

Intra2net

Intra2net Administrator Handbuch



Intra2net Business Server

Intra2net Security Gateway

Intra2net Network Security

Intra2net Administrator Handbuch

Intra2net AG

Veröffentlicht 02. März 2015

Der Inhalt dieses Handbuchs wurde mit Sorgfalt erarbeitet. Die Angaben in Ihrem Handbuch gelten jedoch nicht als Zusicherung von Eigenschaften des Produkts. Die Intra2net AG haftet nur im Umfang ihrer Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen. Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen, sowie Änderungen und Versionsinformationen für Intranator finden Sie im Internet unter <http://www.intra2net.com>

Der Intranator baut in Abhängigkeit von der System-Konfiguration Kommunikationsverbindungen auf. Um ungewollte Gebühren und Datenverluste zu vermeiden, sollten Sie das Produkt unbedingt überwachen, sowie in regelmäßigen Abständen Datensicherungen durchführen. Intra2net AG übernimmt keine Verantwortung für Datenverlust, ungewollte Verbindungskosten und Schäden, die durch den unbeaufsichtigten Betrieb des Produkts entstanden sind.

Intranator und das Intranator-Logo sind eingetragene Warenzeichen der Intra2net AG. Erwähnte Firmen- und Produktnamen sind in der Regel Warenzeichen der entsprechenden Firmen bzw. Hersteller.

Copyright © 1999-2015 Intra2net AG. Alle Rechte vorbehalten. Kein Teil dieses Handbuchs darf ohne schriftliche Genehmigung der Firma Intra2net AG in irgendeiner Form reproduziert oder wiederverwertet werden.

Intra2net AG
Mömpelgarder Weg 8
72072 Tübingen
Deutschland

Gültig für Intranator Server Version 6.1.14

Gültig für Intranator Groupware Client Version 2.3.0

1. Installation	1
1. Willkommen	2
1.1. Über dieses Handbuch	2
1.2. Werkseinstellungen	2
2. Installation auf eigener Hardware	3
2.1. Hardwareauswahl	3
2.2. Installation als virtuelle Maschine	3
2.3. Standort	3
2.4. BIOS	4
2.5. RAID	5
2.6. Installation von CD	6
2.7. Lösen von Kompatibilitätsproblemen	6
3. Installation der Appliance	8
3.1. Lieferumfang	8
3.1.1. Intranator Appliance Eco	8
3.1.2. Intranator Appliance Pro	8
3.1.3. Intranator Appliance Ultimate	8
3.2. Standort	9
3.3. Anschlüsse	9
3.4. Software	9
4. Installation als virtuelle Maschine	10
4.1. Vergleich mit echter Hardware	10
4.1.1. Ungleichmäßige Ausführungsgeschwindigkeit	10
4.1.2. Geringere I/O-Performance	10
4.1.3. Kontakt mit ungefilterten Netzwerkpaketen	11
5. Installation auf VMware vSphere Hypervisor 4 (ESXi)	13
5.1. Konfiguration der virtuellen Maschine	13
5.2. Virtuelle Maschine mit direktem Internetzugang	18
5.3. Installation des Intranators	21
6. Installation auf Microsoft Hyper-V unter Windows Server 2012 R2	23
6.1. Konfiguration der virtuellen Maschine	23
6.2. Installation des Intranators	30
7. Die Konsole	31
7.1. Hardwareerkennung	31
7.2. Netzwerkkarten	31
7.3. DNS und DHCP	32
7.4. Firewall-Notmodus	32
7.5. In Auslieferungszustand zurücksetzen	32
7.6. Das root-Passwort	32
7.7. Die Linux-Shell	32
8. Die Weboberfläche	34
8.1. Zugriff auf die Weboberfläche	34
8.2. Lizenzcode	34
8.3. Die Hauptseite	34
8.4. Die Warteschlange	35
8.5. Die Konfigurationsprüfung	36
2. Allgemeine Funktionen	37
9. Intranet	38
9.1. IPs und Netze	38
9.2. Zugriffsrechte eines Netzwerkobjekts	38
9.3. Domain und DNS	39
9.3.1. DNS-Server für Lokale Domain	39
9.3.2. DNS für lokale Domain weiterleiten	39

9.3.3. DNS für andere Domains weiterleiten	39
9.3.4. DNS-Rebind verhindern	40
9.4. Clients eintragen	40
9.5. DHCP	40
9.6. Bereiche eintragen	41
9.7. Import/Export von Rechnerprofilen	41
9.7.1. Import von Rechnern	41
9.7.2. Export von Rechnern	41
9.8. Routing im Intranet	42
10. SSL-Verschlüsselung und Zertifikate	43
10.1. Prinzip und Gefahren der SSL-Verschlüsselung	43
10.2. Zertifikate richtig erstellen	43
10.2.1. Der Rechnername	43
10.2.2. Konfiguration	44
10.3. Zertifikate auf Clients installieren	44
10.3.1. Installation unter Windows	44
10.3.2. Verteilen von Zertifikaten über Active Directory	48
10.4. Benutzer sensibilisieren	49
10.5. Verwenden einer externen Zertifizierungsstelle	49
10.6. Verschlüsselungsstärke	50
11. Internet	51
11.1. Einwahl mit ISDN	51
11.2. Einwahl mit DSL (PPPoE)	51
11.3. Einwahl mit DSL (PPTP)	51
11.4. Router mit fester IP	52
11.5. Router mit DHCP oder Kabelanschluss	52
11.6. Router im lokalen Netz	52
11.7. Offizielle IPs und DMZ	53
11.7.1. Klassisches Routing	53
11.7.2. Statische NAT	54
11.7.3. Proxy-ARP	55
11.8. Verbindungsautomatik	56
11.9. Ausweichen auf andere Provider im Fehlerfall (Fallback)	57
11.10. Masquerading / NAT	57
11.11. Lockruf	57
11.12. DynDNS	58
11.12.1. Anbieter	58
11.12.2. Aktualisierung und verwendete IP	59
11.13. Zugriff von außen	59
12. Proxy	60
12.1. Überblick	60
12.2. Zugang zum Proxy	60
12.3. Proxykonfiguration	61
12.4. URL-Filter	61
12.4.1. Proxy-Profile	61
12.4.2. Proxy-Zugriffslisten	61
12.4.3. Zeitsteuerung	62
12.5. Web-Content Filter	62
12.6. Proxy-VirensScanner	63
13. Statistik und Datenschutz	64
13.1. Proxy-Statistik	64
13.1.1. Proxy-Protokollierung	64
13.1.2. Auswertung	64

13.1.3. Methodik	64
13.2. Internet-Zugriffsstatistik	65
13.2.1. Methodik	65
13.3. Speicherverbrauchsstatistik	66
13.4. Datenschutz	66
14. Benutzermanager	67
14.1. Benutzergruppen	67
14.1.1. Zugriffsrechte	67
14.1.2. Administrationsrechte	68
14.2. Benutzer	68
14.2.1. Einstellungen für E-Mail und Groupware	68
14.3. Import/Export von Benutzerprofilen	69
14.3.1. Import von Benutzern	69
14.3.2. Export von Benutzern	69
15. E-Mail	70
15.1. E-Mail-Versand	70
15.1.1. Rechte	70
15.1.2. SMTP-Submission	70
15.1.3. Versandmethoden	70
15.1.4. Versand über Relayserver	70
15.1.5. Direkter Versand	71
15.2. E-Mail-Empfang auf dem Client (POP oder IMAP)	71
15.3. E-Mail-Empfang auf dem Intranator	72
15.3.1. Konzepte	72
15.3.2. Abruf einzelner POP-Konten	74
15.3.3. Direkte Zustellung per SMTP	74
15.3.4. Abruf von POP-Sammelkonten (Multidrop)	75
15.4. Weiterleitung von gesamten Domains	76
15.4.1. Konzept	76
15.4.2. Empfängeradressprüfung	77
15.4.3. Weiterleitung einzelner POP-Konten	80
15.5. E-Mail-Adressierung	80
15.5.1. Adresseinstellungen	80
15.5.2. E-Mail-Adressen und Aliases	80
15.6. E-Mail-Verarbeitung	81
15.6.1. Weiterleitung	81
15.6.2. Automatische Antwort	81
15.6.3. Sortierung	82
15.7. E-Mail-Filter	82
15.7.1. Spamfilter	82
15.7.2. Virenscanner	87
15.7.3. Anhangfilter	87
15.8. Archivierung	88
15.8.1. Schnittstelle	88
15.8.2. Anbindung des MailStore Servers	89
15.9. Automatischer Transfer	91
15.10. Verteiler	91
15.11. Weitere Einstellungen	92
15.12. Warteschlange	92
15.13. Aufbau des Mailsystems	93
15.14. Unterschiede zwischen den Lizenzen	93
16. Dienste	95
16.1. Fax	95

16.1.1. ISDN-Anschluss	95
16.1.2. Empfang	95
16.1.3. Versand	95
16.1.4. Unterschiede zwischen den Lizenzen	98
16.2. Zeitserver	98
16.3. Überwachung per SNMP	98
16.4. Fernzugriff / RAS	99
17. Systemfunktionen	100
17.1. Lizenz	100
17.1.1. Demomodus	100
17.1.2. Lizenzcode	100
17.1.3. Updatezeitraum	100
17.2. Updates	101
17.2.1. Update-Fernsteuerung via Partnerweb	101
17.3. Backup	101
17.3.1. Auslagern	102
17.3.2. Rücksichern	102
17.3.3. Vorgehen bei Festplattenschäden oder Hardwaretausch	102
17.4. Betrieb hinter einer Firewall	103
17.5. Logdateien	104
17.6. Logcheck Reports	104
17.7. Zeitgesteuertes Herunterfahren	104
3. Groupware Client	105
18. Einführung	106
18.1. Systemvoraussetzungen	106
18.2. Übersicht der Funktionen	106
18.3. Bekannte Einschränkungen	107
19. Installation	108
19.1. Installation des Programms	108
19.2. Verteilung des Programms über Active Directory	108
19.3. Grundkonfiguration mit Outlook 2013	109
19.3.1. Beheben von falsch erkannten Ordnerhierarchien	118
19.4. Grundkonfiguration mit Outlook 2010	120
19.5. Grundkonfiguration mit Outlook 2007	129
19.6. Grundkonfiguration mit Outlook 2003	136
20. Konten konfigurieren	144
20.1. Groupware-Konto	144
20.2. IMAP E-Mail-Konto	145
20.2.1. Ansicht	145
20.2.2. Abonnieren von Ordnern	146
20.2.3. Ordner für Gesendete Elemente	147
20.2.4. Behandlung von gelöschten E-Mails	150
20.3. Bestehende Daten übernehmen	152
20.3.1. Vorbereiten der Datendatei	152
20.3.2. Übernehmen der Groupwaredaten	153
20.3.3. Übernehmen der E-Mails	155
20.3.4. Datendatei schließen	156
21. Freigaben und Zugriff auf fremde Ordner	158
21.1. Eigene Ordner freigeben	158
21.1.1. Gelesen-Status gemeinsam/individuell	159
21.2. Fremde Ordner verbinden	160
21.3. Mehrere Serverkonten	162
22. Erweiterte Funktionen	163

22.1. Ordner von der Synchronisation ausschließen	163
22.2. Ordner manuell verbinden	163
22.2.1. Umstellen auf Manuelles Verbinden	164
22.2.2. Einen einzelnen Ordner verbinden	164
22.2.3. Verbindung eines Ordners aufheben	166
22.3. Posteingang/Meldungen	167
22.3.1. Ordnername	167
22.3.2. Ordnerhierarchie	167
22.4. Ordneroptionen	167
22.5. Serverseitige Einstellungen in Outlook bearbeiten	169
22.6. Synchronisationsfrequenz von E-Mails konfigurieren	170
22.7. Frei-/Gebucht-Informationen verwenden	173
22.7.1. Outlook 2013 und 2010	173
22.7.2. Outlook 2007 und Outlook 2003	174
22.8. Mehrere Absenderadressen	176
22.9. Erinnerungen und Nachverfolgen von E-Mails	177
22.10. Kennzeichnung als Privat	178
22.11. Erinnerungen in gemeinsam genutzten Ordnern	179
22.12. Festlegen des Speicherorts für IMAP-Cache-PSTs	180
22.13. Benutzerdefinierte Felder in Kontakten	180
22.14. Anzeige des Quelltextes von Objekten	181
23. Kompatibilität und Zusammenarbeit	182
23.1. Personal-Firewalls auf dem Client	182
23.2. VirensScanner auf dem Client	182
23.3. Kompatibilität mit PDAs und Mobiltelefonen	182
23.4. Sonstige Programme	183
24. Migration vom Intranator Groupware Connector	184
24.1. Wahl des Migrationsverfahrens	184
24.2. Die automatische Migration	184
24.2.1. Überblick	184
24.2.2. Die Migration in einzelnen Schritten	185
24.3. Die manuelle Migration	197
24.3.1. Überblick	197
24.3.2. Die Migration in einzelnen Schritten	198
25. Referenzinformationen	204
25.1. Synchronisierbare Daten	204
25.1.1. Aufgaben	204
25.1.2. Termine	205
25.1.3. Notizen	206
25.1.4. Kontakte	206
25.1.5. Kontaktgruppen	209
25.1.6. E-Mails	209
25.1.7. Alle Objekte	210
25.2. Erweiterte Einstellungen in der Registrierung	210
25.2.1. Einstellungen für den Store	211
25.2.2. Einstellungen für das Add-In	214
25.3. Datenformate	214
4. Web-Groupware und ActiveSync	216
26. Einführung in die Web-Groupware	217
26.1. Die Anzeigemodi	217
27. E-Mail	218
27.1. E-Mails lesen und bearbeiten	218
27.1.1. E-Mails anzeigen	218

27.1.2. Gelöschte E-Mails	218
27.1.3. E-Mails exportieren	219
27.2. E-Mails senden	220
27.2.1. Neue Nachricht	220
27.2.2. Signaturen anhängen	221
27.3. Ordner verwalten	221
27.3.1. Ordnerhierarchie	221
27.3.2. Ordner organisieren	222
27.3.3. Ordner abonnieren	222
27.3.4. Ordner freigeben	223
28. Adressbuch	225
29. Mobile Geräte per ActiveSync anbinden	226
29.1. Einführung	226
29.2. Einstellungen auf dem Server	226
29.3. Besonderheiten und Tipps	227
29.3.1. Löschen von E-Mails auf dem Server	227
29.3.2. Synchronisationsschritte	228
29.3.3. Geräte verwalten und neu synchronisieren	228
29.3.4. Synchronisieren von mehreren Kalendern oder Kontakteordnern	228
30. ActiveSync mit Android-Geräten	229
31. ActiveSync mit Apple iOS-Geräten	234
32. Referenzinformationen	238
5. Firewall	239
33. Auswahl der Firewall-Regellisten	240
33.1. Regellisten im LAN	240
33.2. Regellisten fürs Internet	240
33.3. Weg der Pakete durch die Firewall	241
33.3.1. Paketwege im LAN und Internet	241
33.3.2. Paketwege bei VPN-Verbindungen	241
34. Firewall-Profile	243
34.1. Basis-LAN Grundregeln	243
34.2. Rechnerprofile	243
34.3. Providerprofile	244
35. Vollständige Regellisten	245
35.1. Komponenten	245
35.1.1. Dienste	245
35.1.2. Netzgruppen	245
35.1.3. Automatische Objekte	246
35.2. Regellisten	246
35.2.1. Grundeinstellungen	246
35.2.2. Durchlaufen der Regelliste	247
35.2.3. Verknüpfung der Regel-Kriterien	247
35.2.4. Die Aktionen	248
35.2.5. Extra-Optionen	248
35.2.6. Besonderheiten bei Provider-Regellisten	250
36. Weitere Funktionen	251
36.1. MAC-Adressen überprüfen	251
36.2. Spoofing im LAN verhindern	251
36.3. Blockieren von IPs nach zu vielen Loginfehlern	251
36.4. Firewall-Notmodus	251
37. Fallbeispiele und Aufgaben	252
37.1. Aufgabe 1: Erweitern eines einfachen Rechnerprofils	252

37.1.1. Musterlösung	252
37.2. Aufgabe 2: Oberfläche nur für eine externe IP erreichbar	253
37.2.1. Musterlösung	253
37.3. Aufgabe 3: Separiertes Gästenetz	254
37.3.1. Musterlösung	254
37.4. Aufgabe 4: Beschränkter Zugang aus dem VPN	255
37.4.1. Musterlösung	256
37.5. Aufgabe 5: Webserver in der DMZ	257
37.5.1. Musterlösung	257
6. VPN	258
38. IPSec Grundlagen	259
38.1. IPSec	259
38.2. Public-Key Kryptographie	259
38.3. Zertifikate	259
38.4. IPSec Verbindungen	260
38.5. Algorithmen	260
38.6. Einschränkungen	261
38.7. Kompatibilität mit anderen IPSec-Gegenstellen	261
39. Schlüsselmanagement	262
39.1. Eigene Schlüssel	262
39.1.1. Zertifizierungsstellen (CAs)	262
39.2. Fremde Schlüssel	263
40. Anbinden von einzelnen PCs	264
40.1. Konzept	264
40.2. Konfiguration auf dem Intranator	264
40.2.1. Voraussetzungen	264
40.2.2. Grundeinstellungen	265
40.2.3. Authentifizierung	265
40.2.4. Tunnel konfigurieren	266
40.2.5. Rechte	267
40.2.6. Aktivierung	268
41. VPN mit dem NCP Secure Entry Client	269
41.1. Installation	269
41.2. Zertifikate	269
41.3. Verbindungen	272
41.4. Intranator	277
42. VPN mit dem Shrew Soft VPN Client	278
42.1. Zertifikate	278
42.2. Verbindung im Client konfigurieren	279
42.3. Intranator	283
42.4. Verbindung aufbauen	283
42.5. Verbindungsprotokolle	284
43. VPN mit dem NetGear ProSafe Client	286
43.1. Kompatibilität	286
43.2. Installation	287
43.3. Zertifikate	287
43.4. Verbindungen	290
43.5. Intranator	293
44. VPN mit Mac OS X	294
44.1. Installation	294
44.2. Zertifikate erzeugen	294
44.3. Zertifikate importieren	295
44.4. Verbindungen konfigurieren	297

44.5. Intranator	300
45. VPN mit dem Apple iPhone	301
45.1. Zertifikat für das iPhone	301
45.2. Zertifikat für den Intranator	304
45.3. Verbindung auf dem Intranator	307
45.4. Verbindung auf dem iPhone	307
46. VPN mit Android	310
46.1. Gerät vorbereiten	310
46.2. Zertifikate	311
46.3. Verbindung auf dem Intranator	314
46.4. Verbindung auf Android	315
46.5. Verbindundsaufbau vereinfachen	317
46.6. Verbindungsprotokolle	319
47. VPN mit dem NCP Client für Windows Mobile	321
47.1. Installation	321
47.2. Zertifikate	321
47.3. Verbindungen	325
47.4. Intranator	329
48. VPN mit dem NCP Client für Symbian	330
48.1. Installation	330
48.2. Zertifikate	330
48.3. Verbindungen	333
48.4. Intranator	337
49. Anbinden von kompletten Netzen	338
49.1. Konzept	338
49.2. Konfiguration auf dem Intranator	339
49.2.1. Voraussetzungen	339
49.2.2. Grundeinstellungen	339
49.2.3. Authentifizierung	339
49.2.4. Tunnel konfigurieren	340
49.2.5. Rechte	340
49.2.6. Aktivierung	340
50. VPN mit ZyXEL ZyWALL Routern	341
50.1. Überblick	341
50.2. Vorbereitung	341
50.3. Installieren des Intranator-Zertifikats	342
50.4. Erzeugen und Installieren des Router-Zertifikats	342
50.5. Konfiguration der VPN-Verbindung	344
50.6. Intranator	347
51. VPN mit ZyXEL ZyWALL USG	348
51.1. Überblick	348
51.2. Vorbereitung	348
51.3. Zertifikate	349
51.4. Verbindung	352
51.4.1. IKE / Phase 1	352
51.4.2. IPSec / Phase 2	353
51.5. Intranator	356
51.6. Logs	356
52. VPN mit Lancom Routern	357
52.1. Überblick	357
52.2. Zertifikat für das Lancom-Gerät	357
52.3. Zertifikat für den Intranator	359
52.4. Verbindung	360

52.5. Intranator	366
52.6. Zertifikate löschen	366
53. VPN mit Linux	367
53.1. Überblick	367
53.2. Zertifikate erzeugen	367
53.3. Verbindungen konfigurieren	368
53.4. Intranator	370
54. Lösen von IP-Adresskonflikten in VPNs durch NAT	371
54.1. Das Problem	371
54.2. Konfiguration	371
54.3. Gleiche IPs in LAN und auf der Gegenseite	372
54.3.1. Umsetzung	373
54.4. Mehrere Gegenstellen mit gleichen IPs	373
54.4.1. Umsetzung	374
54.5. Lokale IPs festgelegt durch Fernwartungs-Dienstleister	374
54.5.1. Umsetzung	375
55. Fehlerdiagnose	376
55.1. Logs lesen	376
55.2. Das Protokollformat des Intranators	376
55.3. Fehler in Phase 1	376
55.4. Fehler in Phase 2	377
7. Anhang	379
A. Lizenzen	380
A.1. Intranator Software Lizenzvertrag	380
A.2. Lizenzierte Software	385
B. Lizenz	387
B.1. Intra2net Groupware Client Lizenzvertrag (EULA)	387
Index	391

Teil 1. Installation

1. Kapitel - Willkommen

Willkommen zum Intranator, der anwenderfreundlichen Lösung, um Ihr Netzwerk mit geringem Aufwand und maximaler Sicherheit an das Internet anzubinden. Intranator regelt die Zugriffsrechte Ihrer einzelnen Arbeitsplätze, verschickt und verwaltet die E-Mail des Teams und ermöglicht es, den Internetzugang jederzeit frei zu wählen, ohne fest an einen Zugangsprovider gebunden zu sein. Alles einfach, alles sicher.

1.1. Über dieses Handbuch

Dieses Handbuch beschreibt die komplette Administration des Intranators von der Installation an bis hin zu seltener benötigten Spezialfunktionen.

1.2. Werkseinstellungen

Im Folgenden sind für erfahrene Benutzer die Werkseinstellungen kurz zusammengefasst. Was diese Werte genau bedeuten und wie sie verändert werden können, wird in den folgenden Kapiteln sowie im Teil 2, „Allgemeine Funktionen“ erklärt.

IP Adresse	192.168.1.254
Netzmaske	255.255.255.0
DNS-Name	intranator
Domain	net.lan
DHCP	aktiviert
DHCP IP-Pool	192.168.1.200 bis 192.168.1.250
HTTP-Proxy	Port 3128
Oberfläche nur über SSL erreichbar	aktiviert
Administrator Login	admin
Administrator Passwort	admin
Backup erstellen	täglich um 02:00 Uhr
Backup-Zugriffsschutz	aktiv, setzen Sie das Passwort unter System > Backup > Einstellungen
E-Mail-VirensScanner	aktiv
E-Mail-Anhangfilter	aktiv für ausführbare Dateien

Achtung



Bitte ändern Sie Login und Passwort nach dem ersten Gebrauch!

2. Kapitel - Installation auf eigener Hardware

2.1. Hardwareauswahl

Die Mindestanforderungen des Intranators an die Hardware sind wie folgt:

- x86-kompatibler Prozessor mit mindestens 2 GHz Taktfrequenz
- Mindestens 2 GB Hauptspeicher (für den Intranator Business Server)
- Mindestens 1 GB Hauptspeicher (für das Intranator Security Gateway und Intranator Network Security)
- Festplatte mit mindestens 40 GB Speicherkapazität
- Zwei Netzwerkkarten
- Ein CD-ROM Laufwerk (nur während der Installation benötigt)

Genauere Details zur unterstützten Hardware finden Sie im Internet unter
http://www.intra2net.com/de/support/unterstuetzte_hardware.php.



Wir empfehlen, nur Komponenten bzw. Komplettgeräte zu verwenden, die dort als "zertifiziert" gelistet sind. Intra2net garantiert dafür heute und auch für zukünftige Intranator-Versionen eine optimale Kompatibilität.

2.2. Installation als virtuelle Maschine

Der Intranator kann auch als virtuelle Maschine installiert werden. Als Virtualisierungsplattform werden insbesondere VMWare vSphere Hypervisor (ESXi) und Microsoft Hyper-V unterstützt. Eine genaue Liste der unterstützten Virtualisierungsplattformen finden Sie im Internet unter
http://www.intra2net.com/de/support/unterstuetzte_hardware.php.



Bei der Installation als virtuelle Maschine sind einige Besonderheiten zu beachten. Diese betreffen vor allem die Sicherheit bei der Funktion als Firewall. Hintergründe dazu sowie eine genaue Anleitung finden Sie ab dem 4. Kapitel, „Installation als virtuelle Maschine“.

2.3. Standort

Stellen Sie den Intranator in einen Bereich mit kontrollierbarem Zugang (z.B. abschließbarer Raum), da es bei physischem Zugriff mit ausreichenden Systemkenntnissen und etwas Zeit möglich ist, den Intranator zu kompromittieren.

Beachten Sie unbedingt die Vorgaben des Hardwareherstellers bezüglich maximaler Umgebungstemperatur und Luftzufuhr. Die meisten Geräte dürfen nicht bei einer Umgebungstemperatur von mehr als 30 °C oder 35 °C betrieben werden.

2.4. BIOS

Im BIOS-Setup sollten vor der Installation des Intranators einige Einstellungen vorgenommen werden. Da das BIOS-Setup bei jedem Hersteller etwas anders aufgebaut ist, sind in der folgenden Tabelle die gängigsten Namen für die nötigen Optionen aufgeführt.

Installieren Sie den Intranator auf einem zertifizierten Server von HP, so finden Sie Hinweise auf die nötigen BIOS-Einstellungen auf dieser Webseite:
http://www.intra2net.com/de/support/server_systeme.php.



Datum und Uhrzeit	Sollte in etwa stimmen (ca. +-10 Min.), da der Intranator bei der Installation ein zeitabhängiges Zertifikat anlegt. Sobald eine Internetverbindung besteht, wird die Zeit über NTP genau gestellt.
IEEE 1394 oder Firewire	Verfügt das System über einen Firewire/IEEE 1394-Port, sollte dieser deaktiviert werden. Über einen aktiven Port lässt sich der komplette Speicherinhalt eines laufenden Systems auslesen und manipulieren. Dies stellt ein Sicherheitsrisiko dar, daher sollte der Port abgeschaltet werden.
Restore on AC Power Loss oder AC Back Function	Auf "On" oder "Full-On". Damit startet der Intranator nach einem Stromausfall oder Herunterfahren durch die USV von selbst. Diese Option finden Sie meistens unter Power Management, Boot Options oder einem ähnlich benannten Menü.
Virtual Install Disk oder Virtual Driver Disk	Einige Serversysteme bieten mit dieser Option ein virtuelles Laufwerk an, welches Treiber für das System oder den RAID-Controller enthält und dadurch die Installation von Windows oder VMWare vereinfachen soll. Schalten Sie diese Option ab, da durch sie die Festplattenerkennung des Intranators gestört werden kann.
Wake on PCI device oder Resume by PCI-E device	Muss für zeitgesteuertes Herunterfahren (siehe Abschnitt 17.7, „Zeitgesteuertes Herunterfahren“) aktiviert sein.



2.5. RAID

Wenn Sie einen RAID-Controller einsetzen, klären Sie zuerst, ob es sich um einen Hardware-RAID-Controller oder um einen Software-RAID-Controller (auch BIOS-RAID oder Host-RAID genannt), handelt. Controller mit eigenem Pufferspeicher (evl. auch mit Pufferbatterie) sind normalerweise Hardware-RAID. Die meisten billigeren oder auf dem Mainboard integrierten SATA-Controller sind dagegen Software-RAID.

Wenn Sie einen Hardware-RAID-Controller einsetzen, verwenden Sie dessen BIOS, um ein für den Intranator geeignetes Volume anzulegen.

Wenn Sie einen Software-RAID-Controller einsetzen, konfigurieren Sie in dessen BIOS keine RAID-Funktionen oder deaktivieren am besten das BIOS des Controllers gleich ganz in dem Sie den Festplattenzugriff auf AHCI stellen. Ziel ist, dass der Intranator die einzelnen Platten separat ansprechen kann. Diese Konfiguration wird häufig auch JBOD genannt. Nach der Installation des Intranators auf die erste Festplatte können Sie in der Webober-

fläche über das Menü System > Hardware > RAID einen RAID-Verbund mit der zweiten Platte anlegen.

2.6. Installation von CD

Der Intranator bringt ein vollständiges Betriebssystem auf Linux-Basis mit. Er kann nicht parallel mit anderen Betriebssystemen auf dem selben Gerät installiert werden. Möchten Sie dennoch weitere Software auf der selben Hardware mitnutzen, setzen Sie dafür eine Virtualisierungslösung ein.

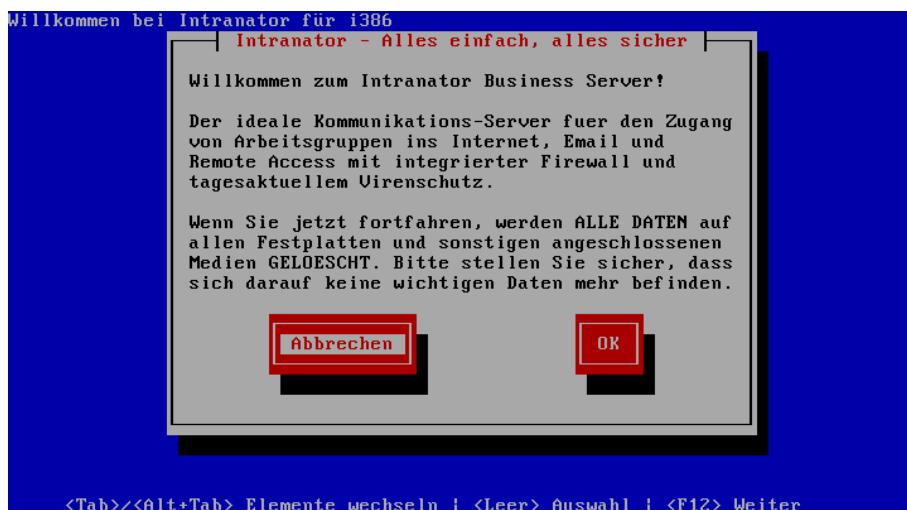
Starten Sie den Rechner von der beiliegenden Intranator Installations-CD. Sie können sowohl ein eingebautes CD- oder DVD-Laufwerk als auch ein per USB angeschlossenes dafür verwenden.

Nach dem erfolgreichen Start von der CD werden Sie aufgefordert, die Installation zu starten.



Achtung

Wenn Sie die Installation starten, werden alle Daten auf den angeschlossenen Festplatten des Rechners überschrieben. Stellen Sie daher vor der Installation sicher, dass alle Festplatten gefahrlos gelöscht werden können.



Wenn die Installation erfolgreich abgeschlossen ist, werden Sie aufgefordert, den Rechner neu zu starten. Die CD wird ausgeworfen, entfernen Sie sie dann aus dem Laufwerk. Der Rechner startet danach von der Festplatte den Intranator. Der Intranator startet in die Installationskonsole, beschrieben im 7. Kapitel, „Die Konsole“.

2.7. Lösen von Kompatibilitätsproblemen

Sollte das Installationsprogramm von der CD gar nicht erst starten oder während der Installation abbrechen, haben Sie es vermutlich mit einem Kompatibilitätsproblem zwischen Hardware und Intranator zu tun.

Versuchen Sie als erstes, ein BIOS-Update vom Hersteller des Rechners oder Mainboards zu bekommen und zu installieren. Prüfen Sie auch unter <http://www.intra2net.com>, ob Sie die neueste Version der Intranator Installations-CD verwenden.

Sollte dies keinen Erfolg bringen, versuchen Sie im BIOS-Setup Optionen wie ACPI und APIC zu finden und anders einzustellen. Bringt auch das keinen Erfolg, können Sie den Intranator im abgesicherten Modus starten. Gehen Sie dafür wie folgt vor:

1. Booten Sie von der Intranator Installations-CD.
2. Es wird das Bootmenü mit einem stilisierten Intranator-Logo angezeigt.
3. Sie haben jetzt 5 Sekunden Zeit, am Systemprompt **safe** einzugeben und mit Return zu starten.
4. Das Installationsprogramm startet jetzt im abgesicherten Modus.

Dadurch wird das Powermanagement des Intranators deaktiviert. Dies hat zur Folge, dass das System etwas mehr Strom benötigt und sich beim Herunterfahren nicht selbst abschalten kann. Wird das System beim ersten erfolgreichen Start nach der Installation im abgesicherten Modus hochgefahren, wird dieser auch bei späteren Starts aktiviert.

3. Kapitel - Installation der Appliance

3.1. Lieferumfang

3.1.1. Intranator Appliance Eco

Folgendes ist enthalten:

- Intranator Appliance Eco
- Netzteil für 100-240 VAC, 50/60Hz
- Ein Stromkabel mit Kaltgerätestecker
- 4 Gummifüße
- Ein Netzwerkkabel
- Das Installationshandbuch "Erste Schritte"

Ein Rackmountkit ist unter Artikelnummer I2N-AEC-120 optional erhältlich.

Zum Betrieb des Geräts ist unbedingt ein Lizenzcode eines der Intranator Serverprodukte erforderlich. Dieser muss separat erworben werden. Den Lizenzcode finden Sie auf dem Lizenzzertifikat, welches Sie beim Kauf einer Intranator Lizenz erhalten.

3.1.2. Intranator Appliance Pro

Folgendes ist enthalten:

- Intranator Appliance Pro im Rack-fähigen Gehäuse mit 2 Höheneinheiten
- Ein Rackmountkit bestehend aus 2 Bügeln und 8 Schrauben
- 4 Gummifüße für den Betrieb außerhalb eines Racks
- Ein Stromkabel mit Kaltgerätestecker
- Ein Netzwerkkabel
- Das Installationshandbuch "Erste Schritte"

Eine ISDN-Karte zur Nutzung der Faxfunktion ist unter Artikelnummer I2N-APR-120 optional erhältlich.

Zum Betrieb des Geräts ist unbedingt ein Lizenzcode eines der Intranator Serverprodukte erforderlich. Dieser muss separat erworben werden. Den Lizenzcode finden Sie auf dem Lizenzzertifikat, welches Sie beim Kauf einer Intranator Lizenz erhalten.

3.1.3. Intranator Appliance Ultimate

Folgendes ist enthalten:

- Intranator Appliance Ultimate im Rack-Gehäuse mit einer Höheneinheit
- Ein Satz Schienen zur Befestigung im Rack

- Ein Stromkabel mit Kaltgerätestecker
- Ein Netzwerkkabel
- Das Installationshandbuch "Erste Schritte"

Zum Betrieb des Geräts ist unbedingt ein Lizenzcode eines der Intranator Serverprodukte erforderlich. Dieser muss separat erworben werden. Den Lizenzcode finden Sie auf dem Lizenzzertifikat, welches Sie beim Kauf einer Intranator Lizenz erhalten.

3.2. Standort

Stellen Sie den Intranator in einen Bereich mit kontrollierbarem Zugang (z.B. abschließbarer Raum), da es bei physischem Zugriff mit ausreichenden Systemkenntnissen und etwas Zeit möglich ist, den Intranator zu kompromittieren.

Stellen Sie Ihren Intranator auf eine feste, ebene Fläche oder montieren ihn in ein passendes Rack. Vor und hinter dem Gerät, sowie rechts und links vorne, muss ausreichend Freiraum vorhanden sein, um die Zirkulation der Luft zu gewährleisten. Die Lüftungsöffnungen dürfen auf keinen Fall verdeckt sein.

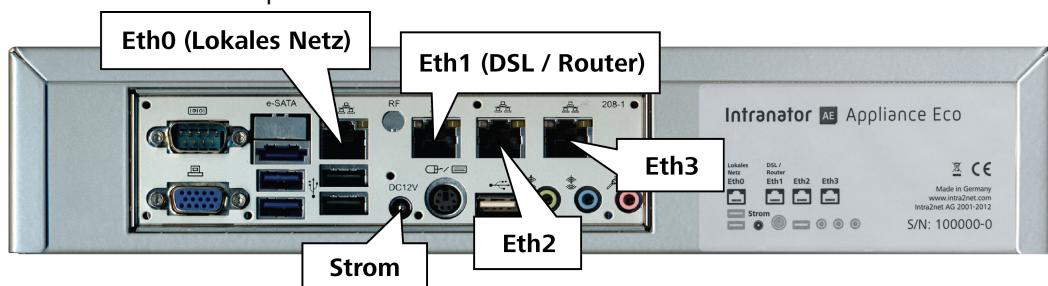


Achtung

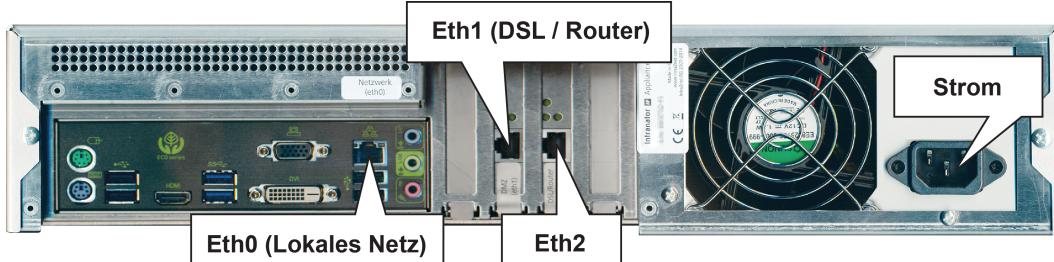
Die Umgebungstemperatur des Geräts darf im Betrieb auch kurzzeitig niemals 35 °C übersteigen.

3.3. Anschlüsse

Die Anschlüsse für LAN, ISDN und DSL und Strom befinden sich auf der Rückseite des Gerätes und sind entsprechend beschriftet.



Rückseite Intranator Appliance Eco



Rückseite Intranator Appliance Pro

3.4. Software

Die Intranator-Software ist auf der Appliance bereits gebrauchsfertig installiert.

4. Kapitel - Installation als virtuelle Maschine

4.1. Vergleich mit echter Hardware

Virtualisierungssysteme bringen im Vergleich zur Installation auf echter Hardware einige Vorteile wie z.B. Hardware-Konsolidierung, Energiesparen oder bessere Ausfallsicherheit durch Migrationsmöglichkeiten mit sich. Gleichzeitig kommt es allerdings auch zu den im Folgenden beschriebenen Nachteilen.

4.1.1. Ungleichmäßige Ausführungsgeschwindigkeit

Das Betriebssystem kann nicht mehr selbst entscheiden, welche Prozesse wann genau ausgeführt werden sollen, denn die Virtualisierungslösung kann die Ausführung des gesamten virtualisierten Systems anhalten oder verzögern.

Das Faxprotokoll G3 schreibt aber genaue Antwortzeiten vor. Da das virtualisierte System den Faxprozess nicht mehr entsprechend priorisieren und steuern kann, wird das Protokoll verletzt.

Daher ist Faxen auf einer virtuellen Maschine generell nicht möglich.

4.1.2. Geringere I/O-Performance

Das Betriebssystem kann nicht mehr direkt auf die Hardware von Netzwerkkarten oder Speichersystemen zugreifen, sondern muss hierfür auf eine Funktion der Virtualisierungslösung zugreifen. Dafür muss mehrfach zwischen Gast und Wirt umgeschaltet werden. Dies verringert nicht nur den maximal möglichen Durchsatz, sondern erhöht vor allem die Latenz.

Sind die Festplatten nicht lokal auf dem Virtualisierungsserver installiert, sondern z.B. über ein SAN angebunden, kommt noch die Latenz für den Transfer über das SAN hinzu. Auf verschiedenen SAN-Lösungen können aber sehr unterschiedliche Latenzzeiten beobachtet werden. Lösungen, die auf iSCSI basieren, tendieren eher zu hohen Latenzzeiten. Lösungen mit Fibre Channel oder FCoE (Fibre Channel over Ethernet) tendieren eher zu besseren Latenzzeiten. Durch zusätzliche Schichten wie z.B. Storage-Virtualisierung können noch zusätzliche Latzenzen hinzukommen.

Die meisten Aufgaben eines Intranators werden typischerweise durch die Latenz von Festplattenzugriffen beschränkt und nicht durch Festplattendurchsatz oder fehlende CPU-Leistung. Dieser Punkt kann die Leistung eines Intranators also merklich beeinträchtigen.

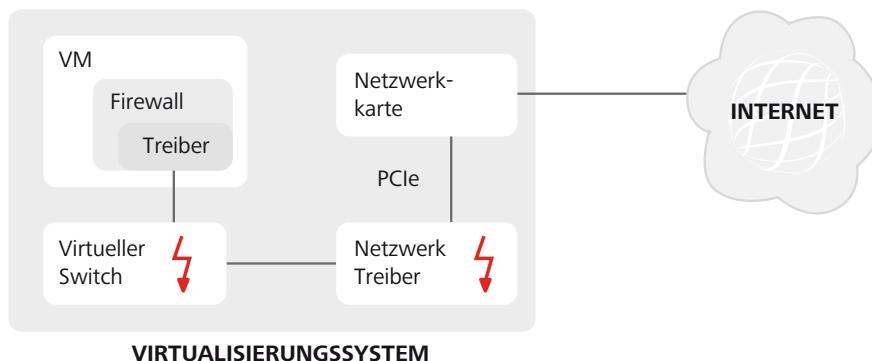
Wir empfehlen, dies durch den Einsatz schnellerer Festplatten (15.000 RPM) oder Solid-State-Disks zu kompensieren.

