:** Enter pairs of the domain and the IP address. If Gibraltar receives a DNS request concerning one of the domains quoted, Gibraltar forwards the request to the according IP address. Mostly used are internal DNS servers (e.g. internaldns.esys.at).
5. **Add server:** Click this button to add a new DNS server.
6. **Delete marked entries** : Mark the entries in the element group by activating the checkbox and click this button in the heading line afterwards to delete the marked entries.
7. **Delete Server** : Click this button to delete a DNS server.
8. **Save:** Confirm your changes with clicking the button **Save**.

8.5.1.2 Network interface

Each network interface in **GibADMIN** is represented as a card on which the various settings like name, static or dynamic IP and starting or stopping the interface can be performed.

- **State:** Shows the current state of the network interface: **(started)** or **(stopped)**.
Start interface : Click this button to start the interface if the current state is **(stopped)**.
Stop interface : Click this button to stop the interface if the current state is **(started)**.
- **MAC address:** Shows the worldwide unique MAC address of the network interface card.

TIP: To identify the network interfaces for configuring with GibADMIN, you should write the MAC address on each network interface card. This will help you to connect to the correct network interface card.

- **Interface:** Enter a descriptive name for the network card to simplify the configuration of Gibraltar. You can for example enter the names ("ext0", "ext1" ...) for your external IP addresses and ("int0", "int1" ...) for your internal IP addresses. The name must not be "lo" nor start with "eth", "ppp", "slip", "ipsec", "sit" and "wlan". Changing the name for the network interface card later might cause problems with the firewall rules.
- **Start automatically:** Mark this checkbox if you want the network interface to start automatically when Gibraltar boots.
- **IP address:** The option fields **dynamic** and **static** fix the allocation for IP addresses for this network interface. If you choose **dynamic**, the network interface searches for a DHCP server while booting, which transmits the IP address and further network settings. If you choose **static** you have to enter one (or more) IP address(es) by clicking the button **Add IP**. This IP address(es) has (have) to be up to the [CIDR-Notation](#) (e.g: 192.168.0.10/24 for the IP address 192.168.0.10 with subnet mask 255.255.255.0) to set beside the IP address also the number of bits (subnet mask) used for the identification of the network. You can delete the entries in the element group by activating the checkbox and clicking the button **Delete marked entries**  in the heading line afterwards. If you want to delete only one entry, click the button **Delete IP address**  besides the entry.
- **Speed and Duplex mode:** Select the speed of your network connection here. If your Internet-Provider requires special network settings for communication with your modem, you have to change this here.

ATTENTION: When you change the settings of the network interface card, with which you are configuring GibADMIN, the connection can be interrupted!

ATTENTION: If you change the settings of the network interface card, that builds the connection to the default gateway, you also have to check or maybe reconfigure the settings on the card Routing.

- **Save:** Confirm your changes with clicking the button **Save**.

The screenshot shows a window titled "Network settings" with a help icon in the top right corner. Below the title bar are five tabs: "DNS", "ext", "int", "Routing", and "Connection test". The "ext" tab is selected. The main content area displays the following information:

- State: (started) with a red stop icon.
- MAC address: 00:0c:6e:86:c0:23
- Interface: ext (in a text box)
- Start automatically:
- IP address: dynamic static
- Static IPs: A table with a header "IP address/netmask" and a single row containing "80.50.30.50/24" and a checkbox with an "x" icon.
- An "Add IP" button below the static IP table.
- A "Save" button at the bottom.

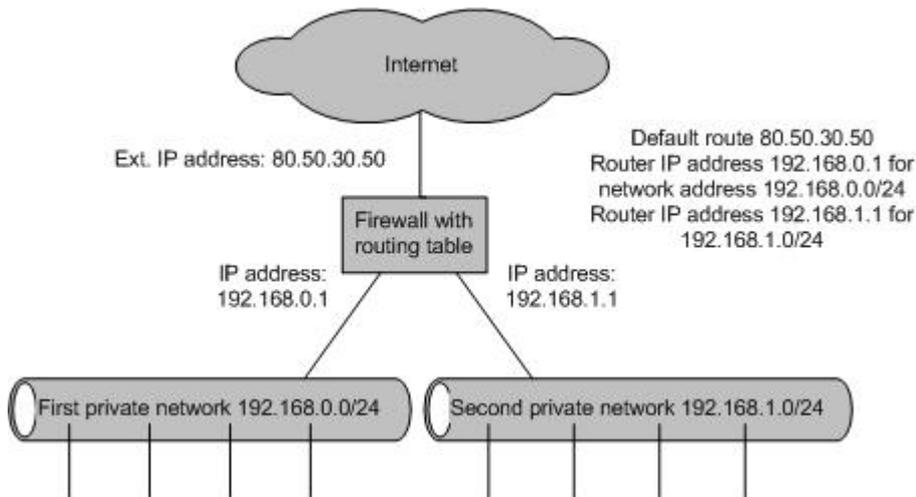
Bridges

If a network interface is part of a bridge, it's no reasonable to set the IP address. That's why network interfaces that are assigned to a bridge, aren't reachable. They are marked by the note **(bridged)** in the head of the tab.

Once a bridge is set, an additional tab for the configuration of the bridge will be created. On this new tab the IP address of the bridge can be configured. Also deleting the bridge happens on this tab.

8.5.1.3 Routing

Routing is concerned for forwarding data packages. Every packet will be examined whether it fits to one of the network addresses that are in the routing table. If it fits, it will be forwarded to the specified router IP. If it doesn't fit to any network address, the packet will be forwarded to the default route.



- **Default route:** Enter the IP address for the default route in this text field. The packets that don't fit to any other route are forwarded to this IP address.
- **Additional routes:** This element group lists all additional routes.
- **Router IP address:** Enter the IP address of the router that should receive IP packets.
- **Network address:** Enter the network address of the destination network. If a packet fits to one of the addresses it will be forwarded to the suitable router.
- **Add Route:** Click this button to insert a new route.
- **Delete route** (⊗): Click this button to delete a route.
- **Delete marked entries** (⊗): Mark the entries in the element group by activating the checkbox and click this button in the heading line afterwards to delete the marked entries.
- **Save:** Confirm your changes with clicking the button **Save**.

Network settings ?

DNS ext int **Routing** Connection test

Default route:

Additional routes:

Router IP address	Network address	⊗
<input type="text" value="192.168.0.1"/>	<input type="text" value="192.168.0.0/24"/>	<input type="checkbox"/> ⊗

8.5.1.4 Connection test

The card **Connection test** offers the possibility to check your Internet connection.

1. Choose **Network** in the main menu.
2. Choose the tab **Connection test**.
3. **Host:** Enter the IP address or the name of the host to which you want to test your connection (e.g: 10.11.12.13 or www.esys.at).
4. **Action:** Choose one of the listed commands (ping or traceroute). The command **ping** sends ICMP packets to the host. If you get answer packets the connection is o.k else you have to check your default route or **Dial-in** settings. The command **traceroute** lists all steps between Gibraltar and the host if the connection is o.k.
5. **Test:** Click this button to start the test and send ICMP packets to the denoted host.
6. **Back:** By clicking this button you get back to the start display of this tab.

The screenshot shows a web interface for network settings. At the top, there's a header 'Network settings' with a help icon. Below it are several tabs: 'DNS', 'ext', 'int', 'Routing', and 'Connection test'. The 'Connection test' tab is active. Inside this tab, there's a 'Host' input field containing '192.168.0.17', an 'Action' dropdown menu set to 'ping', and a 'Test' button below them.

8.5.2 Definitions

In order to simplify the configuration and maintenance of the firewall it is recommended to define aliases for hosts and services. These aliases can then be assembled to named groups. The administrator can use names instead of IP addresses, ports and network ranges. Create an alias **webserver1** for the IP address of your internal web server for example. Another advantage is that you only must edit the IP address at one place if one is changed.

Another useful feature is the definition of services. Assemble some protocols and ports to a single service. This service can be used in firewall and nat rules definition instead of creating many rules for every single port.

EXAMPLE: Create a service web containing TCP ports 80 and 443. This service can be used to allow reaching a web server by defining the firewall rules.

8.5.2.1 Host/Net aliases

A Host/Net alias is a name for a single IP address (Host), for a network range or for a FQDN.

You can define as many aliases as you want. A single alias contains the following elements:

- **Name:** Choose a name for the host you will recognize again.
- **IP/network address/FQDN:** A single IP address, a network address or a FQDN. A network address must be entered in CIDR notation (e.g. 192.168.0.0/24).
- **MAC address:** MAC address should only be used in special situations (e.g. providers who want to bind the rules to special MAC addresses of their clients).

8.5.2.2 Host/Net groups

Host/Net aliases can be merged to Host/Net groups to simplify the configuration and maintenance of the firewall. If several hosts should have the same permissions for some network areas you can merge them into a group and allow the traffic for that group by creating only one rule instead of one rule for every host. If the hosts within the group change, you only must change the members of the group and not the firewall rules.

The overview shows the existing groups and its members. You can define new groups and edit the existing ones.

Members in groups must be defined before as aliases.

8.5.2.3 Services

Single protocols and ports can be merged to a service to simplify the configuration and maintenance of the firewall. Some of the most common services are predefined. You can add or edit the services list as you need.

A service contains the following information:

- **Name:** A name for the service to recognize it when use it within rule definition.
- **Protocol:** Network protocol (must be used).
- **Source port:** Is not necessary at most of the services because it is chosen at random.

- **Destination port:** Port 80 for http for example.

8.5.2.4 Additional interfaces

Additional interfaces are virtual interfaces that are not existing all the time (e.g. dial in connections). In order to create firewall rules also for these interfaces you must predefine them here. Additional interfaces can be used as incoming or outgoing interface at the rule definition form.

A dial in connection (point-to-point) gets the interface name **ppp** with the current number attached (first connection: "ppp0", second connection "ppp1", ...). It is possible to create more than one point-to-point connections. In order to create firewall rules for all these point-to-point connections you can use the interface name **ppp+** which represents all pppX interfaces. As these point-to-point connections are very common ppp+ is part of the default config.

8.5.3 Dial-In

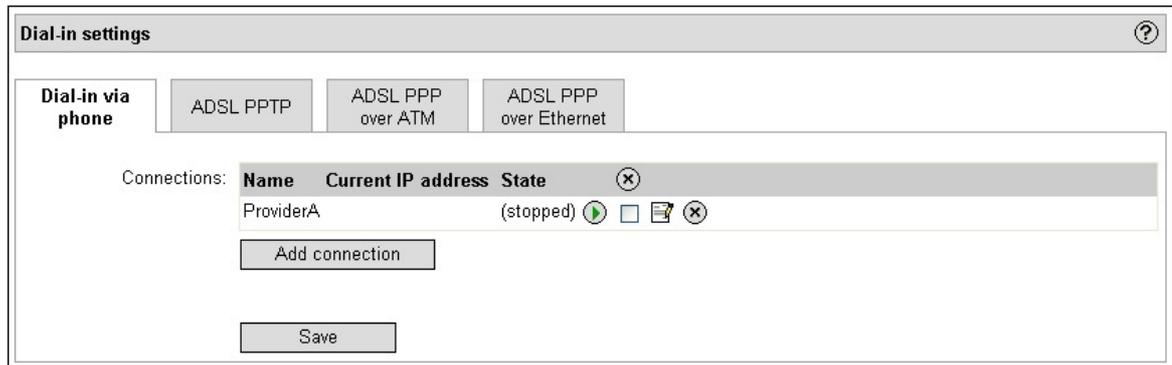
The module **Dial-In** offers the possibility to configure your dial-in via modem - connections and your ADSL connections.

8.5.3.1 Dial-in via phone

The card **Dial-in via phone** shows all possible dial-in connections via a modem. Furthermore you have the possibility to configure, delete, create or stop the connection.

1. Choose **Dial-in** in the main menu.
2. Choose the card **Dial-in via phone**.
3. **Connections:** This element group shows all possible dial-in connections via modem.
4. **Name:** Shows the name of the connection.
5. **Current IP address:** Shows the currently assigned IP address.
6. **State:** Shows the state of the connection: **(started)** or **(stopped)**.
 - **Start connection**  : Click this button to start the connection if the current state is **(stopped)**.
 - **Stop connection**  : Click this button to stop the connection if the current state is **(started)**.
7. **Delete marked entries**  : Mark the entries in the element group by activating the checkbox and click this button in the heading line afterwards to delete the marked entries.
8. **Edit connection**  : Click this button to edit the connection. The browser will redirect to a [detail](#) form, where you can configure the connection.
9. **Delete connection**  : Click this button to delete a connection.
10. **Add connection:** Click this button to add a new connection. The browser will redirect to a [detail](#) form where you can configure the connection.
11. **Save:** Confirm your changes with clicking the button **Save**.

ATTENTION: To create filter rules for this dial-in connection you must use the ppp+ interface in the filter rules form, because this is used for the traffic in this case.



8.5.3.1.1 Dial-in detail view

In the detail view of the card **Dial-in via phone** you can configure your dial-in connection via modem. For your configuration you will need the access data from your provider (username, password, dial-in number, ...).

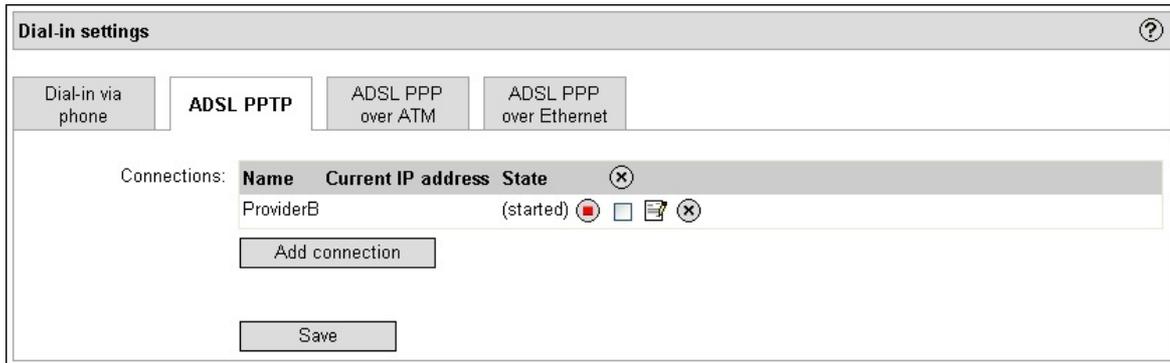
- **Name:** Choose a name for the connection which will be shown in the overview. The name must be unique in all dial-in connections (also ADSL).
- **Authorization:** Choose the authorization type that you can read out of the information you got from your provider.
- **Username:** The username you got from your provider.
- **Password and Password (confirmation):** The password you got from your provider.
- **Port speed (bit/s):** Connection speed of the modem.
- **Type of dialing**
- **Wait for dial tone:** Mark this checkbox if the firewall should wait for a dial tone before starting the connection.
- **Phone number:** Enter the phone number of your provider in this text field.
- **Port:** Choose the port you have connected your modem to from this select box.
- **Default route:** Mark this checkbox if you want to use this connection as the default route.
- **Replace default route:** Replaces the existing default route when the connection comes up.
- **Dial on Demand:** Mark this checkbox if you want the modem to start the connection automatically if any user tries to connect to the Internet.
- **Keep up connection:** The firewall connects automatically after an unwanted interruption.
- **Idle (seconds):** Enter the value for the idle time in this textfield. The value for the idle indicates that Gibraltar should keep the connection up for a certain time although no traffic is passing it. If you insert a value of 30 for idle, Gibraltar waits 30 seconds after the last traffic before it stops the connection.
- **Holdoff (seconds):** Enter the value for the holdoff time in this textfield. The value for the holdoff indicates that Gibraltar should wait for a certain time after stopping a connection before starting the connection again. If you insert a value of 30 for holdoff, Gibraltar waits a minimum of 30 seconds after the last stopping of a connection before it connects again (although a user might tries to connect to the Internet after 10 seconds).
- **Rename dial-in interface:** You can use a special name for the interface instead of ppp0.
- **Routed networks:** Networks that should be routed after connection comes up.
- **Static IPs:** If you have got more than one static IPs from your provider you can enter them here.

8.5.3.2 ADSL PPTP

The firewall can be used to connect to the Internet by using a ADSL PPTP connection. You can add several PPTP connections here. The list shows an overview over the existing connections. You can add, edit or delete connections here. If a connection is up you can see the current IP address of it.

