

Gibraltar Firewall



Rene Mayrhofer

*Linuxwochen
Linz, 13.4.2005
17:00 – 18:00*

Vortragsinhalt

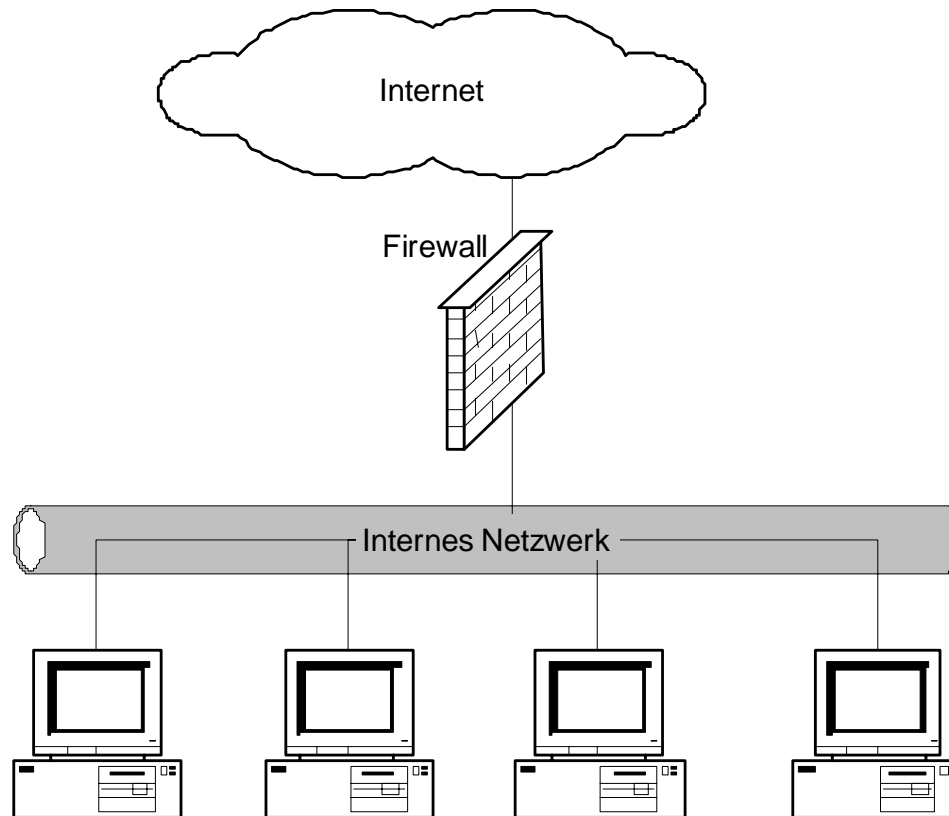
- **Firewalltechnologien**
 - Paketfilter
 - Proxy
 - NAT
 - VPN
- **Gibraltar**
 - Geschichte
 - Funktionen
 - Referenzen
 - Preise

Einführung in Firewalltechnologien



**Firewall, Paketfilter, Proxy-
Server, NAT, VPN**

Was ist eine Firewall?



Firewall - Grundlagen

- Eine Firewall ist der Schwerpunkt der Sicherheitsmaßnahmen
 - gesamter Verkehr muss Kontrollpunkt passieren
 - Verkehr kann überwacht werden
- Durchsetzen der Sicherheitspolitik
 - verhindert, dass Daten nach außen gelangen
- Protokollierung
 - protokolliert den laufenden Netzwerkverkehr
- Verkleinerung der Angriffsfläche
 - trennt verschiedene Bereiche des Firmennetzwerks
 - DMZ (Demilitarisierte Zonen)
- **schützt nur Verbindungen, die durch sie hindurchgehen**
- schützt nicht / nur bedingt gegen Angriffe von innen
- bietet keinen vollständigen Virenschutz
- kann sich nicht selbst einrichten

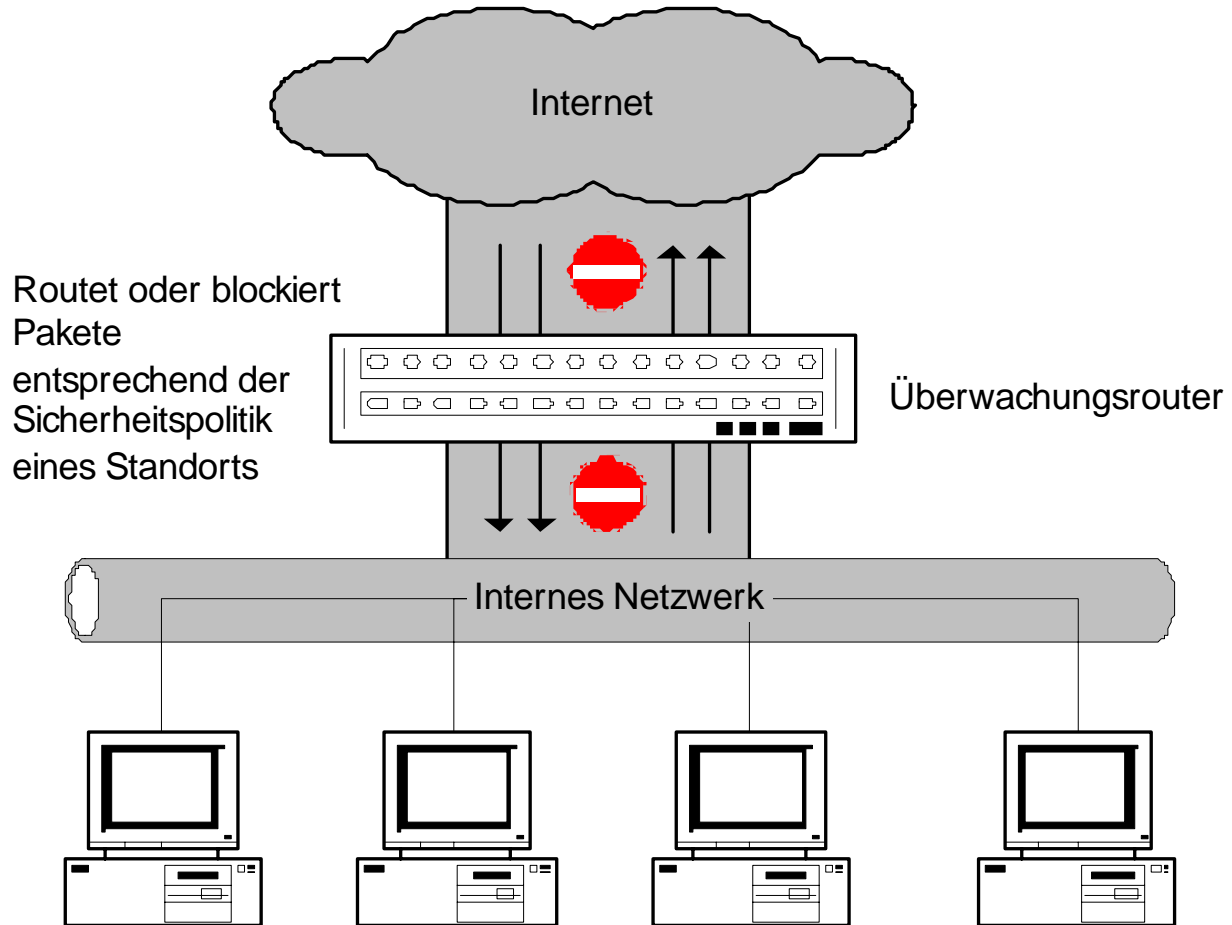
Firewall - Techniken

- **Paketfilterung:** Kern einer jeden Firewall, Umsetzung der Sicherheitsrichtlinien und Überwachung des Netzwerktraffics
- **Proxy-Dienste:** Sicherheits- und Performancefunktion. Application-Level-Inspection, Deep Inspection
- **NAT** (Network – Adress – Translation): Adressübersetzung
- **VPN** (Virtuelle Private Netzwerke): **IPSec**