Außerdem empfehlen wir das virtuelle Laufwerk für den Intranator nicht als dynamisch wachsend / bei Bedarf zugeteilt zu konfigurieren, sondern von Anfang an vollständig zuzuweisen und zu allozieren. Wenn das Laufwerk erst bei Bedarf wächst, kostet dies Performance bei Schreibzugriffen. Außerdem werden zusätzliche Verwaltungsinformationen benötigt, die vor einem Zugriff erst abgerufen und danach evtl. angepasst werden müssen. Bei klassischen Festplatten werden durch die ungleichmäßige Aufteilung der Blöcke zusätzliche Repositionierungen der Schreib-/Leseköpfe benötigt.

4.1.3. Kontakt mit ungefilterten Netzwerkpaketen

Wird der Intranator als Router und Firewall eingesetzt und stellt damit die Verbindung zum Internet her, kommt er direkt mit Netzwerkpaketen aus dem Internet in Berührung. Der Intranator ist dafür konzipiert und kann mit nicht standardkonformen oder gar bösartigen Paketen korrekt umgehen. Auch werden evtl. erkannte Lücken in den Treibern oder Funktionen zeitnah durch Updates geschlossen.

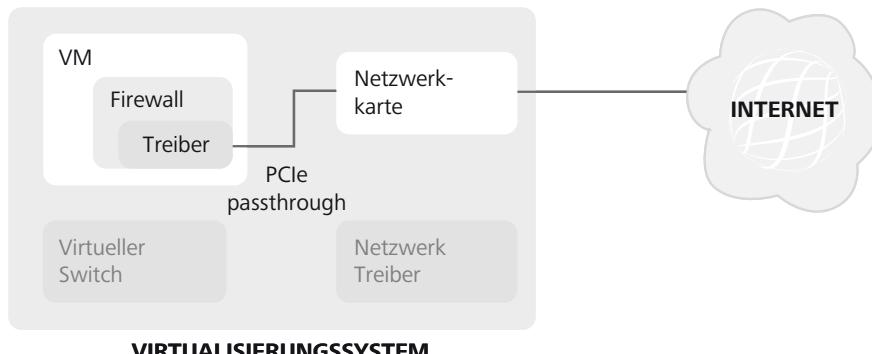
Wird der Intranator als virtuelle Maschine betrieben und seine Netzwerkkarten über die regulären Netzwerkfunktionen eines Virtualisierungssystems verwaltet, dann wird das Virtualisierungssystem diesen Paketen ungefiltert ausgesetzt. Dies gilt normalerweise für den Netzwerkkartentreiber und den virtuellen Switch.



Virtualisierungssysteme sind in der Regel nicht als Firewall konzipiert. Daher werden Updates der Treiber für die Netzwerkkarten und den virtuellen Switch nicht so kritisch eingestuft und dementsprechend weniger schnell verteilt und eingespielt. Dies erhöht letztendlich das Risiko von Störungen oder Angriffen.

Wir raten daher dringend davon ab, Netzwerkkarten, die direkt mit dem Internet verbunden sind, über die regulären Netzwerkfunktionen des Virtualisierungssystems (typischerweise virtuelle Switches) anzubinden.

Stattdessen empfehlen wir, die entsprechenden Netzwerkkarten als komplette PCI-Geräte an die virtuelle Maschine durchzurichten. Der Intranator steuert damit die Hardware über PCI-Zugriffe direkt an und die Virtualisierungslösung kommt gar nicht erst mit diesen Netzwerkpaketen in Berührung.



Achtung



Beachten Sie, dass diese Funktion nicht von allen Virtualisierungssystemen angeboten wird und auch dann nur mit Unterstützung der Hardware (Intel

VT-d bzw. AMD-Vi in Prozessor und Chipsatz sowie passenden Beschreibungstabellen im BIOS) verfügbar ist. Prüfen Sie daher bereits in der Planungsphase die Kompatibilität.

Außerdem ist beim Durchreichen von kompletten PCI-Geräten in der Regel keine Live-Migration der VM mehr möglich. Eine VM muss daher vor einer Migration auf eine andere Hardware erst heruntergefahren werden.

Verwenden Sie alternativ eine zusätzliche Hardware-Firewall oder installieren den Intranator nicht als virtuelle Maschine, sondern auf dedizierter Hardware.

5. Kapitel - Installation auf VMware vSphere Hypervisor™ 4 (ESXi)

Für die Basis-Virtualisierungsplattform VMware vSphere Hypervisor™ (früher VMware ESXi™) wird unter dieser URL eine dauerhafte, kostenlose Lizenz angeboten: <http://www.vmware.com/go/get-free-esxi>.

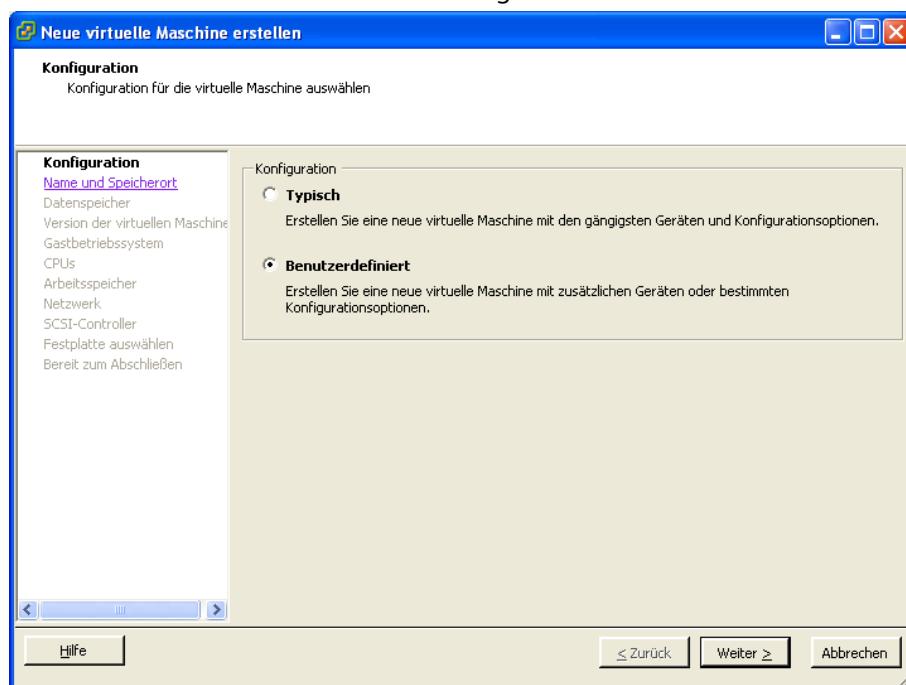
Für weitergehende Management- und Überwachungsfunktionen benötigen sie kostenpflichtige Lizenzen. Eine Übersicht über die verschiedenen Produkte finden Sie unter Compare vSphere Editions [<http://www.vmware.com/products/vsphere/compare.html>].

Der Intranator enthält von Haus aus alle Treiber und Programme, die für den zuverlässigen Betrieb auf VMware vSphere Hypervisor™ 4 nötig sind. Dies sind der paravirtualisierte Netzwerktreiber (VMXNET 3), der paravirtualisierte SCSI-Treiber (pvscsi) sowie die open-vm-tools. Eine zusätzliche Installation der VMware Tools oder anderer Treiber oder Programme ist nicht notwendig.

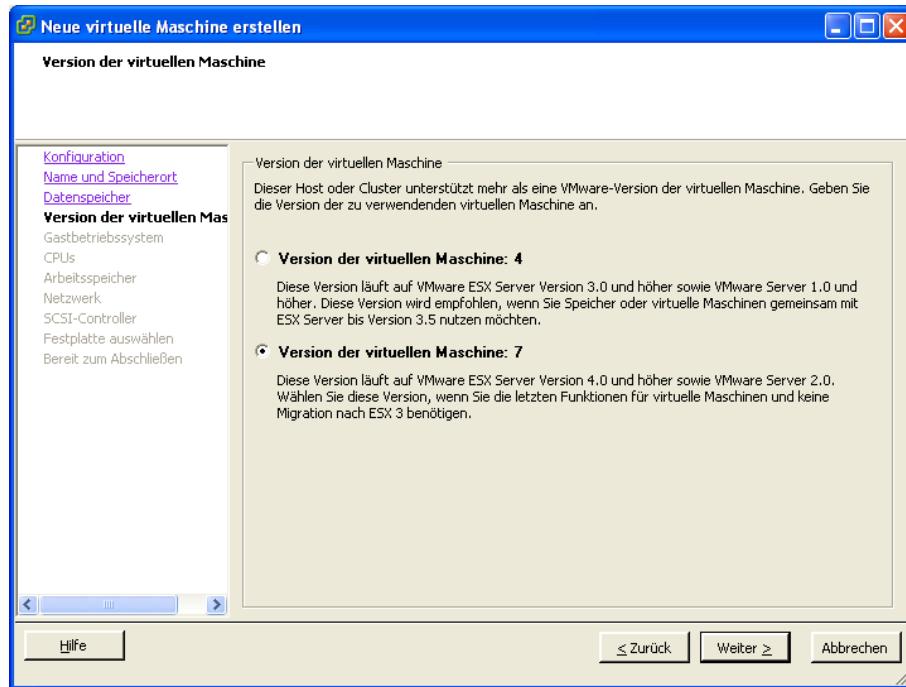
5.1. Konfiguration der virtuellen Maschine

Gehen Sie für die Installation einer virtuellen Maschine wie folgt vor:

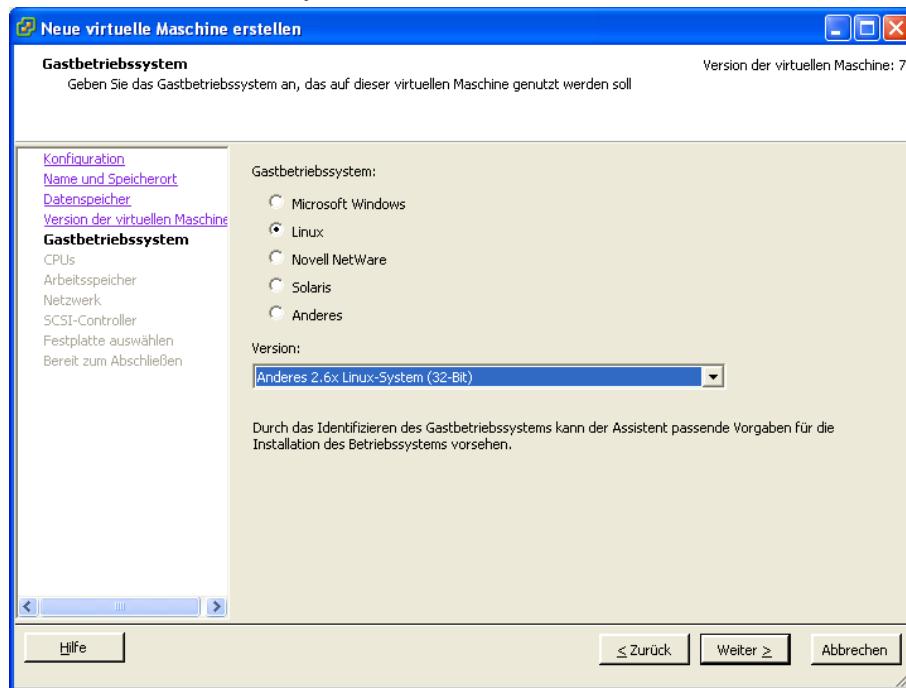
1. Starten Sie den vSphere Client, verbinden sich mit dem vSphere-Server und legen eine neue VM an.
2. Wählen Sie die benutzerdefinierte Konfiguration.



3. Benennen Sie die VM und weisen einen passenden Datenspeicher zu.
4. Wählen Sie eine virtuelle Maschine der Version 7

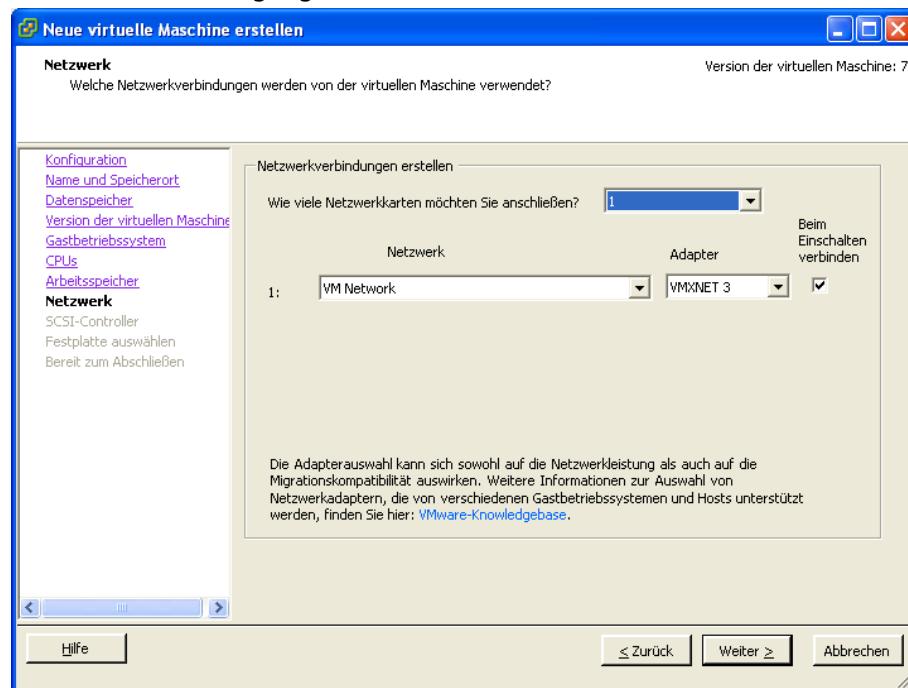


5. Wählen Sie als Betriebssystem ein Anderes 2.6x Linux (32-Bit).

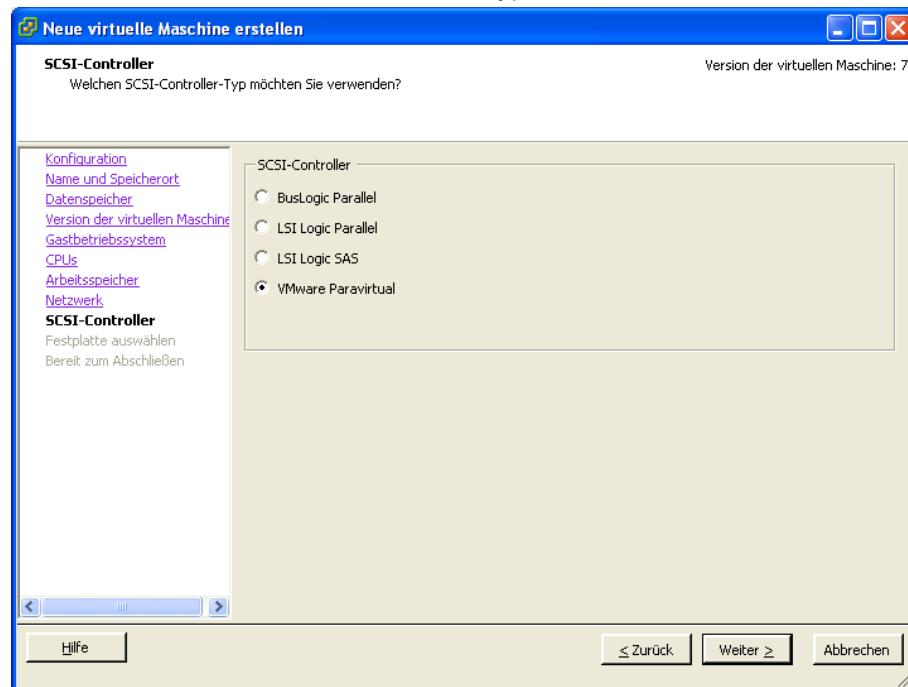


6. Geben Sie für den Intranator eine oder mehr CPUs frei. Der Intranator erkennt beim Start automatisch die Anzahl der verfügbaren CPUs und nutzt diese.
7. Geben Sie für den Intranator genügend Arbeitsspeicher frei. Wir empfehlen mindestens 2 GB bis 50 Benutzer, darüber entsprechend mehr.
8. Schließen Sie Netzwerkkarten des Typs VMXNET 3 an. Die Anzahl hängt vom Layout des lokalen Netzes und dem Einsatzzweck des Intranators ab.

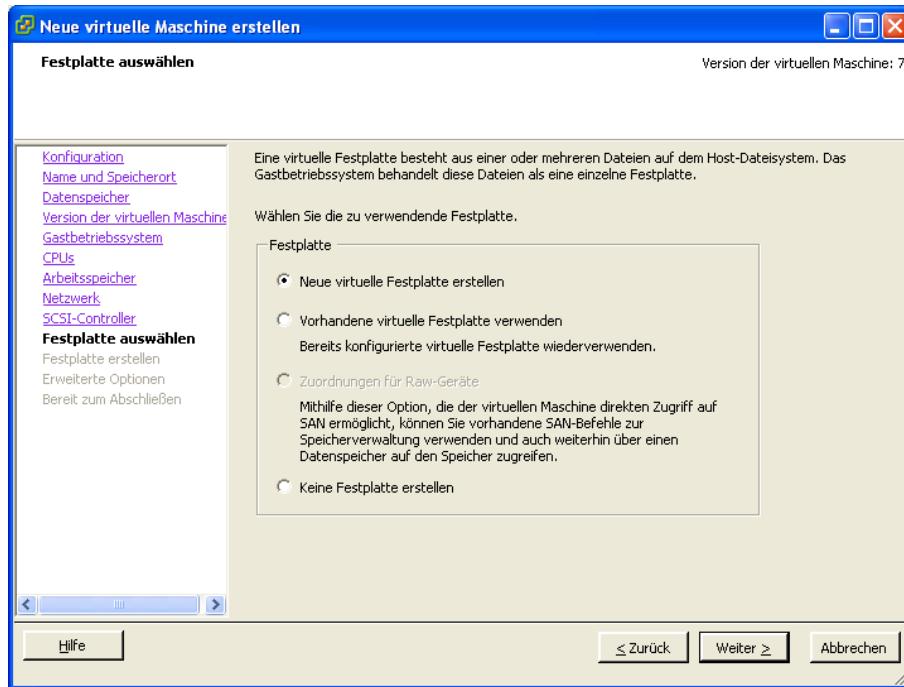
Es wird dringend davon abgeraten, direkt mit dem Internet verbundene Netzwerkkarten auf diese Weise anzubinden. Beachten Sie dazu Abschnitt 5.2, „Virtuelle Maschine mit direktem Internetzugang“.



9. Wählen Sie einen SCSI-Controller vom Typ VMware Paravirtual.



10. Legen Sie eine neue virtuelle Festplatte an.

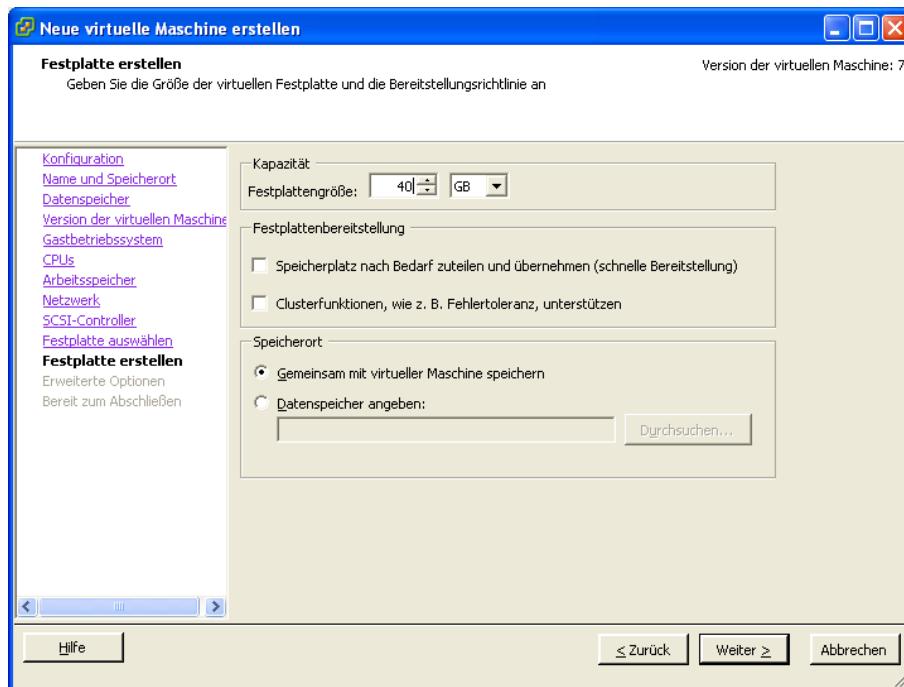


11. Weisen Sie dem Intranator eine Festplatte von mindestens 40 GB zu. Wird der Intranator nur zum Scannen von E-Mails und als HTTP-Proxyserver eingesetzt, reichen diese 40 GB im Normalfall auch aus. Nur wenn umfangreiche Statistikdaten für viele Benutzer längerfristig gespeichert werden sollen, wird mehr Speicher benötigt.

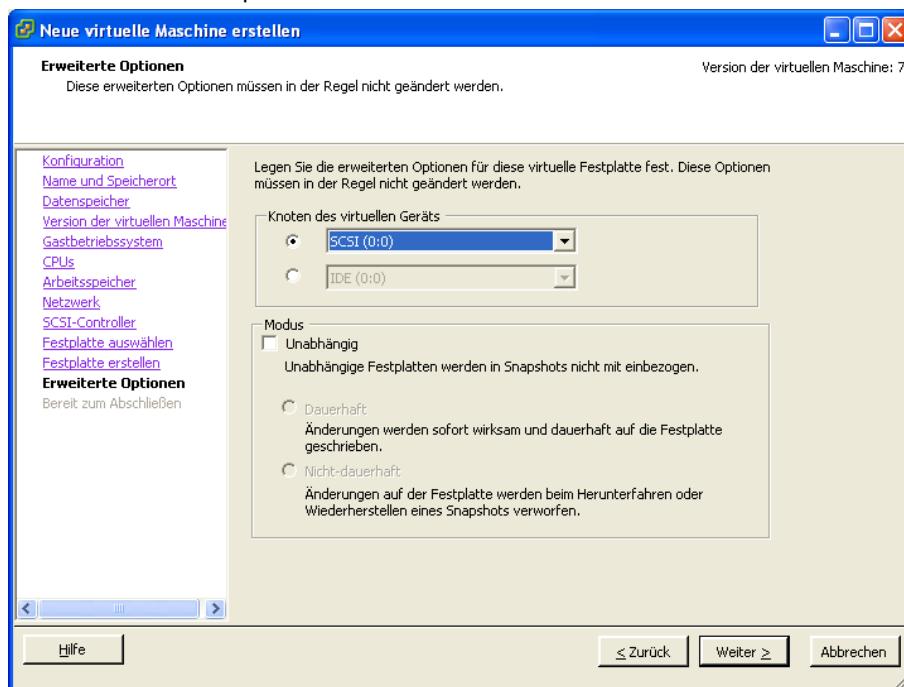
Werden E-Mails oder Groupwaredaten dauerhaft auf dem Intranator abgelegt, wird mehr Festplattenplatz benötigt. Als Faustformel gilt Folgendes: (Gesamtes E-Mail-Volumen aller Benutzer + Statistikdaten) * (Anzahl auf dem System gespeicherter Backupsätze + 2) + 20 GB. Die Anzahl auf dem System gespeicherter Backupsätze beträgt dabei mindestens 1, empfohlen wird 2.

Kalkulieren Sie immer etwas Reserve ein, da ein Vergrößern der Festplatte im Betrieb derzeit nicht unterstützt wird.

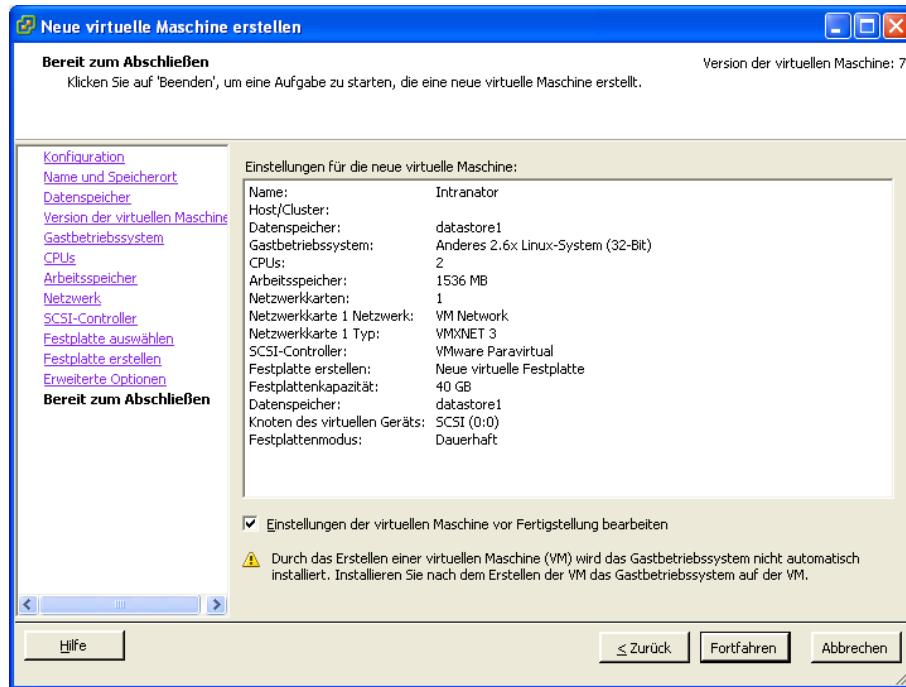
Weisen Sie dem Intranator die gesamte Festplattenkapazität sofort zu, da dies in der Regel zu schnelleren Zugriffszeiten führt.



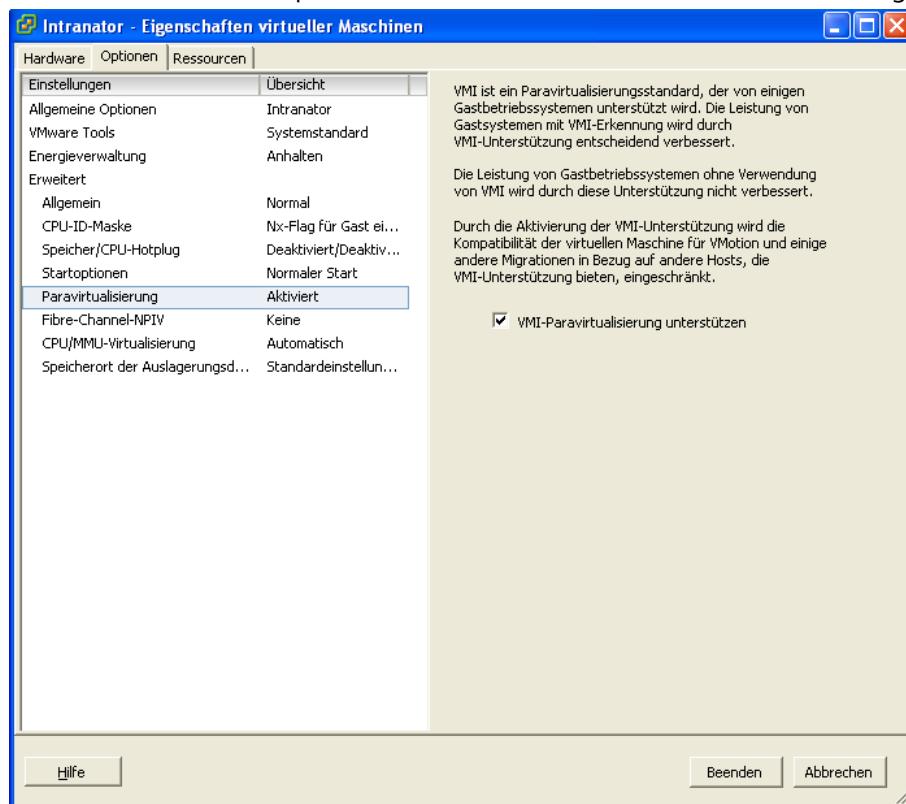
12 Weisen Sie die Festplatte auf Knoten SCSI(0:0) zu.



13. Bearbeiten Sie die Einstellungen vor der Fertigstellung.



14. Öffnen Sie das Menü Optionen und aktivieren die VMI-Paravirtualisierung.



5.2. Virtuelle Maschine mit direktem Internetzugang

Wie in Abschnitt 4.1.3, „Kontakt mit ungefilterten Netzwerkpaketen“ beschrieben, empfehlen wir, Netzwerkkarten, die direkt mit dem Internet verbunden sind, als komplette PCI-Geräte an die VM durchzurichten.

Diese Funktionalität wird VMDirectPath genannt und benötigt die Unterstützung durch Prozessor, Mainboard und BIOS. Von Intel wird dies VT-d genannt, bei AMD heißt es AMD-Vi oder IOMMU. Diese Funktionen sind meist nur bei Serversystemen implementiert, bei für den Desktop-Einsatz konzipierten Rechnern fehlt häufig eine vollständige Unterstützung durch alle Komponenten. Weitere Informationen dazu finden Sie bei VMware und Ihrem Hardwarehersteller.

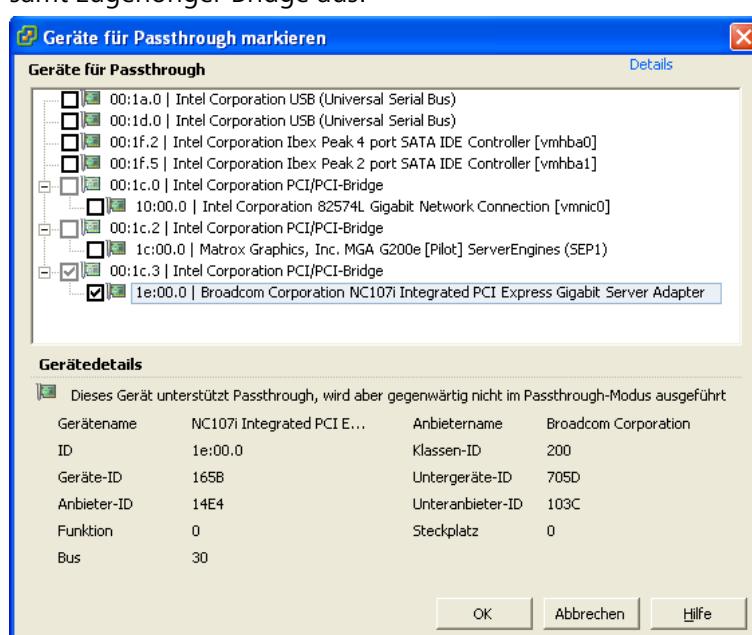
5.2.1. Vorbereitung des Servers

Bevor eine Netzwerkkarte direkt an eine VM übergeben werden kann, muss Sie im VMware-Server freigegeben werden:

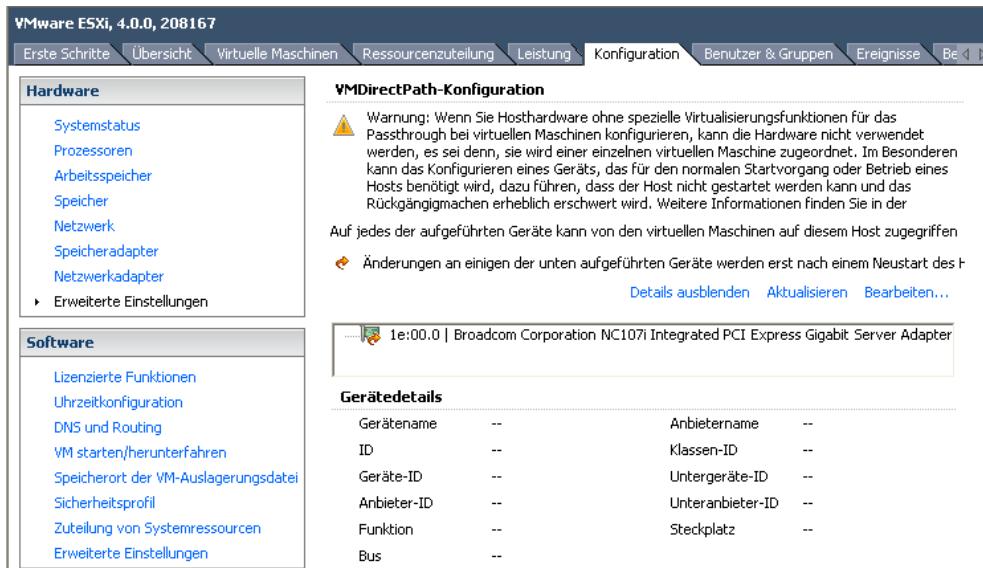
1. Starten Sie den vSphere Client und verbinden sich mit dem ESXi-Server. Wählen Sie links den Server selbst aus und öffnen das Menü Konfiguration.



2. Klicken Sie auf Passthrough konfigurieren und wählen die entsprechende Netzwerkkarte samt zugehöriger Bridge aus.



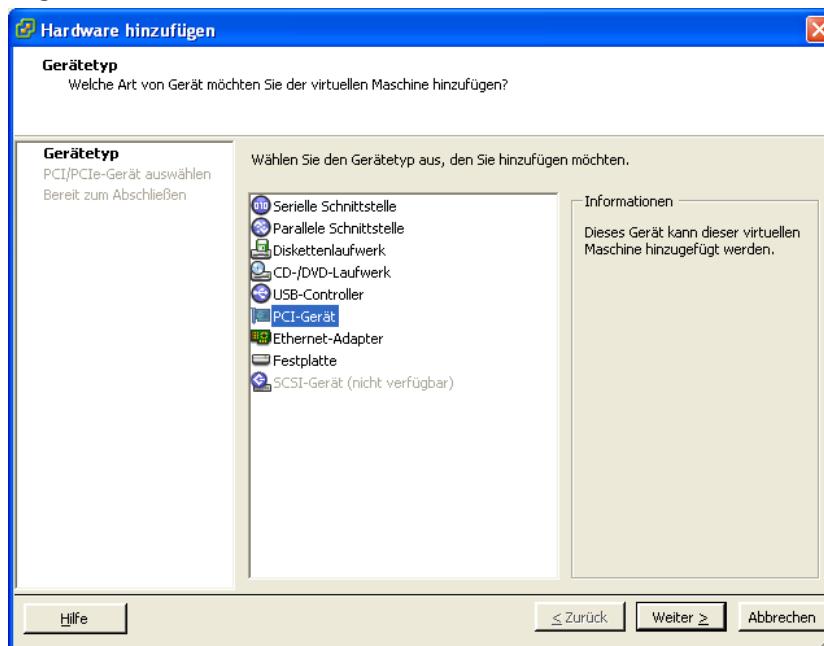
3. Die Netzwerkkarte steht nach einem Neustart des VMware-Servers für VMDirectPath zur Verfügung.



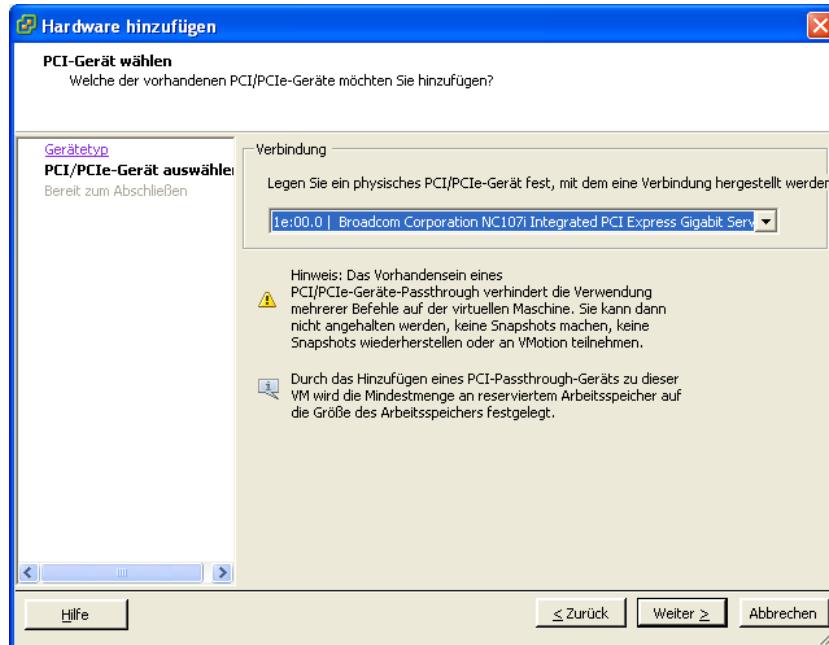
5.2.2. Einbinden der Netzwerkkarte in die VM

Die Netzwerkkarte kann nun wie folgt eingebunden werden:

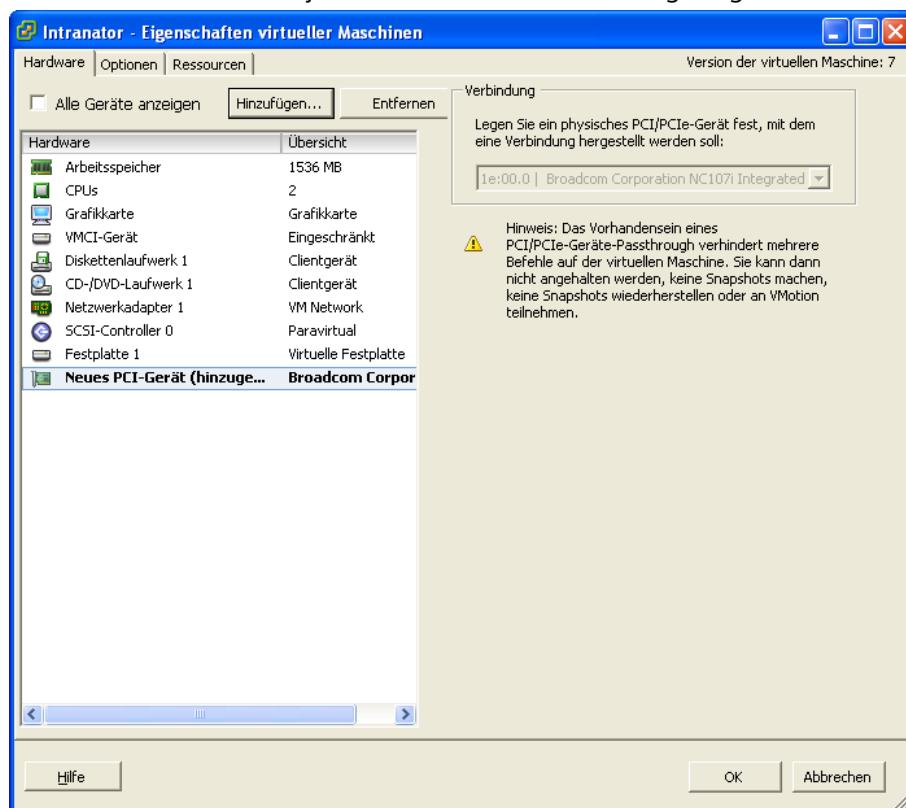
1. Öffnen Sie die Konfiguration der VM und klicken im Menü Hardware auf Hinzufügen.
2. Fügen Sie ein PCI-Gerät hinzu.



3. Wählen Sie die vorhin freigegebene Netzwerkkarte aus und Schließen das Hinzufügen ab.



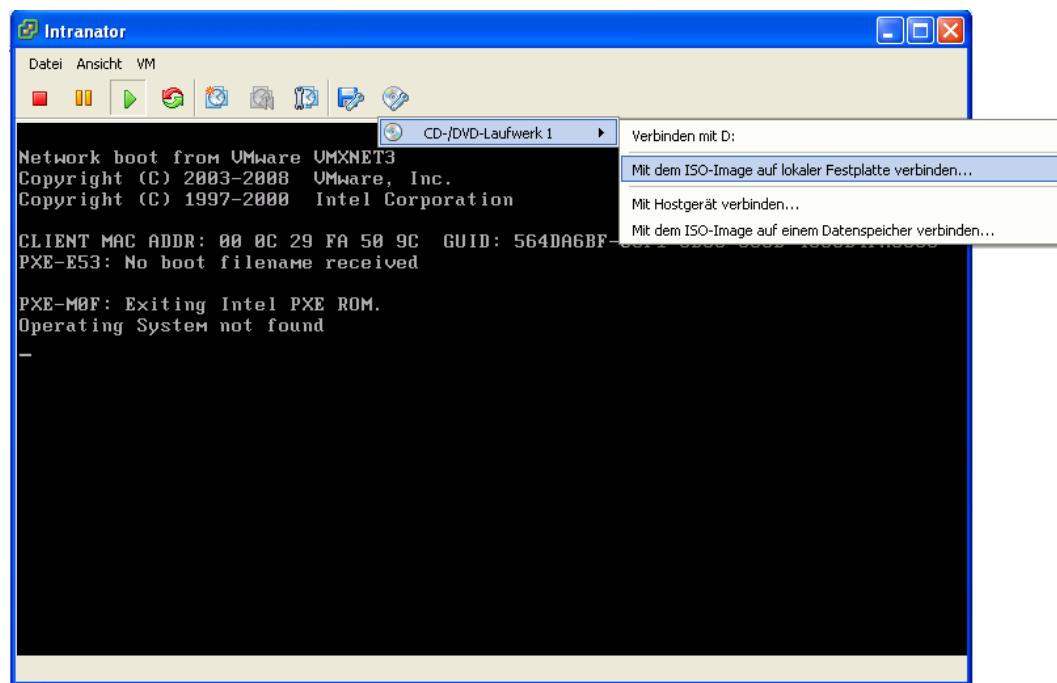
4. Die Netzwerkkarte wird jetzt als zusätzliches Gerät angezeigt.



