Benutzerhandbuch

Gibraltar Firewall - Version 2.6

© 2008 by eSYS Informationssysteme GmbH

Gibraltar Firewall

© 2008 by eSYS Informationssysteme GmbH

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

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

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

Printed: Juli 2008 in Attnang-Puchheim, AUSTRIA

Publisher

eSYS Informationssysteme GmbH

Managing Editor

Thomas Mayrhofer

Technical Editors

Dipl.-Ing. Richard Leitner

Mag. Andreas Wöckl

Manuel Hofer

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

Inhaltsverzeichnis

Vorwort 0

Teil I Einführung 1

1 Gibraltar ... 1
2 Funktionsumfang ... 1

Teil II Grundlagen 3

1 Firewall ... 3
2 Addressübersetzung (NAT) ... 5
3 Proxy-Dienste ... 5
4 Virtuelle Private Netzwerke (VPN) ... 6

Teil III Hardware 7

Teil IV Installation 7

Teil V Lizenzierung 9

Teil VI Das Webinterface 10

Teil VII Anwendungsbeispiele 12

1 ADSL ... 14
2 Internet-Gateway ... 18
3 Firewall und DMZ ... 21
4 IPSec VPN ... 26
5 Active Directory/Open VPN ... 32
6 Proxy Server ... 36
7 Bandbreitenmanagement Citrix und VOIP transparent ... 40
8 Bandbreitenmanagement Citrix und VOIP mit VPN ... 47
9 Bandbreitenmanagement VoIP ... 54
10 Bandbreitenmanagement Web Traffic ... 57

Teil VIII Konfiguration 58

1 Lizenzinformation ... 60
2 System ... 62
Allgemeine Einstellungen ... 63
Systemlogs anzeigen ... 65
Suche im Syslog ... 65
Festplatte konfigurieren ... 65
Failover/Heartbeat ... 66
Logins blockieren ... 66
Aktive Verbindungen ... 67
3 Monitoring ... 67
System ... 68
Mail ... 68

© 2008 by eSYS Informationssysteme GmbH

Interfaces ... **69**
Traffic accounting ... **69**
Traffic shaping ... **69**
Troubleshooting ... **70**
4 Dienste ... **70**
5 Netzwerk ... **72**
Netzwerk ... **72**
DNS ... 73
Netzwerkkarte ... 73
Routing ... 75
Verbindungstest ... 76
Definitionen ... **76**
Host/Netz Aliases ... 77
Host/Netz Gruppen ... 77
Services ... 77
Zusätzliche Interfaces ... 78
Dial-in ... **78**
Telefoneinwahl ... 78
Telefoneinwahl - Detailansicht ... 79
ADSL PPTP ... 79
ADSL PPTP - Detailansicht ... 80
ADSL PPP over ATM ... 81
ADSL PPP over ATM - Detailansicht ... 81
ADSL PPP over Ethernet ... 82
ADSL PPP over Ethernet - Detailansicht ... 82
Bridging ... **83**
VLAN ... **84**
DHCP-Server ... **85**
DHCP - Allgemeine Einstellungen ... 85
DHCP - Konfiguration ... 85
DHCP leases ... 86
DHCP-Relay ... 86
Dynamic DNS ... **86**
6 Firewall ... **87**
Firewallregeln ... **87**
Übersicht aktiver Regeln ... **90**
Erweiterte Einstellungen ... **91**
Firewallregel bearbeiten ... **91**
Firewallregel - Erweitert ... **93**
Firewallregel - Erweitert P2P ... **96**
7 NAT ... **96**
NAT-Regeln ... **96**
Übersicht aktiver Regeln ... **99**
NAT-Regel bearbeiten ... **99**
8 Benutzer ... **101**
Benutzerverwaltung ... **101**
LDAP Einstellungen ... **104**
Freeradius Accounting ... **107**
9 Mail ... **108**
Mail-Relay ... **109**
Mail - Allgemeine Einstellungen ... 109
Weiterleitung ausgehend ... 110
Weiterleitung eingehend ... 111
Allgemeine Überprüfungen ... 111
SMTP Authentifizierung ... 112
AntiSpam ... **112**
AntiSpam (1) ... 112

© 2008 by eSYS Informationssysteme GmbH

AntiSpam (2) ... 114
Blacklists and Whitelists ... 115
Spracheinschränkungen ... 116
Regeln updaten ... 117
AntiVirus ... 117
10 VPN ... 117
Open VPN ... 117
Allgemeine Einstellungen ... 118
Erweiterte Einstellungen ... 119
Status ... 119
IPSec ... 120
IPSec - Allgemeine Einstellungen ... 120
Tunnel ... 120
Tunnel - Standard ... 121
Tunnel - Erweitert ... 123
Watchdog ... 123
PPTP ... 123
PPTP - Allgemeine Einstellungen ... 124
PPTP - Erweiterte Einstellungen ... 124
L2TP ... 124
L2TP - Allgemeine Einstellungen ... 125
Zertifikate ... 125
Certificate Revocation List ... 126
Hostzertifikat erstellen ... 126
Clientzertifikat erstellen ... 127
SSL ... 128
SSL VPN ... 128
11 Proxy-Server ... 129
HTTP-Proxy ... 129
Allgemeine Einstellungen ... 130
Proxy Cache ... 130
Authentifizierung ... 131
Content Filter ... 131
Ausnahmen ... 131
PureSight Content Scanner ... 131
POP3-Proxy ... 133
Allgemeine Einstellungen ... 133
Anlagen umbenennen ... 134
FTP-Proxy ... 135
Ausgehend ... 135
Eingehend ... 136
Anonymisierung ... 136
Anon Anonymisierer ... 136
Tor Anonymisierer ... 137
Freenet ... 137
12 Snort IDS ... 138
Allgemein ... 138
Output Modules ... 138
Regelupdate ... 138
Snort Regeln ... 139
13 Traffic Shaping ... 139
Allgemeine Einstellungen ... 140
Interface Gruppen ... 140
Klassifizierung ... 140
Klassifizierungsgruppen ... 141
Traffic Shaping Regeln ... 141
Traffic Shaping Regeln - Detail ... 142
Traffic Shaping Regeln - Aktive ... 143

© 2008 by eSYS Informationssysteme GmbH

14 Captive Portal 143
15 Konfigurationen verwalten 143
Konfiguration - Allgemeine Einstellungen 144
Konfiguration speichern 144

Teil IX Support 145

Teil X Update 145

1 Versionsinfo 145
2 Online update 145
3 CF Image Upload 146
4 Remove updated files and Rollback 146

Teil XI Anhang 146

Index 147

© 2008 by eSYS Informationssysteme GmbH

1 Einführung

1.1 Gibraltar

Wir freuen uns, dass Sie sich zum Kauf eines Gibraltar Security Gateways oder der Gibraltar Security Software entschieden haben.

Gibraltar wird in folgenden Varianten angeboten:

- **Gibraltar Software**: als hardwareunabhängige Software-Lösung
- **Gibraltar Security Gateway**: Gibraltar vorinstalliert auf spezieller Hardware (Appliance)

Dieses Handbuch führt sie schrittweise durch die Installation von Gibraltar und soll dem Administrator als Nachschlagwerk dienen. Sollten Sie noch nie eine Firewall konfiguriert haben, verweisen wir in diesem Zusammenhang insbesondere auf das Kapitel Anwendungsbeispiele. In diesem Kapitel finden sie schrittweise Anleitungen für gebräuchliche Anwendungsszenarien. Diese Anwendungsbeispiele sind sehr gut geeignet, um direkt mit der Konfiguration von Gibraltar beginnen.

Das vorliegende Benutzerhandbuch finden sie in der jeweils aktuellsten Version auch im Internet unter www.gibraltar.at, sowie in Form einer Onlinehilfe direkt im Webinterface von Gibraltar (GibAdmin)

Sollten sie Fragen oder Verbesserungsvorschläge zum vorliegenden Benutzerhandbuch haben, bitten wir Sie uns eine E-Mail unter support@gibraltar.at zu schicken.

1.2 Funktionsumfang

Gibraltar Security Produkte vereinen mehrere wichtige Sicherheitsanwendungen in einem Produkt (Unified Threat Management). Durch die Kombination vieler verschiedener Sicherheitsanwendungen ist es möglich, einer Vielzahl von aktuellen Bedrohungen zu begegnen. Der Funktionsumfang von Gibraltar im Detail (detaillierter Informationen finden Sie auch auf unserer Homepage www.gibraltar.at):

System und Management

- Speziell gehärteter OS-Kernel basierende auf Debian Linux
- ReadOnly Bootmedien: USB, CD-ROM
- Konventionelle Bootmedien: Compact Flash, Festplatte
- Sprachen: Deutsch, Englisch
- Management: Remote mittels webbasiertem Konfigurationswerkzeug (SSL) oder Remote Login (SSH)
- Einfaches Konfigurationsmanagement
- Benutzerverwaltung: LDAP (lokal und extern), Active Directory
- Automatisches Software-Update-Service
- High-Availability: Hot-Standby
- Ausführliche Protokollierung und interaktive Auswertung

Schnittstellen

- Beliebige Anzahl von Netzwerk-Schnittstellen

© 2008 by eSYS Informationssysteme GmbH

- Beliebige Anzahl von IP-Adresses je Netzwerk-Schnittstelle.
- Ethernet 10/100/1000: statische oder dynamische IP-Adressen
- ADSL (PPTP, PPPoATM, PPPoE), ISDN
- VLAN's
- Bridging
- Grafische Traffic-Auswertungen

Firewall und Paketfilter

- Stateful Packet Inspection Firewall
- Unterstützung aller gängigen Netzwerkprotokolle (Protokoll Pass Through: PPTP, FTP, H.323, IRC)
- Flexibler Paketfilter: Schnittstelle, MAC Adresse, IP Adresse, Port, Service, etc.
- Schutz vor DoS/Flood Angriffen
- Einschränkung von Peer-2-Peer Diensten (P2P)
- Dynamische und statische Adressübersetzung: Network Address Translation (NAT), Port Address Translation (PAT)
- Load Balancing
- Transparentes Layer 2 Firewalling (Bridged Mode)
- Randomized IP Sequencing
- Gezielte TTL Manipulation

Web Filter

- Proxy-Server (transparent)
- Caching-Proxy
- Authentifizierung: LDAP (lokal und extern), Active Directory
- Blocken von Webseiten nach dynamischer Kategorisierung (Inhaltsanalyse)
- Benutzerdefinierte und serverbasierte Blocklisten für URLs und Domänen
- Prüfung auf gefährliche Inhalte (Cookies, ActiveX, JavaScript)
- Detaillierte Protokollierung und interaktive Auswertung

E-Mail Filter

- Virenfilter: Protokolle SMTP und POP3
- Spamfilter: Protokolle SMTP und POP3
- Filterung von unerwünschten E-Mail-Anhängen
- Grafische Auswertungen
- Bild- und PDF-Spam-Erkennung
- Löschen, Kennzeichnen oder Isolieren von Spam-Mails
- Erkennung von Phishing-Mails
- SMTP-E-Mail-Verschlüsselung (TLS)
- Selbstlernender trainierbarer Filter (Bayes-Filter)
- Sender Policy Framework (SPF)
- Blacklisting (RBL) und Hashüberprüfung (Razor, DCC)
- Regelbasierte Prüfung (SpamAssassin) mit automatischen Update
- Prüfung auf RFC-Konformität
- Verzögern von Bulk-Mails (Teergrube)

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

© 2008 by eSYS Informationssysteme GmbH

- Unbeschränkte Anzahl von Tunnels und Clients
- NAT Traversal
- IPSec Verschlüsselung: AES, 3DES, Blowfish, Twofish, CAST, Serpent
- IPSec Authentifizierung: PSK und X.509 Zertifikate
- Perfect Forward Secrecy (PFS)
- Zertifikatsverwaltung

Traffic Shaping und Bandbreitenmanagement

- Eingehender und ausgehender Traffic
- Vordefinierte und benutzerdefinierte Traffic-Klassen: z.B: VOIP, Citrix, RDP..
- Minimal garantierte und maximale Bandbreite pro Klasse
- VPN-Bandbreitenmanagement (über IPSec)
- Aufteilung der Gesamtbandbreite: IP-Adressen bzw. Netze
- Grafische Auswertungen

Captive Portal

- Browser-basierte Authentifizierung für (WLAN-) Hotspots
- Automatischer Redirect auf Login-Maske
- Authentifizierung: LDAP (lokal und extern), Active Directory, externer RADIUS-Server
- Gleichzeitige Bereitstellung öffentlicher und privater Netzwerkdienste
- Protokollierung der Datenmengen und Online-Zeiten
- Flexible Berechtigungen

Anonymisierung

- Anonymisierung von ausgewähltem Netzwerkverkehr
- Ermöglicht anonymes Surfen im Internet
- JAP Anonymisierungs-Proxy
- TOR Anonymity Network
- Freenet HTTP - Portal

Zusatzdienste

- Dynamisches DNS
- DHCP Server
- Secure DNS Resolver
- SSL Wrapper für beliebige TCP Dienste
- Transparentes FTP-Virenscanning

2 Grundlagen

2.1 Firewall

Um eine Firewall wie Gibraltar konfigurieren zu können ist es sehr wichtig, deren Wirkungsweise und Techniken zu verstehen. Es gilt der Grundsatz: **"Nur eine richtig konfigurierte Firewall erhöht die Sicherheit"**. Aus diesem Grund wollen wir an dieser Stelle die wichtigsten Grundlagen erklären und einige wesentliche Begriffe in diesem Zusammenhang erläutern. Eine ausführliche Erklärung aller verwendeten Techniken würde jedoch den Rahmen dieses Benutzerhandbuchs sprengen. Empfehlenswerte Literatur zum

© 2008 by eSYS Informationssysteme GmbH

Thema Firewalls finden sie im Anhang.

Eine Firewall ist eine Netzwerk-Sicherheitskomponente, die Netzwerkverkehr anhand eines definierten Firewall-Regelwerks (Policy) erlaubt oder verbietet. Das Ziel einer Firewall ist es, den Datenverkehr zwischen Netzwerksegmenten mit verschiedenen Vertrauensstufen abzusichern. Ein typischer Einsatzzweck ist es, den Übergang zwischen einem lokalen Netzwerk (LAN) und dem Internet zu kontrollieren.

Firewall-Typen

Üblicherweise wird zwischen Netzwerkfirewalls und Personal-Firewalls unterschieden. Bei Netzwerkfirewalls handelt es sich um ein dediziertes Gerät, welches mindestens zwei Netzwerke oder Netzwerksegmente voneinander trennt. Die Firewall wird in diesem Zusammenhang dazu verwendet, den Datenverkehr zwischen den angeschlossenen Netzwerksegmenten zu regeln. Zur Trennung der einzelnen Netzwerksegmente verfügt eine Netzwerk-Firewall in der Regel über mehrere unabhängige Netzwerk-Schnittstellen.
Eine Personal-Firewall ist hingegen eine Software, welche auf dem zu schützenden Computer direkt installiert wird und nur einen einzelnen Computer schützt.

Gibraltar ist eine Netzwerkfirewall und kann wahlweise auf eigener Hardware oder auf Gibraltar Security Appliances betrieben werden.

Eine Firewall kann mit verschiedenen Methoden unerwünschten Netzwerkverkehr von erwünschtem Netzwerkverkehr unterscheiden. Die wichtigste Komponente einer Firewall ist in diesem Zusammenhang der Paketfilter.

Paketfilter

Ein Paketfilter ist eine Software, die den ein- und ausgehenden Datenverkehr nach definierten Kriterien analysiert und filtert. Als Filterkriterien können verschiedene Informationen in den einzelnen Datenpaketen verwendet werden. Gängige Filterkriterien sind:

- Netzwerk-Protokoll
- Quell- und Zieladresse
- Quell- und Zielport

Durch Definition entsprechender Regeln (Firewall-Regeln, Policy) wird festgelegt, was mit den jeweiligen Datenpaketen passieren soll. Grundsätzlich besteht die Möglichkeit, Pakete an ein anderes Netzwerk weiterzuleiten (**ACCEPT**), Pakete zu ignorieren (**DENY**), mit einer Bemerkung zurückzuschicken (**REJECT**) oder auch zu protokollieren (**LOG**). Der Paketfilter ist somit der Kern jeder Firewall und entsprechend wichtig ist eine lückenlose Konfiguration der Firewall-Regeln.

Gibraltar arbeitet nach dem Prinzip **"Was nicht erlaubt wird ist verboten"**. Das bedeutet, standardmäßig verbietet Gibraltar jeden Netzwerkverkehr bis auf wenige Ausnahmen, welche für die Wartung der Firewall notwendig sind. Erst der Administrator definiert in der Folge, welcher Netzwerkverkehr erlaubt sein soll.

Stateful Packet Inspection

Stateful Inspection ist eine erweiterte Form der Paketfilterung. Die Schwäche eines einfachen

© 2008 by eSYS Informationssysteme GmbH

Paketfilters ist es, dass jedes Paket einzeln betrachtet wird und nur anhand der Informationen in diesem EINEN Datenpaket entschieden wird, ob es gültig ist oder nicht. Die zustandsgesteuerte Filterung merkt sich dagegen den Status einer Verbindung und kann ein neues Datenpaket einem zusammenhängenden logischen Datenstrom zuordnen. Diese Information kann als weiteres Filterkriterium herangezogen werden. Dadurch ist es etwa möglich, Antwortpakete auf eine gewünschte Verbindung (z.B. Abruf eines Webservers) automatisch ebenfalls als gewünscht zu akzeptieren.

2.2 Addressübersetzung (NAT)

Network Address Translation (NAT) ist ein Sammelbegriff für Verfahren, um automatisiert und transparent Adressinformation in Datenpaketen durch andere zu ersetzen. NAT ist eine der Kernfunktionen von Routern und Firewalls. NAT ist ein wichtiges Hilfsmittel, um die Struktur des eigenen Netzwerks zu verbergen, und ein internes Netzwerk nach außen hin über eine einzelne öffentliche IP-Adresse auftreten zu lassen. Dies ist sowohl ein Sicherheitsvorteil wie auch meistens eine Notwendigkeit, da aufgrund der Adressknappheit bei IPv4-Adressen kaum ein Unternehmen für jeden Internet-PC über eine separate öffentliche IP-Adresse verfügt.

Man unterscheidet folgende Arten von NAT:

- **Source NAT (SNAT):** Ausgehender Netzwerkverkehr wird mit einer festgelegten (öffentlichen) IP-Adresse maskiert.
- **Destination NAT (DNAT):** Eingehender Netzwerkverkehr wird an eine alternative Netzwerkadresse weitergeleitet. Diese Funktion kann z.B. dazu verwendet werden, am Router eingehende Anfragen an einen Webserver an den entsprechenden internen Webserver weiterzuleiten.

Als Sonderfälle können auch noch folgende Arten von NAT betrachtet werden:

- **Masquerading:** Ausgehender Netzwerkverkehr wird mit einer dynamisch zugewiesenen IP-Adresse maskiert.
- **Redirection:** Eingehender Netzwerkverkehr wird an einen anderen Port auf dem Router weitergeleitet. Die Zieladresse wird in diesem Fall nicht verändert.

2.3 Proxy-Dienste

Ein Proxy oder Proxy-Server ist ein Dienstprogramm für Computernetzwerke, das im Datenverkehr vermittelt und als Stellvertreter agiert. Es macht den Datenverkehr effizienter bzw. schneller, kann aber auch durch den Einsatz von Zugriffskontrollmechanismen die Sicherheit erhöhen.

Im einfachsten Fall leiten Proxy Server Daten weiter. Hier ist von der Existenz eines Proxy Server nichts zu spüren. In der Regel meint man mit einem Proxy einen http-Proxy, der zwischen Webbrowser (Client) und Webserver vermittelt. Hier hat der Proxy mehrere Hauptfunktionen:

- **Zwischenspeicher (Cache):** Der Proxy kann gestellt Anfragen bzw. deren Ergebnis

© 2008 by eSYS Informationssysteme GmbH

speichern. Wird die Anfrage erneut gestellt, kann diese aus dem Speicher beantwortet werden, ohne zuerst den Webserver zu fragen. Dadurch können Webanfragen schneller beantwortet werden und die Netzlast wird verringert.

- **Filter:** Ein Proxy ermöglicht die eingehende Prüfung und Filterung der über ihn laufenden Inhalte. Das ist möglich, weil der Proxy die Daten die er transportiert auch "versteht". Er arbeitet auf der sogenannten Anwendungsebene. Ein Proxy ist notwendig, um Inhalte auf Viren oder gefährliche Inhalte zu überprüfen. Eine eingehende Analyse des Datenstroms ist nur mit Verwendung eines Proxy möglich.
- **Zugriffssteuerung:** Ein Proxy kann dazu verwendet werden, nur einer eingeschränkten Gruppe von Benutzern Zugriff auf ausgewählte Webseiten oder das gesamte Internet zu erlauben.

Proxy Server existieren für beinahe alle Internet-Dienste. In Gibraltar sind folgende Proxy Server integriert:

- **HTTP Proxy:** Überprüft den Webtraffic hinsichtlich Viren und gefährlichen oder unerwünschtem Inhalt (Content-Filter, Content-Scanner und Webfilter)
- **SMTP Proxy:** Überprüft den E-Mail-Verkehr zwischen Mailservern. Ermöglicht die Überprüfung von E-Mails auf Spam und Viren.
- **POP3 Proxy:** Überprüft jene E-Mails, die von externen POP3 Mailservern abgerufen werden. Ermöglicht die Überprüfung von E-Mails auf Spam und Viren.
- **FTP Proxy:** Überprüft FTP Traffic und ermöglicht die Überprüfung der übertragenen Daten auf Viren

Transparenter Proxy

Von einem transparenten Proxy spricht man, wenn am Client der Proxy nicht explizit eingestellt werden muss und der Proxy Server verpflichtend verwendet werden muss. Dazu werden alle eingehenden Anfragen auf den jeweiligen Port (z.B. http, Port 80) automatisch mittels **REDIRECT** auf den entsprechenden Proxy Server umgeleitet. Der Benutzer hat keine Möglichkeit, den Proxy Server zu umgehen. Sämtliche in Gibraltar verwendeten Proxy Server können transparent betrieben werden.

2.4 Virtuelle Private Netzwerke (VPN)

Ein VPN (Virtuelles privates Netzwerk) ist ein Computernetz, das zum Transport privater Daten ein öffentliches Netz nutzt. Es ermöglicht somit eine sichere Übertragung über ein unsicheres Netzwerk. Teilnehmer eines VPN können Daten wie in einem internen LAN austauschen. Einzelne Teilnehmer selbst müssen hierzu nicht direkt verbunden sein. Die Verbindung über das öffentliche Netz wird üblicherweise verschlüsselt.
Eine Verbindung der Netze wird über einen Tunnel zwischen einem VPN-Client und einem VPN-Server ermöglicht.

Insgesamt unterscheidet man 4 Arten von VPNs, wobei 2 davon in Gibraltar verwendet werden:

- **Site-to-Site:** Verbindung von zwei Netzwerken durch einen VPN-Gateway auf jeder Seite. Diese bauen dann untereinander eine VPN-Verbindung auf, die meist permanent bestehen bleibt. Andere Rechner im Netzwerk können nun den VPN-Gateway verwenden, um Daten in das andere Netz zu senden. So lassen sich z.B. zwei entfernte Standorte einer Firma verbinden. Gibraltar verwendet für die Herstellung von Site-to-Site VPNs das IPSec Protokoll.

© 2008 by eSYS Informationssysteme GmbH

- **Site-to-End:** VPNs werden auch oft verwendet, um Mitarbeitern außerhalb einer Organisation oder eines Unternehmens Zugriff auf das interne Netz zu geben. Dabei baut der Computer des Mitarbeiters eine VPN-Verbindung zu einem ihm bekannten VPN-Gateway des Unternehmens auf. Über diese Verbindung ist es dem Mitarbeiter nun möglich, so zu arbeiten, als ob er im lokalen Netzwerk der Firma eingebunden wäre (Remote Access VPN). Gibraltar bietet mehrere Möglichkeiten um Remote Access VPN zu nutzen.

Durch die Verwendung von Passwörtern, öffentlichen Schlüsseln oder durch ein digitales Zertifikat kann die Authentifizierung der VPN-Endpunkte gewährleistet werden. Aus Sicherheitsgründen ist es notwendig, den VPN-Verkehr zusätzlich auch durch den Paketfilter (Firewall) zu beschränken. Ansonsten würde es sehr leicht möglich sein, Würmer oder Trojaner in das Netzwerk einzuschleusen.

3 Hardware

Sollten sie einen Gibraltar Security Gateway erworben haben finden Sie Gibraltar bereits vorinstalliert auf Ihrem jeweiligen Gerät (Appliance).

Zusätzlich zur Hardware-Variante steht Gibraltar jedoch nach wie vor als reine Software-Version zur Verfügung. Dabei handelt es sich um ein Live-CD-System. Das bedeutet, die Software (Gibraltar) bootet direkt von CD und läuft auch von CD. Eine Festplatteninstallation ist nicht notwendig. Als Mindestanforderung benötigen sie demnach einen PC mit bootbarem CD-ROM Laufwerk und mindestens 2 Linux-kompatiblen Netzwerkkarten.

Für einen reibungslosen Betrieb von Gibraltar mit Webinterface empfehlen wir:

- PC Pentium (>600 MHz)
- >=256 MB RAM
- bootable CD-ROM 32x oder besser
- HDD für größere Log-Files, Proxys und E-Mail-Relay (SMTP-Proxy)
- USB-Speichermedium
- 2 x 100 MBit/s Netzwerkkarte mit 3COM, Intel oder Realtek Chipsatz

Kompatibilität:

- Netzwerkkarte: alle PCI basierten 10/100 oder 1000 MBit/s
- Modem: AT-Standard
- USB-Modem: ACM-Standard (nicht getestet)
- DSL-Modem: Alcatel USB Speedtouch oder alle Ethernet Modems

4 Installation

Gibraltar ist ein vollwertiges Betriebssystem und benötigt aus diesem Grund keine Festplatteninstallation und kein darunterliegendes weiteres Betriebssystem. Die Konfiguration von Gibraltar erfolgt mittels einem einfach zu bedienenden Webinterface. Je nachdem, welche Gibraltar-Variante sie verwenden, müssen sie folgende Schritte durchführen:

© 2008 by eSYS Informationssysteme GmbH

Gibraltar Software

Die Software-Variante von Gibraltar bootet und läuft direkt von CD-ROM. Sie benötigen also für Gibraltar einen eigenen PC, der in weiterer Folge als Firewall verwendet wird. Um die Gibraltar Software herunterzuladen und zu installieren gehen Sie wie folgt vor:

1. **Download der Gibraltar Software:** Sollten sie noch keine Gibraltar CD zur Verfügung haben, laden sie eine aktuelle Version der Gibraltar Software (ISO Image) von unserer Homepage www.gibraltar.at herunter. Gibraltar wird in Form eines komprimierten ISO Images zum Download bereitgestellt.
2. **Entpacken:** Nachdem Sie Gibraltar heruntergeladen haben, entpacken Sie die Datei mit einer gängigen Komprimierungssoftware (z.B. WinZip oder WinRAR). Das Gibraltar ISO Image wurde mit bzip2, einem frei verfügbaren Komprimierungsprogramm komprimiert.
3. **Brennen einer Gibraltar CD:** Brennen Sie das entpackte ISO Image auf CD und erstellen Sie so eine bootfähige Gibraltar CD.
4. **Starten von Gibraltar:** Starten Sie Ihren PC und booten Sie Gibraltar von CD

ACHTUNG: Sollte Gibraltar nicht von CD starten, so ist Ihr Computer entweder nicht in der Lage, von CD zu starten oder sie müssen die Bootreihenfolge im BIOS korrigieren. Stellen Sie im BIOS sicher, dass Ihr Computer zuerst von CD und erst anschließend von anderen Medien bootet.

Die restlichen Schritte sind ident mit der Installation eines Gibraltar Security Gateways.

Gibraltar Security Gateway

Bei allen Gibraltar Security Gateways ist Gibraltar bereits auf dem Gerät vorinstalliert und kann sofort in Betrieb genommen werden. Dazu gehen sie wie folgt vor:

1. **Starten des Gibraltar Security Gateway:** Schließen Sie den Gibraltar Security Gateway mit dem beiliegenden Kabel an Ihre Stromversorgung an.
2. **Netzwerkverbindung herstellen:** Verbinden Sie eine der Netzwerkschnittstellen mit Ihrem Netzwerkverteiler (Switch oder Hub).

ACHTUNG: Beim Startvorgang wird jeder Netzwerkschnittstelle des Gibraltar Security Gateways automatisch eine IP-Adresse zugeordnet. Welche Schnittstelle welche Adresse bekommt ist vom Typ abhängig. Entnehmen sie die genaue Zuordnung der IP-Adressen der Ihrem Gibraltar Security Gateway beiliegenden Kurzanleitung. Die Netzwerkschnittstellen erhalten die Adressen in folgender Reihenfolge: 10.0.0.1, 10.0.1.1, 10.0.2.1, etc.

3. **IP-Adresse auf Administrations-PC einstellen:** Sie können Gibraltar mit jedem beliebigen PC konfigurieren. Achten Sie jedoch darauf, dass Ihr Administrations-PC sich im selben IP-Adressbereich wie Gibraltar befindet. Falls Sie auf das Netzwerk-Interface mit der Adresse 10.0.0.1 zugreifen wollen, konfigurieren sie Ihren Administrations-PC mit der IP-Adresse 10.0.0.2 und der Subnet-Maske 255.255.255.0.
4. **Zugriff auf das Webinterface (GibADMIN):** Geben Sie in Ihrem Webbrowser die IP-Adresse von Gibraltar in folgender Form ein: **https://10.0.x.x** (z.b: https://10.0.0.1)

© 2008 by eSYS Informationssysteme GmbH

ACHTUNG: Der Zugriff auf das Webinterface von Gibraltar erfolgt aus Sicherheitsgründen mittels SSL (Secure Socket Layer, Port 443). Es ist daher notwendig, im Browser **https** anstatt http einzugeben. Der Port, an dem das Webinterface antwortet kann vom Administrator bei Bedarf geändert werden.

5. **Anmeldung am Webinterface:** Melden sie sich mit dem Benutzernamen **root** an der Gibraltar Firewall an. **Ein Passwort ist bei der ersten Anmeldung nicht erforderlich**. **Vergessen Sie jedoch nicht, nach der ersten Anmeldung ein sicheres Passwort zu setzen**.
6. **Upload der Lizenzdatei:** Damit Sie Gibraltar konfigurieren können, ist es notwendig eine gültige **Lizenzdatei** im Webinterface hochzuladen. Dieser Schritt ist nur notwendig, wenn werkseitig noch keine Lizenz eingespielt wurde. Standardmäßig sind alle Gibraltar Security Gateways jedoch bereits mit einer Lizenzdatei ausgestattet. Zum Testen von Gibraltar können sie jederzeit online eine für 30 Tage gültige **Testlizenz** über unsere Homepage www.gibraltar.at anfordern. Privatbenutzer erhalten auf Anfrage eine kostenlose Lizenzdatei per E-Mail. Die Privatlizenz ist auf maximal 5 Netzwerkgeräte beschränkt.
7. **Beginnen Sie mit der Konfiguration**

ACHTUNG: Vergeben Sie ein **sicheres Passwort mit mindestens 12 Zeichen**. Ein sicheres Passwort sollte neben alphanumerischen Zeichen auch numerische Zeichen und Sonderzeichen enthalten (z.B. D1eSPw@). Das Firewall-Passwort ist der Schlüssel zu Ihrem Netzwerk. Standardmäßig ist der Fernzugriff auf die Firewall über jedes Interface erlaubt. Diese Einstellung kann natürlich jederzeit geändert werden.

5 Lizenzierung

Gibraltar überzeugt durch ein einmaliges Preis-/Leistungsverhältnis. Durch die weitgehende Verwendung von Open Source Komponenten und die tatkräftige Unterstützung der Debian Community sind wir in der Lage, Gibraltar als professionelles Security Produkt zu einem außerordentlich günstigen Preis anbieten zu können.

Sie können Gibraltar sowohl im Online-Shop auf unserer Webseite als auch direkt bei unseren Gibraltar Partnern und Resellern erwerben. Eine vollständige und aktuelle Preisliste mit den Listenpreisen von Gibraltar erhalten Sie vom Hersteller oder von einem autorisierten Gibraltar Reseller oder Partner.

Für den Betrieb von Gibraltar ist eine gültige Aktivierungslizenz notwendig. Gibraltar funktioniert nicht fehlerfrei ohne Lizenzdatei. Ohne Lizenzdatei werden von Gibraltar keine Pakete geroutet und der Zugriff auf das webbasierte Konfigurationstool ist nicht möglich.

Weil Gibraltar zu einem großen Teil Open Source Komponenten verwendet, ist die Aktivierungslizenz für private User, die die urheberrechtlich geschützten Tools nutzen möchten, kostenlos.

Was benötigt man, damit man Gibraltar verwenden kann?

Gibraltar ist Betriebssystem und Anwendung zugleich. Das bedeutet, für den Betrieb von

© 2008 by eSYS Informationssysteme GmbH

Gibraltar benötigen Sie mindestens folgende Komponenten:

- **Gibraltar Software:** steht kostenlos als ISO-Image zum Download zur Verfügung
- **Gibraltar Lizenzdatei:** muss erworben werden. Für Privatuser kostenlos
- kompatible Hardware: am besten eine Gibraltar Security Appliance
- **Optional:** Lizenz für den Virenscanner powered by Kaspersky Labs
- **Optional:** Lizenz für den Contentfilter powered by Puresight ™ *

Wo erhalte ich eine Gibraltar Lizenz?

- **Privatlizenz:** Formloses E-Mail mit Ihrem Namen an office@gibraltar.at. Die Privatlizenz gilt für maximal 5 Netzwerkgeräte und wird Ihnen innerhalb weniger Tage per E-Mail zugeschickt.
- **Testlizenz:** Eine für 30 Tage gültige Testlizenz kann online auf der Gibraltar Webseite angefordert werden. Sie erhalten eine Testlizenz sofort (innerhalb weniger Minuten) per E-Mail zugeschickt.
- **Reguläre Lizenz:** Eine reguläre Lizenz kann online auf der Gibraltar Webseite (Online Shop), per E-Mail beim Hersteller oder bei einem autorisierten Gibraltar Partner oder Reseller erworben werden.
- **Ermäßigte Lizenzen für Schulen und Universitäten bzw. Non-Profit Organisationen:** Kontaktieren Sie bitte office@gibraltar.at

Gibraltar Security Gateway:

Unsere Gibraltar Security Gateways werden bereits mit Gibraltar vorinstalliert und mit einer gültigen Lizenz geliefert. Sie brauchen eine Gibraltar Security Appliance nur mehr anstecken und können sofort mit der Konfiguration beginnen.

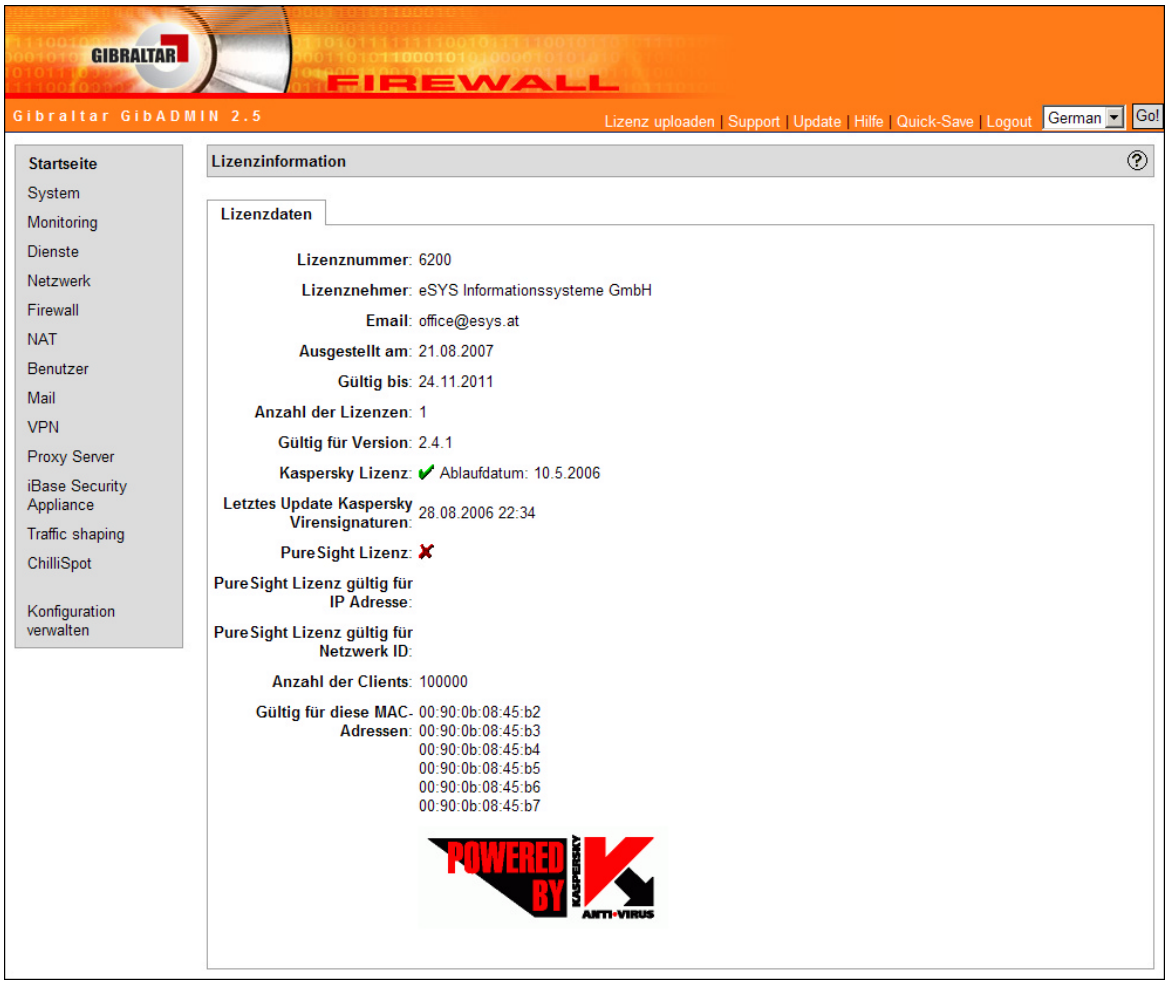
*** Trademark of PureSight Technologies Ltd.**

6 Das Webinterface

Gibraltar wird alternativ mit einem webbasierten Konfigurationstool (**GibADMIN**) oder mittels Konsole (SSH) konfiguriert. Wir empfehlen generell die Benützung der intuitiven Weboberfläche.

GibADMIN kann mit jedem beliebigen Internet-Browser gestartet werden. Geben sie dazu in der Adresszeile die IP-Adresse Ihrer Firewall ein (siehe Installation).

© 2008 by eSYS Informationssysteme GmbH



ACHTUNG: Bis der Web-Server des GibADMIN nach dem Starten voll funktionstüchtig ist, kann es einige Sekunden dauern.

Der **GibADMIN** gliedert sich in folgende Hauptbereiche:

- **Titelleiste:** In der Titelleiste finden Sie die genaue Versionsnummer Ihrer Gibraltar-Version, wichtige allgemeine Befehle und die Sprachauswahl
- **Hauptmenü:** Im Hauptmenü sind die Module von Gibraltar aufgelistet.
- **Arbeitsbereich:** Im Arbeitsbereich werden die Konfigurationsformulare angezeigt.

Die Titelleiste:

- **Lizenz uploaden:** Upload der Lizenzdateien. Es ist sowohl für den Betrieb von Gibraltar wie auch für zusätzliche Komponenten (Virenscanner, Content-Scanner) eine gültige Lizenzdatei notwendig.
- **Support:** Online-Supportformular. Ermöglicht das Senden von Anfragen direkt an unseren technischen Support. Beachten Sie bitte, dass die Firewall bereits über eine Internet-Verbindung verfügen muss um erfolgreich Support-Anfragen verschicken zu können. Alternativ dazu erreichen Sie unseren technischen Support unter der E-Mail-Adresse support@gibraltar.at.
- **Update:** Update Ihrer Gibraltar Version auf die jeweils aktuellste Version oder manueller Download von Security-Updates und Software-Patches.
- **Hilfe:** Online Hilfe (html-Version des vorliegenden Benutzerhandbuchs)
- **Quick-Save:** Die aktuelle Konfiguration wird auf das festgelegte Standard-Speicherziel gespeichert. Dieses Standard-Speicherziel muss vorher unter

© 2008 by eSYS Informationssysteme GmbH

Konfiguration verwalten festgelegt werden.
- **Logout:** Beendet die aktuelle Gibraltar Sitzung und meldet den aktuellen Benutzer von GibADMIN ab.
- **Sprachauswahl:** Wechselt die Sprache von GibADMIN.

Zu Beginn jeder **GibADMIN** Sitzung wird der Anmeldebildschirm angezeigt. Sie werden aufgefordert, Ihren Benutzernamen und das entsprechende Passwort einzugeben. Bei der ersten Anmeldung verwenden Sie dazu den Benutzer "**root**" und lassen das Passwort frei. Sie müssen nur die Schaltfläche **Login** betätigen, um sich bei Gibraltar anzumelden. Als ersten Schritt sollten Sie natürlich für den Benutzer "**root**" ein Passwort festlegen. Die Schaltfläche **Passwort ändern** befindet sich im Menü **System**.

xPICTURE login.apgz

HINWEIS: In der Titelleiste des Browserfensters wird der Hostname der aktuell konfigurierten Firewall angezeigt, damit Sie die einzelnen Browserfenster unterscheiden können, wenn Sie gleichzeitig mehrere Gibraltars bearbeiten.

7 Anwendungsbeispiele

Nachfolgend werden exemplarisch verschiedene Anwendungsbeispiele beschrieben, in denen Gibraltar zum Einsatz kommen könnte. Es handelt sich dabei um Mindestkonfigurationen, die dem Netzwerkadministrator dabei helfen sollen, die Funktionsweise von Gibraltar zu verstehen. Bei den vorliegenden Anleitungen handelt es sich um Klick-Anleitungen, welche ohne Vorkenntnisse von Gibraltar durchgeführt werden können.

Szenario 1: ADSL-PPTP Wählverbindung und DHCP

Konfiguration von Gibraltar als Internet-Gateway mit Einwahl über ADSL-PPTP. Die öffentliche IP-Adresse wird dynamisch bezogen. Gibraltar wird als DHCP-Server für das lokale Netzwerk konfiguriert. Alle Clients im lokalen Netzwerk erhalten uneingeschränkten Zugriff auf das Internet. Der Zugriff vom Internet auf das lokale Netzwerk wird verboten.

Szenario 2: Internet-Gateway mit öffentlicher IP-Adresse

Konfiguration von Gibraltar als Internet-Gateway mit fixer öffentlicher IP-Adresse. Alle Clients im lokalen Netzwerk erhalten uneingeschränkten Zugriff auf das Internet. Der Zugriff vom Internet auf das lokale Netzwerk wird verboten. **Dieses Szenario kann als Grundlage für die meisten Breitband-Verbindungen verwendet werden.**

Szenario 3: Internet-Gateway und Einrichtung einer DMZ

Konfiguration von Gibraltar als Internet-Gateway und Definition einer DMZ (Demilitarisierte Zone). In der DMZ befinden sich ein WWW und ein Mailserver.

Szenario 4: Konfiguration eines VPN-Tunnels zwischen zwei Gibraltars

Konfiguration eines IPSec-VPN-Tunnels zu einer anderen Gibraltar. Es werden zwei Standorte über das Internet mit einem VPN-Tunnel verbunden. Weiters wird es Aussendienstmitarbeitern ermöglicht, sich über PPTP gesichert ins interne Firmennetzwerk einzuwählen. Die Benutzerverwaltung erfolgt über den lokalen Gibraltar LDAP Server.

© 2008 by eSYS Informationssysteme GmbH

Szenario 5: Verwendung Microsoft Active Directory und Konfiguration OpenVPN für Fernzugriff

Konfiguration von Gibraltar in Verbindung mit Microsoft Active Directory. Gewisse Active Directory Benutzer sollen nachfolgende Dienste mit Ihren gewohnten Benutzernamen und Passwörtern nutzen können. Der Zugriff auf diese Dienste kann mit Active Directory Sicherheitsgruppen gesteuert werden. Konfiguration von OpenVPN für den Fernzugriff.

Szenario 6: Konfiguration von Gibraltar als Application Level Proxy für http, ftp und pop3

In diesem Szenario wird Gibraltar auf einem Rechner konfiguriert, der mit zwei Netzwerkkarten ausgestattet ist, wobei eine der Internetverbindung und die andere der Verbindung ins interne Netz dient. Gibraltar soll das interne Netz schützen und den Benutzern im lokalen Netzwerk alle Dienste im Internet zur Verfügung stellen. Von außen darf kein Zugriff auf das interne Netz möglich sein. Zusätzlich sollen noch Proxy-Server eingerichtet werden. Ein HTTP-Proxy, der die vom internen Netz angeforderten Seiten auf der Festplatte der Firewall zwischenspeichert und somit eine erneute Anforderung beschleunigt. Ein FTP-Proxy, der entweder Anfragen aus dem internen Netz übernimmt und somit die Topologie verschleiert, oder aber von aussen Anfragen entgegennimmt und an einen internen FTP-Server weiterleitet. Weiters wird ein POP3-Proxy konfiguriert, der die Abfragen von Clients im internen Netz übernimmt und beim Abholen vom externen Postfach die Mails auf Viren und Spam überprüft.

Szenario 7: Konfiguration von Gibraltar als Traffic Shaper für Citrix und VoIP transparent

Konfiguration von Gibraltar als transparenten Traffic Shaper auf einem Rechner mit 2 Netzwerkkarten mit Hilfe einer Netzwerkbrücke, um einen transparenten Modus zu ermöglichen. Ziel dieses Szenarios ist es in einer Citrix-Terminalserverumgebung dem unternehmenskritische Protokoll ICA sowie dem VOIP-Traffic mindestens je 35% der verfügbaren Bandbreite zur Verfügung zu stellen.

Szenario 8: Konfiguration von Gibraltar als Traffic Shaper für Citrix und VoIP mit VPN

Konfiguration von 3 Gibraltars die mittels IPSEC-VPN miteinander vernetzt werden.Weiters ist es Ziel dieses Szenarios ist es in einer Citrix-Terminalserverumgebung dem unternehmenskritische Protokoll ICA sowie dem VOIP-Traffic mindestens je 35% der verfügbaren Bandbreite zur Verfügung zu stellen.

Szenario 9: Konfiguration von Gibraltar als Bandbreitenmanager für Voice over IP

Konfiguration von Gibraltar zur Sicherstellung einer minimalen Bandbreite für eine interne VOIP-Telefonanlage mit der IP 192.168.0.40. Ziel dieses Szenarios ist es, der internen Telefonanlage eine Minimalbandbreite von 1 Mbit Download und 512 kb Upload zur

© 2008 by eSYS Informationssysteme GmbH

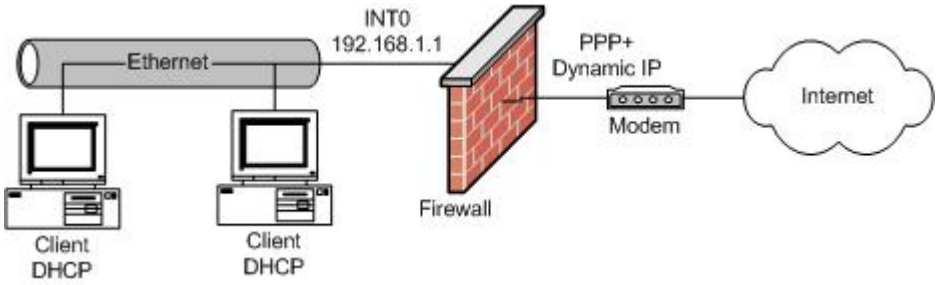
Verfügung zu stellen.

Szenario 10: Konfiguration von Gibraltar als Bandbreitenmanager für Web Traffic

Konfiguration von Gibraltar zur Sicherstellung einer minimalen Bandbreite für Web Traffic (HTTP, HTTPS). Weiters soll auch für das Abrufen von Emails über POP3 eine minimale Bandbreite zur Verfügung gestellt werden.

7.1 ADSL

Konfiguration von Gibraltar als Internet-Gateway mit Einwahl über ADSL-PPTP. Die öffentliche IP-Adresse wird dynamisch bezogen. Gibraltar wird als DHCP-Server für das lokale Netzwerk konfiguriert. Alle Clients im lokalen Netzwerk erhalten uneingeschränkten Zugriff auf das Internet. Der Zugriff vom Internet auf das lokale Netzwerk wird verboten.



Systemvoraussetzungen

PC mit zwei kompatiblen Netzwerkkarten oder Gibraltar Security Gateway und ein ADSL PPTP Modem.

HINWEIS: Alle angegebenen Werte sind nur Beispiele. Sie müssen diese Werte an Ihre individuellen Gegebenheiten anpassen.

Installation von Gibraltar

Installieren sie Gibraltar wie im Kapitel Installation beschrieben.

Systemeinstellungen

Es werden zuerst allgemeine Systemeinstellungen vorgenommen.

1. Wählen Sie im Hauptmenü den Punkt **System**.
2. Wählen Sie die Registerkarte **Allgemeine Einstellungen**.
3. **Name des Systems**: Geben Sie in dieses Textfeld den gewünschten Systemnamen (z.B. "gibraltar") ein.
4. **Domäne**: Geben Sie hier die Domäne ein, in die Gibraltar integriert werden soll (z.B. "gibraltar.at").
5. **Zeitzone**: Wählen Sie die Zeitzone, in der Sie Gibraltar betreiben wollen.
6. **Administrator E-Mail**: Geben Sie die Administrator E-Mail Adresse ein, an die Systemmeldungen gesendet werden sollen.
7. **Speichern**: Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

© 2008 by eSYS Informationssysteme GmbH

Netzwerkeinstellungen - Netzwerkkarte

Die IP-Adressen der Netzwerkschnittstellen von Gibraltar werden definiert. Sowohl die externe wie auch die interne Netzwerkschnittstelle sollen statische IP-Adressen erhalten.

1. Wählen Sie im Hauptmenü den Punkt **Netzwerk**.
2. Wählen Sie die Registerkarte **eth0**.
3. **Interface:** Geben Sie in dieses Textfeld die gewünschte Bezeichnung für diese Netzwerkkarte ein (z.B.: "int0", damit Sie die Netzwerkkarte für das interne Netzwerk eindeutig identifizieren können).
4. **Automatisch starten:** Markieren Sie dieses Kontrollkästchen, damit die Netzwerkkarte beim Systemstart automatisch gestartet wird.
5. **IP-Adresse:** Wählen Sie die Option **statisch**, da die IP-Adresse für diese Netzwerkkarte statisch vergeben werden soll.
6. **Statische IPs:** Ändern Sie die IP-Adresse im Textfeld **IP-Adresse/Netzwerkmaske** auf die von Ihnen für Gibraltar vorgesehene IP-Adresse (CIDR-Notation: z.B. 192.168.0.1/24).
7. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.
8. Wählen Sie die Registerkarte **eth1**.
9. **Interface:** Geben Sie in dieses Textfeld die gewünschte Bezeichnung für diese Netzwerkkarte ein (z.B.: "ext0", damit Sie die Netzwerkkarte für den externen Netzwerkbereich eindeutig identifizieren können).
10. **Automatisch starten:** Markieren Sie dieses Kontrollkästchen, damit die Netzwerkkarte beim Systemstart automatisch gestartet wird.
11. **IP-Adresse:** Wählen Sie die Option **statisch**, da die IP-Adresse für diese Netzwerkkarte statisch vergeben werden soll.
12. **Statische IPs:** Ändern Sie die IP-Adresse im Textfeld **IP-Adresse/Netzwerkmaske** auf die von Ihnen für Gibraltar vorgesehene IP-Adresse (CIDR-Notation: z.B. 10.0.0.140/24).
13. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

ACHTUNG: Durch das Verändern der IP-Adresse auf der Netzwerkkarte, über die Sie auf Gibraltar zugreifen, wird die Verbindung unterbrochen und Sie müssen für Ihren Arbeitsplatzrechner ebenfalls die IP-Adresse anpassen.

Verbinden Sie nun Ihr ADSL Modem mit dem Interface "ext0" von Gibraltar.

Netzwerkeinstellungen - Routing

Auf dieser Registerkarte sind für diese Konfiguration keine Einstellungen notwendig, da die Standardroute bei der Konfiguration des ADSL-Modems festgelegt wird.

Dial-In PPTP

Die ADSL-Verbindung wird definiert. Dabei wird ein PPTP Tunnel von Gibraltar zum ADSL-Modem aufgebaut. Sie benötigen dazu die Zugangsdaten Ihres Providers.

1. Wählen Sie im Hauptmenü den Punkt **Netzwerk**.
2. Wählen Sie den Untermenüpunkt **Dial-in**.
3. Wählen Sie die Registerkarte **ADSL-PPTP**.
4. **Verbindung hinzufügen:** Betätigen Sie diese Schaltfläche, um eine Verbindung hinzuzufügen. Sie werden in die Detailansicht weitergeleitet.

© 2008 by eSYS Informationssysteme GmbH

5. **Name:** Geben Sie hier den von Ihnen für diese Verbindung vorgesehenen Namen ein. Dieser Name dient dazu, die konfigurierte Verbindung in der Übersichtsliste der Registerkarte **ADSL-PPTP** eindeutig zu identifizieren und muss daher unterschiedlich von bereits konfigurierten Verbindungen (auch ADSL Verbindungen) sein.
6. **IP-Adresse des Modems:** Geben Sie hier die interne IP Adresse des ADSL-Modems ein (z.B: 10.0.0.138).
7. **Benutzername:** Geben Sie hier den vom Provider für Sie eingerichteten Benutzernamen ein.
8. **Passwort** und **Passwort (Bestätigung):** Geben Sie in diese beiden Textfelder das vom Provider für Sie eingerichtete Passwort ein.
9. **Standardroute:** Aktivieren Sie dieses Kontrollkästchen, da Gibraltar diese Verbindung als Standardroute verwenden soll.
10. **Verbindung aufrechterhalten:** Aktivieren Sie dieses Kontrollkästchen, damit Ihre Internetverbindung nach einem ungewollten Abbruch wieder aufgebaut wird.
11. **Einwahlinterface umbenennen auf:** Geben Sie hier den Wert "extEinwahl" ein, um Ihr Einwahlinterface bei den Firewall und NAT-Regeln verwenden zu können.
12. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.
13. **Verbindung herstellen**  **:** Betätigen Sie diese Schaltfläche, um die Verbindung über das Modem zu Ihrem Provider herzustellen.

Firewallregeln

Es werden die Firewallregeln definiert. Die Clients im lokalen Netzwerk erhalten uneingeschränkten Zugriff auf das Internet. Da Gibraltar für die internen Clients als DNS-Server fungiert, müssen DNS-Anfragen an die Firewall explizit erlaubt werden.

1. Wählen Sie im Hauptmenü den Punkt **Firewall**.
2. Wählen Sie die Registerkarte **Firewallregeln**.
3. **Interface:** Wählen Sie aus dem Auswahlfeld **eingehend** den Wert "int0" für die Netzwerkkarte (bzw. Ihre Benennung der Netzwerkkarte). Wählen Sie aus dem Auswahlfeld **ausgehend** den Wert "extEinwahl" für das Modem. Betätigen Sie die Schaltfläche **Go!**. Es werden nun alle Filterregeln in der Elementgruppe **Filterregeln** angezeigt, die für Pakete bestimmt sind, die von der Netzwerkkarte "int0" auf das Modem "extEinwahl" geschickt werden. In diese Richtung wollen wir alle Anfragen erlauben.
4. **Regel hinzufügen:** Betätigen Sie diese Schaltfläche, um eine neue Regel in diesem Bereich ("int0 -> extEinwahl") einzufügen. Sie werden in die Detailansicht weitergeleitet.
5. **Quelladresse:** Wählen Sie aus der Auswahlliste ANY, um alle zutreffenden Quelladressen zu erlauben.
6. **Zieladresse:** Wählen Sie aus der Auswahlliste ANY, um alle Zieladressen zu erlauben.
7. **Kommentar:** Geben Sie einen (möglichst aussagekräftigen) Kommentar Ihrer Wahl ein. Alle übrigen Felder müssen in diesem Fall nicht konfiguriert werden.
8. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.
9. **Eingehend:** Wählen Sie den Wert "int0".
10. **Ausgehend:** Wählen Sie den Wert "local".
11. **Go!:** Betätigen Sie diese Schaltfläche, um die Filterregeln anzuzeigen, die Pakete betreffen, die aus dem internen Netzwerk lokal für die Firewall bestimmt sind.
12. **Quelladresse:** Wählen Sie aus der Auswahlliste ANY, um alle zutreffenden Quelladressen zu erlauben.
13. **Zieladresse:** Wählen Sie aus der Auswahlliste ANY, um alle Zieladressen zu erlauben.

© 2008 by eSYS Informationssysteme GmbH

14. **Service:** Wählen Sie den Wert "dns", um DNS Anfragen an die Firewall zuzulassen.
15. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

NAT - Regeln

Der ausgehende Netzwerkverkehr wird mit der jeweils zugewiesenen offiziellen IP-Adresse maskiert.

1. Wählen Sie im Hauptmenü den Punkt **NAT**.
2. Wählen Sie auf der Registerkarte **NAT Regeln** aus der Auswahlliste den Track "outgoing extEinwahl", da alle Pakete, die über das ADSL-Modem "extEinwahl" die Firewall verlassen, mit der öffentlichen IP-Adresse maskiert werden müssen.
3. **Regel hinzufügen:** Betätigen Sie diese Schaltfläche, um eine neue Regel hinzuzufügen. Sie werden in die Detailansicht weitergeleitet.
4. **Quell IP-Adresse:** Geben Sie in dieses Textfeld die Netzwerkadresse 192.168.0.0/24 ein, da alle Pakete, die aus dem internen Netzwerk kommen und über das Modem die Firewall verlassen, verändert werden müssen.
5. **Aktion:** Wählen Sie aus diesem Auswahlfeld den Wert MASQUERADE, da die öffentliche IP-Adresse dynamisch zugewiesen wird und wir diese daher nicht mit einer fixen IP-Adresse maskieren können. Durch die Auswahl von MASQUERADE ist kein Eintrag in das Textfeld **--to** erlaubt.
6. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

DHCP-Server

Der DHCP-Server für das lokale Netzwerk wird konfiguriert.

1. Wählen Sie im Hauptmenü den Punkt **DHCP-Server**.
2. Wählen Sie die Registerkarte **Allgemeine Einstellungen**.
3. **Domäne:** Geben Sie in dieses Textfeld die Domäne ein, die den DHCP-Clients zugewiesen werden soll.
4. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.
5. Wählen Sie die Registerkarte **int0**.
6. **DHCP aktivieren:** Markieren Sie dieses Kontrollkästchen, um DHCP für diese Netzwerkkarte zu aktivieren.
7. **IP-Adresse:** Wählen Sie aus der Auswahlliste jene IP-Adresse aus, über die dynamische IP-Adressen vergeben werden sollen (192.168.0.1).
8. **IP Wertebereich:** Betätigen Sie die Schaltfläche **Wertebereich hinzufügen**, um einen neuen IP-Wertebereich hinzuzufügen.
9. **Von inkl. IP:** Geben Sie hier die erste IP-Adresse ein, die dynamisch vergeben werden soll (192.168.0.10).
10. **Bis inkl. IP:** Geben Sie hier die letzte IP-Adresse ein, die dynamisch vergeben werden soll (192.168.0.20). Somit werden IP-Adressen von 192.168.0.10 bis 192.168.0.20 an Clients dynamisch vergeben.
11. **DNS Server:** Betätigen Sie hier die Schaltfläche **Server hinzufügen**, um einen DNS Server hinzuzufügen.
12. **IP-Adresse:** Geben Sie hier die IP-Adresse Ihres DNS Servers ein. Da Gibraltar als DNS-Server konfiguriert ist, können Sie hier 192.168.0.1 eingeben.
13. **Router:** Betätigen Sie die Schaltfläche **Router hinzufügen**, um einen Router hinzuzufügen.
14. **IP-Adresse:** Geben Sie in der Elementgruppe Router in dieses Textfeld die

© 2008 by eSYS Informationssysteme GmbH

IP-Adresse Ihres Routers ein. Da Sie Gibraltar als Router konfiguriert haben, können Sie hier 192.168.0.1 eingeben.

15. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

Dienste

Der entsprechende Dienst für den DHCP-Server wird aktiviert.

1. Wählen Sie im Hauptmenü den Punkt **Dienste**.
2. **Verfügbare Dienste:** Markieren Sie in dieser Elementgruppe beim Eintrag **DHCP-Server** die Option **Ein**. Dadurch wird bei einem Neustart der DHCP-Server wieder automatisch gestartet.
3. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.
4. **Dienst starten** **:** Betätigen Sie diese Schaltfläche beim Eintrag **DHCP-Server**, wenn der DHCP-Server nicht gestartet ist. Dadurch wird der Dienst gestartet. Der Status verändert sich auf **(gestartet)** und die Schaltfläche zu **Dienst stoppen** .

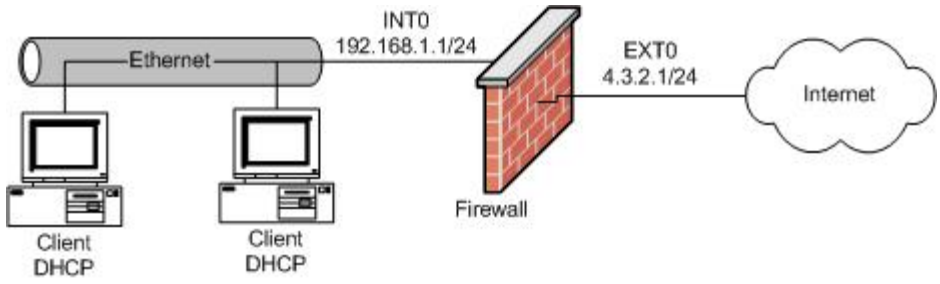
Konfiguration speichern

1. Speichern Sie die Konfiguration auf einem USB-Stick oder auf der Harddisk.

Damit sind alle notwendigen Einstellungen komplett und Ihre Clients können über Gibraltar das Internet benützen. Durch das Speichern der Konfiguration können Sie jederzeit den jetzigen Stand wiederherstellen, indem Sie die Diskette oder den USB-Stick in den Computer geben und Gibraltar neu booten.

7.2 Internet-Gateway

Konfiguration von Gibraltar als Internet-Gateway mit fixer öffentlicher IP-Adresse. Alle Clients im lokalen Netzwerk erhalten uneingeschränkten Zugriff auf das Internet. Der Zugriff vom Internet auf das lokale Netzwerk wird verboten. **Dieses Szenario kann als Grundlage für die meisten Breitband-Verbindungen verwendet werden.**



Systemvoraussetzungen

PC mit zwei kompatiblen Netzwerkkarten oder Gibraltar Security Gateway.
Breitband-Internet mit fixer öffentlicher IP-Adresse (z.B. XDSL)

HINWEIS: Alle angegebenen Werte sind nur Beispiele. Sie müssen diese Werte an Ihre individuellen Gegebenheiten anpassen.

Installation von Gibraltar

© 2008 by eSYS Informationssysteme GmbH

Installieren sie Gibraltar wie im Kapitel Installation beschrieben.