ISO/OSI – 7-Schichtenmodell

Schicht	ISO/OSI-Modell		TCP/IP-Modell
7	Applikationsschicht	Applikations- Protokolle	telnet, ftp, nfs rlogin, DNS smtp, snmp X-Windows Socket library
6	Präsentationsschicht		
5	Kommunikations- Steuerungsschicht		
4	Transportschicht	Transport- Protokolle	TCP UDP
3	Netzwerkschicht	Internetwork- Protokolle	IP EGP, RIP ICMP ARP, RARP
2	Sicherungsschicht	Network- Access- Protokolle	Ethernet CSMA/CD Token Ring FDDI
1	Bitübertragungsschicht		

Paketfilterung



Paketfilter

- Paketfilter arbeiten auf **Ebenen 3 und 4** des ISO/OSI Schichtenmodells
- routen Pakete zwischen internen und externen Hosts
- arbeiten selektiv
- erlauben und blockieren Pakete

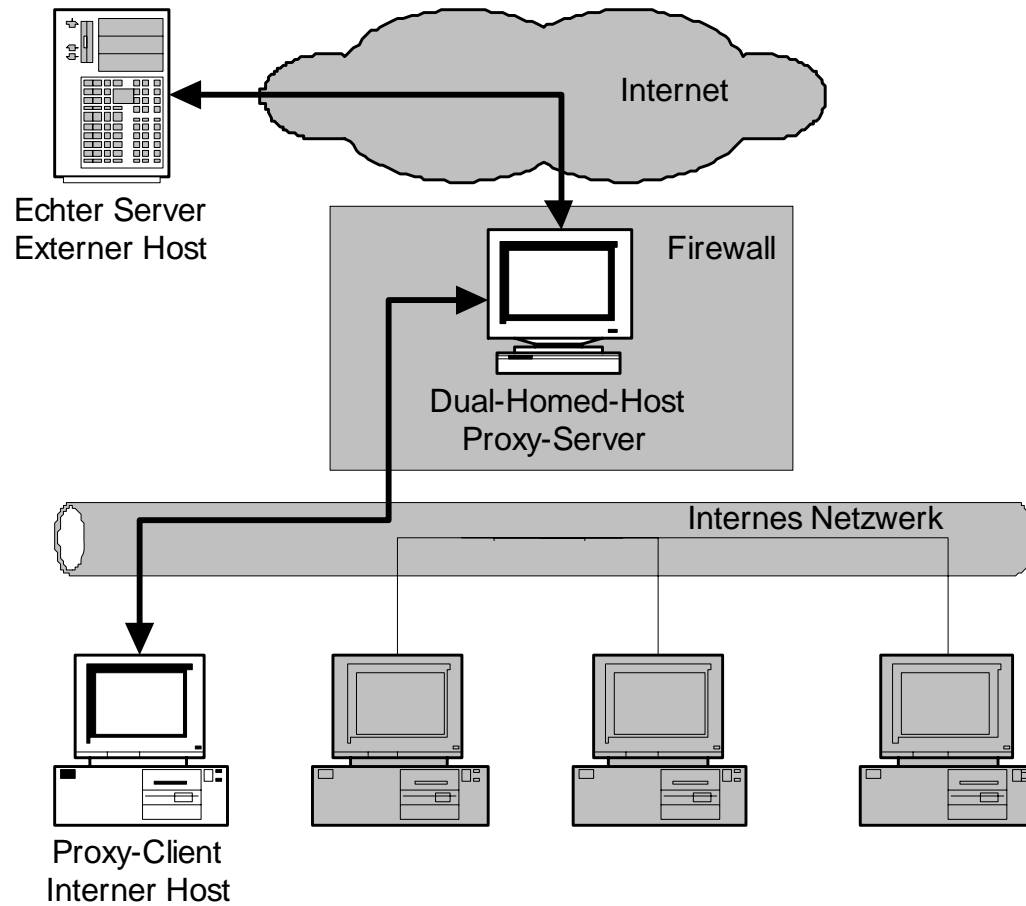
- Paket-Header für IPv4:
 - IP-Quelladresse
 - IP-Zieladresse
 - Protokoll
 - TCP oder UDP-Quellport
 - TCP oder UDP-Zielport
 - ICMP-Meldungstyp
 - Paketgröße
 - ...

- Prinzipielle Unterscheidung zwischen **stateless** und **stateful** Filterung

ISO/OSI – 7-Schichtenmodell

Schicht	ISO/OSI-Modell		TCP/IP-Modell
7	Applikationsschicht	Applikations- Protokolle	telnet, ftp, nfs rlogin, DNS smtp, snmp X-Windows Socket library
6	Präsentationsschicht		
5	Kommunikations- Steuerungsschicht		
4	Transportschicht	Transport- Protokolle	TCP UDP
3	Netzwerkschicht	Internetwork- Protokolle	IP EGP, RIP ICMP ARP, RARP
2	Sicherungsschicht	Network- Access- Protokolle	Ethernet CSMA/CD Token Ring FDDI
1	Bitübertragungsschicht		

Proxy - Dienste



Proxy - Dienste

- Proxys arbeiten auf den **Ebenen 5 bis 7**
- Stellvertreter
- spezielle Anwendungen oder Server-Programme, die Benutzeranfragen an Internet-Dienste entgegennehmen und sie an den eigentlichen Dienst weiterleiten.
- Application-Level-Gateways
- Erhöhung der Sicherheit
- höhere Effektivität des Netzwerks bei caching Proxys
- transparent oder nicht transparent
- Kann für bestimmte Protokolle nötig sein, da Eingriff auf Ebenen 5 bis 7 bei NAT nötig sind (z.B. FTP, H.323)

ISO/OSI – 7-Schichtenmodell

Schicht	ISO/OSI-Modell		TCP/IP-Modell
7	Applikationsschicht	Applikations- Protokolle	telnet, ftp, nfs rlogin, DNS smtp, snmp X-Windows Socket library
6	Präsentationsschicht		
5	Kommunikations- Steuerungsschicht		
4	Transportschicht	Transport- Protokolle	TCP UDP
3	Netzwerkschicht	Internetwork- Protokolle	IP EGP, RIP ICMP ARP, RARP
2	Sicherungsschicht	Network- Access- Protokolle	Ethernet CSMA/CD Token Ring FDDI
1	Bitübertragungsschicht		

Mögliche Ebenen für Filterung

- Erinnerung: ISO/OSI Schichtenmodell bietet verschiedene Punkte zum Filtern von Netzwerkverkehr
- Für Firewalls interessant sind:
 - Layer 2: sog. "Bridging" Firewalls, auch als "transparente" oder "unsichtbare" Firewalls beschrieben
 - Layer 3: "normale" Firewalls
 - Layer (5 –) 7: "Deep Inspection" / "Content Inspection" / "Intelligent" / "Smart" / (hier bitte das aktuelle Marketing Buzz-Word der Woche einsetzen) Firewalls

