



User Manual

Gibraltar Firewall - release 2.4

Gibraltar Firewall

© 2006 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: Februar 2008 in Attnang-Puchheim, AUSTRIA

Publisher

eSYS Informationssysteme GmbH

Managing Editor

Thomas Mayrhofer

Technical Editors

Dipl.-Ing. Richard Leitner

Mag. Andreas Wöckl

Special thanks to: Dipl.-Ing. Dr. Rene Mayrhofer

Table of Contents

Vorwort	0
Part I Introduction	2
1 Gibraltar - Development	2
2 Gibraltar - Features	2
Part II Firewall basics	6
1 Firewall	6
2 Network Address Translation (NAT)	7
3 Proxy services	7
4 Virtual Private Networks (VPN)	8
Part III Hardware requirements	8
Part IV Installation	9
Part V Licensing	9
Part VI The webinterface	10
Part VII Practical examples	11
1 ADSL	13
2 Internet-Gateway	16
3 Firewall und DMZ	18
4 IPSec VPN	23
5 Active Directory	27
6 Proxy Server	30
7 Traffic Shaping Citrix	32
8 Traffic Shaping VoIP	37
9 Traffic Shaping Web Traffic	38
Part VIII Support	40
Part IX Update	40
1 Version info	40
2 Online update	41
3 Upload CF image	41
4 Remove updated files and Rollback	42
Index	43

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 und 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
- Authentication: 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 responsible 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 (≥ 600 MHz)
- ≥ 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.

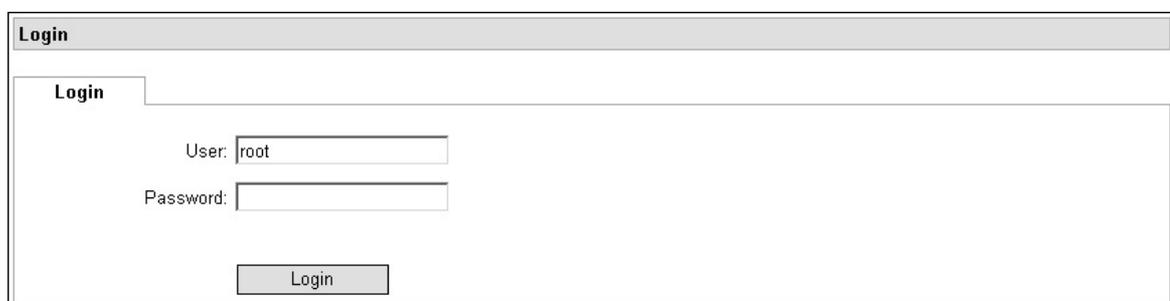


NOTE: It can take a few seconds, until the www server of GibADMIN is fully functional.

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 web browser window titled "Login". Inside the window, there is a form with a "Login" label. The form contains two input fields: "User:" with the text "root" entered, and "Password:". Below the input fields 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

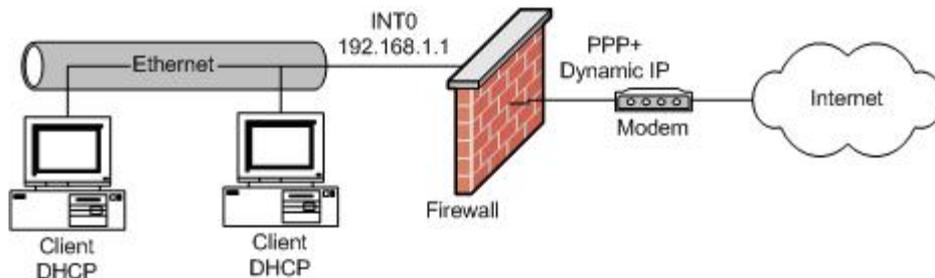
Configuration of Gibraltar as a transparent traffic shaper that can be activated without changing the current network infrastructure. This scenario shows how to ensure the usage of 70 per cent of the bandwidth for the Citrix terminal sessions (protocol ICA). The other services get only 80 per cent of 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 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.

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.