Systemeinstellungen

Systemeinstellungen wie in Szenario 1

Netzwerkeinstellungen - Netzwerkkarte

Die IP-Adressen der Netzwerkschnittstellen werden definiert. Die externe Schnittstelle erhält die vom Provider zugewiesene öffentliche IP-Adresse.

1. Wählen Sie im Hauptmenü den Punkt **Netzwerk**.
2. Wählen Sie die Registerkarte **eth0**.
3. **Interface:** Geben Sie in dieses Textfeld die gewünschte Bezeichnung für diese Netzwerkkarte ein (z.B.: "int0", damit Sie die Netzwerkkarte für das interne Netzwerk eindeutig identifizieren können).
4. **Automatisch starten:** Markieren Sie dieses Kontrollkästchen, damit die Netzwerkkarte beim Systemstart automatisch gestartet wird.
5. **IP-Adresse:** Wählen Sie die Option **statisch**, da die IP-Adresse für diese Netzwerkkarte statisch vergeben werden soll.
6. **Statische IPs:** Ändern Sie die IP-Adresse im Textfeld **IP-Adresse/Netzwerkmaske** auf die von Ihnen für Gibraltar vorgesehene IP-Adresse (CIDR-Notation: z.B. 192.168.0.1/24).
7. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.
8. Wählen Sie die Registerkarte **eth1**.
9. **Interface:** Geben Sie in dieses Textfeld die gewünschte Bezeichnung für diese Netzwerkkarte ein (z.B.: "ext0", damit Sie die Netzwerkkarte für den externen Netzwerkbereich eindeutig identifizieren können).
10. **Automatisch starten:** Markieren Sie dieses Kontrollkästchen, damit die Netzwerkkarte beim Systemstart automatisch gestartet wird.
11. **IP-Adresse:** Wählen Sie die Option **statisch**, da die IP-Adresse für diese Netzwerkkarte statisch vergeben werden soll.
12. **Statische IPs:** Ändern Sie die IP-Adresse im Textfeld **IP-Adresse/Netzwerkmaske** auf die von Ihnen für Gibraltar vorgesehene IP-Adresse (CIDR-Notation: z.B. 4.3.2.1/26).
13. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

ACHTUNG: Durch das Verändern der IP-Adresse auf der Netzwerkkarte, über die Sie auf Gibraltar zugreifen, wird die Verbindung unterbrochen und Sie müssen für Ihren Arbeitsplatzrechner ebenfalls die IP-Adresse anpassen.

Netzwerkeinstellungen - Routing

Die Standardroute wird definiert.

1. Wählen Sie im Hauptmenü den Punkt **Netzwerk**.
2. Wählen Sie die Registerkarte **Routing**.
3. **Standardroute:** Geben Sie in dieses Feld die vom Provider vorgegebene Standardroute ein.
4. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

© 2008 by eSYS Informationssysteme GmbH

Firewallregeln

Es werden die Firewallregeln definiert. Die Clients im lokalen Netzwerk erhalten uneingeschränkten Zugriff auf das Internet. Da Gibraltar für die internen Clients als DNS-Server fungiert, müssen DNS-Anfragen an die Firewall explizit erlaubt werden.

1. Wählen Sie im Hauptmenü den Punkt **Firewall**.
2. **Interface:** Wählen Sie aus dem Auswahlfeld **eingehend** den Wert "int0" für die interne Netzwerkkarte. Wählen Sie aus dem Auswahlfeld **ausgehend** den Wert "ext0" für die externe Netzwerkkarte. Betätigen Sie die Schaltfläche **Go!**. Es werden nun alle Filterregeln in der Elementgruppe **Filterregeln** angezeigt, die für Pakete bestimmt sind, die von der Netzwerkkarte "int0" auf die Netzwerkkarte "ext0" geschickt werden. In diese Richtung wollen wir alle Anfragen erlauben.
3. **Regel hinzufügen:** Betätigen Sie diese Schaltfläche, um eine neue Regel in diesem Bereich ("int0 -> ext0") einzufügen. Sie werden in die Detailansicht weitergeleitet.
4. **Quelladresse:** Wählen Sie aus der Auswahlliste ANY, um alle Quelladressen zu erlauben.
5. **Zieladresse:** Wählen Sie aus der Auswahlliste ANY, um alle Zieladressen zu erlauben.
6. **Kommentar:** Geben Sie einen (möglichst sprechenden) Kommentar Ihrer Wahl ein. Alle übrigen Felder müssen in diesem Fall nicht konfiguriert werden.
7. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.
8. **Eingehend:** Wählen Sie den Wert "int0".
9. **Ausgehend:** Wählen Sie den Wert "local".
10. **Go!:** Betätigen Sie diese Schaltfläche, um die Filterregeln anzuzeigen, die Pakete betreffen, die aus dem internen Netzwerk lokal für die Firewall bestimmt sind.
11. **Quelladresse:** Wählen Sie aus der Auswahlliste ANY, um alle zutreffenden Quelladressen zu erlauben.
12. **Zieladresse:** Wählen Sie aus der Auswahlliste ANY, um alle Zieladressen zu erlauben.
13. **Service:** Wählen Sie den Wert "dns", um DNS Anfragen an die Firewall zuzulassen.
14. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

NAT - Regeln

Mittels SNAT (Source NAT) werden alle ausgehenden Datenpakete mit der öffentlichen IP-Adresse maskiert.

1. Wählen Sie im Hauptmenü den Punkt **NAT**.
2. **Track:** Wählen Sie auf der Registerkarte **NAT Regeln** aus der Auswahlliste den Track "outgoing ext0", da alle Pakete, die über die Netzwerkkarte "ext0" die Firewall verlassen, mit der öffentlichen IP-Adresse maskiert werden müssen.
3. **Regel hinzufügen:** Betätigen Sie diese Schaltfläche, um eine neue Regel hinzuzufügen. Sie werden in die Detailansicht weitergeleitet.
4. **Quell IP-Adresse:** Geben Sie in dieses Textfeld die Netzwerkadresse 192.168.0.0/24 ein, da alle Pakete, die aus dem internen Netzwerk kommen und über die externe Netzwerkkarte die Firewall verlassen, verändert werden müssen.
5. **Aktion:** Wählen Sie aus diesem Auswahlfeld den Wert SNAT, da die Quell IP-Adresse mit Ihrer fixen, öffentlichen IP-Adresse maskiert wird.
6. **--to:** Geben Sie hier die öffentliche IP-Adresse ein, die Ihnen Ihr Provider zugewiesen hat. Damit werden alle Pakete, die vom internen Netzwerk nach außen geschickt werden, mit dieser IP-Adresse maskiert.

© 2008 by eSYS Informationssysteme GmbH

7. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

DHCP-Server

DHCP-Server Einstellungen wie in Szenario 1

Dienste

Aktivieren Sie den Dienst DHCP-Server, wie in Szenario 1 beschrieben.

Konfiguration speichern

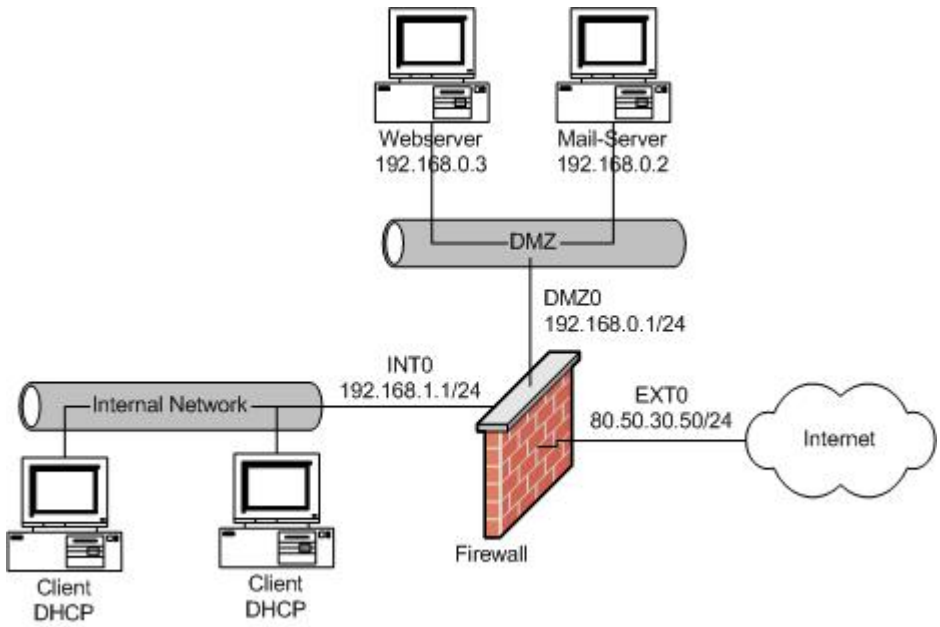
1. Speichern Sie die Konfiguration auf einem USB-Stick oder auf der Harddisk.

Damit wurden alle Einstellungen vorgenommen und Ihre Clients können über Gibraltar das Internet benützen. Durch das Speichern der Konfiguration können Sie jederzeit den jetzigen Stand wiederherstellen, indem Sie die Diskette oder den USB Stick in den Computer geben und Gibraltar neu booten.

7.3 Firewall und DMZ

Konfiguration von Gibraltar als Internet-Gateway und Definition einer DMZ (Demilitarisierte Zone). In der DMZ befinden sich ein WWW und ein Mailserver.

- **int0** für das interne Netzwerk
- **dmz0** für die DMZ
- **ext0** für das Internet



Systemvoraussetzungen

PC mit drei kompatiblen Netzwerkkarten oder Gibraltar Security Gateway.
Breitband-Internet mit fixer öffentlicher IP-Adresse (z.B. XDSL)

© 2008 by eSYS Informationssysteme GmbH

Installation von Gibraltar

Installieren sie Gibraltar wie im Kapitel Installation beschrieben.

Systemeinstellungen

Systemeinstellungen wie in Szenario 1

Netzwerkeinstellungen - Netzwerkkarten

1. Wählen Sie im Hauptmenü den Punkt **Netzwerk**.
2. Wählen Sie die Registerkarte **eth0**.
3. **Interface:** Geben Sie in dieses Textfeld die gewünschte Bezeichnung für diese Netzwerkkarte ein (z.B.: "ext0" für die Netzwerkkarte ins Internet).
4. **Automatisch starten:** Markieren Sie dieses Kontrollkästchen, damit diese Netzwerkkarte bei einem Neustart automatisch gestartet wird.
5. **IP-Adresse:** Wählen Sie die Option **statisch**, da die IP-Adresse für diese Netzwerkkarte statisch vergeben werden soll.
6. **Statische IPs:** Ändern Sie die IP-Adresse im Textfeld **IP-Adresse/Netzwerkmaske** auf die von Ihnen für Gibraltar vorgesehene IP-Adresse (CIDR-Notation: z.B. 80.50.30.50/24).
7. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.
8. Wählen Sie die Registerkarte **eth1**.
9. **Interface:** Geben Sie in dieses Textfeld die gewünschte Bezeichnung für diese Netzwerkkarte ein (z.B.: "int0" für die Netzwerkkarte ins interne Netzwerk).
10. **Automatisch starten:** Markieren Sie dieses Kontrollkästchen, damit diese Netzwerkkarte bei einem Neustart automatisch gestartet wird.
11. **P-Adresse:** Wählen Sie die Option **statisch**, da auch die IP-Adresse für diese Netzwerkkarte statisch vergeben werden soll.
12. **Statische IPs:** Ändern Sie die IP-Adresse im Textfeld **IP-Adresse/Netzwerkmaske** auf die von Ihnen für Gibraltar vorgesehene IP-Adresse (CIDR-Notation: z.B. 192.168.1.1/24).
13. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.
14. Wählen Sie die Registerkarte **eth2**.
15. **Interface:** Geben Sie in dieses Textfeld die gewünschte Bezeichnung für diese Netzwerkkarte ein (z.B.: "dmz0" für die Netzwerkkarte, die die demilitarisierte Zone (DMZ) einbinden soll).
16. **Automatisch starten:** Markieren Sie dieses Kontrollkästchen, damit diese Netzwerkkarte bei einem Neustart automatisch gestartet wird.
17. **IP-Adresse:** Wählen Sie die Option **statisch**, da die IP-Adresse für diese Netzwerkkarte statisch vergeben werden soll.
18. **Statische IPs:** Ändern Sie die IP-Adresse im Textfeld **IP-Adresse/Netzwerkmaske** auf die von Ihnen für Gibraltar vorgesehene IP-Adresse (CIDR-Notation: z.B. 192.168.0.1/24).
19. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

Das interne Netzwerk hat somit den Adressbereich 192.168.1.0/24 und die DMZ den Adressbereich 192.168.0.0/24. Dementsprechend sind auch Ihre Rechner zu konfigurieren, damit sie über die Firewall das Internet bzw. die Server in der DMZ erreichen können.

ACHTUNG: Durch das Verändern der IP-Adresse auf der Netzwerkkarte, über die Sie auf

© 2008 by eSYS Informationssysteme GmbH

Gibraltar zugreifen, wird die Verbindung unterbrochen und Sie müssen für Ihren Arbeitsplatzrechner ebenfalls die IP-Adresse anpassen.

Netzwerkeinstellungen - Routing

1. Wählen Sie im Hauptmenü den Punkt **Netzwerk**.
2. Wählen Sie die Registerkarte **Routing**.
3. **Standardroute:** Geben Sie in dieses Feld die vom Provider vorgegebene Standardroute ein. An diese Adresse werden alle Pakete weitergeleitet, die nicht zur Weiterleitung an andere Netze bestimmt sind.
4. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

Als nächstes müssen Sie konkrete Filterregeln setzen, um Paketen den Weg ins Internet oder auf die Server offen zu lassen. Standardmäßig ist jeglicher Verkehr über die Firewall unterbunden. Nur die von Ihnen gestatteten Pakete können die Firewall passieren. Wir wollen den Verkehr vom internen Netzwerk nach außen zulassen. Von der DMZ sollen sich die Mitarbeiter die E-Mails vom Mailserver via POP3 abholen können. Außerdem dürfen sie den WWW-Server benutzen.

Firewallregeln

1. Wählen Sie im Hauptmenü den Punkt **Firewall**.
2. Wählen Sie die Registerkarte **Firewallregeln**.
3. **Eingehend:** Wählen Sie als eingehendes Interface "int0".
4. **Ausgehend:** Wählen Sie als ausgehendes Interface "ext0".
5. **Go!**: Betätigen Sie diese Schaltfläche, um die Filterregeln für Pakete von "int0" nach "ext0" anzuzeigen.
6. **Regel hinzufügen:** Betätigen Sie diese Schaltfläche, um eine neue Filterregel hinzuzufügen, die Pakete von innen nach außen durchläßt. Sie werden in die Detailansicht weitergeleitet.
7. **Quelladresse:** Wählen Sie aus der Auswahlliste ANY, um alle Quelladressen zu erlauben.
8. **Zieladresse:** Wählen Sie aus der Auswahlliste ANY, um alle Zieladressen zu erlauben.
9. **Speichern:** Betätigen Sie die Schaltfläche **Speichern**.
10. **Eingehend:** Belassen Sie die Einstellung des eingehenden Interfaces auf "int0".
11. **Ausgehend:** Wählen Sie aus der Auswahlliste des ausgehenden Interfaces "dmz0".
12. **Go!**: Betätigen Sie diese Schaltfläche, um die Filterregeln für die Pakete von "int0" nach "dmz0" anzuzeigen.
13. **Regel hinzufügen:** Betätigen Sie diese Schaltfläche, um eine neue Filterregel hinzuzufügen, die Pakete von "int0" nach "dmz0" durchläßt.
14. **Quelladresse:** Wählen Sie aus der Auswahlliste ANY, um alle Quelladressen zu erlauben.
15. **Zieladresse:** Wählen Sie aus der Auswahlliste ANY, um alle Zieladressen zu erlauben.
16. **Service:** Wählen Sie den Eintrag "pop3".
17. **Speichern:** Lassen Sie in der folgenden Detailansicht alle Felder entsprechend den Standardeinstellungen.
18. **Weitere Regel hinzufügen:** Betätigen Sie diese Schaltfläche, um eine weitere Filterregel hinzuzufügen.
19. **Service:** Wählen Sie den Eintrag "http".
20. **Quelladresse:** Wählen Sie aus der Auswahlliste ANY, um alle Quelladressen zu erlauben.
21. **Zieladresse:** Wählen Sie aus der Auswahlliste ANY, um alle Zieladressen zu erlauben.

© 2008 by eSYS Informationssysteme GmbH

22. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern. Somit können Sie vom internen Netzwerk Ihre Mails auf dem Mailserver in der DMZ abfragen und auch auf den WWW-Server in der DMZ zugreifen.

Auf der Firewall wird ein Mail-Relay betrieben, der eingehende Mails via SMTP an den Mailserver in der DMZ weiterleitet. Daher muss es SMTP Paketen erlaubt sein, die Firewall zu erreichen.

1. Wählen Sie im Hauptmenü den Punkt **Firewall**.
2. Wählen Sie die Registerkarte **Firewallregeln**.
3. **Eingehend:** Wählen Sie als eingehendes Interface "ext0".
4. **Ausgehend:** Wählen Sie als ausgehendes Interface "local".
5. **Go!**: Betätigen Sie diese Schaltfläche, um die Filterregeln für Pakete anzuzeigen, die von außen ("ext0") auf der Firewall eingehen.
6. **Regel hinzufügen:** Betätigen Sie diese Schaltfläche, um eine Filterregel hinzuzufügen. Sie werden in die Detailansicht weitergeleitet.
7. **Quelladresse:** Wählen Sie aus der Auswahlliste ANY, um alle Quelladressen zu erlauben.
8. **Zieladresse:** Wählen Sie aus der Auswahlliste ANY, um alle Zieladressen zu erlauben.
9. **Service:** Wählen Sie den Eintrag "smtp".
10. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

Um E-Mails über Gibraltar verschicken zu können, muss auch der SMTP Port von innen auf die Firewall zugänglich sein.
Wiederholen Sie den vorigen Vorgang für das eingehende Interface "int0" und das ausgehende Interface "local". Zusätzlich schränken Sie die Quell IP-Adressen auf die des internen Netzwerkes ein, indem Sie in das Feld Quell IP-Adresse den Wert "192.168.1.0/24" eingeben.
Weiters sollen auch DNS Anfragen an den lokal auf Gibraltar laufenden DNS Server möglich sein. Fügen Sie dazu sowohl für das eingehende Interface "int0" und das ausgehende Interface "local", als auch für das eingehende Interface "dmz0" und das ausgehende Interface "local" eine Filterregel ein, die Pakete für den Service "dns" akzeptiert.
Damit der Mailserver auch selbst E-mails versenden kann, müssen Sie für das eingehende Interface "dmz0" und das ausgehende Interface "local" TCP Pakete auf den Service "smtp" zulassen.

Damit die Pakete im Internet auch korrekt weitergeleitet werden, müssen die internen Adressen beim Verlassen der Firewall mit der öffentlichen IP-Adresse als Quell IP-Adresse maskiert werden (NAT). Auch Anfragen an den HTTP Port (80) der Firewall müssen an den WWW-Server in der DMZ weitergeleitet werden. Diese Konfigurationen nehmen wir im NAT Modul vor.

NAT - Regeln

1. Wählen Sie im Hauptmenü den Punkt **NAT**.
2. Wählen Sie die Registerkarte **NAT-Regeln**.
3. **Track:** Wählen Sie aus diesem Auswahlfeld den Wert "outgoing ext0", um die ausgehenden Pakete zu maskieren.
4. **Regel hinzufügen:** Betätigen Sie diese Schaltfläche, um eine NAT Regel hinzuzufügen. Sie werden in die Detailansicht weitergeleitet.
5. **Quell IP-Adresse:** Geben Sie hier den Wert 192.168.1.0/24 ein, damit alle Pakete, die

© 2008 by eSYS Informationssysteme GmbH

aus diesem Netz kommen und über "ext0" die Firewall verlassen, eine neue Quell IP-Adresse bekommen.
6. **Aktion:** Belassen Sie die Auswahl auf "SNAT", weil die Quell IP-Adresse auf eine uns bekannte öffentliche IP-Adresse verändert werden soll.
7. **--to:** Geben Sie hier die neue Quell IP-Adresse ein (in unserem Fall: 80.50.30.50).
8. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

Wiederholen Sie den Vorgang mit der Quell IP-Adresse 192.168.0.0/24, da auch die Pakete aus der DMZ verändert werden müssen.

Um Anfragen auf den Port 80 der Firewall an den WWW-Server weiterzuleiten, müssen folgende Einstellungen gemacht werden:

1. Wählen Sie im Hauptmenü den Punkt **NAT**.
2. Wählen Sie die Registerkarte **NAT-Regeln**.
3. **Track:** Wählen Sie aus diesem Auswahlfeld den Wert "incoming ext0", um die ausgehenden Pakete zu maskieren.
4. **Regel hinzufügen:** Betätigen Sie diese Schaltfläche, um eine NAT Regel hinzuzufügen. Sie werden in die Detailansicht weitergeleitet.
5. **Ziel IP-Adresse:** Geben Sie hier den Wert 80.50.30.50 ein, da die Anfragen an der IP-Adresse der Firewall eingehen.
6. **Service:** Wählen Sie aus dem Auswahlfeld den Wert "http".
7. **Aktion:** Belassen Sie die Auswahl auf "DNAT", weil die Ziel IP-Adresse verändert werden soll.
8. **--to:** Geben Sie hier die neue Ziel IP-Adresse ein (in unserem Fall: 192.168.0.3).
9. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

Dadurch wird die Ziel IP-Adresse von HTTP Paketen auf die Adresse des WWW-Servers (192.168.0.3) verändert. Damit das Paket auch den WWW-Server erreichen kann, ist jedoch noch der Eintrag einer Paketfilterregel im Modul Firewall nötig. Diese erlaubt es einem HTTP-Paket erst, von außen in die DMZ vorzudringen.

1. Wählen Sie im Hauptmenü den Punkt **Firewall**.
2. Wählen Sie die Registerkarte **Firewallregeln**.
3. **Eingehend:** Wählen Sie als eingehendes Interface "ext0".
4. **Ausgehend:** Wählen Sie als ausgehendes Interface "dmz0".
5. **Go!:** Betätigen Sie diese Schaltfläche, um die Filterregeln für Pakete anzuzeigen, die von "ext0" nach "dmz0" gelangen sollen.
6. **Regel hinzufügen:** Betätigen Sie diese Schaltfläche, um eine Filterregel hinzuzufügen. Sie werden in die Detailansicht weitergeleitet.
7. **Quelladresse:** Wählen Sie aus der Auswahlliste ANY, um alle Quelladressen zu erlauben.
8. **Ziel IP-Adresse:** Geben Sie in dieses Textfeld die IP-Adresse des WWW-Servers ein (192.168.0.3).
9. **Service:** Wählen Sie den Eintrag "http".
10. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

Konfiguration des Mail-Relay

Das Mail-Relay empfängt die E-mails, die für Ihre Domäne bestimmt sind, und leitet sie an einen in der DMZ gelegenen Mailserver weiter. Dadurch ist Ihr Mailserver von außen nicht

© 2008 by eSYS Informationssysteme GmbH

direkt erreichbar und somit besser vor Angriffen geschützt. Um eingehende Mails an den internen Mailserver weiterzuleiten, gehen Sie folgendermaßen vor.

1. Wählen Sie aus dem Hauptmenü den Punkt **Mail**.
2. Wählen Sie die Registerkarte **Weiterleitung eingehend**.
3. **Verwaltete Domänen:** Geben Sie in diese Elementgruppe die Domänen ein, die Sie auf Ihren Mailservern verwalten.
4. **Server hinzufügen:** Betätigen Sie diese Schaltfläche, um einen Server hinzuzufügen.
5. **Domäne:** Geben Sie in dieses Textfeld die zu verwaltende Domäne ein (z.B. "esys.at").
6. **Mailserver IP:** Geben Sie hier die IP-Adresse des Mailservers ein, der die Mails für die angegebene Domäne verwaltet (z.B. 192.168.0.2).
7. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.
8. Wählen Sie aus dem Hauptmenü den Punkt **Mail**.
9. Wählen Sie die Registerkarte **Allgemeine Einstellungen**.
10. **Viren und Spamchecks aktivieren:** Aktivieren Sie diese Option, wenn Sie Ihre Mails auf Viren und Spam überprüfen wollen.
11. **Mails scannen für:** Aktivieren Sie die jeweiligen Domänen, die Sie auf Mails bzw. Spam überprüfen wollen
12. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

Um die Einstellungen für den Mailversand nach außen hin vorzunehmen, gehen Sie folgendermaßen vor:

1. Wählen Sie aus dem Hauptmenü den Punkt **Mail**.
2. Wählen Sie die Registerkarte **Weiterleitung ausgehend**.
3. **Lokale Netzwerke:** Betätigen Sie die Schaltfläche **Netzwerkadresse hinzufügen**, um eine Netzwerkadresse hinzuzufügen. Allen Netzwerken in dieser Liste ist das Versenden von E-Mails erlaubt. Belassen Sie den bereits vorhandenen Eintrag 127.0.0.1/8, denn die Firewall selbst versendet ebenfalls E-Mails an den Administrator.
4. **Netzwerkadresse:** Geben Sie hier den Wert 192.168.1.0/24 ein, da Clients aus unserem internen Netzwerk Mails versenden dürfen. Auch aus der DMZ werden Mails gesendet. Fügen Sie die Netzwerkadresse 192.168.0.0/24 hinzu.
5. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

Konfiguration speichern

1. Speichern Sie die Konfiguration auf einem USB-Stick oder auf der Harddisk.

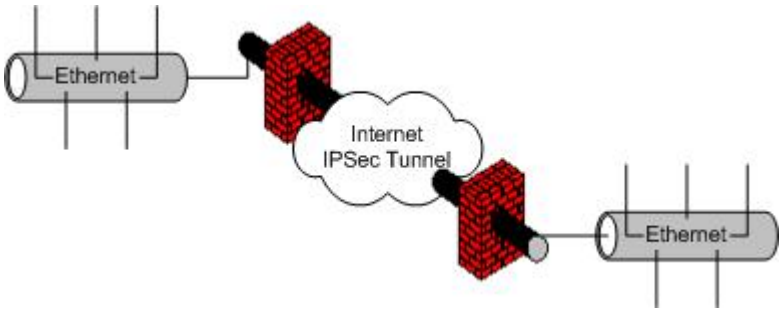
Damit sind die Einstellungen vollkommen und Ihre Netzwerke eingerichtet. Durch das Speichern der Konfiguration können Sie jederzeit den jetzigen Stand wiederherstellen, Sie den USB Stick anstecken und Gibraltar neu booten.

7.4 IPSec VPN

Konfiguration eines IPSec-VPN-Tunnels zu einer anderen Gibraltar. Es werden zwei Standorte über das Internet mit einem VPN-Tunnel verbunden. Weiters wird es Aussendienstmitarbeitern ermöglicht, sich über PPTP gesichert ins interne Firmennetzwerk

© 2008 by eSYS Informationssysteme GmbH

einzuwählen. Die Benutzerverwaltung erfolgt über den lokalen Gibraltar LDAP Server.



Systemvoraussetzungen

PC mit zwei kompatiblen Netzwerkkarten oder Gibraltar Security Gateway.
Breitband-Internet mit fixer öffentlicher IP-Adresse (z.B. XDSL)

Installation von Gibraltar

Installieren sie Gibraltar wie im Kapitel Installation beschrieben.

Systemeinstellungen

Systemeinstellungen wie in Szenario 1

Netzwerkeinstellungen - Interfaces

Netzwerk- sowie Routingeinstellungen wie in Szenario 2

ACHTUNG: Durch das Verändern der IP-Adresse auf der Netzwerkkarte, über die Sie auf Gibraltar zugreifen, wird die Verbindung unterbrochen und Sie müssen für Ihren Arbeitsplatzrechner ebenfalls die IP-Adresse anpassen.

Standardroute festlegen

1. Wählen Sie die Registerkarte **Routing**.
2. **Standardroute:** Geben Sie in dieses Feld die vom Provider vorgegebene Standardroute ein. An diese Adresse werden alle Pakete weitergeleitet, die nicht zur Weiterleitung an andere Netze bestimmt sind.
3. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

Firewallregeln

Firewallregeln wie in Szenario 2

NAT - Regeln

NAT-Regeln wie in Szenario 2

Verbindung eines Remote-Computers mit dem internen Netzwerk via PPTP

1. Wählen Sie im Hauptmenü den Punkt **VPN**.

© 2008 by eSYS Informationssysteme GmbH

2. Wählen Sie den Untermenüpunkt **PPTP**.
3. Wählen Sie die Registerkarte **Allgemeine Einstellungen**.
4. **Lokale IP (mit Netzwerkmaske):** Geben Sie hier die IP-Adresse ein, mit der der Remote Computer mit dem internen Netzwerk Verbindung aufnimmt. Diese IP-Adresse muss also aus dem Bereich des internen Netzwerkes kommen (z.B. 192.168.1.100/24). Geben Sie unbedingt auch die Netzwerkmaske an.
5. **Remote IP von:** Geben Sie hier die erste IP-Adresse eines IP-Adressbereichs ein. Aus diesem Adressbereich bekommt ein Remote Computer eine IP-Adresse zugewiesen (z.B. 192.168.1.211).
6. **Remote IP bis:** Geben Sie hier die letzte IP-Adresse eines IP-Adressbereichs ein. Aus diesem Adressbereich bekommt ein Remote Computer eine IP-Adresse zugewiesen (z.B. 192.168.1.220). Durch die Einstellung des Bereiches von 192.168.1.211-192.168.1.220 können 10 IP-Adressen für Remote Computer vergeben werden.
7. **Domäne:** Geben Sie die Domäne ein, der der Remote Computer angehören soll.
8. **DNS Server:** Geben Sie die IP des DNS Server an, den die Remote Computer erhalten sollen.
9. **WINS Server:** Geben Sie die IP des WINS Server an, den die Remote Computer erhalten sollen. (optional)
10. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

PPTP-Remote Benutzer

1. Wählen Sie den Menüpunkt **Benutzer**.
2. Sie werden automatisch zur Registerkarte **LDAP Einstellungen** weitergeleitet.
3. Wählen Sie den Wert "local OpenLDAP" und starten Sie gleich darauf den LDAP-Dienst in der selben Maske.
4. Wechseln Sie zur Registerkarte **Benutzer**.
5. Fügen Sie einen Benutzer mit gewünschtem Benutzernamen und Passwort hinzu und aktivieren Sie das Kontrollkästchen **VPN**.
6. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

Filterregeln für PPTP Zugang einrichten

1. Wählen Sie im Hauptmenü den Punkt **Firewall**.
2. Wählen Sie die Registerkarte **Firewallregeln**.
3. **Eingehend:** Wählen Sie als eingehendes Interface "ext0".
4. **Ausgehend:** Wählen Sie als ausgehendes Interface "local".
5. **Go!:** Betätigen Sie diese Schaltfläche, um die Filterregeln für Pakete von "ext0" nach "local" anzuzeigen.
6. **Regel hinzufügen:** Betätigen Sie diese Schaltfläche, um eine Filterregel hinzuzufügen.
7. **Quelladresse:** Wählen Sie aus der Auswahlliste ANY, um alle Quelladressen zu erlauben.
8. **Zieladresse:** Wählen Sie aus der Auswahlliste ANY, um alle Zieladressen zu erlauben.
9. **Service:** Wählen Sie den Eintrag "pptp".
10. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

Um dem Remote Benutzer auch Zugriff auf das Netz hinter der Firewall zu geben, müssen Sie zusätzliche Filterregeln für den PPTP Zugang definieren. Diese Regeln müssen den Datenverkehr vom PPTP Zugang ins interne Netz weiterleiten (FORWARD-Regeln).

1. Wählen Sie die Registerkarte **Firewallregeln**.

© 2008 by eSYS Informationssysteme GmbH

2. **Eingehend:** Wählen Sie als eingehendes Interface "ppp+".
3. **Ausgehend:** Wählen Sie als ausgehendes Interface "int0".
4. **Go!:** Betätigen Sie diese Schaltfläche, um die Filterregeln für Pakete von "ppp+" nach "int0" anzuzeigen.
5. **Regel hinzufügen:** Betätigen Sie diese Schaltfläche, um eine Filterregel hinzuzufügen.
6. **Quelladresse:** Wählen Sie aus der Auswahlliste ANY, um alle Quelladressen zu erlauben.
7. **Zieladresse:** Wählen Sie aus der Auswahlliste ANY, um alle Zieladressen zu erlauben.
8. **Service:** Wählen Sie den Eintrag "ANY".
9. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

Starten des PPTP-Server Dienstes

1. Wählen Sie im Hauptmenü den Punkt **Dienste**.
2. **Verfügbare Dienste:** Markieren Sie in dieser Elementgruppe beim Eintrag **PPTP** die Option **Ein**. Dadurch wird bei einem Neustart der PPTP Server wieder automatisch gestartet.
3. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.
4. **Dienst starten**  **:** Betätigen Sie diese Schaltfläche beim Eintrag **PPTP**, wenn der PPTP Server nicht gestartet ist. Dadurch wird der Dienst gestartet. Der Status verändert sich auf **(gestartet)** und die Schaltfläche zu **Dienst stoppen**  .

Somit ist der Zugang via PPTP eingerichtet und der Remote Benutzer kann sich mit seinen Anmeldedaten am internen Netzwerk anmelden.

Für die Einrichtung des IPSec Tunnels verwenden wir zwei Gibraltar Firewalls: "gibraltar1" und "gibraltar2".

Starten des IPSec Dienstes

1. Wählen Sie im Hauptmenü den Punkt **Dienste**.
2. **Verfügbare Dienste:** Markieren Sie in dieser Elementgruppe beim Eintrag **IPSec** die Option **Ein**. Dadurch wird bei einem Neustart der IPSec Dienst wieder automatisch gestartet.
3. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.
4. **Dienst starten**  **:** Betätigen Sie diese Schaltfläche beim Eintrag **IPSec**, wenn der IPSec Dienst nicht gestartet ist. Dadurch wird der Dienst gestartet. Der Status verändert sich auf **(gestartet)** und die Schaltfläche zu **Dienst stoppen**  .

IPSec

1. Wählen Sie im Hauptmenü den Punkt **IPSec**.
2. Wählen Sie die Registerkarte **Allgemeine Einstellungen**.
3. **Für IPSec aktivieren:** Markieren Sie die Kontrollkästchen jener Netzwerkkarten, auf denen Sie IPSec aktivieren wollen (z.B. "ext0").
4. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

Zertifikat downloaden

Um das Zertifikat bei der Gegenstelle bekannt zu geben, müssen Sie es downloaden und bei

© 2008 by eSYS Informationssysteme GmbH

der Gegenstelle wieder hochladen. Wir verwenden hierfür wiederum die zwei Gibraltar Firewalls "gibraltar1" und "gibraltar2".

1. Wählen Sie im Hauptmenü der Firewall "gibraltar1" den Punkt **VPN**.
2. Wählen Sie den Untermenüpunkt **IPSec**.
3. Wählen Sie die Registerkarte **Zertifikate**.
4. **Host Zertifikate:** In dieser Elementgruppe werden die selbst erstellten Zertifikate und die hochgeladenen Zertifikate der Gegenstellen angezeigt.
5. **Zertifikat downloaden**  **:** Betätigen Sie diese Schaltfläche, um das Zertifikat ("gibraltar.pem") herunterzuladen. Sie müssen einen Speicherort angeben. Benennen Sie dieses Zertifikat um, damit Sie es als Zertifikat dieser Firewall später eindeutig identifizieren können (z.B. "gibraltar1Cert.pem"). Laden Sie dieses Zertifikat anschließend bei der Gegenstelle wieder hoch.
6. Wechseln Sie zur anderen Firewall "gibraltar2", melden Sie sich an und laden Sie das Zertifikat mit dem Namen "gibraltar1Cert" in die Elementgruppe **Host Zertifikate** hoch.
7. Laden Sie von der Firewall "gibraltar2" das Zertifikat "gibraltar.pem" herunter und laden es auf der Firewall "gibraltar1" in der Elementgruppe **Host Zertifikate** hoch, nachdem Sie es umbenannt haben (z.B. "gibraltar2Cert").

Damit besitzt nun jede Firewall das Zertifikat der Gegenstelle und es kann mit der Konfiguration der Tunnel begonnen werden.

IPSec Tunnel einrichten

1. Wählen Sie im Hauptmenü der Firewall "gibraltar1" den Punkt **VPN**.
2. Wählen Sie den Untermenüpunkt **IPSec**.
3. Wählen Sie die Registerkarte **Tunnel**.
4. **Tunnel hinzufügen:** Betätigen Sie diese Schaltfläche, um einen Tunnel hinzuzufügen.
5. **Bezeichnung:** Geben Sie eine Bezeichnung für den Tunnel ein (z.B. "gib1Tunnel").
6. **Status nach Start:** Wählen Sie hier, welchen Status der Tunnel nach einem Neustart des IPSec Dienstes annehmen soll (z.B. "(standby)").
7. **Lokale IP:** Wählen Sie die IP-Adresse von "gibraltar1", über die der Tunnel erstellt wird. Beachten Sie, dass Sie hier nur IP-Adressen von Netzwerkkarten wählen können, die Sie in der Registerkarte **Allgemeine Einstellungen** für IPSec aktiviert haben. Sind Sie im Begriff zwei Standorte miteinander zu vernetzen, so werden Sie hier die offizielle IP-Adresse wählen.
8. **Lokales Subnetz:** Geben Sie hier das lokale Subnetz an, wenn Sie es durch den Tunnel erreichbar machen wollen.
9. **Lokales Zertifikat:** Wählen Sie hier das Zertifikat aus, das Sie zuerst erstellt haben ("gibraltar1Cert").
10. **IP Gegenstelle:** Geben Sie hier die IP-Adresse der Gegenstelle ein (Die offizielle IP-Adresse von "gibraltar2").
11. **Subnetz Gegenstelle:** Geben Sie hier das Subnetz der Gegenstelle ein, wenn Sie es über den Tunnel erreichbar machen wollen.
12. **Autorisierung:** Wählen Sie die Autorisierungsvariante aus (in diesem Fall X.509). Wählen Sie aus dem Auswahlfeld das Zertifikat der Gegenstelle aus ("gibraltar2Cert").
13. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern. Sie werden in die Übersicht weitergeleitet.
14. Wechseln Sie zur Firewall "gibraltar2" und erstellen Sie einen Tunnel "gib2Tunnel", der als Endpunkt die IP Adresse der Firewall "gibraltar1" hat.

© 2008 by eSYS Informationssysteme GmbH

IPSec Tunnel starten/stoppen

1. **IPSec Tunnel starten** **:** Betätigen Sie diese Schaltfläche, um den Tunnel zu starten, wenn der aktuelle Status **(deaktiviert)** oder **(standby)** ist.
2. **IPSec Tunnel aktivieren (Standby Modus)** **:** Betätigen Sie diese Schaltfläche, um den Tunnel in den Standby Modus zu versetzen, wenn der aktuelle Status **(deaktiviert)** ist.
3. **IPSec Tunnel stoppen (Standby Modus)** **:** Betätigen Sie diese Schaltfläche, um den Tunnel in den Standby Modus zu versetzen, wenn der aktuelle Status **(gestartet)** ist.
4. **IPSec Tunnel deaktivieren** **:** Betätigen Sie diese Schaltfläche, um den Tunnel zu deaktivieren, wenn der aktuelle Status **(standby)** oder **(gestartet)** ist.

Filterregeln für IPSec Tunnel einrichten

Um dem Remote Benutzer auch Zugriff auf das Netz hinter der Firewall zu geben, müssen Sie zusätzliche Filterregeln für den IPSec Tunnel definieren. Diese Regeln müssen den Datenverkehr vom IPSec Tunnel ins interne Netz weiterleiten (FORWARD-Regeln).

1. Wählen Sie im Hauptmenü den Punkt **Firewall**.
2. Wählen Sie die Registerkarte **Firewallregeln**.
3. **Eingehend:** Wählen Sie als eingehendes Interface "ipsec0".
4. **Ausgehend:** Wählen Sie als ausgehendes Interface "int0".
5. **Go!:** Betätigen Sie diese Schaltfläche, um die Filterregeln für Pakete von "ipsec0" nach "int0" anzuzeigen.
6. **Regel hinzufügen:** Betätigen Sie diese Schaltfläche, um eine Filterregel hinzuzufügen.
7. **Quelladresse:** Wählen Sie aus der Auswahlliste ANY, um alle Quelladressen zu erlauben.
8. **Zieladresse:** Wählen Sie aus der Auswahlliste ANY, um alle Zieladressen zu erlauben.
9. **Service:** Wählen Sie den Eintrag "ANY".
10. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.
11. **Eingehend:** Wählen Sie als eingehendes Interface "int0".
12. **Ausgehend:** Wählen Sie als ausgehendes Interface "ipsec0".
13. **Go!:** Betätigen Sie diese Schaltfläche, um die Filterregeln für Pakete von "int0" nach "ipsec0" anzuzeigen.
14. **Regel hinzufügen:** Betätigen Sie diese Schaltfläche, um eine Filterregel hinzuzufügen.
15. **Quelladresse:** Wählen Sie aus der Auswahlliste ANY, um alle Quelladressen zu erlauben.
16. **Zieladresse:** Wählen Sie aus der Auswahlliste ANY, um alle Zieladressen zu erlauben.
17. **Service:** Wählen Sie den Eintrag "ANY".
18. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

Konfiguration speichern

1. Speichern Sie die Konfiguration auf einem USB-Stick oder auf der Harddisk.

Damit sind die Einstellungen vollkommen und Ihre VPN Tunnels eingerichtet. Durch das Speichern der Konfiguration können Sie jederzeit den jetzigen Stand wiederherstellen, indem Sie die den USB Stick in den Computer geben und Gibraltar neu booten.

© 2008 by eSYS Informationssysteme GmbH

7.5 Active Directory/Open VPN

Konfiguration von Gibraltar in Verbindung mit Active Directory. Gewisse Active Directory Benutzer sollen nachfolgende Dienste mit Ihren gewohnten Benutzernamen und Passwörtern nutzen können. Der Zugriff auf diese Dienste kann mit Active Directory Sicherheitsgruppen gesteuert werden. Konfiguration von OpenVPN für den Fernzugriff.

- **HTTP-Proxy** zum Schutz des HTTP-Traffic
- **SMTP-Authentifizierung** damit Mitarbeiter von extern über die Firewall Mails versenden können
- **OpenVPN** zur gesicherten Einwahl ins interne Netz

Folgende Voraussetzungen der Active Directory Domäne sind gegeben:

- Domänenname: "**firma.local**"
- Organisationseinheit des Active Directory Benutzers für die Kommunikation mit Gibraltar: **firma.local/firma/Benutzer**
- Loginname des Active Directory Benutzers: "**gibuser**"
- Organisationseinheit für die Active Directory Gruppen zur Steuerung des Zugriffs auf die einzelnen Dienste: **firma.local/firma/Gruppen**
- Eine domänenlokale Gruppe "**dl_http**" in der Organisationseinheit "firma.local/firma/Gruppen" für die Steuerung des Zugriffs auf den HTTP-Proxy.
- Eine domänenlokale Gruppe "**dl_smtp**" in der Organisationseinheit "firma.local/firma/Gruppen" für die Steuerung des Zugriffs auf die SMTP-Authentifizierung
- Eine domänenlokale Gruppe "**dl_vpn**" in der Organisationseinheit "firma.local/firma/Gruppen" für die Steuerung der Einwahl via VPN.
- Internes Netz: **192.168.0.0/24**
- Externe IP: **1.1.1.1**

Hinweis: Alle angegebenen Werte sind nur Beispiele. Sie müssen diese Werte an Ihre individuellen Gegebenheiten anpassen.

Systemvoraussetzungen

PC mit zwei kompatiblen Netzwerkkarten oder Gibraltar Security Gateway.

Installation von Gibraltar

Installieren sie Gibraltar wie im Kapitel Installation beschrieben.

Systemeinstellungen

Systemeinstellungen wie in Szenario 2

Netzwerkeinstellungen - Netzwerkkarte

Netzwerk- sowie Routingeinstellungen wie in Szenario 2

ACHTUNG: Durch das Verändern der IP-Adresse auf der Netzwerkkarte, über die Sie auf Gibraltar zugreifen, wird die Verbindung unterbrochen und Sie müssen für Ihren Arbeitsplatzrechner ebenfalls die IP-Adresse anpassen.

© 2008 by eSYS Informationssysteme GmbH

Firewallregeln

Firewallregeln wie in Szenario 2

NAT - Regeln

NAT-Regeln wie in Szenario 2

Integration in Active Directory

Um alle Dienste mit den bestehenden Windows-Logins nutzen zu können, muss Gibraltar in das Active Directory integriert werden. Gehen Sie folgendermaßen vor:

1. Wählen Sie die Registerkarte **Benutzer**.
2. Sie werden automatisch zur Registerkarte **LDAP Einstellungen** weitergeleitet.
3. **Server:** Wählen Sie "Active Directory".
4. **IP Domaincontroller:** Geben Sie hier die IP-Adresse eines Domaincontrollers an.
5. **Benutzer für Kommunikation mit dem AD:** Geben Sie hier den Namen eines Active Directory Benutzers ("gibuser") ein. Dieser Benutzer muss **keine** Administratorenrechte haben, da er lediglich zur Kommunikation mit dem Active Directory verwendet wird.
6. **AD Benutzerpasswort:** Geben Sie hier das Passwort des Benutzers "gibuser" ein und wiederholen Sie es im folgendem Feld.
7. **Organisationseinheit dieses AD-Benutzers:** Geben sie hier die Organisationseinheit des AD Benutzers "gibuser" ein. ("ou=Benutzer,ou=firma").
8. **Organisationseinheit AD Gruppen:** Geben Sie die Organisationseinheit für die AD Gruppen ein: ("ou=Gruppen,ou=firma").
9. **Domäne:** Geben sie hier den FQDN der internen Windows Domäne ein ("firma.local")
10. **Speichern:** Betätigen Sie diese Schaltfläche, um die Werte zu speichern.
11. **Domäne beitreten:** Betätigen Sie diese Schaltfläche, um einer Active Directory Domäne beizutreten.
12. **Domänenadministrator:** Geben sie hier den Windows Loginnamen eines Domänenadministrators an.
13. **Passwort:** Geben Sie hier das Passwort des Domänenadministrators an.
14. **Domäne beitreten:** Betätigen Sie diese Schaltfläche, um einer Active Directory Domäne beizutreten.
15. **AD Gruppen auswählen:** Betätigen Sie diese Schaltfläche, um Active Directory Gruppen für die Steuerung der Zugriffe auszuwählen. Es werden alle Gruppen aufgelistet, die sich in der Organisationseinheit "ou=Gruppen,ou=firma" befinden.
16. **VPN Gruppe:** Wählen Sie hier die Gruppe "dl_vpn"
17. **HTTP-Proxy Gruppe:** Wählen Sie hier die Gruppe "dl_http".
18. **Mail Gruppe:** "Wählen Sie hier die Gruppe "dl_mail".
19. **Speichern:** Betätigen Sie diese Schaltfläche, um die Werte zu speichern.
20. Fügen Sie nun mit Hilfe des Active Directory Snap In die autorisierten Benutzer in die jeweiligen Gruppen.

HTTP-Proxy konfigurieren

1. Wählen Sie im Hauptmenü den Punkt **Proxy Server.**

© 2008 by eSYS Informationssysteme GmbH

2. Wählen Sie den Untermenüpunkt **HTTP Proxy**.
3. Wählen Sie die Registerkarte **Proxy Cache**.
4. **Hauptspeicher für Proxy (in MB):** Geben Sie hier einen Wert an, wie viel Hauptspeicher für den Proxy-Cache zur Verfügung gestellt werden soll. Dieser Teil des Hauptspeichers wird dadurch für übrige Dienste blockiert. Belassen Sie den Wert auf 4.
5. **Maximale Größe des Objekts (in KB):** Dieser Wert legt fest, bis zu welcher Größe Objekte im Cache zwischengespeichert werden, die auf besuchten Homepages angezeigt werden. Überschreitet ein Objekt diesen Wert, so wird es nicht für einen weiteren Aufruf im Cache zwischengespeichert.
6. **Cache auf Festplatte verwenden:** Markieren Sie dieses Kontrollkästchen, wenn Sie eine Festplatte im Modul **System** eingebunden haben und diese auch als Cache für den HTTP-Proxy zur Verfügung stellen wollen.
7. **Größe des Disk-Cache (in MB):** Wenn Sie das Kontrollkästchen **Cache auf der Festplatte verwenden** markiert haben, können Sie in diesem Textfeld den Speicherplatz eingeben, den Sie für den HTTP-Proxy auf der Festplatte zur Verfügung stellen wollen.
8. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.
9. Wählen Sie die Registerkarte **Authentifizierung**.
10. **Authentifizierungsmethode:** Wählen Sie hier den Wert "Authentifizierung über LDAP".
11. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.
12. Wählen Sie die Registerkarte **Content Filter**.
13. **Kaspersky Anti-Virus:** Markieren Sie dieses Kontrollkästchen, um den Kaspersky Anti-Virus Scanner zu aktivieren, sofern Sie für diesen eine gültige Lizenz erworben haben.
14. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.
15. Erstellen Sie nun eine Firewallregel, die für den TCP Port 3128 von int->local die Pakete erlaubt, damit Ihre Benutzer den HTTP-Proxy verwenden können.
16. Starten Sie anschließend im Modul **Dienste** den **HTTP-Proxy** Dienst, damit die Einstellungen aktiviert werden und stellen Sie den Starttyp auf "automatisch".

Wichtig: Damit Ihre Benutzer den HTTP-Proxy verwenden können muss dieser bei den jeweiligen Internet Browsern eingetragen werden. Am leichtesten lösen Sie diese Aufgabe mit Hilfe von Active Directory Gruppenrichtlinien! Damit können nun alle Benutzer, die sich in der Gruppe "dl_http" befinden den HTTP-Proxy ohne Eingabe von Benutzernamen und Passwort verwenden.

Mail Authentifizierung konfigurieren

1. Wählen Sie im Hauptmenü den Punkt **Mail.**.
2. Wählen Sie die Registerkarte **SMTP-Authentifizierung.**
3. **Authentifizierung verwenden:** Aktivieren Sie dieses Kontrollkästchen, um die Authentifizierung zu verwenden.
4. **Speichern**: Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.
5. Erstellen Sie nun eine Firewallregel, die für den TCP Port 25 von ext->local die Pakete erlaubt, damit Ihre Benutzer über Gibraltar Mails versenden können.
6. Starten Sie anschließend im Modul **Dienste** den **Mail Server** Dienst, damit die Einstellungen aktiviert werden und stellen Sie den Starttyp auf "automatisch".

Konfigurieren Sie nun bei den Mailclients Ihrer Benutzer Gibraltar als SMTP-Server. Vergessen Sie dabei nicht, dass der SMTP-Server eine gesicherte Verbindung (SSL) benötigt

© 2008 by eSYS Informationssysteme GmbH

(Bspw. bei Microsoft Outlook Express in den erweiterten Kontooptionen einzustellen)

Erstellen eines Zertifikates

Für die Authentifizierung bei OpenVPN werden Benutzerzertifikate verwendet. Damit Sie Zertifikate im Active Directory speichern können, müssen zuerst die Berechtigungen auf das Schema für den Active Directory Benutzer "gibuser" adaptiert werden. Melden Sie sich als Schemaadministrator auf einem Domänencontroller an und geben Sie folgende Befehlszeile ein:

```
dsacls ou=Benutzer,ou=firma,dc=firma,dc=local /I:S /G "firma\gibuser:RPWP;userPKCS12;user"
```

Um ein Benutzerzertifikat zu erstellen gehen Sie folgendermaßen vor:

1. Wählen Sie im Hauptmenü den Punkt **VPN.**.
2. Wählen Sie die Untermenüpunkt **Zertifikate.**
3. **Clientzertifikat generieren:** Betätigen Sie diese Schaltfläche, um ein neues Zertifikat hinzuzufügen.
4. Füllen Sie alle Felder sinngemäß aus und wählen Sie bei **Eigentümer** den Active Directory Benutzer, für den Sie das Zertifikat generieren wollen. Notieren Sie sich das Passwort, da Ihre Benutzer dieses zur Herstellung der OpenVPN Verbindung benötigen.
5. Speichern Sie das soeben erstelle Zertifikat auf Ihrer lokalen Festplatte ab.

Konfiguration des OpenVPN Dienstes

Zur Konfiguration des OpenVPN Dienstes gehen Sie folgendermaßen vor:

1. Wählen Sie im Hauptmenü den Punkt **VPN.**.
2. Wählen Sie den Untermenüpunkt **OpenVPN**.
3. **IP-Adresse:** Wählen Sie hier die Ihre offizielle IP Adresse. ("1.1.1.1")
4. **Geroutete Netzwerke**: Geben Sie hier das interne Netzwerk an, das über OpenVPN erreichbar sein soll. ("192.168.0.0/24)
5. **Speichern**: Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.
6. Erstellen Sie nun eine Firewallregel, die alle Pakete vom Interface **tun+** (virtuelles Interface der OpenVPN Einwahl) nach **int** erlaubt.
7. Starten Sie anschließend im Modul **Dienste** den OpenVPN Dienst, damit die Einstellungen aktiviert werden und stellen Sie den Starttyp auf "automatisch".

Windows Client installieren

Der für OpenVPN notwendige Client für Ihre Benutzer kann auf der Seite http://openvpn.se/ heruntergeladen werden.
Nach der Installation des Pakets für Windows kann nach Wunsch noch die deutsche Version (oder spanische, italienische, französische, schwedische oder norwegische Version) heruntergeladen werden. Diese Datei muss anschließend nach c:\Programme\OpenVPN\bin kopiert werden und ersetzt das englischsprachige Original.
Nach dem Starten (Client startet automatisch bei jedem Neustart) befindet sich in der Taskleiste (Rechts unten neben der Uhrzeit) ein neues Symbol - der OpenVPN Client. Um den OpenVPN Client für die Einwahl zu konfigurieren gehen Sie folgendermaßen vor:

1. Kopieren Sie das soeben heruntergeladene Zertifikat ins Verzeichnis "c:\programme\openvpn\config".

© 2008 by eSYS Informationssysteme GmbH

2. Wählen Sie im Hauptmenü den Punkt **VPN.**
3. Wählen Sie den Untermenüpunkt **OpenVPN**.
4. **Clientkonfig. herunterladen:** Betätigen Sie diese Schaltfläche, um die Clientkonfiguration herunterzuladen und speichern Sie diese ins Verzeichnis "c:\programme\openvpn\config".
5. Starten Sie mit der rechten Maustaste die OpenVPN Verbindung und geben Sie dabei das Passwort ein, das Sie bei der Erstellung des Zertifikates gewählt haben.

Nach erfolgreicher Einwahl haben Ihre Benutzer Zugriff auf die internen Ressourcen.

Active Directory Gruppen

Konfigurieren Sie nun die Mitgliedschaft in den jeweiligen Gruppen, um Ihren Benutzern den Zugriff auf die Dienste zu erlauben. Fügen Sie bspw. einen Benutzer "user1" in die Gruppe "dl_http", damit dieser den HTTP-Proxy verwenden kann!

ACHTUNG: Aus Performancegründen cachet sich der HTTP-Proxy die Authentifizierungsdaten. Sollten Sie den Benutzer "user1" wieder aus der Gruppe "dl_http" entfernen, so wird diese Einstellung erst nach einer Stunde wirksam. Um dies zu beschleunigen starten Sie einfach den HTTP-Proxy Dienst neu!.

Konfiguration speichern

1. Speichern Sie die Konfiguration auf einem USB-Stick oder auf der Harddisk.

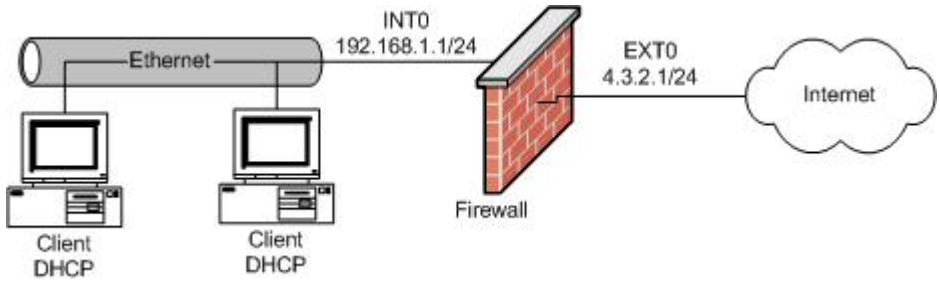
Damit sind die Einstellungen vollkommen und der angelegte Benutzer kann einen VPN Tunnel aufbauen. Durch das Speichern der Konfiguration können Sie jederzeit den jetzigen Stand wiederherstellen, indem Sie den USB Stick in den Computer geben und Gibraltar neu booten.

7.6 Proxy Server

In diesem Szenario wird Gibraltar auf einem Rechner konfiguriert, der mit zwei Netzwerkkarten ausgestattet ist, wobei eine der Internetverbindung und die andere der Verbindung ins interne Netz dient. Gibraltar soll das interne Netz schützen und den Benutzern im lokalen Netzwerk alle Dienste im Internet zur Verfügung stellen. Von außen darf kein Zugriff auf das interne Netz möglich sein. Zusätzlich sollen noch Proxy-Server eingerichtet werden. Ein HTTP-Proxy, der die vom internen Netz angeforderten Seiten auf der Festplatte der Firewall zwischenspeichert und somit eine erneute Anforderung beschleunigt. Ein FTP-Proxy, der entweder Anfragen aus dem internen Netz übernimmt und somit die Topologie verschleiert, oder aber von aussen Anfragen entgegennimmt und an einen internen FTP-Server weiterleitet. Weiters wird ein POP3-Proxy konfiguriert, der die Abfragen von Clients im internen Netz übernimmt und beim Abholen vom externen Postfach die Mails auf Viren und Spam überprüft.

HINWEIS: Dieses Szenario zeigt nur eine einfache Konfiguration der Dienste. Für detailliertere Informationen schlagen Sie bitte in den speziellen Bereichen nach.

© 2008 by eSYS Informationssysteme GmbH



HINWEIS: Alle angegebenen Werte sind nur Beispiele. Sie müssen diese Werte an Ihre individuellen Gegebenheiten anpassen.

Systemvoraussetzungen

PC mit drei kompatiblen Netzwerkkarten oder Gibraltar Security Gateway.

Installation von Gibraltar

Installieren sie Gibraltar wie im Kapitel Installation beschrieben.

Systemeinstellungen

Systemeinstellungen wie in Szenario 1

Systemeinstellungen - Festplatte

1. Wählen Sie im Hauptmenü den Punkt **System**.
2. Wählen Sie die Registerkarte **Festplatte konfigurieren**.
3. **Festplatte verwenden:** Wählen Sie aus dem Auswahlfeld jene Festplatte aus, die Sie als Cache für den HTTP-Proxy verwenden wollen.
4. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

Netzwerkeinstellungen - Netzwerkkarte

Netzwerk- sowie Routingeinstellungen wie in Szenario 2

ACHTUNG: Durch das Verändern der IP-Adresse auf der Netzwerkkarte, über die Sie auf Gibraltar zugreifen, wird die Verbindung unterbrochen und Sie müssen für Ihren Arbeitsplatzrechner ebenfalls die IP-Adresse anpassen.

Firewallregeln

Firewallregeln wie in Szenario 2

NAT - Regeln

NAT-Regeln wie in Szenario 2

DHCP-Server

DHCP-Server Einstellungen wie in Szenario 1

© 2008 by eSYS Informationssysteme GmbH

Dienste

Aktivieren Sie den Dienst DHCP-Server, wie in Szenario 1 beschrieben.

HTTP-Proxy konfigurieren

1. Wählen Sie im Hauptmenü den Punkt **Proxy Server.**
2. Wählen Sie den Untermenüpunkt **HTTP Proxy**.
3. Wählen Sie die Registerkarte **Allgemeine Einstellungen**.
4. Markieren Sie in der Elementgruppe **Transparentes Proxying erlauben** Ihr internes Interface. Dadurch werden alle Anfragen vom internen Netz an den Port 80 automatisch an den Port 3128 (bzw. den Port, der im Textfeld **Port** definiert ist) weitergeleitet, auf dem der HTTP-Proxy lauscht.
5. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.
6. Wählen Sie die Registerkarte **Proxy Cache**.
7. **Hauptspeicher für Proxy (in MB):** Geben Sie hier einen Wert an, wie viel Hauptspeicher für den Proxy-Cache zur Verfügung gestellt werden soll. Dieser Teil des Hauptspeichers wird dadurch für übrige Dienste blockiert. Belassen Sie den Wert auf 4.
8. **Maximale Größe des Objekts (in KB):** Dieser Wert legt fest, bis zu welcher Größe Objekte im Cache zwischengespeichert werden, die auf besuchten Homepages angezeigt werden. Überschreitet ein Objekt diesen Wert, so wird es nicht für einen weiteren Aufruf im Cache zwischengespeichert.
9. **Cache auf Festplatte verwenden:** Markieren Sie dieses Kontrollkästchen, wenn Sie eine Festplatte im Modul **System** eingebunden haben und diese auch als Cache für den HTTP-Proxy zur Verfügung stellen wollen.
10. **Größe des Disk-Cache (in MB):** Wenn Sie das Kontrollkästchen **Cache auf der Festplatte verwenden** markiert haben, können Sie in diesem Textfeld den Speicherplatz eingeben, den Sie für den HTTP-Proxy auf der Festplatte zur Verfügung stellen wollen.
11. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.
12. Wählen Sie die Registerkarte **Content Filter**.
13. **Kaspersky Anti-Virus:** Markieren Sie dieses Kontrollkästchen, um den Kaspersky Anti-Virus Scanner zu aktivieren, sofern Sie für diesen eine gültige Lizenz erworben haben.
14. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.
15. Starten Sie anschließend im Modul **Dienste** den **HTTP-Proxy** Dienst, damit die Einstellungen aktiviert werden und stellen Sie dessen Starttyp auf automatisch.

FTP-Proxy konfigurieren:

Der FTP-Proxy wird in diesem Beispiel so konfiguriert, dass er einen intern vorhandenen FTP-Server von der Außenwelt abschirmt, indem er die Anfragen von außen übernimmt und selbst die geforderten Daten vom internen FTP-Server abholt und nach außen wieder weitergibt.

1. Wählen Sie im Hauptmenü den Punkt **FTP-Proxy**.
2. Wählen Sie die Registerkarte **Eingehend**.
3. **Ziel FTP Server:** Geben Sie in dieses Textfeld die IP-Adresse Ihres internen FTP-Servers ein, auf den von außen zugegriffen werden soll.
4. **Ziel FTP Port:** Geben Sie hier den Port ein, auf dem der FTP-Server die

© 2008 by eSYS Informationssysteme GmbH

FTP-Dienste zur Verfügung stellt. Im Normalfall können Sie den Wert auf 21 belassen (Standard FTP-Port).
5. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.
6. Starten Sie anschließend im Modul **Dienste** den **FTP-Proxy** Dienst, damit die Einstellungen aktiviert werden und stellen Sie dessen Starttyp auf automatisch.

Damit der FTP-Proxy auch die Pakete annimmt muss noch eine Firwallregel erstellt werden.