ADSL-PPTP connections can be started and stopped as you need.

ATTENTION: To create filter rules for this dial-in connection you must use the ppp+ interface in the filter rules form, because this is used for the traffic in this case.



8.5.3.2.1 ADSL PPTP detail view

In the detail view of the card ADSL PPTP you can configure your dial-in connection. For your configuration you will need the access data from your provider (username, password, ...).

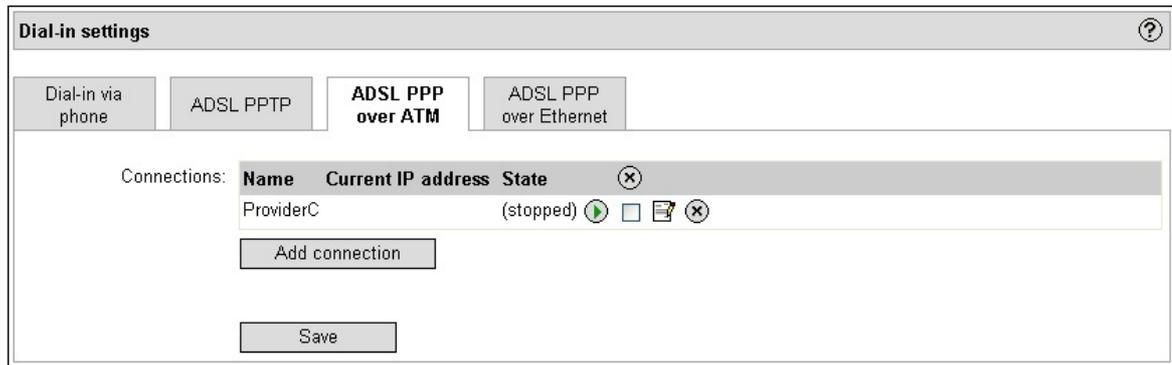
- **Name:** Choose a name for the connection which will be shown in the overview. The name must be unique in all dial-in connections
- **IP address of modem:** IP address of the PPTP modem
- **Username:** The username you got from your provider.
- **Password and Password (confirmation):** The password you got from your provider.
- **Start automatically:** Mark this checkbox if the firewall should start the connection after a reboot.
- **Default route:** Mark this checkbox if you want to use this connection as the default route.
- **Replace default route:** Replaces the existing default route when the connection comes up.
- **Dial on Demand:** Mark this checkbox if you want the modem to start the connection automatically if any user tries to connect to the Internet.
- **Keep up connection:** The firewall connects automatically after an unwanted interruption.
- **Idle (seconds):** Enter the value for the idle time in this textfield. The value for the idle indicates that Gibraltar should keep the connection up for a certain time although no traffic is passing it. If you insert a value of 30 for idle, Gibraltar waits 30 seconds after the last traffic before it stops the connection.
- **Use MPPE:** Use the Microsoft Point-to-Point Encryption protocol to encrypt the data.
- **Rename dial-in interface:** You can use a special name for the interface instead of ppp0.
- **Routed networks:** Networks that should be routed after connection comes up.
- **Static IPs:** If you have got more than one static IPs from your provider you can enter them here.

8.5.3.3 ADSL PPP over ATM

The firewall software can be used to create a connection via ADSL PPP over ATM. The list shows an overview over the existing connections. You can add, edit or delete connections here. If a connection is up you can see the current IP address of it.

ADSL PPP connections can be started and stopped as you need.

ATTENTION: To create filter rules for this dial-in connection you must use the ppp+ interface in the filter rules form, because this is used for the traffic in this case.



8.5.3.3.1 ADSL PPP detail view

In the detail view of the card ADSL PPP over ATM you can configure your dial-in connection. For your configuration you will need the access data from your provider (username, password, ...).

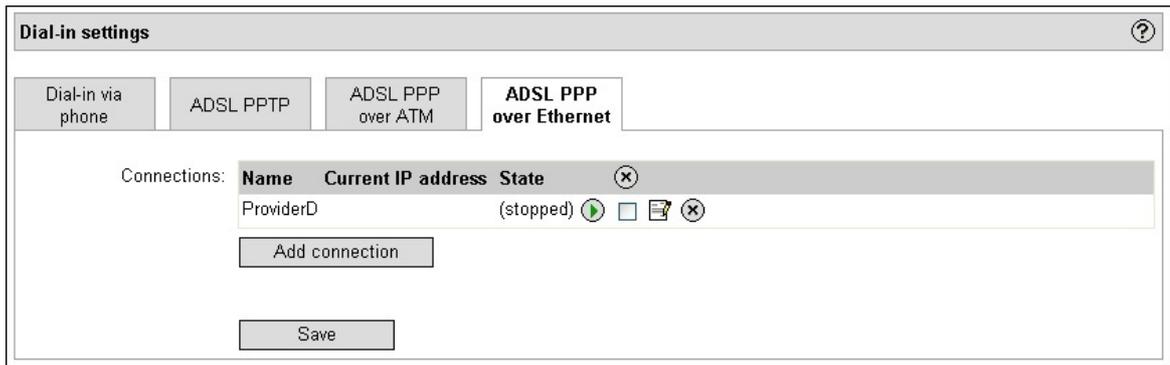
- **Name:** Choose a name for the connection which will be shown in the overview. The name must be unique in all dial-in connections.
- **Authorization:** Choose the authorization type that you can read out of the information you got from your provider.
- **VPI/VCI ATM Pair:** Values for Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) you got from your provider.
- **Username:** The username you got from your provider.
- **Password and Password (confirmation):** The password you got from your provider.
- **Start automatically:** Mark this checkbox if the firewall should start the connection after a reboot.
- **Default route:** Mark this checkbox if you want to use this connection as the default route.
- **Replace default route:** Replaces the existing default route when the connection comes up.
- **Dial on Demand:** Mark this checkbox if you want the modem to start the connection automatically if any user tries to connect to the Internet.
- **Keep up connection:** The firewall connects automatically after an unwanted interruption.
- **Idle (seconds):** Enter the value for the idle time in this textfield. The value for the idle indicates that Gibraltar should keep the connection up for a certain time although no traffic is passing it. If you insert a value of 30 for idle, Gibraltar waits 30 seconds after the last traffic before it stops the connection.
- **Use MPPE:** Use the Microsoft Point-to-Point Encryption protocol to encrypt the data.
- **Rename dial-in interface:** You can use a special name for the interface instead of ppp0.
- **Routed networks:** Networks that should be routed after connection comes up.
- **Static IPs:** If you have got more than one static IPs from your provider you can enter them here.

8.5.3.4 ADSL PPP over Ethernet

The firewall software can be used to create a connection via ADSL PPP over Ethernet. The list shows an overview over the existing connections. You can add, edit or delete connections here. If a connection is up you can see the current IP address of it.

ADSL PPP connections can be started and stopped as you need.

ATTENTION: To create filter rules for this dial-in connection you must use the ppp+ interface in the filter rules form, because this is used for the traffic in this case.



8.5.3.4.1 ADSL PPP over Ethernet detail view

In the detail view of the card ADSL PPP over ATM you can configure your dial-in connection. For your configuration you will need the access data from your provider (username, password, ...).

- **Name:** Choose a name for the connection which will be shown in the overview. The name must be unique in all dial-in connections.
- **Interface:** Choose the interface that is connected to the modem of your provider.
- **Authorization:** Choose the authorization type that you can read out of the information you got from your provider.
- **Username:** The username you got from your provider.
- **Password and Password (confirmation):** The password you got from your provider.
- **Start automatically:** Mark this checkbox if the firewall should start the connection after a reboot.
- **Default route:** Mark this checkbox if you want to use this connection as the default route.
- **Replace default route:** Replaces the existing default route when the connection comes up.
- **Dial on Demand:** Mark this checkbox if you want the modem to start the connection automatically if any user tries to connect to the Internet.
- **Keep up connection:** The firewall connects automatically after an unwanted interruption.
- **Idle (seconds):** Enter the value for the idle time in this textfield. The value for the idle indicates that Gibraltar should keep the connection up for a certain time although no traffic is passing it. If you insert a value of 30 for idle, Gibraltar waits 30 seconds after the last traffic before it stops the connection.
- **Maximum transmit unit (MTU)**
- **Maximum receive unit (MRU)**
- **Rename dial-in interface:** You can use a special name for the interface instead of ppp0.
- **Routed networks:** Networks that should be routed after connection comes up.
- **Static IPs:** If you have got more than one static IPs from your provider you can enter them here.

8.5.4 Bridging

At this form you can connect two or more network interfaces to a bridge. A bridge connects two or more network segments on layer 2 of the ISO/OSI model. The firewall is a so called MAC bridge which means that the firewall stores the MAC addresses of all devices connected to the bridge interfaces. If a request for a special MAC address in this table is coming in it is forwarded to the correct network interface of the bridge.

By using a bridge the firewall can be used transparently at the layer 3 (IP layer) of the ISO/OSI model and can forward an official IP to an internal server without even recognizing the existence of the firewall. Nevertheless the traffic is filtered and checked.

Because the traffic is crossing the interfaces transparently, no routing or NAT is needed. The bridges are mostly used when the firewall works as a transparent traffic shaper or as a transparent intrusion detection system (IDS) because it can be integrated in an existing network very easily. Nothing must be changed at the existing infrastructure.

ATTENTION: Use bridging of two or more network interfaces only if you completely understand the logic of the technique. Improper use of this service can lead to security

vulnerabilities.

- **Interface:** Name of the bridge interface (can be defined by you).
- **Static IPs:** Enter IP addresses, that should be assigned to the bridge.
- **Add IP:** Click this button to allocate a new IP address to the bridge.
- **Delete IP address:** Click this button to delete the according IP address.
- **Bridged interfaces:** Choose the interfaces that should become a part of this bridge. The bridge will connect the network segments that are attached to these interfaces.

NOTE: Creating the bridge after clicking the button Save can take a few minutes. Please be patient.

8.5.5 VLAN

The firewall supports the usage of virtual local area networks (VLAN). A VLAN is a virtual network within a physical network. The usage of VLAN is especially in the following cases reasonable:

- The load of broadcasts in the LAN is getting too high. This can happen especially in Microsoft Windows environments.
- A big switched network should be divided up because of security reasons.

A solution for the problems above is the usage of VLANs. VLANs can be created at one switch or over several switches and can also be used for multi-site networks. Creating VLANs is not so extensive than using separated routers and switches to divide the physical networks.

How does it work

Each VLAN receives an own definite number. This number is called VLAN ID. A device with VLAN ID 1, is able to communicate with every other device in the same VLAN, but not with a device in another VLAN with the ID=2,3,...

- **Physical Interface:** Choose the physical interface that should host VLAN interfaces.
- **Logical Interface:** Enter the name of the Interface.
- **VLAN ID:** Assign the VLAN ID for the virtual interface here. Note that you have to assign the VLAN ID to the switch also.
- **Static IPs:** Set the IP address that should be assigned to the new VLAN interface.

NOTE: Creating the VLAN interface after clicking the button "Save" can take a few minutes. Please be patient.

8.5.6 DHCP server

The module **DHCP server** offers the possibility to enable dynamic IP allocation in your local network. If a new computer is integrated into the network, it can get an IP address from the available range of the **DHCP server** via DHCP. At the same time he gets other network settings (default route, DNS server etc.) and doesn't have to be configured by the network administrator manually.

In **GibADMIN** you have the possibility to configure a DHCP server for every network interface. Therefore a further card for every network interface with static IP addresses is available, besides the card **General settings** .

8.5.6.1 DHCP - general settings

On the card **General settings** you can set the domain, in which the DHCP server is located and in which computers, that get assigned an IP address from this DHCP server should be.

1. Choose **DHCP server** in the main menu.
2. Choose the card **General settings**.
3. **Domain:** Enter the name of the domain a client should be assigned to in this textfield.
4. **Save:** Confirm your changes with clicking the button **Save**.

ATTENTION: Running more than one DHCP server in your physical network can lead to undesirable side effects and complications.

8.5.6.2 DHCP - configuration

If you want to offer network settings with a DHCP server, you must configure the settings of each network interface that should offer network settings.

Activate DHCP: Activates the DHCP server at the selected network interface.

IP address: Select the IP address where the DHCP server should answer DHCP requests of the clients.

IP range: Set the IP range that should be available for the clients. Enter the first and the last IP of the range.

DNS server: IP addresses of the DNS servers that are transmitted to the clients.

Router: The IP address of the router (default gateway, standard route) transmitted to the client.

WINS server: IP addresses of WINS servers that are transmitted to the clients.

NTP server: IP address of NTP (network time protocol) servers.

TFTP server IP or hostname: IP address or hostname of a TFTP server that can offer information for devices that load their system or system configuration over the network (e.g. VoIP devices).

Reservations: Assign a specified IP address to a specific network device defined by a specific MAC address. These reservations can be used for WLAN clients for example so that other devices will not get an IP address.

8.5.6.3 DHCP leases

Shows a list with currently connected DHCP clients. A lease is the time period where the DHCP server preserves a special IP for a DHCP client.

- **IP address:** The IP address of the client.
- **Hostname:** Hostname of the client.
- **MAC address:** MAC address of the network interface card that got this address.
- **Lease begin (UTC):** Timestamp when the client got this IP address.
- **Lease end (UTC):** Timestamp until the IP address is preserved for the MAC address.

8.5.6.4 DHCP relay

A DHCP relay is needed to forward DHCP request of a client to another network segment (the DHCP server is located in a different network segment than the clients).

IP address of the DHCP server: The IP address of the DHCP server where the requests should be forwarded to.

DHCP relay: Choose the interfaces which are part of the DHCP relay (also the interface where the DHCP server is connected to).

ATTENTION: Additionally to starting the services at the module services you must add a firewall rule to allow DHCP packets from the clients' network segment to the server network segment.

8.5.6.5 Dynamic DNS

With Dynamic DNS (DDNS) you can assign a host name (Fully Qualified Domain Name FQDN) for your official IP address, even if this IP address is assigned dynamically. Therefore you have to set an account at your contractor of this service (<http://www.dyndns.org> offers the possibility to get up to five free host name entries).

- **Update on dialing in:** Mark this checkbox, if the IP address on your host name should be assigned new whenever you dial in.
- **Update Interval (minutes):** Enter the interval, in which the IP address should be assigned new to your host name. This update will only occur, when the IP address changed in the meanwhile.
- **Hostname:** Enter here the host name, you choose for the Gibraltar firewall in the DynDNS.
- **Login:** Enter the username for your account, you choose in the DynDNS.
- **Password:** Enter the password for your account at DynDNS.
- **Current IP address:** Here you are shown the current IP address, that Gibraltar got assigned.

8.6 Firewall-rules

At the module Firewall the filter rules of the packet filter are defined. This is the core feature of a firewall. You must define which packets may pass the firewall, which should be blocked or logged. To specify which packets you mean the rules define some filters to select the specific packets. A firewall rule (policy) is created for an incoming and an outgoing interface (Track).

NOTE: The firewall is blocking all traffic by default. Only the web interface and the secure shell can be reached at each interface. Therefore, if the firewall is not configured, it is no security leak, but blocks all traffic - also from internal interface to external.

8.6.1 Firewall rules

Choosing the incoming and outgoing interfaces

In the overview "Firewall rules" you can see the rules which are filtered by the incoming and the outgoing interface. A overview over all active firewall rules can be shown at the specific register card.

In order to create a new filter rule you must select the incoming and the outgoing interface. The rule only filters packets that are incoming at the incoming interface and leave the firewall through the outgoing interface. The way of the packet is called Track in this manual.

If you plan to filter a packet from the internal to the external interface, select the internal interface at the select box **incoming** (e.g. "int0") and the external interface at the select box **outgoing**. Then press the button Go! right beside the select box for the outgoing interfaces and the rules of the selected track are shown below.

There are some special entries in the select box. Choose "**ANY**" when you do not want to filter the packets for a specific interface. The filter rules are active for all available interfaces.

"**LOCAL**" means those packets that originate directly from the firewall or that are sent to the firewall itself. This can be a request to a local proxy or packets for creating VPN tunnels (ipsec, PPTP). You can create a filter for all packets that reach the firewall by passing one special interface by selecting the interface at the incoming select box and by using LOCAL at the outgoing side. If you have already configured some IPsec tunnels the interfaces are also shown in the select boxes (e.g. "ipsec0").