Layer 2 Firewalls

- Firewall funktioniert wie Bridge, d.h. die angeschlossenen Ethernet-Segmente sind transparent auf Ethernet-Ebene miteinander verbunden
- Allerdings: nicht jedes Paket wird weitergeleitet, sondern es wird nach üblichen Firewall-Regeln gefiltert (also z.B. Quell-/Ziel-MAC, -IP, -Port, etc.)
- Vorteile:
 - **Kein Routing**, also muss auch kein Gateway bei den angeschlossenen Computern eingetragen werden
 - Daher bei bestehenden Netzwerkstrukturen **keinerlei Aufwand zur Rekonfiguration** – eine Layer 2 Firewall kann als Ersatz für ein Netzkabel „dazwischengesteckt“ werden
 - Firewall selbst benötigt **keine IP-Adressen** und ist daher über das Netzwerk auch nicht (zumindest nicht direkt!) angreifbar

Layer 3 Firewalls

- Übliche Firewalltechnik, d.h. die Firewall arbeitet wie ein Router
- Mindestens eine IP-Adresse pro Netzwerkschnittstelle
- Angeschlossene Computer verwenden die Firewall als Gateway
- Vorteil: **bekannte Struktur**

Layer 7 Firewalls

- Einbindung in Netzwerk entweder als Layer 2 oder Layer 3 Firewall
- Untersuchung der Pakete zusätzlich auf höheren ISO/OSI Schichten (Anwendungsschichten 5-7), also im Datenbereich aus Sicht von IP bzw. TCP/UDP ⇒ „Deep Inspection“
- Daher: mehr Information zur Entscheidung ob Paket weitergeleitet oder verworfen/zurückgewiesen werden soll
- Vorteile:
 - Applikationsprotokoll wird in Entscheidung mit einbezogen
⇒ **mehr Freiraum und Sicherheit**
 - **Zusatzdienste** auf Applikationsebene möglich, die direkt auf den übertragenen Daten arbeiten (applikationsabhängig!)
z.B.: transparenter Virenschutz (HTTP, FTP, SMTP, POP3, IMAP4, ...),
Blockieren von Cookies (HTTP), Blockieren von Javascript etc. (HTTP)
- Nachteile:
 - **deutlich höherer Ressourcenbedarf** (CPU, RAM, HDD)
 - erhöhte Latenz

Anwendungsbeispiel: transparenter HTTP Proxy

- Möglichkeiten für Layer 7-Transparenz:
 - Direkte Untersuchung der einzelnen Pakete im Kernel (äquivalent zur Prüfung der ISO/OSI Schichten 2 – 4)
 - ⇒ Problem der Komplexität
 - **Umleitung** der Pakete an einen erweiterten HTTP Proxy
 - ⇒ besser durch Modularisierung
- Verhält sich so als ob im Web-Client der HTTP Proxy eingetragen wäre, allerdings ohne den damit verbundenen administrativen Aufwand
- Erlaubt im Prinzip beliebige Änderungen an den in HTTP übertragenen Daten, z.B.:
 - Filterung nach erlaubten/unerwünschten URLs (wichtig für öffentliche Zugänge, Schulen, etc.)
 - Transparente Entfernung von **Viren** (on-the-fly)
 - **Benutzerauthentifizierung**
 - Entfernung ungewünschter HTML-Tags bzw. Inhalte (**ActiveX**, **JavaScript**, **Cookies**, **Pop-Ups**, etc.)
 - Beschleunigung durch **Caching**

NAT – Network – Address Translation

- Veränderung von Netzwerkadressen
- Router verändert Pakete
 - nach außen: Quelladresse wird verändert
 - nach innen: Zieladresse wird verändert
- Häufigste Anwendung: Masquerading / Maskierung:
 - Problem: Durch IPv4-Adressknappheit wird von Providern oft nur eine einzige IP-Adresse zur Verfügung gestellt, obwohl mehrere Computer angebunden werden sollen
 - Lösung: Interne Rechner bekommen private, im Internet nicht verwendbare Adressen. Bei der Weiterleitung ins Internet ersetzt die Firewall die Quelladresse aller Pakete durch ihre eigene, Antwortpakete gehen daher direkt an die Firewall. Durch interne Zuordnungstabellen können die Antwortpakete an die richtigen internen Rechner weitergeleitet werden.

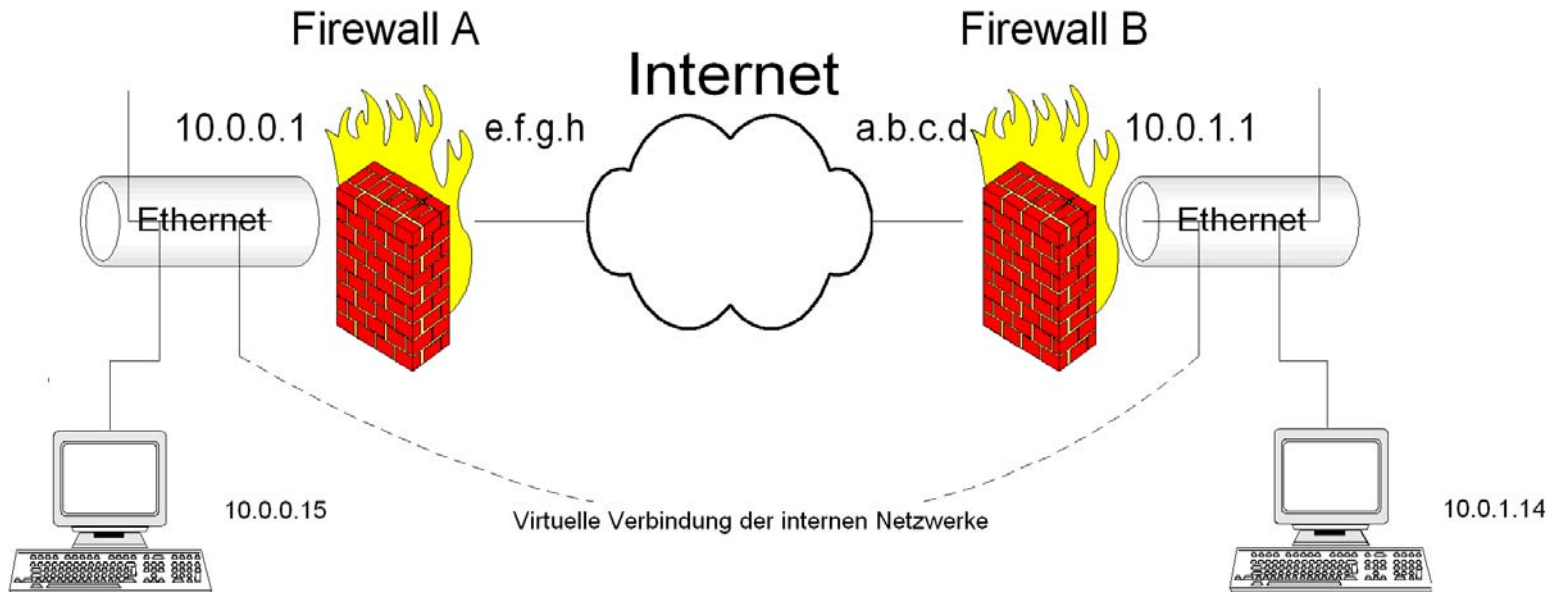
NAT (2)