1. Wählen Sie im Hauptmenü den Punkt **Firewall**.
2. Wählen Sie die Registerkarte **Firewallregeln**.
3. **Eingehend:** Wählen Sie als eingehendes Interface "ext0".
4. **Ausgehend:** Wählen Sie als ausgehendes Interface "local".
5. **Go!**: Betätigen Sie diese Schaltfläche, um die Filterregeln für Pakete anzuzeigen, die von außen ("ext0") auf der Firewall eingehen.
6. **Regel hinzufügen:** Betätigen Sie diese Schaltfläche, um eine Filterregel hinzuzufügen. Sie werden in die Detailansicht weitergeleitet.
7. **Quelladresse:** Wählen Sie aus der Auswahlliste ANY, um alle Quelladressen zu erlauben.
8. **Zieladresse:** Wählen Sie aus der Auswahlliste ANY, um alle Zieladressen zu erlauben.
9. **Service:** Wählen Sie den Eintrag "ftp".
10. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

POP3-Proxy:

1. Wählen Sie im Hauptmenü den Punkt **POP3-Proxy**.
2. Wählen Sie die Registerkarte **Allgemeine Einstellungen**.
3. Markieren Sie in der Elementgruppe **Transparentes Proxying erlauben** Ihr internes Interface. Dadurch werden alle Anfragen vom internen Netz an den Port 110 automatisch an den Port 8110 (bzw. den Port, der im Textfeld **Port** definiert ist) weitergeleitet, auf dem der POP3-Proxy lauscht.
4. Führen Sie hier Änderungen nach Ihren speziellen Bedürfnissen durch. Die Standardeinstellungen stellen jedoch schon eine gute Basis dar. Aktivieren Sie das Kontrollkästchen für Kaspersky Anti-Virus, wenn Sie eine gültige Kaspersky Lizenz erworben haben.
5. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.
6. Wählen Sie die Registerkarte **Anlagen umbenennen**.
7. **Anlagen umbenennen:** Markieren Sie dieses Kontrollkästchen, wenn die in der unten angeführten Elementgruppe angeführten Dateianhänge beim Empfang als Attachment umbenannt werden sollen.
8. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.
9. Starten Sie anschließend im Modul **Dienste** den **POP3-Proxy** Dienst, damit die Einstellungen aktiviert werden.

Konfiguration speichern

1. Speichern Sie die Konfiguration auf einem USB-Stick oder auf der Harddisk.

Damit sind die Einstellungen vollkommen und Ihre Clients können über Gibraltar das Internet benützen. Durch das Speichern der Konfiguration können Sie jederzeit den jetzigen Stand wiederherstellen, indem Sie die Diskette oder den USB Stick in den Computer geben und Gibraltar neu booten.

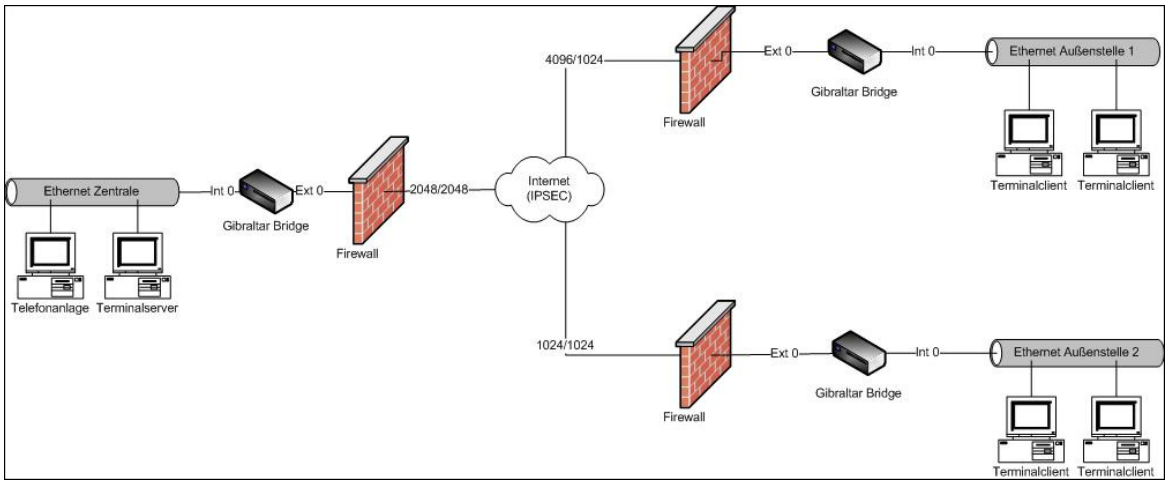
© 2008 by eSYS Informationssysteme GmbH

7.7 Bandbreitenmanagement Citrix und VOIP transparent

Konfiguration von Gibraltar als transparenten Traffic Shaper auf einem Rechner mit 2 Netzwerkkarten mit Hilfe einer Netzwerkbrücke, um einen transparenten Modus zu ermöglichen. Ziel dieses Szenarios ist es in einer Citrix-Terminalserverumgebung dem unternehmenskritische Protokoll ICA sowie dem VOIP-Traffic mindestens je 35% der verfügbaren Bandbreite zur Verfügung zu stellen. Weiters wird dem restlichem Traffic aus Latenzgründen eine Bandbreite von maximal 75 % ermöglicht. Dies ist bei latenzkritischen Anwendungen wie VOIP und Terminalservertechnologien unumgänglich, sollte der Provider nicht auf gesetzte TOS-Bits reagieren (dies ist im Regelfall auch so). Zur Gewährleistung einer ordnungsgemäßen Funktionalität dürfen darüber hinaus maximal 95 % der verfügbaren Bandbreite verwendet werden! Folgende Ausgangssituation ist gegeben:

- Zentrale mit 2048/2048 Internetanbindung (192.168.0.0/24), IP-Telefonanlage: 192.168.0.100
- Aussenstelle1 mit 4096/1024 Internetanbindung (192.168.1.0/24), IP-Telefonanlage: 192.168.1.100
- Aussenstelle2 mit 1024/1024 Internetanbindung (192.168.2.0/24), IP-Telefonanlage: 192.168.2.100

Die Aussenstellen sind bereits mit einem Drittprodukt mit der Zentrale über einen gesicherten IPSec Tunnel verbunden.



Systemvoraussetzungen

PC mit zwei kompatiblen Netzwerkkarten oder Gibraltar Security Gateway.

Installation von Gibraltar - Zentrale

Installieren sie Gibraltar wie im Kapitel Installation beschrieben.

Systemeinstellungen

Systemeinstellungen wie in Szenario 1

Netzwerkeinstellungen - Netzwerkkarte

© 2008 by eSYS Informationssysteme GmbH

1. Wählen Sie im Hauptmenü den Punkt **Netzwerk**.
2. Wählen Sie die Registerkarte **eth1**.
3. **Interface:** Geben Sie in dieses Textfeld die gewünschte Bezeichnung für diese Netzwerkkarte ein (z.B.: "int0", damit Sie die Netzwerkkarte für das interne Netzwerk eindeutig identifizieren können).
4. **Automatisch starten:** Markieren Sie dieses Kontrollkästchen, damit die Netzwerkkarte beim Systemstart automatisch gestartet wird.
5. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.
6. Wählen Sie die Registerkarte **eth0**.
7. **Interface:** Geben Sie in dieses Textfeld die gewünschte Bezeichnung für diese Netzwerkkarte ein (z.B.: "ext0", damit Sie die Netzwerkkarte für den externen Netzwerkbereich eindeutig identifizieren können).
8. **Automatisch starten:** Markieren Sie dieses Kontrollkästchen, damit die Netzwerkkarte beim Systemstart automatisch gestartet wird.
9. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.
10. Wählen Sie die Registerkarte **Bridging**.
11. **Interface:** Vergeben Sie einen Namen für die Bridge (z.B: "myBridge").
12. **Statische IPs:** Ändern Sie die IP-Adresse im Textfeld **IP-Adresse/Netzwerkmaske** auf die von Ihnen für Gibraltar vorgesehene IP-Adresse (CIDR-Notation: z.B. 192.168.0.1/24). Sie können die Konfiguration später über diese Adresse der Bridge fortsetzen.
13. **Bridged Interfaces:** Wählen Sie die Interfaces "int0" und "ext0".
14. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern und die Bridge zu erstellen

ACHTUNG: Durch das Verändern der IP-Adresse auf der Netzwerkkarte, über die Sie auf Gibraltar zugreifen, wird die Verbindung unterbrochen und Sie müssen für Ihren Arbeitsplatzrechner ebenfalls die IP-Adresse anpassen.

Netzwerkeinstellungen - Routing

Die Standardroute wird definiert.

1. Wählen Sie im Hauptmenü den Punkt **Netzwerk**.
2. Wählen Sie die Registerkarte **Routing**.
3. **Standardroute:** Geben Sie in dieses Feld eine Standardroute ein, damit Sie die Bridge auch von extern über IPSec erreichen können.
4. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

Firewallregeln

1. Wählen Sie im Hauptmenü den Punkt **Firewall**.
2. **Interface:** Wählen Sie aus dem Auswahlfeld **eingehend** den Wert "int0 bridged" für die interne Netzwerkkarte. Wählen Sie aus dem Auswahlfeld **ausgehend** den Wert "ext0 bridged" für die externe Netzwerkkarte. Betätigen Sie die Schaltfläche **Go!**. Es werden nun alle Filterregeln in der Elementgruppe **Filterregeln** angezeigt, die für Pakete bestimmt sind, die von der Netzwerkkarte "int0" auf die Netzwerkkarte "ext0" geschickt werden.
3. **Regel hinzufügen:** Betätigen Sie diese Schaltfläche, um eine neue Regel in diesem Bereich ("int0 -> ext0") einzufügen. Sie werden in die Detailansicht weitergeleitet.
4. **Quelladresse:** Wählen Sie aus der Auswahlliste ANY, um alle Quelladressen zu

© 2008 by eSYS Informationssysteme GmbH

erlauben.
5. **Zieladresse:** Wählen Sie aus der Auswahlliste ANY, um alle Zieladressen zu erlauben.
6. **Kommentar:** Geben Sie einen (möglichst sprechenden) Kommentar Ihrer Wahl ein. Alle übrigen Felder müssen in diesem Fall nicht konfiguriert werden.
7. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

Erstellen Sie eine weitere Regel mit für "ext0 bridged" -> "int0 bridged" mit denselben Einstellungen.

WICHTIG: Positionieren Sie Gibraltar jetzt so, dass das interne Interface am Switch für das interne LAN hängt und das externe Interface direkt zum Router (eventuell mit ausgekreuztem Kabel) führt. Damit befindet sich Gibraltar jetzt im transparentem Modus und kann den Verkehr von innen nach außen und umgekehrt regeln und regulieren.

Nun legen wir eine Netzwerk-Definition für die beiden Aussenstellen und die Telefonanlage an.

Netzwerk - Definitionen

1. Wählen Sie im Hauptmenü den Punkt **Netzwerk**.
2. Wählen Sie den Untermenüpunkt **Definitionen**.
3. Wählen Sie die Registerkarte **Host/Netz Aliases**.
4. Definieren Sie je einen Host/Netz Alias für die Aussenstelle 1 und die Aussenstelle 2 (z. B: "net1" für 192.168.1.0/24 und "net2" für 192.168.2.0/24).
5. Definieren Sie einen Host/Netz Alias "voip" für die Telefonanlage 192.168.0.100.
6. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

Um Bandbreitenmanagement zu ermöglichen müssen nun folgende Schritte unternommen werden:
- Definition der Bandbreiten der Interfaces
- Klassifizierung von Traffic für die Zuweisung zu Shaping Regeln
- Anlegen der Regeln, die dann die Regulierung vornehmen.

Traffic shaping

1. Wählen Sie im Hauptmenü den Punkt **Traffic shaping**.
2. Wählen Sie die Registerkarte **Allgemeine Einstellungen**.
3. **Bandbreiten:** Definieren Sie für das Interface "ext0" den Wert 2048 für Up- und Download.
4. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.
5. Wählen Sie die Registerkarte **Klassifizierung.**
6. **Klassifizierung hinzufügen:** Betätigen Sie diese Schaltfläche, um eine neue Klassifizierung für die ICA Quellports hinzuzufügen.
7. **Name:** Geben Sie hier einen Namen für die Klassifizierung (z.B: "icaSource").
8. **Quelladresse, Zieladresse:** Wählen Sie hier den Wert "ANY".
9. **Service:** Wählen Sie hier den Wert "ica_source".
10. **TOS:** Wählen Sie hier den Wert "Minimize Delay".
11. **Speichern:** Betätigen Sie diese Schaltfläche, um die Klassifizierung zu speichern.
12. **Abbrechen:** Betätigen Sie diese Schaltfläche, um zur Übersicht zu gelangen.
13. **Klassifizierung hinzufügen:** Betätigen Sie diese Schaltfläche, um eine neue Klassifizierung für die ICA Zielports hinzuzufügen.
14. **Name:** Geben Sie hier einen Namen für die Klassifizierung (z.B: "icaDest").

© 2008 by eSYS Informationssysteme GmbH

15. **Quelladresse, Zieladresse:** Wählen Sie hier den Wert "ANY".
16. **Service:** Wählen Sie hier den Wert "ica_destination".
17. **TOS:** Wählen Sie hier den Wert "Minimize Delay".
18. **Speichern:** Betätigen Sie diese Schaltfläche, um die Klassifizierung zu speichern.
19. **Abbrechen:** Betätigen Sie diese Schaltfläche, um zur Übersicht zu gelangen.
20. **Klassifizierung hinzufügen:** Betätigen Sie diese Schaltfläche, um eine neue Klassifizierung für die Quellpakete der Telefonanlage hinzuzufügen.
21. **Name:** Geben Sie hier einen Namen für die Klassifizierung (z.B: "voipSource").
22. **Quelladresse:** Wählen Sie hier die Definition "voip".
23. **Zieladresse:** Wählen Sie hier den Wert "ANY".
24. **TOS:** Wählen Sie hier den Wert "Minimize Delay".
25. **Speichern:** Betätigen Sie diese Schaltfläche, um die Klassifizierung zu speichern.
26. **Abbrechen:** Betätigen Sie diese Schaltfläche, um zur Übersicht zu gelangen.
27. **Klassifizierung hinzufügen:** Betätigen Sie diese Schaltfläche, um eine neue Klassifizierung für die Zielpakete der Telefonanlage hinzuzufügen.
28. **Name:** Geben Sie hier einen Namen für die Klassifizierung (z.B: "voipDest").
29. **Quelladresse:** Wählen Sie hier den Wert ANY.
30. **Zieladresse:** Wählen Sie hier die Definition "voip".
31. **TOS:** Wählen Sie hier den Wert "Minimize Delay".
32. **Speichern:** Betätigen Sie diese Schaltfläche, um die Klassifizierung zu speichern.
33. **Abbrechen:** Betätigen Sie diese Schaltfläche, um zur Übersicht zu gelangen.
34. **Klassifizierung hinzufügen:** Betätigen Sie diese Schaltfläche, um eine neue Klassifizierung für den ICMP Traffic hinzuzufügen.
35. **Name:** Geben Sie hier einen Namen für die Klassifizierung (z.B: "icmp").
36. **Quelladresse, Zieladresse:** Wählen Sie hier den Wert "ANY".
37. **Service:** Wählen Sie hier den Wert "CUSTOM".
38. **Protokoll:** Wählen Sie hier den Wert "ICMP".
39. **TOS:** Wählen Sie hier den Wert "Minimize Delay".
40. **Speichern:** Betätigen Sie diese Schaltfläche, um die Klassifizierung zu speichern.
41. **Abbrechen:** Betätigen Sie diese Schaltfläche, um zur Übersicht zu gelangen.
42. **Klassifizierung hinzufügen:** Betätigen Sie diese Schaltfläche, um eine neue Klassifizierung für den restlichen Traffic hinzuzufügen.
43. **Name:** Geben Sie hier einen Namen für die Klassifizierung (z.B: "rest").
44. **Quelladresse, Zieladresse:** Wählen Sie hier den Wert "ANY".
45. **Speichern:** Betätigen Sie diese Schaltfläche, um die Klassifizierung zu speichern.

Um den gesamten ICA-Traffic und auch ICMP gemeinsam priorisieren zu können, müssen die Klassifizierungen zu einer Gruppe zusammengefasst werden. Weiters werden auch die Quell- und Zielpakete der Telefonanlage zu einer Gruppe zusammengefasst.

1. Wählen Sie die Registerkarte **Klassifizierungsgruppen**.
2. **Gruppe hinzufügen:** Betätigen Sie diese Schaltfläche, um eine neue Klassifizierungsgruppe hinzuzufügen.
3. **Name:** Geben Sie hier einen Namen für die Gruppe ein (z.B: "ica").
4. **Mitglied hinzufügen:** Wählen Sie hier die Mitglieder "icaSource", "icaDest" und "icmp".
5. **Speichern:** Betätigen Sie diese Schaltfläche, um die Gruppe zu speichern.
6. **Abbrechen:** Betätigen Sie diese Schaltfläche, um zur Übersicht zu gelangen.
7. **Gruppe hinzufügen:** Betätigen Sie diese Schaltfläche, um eine neue Klassifizierungsgruppe hinzuzufügen.
8. **Name:** Geben Sie hier einen Namen für die Gruppe ein (z.B: "voip").
9. **Mitglied hinzufügen:** Wählen Sie hier die Mitglieder "voipSource", "voipDest".

© 2008 by eSYS Informationssysteme GmbH

10. **Speichern:** Betätigen Sie diese Schaltfläche, um die Gruppe zu speichern.

Zum Abschluss müssen noch die Regeln für die beiden Aussenstellen gesetzt werden. Diese Regeln nehmen nun die Bandbreitenregulierung vor. Zuerst regulieren wir den Upload der Zentrale - dies ist aus Sicht der Gibraltar nun der Track "outgoing ext0".

1. Wählen Sie die Registerkarte **Traffic Shaping Regeln**.
2. **Track:** Wählen Sie "outgoing ext0". Gibraltar verwendet nun die definierte Upload-Bandbreite des Interfaces "ext0". Dieser Traffic stellt den Upload der Zentrale dar!
3. **Regel hinzufügen:** Klicken Sie diesen Button, um eine neue Shaping Regel hinzuzufügen.
4. **Name:** Vergeben Sie einen Namen für die Regel (z.B: "ruleNet1"). Sie können die Wirkungsweise dieser Regel im Modul Monitoring gezielt analysieren.
5. **Mitglied hinzufügen:** Klicken Sie diesen Button, um Klassifizierungen bzw. Klassifizierungsgruppen hinzuzufügen.
6. Wählen Sie die Klassifizierungsgruppe "ica" und vergeben Sie die Werte "360" für Min und "1024" für Max.
7. Wählen Sie die Klassifizierungsgruppe "voip" und vergeben Sie die Werte "360" für Min und "1024" für Max.
8. Wählen Sie die Klassifizierung "rest" und vergeben Sie die Werte "250" für Min und "768" für Max.
9. **Speichern:** Betätigen Sie diese Schaltfläche, um die Regel zu speichern.
10. Wählen Sie die Registerkarte **Fortgeschritten**.
11. **Zieladresse:** Wählen Sie die Definition "net1", da diese Regel nur für dieses Zielnetz gelten soll
12. **Bandbreite (kbit) für Netze:** Wählen Sie den Wert "1024", da wir für dieses Netz nur ein Maximum von 1024kbit zur Verfügung stellen. Der gesamte Traffic, der von der Zentrale in dieses Netz läuft, darf somit 1024kbit nicht übersteigen.
13. **Speichern:** Betätigen Sie diese Schaltfläche, um die Regel zu speichern.
14. **Abbrechen:** Betätigen Sie diese Schaltfläche, um zur Übersicht zu gelangen.
15. **Regel hinzufügen:** Klicken Sie diesen Button, um eine neue Shaping Regel hinzuzufügen.
16. **Name:** Vergeben Sie einen Namen für die Regel (z.B: "ruleNet2")
17. **Mitglied hinzufügen:** Klicken Sie diesen Button, um Klassifizierungen bzw. Klassifizierungsgruppen hinzuzufügen.
18. Wählen Sie die Klassifizierungsgruppe "ica" und vergeben Sie die Werte "360" für Min und "1024" für Max.
19. Wählen Sie die Klassifizierungsgruppe "voip" und vergeben Sie die Werte "360" für Min und "1024" für Max.
20. Wählen Sie die Klassifizierung "rest" und vergeben Sie die Werte "250" für Min und "768" für Max.
21. **Speichern:** Betätigen Sie diese Schaltfläche, um die Regel zu speichern.
22. Wählen Sie die Registerkarte **Fortgeschritten**.
23. **Zieladresse:** Wählen Sie die Definition "net2", da diese Regel nur für dieses Zielnetz gelten soll
24. **Bandbreite (kbit) für Netze:** Wählen Sie den Wert "1024", da wir für dieses Netz nur ein Maximum von 1024kbit zur Verfügung stellen. Der gesamte Traffic, der von der Zentrale in dieses Netz läuft, darf somit 1024kbit nicht übersteigen.
25. **Speichern:** Betätigen Sie diese Schaltfläche, um die Regel zu speichern.

© 2008 by eSYS Informationssysteme GmbH

Anmerkung:

Um den ganzen Traffic unter Kontrolle zu bringen ist es natürlich auch notwendig, dass der Download-Traffic in der Zentrale reguliert wird. Wäre dies nicht der Fall, dann könnte ein massiver Download in der Zentrale die Upload-Pakete aus den Aussenstellen blockieren.

1. Wählen Sie die Registerkarte **Traffic Shaping Regeln**.
2. **Track:** Wählen Sie "incoming ext0". Gibraltar verwendet nun die definierte Download-Bandbreite des Interfaces "ext0". Dieser Traffic stellt den Download der Zentrale dar!
3. **Regel hinzufügen:** Klicken Sie diesen Button, um eine neue Shaping Regel hinzuzufügen.
4. **Name:** Vergeben Sie einen Namen für die Regel (z.B: "ruleDownload"). Sie können die Wirkungsweise dieser Regel im Modul Monitoring gezielt analysieren.
5. **Mitglied hinzufügen:** Klicken Sie diesen Button, um Klassifizierungen bzw. Klassifizierungsgruppen hinzuzufügen.
6. Wählen Sie die Klassifizierungsgruppe "ica" und vergeben Sie die Werte "716" für Min und "2048" für Max.
7. Wählen Sie die Klassifizierungsgruppe "voip" und vergeben Sie die Werte "716" für Min und "2048" für Max.
8. Wählen Sie die Klassifizierung "rest" und vergeben Sie die Werte "500" für Min und "1536" für Max.
9. **Speichern:** Betätigen Sie diese Schaltfläche, um die Regel zu speichern.

Anmerkung: Da wir beim Download-Shaping nicht gezielt ein Netz regulieren wollen, ist es hier nicht notwendig, auf der Registerkarte "Erweitert" eine Zieladresse zu definieren!

Konfiguration speichern

1. Speichern Sie die Konfiguration auf einem USB-Stick oder auf der Harddisk.

Damit wird nun der Verkehr in die beiden Aussenstellen anhand den verschiedenen Bandbreiten reguliert. Ein Druckjob von der Zentrale in die Aussenstellen, der bspw. nicht im ICA-Strom enthalten ist, würde nun kein Problem mehr verursachen. Um auch den ausgehenden Verkehr der Aussenstellen zu kontrollieren sind folgende Konfigurationsschritte nötig (Netzwerk- und Systemeinstellungen gleich wie in Zentrale):

Netzwerk - Definitionen

1. Wählen Sie im Hauptmenü den Punkt **Netzwerk**.
2. Wählen Sie den Untermenüpunkt **Definitionen**.
3. Wählen Sie die Registerkarte **Host/Netz Aliases**.
4. Definieren Sie einen Host/Netz Alias "voip" für die Telefonanlage 192.168.0.100.
5. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

Traffic shaping (Aussenstelle 1)

1. Wählen Sie im Hauptmenü den Punkt **Traffic shaping**.
2. Wählen Sie die Registerkarte **Allgemeine Einstellungen**.
3. **Bandbreiten:** Definieren Sie für das Interface "ext0" den Wert "1024" für den Upload sowie den Wert "4096" für Download.
4. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

© 2008 by eSYS Informationssysteme GmbH

5. Legen Sie nun die Klassifizierungen und Klassifizierungsgruppen genau so, wie in der Zentrale an.
6. Wählen Sie die Registerkarte **Traffic Shaping Regeln**.
7. **Track:** Wählen Sie "outgoing ext0". Gibraltar verwendet nun die definierte Upload-Bandbreite des Interfaces "ext0". Dieser Traffic stellt den Upload der Aussenstelle dar.
8. **Regel hinzufügen:** Klicken Sie diesen Button, um eine neue Shaping Regel hinzuzufügen.
9. **Name:** Vergeben Sie einen Namen für die Regel (z.B: "ruleUpload")
10. **Mitglied hinzufügen:** Klicken Sie diesen Button, um Klassifizierungen bzw. Klassifizierungsgruppen hinzuzufügen.
11. Wählen Sie die Klassifizierungsgruppe "ica" und vergeben Sie die Werte "360" für Min und "1024" für Max.
12. Wählen Sie die Klassifizierungsgruppe "voip" und vergeben Sie die Werte "360" für Min und "1024" für Max.
13. Wählen Sie die Klassifizierung "rest" und vergeben Sie die Werte "250" für Min und "768" für Max.
14. **Speichern:** Betätigen Sie diese Schaltfläche, um die Regel zu speichern.

Auch in der Aussenstelle ist es wichtig, den Download Traffic zu regulieren. Gehen Sie dafür folgendermaßen vor:

1. Wählen Sie die Registerkarte **Traffic Shaping Regeln**.
2. **Track:** Wählen Sie "incoming ext0". Gibraltar verwendet nun die definierte Download-Bandbreite des Interfaces "ext0". Dieser Traffic stellt den Download der Aussenstelle dar.
3. **Regel hinzufügen:** Klicken Sie diesen Button, um eine neue Shaping Regel hinzuzufügen.
4. **Name:** Vergeben Sie einen Namen für die Regel (z.B: "ruleDownload")
5. **Mitglied hinzufügen:** Klicken Sie diesen Button, um Klassifizierungen bzw. Klassifizierungsgruppen hinzuzufügen.
6. Wählen Sie die Klassifizierungsgruppe "ica" und vergeben Sie die Werte "360" für Min und "1024" für Max.
7. Wählen Sie die Klassifizierungsgruppe "voip" und vergeben Sie die Werte "360" für Min und "1024" für Max.
8. Wählen Sie die Klassifizierung "rest" und vergeben Sie die Werte "2000" für Min und "3072" für Max.
9. **Speichern:** Betätigen Sie diese Schaltfläche, um die Regel zu speichern.

Anmerkung: Es bringt in diesem Szenario keine Vorteile, wenn man in der Aussenstelle den ICA bzw. den VOIP-Traffic ein Maximum von 4096 gibt, da von der Zentrale aus ohnehin nur ein Maximum an 1024kbit zur Verfügung gestellt wird. Wichtig ist auf jedem Fall die Limitierung des Resttraffics auf 75% (3072 kbit), um einen Puffer für die VOIP- und ICA-Pakete bereit zu stellen.

Konfiguration speichern

1. Speichern Sie die Konfiguration auf einem USB-Stick oder auf der Harddisk.

Führen sie nun die gleiche Konfiguration auf der Gibraltar in der Aussenstelle 2 mit dem Bandbreitenwert 1024/1024 kbit durch. Damit kontrollieren Sie auf beiden Endpunkten den

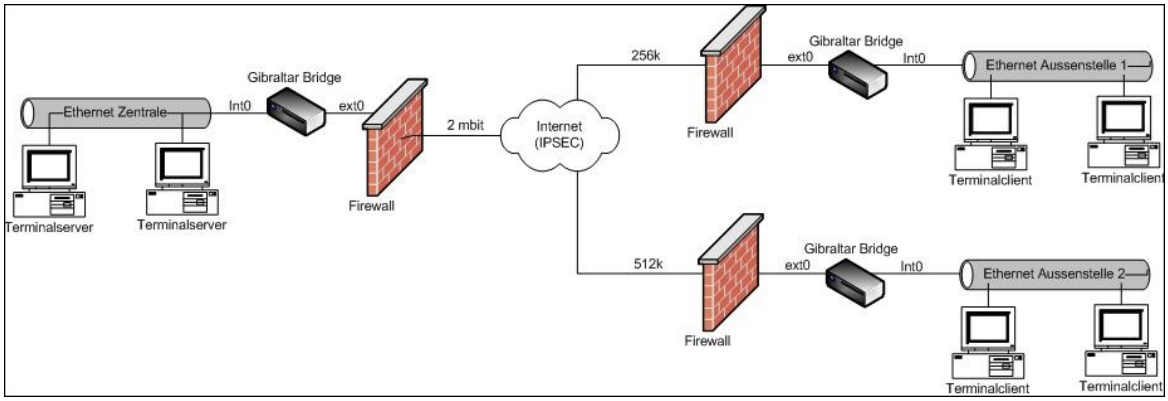
© 2008 by eSYS Informationssysteme GmbH

Verkehr und verhindert damit, dass zu große Druckjobs oder Downlaods ihre ICA-Sessions und Telefongespräche in Mitleidenschaft ziehen. Eine grafische Auswertung der Bandbreitenregulierung sehen Sie im Modul Monitoring.

7.8 Bandbreitenmanagement Citrix und VOIP mit VPN

Konfiguration von 3 Gibraltars die mittels IPSEC-VPN miteinander vernetzt werden.Weiters ist es Ziel dieses Szenarios ist es in einer Citrix-Terminalserverumgebung dem unternehmenskritische Protokoll ICA sowie dem VOIP-Traffic mindestens je 35% der verfügbaren Bandbreite zur Verfügung zu stellen. Dem restlichem Traffic wird aus Latenzgründen wie in Szenario 7 nur ein Maximum von 75 % gewährt. Folgende Ausgangssituation ist gegeben:

- Zentrale mit 4096/2048 Internetanbindung (192.168.0.0/24), IP-Telefonanlage: 192.168.0.100
- Aussenstelle1 mit 4096/1024 Internetanbindung (192.168.1.0/24), IP-Telefonanlage: 192.168.1.100
- Aussenstelle2 mit 1024/1024 Internetanbindung (192.168.2.0/24), IP-Telefonanlage: 192.168.2.100



Systemvoraussetzungen

PC mit zwei kompatiblen Netzwerkkarten oder Gibraltar Security Gateway.

IPSEC-VPN

Die Aussenstellen und die Zentrale gemäß Szenario 4 mittels IPSEC-VPN miteinander verbinden.

Netzwerk - Definitionen

1. Wählen Sie im Hauptmenü den Punkt **Netzwerk**.
2. Wählen Sie den Untermenüpunkt **Definitionen**.

© 2008 by eSYS Informationssysteme GmbH

3. Wählen Sie die Registerkarte **Host/Netz Aliases**.
4. Definieren Sie je einen Host/Netz Alias für die Aussenstelle 1 und die Aussenstelle 2 (z. B: "net1" für 192.168.1.0/24 und "net2" für 192.168.2.0/24).
5. Definieren Sie einen Host/Netz Alias "voip" für die Telefonanlage 192.168.0.100.
6. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

Um Bandbreitenmanagement zu ermöglichen müssen nun folgende Schritte unternommen werden:

- Definition der Bandbreiten der Interfaces
- Klassifizierung von Traffic für die Zuweisung zu Shaping Regeln
- Anlegen der Regeln, die dann die Regulierung vornehmen.

Traffic shaping

1. Wählen Sie im Hauptmenü den Punkt **Traffic shaping**.
2. Wählen Sie die Registerkarte **Allgemeine Einstellungen**.
3. **Bandbreiten:** Definieren Sie für das Interface "ext0" den Wert 2048 für Up- und 4096 für Download.
4. Wählen Sie für das Interface "int0" für Upload den Wert "4096" und für Download den Wert 2048.
5. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

Anmerkung: Wenn IPSEC im Spiel ist, dann sind einige Sonderfälle bei der Implementierung von Bandbreitenmanagement zu beachten. Würde man hier auf der Basis von "ext0" implementieren, so könnte Gibraltar nur ESP-verschlüsselte Pakete analysieren und somit natürlich keine Regulierung vornehmen. Die wieder entschlüsselten bzw. noch nicht verschlüsselten Pakete sind erst wieder auf dem internen Interface "int0" "sichtbar". Da Gibraltar für Outgoing-Tracks immer die definierte Upload-Bandbreite verwendet, gilt es bei dem internen Interface die Bandbreiten "verkehrt" anzulegen, damit man die Up- und Download-Bandbreiten genau widerspiegeln kann.

- "outgoing int0" = Download der Zentrale -> Pakete, die vom externen Interface an das interne gehen.
- "incoming int0" = Upload der Zentrale -> Pakete, die vom internen Interface an das externe gehen.

6. Wählen Sie die Registerkarte **Klassifizierung.**
7. **Klassifizierung hinzufügen:** Betätigen Sie diese Schaltfläche, um eine neue Klassifizierung für die ICA Quellports hinzuzufügen.
8. **Name:** Geben Sie hier einen Namen für die Klassifizierung (z.B: "icaSource").
9. **Quelladresse, Zieladresse:** Wählen Sie hier den Wert "ANY".
10. **Service:** Wählen Sie hier den Wert "ica_source".
11. **TOS:** Wählen Sie hier den Wert "Minimize Delay".
12. **Speichern:** Betätigen Sie diese Schaltfläche, um die Klassifizierung zu speichern.
13. **Abbrechen:** Betätigen Sie diese Schaltfläche, um zur Übersicht zu gelangen.
14. **Klassifizierung hinzufügen:** Betätigen Sie diese Schaltfläche, um eine neue Klassifizierung für die ICA Zielports hinzuzufügen.
15. **Name:** Geben Sie hier einen Namen für die Klassifizierung (z.B: "icaDest").
16. **Quelladresse, Zieladresse:** Wählen Sie hier den Wert "ANY".
17. **Service:** Wählen Sie hier den Wert "ica_destination".
18. **TOS:** Wählen Sie hier den Wert "Minimize Delay".
19. **Speichern:** Betätigen Sie diese Schaltfläche, um die Klassifizierung zu speichern.

© 2008 by eSYS Informationssysteme GmbH

20. **Abbrechen:** Betätigen Sie diese Schaltfläche, um zur Übersicht zu gelangen.
21. **Klassifizierung hinzufügen:** Betätigen Sie diese Schaltfläche, um eine neue Klassifizierung für die Quellpakete der Telefonanlage hinzuzufügen.
22. **Name:** Geben Sie hier einen Namen für die Klassifizierung (z.B: "voipSource").
23. **Quelladresse:** Wählen Sie hier die Definition "voip".
24. **Zieladresse:** Wählen Sie hier den Wert "ANY".
25. **TOS:** Wählen Sie hier den Wert "Minimize Delay".
26. **Speichern:** Betätigen Sie diese Schaltfläche, um die Klassifizierung zu speichern.
27. **Abbrechen:** Betätigen Sie diese Schaltfläche, um zur Übersicht zu gelangen.
28. **Klassifizierung hinzufügen:** Betätigen Sie diese Schaltfläche, um eine neue Klassifizierung für die Zielpakete der Telefonanlage hinzuzufügen.
29. **Name:** Geben Sie hier einen Namen für die Klassifizierung (z.B: "voipDest").
30. **Quelladresse:** Wählen Sie hier den Wert ANY.
31. **Zieladresse:** Wählen Sie hier die Definition "voip".
32. **TOS:** Wählen Sie hier den Wert "Minimize Delay".
33. **Speichern:** Betätigen Sie diese Schaltfläche, um die Klassifizierung zu speichern.
34. **Abbrechen:** Betätigen Sie diese Schaltfläche, um zur Übersicht zu gelangen.
35. **Klassifizierung hinzufügen:** Betätigen Sie diese Schaltfläche, um eine neue Klassifizierung für den ICMP Traffic hinzuzufügen.
36. **Name:** Geben Sie hier einen Namen für die Klassifizierung (z.B: "icmp").
37. **Service:** Wählen Sie hier den Wert "CUSTOM".
38. **Protokoll:** Wählen Sie hier den Wert "ICMP".
39. **TOS:** Wählen Sie hier den Wert "Minimize Delay".
40. **Speichern:** Betätigen Sie diese Schaltfläche, um die Klassifizierung zu speichern.
41. **Abbrechen:** Betätigen Sie diese Schaltfläche, um zur Übersicht zu gelangen.
42. **Klassifizierung hinzufügen:** Betätigen Sie diese Schaltfläche, um eine neue Klassifizierung für den restlichen Traffic hinzuzufügen.
43. **Name:** Geben Sie hier einen Namen für die Klassifizierung (z.B: "rest").
44. **Quelladresse, Zieladresse:** Wählen Sie hier den Wert "ANY".
45. **Speichern:** Betätigen Sie diese Schaltfläche, um die Klassifizierung zu speichern.

Um den gesamten ICA-Traffic und auch ICMP gemeinsam priorisieren zu können, müssen die Klassifizierungen zu einer Gruppe zusammengefasst werden. Weiters werden auch die Quell- und Zielpakete der Telefonanlage zu einer Gruppe zusammengefasst.

1. Wählen Sie die Registerkarte **Klassifizierungsgruppen**.
2. **Gruppe hinzufügen:** Betätigen Sie diese Schaltfläche, um eine neue Klassifizierungsgruppe hinzuzufügen.
3. **Name:** Geben Sie hier einen Namen für die Gruppe ein (z.B: "ica").
4. **Mitglied hinzufügen:** Wählen Sie hier die Mitglieder "icaSource", "icaDest" und "icmp".
5. **Speichern:** Betätigen Sie diese Schaltfläche, um die Gruppe zu speichern.
6. **Abbrechen:** Betätigen Sie diese Schaltfläche, um zur Übersicht zu gelangen.
7. **Gruppe hinzufügen:** Betätigen Sie diese Schaltfläche, um eine neue Klassifizierungsgruppe hinzuzufügen.
8. **Name:** Geben Sie hier einen Namen für die Gruppe ein (z.B: "voip").
9. **Mitglied hinzufügen:** Wählen Sie hier die Mitglieder "voipSource", "voipDest".
10. **Speichern:** Betätigen Sie diese Schaltfläche, um die Gruppe zu speichern.

Zum Abschluss müssen noch die Regeln für die beiden Aussenstellen gesetzt werden. Diese Regeln nehmen nun die Bandbreitenregulierung vor. Zuerst regulieren wir den Upload der Zentrale - dies ist aus Sicht der Gibraltar nun der Track "incoming int0".

© 2008 by eSYS Informationssysteme GmbH

1. Wählen Sie die Registerkarte **Traffic Shaping Regeln**.
2. **Track:** Wählen Sie "incoming int0". Gibraltar verwendet nun die definierte Download-Bandbreite des Interfaces "int0". Dieser Traffic stellt den Upload der Zentrale dar!
3. **Regel hinzufügen:** Klicken Sie diesen Button, um eine neue Shaping Regel hinzuzufügen.
4. **Name:** Vergeben Sie einen Namen für die Regel (z.B: "ruleNet1"). Sie können die Wirkungsweise dieser Regel im Modul Monitoring gezielt analysieren.
5. **Mitglied hinzufügen:** Klicken Sie diesen Button, um Klassifizierungen bzw. Klassifizierungsgruppen hinzuzufügen.
6. Wählen Sie die Klassifizierungsgruppe "ica" und vergeben Sie die Werte "360" für Min und "1024" für Max.
7. Wählen Sie die Klassifizierungsgruppe "voip" und vergeben Sie die Werte "360" für Min und "1024" für Max.
8. Wählen Sie die Klassifizierung "rest" und vergeben Sie die Werte "250" für Min und "768" für Max.
9. **Speichern:** Betätigen Sie diese Schaltfläche, um die Regel zu speichern.
10. Wählen Sie die Registerkarte **Fortgeschritten**.
11. **Zieladresse:** Wählen Sie die Definition "net1", da diese Regel nur für dieses Zielnetz gelten soll
12. **Bandbreite (kbit) für Netze:** Wählen Sie den Wert "1024", da wir für dieses Netz nur ein Maximum von 1024kbit zur Verfügung stellen. Der gesamte Traffic, der von der Zentrale in dieses Netz läuft, darf somit 1024kbit nicht übersteigen.
13. **Speichern:** Betätigen Sie diese Schaltfläche, um die Regel zu speichern.
14. **Abbrechen:** Betätigen Sie diese Schaltfläche, um zur Übersicht zu gelangen.
15. **Regel hinzufügen:** Klicken Sie diesen Button, um eine neue Shaping Regel hinzuzufügen.
16. **Name:** Vergeben Sie einen Namen für die Regel (z.B: "ruleNet2")
17. **Mitglied hinzufügen:** Klicken Sie diesen Button, um Klassifizierungen bzw. Klassifizierungsgruppen hinzuzufügen.
18. Wählen Sie die Klassifizierungsgruppe "ica" und vergeben Sie die Werte "360" für Min und "1024" für Max.
19. Wählen Sie die Klassifizierungsgruppe "voip" und vergeben Sie die Werte "360" für Min und "1024" für Max.
20. Wählen Sie die Klassifizierung "rest" und vergeben Sie die Werte "250" für Min und "768" für Max.
21. **Speichern:** Betätigen Sie diese Schaltfläche, um die Regel zu speichern.
22. Wählen Sie die Registerkarte **Fortgeschritten**.
23. **Zieladresse:** Wählen Sie die Definition "net2", da diese Regel nur für dieses Zielnetz gelten soll
24. **Bandbreite (kbit) für Netze:** Wählen Sie den Wert "1024", da wir für dieses Netz nur ein Maximum von 1024kbit zur Verfügung stellen. Der gesamte Traffic, der von der Zentrale in dieses Netz läuft, darf somit 1024kbit nicht übersteigen.
25. **Speichern:** Betätigen Sie diese Schaltfläche, um die Regel zu speichern.

Anmerkung
Um den ganzen Traffic unter Kontrolle zu bringen ist es natürlich auch notwendig, dass der Download-Traffic in der Zentrale reguliert wird. Wäre dies nicht der Fall, dann könnte ein massiver Download in der Zentrale die Upload-Pakete aus den Aussenstellen blockieren.

© 2008 by eSYS Informationssysteme GmbH

1. Wählen Sie die Registerkarte **Traffic Shaping Regeln**.
2. **Track:** Wählen Sie "outgoing int0". Gibraltar verwendet nun die definierte Upload Bandbreite des Interfaces "int0". Dieser Traffic stellt den Download der Zentrale dar!
3. **Regel hinzufügen:** Klicken Sie diesen Button, um eine neue Shaping Regel hinzuzufügen.
4. **Name:** Vergeben Sie einen Namen für die Regel (z.B: "ruleDownload"). Sie können die Wirkungsweise dieser Regel im Modul Monitoring gezielt analysieren.
5. **Mitglied hinzufügen:** Klicken Sie diesen Button, um Klassifizierungen bzw. Klassifizierungsgruppen hinzuzufügen.
6. Wählen Sie die Klassifizierungsgruppe "ica" und vergeben Sie die Werte "1432" für Min und "4096" für Max.
7. Wählen Sie die Klassifizierungsgruppe "voip" und vergeben Sie die Werte "1432" für Min und "4096" für Max.
8. Wählen Sie die Klassifizierung "rest" und vergeben Sie die Werte "1000" für Min und "3072" für Max.
9. **Speichern:** Betätigen Sie diese Schaltfläche, um die Regel zu speichern.

Anmerkung: Da wir beim Download-Shaping nicht gezielt ein Netz regulieren wollen, ist es hier nicht notwendig, auf der Registerkarte "Erweitert" eine Zieladresse zu definieren!

Sonderfall Gibraltar mit Mail Relay bzw. Proxy

Sollten Sie Gibraltar in diesem Szenario nun auch als Mail-Relay bzw. HTTP, FTP oder POP3-Proxy verwenden, dann tritt folgender Sonderfall ein: Mit den Regeln auf "outgoing int" und "incoming int" regulieren wir bereits den Upload und Download-Traffic vom bzw. ins interne Netz. Fungiert Gibraltar jedoch als Mail-Relay bzw. Proxy, so "produziert" die Firewall selber ja auch Up- und Download Traffic, der bis zu diesem Zeitpunkt noch nicht reguliert wird. Gehen Sie in diesem Spezialfall folgendermaßen vor:

1. Wählen Sie die Registerkarte **Klassifizierung**.
2. **Klassifizierung hinzufügen:** Betätigen Sie diese Schaltfläche, um eine neue Klassifizierung für IPSEC hinzuzufügen. Es ist das Ziel, IPSEC-Traffic ein Maximum von 100% zu geben, da innerhalb dieses IPSEC-Traffics ja die ICA- und VOIP-Pakete verschlüsselt sind!
3. **Name:** Geben Sie hier einen Namen für die Klassifizierung (z.B: "ipsec").
4. **Quelladresse, Zieladresse:** Wählen Sie hier den Wert "ANY".
5. **Service:** Wählen Sie hier den Wert "ipsec".
6. **Speichern:** Betätigen Sie diese Schaltfläche, um die Klassifizierung zu speichern.
7. **Abbrechen:** Betätigen Sie diese Schaltfläche, um zur Übersicht zu gelangen.
8.  : Klicken Sie diesen Button um die Klassifizierung "ipsec" vor der "rest" Klassifizierung zu platzieren.
9. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderung der Reihenfolge zu speichern.
10. Wählen Sie die Registerkarte **Traffic Shaping Regeln**.
11. **Track:** Wählen Sie "incoming ext0". Gibraltar verwendet nun die definierte Download Bandbreite des Interfaces "ext0". Dieser Traffic stellt den Download der Zentrale UND den Traffic dar, den Gibraltar selber durch die Proxies produziert!
12. **Regel hinzufügen:** Klicken Sie diesen Button, um eine neue Shaping Regel hinzuzufügen.
13. **Name:** Vergeben Sie einen Namen für die Regel (z.B: "limitGibDownload"). Sie können die Wirkungsweise dieser Regel im Modul Monitoring gezielt analysieren.
14. **Mitglied hinzufügen:** Klicken Sie diesen Button, um Klassifizierungen bzw.

© 2008 by eSYS Informationssysteme GmbH

Klassifizierungsgruppen hinzuzufügen.
15. Wählen Sie die Klassifizierungsgruppe "ipsec" und vergeben Sie die Werte "2864" für Min und "4096" für Max.
16. Wählen Sie die Klassifizierung "rest" und vergeben Sie die Werte "1000" für Min und "3072" für Max.
17. **Speichern:** Betätigen Sie diese Schaltfläche, um die Regel zu speichern.
18. Wählen Sie die Registerkarte **Traffic Shaping Regeln**.
19. **Track:** Wählen Sie "outgoing ext0". Gibraltar verwendet nun die definierte Upload Bandbreite des Interfaces "ext0". Dieser Traffic stellt den Upload der Zentrale UND den Traffic dar, den Gibraltar selber durch die Proxies produziert!
20. **Regel hinzufügen:** Klicken Sie diesen Button, um eine neue Shaping Regel hinzuzufügen.
21. **Name:** Vergeben Sie einen Namen für die Regel (z.B: "limitGibUpload"). Sie können die Wirkungsweise dieser Regel im Modul Monitoring gezielt analysieren.
22. **Mitglied hinzufügen:** Klicken Sie diesen Button, um Klassifizierungen bzw. Klassifizierungsgruppen hinzuzufügen.
23. Wählen Sie die Klassifizierungsgruppe "ipsec" und vergeben Sie die Werte "720" für Min und "1024" für Max.
24. Wählen Sie die Klassifizierung "rest" und vergeben Sie die Werte "250" für Min und "768" für Max.
25. **Speichern:** Betätigen Sie diese Schaltfläche, um die Regel zu speichern.

Damit ist nun auch sichergestellt, dass große Mails bzw. Proxy-Downloads die Latenzzeiten der unternehmenskritischen Protokolle nicht belasten!

Konfiguration speichern

1. Speichern Sie die Konfiguration auf einem USB-Stick oder auf der Harddisk.

Damit wird nun der Verkehr in die beiden Aussenstellen anhand den verschiedenen Bandbreiten reguliert. Ein Druckjob von der Zentrale in die Aussenstellen, der bspw. nicht im ICA-Strom enthalten ist, würde nun kein Problem mehr verursachen. Um auch den ausgehenden Verkehr der Aussenstellen zu kontrollieren sind folgende Konfigurationsschritte nötig (Netzwerk- und Systemeinstellungen gleich wie in Zentrale):

Netzwerk - Definitionen

1. Wählen Sie im Hauptmenü den Punkt **Netzwerk**.
2. Wählen Sie den Untermenüpunkt **Definitionen**.
3. Wählen Sie die Registerkarte **Host/Netz Aliases**.
4. Definieren Sie einen Host/Netz Alias "voip" für die Telefonanlage 192.168.0.100.
5. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

Traffic shaping (Aussenstelle 1)

1. Wählen Sie im Hauptmenü den Punkt **Traffic shaping**.
2. Wählen Sie die Registerkarte **Allgemeine Einstellungen**.
3. **Bandbreiten:** Definieren Sie für das Interface "ext0" den Wert "1024" für den Upload sowie den Wert "4096" für Download.
4. Wählen Sie für das Interface "int0" für Upload den Wert "4096" und für Download den Wert 1024.
5. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

© 2008 by eSYS Informationssysteme GmbH

6. Legen Sie nun die Klassifizierungen und Klassifizierungsgruppen genau so, wie in der Zentrale an.
7. Wählen Sie die Registerkarte **Traffic Shaping Regeln**.
8. **Track:** Wählen Sie "incoming int0". Gibraltar verwendet nun die definierte Download-Bandbreite des Interfaces "int0". Dieser Traffic stellt den Upload der Aussenstelle dar.
9. **Regel hinzufügen:** Klicken Sie diesen Button, um eine neue Shaping Regel hinzuzufügen.
10. **Name:** Vergeben Sie einen Namen für die Regel (z.B: "ruleUpload")
11. **Mitglied hinzufügen:** Klicken Sie diesen Button, um Klassifizierungen bzw. Klassifizierungsgruppen hinzuzufügen.
12. Wählen Sie die Klassifizierungsgruppe "ica" und vergeben Sie die Werte "360" für Min und "1024" für Max.
13. Wählen Sie die Klassifizierungsgruppe "voip" und vergeben Sie die Werte "360" für Min und "1024" für Max.
14. Wählen Sie die Klassifizierung "rest" und vergeben Sie die Werte "250" für Min und "768" für Max.
15. **Speichern:** Betätigen Sie diese Schaltfläche, um die Regel zu speichern.

Auch in der Aussenstelle ist es wichtig, den Download Traffic zu regulieren. Gehen Sie dafür folgendermaßen vor:

1. Wählen Sie die Registerkarte **Traffic Shaping Regeln**.
2. **Track:** Wählen Sie "outgoing int0". Gibraltar verwendet nun die definierte Upload-Bandbreite des Interfaces "int0". Dieser Traffic stellt den Download der Aussenstelle dar.
3. **Regel hinzufügen:** Klicken Sie diesen Button, um eine neue Shaping Regel hinzuzufügen.
4. **Name:** Vergeben Sie einen Namen für die Regel (z.B: "ruleDownload")
5. **Mitglied hinzufügen:** Klicken Sie diesen Button, um Klassifizierungen bzw. Klassifizierungsgruppen hinzuzufügen.
6. Wählen Sie die Klassifizierungsgruppe "ica" und vergeben Sie die Werte "360" für Min und "1024" für Max.
7. Wählen Sie die Klassifizierungsgruppe "voip" und vergeben Sie die Werte "360" für Min und "1024" für Max.
8. Wählen Sie die Klassifizierung "rest" und vergeben Sie die Werte "2000" für Min und "3072" für Max.
9. **Speichern:** Betätigen Sie diese Schaltfläche, um die Regel zu speichern.

Anmerkung: Es bringt in diesem Szenario keine Vorteile, wenn man in der Aussenstelle den ICA bzw. den VOIP-Traffic ein Maximum von 4096 gibt, da von der Zentrale aus ohnehin nur ein Maximum an 1024kbit zur Verfügung gestellt wird. Wichtig ist auf jedem Fall die Limitierung des Resttraffics auf 75% (3072 kbit), um einen Puffer für die VOIP- und ICA-Pakete bereit zu stellen.

Konfiguration speichern

1. Speichern Sie die Konfiguration auf einem USB-Stick oder auf der Harddisk.

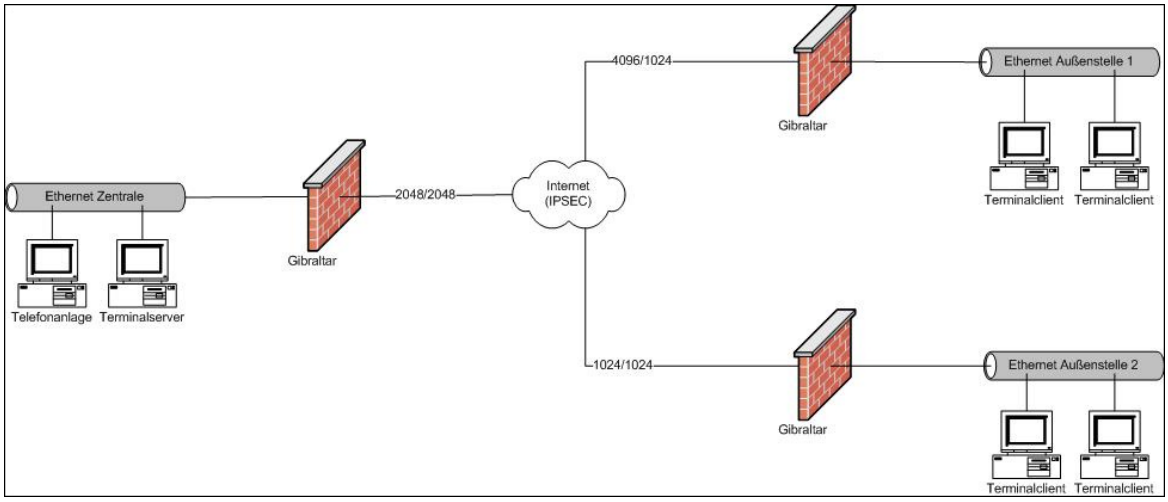
Führen sie nun die gleiche Konfiguration auf der Gibraltar in der Aussenstelle 2 mit dem Bandbreitenwert 1024/1024 kbit durch. Damit kontrollieren Sie auf beiden Endpunkten den

© 2008 by eSYS Informationssysteme GmbH

Verkehr und verhindert damit, dass zu große Druckjobs oder Downlaods ihre ICA-Sessions und Telefongespräche in Mitleidenschaft ziehen. Eine grafische Auswertung der Bandbreitenregulierung sehen Sie im Modul Monitoring.

7.9 Bandbreitenmanagement VoIP

Konfiguration von Gibraltar zur Sicherstellung einer minimalen Bandbreite für eine interne VOIP-Telefonanlage mit der IP 192.168.0.40. Ziel dieses Szenarios ist es, der internen Telefonanlage eine Minimalbandbreite von 1 Mbit Download und 512 kb Upload zur Verfügung zu stellen. Die Internetanbindung stellt eine Bandbreite von 2048 Download und 1024 Upload zur Verfügung. Weiters wird dem restlichem Traffic aus Latenzgründen eine Bandbreite von maximal 75 % ermöglicht. Dies ist bei latenzkritischen Anwendungen wie VOIP und Terminalservertechnologien unumgänglich, sollte der Provider nicht auf gesetzte TOS-Bits reagieren (dies ist im Regelfall auch so). Zur Gewährleistung einer ordnungsgemäßen Funktionalität dürfen **maximal 95 %** der verfügbaren Bandbreite verwendet werden!



Systemvoraussetzungen

PC mit zwei kompatiblen Netzwerkkarten oder Gibraltar Security Gateway.

Installation von Gibraltar

Installieren sie Gibraltar wie im Kapitel Installation beschrieben.

Systemeinstellungen

Systemeinstellungen wie in Szenario 1

Netzwerkeinstellungen - Netzwerkkarte

Netzwerk- sowie Routingeinstellungen wie in Szenario 2

© 2008 by eSYS Informationssysteme GmbH

ACHTUNG: Durch das Verändern der IP-Adresse auf der Netzwerkkarte, über die Sie auf Gibraltar zugreifen, wird die Verbindung unterbrochen und Sie müssen für Ihren Arbeitsplatzrechner ebenfalls die IP-Adresse anpassen.

Firewallregeln

Firewallregeln wie in Szenario 2

Netzwerk - Definitionen

1. Wählen Sie im Hauptmenü den Punkt **Netzwerk**.
2. Wählen Sie den Untermenüpunkt **Definitionen**.
3. Wählen Sie die Registerkarte **Host/Netz Aliases**.
4. Definieren Sie einen Host/Netz Alias mit dem Namen "voipHost" für die IP-Adresse 192.168.0.40.
5. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

Um Bandbreitenmanagement zu ermöglichen müssen nun folgende Schritte unternommen werden:

- Definition der Bandbreiten der Interfaces
- Klassifizierung von Traffic für die Zuweisung zu Shaping Regeln
- Anlegen der Regeln, die dann die Regulierung vornehmen.

Traffic shaping

1. Wählen Sie im Hauptmenü den Punkt **Traffic shaping**.
2. Wählen Sie die Registerkarte **Allgemeine Einstellungen**.
3. **Bandbreiten:** Definieren Sie für das Interface "ext0" den Wert "2048" für den Download und "1024" für den Upload.
4. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.
5. Wählen Sie die Registerkarte **Klassifizierung.**
6. **Klassifizierung hinzufügen:** Betätigen Sie diese Schaltfläche, um eine neue Klassifizierung für die Quelladresse der VOIP-Telefonanlage hinzuzufügen.
7. **Name:** Geben Sie hier einen Namen für die Klassifizierung (z.B: "voipSource").
8. **Quelladresse:** Wählen Sie hier den Wert "voipHost".
9. **Zieladresse:** Wählen Sie hier den Wert "ANY".
10. **TOS:** Wählen Sie hier den Wert "Minimize Delay".
11. **Speichern:** Betätigen Sie diese Schaltfläche, um die Klassifizierung zu speichern.
12. **Klassifizierung hinzufügen:** Betätigen Sie diese Schaltfläche, um eine neue Klassifizierung für die Zieladresse der VOIP-Telefonanlage hinzuzufügen.
13. **Name:** Geben Sie hier einen Namen für die Klassifizierung (z.B: "voipDest").
14. **Quelladresse:** Wählen Sie hier den Wert "ANY".
15. **Zieladresse:** Wählen Sie hier den Wert "voipHost".
16. **TOS:** Wählen Sie hier den Wert "Minimize Delay".
17. **Speichern:** Betätigen Sie diese Schaltfläche, um die Klassifizierung zu speichern.
18. **Klassifizierung hinzufügen:** Betätigen Sie diese Schaltfläche, um eine neue Klassifizierung für den ICMP Traffic hinzuzufügen.
19. **Name:** Geben Sie hier einen Namen für die Klassifizierung (z.B: "icmp").
20. **Service:** Wählen Sie hier den Wert "CUSTOM".
21. **Protokoll:** Wählen Sie hier den Wert "ICMP".
22. **Speichern:** Betätigen Sie diese Schaltfläche, um die Klassifizierung zu speichern.
23. **Klassifizierung hinzufügen:** Betätigen Sie diese Schaltfläche, um eine neue

© 2008 by eSYS Informationssysteme GmbH

Klassifizierung für den restlichen Traffic hinzuzufügen.
24. **Name:** Geben Sie hier einen Namen für die Klassifizierung (z.B: "rest").
25. **Quelladresse, Zieladresse:** Wählen Sie hier den Wert "ANY".
26. **Speichern:** Betätigen Sie diese Schaltfläche, um die Klassifizierung zu speichern.

Um den gesamten VOIP-Traffic und auch ICMP gemeinsam priorisieren zu können, müssen die Klassifizierungen zu einer Gruppe zusammengefasst werden.

1. Wählen Sie die Registerkarte **Klassifizierungsgruppen**.
2. **Gruppe hinzufügen:** Betätigen Sie diese Schaltfläche, um eine neue Klassifizierungsgruppe für die VOIP-Hosts und "icmp" hinzuzufügen.
3. **Name:** Geben Sie hier einen Namen für die Gruppe ein (z.B: "highPrio").
4. **Mitglied hinzufügen:** Wählen Sie hier die Mitglieder "voipSource", "voipDest" und "icmp".
5. **Speichern:** Betätigen Sie diese Schaltfläche, um die Gruppe zu speichern.

Nun müssen die Shaping Regeln für die Minimalbandbreiten erstellt werden.

1. Wählen Sie die Registerkarte **Traffic Shaping Regeln**.
2. **Track:** Wählen Sie "incoming ext0", um eingehenden Traffic ins interne Netzwerk zu shapen.
3. **Regel hinzufügen:** Klicken Sie diesen Button, um eine neue Shaping Regel hinzuzufügen.
4. **Name:** Vergeben Sie einen Namen für die Regel (z.B: "ruleDownload")
5. **Mitglied hinzufügen:** Klicken Sie diesen Button, um Klassifizierungen bzw. Klassifizierungsgruppen hinzuzufügen.
6. Wählen Sie die Klassifizierungsgruppe "highPrio" und vergeben Sie die Werte "1024" für Min und "2048" für Max.
7. **Mitglied hinzufügen:** Klicken Sie diesen Button, um Klassifizierungen bzw. Klassifizierungsgruppen hinzuzufügen.
8. Wählen Sie die Klassifizierung "rest" und vergeben Sie die Werte "800" für Min und "1536" für Max.
9. **Speichern:** Betätigen Sie diese Schaltfläche, um die Regel zu speichern.
10. **Regel hinzufügen:** Klicken Sie diesen Button, um eine neue Shaping Regel hinzuzufügen.
11. **Track:** Wählen Sie "outgoing ext", um ausgehenden Traffic zu shapen.
12. **Name:** Vergeben Sie einen Namen für die Regel (z.B: "ruleUpload")
13. **Mitglied hinzufügen:** Klicken Sie diesen Button, um Klassifizierungen bzw. Klassifizierungsgruppen hinzuzufügen.
14. Wählen Sie die Klassifizierungsgruppe "highPrio" und vergeben Sie die Werte "512" für Min und "1024" für Max
15. **Mitglied hinzufügen:** Klicken Sie diesen Button, um Klassifizierungen bzw. Klassifizierungsgruppen hinzuzufügen.
16. Wählen Sie die Klassifizierung "rest" und vergeben Sie die Werte "450" für Min und "768" für Max.
17. **Speichern:** Betätigen Sie diese Schaltfläche, um die Regel zu speichern.

Konfiguration speichern

1. Speichern Sie die Konfiguration auf einem USB-Stick oder auf der Harddisk.

Es wird nun Ihrer Telefonanlage im Bedarfsfall immer eine Minimalbandbreite von 1Mbit

© 2008 by eSYS Informationssysteme GmbH

Download und 512kbit Upload zur Verfügung gestellt. Sollten Sie Probleme in der Sprachqualität feststellen, so adaptieren Sie bitte die Werte der Klassifizierung "rest" in den Regeln nach unten. Eine detaillierte Auswertung Ihres Bandbreitenmanagements sehen Sie im Monitoring.

7.10 Bandbreitenmanagement Web Traffic

Konfiguration von Gibraltar zur Sicherstellung einer minimalen Bandbreite für Web Traffic (HTTP, HTTPS). Weiters soll auch für das Abrufen von Emails über POP3 eine minimale Bandbreite zur Verfügung gestellt werden. Für diese Dienste soll eine Minimalbandbreite von 1024 kbit zur Verfügung gestellt werden. Die Gesamtbandbreite beträgt 2048 kbit. (Up und Download). Da diese Dienste keine latenzkritischen Anwendungen sind, ist es nicht erforderlich den Resttraffic auf 75% der Bandbreite zu beschränken.

Systemvoraussetzungen

PC mit zwei kompatiblen Netzwerkkarten oder Gibraltar Security Gateway.

Installation von Gibraltar

Installieren sie Gibraltar wie im Kapitel Installation beschrieben.