TIP: The selection of the incoming interface "ANY" and outgoing interface "ANY" denote FORWARD-filter rules (packets going through the firewall are checked), where incoming and outgoing interface are not relevant. But therewith no INPUT- or OUTPUT-filter rules can be created (packets determined for the firewall and packets coming from the firewall).

Configuration of dynamic packet filter (Stateful Inspection)

Dynamic packet filtering allows to filter packets that can be associated to an existing connection (connection tracking). This technique is used to allow reply packets automatically. There is no need to create a separate rule for the replies. E.g. if you want to allow the access to a web server, you need only to add a rule to allow traffic for the destination port 80 from internal to external interface at a firewall that supports stateful inspection. The replies to the http requests are allowed to pass the firewall automatically.

Allow established: Allow all packets that are part of a already established connection. This means the replies a http server sends when it gets the requests from a client from the net behind the firewall for example. This setting is valid for all packets in the current track (incoming and outgoing interface).

Allow related: Allow all packets that can be bound to an already established connection. The best example for this setting is the ftp-data port. To allow FTP traffic you only must allow traffic to pass the firewall at port TCP/21. This port is used for ftp session communication. The ftp data is sent to another port (normally port 20). There is no extra rule needed if Allow related is activated.

Change the order of the rules

The order of the firewall rules is important. They are executed top-down. The current order of the firewall rules can be changed by using the "Move" fields or by using the arrow buttons on the right side of the rule definition.

Firewall rules

Interface: incoming: ANY outgoing: ANY Go!

State: Allow established Allow related

Move: From index: To index: Go!

Save Add rule

Active	Source	Destination	Protocol	Source port	Dest. port	Action	
<input checked="" type="checkbox"/>	ANY	ANY	TCP	ANY	ANY	flood-protect	ⓘ □ ▲ ▼ ↻ ⊞ ⊗
<input checked="" type="checkbox"/>	ANY	ANY	TCP	ANY	ANY	flood-protect	ⓘ □ ▲ ▼ ↻ ⊞ ⊗
<input checked="" type="checkbox"/>	ANY	ANY	ICMP	ANY	ANY	flood-protect	ⓘ □ ▲ ▼ ↻ ⊞ ⊗
<input checked="" type="checkbox"/>	ANY	ANY	ANY	ANY	ANY		□ ▲ ▼ ↻ ⊞ ⊗
<input checked="" type="checkbox"/>	ANY	ANY	ANY	ANY	ANY	●	□ ▲ ▼ ↻ ⊞ ⊗

Add rule

Save

Overview over the packet filter rules

The filter rules are executed top down until one of the rules matches the fields of the incoming packet. Therefore the order of the rules is very important. After selecting an incoming and an outgoing interface the filter rules for the specified track are shown in the list below. In this list you can change the order of the rules and edit or delete rules.

- Add rule: Create a new packet filter rule at the end of the currently selected list. The detailed view of the rule is opened. This button is at the top and at the bottom of the element group.
- Save: Saves the current settings and the order of the rules. This button must also be

pressed when you deleted a rule.

The following fields are shown in the overview:

- **Active:** Activate or deactivate the filter rule. Deactivated rules are not executed.
- **Source:** Shows the source IP/source net/source FQDN of the rule. If you do not set the source IP (ANY), this filter field is ignored and all source addresses match.
- **Destination:** Shows the destination IP/destination net/destination FQDN of the rule. If you do not set the destination IP (ANY), this filter field is ignored and all destination addresses match.
- **Service:** Shows the service of the rule.
- **Source port:** Source port of the rule. This option is only shown when you selected CUSTOM at the option Service.
- **Destination port:** Destination port of the rule. This option is only shown when you selected CUSTOM at the option Service.
- **Action:** Shows the action that is executed when the packet matches the filter rule. The following options are available: ACCEPT, DROP, LOG, REJECT, and NONE.
 - **ACCEPT:** The packet is forwarded.
 - **DROP:** The packet is dropped.
 - **LOG:** Creates an entry in the syslog. This option does not drop or accept the packet. You also must add another rule after the LOG rule to accept or drop the packet.
 - **REJECT:** Stops the packet as the option DROP, but also sends an ICMP message to the sender of the packet ("port-unreachable").
 - **NONE:** The packet is ignored by the filter. This option is only needed for monitoring special packets where you do not want to set an action.
 - If overview shows some other actions like "flood-protect" or something else, the rule is a default rule that cannot be edited or deleted by the user.
- **Comment** ⓘ: Shows a tooltip with the comment of the rule. Go to the picture with your mouse pointer and you can read it. You can create your own comments to each rule.
- **Delete marked entries** ✕: Delete all rules you have selected in the column below. Do not forget to press the button "Save" afterwards.
- **Move up** ▲ or **down** ▼: You can change the order of the rules by pressing these buttons. The order of the rules is very important. Do not forget to press the button "Save" afterwards.
- **Edit rule** 📄: Press this button to go to the detailed view of the rule and edit the options.
- **Insert rule below** ➕: Press this button when you want to add a new rule below the current rule. You are forwarded to the detailed view of a new rule.
- **Delete rule** ✕: Press this button to delete the rule.

8.6.2 Overview active rules

This overview shows all active rules independently of their incoming and outgoing interfaces. Additionally to the columns you can also see in the overview of a special track you can see another column that shows the track of the rule.

It is not possible to create new rules here. The existing rules can be edited and deleted.

8.6.3 Firewall - Extended Settings

At the extended settings you can configure the following settings for the packet filter:

- **DNS refresh rate:** If you use hostnames in the firewall rules this option defines the interval when the hostnames are resolved to IP addresses by asking the DNS servers. The firewall rules are refreshed by this action.
- **Maximum concurrent connections:** Depends of the size of the RAM.
- **TCP liberal:** Deactivates the strong TCP checks. TCP connections are not interrupted when

the connection produces INVALID packets.

- **Activate ARP caching:** Activates/deactivates the ARP cache (the table that assigns MAC addresses to IP addresses). It is necessary to deactivate the ARP cache in special situations. It is activated by default.
- **ARP cache size (entries):** The maximum number of entries in the ARP cache.

8.6.4 Firewall rules - Default

In the detailed view it is possible to create or edit the firewall rules. The following settings are available:

- **Activate rule:** Mark or unmark this checkbox if you want to activate / deactivate the rule.
- **Source address:** Enter a Host/Net alias or a Host/Net group or choose **CUSTOM** and enter an IP address or a network address in the textfield. If the packet comes from this IP or network address the rule will match. If the source address for this rule is irrelevant, choose the option **ANY** from the selection field. If all addresses except the chosen one should be included, mark the checkbox **except** besides the textfield.
- **Destination address:** Enter a Host/Net alias or a Host/Net group or choose **CUSTOM** and enter an IP address or a network address in the textfield. If the corresponding packet has the chosen IP address or an IP address in the chosen range as destination address, this rule matches. If the destination address for this rule is irrelevant, choose the option **ANY** from the selection field. If all addresses except the chosen one should be included, mark the checkbox **except** besides the textfield.
- **Service:** Service (protocol and port) of the packet. Services can be defined freely and can contain more than one protocols and ports. The definitions of the services are at the module network. If you select **ANY**, this option is not used for checking the packet. If you select **CUSTOM**, other fields are displayed to select the protocol and the ports (in case of TCP or UDP).
- **Status:** Checks if the packet is a SYN or a ACK packet depending on the state of the connection.
- **Action:** Action to be executed if the packet matches the rule. Possible values are **ACCEPT**, **DROP**, **LOG**, **REJECT**, or **NONE**.
- **Comment:** Describes the rule.
- **Activate monitoring:** Activates the monitoring functionality for the current rule. If you activate this the traffic matching this rule is monitored and can be printed out graphically. Enter a identifier to select the rules at the module Monitoring.
- **Create a monitoring rule for every IP address in the source:** If you entered a network address at the source address field, you can mark this checkbox to create a monitoring rule for each IP address within the network segment you entered above.
- **Create a monitoring rule for every IP address in the destination:** If you entered a network address at the destination address field, you can mark this checkbox to create a monitoring rule for each IP address within the network segment you entered above.

ATTENTION: If you want to monitor the whole traffic for the net 192.168.0.0/24 you must create monitoring rules in both directions (**int -> ext** and **ext -> int**).

Fields, that can only be configured if you choose a specific protocol are the following:

- **Choosing CUSTOM for services and TCP or UDP for protocols:**
 - **Source port:** Choose a source port. If the packet comes from the selected port, the further options of this rule are checked. If you don't quote a source port, this option will be ignored and not accounted at the proving of the package. You can either choose a port from 1 to 65535 or a certain range. A range of ports can be declared through a start port and an end port, divided by a colon (e.g. 2400:2600 means all the ports from 2400 to 2600). Optionally you can choose all ports from or to a certain port. Entering a colon followed by a port number means all the ports up to this number. By entering a port number followed by a colon you choose all the ports higher than the port number (e.g. :500 means all the ports from 1-500; 500: means all the ports from 500 to 65535).
 - **Destination port:** Enter a port in the textfield Destination port. If the packet arrives at the selected port, this rule will match and all options will be checked. The entries in the textfield

works like in the selection field **Source port**.

- **Choosing CUSTOM for services and ICMP for protocols:**

ICMP-Type: Choose the type of the ICMP-packet from this selection list. Following options are possible. **ANY** means all types.

- **echo-request**
- **echo-reply**
- **destination-unreachable**
- **source-quench**
- **redirect**
- **router-advertisement**
- **router-solicitation**
- **time-exceeded**
- **parameter-problem**
- **timestamp-request**
- **timestamp-reply**
- **address-mask-request**
- **address-mask-reply**

8.6.5 Firewall rules - Advanced

The first part - **Match Extensions** - deals with the check of the rules because of the configured values. If the packet matches the values, the rule matches and the packet will be treated in the configured way.

Options in this context:

Fragmentation: Choose a value from this select box if you want to check if a packet is part of a bigger packet. Packets that exceed a certain limit are fragmented (divided into smaller parts). You can select one of the following values:

- **none:** Choose this option if you don't want to check for fragmentation.
- **not fragmented:** Choose this option if you want to handle not fragmented packets.
- **fragmented:** Choose this option if you want to handle fragmented packets.

If, e.g. the packet has been divided into three small packets, a bit for fragmentation is set at the second and the third packet. If you have chosen **fragmented**, these packets are filtered. If you have chosen **not fragmented**, the first packet is filtered.

MAC-Source: Enter a source MAC-address in this textfield if you want to filter specific MAC-addresses. Each network interface can be specified through an unique identifier. This identifier consists of a six-part combination of hexadecimal numbers, in which the manufacturer and the type of network are encrypted. Restricting on MAC-address means a significant increase of security but also a lot of maintenance.

Limit: Using this option you will have the possibility to filter packets along their frequency of occurrence. If, for example, requests of a certain IP address on different ports of Gibraltar are increasing rapidly, you can configure a limit, up to which the rule matches. If the number of requests exceeds the determined limit, the rule does not match any more. Possible values for timeframe are **/second**, **/minute**, **/hour** or **/day**. Using the additional value **Limit burst** lets you trap a burst of packets (e.g. establishing a connection). The limit option can easily be explained looking at a container with a hole, holding a certain amount of objects. As long as there are objects in the container, the rule matches. At the beginning the number of objects in the container is identical with the number you configured at the limit burst option. For each incoming packet, one object is removed through the hole. If the limit is not reached during the specified timeframe, the number of objects is increased by one. If the limit is reached, the rule does not longer match.

- Example for application: Protection against DoS attacks (SYN flood, Ping of Death)

SPI: Enter a value if you want to match packets from the AH- or ESP protocols, which are based on the Security Parameter Index (SPI). Every function of IPSec adds an optional header to the IP-packet. With the SPI, that is included in this additional header, you enter a numerical value, on which's base the encoding process is chosen. Also a range can be entered here, whereby the start- and the endvalue - divided by a colon have to be given. The startvalue has to be

lower than the endvalue. (e.g. 480:500)

Length: Enter a numerical value into this textfield to check the length of a packet. This value can either be a single value or a range of values, whereby the start- and the endvalue have to be divided by a colon and the startvalue has to be lower than the endvalue (e.g. 800:1000). Length is specified in bytes.

TTL: This value specifies the **time to live**. Time to live means the number of hops of a packet on its way through the Internet. If the TTL is exceeded, the rule does not match any more.

The second part - **Package Modification** - deals with the modification of the packets. Incoming packets can be modified in the following form.

TTL: Choose a value of this select box if you want to change the value of the TTL field.

- **none:** Choose this option if you do not want to change the value of the TTL field.
- **set:** Choose this option if you want to set the value of the TTL field.
- **inc:** Choose this option if you want to increment the value of the TTL field.
- **dec:** Choose this option if you want to decrement the value o

The screenshot shows the 'Firewall rules' configuration window with the 'Advanced' tab selected. The 'Match Extensions' section includes a 'Fragmentation' dropdown set to 'none', a 'MAC-Source' text field, a 'Limit' text field with a '/second' dropdown, and a 'Limit-burst' text field. Below these are 'SPI' (with a note 'only for ESP or AH protocol type'), 'Length', and 'TTL' text fields. The 'Package Modification' section has a 'TTL' dropdown set to 'none' and an empty text field. 'Save' and 'Cancel' buttons are at the bottom.

8.6.6 Firewall rules - Advanced P2P

On this tab you can configure some Peer-to-peer services (file sharing). If you choose "DROP" in the basic setting of the rule, you can prohibit the traffic for this service by activating one or more checkboxes. Thereby the data exchange will be constricted and nearly completely prohibited.

8.7 NAT

NAT (Network Address Translation) means the manipulation of target or destination IP addresses or ports. There are many reasons for manipulating packages. Often there are not enough public IP addresses that you get from the provider. Or there is a transparent proxy running, which catches the IP-connection and directs it to a local port.

GibADMIN offers a module for NAT. There you have to set, which packets should be manipulated. For that you have to select the interface and the direction of the packet in a select box. Gibraltar creates an **outgoing-** and an **incoming track** for every network interface. Depending on the selection, only packets for the respectively direction on the chosen network interface are handled. Therefrom you get the possibilities how to handle the packet.

The name **track** means a way, the packet can go. There are incoming and outgoing tracks, depending on, if the packet comes into the firewall over an interface or if the packet leaves the firewall.

TIP: In the NAT module you can use the same aliases for hosts, nets and ports, that were defined by you in the firewall module.

8.7.1 NAT rules

The construction of the form is very close to the construction of the **Firewall** module.

When a packet comes in, the NAT rules are processed from above to below, until the options of a rule match the incoming packet. Therefore the ranking of the rules is enormously important. After a track has been chosen from the selection field **Track**, the NAT rules according to this track are listed in the element group below. In the overview the range can be changed. Also editing and deleting of single rules is done here.

NOTE: "Originated from Gibraltar" is a special track. It enables you to mask packets that are sent from a service that runs on Gibraltar. Take an HTTP proxy for example: Only a certain number of users - limited by authentication - are allowed to access homepages via HTTP proxy. But you also have an own homepage in the DMZ, which also is accessible for this limited group of users only. Whenever these users access to your own homepage, their browser will send an inquiry to the Gibraltar HTTP proxy. Afterwards the proxy sends an inquiry to the DNS server, that should convert the name of the own homepage into an IP address. This IP address is the external IP address of Gibraltar. Inquiries from outside are forwarded to the webserver in the DMZ by Gibraltar correctly. But if the HTTP proxy sends it's inquiry to the external IP address now, the answer packets won't be served correctly. Thus it is necessary to mask the own homepage with the address of the webserver in the DMZ when an inquiry is sent from the own network to the own homepage. Only thereby the packets will find the right way. This track will be used only in exceptional cases.