5.3. Installation des Intranators

1. Starten Sie die virtuelle Maschine und öffnen die Konsole.
2. Die virtuelle Maschine versucht aus dem Netz zu booten, dies schlägt aber mit `Operating System not found` fehl.

3. Klicken Sie in der Werkzeugeiste der Konsole auf das CD-Symbol und verbinden damit das CD-Laufwerk der virtuellen Maschine mit der ISO-Datei der Intranator Installations-CD oder einem lokalen CD-Laufwerk.



4. Warten Sie ca. 5 Sekunden bis das CD-Laufwerk vollständig verbunden ist.
5. Klicken Sie in die Konsole um diese zu aktivieren und drücken die Escape-Taste. Die VM bootet jetzt von der Intranator Installations-CD.

Die restliche Installation läuft ab wie in Abschnitt 2.6, „Installation von CD“ beschrieben.

6. Kapitel - Installation auf Microsoft Hyper-V unter Windows Server 2012 R2

Das Virtualisierungssystem Hyper-V ist Bestandteil des Windows Server 2012 R2 von Microsoft und kann als Rolle in diesem aktiviert werden.

Zusätzlich ist auch der dauerhaft kostenlose Microsoft Hyper-V Server 2012 R2 erhältlich. Dieser kann aber nur über Kommandozeile und Powershell bedient werden, was Konfiguration und Wartung deutlich erschwert. Wir können diesen daher nur erfahrenen Windows-Administratoren mit umfassenden Kenntnissen in der Bedienung per Kommandozeile empfehlen und bieten dafür auch keinen Support an. Wir empfehlen daher für Virtualisierung mit Hyper-V den Windows Server 2012 R2 zu verwenden.

Der Intranator Server enthält von Haus aus alle Treiber und Programme, die für den zuverlässigen Betrieb auf Microsoft Hyper-V unter Windows Server 2012 R2 nötig sind. Eine zusätzliche Installation der Integrationsdienste oder anderer Treiber oder Programme ist nicht notwendig oder möglich.



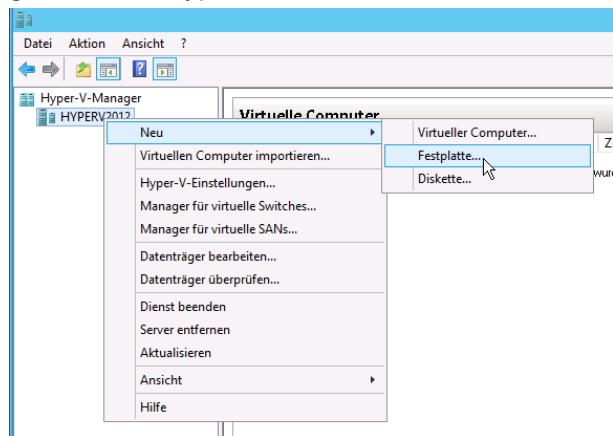
Achtung

Hyper-V bietet keine Möglichkeit PCI-Geräte wie Netzwerkkarten direkt an eine VM durchzurichten. Daher raten wir dringend davon ab, einen damit virtualisierten Intranator ohne zusätzliche Hardware-Firewall einzusetzen. Weitere Informationen dazu finden Sie in Abschnitt 4.1.3, „Kontakt mit ungefilterten Netzwerkpaketen“.

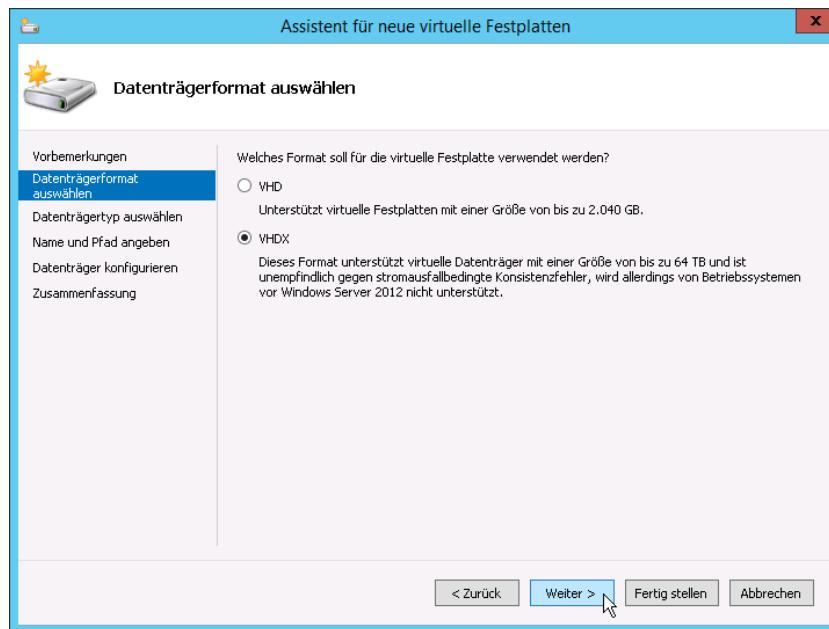
6.1. Konfiguration der virtuellen Maschine

Gehen Sie für die Installation einer virtuellen Maschine wie folgt vor:

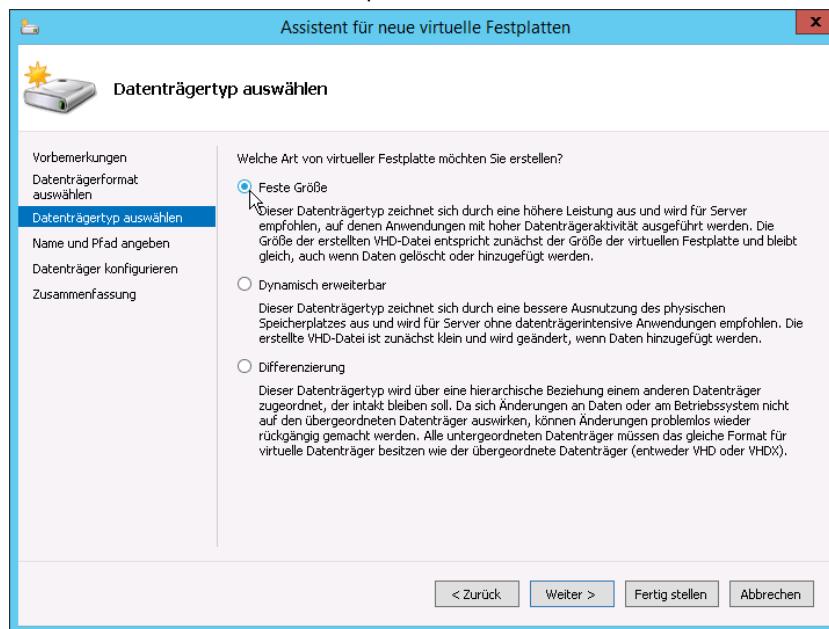
1. Öffnen Sie den Hyper-V-Manager und klicken mit der rechten Maustaste auf die gewünschte Hyper-V-Instanz. Wählen Sie Neu > Festplatte....



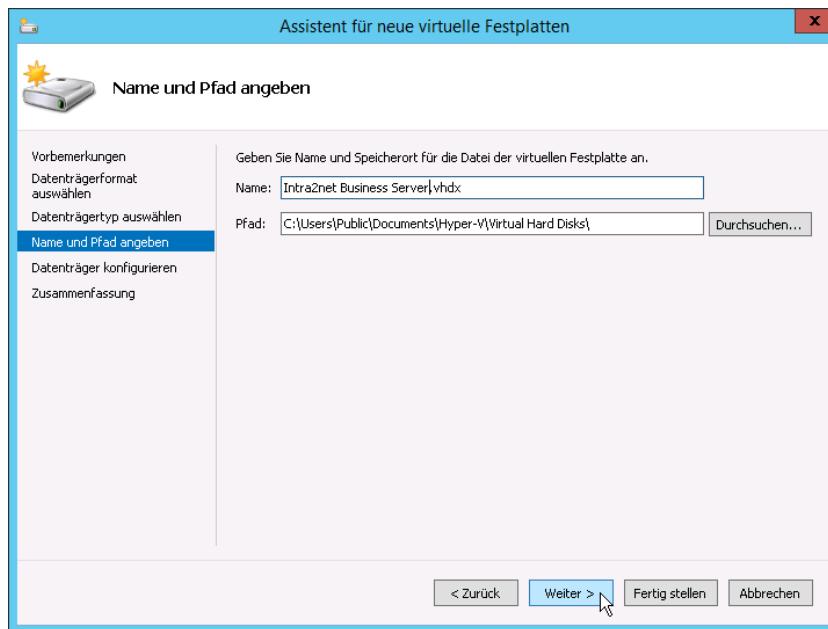
2. Wählen Sie das Format VHDX.



3. Wählen Sie eine virtuelle Festplatte mit Fester Größe.



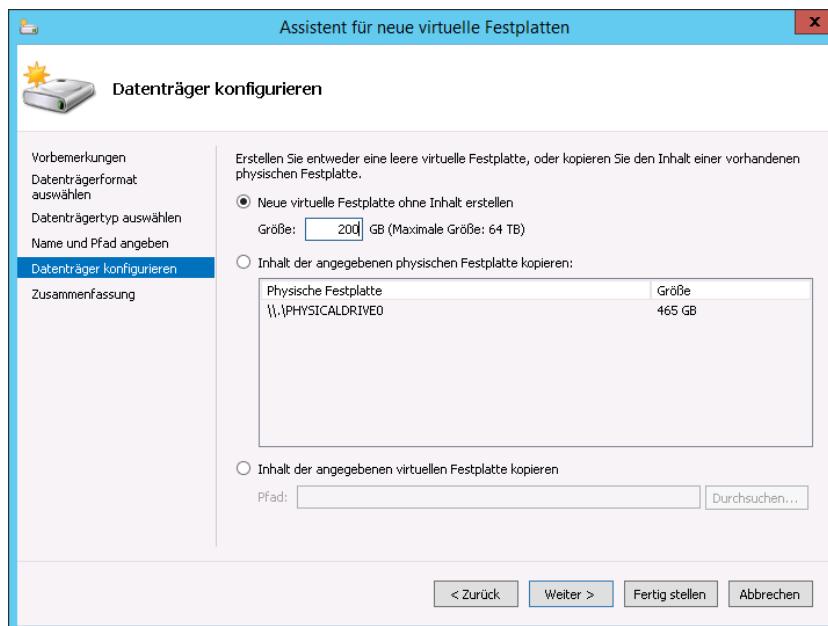
4. Geben Sie der virtuellen Festplatte einen zur zukünftigen VM passenden Namen.



- Weisen Sie dem Intranator eine Festplatte von mindestens 40 GB zu. Wird der Intranator nur zum Scannen von E-Mails und als HTTP-Proxyserver eingesetzt, reichen diese 40 GB im Normalfall auch aus. Nur wenn umfangreiche Statistikdaten für viele Benutzer längerfristig gespeichert werden sollen, wird mehr Speicher benötigt.

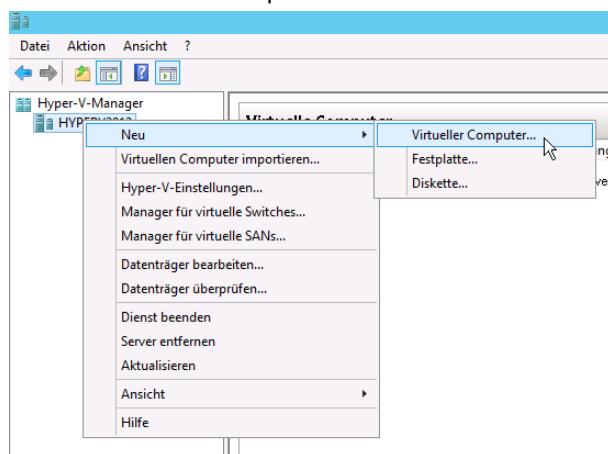
Werden E-Mails oder Groupwaredaten dauerhaft auf dem Intranator abgelegt, wird mehr Festplattenplatz benötigt. Als Faustformel gilt Folgendes: (Gesamtes E-Mail-Volumen aller Benutzer + Statistikdaten) * (Anzahl auf dem System gespeicherter Backupsätze + 2) + 20 GB. Die Anzahl auf dem System gespeicherter Backupsätze beträgt dabei mindestens 1, empfohlen wird 2.

Kalkulieren Sie immer etwas Reserve ein, da ein Vergrößern der Festplatte im Betrieb derzeit nicht unterstützt wird.

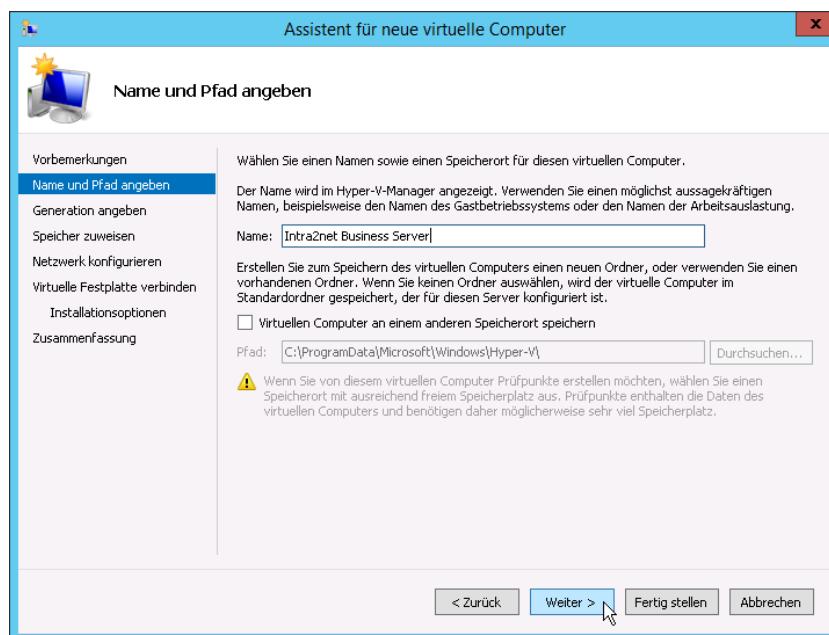


- Legen Sie die virtuelle Festplatte fertig an.

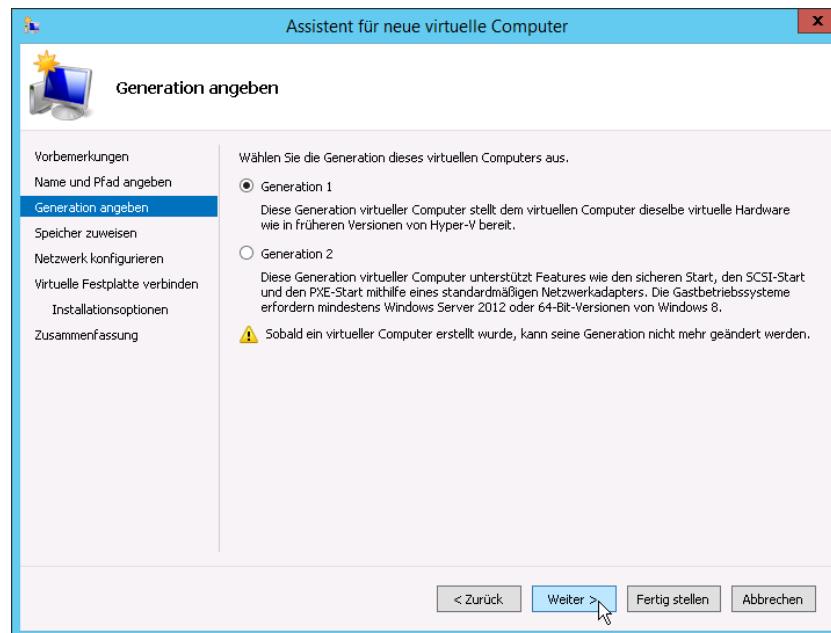
7. Klicken mit der rechten Maustaste auf die gewünschte Hyper-V-Instanz und wählen Neu > Virtueller Computer....



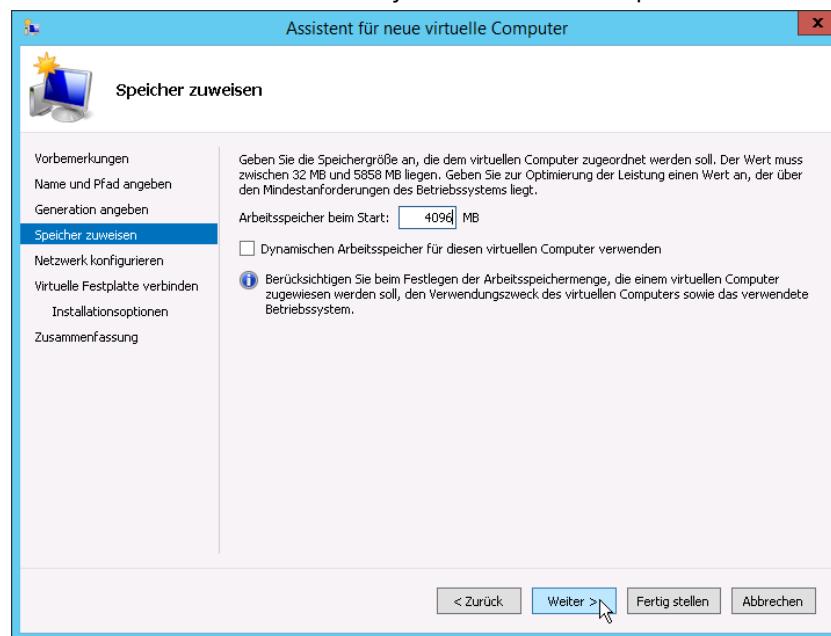
8. Geben Sie der VM einen Namen.



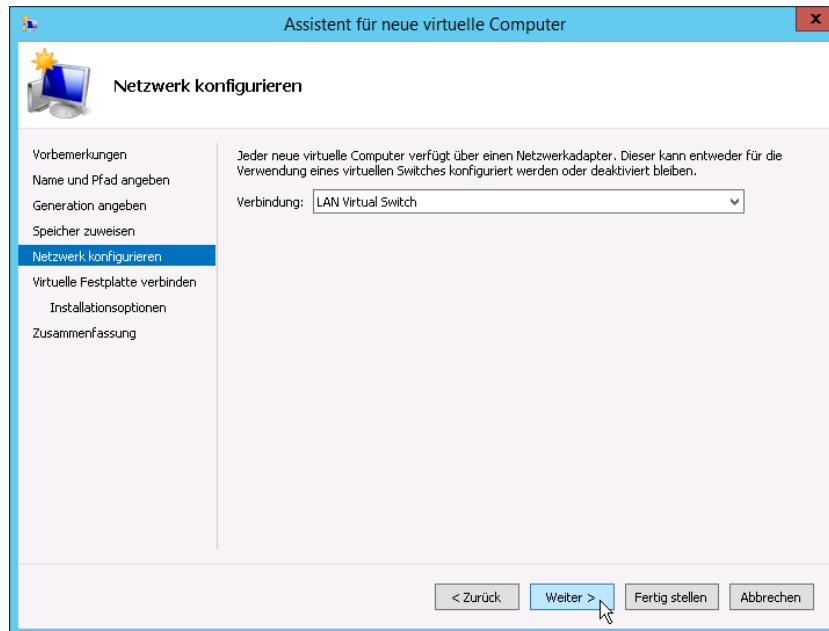
9. Wählen Sie Generation 1.



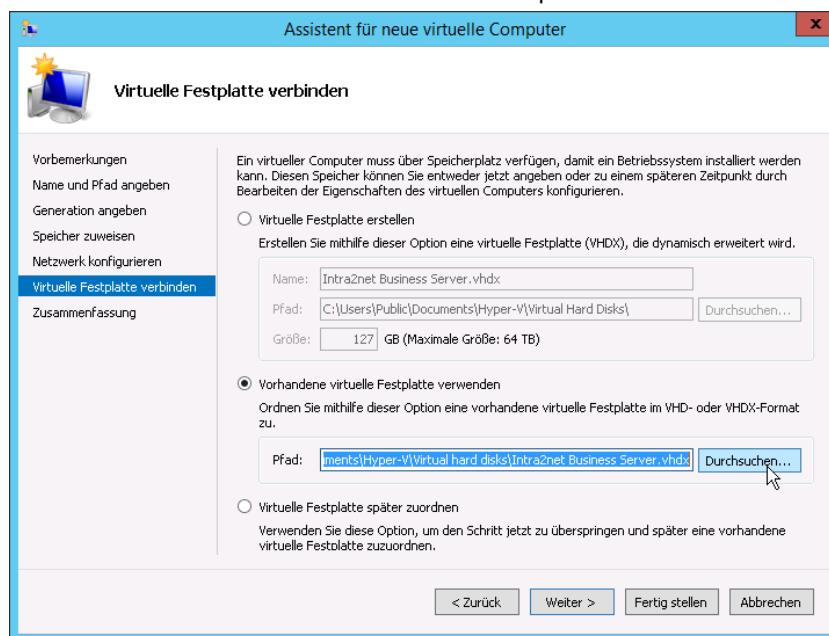
10. Weisen Sie der VM ausreichend Arbeitsspeicher zu. Verwenden Sie mindestens 2 GB. Deaktivieren Sie die Funktion Dynamischer Arbeitsspeicher.



11. Verbinden Sie die VM mit dem virtuellen Switch der mit dem lokalen Netzwerk verbunden ist.



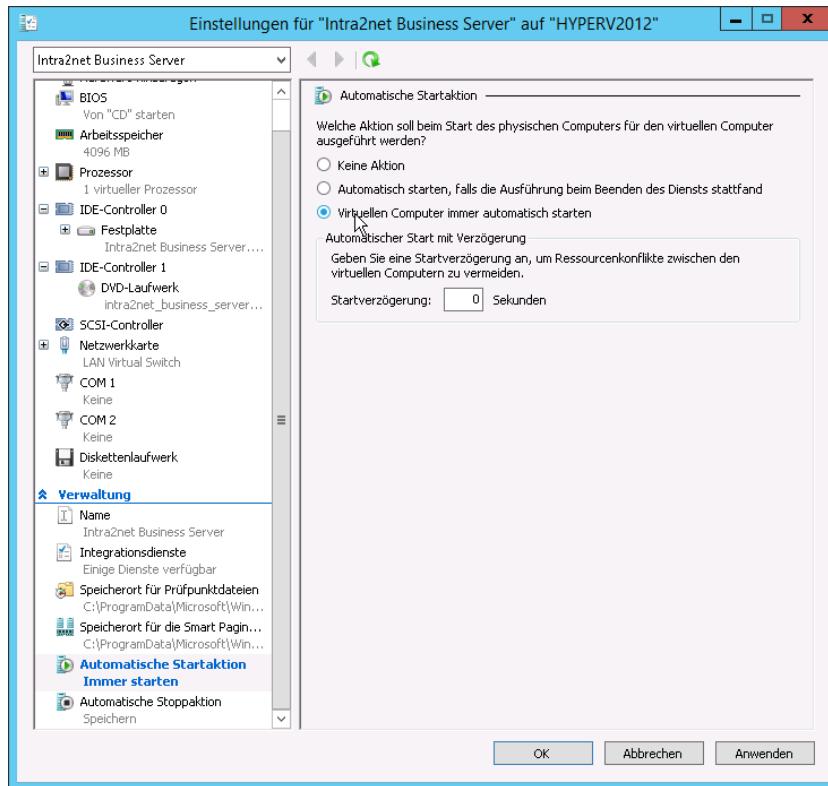
12 Weisen Sie die vorher erstellte virtuelle Festplatte zu.



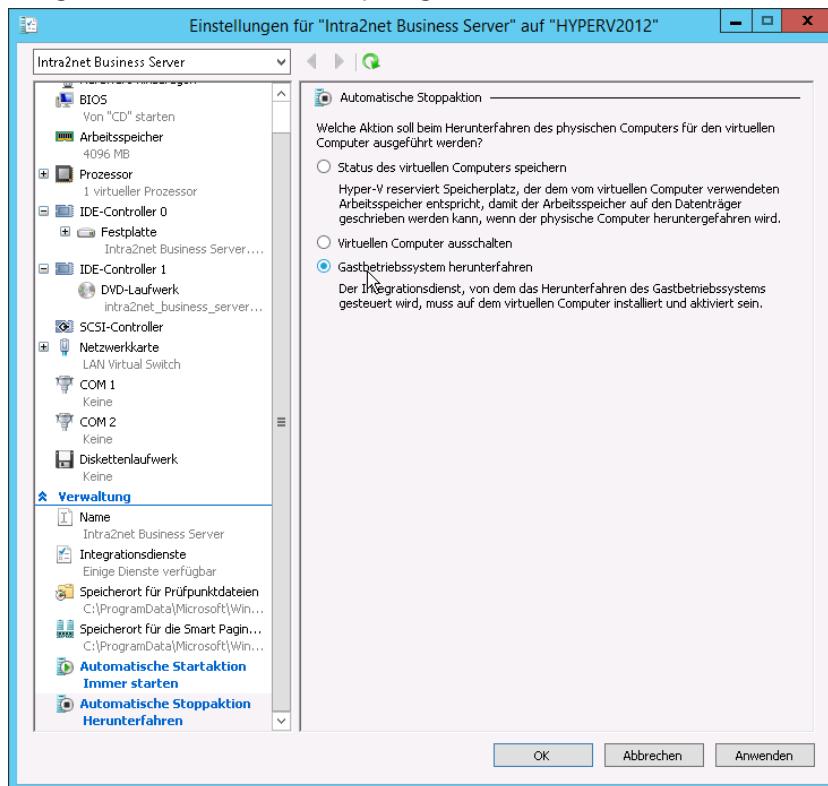
13. Schließen Sie das Anlegen der VM ab.

14. Klicken Sie die neue VM mit der rechten Maustaste an und öffnen die Einstellungen.

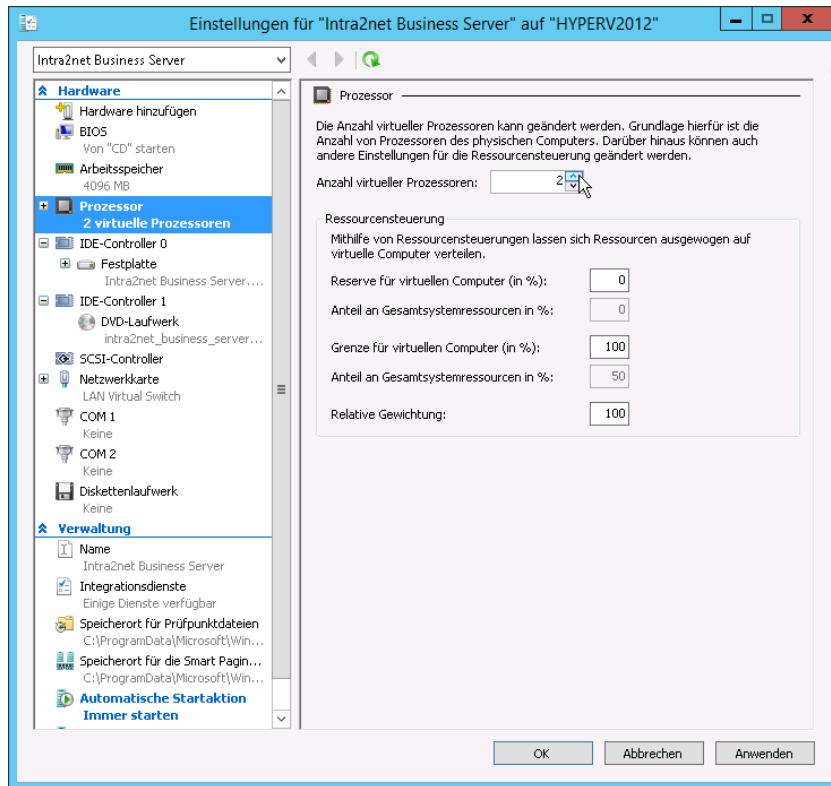
15. Lassen Sie die VM immer automatisch starten damit die VM immer verfügbar ist.



16. Lassen Sie die VM bei Herunterfahren des Hyper-V-Servers immer herunterfahren. Dies beugt Problemen durch Zeitsprünge vor.

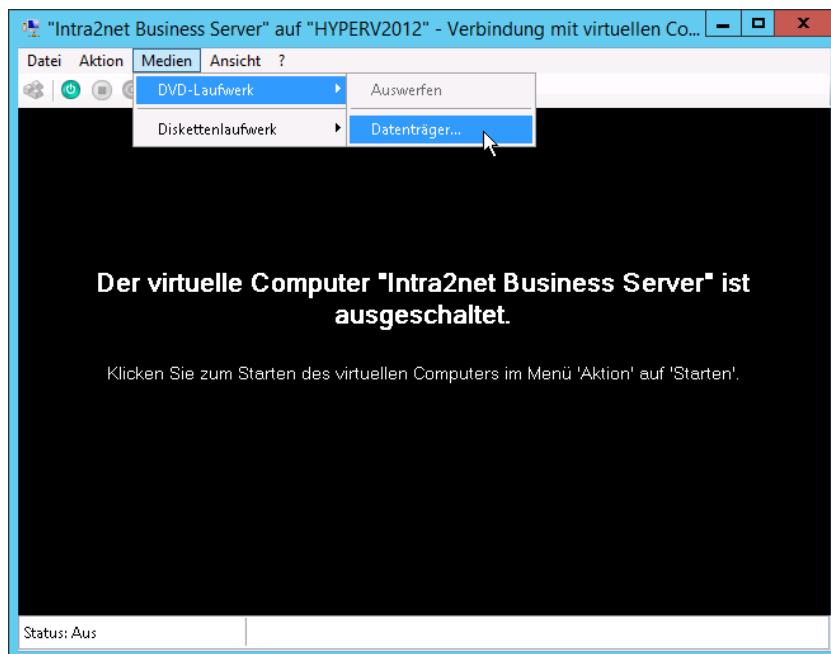


17. Erhöhen Sie die Anzahl der zugewiesenen Prozessorcores je nach verfügbaren Ressourcen. Diese Einstellung können Sie auch später noch an den Bedarf anpassen.



6.2. Installation des Intranators

1. Öffnen Sie die neue VM durch einen Doppelklick.
2. Öffnen Sie das Menü Medien > DVD-Laufwerk > Datenträger.... Wählen Sie die ISO-Datei mit der Installations-CD aus. Diese können Sie unter <http://www.intra2net.com/> herunterladen.



3. Starten Sie die virtuelle Maschine über den grünen Startknopf.
- Die restliche Installation läuft ab wie in Abschnitt 2.6, „Installation von CD“ beschrieben.

7. Kapitel - Die Konsole

Nach der Grundinstallation startet der Intranator direkt in das Konsolenmenü.

Dies können Sie auch bei einem fertig installierten Intranator erreichen, indem Sie Monitor und Tastatur anschließen und sich mit Benutzername und Passwort eines Mitglieds der Administratorengruppe (standardmäßig **admin**) anmelden.

7.1. Hardwareerkennung

Über das Menü Treiber Einstellungen werden die Treiber für unterstützte ISDN-Karten konfiguriert. Die Karten werden automatisch erkannt und die gefundene Konfiguration angezeigt.

Bei der Erstinstallation wird dieses Menü automatisch aufgerufen. Wurde nach der Erstinstallation etwas an den ISDN-Karten verändert, muss der Intranator über dieses Menü an die neue Konfiguration angepasst werden.

7.2. Netzwerkkarten

Über das Menü Netzwerkkarten Einstellungen werden die Treiber für die Netzwerkkarten konfiguriert. Die Karten werden automatisch erkannt und die gefundene Konfiguration angezeigt.

Außerdem wird der aktuelle Verbindungszustand angezeigt (x steht dabei für verbunden, o für nicht verbunden). Dies ist hilfreich, um die angezeigten Namen der Netzwerkkarten (eth0, eth1,...) den richtigen Buchsen am Gerät zuzuordnen. Wir empfehlen, die Buchsen gleich an dieser Stelle mit Klebefolie zu beschriften.

Über dieses Menü kann den Netzwerkkarten eine IP-Adresse zugeordnet werden. Wählen Sie bei der Installation die IP-Adresse passend zu Ihrem bestehenden lokalen Netz. Achten Sie darauf, dass diese IP nicht bereits von einem anderen Gerät verwendet wird.

Die IPs im lokalen Netz sollten aus einem der dafür vorgesehenen privaten Netzbereiche stammen. Dies sind:

- 10.0.0.0 / 255.0.0.0 (bis 10.255.255.255)
- 172.16.0.0 / 255.240.0.0 (bis 172.31.255.255)
- 192.168.0.0 / 255.255.0.0 (bis 192.168.255.255)

Verwenden Sie für das lokale Netz den Typ Intranet (LAN mit NAT) und für die Verbindung zum Internet den Typ DSL/Router. Bei der Verbindung zum Internet können an dieser Stelle keine IPs hinterlegt werden, dies findet später im Rahmen der Konfiguration von Providern statt.

Weitere Informationen zu den verschiedenen Konfigurationstypen für Netzwerkkarten finden Sie im Abschnitt 9.1, „IPs und Netze“.

Bei der Erstinstallation wird dieses Menü automatisch aufgerufen. Wurde nach der Installation etwas an den Netzwerkkarten verändert, muss der Intranator über dieses Menü an die neue Konfiguration angepasst werden.

7.3. DNS und DHCP

Über dieses Menü können der Rechnername und die Domain des Intranators festgelegt werden.



Achtung

Verwenden Sie im lokalen Netz auf keinen Fall Ihre offizielle Domain (endet z.B. auf ".de", ".com" oder ähnliches), sondern eine nur lokal gültige (endet z.B. auf ".local" oder ".lan"). Ansonsten wird Ihre Webseite nicht mehr aus dem lokalen Netz erreichbar sein und häufig kommt es auch zu Problemen bei der E-Mail-Zustellung.

Bei der Erstinstallation wird dieses Menü automatisch aufgerufen. Dann ist es auch möglich, hier einen DHCP-Pool zu konfigurieren oder die Funktion als DHCP-Server zu deaktivieren.

7.4. Firewall-Notmodus

Sollte man sich mit der Firewall aus der Weboberfläche ausgesperrt haben, kann der Zugriff über diesen Menüpunkt kurzzeitig wieder freigeschaltet werden.

Details finden Sie im Abschnitt 36.4, „Firewall-Notmodus“.

7.5. In Auslieferungszustand zurücksetzen

Mit dieser Funktion kann der Intranator in den Zustand nach der Auslieferung oder Erstinstallation zurückgesetzt werden. Alle Einstellungen, Benutzerdaten, Passwörter, E-Mails, Statistikdaten, Logdateien und Backups werden vom Intranator gelöscht. Nur die Version der Intranator-Software bleibt auf dem aktuellen Stand und wird nicht zurückgesetzt.

Das Gerät startet danach automatisch neu.

7.6. Das root-Password

Das root-Password wird nur zum Zugang auf die Linux-Shell benötigt und ist unabhängig vom Administrator-Password. Es wird zum normalen Betrieb oder Administration nicht benötigt.

Es ist bei der Appliance Pro 12 Zeichen lang und wird für jede Maschine individuell mit einem Zufallsgenerator erzeugt. Danach wird es bei Intra2net verschlüsselt gespeichert. Falls ein Händler oder Kunde Zugriff auf die Linux-Shell wünscht, kann es bei Intra2net angefordert werden. Das dafür nötige Formular ist im Partnerweb erhältlich.

Am Ende der Installation der Softwareversion des Intranators muss das root-Password eingegeben werden. Achten Sie hier unbedingt darauf, dass das Passwort lang genug ist (mindestens 10 Zeichen) und nicht leicht z.B. aus einem Wörterbuch erraten werden kann. Notieren Sie das Passwort und bewahren es an einem sicheren Ort (z.B. Safe) auf. Verwenden Sie ein anderes Passwort als für den Administrator-Benutzer oder für andere Systeme.

7.7. Die Linux-Shell

Die Linux-Shell wird zum normalen Betrieb oder zur Administration nicht benötigt.

Ein Zugriff als root-Benutzer auf die Linux-Shellebene ist von der Konsole aus und über SSH möglich. Wechseln Sie mit ALT+F2 von der Intranator-Konsole auf den Login der Linux-Shell.



Achtung

Änderungen auf der Linux-Shell können die Funktion, Stabilität und Sicherheit des Intranators stark beeinträchtigen. Dies muss sich nicht sofort zeigen, sondern kann auch erst nach einiger Zeit z.B. mit einem Update zu Störungen führen.

8. Kapitel - Die Weboberfläche

8.1. Zugriff auf die Weboberfläche

Starten Sie einen Webbrowser und öffnen Sie folgende URL:

<https://192.168.1.254>

Falls Sie den Intranator auf eine andere IP gestellt haben, müssen Sie natürlich diese verwenden.

Beim ersten Aufruf wird Ihr Webbrowser eine Sicherheitswarnung anzeigen, denn die verschlüsselte Verbindung (https) wird mit einem nicht vertrauenswürdigen und nicht zum Servernamen passenden Zertifikat aufgebaut. Diese Warnungen lassen sich beim ersten Aufruf nicht vermeiden. Öffnen Sie die Webseite dennoch.

Für den späteren Betrieb ist es wichtig, dass solche Zertifikatswarnungen nicht mehr erscheinen. Wie Sie das richtig konfigurieren, ist im 10. Kapitel, „SSL-Verschlüsselung und Zertifikate“ beschrieben.

8.2. Lizenzcode

Bei den Appliance-Modellen müssen Sie beim ersten Zugriff auf die Weboberfläche den Lizenzcode eingeben. Diesen finden Sie auf dem der Lieferung beiliegenden Lizenzzertifikat. Danach haben Sie 30 Tage Zeit, die Lizenz online zu aktivieren.

Haben Sie keine Hardware von Intra2net erworben, befindet sich das Gerät für 30 Tage im Demomodus. Sobald das Gerät über eine Internetverbindung verfügt, können Sie im Menüpunkt Information > Lizenz einen Lizenzcode eingeben um das Gerät vollständig nutzen zu können.

8.3. Die Hauptseite

Mit folgenden Benutzerdaten können Sie sich nach der Installation das erste Mal einloggen:

Administrator Login	admin
Administrator Passwort	admin

Im oberen Bereich der Hauptseite können Internetverbindungen über unterschiedliche Provider aufgebaut und getrennt werden, E-Mail-Transfers angestoßen, sowie VPN Verbindungen kontrolliert werden.

Der untere Bereich zeigt Statusinformationen an.

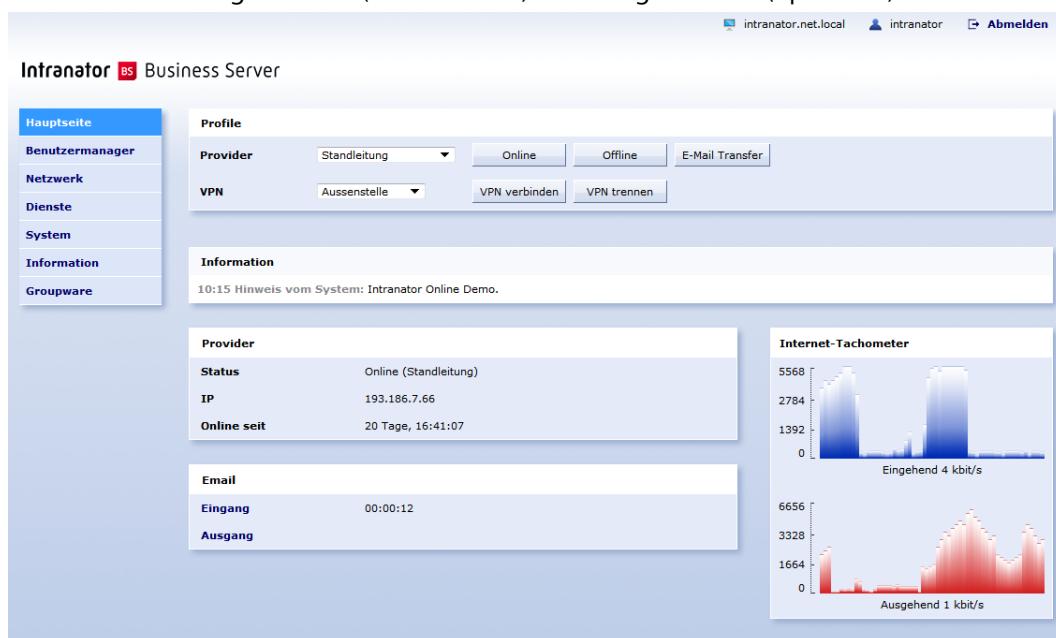
Der Informationsbereich zeigt Status- und Fehlermeldungen an. Fehlermeldungen können, wenn Sie zur Kenntnis genommen wurden, durch Klicken auf das OK dahinter entfernt werden. Ansonsten verschwinden sie nach einem Timeout (abhängig von Wichtigkeit und Typ).

Der Providerbereich zeigt den aktuellen Provider, IP und Timeout.

Der E-Mail-Bereich zeigt den aktuellen E-Mail-Transfer. Ein Klick auf Eingang öffnet während des E-Mail-Transfers ein Fenster mit einem Livelog von fetchmail zur Fehlerdiagnose beim E-Mail-Empfang. Ein Klick auf Ausgang öffnet die E-Mail-Warteschlange.

Der VPN Bereich zeigt die aktuell aktiven VPN Verbindungen an.

Rechts davon wird das Internet-Tachometer angezeigt. Darin wird die Auslastung der Internetleitung innerhalb der letzten Minute als Balkendiagramm angezeigt. Die Anzeige ist unterteilt in eingehenden (downstream) und ausgehenden (upstream) Datenverkehr.



In der Standardkonfiguration haben alle, die aus dem lokalen Netz auf die Hauptseite zugreifen, das Recht, diese zu sehen und Verbindungen aufzubauen und zu trennen. Dies kann über die Rechte der „Alle“-Gruppe geändert werden. Siehe dazu auch Abschnitt 14.1, „Benutzergruppen“.