Systemeinstellungen

Systemeinstellungen wie in Szenario 1

Netzwerkeinstellungen - Netzwerkkarte

Netzwerk- sowie Routingeinstellungen wie in Szenario 2

ACHTUNG: Durch das Verändern der IP-Adresse auf der Netzwerkkarte, über die Sie auf Gibraltar zugreifen, wird die Verbindung unterbrochen und Sie müssen für Ihren Arbeitsplatzrechner ebenfalls die IP-Adresse anpassen.

Firewallregeln

Firewallregeln wie in Szenario 2

Traffic shaping

1. Wählen Sie im Hauptmenü den Punkt **Traffic shaping**.
2. Wählen Sie die Registerkarte **Allgemeine Einstellungen**.
3. **Bandbreiten:** Definieren Sie für das Interface "ext0" den Wert "2048" für den Upload und den Download.
4. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.
5. Wählen Sie die Registerkarte **Klassifizierung.**
6. **Klassifizierung hinzufügen:** Betätigen Sie diese Schaltfläche, um eine neue Klassifizierung für den Web-Traffic .
7. **Name:** Geben Sie hier einen Namen für die Klassifizierung (z.B: "web").
8. **Quelladresse:** Wählen Sie hier den Wert "ANY".
9. **Zieladresse:** Wählen Sie hier den Wert "ANY".

© 2008 by eSYS Informationssysteme GmbH

10. **Service:** Wählen Sie hier den Wert "web".
11. **Speichern:** Betätigen Sie diese Schaltfläche, um die Klassifizierung zu speichern.
12. **Klassifizierung hinzufügen:** Betätigen Sie diese Schaltfläche, um eine neue Klassifizierung für den Web-Traffic .
13. **Name:** Geben Sie hier einen Namen für die Klassifizierung (z.B: "pop3").
14. **Quelladresse:** Wählen Sie hier den Wert "ANY".
15. **Zieladresse:** Wählen Sie hier den Wert "ANY".
16. **Service:** Wählen Sie hier den Wert "pop3".
17. **Speichern:** Betätigen Sie diese Schaltfläche, um die Klassifizierung zu speichern.

Nun müssen wir diese beiden Definitionen zu einer Gruppe zusammenfügen

1. Wählen Sie die Registerkarte **Klassifizierungsgruppen**.
2. **Gruppe hinzufügen:** Betätigen Sie diese Schaltfläche, um eine neue Klassifizierungsgruppe hinzuzufügen.
3. **Name:** Geben Sie hier einen Namen für die Gruppe ein (z.B: "groupWeb").
4. **Mitglied hinzufügen:** Wählen Sie hier die Mitglieder "pop3" und "web".
5. **Speichern:** Betätigen Sie diese Schaltfläche, um die Gruppe zu speichern.
6. **Abbrechen:** Betätigen Sie diese Schaltfläche, um zur Übersicht zu gelangen.
7.

Nun müssen die Shaping Regeln für die Minimalbandbreiten erstellt werden.

1. Wählen Sie die Registerkarte **Traffic Shaping Regeln**.
2. **Track:** Wählen Sie "incoming ext", um eingehenden Traffic zu shapen.
3. **Regel hinzufügen:** Klicken Sie diesen Button, um eine neue Shaping Regel hinzuzufügen.
4. **Name:** Vergeben Sie einen Namen für die Regel (z.B: "ruleDownload")
5. **Mitglied hinzufügen:** Klicken Sie diesen Button, um Klassifizierungen bzw. Klassifizierungsgruppen hinzuzufügen.
6. Wählen Sie die Klassifizierungsgruppe "groupWeb" und vergeben Sie die Werte "1024 " für Min und "2048" für Max.
7. **Speichern:** Betätigen Sie diese Schaltfläche, um die Regel zu speichern.

Damit ist sichergestellt, dass für HTTP, HTTPS und POP3-Traffic die Minimalbandbreiten von 1024 kbit zur Verfügung gestellt sind.

Konfiguration speichern

1. Speichern Sie die Konfiguration auf einem USB-Stick oder auf der Harddisk.

8 Konfiguration

Bevor Sie mit der Konfiguration von Gibraltar mittels **GibADMIN** beginnen, werden wir Ihnen einen kurzen Überblick über regelmäßig verwendete Bedienungselemente geben. Grundsätzlich ist zu erwähnen, dass die Schaltflächen **Vorwärts** und **Zurück** des Browsers bei der Navigation durch den **GibADMIN** nicht verwendet werden sollten. Werden diese dennoch verwendet und anschließend eine Schaltfläche im **GibADMIN** betätigt, wird eine entsprechende Hinweismeldung angezeigt.

Verknüpfung

Eine Verknüpfung bezeichnet eine Weiterleitung zu einer anderen Seite im **GibADMIN** und verhält sich genauso wie ein Link auf eine andere HTML Seite. Verknüpfungen finden Sie zB

© 2008 by eSYS Informationssysteme GmbH

links im Hauptmenü.

Schaltflächen

Durch das Betätigen einer Schaltfläche wird ein Befehl im Hintergrund ausgeführt, der je nach Bedeutung der Schaltfläche zum Beispiel die von Ihnen durchgeführten Änderungen im Formular speichert. Es ist auch möglich, dass Sie durch die Betätigung einer Schaltfläche auf ein anderes Formular im **GibADMIN** weitergeleitet werden, ähnlich einer Verknüpfung. Schaltflächen müssen immer nach einer Eingabe oder Veränderung im Webformular betätigt werden, damit die Eingaben auch korrekt verarbeitet werden.

Kontexthilfe: Lädt den entsprechenden Abschnitt der Online Hilfe. Diese Schaltfläche finden Sie in der Titelleiste jedes Moduls.

Nach oben reihen: Verschiebt die Zeile einer Liste einen Eintrag nach oben. Diese Funktion wird bei Listen verwendet, bei denen die Reihenfolge von Bedeutung ist. Nach dem Verschieben einer Zeile müssen Sie die Schaltfläche **Speichern** betätigen, damit die Änderungen wirksam werden.

Nach unten reihen: Verschiebt die Zeile einer Liste einen Eintrag nach unten. Diese Funktion wird bei Listen verwendet, bei denen die Reihenfolge von Bedeutung ist. Nach dem Verschieben einer Zeile müssen Sie die Schaltfläche **Speichern** betätigen, damit die Änderungen wirksam werden.

Löschen: Löscht einen Eintrag aus einer Liste. Durch die anschließende Betätigung der Schaltfläche **Speichern** werden die Einträge dauerhaft gelöscht und die Konfigurationsdatei neu erstellt.

Eintrag bearbeiten: Bearbeitet einen Listeneintrag im Bearbeitungsmodus.

Einfügen: Fügt einen neuen Listeneintrag unterhalb des gewählten Eintrags ein.

Info: Zeigt einen kurzen Informationstext in einem gelben Kästchen.

Starten: Diese Schaltfläche dient zum Starten von Diensten und Geräten.

Stoppen: Diese Schaltfläche dient zum Stoppen von Diensten und Geräten.

Standby: Durch das Betätigen dieser Schaltfläche wechseln Sie in den Standby Modus. Im Standby Modus befinden sich zum Beispiel IPSec-Tunnel Endpunkte, die auf einen Aufbau des Tunnels von außen warten.

E-Mail: Öffnet ein E-Mail-Formular

Download: Herunterladen der entsprechenden Datei.

CIDR - Classless Inter Domain Routing

GibADMIN verwendet zur Angabe von IP-Adressen in Verbindung mit den Subnetzmasken die CIDR Notation.
Eine CIDR Adresse enthält neben der Standard 32-Bit IP-Adresse auch Informationen darüber, wie viele Bits für die Identifikation des Netzwerks verwendet werden. Beispielsweise zeigt in der CIDR Adresse 192.168.0.1/24 der Wert „/24" an, das die ersten 24 Bit der Adresse für die Identifizierung des Netzwerks verwendet werden. Die restlichen Bits identifizieren den einzelnen Rechner. Die letzte gültige Adresse dieses Netzwerks ist somit 192.168.0.254/24.
Der CIDR Block, das ist der Wert mit dem Schrägstrich, kann Werte von /13 bis /27 annehmen.

Einige Beispiele:

© 2008 by eSYS Informationssysteme GmbH

CIDR-Block	Anzahl entsprechender Klasse C Netzwerke	Anzahl der möglichen Rechner
/27	1/8 eines Klasse C Netzes	32
/25	1/2 Klasse C Netz	128
/24	1 Klasse C Netz	256
/16	256 Klasse C Netze	65536
/13	2048 Klasse C Netze	524288

255.255.0.0 entspricht /16.
255.255.255.0 entspricht /24.
255.255.255.192 entspricht /26.

8.1 Lizenzinformation

Gibraltar benötigt zum Betrieb eine gültige Lizenzdatei. Sie erhalten Ihre Lizenzdatei beim Kauf von Gibraltar. Auf den Gibraltar Security Gateways ist die Lizenz bereits vorinstalliert.

In der Lizenzdatei sind die MAC-Adressen der lizenzierten Netzwerkschnittstellen eincodiert. Eine Gibraltar-Lizenz ist also nur auf jenen Geräten gültig, deren MAC-Adressen in der Lizenzdatei enthalten sind.

HINWEIS: Grundsätzlich besteht die Möglichkeit, die MAC-Adressen von Reservegeräten bereits beim Kauf in die Lizenz eincodieren zu lassen. Die Lizenz ist dann sowohl auf dem Hauptgerät als auch auf dem Reservegerät gültig. Für das Reservegerät muss keine neue Lizenz angefordert werden.

WICHTIG: Sollten Sie die Hardware wechseln müssen und keine für die neue Hardware gültige Lizenz vorhanden sein, besteht die Möglichkeit direkt im **GibADMIN** eine temporäre Lizenz für 10 Tage zu beantragen. Diese wird automatisch generiert und muss innerhalb der Laufzeit durch eine vollwertige neue Lizenz ersetzt werden.

Die Lizenzdatei

So erhalten Sie Ihre Lizenzdatei:

- **Beim Kauf von Gibraltar Software:** Per E-Mail vom Hersteller oder vom autorisierten Gibraltar Partner
- **Beim Kauf von Gibraltar Security Gateways:** Die Lizenz ist bereits am Gerät installiert
- **Testlizenz:** Eine Testlizenz für 30 Tage kann online auf der Gibraltar Webseite angefordert werden
- **Privatlizenz:** Eine kostenlose Privatlizenz die für maximal 5 Netzwerkgeräte gültig ist, erhalten sie per E-Mail vom unserem Support (support@gibraltar.at). Eine formlose Anfrage genügt.

Ein Beispiel für den Namen einer Lizenzdatei ist:
`gib_2_4_5116_Stadtgemeinde_GS50Y1_22_07_2007.key`
Folgende Informationen sind im Namen der Lizenzdatei eincodiert und sofort ersichtlich:

- **Versionsnummer:** gib_2_4
- **Lizenznummer:** 5116

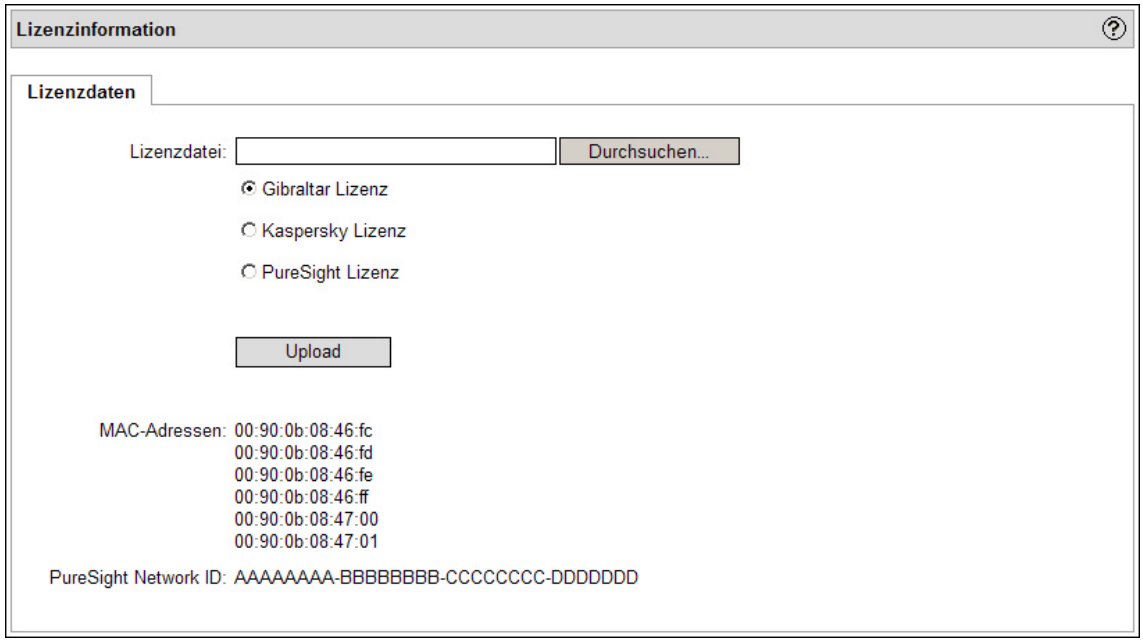
© 2008 by eSYS Informationssysteme GmbH

- **Name des Lizenznehmers:** Stadtgemeinde
- **Produkt:** GS50 (Gibraltar Software 50)
- **Laufzeit:** bis 22.7.2007

Installation der Lizenzdatei

Sollte noch keine Lizenzdatei installiert sein, werden Sie beim ersten Start des **GibADMIN** dazu aufgefordert.

1. **Lizenzdatei:** Betätigen Sie die Schaltfläche Durchsuchen... und wählen Sie im Öffnen Dialog Ihre Lizenzdatei aus.
2. **Gibraltar Lizenz:** Markieren Sie diese Option, wenn Sie eine Lizenz für Gibraltar hochladen wollen.
3. **Kaspersky Lizenz:** Markieren Sie diese Option, wenn Sie eine Lizenz für den Kaspersky Viren Scanner hochladen wollen.
4. **Puresight Lizenz:** Markieren Sie diese Option, wenn Sie eine Lizenz für den Puresight Content Scanner hochladen wollen.
5. **Upload:** Betätigen Sie diese Schaltfläche, um die Lizenzdatei hochzuladen.
6. **MAC-Adressen:** Hier werden die MAC-Adressen aller in den Rechner eingebaut Netzwerkkarten angezeigt. Diese Information wird benötigt, um eine gültige Lizenz erwerben zu können.
7. **Puresight Network ID:** Diese ID wird benötigt, wenn Sie eine Lizenz für den Puresight Content Scanner anfordern wollen.

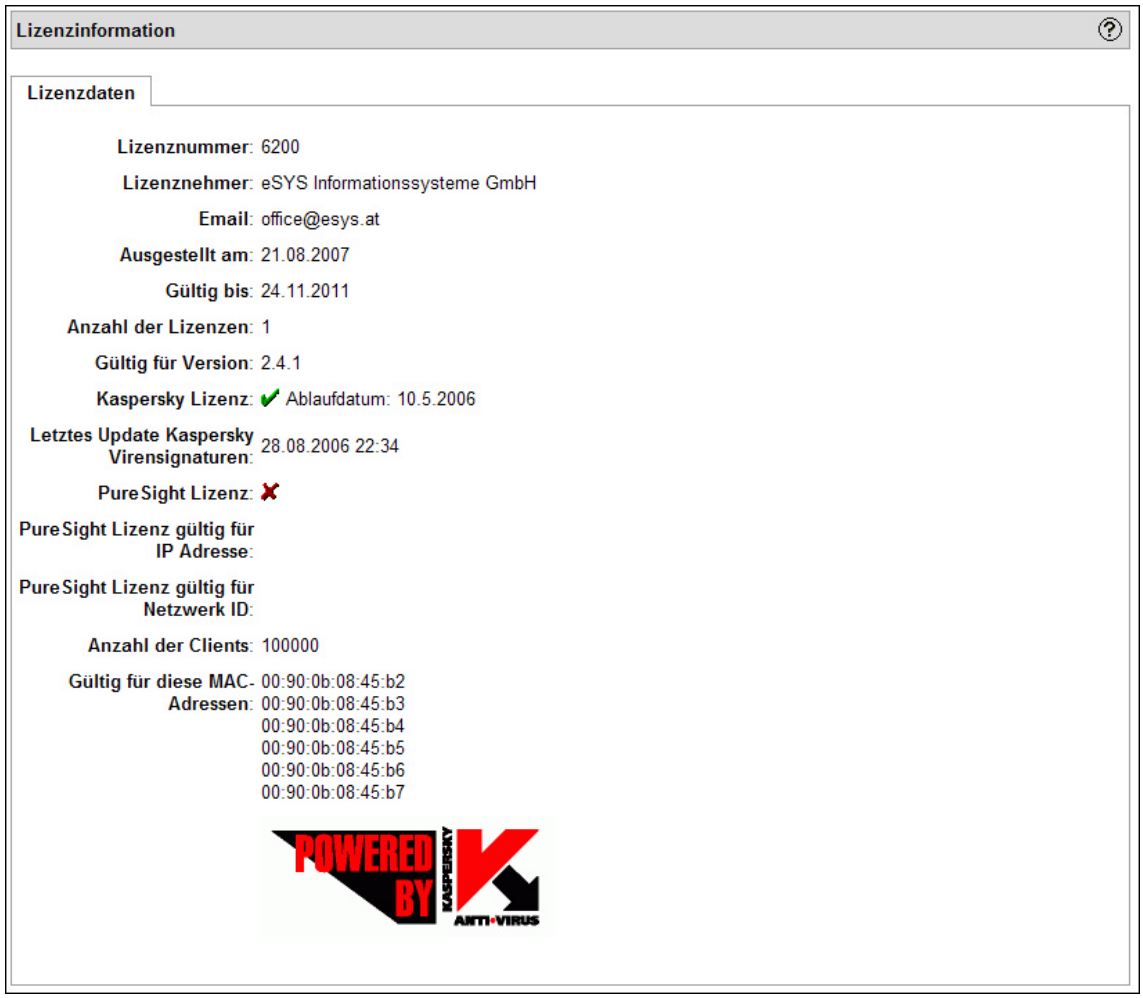


Nach dem erfolgreichen Hochladen der Lizenzdatei werden Sie in das Login Formular weitergeleitet.

1. **Benutzer:** Geben Sie den Benutzer "root" ein.
2. **Passwort:** Geben Sie das Passwort des Benutzers "root" ein. Bei der ersten Anmeldung ist das Passwort leer.
3. **Login:** Betätigen Sie diese Schaltfläche, um sich an Gibraltar anzumelden.

© 2008 by eSYS Informationssysteme GmbH

Nach dem erfolgreichen Login werden die Lizenzinformationen angezeigt.

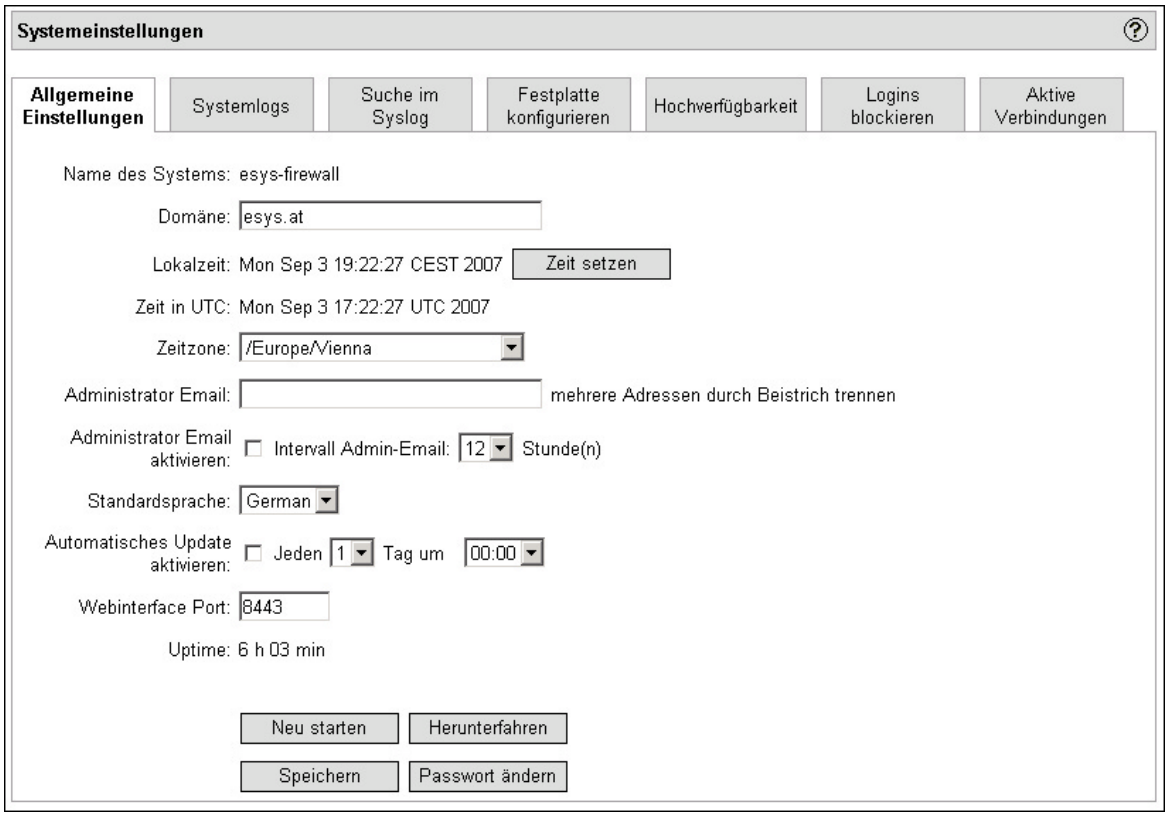


8.2 System

Im Modul **System** können folgende grundlegenden Einstellungen und Aufgaben vorgenommen werden:

- **Allgemeine Einstellungen:** Systemname, Systemzeit, Zeitzone, E-Mail des Administrators, Sprache, Automatisches Update, Port für GibADMIN
- **Systemlogs:** Anzeige der Systemlogs und Suche in den Systemlogs
- **Festplatten:** Einbinden und Konfigurieren von Festplatten
- **Heartbeat:** Konfiguration der Hochverfügbarkeitslösung Heartbeat
- **Logins blockieren:** Sperre bei fehlerhaftem Login definieren
- **Aktive Verbindungen:** Zeigt alle derzeit aktiven Verbindungen mit der Firewall

© 2008 by eSYS Informationssysteme GmbH



8.2.1 Allgemeine Einstellungen

Folgende Einstellungen können vorgenommen werden:

- **Name des Systems:** Hostname der Gibraltar Firewall
- **Domäne:** Netzwerkdomäne (z.B.: example.com). Sollten sie keine eigene öffentliche Domäne verwalten, geben Sie "local" ein.

HINWEIS: Der Hostname und die Domäne ergeben zusammen den "Fully Qualified Domain Name" (FQDN) der Gibraltar Firewall. Dieser FQDN sollte im DNS auflösbar sein, damit jene Mails, die direkt von der Firewall verschickt werden, auch ordnungsgemäß zugestellt werden können. Viele Mailserver und Spamfilter verwenden Mechanismen, die E-Mails von nicht auflösbaren FQDNs nicht annehmen. Erstellen Sie also einen eigenen DNS Eintrag für die Gibraltar Firewall.

- **Lokalzeit:** Die aktuelle Systemzeit. Klicken Sie auf die Schaltfläche Zeit setzen, um Gibraltar aufzufordern, die aktuelle Systemzeit mit einem Zeitserver im Internet zu synchronisieren. Dafür ist es jedoch notwendig, dass Gibraltar eine Verbindung mit dem Internet herstellen kann. Sie sollten also vorher die Netzwerkkonfiguration durchführen.
- **Zeit in UTC:** Hier wird die Zeit in der Weltzeit UTC (Universal Time Coordinated) angezeigt.
- **Zeitzone:** Auswahl der Zeitzone.
- **Administrator Email:** E-Mail-Adresse des Administrators. An diese Adresse werden Systemmitteilungen von Gibraltar gesendet, also auch Fehlermeldungen und Benachrichtigungen über mögliche Attacken. Mehrere Adresse können Sie mit Beistrichen getrennt angeben.
- **Administrator Email aktivieren:** Aktiviert die Zusendung von Systeminformationen

© 2008 by eSYS Informationssysteme GmbH

an die angegebene E-Mail-Adresse. Deaktivieren sie diesen Punkt, wenn sie keine Nachrichten von Gibraltar erhalten wollen.
- **Intervall Admin-Email:** Intervall für die Zusendung von Systemnachrichten.
- **Standardsprache:** Standardsprache in der GibADMIN startet.
- **Automatisches Update aktivieren:** Aktiviert die automatischen Updates von Gibraltar. Software-Updates und Security-Patches werden von Gibraltar Webservern in Form von Patches zur Verfügung gestellt. Diese können von Gibraltar automatisch heruntergeladen und installiert werden. Sie können das Intervall und die Uhrzeit für den Download festlegen.
- **Webinterface Port**: Port für den Zugriff auf GibADMIN. Ändern Sie diesen Wert, falls Sie nicht über Port 443 auf das Webinterface zugreifen wollen. Näheres Informationen finden Sie unter dem Punkt Port für Zugriff auf das Webinterface ändern.
- **Uptime:** Zeigt an, wie lange Gibraltar ohne Unterbrechung läuft.
- **Speichern:** Änderungen speichern.

Port für Zugriff auf das Webinterface ändern

GibADMIN ist standardmäßig über den Port 443 (HTTPS) erreichbar. Falls Sie diesen Port für den Betrieb einer sicheren Webseite benötigen, können sie für die Wartung von Gibraltar einen anderen Port auswählen (z.B. 8443).
Nach dem Ändern des Zugriffsports wird der Webserver auf Gibraltar neu gestartet und Sie können den **GibADMIN** nicht mehr unter dem bisherigen Port erreichen. Nach der Aktualisierung wird Ihnen in der Durchführungsbestätigung der aktualisierte Link für **GibADMIN** gezeigt.

ACHTUNG: Je nach Hardwareausstattung kann es bis zu mehreren Minuten dauern, bis der Webserver von **GibADMIN** neu gestartet wurde. In dieser Zeit ist **GibADMIN** nicht erreichbar.

- **Neu starten:** Startet Gibraltar neu. Der Befehl muss vor Ausführung bestätigt werden.
- **Herunterfahren:** Fährt Gibraltar herunter: Der Befehl muss vor Ausführung bestätigt werden.

ACHTUNG: Durch einen Neustart bzw. das Herunterfahren geht der **GibADMIN** offline. Sie können erst nach einem vollständigen Neustart des Systems wieder darauf zugreifen.

Passwort ändern

1. Wählen Sie im Hauptmenü den Befehl **System.**
2. Wählen Sie die Registerkarte **Allgemeine Einstellungen**.
3. **Passwort ändern:** Klicken Sie auf den Button **`Passwort ändern`**. Sie werden daraufhin aufgefordert, ein neues Passwort einzugeben und dieses zu wiederholen. Speichern Sie das Passwort mit einem Klick auf **`Speichern`**.

ACHTUNG: Verwenden Sie umbedingt sichere Passwörter für Ihre Firewall. Die Firewall ist eine Zugangstür zu Ihrem Netzwerk. Aus diesem Grund empfehlen wir dringend, folgende Passwortrichtlinien einzuhalten:
- Länge des Passworts sollte mindestens 12 Zeichen sein
- Verwendung von Buchstaben, Zahlen und Sonderzeichen

© 2008 by eSYS Informationssysteme GmbH

- Keine bekannten Wörter (Lexikonattacken)

8.2.2 Systemlogs anzeigen

In den Systemlogs von Gibraltar werden alle wichtigen Systemereignisse protokolliert. Das Systemlog ist eine wichtige Quelle, um das Verhalten von Gibraltar nachvollziehen zu können. Beispiele für Einträge im Systemlog sind:

- Verworfene Datenpakete
- Starten und Beenden von Diensten
- Fehlermeldungen

Folgende Einstellungen können vorgenommen werden:

- **Anzahl der Logs:** Anzahl der Zeilen, die im GibADMIN angezeigt werden.
- **Wiederholfrequenz in Sekunden:** Aktualisierungsrate bei automatischer Aktualisierung der Anzeige.

  (gestartet) **:** Die Anzeige wird im angegebenen Intervall automatisch aktualisiert. Betätigen Sie die Schaltfläche, um die automatische Aktualisierung zu stoppen.

  (gestoppt) **:** Die Anzeige wird nicht automatisch aktualisiert. Betätigen Sie die Schaltfläche, um die automatische Aktualisierung zu starten.

ACHTUNG: Wählen Sie keinen zu kurzen Intervall (< 5 sec), da sonst ein Stoppen dieser Funktion äußerst schwierig werden kann.

- **IP des externen Syslog-Servers:** Geben Sie hier die IP-Adresse eines externen Syslog-Servers ein, falls Sie einen externen Syslog Server verwenden möchten.
- **Syslog Einträge von anderen Rechnern erlauben:** Aktivieren Sie dieses Kontrollkästchen, wenn Sie Syslog-Einträge von anderen Geräten erlauben wollen. Beachten Sie, dass Sie eine **ACCEPT** Regel für den **UDP Port 514** vom jeweiligem Interface auf LOCAL erstellen müssen!

8.2.3 Suche im Syslog

Ermöglicht eine Volltextsuche in der Syslog-Datei. Geben Sie in das vorgesehene Textfeld Ihren Suchbegriff ein und Klicken Sie auf **Start**. Es werden alle Zeilen des Syslogs gezeigt, in denen der Suchbegriff als Teil enthalten ist.

8.2.4 Festplatte konfigurieren

Um in Gibraltar eine Festplatte verwenden zu können, muss diese zuerst in das System eingebunden werden. Gibraltar läuft grundsätzlich ohne Festplatte. Für bestimmte Aufgaben wie z.B. Proxy-Server und das Speichern von umfangreichen Log-Dateien wird jedoch die Verwendung einer Festplatte dringend empfohlen. Mit dieser Funktion können nur IDE-Festplatten und SATA-Festplatten eingebunden werden.

ACHTUNG: Durch die Verwendung einer Festplatte für Gibraltar werden sämtliche darauf befindlichen Daten gelöscht!

© 2008 by eSYS Informationssysteme GmbH

1. Wählen Sie im Hauptmenü den Punkt **System**.
2. Wählen Sie die Registerkarte **Festplatte konfigurieren**.
3. Wählen Sie aus dem Auswahlfeld **Festplatte verwenden** jene Festplatte aus, die Sie für Gibraltar verwenden wollen. Sie können durch die angezeigte Festplattengröße die richtige Festplatte identifizieren. Beachten Sie, dass die ausgewählte Festplatte formatiert wird und somit alle darauf befindlichen Daten gelöscht werden.

Einbinden der Festplatte

1. Klicken Sie auf den Button **Speichern**, um die ausgewählte Festplatte zu formatieren und für die Verwendung in Gibraltar vorzubereiten.
2. Bestätigen Sie die Aktion mit dem Button **Ja**, wenn Sie absolut sicher sind, dass durch die Formatierung der Festplatte keine noch benötigten Daten verloren gehen. Dadurch wird die Formatierung gestartet. Dieser Vorgang kann mehrere Minuten dauern.
3. Nach erfolgter Formatierung muss Gibraltar neu gestartet werden, damit die Festplatte auch korrekt in das Dateisystem eingebunden werden kann. Speichern Sie vorher die Konfiguration Wählen Sie dazu aus dem Hauptmenü den Punkt **Konfiguration verwalten**.
4. Wählen Sie die Registerkarte **Konfiguration speichern**.
5. Wählen Sie das von Ihnen verwendete Speichermedium und betätigen Sie anschließend die Schaltfläche **Speichern**.
6. Wählen Sie im Hauptmenü den Punkt **System**.
7. Betätigen Sie die Schaltfläche **Neu starten**, um Gibraltar neu zu booten.
8. Betätigen Sie in der Sicherheitsabfrage die Schaltfläche **Ja**, um den Rebootvorgang zu starten. Anschließend verlieren Sie natürlich die Verbindung zum **GibADMIN**. Sie können sich nach einigen Minuten - wenn Gibraltar den Startvorgang abgeschlossen hat - wieder in gewohnter Weise am **GibADMIN** anmelden.

8.2.5 Failover/Heartbeat

Mit der Hochverfügbarkeitslösung "Heartbeat" ist es möglich, zwei Gibraltar Firewalls redundant und ausfallsicher zu betreiben. Ein Gerät fungiert dabei als Hauptfirewall (Master), die zweite als Standby-Gerät (Slave). Beide Firewalls werden entweder direkt mit einem Cross-Over-Kabel oder indirekt über einen Switch miteinander verbunden.
Fällt die Hauptfirewall aus übernimmt das Standby-Gerät sämtliche Funktionen und sorgt dafür, dass ein weitgehend unterbrechungsfreier Betrieb gewährleistet ist.

Eine aktuelle und detaillierte Anleitung zur Konfiguration von Heartbeat finden Sie auf der Gibraltar Homepage www.gibraltar.at. Gerne hilft Ihnen auch unser Support weiter.

8.2.6 Logins blockieren

Mit dieser Funktion können Sie verhindern, dass ein Angreifer eine SSH Brute Force Attacke auf Gibraltar startet und somit eine Vielzahl an Passwortkombinationen testet. Gleichzeitig werden auch Anmeldeversuche beim **GibADMIN** überwacht. Im gegebenen Fall wird jene IP-Adresse blockiert, von der die Anmeldeversuche gestartet wurden.

1. Wählen Sie im Hauptmenü den Punkt **System**.
2. Wählen Sie die Registerkarte **Logins blockieren**.

© 2008 by eSYS Informationssysteme GmbH

4. **Überprüfungsintervall:** Zeitraum in Sekunden, der für die Überprüfung herangezogen wird.
4. **Anzahl der Anmeldeversuche im Intervall:** Anzahl der maximal erlaubten Anmeldeversuche innerhalb des angegebenen Zeitraums. Werden mehr Ameldeversuche (z.B. 5) innerhalb des angegebenen Zeitraums (30 Sekunden) gemacht, wird die Sperre aktiv.
5. **Dauer der Sperre in Sekunden:** Die betroffene IP-Adresse wird für die angegebene Dauer gesperrt. Eine erneute Anmeldung an Gibraltar ist erst wieder nach Ablauf der Dauer möglich.
6. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

8.2.7 Aktive Verbindungen

Auf dieser Registerkarte werden alle aktuell auf der Firewall offenen Netzwerk-Verbindungen angezeigt.

Sie finden hier folgende Detailinformationen zu den einzelnen Verbindungen:

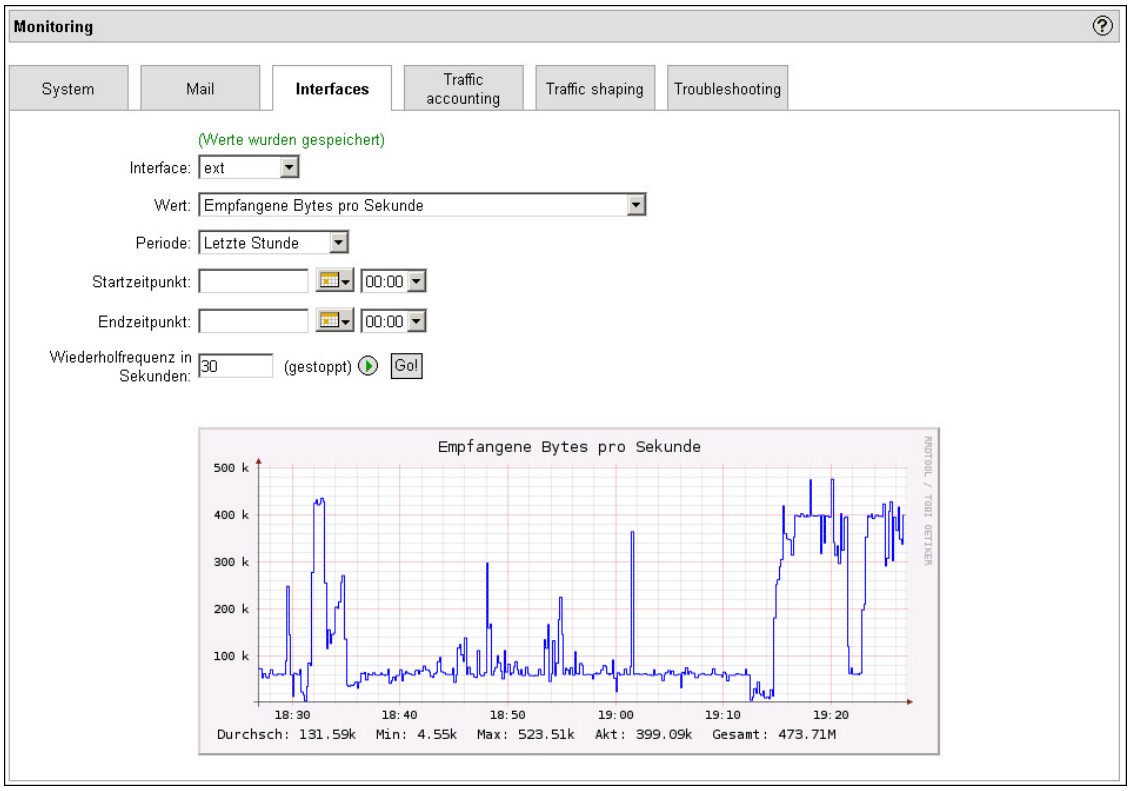
- **Quell IP-Adresse:** Ursprung der Verbindung
- **Ziel IP-Adresse:** Ziel der Verbindung
- **Protokoll:** Netzwerkprotokoll der Verbindung
- **Quellport:** Quellport der Verbindung
- **Zielport:** Zielport der Verbindung (z.B. 80 bei Zugriff auf einen Webserver)
- **Zeit:** Restlaufzeit der Verbindung in Sekunden.
- **Status:** Aktueller Status der Verbindung

8.3 Monitoring

Im Modul Monitoring können Sie verschiedene grafische Auswertungen durchführen und den Datenverkehr aufzeichnen. Folgende Möglichkeiten werden geboten:

- **Systemauswertungen** (CPU-Last, Speicher)
- **Mailauswertungen** (Eingehende und ausgehende Mails)
- **Interfaceauswertungen** (Empfangene Bytes, Gesendete Bytes)
- **Traffic Accounting** (Detaillierte Protokollierung des Datenverkehrs mit frei definierbaren Monitoring-Regeln)
- **Traffic Shaping** (Überwachung der Shaping Klassen)

© 2008 by eSYS Informationssysteme GmbH



8.3.1 System

Zeigt die Auslastung des Prozessors und die Speichernutzung

- **Wert:** Art der Auswertung (Speicher oder Prozessor)
- **Periode:** Auswahl eines Zeitraums für die Auswertung. Wählen Sie CUSTOM für einen spezifischen Zeitraum.
- **Startzeitpunkt:** Startzeitpunkt für die Auswertung
- **Endzeitpunkt:** Endzeitpunkt für die Auswertung
- **Wiederholfrequenz in Sekunden:** Aktualisierungsrate der Grafik. Durch starten der automatischen Aktualisierung wird die Auswertung im definierten Intervall neu aufgebaut.
- **Go!:** Auswertung durchführen.

8.3.2 Mail

Zeigt eine Auswertung aller eingehenden und ausgehenden E-Mails.

- **Wert:** Art der Auswertung (Eingehende oder ausgehende E-Mails)
- **Periode:** Auswahl eines Zeitraums für die Auswertung. Wählen Sie CUSTOM für einen spezifischen Zeitraum.
- **Startzeitpunkt:** Startzeitpunkt für die Auswertung
- **Endzeitpunkt:** Endzeitpunkt für die Auswertung
- **Wiederholfrequenz in Sekunden:** Aktualisierungsrate der Grafik. Durch starten der automatischen Aktualisierung wird die Auswertung im definierten Intervall neu aufgebaut.
- **Go!:** Auswertung durchführen.

© 2008 by eSYS Informationssysteme GmbH

8.3.3 Interfaces

Zeigt eine Auswertung des Netzwerkverkehrs auf dem ausgewählten Netzwerkinterface.

- **Interface:** Netzwerkinterface (Netzwerkschnittstelle) für die Auswertung
- **Wert**: Art der Auswertung
- **Periode:** Auswahl eines Zeitraums für die Auswertung. Wählen Sie CUSTOM für einen spezifischen Zeitraum.
- **Startzeitpunkt:** Startzeitpunkt für die Auswertung
- **Endzeitpunkt:** Endzeitpunkt für die Auswertung
- **Wiederholfrequenz in Sekunden:** Aktualisierungsrate der Grafik. Durch starten der automatischen Aktualisierung wird die Auswertung im definierten Intervall neu aufgebaut.
- **Go!:** Auswertung durchführen.

8.3.4 Traffic accounting

Zeigt die Auswertung der von Ihnen erstellten Regeln für das **Traffic accounting.** Monitoring Regeln ermöglichen die detaillierte Protokollierung des Netzwerkverkehrs und können im Modul Firewall erstellt werden. Monitoring-Regeln können für jede Filterregel im Paketfilter erstellt werden und bieten so eine sehr gute Möglichkeit, den Netzwerkverkehr zu analysieren.

Mit dieser Funktion ist es z.B. möglich, den Zugriff auf einen Webserver im internen Netzwerk zu protokollieren. Aktivieren Sie hierzu bei der entsprechenden Firewall-Regel, welche den Zugriff auf den Webserver erlaubt, die Monitoring-Funktion.

- **Regel auswählen:** Auswahl der entsprechenden vorkonfigurierten Regel für die Auswertung
- **Wert:** Art der Auswertung
- **Periode:** Auswahl eines Zeitraums für die Auswertung. Wählen Sie CUSTOM für einen spezifischen Zeitraum.
- **Startzeitpunkt:** Startzeitpunkt für die Auswertung
- **Endzeitpunkt:** Endzeitpunkt für die Auswertung
- **Wiederholfrequenz in Sekunden:** Aktualisierungsrate der Grafik. Durch starten der automatischen Aktualisierung wird die Auswertung im definierten Intervall neu aufgebaut.
- **Go!:** Auswertung durchführen.

8.3.5 Traffic shaping

Zeigt Auswertungen zu den Traffic Shaping Regeln (Bandbreitenmanagement). Das Erstellen von Traffic Shaping Klassen wird im Modul Traffic shaping erläutert. Das Monitoring der Shaping-Klassen soll eine optimale Einstellung der Bandbreiten sicherstellen.

- **Track:** Interface, für das die Traffic Shaping Regel erstellt wurden
- **Regel auswählen**: Auswahl der entsprechenden vorkonfigurierten Regel für die

© 2008 by eSYS Informationssysteme GmbH

Auswertung
- **Wert:** Art der Auswertung
- **Periode:** Auswahl eines Zeitraums für die Auswertung. Wählen Sie CUSTOM für einen spezifischen Zeitraum.
- **Startzeitpunkt:** Startzeitpunkt für die Auswertung
- **Endzeitpunkt**: Endzeitpunkt für die Auswertung
- **Wiederholfrequenz in Sekunden:** Aktualisierungsrate der Grafik. Durch starten der automatischen Aktualisierung wird die Auswertung im definierten Intervall neu aufgebaut.
- **Go!:** Auswertung durchführen.

8.3.6 Troubleshooting

Im laufenden Betrieb kann es zu Situationen kommen, in denen das Monitoring fehlerhaft wird. Dies merken Sie entweder daran, dass sich der entsprechende Dienst nicht mehr starten lässt, oder in den entsprechenden Übersichten anstatt einer grafischen Auswertung eine Fehlermeldung angezeigt wird.

Um die fehlerhafte Situation zu beheben, können Sie mit einer der folgenden Aktionen das Monitoring neu initialisieren:
- **Neuinitialisierung:** Versucht eine Neuinitialisierung des Monitoring-Dienstes. Aufgezeichnete Daten bleiben erhalten. Bringt diese Aktion nicht den gewünschten Erfolg müssen Sie die Monitoring-Datenbanken löschen.
- **Datenbanken löschen:** Löscht die Monitoring-Aufzeichnungen und initialisiert den Monitoring-Dienst neu.
- **Interfaces Fehler konfigurieren**: Entfernt alle Aufzeichnungen für den Interface-Traffic.

8.4 Dienste

Viele Funktionen in Gibraltar setzen den Start eines entsprechenden Dienstes voraus. Bei diesen Funktionen handelt es sich meist um Zusatzfunktionen, die für den Betrieb der Firewall nicht unbedingt notwendig sind und deshalb standardmäßig deaktiviert sind. Starten Sie einen Dienst dann wenn Sie die entsprechende Funktion benötigen.
Jeder Dienst kann gestartet und gestoppt bzw. neu gestartet werden.

Folgende Aktionen stehen im Zusammenhang mit Diensten zur Verfügung:
- **Starten eines Dienstes**
- **Stoppen eines Dienstes**
- **Automatischer Start eines Dienstes beim Systemstart**

Dienstbeschreibung:

- **Anon Anonymisierer:** Anon-Proxy: Ermöglicht die Konfiguration der Anonymisierungs-Funktion Anon-Proxy
- **Captive Portal:** Ein Captive Portal ist ein HotSpot-Dienst, durch den es möglich ist, für Benutzer den Netzwerkzugang auf Basis von Zeitdauer bzw. Datenmenge zu beschränken
- **DHCP-Server:** Startet den in Gibraltar integrierten DHCP-Server
- **DHCP-Relay:** Aktiviert den Dienst zur Konfiguration von DHCP-Relay

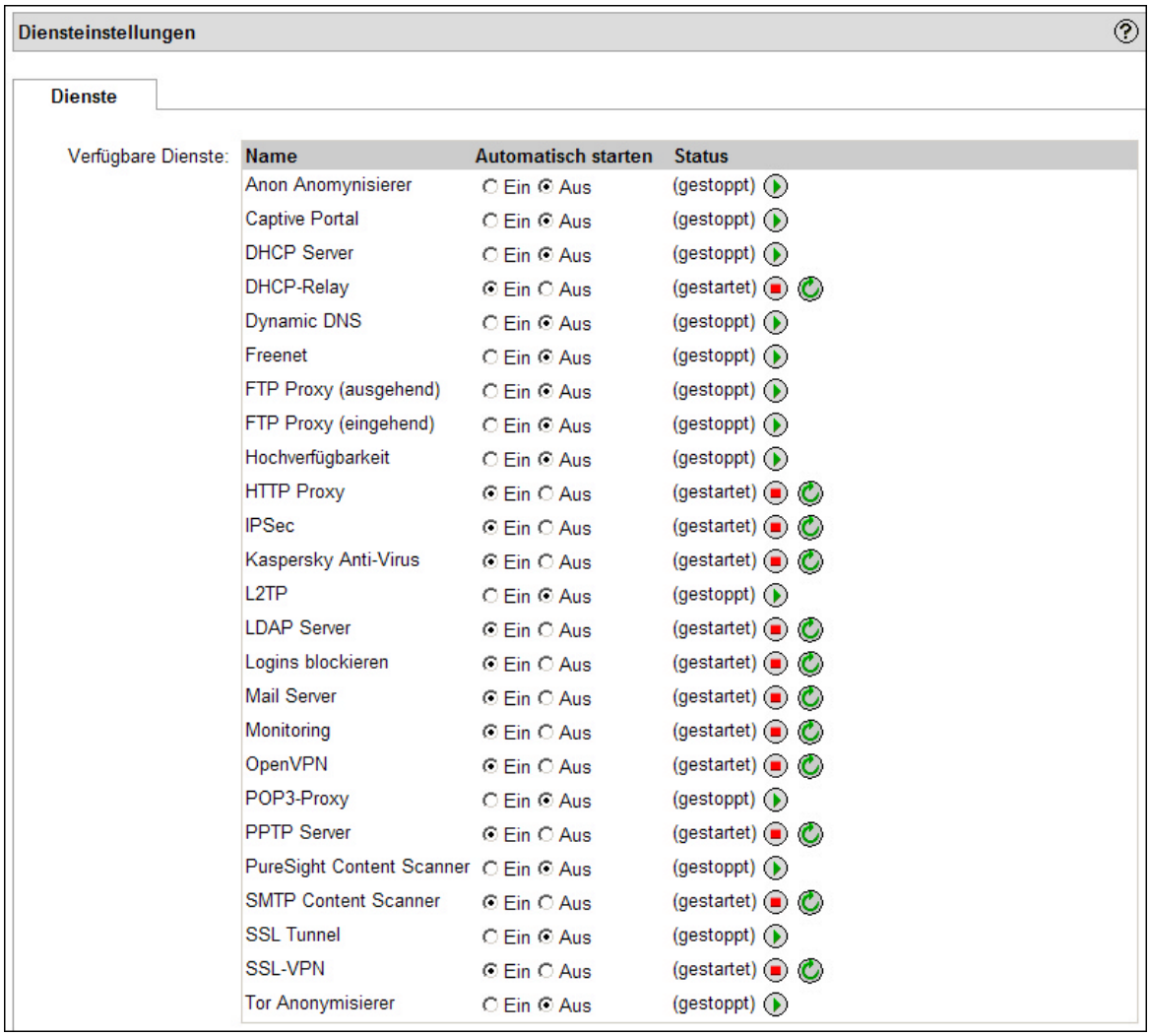
© 2008 by eSYS Informationssysteme GmbH

- **Dynamic DNS:** Ermöglicht die Konfiguration von Dynamic DNS
- **Freenet:** Startet die in Gibraltar integrierte Anonymisierungs-Komponente Freenet
- **FTP Proxy (ausgehend):** FTP-Proxy Server für ausgehenden FTP-Traffic
- **FTP Proxy (eingehend):** FTP-Proxy Server für eingehenden FTP-Traffic
- **Hochverfügbarkeit:** Dienst für die Konfiguration der Hochverfügbarkeitslösung Heartbeat
- **HTTP Proxy:** Transparenter http-Proxy Server
- **IPSec:** Dienst für die Konfiguration von IPSec/VPN Tunnels und IPSec/Clients
- **Kaspersky Anti-Virus:** Kaspersky Antivirus Prüfung für HTTP, FTP und SMTP
- **L2TP:** Dienst für die Konfiguration von L2TP IPSec Verbindungen
- **LDAP Server:** Integrierter LDAP Verzeichnisserver zur Benutzerverwaltung
- **Logins blockieren:** Aktiviert die Loginüberprüfung
- **Mail Server:** Aktiviert den in Gibraltar integrierten Mailserver für das Mail-Relay (Mail-Proxy)
- **Monitoring**: Aktiviert die Monitoring-Funktionen
- **OpenVPN:** Aktiviert den OpenVPN Server
- **POP3 Proxy:** Aktiviert den POP3-Proxy Server
- **PPTP:** Ermöglicht die Konfiguration von PPTP VPN Verbindungen
- **PureSight Content Scanner:** Aktiviert die aktive Inhaltsüberprüfung von Webinhalten mittels dem Puresight CSDK
- **SMTP Content Scanner:** Ermöglicht die Konfiguration der Mailprüfungen
- **Snort IDS:** Intrusion Detection System zur Überwachung von möglichen Angriffen
- **SSL Tunnel:** Ermöglicht die Konfiguration von SSL Verbindungen
- **SSL VPN:** Aktiviert den SSL-VPN Dienst.
- **Tor Anonymisierer:** Ermöglicht die Konfiguration der Anonymisierungs-Funktion Tor

ACHTUNG: In gewissen Situationen kann das Starten eines Dienstes fehlschlagen. Sollte dies der Fall sein, wird die Fehlermeldung des Systems (in englischer Sprache) ausgegeben. Beispiele hierfür sind das Starten vom DHCP Server, wenn noch kein Interface für DHCP aktiviert ist.

ANMERKUNG: Damit Ihre Mails auf Viren und Spam überprüft werden, muss auch der SMTP Content Scanner Dienst unter dem Menüpunkt Dienste gestartet werden.

© 2008 by eSYS Informationssysteme GmbH



8.5 Netzwerk

8.5.1 Netzwerk

Im Modul **Netzwerk** werden grundlegende Netzwerkeinstellungen getätigt.

- **Interne und externe DNS-Server**
- **Netzwerkkarten und Adressen**
- **Routing**
- **Verbindungstest**
- **Definitionen von Hosts, Netzen, Gruppen und Services**
- **Bridging**
- **VLAN**
- **DHCP-Server**
- **Dynamic DNS**

© 2008 by eSYS Informationssysteme GmbH

8.5.1.1 DNS

Durch die Angabe von externen DNS-Servern erreichen Sie, dass Gibraltar DNS-Anfragen an diese Server weiterleitet und nicht die Wurzel-DNS-Server für die Auflösung von DNS-Anfragen verwendet. Zusätzlich können für andere Domänen (bspw. ihre internen Active-Directory-Domänen) eigene Domain Name Server definiert werden. Durch Eintragen der Domäne und der IP-Adresse des DNS-Servers werden Anfragen an diese Domäne an den richtigen Server weitergeleitet.

1. Wählen Sie im Hauptmenü den Punkt **Netzwerk**.
2. Wählen Sie die Registerkarte **DNS**.
3. **Externe DNS-Server:** Geben Sie hier die von Ihrem Provider zur Verfügung gestellten externen DNS-Server ein. Sollten hier keine DNS-Server angegeben werden, werden die Root-DNS-Server für die Namensauflösung verwendet.
4. **Interne DNS-Server:** Geben Sie hier Paare aus Domäne und IP-Adresse ein. Sollte eine DNS Anfrage an Gibraltar erfolgen, die eine der hier eingetragenen Domänen betrifft, so wird diese Anfrage an die entsprechende IP-Adresse weitergegeben. Meistens werden hierbei interne DNS-Server verwendet (z.B. internaldns.esys.at)
5. **Server hinzufügen:** Betätigen Sie diese Schaltfläche, um einen Server hinzuzufügen.
6. **Markierte Einträge löschen** : Markieren Sie jene Einträge in der Elementgruppe durch Aktivieren des Kontrollkästchens, die Sie löschen wollen. Betätigen Sie anschließend diese Schaltfläche, um die Elemente zu löschen.
7. **Server löschen** : Betätigen Sie diese Schaltfläche, um den Server zu löschen.
8. **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

8.5.1.2 Netzwerkkarte

Für jede in Gibraltar eingebaute Netzwerkkarte wird eine Registerkarte erzeugt, auf der die verschiedenen Einstellungen wie Name, statische oder dynamische IP Adressvergabe und Starten oder Stoppen der Netzwerkkarte durchgeführt werden.

- **Status:** aktueller Status der Netzwerkkarte (**gestartet**) oder (**gestoppt**).
  Interface starten : Starten und aktivieren der Netzwerkkarte, wenn der aktuelle Status (**gestoppt**) ist.
  Interface stoppen : Stoppen und deaktivieren der Netzwerkkarte, wenn der aktuelle Status (**gestartet**) ist.
- **MAC-Adresse:** Zeigt die weltweit eindeutige Kennungsnummer der Netzwerkkarte.

TIPP: Um die Netzwerkkarten in Gibraltar beim Herstellen der Netzwerkverbindungen eindeutig für die Konfiguration im GibADMIN identifizieren zu können, sollten Sie die MAC-Adresse auch außen auf der Netzwerkkarte vermerken. So ist es Ihnen jederzeit möglich, die richtigen Netzwerkkarten zu verbinden.

- **Interface:** Interne Bezeichnung der Netzwerkkarte. Die "sprechende" Benennung der Netzwerkkarte erleichtert die Administration. Sie können beispielsweise das Interface, das mit dem Internet verbunden ist, "ext0" nennen, und das Interface, das mit dem internen Netzwerk verbunden ist, "int0". Die Benennung darf nicht "lo" sein und auch nicht folgendermaßen beginnen: "eth", "ppp", "slip", "ipsec", "sit", "wlan".
- **Automatisch starten:** Die Netzwerkkarte wird bei einem Neustart von automatisch Gibraltar aktiviert.

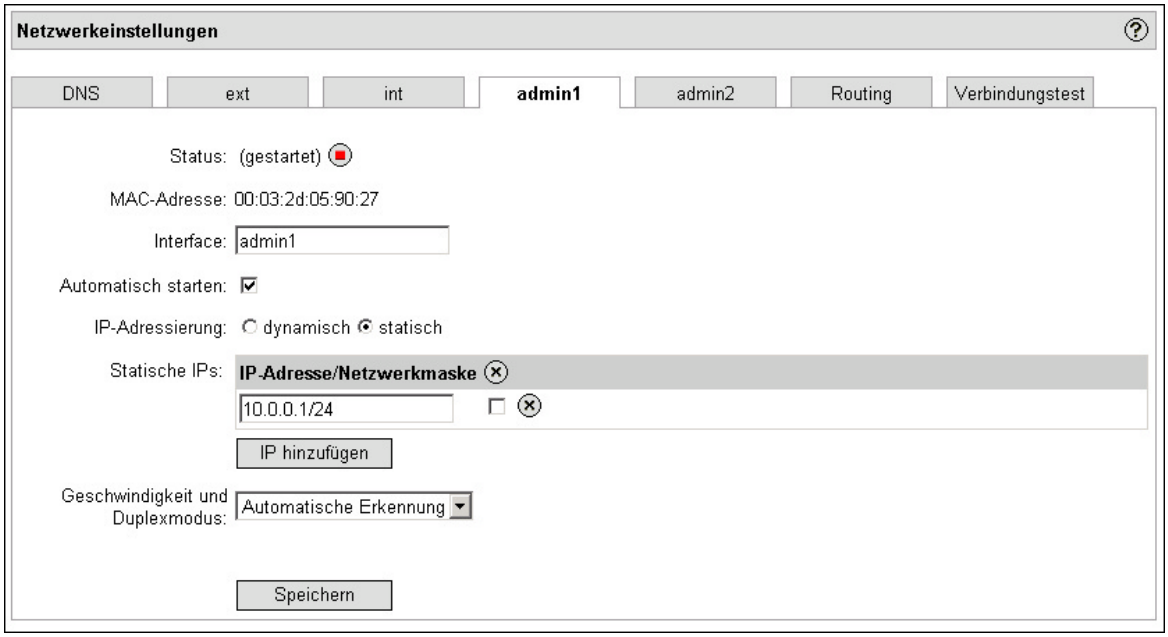
© 2008 by eSYS Informationssysteme GmbH

- **IP-Adresse:** IP-Adresse der Netzwerkkarte. Die IP-Adresse kann sowohl dynamisch wie auch statisch sein. Ist dynamisch gewählt, so sucht sich Gibraltar beim Starten einen DHCP Server, der ihr dynamisch eine IP-Adresse und weitere Netzwerkeinstellungen übermittelt. Wenn Sie statisch wählen, so ist (sind) von Ihnen eine (oder mehrere) IP-Adresse(n) durch Betätigung der Schaltfläche IP hinzufügen zu vergeben. Dabei ist die CIDR-Notation (z.B.: 192.168.0.10/24 für die IP-Adresse 192.168.0.10 mit Subnetzmaske 255.255.255.0) zu verwenden, um neben der IP-Adresse auch die Anzahl der für die Identifikation des Netzwerkes verwendeten Bits (die Subnetzmaske) festzulegen. Wollen Sie eine IP-Adresse löschen, betätigen Sie die Schaltfläche IP-Adresse löschen ⊗ neben diesem Eintrag. Wollen Sie mehrere IP-Adressen löschen, markieren Sie die Kontrollkästchen der zu löschenden Einträge und betätigen die Schaltfläche Markierte Einträge löschen ⊗ in der Kopfzeile der Elementgruppe.
- **Geschwindigkeit und Duplexmodus:** Hier können sie die Geschwindigkeit Ihrer Netzwerkkarte einstellen. Gewisse Internetanbieter verlangen bestimmte Einstellungen bei der Kommunikation mit den Modems.

ACHTUNG: Wenn Sie die Einstellungen der Netzwerkkarte, über die Sie zurzeit den GibADMIN bedienen, verändern, kann die Verbindung unterbrochen werden.

ACHTUNG: Wenn Sie die Einstellungen der Netzwerkkarte ändern, die die Verbindung zum Standardgateway darstellt, so müssen Sie auch die Einstellungen auf der Registerkarte Routing überprüfen bzw. neu durchführen.

- **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.



Bridges

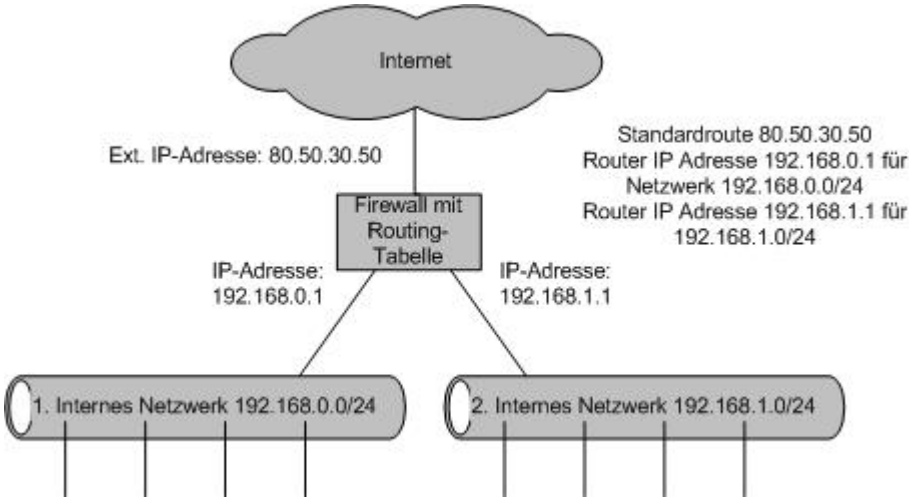
Wenn eine Netzwerkkarte Teil einer Bridge ist, macht es keinen Sinn, für diese Netzwerkkarte Werte einzurichten. Daher sind jene Netzwerkkarten, die ein Bridge zu geordnet sind, nicht mehr erreichbar und durch den Zusatz **(bridged)** im Titel der Registerkarte gekennzeichnet.

© 2008 by eSYS Informationssysteme GmbH

Ist eine Bridge eingerichtet, so wird eine zusätzliche Registerkarte für die Konfiguration dieser Bridge angezeigt. Auf dieser Registerkarte kann die IP-Adresse der Bridge konfiguriert werden. Auch das Entfernen der Bridge ist hier durchzuführen.

8.5.1.3 Routing

Das **Routing** regelt die Weiterleitung von Datenpaketen. Dabei wird die Zieladresse eines Datenpakets dahingehend untersucht, ob sie in eines der angegebenen Netze passt. Ist dies der Fall, wird das Paket an die entsprechende Router IP weitergeleitet. Passt die Zieladresse in keine der in der Liste angegebenen Netze, so wird das Paket an die Standardroute weitergeleitet.