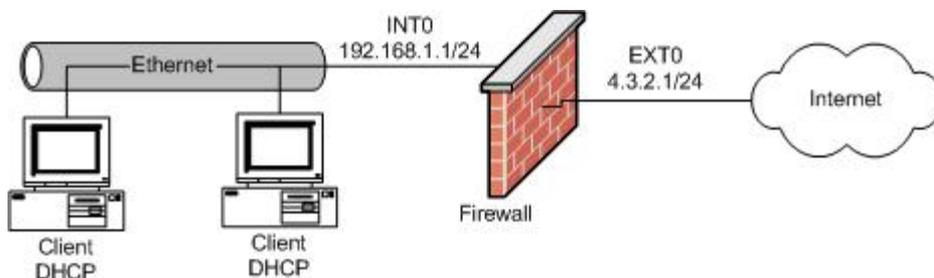
1. Choose **Services** in the main menu.
2. **Available services:** Select the option **On** next to **DHCP server**. Thus the DHCP server will be started automatically, when Gibraltar reboots.
3. **Save:** Confirm your changes with clicking the button **Save**.
4. **Start service** : Click this button 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

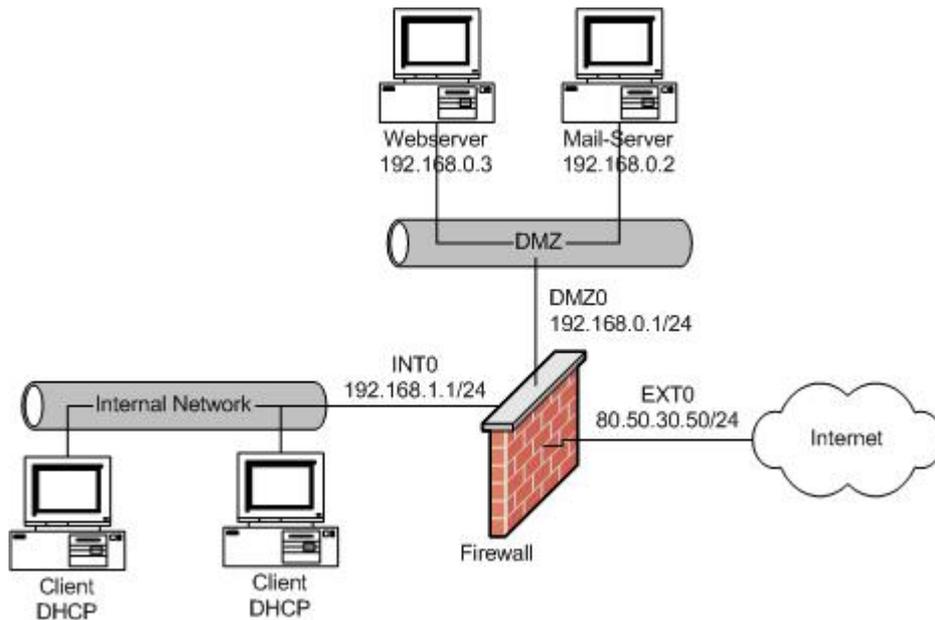
1. Save your configuration on an USB-stick or to the HDD.

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 mailserver 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 you 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:

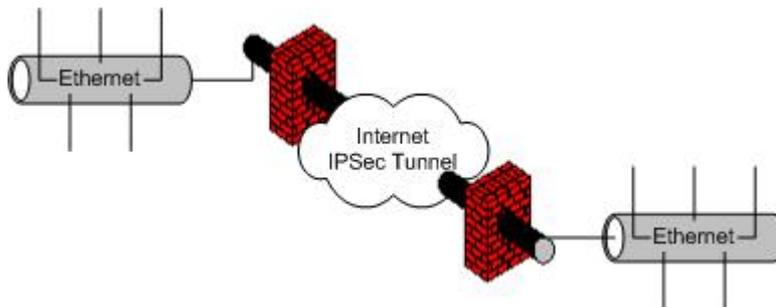
1. Choose **Mail** in the main menu.
2. Choose the tab **Relay outgoing**.
3. **Local networks:** Click the button **Add network address** to add a new network address. All networks in this list are allowed to send e-mails. Keep the setting 127.0.0.1/8 because Gibraltar also sends e-mails to the administrator.
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.