Im Menü auf der linken Seite werden alle Menüpunkte, auf die der aktuell eingeloggte Benutzer Zugriff hat, in voller Schriftfarbe dargestellt. Die Menüpunkte, auf die er keinen Zugriff hat, werden in schwacher Schriftfarbe dargestellt. Letztere können aber dennoch angewählt werden, es öffnet sich dann ein Login-Fenster.

8.4. Die Warteschlange

Normalerweise werden Änderungen an der Konfiguration bei einem Klick auf Änderungen speichern sofort aktiviert. Da dies bei einigen Einstellungen nicht sinnvoll ist (z.B. bei der Netzwerkkonfiguration oder über eine Fernwartungssitzung), gibt es die Warteschlange.

Ist sie aktiv, werden alle Änderungen gesammelt. Sie können unter System > Warteschlange eingesehen und zusammen verworfen oder aktiviert werden.

Sie kann entweder unter System > Warteschlange manuell aktiviert werden oder wird beim Ändern von einigen Einstellungen (Netzwerk, Firewall) automatisch aktiviert.

Die Warteschlange gilt für alle Benutzer des Systems gemeinsam. Wird eine gewisse Zeit keine Änderung gemacht, löscht sich die Warteschlange von selbst. Ist die Warteschlange

längere Zeit aktiv, kann es zu Störungen bei der Konfiguration von neuen Rechnern über DHCP kommen.

Werden Änderungen gemacht, die wegen Abhängigkeiten alleine nicht gültig sind (z.B. Ändern eines Netzwerkes, wenn noch IPs im alten Netz liegen), so werden diese Änderungen normalerweise nicht zugelassen und als Fehler rot hinterlegt dargestellt. Die Warteschlange lässt solche Änderungen zu. Sie können damit die Abhängigkeiten korrigieren. Erst, wenn Sie die Änderungen in der Warteschlange ausführen wollen, müssen wieder alle Abhängigkeiten erfüllt sein.

8.5. Die Konfigurationsprüfung

Unter Information > System > Konfiguration werden alle Warnungen und Fehler des Konfigurationsprüfungssystems angezeigt. Da es wegen der teilweise recht komplexen Abhängigkeiten manchmal dazu kommen kann, dass Fehler noch angezeigt werden, obwohl sie schon behoben wurden, gibt es die Funktion Konfiguration prüfen.

Teil 2. Allgemeine Funktionen

9. Kapitel - Intranet

9.1. IPs und Netze

Unter Netzwerk > Interfaces können die Netzwerkkarten des Systems konfiguriert werden.

Folgende Typen / Modi können für die Netzwerkkarten eingestellt werden:

LAN mit NAT	Lokales Netz. Beim Zugriff ins Internet werden die lokalen IP-Adressen auf die Internet-IP des Intranators umgeschrieben (Network Address Translation, NAT). Dies ist die normale Konfiguration für lokale Netze.
LAN ohne NAT	Lokales Netz. Beim Zugriff ins Internet findet kein NAT statt. Verwenden Sie diesen Modus für eine DMZ (DeMilitarized Zone) mit offiziellen IPs oder wenn der Intranator nicht direkt den Zugriff ins Internet herstellt und ein anderer Router für die NAT zuständig ist.
DSL/Router	Netzwerkkarte, über die der Zugang ins Internet geroutet wird. Entweder über ein DSL-Modem oder einen Router. Welches von beiden verwendet wird, hängt vom Typ des verwendeten Providerprofils ab. Der Providertyp und die IPs werden nicht hier, sondern unter Netzwerk > Provider > Profile eingestellt.
Proxy-ARP	Lokales Netz ohne NAT mit IPs aus dem Bereich des Routers. Eine genaue Beschreibung finden Sie in Abschnitt 11.7.3, „Proxy-ARP“.
nicht verwendet	nicht aktiv.

Den LAN-Netzwerkkarten kann ein Firewallprofil zugewiesen werden. Dies gilt dann für alle IPs aus diesem Netz, für die nicht eine spezifischere Konfiguration (z.B. durch Eintrag als Rechner oder Bereich) vorgenommen wurde. Näheres ist beschrieben unter Abschnitt 9.2, „Zugriffsrechte eines Netzwerkobjekts“.

9.2. Zugriffsrechte eines Netzwerkobjekts

Für jedes Netzwerkobjekt (Netz, Rechner, VPN,...) kann derselbe Block von Rechten vergeben werden.

Firewallregelliste	Anhand dieser Firewallregelliste werden alle von diesem Objekt (Rechner, Netz,...) versendeten Pakete geprüft. Eine detaillierte Beschreibung der Firewallregellisten finden Sie in Teil 5, „Firewall“.
Proxy Profil	Damit kann entweder ein Proxyprofil diesem Objekt fest zugewiesen oder die Benutzerauthentifizierung aktiviert werden.
E-Mail-Relaying erlaubt	Es wird erlaubt, E-Mails an Domains zu versenden, die nicht lokal auf dem Intranator liegen. Das Versenden von E-Mails muss vorher allerdings in der Firewallregelliste zugelassen werden.

DNS-Anfragen ins Internet erlaubt	Es wird erlaubt, DNS-Anfragen zu stellen, die der Intranator selbst nicht auflösen kann. Mit dieser Funktion kann man ein ständig auftretendes Wählen durch DNS-Anfragen verhindern sowie von einigen Hackern genutzte DNS-Tunnel zur Datenübermittlung blockieren.
-----------------------------------	---

9.3. Domain und DNS

Der Intranator leitet DNS-Anfragen ins Internet weiter. Wie und wohin wird beim aktuell aktiven Provider eingestellt, siehe 11. Kapitel, „Internet“.

Außerdem kann er entweder selbst für die lokale Domain als DNS-Server fungieren oder diese Aufgabe an einen anderen Server delegieren.

9.3.1. DNS-Server für Lokale Domain

Der eigene Rechnername und die lokale Domain können unter Netzwerk > DNS > Einstellungen eingestellt werden. Stellen Sie ein, dass das lokale System für die lokale Domain zuständig ist.

Der Intranator ist dann DNS-Server für die lokale Domain. Alle unter Netzwerk > Intranet > Rechner eingetragenen Rechnernamen können per DNS aufgelöst werden.

Es wird dringend davon abgeraten, die offizielle Domain einer Firma (z.B. „meinefirma.de“) auch im lokalen Netz zu verwenden. Da der Intranator ja DNS-Server für die lokale Domain ist, kann er Anfragen für die im externen DNS-Server des Web-Providers konfigurierten Rechner, wie z.B. „www“, nicht beantworten.

Verwenden Sie stattdessen eine nur lokal gültige Domain, wie z.B. „meinefirma.lan“. Wegen einem Internet-Standard zu Broadcast-DNS empfehlen wir auch, für diese Domains nicht „.local“ zu verwenden, denn mit einigen Mac OS oder Linux-Versionen funktioniert die Namensauflösung nicht mehr, wenn „.local“ in der lokalen Domain verwendet wird.

9.3.2. DNS für lokale Domain weiterleiten

Verwenden Sie einen anderen DNS-Server für die lokale Domain (z.B. einen Windows Domain Controller), tragen Sie den Rechnernamen und die Domain des Intranators unter Netzwerk > DNS > Einstellungen ein. Stellen Sie die Zuständigkeit für die lokale Domain auf anderer Server. Tragen Sie die IP des zuständigen DNS-Servers und (wenn vorhanden) des alternativen Servers in die Felder 1. und 2. ein.

Hinterlegen Sie unbedingt auf diesen DNS-Servern einen A-Eintrag für den Intranator mit seiner IP.

9.3.3. DNS für andere Domains weiterleiten

Der Intranator kann Anfragen für andere nicht-öffentliche Domains an fest hinterlegte Server weiterleiten. Dies macht z.B. Sinn, wenn verschiedene Standorte per VPN verbunden sind und Namen in den lokalen Domains der jeweils anderen Standorte aufgelöst werden können sollen.

Tragen Sie diese Domains und die IPs der zugehörigen DNS-Server unter Netzwerk > DNS > Weiterleitung ein.

9.3.4. DNS-Rebind verhindern

Bei einem sogenannten DNS-Rebind-Angriff liefert ein externer DNS-Server eine IP aus dem lokalen Netz zurück. Dadurch kann ein externer Angreifer einen Webbrowser dazu bringen, ferngesteuert Verbindungen ins Lokale Netz aufzubauen. Details zu diesem Angriff finden Sie bei Wikipedia [http://en.wikipedia.org/wiki/DNS_rebinding].

Der Intranator kann diese Angriffe wirkungsvoll verhindern, indem er Antworten mit lokalen IPs von externen DNS-Servern blockiert. Damit das nicht zu Störungen führt, dürfen unter Netzwerk > Provider > Profile : Einstellungen nur tatsächlich extern liegende DNS-Server eingetragen sein.

Alle DNS-Server, die für lokale oder lokal geroutete Domains zuständig sind, müssen unter den entsprechenden Domains als DNS-Weiterleitung konfiguriert werden. Die dort hinterlegten Server dürfen dann mit lokalen IPs antworten.

9.4. Clients eintragen

Unter Netzwerk > Intranet > Rechner können einzelne Rechner eingetragen werden. Jedem eingetragenen Rechner können damit eigene Zugriffsrechte (siehe Abschnitt 9.2, „Zugriffsrechte eines Netzwerkobjekts“) zugewiesen werden.

Außerdem ist der Rechner automatisch per DNS unter seinen Namen erreichbar (Primärer Name sowie den unter "Alias" eingetragenen sekundären Namen). Ein Eintrag für Reverse-DNS (welchen DNS-Namen hat die IP x?) wird auch automatisch angelegt.

Ist eine MAC Adresse eingestellt, so werden DHCP Anfragen mit dieser MAC mit der eingestellten IP beantwortet (statisches DHCP). Ist eine IP Adresse im Feld eingegeben, so kann mit einem Klick auf Erkennen die dazugehörige MAC gesucht werden.

Über Wake-On-LAN können Sie ein spezielles IP-Paket („Magic Packet“) an die angegebene MAC-Adresse senden. Die meisten Rechner können dadurch über das Netz eingeschaltet werden. Es kann sein, dass Sie Einstellungen im BIOS des Rechners vornehmen müssen um diese Funktion zu aktivieren.

Wurde der Rechner über dynamisches DHCP angelegt, so wird angezeigt, bis wann sein Lease gültig ist. Wird es bis dahin nicht erneuert, wird der gesamte Eintrag gelöscht.

Auch bei Rechnern, die über dynamisches DHCP angelegt wurden, ist es möglich, andere Rechte oder Aliasnamen einzutragen. Da diese Einstellungen jedoch verloren gehen, wenn der Rechner länger nicht aktiv ist (z.B. Wochenende, Urlaub), empfehlen wir, solche Rechner aus dem dynamischen DHCP Pool zu nehmen und eine andere IP außerhalb eines Pools zuzuweisen. Ändern Sie dazu einfach die IP und klicken auf Einstellungen speichern.

9.5. DHCP

Der Intranator enthält einen DHCP Server. Wurde eine MAC-Adresse unter Netzwerk > Intranet > Rechner hinterlegt, so bekommt ein anfragender Rechner immer die entsprechende IP zugewiesen. Ist eine MAC bisher noch nicht bekannt, so weist der DHCP-Server eine IP aus einem der DHCP-Bereiche (siehe Abschnitt 9.6, „Bereiche eintragen“) zu.

Es darf in einem Netz immer nur ein DHCP-Server aktiv sein. Der Intranator prüft daher beim Start, ob ein anderer DHCP-Server aktiv ist und deaktiviert seinen eigenen gegebenenfalls.

Normalerweise übermittelt der Intranator sich selbst als Standardgateway und DNS-Server. Unter Netzwerk > Intranet > DHCP können diese Werte, sowie Server für WINS und NTP-Zeitsynchronisation, umgestellt werden. Werden die Felder leer gelassen, wird der Intranator verwendet.



Achtung

Wir raten davon ab, ein anderes Standardgateway zu verwenden. Funktionen wie Port-Forwarding und der Zugriff auf lokale Rechner über VPN können dann unter Umständen nicht mehr funktionieren.

9.6. Bereiche eintragen

Unter Netzwerk > Intranet > Bereiche können IP-Bereiche (Von-Bis) eingetragen werden. Diesem gesamten Bereich können damit eigene Zugriffsrechte (siehe Abschnitt 9.2, „Zugriffsrechte eines Netzwerkobjekts“) zugewiesen werden.

Im Gegensatz zu den einzelnen Rechnern kann der Intranator für Bereiche keine DNS-Funktion übernehmen.

Wird ein Bereich als DHCP-Pool verwendet, so werden den IPs im Bereich vorerst keine Rechte zugeordnet. Erst, wenn ein Rechner eine DHCP-Anfrage stellt, so wird ihm eine IP aus einem der DHCP-Pools zugewiesen. Der Rechner wird dazu automatisch in Netzwerk > Intranet > Rechner angelegt.

Haben Sie mehrere unterschiedliche lokale Netze, müssen Sie für jedes dieser Netze einen eigenen DHCP-Pool anlegen

9.7. Import/Export von Rechnerprofilen

Die verschiedenen Einstellungen für die Rechner können auch in einer Datei zusammengefasst eingespielt oder exportiert werden. Hierzu können Sie entweder eine vorbereitete XML- oder eine CSV-Datei (Comma Separated Value) auf den Intranator hochladen bzw. herunterladen. Dies ist besonders sinnvoll, wenn Sie bereits eine Rechnerdatenbank besitzen, aus der sich die Daten exportieren lassen.

9.7.1. Import von Rechnern

Hier laden Sie eine XML oder CSV Datei mit Rechnern für den Import hoch. Die Feldnamen des XML Imports entnehmen Sie bitte der DTD, die Sie von dieser Konfigurationsseite herunterladen können. Den Aufbau des CSV Formats entnehmen Sie am besten einer zuvor exportierten CSV Datei. Das Feld „access_right“ enthält den Namen des für diesen Rechner verwendeten Zugriffsrechts.



Hinweis

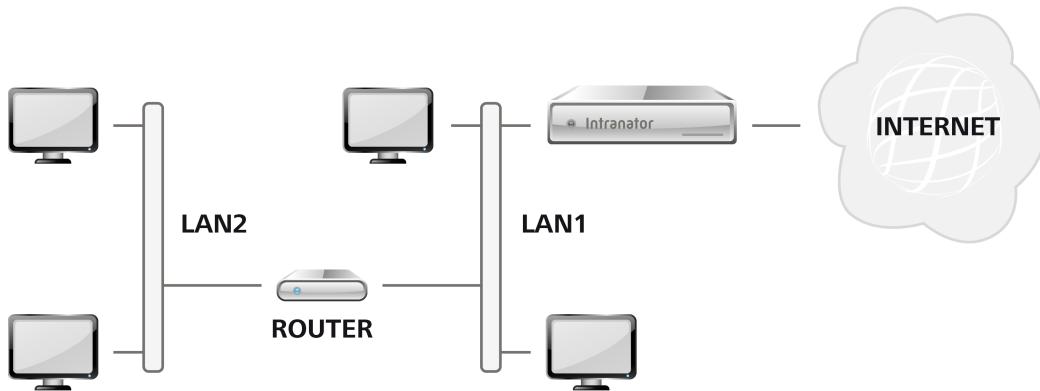
Bitte beachten Sie, dass das eingetragene Zugriffsrecht exakt mit dem Namen eines Zugriffsrechts im System übereinstimmen muss.

9.7.2. Export von Rechnern

Hier wählen Sie die Rechner für den Export aus, wahlweise als XML- oder CSV-Format. Die Feldnamen des XML Exports entnehmen Sie bitte der DTD. Beim CSV-Format stehen die Feldnamen in der ersten Zeile.

9.8. Routing im Intranet

Der Intranator kann über mehrere interne Netze routen. Dies ist sinnvoll z.B. wenn mehrere Firmen sich einen Intranator teilen oder wenn einzelne Stockwerke oder Abteilungen unterschiedliche Netze verwenden.



Ein Rechner oder Router im Netz des Intranators muss dabei zwischen den Netzen routen. Geben Sie dessen IP unter Netzwerk > Intranet > Routing als Gateway IP ein. Soll der Intranator selbst zwischen den Netzen routen, so schließen Sie das andere Netz an eine der Netzwerkkarten des Intranators an und tragen das Netz unter Netzwerk > Interfaces ein (siehe Abschnitt 9.1, „IPs und Netze“).

Das Routing im Intranet funktioniert nur für interne Netze (an internen Netzwerkinterfaces) und kann nicht verwendet werden, um spezielle Routen ins Internet zu legen (am externen Netzwerkinterface). Verwenden Sie hierfür die Providereinstellungen, siehe Abschnitt 11.4, „Router mit fester IP“.

Auch für ein gesamtes geroutetes Netz können Rechteeinstellungen hinterlegt werden. Für geroutete Netze gelten nur die Rechte des Routings selbst, nicht die Rechte des Netzes über das das Gateway angeschlossen ist und die unter Netzwerk > Interfaces eingestellt werden.

Die Firewall des Intranators ist nur für Verbindungen von dem gerouteten Netz ins Internet und andere, direkt an den Intranator angeschlossene Netze wirksam. Die Firewall funktioniert prinzipbedingt nicht für Verbindungen zwischen dem gerouteten und dem am Intranator und Router angeschlossenen Netz. Um die Intranator-Firewall zwischen verschiedenen lokalen Netzen nutzen zu können, müssen diese Netze direkt an eine Netzwerkschnittstelle des Intranators angeschlossen werden anstatt Sie über einen separaten Router zu verbinden.

10. Kapitel - SSL-Verschlüsselung und Zertifikate

10.1. Prinzip und Gefahren der SSL-Verschlüsselung

Durch die Verschlüsselung wird sichergestellt, dass nur Client und Server die übertragenen Daten kennen. Was aber passieren kann ist, dass sich jemand beim Verbindungsaufbau zwischen Client und Server hängt und ab dann alles mitlesen und verändern kann (sog. Man-in-the-middle-Angriff). Um das zu verhindern, authentifiziert sich der Server beim Verbindungsaufbau mit einem Sicherheitszertifikat gegenüber dem Client.

Der Server sendet sein Zertifikat an den Client und dieser überprüft es anhand von 3 Kriterien:

1. Aussteller des Zertifikats ist eine dem Client bekannte Zertifizierungsstelle.
2. Genau der Server, den der Client kontaktiert hat, ist im Zertifikat als Eigentümer ausgewiesen. Dafür vergleicht der Client den von ihm kontaktierten Rechnernamen mit dem Feld Rechnername (Common Name, abgekürzt CN) im Zertifikat.
3. Die aktuelle Uhrzeit liegt innerhalb des Gültigkeitszeitraums des Zertifikats.

Erst, wenn alle 3 Kriterien stimmen, kann sich der Client sicher sein, mit dem richtigen Server zu sprechen und ein Angriff kann ausgeschlossen werden.

Ein in der Praxis tatsächlich beobachteter Angriff sieht wie folgt aus: Ein Hacker sitzt mit einem ganz normalen Notebook z.B. an einem WLAN-Hotspot am Flughafen. Über eine spezielle Software leitet er alle WLAN-Verbindungen über sein Notebook um. Wenn jemand eine verschlüsselte Verbindung aufbauen möchte, präsentiert die Software dem Anwender ein anderes Zertifikat. Dieses Zertifikat ist ganz legal von einer vertrauenswürdigen Zertifizierungsstelle auf eine dem Hacker gehörende Domain ausgestellt worden. Das einzige was bei diesem Angriff den Anwender davor warnen kann, dass die Verbindung vom Hacker abgehört und manipuliert wird, ist der Warnhinweis des Browsers, dass Webseite und Zertifikat nicht zusammenpassen.

Warnungen vor falschen Sicherheitszertifikaten dürfen daher nicht ignoriert werden.

10.2. Zertifikate richtig erstellen

10.2.1. Der Rechnername

Der Name, (oder die IP) den Sie im Webbrowser, E-Mail-Programm etc. eingeben um den Server anzusprechen, muss genau mit dem Feld Rechnername (CN) im Zertifikat übereinstimmen. Das heißt, wenn Sie den Intranator z.B. über die Rechnernamen `intranator.net.lan` und `meinintranator.dyndns.org` ansprechen wollen, benötigen Sie 2 verschiedene Zertifikate.

Der Intranator bietet daher die Möglichkeit, ein Zertifikat für die interne Schnittstelle und ein anderes für die Internet-Schnittstelle zu konfigurieren.

Damit die Prüfung des Rechnernamens durchgängig funktionieren kann, muss der Intranator von allen Clients im lokalen Netz unter seinem konfigurierten DNS-Namen erreichbar sein. Beachten Sie daher unbedingt Abschnitt 9.3, „Domain und DNS“ und testen, ob der Intranator unter seinem vollständigen Namen (also inkl. Domain) auch von den Clients im lokalen Netz erreichbar ist.

Wir raten davon ab, eine IP-Adresse als Rechnernamen im Zertifikat zu hinterlegen.

10.2.2. Konfiguration

Öffnen Sie die Seite System > Schlüssel > Eigene Schlüssel und legen einen neuen Schlüssel an. Der Name ist egal, es macht aber Sinn, hier den Rechnernamen zu verwenden.

Als Schlüssellänge empfehlen Institutionen wie das BSI bzw. Bundesnetzagentur momentan 2048 Bit (siehe Algorithmenkatalog bei der Bundesnetzagentur).

Tragen Sie in das Feld Rechnername (CN) den Rechnernamen (siehe oben) ein. Alle anderen Felder können Sie entweder leer lassen oder nach Belieben füllen.

Wurde der Schlüssel angelegt, können Sie ihn unter System > Weboberfläche > Sicherheit verwenden. Bei Server Schlüssel für SSL wählen Sie den Schlüssel aus, der für Verbindungen aus dem lokalen Netz genutzt werden soll. Bei SSL Server Schlüssel für Verbindungen aus dem Internet wählen Sie den Schlüssel für Verbindungen aus dem Internet.

10.3. Zertifikate auf Clients installieren

Wenn Sie neue Zertifikate selbst erstellt haben, sind sie auf dem Client noch nicht bekannt. Die Clientsoftware warnt Sie daher vor einem Schlüssel von unbekannter Zertifizierungsstelle.

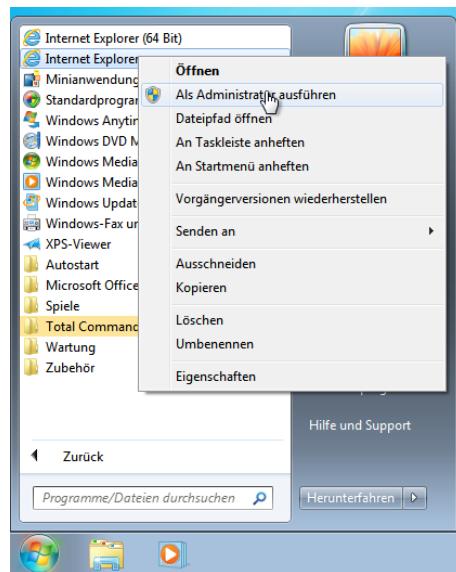
Bauen Sie die Verbindung auf und installieren Sie das Zertifikat im Client. Bei folgenden Sitzungen darf Sie das Programm nicht mehr vor ungültigen Zertifikaten warnen.

10.3.1. Installation unter Windows

Im Folgenden wird beschrieben, wie Sie das Zertifikat des Intranators in das Zertifikatssystem von Windows installieren. Beachten Sie, dass einige Programme (wie z.B. Mozilla Firefox) ihr eigenes Zertifikatssystem mitbringen. Sollen solche Programme mit dem Intranator genutzt werden, muss das Zertifikat dort zusätzlich installiert werden.

1. Starten Sie den Internet Explorer als Administrator. Klicken Sie dafür in der Startleiste mit Rechts auf den Programmnamen und wählen dann Als Administrator ausführen. Es kann kein anderer Browser verwendet werden und es müssen administrative Rechte für das Programm verfügbar sein.

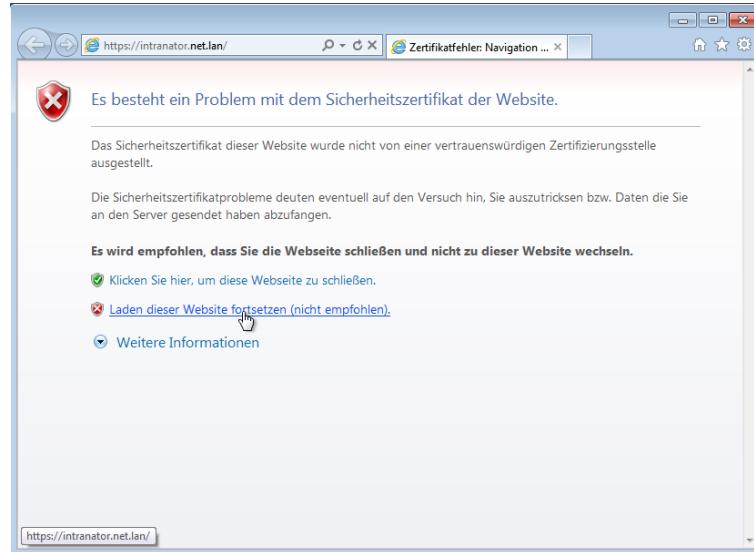
Unter Windows XP und 2003 ist ein Ausführen als Administrator nicht notwendig.



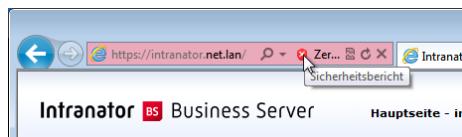
2. Öffnen Sie die Oberfläche des Intranator Business Servers per https. Hier im Beispiel wird <https://intranator.net.lan> verwendet. Ersetzen Sie dies durch den vollständigen Rechnernamen inkl. Domain Ihres Intranator Business Servers.

Greifen Sie unbedingt über einen DNS-Namen zu, verwenden Sie nicht die IP. Sollte der Intranator Business Server nicht per DNS-Namen erreichbar sein, müssen Sie evtl. die DNS-Konfiguration anpassen. Dies wird im Abschnitt 9.3, „Domain und DNS“ beschrieben.

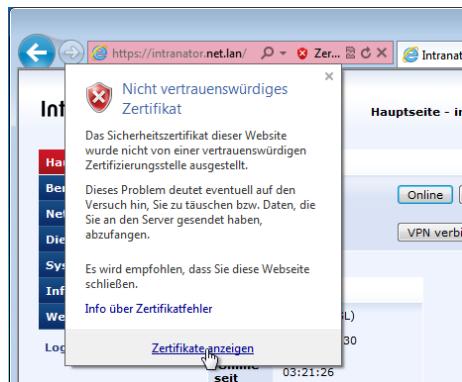
3. Der Internet Explorer erkennt die Zertifizierungsstelle des Servers noch nicht als vertrauenswürdig. Werden zusätzlich noch andere Zertifikatsprobleme erkannt, muss zuerst das Zertifikat des Intranator Business Servers angepasst werden. Dies wird im 10. Kapitel, „SSL-Verschlüsselung und Zertifikate“ beschrieben.



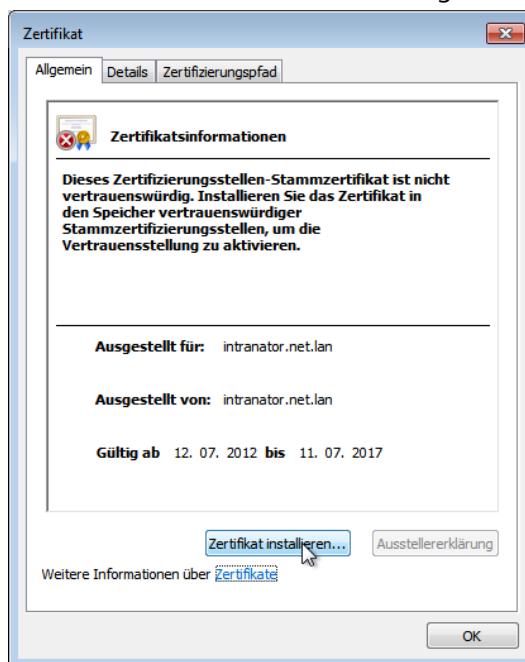
4. Klicken Sie auf Laden dieser Webseite fortsetzen (nicht empfohlen).
5. Klicken Sie auf das rote Schild in der URL-Zeile um sich den Sicherheitsbericht anzeigen zu lassen.



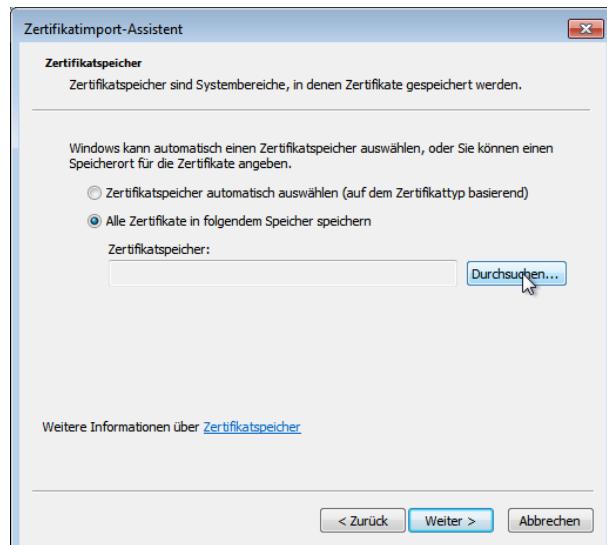
- Klicken Sie im Sicherheitsbericht auf Zertifikate anzeigen.



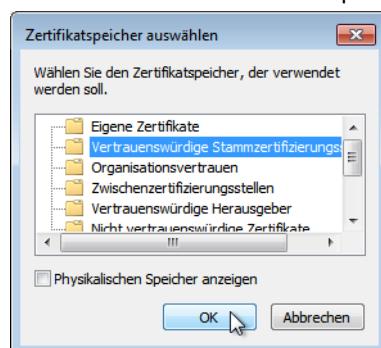
- Klicken Sie in der Zertifikatsanzeige auf Zertifikat installieren. Ist diese Schaltfläche nicht vorhanden, so fehlen die nötigen Administrationsrechte.



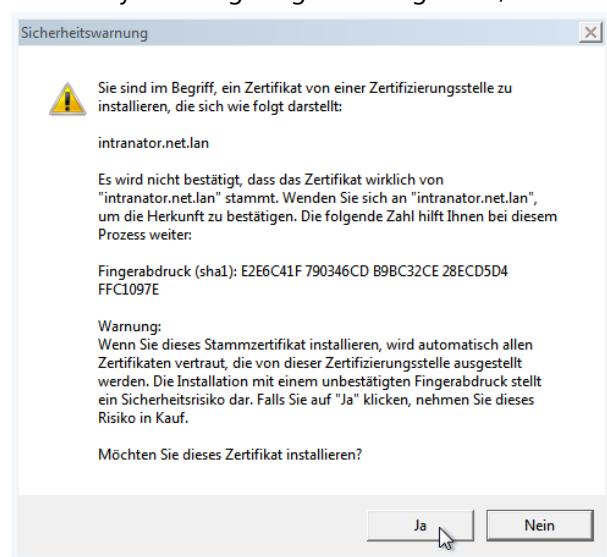
- Es öffnet sich ein Assistent zum Zertifikatsimport. Lassen Sie das Zertifikat in einem ausgewählten Speicher speichern und klicken auf Durchsuchen... zur Auswahl des Zertifikatsspeichers.



- Wählen Sie den Zertifikatsspeicher Vertrauenswürdige Stammzertifizierungsstellen.



- Schließen Sie den Assistent ab. Sie bekommen eine Sicherheitswarnung vom Betriebssystem angezeigt. Bestätigen Sie, dass Sie das Zertifikat installieren möchten.



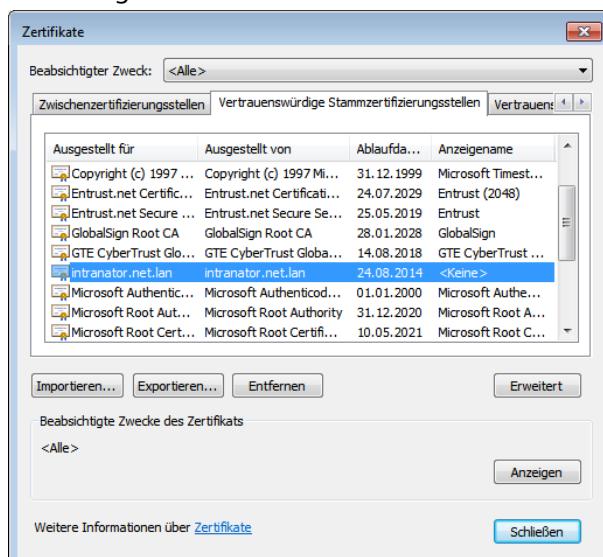
- Schließen Sie den Internet Explorer.
- Öffnen Sie den Internet Explorer erneut, diesmal nicht mit Administratorrechten, sondern mit normalen Benutzerrechten.

13. Öffnen Sie wieder die Oberfläche des Intranator Business Servers. Diesmal darf keine Zertifikatswarnung erscheinen. Neben der URL wird ein Schlosssymbol angezeigt.



Sollte es bei der Installation des Zertifikats zu Problemen kommen, finden Sie hier einige Punkte, die Sie kontrollieren sollten:

- Öffnen Sie im Internet Explorer die Internetoptionen, Reiter Inhalte und klicken auf Zertifikate. Das Zertifikat des Intranators sollte im Reiter Vertrauenswürdige Stammzertifizierungsstellen enthalten sein.



- Wird das Zertifikat dort nicht angezeigt, suchen Sie, ob es nicht in einem anderen Zertifikatsspeicher enthalten ist. Installieren Sie es dann erneut und wählen diesmal Vertrauenswürdige Stammzertifizierungsstellen als Ziel aus.
- Bei einigen Versionen von Windows gibt es einen bekannten Fehler bei den Berechtigungen zum Zertifikatsspeicher. Weitere Informationen finden Sie unter <http://support.microsoft.com/kb/932156>.
- Bei einigen Systemen haben wir im Zusammenhang mit Imaging-Systemen Probleme mit dem Eigentümer des Zertifikatsspeichers beobachtet. In diesem Falle muss über den Registry-Editor der Eigentümer dieses Schlüssels auf den aktuellen Benutzer umgestellt werden: `HKEY_CURRENT_USER\Software\Microsoft\SystemCertificates\Root\ProtectedRoots`. Vergeben Sie danach Leserechte für den Benutzer.

10.3.2. Verteilen von Zertifikaten über Active Directory

Werden die Client-PCs mit einem Active Directory verwaltet, kann man dieses nutzen um das Zertifikat des Intranators an alle zu verteilen.

Exportieren Sie dazu das verwendete Zertifikat aus dem Intranator über das Menü System > Schlüssel > Eigene Schlüssel als .cer-Datei.

Befolgen Sie dann die Hinweise von Microsoft zur Verteilung des Zertifikats: <http://technet.microsoft.com/de-de/library/cc758128.aspx>

10.4. Benutzer sensibilisieren

1. Die Benutzer dürfen sich auf keinen Fall daran gewöhnen, dass Sie Zertifikatswarnungen des Browsers einfach so akzeptieren. Daher müssen die Zertifikate von Anfang an auf den Rechnern korrekt konfiguriert werden.
2. Erklären Sie den Benutzern, dass Sie vor allem beim Zugriff von außen (z.B. auf Web-Groupware) auf keinen Fall eine Zertifikatswarnung akzeptieren dürfen. Stattdessen soll der IT-Verantwortliche oder der Intranator-Fachhändler kontaktiert werden.

10.5. Verwenden einer externen Zertifizierungsstelle

Es gibt viele Zertifizierungsstellen (Certificate Authority, abgekürzt CA), die das Erstellen von Zertifikaten als Dienstleistung anbieten. Diese Zertifizierungsstellen sind in den meisten Browsern von vorneherein als vertrauenswürdig hinterlegt. Damit muss also auf den Clients vor der Nutzung nicht zuerst ein Zertifikat installiert werden.

Zertifizierungsstellen signieren aber nur Zertifikate mit offiziellen, extern erreichbaren DNS-Namen. Es ist also nicht möglich eine Zertifizierungsstelle für lokale DNS-Namen (wie z.B. `intranator.net.lan`) oder IP-Adressen zu nutzen.

Um ein solches Zertifikat mit dem Intranator zu verwenden, gehen Sie am besten wie folgt vor:

1. Konfigurieren Sie einen DNS-Namen für die externe IP des Intranators in einer offiziellen Domain die Ihnen gehört (z.B. `mail.meinedomain.de`).
2. Erstellen Sie auf dem Intranator ein Zertifikat und tragen dabei den externen DNS-Namen unter Rechnername ein.
3. Wählen Sie eine Zertifizierungsstelle aus. Eine kurze, unvollständige Liste einiger Anbieter (alphabetisch): Comodo [<http://www.comodo.com/>], GeoTrust [<http://www.geotrust.com/>], GlobalSign [<http://www.globalsign.com/>], Go Daddy [<http://www.godaddy.com/ssl/>], StartSSL [<http://www.startssl.com/>], VeriSign/Symantec [<http://www.verisign.com/>].
4. Kaufen Sie ein Zertifikat über die Webseite der von Ihnen gewählten Zertifizierungsstelle. Es reicht ein einfaches SSL-Zertifikat für eine Webseite. Extended Validation (EV) oder ein Wildcard Certificate sind normalerweise nicht notwendig.
5. Im Verlauf der Zertifikatsausstellung werden Sie von der Zertifizierungsstelle aufgefordert, eine Zertifikatsanforderung (Certificate Request) zu liefern. Diese können Sie aus dem Intranator im Menü System > Schlüssel > Eigene Schlüssel : CA exportieren.
6. Sie bekommen von der Zertifizierungsstelle am Ende 2 Dinge: Ein Zertifikat und eine Zertifikatkette (Certificate Chain oder Intermediate Certificate genannt). Beides importieren Sie im Intranator im Menü System > Schlüssel > Eigene Schlüssel : CA.
7. Achten Sie darauf, dass jedes Zertifikat eine begrenzte Gültigkeitsdauer hat. Kurz vor Ablauf werden Sie normalerweise von der Zertifizierungsstelle darauf hingewiesen, das Zertifikat verlängern zu lassen.

10.6. Verschlüsselungsstärke

Die Kryptographie und die Leistungsfähigkeit von CPUs entwickelte sich in den letzten Jahren schnell weiter. Bisher als sicher geltende Verschlüsselungsverfahren sind mittlerweile als geknackt anzusehen und sollten daher nicht mehr eingesetzt werden. Gleichzeitig gibt es aber auch noch ältere Systeme, die mit neueren Verfahren noch nicht umgehen können.

Der Intranator erlaubt daher eine gezielte Steuerung der angebotenen Verschlüsselungsverfahren, getrennt nach Verbindungen im lokalen Netz und Internet. Diese ist zu finden im Menü System > Weboberfläche > Sicherheit. Die dort gewählten Einstellungen gelten für die mit SSL bzw. TLS gesicherten Verbindungen bei folgenden Protokollen bzw. Diensten: Die Weboberfläche und Webgroupware, ActiveSync, POP3(S), IMAP(S) und SMTP-Submission.

Für jeden der beiden Bereiche gibt es dabei folgende Optionen:

Schwach	Erlaubt Verbindungen mit schwachen und als geknackt geltenden Verschlüsselungsverfahren wie z.B. RC4. Diese Einstellung ist ein Sicherheitsrisiko und sollte nur ausnahmsweise aktiviert werden.
Windows XP kompatibel	Erlaubt schwächere Verschlüsselung und Schlüssel-Austauschverfahren, um Kompatibilität mit älteren Betriebssystemen wie z.B. Windows XP herzustellen. Diese Einstellung schaltet jedoch das als geknackt geltende RC4-Verfahren ab. Mit neueren Systemen die diese unterstützen, werden automatisch stärkere Verfahren, inkl. PFS, ausgehandelt.
Stark (nur PFS)	Erzwingt PFS für alle Verbindungen. Zusätzlich werden alle Verbindungen nur mit dem AES Verfahren verschlüsselt. Dies ist die empfohlene Einstellung für alle Verbindungen.

Perfect Forward Secrecy (PFS): bewirkt, dass die übermittelten Daten auch dann nicht entschlüsselt werden können, wenn zu einem späteren Zeitpunkt der private Schlüssel des Intranators bekannt werden sollte und eine früher aufgezeichnete Übertragung dann mit Kenntnis des privaten Schlüssels analysiert wird.

Der private Schlüssel kann z.B. durch einen erfolgreichen Angriff auf den Intranator, durch Diebstahl des gesamten Geräts oder staatliche Maßnahmen in die falschen Hände geraten. In diesem Moment könnten ohne PFS alle früheren Verbindungen, sofern sie jemand aufgezeichnet haben sollte, entschlüsselt werden.

PFS handelt beim Verbindungsaufbau einen nur für diese Verbindung geltenden, temporären Schlüssel aus ohne diesen dabei über die Leitung zu übertragen. Dieser wird nach Ende der Verbindung gelöscht und kann daher zu einem späteren Zeitpunkt nicht mehr rekonstruiert und missbraucht werden.

11. Kapitel - Internet

Der Intranator kann für mehrere Provider konfiguriert werden. Fällt ein Provider aus, so kann vollautomatisch auf einen anderen Provider ausgewichen werden.

11.1. Einwahl mit ISDN

Der Intranator kann ISDN Wahlverbindungen aufbauen. Es werden nur HDLC-Wahlverbindungen unterstützt (kein X.75, keine ISDN-Standleitungen, nur Euro-ISDN, kein 1TR6).