- Vorteile
 - NAT unterstützt die Kontrolle der Firewall über nach außen gerichtete Verbindungen
 - eingehender Verkehr kann eingeschränkt werden
 - interne Konfiguration des Netzwerks wird verborgen
- Nachteile
 - ev. Problem mit eingebetteten IP-Adressen
 - Verschlüsselung und Authentifizierung erschwert
 - Protokollierung bei dynamischer Adresszuweisung
 - Dynamische Zuweisung von Ports stört Paketfilterung
 - Diverse Protokolle übertragen IP-Adressen der Clients auf Anwendungsebene (z.B. FTP, H.323) ⇒ spezielle Unterstützung muss in NAT eingebaut werden

Virtuelle Private Netzwerke (VPN)

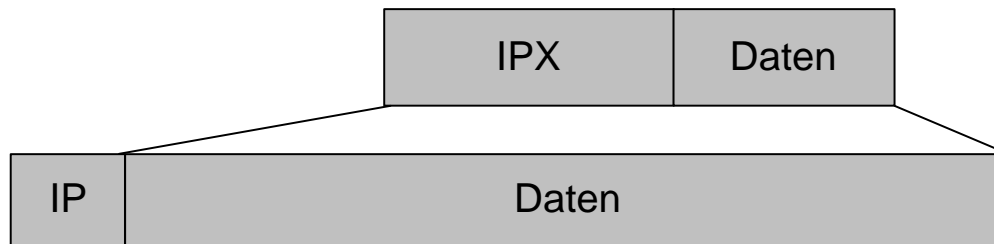
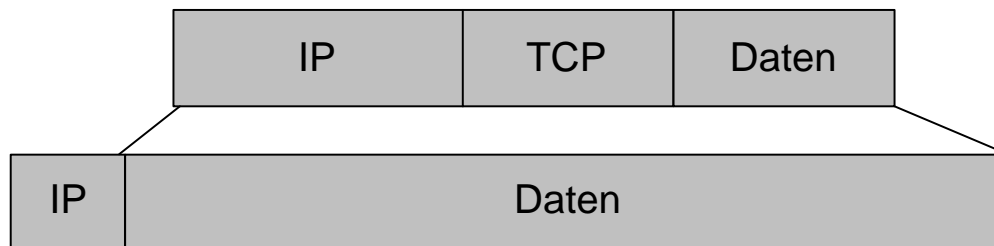
- öffentliches Netz wird privat genutzt
- **Vertraulichkeit** durch Verschlüsselung
- **Integrität** wird geschützt
- **Authentizität** wird sichergestellt
- Daten werden gekapselt
- Methoden
 - End-zu-End Verschlüsselung
 - Tunnel

VPN - Prinzip



VPNs für Tunnel

- Meist im Tunnel-Modus betrieben: Rechner hinter den jeweiligen Gateways können transparent miteinander kommunizieren, obwohl die Gateways keine direkte Verbindung haben
- Methode: „Verpacken“ der Pakete, die zwischen den internen Rechnern ausgetauscht werden sollen in IPv4-Pakete



Tunneling

- Verschiedene Implementierungen von Tunneling (Beispiele):
 - GRE (unverschlüsselt)
 - IPv6-over-IPv4 (unverschlüsselt, Übergangsmaßnahme zu IPv6)
 - PPP-over-Ethernet (unverschlüsselt)
 - PPP-over-ATM (unverschlüsselt)
 - L2TP (**unverschlüsselt!**)
 - PPTP (nur bedingt sicher)
 - **IPSec**
 - OpenVPN
 - VTun (unsicher!)
 - CIPE (unsicher!)
 - Tinc (unsicher!)
 - (höchstwahrscheinlich unsicher!)

Gibraltar Firewall



GIBRALTAR

Geschichte
Prinzip
Vor- und Nachteile
Referenzen
Preise

Gibraltar - Entstehung

- Diverse Debian-basierte Firewalls seit 1999 im Einsatz
- Projektbeginn Juli 2000 von Rene Mayrhofer
- 2000 – 2002: permanente Weiterentwicklung, gestützt auf Verbesserungsvorschläge aus der wachsenden Community
- 2001: Erstentwicklungen zur Web-basierten Administrationsoberfläche, Entwicklung eines entsprechenden Frameworks an der Johannes Kepler Universität Linz
- 2002: erste Ideen zu einer kommerziellen Version
- 2/2003: Partnerschaft von Rene Mayrhofer mit der eSYS Informationssysteme GmbH. Start der kommerziellen Entwicklung
- 11/2003: Präsentation der Version 1.0. Erste Version mit Webinterface
- 5/2004: Gibraltar v2
- 11/2004: Gibraltar v2.1
- 04/2005: Gibraltar v2.2

Gibraltar – Zahlen und Fakten

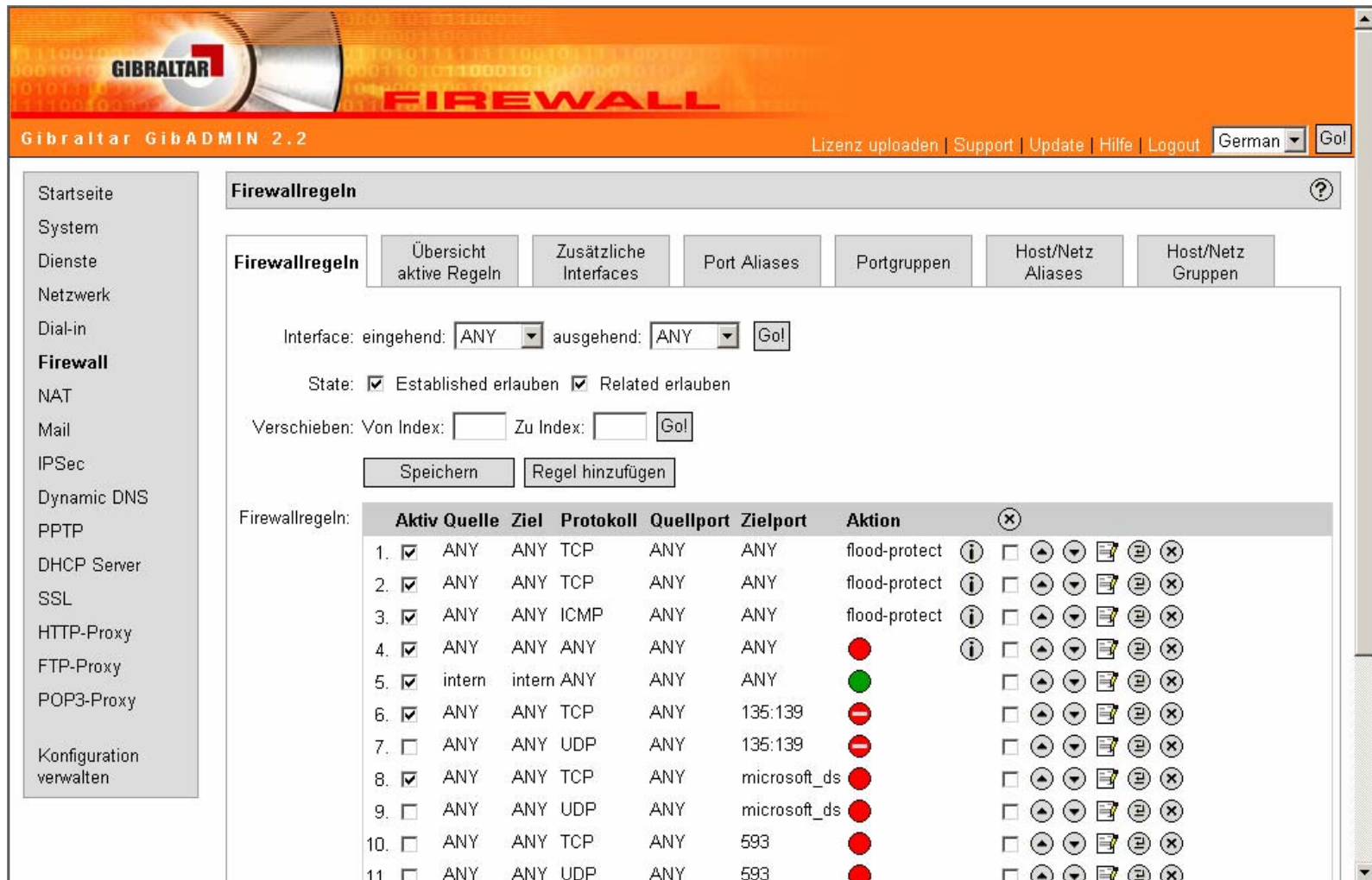
- geschätzte Installationen der freien Version: über 1000
- kommerzielle Installationen: ca. 200
- Testinstallationen (Testlizenzen) seit 11/2003: ca. 3000
- tägliche Anzahl von Zugriffen auf Homepage: 600-1000
- Mailingliste: knapp 500 Mitglieder