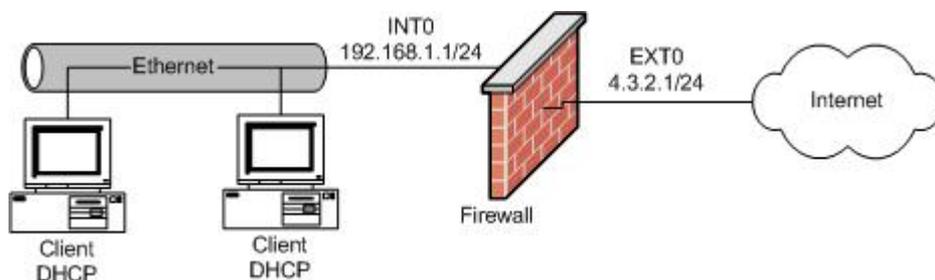
Saving configuration

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

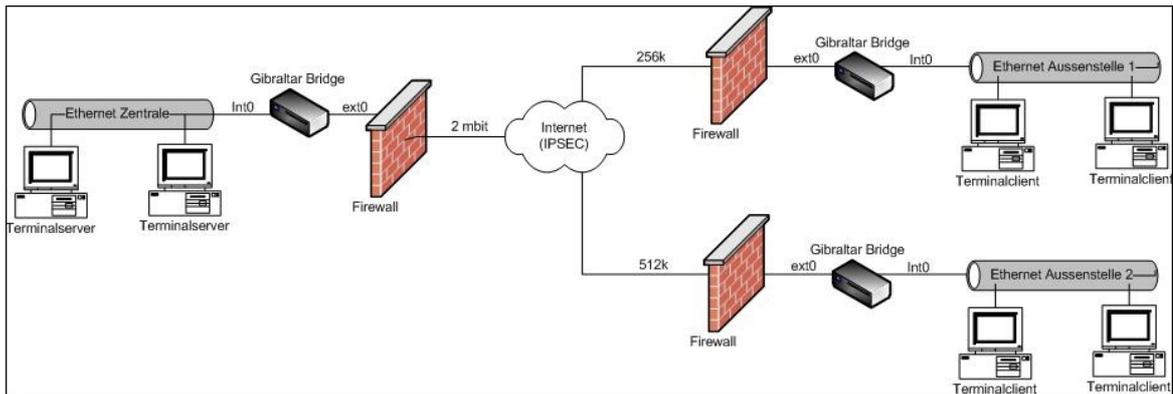
1. Save your configuration.

7.7 Traffic Shaping Citrix

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 70 % of the available bandwidth. Because of latency the remaining traffic only gets a maximum of 80 % of the total bandwidth. Only 95 % of the total bandwidth may be used to ensure a optimal functionality. The following initial situation is given:

- Headquarter with 2mbit internet connection
- Site 1 with 256 k internet connection
- Site 2 with 512k internet connection

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. **IP address:** Choose the option field **static** to define the IP address for this network interface statically.
6. **Static IPs:** Alter the IP address in the textfield **IP address/netmask** to the IP address in your internal network (CIDR-Notation: e.g. 192.168.0.1/24).
7. **Save:** Confirm your changes with clicking the button **Save**.
8. Choose the tab of the interface **eth0**.
9. **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).
10. **Start automatically:** Mark this checkbox to start the network interface automatically, when Gibraltar boots.
11. **IP address:** Delete the existing IP address.
12. **Save:** Confirm your changes with clicking the button **Save**.
13. Choose the index card **Bridging**.
14. **Interface:** Allocate a name for the bridge (e.g. "myBridge")
15. **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.
16. **Bridged Interfaces:** Choose the interfaces "int0" and "ext0".
17. **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.
6. **Service:** Choose ACCEPT from the selection box to allow all services.
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 position 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. **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

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.
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. **Add classification:** Click this button for adding a new classification for the ICA destination ports.
13. **Name:** Enter a name for the new classification (e.g. "icaDest").
14. **Source address, Destination address:** Select the value ANY from the select boxes.
15. **Service:** Select the value "ica_destination" from the select box.
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. **Source address, Destination address:** Select the value ANY from the select boxes.
21. **Service:** Select the value "CUSTOM" from the select box.
22. **Protocoll:** Select the value "ICMP".
23. **Save:** Confirm your changes with clicking the button **Save**.
24. **Add classification:** Click this button for adding a new classification for the remaining traffic.
25. **Name:** Enter a name for the new classification (e.g. "other").
26. **Source address, Destination address:** Select the value ANY from the select boxes.
27. **Save:** Confirm your changes with clicking the button **Save**.

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

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

To finish the configuration you must set the rules for the two external offices.