Als Protokoll kommt nur syncPPP mit PAP- oder CHAP-Authentifizierung zum Einsatz. ISDN-Datenkompression wird nicht unterstützt, eine Kanalbündelung ebenfalls nicht.

11.2. Einwahl mit DSL (PPPoE)

Der Intranator unterstützt DSL mit PPPoE wie es z.B. von der Deutschen Telekom eingesetzt wird. In den Intranator ist kein DSL-Modem eingebaut, daher muss an eine Netzwerkschnittstelle eines angeschlossen werden und diese auf den Typ „DSL/Router“ konfiguriert werden. Es werden nur DSL-Modems mit Ethernetanschluss unterstützt, keine USB-Modelle.

Von vielen Providern wird bei Vertragsabschluss ein Router mit integriertem Modem mitgeliefert. Einige dieser Router lassen sich in einen Nur-Modem-Modus, manchmal auch PPPoE-Passthrough genannt, schalten. Wenn dies möglich ist, sollten Sie diese Konfiguration wählen. Ist das nicht möglich, sollte der Router durch ein reines DSL-Modem ersetzt werden.

Folgende Gründe sprechen für den Einsatz eines Modems und nicht eines (NAT-)Routers vor dem Intranator:

- Das VPN funktioniert nur eingeschränkt und hinter einigen Routern überhaupt nicht
- Ein automatisches Ausweichen bei Providerfehlern auf einen anderen Provider ist nicht möglich
- Die Konfiguration eines Zugriffs von außen auf den Intranator ist komplexer

Wenn Sie den Intranator an ein VDSL-Modem der Deutschen Telekom anschließen, müssen Sie bei der Option VLAN auf Schnittstelle die VLAN-ID 7 eintragen.

Beim Verbindungsaufbau mit PPPoE ist es wichtig, das Login richtig zu wählen. Weitere Informationen hierzu bekommen Sie von Ihrem Provider. Fragen Sie nach Einwahleinstellungen für Router.

11.3. Einwahl mit DSL (PPTP)

Der Intranator unterstützt DSL auf Basis des PPTP-Protokolls. Es wird vor allem in Österreich eingesetzt, teilweise ist es auch noch in Frankreich und den Niederlanden in Verwendung.

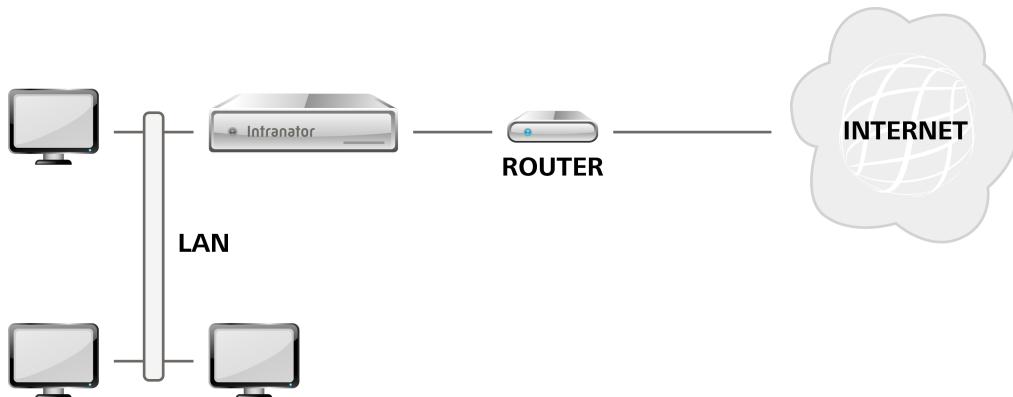
Das DSL-Modem wird wie bei PPPoE über die Ethernetschnittstelle an den Intranator angeschlossen.

Bei PPTP-Verbindungen muss zum Aufbau der Verbindung die IP des DSL Modems einge stellt werden. Bei den allermeisten Modems wird hier die 10.0.0.138 verwendet. Manche Provider vergeben diese IP auch per DHCP. Im Intranator ist beides konfigurierbar.

Bei einigen Providern muss eine spezielle Providerkennung (sog. „Phone“-Feld des PPTP- Protokolls) eingetragen werden. Lassen Sie dieses Feld erst einmal leer und fragen Sie bei Problemen mit dem Verbindungsaufbau beim Provider nach den richtigen Konfigurations- daten.

11.4. Router mit fester IP

Beim Providertyp Router mit fester IP kann an einer auf den Typ „DSL/Router“ konfigurier ten Netzwerkschnittstelle ein Router angeschlossen werden. Der Intranator routet die IP- Pakete dann direkt an diesen weiter.



Geben Sie bei der Konfiguration unter „Lokale IP“ die externe IP des Intranators ein. Diese muss zusammen mit der Router-IP in einem Netz liegen. Dieses darf sich nicht mit dem lokalem Netz oder einem der lokal gerouteten Netze (siehe Abschnitt 9.8, „Routing im Intranet“) überschneiden.

11.5. Router mit DHCP oder Kabelanschluss

Dieser Providertyp wird verwendet, wenn ein Router an einer auf den Typ „DSL/Router“ konfigurierten Netzwerkschnittstelle angeschlossen ist. Die IPs werden per DHCP vom Router erfragt. Dieses Verfahren kommt auch bei Internet über Kabelanschluss (Breitbandkabel, u.a. für Kabelfernsehen) zum Einsatz, hierbei wird der Intranator an das Kabelmodem und nicht an einen Router angeschlossen.



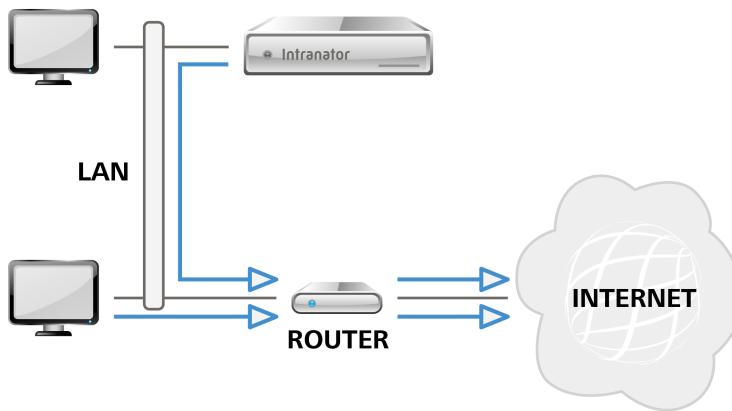
Tipp

Sie müssen das Kabelmodem kurz ausschalten, wenn Sie den Intranator das erste Mal anschließen oder die Netzwerkkarte getauscht haben. Dadurch kann es sich auf die MAC-Adresse des Intranators einstellen.

11.6. Router im lokalen Netz

Soll der Intranator nur eingeschränkt, z.B. nur als E-Mail-Server, verwendet werden, so kann es sinnvoll sein, den Internetzugang für die Rechner im lokalen Netz über einen anderen Router abzuwickeln. Damit auch der Intranator den anderen Router zum Zugang

ins Internet verwenden kann, obwohl er nicht über die externe sondern über die interne Schnittstelle angesprochen wird, gibt es den Providertyp „Router im lokalen Netz“.



In dieser Konfiguration kann die Firewall nur sehr eingeschränkt wirken. Außerdem gibt es Einschränkungen für VPN und Port-Forwarding.

11.7. Offizielle IPs und DMZ

Stehen mehrere offizielle IPs zur Verfügung und soll damit ein Server in einer De-Militarized Zone (DMZ) angebunden werden, so kann dies in drei unterschiedlichen Varianten erfolgen.



Hinweis

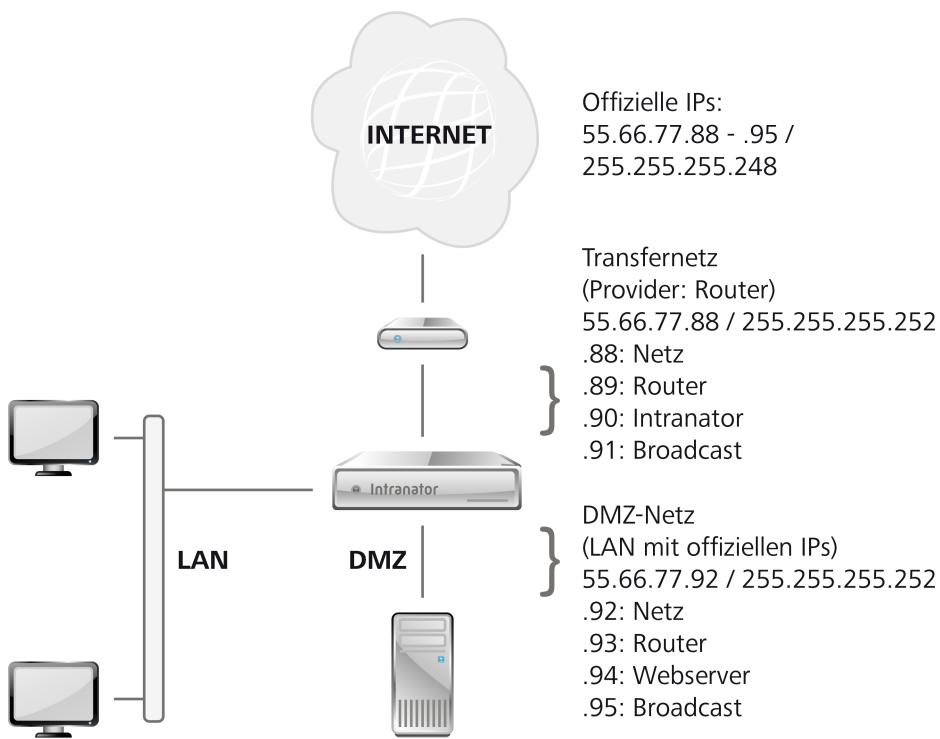
Bitte beachten Sie, dass Sie bei allen Verfahren immer mindestens 8 offizielle IPs benötigen, um (mindestens) einen Server in einer DMZ anbinden zu können.

11.7.1. Klassisches Routing

Vorteile	einfach verständlich, weit verbreitet
Nachteile	Verschwendung von IP-Adressen durch Teilung des Netzes, Subnetz-Routing muss auf dem Router eingetragen werden

Bei dieser Variante wird das vorhandene Netz mit offiziellen IPs in zwei kleinere Subnetze geteilt: Ein sog. Transfernetz zwischen Router und Intranator und ein DMZ-Netz. Da pro Subnetz immer zwei IPs für Netzadresse und Broadcast benötigt werden und der Intranator in beiden Netzen eine IP benötigt, stehen von 8 offiziellen IPs am Ende nur eine für einen Server in der DMZ zur Verfügung.

Auf dem Router muss eingestellt werden, dass das direkt angeschlossene Netz (Transfernetz) verkleinert wurde und dass das DMZ-Netz über den Intranator geroutet wird. Da der Benutzer auf einen vom Provider gestellten Router oft keinen Zugriff hat, muss diese Einstellung der Provider für Sie vornehmen.



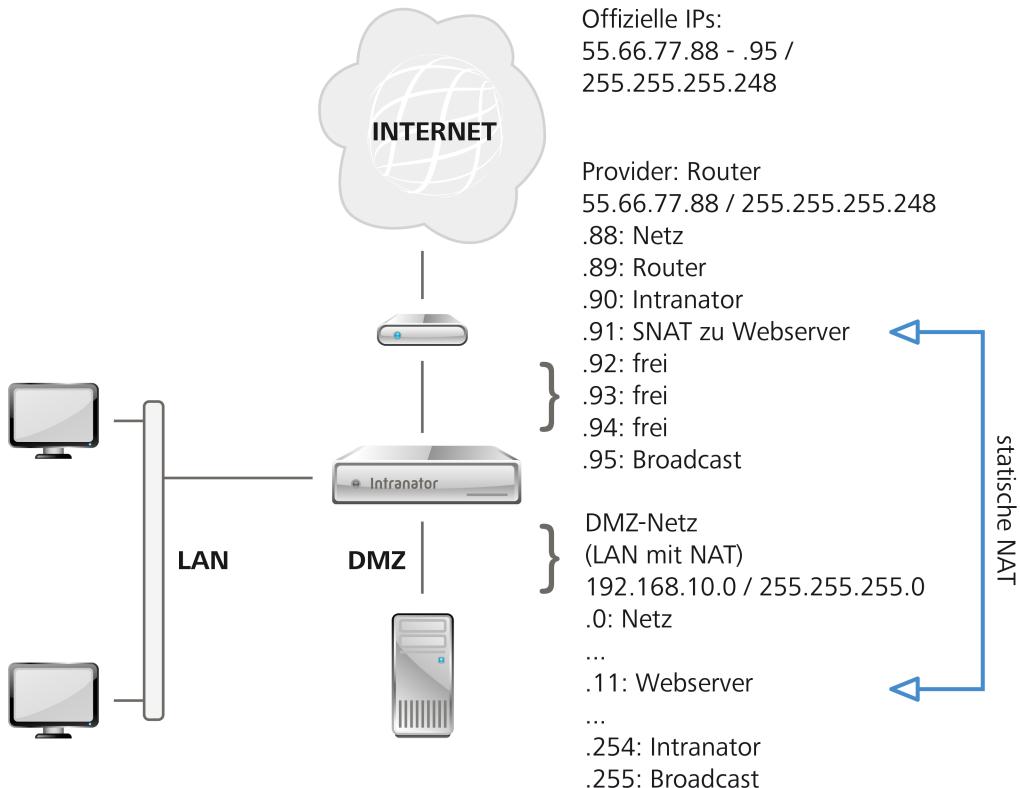
11.7.2. Statische NAT

Vorteile	flexibel, gute Ausnutzung der IPs
Nachteile	funktioniert nicht mit allen Protokollen

Bei dieser Variante wird die DMZ wie ein normales LAN mit IPs aus dem privaten Adressraum (z.B. 192.168.x.x) eingerichtet. Legen Sie alle DMZ-Server unter Netzwerk > Intranet > Rechner an. Im Menü Netzwerk > Firewall > Statische NAT wird dann eine Weiterleitung der offiziellen IP auf den Server in der DMZ konfiguriert.

Der Intranator legt automatisch ein virtuelles Netzwerkinterface beim Provider an, sobald die offizielle IP im Netz zwischen Router und Intranator liegt. Deshalb benötigen Sie auf dem Router keine speziellen Routingeinträge für diese IPs.

Da der Server nur seine IP aus dem LAN - nicht aber seine offizielle - kennt, funktionieren manche Protokolle nicht, denn einige Protokolle übertragen zusätzlich die verwendete IP im normalen Datenstrom. Bei einigen Protokollen kann der Intranator dies kompensieren (z.B. FTP und PPTP), bei anderen aber nicht (z.B. H.323).



11.7.3. Proxy-ARP

Vorteile	funktioniert mit allen Protokollen, gute Ausnutzung der IPs
Nachteile	komplexere Konfiguration

Bei Proxy-ARP wird das Netz zwischen Router und Intranator mit den gleichen Daten ein weiteres mal als DMZ angelegt. Unter Netzwerk > Interfaces tragen Sie für die DMZ den Typ "Proxy-ARP" ein. Geben Sie dem Intranator in diesem Netz die gleiche IP wie Sie sie auch unter Netzwerk > Provider > Profile eingetragen haben. Tragen Sie unbedingt alle Rechner in dem DMZ-Netz einzeln unter Netzwerk > Intranet > Rechner ein. Der Intranator geht davon aus, dass alle dort nicht eingetragenen Rechner in dem Netz zwischen Intranator und Router liegen.

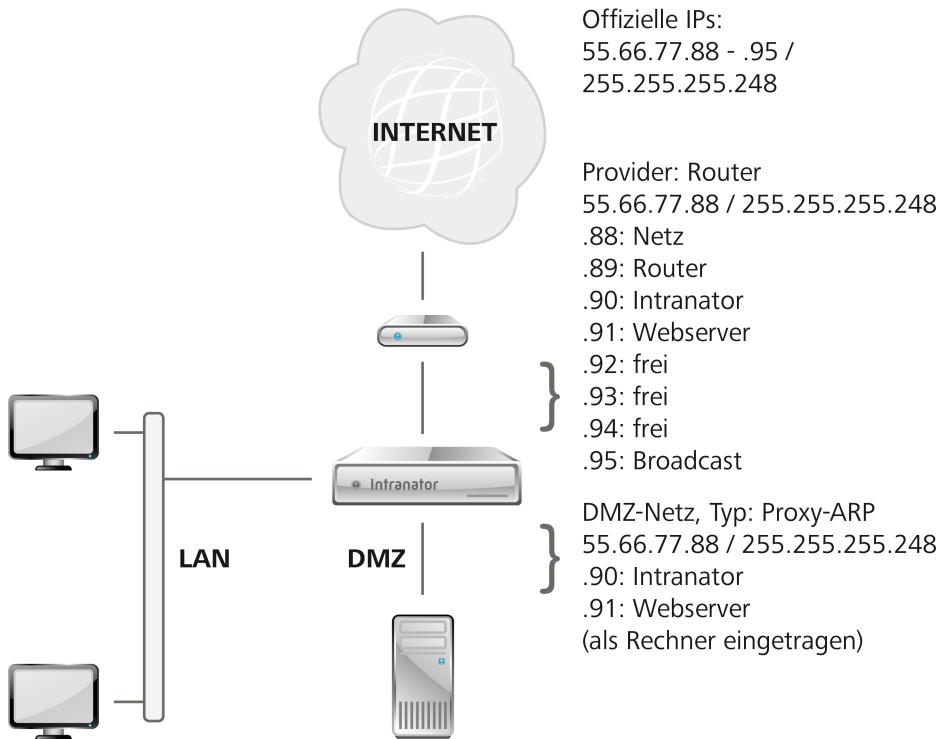
Stellen Sie das Default-Gateway auf dem Server in der DMZ auf den Intranator. Der Intranator vermittelt jetzt zwischen den beiden Netzteilen, ohne dass die beteiligten Rechner davon etwas mitbekommen. Für die Rechner sieht es so aus, als ob es sich um ein einzelnes, größeres Netz handelt. Selbstverständlich kontrolliert die Firewall den Datenverkehr zwischen den beiden Netzteilen.

Auf dem Router müssen Sie für das interne Netz keine speziellen Einstellungen vornehmen.

Achtung



Bei der Erstinstallation kann es leicht zu Problemen mit dem ARP-Cache des Routers kommen. Der Router denkt dann, dass der Server noch im Netz zwischen Router und Intranator liegt. Konfigurieren Sie zuerst den Intranator, dann den Server in der DMZ und starten danach den Router neu um dieses Problem zu vermeiden.



11.8. Verbindungsautomatik

Unter Netzwerk > Provider > Automatik wird festgelegt, welcher Provider normalerweise für den Verbindungsauftbau verwendet wird. Außerdem wird der Modus des Verbindungsauftbaus konfiguriert.

Bei manuellem Verbindungsauftbau geht der Intranator nur Online, wenn ein Benutzer auf der Hauptseite auf Online klickt oder eine zeitgesteuerte Aktion (z.B. automatischer E-Mail-Transfer) gestartet wird.

Bei Verbindungsauftbau bei Bedarf geht der Intranator erst online, sobald ein Rechner mit entsprechenden Firewall-Zugriffsrechten ein Paket ins Internet senden will. Auch zeitgesteuerte Aktionen (wie z.B. automatischer E-Mail-Transfer) lösen einen Wählvorgang aus.

Ist der Intranator auf immer online gestellt, versucht der Intranator ständig eine Verbindung offen zu halten.

Bei manuellem und bei Verbindungsauftbau bei Bedarf bleibt der Intranator solange online, bis der Provider die Verbindung beendet (z.B. durch Zwangstrennung) oder (sofern konfiguriert) die Verbindung für eine gewisse Zeit nicht genutzt wird (Verbindungs-Timeout).

Es kann eine Uhrzeit festgelegt werden, zu der der Intranator auf jeden Fall die Verbindung kurz trennt. Dies kann sinnvoll sein um z.B. eine Zwangstrennung durch den Provider nach 24 Stunden auf eine feste Zeit in der Nacht zu legen. Nach der Zwangstrennung wird die Verbindung nur im Modus immer online sofort wieder aufgebaut.

11.9. Ausweichen auf andere Provider im Fehlerfall (Fallback)

Erkennt der Intranator, dass die Verbindung zu einem Provider gestört ist, kann er automatisch auf einen anderen ausweichen. Dafür wird beim primären Provider im Reiter Einstellungen unter der Option Ausweichprovider (Fallback) der Provider ausgewählt, der im Fehlerfall einspringen soll.

Da ein Ausweichprovider häufig nach Zeit oder Datenvolumen abgerechnet wird oder auch eine langsamere Leitung anbietet, ist es wichtig, auch automatisch wieder auf den primären Provider zurück zu wechseln. Dafür ist die Option Ausweichen für gedacht. Nach Ablauf der dort hinterlegten Zeit wird versucht, wieder die Verbindung zum primären Provider aufzubauen. Ist er weiterhin nicht erreichbar, wird wieder eine Verbindung zum Ausweichprovider aufgebaut.

Sie sollten die Zeit nicht zu kurz (z.B. 3 Minuten) wählen, da dadurch bestehende Verbindungen der Benutzer unterbrochen werden. Es hat sich ein größeres Zeitintervall (z.B. 60 Minuten) als sinnvoll erwiesen.

11.10. Masquerading / NAT

Alle lokalen IP Adressen werden beim Internetzugriff maskiert und auf die externe IP des Intranators umgelegt (n:1 NAT / Masquerading). Nur für IPs aus Netzen mit dem Modus "LAN ohne NAT" wird kein NAT durchgeführt (siehe Abschnitt 9.1, „IPs und Netze“).

Das Masquerading kann einige Protokolle durcheinanderbringen. Die wichtigsten werden vom Intranator vollautomatisch korrigiert:

Aktives FTP, PPTP, IRC, Quake, Cuseeme, Realaudio, Vdolive.

Für die fehlenden (z.B. ICQ oder Gnutella) verfügt der Intranator über einen Socks 5 Proxyserver auf Port 1080. Alle Rechner mit Vollzugriff können diesen ohne extra Login verwenden. Er muss nur unter Dienste > Proxy > Socks aktiviert werden.

Bei einigen Protokollen ist es zusätzlich nötig, die Option „Eingehende Socks Verbindungen aktiviert“ in der Firewallkonfiguration für den entsprechenden Provider zu verwenden.

11.11. Lockruf

Möchte man von außen auf den Intranator zugreifen (z.B. für VPN), dieser ist aber nicht online, so kann man ihn mit der Lockruf-Funktion online schicken.

Unter Netzwerk > Provider > Lockruf kann man eine MSN konfigurieren, auf der der Intranator auf Anrufe wartet. Wird bei einem Anruf auf dieser MSN die angegebene Telefonnummer mit der Rufnummernübertragung übertragen, so geht der Intranator online.

Ist der Intranator bereits online, so gibt es 2 Möglichkeiten: Ist der Standard-Provider ausgewählt, so bleibt er mit dem bisherigen Provider online. Ist ein Provider explizit ausgewählt, so wechselt er bei einem Lockruf auf diesen.

Für den Lockruf wird ein normaler Sprachanruf verwendet. Er kann also z.B. von jedem Handy ausgeführt werden. Es kommt bei einem Anruf kein Freizeichen; nach einer kurzen Pause kommt ein Besetztton und die Meldung „Kein Endgerät erreichbar“ oder eine vergleichbare Meldung des Telefons.

Bei der Telefonnummer können die Wildcards * und ? verwendet werden. Bei „+49-040“ dürfen z.B. alle Hamburger einen Lockruf initiieren.

11.12. DynDNS

Damit der Intranator trotz wechselnder IP Adressen z.B. für VPN oder externen HTTPS-Zugriff über das Internet erreichbar bleiben kann, kann der Intranator seine IP Adresse über DynDNS-Dienste bekanntgeben. Dabei teilt der Intranator seine neue IP nach jeder Einwahl einem DynDNS-Anbieter mit. Über einen normalen DNS-Namen wie z.B. `intranator.dyndns.org` kann man dann auf den Intranator unter seiner momentan verwendeten externen IP zugreifen.

Unter Dienste > DynDNS können Sie mehrere Konten bei verschiedenen DynDNS-Anbietern konfigurieren.

11.12.1. Anbieter

Folgende DynDNS-Dienste werden momentan vom Intranator unterstützt:

Anbieter	Preis	Einstellungen im Intranator
No-IP [http://www.no-ip.com/]	Kostenlos (bis 5 Einträge)	<ul style="list-style-type: none">• Protokoll: dyndns• Alternativer Server: dynupdate.no-ip.com
DNSdynamic [http://www.dnsdynamic.org/]	Kostenlos	<ul style="list-style-type: none">• Protokoll: dyndns• Alternativer Server: www.dnsdynamic.org
ChangeIP.com [http://www.changeip.com/]	Kostenlos	<ul style="list-style-type: none">• Protokoll: dyndns• Alternativer Server: nic.changeip.com
DyNS [http://www.dyns.cx/]	5 US\$ einmalig	<ul style="list-style-type: none">• Protokoll: dysns
Dyn [http://www.dyn.com/dns/]	25 US\$ / Jahr	<ul style="list-style-type: none">• Protokoll: dyndns
Namemaster [http://www.dyndnsfree.de/]	12 € / Jahr	<ul style="list-style-type: none">• Protokoll: dyndns• Alternativer Server: dynup.de
DHS [http://www.dhs.org/]	5 US\$ / Jahr	<ul style="list-style-type: none">• Protokoll: dhs

Alle Angaben ohne Gewähr.

Hier finden Sie eine umfangreiche Liste mit weiteren DynDNS-Anbietern [<http://dnslookup.me/dynamic-dns/>]. Wir können allerdings nicht garantieren, dass diese Anbieter alle mit dem Intranator kompatibel sind.

11.12.2. Aktualisierung und verwendete IP

Für jeden Internetprovider kann unter Netzwerk > Provider > Profile : Dienste eingestellt werden, ob bei einer Einwahl die DynDNS-Dienste (es können zur Sicherheit mehrere gleichzeitig konfiguriert werden) aktualisiert werden sollen.

Die verwendete IP Adresse, ist normalerweise die externe IP des Intranators. Es kann aber vorkommen, dass eine Verbindung mehrfach NAT durchläuft und im Internet daher eine andere Adresse bekannt gegeben werden soll. Dies kann über die Einstellung „DynDNS IP von Webseite holen“ konfiguriert werden. Der Intranator fragt dann vorher einen Webserver nach der IP, von der die Anfrage kommt, und übermittelt diese dann an den DynDNS-Server.

11.13. Zugriff von außen

Der Intranator ermöglicht den Zugriff per POP3S und IMAPS (verschlüsseltes POP3/IMAP4) auf die E-Mails vom Internet aus. Außerdem kann man vom Internet aus per HTTPS auf die Oberfläche und Web-Groupware zugreifen.

Dies wird über die unter Netzwerk > Provider > Profile : Firewall eingestellte Firewallregel-liste konfiguriert.

Für HTTPS Verbindungen ist es möglich, einzustellen, ob nur auf das Webmail-System oder auf die komplette Oberfläche zugegriffen werden soll. Das hängt von den Benutzergruppen ab, in denen der angemeldete Benutzer ist. Die Rechte für den Zugriff von außen werden unter Benutzermanager > Gruppen > Administrationsrechte eingestellt.

Für die Verbindungen von außen ist es sinnvoll, einen anderen SSL-Schlüssel als für die Verbindungen von innen zu verwenden, denn die Browser vergleichen den DNS Namen einer Webseite und den Namen im Schlüssel um sicherzustellen, dass kein Man-in-the-Middle Angriff ausgeführt wird.

Legen Sie also unter System > Schlüssel einen X.509 Schlüssel mit dem DynDNS Namen des Intranators als Rechnername (CN) an (siehe auch Abschnitt 10.2, „Zertifikate richtig erstellen“).

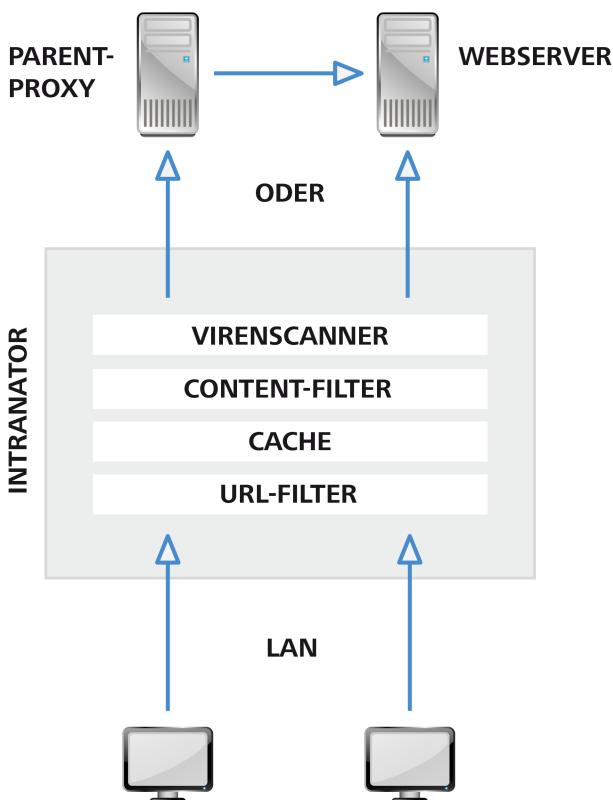
12. Kapitel - Proxy

12.1. Überblick

Der Intranator verfügt über einen HTTP Proxy. Der Proxy kann für folgende Funktionen verwendet werden:

- Beschleunigung des Zugriffs (Cache)
- Filtern von unerwünschtem Inhalt
- Filtern von gefährlichem Inhalt (Viren, Trojanische Pferde, ...)
- Protokollieren aller Zugriffe

Der Proxy ist intern aus verschiedenen Modulen aufgebaut, die diese Funktionen bereitstellen. Da diese Module separat arbeiten, ist es nicht immer möglich, die Einstellungen modulübergreifend vorzunehmen (z.B. für Whitelists).



12.2. Zugang zum Proxy

Der HTTP-Proxy des Intranator liegt normalerweise auf Port 3128. Dies kann aber unter Dienste > Proxy > Einstellungen geändert werden.

Will man den Proxy direkt verwenden, muss man ihn im Browser auf jedem Clientrechner eintragen. Der Proxy kann dann für HTTP, HTTPS und FTP verwendet werden.

Für HTTP kann man auch den Transparenten Proxy verwenden. Dafür muss man auf dem Client nichts einstellen und der Intranator leitet alle HTTP-Zugriffe (transparent für den

Client) auf den Proxy weiter. Der Transparente Proxy funktioniert nicht für HTTPS und FTP. Im Intranator wird der Transparente Proxy über die Firewallregel der Clients aktiviert.

Wenn man mit dem Proxy den Zugriff auf bestimmte Seiten sperren will, sollte man dafür sorgen, dass der Proxy nicht umgangen werden kann. Dies kann durch die Einstellung Proxyzwang in der Firewallregel des Clients erreicht werden.

12.3. Proxykonfiguration

Normalerweise sind über den Proxy nur Zugriffe auf die Zielports 21 und 80, sowie auf 443 für SSL erlaubt. Der Grund dafür ist, dass man die CONNECT-Funktion des Proxys generell auch für andere Protokolle als HTTP nutzen kann und daher eventuelle Firewall-Beschränkungen umgangen werden könnten. Einige Webserver verwenden aber auch andere Ports, wie z.B. 81, 8080 usw. Sollen die Clients diese benutzen können, so müssen sie unter Dienste > Proxy > Einstellungen in die Felder Erlaubte Ports bzw. Erlaubte SSL Ports eingetragen werden.

Normalerweise greift der Proxy direkt auf die angeforderten Server im Internet zu. Es ist allerdings auch möglich, dass der Intranator alle Anfragen an einen anderen Proxy weiterleitet (Parent-Proxy). Dieser kann unter Netzwerk > Provider > Profile : Dienste konfiguriert werden. Damit kann für jeden Provider ein unterschiedlicher Proxy verwendet werden.

12.4. URL-Filter

Der URL-Filter kann Seiten anhand der URL oder IP sperren. Die Zugriffskontrolle geschieht über Proxy-Profile. Diese werden entweder dem Netzwerkobjekt direkt (siehe Abschnitt 9.2, „Zugriffsrechte eines Netzwerkobjekts“), oder bei Proxy-Authentifizierung über die Rechte des angemeldeten Benutzers (siehe Abschnitt 14.1.1, „Zugriffsrechte“) zugewiesen.

12.4.1. Proxy-Profile

Proxy-Profile werden unter Dienste > Proxy > Profile konfiguriert. In einem Profil werden mehrere Proxy-Zugriffslisten zusammengefasst.

Für das Zusammenfassen gelten folgende Regeln:

- Werden mehrere Sperrlisten (gekennzeichnet mit „-“) zusammengefasst, sind alle ihre Seiten gesperrt
- Werden mehrere Freigabelisten (gekennzeichnet mit „+“) zusammengefasst, sind alle Seiten gesperrt, die nicht in mindestens einer Freigabeliste enthalten sind
- Werden Freigabelisten und Sperrlisten zusammengefasst, sind alle in den Sperrlisten enthaltenen Seiten gesperrt. Ist eine Seite sowohl in einer Freigabeliste als auch in einer Sperrliste enthalten, so ist sie freigegeben

12.4.2. Proxy-Zugriffslisten

Zugriffslisten werden unter Dienste > Proxy > Zugriffslisten verwaltet. Eine Zugriffsliste kann entweder hochgeladen (für große Listen), direkt im Browser editiert werden (für kleinere Listen) oder vordefiniert sein. Außerdem gibt es 3 verschiedene Listentypen:

Domain oder URL	hier wird eine komplette Domain oder eine URL gesperrt (oder freigegeben). Beispiel: „www.sex.com/offer“ – hier wird der Zugriff
-----------------	--

	auf www.sex.com/offer explizit gesperrt, nicht aber z.B. auf www.sex.com/free
Wildcard	hier kann das bekannte Wildcard-Zeichen „*“ verwendet werden um Teile der URL zu erkennen. Beispiel: „*.mp3“ – sperrt den Zugriff auf alle URLs bei denen am Schluss „.mp3“ steht; „*sex*“ – sperrt den Zugriff auf alle URLs die irgendwo „sex“ enthalten
Regular Expression	die URLs werden durch POSIX regular expressions geprüft. Für Experten, die wissen, was sie tun

Wurde unter Dienste > Proxy > Einstellungen die Option IP-Adressen der URLs sperren aktiviert, so werden alle Domainnamen in den Zugriffslisten aufgelöst und die dazugehörigen IPs auch gesperrt. Damit ist es nicht möglich, den URL-Filter durch Eingabe einer IP zu umgehen.

12.4.3. Zeitsteuerung

Es ist möglich, den Proxy so zu konfigurieren, dass er abhängig von Tageszeit und Wochentag unterschiedliche Seiten sperrt bzw. freigibt. Damit können z.B. außerhalb der regulären Arbeitszeit oder in Pausenzeiten privat genutzte Webseiten freigegeben werden.

Definieren Sie dazu zuerst unter Dienste > Proxy > Zeiten die gewünschten Zeiträume. Bei der Verwendung von Sperrlisten empfehlen wir, ein Zeitprofil für die eingeschränkteren Uhrzeiten (z.B. "Kernarbeitszeit") anzulegen.

Danach können Sie unter Dienste > Proxy > Profile ein Profil so zusammenstellen, dass einige der Zugriffslisten nur zu bestimmten Uhrzeiten gelten. Wählen Sie dafür in dem Dropdown-Menü Zeitprofil zuerst das passende aus, wählen dann die entsprechende Zugriffsliste und klicken dann auf < um sie zum Profil hinzuzufügen.

Wenn beispielsweise Erotik-Seiten nie erreichbar sein sollen, Webmail-Dienste dagegen nur außerhalb der Kernarbeitszeit, dann fügen Sie die Zugriffsliste Erotik mit dem Zeitprofil Jederzeit, die Zugriffsliste Mail dagegen mit dem Zeitprofil Kernarbeitszeit hinzu.

Beachten Sie, dass ein Proxy-Profil immer nur 2 verschiedene Zeitblöcke enthalten kann: Jederzeit und eines der definierbaren Zeitprofile.

12.5. Web-Content Filter

Der Web-Content Filter untersucht den Inhalt der über den Proxy angeforderten HTML-Seiten. Treten gewisse Worte und Wortkombinationen gehäuft auf, kann die Seite gesperrt werden.

Unter Dienste > Proxy > Webfilter können verschiedene Wortkategorien ausgewählt, sowie der Schwellwert für das Ansprechen (Option Gewichtung des Wortfilters) eingestellt werden.

Sollen einige Domains von der Überprüfung ausgenommen werden, so können diese hier eingetragen werden.

Derzeit ist es weder möglich eigene Wortlisten zu konfigurieren, noch die Wortlisten oder den Schwellwert abhängig vom Clientrechner oder Benutzer einzustellen. Beides ist aber in Planung.

12.6. Proxy-VirensScanner

Der Proxy-VirensScanner kann alle Daten, die den Proxy passieren, auf Viren untersuchen. Dazu wird zuerst die komplette Datei auf den Intranator geladen und dort überprüft. Ist sie virenfrei, wird sie zum Browser durchgelassen. Ist sie infiziert, wird der Transfer sofort abgebrochen.

Da der Benutzer dabei nur eine allgemeine Fehlermeldung angezeigt bekommt, werden gleichzeitig alle folgenden Zugriffe auf eine Hinweisseite umgeleitet („gesperrt“). Dort wird der gefundene Virus, die URL usw. angezeigt. Durch einen Link kann der Benutzer dies bestätigen („entsperren“).

Lädt der Benutzer größere Dateien, bemerkt der Benutzer das Warten auf die komplette Datei. Um dem Benutzer ein Feedback über den Downloadfortschritt zu geben, überträgt der Intranator immer genau ein 1024tel der bei ihm eingegangenen Daten. Zeigt der Browser also z.B. 50 Bytes / Sek. an, so fließen die Daten mit 50 KBytes / Sek. zum Intranator.

Über das HTTP-Protokoll können Multimediadaten auch per Streaming übertragen werden. Da der VirensScanner immer nur komplett Dateien scannen kann, blockiert der Proxy-VirensScanner dies. Um Streaming dennoch zu ermöglichen, kann der Proxy-VirensScanner unter Dienste > Proxy > Antivirus für bestimmte Datentypen und für bestimmte Domains deaktiviert werden.

13. Kapitel - Statistik und Datenschutz

13.1. Proxy-Statistik

13.1.1. Proxy-Protokollierung

Im Menü Information > Statistik > Einstellungen wird konfiguriert, ob der im Intranator enthaltene Proxyserver (siehe 12. Kapitel, „Proxy“) alle Webseitenzugriffe in eine Logdatei protokollieren soll oder nicht. Außerdem können diese Logdateien auch automatisch ausgewertet und aufbereitet werden.

Die Proxy-Logdateien werden, wenn aktiviert, in monatsweise umbrochene Dateien geschrieben. Diese sind im Menü Information > System > Logdateien abrufbar. Sie werden im Standardformat des Squid-Proxys gespeichert. Dabei wird die Zeit als Unix-Zeit in Sekunden seit 1.1.1970 0:00h, UTC angegeben. Wenn Sie die Dateien von Hand durchsuchen möchten, empfiehlt es sich, die Zeit über die Funktion Herunterladen mit normaler Zeit umrechnen zu lassen.

13.1.2. Auswertung

Wenn aktiviert werden die Proxy-Logdateien auf Monatsbasis ausgewertet und als Statistik bereitgestellt. Der aktuelle Monat wird immer zur vollen Stunde aktualisiert. Diese Statistik ist unter Information > Statistik > Proxy abrufbar.

Die Statistik kann über die Auswahlbox in der oberen Zeile nach Webseiten, Rechnern oder Benutzern summiert werden. Eine Darstellung von Benutzerlogins ist nur sinnvoll, wenn der Proxy mit Authentifizierung genutzt wird.

Die Zeilen sind standardmäßig nach Zugriffsdauer sortiert, über einen Klick in die Kopfzeile können sie nach den anderen angezeigten Werten umsortiert werden.

Die Statistik kann von der Übersicht über Webseiten, Rechner und Benutzer weiter auf einzelne Rechner, Webseiten oder Tage eingegrenzt werden. Dies wird über einen Klick jeweils in die erste dargestellte Spalte erreicht.

Über das Pfeilsymbol hinter jeder Webseite kann diese direkt im Browser geöffnet und ihr Inhalt untersucht werden. Soll eine Seite in Zukunft gesperrt werden, so kann sie mit der Checkbox in der letzten Spalte markiert und über den Button unten direkt zu einer URL-Sperrliste hinzugefügt werden.

Viele Webseiten laden Ihren Inhalt, sei es nun Text oder Banner-Werbung, von unterschiedlichen Servern. Sie werden in Ihrer "Top 50 Webseiten" Auswertung deswegen Server wie google-analytics.com, doubleclick.net und weitere finden, welche beim Aufruf auf einer Webseite passiv mitgeladen wurden. Diese Inhalte wurde nicht aktiv vom Benutzer angesteuert.

13.1.3. Methodik

Im Folgenden wird beschrieben, wie die einzelnen Zugriffe kumuliert und in die dargestellten Werte umgewandelt werden.

Um eine Übersicht erst zu ermöglichen, speichert die Statistik nur einen verkürzten Namen der aufgerufenen Webadresse. Aus „<http://www.web.de/shopping/>“ sowie „[web.de/mail/](http://www.web.de/mail/)“ wird in beiden Fällen „[web.de](http://www.web.de/)“.