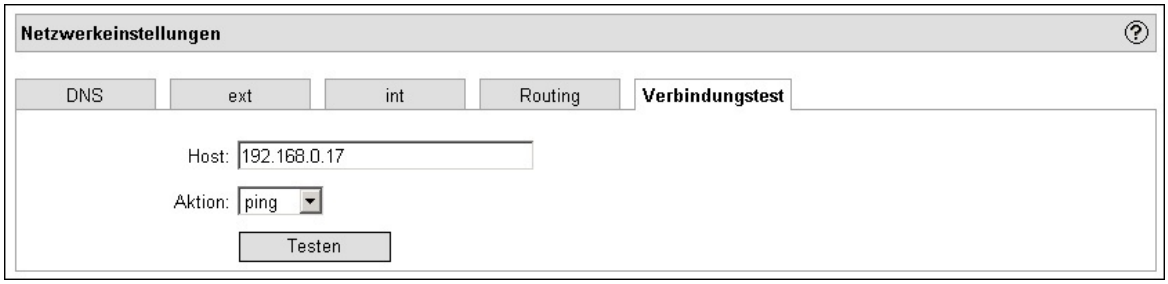
- **Standardroute:** IP-Adresse, über die Pakete weitergeleitet werden sollen, wenn sie nicht für eines der in der Liste unten angeführten Netzwerke bestimmt sind.
- **Zusätzliche Routen:** Diese Elementgruppe zeigt alle zusätzlichen Routen.
- **Router IP-Adresse:** Geben Sie hier die IP-Adresse des Routers an, an den die IP Pakete weitergeleitet werden sollen.
- **Netzwerkadresse:** Geben Sie hier die Netzwerkadresse des Zielnetzwerkes ein. Hat ein Paket eine Zieladresse aus einem der angegebenen Netzwerkbereiche, wird es an den entsprechenden Router weitergeleitet.
- **Route hinzufügen:** Betätigen Sie diese Schaltfläche, um eine Route hinzuzufügen.
- **Route löschen** ⊗**:** Betätigen Sie diese Schaltfläche, um eine Route zu löschen.
- **Markierte Einträge löschen** ⊗**:** Markieren Sie jene Einträge in der Elementgruppe durch Aktivieren des Kontrollkästchens, die Sie löschen wollen. Betätigen Sie anschließend diese Schaltfläche in der Kopfzeile, um die Elemente zu löschen.
- **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

© 2008 by eSYS Informationssysteme GmbH

8.5.1.4 Verbindungstest

Der Verbindungstest stellt eine einfache Möglichkeit dar, die Netzwerkverbindung zu überprüfen. Dabei werden die beiden bekannten Netzwerktools **ping** und **traceroute** verwendet.

- **Host:** Geben Sie hier eine IP-Adresse oder den Namen eines Hosts an, zu dem Sie eine Verbindung testen wollen (z.B. 10.11.12.13 oder www.esys.at).
- **Aktion:** Wählen Sie hier die Aktion aus, die Sie durchführen möchten (ping oder traceroute). Der Befehl **ping** schickt ICMP Pakete zum angegebenen Host. Werden diese Pakete beantwortet, so besteht eine Verbindung zu diesem Host. Der Befehl **traceroute** listet alle Stationen zwischen Gibraltar und dem angewählten Host auf, die bei der Übertragung passiert werden.
- Testen: Durch Betätigung dieser Schaltfläche wird der Befehl ausgeführt und es werden ICMP Pakete zum angegebenen Host geschickt.
- **Zurück:** Durch Betätigen dieser Verknüpfung gelangen Sie wieder auf den Ausgangsbildschirm dieser Registerkarte.



8.5.2 Definitionen

Um die Konfiguration und Wartung von Gibraltar zu vereinfachen besteht die Möglichkeit, für einzelne Hosts, Gruppen von Hosts, Netzwerke und Services Namen zu vergeben. Dies ermöglicht dem Administrator bei der Erstellung von Firewall-Regeln und anderen Einstellungen die Verwendung von aussagekräftigen Namen anstatt von IP-Adressen, Ports und Netzwerkbereichen. Sie können z.B. stellvertretend für Ihren internen Webserver mit der IP-Adresse 10.0.10.100 den Namen **webserver1** definieren.

Eine sehr praktische Funktion in diesem Zusammenhang ist auch die Definition von Services. Mehrere Protokolle und Ports werden dabei zu einzelnen Services zusammengefasst. Dies ermöglicht in weiterer Folge für diesen Service eine einzelne Firewall-Regel zu erstellen anstatt einzelne Regeln für jedes Teilprotokoll.

© 2008 by eSYS Informationssysteme GmbH

BEISPIEL: Definieren Sie ein Service **Web**, welches die TCP Ports 80 und 443 beinhaltet. Sie können dann in weiterer Folge beide Ports mit einer Regel freischalten oder zu einem internen Webserver weiterleiten.

TIPP: Nutzen Sie die Möglichkeiten der Definition von Hosts, Netzen und Services. Sie wird Ihnen in der Folge die Administration der Firewall wesentlich erleichtern.

8.5.2.1 Host/Netz Aliases

Ein Host/Netz Alias ist ein Name für eine einzelne IP-Adresse (Host), für ein gesamtes Netzwerk oder für einen FQDN.

Sie können beliebig viele Host/Netz Aliases definieren. Ein Eintrag besteht auf folgenden Informationen:

- **Name:** Frei wählbarer Name
- **IP-Adresse/Netzwerkadresse/FQDN:** Eine einzelne IP-Adresse, ein gesamtes Netzwerk oder ein FQDN. Ein Netzwerk wird in CIDR-Notation (z.B. 192.168.0.0/24) angegeben.
- **MAC-Adresse:** Die MAC-Adresse des entsprechenden Hosts. Diese Information ist optional und kann dazu verwendet werden, MAC-Adressen mit Namen zu belegen und entsprechende Filterregeln zu erstellen. MAC Adressen sollten nur in Ausnahmefällen verwendet werden (z.B. von Providern zur Unterscheidung ihrer Kunden).

8.5.2.2 Host/Netz Gruppen

Host/Netz Aliases können zu Host/Netz Gruppen zusammengefasst werden. Das ermöglicht eine wesentliche Vereinfachung der Wartung. Wollen Sie z.B. mehreren Hosts identische Netzwerk-Berechtigungen geben, können Sie diese Hosts zu einer Gruppe zusammenfassen. In weiterer Folge benötigen Sie nur eine einzelne Filterregel. Ändert sich die Zusammensetzung der Gruppe, reicht es, die Gruppe zu bearbeiten. Eine Adaptierung der Firewall-Regeln ist nicht mehr notwendig.

Die Übersicht zeigt die bestehenden Gruppen und ihre Mitglieder. Sie können hier neue Gruppen definieren und die bestehenden Gruppen bearbeiten.
Mitglied einer Gruppe können nur zuvor definierte Host/Netz Aliases sein.

8.5.2.3 Services

Sie können einzelne Protokolle und Ports zu Services zusammenfassen und benennen. Das erleichtert die Konfiguration von Firewall- und NAT-Regeln. Gängige Services wurden bereits vorkonfiguriert und benannt. Sie können die Serviceliste beliebig erweitern und bearbeiten. Ein Service kann aus beliebig vielen Einträgen bestehen.

Ein Service besteht aus folgenden Informationen:

- **Name:** Frei wählbarer Name für das Service (z.B. Web)
- **Protokoll:** Netzwerkprotokoll (muss ausgewählt werden)
- **Quellport:** bei den meisten Services nicht erforderlich, da dieser meistens zufällig generiert wird.

© 2008 by eSYS Informationssysteme GmbH

- **Zielport:** z.B. Port 80 bei http

8.5.2.4 Zusätzliche Interfaces

Zusätzliche Interfaces sind virtuelle Netzwerkschnittstellen, welche nicht permanent zur Verfügung stehen (z.B. VPN-Tunnel). Um für derartige Interfaces Filterregeln definieren zu können, ist es notwendig, diese Interfaces vorher zu definieren. Sie können in weiterer Folge als eingehendes oder ausgehendes Interface ausgewählt werden.

Bspw. wird einer Point-to-Point Verbindung (z.B. Telefonwählleitung, ADSL, PPTP Remote Zugang) der Interfacename **ppp** zugeteilt, wobei daran noch die laufende Nummer der Verbindung angehängt wird (erste Verbindung: "ppp0"; zweite Verbindung: "ppp1"; usw.). Es können jedoch mehrere PPTP Verbindungen gleichzeitig aufgebaut werden. Um Filterregeln für alle Point-to-Point Verbindungen zu erzeugen, geben Sie hier den Interfacenamen **ppp+** ein. Da eine Point-to-Point Verbindung häufig vorkommt, wurde ppp+ in die Standardkonfiguration integriert.

8.5.3 Dial-in

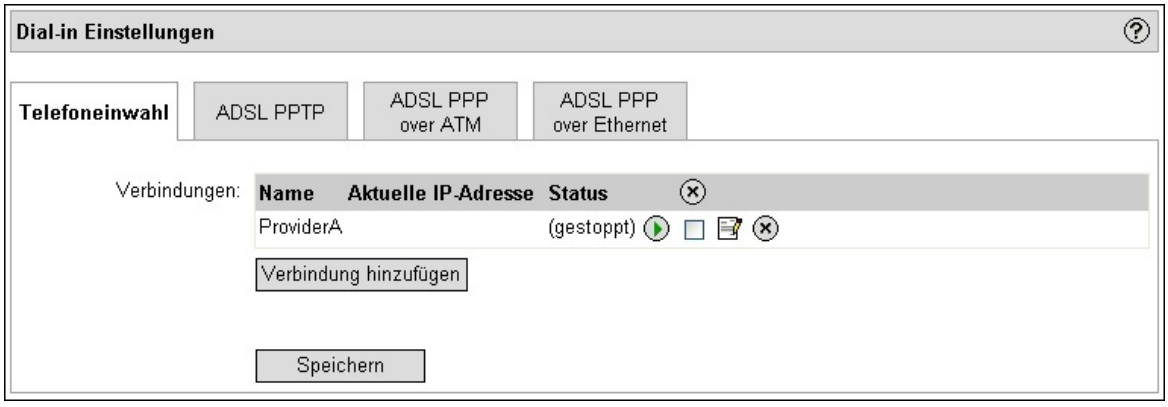
Im **Dial-in** Modul werden die Einstellungen für Wählverbindungen und ADSL Zugänge vorgenommen.

8.5.3.1 Telefoneinwahl

Sie können Gibraltar zur Herstellung von Dial-Up Internetverbindungen verwenden. Es kann eine beliebige Anzahl von Wählverbindungen mit Analogem Modem oder ISDN Modem definiert werden. In dieser Liste sehen Sie eine Übersicht über die bestehenden Dial-Up Verbindungen und können diese bearbeiten. Zusätzlich wird bei einer gestarteten Verbindung die aktuell zugewiesene IP-Adresse angezeigt.

Wählverbindungen können nach Bedarf gestartet und gestoppt werden.

ACHTUNG: Um Filterregeln für eine Wählverbindung zu können, müssen Sie das Interface ppp+ im Filterregelformular verwenden, da der Verkehr bei dieser Dial-in Verbindung über dieses Interface läuft.



© 2008 by eSYS Informationssysteme GmbH

8.5.3.1.1 Telefoneinwahl - Detailansicht

Bei der Definition einer Wählverbindung können folgende Einstellungen vorgenommen werden:

- **Name:** Frei zu wählender Name für die Verbindung. Der Name wird in der Übersicht der Wählverbindungen angezeigt. Jeder Name kann global nur einmal vergeben werden. Dies gilt auch für bereits konfigurierte ADSL-Verbindungen.
- **Autorisierung:** Wählen Sie das gewünschte Autorisierungsverfahren **PAP** und **CHAP** . Es handelt sich hier um zwei unterschiedliche Anmeldeverfahren, mit denen Sie sich bei Ihrem Provider identifizieren müssen. Entnehmen Sie die für Sie relevante Option aus den Anmeldeunterlagen Ihres Providers.
- **Benutzername:** Vom Provider zugewiesener Benutzername
- **Passwort** und **Passwort (Bestätigung):** Vom Provider zugewiesenes Passwort.
- **Anschlussgeschwindigkeit (Bit/s):** Anschlussgeschwindigkeit des Modems
- **Wählverfahren:** Art des Wählverfahrens.
- **Auf Freizeichen warten:** Aktivieren Sie diese Option, wenn das Modem vor dem Verbindungsaufbau auf ein Freizeichen warten soll.
- **Telefonnummer:** Telefonnummer für die Einwahl. Achten Sie darauf, dass die Nummer vollständig eingegeben wird.
- **Anschluss:** Anschluss des Modems
- **Standardroute:** Aktivieren Sie diese Option, falls die Wählverbindung als Standardroute verwendet werden soll.
- **Standardroute ersetzen:** Ersetzt beim Aufbau der Verbindung eine bestehende statische Route.
- **Dial on Demand:** Aktiviert das Wählen bei Bedarf. Es wird automatisch eine Verbindung hergestellt, wenn eine Client-Anforderung vorliegt.
- **Verbindung aufrecht erhalten:** Die Verbindung wird nach einem ungewollten Verbindungsabbruch automatisch wiederhergestellt.
- **Idle (Sekunden):** Geben Sie hier die Wartezeit ein, wie lange das Modem die Verbindung aufrecht erhalten soll, wenn kein Verkehr mehr über die Leitung läuft. Sollten Sie hier zum Beispiel den Wert 10 eingeben, so wartet das Modem nach der letzten Aktivität im Internet noch zehn Sekunden, bis es die Verbindung automatisch beendet.
- **Holdoff (Sekunden):** Geben Sie hier die Wartezeit ein, wie lange das Modem nach dem Beenden einer Verbindung den neuerlichen Aufbau einer Verbindung verhindert. Erst nach Ablauf dieser Zeit kann die Verbindung wieder hergestellt werden.
- **Einwahlinterface umbenennen auf:** Definieren Sie einen individuellen Namen für das Interface der Wählverbindung (z.B. ext statt ppp+)
- **Geroutete Netzwerke:** Netzwerke, die nach erfolgter Einwahl geroutet werden sollen.
- **Statische IPs:** Zusätzliche statische IP-Adressen, die der Provider an Sie vergeben hat.

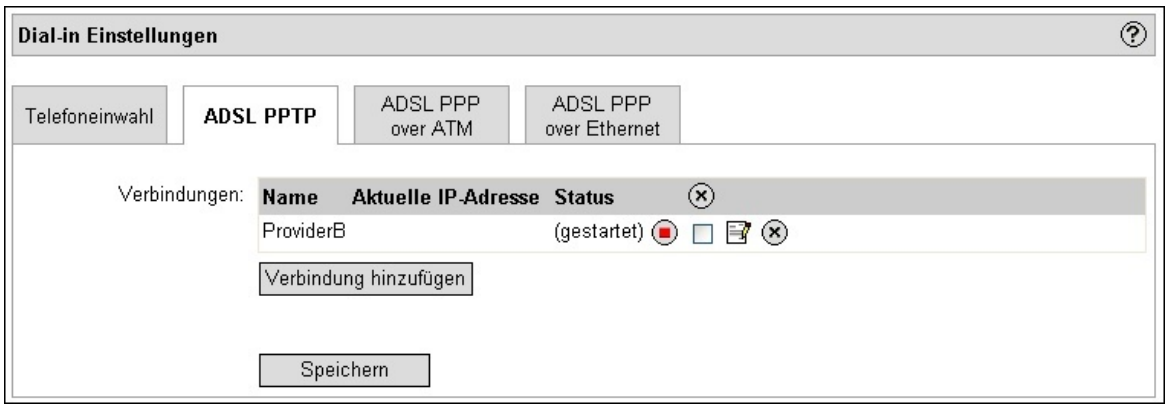
8.5.3.2 ADSL PPTP

Sie können Gibraltar zur Herstellung von ADSL-PPTP Internetverbindungen verwenden. Es kann eine beliebige Anzahl von PPTP Verbindungen definiert werden. In dieser Liste sehen Sie eine Übersicht über die bestehenden ADSL-PPTP Verbindungen und können diese bearbeiten. Zusätzlich wird bei einer gestarteten Verbindung die aktuell zugewiesene IP-Adresse angezeigt.

© 2008 by eSYS Informationssysteme GmbH

ADSL-PPTP Verbindungen können nach Bedarf gestartet und gestoppt werden.

ACHTUNG: Um Filterregeln für eine ADSL-PPTP Verbindung erstellen zu können, müssen Sie das Interface ppp+ im Filterregelformular verwenden, da der Verkehr bei dieser Verbindung über dieses Interface läuft.



8.5.3.2.1 ADSL PPTP - Detailansicht

Bei der Definition einer ADSL-PPTP Verbindung können folgende Einstellungen vorgenommen werden:

- **Name:** Frei zu wählender Name für die Verbindung. Der Name wird in der Übersicht der Verbindungen angezeigt. Jeder Name kann global nur einmal vergeben werden. Dies gilt auch für bereits konfigurierte Wählverbindungen.
- **IP-Adresse des Modems:** IP-Adresse Ihres PPTP-Modems (z.B. 10.0.0.138).
- **Benutzername:** Vom Provider zugewiesener Benutzername
- **Passwort** bzw. **Passwort (Bestätigung):** Vom Provider zugewiesenes Passwort.
- **Automatisch starten:** Die Verbindung wird automatisch gestartet.
- **Standardroute:** Aktivieren Sie diese Option, falls diese Verbindung als Standardroute verwendet werden soll.
- **Standardroute ersetzen:** Ersetzt beim Aufbau der Verbindung eine bestehende statische Route.
- **Dial on Demand**: Aktiviert das Wählen bei Bedarf. Es wird automatisch eine Verbindung hergestellt, wenn eine Client-Anforderung vorliegt
- **Verbindung aufrechterhalten:** Die Verbindung wird nach einem ungewollten Verbindungsabbruch automatisch wiederhergestellt.
- **Idle (Sekunden):** Geben Sie hier die Wartezeit ein, wie lange das Modem die Verbindung aufrecht erhalten soll, wenn kein Verkehr mehr über die Leitung läuft. Sollten Sie hier zum Beispiel den Wert 10 eingeben, so wartet das Modem nach der letzten Aktivität im Internet noch zehn Sekunden, bis es die Verbindung automatisch beendet.
- **MPPE verwenden:** Verwendet das Microsoft Point-to-Point Encryption Protokoll zur Verschlüsselung der Daten.
- **Einwahlinterface umbenennen auf:** Definieren Sie einen individuellen Namen für das Interface der Wählverbindung (z.B. ext statt ppp+)
- **Geroutete Netzwerke:** Netzwerke, die nach erfolgter Einwahl geroutet werden sollen.
- **Statische IPs:** Zusätzliche statische IP-Adressen der Verbindung

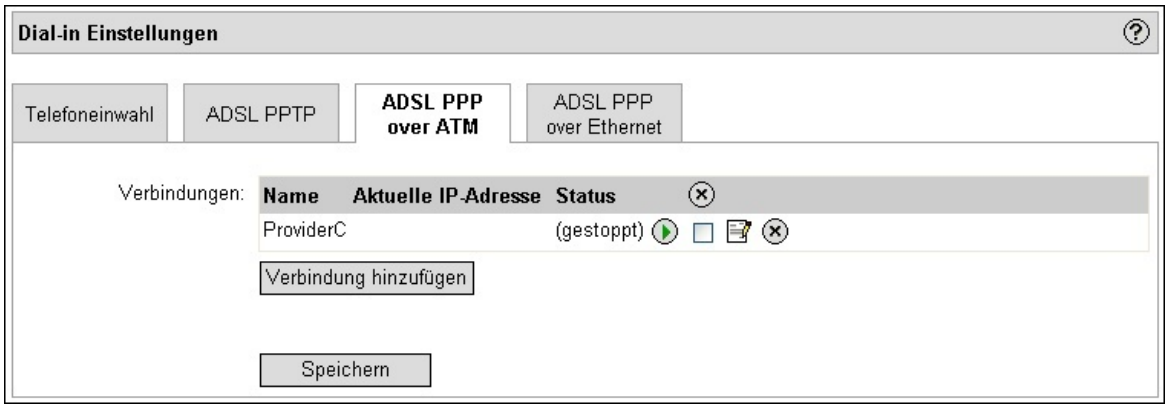
© 2008 by eSYS Informationssysteme GmbH

8.5.3.3 ADSL PPP over ATM

Sie können Gibraltar zur Herstellung von ADSL PPP over ATM Internetverbindungen verwenden. Es kann eine beliebige Anzahl von Verbindungen definiert werden. In dieser Liste sehen Sie eine Übersicht über die bestehenden Verbindungen und können diese bearbeiten. Zusätzlich wird bei einer gestarteten Verbindung die aktuell zugewiesene IP-Adresse angezeigt.

ADSL over ATM Verbindungen können nach Bedarf gestartet und gestoppt werden.

ACHTUNG: Um Filterregeln für eine ADSL over ATM Verbindung erstellen zu können, müssen Sie das Interface ppp+ im Filterregelformular verwenden, da der Verkehr bei dieser Verbindung über dieses Interface läuft.



8.5.3.3.1 ADSL PPP over ATM - Detailansicht

Bei der Definition einer ADSL PPP over ATM Verbindung können folgende Einstellungen vorgenommen werden:

- **Name:** Frei zu wählender Name für die Verbindung. Der Name wird in der Übersicht der Verbindungen angezeigt. Jeder Name kann global nur einmal vergeben werden. Dies gilt auch für bereits konfigurierte Wählverbindungen.
- **Autorisierung:** Wählen Sie das gewünschte Autorisierungsverfahren **PAP** und **CHAP** . Es handelt sich hier um zwei unterschiedliche Anmeldeverfahren, mit denen Sie sich bei Ihrem Provider identifizieren müssen. Entnehmen Sie die für Sie relevante Option aus den Anmeldeunterlagen Ihres Providers.
- **VPI/VCI ATM Paar:** Werte für den Virtual Path Identifier (VPI) und den Virtual Channel Identifier (VCI)
- **Benutzername:** Vom Provider zugewiesener Benutzername
- **Passwort** bzw. **Passwort (Bestätigung):** Vom Provider zugewiesenes Passwort.
- **Automatisch starten:** Die Verbindung wird automatisch gestartet.
- **Standardroute:** Aktivieren Sie diese Option, falls diese Verbindung als Standardroute verwendet werden soll.
- **Standardroute ersetzen:** Ersetzt beim Aufbau der Verbindung eine bestehende statische Route.
- **Dial on Demand:** Aktiviert das Wählen bei Bedarf. Es wird automatisch eine Verbindung hergestellt, wenn eine Client-Anforderung vorliegt
- **Verbindung aufrechterhalten:** Die Verbindung wird nach einem ungewollten

© 2008 by eSYS Informationssysteme GmbH

Verbindungsabbruch automatisch wiederhergestellt.

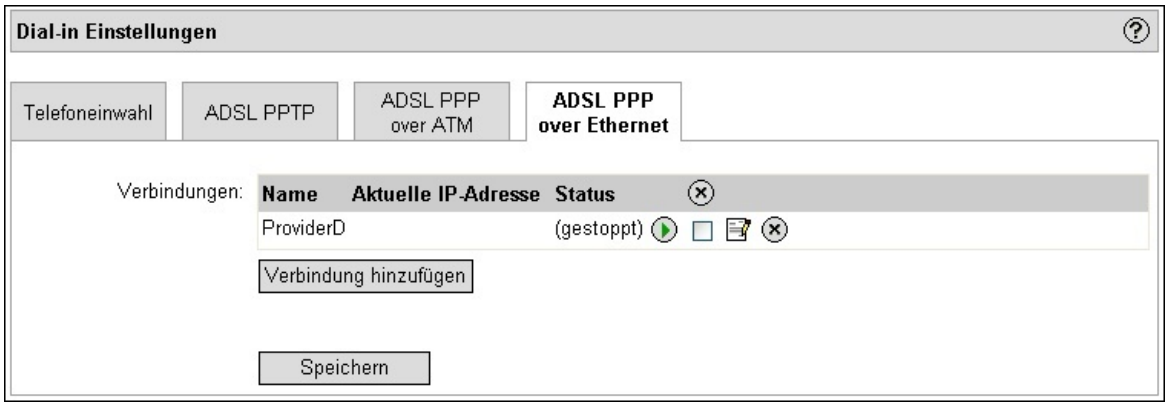
- **Idle (Sekunden):** Geben Sie hier die Wartezeit ein, wie lange das Modem die Verbindung aufrecht erhalten soll, wenn kein Verkehr mehr über die Leitung läuft. Sollten Sie hier zum Beispiel den Wert 10 eingeben, so wartet das Modem nach der letzten Aktivität im Internet noch zehn Sekunden, bis es die Verbindung automatisch beendet.
- **MPPE verwenden:** Verwendet das Microsoft Point-to-Point Encryption Protokoll zur Verschlüsselung der Daten.
- **Einwahlinterface umbenennen auf:** Definieren Sie einen individuellen Namen für das Interface der Wählverbindung (z.B. ext statt ppp+)
- **Geroutete Netzwerke:** Netzwerke, die nach erfolgter Einwahl geroutet werden sollen.
- **Statische IPs:** Zusätzliche statische IP-Adressen der Verbindung

8.5.3.4 ADSL PPP over Ethernet

Sie können Gibraltar zur Herstellung von ADSL PPP over Ethernet Internetverbindungen verwenden. Es kann eine beliebige Anzahl von Verbindungen definiert werden. In dieser Liste sehen Sie eine Übersicht über die bestehenden ADSL PPP over Ethernet Verbindungen und können diese bearbeiten. Zusätzlich wird bei einer gestarteten Verbindung die aktuell zugewiesene IP-Adresse angezeigt.

ADSL PPP over Ethernet Verbindungen können nach Bedarf gestartet und gestoppt werden.

ACHTUNG: Um Filterregeln für eine ADSL PPP over Ethernet Verbindung erstellen zu können, müssen Sie das Interface ppp+ im Filterregelformular verwenden, da der Verkehr bei dieser Verbindung über dieses Interface läuft.



8.5.3.4.1 ADSL PPP over Ethernet - Detailansicht

Bei der Definition einer ADSL PPP over Ethernet Verbindung können folgende Einstellungen vorgenommen werden:
erden in die Detailansicht weitergeleitet.

- **Name:** Frei zu wählender Name für die Verbindung. Der Name wird in der Übersicht der Verbindungen angezeigt. Jeder Name kann global nur einmal vergeben werden. Dies gilt auch für bereits konfigurierte Wählverbindungen.

© 2008 by eSYS Informationssysteme GmbH

- **Interface:** Wählen Sie jenes Interface, das die Verbindung herstellt.
- **Autorisierung:** Wählen Sie das gewünschte Autorisierungsverfahren **PAP** und **CHAP** . Es handelt sich hier um zwei unterschiedliche Anmeldeverfahren, mit denen Sie sich bei Ihrem Provider identifizieren müssen. Entnehmen Sie die für Sie relevante Option aus den Anmeldeunterlagen Ihres Providers.
- **Benutzername:** Vom Provider zugewiesener Benutzername
- **Passwort** bzw. **Passwort (Bestätigung):** Vom Provider zugewiesenes Passwort.
- **Automatisch starten:** Die Verbindung wird automatisch gestartet.
- **Standardroute:** Aktivieren Sie diese Option, falls diese Verbindung als Standardroute verwendet werden soll.
- **Standardroute ersetzen:** Ersetzt beim Aufbau der Verbindung eine bestehende statische Route.
- **Dial on Demand:** Aktiviert das Wählen bei Bedarf. Es wird automatisch eine Verbindung hergestellt, wenn eine Client-Anforderung vorliegt
- **Verbindung aufrechterhalten:** Die Verbindung wird nach einem ungewollten Verbindungsabbruch automatisch wiederhergestellt.
- **Idle (Sekunden):** Geben Sie hier die Wartezeit ein, wie lange das Modem die Verbindung aufrecht erhalten soll, wenn kein Verkehr mehr über die Leitung läuft. Sollten Sie hier zum Beispiel den Wert 10 eingeben, so wartet das Modem nach der letzten Aktivität im Internet noch zehn Sekunden, bis es die Verbindung automatisch beendet.
- **Maximum transmit unit (MTU):** Konfigurieren Sie diese Option falls benötigt
- **Maximum receive unit (MRU):** Konfigurieren Sie diese Option falls benötigt
- **Einwahlinterface umbenennen auf:** Definieren Sie einen individuellen Namen für das Interface der Wählverbindung (z.B. ext statt ppp+)
- **Geroutete Netzwerke:** Netzwerke, die nach erfolgter Einwahl geroutet werden sollen.
- **Statische IPs:** Zusätzliche statische IP-Adressen der Verbindung

8.5.4 Bridging

Im Bridging Modul können zwei oder mehrere Netzwerkkarten zu einer Bridge zusammengefügt werden. Eine Bridge ist die Verbindung zweier Netzwerke auf Ebene 2 des Netzwerkschichtenmodells. Gibraltar ist eine so genannte MAC Bridge. Dabei wird auf der Firewall eine Tabelle aufgebaut, welche die MAC-Adressen aller kommunizierenden Geräte in den verbundenen Netzwerken enthält. Entsprechend dieser Tabelle werden in weiterer Folge sämtliche Netzwerkanfragen an das jeweils richtige Netzwerk weitergeleitet.
Durch die Verwendung einer Bridge kann Gibraltar auf Ebene 3 (TCP/IP) des Netzwerkschichtenmodells transparent eingesetzt werden. Sie können so zum Beispiel die offizielle IP-Adresse der Bridge an einen hinter Gibraltar liegenden Server weitergeben und dennoch den Verkehr, der über die Bridge läuft überprüfen und filtern.
Eine Bridge erlaubt es, IP-Pakete völlig transparent über die beiden Netzwerkkarten zu schicken. Es ist kein Routing oder NAT notwendig. Diese Technik ist bei einer Verwendung von Gibraltar als transparenter Traffic Shaper notwendig. Eine weitere Anwendungsmöglichkeit ist die transparente Einbindung von IDS (Intrusion Detection Systems).

ACHTUNG: Erzeugen Sie nur dann eine Bridge aus zwei oder mehr Netzwerkinterfaces, wenn Ihnen der Hintergrund dieser Technik vollkommen klar ist. Bei falscher Konfiguration

© 2008 by eSYS Informationssysteme GmbH

kann es zu problematischen Sicherheitslücken kommen.

- **Interface:** Eine frei zu wählende Bezeichnung für die Bridge.
- **Statische IPs:** IP-Adresse(n) an, die der Bridge zugewiesen werden sollen.
- **IP hinzufügen:** Betätigen Sie diese Schaltfläche, wenn Sie eine neue IP-Adresse eingeben wollen, die der Bridge zugewiesen werden soll.
- **Bridged Interfaces:** Jene Netzwerkschnittstellen, die Teil der Bridge werden sollen. Die Bridge verbindet anschließend die Netzwerkbereiche, die an diesen Netzwerkinterfaces hängen.

HINWEIS: Die Erstellung der Bridge nach dem Betätigen der Schaltfläche "Speichern" kann etwas dauern. Haben Sie bitte etwas Geduld.

8.5.5 VLAN

Gibraltar unterstützt die Erstellung von virtuellen lokalen Netzwerken (VLAN). Ein VLAN ist ein virtuelles lokales Netzwerk innerhalb eines physikalischen Netzwerkes. Die Unterteilung von physikalischen Netzwerken in einzelne VLANs ist vor allem in folgenden Situationen zielführend:

- Die Broadcast-Last wird sehr hoch. Dieses Problem tritt häufig in MS-Windows-Netzwerken auf.
- Ein großes geswitchtes Netzwerk soll sicherheitstechnisch unterteilt werden.

Eine Lösung für diese Probleme sind VLANs. Mit Hilfe von VLANs können auf einem Switch oder über mehrere Switches hinweg virtuell getrennte Netze betrieben werden. Diese Technik eignet sich auch für die standortübergreifende Vernetzung (z. B. per ATM) mehrerer VLANs über einen Switch bzw. Router. Dabei ist der Realisierungsaufwand von VLANs deutlich geringer als die physikalische Trennung eines Netzwerks mit separaten Switches und Routern.

Funktionsweise

Jedem VLAN wird eine eindeutige Nummer zugeordnet. Man nennt diese Nummer VLAN ID. Ein Gerät, das zum VLAN mit der ID=1 gehört, kann mit jedem anderen Gerät im gleichen VLAN kommunizieren, nicht jedoch mit einem Gerät in einem anderen VLAN mit ID=2, 3, ...

- **Physisches Interface:** Netzwerkschnittstelle, auf welchem ein VLAN gebildet werden soll.
- **Logisches Interface:** Frei zu vergebender Name für das VLAN Interface.
- **VLAN ID:** VLAN ID für das virtuelle Interface. Beachten Sie, dass Sie auch am Switch die VLAN ID vergeben müssen.
- **Statische IPs:** Definieren sie jene IP-Adressen, die dem neuen VLAN-Interface zugewiesen werden sollen.

HINWEIS: Die Erstellung des VLAN Interfaces nach dem Betätigen der Schaltfläche "Speichern" kann etwas dauern. Haben Sie bitte etwas Geduld.

© 2008 by eSYS Informationssysteme GmbH

8.5.6 DHCP-Server

Ein **DHCP-Server** dient der dynamischen Zuweisung von IP-Adressen und Netzwerkeinstellungen innerhalb eines Netzwerks. Wird ein Computer neu in das Netzwerk integriert, so kann er via DHCP eine IP-Adresse aus dem vom **DHCP-Server** zur Verfügung gestellten Bereich beziehen. Gleichzeitig erhält er auch andere Netzwerkeinstellungen (Standardroute, DNS-Server etc.) und muss somit nicht vom Netzwerkadministrator manuell konfiguriert werden.

Im **GibADMIN** besteht die Möglichkeit, für jedes Netzwerkinterface einen DHCP-Server zu konfigurieren. Daher ist neben der Registerkarte für **Allgemeine Einstellungen** auch für jedes Netzwerkinterface mit statischer IP-Adresse eine Registerkarte vorhanden.

8.5.6.1 DHCP - Allgemeine Einstellungen

Definieren Sie die allgemeinen Einstellungen für den DHCP-Server.

- **Domäne:** Domänenname des DHCP-Netzwerks. Der angegebene Domänenname wird sämtlichen DHCP-Clients zugewiesen.
- **Standard Lease Periode:** Die Dauer, für die ein Lease standardmäßig gültig ist, wenn vom Client nicht explizit eine andere Lease-Dauer angefordert wird.
- **Maximale Lease Periode:** Die maximale Lease Dauer, die der DHCP-Server dem Client erlaubt.

ACHTUNG: Wenn Sie in einem physikalischen Netzwerk mehrere DHCP-Server laufen haben, kann es zu Komplikationen und unerwünschten Nebeneffekten kommen.

8.5.6.2 DHCP - Konfiguration

Um für einen Netzwerkbereich einen DHCP-Server zur Verfügung zu stellen, sind einige detailliertere Einstellungen erforderlich, die in der Registerkarte jener Netzwerkkarte durchgeführt werden müssen, die IP-Adressen im Netzwerk anbieten soll.

- **DHCP aktivieren:** Aktiviert für das entsprechende Netzwerk-Interface den DHCP-Server.
- **IP-Adresse:** Definiert, über welche der Netzwerkkarte zugewiesene IP-Adresse der DHCP-Server den Clients antworten soll.
- **IP Wertebereich:** Jene IP-Adressbereiche aus denen die Clients die IP-Adressen beziehen können. Ein Adressbereich besteht aus einer Start-IP- und einer End-IP-Adresse.
- **DNS Server:** Die IP-Adressen der DNS-Server, die an die DHCP-Clients übermittelt werden.
- **Router:** Die IP-Adressen der Router (Standardgateway), die an die DHCP-Clients übermittelt werden.
- **WINS Server:** Die IP-Adressen der WINS-Server, die an die DHCP-Clients übermittelt werden.
- **Reservierungen:** Reservierung einer IP-Adresse für ein Gerät mit einer bestimmten MAC-Adresse. Die Reservierung können Sie z.B. zur Beschränkung der IP-Adressvergabe in WLANs verwenden.

© 2008 by eSYS Informationssysteme GmbH

8.5.6.3 DHCP leases

Zeigt eine Liste mit den derzeit aktuellen DHCP-Clients. Ein Lease bezeichnet jenen Zeitraum, für den der DHCP-Server für ein Gerät mit einer bestimmten MAC-Adresse eine definierte IP-Adresse bereithält.

- **IP-Adresse:** Dem Client zugewiesene IP-Adresse.
- **Hostname:** Hostname des Clients.
- **MAC-Adresse:** MAC-Adresse jener Netzwerkkarte, die die DHCP-Einstellungen bezogen hat.
- **Lease Beginn:** Zeitpunkt der Zuweisung der IP-Adresse für diesen Client.
- **Lease Ende:** Zeitpunkt, bis zu dem die zugewiesene IP-Adresse für die angegebene MAC-Adresse reserviert wird. So kann sichergestellt werden, dass regelmäßige DHCP-Clients immer die gleiche IP-Adresse erhalten.

8.5.6.4 DHCP-Relay

Der Dienst DHCP-Relay wird benötigt, wenn Sie DHCP-Anforderungen von Clients in andere Netzwerksegmente weiterleiten wollen. Das ist notwendig, wenn sich der DHCP-Server in einem anderen Netzwerksegment als die Clients befindet.

Wollen Sie das DHCP-Relay aktivieren müssen Sie folgende Einstellungen treffen:

- **IP-Adresse des DHCP-Servers:** Die IP-Adresse des DHCP-Servers, an den die DHCP-Requests gestellt werden
- **Interfaces:** Aktivieren Sie jene Interfaces, die an der Weiterleitung der DHCP-Requests beteiligt sind (also auch jenes, wo der DHCP-Server hängt).

ACHTUNG: Zusätzlich zur Aktivierung des DHCP-Relays benötigen Sie auch entsprechende Firewall-Regeln, welche die DHCP-Request vom Client zum Server erlauben.

8.5.7 Dynamic DNS

Mit Dynamic DNS (DDNS) können Sie einen Hostnamen (Fully Qualified Domain Name FQDN) für Ihre offizielle IP-Adresse vergeben, auch wenn diese dynamisch zugewiesen wird. Dazu müssen Sie einen Account bei einem Anbieter dieses Services anlegen (http://www.dyndns.org bietet die Möglichkeit für bis zu 5 Gratis Hostnamen-Eintragungen).

- **Update bei Einwahl:** Aktualisiert den DNS-Eintrag mit der aktuellen IP-Adresse bei jeder Einwahl in das Internet.
- **Update Intervall (Minuten):** Update-Intervall, in dem der DNS-Eintrag automatisch aktualisiert wird. Ein Update wird nur ausgeführt, wenn sich die IP-Adresse in der Zwischenzeit geändert haben sollte.
- **Hostname:** Hostname der Gibraltar Firewall. Entspricht dem von Ihnen gewählten Hostnamen bei DynDNS.
- **Login:** Benutzername Ihres DynDNS-Accounts.
- **Passwort:** Passwort Ihres DynDNS-Accounts.
- **Aktuelle IP-Adresse:** Aktuell zugewiesene IP-Adresse.

© 2008 by eSYS Informationssysteme GmbH

8.6 Firewall

Im Modul **Firewall** werden die Filterregeln für den Paketfilter festgelegt. Dabei handelt es sich um die Kernfunktionalität der Firewall. Es wird festgelegt, welche Pakete die Firewall passieren dürfen, welche geblockt oder abgelehnt werden und welche Pakete zusätzlich protokolliert werden. Anhand mehrerer Filterkriterien können einzelne Pakete unterschieden und individuelle Regeln erstellt werden.
Eine Firewall-Regel (Policy) wird immer für ein eingehendes und ein ausgehendes Interface (Track) erstellt. So kann z.B. eine Regel erstellt werden, die den gesamten Verkehr blockiert, der von der externen Netzwerkschnittstelle auf die interne Netzwerkschnittstelle vorgesehen ist.

HINWEIS: Standardmäßig ist Gibraltar so konfiguriert, dass kein Vekehr passieren darf. Es ist lediglich ein Wartungszugriff auf Gibraltar gestattet. Eine nicht konfigurierte Gibraltar Firewall stellt also kein Sicherheitsrisiko dar sondern blockiert jeglichen Verkehr. Dies gilt auch für den Netzwerkverkehr vom internen Netzwerk in das Internet.

8.6.1 Firewallregeln

Auswahl des ein- und ausgehenden Interfaces

In der Übersicht "Firewallregeln" finden Sie immer nur jene Regeln, welche für das entsprechende eingehende und ausgehende Interface definiert sind. Eine Gesamtübersicht aller Regeln finden sie in der entsprechenden Registerkarte.
Um eine Filterregel zu erstellen, müssen Sie sowohl das eingehende wie auch das ausgehende Interface auswählen. Die Firewall-Regel gilt dann für jene Datenpakete, die beim eingehenden Interface hereinkommen und beim ausgehenden Interface hinausgehen. Wir nennen den Weg eines Datenpakets einen Track.

Sollen zum Beispiel Pakete vom internen Interface auf das externe gefiltert werden, so wählen Sie im Auswahlfeld **eingehend** den Namen des internen Interfaces aus (z.B. "int0") und im Auswahlfeld **ausgehend** den Namen des externen Interfaces (z.B. "ext0"). Anschließend betätigen Sie die Schaltfläche **Go!** und die Anzeige der Filterregeln in der darunterliegenden Elementgruppe wird aktualisiert und jene Regeln werden aufgelistet, die für den ausgewählten Weg bereits gespeichert worden sind.

In der Auswahlliste befinden sich auch einige besondere Einträge. Der Listeneintrag "**ANY**" sollte gewählt werden, wenn Sie die Filterung nicht auf ein spezielles Interface beschränken wollen. Die Filterregeln werden in der Folge auf alle zur Verfügung stehenden Interfaces angewendet.
Der Listeneintrag "**LOCAL**" bezeichnet jene Pakete, die direkt von Gibraltar bzw. direkt zu Gibraltar gesendet werden. Das können zum Beispiel Zugriffe auf den lokalen Proxy, oder auch zu einem (IPSec-, PPTP-, SSL-) Tunnel gehörige Pakete sein. Sie können also einen Filter auf alle jene Pakete anwenden lassen, die von einem bestimmten Interface auf Gibraltar selbst geschickt werden sollen, indem Sie als eingehendes Interface das Entsprechende auswählen und als ausgehendes Interface "LOCAL" auswählen. Für bereits konfigurierte IPSec Interfaces werden ebenfalls Einträge in den Auswahlfeldern erzeugt (z.B. "ipsec0").

HINWEIS: Die Auswahl eingehendes Interface "ANY" und ausgehendes Interface "ANY" bezeichnet FORWARD-Filterregeln (durch die Firewall durchgehende Pakete werden überprüft), bei denen das eingehende und das ausgehende Interface nicht relevant sind. Es können damit jedoch keine INPUT- oder OUTPUT-Filterregeln (für die Firewall bestimmte

© 2008 by eSYS Informationssysteme GmbH

bzw. von der Firewall kommende Pakete werden überprüft) erzeugt werden.

Konfiguration des dynamischen Paketfilters (Stateful Inspection)

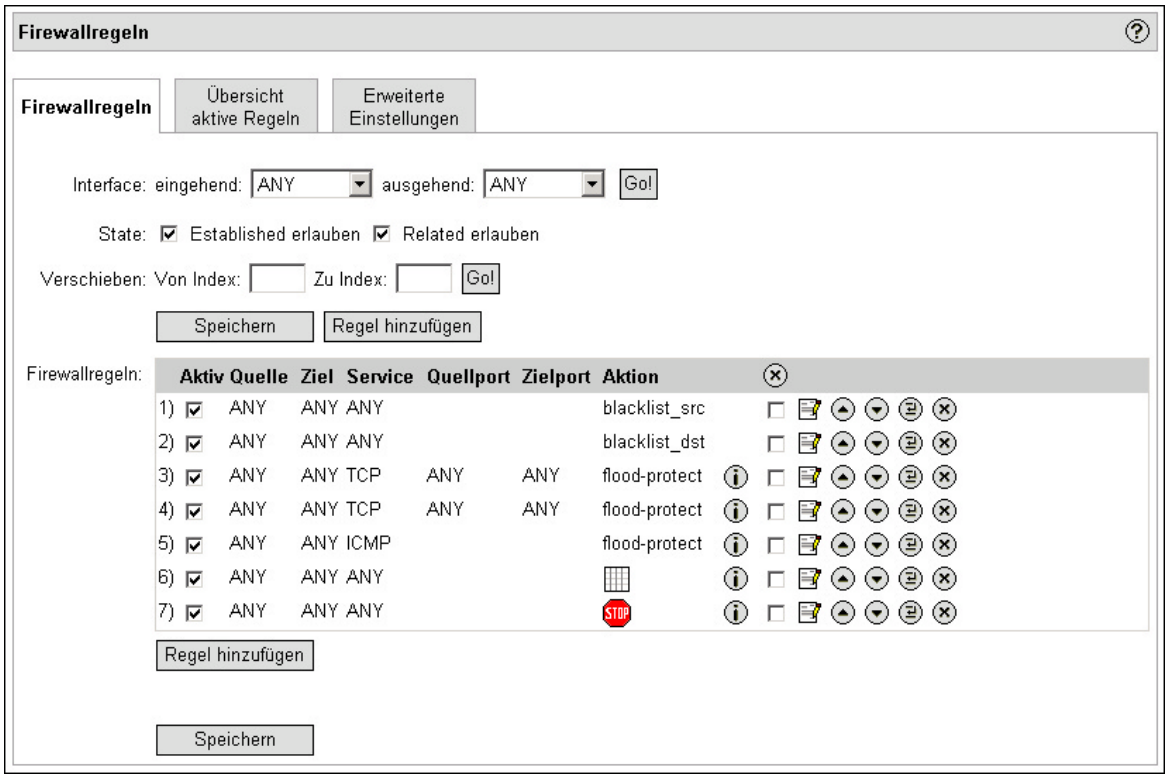
Die dynamische Paketfilterung erlaubt es, Pakete zu filtern, die einer bereits bestehenden Verbindung zugeordnet werden können (Connection Tracking). Damit ist es möglich, Antwortpakete zu bereits bestehenden Verbindungen automatisch zu erlauben. Es muss keine separate Regel für den Antwortverkehr erstellt werden. Wollen Sie z.B. den Zugriff auf externe Webserver erlauben, so reicht es im Fall von Stateful Inspection, den ausgehenden Datenverkehr den Zielport 80 zu erlauben. Die Antwortpakete der Webserver werden in diesem Fall automatisch akzeptiert und der entsprechenden bestehenden Verbindung zugeordnet.

- **Established erlauben:** Es werden alle Pakete erlaubt, die einer bereits bestehenden Verbindung zugeordnet werden können. Beispielsweise wären dies Antwortpakete einer HTTP Anfrage nach außen, wobei Gibraltar diese Antwortpakete des HTTP-Servers an den Client als **established** erkennt. Die Einstellung gilt für alle Pakete in der aktuellen Kombination von eingehendem und ausgehendem Interface.
- **Related erlauben:** Es wird die Weiterleitung aller Pakete erlaubt, die als zu einer bereits bestehenden Verbindung zugehörig angesehen werden können. Bspw. funktioniert der Verbindungsaufbau bei FTP über den Port 21, die Daten werden über den Port 20 transportiert. Gibraltar erkennt diese zur Kontrollverbindung zugehörige Datenverbindung auf dem Port 20 als **related**. Die Einstellung gilt für alle Pakete in der aktuellen Kombination von eingehendem und ausgehendem Interface.

Ändern der Reihenfolge

Firewall-Regeln werden in einer definierten Reihenfolge abgearbeitet. Die Abarbeitungsreihenfolge entspricht der Sortierung in der Übersicht. Wollen Sie also erreichen, dass eine bestimmte Regeln vor oder nach einer anderen Regeln abgearbeitet werden soll, ist es notwendig, die Sortierung nachträglich zu ändern. Sie können dies erreichen indem Sie den Indexeintrag der entsprechenden Regel verändern.

© 2008 by eSYS Informationssysteme GmbH



Regelübersicht

Die Paketfilterregeln werden beim Eintreffen eines Paketes von oben nach unten abgearbeitet, bis die Optionen einer Regel auf das eintreffende Paket zutreffen. Die Reihenfolge der Paketfilterregeln ist daher von großer Bedeutung. Nachdem ein eingehendes und ein ausgehendes Interface in den entsprechenden Auswahlfeldern ausgewählt wurden, werden in der Elementgruppe **Firewallregeln** die zu diesem Track zugehörigen Paketfilterregeln dargestellt. In der Übersicht der Paketfilterregeln kann die Reihenfolge verändert werden. Auch das Editieren oder Löschen einzelner Regeln wird von hier aus durchgeführt.

- **Regel hinzufügen:** Erzeugt eine neue Filterregel am Ende der Liste. Sie werden in die Detailansicht der Regel weitergeleitet. Diese Schaltfläche findet sich sowohl am Anfang als auch am Ende der Übersicht.
- **Speichern:** Speichert die aktuellen Einstellungen der Übersicht und die Reihenfolge der Regeln.

In der Übersicht finden Sie folgende Informationen:

- **Aktiv:** Aktiviert oder deaktiviert eine Firewall-Regel. Deaktivierte Regeln werden nicht berücksichtigt.
- **Quelle:** Zeigt die Quell IP-Adresse/das Quell Subnetz/den Quell FQDN dieser Regel. Wird keine IP-Adresse angegeben (ANY), so ist die Quelle für diese Regel irrelevant und es werden alle Quelladressen akzeptiert.
- **Ziel:** Zeigt die Ziel IP-Adresse/das Ziel Subnetz/den Ziel FQDN dieser Regel. Wird keine IP-Adresse angegeben (ANY), so ist das Ziel für diese Regel irrelevant und es werden alle Zieladressen akzeptiert.
- **Service:** Service dieser Regel. Wird kein Service angegeben (ANY), so wird dieser ignoriert.

© 2008 by eSYS Informationssysteme GmbH

- **Quellport:** Quellport der Regel. Dieser Wert wird nur dargestellt, sofern beim Service der Wert **CUSTOM** gewählt wurde, da ein Service auch die Quellportdefinitionen enthält.
- **Zielport:** Zielport einer Regel. Dieser Wert wird nur dargestellt, sofern beim Service der Wert **CUSTOM** gewählt wurde, da ein Service auch die Quellportdefinitionen enthält.
- **Aktion:** Zeigt, wie in weiterer Folge mit dem Paket verfahren werden soll, wenn diese Regel greift. Folgende Werte sind möglich: **ACCEPT**, **DROP**, **LOG**, **REJECT** und **NONE**
  ACCEPT: Paket wird zur Weiterleitung freigegeben.
  DROP: Paket wird verworfen.
  LOG: Es wird ein Eintrag in der Syslog-Datei erzeugt. Diese Einstellung sagt aber nichts darüber aus, wie das Paket weiter behandelt wird. Folgt im Anschluss an eine Regel mit einem Target **LOG** eine Regel mit gleicher Konfiguration nur mit dem Target **ACCEPT**, so wird zwar ein Eintrag in der LOG Datei erzeugt, anschließend wird das Paket jedoch akzeptiert und weitergeleitet.
  REJECT: Verweigert dem Paket die Weiterleitung wie **DROP**, es wird jedoch gleichzeitig eine ICMP Fehlernachricht ("port-unreachable") an den Sender des Pakets zurückgesendet
  NONE: Das Paket wird von dieser Regel ignoriert. Sie benötigen diese Aktion, um bspw. Monitoring Regeln zu erstellen.
  Wird hier ein anderer Wert angezeigt (z.B. flood-protect), so handelt es sich um spezielle Regeln, die nicht verändert werden können. Diese Regeln dienen dazu, die Sicherheit und Zuverlässigkeit von Gibraltar zu erhöhen.
- **Kommentar** : Zeigt einen Tooltip (Bewegen Sie den Mauszeiger über das Symbol) mit dem Kommentar zur entsprechenden Regel. Sie können zu jeder Regel einen eigenen Kommentar erstellen.
- **Markierte Einträge löschen** : Markieren Sie jene Einträge in der Elementgruppe durch Aktivieren des Kontrollkästchens, die Sie löschen wollen. Betätigen Sie anschließend die Schaltfläche in der Kopfzeile, um die Elemente zu löschen.
- **Regel nach oben schieben** und **Regel nach unten schieben** : Betätigen Sie eine dieser Schaltflächen, um die entsprechende Regel in der Reihenfolge nach oben bzw. nach unten zu verschieben. Diese Funktionen sind notwendig, da sämtliche Regeln von oben nach unten abgearbeitet werden und jeweils die erste zutreffende Regel ein Paket behandelt.
- **Regel bearbeiten** : Betätigen Sie diese Schaltfläche, um die entsprechende Regel zu bearbeiten. Sie werden in die Detailansicht der Regel weitergeleitet.
- **Regel darunter einfügen** : Betätigen Sie diese Schaltfläche, um nach dieser Regel eine neue Regel einzufügen. Sie werden in die Detailansicht der Regel weitergeleitet.
- **Regel löschen** : Betätigen Sie diese Schaltfläche, um die Regel zu löschen. Falls Sie eine Regel nur zeitweilig deaktivieren wollen, siehe oben (Aktiv).

8.6.2 Übersicht aktiver Regeln

In der Übersicht aller aktiven Regeln finden Sie eine komplette Auflistung aller Firewall-Regeln unabhängig vom Track. Zusätzlich zu jenen Informationen, die sie auch in der Übersicht "Firewallregeln" finden, enthält diese Übersicht auch den Track der Regel. Die Spalte Interface zeigt das eingehende und das ausgehende Interface in der Form **EINGEHEND -> AUSGEHEND**.

© 2008 by eSYS Informationssysteme GmbH

In dieser Übersicht ist es nicht möglich, neue Regeln zu erstellen. Sie können jedoch bestehende Regeln bearbeiten oder löschen.

8.6.3 Erweiterte Einstellungen

Unter den erweiterten Einstellungen können Sie folgende Details des Paketfilters konfigurieren:

- **DNS Aktualisierungsrate:** Wenn in den Firewallregeln Hostnamen verwendet werden, werden die im hier angegebenen Intervall beim DNS-Server nachgeschlagen und die Firewallregeln damit aktualisiert.
- **Maximale gleichzeitige Verbindungen:** Die maximale Anzahl gleichzeitiger Verbindungen, welche Gibraltar bearbeiten kann.
- **TCP liberal:** Deaktiviert die strikte TCP-Prüfung. TCP-Verbindungen werden dann nicht beim Auftreten von INVALID Paketen abgebrochen.
- **ARP-Caching aktivieren:** Aktiviert oder deaktiviert den ARP-Cache (Zuordnung von MAC-Adressen zu IP-Adressen). In manchen Fällen kann es notwendig sein, das ARP-Caching zu deaktivieren. Standardmäßig ist das ARP-Caching aktiviert.
- **Größe des ARP-Cache (Einträge):** Die maximale Anzahl der Einträge im ARP-Cache.

8.6.4 Firewallregel bearbeiten

In der Detailansicht werden Firewall-Regeln bearbeitet oder neu erstellt. Folgende Einstellungen können vorgenommen werden:

- **Regel aktivieren:** Aktiviert die Firewall-Regel. Deaktivierte Regeln werden nicht berücksichtigt.
- **Quelladresse:** Quelladresse (Absender) des Datenpakets. Sie können sowohl einen bereits definierten Host/Netz Alias oder eine Host/Netz Gruppe auswählen. Alternativ ist es möglich, eine frei definierte IP-Adresse, einen IP-Adressbereich oder einen FQDN anzugeben (CUSTOM). Ist die Quelladresse für diese Regel nicht relevant, so wählen Sie aus dem Auswahlfeld die Option **ANY**. Sollten alle Adressen außer der angegebenen berücksichtigt werden, aktivieren Sie das Kontrollkästchen **ausgenommen** neben dem Textfeld.
- **Zieladresse:** Zieladresse (Empfänger) des Datenpakets. Sie können sowohl einen bereits definierten Host/Netz Alias oder eine Host/Netz Gruppe auswählen. Alternativ ist es möglich, eine frei definierte IP-Adresse, einen IP-Adressbereich oder einen FQDN anzugeben (CUSTOM). Ist die Zieladresse für diese Regel nicht relevant, so wählen Sie aus dem Auswahlfeld die Option **ANY**. Sollten alle Adressen außer der angegebenen berücksichtigt werden, aktivieren Sie das Kontrollkästchen **ausgenommen** neben dem Textfeld.
- **Service:** Service (Protokoll und Ports) des Datenpakets. Services können frei definiert werden und mehrere Protokolle oder Ports umfassen. Sie finden die Definitionen der Services im Modul **Netzwerk**. Sollten Sie die Option **ANY** wählen, so wird dieses Feld bei der Überprüfung des Paketes nicht berücksichtigt. Sollten Sie hier den Service **CUSTOM** wählen, so wird das Formular automatisch erweitert (Java Script Aktivierung erforderlich). Sollte Java Script nicht aktiviert sein, so betätigen Sie nach der Auswahl des Protokolls die **Go!** Schaltfläche. Die Optionen, die bei der Auswahl der Protokolle **TCP** und **UDP** zusätzlich konfiguriert werden können, werden weiter unten im Punkt **Besonderheiten von TCP/UDP** näher erläutert.
- **Status:** Status der Verbindung für dynamische Paketfilterung. Die möglichen

© 2008 by eSYS Informationssysteme GmbH

Optionen sind
ANY: Der Status des zu prüfenden Pakets wird ignoriert.
NEW: Behandelt alle Pakete, die das erste Mal mit dieser Adresskombination auf Gibraltar treffen, also beim Aufbau einer neuen Verbindung.
ESTABLISHED und **RELATED:** Diese Optionen werden im Kapitel **Firewallregeln** im Punkt **Konfiguration des dynamischen Paketfilters** erläutert.
INVALID: Behandelt alle Pakete, die mit keiner Gibraltar bekannten Verbindung in Zusammenhang gebracht werden können, jedoch auch nicht eine neue Verbindung aufbauen.

- **Aktion:** Aktion die ausgeführt wird, wenn ein Datenpaket die angegebenen Kriterien erfüllt. Die möglichen Aktionen sind **ACCEPT**, **DROP**, **LOG**, **REJECT** oder **NONE**, Eine Beschreibung der Aktionen finden Sie im Kapitel **Firewallregeln**.
- **Kommentar:** Kommentar zur Firewall-Regel. Der Kommentar wird als Tooltip in der Regelübersicht angezeigt.
- **Monitoring aktivieren:** Aktiviert das Monitoring für die angegebene Regel. Bei aktiviertem Monitoring wird der Traffic auf den die angegebene Regel zutrifft protokolliert und kann in weiterer Folge grafisch ausgewertet werden. Zur Identifikation der Regel im **Monitoring**-Modul müssen sie einen Namen definieren.
- **Monitoring-Regel für jede IP-Adresse in der Quelladresse erzeugen:** Aktivieren Sie dieses Kästchen, wenn Sie für jede IP-Adresse im Quellbereich eine Monitoring Regel erzeugen wollen. Wenn Sie bspw. für das Netz 192.168.0.0/24 eine detaillierte Traffic-Auswertung brauchen, so verwenden Sie diesen Wert für den Quellbereich und aktivieren gleichzeitig diese Option.
- **Monitoring-Regel für jede IP-Adresse in der Zieladresse erzeugen:** Aktivieren Sie dieses Kästchen, wenn Sie für jede IP-Adresse im Zielbereich eine Monitoring Regel erzeugen wollen. Wenn Sie bspw. für das Netz 192.168.0.0/24 eine detaillierte Traffic-Auswertung brauchen, so verwenden Sie diesen Wert für den Zielbereich und aktivieren gleichzeitig diese Option.

ACHTUNG: Wenn Sie beispielsweise den gesamten Traffic des Netzes 192.168.0.0/24 mitprotokollieren wollen, dann brauchen Sie je eine Regel für den eingehenden und für den ausgehenden Verkehr. Bspw. von **int** -> **ext** und von **ext** -> **int**!

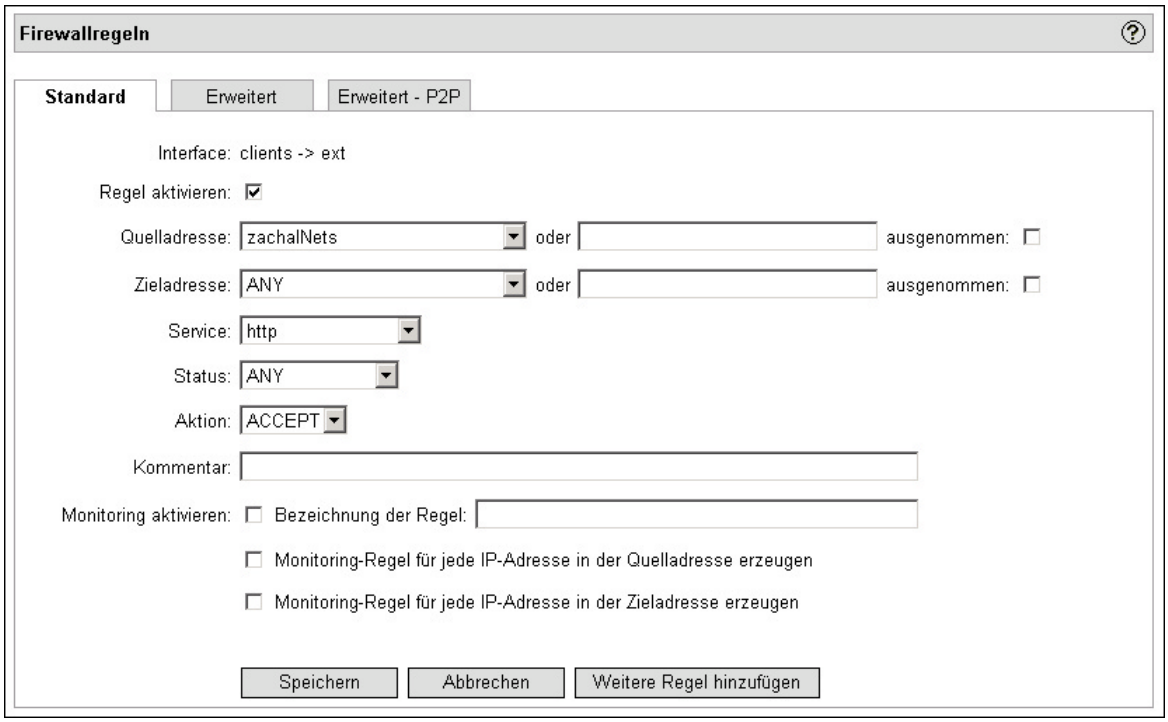
Die Felder, die nur bei Auswahl eines bestimmten Protokolls konfiguriert werden können, sind folgende:

- **Auswahl des Protokolls TCP oder UDP:**
  Quellport: Im Auswahlfeld **Quellport** wählen Sie einen der angegebenen Ports aus. Kommt das zu überprüfende Paket vom ausgewählten Port, so werden die weiteren Optionen dieser Regel überprüft. Bei der Auswahl von **ANY** wird diese Option ignoriert und bei der Überprüfung des Pakets nicht berücksichtigt. Die Option **CUSTOM** erlaubt die Angabe eines nicht in der Liste angeführten Ports oder eines Portbereichs im nebenstehenden Textfeld. Sie können entweder einen Port von 1 bis 65535 angeben oder einen Bereich. Ein Bereich wird durch die Angabe von Startport und den Endport, getrennt durch einen Doppelpunkt, definiert (z.B.: 2400:2600 bezeichnet die Ports von 2400 bis 2600). Optional besteht die Möglichkeit, alle Ports bis oder ab einem bestimmten Port zu wählen. Durch die Angabe eines Doppelpunkts gefolgt von einer Portnummer werden alle Ports bis zu dieser Nummer berücksichtigt, durch die Angabe einer Portnummer gefolgt von einem Doppelpunkt werden alle Ports ab dieser Portnummer miteinbezogen (z.B.: :500 für alle Ports von 1-500; 500: für alle Ports von 500 bis 65535).
  Zielport: Im Auswahlfeld **Zielport** wählen Sie einen der angegebenen Ports aus.

© 2008 by eSYS Informationssysteme GmbH

Kommt das zu überprüfende Paket am ausgewählten Port an, so trifft diese Option zu und die restlichen Optionen werden überprüft. Die Auswahl aus dem Auswahlfeld bzw. die Eingabe im Textfeld erfolgt wie beim Quellport.