- seit 11/2004: ca. 20 Vertriebs- und Supportpartner in
 - Österreich
 - Deutschland
 - Schweiz
 - Italien
 - USA
 - Finnland
 - Griechenland

Grundprinzipien

- basierend auf Debian GNU/Linux 3.0 (**woody++**, demnächst **sarge**)
- bootet und läuft vollständig von CD-ROM
- minimale Hardwareanforderungen
- vollständig mittels Webinterface konfigurierbar
- sicher durch Verwendung von gängigen Open-Source-Komponenten und Live CD Technology
- Extras
 - Virtuelle Private Netzwerke
 - Kaspersky Antivirus Engine
 - State-of-the-art Spamschutz
 - ab Version 2.3: Failover mit Hot-Standby für hohe Verfügbarkeit
 - Traffic Shaping
 - Transparentes Firewalling

Das Webinterface



Gibraltar GibADMIN 2.2 Lizenz uploaden | Support | Update | Hilfe | Logout German Go!

Firewallregeln ?

Firewallregeln
Übersicht aktive Regeln
Zusätzliche Interfaces
Port Aliases
Portgruppen
Host/Netz Aliases
Host/Netz Gruppen

Interface: eingehend: ausgehend: Go!

State: Established erlauben Related erlauben

Verschieben: Von Index: Zu Index: Go!

Speichern Regel hinzufügen

Firewallregeln:	Aktiv	Quelle	Ziel	Protokoll	Quellport	Zielport	Aktion	
1.	<input checked="" type="checkbox"/>	ANY	ANY	TCP	ANY	ANY	flood-protect	
2.	<input checked="" type="checkbox"/>	ANY	ANY	TCP	ANY	ANY	flood-protect	
3.	<input checked="" type="checkbox"/>	ANY	ANY	ICMP	ANY	ANY	flood-protect	
4.	<input checked="" type="checkbox"/>	ANY	ANY	ANY	ANY	ANY		
5.	<input checked="" type="checkbox"/>	intern	intern	ANY	ANY	ANY		
6.	<input checked="" type="checkbox"/>	ANY	ANY	TCP	ANY	135:139		
7.	<input type="checkbox"/>	ANY	ANY	UDP	ANY	135:139		
8.	<input checked="" type="checkbox"/>	ANY	ANY	TCP	ANY	microsoft_ds		
9.	<input type="checkbox"/>	ANY	ANY	UDP	ANY	microsoft_ds		
10.	<input type="checkbox"/>	ANY	ANY	TCP	ANY	593		
11.	<input type="checkbox"/>	ANY	ANY	UDP	ANY	593		

System

- Live CD Technology: bootet und läuft vollständig von CD ROM
- Keine Festplatteninstallation notwendig
- Speziell gehärteter Linux Kernel
- Sprachen: Deutsch, Englisch
- Fernkonfiguration mittels Webinterface oder remote login
- Einfaches Konfigurationsmanagement
- Automatische Live Updates
- Minimale Hardwareanforderungen

Systemeinstellungen

Allgemeine Einstellungen

Systemlogs

Beschädigte Dateien

Festplatte konfigurieren

Name des Systems:

Domäne:

Lokalzeit: Mon Apr 11 13:42:58 CEST 2005

Zeit in UTC: Mon Apr 11 11:42:58 UTC 2005

Zeitzone:

Administrator Email:

Intervall Admin-Email: Stunde(n)

Standardsprache:

Automatisches Update aktivieren: Jeden Tag um

Webinterface Port:

Neu starten

Herunterfahren

Speichern

Passwort ändern

Netzwerkunterstützung

- Ethernet 10/100/1000 MBit/s: statisch oder DHCP, virtuelle IP Adressen
- ADSL Ethernet Modems: PPP over Ethernet, PPTP
- ADSL USB Modems: PPP over ATM
- Modem Dial In: Seriell, USB
- Unbegrenzte Anzahl von Netzwerkschnittstellen

Gibraltar GibADMIN 2.2

Lizenz uploaden | Support | Update | Hilfe | Logout | German | Go!

Netzwerkeinstellungen

DNS | int | ext | Routing | Verbindungstest

DNS Server:

Domäne	IP-Adresse	
www.gibraltar.at	10.50.50.2	<input type="checkbox"/>


Server hinzufügen

Speichern

Stateful Packet Inspection

- Protokollunterstützung: ICMP, TCP, UDP, GRE, ESP, AH, IPv6-over-IPv4
- Flexibler Paketfilter: Schnittstelle, MAC-Adresse, IP-Adresse, Service, Port,...
- NAT: Network Address Translation
- PAT: Port Address Translation
- Freie Definition von Aliases und Gruppen: Adressen und Ports
- DoS/Flood-Protection: vordefiniert, erweiterbar
- Randomized IP Sequencing
- Gezielte TTL Manipulation
- Protokoll Pass Through: PPTP, FTP, H.323, IRC

Firewall - Regeln


Gibraltar GibADMIN 2.2 [Lizenz uploaden](#) [Support](#) [Update](#) [Hilfe](#) [Logout](#) German

- Startseite
- System
- Dienste
- Netzwerk
- Dial-in
- Firewall**
- NAT
- Mail
- IPSec
- Dynamic DNS
- PPTP
- DHCP Server
- SSL
- HTTP-Proxy
- FTP-Proxy
- POP3-Proxy
- Konfiguration verwalten

Firewallregeln ?