- **Active:** Mark or unmark this checkbox if you want to activate / deactivate the rule.
- **Source:** Shows the source IP address of the rule. If no IP address is set (ANY), the source IP address is irrelevant for this rule, and all source IP addresses are accepted. If - in front of the IP address - an exclamation mark is shown, all source IP addresses except the listed one will be proven (negation).
- **Destination:** Shows the destination IP address/destination subnet of the rule. If no IP address is set (ANY), the destination IP address is irrelevant for this rule, and all destination IP addresses are accepted. If in front of the IP address an exclamation mark is shown, all destination IP addresses except the listed one will be proven (negation).
- **Service:** Shows the service or the protocol for the rule. If no protocol is set (ANY), the field will be ignored.
- **Dest. port:** Shows the destination port for this rule. Because of this setting, the service, that matches for this rule is identified. For example dest.port 80 filters all packets that come from http connections. In this column entries are only allowed at the protocols TCP and UDP, because only this ports work. If no destination port is set for the shown rule, ANY will be displayed in the overview.
- **Action:** Enter the further treatment of the packet if all the set options are complied. If you are editing the NAT rules of an **incoming** track, **DNAT** and **REDIRECT** are visible. If you are editing the NAT rules of an **outgoing** track, **SNAT** and **MASQUERADE** are visible.
 - **DNAT (Destination NAT):** The destination address of a packet is translated to redirect a packet to another host. If you are running a web server in your internal network, all requests are arriving at the external interface of Gibraltar and are redirected to the internal IP address of your web server. Also all further packets of this inquiry are modified.
 - **REDIRECT:** All packets are redirected to another local port on Gibraltar. Using this option you can reroute all public requests to a proxy server without changing the destination address of the packet.

- **SNAT (Source NAT):** Using this option, the source address of a packet is translated. For example: A client from the internal network sends an request. He uses the IP address 192.168.0.36 and sends an HTTP request to 193.172.22.54. As the internal client uses a private IP address, the packet would be dropped when leaving the private network. For this reason, Gibraltar translates the source IP address using **SNAT**. In succession Gibraltar accepts the reply and forwards it to the requesting client.
- **MASQUERADE:** This option is used in association with dynamically assigned public IP addresses (e.g. dial-in connections). If a connection terminates, all corresponding connections will be deleted. This is necessary because of the possibility that another member could receive the IP address you were using before, which could lead to a misuse of this corresponding connections.
- **--to:** Shows the IP address which is used to masquerade the packet.

ATTENTION: The translation of packets using NAT does no packet filtering. You have to configure separate filter rules for all modified packets, because packet filtering is - in case of incoming packets - done after translation and - in case of outgoing packets - before translation.

8.7.2 Overview active rules

An overview over all active NAT rules. No new rules can be created here. Existing rules can be deleted or edited.

8.7.3 NAT Rule details

The card **Default** offers the possibility to configure the following options:

- **Activate rule:** Mark or unmark this checkbox if you want to activate / deactivate the rule.
- **Source address:** Choose from the selection menu a **Host/Net alias** or a **Host/Net group** or choose **CUSTOM** and enter an IP address or a network address in the textfield. If the actual packet comes from this IP address or from this network range, this rule matches. If you choose the option **ANY** from the selection field, this option will be ignored, and the rule matches without consideration of the source address. If you mark the checkbox **except**, the entered IP address will be negated. This means, that the rule matches to all source IP addresses except the one you entered. In the overview this case is shown with an exclamation mark in front of the IP address.
- **Destination address:** Choose from the selection menu a **Host/Net alias** or a **Host/Net group** or choose **CUSTOM** and enter an IP address or a network address in the textfield. If the actual packet is determined for this IP address or for this network range, this rule will match. If you choose the option **ANY** from the selection field, this option will be ignored, and the rule will match without consideration of the destination address. If you mark the checkbox **except**, the entered IP address will be negated. This means, that the rule will match to all destination IP addresses except the one you entered. In the overview this case is shown with an exclamation mark in front of the IP address.

- **Service:** Choose one of the services from the selection list or choose **ANY** if you want this field to be ignored, because all packets should be filtered. If you choose **CUSTOM**, you can set further details for this rule in the fields that appear afterwards.
- **Action:** Choose the kind of alteration you want to make from this select box.
 - **Incoming Track:**
 - **DNAT:** Destination Network Address Translation: The target IP address is modified to a specified value.
 - **REDIRECT:** The request will be forwarded to an other port.
 - **Outgoing Track:**
 - **SNAT:** Source Network Address Translation: The source IP address is modified to a specified value.
 - **MASQUERADE:** The source IP address is modified to the IP address that Gibraltar got by using a DHCP server (especially used for dial-in connections where the IP address is not fixed; also used in connections that do not get a fixed IP address).
- **--to:** Enter the IP address or port you want to redirect the packet to. For example, if you want to redirect all HTTP requests to an internal web server, you have to enter its IP address here. If you chose the action **MASQUERADE**, no entry in this field is allowed. If you chose an other action, an entry is necessary.
 - **IP address:** Enter the IP address, the packet should be masqueraded with.
 - **Port:** Enter at the selection of the option **REDIRECT** in target the local port, to which the inquiry should be redirected. For example a transparent proxy for a certain port.
 - **IP range to:** Here you can enter a further IP address, which builds a range with the IP address entered in the textfield IP address. This option is used for load balancing for inquiries to several identity www-servers. Inquiries are redirected to the IP addresses in the range by Round-Robin-process and thereby the load is balanced to several servers.
- **Comment:** Enter a comment for this rule in this textfield.

ATTENTION: The modification of the packets because of NAT does not mean that packet filtering is done! You have to configure separate filter rules for all modified packets as in the case of incoming packets the packet filtering will only be done after the modification and in the case of outgoing packets before the change.

Specifics of TCP/UDP

- **Source port:** Enter the port, that sends the packet in this textfield. If the packet comes from the entered port, the further options of the rule will be checked. If you leave this field blank, this option will be ignored and irrelevant for the check of the packet. You can either choose a port from 1 to 65535 or a certain range. A range of ports can be declared through a start port and an end port, divided by a colon (e.g. 2400:2600 means all the ports from 2400 to 2600). Optionally you can choose all ports from or to a certain port. By entering a colon followed by a port number, all the ports up to this number are meant. By entering a port number followed by a colon, all the ports up from this port number are meant (e.g. :500 means all ports from 1 to 500, 500: means all ports from 500 to 65535).
- **Destination port:** Enter the port, the packet goes to. If the packet arrives at the entered port, this rule will match and all options will be checked. The entry in the textfield works as in **Source port**.

NAT rules

Default

Interface: outgoing ext

Activate rule:

Source address: Mailserver or except:

Destination address: ANY or except:

Protocol: TCP

Source port: ANY or

Destination port: smtp/25 or

Action: SNAT

--to: IP address: 200.80.10.52 Port:

IP range to:

Comment:

Save Cancel

8.8 User

The user management of the firewall is used by several services. By default the integrated OpenLDAP server is used (similar to a phone book). Alternatively it is possible to get the users out of an external OpenLDAP server or of an Microsoft Active Directory server.

The following services use the central user management:

- HTTP Proxy
- SMTP Authentication
- Captive Portal
- VPN (PPTP/L2TP)
- OpenVPN

8.8.1 User management settings

Overview - local/external OpenLDAP server

After selecting and starting the LDAP server you can add users to the user management system. The card **User** shows all users and their permissions. The permissions can be changed by activating/deactivating the check boxes in this overview.

NOTE: Adding and editing users only work with local or external OpenLDAP servers. If you are using an Active Directory (AD) you must change the permissions in the user management of the AD.

Overview - Active Directory

If you are using a Microsoft Active Directory to manage your users, the list with the users and their permissions is fetched from the AD server. Changing the permissions is only possible at the AD server and not within the web interface of the firewall. OpenVPN certificates for users can be downloaded, if you have already created some.

New users - local/external OpenLDAP server

Create new users here:

- **Username:** The username for the new user.
- **Password:** Enter a new password.
- **Password (confirmation):** Confirm the new password.
- **First name:** Enter the first name of the user.
- **Sure name:** Enter the sure name of the user.
- **Email:** Enter the email address of the user.
- **VPN (PPTP/L2TP):** Check this box if the user should be allowed to use the VPN.
- **HTTP-Proxy:** Check this box if the user should be allowed to use the HTTP proxy.
- **Mail:** Check this box if the user should be allowed to use the SMTP authentication.
- **Captive Portal:** Check this box if the user should be allowed to use the captive portal.

Details - local/external OpenLDAP server

Change the settings for a user in the detailed overview.

- **Username:** The username of the user. Cannot be changed here.
- **Change password?:** Check this box if you want to change the user's password.
- **VPN (PPTP/L2TP):** Check this box if the user should be allowed to use the VPN. The button "Edit VPN attributes" you can change the VPN settings for PPTP or L2TP.
- **HTTP-Proxy:** Check this box if the user should be allowed to use the HTTP proxy.
- **Mail:** Check this box if the user should be allowed to use the SMTP authentication.
- **Captive Portal:** Check this box if the user should be allowed to use the captive portal. The button "Edit Chillisport attributes" forwards you to the detailed settings of the captive portal (Download settings for the user for example). The button "Reset RADIUS counter" resets these settings.
- **Download Client Certificate:** If you created a client certificate for a user, you can download it here again.

VPN Attributes - local/external OpenLDAP server

- **Assigned IP (blank for any IP):** Set this value if the user should get a static IP when he connects through PPTP.
- **Disconnect after session timeout (seconds):** If you set this value, the PPTP or L2TP connection will be disconnected after this period of time.

Captive Attributes - local/external OpenLDAP server

- **Disconnect after session timeout (seconds):** If you set this value, the user will be disconnected after this period of time. (Note: If the client uses VPN and Captive portal, this value is the same for both services)
- **Session Time Used:** Shows how long the user has already been connected. This value can be reset by the button besides.
- **Disconnect after idle timeout (seconds):** The connection is disconnected after the period of time with no interaction.
- **Maximum client upload amount (MB):** Set the amount of data a user is allowed to upload in MB.
- **MBytes uploaded:** Shows how many MB a user has already been uploading.
- **Maximum client download amount (MB):** Set the amount of data a user is allowed to download in MB.
- **MBytes downloaded:** Shows how many MB a user has already been downloading.
- **Maximum Transfer amount (MB):** This value sets the maximum transfer amount for up- and download.
- **Maximum upload rate (kBit/sec):** This value sets the bandwidth for upload.
- **Maximum download rate (kBit/sec):** This value sets the bandwidth for download.
- **Logouttime:** The connection will be disconnected when the time reaches this value.

8.8.2 LDAP Settings

When you press the link "User" in the main menu for the first time, you will automatically be forwarded to the second index card **LDAP Settings**. Here you can select the LDAP server you want to use. By default the local LDAP server is used.

Local OpenLDAP Server (Standard)

You can start the LDAP server by pressing the "Start" button (green arrow).

After starting the server you can add new users at the index card **User**.

External OpenLDAP Server

ATTENTION: Using an external OpenLDAP server requires deep knowledge in administration of an OpenLDAP server (e.g. configuration of access control lists) and should only be done by professionals.

Instead of the local OpenLDAP server you can also use an existing OpenLDAP server. If you want to do so, select "external LDAP" in the select box "Server". After you selected this value additional text fields are shown.

- **LDAP Server:** IP Adresse or Hostname of the external LDAP server. (**ATTENTION:** if you want to use the TLS encryption, you **must** use the hostname that is encoded as common name into the TLS certificate)
- **LDAP Port:** Port where the LDAP server listens at (default 389)
- **RootDN** (if you can use the LDAP initialization file)
- **Root OU:** ou=admin (if you can use the LDAP initialization file)
- **Root DC:** dc=gibraltar,dc=local (if you can use the LDAP initialization file)
- **RootPW:** Was created randomly. After you imported the LDAP initialization file it is recommended to change the password.
- **Confirm RootPW**
- **Change ldap passwords:** Pressing this button changes some other passwords. The different services need special users with specific permissions. Their passwords can be changed here.
- **TLS:** If you want to use a connection that is encrypted using TLS you must create a certificate for the external OpenLDAP server. Additionally the server must be configured for StartTLS or SSL. StartTLS encrypts using the standard port after sending a specific command. SSL uses a specific port (636). This port is used for encrypted communication. Both types must be activated because both of them are used by the different services.
- **Download LDAP Schema:** The OpenLDAP server at the firewall uses its own schemes to store the user data. You can download the scheme here to import it to your external LDAP server.
- **Download LDAP Init Data:** Additionally to the scheme you need a basic initialization scheme which can be downloaded here.

NOTE: The external LDAP server is only recommended for a high amount of users or for integration of a already existing LDAP structure. For most of the cases the local OpenLDAP server should be enough. This server does not need any special handling and is pre-configured for the usage as user management system for the firewall.

NOTE: If you use an external server you should encrypt the connection.

SSL certificate

For encrypting the connection to the external OpenLDAP server you need to create a server certificate. This certificate can be created with OpenSSL. The OpenLDAP server must be configured afterwards to use this certificate. Please read the manual of your distribution for the usage of the SSL certificates.

Microsoft Active Directory

In order to use Microsoft Active Directory (AD) for authentication, select the specified entry in the select box **Server**.

- **IP Domaincontroller:** IP address or hostname of the domain controller. (**ATTENTION:** if you want to use the TLS encryption, you **must** use the hostname that is encoded as common name into the TLS certificate)
- **LDAP Port:** Port where the LDAP server listens at (default 389)
- **User for AD communication:** Name of a user for authenticating the firewall at the Active Directory. It is recommended to avoid using the account Administrator, but a special user for firewall communication. This account should only be a common user account. Special permissions are only necessary to store OpenVPN certificates.
- **AD user password/Confirm AD user password:** Password of the user account.
- **Organisation unit of this AD user:** Name of the OU (Organisationseinheit) where the user is member of.
- **Domain:** Name of the domain (e.g. mydomain.local).
- **TLS:** To use a TLS encrypted connection you must create a certificate for your AD server and the server must be configured to use it correctly. Für eine mit TLS-verschlüsselte Verbindung muss für den AD Server ein Zertifikat erstellt werden und der Server entsprechend konfiguriert werden (Certificate Authority).
- **Join/Leave domain:** In order to join the domain you need username and password of a domain administrator.
- **Select AD groups:** You must create groups for the specific services (Mail, HTTP proxy, Chillispot, VPN). The users that should get the permissions to use the services must be members of these groups.

User management settings

User | **LDAP Settings** | Freeradius Accounting

Server: Active Directory

IP Domaincontroller: 192.168.1.100

LDAP Port: 389

AD user: manager

AD user password: *****

Confirm AD userpassword: *****

Organizational Unit AD users: ou=admin

Organizational Unit AD Groups: ou=users

Domain: mydomain.local

TLS: Upload TLS Certificate

Not yet uploaded!

Now you have to join the AD domain to use all available services!

Join domain

Select AD Groups

Save

Permissions of the AD user that is used for authentication

It is recommended to create a common user account which is used for authentication at the AD. By creating a separate user you avoid storing a domain administrator at the firewall. For saving the client certificates you must extend the permissions by using the tool dsacils. DSACLS (dsacils.exe) is a command line tool to change the permissions and security settings of

Active Directory objects.

If you called the user as in the picture above you can get the permissions of the user with the following command::

```
dsacls cn=firewall,ou=esys,dc=esys,dc=local
```

Diese Berechtigungen müssen mit folgendem Befehl erweitert werden:

```
dsacls ou=admin,dc=mydomain,dc=local /I:S /G "users\admin:RPWP;userPKCS12;user"
```

The permissions of the user admin must be extended with Read and Write permissions (RPWP-Right Property, Write Property) for the attribute userPKCS12. This attribute is used for storing the client certificates. For more details visit [DSACLs commands](#).

Join domain

In order to use the services PPTP and L2TP the firewall must join the domain. The following settings must be done therefore:

- **Domain controller:** IP address of the domain controller
- **Domain administrator:** AD user with the permissions as domain administrator
- **Password**

NOTE: The account data of the administrator is only used to join the domain and is not stored at the firewall.

Select AD Groups

Each service that needs authentication is represented as a select box here. Select the specific group for the service. All users within is this group are allowed to use the service.

NOTE: It is possible to select one group in all four services. The members of this group are allowed to use all services.

SSL certificate

Find a detailed explanation how to integrate a SSL certificate here:

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.itame.doc/am60_in_stall166.html

8.8.3 Freeradius Accounting

At this index card you can configure where to store the connection specific information to (file or database). You can use this information with special programs to get reports of the network usage. A freeware tool is for example [Radiusreport](#).