1. Choose the tab **Traffic shaping rules**.
2. **Track:** Choose "outgoing ext0".
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 "highPrio" and set the values "180" for Min and "256" for Max.
7. Choose the classification "other" and set the values "76" for Min and "205" for Max.
8. **Save:** Confirm your changes with clicking the button **Save**.
9. Choose the tab **Advanced**.
10. **Destination address:** Choose the definition "net1", because this rule should only be valid for this destination net.
11. **Bandwidth (kbit) for nets:** Choose the value "256".
12. **Save:** Confirm your changes with clicking the button **Save**.
13. **Cancel:** Click this button to return to the overview.
14. **Add rule:** Click this button to add a new rule.
15. **Name:** Enter a name for the new rule (e.g. "ruleNet2").
16. **Add member:** Click this button to add classifications or classification groups.
17. Choose the classification group "highPrio" and set the values "360" for Min and "512" for Max.
18. Choose the classification "other" and set the values "152" for Min and "410" for Max.
19. **Save:** Confirm your changes with clicking the button **Save**.
20. Choose the tab **Advanced**.
21. **Destination address:** Choose the definition "net2", because this rule should only be valid for this destination net.
22. **Bandwidth (kbit) for nets:** Choose the value "512".
23. **Save:** Confirm your changes with clicking the button **Save**.

Save config

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

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 value "256" for the interface "ext0" 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 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. **Save**: Confirm your changes with clicking the button **Save**.
11. **Add classification**: Click this button for adding a new classification for the ICA destination ports.
12. **Name**: Enter a name for the new classification (e.g. "icaDest").
13. **Source address, Destination address**: Select the value ANY from the select boxes.
14. **Service**: Select the value "ica_destination" from the select box.
15. **Save**: Confirm your changes with clicking the button **Save**.
16. **Add classification**: Click this button for adding a new classification for ICMP. ICMP should be managed by default for error diagnosis.
17. **Name**: Enter a name for the new classification (e.g. "icmp").
18. **Source address, Destination address**: Select the value ANY from the select boxes.
19. **Service**: Select the value "CUSTOM" from the select box.
20. **Protocol**: Select the value "ICMP".
21. **Save**: Confirm your changes with clicking the button **Save**.
22. **Add classification**: Click this button for adding a new classification for the remaining traffic.
23. **Name**: Enter a name for the new classification (e.g. "other").
24. **Source address, Destination address**: Select the value ANY from the select boxes.
25. **Save**: Confirm your changes with clicking the button **Save**.
26. Choose the tab **Classification Group**.
27. **Add group**: Click this button to add a new classification group containing "icaSource" and "icmp".
28. **Name**: Enter a name for the group (e.g. "highPrio").
29. **Add member**: Choose the members "icaSource", "icaDest", and "icmp".
30. **Save**: Confirm your changes with clicking the button **Save**.
31. Choose the tab **Traffic shaping rules**.
32. **Track**: Choose "outgoing ext0".
33. **Add rule**: Click this button to add a new rule.
34. **Name**: Enter a name for the new rule (e.g. "ruleHeadquarter").
35. **Add member**: Click this button to add classifications or classification groups.
36. Choose the classification group "highPrio" and set the values "180" for Min and "256" for Max.
37. Choose the classification "other" and set the values "76" for Min and "205" for Max.
38. **Save**: Confirm your changes with clicking the button **Save**.
39. **Cancel**: Click this button to return to the overview.

Complete the configuration for site 2 with the bandwidth value of 512 kbit analogous. 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.

7.8 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. 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

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. **BE CAREFUL:** Choose the value 2048 only if you are sure you really do have this bandwidth. In most cases the bandwidth is dithering. If you notice some troubles during your telephone calls, adapt this value down to a lower one.
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**.

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. **Save:** Confirm your changes with clicking the button **Save**.
8. **Add rule:** Click this button to add a new rule.
9. **Track:** Choose "outgoing ext0" to manage outgoing traffic.
10. **Name:** Enter a name for the new rule (e.g. "ruleUpload").
11. **Add member:** Click this button to add classifications or classification groups.
12. Choose the classification group "highPrio" and set the values "1024" for Min and "2048" for Max.
13. **Save:** Confirm your changes with clicking the button **Save**.

Save config

1. Save your configuration on an USB-stick.

The above configuration ensures a minimal bandwidth of 1 MBit for your telephone system. If you notice some troubles during your telephone calls, adapt this values for the interfaces down to a lower one. A detailed reporting of your bandwidth management can be seen at Monitoring.