Firewallregeln
Übersicht
aktive Regeln
Zusätzliche
Interfaces
Port Aliases
Portgruppen
Host/Netz
Aliases
Host/Netz
Gruppen

Interface: eingehend: ausgehend:

State: Established erlauben Related erlauben

Verschieben: Von Index: Zu Index:

Firewallregeln:	Aktiv	Quelle	Ziel	Protokoll	Quellport	Zielport	Aktion						
1.	<input checked="" type="checkbox"/>	ANY	ANY	TCP	ANY	ANY	flood-protect		<input type="checkbox"/>				
2.	<input checked="" type="checkbox"/>	ANY	ANY	TCP	ANY	ANY	flood-protect		<input type="checkbox"/>				
3.	<input checked="" type="checkbox"/>	ANY	ANY	ICMP	ANY	ANY	flood-protect		<input type="checkbox"/>				
4.	<input checked="" type="checkbox"/>	ANY	ANY	ANY	ANY	ANY			<input type="checkbox"/>				
5.	<input checked="" type="checkbox"/>	intern	intern	ANY	ANY	ANY			<input type="checkbox"/>				
6.	<input checked="" type="checkbox"/>	ANY	ANY	TCP	ANY	135:139			<input type="checkbox"/>				
7.	<input type="checkbox"/>	ANY	ANY	UDP	ANY	135:139			<input type="checkbox"/>				
8.	<input checked="" type="checkbox"/>	ANY	ANY	TCP	ANY	microsoft_ds			<input type="checkbox"/>				
9.	<input type="checkbox"/>	ANY	ANY	UDP	ANY	microsoft_ds			<input type="checkbox"/>				
10.	<input type="checkbox"/>	ANY	ANY	TCP	ANY	593			<input type="checkbox"/>				
11.	<input type="checkbox"/>	ANY	ANY	UDP	ANY	593			<input type="checkbox"/>				

Konfiguration einer Firewall-Regel

Firewallregeln

Standard

Erweitert

Erweitert - P2P

Interface: int -> ext

Regel aktivieren:

Quelladresse: intern oder ausgenommen:

Zieladresse: ext_ip_jup1 oder ausgenommen:

Protokoll: TCP

Quellport: CUSTOM oder

Zielport: pop3/110 oder

Status: NEW

Aktion: ACCEPT

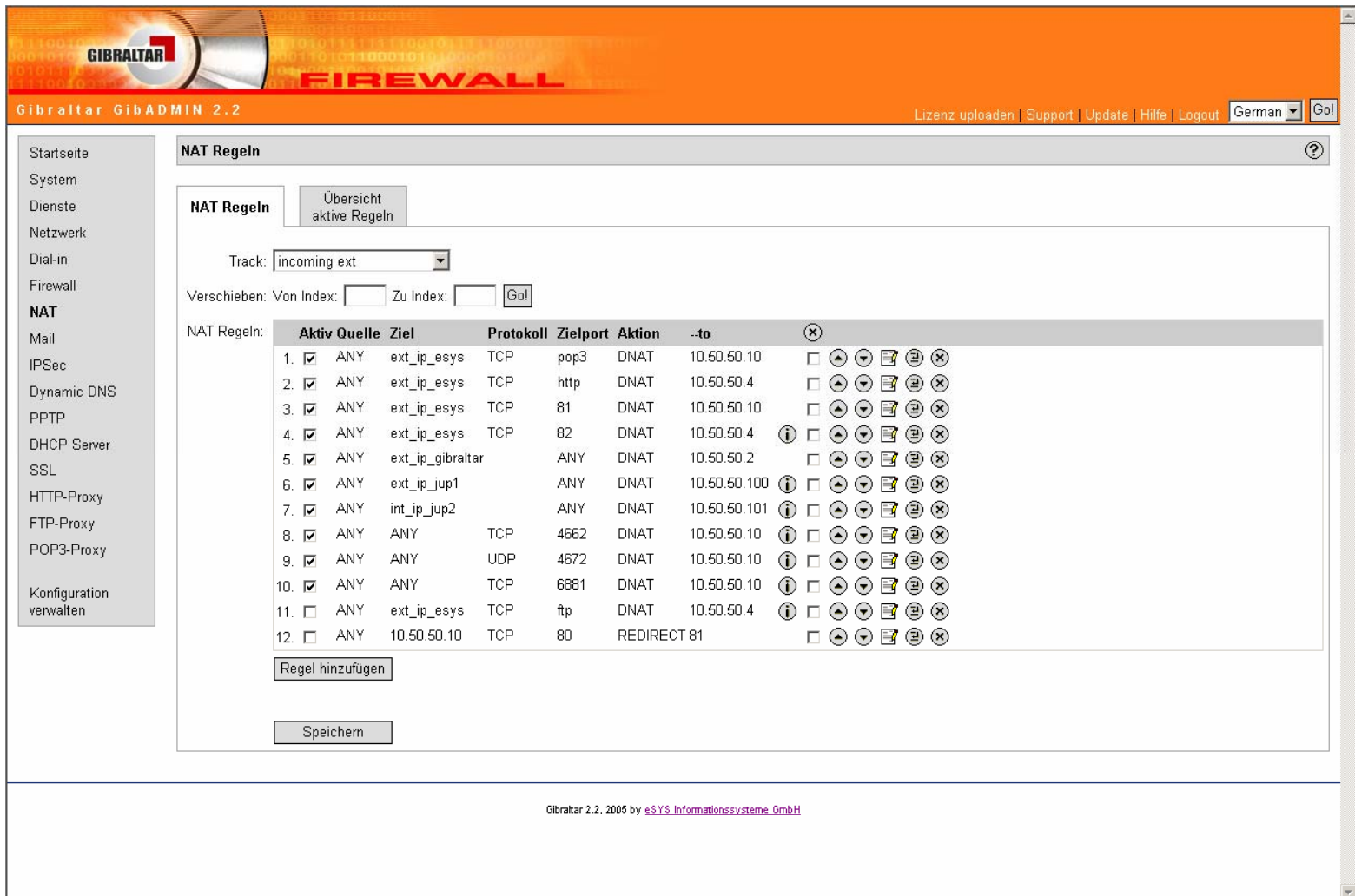
Kommentar:

Speichern

Abbrechen

Weitere Regel hinzufügen

NAT (Network – Address – Translation)



GIBRALTAR FIREWALL
Gibraltar GibADMIN 2.2

Lizenz uploaden | Support | Update | Hilfe | Logout German Go!

Startseite
System
Dienste
Netzwerk
Dial-in
Firewall
NAT
Mail
IPSec
Dynamic DNS
PPTP
DHCP Server
SSL
HTTP-Proxy
FTP-Proxy
POP3-Proxy
Konfiguration verwalten

NAT Regeln Übersicht aktive Regeln

Track: incoming ext

Verschieben: Von Index: Zu Index: Go!