Die meisten Webseiten bestehen nicht nur aus in HTML formatiertem Text, sondern auch aus Grafiken, Flash-Animationen etc. Um eine einigermaßen aussagefähige Zahl für die Anzahl der aufgerufenen Webseiten zu bekommen, werden für die unter Seitenzugriffe angezeigte Zahl nur die Aufrufe gezählt, bei denen einer der folgenden Datentypen übermittelt wurde:

- text/html
- text/plain
- text/javascript

Nach dem Abruf einer Webseite gibt es für den Proxy leider keine Möglichkeit, genau festzustellen, wie lange eine Seite wirklich gelesen wird. Deswegen kann die Proxy-Statistik die Dauer nur annähernd berechnen.

Für jeden Erstaufruf einer Webseite werden 60 Sekunden Verweildauer angesetzt. Erfolgt innerhalb dieser Minute ein weiterer Zugriff auf den gleichen Server, so wird der zeitliche Abstand zum letzten Zugriff auf die Dauer addiert. Ist der zeitliche Abstand zwischen zwei Zugriffen mehr als 60 Sekunden, so werden die ursprünglichen 60 Sekunden erneut angesetzt. Für die Verweildauer werden nur Abrufe von Datentypen gezählt, die auch als Seitenzugriff gezählt werden (siehe oben).

Bei Zeitraumübersichten wird die Anzahl der Seitenzugriffe einer Stunde zusammengefasst und das dargestellte Quadrat wird umso dunkler, je mehr Zugriffe in dieser Stunde stattfanden.

Wird der Zugriff auf eine Webseite durch einen Proxy-Filtermechanismus blockiert, so wird der Zugriff weiterhin wie ein normaler Zugriff protokolliert und ausgewertet. Eine getrennte Auswertung nach erlaubten und blockierten Zugriffen ist nicht möglich.

13.2. Internet-Zugriffsstatistik

Über diese Statistik können sowohl Übertragungsvolumen und Onlinezeit der einzelnen Internetprovider als auch der an den Intranator angeschlossenen Rechner überwacht werden.

Für die Daten der Providerstatistik wird das tatsächlich übertragene IP-Datenvolumen (ohne Kapselung z.B. in PPPoE) und die Zeit, die der Intranator im Modus Online war, verwendet. Diese Zahlen sollten mit dem übereinstimmen, was Ihnen Ihr Provider in Rechnung stellt.

Die Internet-Zugriffsstatistik wird alle 15 Minuten aktualisiert; der Zeitpunkt der letzten Aktualisierung wird unten angezeigt.

Die einzelnen Statistikseiten wie z.B. die monatliche Übertragungsstatistik aller Rechner können als CSV-Datei exportiert und dann für weitere Analysen in ein Tabellenkalkulationsprogramm importiert werden.

13.2.1. Methodik

Als Übertragungsvolumen der Clients werden Pakete gezählt, die ins Internet oder auf den Proxyserver des Intranators gehen. Sollten über den Proxy Webseiten eines Intranet-Servers abgerufen werden, so können diese Zugriffe die Statistik verfälschen. Sollte ein Client Daten in einen VPN-Tunnel senden, so wird das unverschlüsselte Datenvolumen

gezählt. Die durch Verschlüsselung, Authentifizierung und Kapselung hinzukommenden Daten werden beim Client nicht mitgerechnet.

E-Mail-Transfers zählen nicht zum Transfervolumen eines Clients.

Die Onlinezeit eines Clients ist die Zeit, in der ein zum Übertragungsvolumen gezählter Datentransfer stattfindet. Liegt zwischen 2 Datentransfers eine Zeitspanne, die kleiner ist als der Timeout, so zählt auch diese Zeitspanne zur Onlinezeit. Der Timeout entspricht dem Verbindungstimeout des eingestellten Providers oder beträgt bei ausgeschaltetem Timeout 300 Sekunden.

13.3. Speicherverbrauchsstatistik

Unter Information > Statistik > Speicherplatz wird angezeigt, wie die einzelnen Partitionen des Systems ausgelastet sind und in Vergangenheit waren. Die Systempartition sollte relativ konstant bis leicht steigend ausgelastet sein. Spool- und Logpartition sollten im Normalbetrieb nur zu einem Bruchteil ausgelastet sein.

Bemerken Sie eine starke Auslastung der Partition für E-Mail, Cache und Backup und vermuten ein großes Volumen von E-Mails, können Sie über die Benutzerstatistik herausfinden, welcher Benutzer wie viel Platz mit seinen E-Mails belegt.

13.4. Datenschutz

Vor allem die Auswertungen der Proxy-Logdateien erlauben eine genaue Überwachung des Websurf-Verhaltens einzelner Mitarbeiter. In vielen Fällen kollidiert eine solch detaillierte Auswertung mit Datenschutzbestimmungen. Über die Seite Information > Datenschutz lässt sich daher der Zugriff auf einzelne kritische Funktionen nach dem Vier-Augen-Prinzip einschränken.

Nur ein besonders berechtigter Mitarbeiter (z.B. Betriebsrat) bekommt dafür ein Datenschutzpasswort. Bestimmte Auswertungen sowie die Deaktivierung des Datenschutzpasswortes lassen sich ab dann nur vornehmen, wenn sowohl ein Administrator eingeloggt als auch das Datenschutzpasswort eingegeben ist. Bekommt der besonders berechtigte Mitarbeiter für sein reguläres Benutzerkonto keine Administratorrechte zugewiesen, so ist sichergestellt, dass nur der Administrator und der besonders berechtigte Mitarbeiter gemeinsam die Statistik abrufen können.

Der Unterschied zwischen „vollständigem Zugriff“ und Zugriff ohne Datenschutzpasswort auf die Proxy-Statistiken ist, dass nur bei vollständigem Zugriff die Statistiken einzelner Rechner und Benutzer eingesehen werden können. Andernfalls ist nur die Top 50 der Webseiten sichtbar, die Abrufe können nicht einzelnen Benutzern zugeordnet werden.

14. Kapitel - Benutzermanager

Über den Benutzermanager werden alle Benutzer, Benutzereinstellungen (wie z.B. E-Mail-Adressen und -Weiterleitungen) sowie alle Zugriffsrechte (u.a. für die Administration, Proxy, usw.) verwaltet.

Beim Benutzer selbst werden nur seine Einstellungen gespeichert, die Zugriffsrechte werden ausschließlich über die Benutzergruppen verwaltet.

14.1. Benutzergruppen

Jeder Benutzer erhält seine Zugriffsrechte von den Benutzergruppen, in denen er Mitglied ist. Ein Benutzer kann in beliebig vielen Gruppen Mitglied sein.



Tipp

Sie können unter Dienste > E-Mail > Verteiler eine Mailingliste für eine Gruppe anlegen. Dann können Sie z.B. mit einer E-Mail an `<alle@net.lan>` alle Mitarbeiter erreichen.

Es gibt 2 spezielle Benutzergruppen: Zum einen die Administratoren-Gruppe. Sie hat alle Zugriffsrechte und ist die Einzige, die auf die Konsole zugreifen darf.

Zum anderen die Alle-Gruppe. Alle Benutzer sind Mitglied in dieser Gruppe.



Achtung

Alle Zugriffsrechte, die die Alle-Gruppe erhält, sind ohne Login und Passwort zugänglich. Also kann auch ein Guest ganz ohne Login diese Seiten aufrufen und bearbeiten.

14.1.1. Zugriffsrechte

Alle Rechte, die in mindestens einer Gruppe eines Benutzers erlaubt sind, sind für den Benutzer erlaubt.

Bei den Proxy-Profilen werden alle Profile aus den Gruppen eines Benutzers so zusammengefügt, dass alle Seiten, die in mindestens einer Gruppe erlaubt sind, für den Benutzer erlaubt sind. Weitere Informationen zu Proxy-Profilen finden Sie in Abschnitt 12.4, „URL-Filter“.

Ist der E-Mail-Anhangfilter aktiviert, können eingehende E-Mails anhand der Gruppe mit unterschiedlichen Filterlisten bearbeitet werden. Ist ein Benutzer in mehreren Gruppen mit unterschiedlichen Filterlisten Mitglied, so werden die Filterlisten gemischt. Freigabelisten haben dabei Vorrang vor Sperrlisten. Weitere Informationen zum E-Mail-Anhangfilter finden Sie in Abschnitt 15.7.3, „Anhangfilter“.

Da alle Benutzer automatisch Mitglied der „Alle“-Gruppe sind, sind die Rechte der „Alle“-Gruppe effektiv die Mindestrechte, die Sie Benutzern vergeben können.

E-Mail-Quota ist der Speicherplatz, welchen die Mailboxen der Mitglieder einer Gruppe einzeln maximal belegen dürfen (nicht alle Mitglieder gemeinsam). Ist das Limit erreicht, werden keine neuen E-Mails mehr angenommen (Fehlermeldung „450 Over Quota“ geht nach Ablauf der E-Mail-Warteschlangenzzeit an den Absender). Die meisten IMAP-E-Mail-

Clients zeigen ab einer Belegung von 90% eine Warnung an. Ist der Benutzer in mehreren Gruppen Mitglied, gilt für ihn die größte Quota aus seinen Benutzergruppen.

Über die Option SMTP-Authentifizierung und E-Mail-Relying kann man steuern, ob sich die Mitglieder der Gruppe zum Versand von E-Mails an externe Empfänger am Intranator anmelden können (SMTP-Authentifizierung). Beachten Sie, dass die Mitglieder einer Gruppe mit E-Mail-Relying aus dem Internet unbedingt Passwörter hoher Qualität benötigen. Ansonsten kann das Passwort automatisiert erraten und der Intranator zum Versand von Spam missbraucht werden.

14.1.2. Administrationsrechte

Unter Benutzermanager > Gruppen : Administrationsrechte können Sie im unteren Bildschirmteil den Zugriff auf jede einzelne Seite der Oberfläche reglementieren. Im oberen Teil lässt sich einstellen, ob die unten eingestellten Rechte auch über das Internet genutzt werden können sollen (Fernadministration), oder ob nur Zugriff auf Web-Groupware möglich sein soll.

Außerdem lässt sich einstellen, ob das Aufbauen und Trennen von Internet- und VPN-Verbindungen gestattet ist oder nicht.

Wenn Sie möchten, dass ohne Login die Hauptseite verborgen sein soll, müssen Sie einfach der Alle-Gruppe das Zugriffsrecht „Hauptseite“ entziehen.

14.2. Benutzer

Wird ein Benutzer deaktiviert, so kann er sich nicht mehr einloggen und neue E-Mails werden nicht mehr abgelegt (Fehlermeldung: Over Quota). Die E-Mail-Weiterleitungen sind aber weiterhin aktiv. Wir empfehlen, diese Option z.B. für ausgeschiedene Mitarbeiter, die weiterhin unter ihrer E-Mail-Adresse erreichbar bleiben sollen.

Jeder Benutzer kann, wenn es seine Zugriffsrechte erlauben, u.a. sein Passwort und seine E-Mail-Einstellungen auf den Unterseiten von Benutzermanager > Eigenes Profil selbst ändern.

Alle Passwörter werden automatisch auf ihre Qualität überprüft. Dabei kommen verschiedene Algorithmen zur Mustererkennung und Lexika zum Einsatz. Der Benutzer wird gewarnt, wenn das Passwort nur eine geringe Sicherheit bietet. Unterschreitet ein Passwort eine Mindestqualität, wird es abgelehnt.

14.2.1. Einstellungen für E-Mail und Groupware

Über die Reiter im Menü Benutzermanager > Benutzer können benutzerspezifische Einstellungen für das E-Mail-System vorgenommen werden. Diese werden in Abschnitt 15.5, „E-Mail-Adressierung“, Abschnitt 15.6, „E-Mail-Verarbeitung“ und Abschnitt 15.7.1.5, „Benutzerabhängiger Spamfilter“ näher beschrieben.

Auf dem Reiter Benutzermanager > Benutzer : Groupware können die Standardordner für den Benutzer festgelegt werden. Für jeden Benutzer werden automatisch die E-Mail Standardordner (Entwürfe, Gesendete E-Mails, Papierkorb) vom System angelegt. Die Groupware-Standardordner werden dagegen erst bei der ersten Verwendung der Groupware durch diesen Benutzer angelegt. Die Namen der Standardordner können von E-Mail-Clients über die XLIST-Protokollerweiterung abgerufen werden. Sie werden außerdem von der Webgroupware und ActiveSync verwendet.

Die Einstellungen für Webmail werden in Abschnitt 27.2.2, „Signaturen anhängen“, die für ActiveSync in Abschnitt 29.3.3, „Geräte verwalten und neu synchronisieren“ erklärt.

14.3. Import/Export von Benutzerprofilen

Für eine große Anzahl an Benutzern kann es hilfreich sein, eine Datei extern zu erstellen und dann auf den Intranator zu übertragen. Dies können Sie mit der Import/Export Funktion leicht durchführen. Akzeptiert bzw. ausgegeben werden XML Dateien oder CSV Dateien (Comma Separated Values).

14.3.1. Import von Benutzern

Hier laden Sie eine XML oder CSV Datei mit Benutzern für den Import hoch. Die Feldnamen des XML Imports entnehmen Sie bitte der DTD, die sie in der Import/Export Onlinehilfe herunterladen können. Den Aufbau des CSV Formats entnehmen Sie einer zuvor exportierten CSV Datei.



Hinweis

Bitte beachten Sie, dass die Namen der angegebenen Gruppen mit den Namen der Gruppen im System exakt übereinstimmen muss. Das gleiche gilt für die Erkennung von E-Mail-Domains.

14.3.2. Export von Benutzern

Hier wählen Sie die Benutzer für den Export aus, wahlweise als XML- oder CSV-Format. Die Feldnamen des XML Exports entnehmen Sie bitte der DTD. Den Aufbau des CSV Formats können Sie der CSV Datei entnehmen.

15. Kapitel - E-Mail

15.1. E-Mail-Versand

15.1.1. Rechte

Der Intranator enthält einen SMTP Server für den E-Mail-Versand. Alle Netzwerkobjekte (u.a. Netze, Rechner, VPNs,...), bei denen das Recht „E-Mail Relaying erlaubt“ gesetzt ist (siehe Abschnitt 9.2, „Zugriffsrechte eines Netzwerkobjekts“) und die Firewalleinstellungen Zugriff auf den SMTP-Port erlauben, dürfen den Intranator zum Senden von E-Mails ins Internet (relayen) ohne weitere Authentifizierung verwenden.

Aus Netzen ohne das Recht „E-Mail Relaying erlaubt“ (z.B. auch dem Internet) ist es nach Authentifizierung mit einem aktiven Account aus dem Benutzermanager (siehe Abschnitt 14.2, „Benutzer“) und entsprechenden Rechten (siehe Abschnitt 14.1.1, „Zugriffsrechte“) auch erlaubt.

Der Versand von E-Mails an lokale Adressen des Intranators ist kein Relaying und ist aus allen Netzen, denen die Firewall Zugriff auf den SMTP-Port gestattet, möglich.

15.1.2. SMTP-Submission

Einige Internetprovider erlauben Ihren Kunden keinen direkten Verbindungsaufbau zu TCP-Port 25 (SMTP) um den Versand von Spam zu minimieren. Dadurch ist es dann aber auch nicht mehr möglich, den Intranator zu nutzen, um von unterwegs aus E-Mails zu versenden. Daher unterstützt der Intranator SMTP-Submission auf TCP-Port 587.

Stellen Sie Ihren mobilen E-Mail-Client einfach von Port 25 auf Port 587 um und aktivieren die Authentifizierung mit Ihrem Intranator-Benutzernamen. Außerdem sollten Sie die Verschlüsselung per TLS aktivieren (in manchen Programmen fälschlicherweise SSL genannt).

15.1.3. Versandmethoden

E-Mails ins Internet können entweder direkt an den Zielserver oder an einen SMTP-Relayserver gesendet werden, der dann den weiteren Versand übernimmt. Relayserver bieten eigentlich alle Provider von Webseiten, aber auch viele Zugangsprovider an.

Um das Spamaufkommen zu verringern, nehmen die meisten Mailserver keine direkt versendeten Mails mehr von IPs an, die für Einwahl oder DSL genutzt werden. Wir raten daher unbedingt zur Verwendung eines Relayservers.



Hinweis

Die Versand- und Empfangswege von E-Mails sind unabhängig voneinander. Sie können also problemlos z.B. E-Mails direkt per SMTP empfangen, für den Versand aber einen Relayserver verwenden.

15.1.4. Versand über Relayserver

E-Mail-Relayserver werden als Versandprofil unter Dienste > E-Mail > Versand hinterlegt. Um unterschiedliche E-Mail-Versandmethoden für unterschiedliche Internet-Provider zu ermöglichen, werden diese Versandprofile unter Netzwerk > Provider > Profile : Dienste

den verschiedenen Internetprovidern zugewiesen und aktiviert, sobald der Intranator mit dem entsprechenden Provider online ist.

Beinahe alle Relayserver fordern eine Authentifizierung mit Login und Passwort über SMTP-AUTH. Das alte Verfahren SMTP-after-POP kommt heutzutage kaum noch zum Einsatz und sollte auf SMTP-AUTH umgestellt werden.

15.1.5. Direkter Versand

Viele E-Mail-Provider verwenden relativ aggressive Methoden, um dem Empfang von Spam zu reduzieren. Daher wird die Konfiguration und Anbindung der sendenden E-Mail-Server Tests unterworfen, bevor E-Mails durchgelassen werden. Es empfiehlt sich daher in den meisten Fällen, den Versand über einen Relayserver abzuwickeln (siehe voriges Kapitel).

Wer E-Mails direkt versenden will, muss vorher folgende Kriterien erfüllen:

- Vom Provider fest zugewiesene IP-Adresse.
- Die DNS-Rückwärtsauflösung (reverse lookup, PTR-Eintrag) für die IP muss möglich sein und exakt mit dem externen E-Mail-Servernamen des Intranators übereinstimmen. Dieser wird unter Dienste > E-Mail > Einstellungen festgelegt. Wollen Sie die Rückwärtsauflösung eintragen oder ändern, wenden Sie sich an Ihren Zugangsprovider; er muss diese Einstellung für Sie vornehmen. Unter System > Diagnose > DNS können Sie Ihre externe IP eingeben und überprüfen, wie die DNS-Rückwärtsauflösung Ihrer IP eingestellt ist.
- Der unter Dienste > E-Mail > Einstellungen eingestellte externe E-Mail-Servername muss per DNS abfragbar sein (Vorwärtsauflösung, A-Eintrag) und auf die externe IP des Intranators zeigen. Um diesen DNS-Eintrag anzulegen, wenden Sie sich an Ihren Web-space- oder Domain-Provider.
- Die fest zugewiesene IP-Adresse sollte auf den Kunden selbst und nicht den Provider registriert sein. Dies kann beim RIPE unter <http://www.ripe.net/> überprüft werden.

15.2. E-Mail-Empfang auf dem Client (POP oder IMAP)

Jeder Benutzer bekommt automatisch einen E-Mail-Account mit seinem Namen auf dem Intranator. Es kann per POP3 und IMAP4 auf diesen Account zugegriffen werden, eine Umstellung auf dem Intranator ist dafür nicht nötig.

Wir empfehlen für den Transfer der E-Mails vom Intranator zum Client das IMAP-Protokoll zu verwenden. Denn IMAP bietet folgende Vorteile:

- Alle E-Mails (inkl. abgelegter E-Mails in ihren Ordnerstrukturen) sind zentral zugänglich. Zugriff ist auch per Webmail, Notebook oder Organizer möglich.
- Das IMAP-Protokoll erlaubt es, nur Teile einer E-Mail herunterzuladen. Beim Prüfen auf wichtige Nachrichten, z.B. per Mobilfunk, müssen große Attachments nicht heruntergeladen werden.
- Mehrere Benutzer können gleichzeitig auf einen Account zugreifen. Bei gemeinsam genutzten Accounts (wie z.B. Faxeingang, Info oder Sales) kommt es daher nicht dazu, dass mehrere Mitarbeiter eine E-Mail beantworten.

- Über die Rechteverwaltung von IMAP ist es möglich, anderen Benutzern bestimmte Rechte (z.B. nur Leserechte) für einzelne Ordner zu geben. Dies ist z.B. für das Sekretariat oder Urlaubsvertretung hilfreich.
- Die E-Mails auf dem Intranator werden automatisch mit ins Backup einbezogen und gehen daher bei einem Defekt des Clientrechners nicht verloren.
- Alle E-Mails liegen auf dem Server, deshalb bedeutet ein Absturz des Mailprogramms oder der Wechsel zu einem anderen Programm keinen Verlust von E-Mails.

Der Intranator verwendet intern den Cyrus-Mailserver. Er wurde von der Carnegie Mellon University entwickelt und wird dort und anderswo zur Verwaltung von mehreren 10.000 E-Mail-Accounts eingesetzt. Auch größere Ordnerstrukturen oder Ordner mit 100.000 E-Mails werden ohne Schwierigkeiten unterstützt.



Hinweis

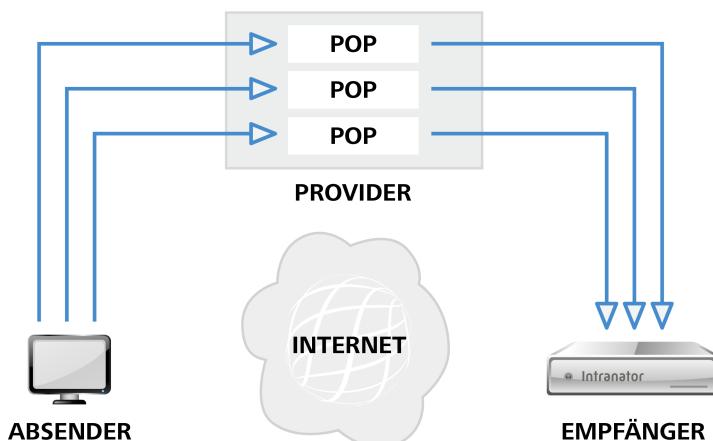
Wir raten bei Verwendung von POP3 dringend davon ab, die Option E-Mails für *n* Tage auf dem Server belassen im E-Mail-Client zu aktivieren, denn dem POP3-Protokoll fehlen die für eine zuverlässige Funktion nötigen Operationen. Verwenden Sie statt dessen IMAP.

15.3. E-Mail-Empfang auf dem Intranator

15.3.1. Konzepte

Es gibt 3 verschiedene Konzepte, wie eingehende E-Mails auf den Intranator kommen können.

15.3.1.1. Abruf einzelner POP-Konten



Bei einem Provider wird für jede E-Mail-Adresse ein eigenes POP-Postfach angelegt. Der Intranator holt jedes dieser Postfächer separat ab und stellt den Inhalt an den Empfänger zu.

Vorteile:

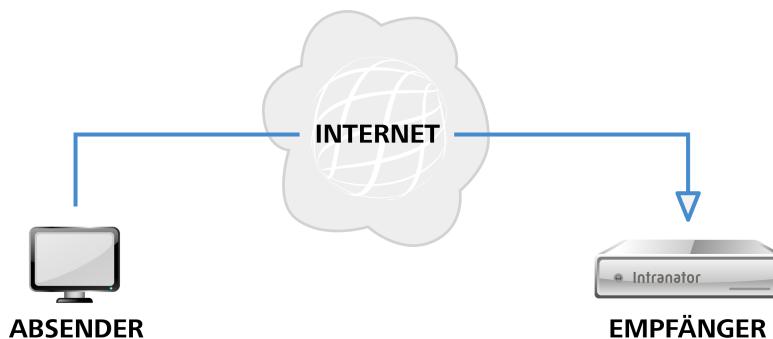
- Bei fast allen Providern verfügbar

- Keine Nichtzustellbarkeits-E-Mails (Bounces), da der Provider alle gültigen Adressen kennt

Nachteile:

- Bei vielen Konten höherer Administrationsaufwand
- Konten werden sequentiell abgearbeitet; bei hoher Anzahl an Konten daher höherer Zeitbedarf

15.3.1.2. Direkte Zustellung per SMTP



Der Absender sendet die E-Mails direkt und ohne zwischengeschalteten Provider zum Intranator.

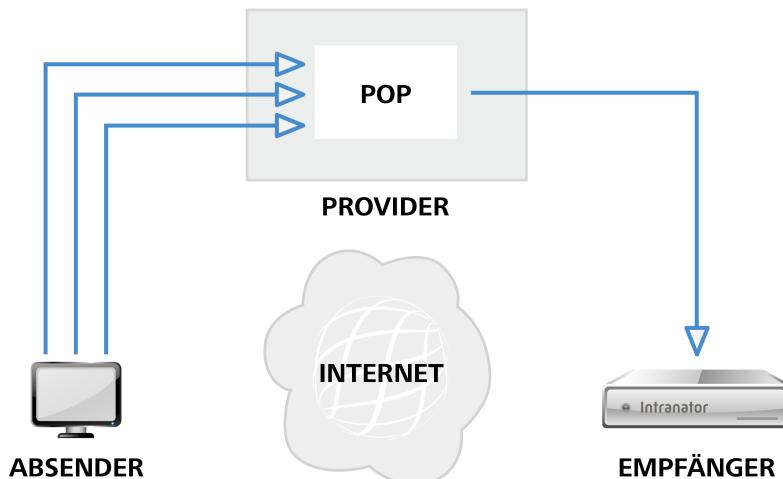
Vorteile:

- Neue E-Mails kommen sofort an
- Keine Nichtzustellbarkeits-E-Mails (Bounces)

Nachteile:

- Es wird eine fest zugewiesene IP-Adresse benötigt

15.3.1.3. Abruf von POP-Sammelkonten (Multidrop, Catch-All)



Alle E-Mails für eine Domain werden bei einem Provider in einem einzigen POP-Konto gesammelt. Der Intranator ruft dieses Konto ab und teilt die E-Mails dann auf die passenden Empfänger auf.

Vorteile:

- Geringerer Administrationsaufwand, da beim Provider nur ein Konto gepflegt werden muss.

Nachteile:

- Kein Standard für Multidrop-Kopfzeile
- Nur bei sehr wenigen Provider funktioniert es vollständig (Mehrere Empfänger in einer Domain, BCC, ...)
- Nichtzustellbarkeits-E-Mails (Bounces) nicht vermeidbar

15.3.1.4. Empfehlung

Wir empfehlen bis zu einer Anzahl von ca. 15 Benutzern den Abruf einzelner POP-Konten. Bei mehr Benutzern bietet sich dann die direkte Zustellung per SMTP an.

Von der Verwendung von POP-Sammelkonten (Multidrop, Catch-All) raten wir generell ab.

15.3.2. Abruf einzelner POP-Konten

Sollen E-Mails von einem einzelnen POP3-Konto bei einem Provider abgeholt werden, so kann dies unter Dienste > E-Mail > Abholen konfiguriert werden. Es können für einen Benutzer beliebig viele externe Konten eingetragen werden.

Unter Verschlüsselung kann eingestellt werden, wie weit die Verbindung zum Server verschlüsselt wird. Bei manchen schlecht konfigurierten Servern führt die automatische Verschlüsselungserkennung zu Problemen beim Verbindungsaufbau. Hierfür ist der Modus "Keine" Verschlüsselung gedacht.

15.3.3. Direkte Zustellung per SMTP

Haben Sie eine feste IP, ist es möglich die E-Mails direkt vom Absender zum Intranator senden zu lassen. Dazu müssen Sie Ihre statische IP von Ihrem Domain-Provider (normalerweise der, der auch für die Webseite zuständig ist) als MX (MailExchange) in der Domain eintragen lassen. Außerdem müssen Sie den SMTP-Port in der Firewall öffnen (siehe Abschnitt 34.3, „Providerprofile“).

Die direkte Zustellung von eingehenden E-Mails per SMTP ist vollkommen unabhängig vom Versand der E-Mails. Die strengen Kriterien für den direkten E-Mail-Versand aus Abschnitt 15.1.5, „Direkter Versand“ haben hier keine Relevanz und ein Versand über Relayserver ist problemlos möglich.



Achtung

Verwenden Sie den Intranator mit dynamischen IPs und DynDNS auf keinen Fall zum direkten Empfang per SMTP, auch wenn einige DynDNS-Provider

dies anbieten, denn beim Wechsel der IP oder einer Leitungsstörung können Fremde Ihre E-Mails empfangen.

15.3.4. Abruf von POP-Sammelkonten (Multidrop)

Der Intranator kann die E-Mails für eine Domain per Multidrop aus einem POP3 Konto abholen und dann verteilen.



Achtung

Wegen der massiven Nachteile (siehe oben) rät Intra2net von der Verwendung dieses Verfahrens generell ab!

Der Provider muss die Möglichkeit anbieten, alle E-Mails für eine Domain in ein Konto zu speichern oder einen „Catch-All“ Account einzurichten, an den alle E-Mails mit unbekanntem Empfänger gehen.

Außerdem wird zum Verteilen ein sog. Multidrop Header benötigt, den der Mailserver des Providers in den Kopf der E-Mail einfügen muss. In ihm wird der wirkliche Empfänger (Envelope / RCPT-To) der E-Mail gesichert.

Es gibt jedoch verschiedene Typen von Multidrop-Headern:

Normaler Header	Er heißt z.B. X-Envelope-To:, Envelope-to:, X-Original-To: oder X-RCPT-To: und enthält nur die E-Mail-Adresse des Empfängers. Dieser Typ wird hauptsächlich von der Exim Software angeboten. Tragen Sie den Namen des Headers (mit Doppelpunkt) in das „Multidrop Header“ Feld ein.
Qvirtual	Er heißt Delivered-To: und wird hauptsächlich von Qmail verwendet. Er enthält vor der eigentlichen Empfängeradresse eine Domänenkennung. Tragen Sie die Domänenkennung in das „Multidrop Header“ Feld ein. Beispiele dafür sind „mbox-ihredomain.de-“ oder „ihredomain.de-“
Received	Die E-Mail enthält keinen Multidrop-Header. Der Intranator versucht, die Empfängeradresse aus den Received-Informationen im Header zu ermitteln. Dies kann bei manchen Providern zu Problemen führen. Einige E-Mails werden dann an den Postmaster (siehe Abschnitt 15.11, „Weitere Einstellungen“) zugestellt. Diese Option ist daher nur als Notlösung gedacht, falls ein Provider keinen Multidrop-Header überträgt.



Tipp

Ist der Provider nicht in der Lage, zuverlässig Envelope-Header einzufügen, so empfiehlt es sich, bei einem anderen Provider (z.B. 1&1) für wenige Euro pro Monat eine Domain extra für den Mailempfang einzurichten (z.B. „meine-firma-mail.de“). Der bisherige Provider kann dann alle E-Mails an die Domain 1:1 an die neue Domain weiterleiten.

Beispiel 15.1. Beispielausschnitt aus einem E-Mail-Header mit normalem Envelope-Header

```
Received: from localhost (localhost.localdomain [127.0.0.1])
      by fire.local (8.11.6/8.11.6) with ESMTP id g3SM02D10977
      for <gerd@localhost>; Mon, 29 Apr 2002 00:24:02 +0200
Envelope-to: gerd@klickmich.de
Delivery-date: Sun, 28 Apr 2002 21:22:01 +0200
Received: from pop.kundenserver.de [212.227.126.129]
      by localhost with POP3 (fetchmail-5.9.0)
      for gerd@localhost (single-drop); Mon, 29 Apr 2002 00:24:02 +0200 (CEST)
Received: from [4.43.46.11] (helo=intranator.net.local)
      by mxng00.kundenserver.de with smtp (Exim 3.22 #2)
      id 171uF3-0007Sd-00
      for gerd@klickmich.de; Sun, 28 Apr 2002 21:21:50 +0200
Message-ID: <j60jo.a5626@intranator.net.local>
To: gerd@klickmich.de
Subject: Test
```

Das einfache To: ist kein Multidrop-Header!

Beispiel 15.2. Beispielausschnitt aus einem E-Mail-Header mit Qvirtual-Header

```
Return-Path: <k.schuster@irgendwo.de>
Delivered-To: klickmich.de-m.muster@klickmich.de
Received: (qmail 29628 invoked from network); 30 Jun 2002 14:47:38 -0000
Received: from moutng1.kundenserver.de (212.227.126.171)
      by pluto.link-m.de with SMTP; 30 Jun 2002 14:47:39 -0000
Received: from [212.227.126.162] (helo=mrelayng1.schlund.de)
      by moutng1.kundenserver.de with esmtp (Exim 3.22 #2)
      id 17OfzF-0003jP-00
      for m.muster@klickmich.de; Sun, 30 Jun 2002 16:47:37 +0200
Received: from [217.81.153.239] (helo=intranator.net.local)
      by mrelayng1.schlund.de with asmtmp (Exim 3.35 #1)
      id 17OfzF-0002Mf-00
      for m.muster@klickmich.de; Sun, 30 Jun 2002 16:47:37 +0200
Received: from storm (storm.net.local [172.16.1.2])
      by intranator.net.local (8.11.6/8.11.6) with SMTP id g5UElmD25862
      for <m.muster@klickmich.de> Sun, 30 Jun 2002 16:47:48 +0200
Message-ID: <001d01c22045$12856700$020110ac@storm>
From: "Karl Schuster" <k.schuster@irgendwo.de>
To: <m.muster@klickmich.de>
Subject: Beispiel
```

Interessant ist hier der „Delivered-To:“ Header. In diesem Beispiel ist die Domänenkennung „klickmich.de-“. Tragen Sie diese in das „Multidrop-Header“ Feld im Intranator ein.

Wird der Multidrop-Header nicht korrekt eingestellt, so werden alle E-Mails, bei denen nicht der wirkliche Empfänger in To: steht, an den Postmaster geschickt. Dies sind z.B. E-Mails mit BCC:, weitergeleitete E-Mails, E-Mails von Mailinglisten oder Spam.

15.4. Weiterleitung von gesamten Domains

15.4.1. Konzept

Bei jeder Domain besteht die Möglichkeit, die E-Mails nicht an die Benutzer des Intranators zuzustellen, sondern sie einem anderen Mail- oder Groupwareserver (z.B. Microsoft

Exchange oder Lotus Domino) zu übergeben. Diese Weiterleitung erfolgt nach der Prüfung auf Viren, verbotene Anhänge und dem globalen Spamfilter.

Unter Dienste > E-Mail > Domains : Weiterleitung kann diese Weiterleitung für jede Domain eingerichtet werden.

Es besteht die Möglichkeit, die Zieldomain der weitergeleiteten E-Mails zu ändern. Wenn Sie also z.B. die Domain **beispiel.de** auf dem Intranator empfangen und bei Domain Adressänderung **xyz.de** eintragen, werden die Zieladressen in allen weitergeleiteten E-Mails auf ...@xyz.de abgeändert. Dies ist vor allem dann hilfreich, wenn der Zielserver nicht umkonfiguriert werden soll.

15.4.2. Empfängeradressprüfung

Kann eine E-Mail nicht zugestellt werden, muss der Absender mit einer Nichtzustellbarkeits-Nachricht (Bounce) darüber informiert werden. Dies gilt natürlich auch für den Fall, dass zwar die Zieldomain vorhanden ist, aber nicht der Benutzer. Sollten Spammer in kurzer Zeit viele E-Mails an ungültige Empfänger senden, kann dieser Mechanismus zu 2 Problemen führen:

- Jede dieser Nichtzustellbarkeits-E-Mails muss an den Absender zugestellt werden und erzeugt dadurch Last. Außerdem sind bei Spam viele Absenderadressen auch wieder falsch und dadurch wird von der anderen Seite wieder eine Nichtzustellbarkeits-Nachricht erzeugt, (Double-Bounce) was die Last weiter erhöht.
- Einige Empfänger betrachten Nichtzustellbarkeits-Antworten auf E-Mails, die nicht von ihnen selbst stammen, als Spam. Kommen davon zu viele in kurzer Zeit, kann es passieren, dass die IP des Intranators auf eine Spam-Blacklist eingetragen wird. Dann können viele normale E-Mails nicht mehr zugestellt werden oder landen beim Empfänger im Spamordner.

Diese Probleme können gelöst werden, indem der Intranator E-Mails mit ungültigen Empfängern gar nicht erst annimmt. Dann ist der sendende Server für die Erzeugung der Nichtzustellbarkeits-Nachricht zuständig, bzw. im Falle eines Spamservers wird erst gar keine erzeugt.

Wird eine Domain auf dem Intranator zugestellt, kennt der Intranator alle gültigen Empfängeradressen und lehnt ungültige gleich vor dem Empfang ab. Dafür ist keine spezielle Konfiguration nötig, dies geschieht vollautomatisch.

Wird eine Domain dagegen an einen anderen Server weitergeleitet, kennt nur dieser die gültigen Adressen. Damit der Intranator dennoch die E-Mails gleich beim Empfang ablehnen kann, gibt es die beiden im Folgenden beschriebenen Verfahren.

15.4.2.1. Empfängeradressprüfung über SMTP-Anfragen

Bevor eine E-Mail angenommen wird, fragt der Intranator kurz beim Zielserver, ob die Adresse gültig ist. Für die Überprüfung wird eine SMTP-Verbindung zum Zielserver aufgebaut und die Zieladresse mit dem `RCPT TO:-`-Befehl überprüft.

Wichtig ist hierbei, dass der Zielserver im Falle einer ungültigen Adresse mit einem Fehlercode im 500er-Bereich (z.B. `550 Recipient address rejected: User unknown`) antwortet. Viele Server akzeptieren in der Standardkonfiguration die Adresse zuerst und senden dann später eine Nichtzustellbarkeits-Nachricht. Bei einigen Servern kann das direkte Ablehnen

durch eine Konfigurationsänderung aktiviert werden. Bei machen Serverprogrammen (wie z.B. Microsoft Exchange vor Version 2007) ist das aber nicht möglich. Dann ist eine Empfängeradressprüfung über SMTP nicht nutzbar.

15.4.2.2. Empfängeradressprüfung über Active Directory und LDAP

Bei diesem Verfahren fragt der Intranator regelmäßig die Liste aller gültigen E-Mail-Adressen bei einem LDAP-Server (z.B. Active Directory) ab. Beim Empfang einer E-Mail kann dann anhand dieser Liste sofort festgestellt werden, ob die Adresse gültig ist oder nicht.

Der Intranator benötigt dafür einen gültigen Login auf dem LDAP-Server. Der LDAP-Login (bind DN) wird üblicherweise als vollständiger Distinguished Name eingegeben (z.B. **CN=Benutzername, CN=Users, DC=meinefirma, DC=local**). Viele Server akzeptieren aber auch einen einfachen Benutzerlogin, wenn dieser direkt in der LDAP-Suchbasis liegt.

Wenn Sie eine Standard-Domäne ohne weitere Organisationseinheiten oder ähnliches verwenden, können Sie bei Microsoft Windows Server 2000 und 2003 den Benutzer-Login als LDAP-Login eingeben. Bei Microsoft Windows Server 2008 geben Sie Vorname und Nachname des Benutzers mit Leerzeichen getrennt ein. Beides Mal wählt der Intranator automatisch den passenden Distinguished Name.

Achtung



Es wird dringend davon abgeraten, ein Konto mit Administrationsrechten zu verwenden. Das Passwort muss auf dem Intranator intern im Klartext abgelegt werden und könnte daher bei einem erfolgreichen Angriff auf den Intranator verwendet werden, um auch den LDAP-Server zu kompromittieren.

Die LDAP-Suchbasis ist der Ausgangspunkt für die Suche bei LDAP-Abfragen: Ein Distinguished Name (DN) des Wurzelknotens von dem zu durchsuchenden Teilbaum (z.B. **DC=meinefirma, DC=local** für die Active-Directory-Domäne „meinefirma.local“).

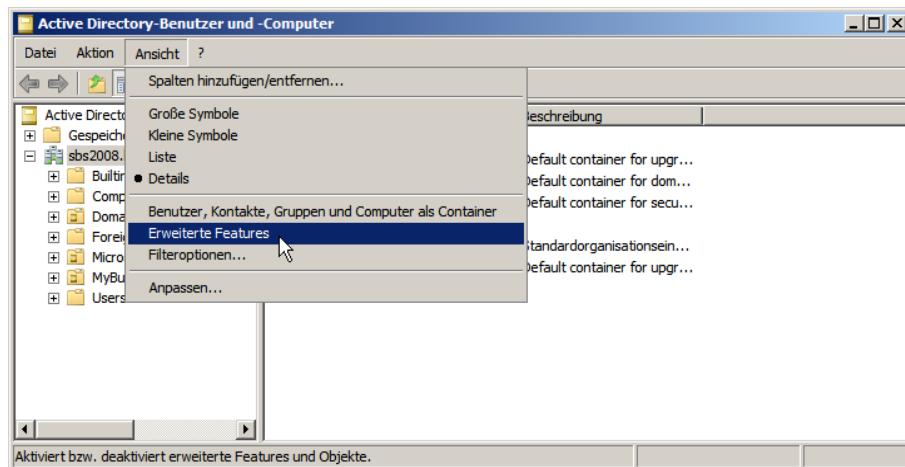
Wenn der LDAP-Server ein Active Directory ist, stellen Sie die Struktur auf Active Directory. Handelt es sich um einen LDAP-Server mit anderen Schemata als bei Active Directory üblich, müssen Sie einen Suchfilter (z.B. **(mail=*)**) und den Namen des Ergebnisattributs (z.B. **mail**) festlegen.

Direkt nachdem die Empfängeradressprüfung konfiguriert wurde, versucht der Intranator die Daten per LDAP auszulesen. Dies muss regelmäßig wiederholt werden. Das Intervall dafür wird unter Dienste > E-Mail > Automatik eingestellt.