Example report from [Radiusreport](#).

```
radiusreport -tba -l peda -f
/var/log/freeradius/radacct/127.0.0.1/detail-20070420
Radius Log Report for: peda
Date Login Logout Overtime Port BandWt-In/Out Total
-----
20/04/2007 15:10:18 15:12:00 1m42s W0 8.3K/34.0K 0h01m
20/04/2007 15:15:06 15:15:18 0m12s W0 10.7K/236.4K 0h01m
20/04/2007 15:21:46 15:21:57 0m11s W0 6.5K/159.8K 0h02m
20/04/2007 15:23:58 15:24:12 0m14s W0 11.9K/106.1K 0h02m
20/04/2007 15:26:24 15:26:30 0m06s W0 27.6K/207.7K 0h02m
20/04/2007 15:27:05 15:27:27 0m22s W0 24.3K/73.4K 0h02m
20/04/2007 15:28:29 15:30:12 1m43s W0 7.7K/47.8K 0h04m
-----
Total Hours: 0h04m
Average Online times: Unavailable - not enough data.
Total Data transferred In/Out: 97.4K/865.4K
```

Internal Accounting:

The whole information is stored at /var/log/freeradius/radaccount. Only available with integrated hard disk.

External Accounting:

The information can also be stored to an external mySQL database.

- **Download Freeradius Database Schema:** Download the mySQL Schema.
- **Database Type:** At the moment we only support mySQL.
- **Database Host:** Address of the external mySQL database server.
- **Database Name:** Name of the database
- **Database Username:** Username of the mySQL server which has write permissions to the database.
- **Database Password**

NOTE: The communication to the database server should only run through an encrypted VPN tunnel.

8.9 Mail

The firewall can be used as a secure mail relay (mail proxy). It receives the mails from outside, performs spam and virus checks and forwards the filtered mails to the internal mail server. If you manage several domains, you can forward the incoming emails to different mail servers.

Preconditions for the usage as mail relay

The following preconditions must be fulfilled to use the firewall as mail relay:

- You have your own mail domain (e.g. example.com).
- You have a mail server in your internal network to manage the boxes for the emails.
- The MX record of your domain (the DNS record for the mail server of your domain) points to the external (public) IP address of your firewall. All emails sent to your domain are then forwarded to your firewall. After the spam and virus checks they are forwarded to your internal mail server.

The firewall ensures for outgoing emails that they only can be sent from authorized hosts.

ATTENTION: To check your mails for viruses and spam you must also start the SMTP Content Scanner in the module Services.

NOTE: If you do not have your own mail server but fetch your emails via POP3 from your provider, you can use the POP3 proxy which is also part of the firewall software.

8.9.1 Mail

8.9.1.1 Mail - General settings

General settings for the mail services can be set here.

- **Maximum message size (in MB):** Enter a restriction for the size of incoming emails. Bigger mails won't be accepted.
- **Activate virus and spam checks:** Activate this checkbox, if you want to activate virus- and spam checks, which you can configure on the register sheets **AntiVirus**, **AntiSpam** and **Common checks**.
- **Sender name:** Enter a name, which will be shown as addresser in the mails, that are dispatched automatically by the virus scanner.
- **Sender address:** Enter an email address, which will be used as email address in the mails, that are dispatched automatically by the virus scanner. Enter an email address that really exists, so that disconcerted users can send you a note or a question easily by answering the email.

- **Period to try sending error messages in days:** The firewall tries to send reports when a mail could not be sent to its recipient for the period of time you set here.
- **Scan mails for:** Choose in this element group the domain names, which's mails you want to check for viruses, spam and other irregularities. The domains listed here are configured in the general settings of Mail Relay (card **Relay incoming**). There you enter the domains, for which the Mail Relay should receive e-mails and pass them through to the adequate mailserver. Only mails for these domains can be checked.

ATTENTION: To check your mails for virus and spam you must also start the SMTP Content Scanner in the module Services.

The screenshot shows the 'Mail relay settings' window with the 'General settings' tab selected. The settings are as follows:

- Maximum message size (in MB): 15
- Activate virus and spam checks:
- Sender name: Gibraltar firewall
- Sender address: postmaster@testdomain.at
- Scan mails for: Domain
 - testdomain.at

A 'Save' button is located at the bottom of the window.

8.9.1.2 Relay outgoing

To enable the outgoing mail relay you have to enter all local networks that should be able to use Gibraltar as mail relay. Gibraltar only relays mails from those networks. All other mails are rejected so that Gibraltar can not be abused by strangers for sending spam mails.

- **Local networks:** Shows the networks that are able to send mails via Gibraltar.
- **SMTP Relay Host:** Enter an SMTP Relay Host (Smarthost), for example if your provider allows sending emails over its smarthost only.
- **Username/Password:** Account information for the smarthost.

The screenshot shows the 'Mail relay settings' window with the 'Relay outgoing' tab selected. The settings are as follows:

- Local networks:

Network address	
127.0.0.0/8	<input type="checkbox"/> <input checked="" type="checkbox"/>
192.168.1.0/24	<input type="checkbox"/> <input checked="" type="checkbox"/>

Buttons for 'Add network address' and 'Save' are visible at the bottom.

TIP: In the list of your firewall rules you must not forget to give permission for the outgoing TCP

port 25 (SMTP) (e.g. incoming "int0" and outgoing "local") so that the mails can be sent by Gibraltar.

8.9.1.3 Relay incoming

Gibraltar is able to receive and relay mails for several domains to other mailservers. Therefore you have to tell Gibraltar which mailserver handles which domain.

- **Managed domains:** This element group lists up the domains, from which Gibraltar receives and passes on mails to the according mail server.

The screenshot shows the 'Mail relay settings' window with the 'Relay incoming' tab selected. It features a table for 'Managed domains' with two columns: 'Domain' and 'Mailserver IP address'. A single entry is visible: 'testdomain.at' in the domain column and '192.168.1.10' in the IP address column. To the right of the IP address is a checkbox and a delete icon. Below the table is an 'Add server' button, and at the bottom is a 'Save' button. The window also has tabs for 'General settings', 'Relay outgoing', 'Common checks', and 'SMTP user authentication'.

8.9.1.4 Common checks

On this card further checks can be configured. For example filtering emails, which headers point out illegal changes, or attachments from emails, which data type is a potential threat. (e.g. .exe or .vbs files)

Action, if bad header found: Choose an action from the selection field that should effect, if the header of an email has an illegal design. Possible options are:

- **Discard and inform sender:** Choose this option, if the mail should be rejected when it exhibits a bad header. The sender gets a note, that says, that his mail had a bad header.
- **Discard:** Choose this option, if the mail should be rejected, without sending a note to the sender.
- **Pass through:** Choose this option, if you want to let the email pass in spite of the bad header. If you choose this option, also the checkbox beside can be marked. If you choose one of the other options, you can not mark it. An error message will be shown if you try to.
- **Pass through and warn sender:** The mail will be passed through, but the sender will get an information mail.

Action, if banned: Choose an action from the selection field that should effect, if the email contains an illegal attachment. Possible options are:

- **Discard and inform sender:** Choose this option, if the mail should be rejected when it has a bad attachment. The sender gets a note, that says, that his mail contains a bad attachment.
- **Discard:** Choose this option, if the mail should be rejected, without sending a note to the sender.
- **Pass through:** Choose this option, if you want to let the email pass in spite of the bad attachment. If you choose this option, also the checkbox beside can be marked. If you choose one of the other options, you can not mark it. An error message will be shown if you try to.
- **Pass through and warn sender:** The mail will be passed through, but the sender will get an information mail.
- **Pass through and warn recipient:** The mail will be passed through, but the recipient will get an information mail.
- **Pass through and warn sender and recipient:** The mail will be passed through, but the sender and the recipient will get an information mail.

Bann file extensions: In this element group you can arrange, which file extensions as attachments should be filtered. All file extensions you enter here, are no longer allowed as attachments.

TIP: The administrator and the quarantine email address of the AntiVirus section is also used for mails with bad headers or attachments containing banned extension files.

8.9.1.5 SMTP Authentication

Gibraltar can be used as SMTP server for sending mails. This can be very useful for external workers that do not have the possibility to reach their outgoing mail server. To use Gibraltar they need account information (username and password) which must be created in the module User.

Only authorized users are allowed to use the Gibraltar firewall as mail relay.

ATTENTION: Don't forget to create a filter rule, that allows external users to access to the port 25 (SMTP port) from outside. Activate this filter rule only after checking that the SMTP authentication is running. Otherwise Gibraltar acts as "Open Relay" and allows every sender to send emails.

8.9.2 AntiSpam

This submodule deals with the settings of the spamfilter. Here you can define the functions and the fidelity of the spamfilter.

8.9.2.1 AntiSpam (1)

- **Modify subject:** Mark this checkbox, if the subject of the email should be modified, in the case that an email is classified as spam.
- **Text to insert in subject:** Enter a text that should be inserted in the subject of an email, if the email is classified as spam. This text will be inserted only if the checkbox **Modify subject** is marked. The text will be inserted in front of the original subject.
- **Email of admin:** Enter an email address. If an email is classified as spam, a notice about the detection of a spam mail will be sent to this address.
- **Quarantine email:** Enter an email address, to which the mail should be sent, if it's classified as spam mail.
- **Add spam detected header:** Enter a value for the assessment of the mail. If this limit value is exceeded at checking the mail for spam, a new value is added to the header of the mail ("Spam detected").
- **Trigger action:** Enter a value, as of the following action should be performed. If the assessment of the mail exceeds the limit value, the action you choose in the following selection field is performed.
- **Eliminate information mail above this spam value:** If the spam value of the currently checked mail is above this value, the notifications will not be sent.
- **Action, if spam:** Choose an action from the selection field, that should effect, when an email is classified as spam. Possible options are:
 - **Discard and inform sender:** Choose this option, if the mail should be rejected when it's classified as spam. The sender gets a note, that says, that his mail was classified as spam. If you entered an email address in the textfields **Email of admin** or **Quarantine email**, the mails will be sent in any case.
 - **Discard:** Choose this option, if the mail should be rejected, without sending a note to the sender. If you entered an email address in the textfields **Email of admin** or **Quarantine email**, the mails will be sent in any case.
 - **Pass through:** Choose this option, if you want to let the email pass in spite of the classification as spam. If you choose this option, also the checkbox beside can be marked. If you choose one of the other options, you can not mark it. An error message will be shown if you try to.
 - **Pass through and warn sender:** The mail will be passed through, but the sender will get an information mail.

- **Spam lovers:** In this element group, you can enter email addresses, that receive emails even if they are classified as spam.
- **Activate Bayes filtering:** Mark this checkbox to check your mails for spam also with a Bayes filter.
- **Bayes training mails come from:** In this list, enter the IP addresses, where emails for training the Bayes filter are coming from. Normally it's your mail server, forwarding the mails to the two addresses on your firewall.

AntiSpam (1)
AntiSpam (2)
Blacklists and Whitelists

Modify subject:

Text to insert in subject:

Email of admin:

Quarantine email:

Add spam detected header:

Trigger action:

Action, if spam: Warn sender:

Spam lovers: **Email**

Activate Bayes filtering:

Bayes training mails come from: **IP address**

<input type="text" value="192.168.1.10"/>	<input type="checkbox"/> <input checked="" type="button" value="x"/>
<input type="text" value="127.0.0.1"/>	<input type="checkbox"/> <input checked="" type="button" value="x"/>

8.9.2.2 AntiSpam (2)

- **RBL lists:** This element group represents the "Blacklists". This are lists, that contain servers from which no mails are received. The servers shown in this list tried to send spam mails several times, and therefore are listed in the RBL lists.
- **Invalid or non_FQDN hostname:** By marking this checkbox the identity of the mailserver, that sends mails, will be proven. When a SMTP connection is built up, the sending server sends a "HELO" or "EHLO" command to identify at the destination server. With his command, the server sends its FQDN. If this FQDN is syntactically incorrect, this restriction works with rejecting the mail.
- **Unknown hostname:** By marking this checkbox, it will be proven, if the FQDN of the sending mail server can be dissolved. Gibraltar checks, if a DNS A or a MX entry exists for the senders FQDN. If there is no entry, the mail will be rejected. **ATTENTION: If the sending mail server is not configured correctly it is possible that Gibraltar blocks mails that should be forwarded.**
- **SPF check:** SPF means Sender Policy Framework. This term describes a method to prevent malpractice of email addresses for sending emails with a counterfeit sender. If an incoming mail has a counterfeit sender, the mail will be rejected. Details about SPF you find under <http://spf.pobox.com>.
- **Non_FQDN sender:** When you mark this checkbox, it will be proven, if the sender address (MAIL FROM) is a FQDN. If it is not, the mail will be rejected.
- **Non_FQDN recipient:** By marking this checkbox, it will be proven, if the recipients address (RCPT TO) is a FQDN. If it is not, the mail will be rejected.
- **Unknown sender domain:** By marking this checkbox you activate the checking of the senders address for a DNS A or MX entry. If there is no such entry, the mail will be rejected.

- **Improperly used sender domain:** When you mark this checkbox, it will be proved if the sender address or the sender domain respectively is registered in a list of known spam senders. If there is an entry in such a list, the mail will be rejected.
- **Recipient not verified:** By marking this checkbox it will be proven, if the recipient address is attainable. If it is not, the mail will be rejected.

Mail relay settings

AntiSpam (1) **AntiSpam (2)** Blacklists and Whitelists

RBL lists: **List** ✕

relays.ordb.org	<input type="checkbox"/> ✕
list.dsbl.org	<input type="checkbox"/> ✕

Activate the following restrictions to avoid the forwarding of questionable mail. Please read the documentation to configure the following items correctly!

- Invalid or non_FQDN hostname
- Unknown hostname
- SPF check
- Non_FQDN sender
- Non_FQDN recipient
- Unknown sender domain
- Improperly used sender domain
- Recipient not verified

8.9.2.3 Blacklists and Whitelists

For individual configuration of the spam filter the administrator can define black and white lists here.

- **Hosts/IPs:** Here you can define a computer by host name or IP address that either should be prohibited from sending emails to you or should be definitively allowed to send emails. Enter the host name or the IP address of the computer in the first column (**Hosts/IPs**). In the second column (**Action**) you can choose if you want to **accept** or **drop** emails from this computer.
- **Domains/Emails:** In this list you can enter domains or separate email addresses that either should be prohibited from sending emails to you or should be allowed to send emails. Enter the domain or the email address in the first column (**Domains/Emails**). In the second column (**Action**) you can choose if you **accept** or **drop** emails from this domain or email address.
- **Recipients:** In this list you can enter recipients who should get mails or who should not get mails. Enter the domain or the email address of the recipient in the first column. In the second column you can choose the action that should be executed on such emails.

8.9.2.4 Language Restrictions

At this form you can set some language restrictions. Gibraltar forwards only the mails that are written in the selected languages or use the selected character sets. If you do not make a decision here any languages and character sets will be forwarded.

Allowed languages: Select the languages in which the mails must be written to be forwarded.

Allowed character sets: Select the character sets in which the mails must be written to be forwarded.

The screenshot shows the 'Mail relay settings' window with the 'Language restrictions' tab selected. The 'Allowed languages' section contains three entries: German, English, and Chinese, each with a checkbox and a delete button. The 'Allowed character sets' section contains two entries: Western character sets and Chinese, each with a checkbox and a delete button. There are 'Add entry' buttons for both sections and a 'Save' button at the bottom.

8.9.2.5 Update rules

In this index card you can arrange, if Gibraltar should update SpamAssassin rules for spam recognition.

8.9.3 AntiVirus

Gibraltar can optionally scan your mails using the Kaspersky AntiVirus engine. You get a license for the Kaspersky AntiVirus service at your Gibraltar partner or directly at the producers.

- **Email of admin:** Enter an email address. If a virus is scanned, a notice about the detection of a virus will be sent to this address. Also the name of the virus is shown, as far as the data base already knows this virus.
- **Quarantine email:** Enter an email address, to which the mail should be sent, if a virus is found in it.
- **Action, if virus found:** Choose an action from the selection field, that should effect, when a virus is found in the email.
- **Virus lovers:** In this element group, you can enter email addresses, that receive emails even if there are viruses in them.

8.10 VPN

There are several possibilities to generate VPN connections with Gibraltar:

Site-to-Site VPN (connecting two LANs):

- IPSec VPN

Site-to-End VPN (Remote VPN, connecting external workers):

- OpenVPN
- PPTP
- L2TP over IPSec
- SSL VPN

8.10.1 Open VPN

OpenVPN is used to connect remote computers to a network by an encrypted connection (as PPTP or L2TP/IPSec). The users authenticate by using certificates which can be revoked at the certificates section at the web interface. Client software is available for free for different platforms (e.g. <http://www.openvpn.net/index.php/downloads.html> - OpenVPN 2.1_rc7 (URL tested on 2008-06-26)).

Gibraltar is only authenticating by certificates because there are some advantages against pre-shared keys like revoking the certificate.