NAT Regeln:

	Aktiv	Quelle	Ziel	Protokoll	Zielport	Aktion	--to		
1.	<input checked="" type="checkbox"/>	ANY	ext_ip_esys	TCP	pop3	DNAT	10.50.50.10	<input type="checkbox"/>	
2.	<input checked="" type="checkbox"/>	ANY	ext_ip_esys	TCP	http	DNAT	10.50.50.4	<input type="checkbox"/>	
3.	<input checked="" type="checkbox"/>	ANY	ext_ip_esys	TCP	81	DNAT	10.50.50.10	<input type="checkbox"/>	
4.	<input checked="" type="checkbox"/>	ANY	ext_ip_esys	TCP	82	DNAT	10.50.50.4		
5.	<input checked="" type="checkbox"/>	ANY	ext_ip_gibraltar	ANY	DNAT	10.50.50.2	<input type="checkbox"/>		
6.	<input checked="" type="checkbox"/>	ANY	ext_ip_jup1	ANY	DNAT	10.50.50.100			
7.	<input checked="" type="checkbox"/>	ANY	int_ip_jup2	ANY	DNAT	10.50.50.101			
8.	<input checked="" type="checkbox"/>	ANY	ANY	TCP	4662	DNAT	10.50.50.10		
9.	<input checked="" type="checkbox"/>	ANY	ANY	UDP	4672	DNAT	10.50.50.10		
10.	<input checked="" type="checkbox"/>	ANY	ANY	TCP	6881	DNAT	10.50.50.10		
11.	<input type="checkbox"/>	ANY	ext_ip_esys	TCP	ftp	DNAT	10.50.50.4		
12.	<input type="checkbox"/>	ANY	10.50.50.10	TCP	80	REDIRECT 81		<input type="checkbox"/>	

Regel hinzufügen

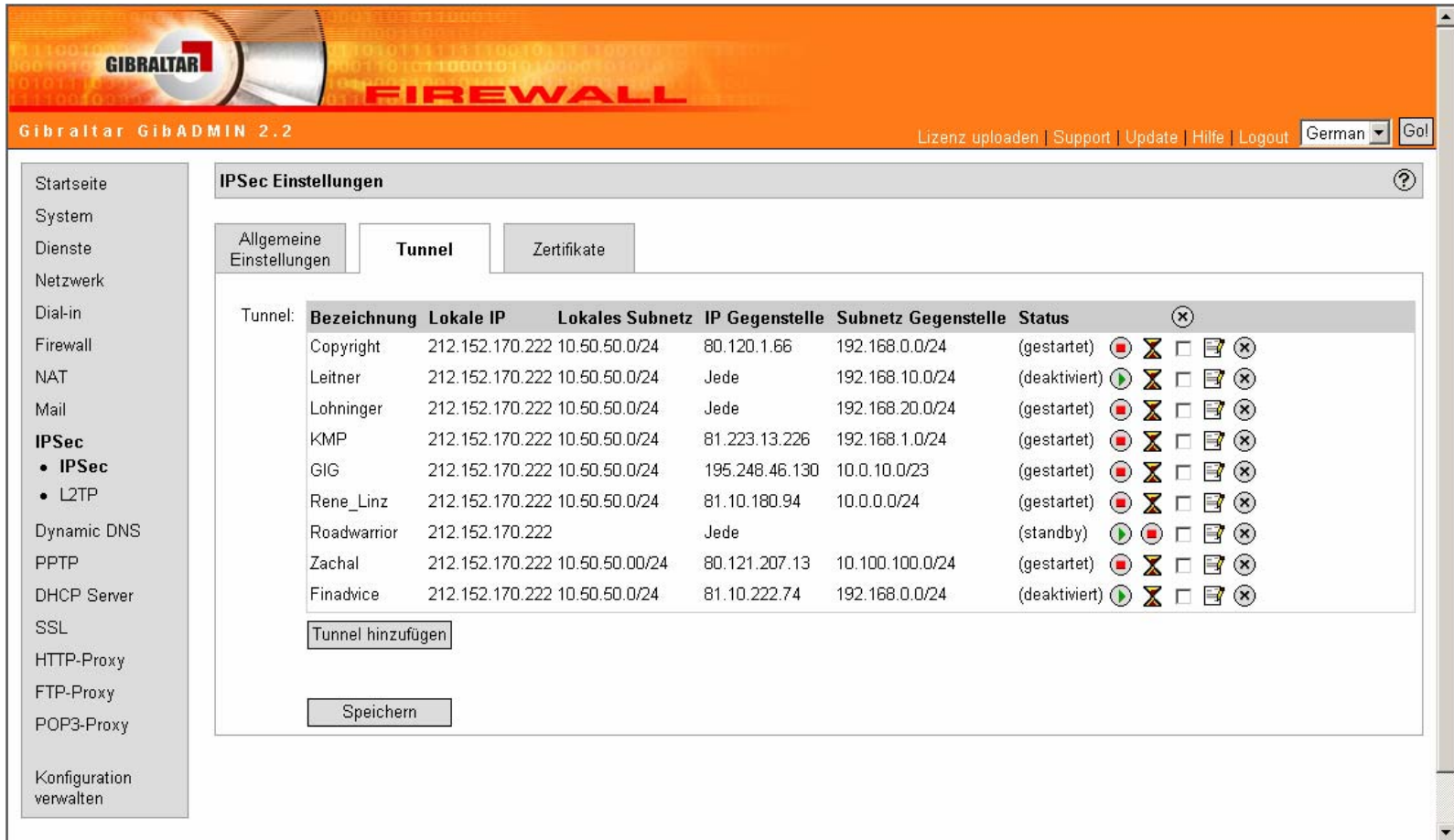
Speichern

Gibraltar 2.2, 2006 by eSYS Informationssysteme GmbH

VPN (Virtuelle Private Netzwerke)

- IPSec Gateway
- PPTP Server: MPPE 128 Bit Encryption
- Network-to-Network VPN (IPSec)
- Network-to-Client VPN: Kompatibel mit MS Windows 2000/XP (IPSec, IPSec/L2TP, PPTP)
- Unbeschränkte Anzahl von VPN Tunneln
- Authentifizierung mit PSK (Private Shared Key) und X.509 Zertifikaten
- Verschlüsselung: 3DES, Blowfish, Serpent, Twofish, CAST, AES
- Authentifizierung PPTP / L2TP: CHAP, MS-CHAPv1, MS-CHAPv2
- NAT traversal
- Perfect Forward Secrecy (PFS)

VPN - Tunnels



GIBRALTAR FIREWALL

Gibraltar GibADMIN 2.2 Lizenz uploaden | Support | Update | Hilfe | Logout German Go!

- Startseite
- System
- Dienste
- Netzwerk
- Dial-in
- Firewall
- NAT
- Mail
- IPSec**
 - IPsec
 - L2TP
- Dynamic DNS
- PPTP
- DHCP Server
- SSL
- HTTP-Proxy
- FTP-Proxy
- POP3-Proxy
- Konfiguration verwalten

IPSec Einstellungen ?

Allgemeine Einstellungen

Tunnel

Zertifikate

Tunnel:	Bezeichnung	Lokale IP	Lokales Subnetz	IP Gegenstelle	Subnetz Gegenstelle	Status	⊗
	Copyright	212.152.170.222	10.50.50.0/24	80.120.1.66	192.168.0.0/24	(gestartet)	⊗
	Leitner	212.152.170.222	10.50.50.0/24	Jede	192.168.10.0/24	(deaktiviert)	⊗
	Lohninger	212.152.170.222	10.50.50.0/24	Jede	192.168.20.0/24	(gestartet)	⊗
	KMP	212.152.170.222	10.50.50.0/24	81.223.13.226	192.168.1.0/24	(gestartet)	⊗
	GIG	212.152.170.222	10.50.50.0/24	195.248.46.130	10.0.10.0/23	(gestartet)	⊗
	Rene_Linz	212.152.170.222	10.50.50.0/24	81.10.180.94	10.0.0.0/24	(gestartet)	⊗
	Roadwarrior	212.152.170.222		Jede		(standby)	⊗
	Zachal	212.152.170.222	10.50.50.00/24	80.121.207.13	10.100.100.0/24	(gestartet)	⊗
	Finadvice	212.152.170.222	10.50.50.0/24	81.10.222.74	192.168.0.0/24	(deaktiviert)	⊗