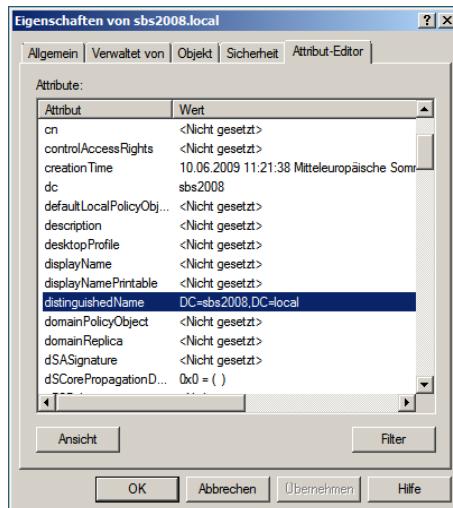
15.4.2.2.1. LDAP-Pfade auf Windows-Servern

Sollten Sie Schwierigkeiten haben, die passenden LDAP-Pfade für Ihren Windows-Server zu finden, wird im Folgenden beschrieben wie Sie an diese Daten herankommen.

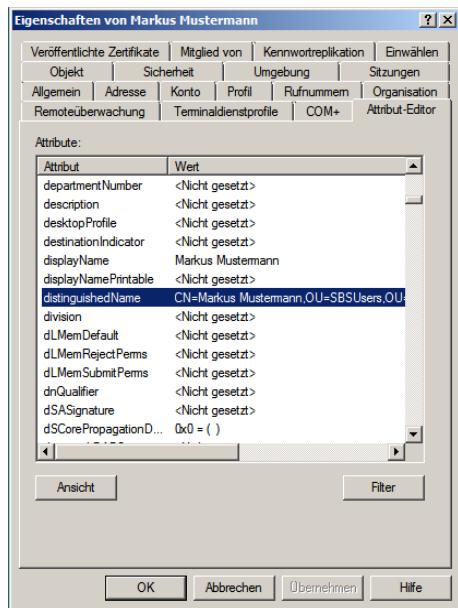
1. Öffnen Sie die Management-Konsole für Active-Directory-Benutzer und -Computer. Diese finden Sie normalerweise unter Verwaltung.
2. Aktivieren Sie im Menü Ansicht die Option Erweiterte Features.



3. Klicken Sie mit Rechts auf die Domain und Öffnen den Dialog Eigenschaften.
4. Im Reiter Attribut-Editor finden Sie das Attribut distinguishedName. Diesen geben Sie im Intranator als LDAP-Suchbasis ein.



5. Schließen Sie die Eigenschaftenanzeige der Domain und suchen den Pfad des Benutzers, den Sie zum Abrufen der Daten verwenden wollen.
6. Klicken Sie mit Rechts auf den Benutzer und Öffnen den Dialog Eigenschaften.
7. Im Reiter Attribut-Editor finden Sie das Attribut distinguishedName. Diesen geben Sie im Intranator als LDAP-Login ein.



15.4.3. Weiterleitung einzelner POP-Konten

Sollen einzelne POP-Konten abgerufen und die E-Mails dann direkt an einen anderen Server weitergeleitet werden, gehen Sie wie folgt vor: Richten Sie wie unter Abschnitt 15.3.2, „Abruf einzelner POP-Konten“ beschrieben das Abholen ein. Leiten Sie mindestens eine Domain an den entsprechenden Zielserver weiter. Wenn Sie nicht bereits eine Domain weiterleiten, richten Sie eine nur intern gültige Domain für diesen Zweck ein (z.B. **.net.1an**).

Unter Dienste > E-Mail > Abholen wählen Sie dann als Empfänger nicht einen lokalen Benutzer des Intranators aus, sondern tragen eine E-Mail-Adresse in der weitergeleiteten Domain ein. Die E-Mails aus dem POP-Konto werden dann nach den üblichen Filtern (Viren, Anhänge, Spam) an die eingegebene Adresse auf dem Zielserver zugestellt.

15.5. E-Mail-Addressierung

15.5.1. Adresseinstellungen

Normalerweise sind in einer Domain alle Systembenutzer erreichbar. Dies ist unter Dienste > E-Mail > Domains : Einstellungen aber abschaltbar. Dann sind in einer Domain nur noch die Adressen gültig, die explizit angegeben sind.

Außerdem ist es möglich, einzustellen, dass E-Mails an unbekannte Empfänger in dieser Domain nicht abgeblockt werden („550 User unknown“), sondern an den Postmaster weitergeleitet werden.

15.5.2. E-Mail-Adressen und Aliases

Jeder Benutzer ist unter seinem Benutzernamen in allen Domains, bei denen die Option „Alle Systembenutzer erreichbar“ aktiv ist, zu erreichen. Zusätzlich können für jeden Benutzer unter Benutzermanager > Benutzer > Adressen Aliases eingerichtet werden, unter denen er zusätzlich erreichbar ist.

Zum einen können diese Aliases, wie die normalen Namen auch, für alle Domains gelten, oder nur für eine spezielle. Damit ist es z.B. möglich, die Adresse „info“ für mehrere Domains an unterschiedliche Benutzer weiterzuleiten.

Wird eine Adresse für @lokale Domains eingetragen, so bedeutet dies, dass sie für alle Domains gültig ist, bei denen die Option „Alle Systembenutzer erreichbar“ aktiv ist.

Außerdem ist es möglich, Aliases für fremde Domains einzutragen. Dies ist evtl. für die automatische Antwort (siehe Abschnitt 15.6.2, „Automatische Antwort“) nötig. Außerdem werden E-Mails an solche Adressen sofort lokal zugestellt und gehen nicht über den Provider. Werden auf einem System keine Domains, sondern nur einzelne POP-Konten verwendet, kann man dadurch den Transfer von hausinternen E-Mails an den Provider und zurück sparen.

Zu jedem Alias kann ein vollständiger Name eingetragen werden. Dieser wird als Absender für Webmail benutzt.

15.6. E-Mail-Verarbeitung

15.6.1. Weiterleitung

Unter Benutzermanager > Benutzer : Weiterleitung können Sie die benutzerabhängige E-Mail-Weiterleitung konfigurieren. Bei der Option E-Mail-Kopie wird die E-Mail an die eingetragene(n) Adresse(n) gesendet und zusätzlich im Konto des Benutzers gespeichert. Mit der Option E-Mail-Umleitung wird die E-Mail nur weitergeleitet und nicht mehr im Konto des Benutzers gespeichert.

Soll die E-Mail an mehrere Empfänger weitergeleitet werden, so geben Sie deren Adressen mit Komma getrennt ein.



Achtung

Verwenden Sie für den Benutzer, der als Postmaster fungiert, nie E-Mail-Umleitung sondern immer E-Mail-Kopie. Denn sollte es ein Problem beim E-Mail-Versand geben, kann auch der Postmaster keine Mails mehr empfangen. Dabei können E-Mails verloren gehen. Da lokal keine Fehler-Benachrichtigungen abgerufen werden können, wird die Fehlersuche unter Umständen deutlich erschwert.

15.6.2. Automatische Antwort

Unter Benutzermanager > Benutzer : Abwesenheit können Sie die Automatische Antwort (Abwesenheitsschaltung) aktivieren. Dann wird jede E-Mail automatisch mit der eingestellten Antwort beantwortet. Um versehentliche E-Mail-Stürme usw. zu vermeiden, wird an jeden Empfänger normalerweise nur jeden Tag eine einzige Antwort geschickt.

Um zu vermeiden, dass Mailinglisten oder Spam-E-Mails automatisch beantwortet werden, antwortet die Abwesenheitsschaltung nur auf E-Mails, in denen eine diesem Benutzer zugewiesene Empfängeradresse in den To:- oder Cc:-Kopfzeilen der E-Mail eingetragen ist.



Achtung

Sie müssen daher alle extern erreichbare E-Mail-Adressen und E-Mail-Aliases dieses Benutzers im Reiter Adressen eintragen (speziell natürlich die externen POP-Konten). Sonst kann die Abwesenheitschaltung nicht funktionieren.

Die Automatische Antwort kann zeitgesteuert aktiviert und deaktiviert werden. Tragen Sie bei von ein Datum ein, wird an diesem Tag zur eingestellten Stunde die Automatische Antwort aktiviert. Tragen Sie bei bis ein Datum ein, wird an diesem Tag zur eingestellten Stunde die Automatische Antwort deaktiviert. Sie können auch eines der Datumsfelder leer lassen, dann ist die automatische Antwort ab sofort bis zum eingestellten Zeitpunkt aktiv bzw. ab dem eingestellten Zeitpunkt aktiv bis sie in diesem Menü wieder abgestellt wird.

15.6.3. Sortierung

Unter Benutzermanager > Benutzer : Sortierung können serverseitige Sortierregeln angelegt werden. Im Vergleich zu Sortierregeln im Clientprogramm haben diese den Vorteil, dass sie direkt beim Empfang der E-Mail ausgeführt werden und auch ohne laufenden Mailclient zuverlässig arbeiten.

Es können beliebig viele Sortierregeln angelegt werden. Bei jeder Regel wird eine Aktion (In Unterordner verschieben, weiterleiten, ablehnen, löschen) hinterlegt. Wird ein oder alle (einstellbar) Sorterkriterium von einer E-Mail erfüllt, wird die Aktion ausgeführt.

Als Kriterium für die Sortierung können alle Kopfzeilen der E-Mail (z.B. Empfänger, Absender, Betreff) verwendet werden. Es können beliebig viele Kriterien für eine Regel zusammengefasst werden.

15.7. E-Mail-Filter

15.7.1. Spamfilter

15.7.1.1. SMTP-Filterung

Empfangen Sie Ihre E-Mails direkt per SMTP, können Sie als erste Stufe zur Spamfilterung E-Mails von bekannten Spamversendern gleich vor der Annahme ablehnen lassen. Dies reduziert die Last auf dem System und vermeidet unnötigen Datentransfer.

Ist die Option IPs via DNS auf SMTP-Ebene überprüfen im Menü Dienste > E-Mailfilter > Spam > Einstellungen aktiv, so wird die IP jedes Servers, der E-Mails direkt per SMTP einliefern will, per DNS überprüft. Dabei werden mehrere Blocklisten abgefragt. Ist die IP auf mehreren Blocklisten gleichzeitig als Spamversender geführt, wird der E-Mail-Empfang von diesem Server generell abgelehnt.

Ist die IP des sendenden Servers nur auf wenigen oder gar keiner Blockliste enthalten, wird die E-Mail angenommen und durch die weiteren Stufen des Spamfilters eingehend geprüft.

15.7.1.2. Markierung

Der Intranator enthält einen mehrstufigen Spamfilter. Dabei wird eine E-Mail sowohl durch Spam-typische Kriterien (spezielle Worte, viele Ausrufezeichen, ungültige Absenderadressen usw.) als auch durch einen bayesischen Wortfilter kategorisiert. Der bayesische

Wortfilter kann durch Vergleiche von Wortkombinationen mit einer vortrainierten Wortsbasis eine Spam-Wahrscheinlichkeit errechnen.

Zusätzlich können noch DNS-basierte Netzwerktests durchgeführt werden. Dabei wird überprüft, ob die in der E-Mail enthaltenen E-Mailadressen und URLs in verschiedenen Blacklists vorkommen. Da diese Überprüfung auch für jede interne E-Mail ausgeführt wird, sollten Sie diese Option nur aktivieren, wenn Ihre Internetverbindung nicht pro Zeiteinheit oder Einwahlversuch abgerechnet wird.

Des Weiteren kann der Intranator E-Mails auch über das Razor Netzwerk überprüfen. Das Razor Netzwerk ist ein Zusammenschluss von E-Mail-Empfängern. Im Razor-Netzwerk werden Spam-E-Mails von Hand als Spam markiert. Diese Information wird dann über das Razor-Netzwerk verteilt. Je mehr Leute eine E-Mail als Spam einstufen, desto schneller wird sie herausgefiltert.

Ist der Spamfilter aktiviert (unter Dienste > E-Mailfilter > Spam > Einstellungen), wird für jede E-Mail ein Spam-Punktwert ermittelt und dieser in einem speziellen E-Mail-Header abgelegt. Dadurch wird aber noch keine E-Mail gelöscht oder verschoben. Der Punktwert wird in dem Header „X-Spam-Level:“ abgelegt. Er errechnet sich durch $(Spampunkte+100)*10$. Dadurch ist der Wert immer positiv und ganzzahlig, was einen Vergleich für die meisten anderen Programme erst ermöglicht. Außerdem wird eine ausführliche Beschreibung, warum eine E-Mail Spam ist oder nicht, im „X-Spam-Status:“ Header abgelegt.

15.7.1.3. Schwellwerte

Je höher der Spam-Punktwert ist, desto höher ist die Wahrscheinlichkeit, dass es sich um Spam handelt. Werte kleiner als 4 weisen normalerweise auf erwünschte E-Mails hin. Bei Werten zwischen 5 und 8 ist die Wahrscheinlichkeit für Spam höher, es kann sich aber dennoch um eine erwünschte E-Mail handeln. Bei Werten von 8 und größer ist die E-Mail ziemlich sicher Spam.

Je niedriger der Schwellwert, desto mehr E-Mails werden rausgefiltert. Gleichzeitig steigt aber auch die Gefahr, dass eine wichtige E-Mail im Spam-Ordner landet.

Im Intranator wird daher typischerweise zwischen 3 Kategorien unterschieden: erwünschte E-Mail, Spamverdacht und Spam.

Der Spamverdacht ist für E-Mails gedacht, die zwar klare Spam-Merkmale aufweisen, aber nicht ganz eindeutig als Spam klassifiziert werden können. Es empfiehlt sich, diese E-Mails regelmäßig (z.B. einmal pro Woche) manuell zu überprüfen.

Spam sind E-Mails, die eindeutig als Spam erkannt wurden. Diese E-Mails müssen normalerweise nicht manuell kontrolliert werden. Für den Fall von Fehlkonfigurationen empfiehlt es sich aber dennoch, diese E-Mails nicht sofort zu löschen sondern für einige Tage aufzubewahren.

Als guten Kompromiss haben sich die Schwellwerte 5 für Spamverdacht und 8 für Spam herausgestellt.

15.7.1.4. Globaler Spamfilter

Unter Dienste > E-Mailfilter > Spam > Global kann der globale Spamfilter aktiviert werden. Er filtert alle empfangenen E-Mails - unabhängig davon, ob sie an einen lokalen Benutzer

gehen oder weitergeleitet werden. Daher empfehlen wir den Globalen Spamfilter vor allem für die Fälle, in denen die E-Mails nicht endgültig auf dem Intranator abgelegt, sondern an einen anderen Server weitergeleitet werden.

15.7.1.4.1. Aktionen

Die folgenden Filteraktionen sind jeweils für Spam und Spamverdacht separat konfigurierbar. Damit können die Kategorien Spamverdacht und Spam unterschiedlich behandelt werden.

Die Option E-Mail-Betreff verändert sorgt dafür, dass jeder betroffenen E-Mail „***SPAM***“ bzw. „***SPAMVERDACHT***“ im Betreff vorangestellt wird. Dies macht vor allem Sinn, wenn die E-Mails normal zugestellt werden.

Bei normal zustellen gehen die betroffenen E-Mails weiterhin ihren normalen Weg und werden nicht gestoppt oder umgeleitet. Dies ist vor allem im Zusammenhang mit dem Verändern des Betreffs und einer Filterregel auf dem Zielserver sinnvoll. Die Filterregel auf dem Zielserver kann die E-Mails dann anhand des Betreffs in entsprechende Unterordner ablegen.

Mit der Option umleiten werden die betroffenen E-Mails an eine Sammeladresse umgeleitet. Wenn Sie hierfür ein Konto auf dem Intranator selber verwenden, achten Sie unbedingt darauf, dort den benutzerabhängigen Spamfilter zu aktivieren und die Spam-E-Mails automatisch nach einiger Zeit löschen zu lassen. Ansonsten besteht die Gefahr, dass das Spam-Konto unbegrenzt wächst.

15.7.1.4.2. Quarantäne

Die Spam-Quarantäne nimmt erkannte Spam-E-Mails auf, hält sie für eine einstellbare Zeit bereit und löscht sie dann. Bei Bedarf können falsch erkannte E-Mails aus der Quarantäne wieder freigegeben und normal zugestellt werden.

Die Spam-Quarantäne selbst ist unter Dienste > E-Mailfilter > Quarantäne > Spam erreichbar. Sie enthält die erkannten Spam-E-Mails aller Empfänger zusammen. Daher ist sie normalerweise nur für Benutzer mit administrativen Rechten erreichbar. Sie kann auch zusätzlich mit einem Datenschutz-Passwort unter Information > Datenschutz nur im 4-Augen-Verfahren zugänglich gemacht werden.

Um jedem Empfänger selbst einen Überblick über seine gefilterten E-Mails zu geben, gibt es die Report-Funktion. Wenn aktiviert, bekommt jeder Empfänger zu den einstellbaren Versandzeiten automatisch eine E-Mail mit einer Übersicht über die gefilterten E-Mails.

In der Report-E-Mail befindet sich unter den Daten zu jeder gefilterten E-Mail ein Link, mit dem die entsprechende E-Mail aus der Quarantäne freigegeben werden kann. Die Report-E-Mails sind nach aufsteigender Spam-Wahrscheinlichkeit sortiert.



Hinweis

Da die Report-E-Mails die Betreff-Zeilen der gefilterten E-Mails enthalten, kann es sein, dass ein zusätzlich auf dem Zielserver oder Client installierter Spamfilter die Report-E-Mails fälschlicherweise als Spam identifiziert.

Setzen Sie einen zusätzlichen Spamfilter ein, sollten Sie daher die Postmaster-adresse des Intranators (Menü Dienste > E-Mail > Einstellungen) dort in die

Whitelist eintragen. Die Postmasteradresse des Intranators wird für die Reports als Absenderadresse verwendet.

15.7.1.5. Benutzerabhängiger Spamfilter

Der benutzerabhängige Spamfilter kann für jeden Benutzer auf dem Intranator individuell konfiguriert werden. Er ist in der Lage, erkannte Spam-E-Mails in speziellen IMAP-Unterordnern des Benutzers abzulegen. Wir empfehlen den Einsatz des benutzerabhängigen Spamfilters daher für die Fälle, in denen die E-Mails endgültig auf dem Intranator abgelegt werden.

Erreicht eine E-Mail einen Benutzer, der unter Benutzermanager > Benutzer : Spamfilter den Spamfilter für sich aktiviert hat, wird die E-Mail überprüft. Der Benutzer-Spamfilter ist zweistufig aufgebaut. Es gibt einen Schwellwert für spamverdächtige E-Mails sowie einen für „richtigen“ Spam. Hat die E-Mail einen Spam-Punktwert größer oder gleich dem eingetragenen Schwellwert wird sie nicht gelöscht, sondern in die IMAP Unterordner „Spamverdacht“ oder „Spam“ des Benutzers abgelegt. Auf Wunsch können Spam-E-Mails auch an eine zentrale Sammeladresse weitergeleitet werden.

Jeder Benutzer hat zusätzlich noch die Möglichkeit, dies durch Blacklists (Alle diese Absender oder Empfänger sind immer Spam) und Whitelists (Alle diese Absender oder Empfänger sind nie Spam) zu beeinflussen.

Wenn ein Benutzer per IMAP auf seine E-Mails zugreift, sind die Unterordner direkt sichtbar. Eventuell muss die Ordnerliste im E-Mail-Programm neu übertragen und die Ordner abonniert werden (subscribe). Beim Zugriff via POP3 bleiben die Spam-E-Mails auf dem Server. Der Benutzer sollte daher den „Spamverdacht“-Ordner regelmäßig per Webmail auf fälschlich gefilterte Nachrichten überprüfen.

15.7.1.6. Glaubwürdige Server

Im Standardmodus prüft der Spamfilter bei allen „Received“-Kopfzeilen einer E-Mail, ob deren IPs in DNS-Blacklisten enthalten sind. Im optimierten Modus wird nur die IP des letzten Servers des Versenders überprüft. Dadurch wird die Spam-Erkennungsrate weiter gesteigert sowie die potentielle Falscherkennung von erwünschten Nachrichten reduziert. Der aktuell verwendete Modus ist unter Dienste > E-Mailfilter > Spam > Glaubwürdige Server einsehbar.

Um die IP des letzten Versender-Servers von gefälschten Daten unterscheiden zu können, muss das System wissen, welche Server glaubwürdig sind. Ein SMTP-Server gilt als glaubwürdig, wenn angenommen werden kann, dass dieser die Received-Zeilen im E-Mail-Header nicht verfälscht und seinen eigenen Received-Eintrag wahrheitsgemäß einfügt. Man kann normalerweise davon ausgehen, dass alle für Empfang und Verarbeitung der eigenen E-Mails konfigurierten Server glaubwürdig sind, da deren Betreiber vertraglich gebunden sind.

Der Intranator versucht automatisch die glaubwürdigen Server zu ermitteln, dabei kommt für jede E-Mail-Empfangsmethode ein angepasstes Verfahren zum Einsatz.

Glaubwürdige Server bei direktem SMTP und POP-Sammelkonten (Multidrop): Der Intranator fragt automatisch per DNS für jede konfigurierte Domain die für den E-Mail-Empfang zuständigen Server (MX-Eintrag der Domain) ab. Diese Server werden der Liste der glaubwürdigen Server hinzugefügt.

In folgenden Fällen kann es notwendig sein, die Liste der glaubwürdigen Server anzupassen:

1. Die E-Mails werden beim für den E-Mail-Empfang zuständigen Server (MX-Eintrag der Domain) entgegengenommen und dann an einen anderen Server weitergeleitet (z.B. zur Überprüfung oder Zwischenspeicherung), bevor Sie zum Intranator gehen. Hier müssen die IPs oder DNS-Namen aller Zwischenserver in die Liste der „weiteren glaubwürdigen Server“ eingetragen werden.
2. Der Intranator bekommt per DNS im lokalen Netz andere Daten für die eigene Domain zu sehen, als es „draußen“ im Internet der Fall ist. Diese Konstellation wird normalerweise „Split-DNS“ genannt. Hier müssen die IPs aller extern für den E-Mail-Empfang zuständigen Server (MX-Eintrag der Domain) in die Liste der „weiteren glaubwürdigen Server“ eingetragen werden.
3. Die E-Mails werden von einem Server unter der Domain A empfangen, dort auf die Domain B umgeschrieben und dann an den Intranator oder für die Domain B zuständigen Server weitergeleitet. Der Intranator kennt nur die Domain B. Hier muss die ursprüngliche Domain A in die Liste der „glaubwürdigen Domains“ aufgenommen werden.

Glaubwürdige Server bei einzelnen POP-Konten: Der Intranator überprüft automatisch per DNS alle unter Dienste > E-Mail > Abholen eingetragenen E-Mail-Server. Diese Server werden als glaubwürdig behandelt. Zusätzlich wird jeder Servername auf die Second-Level-Domain gekürzt, so wird z.B. aus dem Servernamen „pop.1und1.de“ die Domain „1und1.de“. Die für diese Domain zuständigen E-Mail-Server (MX-Einträge) werden abgefragt und zusätzlich als glaubwürdige Server übernommen.

In folgenden Fällen kann es notwendig sein, die Liste der glaubwürdigen Server anzupassen:

1. Der Provider verwendet für seine eigenen E-Mails andere Server als für die E-Mails der Kunden. Tragen Sie in diesem Fall die Domains aller E-Mail-Adressen, die bei Ihnen verwendet werden, in die Liste der „glaubwürdigen Domains“ ein.
2. Beim Provider werden die E-Mails auf einem Server empfangen, z.B. zur Überprüfung an einen anderen Server weitergeleitet und dann nochmal auf einem anderen Server zur Abholung bereitgehalten. In diesem Fall müssen Sie die IPs oder DNS-Namen aller zur Überprüfung verwendeten Zwischenserver in die Liste der „weiteren glaubwürdigen Server“ eintragen.
3. E-Mails werden von einer Domain empfangen und dort automatisiert an eine andere Domain weitergeleitet. Der Intranator holt dann die weitergeleiteten E-Mails ab. Tragen Sie in diesem Fall alle ursprünglichen Domains, von denen aus weitergeleitet wird, in die Liste der „glaubwürdigen Domains“ ein.

Anhand der letzten 1.000 Spam-E-Mails kann der Intranator erkennen, ob die Liste der glaubwürdigen Server korrekt ist. Nach dieser Kalibrierung schaltet der Spamfilter, falls möglich, in den optimierten Modus. Die Kalibrierung wird im laufenden Betrieb stündlich erneut überprüft.



Hinweis

Nach Änderung der glaubwürdigen Server oder Domains werden bis zu 1.000 Spam-Nachrichten benötigt, bevor der Spamfilter automatisch in den optimierten Modus wechselt.

15.7.2. VirensScanner

Unter Dienste > E-Mailfilter > Antivirus kann der E-Mail-VirensScanner aktiviert werden. Ist er aktiviert, werden alle E-Mails, die den Intranator passieren (eingehend, ausgehend, weitergeleitet,...), auf Viren überprüft.

Wurde ein Virus gefunden, so wird er unter Dienste > E-Mailfilter > Quarantäne : Virus-Quarantäne in Quarantäne genommen und kann dort vom Administrator inspiziert werden.

Bei einem gefundenen Virus können Warnungen an den Administrator sowie an den Empfänger gesendet werden. Es werden nur Warnungen an lokale Empfänger versendet.

Da der F-Secure VirensScanner eine heuristische Virenerkennung unterstützt, werden manche Dateien nur als verdächtig eingestuft. Diese können mit der entsprechenden Option auch blockiert werden. Sie sollten diese Option nur deaktivieren, falls häufiger wichtige Dateien falsch erkannt werden.

15.7.3. Anhangfilter

E-Mail-Anhänge können neue, unbekannte Viren enthalten. Diese müssen als ausführbare Dateien auf den PC gelangen. Der Intranator kann E-Mail-Anhänge untersuchen und bestimmte Typen blockieren. So können Sie sichergehen, dass keine ausführbare Datei per E-Mail auf einen Rechner im Intranet gelangt.

Der Anhangfilter untersucht Anhänge anhand der Dateiendung sowie des MIME-Typs. Zusätzlich führt er eine Typerkennung auf die tatsächlich in der E-Mail enthaltenen Daten durch. Archive wie z.B. ZIP oder RAR werden auch durchsucht. Verschlüsselte (mit einem Passwort geschützte) Archive können vom Anhangfilter nicht untersucht werden. Deswegen ist es möglich und ratsam, sie generell zu blockieren.

Auf der Seite Dienste > E-Mailfilter > Anhang > Filterlisten können Sie Filterlisten für Dateianhänge anlegen. Es wird zwischen Freigabe- und Sperrlisten unterschieden. Freigabelisten lassen nur bekannte und freigegebene Anhänge durch, Sperrlisten lassen alles bis auf die aufgeführten Einträge durch.

Die Filterlisten „Alles erlaubt“, „Alles verboten“ sowie „Ausführbare Dateien“ sind vordefiniert. Unter Dienste > E-Mailfilter > Anhang > Einstellungen legen Sie globale Einstellungen zum Anhangfilter sowie die „Standard-Filterliste“ fest. Bei Auslieferung steht sie auf „Ausführbare Dateien“. Ausgehende E-Mails sowie Domain-Weiterleitungen werden über diese Standard-Liste gefiltert.

Eingehende E-Mails verwenden die Filterliste der Benutzergruppen. Diese kann unter Benutzermanager > Gruppen : Rechte zugewiesen werden. Standardmäßig verwenden alle Benutzergruppen die „Standard-Filterliste“. Ist ein Benutzer in mehreren Gruppen mit unterschiedlichen Filterlisten Mitglied, so werden die Filterlisten gemischt. Freigabelisten haben dabei Vorrang vor Sperrlisten. So können Sie generell alle ausführbaren Dateien sperren, jedoch z.B. für die Administrator-Gruppe .exe freigeben.

Wird eine E-Mail gefiltert, so liegt sie unter Dienste > E-Mailfilter > Quarantäne : Anhang in Quarantäne und der Administrator bekommt einen Hinweis. Die E-Mail kann später per Mausklick freigegeben oder gelöscht werden. Alternativ ist es bei eingehenden E-Mails möglich, dass die E-Mail ohne den (potentiell gefährlichen) Anhang ausgeliefert wird. Die Original-E-Mail inkl. Anhang liegt dann in der Quarantäne und kann bei Bedarf freigegeben werden.

15.8. Archivierung

15.8.1. Schnittstelle

Im Menü Dienste > E-Mail > Archivierung kann die Archivierungsschnittstelle des Intranators konfiguriert werden. Die Schnittstelle kann die E-Mails in verschiedenen Formaten schreiben und so an die eingesetzte Archivsoftware angepasst werden. Die verschiedenen Archivierungsmodi sind im Einzelnen:

E-Mail-Kopie an	Von jeder E-Mail wird eine Kopie an diese Adresse gesendet. Die ursprünglichen Empfänger der E-Mail werden in der Kopfzeile <code>x-Envelope-To</code> abgelegt.
Einzelne Dateien (BSMTP-Format)	Jede E-Mail wird in eine einzelne Datei im BSMTP-Format geschrieben. Das BSMTP-Format ist in RFC 2442 [http://tools.ietf.org/html/rfc2442] definiert. In jeder Datei wird nur eine E-Mail abgelegt, mehrere Empfänger werden in einzelnen <code>RCPT-TO</code> -Zeilen angegeben.
Einzelne Dateien (EML/RFC822-Format)	Der Inhalt (Header und Body) jeder E-Mail wird in eine einzelne Datei geschrieben. Dies wird normalerweise EML-Format genannt und wurde erstmals in RFC 822 [http://tools.ietf.org/html/rfc822] beschrieben. In jeder Datei wird nur eine E-Mail abgelegt, pro Empfänger wird eine separate Datei angelegt. Der Absender wird in der Kopfzeile <code>x-Envelope-From</code> , der Empfänger in der Kopfzeile <code>x-Envelope-To</code> abgelegt.
MailStore Proxy	Die einzelnen E-Mails werden in Dateien kompatibel zum Format des MailStore Proxys abgelegt. Damit kann der Intranator wie ein MailStore Proxy an den MailStore Server angebunden werden. Hinweise zur Einrichtung finden Sie in Abschnitt 15.8.2, „Anbindung des MailStore Servers“.

Ist der Spamfilter des Intranators aktiv, können als Spam erkannte E-Mails von der Archivierung ausgeschlossen werden. Wählen Sie einen Schwellwert ab dem E-Mails nicht archiviert werden sollen. Wir empfehlen hier den Wert 8 zu verwenden. Weitere Details zu den Spam-Schwellwerten finden Sie in Abschnitt 15.7.1.2, „Markierung“

Haben Sie einen Archivierungsmodus gewählt, der Dateien ablegt, kann über eine Windows-Freigabe auf diese zugegriffen werden. Sie müssen ein Login und Passwort für

diese Freigabe wählen. Die Archivierungsschnittstelle stellt nur vollständige Dateien zur Verfügung. Die Schnittstelle stellt sicher, dass keine unvollständigen oder nur teilweise geschriebenen Dateien sichtbar werden oder abgerufen werden können.



Achtung

Die Archivierungssoftware ist dafür verantwortlich, dass die E-Mails unverzüglich nach der Archivierung von der Schnittstelle gelöscht werden. Die Schnittstellen-Freigabe ist nicht für ein dauerhaftes Speichern der E-Mail-Dateien ausgelegt und kann den Mailtransfer blockieren, wenn die Dateien nicht regelmäßig abgerufen werden.

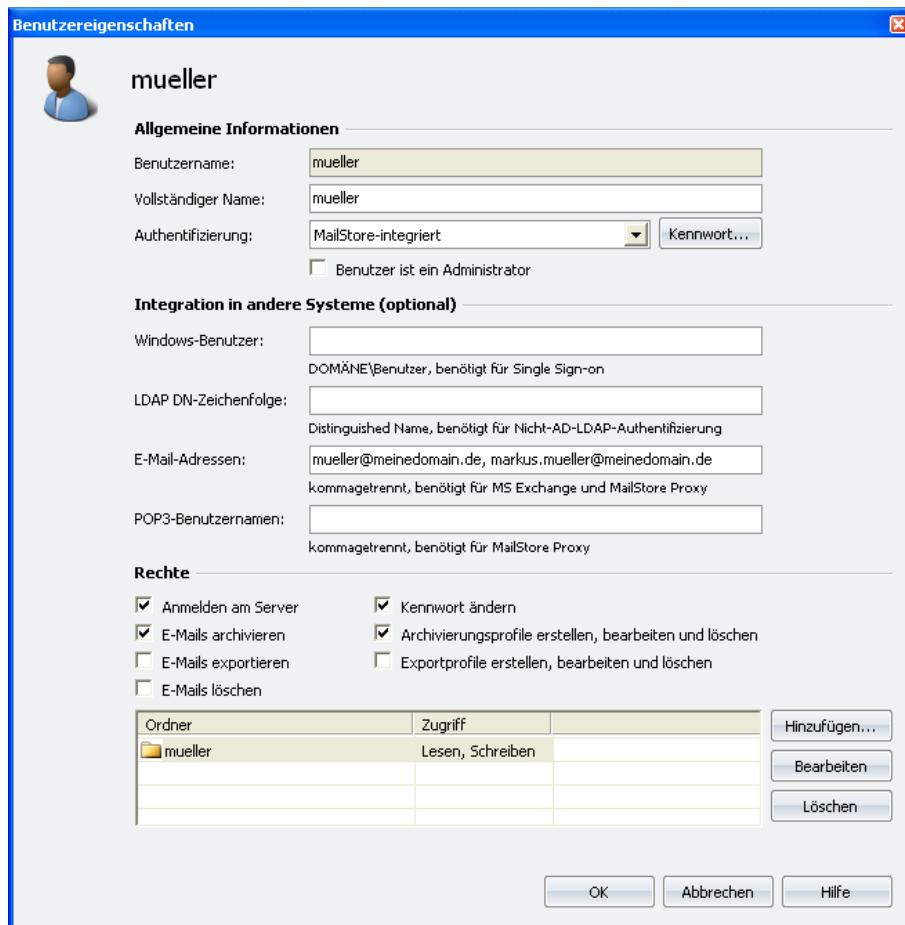
15.8.2. Anbindung des MailStore Servers

Der MailStore Server [<http://www.mailstore.com/>] wird über die im Intranator vorhandene MailStore Proxy Schnittstelle angebunden. Dabei wird von jeder E-Mail, die durch den Intranator geleitet wird, eine Kopie angelegt und in einem speziellen Format an der Archivschnittstelle des Intranators abgelegt. Der MailStore Server ruft jetzt regelmäßig die Dateien an dieser Schnittstelle ab und fügt sie dem Archiv hinzu.

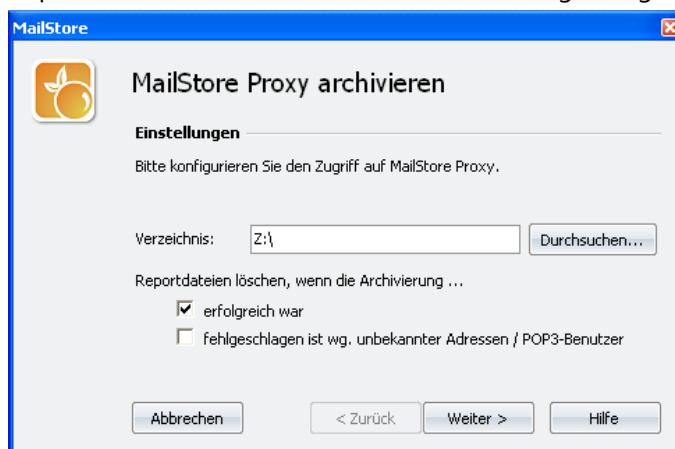
Im Gegensatz zu den anderen Archivierungsmethoden des MailStore Servers (wie z.B. IMAP-Postfach oder Exchange Server) ist dadurch sichergestellt, dass wirklich alle E-Mails archiviert werden. Es ist nicht möglich, dass der Benutzer eine unglücklich konfigurierte Sortierregel oder ein Programmfehler E-Mails löscht, bevor sie archiviert wurden.

Gehen Sie bei der Installation wie folgt vor:

1. Installieren Sie den MailStore Server wie im Handbuch des Herstellers beschrieben: <http://de.help.mailstore.com/>.
2. Stellen Sie den Archivierungsmodus des Intranators im Menü Dienste > E-Mail > Archivierung auf MailStore Proxy und geben Zugangsdaten für den Freigabepfad an.
3. Starten Sie auf dem Rechner mit dem MailStore Server den Windows Explorer (nicht verwechseln mit dem Internet Explorer) und öffnen den in der Oberfläche des Intranators angezeigten Freigabepfad. Verknüpfen Sie die archive-Freigabe dauerhaft mit einem Laufwerksbuchstaben und lassen das Passwort von Windows speichern.
4. Öffnen Sie den MailStore Client, loggen sich mit Administrationsrechten ein und öffnen das Menü Verwaltung.
5. Machen Sie über die Schaltfläche Neuer Benutzer jeden Benutzer Ihres Systems auch dem MailStore Server bekannt. Dabei ist vor allem wichtig, dass im Feld E-Mail-Adressen alle E-Mail-Adressen inkl. Aliases und Weiterleitungen des Benutzers eingetragen sind.



6. Öffnen Sie das Menü E-Mails archivieren und konfigurieren ein neues Archivierungsprofil vom Typ MailStore Proxy.
7. Wählen Sie den eben verknüpften Laufwerksbuchstaben als Verzeichnis und lassen die Reportdateien löschen, wenn die Archivierung erfolgreich war (wichtig!).





8. Legen Sie über die Schaltfläche Zeitgesteuert fest, dass das Archivierungsprotokoll jede Minute ausgeführt werden soll.



15.9. Automatischer Transfer

Der Intranator kann in regelmäßigen Abständen automatisch E-Mails abholen und versenden. Dies ist sogar wochentagsabhängig unter Dienste > E-Mail > Automatik konfigurierbar.

Für den Transfer wird eine Verbindung mit dem Standardprovider (siehe Abschnitt 11.8, „Verbindungsautomatik“) aufgebaut, falls noch keine Verbindung besteht. Ist der Transfer abgeschlossen, so wird, falls niemand surft, die Verbindung sofort wieder getrennt.

Während der Intranator Online ist, werden E-Mails immer sofort versendet.

15.10. Verteiler

Der Intranator bringt eine mächtige Mailinglistenverwaltung mit. Zusätzlich zu den Benutzergruppen können unter Dienste > E-Mail > Verteiler Mailinglisten eingerichtet werden.

Es können zusätzlich zu den internen Benutzern und Gruppen auch externe E-Mail-Adressen hinzugefügt werden. Falls der Intranator nicht eine Domain per Multidrop oder SMTP verwaltet, gibt es das Problem, dass der Verteiler keine von außen erreichbare E-Mail-Adresse hat. Um das zu lösen, kann unter Dienste > E-Mail > Abholen ein POP3 Konto eingestellt werden, von dem E-Mails für die Mailingliste abgeholt werden. Gleichzeitig wird die unter „Externe Mailingliste Adresse“ eingegebene E-Mail-Adresse auch als Antwortadresse in alle E-Mails an die externen Mitglieder eingefügt.

15.11. Weitere Einstellungen

Unter Dienste > E-Mail > Einstellungen können noch einige Parameter des E-Mail-Systems konfiguriert werden.

Der Postmaster ist der Benutzer, der Nachrichten über Fehler und unzustellbare Nachrichten gesendet bekommt. Es gibt einen systemweiten Standard-Postmaster und es ist für jede Domain ein eigener Postmaster einstellbar (unter Dienste > E-Mail > Domains). E-Mails, die die Systemdienste versenden, haben den Postmaster als Absenderadresse. Wenn Sie keine Domain im System konfiguriert haben, sollten Sie bei Externe Adresse des Postmasters eine gültige Adresse eintragen, da viele Server keine E-Mails von ungültigen Absendern annehmen.

E-Mails können nicht unbeschränkt groß sein, da sie für das Verarbeiten (z.B. Virenscan usw.) zwischengespeichert und entpackt werden müssen. Dafür wird die Spool-Partition verwendet, deren Platz beschränkt ist. Als gutes Limit hat sich 100 MB herausgestellt. Die allerwenigsten Systeme nehmen größere Mails an oder versenden sie.

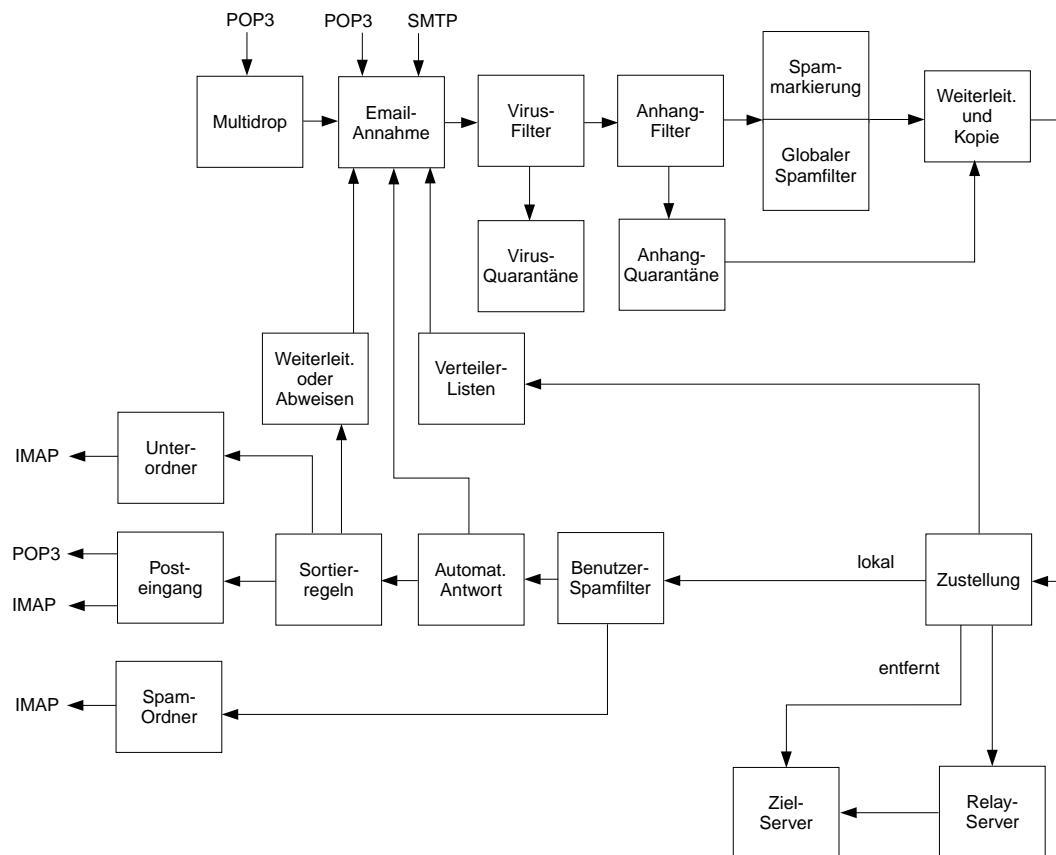
15.12. Warteschlange

Bevor eine E-Mail an einen externen Empfänger versendet wird, landet sie in der Warteschlange unter Dienste > E-Mail > Warteschlange.