To run OpenVPN at clients without administration permissions you must do some adaptations as described [here](#).

If your clients run Microsoft Windows Vista you must turn off the UAC (User Account Control) to use OpenVPN without any troubles.

8.10.1.1 General settings

You can configure the general settings for OpenVPN here.

At your client computer you must install a client software that can be found [here](#). The client software is available for all common platforms. To connect the client software you must store the configuration file and the client certificate to the folder `openvpn\config` at your remote computer. After this the connection can be used.

- **Listen on IP:** IP address of the OpenVPN server at the firewall. Choose **ANY**, if you want to connect to any configured IP address at Gibraltar. You must define an IP address or a hostname for the client configuration in this case.
- **Server IP/Hostname for client configuration:** If you chose ANY in the select box above you must define an IP address or a hostname here which the client can connect to.
- **TCP/UDP:** The protocol you want to use.
- **Port:** The port the server should listen at.
- **Redirect Gateway:** The whole traffic of the client is sent through the VPN connection.
- **Routed networks:** To allow the client to access the local networks you must enter the network addresses here.
- **Download client config:** After finishing the configuration of OpenVPN you can download the configuration file for the client by pressing this button.

NOTE: Starting the OpenVPN service can last several minutes because it creates some encryption keys.

8.10.1.2 Extended settings

The settings at this register card are only for experts and should not be changed in normal situations.

Enable compression: Deactivate the compression that is started by default.

Keep alive (Ping): Interval to check the connection. The client sends a ping to the server.

Keep alive (Timeout): The connection is restarted if there is no response in this period.

assigned client IP range: The client gets an IP address out of this network range.

internal DNS server 1: Internal DNS server that is sent to the client.

internal DNS server 2: Internal DNS server that is sent to the client.

internal WINS server: Internal WINS server that is sent to the client.

Allow Fragmentation: Big packets are fragmented and no bigger packets are sent.
MTU Size: Changes the MTU (Maximum Transfer Unit) size of the interface TUN.
MSS Fix: This option can change the MTU size of TCP connections over the VPN tunnel. This option should be used in combination with "Allow Fragmentation".
Float: Use this option if the IP address of the client is changing during connection. Open connections are not stopped and you can continue working with the new IP address.
Download client config.: Get the client configuration file to upload it at the client.

8.10.1.3 Status

The state of the currently connected OpenVPN users.

The Common Name is the username created at the user management or fetched from Active Directory e.g.

8.10.2 IPsec

IPsec has been developed to enable Virtual Private Networks (VPNs). It offers a lot of protocols that have been developed from the IETF (International Engineering Task Force, www.ietf.org) to ensure a secure and encrypted exchange of IP packets. It can be used for site-to-site and end-to-site connections.

8.10.2.1 IPsec - General settings

Before you can start configuring VPN tunnels you must specify which network interface should be a VPN end point. If the Gibraltar firewall is behind another firewall that implements NAT, you must additionally activate the option "NAT traversal". If you do not have a static external IP address you must select the option "Via default route".

ATTENTION: If you use NAT Traversal, the remote station has to open the UDP port 4500.

8.10.2.2 Tunnel

The card **Tunnel** shows all configured IPsec tunnels.

- **Description:** Shows the description of the tunnel.
- **Local IP address:** Shows the local IP address of the tunnel (has to be an address of one of the network interfaces).
- **Local subnet:** Shows the local subnet associated to this tunnel.
- **Remote IP or FQDN address:** Shows the remote IP address or FQDN of the tunnel ("ANY" means all IP addresses are allowed for the remote IP).
- **Remote subnet:** Shows the remote subnet associated to this tunnel.
- **State:** Shows the current state of the IPsec tunnel: **(started)**, **(standby)**, **(deactivated)**

The following actions can be executed at the overview:

- **Start IPsec tunnel**  : Click this button to start the IPsec tunnel if the current state is **(deactivated)** or **(stopped)**. The tunnel gets the state **(started)** after clicking.
- **Stop IPsec tunnel**  : Click this button to stop the IPsec tunnel if the current state is **(started)**. The tunnel gets the state **(standby)** after clicking.
- **Activate IPsec tunnel**  : Click this button to activate the IPsec tunnel if the current state is **(deactivated)**. The tunnel gets the state **(standby)** after clicking.
- **Deactivate IPsec tunnel**  : Click this button to deactivate the IPsec tunnel if the current state is **(standby)** or **(started)**. The tunnel gets the state **(deactivated)** after clicking.

- **Edit tunnel**  : Click this button to edit the tunnel details. The browser will redirect to a [detail](#) form where you can configure the connection.
- **Delete tunnel**  : Click this button to delete a tunnel.

8.10.2.2.1 Tunnel - Default

The card **Default** offers the possibility to configure the basic settings for an IPSec tunnel.

- **Description:** Enter a description of the tunnel in this textfield.
- **State after start:** Choose the state the IPSec tunnel should have after starting the IPSec service from this select box. Possible values are **(deactivated)**, **(standby)** and **(started)**.
(deactivated): No connection from outside or to outside can be created.
(standby): The tunnel waits for a connection establishment from outside.
(started): If you choose this status, the tunnel will be established directly after starting IPSec, as far as the remote computer has the status **(standby)**.
- **Local IP address:** Choose a local IP address for this tunnel from this select box. The values in the select box depend on how many interfaces and IP addresses have been configured for Gibraltar. The value consists of the IP address and the network interface name (e.g: "10.0.0.1 - int0").
- **Local subnet:** Enter the local subnet for this tunnel to which the remote user should have access in this textfield. So the remote user can also access computers behind the gateway in the specified subnet by the tunnel.
- **Local certificate:** Choose the local certificate for the authorization from this select box. If no local certificate is available, you have to generate a certificate in the [certification management](#).
- **Remote IP or FQDN:** Enter the remote IP address or the FQDN of the computer with which you want to communicate via IPSec, if the tunnel should reach only one certain computer. In this case, you have to select **Host** at the options fields right from the textfield. If you want to allow several hosts to connect to the end point, select the option field **Any remote IP**. So the entry in the textfield **Remote IP address** will be ignored, and different computers can establish the IPSec tunnel.
- **Remote subnet:** Enter the network address of the remote subnet in this textfield. So the local users have access to the remote subnet. The Option "Special handling for road warriors behind NAT gateways: rightsubnetwithin" must be activated only in special situations when you use a roadwarrior that switches to different local area networks and connects to the Gibraltar firewall via IPSec. In this case you can enter 0.0.0.0/0 here to allow connecting to the subnet behind the Gibraltar firewall.
- **Authorization:** Choose the authorization method from the right option field. You can choose **Password**, **X509 certificate** or **Signed by Certified Authority**.
Password: Enter a password. The remote receiver has to enter the same password. This authorization method is called "Shared secret", as both remote receivers share the same key.
X509 certificate: Both remote receivers are exchanging certificates with which they can authenticate each other. Thereby the certificate with which you want to enable authentication has to be chosen from the selection field beside. To be listed in the selection field, the certificate has at first got to be uploaded at the certificate administration in Gibraltar.
Signed by Certified Authority: Certificates are signed by a certified authority, that guarantees the authenticity of the host.
- **Use for L2TP:** Mark this checkbox, if the defined tunnel is supposed for building up a L2TP connection. When you mark this checkbox, you mustn't enter anything in both subnet textfields. Authorization option should be **Signed by Certified Authority**.
- **Local ID:** Enter the local ID for this tunnel. This value is only used if you want to create tunnels to third party products.
- **Remote ID:** Enter the remote ID for this tunnel. This value is only used if you want to create tunnels to third party products.
- **Next router IP:** Enter the IP address of the next router. This option is used if you use two internet connections, for example. Normally GibADMIN recognizes this value automatically and you do not need to enter anything.

ATTENTION: In order to activate data traffic over IPSec tunnels you have to configure filter rules for the corresponding interfaces (e.g. incoming "ipsec0" or outgoing "int0").

8.10.2.2.2 Tunnel - Advanced

It is possible to set advanced options here if necessary. These options are mostly only necessary if you want to create VPN tunnels to third party gateways. If you connect two Gibraltar firewalls you need not change anything here.

Type: Choose the type of the IPSec tunnel from the option field **Tunnel** or **Transport**. The option **Transport** only works with host-to-host connections. **Tunnel** also works with host-to-subnet or subnet-to-subnet connections.

IP compression: Mark this checkbox if you want to activate IP compression. If one of the endpoints of the tunnel deactivates this option, the transmission occurs uncompressed.

PFS (perfect forward secrecy): Mark this checkbox if you want to activate an additional key management protocol, which regenerates the key of the encoding algorithm in temporary intervals. Thereby it's prevented that someone who cracks the key can encode information that he received for a longer time.

Number of trials: Enter the times how often IPSec should try to establish the connection. If you enter the value 0 the number of trials is unlimited.

Keylife (IKE - Phase 1): Enter the period how long the session keys of phase 1 are valid. After expiration of the term the session keys are negotiated again.

Keylife (Phase 2): Enter the period how long the session keys of phase 2 are valid. After expiration of the term the session keys are negotiated again.

Phase 1: Choose the IKE and Hash algorithms and the Diffie Hellman group (DH group) you want to use.

Phase 2: Choose the ESP and Hash algorithms you want to use.

8.10.2.2.3 Watchdog

The IPSec watchdog checks the VPN connection between "Local IP" and "Remote IP". If it is not possible to get a connection between these two IPs the tunnel or the IPSec service is restarted. As local IP choose the IP of the Gibraltar firewall which is part of the local subnet (so it is the local internal IP of Gibraltar in most cases).

8.10.3 PPTP

PPTP (Point-to-Point Tunneling Protocol) was founded by a consortium (Ascend Communications, Microsoft, 3 Com, u.a.) to build VPN tunnels. It tunnels PPP packets through a IP network by encapsulating it into a GRE packet.

PPTP is part of the Microsoft Windows operating systems and therefore it is widespread.

This type of VPN is used for Site-to-End connections (remote VPN). The configuration is very easy.

In the module PPTP you must set the general settings. The user accounts must be created at the user management.

8.10.3.1 General Settings

To enable **PPTP** you need to configure the basic configuration.

- **Local IP (with netmask):** The local IP address in CIDR notation which is used by Gibraltar to handle PPTP connections. The initialization of the PPTP connection must of course take place with a public IP address. Intern, the remote connections handle with this local IP address. Enter the adequate routing entries in the module **Network**, if the remote users are not in the same subnet.
- **Remote IP from** and **Remote IP to:** The clients get one of these IPs if they connect to Gibraltar via PPTP. In the textfield **Remote IP from** enter the first IP address and in the textfield **Remote IP to** enter the last IP address from the range of IP addresses, that a remote user should get.
- **Domain:** The domain the remote users get assigned.
- **DNS server:** The DNS server the remote users get assigned. The DNS server is important to enable a correct address resolution.
- **WINS server:** The WINS server the remote users get assigned. Windows clients might need a WINS server for correct NETBIOS name resolution.

TIP: Don't forget to set packet filter rules for both the TCP-protocol at port 1723 and the GRE-protocol with the action ACCEPT to allow a PPTP connection to the firewall from outside.

8.10.3.2 PPTP - Extended Settings

In this index card you can set adjusted properties of PPTP.

- **Maximum transfer unit (MTU):** Maximum unfragmented transfer unit in bytes.
- **Maximum receive unit (MRU):** Maximum value of the converting data packet.
- **Forward broadcasts:** Activate those interfaces that should forward broadcast packets.

8.10.4 L2TP

L2TP over IPsec offers another option for connecting apart users with the internal network over a secure connection (VPN). Thereby an IPsec tunnel is built up from a remote computer to the firewall. The encrypted data exchange with the network occurs over this tunnel. At the remote computer the Wizard - integrated in Microsoft Windows XP - can be used for creating the VPN tunnel. So additional costs for software can be saved.

You can find a manual for creating and uploading a client certificate to a Microsoft Windows XP remote client on the Gibraltar Homepage. We also provide an EXE-file that automatically uploads the certificate to the right places in Windows XP ([Gibraltar Homepage - Download](#)).

8.10.4.1 L2TP-General settings

NOTE: Please note the suggestions on the [Gibraltar Homepage](#).

The configuration of L2TP is very similar to the configuration of PPTP.

ATTENTION: By using a L2TP connection, the traffic is handled over an IPsec tunnel. Therefore a few additional filter rules are necessary, to enable this traffic to pass the firewall unhindered. The L2TP connection establishment arrives at the IPsec interface of Gibraltar. So you have to allow the traffic from ipsec0 to LOCAL (Source and destination port on UDP/1701). The data itself goes over a PPP interface. Thus you also have to allow the traffic from ppp+ to the according net (e.g. from ppp+ to int). You should only open the ports you will really use.

8.10.5 Certificates

The card **Certificates** offers the possibility to manage your certificates and certificates of other Firewalls. These certificates are managed by three element groups (Host certificates, CA certificates, Private keys).

Host certificate

Host certificates are created at this firewall or at another one to authenticate to each other (public key).

- **File name:** Shows the name of the certificate.
- **Organization:** Shows the organization of the certificate.
- **Owner:** Shows the owner of the certificate.
- **Email:** Shows the email address of the owner.
- **Expiration date:** Shows the expiration date of the certificate.
- **Delete marked entries** : Mark the entries in the element group by activating the checkbox and click this button in the heading line afterwards to delete the marked entries.
- **Delete certificate** : Click this button to delete the user certificate.
- **Download certificate** : Click this button to download the user certificate to your computer.
- **Add certificate:** Click this button to upload a new user certificate. The browser will redirect you to a form where you can upload your user certificate.

CA certificate

CA certificates are certificates from common certification authorities who sign certificates.

- **File name:** Shows the name of the certificate.
- **Organization:** Shows the organization of the certificate.
- **Owner:** Shows the owner of the certificate.
- **Email:** Shows the email address of the owner.
- **Expiration date:** Shows the expiration date of the certificate.
- **Delete marked entries** : Mark the entries in the element group by activating the checkbox and click this button in the heading line afterwards to delete the marked entries.
- **Delete certificate** : Click this button to delete the user certificate.
- **Download certificate** : Click this button to download the user certificate to your computer.
- **Add certificate:** Click this button to upload a new user certificate. The browser will redirect you to a form where you can upload your user certificate.

Private keys

The private keys are the part of a key pair that you should not give to another. It is the private part of the host certificates.

Create certificate

- **Generate cert:** Click this button to generate a new cert. The browser will redirect to a [detail](#) form where you can perform the creation.
- **Generate client cert:** Click this button to generate a new client certificate. You can use the certificates signed by a CA which allow client-to-network VPN connections with Microsoft Windows 2000 and Microsoft Windows XP. The browser will redirect to a form where you can perform the generation.

8.10.5.1 Certificate Revocation List

If you want to revoke client certificates you must use a certificate revocation list (CRL). This can be necessary if a certificate got lost or if an employee leaves the company.

In this overview you can see the already created certificates. You can see a validity date and a state for each of them. You can revoke valid certificates by pressing the button besides the certificate.

NOTE: If you revoke the certificate of a user he is no longer able to connect. You must create a new one if he must authenticate again.

8.10.5.2 Generate host certificate

To create a host certificate you have to enter some information that is encoded in the certificate. You find both in the overview of the certificates.

- **Name of certificate (without file extension):** Enter a name for the certificate in this textfield. If you enter "gibraltar" a user cert "gibraltar.pem" and a private key "gibraltarKey.pem" will be created.
- **Key length:** Choose the length for the key from this select box. The higher the value the higher the safety of the IPSec tunnel using this certs. The disadvantage is that higher values for the key length lead to more work for the computer processor.
- **Validity (days):** Enter the validity of the cert. After expiration the cert will not be accepted any more.
- **Country code:** Enter the land code for your country (e.g: AT for Austria, DE for Germany, US for USA, ...).
- **Region:** Enter your region.
- **City:** Enter your city.
- **Organisation:** Enter the name of the organisation of your company.
- **Organisational unit:** Enter the name of the organisational unit of your company.
- **Owner:** Enter the owner of the certificate.
- **Email:** Enter the email of the owner.

After creating a new host certificate you can download the public part of it in the element group of the host certificates. This public part must be uploaded at the other side of the VPN tunnel to use it for authentication.

8.10.5.3 Generate client certificate

To create a client certificate you have to enter some information that is encoded in the certificate. You find both in the overview of the certificates.