- **Auswahl des Protokolls ICMP:**
  ICMP Typ: Wählen Sie den Typ des ICMP Paketes aus der Auswahlliste. Folgende Optionen sind möglich, wobei die Auswahl des Typs **ANY** auf alle Typen des Pakets zutrifft:
  echo-request
  echo-reply
  destination-unreachable
  source-quench
  redirect
  router-advertisement
  router-solicitation
  time-exceeded
  parameter-problem
  timestamp-request
  timestamp-reply
  address-mask-request
  address-mask-reply



8.6.5 Firewallregel - Erweitert

Neben den gebräuchlichsten Filtereinstellungen werden von Gibraltar auch noch weitere Optionen unterstützt, die eine detailliertere Paketfilterung zulassen.

Der erste Teil - **Match Extensions** - beschäftigt sich mit der Überprüfung der Regeln durch angegebene Werte. Falls das zu überprüfende Paket den angegebenen Werten entspricht (match), trifft diese Regel zu und das Paket wird dementsprechend behandelt.

© 2008 by eSYS Informationssysteme GmbH

Folgende Optionen stehen hierbei zur Verfügung:

- **Fragmentierung:** Wählen Sie aus dem Auswahlfeld eine der Optionen aus, um zu überprüfen, ob das Paket ein Teil eines größeren Pakets ist. Pakete, die eine gewisse Größe überschreiten, werden fragmentiert, also in mehrere kleine Pakete unterteilt. Sie können hier zwischen drei Möglichkeiten auswählen.
  none: Wählen Sie diese Option, wenn Sie diese Funktion nicht verwenden wollen.
  not fragmented: Wählen Sie diese Option, wenn nicht fragmentierte Pakete behandelt werden sollen.
  fragmented: Wählen Sie diese Option, wenn fragmentierte Pakete behandelt werden sollen.
  Wird ein Paket bspw. in drei kleinere Pakete unterteilt, so wird beim zweiten und beim dritten Teil ein Bit für die Fragmentierung gesetzt. Ist nun die Option **fragmented** aktiviert, so werden der zweite und dritte Teil gefiltert. Im Fall der Auswahl **not fragmented** wird nur der erste Teil gefiltert.
- **Quell MAC-Adresse:** Geben Sie hier eine MAC-Adresse an, wenn Sie die Behandlung auf spezielle MAC-Adressen einschränken wollen. Jedes Netzwerkinterface wird durch eine eindeutige Kennung identifiziert. Diese besteht aus einer sechsteiligen Kombination, in der Hersteller und Typ kodiert enthalten sind. Die sechs Teile der Kennung, die aus jeweils zwei hexadezimalen Ziffern (0-9, A-F) bestehen, werden durch Doppelpunkte unterteilt. Durch diese Option kann man nur Pakete von bestimmten Netzwerkkarten bzw. Modems zulassen, was die Sicherheit, jedoch auch den Wartungsaufwand enorm erhöht.
- **Limit:** Durch diese Option haben Sie die Möglichkeit, zu dieser Regel passende Pakete bis zu einer gewissen Anzahl ihres Auftretens zu filtern. Kommt es zum Beispiel durch eine Attacke zu einer Häufung von Anfragen von der IP-Adresse 4.3.2.1 auf verschiedenste Ports von Gibraltar, so kann man durch eine Angabe im Textfeld **Limit** bestimmen, dass die Pakete nur bis zu einer gewissen Anzahl von Anfragen angenommen werden. Hier sind also nur numerische Werte möglich. Diese Anzahl muss in einem in dem anschließenden Auswahlfeld angegebenen, zeitlichen Bereich erfolgen. Mögliche Werte sind hier **/second, /minute**, **/hour** oder **/day**. Durch die zusätzliche Angabe eines Wertes im Textfeld **Limit-burst** können Sie eine manchmal, zum Beispiel beim Verbindungsaufbau, auftretende Häufung an Paketen abfangen. Am einfachsten erklärt ist die Limitoption mit einem Behälter, der ein Loch hat, durch das Objekte entweichen können. Solange Objekte im Behälter sind, spricht die Regel an. Zu Beginn sind soviele Objekte im Behälter, wie der Wert in **Limit-burst** beträgt. Für jedes entsprechende Paket wird ein Objekt durch das Loch entfernt. Erreicht man die durch **Limit** festgesetzte Grenze nicht innerhalb der angegebenen Zeiteinheit, so wird der Vorrat wieder um ein Objekt erhöht, bis er wieder den Wert von **Limit-burst** erreicht. Wird das **Limit** erreicht, so greift diese Regel nicht mehr.
- **Beispiel für die Anwendung: Verhinderung von DoS-Attacken (z.B. SYN-Flood, Ping of Death).**
- **SPI:** Geben Sie hier einen Wert ein, wenn Sie Pakete des AH- bzw. ESP-Protokolls matchen wollen, die auf dem Security Parameter Index (SPI) basieren. Jede Funktion von IPSec fügt einen optionalen Header zum IP Paket hinzu. Mit dem SPI, der in diesem zusätzlichen Header enthalten ist, geben Sie einen numerischen Wert ein, auf dessen Basis die Verschlüsselungsverfahren ausgewählt werden. Es kann hier auch ein Bereich eingegeben werden, wobei der Start- und der Endwert mit einem Doppelpunkt zu trennen sind und der Startwert kleiner als der Endwert sein muss (z.B. 480:500).

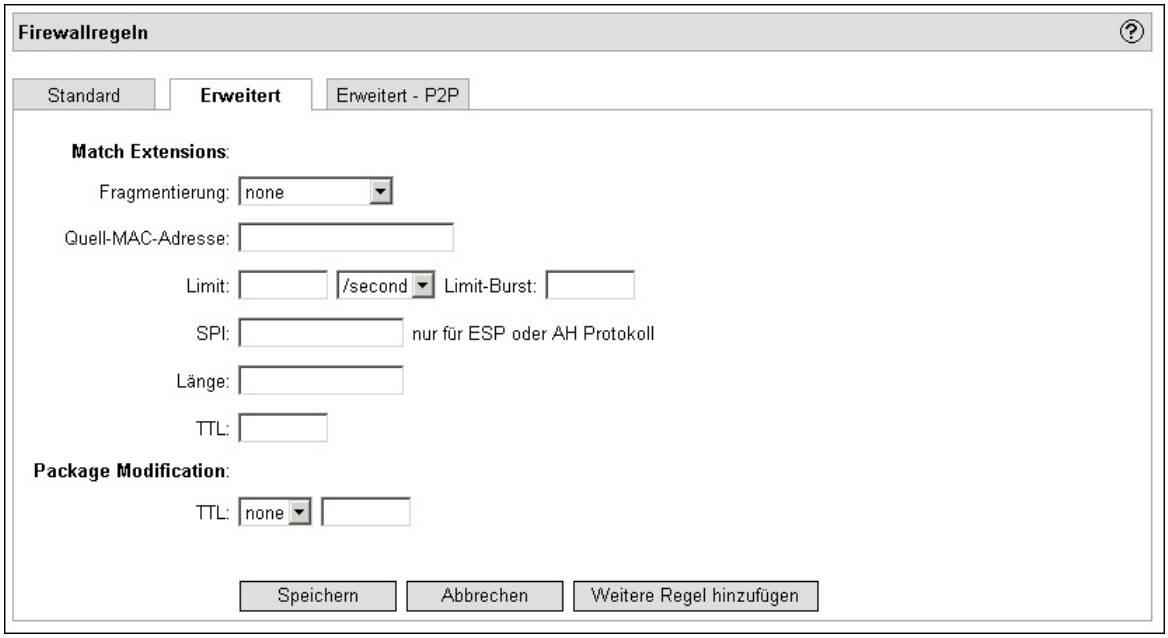
© 2008 by eSYS Informationssysteme GmbH

- **Länge:** Geben Sie einen numerischen Wert in dieses Textfeld ein, um die Länge des Paketes zu überprüfen. Dieser Wert kann sowohl ein einzelner Wert sein, als auch einen Bereich umfassen, der mit einem Doppelpunkt zwischen Start- und Endwert definiert werden muss (z.B. 800:1000) und der kleinere Wert links stehen muss. Trifft ein Paket mit der definierten Länge ein, so wird es entsprechend des Target dieser Regel weiterbehandelt. Die Längenangabe ist in Bytes definiert.
- **TTL:** Durch die Eingabe eines numerischen Wertes in dieses Textfeld **TTL** wird das **Time To Live** Feld des eintreffenden Pakets überprüft. Liegt eine Übereinstimmung vor, so soll entsprechend der Regel vorgegangen werden. Der Wert **Time To Live** in einem Paket gibt an, wie viele Hops, also Schritte ein Paket von einem Netzwerkelement zum nächsten auf dem Weg durch das Internet durchführen soll, bevor es ungültig und verworfen wird.

Der zweite Teil - **Package Modification** - beschäftigt sich mit der Veränderung der Pakete. Eintreffende Pakete werden in der angegebenen Form verändert, wenn sie den Werten der übrigen Optionen entsprechen.

Folgende Optionen stehen hierbei zur Verfügung:

- **TTL:** Wählen Sie aus dem Auswahlfeld eine Option aus, um den Wert des TTL-Feldes des Paketes zu verändern. Mögliche Optionen sind:
  none: Wählen Sie diese Option, um keine Veränderung durchzuführen.
  set: Wählen Sie diese Option, um das TTL-Feld auf den Wert im nebenstehenden Textfeld zu setzen.
  inc: Wählen Sie diese Option, um das TTL-Feld um den Wert im nebenstehenden Textfeld zu erhöhen.
  dec: Wählen Sie diese Option, um das TTL-Feld um den Wert im nebenstehenden Textfeld zu verringern.



© 2008 by eSYS Informationssysteme GmbH

8.6.6 Firewallregel - Erweitert P2P

Auf dieser Registerkarte können Sie Einstellungen zu einigen Peer-to-Peer-Diensten (Filesharing) treffen. Wenn Sie in den Grundeinstellungen der Regel als Aktion "DROP" gewählt haben, können Sie hier durch Auswahl einer oder mehrerer Kontrollkästchen den Verkehr für diese Dienste verbieten. Dadurch wird der Austausch von Daten mittels der angeführten P2P-Dienste erheblich eingeschränkt und damit beinahe verhindert.

Aktivieren Sie jene P2P - Dienste, welche sie verbieten wollen.

8.7 NAT

NAT steht für **Network Address Translation** und bedeutet, dass die Quell- bzw. Ziel-IP-Adresse bzw. auch die Zielports eines Pakets beim Durchlaufen der Firewall verändert werden. Diese Funktion wird in der Regel dafür benötigt, interne IP-Adressen beim Verlassen des internen Netzwerks mit offiziellen IP-Adressen zu maskieren. Das bedeutet, nach außen (ins Internet) kommunizieren alle Datenpakete mit einer öffentlichen IP-Adresse. NAT kann auch dazu verwendet werden, eintreffende Anfragen an eine offizielle IP-Adresse an einen Server mit einer internen IP-Adresse weiterzuleiten (REDIRECT).

Für NAT werden ähnlich der Definition von Firewall-Regeln eigene Regeln definiert. Eine NAT-Regel wird für ein bestimmtes Interface und für eine bestimmte Richtung (outgoing oder incoming) definiert.

BEISPIEL: Will man alle Datenpakete manipulieren, welche das Netzwerk auf dem externen Interface (jene Netzwerkschnittstelle, die mit dem Internet verbunden ist) verlassen, so wählt man den Track **outgoing - ext**. Mit einer derartigen NAT-Regel können alle ausgehenden Datenpakete mit einer offiziellen IP-Adresse versehen werden. Möchte man alle http-Anfragen an einen internen Webserver weiterleiten so erstellt man die entsprechende NAT-Regel im Track **incoming - ext**.

TIPP: Sie können im NAT Modul dieselben Aliases für Hosts, Gruppen und Services verwenden, die von Ihnen im Netzwerkmodul definiert wurden.

8.7.1 NAT-Regeln

NAT-Regeln werden wie bereits erwähnt ähnlich Firewall-Regeln für einen bestimmten Track erstellt und von oben nach unten abgearbeitet, bis die Optionen einer Regel auf das eintreffende Paket zutreffen. Die Reihenfolge der Regeln ist daher von großer Bedeutung. Nachdem ein Track aus dem Auswahlfeld **Track** ausgewählt worden ist, werden in der darunterliegenden Elementgruppe die zu diesem Track zugehörigen NAT-Regeln dargestellt. In der Übersicht kann die Reihenfolge verändert werden. Auch das Editieren oder Löschen einzelner Regeln wird hier durchgeführt.

HINWEIS: Eine Besonderheit stellt der Track "Von Gibraltar ausgehend" dar. Damit können Pakete maskiert werden, die von einem Service ausgeschickt werden, der auf Gibraltar läuft. Als Beispiel kann hier ein HTTP-Proxy dienen: Sie erlauben nur einer durch Authentifizierung eingeschränkten Anzahl an Benutzern den Zugriff auf Homepages via

© 2008 by eSYS Informationssysteme GmbH

HTTP-Proxy. Sie haben jedoch auch eine eigene Homepage im DMZ liegen, auf die auch nur diese Personen zugreifen dürfen. Wenn diese Personen Ihre eigene Homepage aufrufen, wird eine Anfrage von deren Browser an den HTTP-Proxy von Gibraltar gestellt. Der Proxy stellt wiederum eine Anfrage an den DNS-Server, der den Namen der eigenen Homepage auf eine IP-Adresse auflösen soll. Diese IP-Adresse ist die externe IP-Adresse von Gibraltar. Anfragen von außen werden von Gibraltar korrekt auf den Webserver im DMZ umgeleitet. Wenn jedoch der HTTP-Proxy jetzt seine Anfrage an die externe IP-Adresse stellt, werden die Antwortpakete nicht korrekt zugestellt. Daher ist es für Anfragen aus dem eigenen Netz an die eigene Homepage notwendig, diese mit der Adresse des Webserver im DMZ zu maskieren, damit die Pakete ihren richtigen Weg finden. Dieser Track wird nur in Ausnahmefällen Verwendung finden.

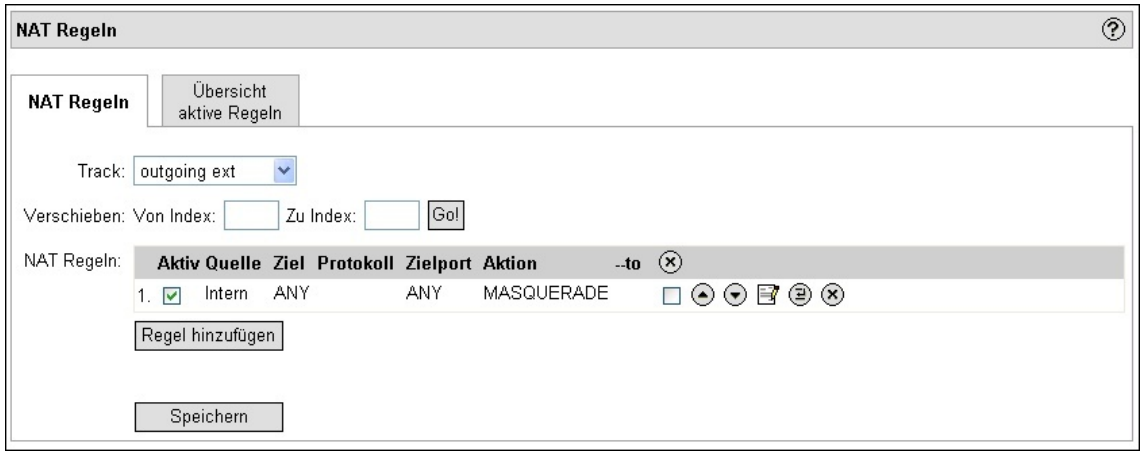
- **Aktiv:** Aktiviert oder deaktiviert die entsprechende Regel.
- **Quelle:** Die Quell IP-Adresse/das Quell Subnetz dieser Regel. Wird keine IP-Adresse angegeben (ANY), so ist die Quell IP-Adresse für diese Regel irrelevant und es werden alle Quelladressen akzeptiert. Wird vor der IP-Adresse ein Rufzeichen dargestellt, so werden alle Quell IP-Adressen außer der hier angegebenen berücksichtigt (Negation).
- **Ziel:** Die Ziel IP-Adresse/das Ziel Subnetz dieser Regel. Wird keine IP-Adresse angegeben (ANY), so ist die Ziel IP-Adresse für diese Regel irrelevant und es werden alle Zieladressen akzeptiert. Wird vor der IP-Adresse ein Rufzeichen dargestellt, so werden alle Ziel IP-Adressen außer der hier angegebenen berücksichtigt (Negation).
- **Service:** Der Service dieser Regel. Wurde kein Service angegeben, so wird das Protokoll angezeigt.
- **Zielport:** Der Port, auf welchen das Paket geschickt werden muss, um von dieser Regel verändert zu werden. Durch diese Einstellung identifiziert man den Dienst, für den diese Regel gültig ist. Zum Beispiel filtert der Zielport 80 die Pakete von HTTP Verbindungen. In dieser Spalte sind nur bei den Protokollen TCP und UDP Einträge zulässig, da nur diese mit Ports arbeiten. Ist für die gezeigte Regel kein Zielport festgelegt, wird in der Übersicht ANY angezeigt.
- **Aktion:** Die Art der Adressübersetzung. Die entsprechende Aktion wird durchgeführt, wenn alle eingestellten Optionen auf ein Datenpaket zutreffen. Bearbeiten Sie gerade die NAT Regeln eines **Incoming** Tracks, so sehen Sie hier entweder **DNAT** oder **REDIRECT**, bearbeiten Sie einen **Outgoing** Track, **SNAT** oder **MASQUERADE**.
  DNAT (Destination NAT): Hier wird die Zieladresse eines Pakets verändert, um das Paket auf einen anderen Computer umzuleiten. Dies ist zum Beispiel der Fall, wenn Sie in Ihrem internen Netz einen Webserver stehen haben. Anfragen kommen an die öffentliche Adresse von Gibraltar und werden durch **DNAT** auf die interne IP-Adresse des WWW Servers umgeleitet. Auch alle weiteren Pakete dieser Anfrage werden dementsprechend verändert.
  REDIRECT: Diese Einstellung leitet ein eintreffendes Paket auf einen anderen Port auf Gibraltar um. Damit können Sie Anfragen an den lokalen Proxy weiterleiten. Die Zieladresse des Pakets wird hierbei nicht verändert.
  SNAT (Source NAT): Mit dieser Einstellung wird die Quell IP-Adresse des Pakets verändert. Dies kann zum Beispiel bei einer HTTP Anfrage eines Clients aus dem privaten Netzwerk durchgeführt werden. Der Client hat die IP-Adresse 192.168.10.36 und versucht eine HTTP Anfrage an den Computer 193.172.22.54. Da der aufrufende Client eine private IP-Adresse hat, würde die Anfrage verworfen werden, sobald sie das private Netz verlässt. Also verändert Gibraltar die Quelladresse des Pakets mit **SNAT**. Dadurch wird das Paket weitergeleitet und die Antwort wieder an Gibraltar zurückgesandt. Beim Eintreffen gibt Gibraltar das Paket wieder an den aufrufenden Client weiter.

© 2008 by eSYS Informationssysteme GmbH

MASQUERADE: Diese Option wird im Zusammenhang mit dynamisch vergebenen, öffentlichen IP-Adressen verwendet, wie sie bei Dial-in Verbindungen Verwendung finden. Dabei werden bei Beendigung der Dial-in Verbindung sämtliche gespeicherte Connections gelöscht. Dies ist notwendig, da ein anderer Teilnehmer, der sich nach Ihnen einwählt, möglicherweise die IP-Adresse zugewiesen bekommt, die vorher von Ihnen verwendet wurde und somit bestehende Verbindungen von Ihnen missbrauchen könnte.

- **--to:** Die Adresse, mit der das Paket maskiert werden soll.
- **Kommentar** : Bewegen Sie den Mauszeiger über dieses Symbol, um den Kommentar zu dieser Regel angezeigt zu bekommen. Dieses Symbol ist nur sichtbar, wenn ein Kommentar zu der Regel eingegeben wurde.
- **Markierte Einträge löschen** : Markieren Sie jene Einträge in der Elementgruppe durch Aktivieren des Kontrollkästchens, die Sie löschen wollen. Betätigen Sie anschließend die Schaltfläche in der Kopfzeile, um die Elemente zu löschen.
- **Regel nach oben schieben** bzw. **Regel nach unten schieben** : Betätigen Sie diese Schaltflächen, um die Regel um eine Zeile nach oben bzw. nach unten zu verschieben. Diese Funktionen sind notwendig, da die Reihenfolge der Regeln bei der Abarbeitung wichtig ist.
- **Regel bearbeiten** : Betätigen Sie diese Schaltfläche, um die Regel zu bearbeiten. Sie werden in die Detailansicht weitergeleitet.
- **Regel darunter einfügen** : Betätigen Sie diese Schaltfläche, um eine neue Regel unter dieser Regel einzufügen. Sie werden in die Detailansicht weitergeleitet.
- **Regel löschen** : Betätigen Sie diese Schaltfläche, um die Regel zu löschen.
- **Regel hinzufügen**: Betätigen Sie diese Schaltfläche, um eine neue Regel hinzuzufügen. Sie werden in die Detailansicht weitergeleitet.
- **Speichern:** Betätigen Sie diese Schaltfläche, um die Änderungen zu speichern.

ACHTUNG: Die Veränderungen an den Paketen, die durch NAT durchgeführt werden, führen noch keine Paketfilterung durch. Es sind somit noch eigene Regeln für die Paketfilterung der veränderten Pakete einzufügen, da die Paketfilterung im Falle von eingehenden Paketen erst nach der Veränderung durchgeführt wird und im Falle von ausgehenden Paketen schon vor der Umwandlung.



© 2008 by eSYS Informationssysteme GmbH

8.7.2 Übersicht aktiver Regeln

Hier finden Sie eine Gesamtübersicht über alle aktiven NAT-Regeln. Sie können in dieser Übersicht keine neuen Regeln erstellen. Bestehende Regeln können bearbeitet oder gelöscht werden.

8.7.3 NAT-Regel bearbeiten

In der Detailansicht werden NAT-Regeln bearbeitet oder neu erstellt. Folgende Einstellungen können vorgenommen werden:

- **Regel aktivieren:** Aktiviert oder deaktiviert die Regel.
- **Quelladresse:** Quelladresse des Datenpakets. Sie können einen bereits definierten Host/Netz Alias oder eine Host/Netz Gruppe auswählen. Alternativ dazu ist es auch möglich, eine frei definierbare IP-Adresse, eine Netzwerkadresse oder einen FQDN anzugeben (CUSTOM). Wählen Sie aus dem Auswahlfeld die Option ANY, wird diese Option nicht berücksichtigt und die Regel ohne Berücksichtigung der Quelladresse angewandt. Wenn Sie das Kontrollkästchen **ausgenommen** markieren, so wird die angegebene IP-Adresse negiert. Das heißt, alle Quell IP-Adressen außer der/den angegebenen werden berücksichtigt. In der Übersicht wird dies durch ein Rufzeichen vor der IP-Adresse dargestellt.
- **Zieladresse:** Zieladresse des Datenpakets. Sie können einen bereits definierten Host/Netz Alias oder eine Host/Netz Gruppe auswählen. Alternativ dazu ist es auch möglich, eine frei definierbare IP-Adresse, eine Netzwerkadresse oder einen FQDN anzugeben (CUSTOM). Wählen Sie aus dem Auswahlfeld die Option ANY, wird diese Option nicht berücksichtigt und die Regel ohne Berücksichtigung der Zieladresse angewandt. Wenn Sie das Kontrollkästchen **ausgenommen** markieren, so wird die angegebene IP-Adresse negiert. Das heißt, alle Ziel IP-Adressen außer der/den angegebenen werden berücksichtigt. In der Übersicht wird dies durch ein Rufzeichen vor der IP-Adresse dargestellt.
- **Service**: Service (Protokoll und Ports) des Datenpakets. Sie finden die Definitionen der Services im Modul **Netzwerk**. Sollten Sie die Option **ANY** wählen, so wird dieses Feld bei der Überprüfung des Paketes nicht berücksichtigt. Sollten Sie hier den Service **CUSTOM** wählen, so wird das Formular automatisch erweitert, wenn Sie Java Script aktiviert haben. Sollte Java Script nicht aktiviert sein, so betätigen Sie nach der Auswahl des Protokolls die **Go!** Schaltfläche. Die Optionen, die bei der Auswahl der Protokolle **TCP** und **UDP** zusätzlich konfiguriert werden können, werden weiter unten im Punkt **Besonderheiten von TCP/UDP** näher erläutert.
- **Aktion**: Die Art der Adressübersetzung und die auszuführende Aktion beim Zutreffen der Regel. Es werden folgende Arten von NAT unterschieden:
  Incoming Track:
  - **DNAT**: Destination Network Address Translation; die Ziel IP-Adresse wird auf eine bestimmte IP-Adresse verändert.
  - **REDIRECT**: Die Anfrage wird auf einen anderen lokalen Port umgeleitet.
- **Outgoing Track**
  - **SNAT**: Source Network Address Translation; die Quell IP-Adresse wird auf eine bestimmte IP-Adresse verändert.
  - **MASQUERADE**: Die Quell IP-Adresse wird verändert (wird verwendet bei dynamischen öffentlichen Adressen - Dial-in!)
- **--to:** IP-Adresse oder Port, der als neue Adresse bzw. als neuer Port für das Paket dienen soll. Sollte bspw. eine HTTP Anfrage an den internen Webserver mit der IP-Adresse 192.168.10.34 weitergereicht werden, so geben Sie hier diese IP-Adresse

© 2008 by eSYS Informationssysteme GmbH

an. Sollten Sie die Aktion **MASQUERADE** gewählt haben, ist ein Eintrag in dieses Feld nicht erlaubt, bei den anderen Aktionen ist er notwendig.
IP-Adresse: IP-Adresse an, mit der das Paket maskiert werden soll.
Port: Bei Auswahl der Option **REDIRECT** geben Sie hier den lokalen Port an, an den die Anfrage umgeleitet werden soll. Hier kann zum Beispiel ein transparenter Proxy an einem bestimmten Port lauschen.
IP Bereich bis: Hier können Sie eine weitere IP-Adresse angeben, die mit der im Textfeld IP-Adresse eingegebenen einen Bereich bildet. Diese Option dient zum Beispiel zur **Lastverteilung** von Anfragen auf mehrere identische WWW Server. Anfragen werden im **Round-Robin Verfahren** an die IP-Adressen im Bereich weitergeleitet und verteilen somit die Last auf mehrere Server.

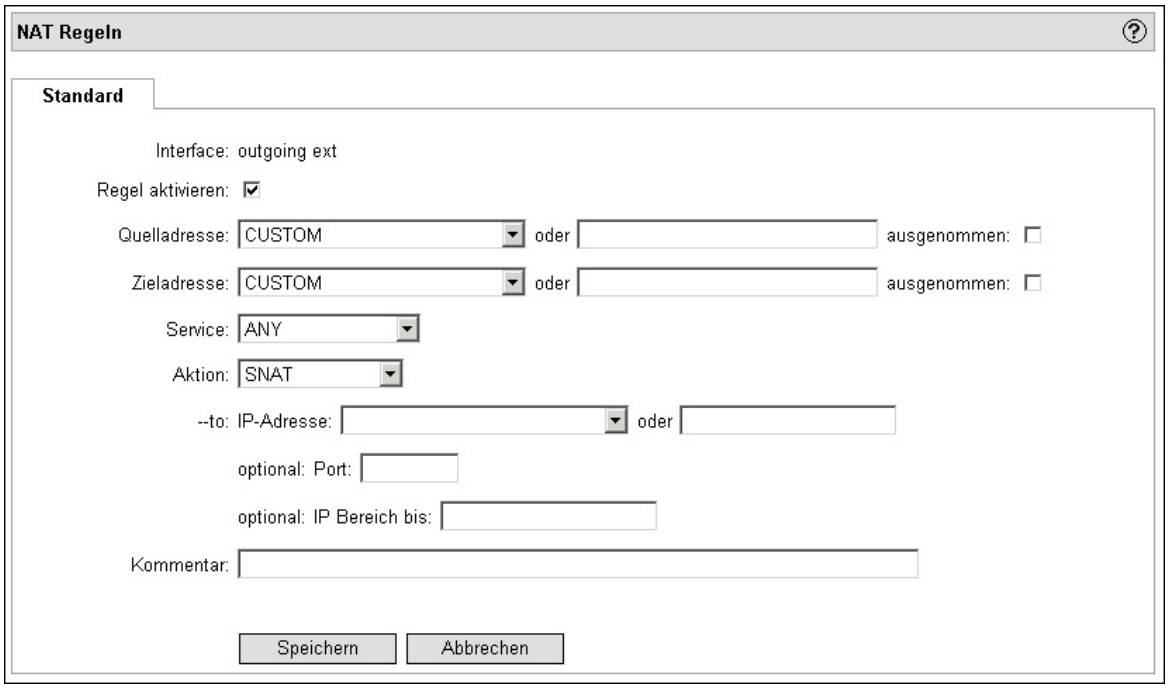
- **Kommentar:** Geben Sie einen kurzen Kommentar als kleine Erklärung oder Gedächtnisstütze ein.

ACHTUNG: Die Veränderungen an den Paketen, die durch NAT durchgeführt werden, führen noch keine Paketfilterung durch. Es sind somit noch eigene Regeln für die Paketfilterung der veränderten Pakete einzufügen, da die Paketfilterung im Falle von eingehenden Paketen erst nach der Veränderung durchgeführt wird und im Falle von ausgehenden Paketen schon vor der Umwandlung.

Besonderheiten von TCP/UDP

- **Quellport:** Kommt das zu überprüfende Paket vom ausgewählten Port, so werden die weiteren Optionen dieser Regel überprüft. Die angeführten Ports entsprechen den gebräuchlichsten und werden gleichzeitig mit dem entsprechenden Dienst angeführt, der über diesen Port läuft. Wählen Sie den von Ihnen gewünschten aus. Bei der Auswahl von **ANY** wird diese Option ignoriert und nicht bei der Überprüfung des Paketes berücksichtigt. Die Auswahl der Option **CUSTOM** erlaubt die Angabe eines nicht in der Liste angeführten Ports oder eines Portbereichs im nebenstehenden Textfeld **Bereich**. Hier können Sie einen Port von 1 bis 65535 angeben oder einen Bereich, indem Sie den Startport und den Endport des Bereiches durch einen Doppelpunkt trennen (z.B.: 2400:2600 bezeichnet die Ports von 2400 bis 2600). Weiters besteht auch die Möglichkeit, alle Ports bis oder ab einem bestimmten Port zu wählen. Durch die Angabe eines Doppelpunkts gefolgt von einer Portnummer werden alle Ports bis zu dieser Nummer berücksichtigt, durch die Angabe einer Portnummer gefolgt von einem Doppelpunkt werden alle Ports ab dieser Portnummer miteinbezogen (z.B.: :500 für alle Ports von 1-500; 500: für alle Ports von 500 bis 65535).
- **Zielport:** Kommt das zu überprüfende Paket am ausgewählten Port an, so trifft diese Option zu und die restlichen Optionen werden überprüft. Die Auswahl aus dem Auswahlfeld bzw. die Eingabe im Textfeld **Bereich** erfolgt wie beim Quellport.

© 2008 by eSYS Informationssysteme GmbH



8.8 Benutzer

Gibraltar besitzt eine zentrale Benutzerverwaltung für mehrere Dienste. Standardmäßig wird der integrierte OpenLDAP Server (Verzeichnisdienst ähnlich einem Telefonbuch) zur Benutzerverwaltung verwendet, allerdings besteht auch die Möglichkeit die Benutzer über einen externen OpenLDAP Server bzw. das Microsoft Active Directory durchzuführen.

Bei den Diensten, die die zentrale Benutzerverwaltung verwenden handelt es sich um:

- **HTTP Proxy**
- **Mail**
- **Captive Portal**
- **VPN (PPTP/L2TP)**
- **OpenVPN**

8.8.1 Benutzerverwaltung

Übersicht - lokaler bzw. externer OpenLDAP Server

Nach der Auswahl bzw. dem Starten des LDAP Servers können anschließend die Benutzer angelegt werden. In der Registerkarte **Benutzer** werden die verschiedenen Benutzer mit den konfigurierten Berechtigungen angezeigt. Die Berechtigungen für die entsprechenden Dienste (VPN, HTTP, HTTP-Proxy, Mail, Captive Portal) können in dieser Übersicht durch das Anklicken der Kontrollkästchen aktiviert bzw. deaktiviert werden.
Über den Button "Benutzer bearbeiten" können die Benutzereinstellungen angezeigt und bearbeitet werden (Siehe Details). Über den Button "Benutzer löschen" können die ausgewählten Benutzer gelöscht werden.

HINWEIS: Benutzer lassen sich nur Anlegen und Bearbeiten, wenn der lokale bzw. ein externer OpenLDAP Server verwendet wird. Bei der Verwendung des Active Directorys

© 2008 by eSYS Informationssysteme GmbH

(AD) können die Benutzer bzw. die Berechtigungen nur über das AD konfigurierte werden.

Übersicht - Active Directory

Bei der Verwendung eines Microsoft Active Directorys zur Benutzerverwaltung werden die verschiedenen Benutzer aus dem AD mit den Berechtigungen in der Übersicht dargestellt. Eine Änderung der Berechtigungen muss im AD erfolgen und kann nicht im Webinterface von Gibraltar durchgeführt werden. Es können allerdings OpenVPN Zertifikate (falls Zertifikate erstellt wurden) heruntergeladen werden.

Neuer Benutzer - lokaler bzw. externer OpenLDAP Server

Über diese Registerkarte kann ein neuer Benutzer angelegt werden.

- **Benutzername:** Der Name des angelegten Benutzers.
- **Passwort:** Neues Passwort für den Benutzer eingeben.
- **Passwort (Bestätigung):** Bestätigen des Passworts.
- **Vorname:** Hier lässt sich für den angelegten Benutzer ein Vorname konfigurieren.
- **Nachname:** Dieses Feld dient zum Speichern eines Nachnamen des Benutzers.
- **E-Mail:** Dieses Feld dient zum Speichern der E-Mail-Adresse des Benutzers.
- **VPN:** Über diese Checkbox lässt sich für den ausgewählten Benutzer die Berechtigung zum Verwenden der VPN Dienste konfigurieren.
- **HTTP-Proxy:** Über diese Checkbox lässt sich für den ausgewählten Benutzer die Berechtigung zum Verwenden des HTTP-Proxies konfigurieren.
- **Mail:** Über diese Checkbox lässt sich für den ausgewählten Benutzer die Berechtigung zum Verwenden der Mailauthentifizierung konfigurieren.
- **Captive Portal:** Über diese Checkbox lässt sich für den ausgewählten Benutzer die Berechtigung zum Verwenden von Captive Portal konfigurieren.

Details - lokaler bzw. externer OpenLDAP Server

Über den Punkt Details lassen sich weitere Einstellungen, wie z.B. das Ändern des Passworts bzw. das Hinzufügen von Namen und E-Mail-Adresse vornehmen.

- **Benutzername:** Der Name des angelegten Benutzers. Dieser Name lässt sich nicht ändern.
- **Passwort ändern?:** Nach Auswahl dieser Checkbox kann das Passwort für den Benutzer geändert werden.
- **Passwort:** Neues Passwort für den Benutzer eingeben.
- **Passwort (Bestätigung):** Bestätigen des Passworts.
- **Vorname:** Hier lässt sich für den angelegten Benutzer ein Vorname konfigurieren.
- **Nachname:** Dieses Feld dient zum Speichern eines Nachnamen des Benutzers.
- **E-Mail:** Dieses Feld dient zum Speichern der E-Mail-Adresse des Benutzers.
- **VPN:** Über diese Checkbox lässt sich für den ausgewählten Benutzer die Berechtigung zum Verwenden der VPN Dienste konfigurieren. Über den Button **VPN Attribute bearbeiten** lässt sich konfigurieren, nach welcher Zeit eine inaktive VPN Verbindung abgebrochen werden soll (gilt für PPTP und L2TP).
- **HTTP-Proxy:** Über diese Checkbox lässt sich für den ausgewählten Benutzer die Berechtigung zum Verwenden des HTTP-Proxies konfigurieren.
- **Mail:** Über diese Checkbox lässt sich für den ausgewählten Benutzer die Berechtigung zum Verwenden der Mailauthentifizierung konfigurieren.

© 2008 by eSYS Informationssysteme GmbH

- **Captive Portal:** Über diese Checkbox lässt sich für den ausgewählten Benutzer die Berechtigung zum Verwenden von Captive Portal konfigurieren. Über den Button Chillispotattribute bearbeiten lassen sich Werte setzen, beispielsweise welche Datenmenge dieser Benutzer noch über Captive Portal heruntergeladen werden darf, bevor die Verbindung beendet wird. Diese Werte lassen sich durch den "Alle Radiuswerte zurücksetzen" zurücksetzen.
- **Benutzerzertifikat herunterladen:** Sollte für den Benutzer ein Client-Zertifikat erstellt worden sein, kann dieses Zertifikat hier heruntergeladen werden. Sollte ein Benutzerzertifikat verloren gegangen sein, so kann es hier wieder heruntergeladen werden.

VPN Attribute - lokaler bzw. externer OpenLDAP Server

- **Fixe IP (Leer für irgendeine IP):** Soll ein Benutzer eine statische IP über PPTP erhalten, so kann diese hier konfiguriert werden.
- **Verbindung nach Sekunden trennen:** Wird für diese Feld ein Wert definiert, so wird die VPN Verbindung (gilt für PPTP und L2TP) nach den angegeben Wert in Sekunden beendet.

Captive Attribute - lokaler bzw. externer OpenLDAP Server

- **Verbindung nach Sekunden trennen:** Wird für diese Feld ein Wert definiert, so wird die Verbindung nach den angegeben Wert in Sekunden beendet. **(Hinweis: Verwendet ein Benutzer sowohl VPN als auch Captive Portal, so gilt dieser Wert für beide Dienste)**
- **bereits abgelaufene Zeit:** Dieser Wert gibt die Zeitdauer an, die ein Benutzer bereits über ChilliSpot eingeloggt war. Der Wert lässt sich durch den Reset-Button wieder zurücksetzen.
- **Verbindung nach Sekunden ohne Aktivität trennen:** Die Verbindung wird nach der angegeben Zeit in Sekunden ohne Aktivität getrennt.
- **Maximale Benutzer Uploadmenge (MBytes):** Dieser Wert gibt an, wieviele Megabytes ein Benutzer über die Verbindung hochladen darf.
- **bereits hochgeladene MBytes:** Dieser Wert gibt die Datenmenge in MB an, die ein Benutzer bereits über ChilliSpot hochgeladen hat. Der Wert lässt sich durch den Reset-Button wieder zurücksetzen.
- **Maximale Benutzer Downloadmenge (MBytes):** Dieser Wert gibt an, wieviele Megabytes ein Benutzer über die Verbindung herunterladen darf.
- **bereits heruntergeladene MBytes:** Dieser Wert gibt die Datenmenge in MB an, die ein Benutzer bereits über ChilliSpot heruntergeladen hat. Der Wert lässt sich durch den Reset-Button wieder zurücksetzen.
- **Maximale Datenmenge (MB):** Dieser Wert gibt an, wieviele Megabytes ein Benutzer gesamt für Up- und Download zur Verfügung hat.
- **Maximale Uploadbandbreite (Bits/sek):** Durch diesen Wert lässt sich die maximale Uploadbandbreite für den Benutzer begrenzen.
- **Maximale Downloadbandbreite (Bits/sek):** Durch diesen Wert lässt sich die maximale Downloadbandbreite für den Benutzer begrenzen.
- **Logoutzeit:** Durch dieses Feld lässt sich die Verbindung zum angegebenen Zeitpunkt automatisch trennen. Der Wert "21.08.2006 12:00:00" trennt die Verbindung am 21. August 2006 um 12:00:00.

© 2008 by eSYS Informationssysteme GmbH

8.8.2 LDAP Einstellungen

Nach der Auswahl des Moduls zur Benutzerverwaltung wird beim ersten Aufruf automatisch auf die zweite Registerkarte **LDAP-Einstellungen** umgeleitet. In diesem Formular muss der zu verwendende LDAP Server ausgewählt werden. Standardmäßig wird der lokale OpenLDAP Server verwendet.

Lokaler OpenLDAP Server (Standard)

Neben dem Feld "Status" wird der aktuelle Status angezeigt (in diesem Fall läuft der Server nicht) und dieser kann auch geändert werden. Durch das Drücken des Start-Buttons (grüner Pfeil) wird der LDAP Server gestartet.

Nach dem Aktivieren des Servers können im Formular **Benutzer** die Benutzer angelegt werden.

HINWEIS: Nach dem Starten des lokalen OpenLDAP Servers wird dieser auch bei jedem Neustart der Firewall gestartet. Er kann über dieses Tab auf Wunsch auch wieder gestoppt (roter Stopbutton) werden.

Externer OpenLDAP Server

ACHTUNG: Die Verwendung eines externen OpenLDAP Servers benötigt ausführliches Wissen über die Administration eines OpenLDAP Servers (z.B. für die Konfiguration der Access Control Lists) und ist daher wirklich nur für Profis ratsam.

Neben dem lokalen OpenLDAP Server kann auch ein externer OpenLDAP Server verwendet werden. In der Auswahlliste "Server" muss hierzu der "external LDAP" Server ausgewählt werden. Anschließend ändert sich die Anzeige (JavaScript muss hierfür aktiviert sein) und zusätzliche Felder müssen ausgefüllt werden:

- **LDAP Server:** IP Adresse bzw. Hostname des externen LDAP Servers. (**Achtung:** Für eine Verschlüsselung der Verbindung mit TLS **MUSS** hier der Hostname verwendet werden, der im TLS Zertifikat unter Common Name enthalten ist)
- **LDAP Port:** Port des LDAP Servers (Standardmäßig 389)
- **Benutzername Administrator**: **manager** (sofern die LDAP Initialisierungsdaten verwendet werden)
- **OU:** ou=**admin** (sofern die LDAP Initialisierungsdaten verwendet werden)
- **Root DC:** dc=**gibraltar**,dc=**local** (sofern die LDAP Initialisierungsdaten verwendet werden)
- **Passwort:** wird zufällig erzeugt. Nach dem Einspielen der LDAP Initialisierungsdaten empfiehlt es sich, das Passwort zu ändern.
- **Passwort bestätigen:** Bestätigen des geänderten Passworts
- **LDAP Passwörter ändern:** Durch diesen Button lassen sich weitere Passwörter ändern. Die verschiedenen Dienste benötigen verschiedene Benutzer mit unterschiedlichen Berechtigungen. Die Passwörter können hier geändert werden.
- **TLS:** Für eine mit TLS-verschlüsselte Verbindung muss für den externen OpenLDAP Server ein Zertifikat erstellt werden und der Server entsprechend für StartTLS bzw. SSL konfiguriert werden. Bei StartTLS erfolgt die Verschlüsselung über den

© 2008 by eSYS Informationssysteme GmbH

Standardport nach dem Verschicken eines speziellen Kommandos, bei SSL erfolgt die Verschlüsselung über einen eigenen Port (636). Über diesen Port wird nur verschlüsselt kommuniziert. Es müssen beide Varianten aktiviert sein, da manche Dienste, die die Benutzerverwaltung verwenden, nur die eine bzw. die andere Variante unterstützen.

- **LDAP Schema herunterladen:** Der OpenLDAP Server auf der Gibraltar Firewall verwendet zur Benutzerverwaltung eigene Schemadateien. Diese Schemadatei kann hier heruntergeladen werden und diese muss anschließend im OpenLDAP Server eingebunden werden.
- **LDAP Initialisierungsdaten herunterladen:** Zusätzlich zu den Schemadateien wird auch das Grundgerüst benötigt, dass hier heruntergeladen werden kann.

TIPP: Diese Variante empfiehlt sich nur für spezielle Installationen mit vielen Benutzern bzw. für bereits vorhandene OpenLDAP Server. Für den Großteil der Installationen ist der lokale OpenLDAP Server völlig ausreichend. Dieser ist direkt auf diese Anwendung abgestimmt und benötigt keine weiteren Einstellungen.

HINWEIS: Bei Verwendung eines externen Servers sollte die Verbindung immer verschlüsselt werden.

SSL Zertifikat
Um die Verbindung zu einem externen OpenLDAP Server zu verschlüsseln, ist es notwendig ein Serverzertifikat zu erstellen. Das Zertifikat kann mit OpenSSL erstellt werden: Anschließend muss der OpenLDAP Server entsprechend konfiguriert werden, um das SSL Zertifikat zu verwenden. Die Anleitung hierfür unterscheidet sich für die verschiedenen Distributionen und sind daher aus der Dokumentation der jeweiligen Distribution zu entnehmen.

Microsoft Active Directory

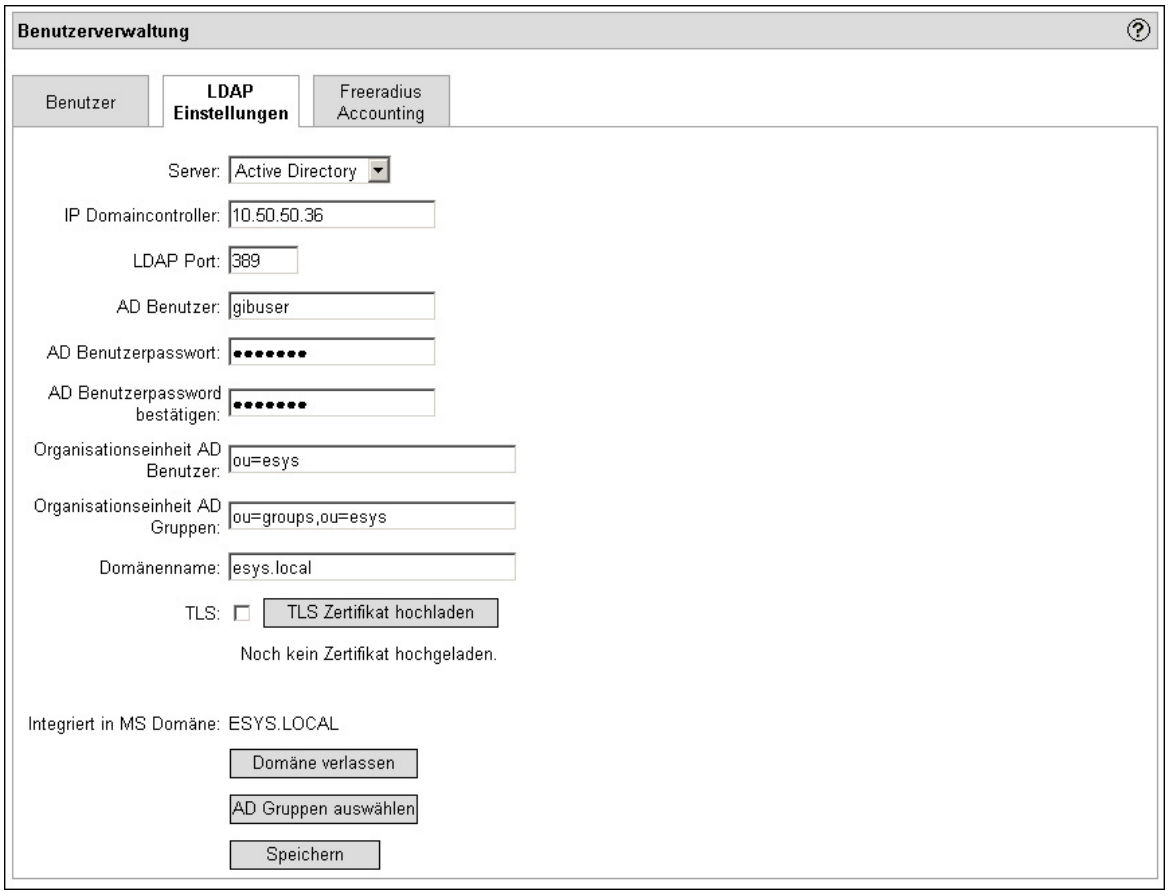
Wollen Sie Microsoft Active Directory (AD) zur Authentifizierung verwenden, wählen Sie den entsprechenden Eintrag in der Auswahlliste **Server**.

- **IP Domänencontroller:** IP Adresse bzw. Hostname des Domänencontrollers. (**Achtung:** Für eine Verschlüsselung der Verbindung mit TLS **MUSS** hier der Hostname verwendet werden, der im TLS Zertifikat unter Common Name enthalten ist)
- **LDAP Port:** LDAP-Port des Directoryservers (Standardmäßig 389)
- **AD Benutzer:** Name eines Benutzers zur Authentifizierung der Firewall am Active Directory. Hier empfiehlt es sich **NICHT** den **Administratoraccount** (meist "administrator") zu verwenden, sondern einen eigenen Benutzer (z.B. gibraltar) anzulegen. Hierfür reicht ein normaler Benutzeraccount. Spezielle Berechtigungen werden nur zum Speichern der OpenVPN Zertifikate benötigt.
- **AD Benutzerpasswort:** Passwort des gewählten Benutzeraccounts.
- **AD Benutzerpasswort bestätigen:** Bestätigen des gewählten Passworts
- **Organisationseinheit AD Benutzer:** Name der OU (Organisationseinheit), in die der AD Benutzer eingegliedert ist.
- **Domänenname:** Domänenname, der beim Konfigurieren des Active Directorys gewählt wurde, z.B. gibraltar.local oder esys.local.
- **TLS:** Für eine mit TLS-verschlüsselte Verbindung muss für den AD Server ein Zertifikat erstellt werden und der Server entsprechend konfiguriert werden (Certificate

© 2008 by eSYS Informationssysteme GmbH

Authority).

- **Domäne beitreten/verlassen:** Zum Beitreten zur Domäne benötigen Sie Benutzername und Passwort eines Domänenadministrators.
- **Gruppen auswählen:** Für die entsprechenden Dienste (Mail, HTTP-Proxy, ChilliSpot, VPN) müssen anschließend die dafür berechtigten Gruppen ausgewählt werden. Dadurch kann konfiguriert werden, dass alle Benutzer in einer bestimmten Gruppe (z.B. internet) den ausgewählten Dienst verwenden dürfen.



Berechtigungen des AD Benutzers, der für die Authentifizierung verwendet wird
Es wird empfohlen, einen normalen Benutzeraccount (z.B. *Firewall* oder *Gibraltar*) anzulegen, mit dem die Authentifizierung durchgeführt wird. Dadurch ist es nicht notwendig, die Benutzerdaten des Domänenadministrators auf der Firewall zu speichern.
Für die Speicherung der Clientzertifikate müssen allerdings die Berechtigungen erweitert werden. Dazu wird das standardmäßig vorhandene Tool **dsacls** des AD verwendet.
Bei DSACLS (dsacls.exe) handelt es sich um ein Befehlszeilentool, das zum Anfordern und Ändern von Berechtigungen und Sicherheitsattributen von Active Directory-Objekten verwendet wird. Es handelt sich um die Befehlszeilenentsprechung der Registerkarte Sicherheit in Windows 2000 Server Active Directory-Snap-In-Tools wie Active Directory-Benutzer und -Computer oder Active Directory-Standorte und -Dienste. (MS DSACLS)

Wurde der Benutzer wie im Bild oben angelegt, so können sich mit folgendem Befehl die Berechtigungen des Benutzers firewall ausgeben lassen:

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

Diese Berechtigungen müssen mit folgendem Befehl erweitert werden:

© 2008 by eSYS Informationssysteme GmbH

```
dsacls ou=esys,dc=esys,dc=local /I:S /G "esys\firewall:RPWP;userPKCS12;user"
```

Die Rechte des Benutzers *firewall* werden dahingehend erweitert, dass dieser Benutzer Lese- und Schreibrechte (RPWP-Right Property, Write Property) auf das Attribut userPKCS12 erweitert werden. In diesem Attribut werden die Clientzertifikate gespeichert. Weitere Informationen können in DSACLS-Befehlssyntax nachgelesen werden.

Domäne beitreten
Für die VPN Dienste PPTP und L2TP ist es notwendig, dass Gibraltar der Domäne als Mitglied beitritt. Dazu müssen Sie folgende Angaben machen:

- **Domänencontroller:** IP Adresse eines Domänencontrollers
- **Domänenadministrator:** AD-Benutzer mit den Rechten eines Domänenadministrators, standardmäßig *administrator*
- **Passwort**

HINWEIS: Die Zugangsdaten des Administrators werden nur zum Beitreten in die Domäne benötigt und nicht dauerhaft auf Gibraltar gespeichert.

AD Gruppen auswählen
Für jeden auf der Firewall verfügbaren Dienst der eine Authentifizierung verlangt, kann in dieser Registerkarte eine Gruppe ausgewählt werden. Alle Benutzer, die sich in den ausgewählten Gruppen befinden, dürfen den zugehörigen Dienst verwenden.

- **VPN Gruppe:** Gruppe, in der sich die Benutzer befinden müssen, um VPN (PPTP und L2TP) verwenden zu dürfen.
- **HTTP-Proxy Gruppe:** Gruppe, in der sich die Benutzer befinden müssen, um den HTTP-Proxy verwenden zu dürfen.
- **Mail Gruppe:**Gruppe, in der sich die Benutzer befinden müssen, um die Mailauthentifizierung verwenden zu dürfen.
- **ChilliSpot Gruppe**: Gruppe, in der sich die Benutzer befinden müssen, um ChilliSpot verwenden zu dürfen.

HINWEIS: Es kann auch für jeden Dienst die gleiche Gruppe ausgewählt werden, ein Benutzer der sich in dieser Gruppe befindet darf dann alle Dienste verwenden.

SSL Zertifikat
Eine Beschreibung zur Integration eines SSL Zertifikates finden Sie auf http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.itame.doc/am60_install166.html

8.8.3 Freeradius Accounting

In dieser Registerkarte kann konfiguriert werden, dass die verbindungsbezogenen Daten in Dateien bzw. in einer Datenbank gespeichert werden. Mit verschiedenen Programmen können aus diesen Dateien anschließend Berichte generiert werden. Ein Freeware-Tool ist z.B. Radiusreport. Dabei handelt es sich um ein Perl-Script, dass die in den Dateien gesammelten Daten aufbereitet.

Beispielauswertung mit Radiusreport.

```
radiusreport -tba -l peda -f
/var/log/freeradius/radacct/127.0.0.1/detail-20070420
Radius Log Report for: peda
Date Login Logout Ontime Port BandWt-In/Out Total
----------------------------------------------------------------
```

© 2008 by eSYS Informationssysteme GmbH

```
20/04/2007 15:10:18 15:12:00 1m42s W0 8.3K/34.0K 0h01m
20/04/2007 15:15:06 15:15:18 0m12s W0 10.7K/236.4K 0h01m
20/04/2007 15:21:46 15:21:57 0m11s W0 6.5K/159.8K 0h02m
20/04/2007 15:23:58 15:24:12 0m14s W0 11.9K/106.1K 0h02m
20/04/2007 15:26:24 15:26:30 0m06s W0 27.6K/207.7K 0h02m
20/04/2007 15:27:05 15:27:27 0m22s W0 24.3K/73.4K 0h02m
20/04/2007 15:28:29 15:30:12 1m43s W0 7.7K/47.8K 0h04m
-------------------------------------------------------------
Total Hours: 0h04m
Average Online times: Unavailable - not enough data.
Total Data transferred In/Out: 97.4K/865.4K
```

Internes Accounting:

Hier werden sämtliche Daten in dem Verzeichnis /var/log/freeradius/radaccount gespeichert. Dies ist nur bei Verwendung einer Festplatte möglich.

Externes Accounting:

Die Daten können auch in einer externen Mysql-Datenbank gespeichert werden.

- **Freeradius Datenbank Schema herunterladen:** Über diesen Button kann das Datenbank Schema für MySQL heruntergeladen werden.
- **Datenbank Typ:** mysql (momentan wird nur MySQL unterstützt.
- **Datenbank Host:** Adresse des externen MySQL Servers
- **Datenbank Name:** Name der Datenbank
- **Datenbank User:** Benutzername des MySQL Servers, der Schreibzugriff auf die Datenbank hat
- **Datenbank Password:** Bestätigung des Passwortes

HINWEIS: Bei der Verwendung eines Datenbankservers sollte die Verbindung zu diesem nur verschlüsselt (z.B. über deinen IPSec-Tunnel) erfolgen.

8.9 Mail

Gibraltar kann als sicherer Mail-Relay-Server (Mailproxy) eingesetzt werden. Das bedeutet, Gibraltar fungiert als offizieller Mailserver und leitet alle eingehenden E-Mails erst nach einer eingehenden Prüfung an die internen Mailserver weiter. Dabei ist Gibraltar in der Lage, jedes eingehende E-Mail zusätzlich auf Viren, Spamverdacht und gefährliche Attachments zu prüfen. Für unterschiedliche Maildomänen können unterschiedliche E-Mail-Server verwendet werden.

Voraussetzungen für die Nutzung des Mail-Relay

Damit Sie die Funktionen des Gibraltar Mailproxy nutzen können müssen Sie folgende Voraussetzungen erfüllt sein:

- Sie verfügen über eine eigene Maildomäne (z.B. esys.at)
- Sie betreiben einen eigenen Mailserver in ihrem internen Netzwerk (am besten in einer DMZ)
- Gibraltar wird zwischen dem Internet und Ihrem Mailserver eingesetzt.
- Der MX-Eintrag (DNS-Eintrag für den Mailserver ihrer Domäne) lautet auf die offizielle IP-Adresse von Gibraltar. Dadurch wird festgelegt, dass alle E-Mails an ihre Domäne an die Gibraltar Firewall geschickt werden. Gibraltar leitet die E-Mails in weiterer Folge an ihre internen Mailserver weiter.

Für ausgehende E-Mails kann mit Gibraltar sichergestellt werden, dass nur authorisierte

© 2008 by eSYS Informationssysteme GmbH

Hosts E-Mails nach außen schicken dürfen.

ANMERKUNG: Damit die E-Mails auf Viren und Spam überprüft werden können, muss der SMTP Content Scanner Dienst unter dem Menüpunkt Dienste gestartet werden.

ANMERKUNG: Falls Sie keinen eigenen Mailserver betreiben, sondern einen externen Mailserver mittels POP3 abrufen, verwenden Sie den in Gibraltar integrierten POP3 Proxy für die Filterung der E-Mails.

8.9.1 Mail-Relay

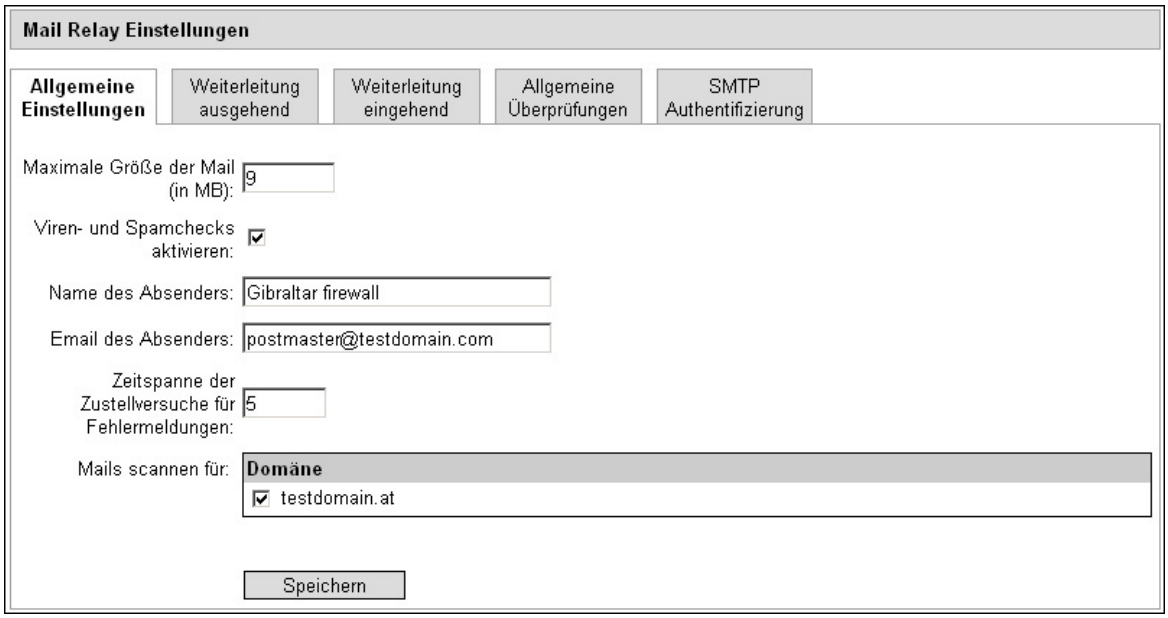
8.9.1.1 Mail - Allgemeine Einstellungen

Definieren Sie die allgemeinen Einstellungen für die Handhabung von E-Mails durch Gibraltar:

- **Maximale Größe der Mail (in MB):** Größenbeschränkung für die Weiterleitung von eingehenden E-Mails in Megabyte. E-Mails, welche die Größenbeschränkung überschreiten, werden nicht angenommen.
- **Viren- und Spamchecks aktivieren:** Aktiviert die Viren und Spamchecks. Die Einstellungen für Viren und Spamchecks werden gesondert vorgenommen.
- **Name des Absenders:** Absendername für E-Mails, welche von Gibraltar versendet werden.
- **Email des Absenders:** Absenderadresse für E-Mails, welche von Gibraltar versendet werden. Geben Sie hier eine real existierende Adresse an, damit verunsicherte Benutzer Ihnen durch einfaches Antworten auf diese Email eine Benachrichtigung oder eine Frage zukommen lassen können.
- **Zeitspanne der Zustellversuche für Fehlermeldungen in Tagen:** Stellen Sie hier ein, wie lange Gibraltar die Zustellung von Unzustellbarkeitsmeldungen versuchen soll, ehe sie verworfen werden.
- **Mails scannen für:** Geben Sie alle E-Mail-Domänen an, für die Sie Prüfungen durchführen wollen.

ANMERKUNG: Damit Ihre Mails auf Viren und Spam überprüft werden, muss auch der SMTP Content Scanner Dienst unter dem Menüpunkt Dienste gestartet werden.

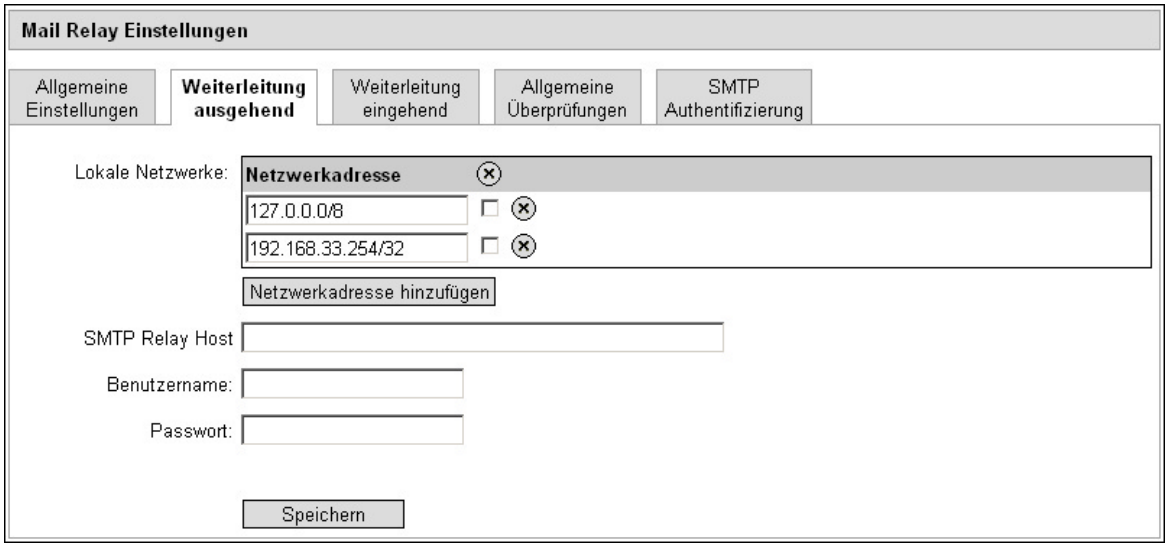
© 2008 by eSYS Informationssysteme GmbH



8.9.1.2 Weiterleitung ausgehend

Damit Gibraltar nicht von fremden Personen zum Versand von Spam Mails missbraucht werden kann, werden standardmäßig keine Emails weitergeleitet. Um ein Versenden mittels Gibraltar zu erlauben, müssen Sie explizit jene Netzwerke oder Hosts angeben, von denen ausgehende Mails zum Weiterversand entgegengenommen werden (relaying).