7.9 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 500 kbit. The whole bandwidth of the line is 2048 kbit.

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. **BE CAREFUL:** Choose the value 2048 only if you are sure you really do have this bandwidth. In most cases the bandwidth is dithering. If you notice some troubles, adapt this value down to a lower one.
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 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 "web" and set the values "500" for Min and "2048" for Max.
7. Choose the classification group "pop3" and set the values "500" for Min and "2048" for Max.
8. **Save:** Confirm your changes with clicking the button **Save**.

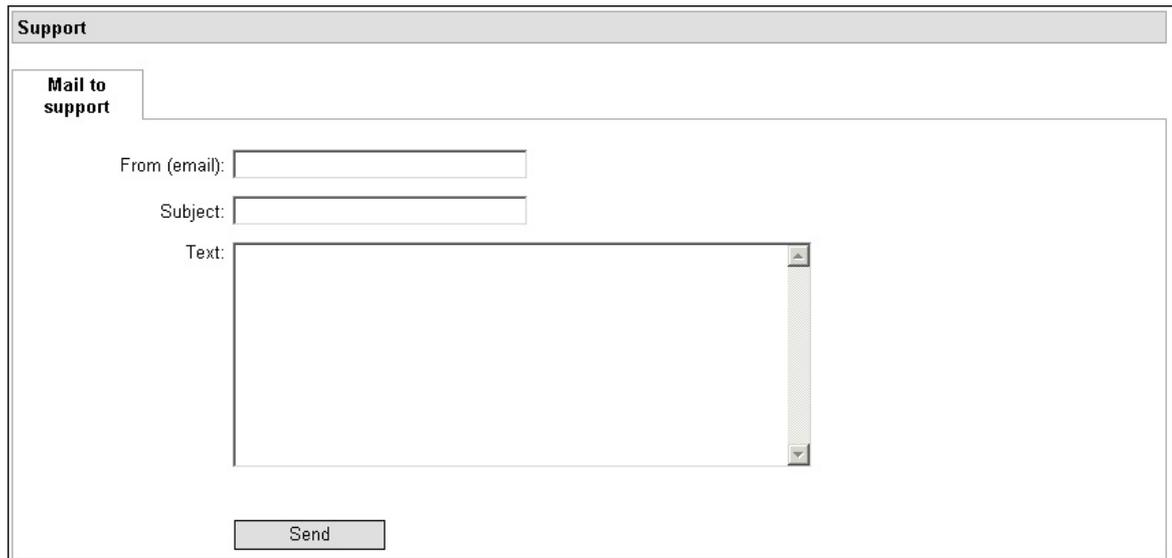
Save config

1. Save your configuration on an USB-stick.

8 Support

The card **Mail to support** offers the possibility to mail technical inquiries to your support.

1. **From (email):** Enter your email address in this textfield, so that your support can answer you immediately.
2. **Subject:** Enter the subject of your support enquiry.
3. **Text:** Enter your enquiry in this textfield. Try to describe your problem carefully.
4. **Send:** Click this button to send your mail.



The screenshot shows a web interface titled "Support". Inside, there is a tab labeled "Mail to support". Below the tab, there are three input fields: "From (email):", "Subject:", and "Text:". The "Text:" field is a large text area with a vertical scrollbar on the right side. At the bottom of the form, there is a "Send" button.

9 Update

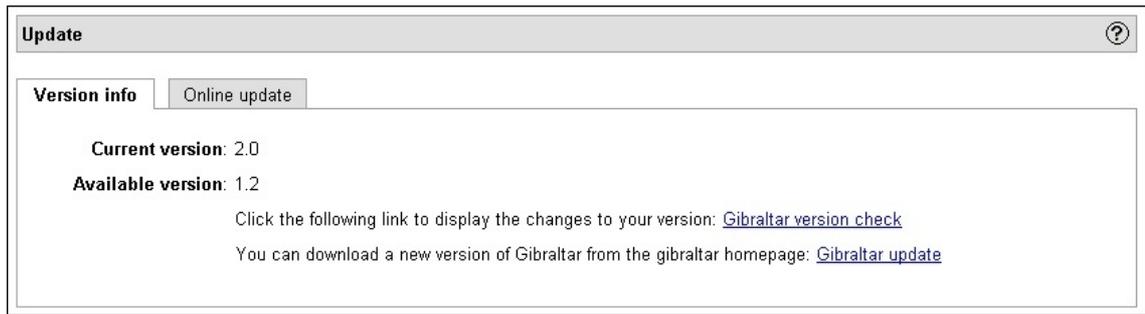
Use the link Update in the header of GibADMIN if you want to get information about new updates and patches for Gibraltar. When you click this link, GibADMIN looks for new patches and updates on the Gibraltar server (<http://www.gibraltar.at>).