- **Key length:** Choose the length for the key from this select box. The higher the value the more the safety of the IPSec tunnel using this certs. The disadvantage is that higher values

for the key length lead to more work for the computer processor.

- **Password:** Enter a password for the certificate. You will need this password later when you want to establish a VPN connection to Gibraltar by using OpenVPN.
- **Validity (days):** Enter the validity of the cert. After expiration the cert will not be accepted any more.
- **Country code:** Enter the land code for your country (e.g: AT for Austria, DE for Germany, US for USA, ...).
- **Region:** Enter your region.
- **City:** Enter your city.
- **Organisation:** Enter the name of the organisation of your company.
- **Organisational unit:** Enter the name of the organisational unit of your company.
- **Owner:** Enter the owner of the certificate.
- **Email:** Enter the email address that belongs to this certificate.

After generating the client certificate you must store it to the client to create a VPN connection by using IPsec or OpenVPN to your Gibraltar firewall.

8.10.6 SSL

SSL (Secure Socket Layer) is a protocol to encrypt data that is sent over the Internet. The module SSL at the firewall can be used to encrypt potentially insecure traffic via SSL. For example you can offer a http server with https by using this service. The whole traffic passing this connection is encrypted and more secure than sending without SSL encryption.

The following settings must be configured to use SSL:

- **Local Port:** The port that is listening for requests from the Internet. All traffic coming to this port is forwarded to the internal server and the port that is specified at the other fields. You can select one of the predefined ports.
- **Port (custom):** Enter another port that is not in the select box.
- **Redirect to (IP):** The internal IP address of the server where the packets should be forwarded to.
- **Redirect to (Port):** Port where the internal server listens for requests.

Example: You want to fetch your emails that are saved at an internal pop3 server from outside your network. Your pop3 server does not support pop3s (SSL encryption). By using the SSL encryption of your firewall you can offer pop3s to external users and forward the requests to the internal pop3 server. The communication between the firewall and your pop3 client is encrypted.

TIP: Do not forget to set a packet filter rule for the port you have chosen to allow the incoming traffic.

8.10.7 SSL VPN

SSL VPN is a web based SSL VPN server. The user connects to the VPN server using his web browser. He can use the services the administrator offers for him. A typical scene is the connection to a Microsoft Windows client using RDP (remote desktop) through the SSL encrypted connection. For using this kind of VPN you do not need any special software at your clients if Java is already installed.

The installing of the SSL VPN is started at the web interface of the firewall. All special configuration of the SSL VPN is done in its own separate web interface. After selecting the network interface and saving the setting you can press the button "Start Installation" to activate the SSL VPN. After the installation you can configure the service with your web browser at **http://<IP_of_the_selected_interface>:28080**.

ATTENTION: It is not possible to install additional extensions or to use the Enterprise Edition of

the SSL VPN. Only the pre-installed packets can be used. If you would like to use additional packets, please inform us to possibly add them in future versions.

A detailed explanation of the SSL VPN in English is available at <https://3sp.com/showSslExplorerCommunity.do> or at https://3sp.com/products/ssl-explorer/documentation/Getting_Started_guide.pdf.

IMPORTANT: Do not forget to start the service at the module Services.

8.11 Proxy server

The firewall offers different kind of proxy server software to secure the network traffic on application layer. A proxy server can have a look into the packets and check the content for viruses or unwanted information.

Another example for a proxy server is the integrated SMTP proxy which is used to filter the content for viruses and spam.

The following proxy server software is included:

- **HTTP proxy** for web traffic
- **POP3 proxy** for email via POP3
- **FTP proxy** for FTP file transfer
- **SMTP proxy** to filter emails for spam and viruses (siehe [Mail](#))

Additionally you can find three different anonymization services that work as proxy, too.

8.11.1 HTTP proxy

In order to use the HTTP proxy you must first do some configuration and start the service. The following options can be used:

- **Transparent proxy server:** The clients' browsers need not be changed. The firewall takes the requests from the clients and starts its own request to get the sites you want.
- **Caching:** Content is stored at the firewall and the browser gets the content from there instead reloading it through the Internet. This reduces bandwidth usage.
- **Authentication:** If you use user authentication, you can manage which users are allowed to access the web sites. You must create or import the users first at the integrated user management.
- **Content filtering:** Remove dangerous content and viruses from http traffic specify by categories.

8.11.1.1 General settings

The following general configuration of the HTTP proxy can be made here:

- **Port:** Enter the port on which the HTTP proxy receives requests. If you do not use the proxy transparently, you must enter this port number at your clients' browser.
- **Allow transparent proxying:** Choose the interfaces, that can communicate with the proxy transparently. Thereby no modifications must be done in the web browsers of the clients. By marking an interface, an adequate NAT rule is created automatically, that redirects inquiries from clients to port 80 automatically to the port you chose.
- **Use hostname for logging:** Mark this checkbox to log the hostname of the accessing computer in the log files instead of logging the IP address. This feature premises a faultless DNS solvation on the firewall.
- **Use parent cache:** Enter an IP address and the port number of a parent proxy cache, if your provider or you within your company offers you this opportunity.

HTTP proxy

General settings | Proxy cache | Authentication | Content filter | Exceptions

Port: 3128

Allow transparent proxying: For the following interfaces:

- eth0
- eth1
- eth2
- eth3

Use hostname for logging:

Use parent cache (e. g.: 1.1.1.1:3128):

Save

8.11.1.2 Proxy cache

Here you can configure the settings for the caching.

- **RAM for proxy (in MB):** RAM used for caching.
- **Maximal size of an object (in KB):** Enter the maximal size an object can have to be stored in the cache. If an object is larger it's not stored in the cache.
- **Use disk cache:** Mark this checkbox if you already have configured a hard disk and want to use a part of this hard disk for caching of data that were inquired via HTTP. Enter the space of the hard disk you want to use for this caching in the textfield besides.
- **Size of disk cache (in MB):** Define the size of the hard disc used for caching preconditioned a hard disc has already been integrated.

8.11.1.3 Authentication

Activate the authentication functionality of the HTTP proxy here. All clients using the proxy must authenticate. For user management use the integrated [user management interface](#).

8.11.1.4 Content filter

Here you can define a filter, that checks the contents of the Internet sites that are viewed by the users. Thereby you can filter viruses, cookies, scripts, flash and ActiveX controls.

- **Kaspersky anti virus:** Mark this checkbox, if you acquired the optional license for the Kaspersky anti virus scanner and if you want to use it for virus checking in the HTTP proxy.
- **Cookie filter:** Mark this checkbox, if you want to prohibit the using of cookies already at the firewall at the HTTP proxy.
- **ActiveX filter:** Mark this checkbox, if you want to prohibit the using of ActiveX controls.
- **JavaScript filter:** Mark this checkbox, if you want to prohibit the using of JavaScript and other script languages.
- **Flash filter:** Mark this checkbox, if you want to prohibit the using of flash applications.

NOTE: Using these filters can stop viewing many web sites. Most of the web sites use such extensions today. So please be careful using the filters (except Kaspersky AntiVirus).

8.11.1.5 Exceptions

On this card you can set URLs that should be excepted from checking by the filters on the **Content filter** card. The virus filter can not be deactivated by that way.

Exceptions: The URLs in the list will be ignored at content filtering (except viruses).

Blocked URLs, domains and regular expressions: The addresses in this list are blocked. You can use three different kinds of entries that block URLs after you saved the changes:

- **Complete URL:** Enter a complete URL like `www.mydomain.com`. Thus this address isn't accessible anymore.
- **A domain and its subdomains:** Enter a domain with a dot in the first place for blocking the domain along with its subdomains (`.mydomain.com` blocks `www.mydomain.com` as well as `ftp.mydomain.com` or `shop.mydomain.com`,...).
- **Single word:** Enter one single word and all URLs that contain this word will be blocked. Consider upper and lower case! (cooking would block addresses like `www.cooking.com`, `www.mydomain.com/cooking`, but NOT `www.mydomain.com/Cooking`.)

8.11.1.6 PureSight Content Scanner

The PureSight content scanner is an extension to the HTTP proxy to block web sites depending on their category (e.g. erotic or gambling).

In order to use the PureSight content scanner you must purchase a separate license file. Of course you have the possibility to test the functionality for 30 days for free.

There are two different versions of the PureSight content scanner:

- **Limited Edition:** The web sites can be blocked by specific categories. You select these categories within the web interface of the firewall and cannot get any specific reports.
- **Enterprise Edition:** When you purchase the enterprise edition you can configure the PureSight content scanner with a separate PureSight web interface. You can do extensive configuration and you can get many specific reports.

How to get a valid PureSight license and how to start the content scanner.

- Click the URL "Upload license" at the menu bar.
- Copy the "PureSight Network ID" into the clipboard and send it to office@gibraltar.at. Also add the internal IP address of the firewall and the edition you want to purchase.
- You will get a license file for uploading at the firewall.
- If you purchased the **Limited Edition** you can choose the categories at the HTTP proxy tab of PureSight where you can select the categories to be blocked.
- If you purchased the **Enterprise Edition** you must start the service at the module Services and after starting you can reach the separate web interface at the URL: <http://ipOfYourFirewall:5000>. Do not forget to add a firewall rule to reach port 5000 from the internal network (int -> LOCAL).

Enterprise Edition

As already said the Enterprise Edition can be reached at a separate web interface (deactivate popup blockers for this IP address). The default password is empty. When you change the password for the first time, be aware that you must enter a blank in the old password field. An empty field is not allowed here.

All configuration options are explained detailed within the PureSight online manual.

ATTENTION: If you change your internal IP address you must order a new license file at office@gibraltar.at for free.

8.11.2 POP3 proxy

The **POP3 proxy** makes it possible to check emails that are recalled from an external POP3 post office box. Thereby different reviews (spam, viruses) can be done. Further the internal network structure is hidden from the external world. If a virus is found in a mail, Gibraltar deletes the mail and it's not forwarded to the recipient. If a mail is classified as spam, you can configure Gibraltar in the way to add the text "*****SPAM*****" to the subject and you get information, why this mail is spam in the textfield of the mail. Afterwards you can create a filter in the client mail program to copy the spam mails in a separate subdirectory. There you can review or also delete the mails. The original mail message is attached to that information mail.

8.11.2.1 General settings

The following settings must be configured:

Port: Enter the port, on which the POP3 proxy should listen for requests.

Allow transparent proxying: Choose the interfaces, that can communicate with the proxy transparently. Thereby no modifications must be made in the mail clients of the clients. By marking an interface, an adequate NAT rule is created automatically, that redirects inquiries from clients to port 110 automatically to the port you choose.

Skip RBL checks: Mark this checkbox, if your Internet service provider checks your mails already with blacklists. By deactivating this check, the performance for recalling mails from the POP3 pigeon hole gets better.

Activate Kaspersky's virus scanner: Mark this checkbox, if you uploaded a valid Kaspersky license and if you want to use the Kaspersky virus scanner.

Check for spam: Mark this checkbox, if you want to check the fetched mails for spam.

Text to insert in subject: Enter a short text that should be added in the subject, if the mail is classified as spam.

Tolerance for spam evaluation: Enter the value (e.g. 5.5) as of the mail should be classified as spam.

Spam handling: Choose the option from the selection field, that comes up to your requirements. Possible values are:

- **Change only subject:** Choose this option, if only the subject should be changed to the text, you entered above. The text of the mail will not be changed. So you don't get a report about the reasons of classifying the mail as spam.
- **Attach mail to report:** If you choose this option, you get a report why the relevant mail was classified as spam. The original mail message is attached unchanged. So a mail in HTML format is obtained and presents a bad risk.
- **Attach mail to report as plain text:** Choose this option, if you want to get a report about the reasons for classifying the mail as spam. The original mail message will be attached converted to the format "text only". Only ASCII characters are displayed.

POP3 proxy ?

General settings Rename attachments

Port:

Skip RBL checks:

Activate Kaspersky's virus scanner:

Check for spam:

Text to insert in subject:

Tolerance for spam evaluation:

Spam handling: ▼

Overwrite HTML tags:

8.11.2.2 Rename attachments

Here you can enter a list of file extensions of attachments, that should be renamed, when they are inquired by the POP3 post office box.

- **Rename attachments:** Mark this checkbox to activate renaming of the files with file extensions listed below.
- **Bann file extensions:** This list shows all file extensions that are not allowed as mail attachments. If you receive an email with such a forbidden attachment nevertheless, this attachment will be renamed. If - for example - the file extension "exe" is listed, the file "setup.exe" will be renamed to "setup.bad" if it was attached to a mail in your POP3 pigeon hole and if you inquire this pigeon hole over the POP3 proxy of Gibraltar.

POP3 proxy

General settings | **Rename attachments**

Rename attachments

Bann file extensions: **List** (X)

ADE	<input type="checkbox"/>	(X)
ADP	<input type="checkbox"/>	(X)
BAS	<input type="checkbox"/>	(X)
BAT	<input type="checkbox"/>	(X)
CHM	<input type="checkbox"/>	(X)
CMD	<input type="checkbox"/>	(X)
COM	<input type="checkbox"/>	(X)
CPL	<input type="checkbox"/>	(X)
CRT	<input type="checkbox"/>	(X)
EML	<input type="checkbox"/>	(X)

Add file extension

Save

8.11.3 FTP proxy

In this module you can do the configuration for the FTP proxys for incoming and outgoing connections.

8.11.3.1 Outgoing

- **Port:** Enter the port, on which the FTP proxy should listen for requests.
- **Allow transparent proxying:** Choose the interfaces, that communicate with the proxy transparently. Thus no modifications must be made in the FTP clients of the clients. By marking an interface, an adequate NAT rule is created automatically, that redirects inquiries from clients to port 21 to the port you choose.
- **Kaspersky Anti-Virus:** Mark this checkbox, if you want to check your FTP traffic for viruses. You will need a valid Kaspersky license to activate this.
- **Use disk cache:** Mark this checkbox, if download files should be buffered in a cache on the hard disk. In the textfield **Size of disk cache (in MB):** you can determine the size of the cache.

ATTENTION: If you use the Microsoft Internet Explorer as FTP client you can run into trouble when downloading big files.

8.11.3.2 Incoming

If you run an FTP server, you should not let it be accessible for the Internet directly. You should hide the server behind a proxy, which receives the inquiries and gets the adequate files from the internal FTP server. The following settings are necessary if you want to make an internal FTP server accessible over the FTP proxy of Gibraltar:

Destination address: Enter the IP address of the internal FTP server, whereto incoming inquiries

should be redirected.

Destination port: Enter the port, on which the internal FTP server should listen for incoming inquiries. Normally it's port 21.

TIP: Do not forget to set a packet filter rule for the port 21 from the external network interface to LOCAL to ACCEPT.

8.11.4 Anonymization

This module offers some programs to make the use of services in the Internet anonymous. Requests to servers can be redirected over anonymization servers to hide the source of the requests. The requesting computer can be hidden completely.

8.11.4.1 Anon Proxy

This module forwards HTTP requests to an anonymization cascade which is offered by special servers. The HTTP request of the user is forwarded to an entry server which must be selected by the user. This server forwards the requests to other servers until it reaches its target.

For further information about the state of development and to get general descriptions please visit [JAP - TU Dresden](#).

1. Choose **Anonymization** in the main menu.
2. Choose the card **Anon proxy**.
3. Servers: Choose one of the given server which is the entry server for the anonymization cascade. The single servers offer different performances which can fluctuate very strongly depending on the time of the day.
4. Anon-proxy IP address: Enter the IP address where the anon-proxy should wait for incoming requests.
5. Port: Enter the port number where the anon-proxy should wait for incoming requests.
6. In combination with HTTP-proxy: Mark this checkbox if you want to use anon-proxy in combination with the default HTTP proxy. The default HTTP proxy forwards your requests to anon-proxy. The anon-proxy relays them to the Internet.
7. **Save:** Click this button, to save the changes.

8.11.4.2 Anonymizer

This module uses the proxy Tor which works similar to the anon-proxy but can also serve other services than HTTP. If you do not enter a Tor directory server into the element group the default directory servers are used.

For further information about the state of development and to get general descriptions please visit [Tor](#).

1. Choose **Anonymization** in the main menu.
2. Choose the card **Anonymizer**.
3. **Port:** Enter the port number where the Tor server should wait for requests.
4. **Tor directory servers:** Enter here new directory servers which should be used instead of the default servers.
 - **Server IP address:** Enter the IP address of the directory server that should be used.
 - **Port:** Enter the port number of the directory server that should be used.
 - **Fingerprint:** Enter the fingerprint of the directory server that should be used.
5. **Save:** Click this button, to save the changes.