- **Lokale Netzwerke:** Jene Netzwerke oder IP-Adressen, von denen E-Mails angenommen und weitergeleitet werden.
- **SMTP Relay Host:** IP-Adresse eines SMTP Relay Host. Alle ausgehenden E-Mails werden an den angegebenen Relay Host weitergeleitet.
- **Benutzername/Passwort:** Zugangsdaten, die Sie für den SMTP Relay Host benötigen.



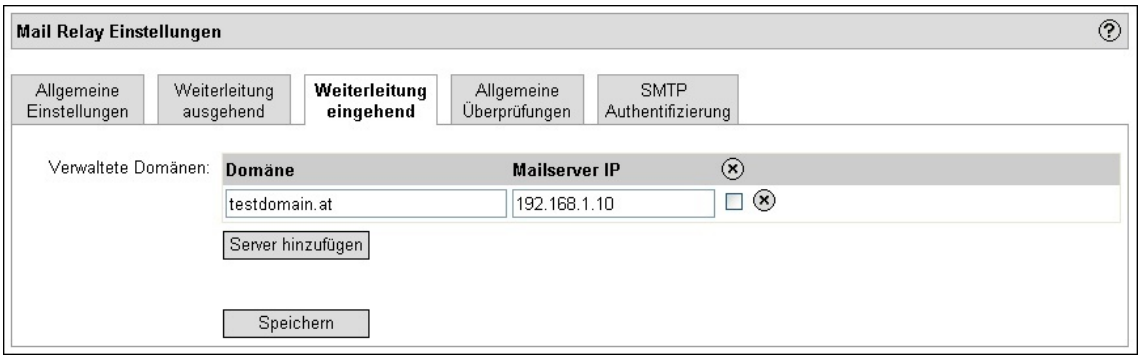
ACHTUNG: Vergessen Sie nicht, in den Firewallregeln den TCP Port 25 (SMTP) zu erlauben (z.B.: eingehend "int0" und ausgehend "local"), damit Ihr Mailserver die Emails an Gibraltar für den Weiterversand übermitteln kann.

© 2008 by eSYS Informationssysteme GmbH

8.9.1.3 Weiterleitung eingehend

Gibraltar kann für mehrere Domänen Mails empfangen und an unterschiedliche Mailserver weiterleiten. Dazu ist es notwendig, Gibraltar den für eine Domäne zuständigen Mailserver mitzuteilen.

- **Domäne:** E-Mail Domäne
- **Mailserver IP:** IP-Adresse des (internen) Mailservers, welcher E-Mails der angegebenen Domäne weiterverarbeitet. Alle eingehenden E-Mails der angegebenen Domäne werden an den angegebenen Mailserver weitergeleitet.



8.9.1.4 Allgemeine Überprüfungen

Unabhängig vom Spamfilter und den Virenchecks werden bei allen E-Mails die Header auf Konformität mit bestehenden Standards und die Art der Dateianhänge geprüft. Sie haben folgende Konfigurationsmöglichkeiten:

- **Aktion für illegale Header:** Wird bei einem E-Mail ein illegaler (z.B. gefälschter) Header erkannt, stehen folgende Aktionen zur Verfügung:
  Verwerfen und Absender verständigen: Das ungültige E-Mail wird verworfen und der Absender verständigt.
  Verwerfen: Das ungültige E-Mail wird verworfen und es wird kein Verständigungsmail geschickt.
  Durchlassen: Das ungültige E-Mail wird zugestellt.
  Durchlassen und Absender verständigen: Das ungültige E-Mail wird zugestellt. Der Absender wird jedoch verständigt, dass das E-Mail nicht gültig war.
- **Aktion für illegale Attachments:** Werden bei einem E-Mail illegale Dateianhänge festgestellt, stehen folgende Aktionen zur Verfügung:
  Verwerfen und Absender verständigen: Das E-Mail wird verworfen und der Absender wird verständigt.
  Verwerfen: Das E-Mail wird verworfen.
  Durchlassen: Das E-Mail wird zugestellt.
  Durchlassen und Absender warnen: Das E-Mail wird zugestellt und der Absender wird verständigt, dass das Attachment ungültig war.
  Durchlassen und Empfänger warnen: Das E-Mail wird zugestellt und der Empfänger wird gewarnt, dass das Attachment ungültig ist.
  Durchlassen und Emfpänger und Absender warnen: Das E-Mail wird zugestellt und Absender und Empfänger werden gewarnt.
- **Dateitypen filtern:** Definieren Sie jene Typen von Dateianhängen, welche gefiltert werden sollen. Die Dateitypen werden anhand der Dateiendung definiert (z.B. .BAT, .EXE).

© 2008 by eSYS Informationssysteme GmbH

Auf dieser Registerkarte können noch zusätzliche Überprüfungen konfiguriert werden. Es handelt sich dabei um die Filterung von Emails, deren Header unerlaubte Veränderungen aufweisen, oder um Dateianhänge an Emails, deren Datentyp eine potentielle Gefahr darstellen (z.B. .exe oder .vbs Dateien).

8.9.1.5 SMTP Authentifizierung

Sie können Gibraltar als SMTP-Server zum Versenden von E-Mails konfigurieren. Das macht z.B. Sinn, wenn Sie mobilen Benutzern erlauben wollen, von außerhalb Ihres Netzwerks über Gibraltar E-Mails via SMTP zu verschicken. Aus Sicherheitsgründen ist dies nur für autorisierte Benutzer möglich. Aktivieren Sie die SMTP-Authentifizierung, falls Sie diese Funktion verwenden möchten.

Es dürfen nur autorisierte Benutzer den Gibraltar SMTP-Server verwenden. Die Benutzer werden im Modul Benutzerverwaltung definiert.

ACHTUNG: Vergessen Sie nicht eine Filterregel zu erstellen, die es den externen Benutzern erlaubt, von außen auf Port 25 (SMTP-Port) zuzugreifen.

8.9.2 AntiSpam

Gibraltar beinhaltet einen leistungsfähigen Spamfilter. Zur Filterung werden mehrere aktuelle Techniken kombiniert.

Eine Übersicht über die aktuell von Gibraltar verwendeten Techniken finden Sie auf der Gibraltar Homepage www.gibraltar.at

8.9.2.1 AntiSpam (1)

Aufgrund der Vielzahl von möglichen Einstellungen im Zusammenhang mit dem Spamfilter von Gibraltar wurde die Konfiguration auf zwei Registerkarten aufgeteilt. Folgende Einstellungen können Sie auf der ersten Registerkarte vornehmen:

- **Betreff verändern:** Aktivieren Sie diese Option, wenn Sie den Betreff von als Spam klassifizierten E-Mails verändern wollen
- **Text in Betreff einfügen:** Der angegebene Text wird bei Spam-Mails vor dem eigentlichen Betreff eingefügt und kann dazu verwendet werden, die klassifizierten E-Mails vom Mail-Client automatisch auszusortieren.
- **Administrator E-Mail:** E-Mail-Adresse an welche die Spam-Benachrichtigungen gesendet werden. Wird ein E-Mail als Spam klassifiziert wird an die angegebene E-Mail-Adresse eine Nachricht mit der Klassifizierung versendet.
- **Quarantäne E-Mail:** E-Mail-Adresse eines Quarantänepostfachs. Alle klassifizierten E-Mails werden an die angegebene E-Mail-Adresse weitergeleitet.
- **Spam Detect Header hinzufügen:** Die Wahrscheinlichkeit, dass es sich bei einem E-Mail um Spam handelt wird auf einer Punkteskala abgebildet. Sie können die Anzahl der Punkte, ab wann dem Header die Spambewertung hinzugefügt wird, selbst festlegen. Dieser Wert kann individuell unterschiedlich sein. Erfahrungsgemäß liegen realistische Grenzwerte für Spam zwischen 4.0 und 7.0 Punkten.
- **Aktion ausführen:** Wird der angegebene Punktewert überschritten, wird die gewählte Aktion ausgeführt.

© 2008 by eSYS Informationssysteme GmbH

- **Mailverständigung unterdrücken ab Spambewertung:** Punktezahl, ab der keine Verständigungen gesendet werden. Dies ist bei eindeutig als Spam klassifizierten E-Mails sinnvoll um das Mailaufkommen zu senken. Dieser Wert muss also deutlich höher sein als die Werte zuvor.
- **Aktion, wenn Spam:** Aktion, die ausgeführt wird, wenn es sich bei einem E-Mail um Spam (Bewertung ab angegebenem Punktewert) handelt. Sie haben folgende Möglichkeiten:

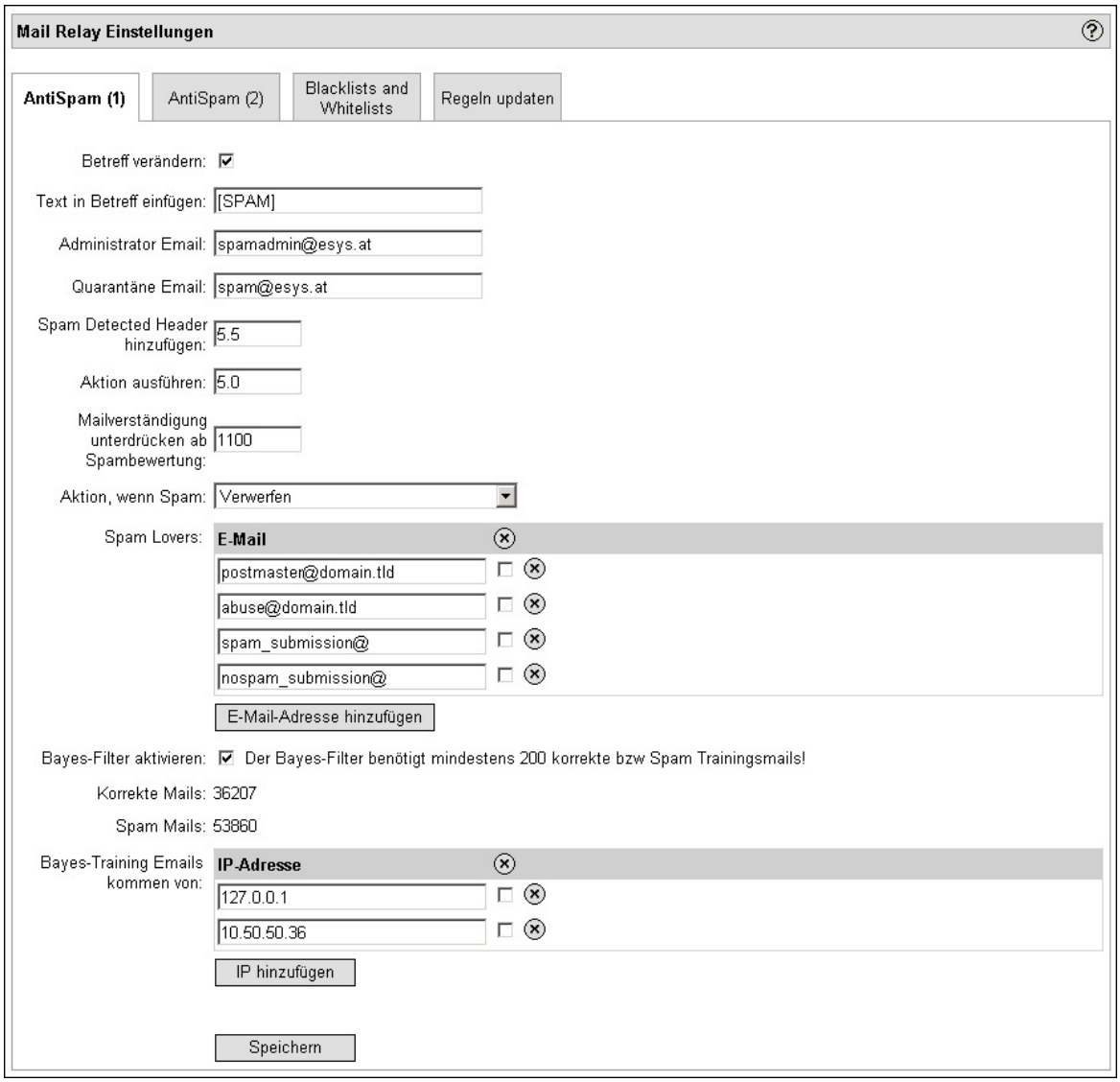
  Verwerfen und Absender verständigen: Das E-Mail wird verworfen und der Absender verständigt. Falls Sie eine Quarantäne E-Mail-Adresse angegeben haben, wird das E-Mail jedoch an diese Adresse zugestellt.

  Verwerfen: Das E-Mail wird verworfen und wird gegebenenfalls an die Quarantäne E-Mail-Adresse zugestellt.

  Durchlassen: Das E-Mail wird durchgelassen

  Durchlassen und Absender warnen: Das E-Mail wird durchgelassen, der Absender wird jedoch gewarnt, dass das E-Mail als Spam klassifiziert wurde.
- **Spam-Lovers:** An die angegebenen E-Mail-Adressen werden auch als Spam klassifizierte E-Mails zugestellt. Es kann z.B. aus rechtlichen Gründen notwendig sein, für gewissen E-Mail-Adressen innerhalb der Organisation keine Spam-Überprüfung durchzuführen.
- **Bayes-Filter aktivieren:** Aktiviert den auf komplexen Wahrscheinlichkeiten basierenden Bayes-Filter. Dieser Filter benötigt zur Erkennung von E-Mails eine große Anzahl an Trainings-E-Mails. Aus Sicherheitsgründen müssen sie jene IP-Adressen festlegen, welche berechtigt sind, dem Gibraltar Spamfilter Trainings-E-Mails zu schicken. Dabei wird es sich in der Regel um Ihre internen Mailserver handeln.

© 2008 by eSYS Informationssysteme GmbH



8.9.2.2 AntiSpam (2)

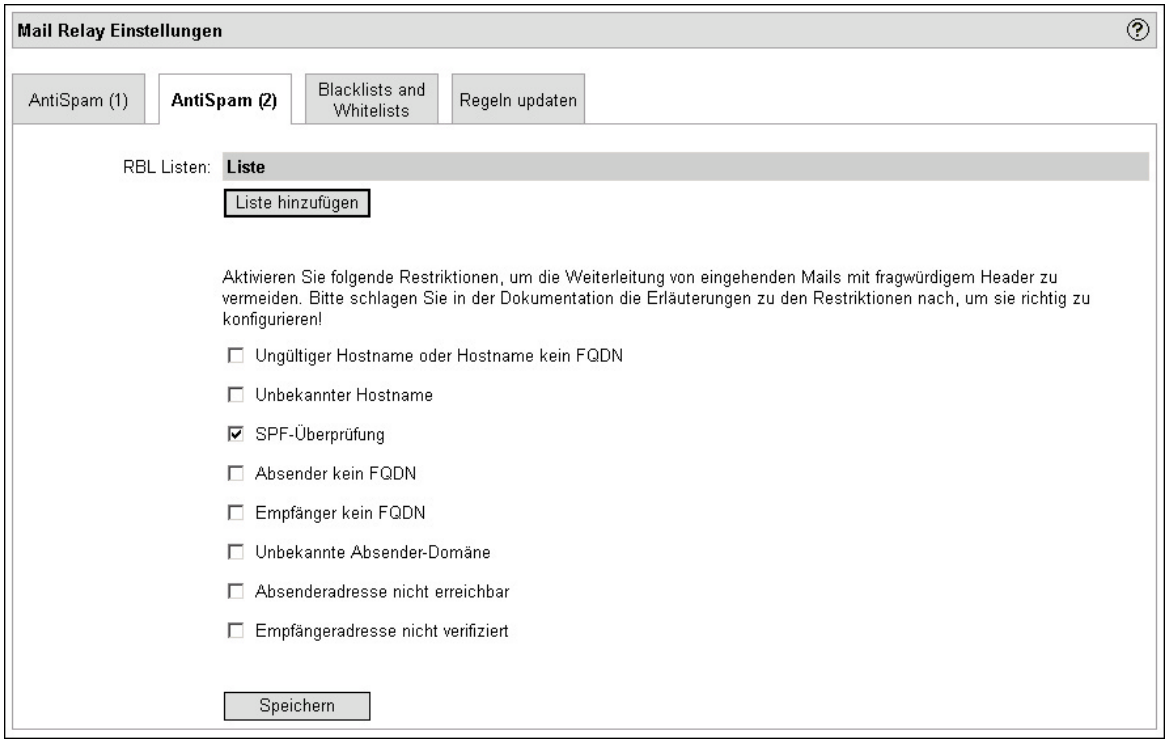
Im zweiten Teil der Spamfilter-Konfiguration definieren Sie Blacklisten, die von Gibraltar abgefragt werden und zusätzliche Filtermethoden.

- **RBL-Listen:** Bei RBL-Listen handelt es sich um öffentliche Datenbanken, in denen jene E-Mail-Server geführt werden, welche bereits mehrmals Spammails versendet haben. Sie können die vorkonfigurierte Liste erweitern oder einschränken. Beachten Sie bitte, dass es durchaus vorkommen kann, dass Mailserver von großen Providern regelmäßig auf RBL-Listen zu finden sind. Diese Funktion kann daher dazu führen, dass in weiterer Folge keine E-Mails mehr von diesen Servern angenommen werden.
- **Ungültiger Hostname oder Hostname kein FQDN:** Die Identität des Absender-Mailservers wird überprüft. Beim Aufbau einer SMTP-Verbindung schickt der versendende Server ein "HELO" oder "EHLO" Kommando, mit dem er sich beim Zielserver identifiziert. Mit diesem Kommando übermittelt er seinen FQDN. Ist dieser syntaktisch nicht korrekt, wirkt sich diese Einschränkung aus und die Mail wird abgewiesen.
- **Unbekannter Hostname:** Es wird überprüft, ob der FQDN des versendenden Mailservers mittels DNS aufgelöst werden kann. Dazu wird wieder der FQDN des Senders verwendet und überprüft, ob für diesen ein DNS A oder ein MX Eintrag

© 2008 by eSYS Informationssysteme GmbH

existiert. Gibt es diesen nicht, wird die Mail abgewiesen. Weiters wird ein Reverse-DNS-Lookup für die IP-Adresse des sendenden Servers durchgeführt und das Ergebnis muss mit dem Hostnamen übereinstimmen. **ACHTUNG: Diese Option kann aufgrund falsch konfigurierter, sendender Mailserver zur Ablehnung von eigentlich erwünschten Emails kommen.**

- **SPF-Überprüfung:** SPF bedeutet Sender Policy Framework. Hinter diesem Begriff steckt eine Technik, die die missbräuchliche Verwendung von Email-Adressen als gefälschter Absender verhindern soll. Es wird geprüft, ob der versendende Mailserver auch berechtigt ist, E-Mails für die Absenderdomäne zu verschicken. Handelt es sich bei der eintreffenden Mail um eine Mail mit gefälschtem Absender, so wird die Mail abgewiesen. Details zu SPF finden Sie unter http://spf.pobox.com.
- **Absender kein FQDN:** Es wird überprüft, ob die Absenderadresse (MAIL FROM) in der Form eines FQDN ist. Ist dies nicht der Fall, wird die Mail abgewiesen.
- **Empfänger kein FQDN:** Es wird überprüft, ob die Empfängeradresse (RCPT TO) in der Form eines FQDN ist. Ist dies nicht der Fall, wird die Mail abgewiesen.
- **Unbekannte Absender-Domäne:** Es wird überprüft, ob die Absenderadresse einen DNS A oder einen MX Eintrag hat. Ist dies nicht der Fall, wird die Mail abgewiesen.
- **Absenderadresse nicht erreichbar:** Es wird überprüft, ob der Absenderadresse ein E-Mail zugestellt werden könnte. Ist dies nicht möglich, so wird die Mail abgewiesen.
- **Empfängeradresse nicht verifiziert:** Es wird überprüft, ob die Empfängeradresse vorhanden und erreichbar ist. Ist die Adresse nicht erreichbar, so wird die Mail abgewiesen.



8.9.2.3 Blacklists and Whitelists

Zur individuellen Anpassung des Spamfilters ist es dem Administrator möglich, eigene Black- und Whitelisten zu führen. Sie können eigene Listen für folgende Bereiche führen:

- **Hosts/IPs:** Definieren Sie einzelne Hostnamen oder IP-Adressen, von denen E-Mails explizit verweigert oder trotz positiver Spam-Klassifikation angenommen

© 2008 by eSYS Informationssysteme GmbH

werden sollen
- **Domänen/Emails:** Definieren Sie jene E-Mail-Domänen oder einzelnen E-Mail-Adressen, von denen E-Mails explizit verweigert oder trotz positiver Klassifikation angenommen werden sollen
- **Empfänger:** Definieren Sie jene E-Mail-Adressen von Empfängern, an welche E-Mails explizit nicht zugestellt oder trotz positiver Klassifikation zugestellt werden sollen.

Für jeden Eintrag in einer Black- und Whitelist können sie alternativ zwischen folgenden Aktionen wählen:

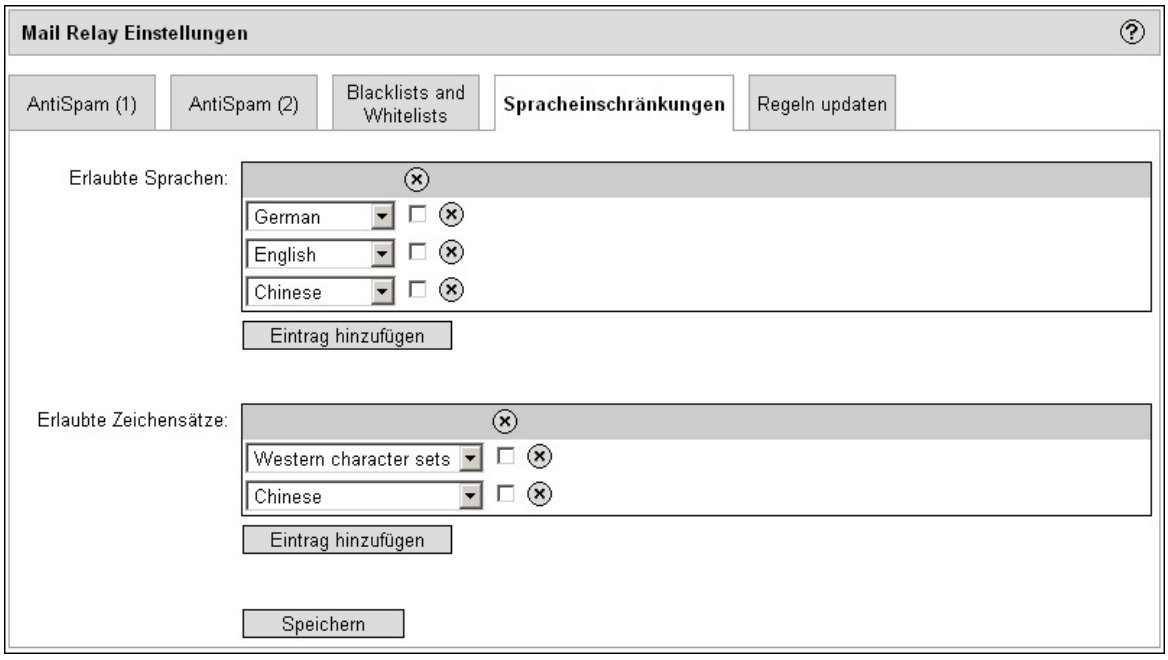
- **Zulassen:** E-Mails werden in jedem Fall zugestellt. Es werden keine Prüfungen durchgeführt.
- **Verweigern:** E-Mails werden in keinem Fall (unabhängig von den Spamfiltereinstellungen) zugestellt.

8.9.2.4 Spracheinschränkungen

In diesem Formular können Sie die Weiterleitung von Emails im Bezug auf die Sprache und den Zeichensatz einschränken. Beachten Sie jedoch, dass sämtliche nicht ausdrücklich erlaubten Sprachen oder Zeichensätze gesperrt werden. Wenn Sie keine Auswahl treffen, wird diese Option deaktiviert.

Erlaubte Sprachen: Wählen Sie hier jene Sprachen aus, in denen Emails verfasst sein müssen, damit sie durch gelassen werden.

Erlaubte Zeichensätze: Wählen Sie hier jene Zeichensätze aus, in denen Emails verfasst sein müssen, damit sie durch gelassen werden.



© 2008 by eSYS Informationssysteme GmbH

8.9.2.5 Regeln updaten

Aktivieren Sie das Kontrollkästchen, wenn Sie die von den Entwicklern von SpamAssassin bereitgestellten Updates für die Spambewertungsregeln automatisch herunterladen wollen.

8.9.3 AntiVirus

Gibraltar ist optional mit einem Virenscanner von Kaspersky Labs ausgestattet. Dieser ist in der Lage alle eingehenden E-Mails auf Viren zu überprüfen. Um den Virenscanner verwenden zu können, benötigen Sie eine gültige Kaspersky for Gibraltar Lizenz. Sie erhalten diese Erweiterung bei jedem Gibraltar Partner oder beim Hersteller.

Folgende Einstellungen können vorgenommen werden:

- **Administrator E-Mail:** Wenn Sie hier eine E-Mail-Adresse angeben, erhalten Sie eine Verständigung, wenn ein Virus erkannt wurde. Diese erfolgt unabhängig von der unten gewählten Aktion.
- **Quarantäne E-Mail:** Wenn Sie hier eine E-Mail-Adresse angeben, werden Mails mit erkannten Viren an diese Adresse geschickt. Diese Aktion erfolgt unabhängig von der unten gewählten Aktion.
- **Aktion, wenn Virus erkannt:** Aktion, die ausgeführt wird, wenn ein Virus erkannt wird.
- **Virus Lovers:** E-Mail-Adressen, welche infizierte E-Mails explizit erhalten sollen.

8.10 VPN

Gibraltar bietet mehrere Möglichkeiten VPNs zu errichten:

Site-to-Site VPN (Standortverbindung):

- IPSec VPN

Site-to-End VPN (Remote VPN, Anbindung von externen Benutzern):

- OpenVPN
- PPTP
- L2TP over IPSec
- SSL VPN

8.10.1 Open VPN

OpenVPN ist ein Dienst zum Erstellen von Virtuellen Privaten Netzwerken (wie z.B. auch PPTP oder L2TP/IPSec) über eine verschlüsselte Verbindung. Die Authentifizierung der Benutzer erfolgt durch Zertifikate, die durch das Zertifikatsmenü der Firewall jederzeit widerrufen werden können. Clients stehen für die verschiedenen Plattformen (z.B.: http://www.openvpn.net/index.php/downloads.html - OpenVPN 2.1_rc7 (Link getestet am 2008-06-26)) kostenlos zur Verfügung.

In der Gibraltar Firewall wird nur die Authentifizierung über PKI (Zertifikate) verwendet, da

© 2008 by eSYS Informationssysteme GmbH

sie im Vergleich zur Variante mit Preshared-Secrets mehr Möglichkeiten, wie z.B. das Widerrufen von Zertifikaten, bietet.

Zu beachten ist allerdings, dass es notwendig ist, einige Anpassungen vorzunehmen, damit OpenVPN auch auf Clients ohne Administratorrechte läuft. Siehe dazu diese Anleitung.

Benutzer von MS Windows Vista müssen den Benutzerkontenschutz (UAC = User Account Control) abschalten, damit OpenVPN fehlerfrei funktioniert.
Sie können dies bequem durchführen, indem Sie auf Start - Programme - OpenVPN - "Disable User Account Control" klicken und die Ausführung bestätigen.

8.10.1.1 Allgemeine Einstellungen

In dieser Registerkarte werden die allgemeinen Einstellungen für OpenVPN durchgeführt.

Auf dem Client wird ein entsprechender OpenVPN Client benötigt, der frei verfügbar ist und auf dieser Seite heruntergeladen werden kann. Der Client ist für alle gängigen Plattformen (Windows, Linux, MacOS) verfügbar. Auf dem Client muss anschließend die Konfigurationsdatei und das Benutzerzertifikat eingebunden werden. Danach kann die Verbindung aufgebaut werden (siehe Anwendungsbeispiel OpenVPN).

- **IP Adresse:** IP-Adresse des Open VPN Servers auf Gibraltar. Wählen Sie **ANY**, falls Sie jede konfigurierte IP-Adresse verwenden wollen. In diesem Fall müssen Sie für die Clientkonfiguration jedoch eine eindeutige IP-Adresse festlegen.
- **Server IP/Hostname für Clientkonfiguration:** nur notwendig wenn Sie **ANY** als IP Adresse für den Server konfiguriert haben. Diese IP/Hostname wird anschließend in der Clientkonfigurationsdatei gespeichert und kann über den Button **Konfiguration herunterladen** heruntergeladen werden.
- **TCP/UDP:** Wählen Sie das gewünschte Übertragungsprotokoll.
- **Port:** Wählen Sie den gewünschten Port für OpenVPN (Standard 1194).
- **Als Gateway verwenden:** Der gesamte Traffic wird über die VPN Verbindung geleitet.
- **Geroutete Netzwerke:** Um Zugriff auf interne Netzwerke zu erlauben, muss zusätzlich das Netzwerk angegeben werden. Sollte z.B. ein externer Mitarbeiter auf das interne 192.168.0.0/24-Netz zugreifen wollen, so muss dieses Netz hier explizit angegeben werden.
- **Clientkonfig. herunterladen:** Nach dem Ändern von Daten in dieser Registerkarte kann eine aktualisierte Konfigurationsdatei über diesen Button heruntergeladen werden und am Client eingespielt werden.

HINWEIS: Beim ersten Start von OpenVPN werden automatisiert einige kryptographische Schlüssel erzeugt. Dieser Vorgang kann einige Sekunden bis einige Minuten dauern.

© 2008 by eSYS Informationssysteme GmbH

8.10.1.2 Erweiterte Einstellungen

Die Einstellungen in dieser Registerkarte sind Experteneinstellungen und im Normalfall für den Benutzer nicht notwendig.

- **Komprimierung aktivieren:** Deaktiviert die standardmäßige Komprimierung.
- **Keep alive (Ping):** Überprüfungsintervall in Sekunden. Zur Überprüfung der Verbindung wird regelmäßig ein Ping an der Server gesendet.
- **Keep alive (Timeout):** Die Verbindung wird neu aufgebaut, falls im angegebenen Zeitraum kein Paket erhalten wurde..
- **IP Bereich:** Netzwerkbereich, aus dem der Client eine IP-Adresse erhält.
- **interner DNS Server 1:** Interner DNS Server (wird an den Client übermittelt)
- **interner DNS Server 2:** Interner DNS Server (wird an den Client übermittelt)
- **interner WINS Server:** Interner WINS Server (wird an den Client übermittelt)
- **Fragmentierung erlauben:** Pakete werden fragmentiert und es werden keine größere Pakete als angegeben versendet.
- **MTU Größe:** Ändert die MTU Größe für das TUN-Interface.
- **MSS Fix:** Durch diesen Wert kann die MTU-Größe von TCP-Verbindungen, die über den OpenVPN Tunnel laufen, verändert werden. Dieser Wert sollte in Verbindung mit "Fragmentierung erlauben" eingesetzt werden.
- **Float:** Durch Float ist es möglich, dass sich die IP Adresse eines Clients verändert (z.B. Dial-In), die Authentifizierungsdaten werden anschließend von der neuen IP akzeptiert und die Verbindung bleibt aufrecht.
- **Neues Serverzertifikat:** Ein neues Serverzertifikat wird erstellt. **Achtung: Es muss zuerst das alte Zertifikat revokiert werden.**
- **Konfiguration herunterladen:** Herunterladen der aktualisierten Konfigurationsdatei nach jeder Konfigurationsänderung.

8.10.1.3 Status

In dieser Registerkarte werden die Statusdaten zu bestehenden OpenVPN Verbindungen aufgelistet.

Der Common Name ist der Name des Benutzers mit der zugewiesenen IP Adresse. Die empfangenen und gesendeten Bytes sind ebenso aufgelistet wie der Zeitpunkt, seit dem die

© 2008 by eSYS Informationssysteme GmbH

Verbindung aufrecht ist.

8.10.2 IPSec

IPSec ist ein Kommunikationsprotokoll zur Herstellung von VPNs. Es kann sowohl als Protokoll für Site-to-Site Verbindungen als auch für End-to-Site Verbindungen (Remote-Zugriff) verwendet werden.

8.10.2.1 IPSec - Allgemeine Einstellungen

Bevor Sie ein IPSec VPN konfigurieren können müssen Sie jene Netzwerkschnittstellen für VPN aktivieren, welche einen VPN Endpunkt bilden sollen. Befindet sich ihre Gibraltar Firewall hinter einer zusätzlichen Firewall mit NAT oder wollen Sie von einem VPN Gateway welcher sich hinter einer NAT-Firewall befindet einen VPN Tunnel aufbauen, ist es erforderlich, die Funktion "NAT Traversal" zu aktivieren. Sollten Sie keine statische IP-Adresse für Ihre Internetverbindung haben, so wählen Sie die Option "Über Standardroute".

ACHTUNG: Wenn Sie NAT Traversal verwenden, müssen Sie auf der Gegenstelle den Traffic auf UDP-Port 4500 erlauben.

8.10.2.2 Tunnel

In der Übersicht "Tunnel" finden Sie alle auf Ihrer Gibraltar Firewall konfigurierten VPN-Tunnel. Die Liste enthält folgende Informationen:

- **Bezeichnung:** Die von Ihnen gewählte Bezeichnung des VPN-Tunnels
- **Lokale IP:** Die IP-Adresse des lokalen Endpunktes des Tunnels
- **Lokales Subnetz:** Die Netzwerkadresse des lokalen Subnetzes, das über den Tunnel erreichbar ist (z.B. internes LAN)
- **IP oder FQDN Gegenstelle:** Die IP-Adresse oder der FQDN der Gegenstelle des Tunnels
- **Subnetz Gegenstelle:** Die Netzwerkadresse der Gegenstelle
- **Status:** Der gegenwärtige Status des VPN-Tunnels. Mögliche Werte sind:
  deaktiviert
  standby
  gestartet

Folgende Aktionen stehen Ihnen in der Übersicht zur Verfügung:

- **Tunnel starten** : Startet den VPN-Tunnel wenn dieser **deaktiviert** oder **standby** ist
- **Tunnel stoppen (Standby Mode)** : Versetzt den VPN-Tunnel in den **standby** Modus wenn dieser aktiviert ist
- **Tunnel aktivieren (Standby Mode)** : Versetzt den VPN-Tunnel in den **standby** Modus wenn dieser deaktiviert ist
- **Tunnel deaktivieren** : Deaktiviert den VPN-Tunnel
- **Tunnel bearbeiten** : Bearbeitet den Tunnel
- **Tunnel löschen** : Löscht den Tunnel

© 2008 by eSYS Informationssysteme GmbH

8.10.2.2.1 Tunnel - Standard

Auf der Registerkarte **Standard** werden die grundlegenden Einstellungen für einen IPSec Tunnel durchgeführt.
Folgende Einstellungen müssen vorgenommen werden:

- **Bezeichnung:** Eine frei zu wählende Bezeichnung für den VPN-Tunnel
- **Status nach dem Start:** Der Status des VPN-Tunnels nach dem Neustart des IPSec-Dienstes. Mögliche Werte sind:
  deaktiviert: Der VPN-Tunnel steht nicht für einen Verbindungsaufbau zur Verfügung und ist deaktiviert
  standby: Eine Verbindung nach außen oder von außen kann aufgebaut werden
  gestartet: Der VPN-Tunnel wird sofort nach dem Start des IPSec-Dienstes aufgebaut, sofern sich die Gegenstelle auf **standby** oder **gestartet** befindet.
- **Lokale IP:** Wählen Sie die lokale IP-Adresse für den VPN-Tunnel. Sie können zwischen den IP-Adressen der von Ihnen für IPSec aktivieren Netzwerkschnittstellen bzw "Via Default Route" wählen.
- **Lokales Subnetz:** Das lokale Subnetz, auf welches die Remotebenutzer der Gegenstelle Zugriff haben sollen.
- **Lokales Zertifikat:** Wählen Sie jenes Zertifikat aus, welches für die Authentifizierung mit der Gegenstelle verwendet werden Soll. Sie können nur ein Zertifikat auswählen, für das es einen private Key gibt. Diese Einstellung benötigen Sie nur wenn Sie mit Zertifikaten authentifizieren wollen. Eine Authentifizierung mit Zertifikaten wird aus Sicherheitsgründen empfohlen.
- **IP oder FQDN Gegenstelle:** Wenn der Tunnel zu einer bestimmten Gegenstelle aufgebaut werden soll, geben Sie hier die IP-Adresse oder den FQDN der Gegenstelle ein und aktivieren Sie die Option **Host**. Falls Sie mit mehreren Hosts Tunnels aufbauen wollen (Site-to-End VPN, Remote VPN) wählen Sie die Option **Jede Gegenstelle** aus. Die Angabe einer bestimmten IP-Adresse ist in diesem Fall nicht notwendig.
- **Subnetz Gegenstelle:** Die Netzwerkadresse des Netzwerks, das sich hinter der Gegenstelle befindet. Die lokalen Benutzer erhalten in weiterer Folge Zugriff auf das angegebene Remote-Subnetz. Option "Spezialfall für Roadwarrior hinter NAT-Gateway: rightsubnetwithin": Wenn Sie einen Laptop hinter einem NAT-Gateway betreiben, dessen IP-Adresse sich ändert, können Sie hier im Feld "Subnetz Gegenstelle" 0.0.0.0/0 angeben und der Roadwarrior kann sich mit dem Subnetz hinter der Gibraltar Firewall verbinden.
- **Autorisierung:** Die Art der zu verwendenden Autorisierungsmethode. Folgende Möglichkeiten stehen zur Verfügung:
  Passwort: Die Autorisierung erfolgt anhand eines Passworts und wird auch noch "**Shared Secret**" genannt. Wählen Sie ein sicheres Passwort und geben Sie dieses auch bei der Konfiguration der Gegenstelle ein.
  X509 Zertifikat: Die Autorisierung erfolgt anhand von Zertifikaten. Wählen Sie jenes Zertifikat aus, welches für die Autorisierung bei der Gegenstelle verwendet werden soll. Bevor Sie ein Zertifikat auswählen können, müssen Sie dieses mit der Zertifikatsverwaltung auf Gibraltar importieren.
  Autorisiert von Zertifizierungsstelle: Die Autorisierung erfolgt durch eine zentrale Zertifizierungsstelle. Dabei werden die Zertifikate der Hosts von einer Zertifizierungsstelle signiert, welche die Authentizität der Hosts überprüft und

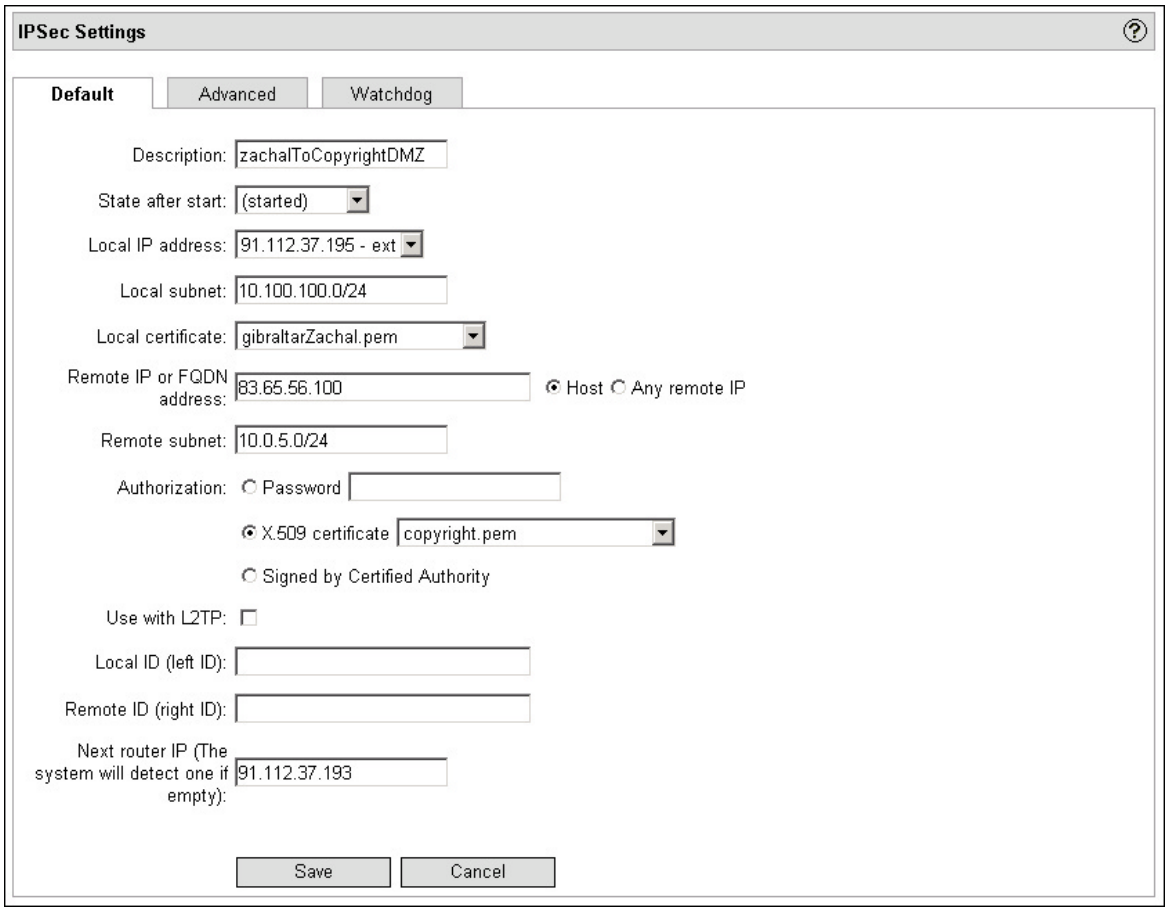
© 2008 by eSYS Informationssysteme GmbH

garantiert.

- **Für L2TP verwenden:** Aktivieren Sie diese Option, wenn der VPN-Tunnel für den Aufbau einer L2TP-Verbindung (Remote VPN) verwendet werden soll. Falls Sie diese Option aktivieren, dürfen Sie in beiden Subnetz-Textfeldern keine Einträge vornehmen. Zusätzlich sollten sie die Option "Autorisiert von Zertifizierungsstelle" auswählen, da Gibraltar in diesem Fall als Zertifizierungsstelle die ordnungsgemäße Autorisierung der Clients sicherstellt.
- **Lokale ID:** Wird teilweise zur Herstellung von VPN-Verbindungen zu Drittprodukten benötigt (left id)
- **Remote ID:** Wird teilweise zur Herstellung von VPN-Verbindungen zu Drittprodukten benötigt (right id)
- **Nächste Router IP:** Die IP-Adresse des nächsten Routers. Diese Option benötigen Sie wenn Sie z.B. über zwei Internetleitungen verfügen. Im Normalfall ermittelt Gibraltar die richtige IP automatisch.

ACHTUNG: Um den Datenverkehr über IPSec Tunnels zu erlauben, müssen Sie für die jeweiligen IPSec Interfaces (zB: eingehend "ipsec0" und ausgehend "int0") Filterregeln definieren.

WICHTIG: Falls Sie vorhaben, für Tunnel mit "Roadwarrior" (Gegenstellen ohne fixe IP-Adresse) keinen gemeinsamen Preshared key zu verwenden, so müssen Sie mit X509 Zertifikaten authentifizieren (empfohlen)!



© 2008 by eSYS Informationssysteme GmbH

8.10.2.2.2 Tunnel - Erweitert

Im Bedarfsfall können Sie für einen IPSec VPN-Tunnel erweiterte Einstellungen vornehmen. Folgende Detaileinstellungen stehen zur Verfügung:

- **Art:** Übertragungsmodus von IPSec. Es stehen folgende Modi zur Verfügung:
  Transport: Im Transportmodus wird der IPSec Header zwischen dem IP-Header und den Nutzdaten eingefügt. Der IP-Header bleibt unverändert und dient weiterhin zum Routing des Pakets vom Sender zum Empfänger. Der Transportmodus wird verwendet, wenn die kryptografischen Endpunkte auch die Kommunikations-Endpunkte sind und funktioniert aus diesem Grund nur bei Host-to-Host Verbindungen.
  Tunnel (Standard): Im Tunnelmodus wird das ursprüngliche Paket gekapselt und die Sicherheitsdienste von IPSec auf das gesamte Paket angewandt. Der neue (äußere) IP-Header dient dazu, die Tunnelenden zu adressieren, während die Adressen der eigentlichen Kommunikationsendpunkte im inneren IP-Header stehen. Der Tunnelmodus kann für Site-to-Site wie auch für Site-to-End Verbindungen verwendet werden.
- **IP Kompression:** Komprimiert die Daten. Diese Einstellung müssen Sie auch an der Gegenstelle vornehmen. Falls ein Tunnelendpunkt diese Option deaktiviert hat, findet die gesamte Übertragung unkomprimiert statt.
- **PFS (Perfect forwarding secrecy):** Aktiviert ein zusätzliches Schlüsselmanagement Protokoll, das den Schlüssel des Verschlüsselungsalgorithmus in zeitlichen Abständen neu generiert. Damit wird verhindert, dass ein kompromittierter Schlüssel ein dauerhaftes Sicherheitsrisiko darstellt.
- **Anzahl der Versuche:** Die Anzahl der Versuche für einen Aufbau des VPN-Tunnels zur Gegenstelle. Geben Sie den Wert 0 ein, wenn Sie diese nicht beschränken wollen.
- **Lebensdauer Key (IKE - Phase 1):** Die Lebensdauer des Schlüssels der ersten Phase
- **Lebensdauer Key (Phase 2):** Die Lebensdauer des Schlüssels der zweiten Phase
- **Phase 1:** Stellen Sie hier IKE und Hash Algorithmen, sowie die Diffie Hellman Gruppen ein.
- **Phase 2:** Stellen Sie hier ESP und Hash Algorithmen für die Phase 2 ein.

8.10.2.2.3 Watchdog

Der IPSec Watchdog überprüft die IPSec Verbindung zwischen "Local IP" und "Remote IP" und startet gegebenenfalls den Tunnel oder die IPSec Verbindung neu.
Es ist auch möglich eine Mailbenachrichtigung zu erhalten. Der Watchdog muss für jeden Tunnel konfiguriert werden. Sie können das Überprüfungsintervall frei wählen.

8.10.3 PPTP

PPTP (Point-to-Point Tunneling Protocol) ist ein von einem Herstellerkonsortium (Ascend Communications, Microsoft, 3 Com, u.a.) entwickeltes Protokoll zum Aufbau eines VPN. Es ermöglicht das Tunneling des PPP durch ein IP-Netzwerk, wobei die einzelnen PPP-Pakete wiederum in GRE-Pakete verpackt werden.

Da PPTP in Microsoft Windows integriert ist, ist es trotz einiger Sicherheitsbedenken sehr weit verbreitet.

© 2008 by eSYS Informationssysteme GmbH

PPTP kann in Gibraltar zur Herstellung von Site-to-End VPN Verbindungen (Remote VPN) verwendet werden. Da mit Microsoft Windows PPTP Verbindungen sehr einfach aufgebaut werden können ist die Konfiguration problemlos.

Im PPTP Modul werden die allgemeinen Einstellungen für PPTP vorgenommen. Einzelne Benutzer können Sie in weiterer Folge mit der in Gibraltar integrierten Benutzerverwaltung für PPTP aktivieren.

8.10.3.1 PPTP - Allgemeine Einstellungen

Wollen Sie PPTP zum Aufbau von VPN-Verbindungen verwenden, ist es erforderlich, folgende Einstellungen vorzunehmen:

- **Lokale IP (mit Netzwerkmaske):** Die lokale IP-Adresse in der CIDR-Notation, über die Gibraltar die Remote-Verbindungen weitergibt. Der Verbindungsaufbau findet natürlich über eine öffentliche IP-Adresse statt. Intern treten die Remote-Verbindungen jedoch über diese lokale IP-Adresse auf. Definieren Sie entsprechende Routing Einträge im Modul Netzwerk, falls die Remotebenutzer nicht im gleichen Subnetz sind.
- **Remote IP von und Remote IP bis:** Jener IP-Adressbereich, aus welchem Remotebenutzer eine IP-Adresse erhalten nachdem Sie erfolgreich angemeldet wurden.
- **Domäne:** Die Domäne, welche den Remotebenutzern zugewiesen wird.
- **DNS Server:** Die IP-Adresse eines DNS Servers im lokalen Netzwerk. Damit wird für den Remotebenutzer eine korrekte Namensauflösung sichergestellt.
- **WINS Server:** Die IP-Adresse eines WINS Servers im lokalen Netzwerk. Sie benötigen diese Einstellung nur, falls Sie einen WINS Server verwenden.

TIPP: Vergessen Sie nicht, die Paketfilterregeln für den Service "pptp" auf "ACCEPT" zu setzen, um eine PPTP Verbindung von außen auf die Firewall aufbauen zu können.

8.10.3.2 PPTP - Erweiterte Einstellungen

Folgende erweiterte Einstellungen können vorgenommen werden:

- **Maximum transmission unit (MTU):** Die maximale Paketgröße in Bytes, die über PPTP übertragen werden kann, ohne dass das Datenpaket fragmentiert werden muss.
- **Maximum receive unit (MRU):** Die maximale Größe eines zu verarbeitenden Datenpakets in Bytes.
- **Broadcasts weiterleiten:** Aktivieren Sie jene Interfaces, über die Broadcasts weitergeleitet werden sollen.

8.10.4 L2TP

L2TP über IPSec stellt eine weitere Variante dar, einzelne Benutzer über eine geschützte Verbindung (VPN) mit dem internen Netzwerk zu verbinden. Dabei wird von einem einzelnen Rechner aus ein IPSec-Tunnel mit der Firewall aufgebaut. Über diesen erfolgt der verschlüsselte Austausch der Daten mit dem internen Netzwerk. Bei dem Remote-Rechner kann dabei der bereits in Microsoft Windows XP integrierte Wizard zur Erstellung von VPN-Zugängen verwendet werden, was zusätzliche Kosten für die Software eines Drittanbieters erspart.

© 2008 by eSYS Informationssysteme GmbH

Eine Anleitung für die Erstellung eines Client-Zertifikats und dessen Upload auf Windows XP wird Ihnen auf unserer Homepage unter der Rubrik "Downloads" zusammen mit einer kleinen EXE-Datei zum Upload des Zertifikats angeboten (Gibraltar Homepage).

8.10.4.1 L2TP - Allgemeine Einstellungen

HINWEIS: Beachten Sie die Hinweise auf der Gibraltar Homepage.

Die Konfiguration der L2TP Verbindungen erfolgt analog der Konfiguration von PPTP.

ACHTUNG: Bei einer L2TP-Verbindung wird der Verkehr über einen IPSec-Tunnel abgewickelt. Es sind daher einige zusätzliche Filteregeln notwendig, damit dieser Verkehr auch ungehindert fließen kann. Der L2TP-Verbindungsaufbau trifft über das IPSec-Interface auf Gibraltar ein. Daher ist von ipsec0 auf LOCAL der Verkehr zu erlauben (Quell- und Zielport auf UDP/1701). Die eigentlichen Daten fließen dann über ein PPP-Interface. Daher ist auch der Verkehr von ppp+ auf das jeweilige Netz zu erlauben (z.B. von ppp+ auf int). Hier sollten Sie nur die benötigten Ports öffnen.

8.10.5 Zertifikate

Auf der Registerkarte **Zertifikate** können Sie selbst erstellte Zertifikate verwalten und die Zertifikate der Gegenstelle hochladen. In drei Elementgruppen werden diese Zertifikate verwaltet (**Host Zertifikate**, **CA Zertifikate** und **Private Schlüssel**).

Host Zertifikate

Host Zertifikate sind Zertifikate, die von Ihnen oder einer VPN-Gegenstelle erstellt wurden und für die Authentifizierung verwendet werden.

- **Dateiname:** Zeigt den Namen der Zertifikatsdatei.
- **Organisation:** Zeigt die Organisation an.
- **Eigentümer:** Zeigt den Eigentümer des Zertifikates an.
- **E-Mail:** Zeigt die E-Mail Adresse des Eigentümers an.
- **Ablaufdatum:** Zeigt an, bis wann dieses Zertifikat gültig ist.
- **Markierte Einträge löschen** : Markieren Sie jene Einträge in der Elementgruppe durch Aktivieren des Kontrollkästchens, die Sie löschen wollen. Betätigen Sie anschließend die Schaltfläche in der Kopfzeile, um die Elemente zu löschen.
- **Zertifikat löschen** : Betätigen Sie diese Schaltfläche, um das Zertifikat zu löschen.
- **Zertifikat downloaden** : Betätigen Sie diese Schaltfläche, um dieses Zertifikat herunterzuladen. Sie müssen anschließend einen Speicherort wählen.
- **Zertifikat hinzufügen:** Betätigen Sie diese Schaltfläche, wenn Sie ein neues Host Zertifikat hochladen möchten.

CA Zertifikate

CA Zertifikate sind Zertifikate von bekannten Zertifizierungsstellen.

- **Dateiname:** Zeigt den Namen der Zertifikatsdatei.
- **Organisation:** Zeigt die Organisation an.

© 2008 by eSYS Informationssysteme GmbH

- **Eigentümer:** Zeigt den Eigentümer des Zertifikates an.
- **E-Mail:** Zeigt die E-Mail Adresse des Eigentümers an.
- **Ablaufdatum:** Zeigt an, bis wann dieses Zertifikat gültig ist.
- **Markierte Einträge löschen :** Markieren Sie jene Einträge in der Elementgruppe durch Aktivieren des Kontrollkästchens, die Sie löschen wollen. Betätigen Sie anschließend die Schaltfläche in der Kopfzeile, um die Elemente zu löschen.
- **Zertifikat löschen :** Betätigen Sie diese Schaltfläche, um das Zertifikat zu löschen.
- **Zertifikat downloaden :** Betätigen Sie diese Schaltfläche, um dieses Zertifikat herunterzuladen. Sie müssen anschließend einen Speicherort wählen.
- **Zertifikat hinzufügen:** Betätigen Sie diese Schaltfläche, wenn Sie ein neues CA Zertifikat hochladen möchten.

Private Schlüssel

Beim privaten Schlüssel handelt es sich um den privaten kryptografischen Schlüssel der lokal erstellten Host Zertifikate

Erzeugen eines Zertifikats

- **Zertifikat generieren:** Betätigen Sie diese Schaltfläche, um ein neues Host-Zertifikat zu generieren. Sie werden in ein Formular zur Generierung weitergeleitet.
- **Clientzertifikat generieren:** Betätigen Sie diese Schaltfläche, um ein neues Clientzertifikat zu generieren. Sie können dieses von einer CA unterschriebene Zertifikate verwenden, um client-to-network VPN Verbindungen mit Windows 2000 und Windows XP zu erlauben. Sie werden in ein Formular zur Generierung weitergeleitet.

8.10.5.1 Certificate Revocation List

Durch eine Certificate Revocation List (CRL) lassen sich bereits ausgestellte Zertifikate widerrufen (z.B. für verlorene Zertifikate oder ehemalige Mitarbeiter) und der Zugang mit diesen Zertifikaten ist anschließend nicht mehr möglich.

In dieser Übersicht sind die ausgestellten Zertifikate enthalten. Für jedes Zertifikat ist das Ablaufdatum sowie der Status angegeben. Gültige Zertifikate können anschließend revokiert, also die Gültigkeit widerrufen werden.

HINWEIS: Ein Benutzer mit einem revokierten Zertifikat kann sich anschließend nicht mehr damit authentifizieren. Es muss gegebenenfalls ein neues Zertifikat ausgestellt werden.

8.10.5.2 Hostzertifikat erstellen

Bei der Erstellung eines Hostzertifikates müssen Sie einige Informationen eingeben, die im Zertifikat abgelegt werden und zur Identifikation dienen. Einige dieser Informationen werden in der Übersichtsanzeige in den Elementgruppen dargestellt, um die Zertifikate voneinander unterscheiden zu können.

- **Name des Zertifikats (ohne Dateiendung):** Geben Sie eine Bezeichnung für das zu erstellende Zertifikat ein (z.B.: standortACert).

© 2008 by eSYS Informationssysteme GmbH

- **Schlüssellänge:** Wählen Sie einen Wert aus der Auswahlliste für die Verschlüsselung des Zertifikats. Je höher dieser Wert ist, desto höher ist auch der Aufwand, um den Schlüssel zu knacken. Damit ist aber auch ein höherer Rechenaufwand bei der Verschlüsselung verbunden.
- **Gültigkeit (Tage):** Dieser numerische Wert gibt die Gültigkeit des Zertifikates in Tagen an. Nach Ablauf dieser Zeitdauer wird das Zertifikat nicht mehr akzeptiert.
- **Landescode:** Geben Sie hier Ihr Länderkürzel ein (z.B. "AT" für Österreich, "DE" für Deutschland).
- **Region:** Geben Sie die Region an, in der Sie sich befinden.
- **City:** Geben Sie die Stadt bzw. den Ort an, in dem Sie sich befinden.
- **Organisation:** Geben Sie hier die Bezeichnung der Organisation oder Firma an, für die das Zertifikat erstellt werden soll.
- **Abteilung:** Geben Sie hier die Bezeichnung der Abteilung an, für die dieses Zertifikat erstellt werden soll.
- **Eigentümer:** Geben Sie hier den Namen des Eigentümers des Zertifikates an.
- **E-Mail:** Geben Sie hier die E-Mail Adresse des Eigentümers des Zertifikates an.

Nachdem Sie ein neues Host Zertifikat erstellt haben, können Sie anschließend den öffentlichen Schlüssel über den GibADMIN herunterladen. Dieser öffentliche Schlüssel muss in weiterer Folge bei der gewünschten VPN-Gegenstelle hochgeladen werden und wird dort für die Authentifizierung der VPN-Verbindung benötigt.

8.10.5.3 Clientzertifikat erstellen

Bei der Erstellung eines Clientzertifikates müssen Sie einige Informationen eingeben, die im Zertifikat abgelegt werden und zur Identifikation dienen.

- **Schlüssellänge:** Wählen Sie einen Wert aus der Auswahlliste für die Verschlüsselung des Zertifikats. Je höher dieser Wert ist, desto höher ist auch der Aufwand um den Schlüssel zu knacken. Damit ist aber auch ein höherer Rechenaufwand bei der Verschlüsselung verbunden.
- **Passwort:** Geben Sie ein Passwort für das zu erstellende Zertifikat ein. Sie brauchen dieses Passwort später, wenn sie mit OpenVPN eine VPN Verbindung zur Gibraltar Firewall aufbauen wollen.
- **Gültigkeit (Tage):** Dieser numerische Wert gibt die Gültigkeit des Zertifikates in Tagen an. Nach Ablauf dieser Zeitdauer wird das Zertifikat nicht mehr akzeptiert.
- **Landescode:** Geben Sie hier Ihr Länderkürzel ein (z.B. AT für Österreich, DE für Deutschland).
- **Region:** Geben Sie die Region an, in der Sie sich befinden.
- **City:** Geben Sie die Stadt bzw. den Ort an, in dem Sie sich befinden.
- **Organisation:** Geben Sie hier die Bezeichnung der Organisation oder Firma an, für die das Zertifikat erstellt werden soll.
- **Abteilung:** Geben Sie hier die Bezeichnung der Abteilung an, für die dieses Zertifikat erstellt werden soll.
- **Eigentümer:** Wählen Sie hier den Eigentümer des Zertifikates aus. Dieser muss in der Benutzerverwaltung angelegt sein.
- **E-Mail:** Geben Sie hier die E-Mail Adresse des Eigentümers des Zertifikates an.

Nachdem Sie ein Clientzertifikat generiert haben, müssen Sie dieses downloaden. Verwenden Sie dieses Zertifikat (client_cert.p12), um eine IPSec bzw. OpenVPN Verbindung zur

© 2008 by eSYS Informationssysteme GmbH

Gibraltar Firewall aufzubauen.

8.10.6 SSL

SSL (Secure Socket Layer) ist ein Verschlüsselungsprotokoll für Datenübertragung im Internet. Die SSL Funktion von Gibraltar kann dazu verwendet werden, potenziell unsichere Services via SSL zu verschlüsseln. Sie können mit dieser Funktion zum Beispiel einen HTTP Server über HTTPS anbieten. Dadurch wird der gesamte Verkehr über diese Verbindung verschlüsselt übertragen und ist somit vor unerwünschtem Zugriff besser geschützt.

Ein SSL Service definieren Sie durch folgende Angaben:

- **Lokaler Port:** Jener Port, an den die Anfragen gesendet werden. In weiterer Folge werden diese Anfragen auf eine IP Adresse und den eigentlichen Port des Services weitergeleitet. Sie können den entsprechenden Port aus einer vordefinierten Liste von SSL Ports auswählen.
- **Port (custom):** Frei zu wählender Port.
- **Weiterleiten an (IP):** IP Adresse an welche die Anfragen weitergeleitet werden.
- **Weiterleiten an (Port):** Port an welchen die Anfragen weitergeleitet werden.

BEISPIEL: Sie wollen von außerhalb Ihres Netzwerks E-Mails von einem internen POP-Server abrufen. Der POP Server unterstützt jedoch kein POP3S (SSL Verschlüsselung). Durch die SSL Funktion von Gibraltar können Sie nach außen POP3S anbieten und alle Anfragen auf diesem Port an den internen POP Server weiterleiten. Die Kommunikation zwischen Gibraltar und dem POP3 Client läuft in diesem Fall verschlüsselt.

TIPP: Vergessen Sie nicht, eine Paketfilterregel für den von Ihnen angegebenen Port auf ACCEPT zu setzen.

8.10.7 SSL VPN

SSL VPN ist ein webbasierter SSL-VPN Server. Der Benutzer verbindet sich mit einem Webbrowser auf den VPN Server und hat anschließend einige Dienste zur Verfügung. Ein typisches Anwendungsszenario ist die Herstellung einer Verbindung zu einem Windows Rechner mit Remote-Desktop (RDP) über die SSL-verschlüsselte Verbindung. Für diese Art von VPN wird, sofern Java auf dem Rechner installiert ist, keine zusätzliche Software benötigt.

Über das Webinterface der Gibraltar Firewall kann der Installierungsprozess gestartet werden, konfiguriert wird SSL VPN über das eigene Webinterface. Nach der Auswahl des Interfaces und dem Speichern kann mit dem Button Installation starten der Installationsprozess gestartet werden.
Anschließend kann mit dem Browser über **http://ip_des_ausgewählten_interfaces:28080** die Installation vorgenommen werden.

ACHTUNG: Es ist nicht möglich während der Installation zusätzliche Pakete bzw. die Enterprise Edition von SSL VPN zu installieren. Es können nur die vorgewählten Pakete verwendet werden. Neue Pakete können nach Anfrage in die nächste Version integriert werden.