Deep Inspection Firewall

- Secure SMTP Relay: eingehend, ausgehend, Attachment Blocking, Block Lists, Viren- und Spamschutz **postfix (+TLS+IPv6+SASL++)**
- Transparenter HTTP Proxy: keine Clientkonfiguration notwendig, Spamschutz **squid (+erweiterte Filter-Patches)**
- User Authentifizierung: Benutzerliste, Active Directory Integration, LDAP
- Content Caching
- Content Scanning: Antivirus, Cookies, JavaScript, Active X
- URL Filter
- FTP Proxy: transparent ausgehend, eingehend **SuSE ftp-proxy + frox**
- Transparenter POP3 Proxy: Antivirus, Spamschutz, und Schutz vor gefährlichen Attachments **p3scan**

SMTP Relay

Mail Relay Einstellungen

**Allgemeine
Einstellungen**

Weiterleitung
ausgehend

Weiterleitung
eingehend

Allgemeine
Überprüfungen

SMTP
Authentifizierung

Maximale Größe der Mail
(in MB):

Viren- und Spamchecks
aktivieren:

Name des Absenders:

Email des Absenders:

Mails scannen für: **Domäne**

- esys.at
- ff-attnang.at
- ffsteindorf.at
- gibraltar.at
- mail.gibraltar.at

Speichern

Mailüberprüfung

Mail Relay Einstellungen

Allgemeine Einstellungen	Weiterleitung ausgehend	Weiterleitung eingehend	Allgemeine Überprüfungen	SMTP Authentifizierung
--------------------------	-------------------------	-------------------------	---------------------------------	------------------------

Aktion für illegale Header: Absender warnen:

Aktion für illegale Attachments: Absender warnen: Empfänger warnen:

Dateitypen filtern:

Liste	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="text" value="exe"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="text" value="vbs"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="text" value="pif"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="text" value="scr"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="text" value="bat"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="text" value="com"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Virenschutz bei E-Mail

Mail Relay Einstellungen

AntiVirus

Administrator Email:

Quarantäne Email:

Aktion, wenn Virus erkannt: Absender warnen: Empfänger warnen:

Virus Lovers: **E-Mail**

- Dualer Schutz:
 - ClamAV
 - Kaspersky

Spamfilter

Mail Relay Einstellungen

AntiSpam (1)

AntiSpam (2)

Blacklists and Whitelists

Betreff verändern:

Text in Betreff einfügen:

Administrator Email:

Quarantäne Email:

Spam Detected Header hinzufügen:

Aktion ausführen:

Aktion, wenn Spam: Absender warnen:

Spam Lovers: **E-Mail**

Spamfilterregeln automatisch aktualisieren:

Bayes-Filter aktivieren:

Bayes-Training Emails kommen von: **IP-Adresse**

Mail Relay Einstellungen

AntiSpam (1)

AntiSpam (2)

Blacklists and Whitelists

RBL Listen: **Liste**

Aktivieren Sie folgende Restriktionen, um die Weiterleitung von Dokumentation die Erläuterungen zu den Restriktionen nach,

Ungültiger Hostname oder Hostname kein FQDN

Unbekannter Hostname

SPF-Überprüfung

Absender kein FQDN

Empfänger kein FQDN

Unbekannte Absender-Domäne

Absenderadresse nicht erreichbar

Empfängeradresse nicht verifiziert

Zusatzdienste

- DHCP Server `dhcpcd 3`
- Secure DNS Resolver `djbdns`
- SSL Wrapper für beliebige TCP Dienste `sslwrap`
- Portscan Detection `psad`
- Anti Spam Filter: `spamassassin` über `amavisd-new`
regelbasiert, Bayes, RBL, Razor und DCC, SPF
- ClamAV Virens Scanner
- Kaspersky Virens Scanner
- In Entwicklung: Failover mit Hot-Standby `heartbeat` mit Erweiterungen
zur Replikation der
Connection-State Tabelle

Vorteil gegenüber Hardware-Lösungen (Watchguard, Sonicwall, Cisco, Zyxel,...)

- Preis
- Skalierbarkeit
- Flexibilität
- Erweiterbarkeit
- Sicherheit durch Open Source
- Sicherheit durch Live-CD-Technology

Vorteile gegenüber Softwarepaketen (Astaro, Checkpoint, Smoothwall,...)

- Preis
- Einfache Installation
- Sicherheit durch Live-CD-Technology
- Keine Festplatte notwendig
- Höhere Ausfallsicherheit

Facts

- Gibraltar ist nicht dauerhaft angreifbar: durch physisch schreibgeschütztes System ist es nicht möglich, sogenannten „malicious code“ dauerhaft zu plazieren
- Gibraltar ist ausgereift: seit dem Jahr 2000 wird Gibraltar weltweit von Linux-Experten verwendet, getestet und weiterentwickelt. Gibraltar verwendet tausendfach getestete Komponenten, deren Quellcode frei verfügbar ist.
- Gibraltar reduziert das Spam-Aufkommen um ca. 95%: durch die Kombination mehrerer Anti-Spam-Maßnahmen (RBL-Listen, Inhaltsanalyse, Bayes-Filter, Razor, DCC, SPF, ...) kann Gibraltar wirksam Spam-Mails erkennen und darauf reagieren.
- Gibraltar ist skalierbar und flexibel: je nach Anforderung kann geeignete Hardware verwendet und auch erweitert werden. Gibraltar unterstützt Load-Balancing und Fail-Over.

Gibraltar – Referenzen

- Referenzen Österreich
 - Universität Linz
 - Fachhochschule Kufstein
 - Fachhochschule Hagenberg
 - Technikum Wien
 - Stadtgemeinde Vöcklabruck
 - Doubrava
 - COPYright by Josef Schürz
 - Kirsch – Muchitsch und Partner
 - GIG Karasekgroup
 - Wolf Systembau
 - Stubai Werkzeugindustrie
 - Financial Advisory GmbH
 - Ebnerbau Mondsee
 - HGS Unternehmensberatung
 - Profactor Steyr
 - Datacontact
 - CARE Österreich
- Referenzen International
 - Universität Washington
 - Universität der Bundeswehr
 - Universität Stuttgart
 - Universität Oxford
 - P&T Luxemburg
 - Graziano Transmissionsi, Italien
 - Scotcomms, GB
 - ARIS AG, Schweiz
 - Calistel, Frankreich
 - COOPService Noncello, Italien
 - Kniel System Electronics
 - Noske-Kaeser GmbH, Deutschland
 - Städtische Überlandwerke Coburg
 - Scene Double, GB

Preise

- Abhängig von der Größe des zu schützenden Netzwerks
- Kostenlose Privatlizenz
- Spezielle Konditionen für Universitäten und Schulen

- Gibraltar Small Business: € 350
- Gibraltar Medium Edition: € 690
- Gibraltar Professional: € 990
- Gibraltar Enterprise Edition: € 1.790

- Jährliche Updategebühr: ab 90 Euro

Fragen?

Dr. Rene Mayrhofer

Thomas Mayrhofer
eSYS Informationssysteme GmbH
Steinhüblstraße 1
4800 Attnang-Puchheim

www.gibraltar.at

www.esys.at

office@gibraltar.at