8.11.4.3 Freenet

Freenet offers information to the Internet without showing who added the information to it. The source of the data is not recognizable. Each Freenet server offer the data for its users and fetches the information from other Freenet servers. You can activate Freenet at your Gibraltar firewall to participate in this global information pool.

ATTENTION: Freenet needs a high amount of RAM space. You can use Freenet only if your Gibraltar firewall has more than 256 MB RAM. Additionally you should offer some GB of your harddisk for storing Freenet data.

For further information about the state of development and to get general descriptions please visit [The Free Network Project](#).

1. Choose **Anonymization** in the main menu.
2. Choose the card **Freenet**.
3. **Server Port:** Enter the port number of the Freenet server which is offered to other Freenet servers.
4. **Client Port:** Enter the port number of the Freenet server which is offered to Freenet clients using special client software.
5. **Access allowed from:** Enter into this element group IP or network addresses that should be allowed to access your Freenet server.
6. **Do announce:** Mark this checkbox if you want to announce your Freenet server to other Freenet servers.
7. **Store size (in MB; min. 256):** Enter the size of storage on harddisk available for the Freenet service.
8. **Bandwidth limit incoming:** Enter the limitation for the incoming bandwidth used by Freenet.
9. **Bandwidth limit outgoing:** Enter the limitation for the outgoing bandwidth used by Freenet.
10. **Maximum number of connections:** Enter the maximum number of connections that should be allowed to access the Freenet server concurrently.
11. **Mainport:** Freenet also offers a seperate web frontend as starting point. Enter here the port number where this web frontend should be reachable.
12. **Access web frontend from:** Enter into this element group the IP or network addresses which should get access to the Freenet web frontend.
13. **Save:** Click this button, to save the changes.

8.12 Snort IDS

In this module the configurations for an **Intrusion Detection System** are set. Snort is used as IDS.

An Intrusion Detection System is a passive system to recognize attacks and intrusions. Snort is open source and the most commonly used IDS.

After an attack an alert or entry in the log files will be accomplished. There are some thousand rules for Snort, similar to anti virus scanners, the rules have to be updated regularly.

8.12.1 General

At this index card some general settings must be made.

- **Listen on Interface:** Choose interface on which Snort should listen.
- **Home Net Address:** Define IP addresses of the networks that are behind the firewall.
- **DNS/HTTP/SMTP Server IPs:** Enter the IP addresses of the specific internal servers you are using.

8.12.2 Output Modules

The IDS can send its output to different locations. At this index card you can select where you want to send the messages to:

- **Use Syslog Output Module:** The IDS sends its messages to the syslog.
- **Use Firewall Alert and Output Solution:** The IDS sends its messages to the given email addresses. You can select the priority that must be reached to send the messages.
- **Use Database Output Module:** An external database server (MySQL or PostgreSQL) is needed for this module. Unfortunately, Snort doesn't support encrypted database connections, so you have to use an IPSec tunnel. Scripts to generate the necessary tables are located locally under `/usr/share/doc/snort-mysql` or `/usr/share/doc/snort-pgsql`. A great external tool to analyze traffic is BASE.

8.12.3 Update Snort Rules

Snort rules are similar to virus signatures, they have to be updated regularly. There are 2 regularly, reasonable rule sources.

- **VRT rules:** Vulnerability Research Team rules are the recommended ones. They are maintained directly from Sourcefire and are well tested. You have to sign in for an snort account at snort.org to get the necessary oinkcode. There are 2 possibilities, just registering which is free or paying for the rules (\$1800/year). If you have chosen to pay for the rules, you get the rules 5 days earlier as the ones who are just registered.
- **Community rules:** Community rules are rules from users for users. These rules are released regularly, but they are not tested very well. The better choice are the VRT rules.

ATTENTION: In order to use the VRT rules, you have to register at snort.org and get an oinkcode to update the rules.

8.12.4 Snort Rules

This tab is used to activate or deactivate rule types. Rules for special services (like MySQL) are only necessary if you have such a service.

ATTENTION: Each rule can be modified with more details after clicking on details.

TIP: Use default settings.

8.13 Traffic shaping

Traffic shaping or QoS (Quality of Service) means managing the available bandwidth and prioritize some traffic. Using this functionality allows to ensure the needed bandwidth for some realtime services like Voice over IP or terminal server protocols. Services that are not realtime relevant can be placed back.

Possibilities of traffic shaping:

- **Prioritizing single services**
- **Ensure a minimum bandwidth for single services**
- **Split the available bandwidth to several hosts.**
- **Prioritizing several networks.**

Since version 2.5 it is also possible to manage incoming traffic. You can select at each network interface if you want to manage "incoming" or "outgoing" traffic. In order to ensure a optimal

bandwidth usage you should not allow more than 95 % of the totally available bandwidth as minimum.

For further information please have a look at the practical examples about traffic shaping [here](#).

8.13.1 General settings

In order to use traffic shaping correctly it is necessary to define the up- and download bandwidth for each network interface that is used. The bandwidth is printed in kbit/sec and can be selected from the select box or can be entered manually if you select CUSTOM.

8.13.2 Interface groups

You can merge several network interfaces to a shaping group.

- **Interface groups:** Enter a name for the new interface group and select the network interfaces that should be added to it. After you created it the group can be used to configure the [shaping rules](#).

8.13.3 Classification

The classifications are used to mark the traffic that should be prioritized. You can create rules here as in the module firewall to mark the packets you want. Please be careful to set the most specific classification to the top of the list. If you want to create a classification for a telephone system at source IP 192.168.1.1 for example, you must add it before the classification for the remaining traffic (Source: ANY; Destination: ANY, Service: ANY). The firewall marks the incoming packets depending on the order of the rules and forwards them to the shaping rules.

At the index card Standard you can configure the options as at the module [Firewall](#) and additionally the following ones:

- **Name:** Name of the classification
- **TOS Bits:** Use this setting to mark VoIP traffic. Many providers and routers filter for these settings to prioritize the VoIP traffic.

The other index cards are the same as in the module [Firewall](#).

Traffic shaping settings

General settings | Interface groups | **Classification** | Classification Group | Traffic shaping rules | Overview active rules

Move: From index: To index:

Classification:

Name	<input type="checkbox"/>					
1) voip_source	<input type="checkbox"/>					
2) voip_dest	<input type="checkbox"/>					
3) smtp_dest	<input type="checkbox"/>					
4) http_dest	<input type="checkbox"/>					
5) rest	<input type="checkbox"/>					

Traffic shaping settings

Default

Advanced

Advanced - P2P

Classification name:

Source address: or except:

Destination address: or except:

Service:

State:

Tos:

Comment:

8.13.4 Classification Group

You can group the classifications to a named group to be used in the shaping rules definitions. We recommend to create a classification "icmp" when you create any kind of prioritizing and add this classification to a group containing the other prioritized services. In case of troubles you can check the ICMP response times and can see that the traffic shaping works when you get short response times when the firewall is under full load.

- **Classification groups:** Set a name for the group and add all necessary classifications to it. You can use this group at the shaping rule definition afterwards.

8.13.5 Traffic shaping rules

The traffic shaping rules are the settings to manage the bandwidth. You can set minimum and maximum available bandwidth for single computers, networks or IP ranges. Further information in configuring traffic shaping can be found at the [practical examples](#). Before you can create the shaping rules you must define the classifications first.

All traffic shaping rules are listed in the overview. You find the following information:

- **Track:** Shows the direction and the interface the shaping rule is created for (e.g. incoming ext -> download).
- **Bw. (kbit):** The whole bandwidth that was defined for the interface at the general settings.
- **Bw. assured (kbit):** The bandwidth that is already used by the shaping rules for this interface.
- **Active:** Activates/deactivates the shaping rule.
- **Name:** Name of the rule.
- **Classification/group:** Select the classification or the classification for this rule.
- **Min:** Minimal bandwidth for this classification/group
- **Max:** Maximum bandwidth for this classification/group

8.13.6 Traffic shaping rules - Detail

When creating a new traffic shaping rule you can do the following configurations at the index card **Standard:**

- **Activate rule:** Activate the current rule.
- **Name:** Name of the current rule.
- **Track:** Network interface and direction of the traffic that should be prioritized.

- **Comment:** Add a comment to be informed in future.
- **Classification/group:** Select the classification or group out of the select box and enter the minimal and maximal values.

The index card **Advanced** contains further settings. See some examples at the [practical examples](#)

- **Source address:** Enter the source address of the traffic you want to manage.
- **Create a rule for every IP address in the source:** If you entered a IP range at the source address field you can select this check box to create a rule for every IP address within this range. This option is needed to split up the available bandwidth to several host in the same size.
- **Destination address:** Enter the destination address of the traffic you want to manage.
- **Create a rule for every IP address in the destination:** If you entered a IP range at the source address field you can select this check box to create a rule for every IP address within this range.
- **Maximum bandwidth (kbit) per IP address:** If you selected one of the options "Create a rule for every IP address in the source" or "Create a rule for every IP address in the destination", you must use this option, too. The upper limit for each IP address within the range is set to this value. This ensures that the different IP addresses do not remove available bandwidth from each other. Within these borders the Min/Max values of the classifications are active.
- **Bandwidth (kbit) for nets:** This option can be used by service providers (ANY = bandwidth of the interface) if you want to shape the traffic to different networks. A detailed manual can be found at the [practical examples](#).

8.13.7 Overview active rules

Here you can see an overview of all active shaping rules. They can be deleted, activated or deactivated here.

8.14 Captive Portal

Captive Portal is a HotSpot service that allows to add restrictions for the users concerning online time and download amount. This service can also be used for wireless LAN. Until the user has not been authenticated, he is redirected to the login mask of the service. After he logged in successfully, he can use all Internet services that are allowed by firewall rules.

You must only select the interface where the services should listen at. After starting the service you will get network information like IP address from the DHCP server that is also part of the service. You will get an IP address out of the range that has been entered at the web interface.

ATTENTION: Be careful that the network range you define here does not touch another network range configured at another interface. This can cause trouble.

The list "Allowed Addresses without authentication" can contain URLs that can be reached without authentication.

At the index card **Default Values** you can limit the users download/upload rates. If you do not enter any values here there is no limit set.

NOTE: If you use an Active Directory authentication the index card is not shown.

8.15 Configuration management

The module **Configuration management** offers several possibilities to store your Gibraltar configuration permanently. As Gibraltar boots completely from CD or Compact flash it is necessary to save the configuration permanently on another medium. At present you have the possibility to save the configuration on USB stick, on floppy disk or on hard disk. You can also send the compressed configuration via email.

The configuration files are stored compressed and in one file. This file is copied to the storage media you chose.

8.15.1 General settings

To enable **Configuration management** you need to configure a basic configuration that you have to set on this card. You have to define the various paths to the storage mediums and set a standard storage medium where Gibraltar saves the config if it reboots or shuts down.

Default save target: The default save target chosen from this options is used automatically for saving the configuration, if Gibraltar shuts down or restarts or if you click to the link "Quick-Save" at the title bar. Thereby the option **Source** has to be singled out. This option makes it possible to save the configuration on the same storage media as it has been loaded from. So for example if you saved your configuration on an USB stick, and the configuration was loaded from the USB stick when Gibraltar started, automatically the new configuration will also be stored on the USB stick, when Gibraltar shuts down.

Save to floppy disk: Choose the floppy disk drive, on which the configuration should be saved. This entry is necessary, if you want to save the configuration on a floppy disk.

Save via email: Enter the email address you want to send the configuration to.

Automatically format floppy or harddisk: Mark this checkbox if you want to automatically format floppy disks or hard disk partitions before saving the config.

Save on shutdown: Mark this checkbox, to save the configuration automatically at the default saving destination, when Gibraltar shuts down.

TIP: If you want to load your config from a storage medium simply put the medium in your computer and boot the firewall. Gibraltar will search for the config while booting and load it again from the device.

8.15.2 Save config

The card **Save configuration** offers the possibility to store and download your current config. Thereby you can set a storage media, on which you want to store the actual configuration, independently from the default storage media. Additionally you have the possibility to download the configuration.

Additionally you can download the configuration or send it via email. If you remove your configuration from hard disk or compact flash, your firewall will be starting with the factory defaults when it is rebooted.

9 Support

You can send support requests directly from the web interface to the support team of the firewall. Please give us as much information as possible. Of course you can only send a request when you have a running Internet connection.

Alternatively you can send your support questions to support@gibraltar.at.



The screenshot shows a web form titled "Support" with a sub-section "Mail to support". It contains three input fields: "From (email):", "Subject:", and a large "Text:" area with a vertical scrollbar. A "Send" button is positioned at the bottom center of the form.

10 Update

This section gives information about updates and patches to you.

10.1 Version info

Shows the currently used version and the newest version available.

10.2 Online update

If necessary the producers offers patches and updates here which can be downloaded and installed automatically (see module [System](#)). With this possibility we can react very fast to upcoming security vulnerabilities.

Alternatively to the automatic download and installation of available patches you can download and install them manually.

All available patches are shown in the list. Already installed patches are marked by a green checkmark.

The following things can be done here:

- **Download and install:** Activate the checkbox beside the patches you want install. Afterwards click the button "Download".
- **Delete:** Activate the checkbox beside the installed patches that you want to remove. Afterwards click the button "Delete" at the bottom.

10.3 Upload CF image

If you are using a Gibraltar Security Gateway your operating system is stored to a compact flash card. To update the basic system you must upload a new version here.

Complete the following steps to update your firewall:

1. Download the new version of the software at the Gibraltar web site.
2. Upload the *.tgz file to the firewall.
3. Reboot the firewall.

10.4 Remove updated files and Rollback

After you completed the update of your firewall you can remove the files of the old firewall version. If you recognize any troubles after the update, you can switch back to the old version of the firewall software (roll back).

Index

- A -

- ACCEPT 69
- active rules 71, 76
- Additional interfaces 62
- Authorization 63, 92
- available settings:
 - * Alert Tuning: 105
 - * General: 105
 - * Output Modules: 105
 - * Preprocessors: 105
 - * Snort Rules: 105
 - * Update Snort Rules: 105
 - o Activate IPS mode 105
 - o Activate/Deactivate rules 105
 - o Activate/Deactivate several preprocessors 105
 - o additional settings 105
 - o Choose available rule sources 105
 - o Database Output Module 105
 - o Define own addresses and services 105
 - o Gibraltar Firewall Alert and Output Solution 105
 - o Select the interface on which Snort should run 105
 - o Syslog Output Module 105

- C -

- CA certificates 95
- certificate 92, 95
- CHAP 63
- Check IP address 64
- client-to-network 94
- Configuratin management 110
- Configuration management 110
- Connection check interval 64
- Connection test 60

- D -

- Default route 59, 63
- Dest IP address 72
- Dest IP address: 69
- DHCP 67
- Dial on Demand 63

- Dial tone 63
- Dial-In 62
- DNS 58
- Domain 58, 68
- DROP 69
- dynamic packet filter 69

- E -

- ESP algorithms 93
- established 69

- F -

- Firewall 5, 69
- Firewall rules 69
- Floppy 110
- FQDN 58
- Fragmentation 73

- H -

- HDD 110
- Holdoff 63

- I -

- ICMP 72
- ICMP-Type 72
- Idle 63
- IKE algorithms 93
- incoming 69, 74
- Installation 8
- Interface 58
- IP address 58
- IP compression 93

- L -

- Limit 73
- Lizenzdatei 47
- Lizenzschlüssel 8
- LOG 69

- M -

- MAC address 58
- Mail of Admin 50

- N -

NAT 74
NAT Traversal 91
Network 57
Number of logs 51

- O -

outgoing 69, 74

- P -

PAP 63
password 50
phone 62
Phone Number 63
ping 60
PPTP 63, 94
Protocol 69, 72
Pulse 63

- R -

range 68
Reboot 50
Refresh frequency 51
REJECT 69
related 69
Relaying 83
Routing 59

- S -

Services 55
Shutdown 50
Source IP address 69, 72
Source MAC address 73
Source port 72
Speichern 49
SPI 73
Start automatically 55, 58
Start service 55
State 72
Stateful Inspection 69
Static IP 58
Stop service 55
Syslogs 51
System name 50

- T -

Target 69
timezone 50
Tone 63
TTL 73
Tunnel 91

- U -

USB 110
Username 63

- X -

X509 92