© 2008 by eSYS Informationssysteme GmbH

Eine ausführliche Anleitung zum SSL VPN (englisch) kann unter https://3sp.com/showSslExplorerCommunity.do bzw. unter https://3sp.com/products/ssl-explorer/documentation/Getting_Started_Guide.pdf nachgelesen werden.

WICHTIG: Vergessen Sie nicht, den SSL VPN Dienst im Menü Dienste zu starten.

8.11 Proxy-Server

Gibraltar verfügt über mehrere Proxy Server, die den Netzwerkverkehr durch Überprüfung auf Applikationsebene sicherer gestalten. Ein Proxy Server "versteht" den Datenverkehr den er übermittelt. So ist es einem HTTP (Web) Proxy bspw. möglich, den gesamten Web-Traffic auf Viren oder gefährlichen Inhalt zu prüfen.
Ein weiteres Beispiel ist der in Gibraltar integrierte SMTP (Mail) Proxy. Mit diesem ist es möglich, den gesamten E-Mail-Traffic auf Viren und Spam zu überprüfen.

Gibraltar verfügt über folgende Proxy-Server:

- **HTTP-Proxy:** für Web-Traffic
- **POP3-Proxy:** für E-Mail via POP3
- **FTP-Proxy:** für FTP Dateitransfer
- **SMTP-Proxy:** für E-Mail via SMTP zwischen Mailservern (siehe Mail - Allgemeine Einstellungen)

Zusätzlich unterstützt Gibraltar drei verschiedene Anonymisierungsdienste, die ebenfalls als Proxy Server arbeiten.

8.11.1 HTTP-Proxy

Um den HTTP-Proxy verwenden zu können, müssen Sie diesen konfigurieren und den entsprechenden Dienst starten. Bei Verwendung stehen Ihnen folgende Funktionen zur Verfügung:

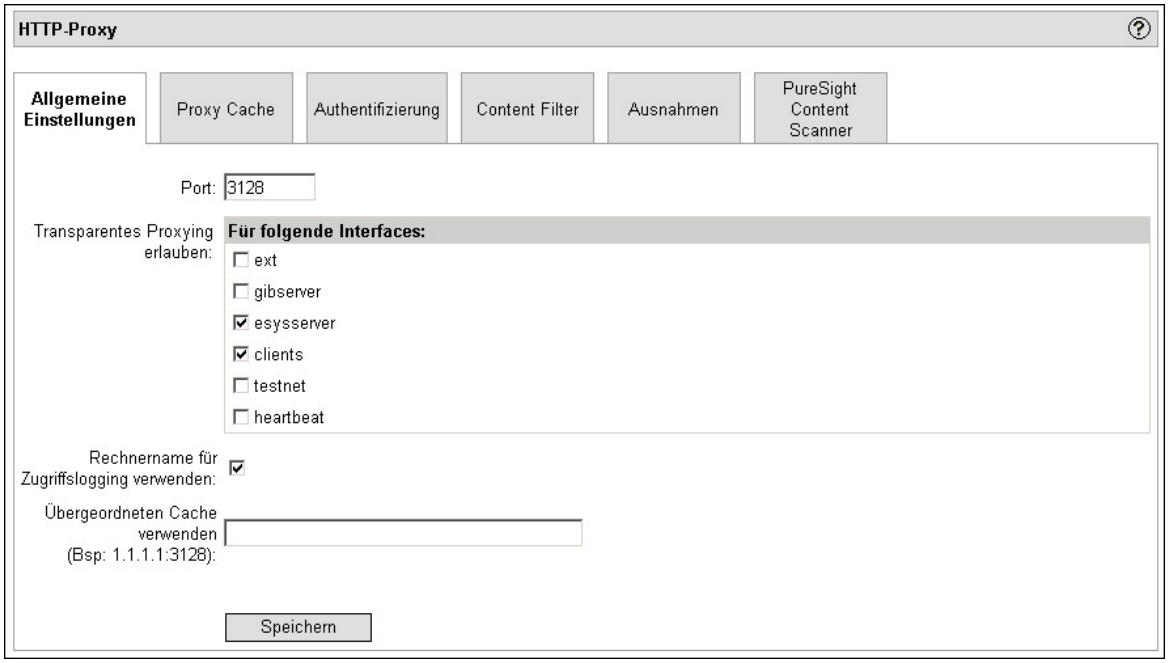
- **Transparenter Proxy-Server:** Die Benutzer müssen keine Einstellungen im Browser vornehmen. Anfragen an Webserver werden von Gibraltar automatisch mit dem transparenten Proxy Server durchgeführt.
- **Caching:** Webinhalte werden auf Gibraltar zwischengespeichert und ohne erneutes Abrufen aus dem Internet dem Benutzer zur Verfügung gestellt. So kann die Bandbreite der Internetverbindung entlastet werden.
- **Authentifizierung:** Nutzen Sie die Authentifizierungsfunktion des Proxy-Servers müssen sich Benutzer vor dem Zugriff auf einen Webserver bei Gibraltar authentifizieren. Die Autorisierung der Benutzer erfolgt mit der integrierten Benutzerverwaltung.
- **Content-Filter:** Gefährliche Inhalte und Viren können aus dem Netzwerkverkehr entfernt werden.
- **Webinhalts-Filter:** Webseiten können je nach Kategorie und Inhalt selektiv gesperrt werden.

© 2008 by eSYS Informationssysteme GmbH

8.11.1.1 Allgemeine Einstellungen

Definieren Sie folgende Einstellungen für den HTTP-Proxy:

- **Port:** Port, an dem der http Proxy Anfragen entgegennimmt. Sollten Sie kein transparentes Proxying aktiviert haben, müssen Sie diesen Port und die IP-Adresse von Gibraltar in den Browsereinstellungen bei den Clients einstellen.
- **Transparentes Proxying:** Wählen Sie jene Interfaces, über die der Proxy transparent anzusprechen ist. Dadurch werden alle Webanfragen automatisch an den Proxy-Server umgeleitet. Ein Konfiguration der Browser ist nicht notwendig. Durch die Aktivierung des transparenten Proxyings wird automatisch eine entsprechende NAT-Regel erzeugt, die sämtliche Anfragen auf Port 80 automatisch auf den von Ihnen gewählten Port für den HTTP-Proxy umleitet.
- **Rechnernamen für Zugriffslogging verwenden:** Aktivieren Sie diese Option, wenn wollen, dass Gibraltar anstatt der IP-Adresse den Hostnamen der auf den Proxy-Server zugreifenden Rechner in den Log-Dateien protokolliert.
- **Übergeordneten Cache verwenden:** IP Adresse und Port eines übergeordneten Proxy Caches.



8.11.1.2 Proxy Cache

Falls Sie Gibraltar als Caching Proxy verwenden wollen definieren Sie folgende Einstellungen:

- **Hauptspeicher für Proxy (in MB):** Größe des Caches im Hauptspeicher.
- **Maximale Größe eins Objekts:** Maximale Größe von Dateien, welche im Cache abgelegt werden. Überschreitet eine Datei diese Größe, wird diese nicht zwischengespeichert.
- **Cache auf Festplatte verwenden:** Legt die Größe eines zusätzlichen Festplatten-Caches fest. Diese Funktion setzt voraus, dass Sie eine Festplatte in Gibraltar eingebunden und aktiviert haben.

© 2008 by eSYS Informationssysteme GmbH

8.11.1.3 Authentifizierung

Aktiviert die Authentifizierungsfunktion für den HTTP-Proxy. Alle Benutzer müssen sich vor Zugriff auf das Web bei Gibraltar authentifizieren. Zur Konfiguration der Benutzer verwenden Sie die in Gibraltar integrierte Benutzerverwaltung.

8.11.1.4 Content Filter

Der Proxy Server von Gibraltar ist in der Lage, Webinhalte auf gefährliche Objekte und Viren zu prüfen. Aktivieren Sie sämtliche Inhalte, die Sie aus dem Webtraffic herausfiltern wollen:

- **Kaspersky Antivirus:** Aktiviert den optionalen Virenscanner von Kaspersky. Diese Funktion setzt eine gültige Virenscannerlizenz für Gibraltar voraus.
- **Cookie Filter:** Löscht alle Cookies aus dem Webtraffic
- **ActiveX Filter:** Löscht alle ActiveX Inhalte aus dem Webtraffic
- **JavaScript:** Löscht den gesamten JavaScript-Code aus dem Webtraffic
- **Flash Filter:** Löscht alle Flash-Filter aus dem Webtraffic

ACHTUNG: Das Filtern dieser Inhalte kann die Funkionalität von Webseiten massiv beeinträchtigen. Nutzen Sie zu diesem Zweck die Möglichkeit, Ausnahmen zu definieren.

8.11.1.5 Ausnahmen

Um einzelne URLs vom Content-Filter auszunehmen bzw. gezielt zu sperren steht Ihnen die Möglichkeit zur Verfügung, Ausnahmen zum Content Filter zu definieren.

- **Ausnahmen:** Definieren Sie URLs, welche vom Content-Filter ignoriert werden
- **Gesperrte URLs, Domains und reguläre Ausdrücke:** Definieren Sie URLs, Domains oder reguläre Ausdrücke, die vom Content-Filter gesperrt werden. Sie können diese Werte in folgender Form eingeben:
  Vollständige URL: eine komplette Internet-Adresse in der Form www.mydomain.com
  Domain oder Subdomain: eine Subdomain in der form .mydomain.com (führender Punkt bedeutet, es werden alle Subdomains von mydomain.com gesperrt)
  Einzelnes Wort: Geben Sie ein einzelnes Wort ein, so werden alle URLs gesperrt, die dieses Wort enhalten. Beachten Sie dabei Groß- und Kleinschreibung.

8.11.1.6 PureSight Content Scanner

Beim PureSight Content Scanner handelt es sich um einen HTTP Content Scanner, mit dem sich auf einfache Weise verschiedene Inhaltskategorien, wie z.B. Erotik- oder Glücksspielseiten, für die Benutzer sperren lassen.

Um den PureSight Content Scanner benutzen zu können, benötigen Sie eine separate Lizenz, welche bei allen Gibraltar Partnern und Resellern sowie beim Hersteller erworben werden kann. Selbstverständlich besteht die Möglichkeit, diese Funktion für 30 Tage kostenlos zu testen. Senden Sie in diesem Fall eine formlose Anfrage an office@gibraltar.at.

© 2008 by eSYS Informationssysteme GmbH

Vom PureSight Content Scanner sind zwei verschiedene Varianten verfügbar:

- **Basis Variante:** Bei dieser Variante können nur bestimmte Kategorien geblockt werden. Die Konfiguration erfolgt über das Webinterface der Gibraltar Firewall und es gibt keine Auswertungen.
- **Enterprise Variante:** Bei dieser Variante wird die Konfiguration durch ein separates webbasiertes Konfigurationstool erledigt. Neben einer detaillierteren Konfiguration der Kategorien (z.B. das Blockieren bestimmter Kategorien zu bestimmten Zeiten) sind auch ausführliche Reports möglich.

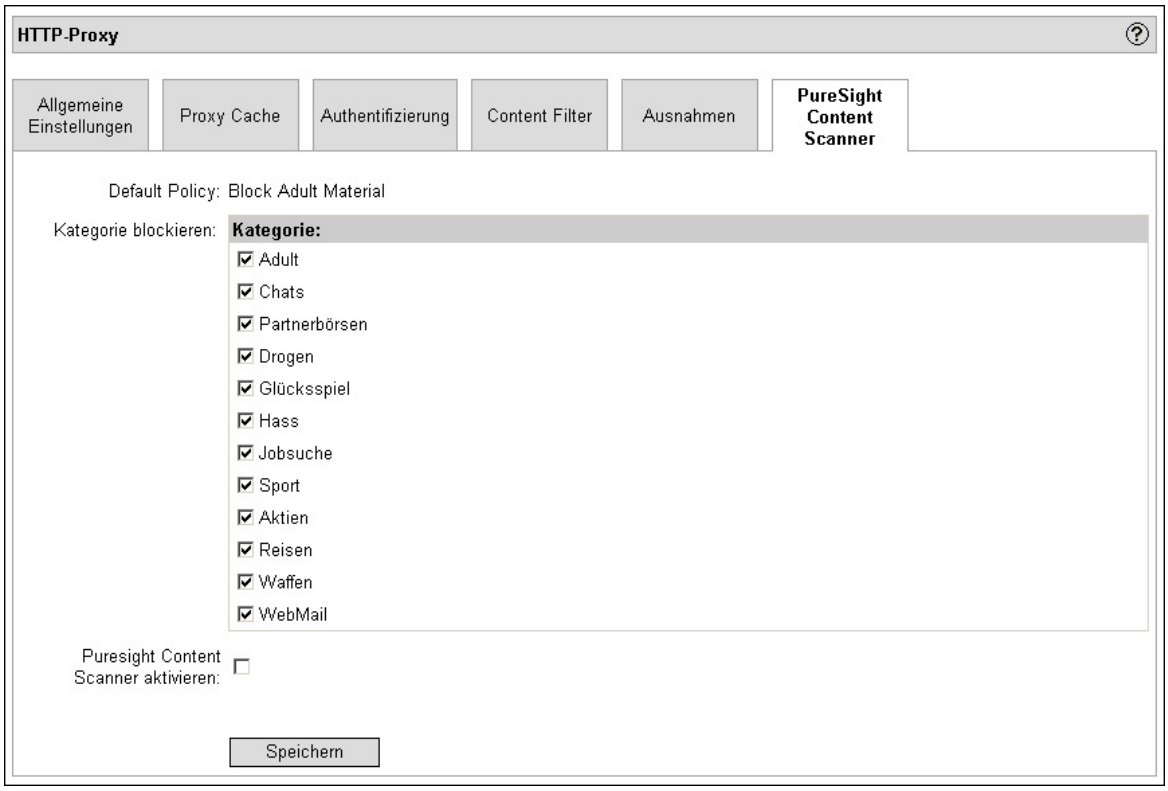
Wie erhalten Sie eine gültige Puresight Lizenz und starten den Puresight Content Scanner.

- Klicken Sie in der Menüleiste auf "Lizenz uploaden"
- Kopieren Sie die "PureSight Network ID" in die Zwischenablage und senden Sie diese in einem Mail an office@gibraltar.at. Bitte geben Sie auch die interne IP Ihrer Gibraltar-Firewall und die gewünschte Version (Basis oder Enterprise) bekannt.
- Sie erhalten von uns eine Lizenzdatei, die Sie auf Ihre Gibraltar Firewall uploaden.
- Sofern Sie die **Basisvariante** lizensiert haben, können Sie in der Registerkarte **Puresight Content Scanner** die zu blockenden Kategorien auswählen.
- Bei der **Enterprise Variante** können Sie im Modul **Dienste** den Puresight Dienst starten und unter der URL: http://ipIhrerFirewall:5000 die **Enterprise Variante** konfigurieren.Vergessen Sie dabei nicht, eine Firewallregel zu erstellen, die von Ihrem internem Interface auf LOCAL Pakete auf dem TCP Port 5000 akzeptiert.

Enterprise Variante
Die Enterprise Variante ist wie bereits erwähnt über ein eigenes Interface erreichbar (Popupblocker für diese IP deaktivieren!), wobei das Standardpasswort leer ist. Beim Ändern des Passwortes müssen Sie darauf achten, dass ein leeres altes Passwort nicht akzeptiert wird. Geben Sie hier ein Leerzeichen ein. Sämtliche Konfigurationsmöglichkeiten sind in der Onlinehilfe des Puresight-Interfaces ausführlich beschrieben!

WICHTIG: Sollte sich Ihre interne IP-Adresse ändern, so geben Sie diese bitte bei office@gibraltar.at bekannt, damit wir Ihnen eine neu kodierte Lizenz zusenden können.

© 2008 by eSYS Informationssysteme GmbH



8.11.2 POP3-Proxy

Der **POP3-Proxy** ermöglicht es, Emails zu überprüfen, die von einem externen POP3 Postfach abgerufen werden. Dabei kann man verschiedene Überprüfungen (Spam, Virus) durchführen. Weiters wird die interne Netzwerkstruktur vor der Außenwelt verborgen. Wird ein Virus in einer Mail gefunden, so wird die Mail gelöscht und nicht an den Empfänger weitergeleitet. Wird eine Mail als Spam klassifiziert, so können Sie Gibraltar so konfigurieren, dass im Betreff ein Text (z.B. "*****SPAM*****") und im Mailtext eine Information eingefügt wird, warum diese Mail als Spam klassifiziert wurde. Im Client-Mailprogramm können Sie anschließend einen Filter erstellen, der die Spam Mails automatisch in ein eigenes Unterverzeichnis kopiert, damit Sie die Mails noch einmal durchsehen oder löschen können. Die Originalmail bekommen Sie als Anhang an diese Informationsmail.

8.11.2.1 Allgemeine Einstellungen

Definieren Sie zur Konfiguration des POP3-Proxy folgende Einstellungen:

- **Port:** Der Port, an dem der POP3-Proxy Anfragen entgegennimmt
- **Transparentes Proxying erlauben:** Jene Netzwerkschnittstellen, an denen die POP3 Anfragen transparent an den POP3-Proxy weitergeleitet werden. Die Funktionalität läuft analog dem HTTP-Proxy. Bei Aktivierung wird automatisch eine entsprechende NAT-Regel erzeugt, die die Anfragen der Clients auf Port 110 automatisch auf den von Ihnen angegebenen Port umleitet. Weiters wird auch die entsprechende Firewallregel automatisch generiert.
- **RBL-Überprüfung auslassen:** Deaktiviert die Überprüfung der Blacklisten (RBL). Diese Option verbessert die Performance, verschlechtert jedoch die Erkennungsrate von Spam-Mails.
- **Kaspersky Virenscanner aktivieren:** Aktiviert die Virenüberprüfung von POP3-Mails

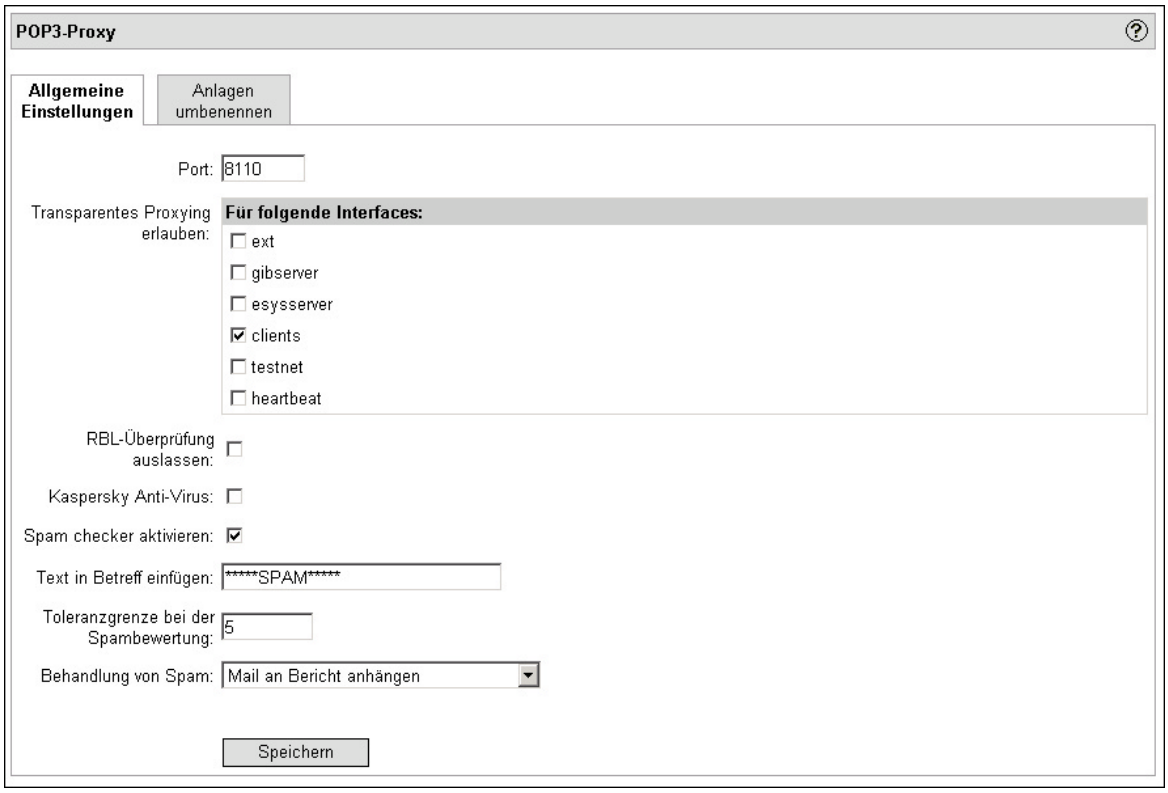
© 2008 by eSYS Informationssysteme GmbH

- **Spam Checker aktivieren:** Aktiviert die Spamüberprüfung von POP3-Mails
- **Text in Betreff einfügen:** Jener Text, der dem Mailbetreff vorangestellt wird, falls ein E-Mail als Spam klassifiziert wird.
- **Toleranzgrenze bei der Spambewertung:** Die Punktezahl, ab wann eine Klassifizierung als Spam vorliegt. Je niedriger, desto strenger arbeitet der Spamfilter. Ein realistischer Wert liegt bei 5 Punkten.
- **Behandlung von Spam:** Jene Aktion, die ausgeführt wird, falls ein E-Mail als Spam klassifiziert wird. Es stehen folgende Möglichkeiten zur Verfügung:

  Nur den Betreff verändern: Fügt dem Mailbetreff den von Ihnen angegebenen Text hinzu.

  Mail an Bericht anhängen: Sendet dem Empfänger der Mail einen Bericht mit der Spam-Bewertung und einer detaillierten Begründung warum das E-Mail als Spam eingestuft wurde. Das Originalmail wird als Anhang beigefügt.

  Mail nur als Text an Bericht anhängen: Sendet dem Empfänger der Mail einen Bericht mit der Spam-Bewertung und eine detaillierte Begründung warum das E-Mail als Spam eingestuft wurde. Das Originalmail wird als Anhang im Format "nur Text" beigefügt. Es werden also nur ASCII-Zeichen dargestellt und somit alle gefährlichen Inhalte, Attachments und Links entfernt.



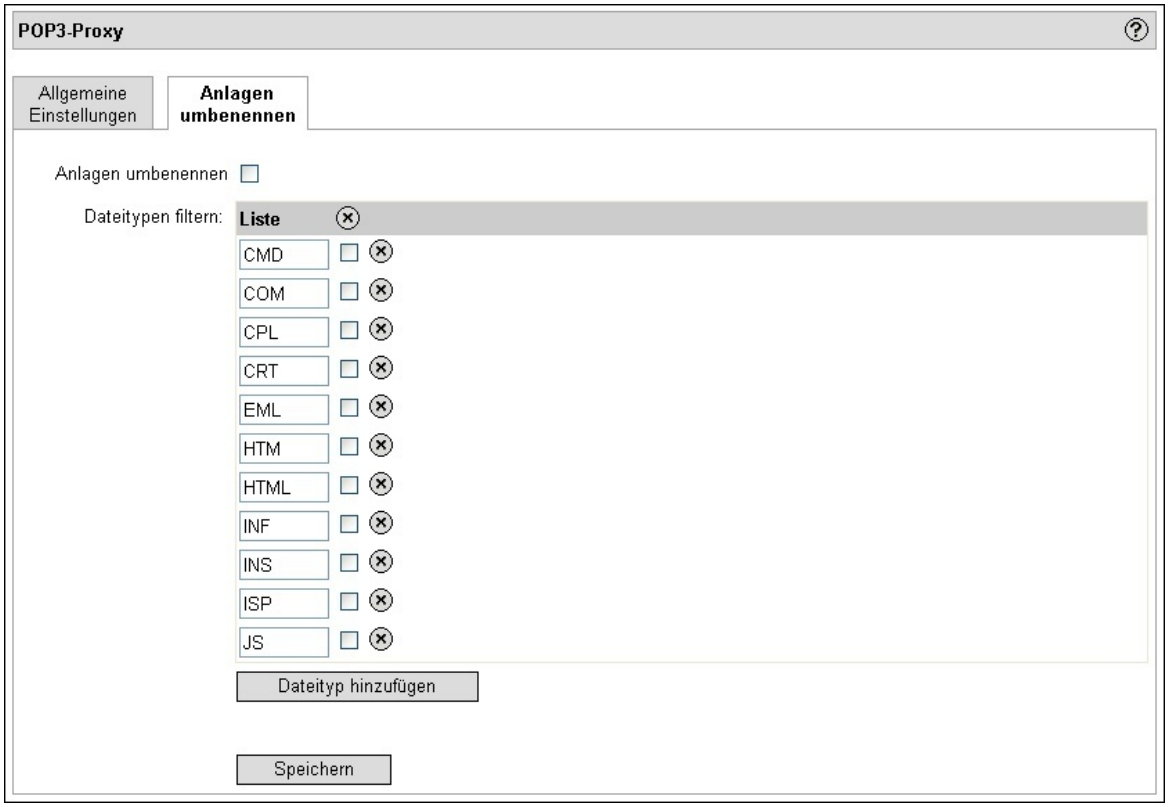
8.11.2.2 Anlagen umbenennen

Gefährliche Dateianhänge können vom POP3-Proxy umbenannt oder gefiltert werden. Erweitern Sie die Liste der Dateianhänge beliebig.

- **Anlagen umbenennen:** Aktiviert das Umbenennen der unten angeführten Dateiendungen. Sämtliche Anhänge mit den entsprechenden Dateiendungen erhalten die Endung **.BAD**

© 2008 by eSYS Informationssysteme GmbH

- **Dateitypen filtern:** Definieren Sie eine Liste mit gefährlichen Dateiendungen die gefiltert werden sollen.



8.11.3 FTP-Proxy

Gibraltar beinhaltet einen FTP-Proxy Server, der sowohl für eingehenden wie auch ausgehenden FTP-Traffic konfiguriert werden kann.

8.11.3.1 Ausgehend

Definition eines Proxy-Servers für ausgehende FTP Anfragen:

- **Port:** Port, an dem der FTP-Proxy anfragen entgegennimmt.
- **Transparentes Proxying erlauben:** Aktiviert jene Netzwerkschnittstellen, an denen der FTP-Proxy Anfragen transparent an den FTP-Proxy umleitet. Die Konfiguration erfolgt analog dem http-Proxy. Bei Aktivierung wird automatisch eine entsprechende NAT-Regel erzeugt, die die Anfragen der Clients auf Port 21 automatisch auf den von Ihnen angegebenen Port umleitet. Weiters wird die entsprechende Firewallregel automatisch generiert.
- **Kaspersky Antivirus:** Aktiviert die Virenüberprüfung für ausgehenden FTP-Traffic. Sie benötigen dafür eine gültige Virenscannerlizenz für Gibraltar.
- **Cache auf Festplatte verwenden:** Aktiviert die Festplatte für die Zwischenspeicherung des FTP-Traffics.

ACHTUNG: Bei der Verwendung des Microsoft Internet Explorers als FTP-Client können Timeout-Probleme bei größeren Dateien auftreten!

© 2008 by eSYS Informationssysteme GmbH

8.11.3.2 Eingehend

Falls sie einen FTP-Server betreiben wollen, sollten Sie diesen nicht direkt aus dem Internet zugänglich machen. Aus sicherheitstechnischen Gründen empfiehlt es sich, den FTP-Traffic über einen FTP-Proxy abzuwickeln. Der Proxy-Server nimmt eingehende FTP-Anfragen entgegen greift seinerseits auf den internen FTP-Server zu. Der interne FTP-Server ist nicht direkt für den Benutzer zugänglich.

TIPP: Vergessen Sie nicht, eine Paketfilterregl für den Port 21 vom externen Interface auf LOCAL auf ACCEPT zu setzen. Dadurch wird der Zugriff auf den Proxy-Server erlaubt.

Definition eines Proxy-Servers für eingehende FTP-Anfragen:

- **Ziel FTP Server:** IP-Adresse oder URL ihres internen FTP-Servers
- **Ziel FTP Port:** Port ihres internen FTP-Servers

8.11.4 Anonymisierung

Dieses Modul bietet einige Programme an, die dem Benutzer ermöglichen, anonym im Internet zu agieren. Dabei werden zum Beispiel Anfragen des Benutzers über verschiedene Server umgeleitet und erst dann an das entsprechende Ziel zugestellt. Dadurch ist es möglich, Internet-Traffic vor Dritten zu verbergen. Bei den von Gibraltar angebotenen Anonymisierungsfunktionen handelt es sich teilweise noch um Projekte im Betastadium. Detaillierte Infos zu den angebotenen Funktionen erhalten Sie direkt bei den Projektbetreibern.

8.11.4.1 Anon Anonymisierer

Das Modul Anon-Proxy leitet die Anfrage an den Port 80 (HTTP) über eine Verschlüsselungskaskade weiter, die von speziellen Anonymisierungsservern angeboten wird. Die Anfrage des Benutzers wird an den hier definierten Ausgangsserver weitergeleitet, der seinerseits die Anfragen an weitere Anonymisierungsserver weitergibt, bis sie schließlich ihr Ziel erreichen und die Antwort zurückgeschickt wird.

Nähere Informationen zum Entwicklungsstand dieses Moduls und genauere Beschreibungen finden Sie unter JAP - TU Dresden.

- **Servers:** Erster Anonymisierungsserver, der als Ausgangspunkt für die Verschlüsselungskaskade dienen soll. Die einzelnen Server bieten unterschiedliche Performance, die auch innerhalb eines Tages stark schwanken kann.
- **Anon-Proxy IP-Adresse:** IP-Adresse, an der der Anon-Proxy auf Anfragen reagieren soll
- **Port:** Port an dem der Anon-Proxy auf Anfragen reagieren soll
- **Kombiniert mit HTTP-Proxy:** Aktiviert die Verbindung von Anon-Proxy mit dem http-Proxy von Gibraltar. Der HTTP-Proxy leitet in diesem Fall sämtliche Anfragen an den Anon-Proxy weiter, der diese wiederum ins Internet weitergibt.

© 2008 by eSYS Informationssysteme GmbH

8.11.4.2 Tor Anonymisierer

Tor arbeitet ähnlich wie Anon-Proxy mit Verschlüsselungskaskaden, kann jedoch auch andere Services bedienen, nicht nur HTTP. Wenn Sie keinen Tor-Verzeichnisserver angeben, werden die Standard-Verzeichnisserver verwendet.

Nähere Informationen zum Entwicklungsstand dieses Moduls und genauere Beschreibungen finden Sie unter Tor.

- **Port:** Portnummer, an dem der Tor-Server Anfragen entgegennehmen soll
- **Tor-Verzeichnisserver:** Jene Verzeichnisserver, die Sie verwenden wollen:
  Server IP-Adresse: IP-Adresse des Verzeichnisservers
  Port: Portnummer des Verzeichnisservers
  Fingerprint: Fingerprint des Verzeichnisservers

8.11.4.3 Freenet

Freenet bietet die Möglichkeit, Informationen im Internet zur Verfügung zu stellen, ohne dass man auf deren Ursprung schließen kann. Es wird also ermöglicht, Daten in das Freenet zu stellen, deren Herkunft man nicht nachvollziehen kann. Alle Freenet-Server halten den Datenbestand gemeinsam und bieten ihn anderen Freenet-Servern und -Benutzern zum Download an. Sie können Freenet auf Ihrer Gibraltar aktivieren, um an diesem gemeinsam Informationspool teilzunehmen.

ACHTUNG: Freenet benötigt sehr viel Speicher. Sie können es nur mit mehr als 256 MB RAM verwenden. Außerdem sollten Sie einige GB Speicherplatz auf der Festplatte reservieren, damit ein Arbeiten mit Freenet gut möglich ist.

Wenn Sie mehr über Freenet wissen möchten, besuchen Sie The Free Network Project.

- **Server Port:** Portnummer, über die der Freenet Server von anderen Servern erreicht werden kann.
- **Client Port:** Portnummer, über die Ihr Freenet Server von Freenet Clients erreicht werden kann.
- **Zugriff erlauben von:** Jene IP-Adressen oder Netzwerkadressen von Freenet Clients, die Zugriff auf Ihren Freenet Server erhalten sollen.
- **Automatisch bekannt machen:** Aktivieren Sie diese Option, damit sich Freenet selbst bei den eingetragenen Freenet-Knotenservern bekannt macht.
- **Speicherplatz (in MB; mind. 256):** Größe des Festplattenspeichers der für Freenet zur Verfügung gestellt wird.
- **Bandbreitenbeschränkung eingehend:** Maximale Bandbreite für eingehende Verbindungen.
- **Bandbreitenbeschränkung ausgehend:** Maximale Bandbreite für ausgehende Verbindungen.
- **Maximale Anzahl der Verbindungen:** Maximale Anzahl gleichzeitiger Verbindungen mit dem Freenet-Server.
- **Mainport:** Freenet stellt auch eine eigene Weboberfläche als Einstiegspunkt zur Verfügung. Geben Sie hier den Port an, über den diese Weboberfläche erreicht werden kann.
- **Weboberfläche erlaubt von:** Jene IP-Adressen oder Netzwerkadressen, die Zugriff

© 2008 by eSYS Informationssysteme GmbH

auf die Weboberfläche Ihres Freenet Servers erhalten sollen.

8.12 Snort IDS

Das Intrusion Detection System (IDS; "Sicherheitsvorfallserkennung") Snort kann hier konfiguriert werden.

Ein IDS erkennt Attacken und Einbrüche in das System. Snort ist ein Open Source Paket und das gebräuchlichste IDS.

Wird eine Attacke erkannt, werden Einträge im Log erzeugt oder Emails versandt. Es gibt Tausende Regeln für Snort, die - ähnlich den Viren Scanner Signaturen - regelmäßig upgedated werden müssen.

8.12.1 Allgemein

Hier werden die Basiseinstellungen vorgenommen.

- **Abzuhörendes Interface:** Wählen Sie das Interface, an dem Snort lauschen soll.
- **Netzwerkadresse der eigenen Netze:** Fügen Sie die IP-Netzwerkbereiche an, die hinter der Firewall im privaten Netz liegen.
- **DNS/HTTP/SMTP Server:** Fügen Sie die IP Adressen der einzelnen Server ein.

8.12.2 Output Modules

Das IDS soll die Vorkommnisse dokumentieren bzw. den Administrator darüber in Kenntnis setzen. Es gibt drei verschiedene Möglichkeiten dafür:

- **Syslog Ausgabemodul verwenden:** Es werden Einträge im Syslog erzeugt.
- **Gibraltar Firewall Alarm- und Ausgabelösung verwenden:** Meldungen werden an die angegebenen Email-Adressen verschickt. Sie können festlegen, ab welcher Priorität der Meldung Emails verschickt werden sollen.
- **Datenbank Ausgabemodul verwenden:** Die Meldungen werden an einen externen Datenbankserver (MySQL oder PostgreSQL) geschickt. Leider unterstützt Snort keine verschlüsselten Verbindungen zu den Datenbank Servern, weshalb Sie auf IPSec Tunnel zurückgreifen sollten. Unter /usr/share/doc/snort-mysql oder /usr/share/doc/snort_pgsql finden Sie Scripte zum Erzeugen der benötigten Tabellen in der Datenbank. Ein großartiges Tool für Auswertungen ist BASE.

8.12.3 Regelupdate

Snort Regeln sind ähnlich wie Virus Scanner Signaturen. Sie müssen auch regelmäßig adaptiert werden. Es gibt nun 2 Wege, wie man regelmäßig Updates bekommen kann:

- **VRT Regeln:** Wir empfehlen die Regeln vom Vulnerability Research Team. Diese

© 2008 by eSYS Informationssysteme GmbH

Regeln werden direkt von Sourcefire betreut und sind ausführlich getestet. Sie müssen sich einen Account bei snort.org besorgen,damit Sie einen Oink-Code bekommen. Hier gibt es wiederum zwei Möglichkeiten: eine freie Variante und eine kommerzielle ($1800/Jahr). Bei der kommerziellen Variante bekommen Sie die neuen Regeln fünf Tage früher als bei der freien.

- **Community Regeln:** Community Regeln sind - wie der Name schon sagt - von der Snort Community gewartet. Diese Regeln werden regelmäßig veröffentlicht, sind jedoch nicht ganz so ausführlich getestet. Die bessere Variante sind die VRT Regeln.

VORSICHT: Damit Sie die VRT Regeln benutzen können, müssen Sie sich bei snort.org registrieren und einen Oink-Code herunterladen.

8.12.4 Snort Regeln

Hier können Sie bestimmte Regeltypen aktivieren oder deaktivieren. Es macht nur Sinn, Regeln für spezielle Dienste zu aktivieren (z.B. mySQL), wenn Sie einen entsprechenden Server im Einsatz haben.

ACHTUNG: Jede Regel kann noch detaillierter konfiguriert werden, wenn Sie den Button rechts neben der Regel benutzen.

TIPP: Verwenden Sie die Standardeinstellungen!

8.13 Traffic Shaping

Unter Traffic Shaping oder QoS (Quality of Service) versteht man Verfahren, mit denen es möglich ist, den Datenverkehr hinsichtlich Bandbreite und Priorisierung zu steuern. Damit ist es z.B. möglich, unternehmenskritischen Echtzeitservices wie Voice over IP oder Terminalserverprotokollen eine notwendige Mindestbandbreite zur Verfügung zu stellen. Nichtkritische Services wie Mail können in Ihrer Priorität zurückgestuft werden.

Möglichkeiten von Traffic Shaping:

- **Priorisierung einzelner Services**
- **Gewährleistung einer Mindestbandbreite für einzelne Services**
- **Aufteilung einer verfügbaren Bandbreite auf mehrere Hosts**
- **Priorisierung verschiedener Netze**

Mit der Gibraltar Version 2.5 ist es nun auch möglich den eingehenden Verkehr zu kontrollieren. Dafür gibt es für jedes Netzwerkinterface eine Auswahlmöglichkeit für "incoming" (eingehende) und "outgoing" (ausgehenden) Traffic. Um ein optimales Bandbreitenmanagement zu gewährleisten ist es nicht möglich, mehr wie 95 % der verfügbaren Bandbreite eines Interfaces als Minimum zur Verfügung zu stellen! Nähere Details zur Implementierung von Traffic Shaping in der Praxis finden sie in den Anwendungsbeispielen.

© 2008 by eSYS Informationssysteme GmbH

8.13.1 Allgemeine Einstellungen

Um Traffic Shaping konfigurieren zu können ist es erforderlich für alle verwendeten Netzwerkschnittstellen die zur Verfügung stehende Minimalbandbreiten für Up- und Download zu definieren. Die Bandbreite wird in kbit/s definiert und kann entweder aus einem der definierten Werte ausgewählt oder manuell eingegeben werden (CUSTOM).

8.13.2 Interface Gruppen

Sie können mehrere Netzwerkschnittstellen für das Traffic Shaping zu einer Shapinggruppe zusammenfassen.

- **Interface Gruppen:** Definieren Sie einen Namen für die Gruppe und fügen Sie die entsprechenden Netzwerkschnittstellen der Shapinggruppe hinzu. Sie können die definierte Gruppe anschließen in den Shaping Regeln verwenden.

8.13.3 Klassifizierung

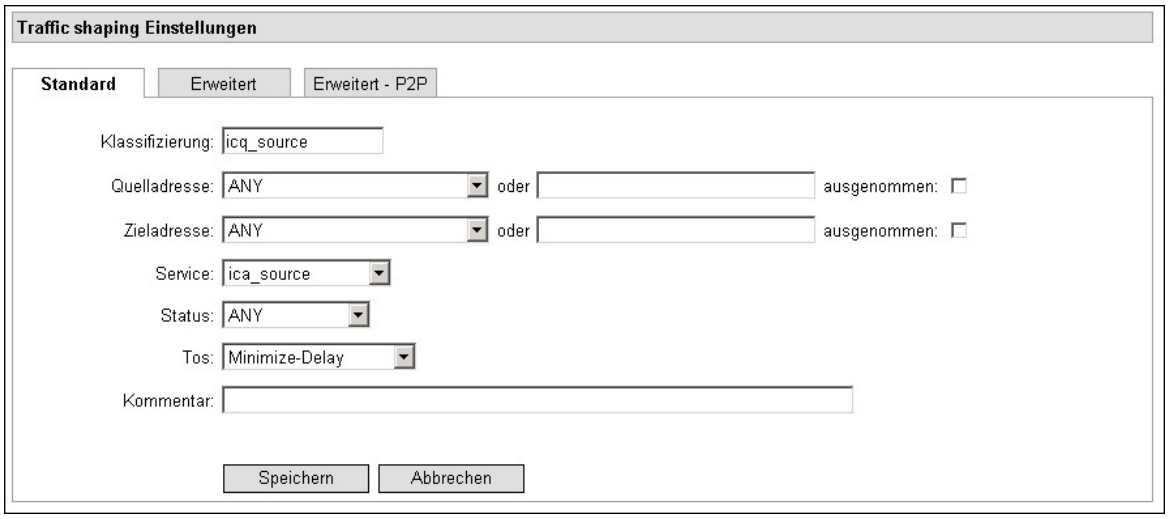
Klassifizierungen werden verwenden, um zu priorisierenden Traffic zu kennzeichnen. Der Editor bietet Ihnen alle Möglichkeiten des Firewallregel-Editors, um Pakete je nach Anforderung zu markieren. Achten Sie darauf, dass die speziellsten Klassifizierungen in der Hierarchie ganz oben stehen. Eine Klassifizierung für eine IP-Telefonanlage mit der Source-IP 192.168.1.1 muss bspw. vor der Klassifizierung des restlichen Traffics stehen (Source: ANY, Destination: ANY, Service: ANY). Gibraltar markiert anhand dieser Reihenfolge die Pakete und ordnet Sie dann den definierten Shaping Regeln zu.

In der Registerkarte **Standard** finden Sie neben den bekannten Feldern aus dem Firewallmodul zusätzlich folgende Einstellungen:

- **Name:** Selbst zu wählender Name für die Klassifizierung
- **TOS Bits:** Verwenden Sie diese Einstellung, um VOIP Traffic zu markieren. Viele Provider bzw. Router reagieren mittlerweile auf diese Bits, um VOIP Traffic zu priorisieren.

Die anderen beiden Registerkarten bieten dieselbe Funktionalität wie das Firewallmodul.

© 2008 by eSYS Informationssysteme GmbH



8.13.4 Klassifizierungsgruppen

Sie können mehrere Klassifizierungen in eine Gruppe zusammenfassen und diese später in den Shaping Regeln verwenden. Es empfiehlt sich bei jeder Art von Priorisierung eine Klassifizierung "icmp" für das ICMP-Protokoll anzulegen und diese gemeinsam mit den anderen zu priorisierenden Services in eine Gruppe zu geben. Beim Troubleshooting kann man im Normalfall dann immer davon ausgehen, dass bei niedrigen ICMP Antwortzeiten unter Vollast ein funktionierendes Bandbreitenmanagement gegeben ist.

- **Klassifizierungsgruppen:** Definieren Sie einen Namen für die Gruppe und fügen Sie die entsprechenden Klasffizierungen hinzu. Sie können die definierte Gruppe anschließen in den Shaping Regeln verwenden.

8.13.5 Traffic Shaping Regeln

Bei den Traffic Shaping Regeln handelt es sich um die eigentlichen Einstellungen zur Beschränkung der Bandbreite. Es ist möglich, für einzelne Rechner, Netze und Ranges für bestimmte Services Mindest- und Maximalbandbreiten zur Verfügung zu stellen. Nähere Details zur Implementierung von Traffic Shaping in der Praxis finden sie in den Anwendungsbeispielen. Vor dem Anlegen der Shaping-Regeln müssen die jeweiligen Klassifizierungen angelegt werden.

In der Übersicht werden sämtliche Traffic Shaping Regeln dargestellt. Sie finden hier folgende Informationen:

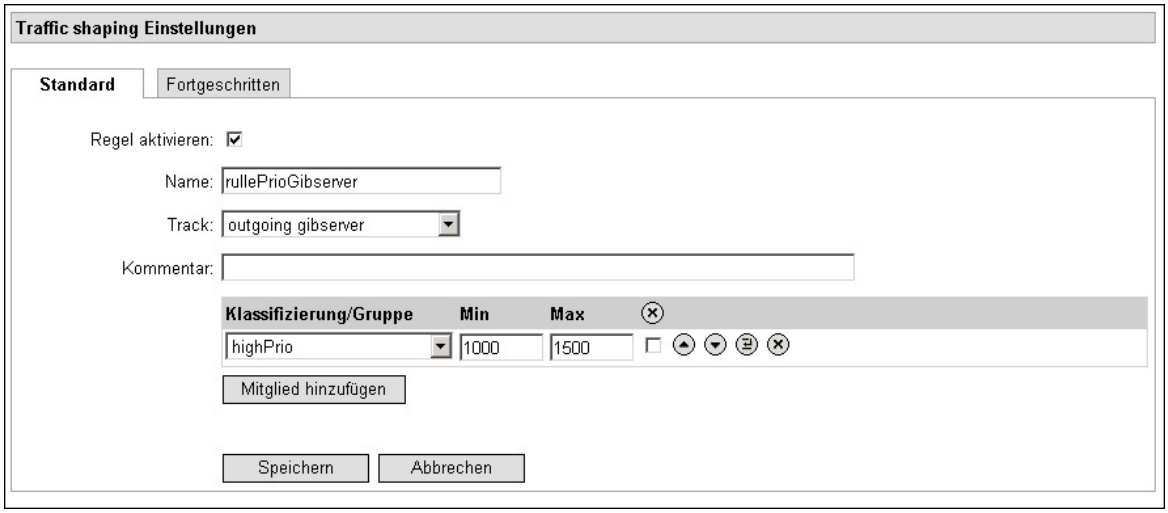
- **Track:** Zeigt die Richtung und das Interface der Shaping Regel an (Bspw: incoming ext -> Download).
- **Bb. (kbit):** Gesamtbandbreite die in den allgemeinen Einstellungen für das entsprechende Interface festgelegt wurde
- **Bb. garantiert (kbit):** Die durch Shaping Regeln bereits vergebene Bandbreite
- **Aktiv:** Aktiviert bzw. deaktiviert die entsprechende Shaping Regel
- **Name:** Frei definierter Name der Regel
- **Klassifizierung/Gruppe:** Verwendete Klassifizierungen bzw. Klassifizierungsgruppen in dieser Regel.
- **Min**: Minimalbandbreite für die Klassifizierung/Gruppe.
- **Max:** Maximalbandbreite für die Klassifizierung/Gruppe.

© 2008 by eSYS Informationssysteme GmbH

8.13.6 Traffic Shaping Regeln - Detail

Beim Erstellen einer Traffic Shaping Regel können in der Registerkarte **Standard** die folgenden Einstellungen vorgenommen werden:

- **Regel aktivieren:** Aktiviert die entsprechende Regel
- **Name:** Frei definierbarer Name der Regel
- **Track:** Netzwerkinterface und Richtung des zu priorisierenden Traffics.
- **Kommentar:** Ein möglichst sprechender Kommentar.
- **Klassifizierung/Gruppe:** Wählen Sie hier die von Ihnen gewünschten Klassifizierungen bzw. Gruppen aus und vergeben Sie Minimal und Maximalwerte.



Die Registerkarte **Fortgeschritten** bietet Ihnen erweiterte Funktionalitäten, die beispielhaft in den Anwendungsbeispielen vorgeführt werden.

- **Quelladresse:** Wählen Sie hier eine Quelladresse oder geben Sie einen eigenen Wert ("CUSTOM") ein, damit diese Regel nur für bestimmte Quelladressen in Ihrem Netz gültig ist.
- **Regel für jede IP-Adresse in der Quelladresse erzeugen:** Falls Sie in der Quelladresse einen IP-Adressbereich, einen Netzalias oder eine Netzgruppe angegeben haben, wird für jede im Bereich enthaltene IP-Adresse eine Regel erzeugt. Sie benötigen diese Einstellung, um für verschiedene Hosts gleich verteilten Uploadtraffic zur Verfügung zu stellen.
- **Zieladresse:** Wählen Sie hier eine Zieladresse oder geben Sie einen eigenen Wert ("CUSTOM") ein, damit diese Regel nur für bestimmte Zieladressen in Ihrem Netz gültig ist.
- **Regel für jede IP-Adresse in der Zieladresse erzeugen:** Falls Sie in der Zieladresse einen IP-Adressbereich, einen Netzalias oder eine Netzgruppe angegeben haben, wird für jede im Bereich enthaltene IP-Adresse eine Regel erzeugt.
- **Maximum Bandbreite (kbit) je IP Adresse:** Verwenden Sie diese Einstellung, wenn Sie "Regel für jede IP-Adresse in der Quelladresse erzeugen" oder "Regel für jede IP-Adresse in der Zieladresse erzeugen" gewählt haben. Gibraltar legt für jede IP

© 2008 by eSYS Informationssysteme GmbH

Adresse ein oberstes Limit mit diesem Wert an. Damit ist gewährleistet, dass sich verschiedene IPs untereinander den Traffic nicht wegnehmen. Innerhalb dieser Grenze gelten dann die von Ihnen definierten Min/Max Werte der Klassifizierungen/Gruppen.

- **Bandbreite (kbit) für Netze:** Verwenden Sie diese Einstellung (ANY=Bandbreite des Interfaces), wenn Sie als Serviceprovider bspw. in verschiedene Netze shapen. Eine detaillierte Anleitung bietet das Szenario Traffic Shaping Citrix.

8.13.7 Traffic Shaping Regeln - Aktive

Diese Registerkarte zeigt eine interfaceunabhängige Übersicht der Shaping Regeln mit Lösch-, Aktivier- und Deaktiviermöglichkeiten.

8.14 Captive Portal

Captive Portal ist ein HotSpot-Dienst, durch den es möglich ist, für Benutzer den Zugang auf Basis von Zeitdauer bzw. Datenmenge zu beschränken. Der Dienst kann, ein entsprechender Wireless Access Point vorausgesetzt, auch für WLAN eingesetzt werden. Die nicht authentifizierten Benutzer werden auf eine Loginmaske umgelenkt und nach dem Anmelden erhalten sie Zugang z.B. zum Internet.

Es muss im Menü nur das Interface ausgewählt werden, auf dem der Dienst laufen soll (z.B. int). Nach dem Starten von Captive Portal im Services-Menü werden auf diesem Interface über den in Captive Portal integrierten DHCP Server IP Adressen aus dem angegebenen IP Bereich (z.B. 192.168.200.0/24) vergeben.

WICHTIG: Der IP Bereich darf sich nicht mit dem IP-Bereich des konfigurierten Interfaces überschneiden! Vergeben Sie immer einen Bereich, der mit keinem anderen kollidiert!

Unter "Adressen, bei denen keine Authentifizierung notwendig ist" können verschiedenen Adresse angegeben werden, zu denen der Benutzer auch ohne Authentifizierung surfen darf.

Mit dieser IP werden die Benutzer anschließend auf die Loginmaske umgelenkt. Nach dem Anmelden hat der Benutzer Zugang zu den freigegebenen Netzen. Dieser Zugriff muss anschließend im Firewall-Modul noch entsprechend konfiguriert werden.

In der Registerkarte **Standardwerte** können Sie Limits für Ihre Captive Portal Benutzer definieren. Bei Fehlen von Standardwerten sind keine Einschränkungen gegeben.

WICHTIG: Sofern Sie die Active Directory integrierte Benutzerverwaltung verwenden, ist die Registerkarte **Standardwerte** nicht vorhanden.

8.15 Konfigurationen verwalten

Sie können die Konfigurationsdaten von Gibraltar bequem auf verschiedenen Speichermedien sichern oder archivieren. Da Gibraltar ein Read-Only System ist, ist es notwendig, die Konfiguration auf einem alternativen Speichermedium abzuspeichern. Zur Verfügung stehen:

- Festplatte

© 2008 by eSYS Informationssysteme GmbH

- USB-Speichermedium
- Diskette
- Festplatte
- Compact Flash

Zusätzlich ist es möglich, die gesamte Konfiguration in komprimierter Form via E-Mail zu verschicken bzw. downzuloaden. Die Konfigurationsdateien werden zur Speicherung in einer einzigen Datei abgelegt und auf das gewählte Speichermedium kopiert.

Diese Art der Konfigurationsverwaltung gestattet es Ihnen bei Problemen oder einem Ausfall der Firewallhardware jederzeit archivierte Versionen der Konfiguration zu laden.

8.15.1 Konfiguration - Allgemeine Einstellungen

Definieren sie die Standardeinstellungen für das Speichern der Konfiguration:

- **Standard Speicher Ziel:** Wählen Sie jenes Medium, auf dem die Konfiguration beim Herunterfahren oder beim Neustart automatisch gesichert wird. Das hier gewählte Medium wird auch verwendet, wenn Sie die Konfiguration mit dem Menüpunkt **Quick-Save** speichern.
  Option Quelle: Die Konfiguration wird auf jenes Medium gespeichert, von welchem sie beim Starten geladen wurde.
- **Speichern auf Diskette:** Jenes Diskettenlaufwerk (wenn vorhanden), auf dem Sie die Konfiguration ablegen wollen
- **Speichern via E-Mail:** E-Mail-Adresse an welche die Konfiguration versendet werden soll.
- **Autoformatierung von Floppy und HDD:** Formatiert das gewählte Medium automatisch, falls auf dem entsprechenden Medium noch kein Dateisystem existiert.
- **Beim Herunterfahren speichern:** Aktiviert die automatische Speicherung der Konfiguration beim Herunterfahren der Firewall

TIPP: Um eine gesicherte Konfiguration zu laden, die auf Diskette oder USB Stick abgelegt ist, geben Sie die Diskette in das Diskettenlaufwerk bzw. stecken Sie den USB Stick an und starten anschließend von der Gibraltar CD. Gibraltar holt sich automatisch diese Konfiguration vom Speichermedium.

8.15.2 Konfiguration speichern

Speichert die Konfiguration auf das gewählte Medium. Diese Einstellung ist unabhängig vom Standardspeichermedium.

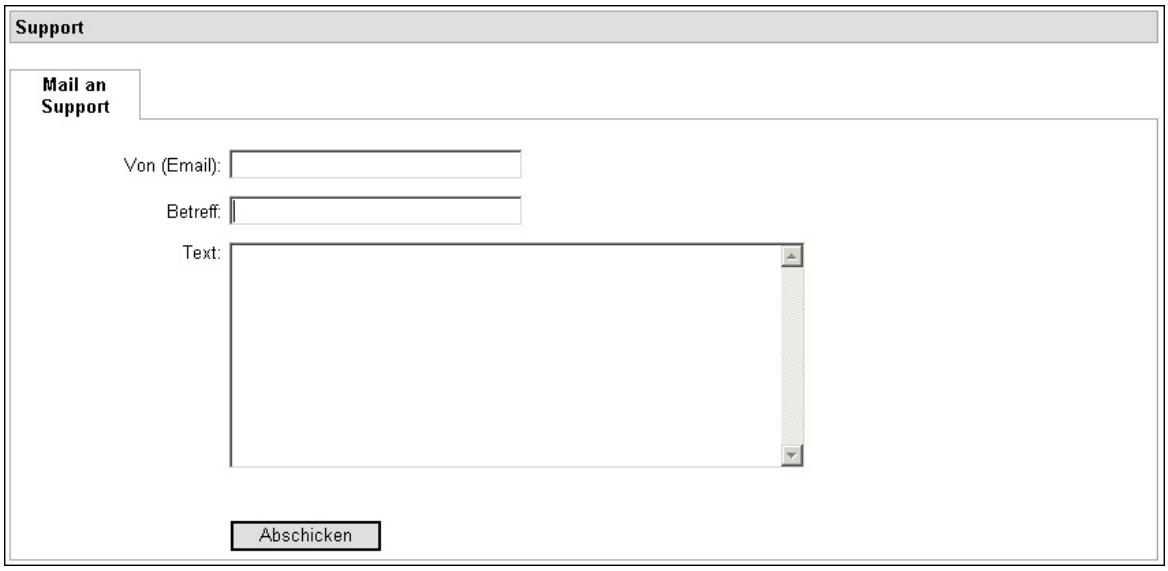
Zusätzlich können Sie die Systemkonfiguration downloaden oder per E-Mail verschicken. Löschen Sie die Konfiguration von der Festplatte oder vom Compact Flash, bootet Gibraltar in weiterer Folge mit einer Standardkonfiguration oder mit einer Konfiguration von einem externen Speichermedium.

© 2008 by eSYS Informationssysteme GmbH

9 Support

Mit dem integrierten Supportformular können Sie eine Supportnachricht direkt an den technischen Support von Gibraltar schicken. Bitte beschreiben Sie Ihr Problem so genau wie möglich. Diese Funktion steht nur zur Verfügung, wenn Sie eine funktionierende Internet-Verbindung haben.

Alternativ dazu können Sie natürlich jederzeit ein E-Mail an support@gibraltar.at senden.



10 Update

Die Update-Funktion informiert Sie über aktuelle Produktupdates und Security-Patches.

10.1 Versionsinfo

Zeigt die Version Ihrer Gibraltar Firewall und die neueste aktuell verfügbare Version.

10.2 Online update

Der Hersteller veröffentlicht im Bedarfsfall Patches und Updates, die von Gibraltar automatisch downgeloadet und installiert werden können (siehe System). So ist es möglich, rasch auf auftretende Sicherheitslücken oder Produktprobleme zu reagieren.

Alternativ zum automatischen Update können Sie verfügbare Patches manuell herunterladen und installieren.

Alle verfügbaren Patches werden in einer Liste angezeigt. Bereits installierte Patches sind mit einem grünen Häckchen markiert.

In der Übersicht stehen Ihnen folgende Möglichkeiten zur Verfügung:

- **Herunterladen:** Aktivieren Sie beim gewünschten Patch das Kontrollkästchen **Herunterladen**. Anschließend klicken Sie auf den Button **Herunterladen und**

© 2008 by eSYS Informationssysteme GmbH

Installieren.

- **Löschen:** Aktivieren Sie bei den gewünschten Patches das Kontrollkästchen **Löschen** . Anschließend klicken Sie auf den Button **Löschen**. Die gewählten Patches werden aus der Konfiguration gelöscht. Beim nächsten Neustart sind diese Patches nicht mehr im System vorhanden.

10.3 CF Image Upload

Falls Sie eine Gibraltar Security Appliance verwenden befindet sich das System auf dem in der Hardware integrierten CompactFlash Speicher. Der Update auf eine neue Version funktioniert denkbar einfach. Führen Sie der Reihe nach folgende Schritte aus:

1. Herunterladen der neuen Version von Gibraltar von der Gibraltar Website (Appliance Image). Sie finden die aktuelle Version von Gibraltar auf den aktuellen Mirror-Server. Eine Liste der zur Verfügung stehenden Mirror-Server finden sie hier.
2. Upload der Image Datei auf die Gibraltar Firewall
3. Neustart der Firewall

10.4 Remove updated files and Rollback

Nachdem Sie auf Ihrer Appliance ein Update der Gibraltar Version durchgeführt haben können Sie die alte Version endgültig von der Hardware löschen. Sollten Sie nach dem Update Probleme haben besteht bis zum endgültigen Löschen der alten Version die Möglichkeit einen Rollback durchzuführen.

11 Anhang

Literatur zum Thema Firewalls:

- Anonymous: Hackers Guide. Markt+Technik Verlag, München 2001
- Barth W.:: Das Firewall Buch. SuSE Press, Nürnberg 2001
- Fischer S., Walther U.: Linux Netzwerke. SuSE Press, Nürnberg 2000
- Siyan, K. und Hare, C.: Internet Firewalls and Network Security. New Riders Publishing, Indianapolis 1995
- Tannenbaum, A.: Computernetzwerke. Pearson Studium, München 2000
- Zwicky, E.D., Cooper S., Chapman D.B.: Einrichten von Internet Firewalls. O´Reilly, Köln 2002

© 2008 by eSYS Informationssysteme GmbH

Index

- A -

Administrator E-Mail: 63
Analog 78
Anschluss 79
Anschlussgeschwindigkeit 79
ANY 91
Anzahl der Logs 65
Ausgehendes Interface 87, 91
Auswahlfeld 58
Autoformatierung 144
Automatisch starten 70, 73
Autorisierung 81, 121
available settings:
* Alert Tuning: 138
* General: 138
* Output Modules: 138
* Preprocessors: 138
* Snort Rules: 138
* Update Snort Rules: 138
o Activate IPS mode 138
o Activate/Deactivate rules 138
o Activate/Deactivate several preprocessors 138
o additional settings 138
o Choose available rule sources 138
o Database Output Module 138
o Define own addresses and services 138
o Gibraltar Firewall Alert and Output Solution 138
o Select the interface on which Snort should run 138
o Syslog Output Module 138

- B -

Benutzer Zertifikate 125
Benutzername 79, 80, 81

- C -

CA Zertifikate 125
CHAP 79
Check IP-Adresse 80
CIDR 58
client-to-network 123

- D -

Dateisystems 144
DHCP 85
Dial on Demand 79
Dial-in 78
Dial-In - Telefoneinwahl 14
Dienste 70
DNAT 99
DNS 73
Domäne 73, 85, 109
Dynamischer Paketfilter 87, 91

- E -

Eingehendes Interface 87, 91
Elementgruppe 58
ESP 123
ESTABLISHED 87, 91

- F -

Features 1
Firewall 3, 87
Firewallregeln 87, 91
Floppy 144
FQDN 73, 109
Fragmentierung 93

- G -

GibADMIN 10
Gnutella 96

- H -

HDD 144
Herunterfahren 63
Hilfe 10
Holdoff 79
Hosts 76

- I -

ICMP 91
Idle 79
IKE 123
Incoming 96
Installation 7

© 2008 by eSYS Informationssysteme GmbH

Interface 73
INVALID 91
IP Compression 123
ISDN 78

- K -

Kazaa 96
Konfiguration 143
Konfiguration speichern 144
Kontrollkästchen 58

- L -

L2TP 124
lease 86
Limit 93
Limit-burst 93
Lizenzdatei 60
Lizenzschlüssel 7
Logout 10

- M -

Mail 109
Mailserver 111
MASQUERADE 99
Modem 78

- N -

Name des Systems 63
NAT 96
NAT-Traversal 120
Netzwerk 72
Netzwerkkarte 73
Neu starten 63
Neustart 63
NEW 91

- O -

Optionsfeld 58
Outgoing 96

- P -

P2P 96
Package Modification 93
PAP 79
Passwort 121
Passwort ändern 63
PFS 123
PPTP 79, 123
Private Schlüssel 125
Protokoll 91, 99
Puls 79

- Q -

Quell IP-Adresse 91, 99
Quelle 144
Quellport 91

- R -

RBL-Listen 109
REDIRECT 99
RELATED 87, 91
Relaying 108
Routen 75
Routing 75

- S -

Schaltfläche 58
SNAT 99
Speichern 62
SPI 93
Sprachauswahl 10
SSL 128
Standardroute 75, 79, 80, 81
Stateful Inspection 87, 91
Support 10
Syslog-Datei 65
System 62
Systemlogs 65

- T -

Target 91, 99
Telefoneinwahl 78
Textfeld 58
Ton 79
Transport 123
TTL 93
Tunnel 120, 128

© 2008 by eSYS Informationssysteme GmbH

- U -

Überprüfungsintervall 80
Übersicht aktive Regeln 90, 99
Update 10

- V -

Verbindungstest 76
Verknüpfung 58
Verschlüsselungsalgorithmen 123
VPI/VCI 81

- W -

Wählverfahren 79
Wertebereich 85
Wiederholfrequenz in Sekunden 65

- X -

X509 Zertifikat 121

- Z -

Zeitzone 63
Zertifikate 125
Ziel IP-Adresse 91, 99
Zielport 91
Zusätzliche Interfaces 78

© 2008 by eSYS Informationssysteme GmbH