ATTENTION: Consider, that access to the published patches is granted only with a valid license, but not with a test license.

9.1 Version info

On this card you get information about the version of Gibraltar you currently are using. The producers of Gibraltar also inform you about new versions on this site.

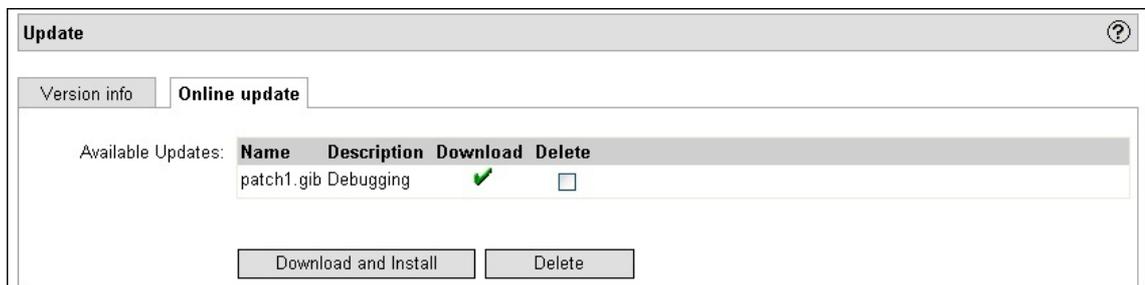
1. Choose **Update** in the header section.
2. Choose the card **Version info**.
3. **Current version:** Shows the version of Gibraltar that you currently are using.
4. **Available version:** Shows the version of Gibraltar that can be downloaded from the Gibraltar server (<http://www.gibraltar.at>).



9.2 Online update

On this card you see the patches that can be downloaded from the Gibraltar webserver. Patches are generated if new security holes are found in the base modules of Gibraltar that need to be repaired very rapidly.

1. Choose **Update** in the header section.
2. Choose the card **Online update**.
3. **Available updates:** This overview shows the updates and patches that can be downloaded from the Gibraltar webserver.
4. **Name:** Shows the name of the patch.
5. **Description:** Here you can see a short description of the functions of the patch.
6. **Download:** Mark this checkbox if you want to download and install the shown patch.
7. **Delete:** Mark this checkbox if you want to delete the patch that has been downloaded earlier.
8. **Download and install:** Click this button to start the download and installation of the patch that you have marked for downloading above.
9. **Delete:** Click this button to delete the patch that you have marked for deleting above.



9.3 Upload CF image

On this tab you can update Gibraltar with a new CF image (compact flash) in case that you start Gibraltar from a CF card. Mainly security appliances start from CF card. Before you upload a new version, make sure that files from older versions are deleted from the CF card. You can do this on the tab **Remove updated files and Rollback**. There you can also get back to the older version after the update by clicking the button **Examine rollback**.

After uploading a new version, Gibraltar needs to restart. Thereby Gibraltar starts with the uploaded image and replaces the files of the old version. The old version will be kept on the CF card, so that it's possible to rollback.

1. Choose **Update** in the title bar.
2. Choose the tab **Upload CF image**.
3. **CF image:** Enter the name of the CF image file, that you downloaded from the Gibraltar homepage or from a mirror. You can also look for the file on your hard disk by clicking the button **Durchsuchen...** The file name should end with .tgz, otherwise Gibraltar won't accept it and no update will be carried out.
4. **Upload:** Click this button to upload the file to Gibraltar.

ATTENTION: Don't forget to save eventual changes of the configuration on an adequate

media before you restart. Otherwise your changes will be lost.

9.4 Remove updated files and Rollback

This index card makes it possible to countermand an online-update.

1. Choose **Update** in the title bar.
2. Choose the index card **Delete old files and Rollback**.
3. **Delete old files**: Click this button to delete files of the last online-update.
4. **Effect Rollback**: Click this button to return to the last version.

Index

- F -

Firewall 6

- I -

Installation 9

- L -

Lizenzschlüssel 9