Dort bleiben auch E-Mails, die wegen Serverfehlern kurzfristig noch nicht zugestellt werden konnten.

Der Administrator kann diese E-Mails aus der Warteschlange löschen oder sie herunterladen.

15.13. Aufbau des Mailsystems



15.14. Unterschiede zwischen den Lizenzen

Intranator-Lizenzen mit Mail Security ermöglichen:

- Annahme von E-Mails von einzelnen POP-Konten, per direkter Zustellung mit SMTP und von POP-Sammelkonten
- Weiterleitung von gesamten Domains
- Weiterleitung von einzelnen E-Mail-Adressen
- Empfängeradressprüfung
- Spamfilter mit Quarantäne
- Anhangfilter
- E-Mail Antivirus
- Schnittstelle zur E-Mail-Archivierung

Intranator-Lizenzen mit Mail Server ermöglichen zusätzlich:

- Dauerhaftes Speichern von E-Mails auf dem Intranator
- E-Mail-Abruf vom Intranator per POP3 und IMAP

- Abwesenheitsschaltung
- E-Mail-Sortierung
- Benutzerbasierter Spamfilter
- Verteilerlisten
- Webmail und Web-Groupware
- ActiveSync

16. Kapitel - Dienste

16.1. Fax

16.1.1. ISDN-Anschluss

Um Faxen zu können, benötigt der Intranator einen ISDN-Anschluss. Eine Liste der unterstützten ISDN-Karten finden Sie unter http://www.intra2net.com/de/support/unterstuetzte_hardware.php. Es kann nur eine ISDN-Karte pro Intranator verbaut werden. Auch bei Karten, die mehrere S₀-Busse anbieten, kann nur einer verwendet werden. Der Intranator kann also maximal auf 2 Kanälen gleichzeitig Faxe senden und empfangen. Wird der Intranator als virtueller Server verwendet, ist die Faxfunktion prinzipbedingt nicht nutzbar.

Der Intranator benötigt einen ISDN-Mehrgeräteanschluss (PTMP). Liefert die Telefongesellschaft einen solchen, kann dieser direkt genutzt werden. Liefert die Telefongesellschaft einen Anlagenanschluss (PTP), muss die daran angeschlossene TK-Anlage einen internen Mehrgeräteanschluss für den Intranator bereitstellen.

Um Kompatibilitätsprobleme zu vermeiden sowie die volle Kapazität des Intranators zu nutzen, sollte der Intranator an einen eigenen Mehrgeräteanschluss an der TK-Anlage angeschlossen werden, der nicht mit anderen Geräten geteilt wird.

Unter System > ISDN > Ortsvorwahl sollten Ländercode und Ortsvorwahl eingestellt werden. Muss bei Ihrer TK-Anlage vor jeder externen Nummer eine 0 vorgewählt werden, kann dies auch hier konfiguriert werden.

Unter System > ISDN > MSN werden dem Intranator die verfügbaren Mehrfachrufnummern (Multiple Subscriber Number oder MSN) bekannt gemacht. Einige Telefonanlagen begrenzen die Anzahl der möglichen MSNs auf 10 Stück. Weder der Euro-ISDN-Standard noch der Intranator kennen ein solches Limit.



Tipp

Sind Sie nicht sicher, auf welche MSNs der angeschlossene S₀-Bus konfiguriert ist, öffnen Sie die messages-Logdatei unter Information > System > Logdateien im Livemode. Alle eingehenden Anrufe werden dort mit der zugehörigen MSN angezeigt.

16.1.2. Empfang

Unter Dienste > Fax > Einstellungen wird der Faxempfang grundsätzlich aktiviert.

Danach kann unter Dienste > Fax > Empfänger der Faxempfang für unterschiedliche Durchwahlen konfiguriert werden. Wird auf einer der dort eingestellten MSNs ein Fax empfangen, wird es per E-Mail an den hinterlegten Intranator-Benutzer gesendet. Das Fax kann in den Formaten PDF, PNG oder TIFF-G3 an die E-Mail angehängt werden.

16.1.3. Versand

16.1.3.1. Einstellungen

Unter Dienste > Fax > Einstellungen wird der Faxversand grundsätzlich aktiviert. Dort werden auch die abgehende MSN sowie die Standardkennung eingestellt.

Da beim Empfang unterschiedliche Durchwahlen unterstützt werden, macht es natürlich auch Sinn, unterschiedliche Kennungen für den Versand zu verwenden. Unter Dienste > Fax > Empfänger kann für jeden Empfänger eine unterschiedliche Kennung eingetragen werden. Diese wird für den Versand verwendet, sobald der im Feld Name eingetragene Name vom Faxprogramm als Benutzername übermittelt wird.

16.1.3.2. Client

Der Intranator verwendet intern den HylaFax-Faxserver. Zum Versand kann daher jeder HylaFax-kompatible Faxclient eingesetzt werden. Eine Übersicht über verfügbare Faxclients bekommen Sie unter http://www.hylafax.org/content/Desktop_Client_Software.

Auf dem Intranator wird der frei verfügbare Client YajHFC mitgeliefert. Er kann im Menü Information > Download heruntergeladen werden.

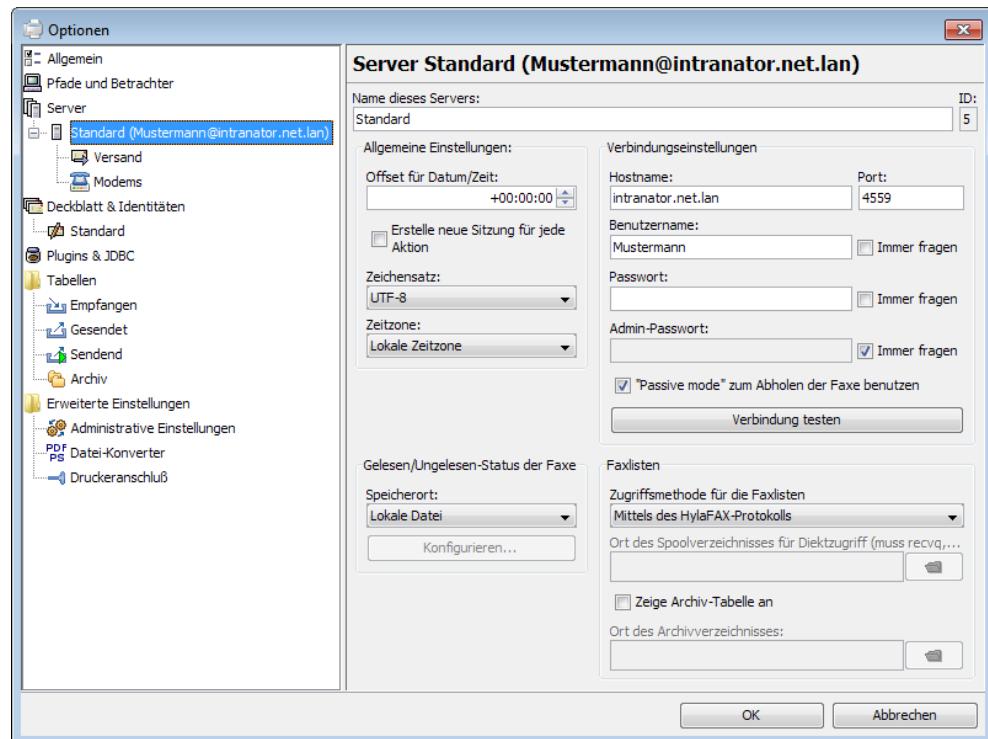
16.1.3.3. Installieren und Konfigurieren von YajHFC

YajHFC (Yet another Java HylaFAX Client) ist geeignet für Windows (XP bis 8, 32 und 64 Bit, nicht jedoch Terminal-Server), Mac OS und Linux. Ein fertiges Installationsprogramm für Windows ist auf dem Intranator im Menü Information > Download > Software zu finden. Für alle anderen Betriebssysteme finden Sie passende Versionen unter <http://www.yajhfc.de/>.

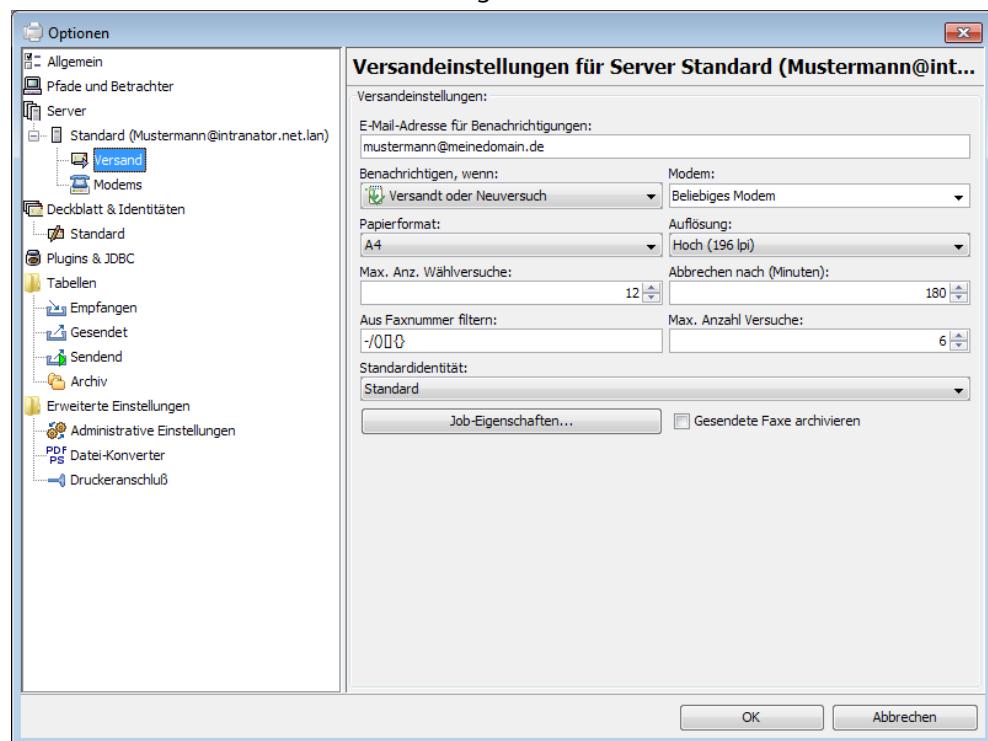
Zum Betrieb wird ein Java Runtime Environment (JRE), Version 6 oder neuer, benötigt. Sie können es von <http://www.java.com> herunterladen.

1. Starten Sie das Installationsprogramm. Wählen Sie den "RedMon"-Portmonitor, wenn Sie beim Installationsprozess danach gefragt werden.
2. Starten Sie YajHFC und öffnen das Menü Extras > Optionen.
3. Tragen Sie im Reiter Server Standard den Namen Ihres Intranators ein. Stellen Sie den Zeichensatz auf UTF-8. Sie können den Benutzernamen frei wählen, ein Passwort ist nicht erforderlich.

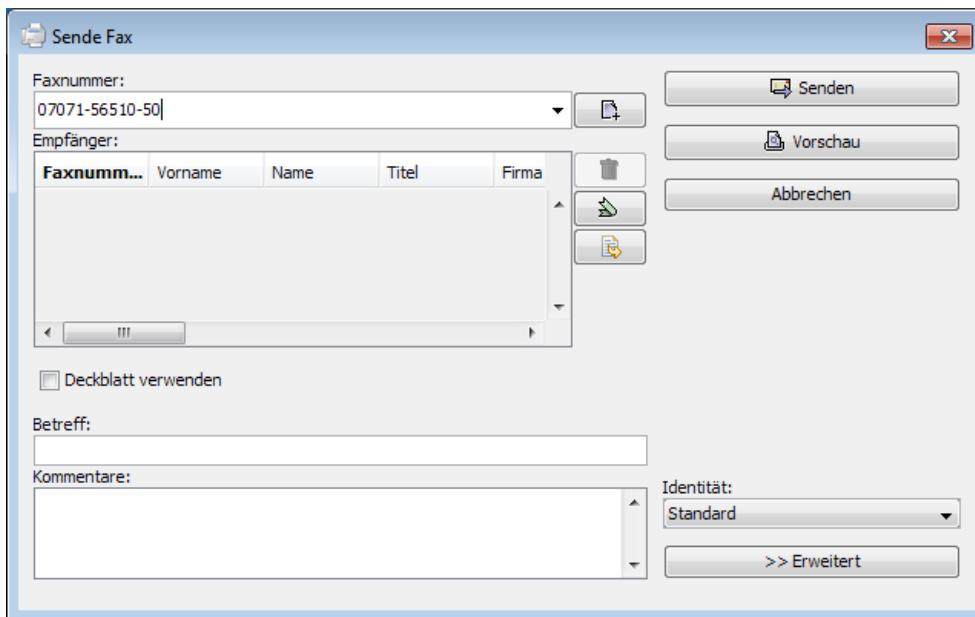
Wenn Sie als Benutzernamen exakt den Namen verwenden, der im Intranator im Menü Dienste > Fax > Empfänger im Feld Name eingetragen ist, werden die dort hinterlegten Namens- und Nummernkennungen für den Versand der Faxe verwendet.



4. Öffnen Sie den Reiter Versand und tragen dort Ihre E-Mail-Adresse ein.



YajHFC ist nun fertig konfiguriert. Zum Versenden von Faxen drucken Sie auf den automatisch installierten Drucker "YajHFC Fax". YajHFC startet automatisch und öffnet einen Dialog zur Eingabe der Faxnummer.



16.1.4. Unterschiede zwischen den Lizenzen

Empfangen und Versenden von Faxen ist nur bei Intranator-Lizenzen möglich, die die Funktion Mail Server enthalten.

16.2. Zeitserver

Der Intranator hält seine eigene Uhrzeit aktuell, indem er sich, sobald er online ist, mit Zeitservern im Internet synchronisiert.

Unter Dienste > Zeitabgleich können die verwendeten Zeitserver eingestellt werden. Standardmäßig werden Zeitserver aus einem öffentlich zugänglichen Pool verwendet. Mehr Informationen über diesen Pool erhalten Sie unter <http://www.pool.ntp.org>.

Die Rechner aus dem Intranet können den Intranator als Quelle für ihre eigene Zeit verwenden. Dafür kann sowohl das NTP- als auch das SMB-Protokoll verwendet werden. Um das NTP-Protokoll zu verwenden, können Sie ein separates NTP-Programm verwenden oder unter Windows den Intranator bei den Eigenschaften der Uhr als Internetzeitserver eintragen. Um das SMB-Protokoll zu verwenden, müssen Sie regelmäßig (z.B. bei jedem Systemstart) folgenden Befehl ausführen:

```
net time \\intranator.net.lan /set /yes
```

Dabei müssen Sie natürlich den lokalen Namen oder die IP-Adresse Ihres Intranators verwenden.

16.3. Überwachung per SNMP

Unter Dienste > Überwachung > SNMP kann man konfigurieren, ob und wie der Intranator Daten für die Überwachung per SNMP bereitstellen soll. Diese Daten können dann von einem zentralen SNMP-Überwachungsdienst abgefragt und ausgewertet werden.

Der Intranator bietet Informationen nicht über die unsicheren SNMP Versionen 1 und 2, sondern nur über die neuere, gesicherte Version 3 an. Es müssen Benutzername, Passwort

und Authentifizierungsprotokoll (MD5 oder SHA1) für die Anmeldung des Überwachungsdienstes beim Intranator angegeben werden.

Es ist sinnvoll, den Überwachungsdienst sich nicht nur beim Intranator anmelden zu lassen, sondern auch alle übertragenen Daten zu verschlüsseln. Wählen Sie dazu ein Verschlüsselungspasswort und ein Verschlüsselungsverfahren (AES oder DES). Es empfiehlt sich hier, das sichere AES zu verwenden, wenn der Überwachungsdienst dies unterstützt. Wenn Sie dann Nur verschlüsselte Datenübertragung aktivieren, muss der Überwachungsdienst korrekt verschlüsseln um die Daten des Intranators abfragen zu können.

Soll der Intranator aus dem lokalen Netz überwacht werden, müssen die Firewall-Einstellungen für den Rechner mit dem Überwachungsdienst dies zulassen. Dazu können Sie z.B. ein einfaches Rechnerprofil anlegen und diesem den zusätzlichen Dienst snmp hinzufügen. Soll der Intranator über das Internet überwacht werden, legen Sie eine VPN-Verbindung zwischen dem Überwachungsserver und dem Intranator. Über diese können dann die Daten abgefragt werden.

Der Intranator bietet über SNMP u.a. verschiedene Informationen zu CPU- und Speicherbelastung, Festplattenbelegung, Netzwerkauslastung, Intranator Version und Status des RAID-Arrays an. Damit diese Informationen von einem Überwachungsprogramm sinnvoll ausgewertet werden können, wird üblicherweise eine Beschreibung der Daten als Management Information Base (kurz MIB) benötigt. Diese sind in der Online-Hilfe der Seite Dienste > Überwachung > SNMP verlinkt.

16.4. Fernzugriff / RAS

Fernzugriff / RAS per ISDN (nur HDLC/syncPPP, kein X.75) ist z.B. für Fernwartung möglich. Unter Netzwerk > Fernzugriff > Anschlüsse müssen zuvor die an die eingewählten Rechner zu vergebenden IPs konfiguriert werden.

Der Fernzugriff kann unter Netzwerk > Fernzugriff > Einstellungen aktiviert werden. Dort wird auch die verwendete MSN eingestellt.

Der Intranator unterstützt keine Verbindungskomprimierung. Einige Clients haben daher Probleme beim Verbindungsauflauf oder die Verbindung bricht sehr häufig wieder zusammen. Deaktivieren Sie daher die Komprimierung im Client.

Als Login für den Fernzugriff werden die normalen Benutzeraccounts verwendet. Die Berechtigung zum Fernzugriff wird über die Benutzergruppen geregelt, die Rechte werden unter Benutzermanager > Gruppen > Rechte eingestellt.

17. Kapitel - Systemfunktionen

17.1. Lizenz

17.1.1. Demomodus

Nach der Installation befindet sich das System im Demomodus. Sie haben dann 30 Tage Zeit, alle Funktionen auszuprobieren. Der Funktionsumfang entspricht einem Intranator Business Server mit der einzigen Einschränkung, dass Backups nicht zurückgespielt werden können und keine Systemupdates erhältlich sind.

Nach Ablauf der 30 Tage werden Internetzugang und E-Mail-Verkehr blockiert. Konfigurationsdaten und E-Mails bleiben aber erhalten.



Hinweis

Der Intranator aktualisiert seine Systemzeit sobald er Online ist. Wird die Systemzeit während der Installation stark ab, kann es sein, dass der Zeitraum für die Demolizenz falsch berechnet wird. Installieren Sie in diesem Fall den Intranator erneut.

17.1.2. Lizenzcode

Haben Sie eine Lizenz erworben, können Sie diese in das System einspielen und damit aktivieren. Dafür benötigt der Intranator eine Internetverbindung. Diese sollte daher bereits konfiguriert sein und der Standardprovider korrekt eingestellt sein (siehe Abschnitt 11.8, „Verbindungsautomatik“).

Geben Sie im Menü Information > Lizenz Ihren vollständigen Lizenzcode ein. Ein vollständiger Lizenzcode besteht aus 5 Blöcken a 4 Zeichen, getrennt mit Bindestrichen (z.B. **A1B2-C3D4-E6F7-G8H9-I0J1**).

Fehlen der neuen Lizenz Funktionen, die auf dem Intranator momentan aktiv genutzt werden, kommt es beim Einspielen der Lizenz zu einem Konflikt und die neue Lizenz wird nicht aktiviert.

Sie haben nun die Möglichkeit, die betroffenen Funktionen zu deaktivieren. Sie werden im Menü Information > Lizenz aufgelistet. Danach können Sie die Lizenz erneut einspielen.

17.1.3. Updatezeitraum

In jeder Lizenz sind Funktions-, Sicherheits-, Spamfilter- und Virensannerupdates für 1 Jahr enthalten. Dieser Zeitraum zählt ab der Registrierung oder dem ersten Prüfen auf Updates. Auf der Seite Information > Lizenz wird das Enddatum angezeigt.

Ist die Lizenz für neue Updates ausgelaufen, läuft das System im aktuellen Zustand normal weiter. Es können auch weiterhin alle bis zum Ablaufdatum freigegebenen Updates eingespielt werden. Außer den Updates für das Intranator-System funktionieren aber auch die Updates für den Virensanner und Spamfilter nicht mehr. Beide Funktionen sind stark von aktuellen Daten abhängig, weshalb sich erfahrungsgemäß die Filterquoten bereits nach wenigen Tagen rapide verschlechtern.

17.2. Updates

Der Intranator enthält ein Updatesystem, mit dem er immer auf dem neuesten Softwarestand gehalten werden kann. Dies ist nötig, um Sicherheitsprobleme schnell beheben zu können und den Kunden neue Funktionen und Möglichkeiten zu bieten. Damit „veraltet“ der Intranator praktisch nicht.

Updates werden grundsätzlich immer übers Internet vom Intra2net-Server heruntergeladen und installiert. Manuelles Einspielen von Dateien ist nur für Notfälle vorgesehen und wird dann gemeinsam mit dem Intra2net-Support durchgeführt.

Unter System > Update > Einstellungen kann das Update konfiguriert werden. Der Intranator prüft in der Standardkonfiguration täglich auf neue Versionen und informiert den Administrator. Dieser kann das Update dann entweder sofort oder zeitlich versetzt einspielen. Zur Einwahl ins Internet wird (wenn nicht schon online) der Standardprovider (siehe Abschnitt 11.8, „Verbindungsautomatik“) verwendet.

Der Intranator führt nach jedem Update einen Reboot durch. Werden mehrere Updates gleichzeitig installiert, so wird das Update stufenweise von Version zu Version ausgeführt und nach jedem Schritt ein Reboot gemacht. Daher kann ein Update über mehrere Versionen eine längere Zeit dauern. Schalten Sie den Intranator nicht während des Updatevorgangs aus!

Die aktuelle Version des Intranators kann unter Information > Version eingesehen werden.

Das Update der Virendatenbanken wird separat von den Intranator-Updates durchgeführt. In der Standardkonfiguration prüft der Intranator stündlich auf neue Virendatenbanken und installiert diese dann vollautomatisch.

Auch die Spammerkmals-Datenbank wird unabhängig von den Intranator-Updates durchgeführt. Diese wird standardmäßig täglich vollautomatisch aktualisiert.

17.2.1. Update-Fernsteuerung via Partnerweb

Die Installation von Updates lässt sich zentral vom Intra2net Partnerweb aus steuern. Dies ist für Händler mit einer großen Anzahl von Intranatoren sehr bequem. Voraussetzung ist die aktivierte Funktion "Update-Fernsteuerung zulassen" unter System > Update > Einstellungen. Die Freischaltung im Partnerweb erfolgt in ca. 5 Minuten.

Im Partnerweb wählen Sie einzelne Intranatoren aus und können dann zu einer gewünschten Uhrzeit auf die neueste Version updaten. Das Installations-Kommando wird beim nächsten Update-Check übermittelt. Liegt die eingestellte Uhrzeit bereits in der Vergangenheit, so wird das Update am darauffolgenden Tag installiert.

17.3. Backup

Der Intranator enthält außer den Konfigurationsdaten bei Verwendung von IMAP auch alle E-Mails. Daher ist ein regelmäßiges Backup umso wichtiger.

Der Intranator beginnt in der Standardkonfiguration täglich um 02:00 Uhr mit dem Sichern aller Daten. Zusätzlich kann unter System > Backup > Einstellungen ein Backup auch manuell angestoßen werden.

Zur Sicherung der Backups kann entweder der Zugriff auf einen Rechner oder Benutzer beschränkt werden oder die Backups zusätzlich per GnuPG verschlüsselt werden. Im Auslieferungszustand werden die Backups aus Sicherheitsgründen auf einen Benutzer mit einem per Zufallsgenerator erzeugten Passwort beschränkt. Ändern Sie dieses Passwort oder schützen Sie Ihre Backups mit einer anderen Methode.

17.3.1. Auslagern

Bei einem Backup werden die Daten in 650 MB großen Dateiblöcken auf die Festplatte geschrieben. Es bleiben immer 2 Backupsätze auf dem Intranator. Selbstverständlich reicht es nicht aus, das Backup in eine Datei auf dem Intranator zu sichern, da z.B. die Festplatte kaputt gehen könnte.

Deshalb können die Backupsätze per HTTP oder SMB/CIFS (Windows Freigabe) vom Intranator auf einen anderen Rechner heruntergeladen werden. Dies kann z.B. durch eine automatisch gestartete Batchdatei geschehen oder indem das Verzeichnis auf dem Intranator einfach in ein bestehendes Backupprogramm mit aufgenommen wird.

Eine andere Möglichkeit ist das automatische entfernte Ablegen. Ist diese Funktion aktiv, lädt der Intranator die Backupdateien automatisch auf einen Zielserver hoch sobald sie erstellt wurden. Dies kann über das FTP- oder SMB-Protokoll geschehen. Per SMB kann der Intranator auch automatisch alte Backupsätze löschen.

17.3.2. Rücksichern

Zum Rückspielen von Backups können Backupsätze per SMB/CIFS auf den Intranator hochgeladen werden. Unter System > Backup > Wiederherstellen kann das Rückspielen gestartet werden.

Es gibt verschiedene Möglichkeiten Backups zurückzuspielen: Komplett (Konfiguration und E-Mails), nur die Konfiguration (alle E-Mails werden dabei gelöscht!) oder nur die E-Mails eines Benutzers.

Die E-Mails eines Benutzers können auch in einen IMAP Unterordner eines Benutzers zurückgespielt werden. Wurden z.B. einzelne wichtige E-Mails aus Versehen gelöscht, so können Sie damit zurückgeholt werden, ohne dass neuere E-Mails überschrieben werden.

Der Intranator kann Backups von alten Versionen zurückspielen. Dabei durchläuft die Konfiguration des Backups intern den Updateprozess. Es ist aber nicht möglich, Backups von neueren Versionen zurückzuspielen.

17.3.3. Vorgehen bei Festplattenschaden oder Hardwaretausch

Nach einem Festplattenschaden oder beim Tausch der für den Intranator verwendeten Hardware empfehlen wir nach der folgenden Liste vorzugehen. Wir raten dringend davon ab, die Daten des Intranators über Festplatten-Imaging-Programme oder ähnliche Lösungen zu transferieren. Bei einem Festplattendefekt würden die Defekte einfach mitkopiert, bei neuer Hardware bereiten häufig auch nur minimale Differenzen in der Festplattengröße Probleme mit dem Dateisystem.

Bei Hardwareumzug

1. Deaktivieren Sie das E-Mail- und Groupwaresystem im Menü Dienste > E-Mail > Einstellungen damit keine neu ankommenden E-Mails verloren gehen können

2. Backup starten
3. Wenn E-Mail-Archivierung in Verwendung: Kontrollieren ob die Archivierungsschnittstelle vollständig abgerufen und geleert wurde
4. Fertiges Backup auf anderen Rechner kopieren

Bei Defekt und Hardwareumzug

5. Aktuelle Installations-CD für den Intranator von www.intra2net.com [<http://www.intra2net.com>] herunterladen und auf CD brennen
6. Von der Installations-CD starten und Intranator installieren
7. Tragen Sie in der Installations-Maske den IP-Bereich Ihres lokalen Netzes ein
8. Verfügt die neue Hardware über 2 Festplatten, aktivieren Sie jetzt über die Weboberfläche, Menü System > Hardware > RAID, die Festplattenspiegelung
9. Öffnen Sie die Weboberfläche des Intranators und setzen ein neues Passwort für die Backup-Freigabe (Menü System > Backup > Einstellungen)
10. Kopieren Sie das Backup vom anderen Rechner auf die Restore-Freigabe des Intranators
11. Spielen Sie das Backup mit Konfiguration und E-Mails auf den Intranator zurück
12. Aktivieren Sie das E-Mail- und Groupwaresystem wieder, sofern Sie dieses vorher deaktiviert hatten
13. Konfiguration, E-Mails und Statistikdaten sind wiederhergestellt und funktionsfähig wie vorher

17.4. Betrieb hinter einer Firewall

Betreiben Sie den Intranator nicht direkt am Internet, sondern hinter einer Firewall, müssen Sie einige Verbindungen auf dieser freischalten.



Hinweis

Intra2net behält sich vor, die hinter den DNS-Namen stehenden IP-Adressen jederzeit und ohne Ankündigung zu verändern. Ausschließlich Änderungen an den DNS-Namen werden mit den Updates angekündigt. Sollte Ihre Firewall keine DNS-Namen annehmen und regelmäßig aktualisieren können, ist es ratsam, die DNS-Namen entweder regelmäßig zu überprüfen oder alle vom Intranator zu den entsprechenden Ports ausgehenden Verbindungen freizugeben.

Zu folgenden Zielen muss der Intranator Verbindungen aufbauen können (ausgehende Verbindungen):

Ziel	Protokoll	Zielport	Funktion
update.intranator.com	TCP	443 (https)	System-Updates, Antispam-Updates und Lizenzen
fsbwserver.f-secure.com	TCP	80 (http)	Virendatenbank-Updates

Ziel	Protokoll	Zielport	Funktion
intra2net.pool.ntp.org oder ein von Ihnen gewählter NTP-Server	TCP und UDP	123 (ntp)	Zeitabgleich
support.intranator.com	TCP	5000 bis 5050	Hersteller-Fernwartung
Ihr DNS-Server	TCP und UDP	53 (dns)	Namensauflösung
Mehrere Server	TCP	2703	Razor Spamerkennung

Weitere evtl. freizuschaltende Dienste sind E-Mail (POP3 und SMTP) sowie HTTP, HTTPS und FTP für den Proxy des Intranators.

17.5. Logdateien

Unter Information > System > Logdateien bietet der Intranator Zugriff auf die internen Logfiles (/var/log/messages und /var/log/maillog). Sie können entweder heruntergeladen werden oder die letzten Zeilen in einem Livelog angesehen werden.

Die Logfiles werden, sobald Sie eine gewisse Größe erreicht haben, rotiert. Die letzten 4 Versionen sind dabei auf dem Intranator gespeichert, ältere werden gelöscht.

17.6. Logcheck Reports

Unter Information > System > Report kann eingestellt werden, dass der Intranator täglich eine Auswertung der in den Logfiles gespeicherten Ereignisse per E-Mail versendet. Diese wird mit Logcheck und Fireparse durchgeführt.

Ist der Empfänger extern (z.B. der Händler), ist es aus Sicherheitsgründen ratsam, diese E-Mails zu verschlüsseln. Der Intranator bietet dafür eine PGP- und GnuPG-kompatible Verschlüsselung mit Passwort (symmetrische Verschlüsselung mit 256-Bit AES) an.

17.7. Zeitgesteuertes Herunterfahren

Um Strom zu sparen kann sich der Intranator automatisch ausschalten, wenn er nicht benötigt wird. Im Menü System > Herunterfahren können Sie Uhrzeiten programmieren, zu denen er sich ausschalten soll. Wenn Sie E-Mails direkt über SMTP empfangen, sollten Sie diese Funktion nicht nutzen, da ansonsten E-Mails als unzustellbar zum Absender zurückgesendet werden könnten. Auch VPN, Web-Groupware, Fernwartung, Portforwardings etc. funktionieren nicht während das Gerät ausgeschaltet ist.

Das Gerät schaltet sich zur programmierten Uhrzeit wieder ein. Dafür wird die Unterstützung des BIOS benötigt. Im BIOS muss dafür normalerweise eine Option wie Wake on PCI device oder Resume by PCI-E device aktiviert werden.

Testen Sie diese Funktion vor dem Einsatz über die Test-Schaltfläche. Das Gerät fährt herunter und muss sich nach 3 Minuten von alleine wieder einschalten. Sollte dies nicht geschehen, müssen Sie die Konfiguration des BIOS anpassen.

Teil 3. Groupware Client

18. Kapitel - Einführung

18.1. Systemvoraussetzungen

Betriebssystem	<ul style="list-style-type: none"> • Microsoft Windows 8 (32 und 64 Bit auf Intel x86-Plattform) • Microsoft Windows 7 (32 und 64 Bit) • Microsoft Windows 2008 Server (32 und 64 Bit) • Microsoft Windows Vista (32 und 64 Bit) • Microsoft Windows 2003 Server (32 und 64 Bit) • Microsoft Windows XP (32 Bit) <p>Der Betrieb in Terminal-Server-Umgebungen ist ohne Einschränkungen möglich.</p>
Microsoft Outlook	<ul style="list-style-type: none"> • Microsoft Outlook 2013 (32 Bit) • Microsoft Outlook 2010 (32 Bit) • Microsoft Outlook 2007 (mindestens SP1) • Microsoft Outlook 2003 (mindestens SP2)
Server	Intranator Server ab Version 6.0.0



Achtung

Es darf nur eine Version von Microsoft Office-Produkten auf dem System installiert sein. Sowohl unterschiedliche Versionen von Outlook und anderen Office-Komponenten, als auch verschiedene Versionen von Outlook gleichzeitig (wie von Outlook 2013 teilweise unterstützt, sog. Side-By-Side-Installationen), können mit dem Groupware Client nicht zuverlässig genutzt werden.

Auch von der Verwendung von Click-to-Run-Installationen von Microsoft Office raten wir ab, da wir in einigen Fällen Fehlfunktionen im Zusammenhang mit Click-to-Run beobachtet haben.

18.2. Übersicht der Funktionen

- Gemeinsamer Zugriff auf Termine, Kontakte, Aufgaben und Notizen
- Ordner anderer Benutzer lassen sich an beliebiger Stelle direkt in Outlook einblenden und können lokal frei benannt werden
- Sicherung der Groupware-Daten auf dem Server
- Synchronisation aller Ordner im Hintergrund
- Einstellbarer Synchronisationsrhythmus pro Ordner

- Gleichzeitige Verbindungen mit mehreren unterschiedlichen Servern um z.B. Daten in Zentrale und Außenstellen gemeinsam zu nutzen
- Konfiguration der serverseitigen Abwesenheitsschaltung und E-Mail-Weiterleitung innerhalb von Outlook
- Verwenden und Aktualisieren von Frei-/Gebucht-Informationen zusammen mit dem Intranator Server.
- Webzugriff auf E-Mails, Termine, Kontakte, Aufgaben und Notizen (Funktion des Intranator Servers 6.0, siehe 26. Kapitel, „Einführung in die Web-Groupware“)
- Webzugriff auf E-Mails, Termine, Kontakte, Aufgaben und Notizen mit einer speziell für Mobilgeräte optimierten Oberfläche (Funktion des Intranator Servers 6.0, siehe 26. Kapitel, „Einführung in die Web-Groupware“)
- Synchronisation der Daten auf mobile Geräte per ActiveSync (Funktion des Intranator Servers 6.1, siehe 29. Kapitel, „Mobile Geräte per ActiveSync anbinden“)

18.3. Bekannte Einschränkungen

Folgende, von Microsoft Outlook unterstützte Funktionen, können mit dem Intra2net Groupware Client nicht genutzt werden:

- Der Intra2net Groupware Client kann nicht zusammen mit einer Datendatei von Microsoft Exchange im selben Profil verwendet werden. Der gemeinsame Einsatz in verschiedenen Outlook-Profilen auf dem selben PC ist dagegen problemlos möglich.
- Geänderte Teilnehmer in einem Serienelement eines Serientermins
- Bei Outlook 2003 und 2007: Nachverfolgungs-Markierung mit Datumsangabe für E-Mails. Die Nachverfolgungs-Markierung wird ohne Zeitangabe gespeichert. Für Outlook 2010 und neuer siehe Abschnitt 22.9, „Erinnerungen und Nachverfolgen von E-Mails“.
- Journal-Funktion
- Verknüpfung von Groupware-Objekten untereinander (z.B. zwischen Kontakt und Termin)

Beachten Sie hierzu auch Abschnitt 25.1, „Synchronisierbare Daten“.

19. Kapitel - Installation

19.1. Installation des Programms

1. Rufen Sie die MSI-Datei aus dem ZIP-Archiv mit dem Windows Installer auf.
2. Folgen Sie den Anweisungen auf dem Bildschirm und lesen Sie sich insbesondere den Softwareüberlassungsvertrag (EULA) aufmerksam durch. Dieser ist ansonsten auch noch in Abschnitt B.1, „Intra2net Groupware Client Lizenzvertrag (EULA)“ zu finden.
3. Wählen Sie den Ordner, in den das Programm installiert werden soll und drücken Sie auf Weiter.



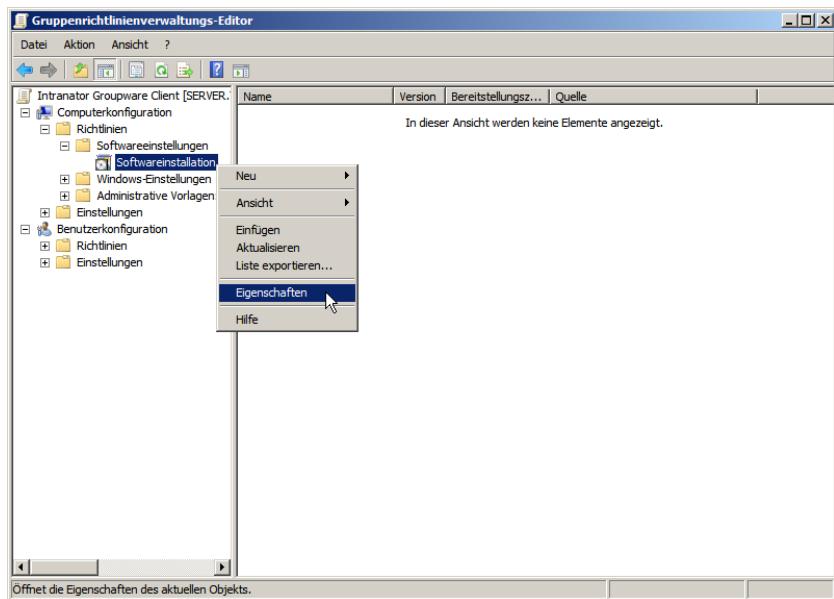
Im Folgenden finden Sie die nächsten Schritte, aufgeteilt nach den verschiedenen Versionen von Outlook.

19.2. Verteilung des Programms über Active Directory

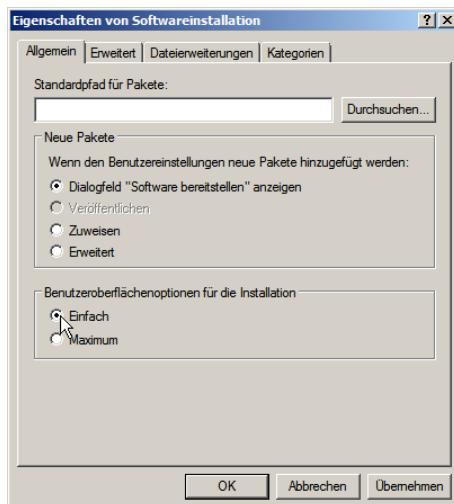
Das Programm wird als MSI-Datei geliefert und kann auf regulärem Weg per Active Directory auf den Rechnern einer Windows Domäne verteilt und aktualisiert werden. Eine Anleitung zur Softwareverteilung per Active Directory finden Sie unter <http://support.microsoft.com/kb/816102>.

Beachten Sie, dass das Programm mit der Benutzeroberflächenoption Einfach installiert werden muss:

1. Starten Sie den Gruppenrichtlinienverwaltungs-Editor und öffnen den Baum bis zur Softwareinstallation
2. Klicken Sie mit Rechts auf die Softwareinstallation und öffnen die Eigenschaften



3. Wählen Sie die Benutzeroberflächenoption Einfach.



4. Fügen Sie erst jetzt die MSI des Groupware Clients zur Softwareinstallation der Richtlinie hinzu.

19.3. Grundkonfiguration mit Outlook 2013

Outlook verwendet den Intra2net Groupware Client, indem ein spezieller Typ von Datendatei in ein Outlook-Profil eingebunden wird. Legen Sie wie im Folgenden beschrieben ein neues, leeres Profil an, konfigurieren ein E-Mail-Konto und binden die spezielle Datendatei ein.

Legen Sie unbedingt immer ein neues Profil an, auch wenn Sie Daten aus einer bestehenden Outlook-Konfiguration übernehmen wollen. Bestehende Daten können nach der Grundkonfiguration in das neue Profil importiert werden. Dies wird in Abschnitt 20.3, „Bestehende Daten übernehmen“ beschrieben.

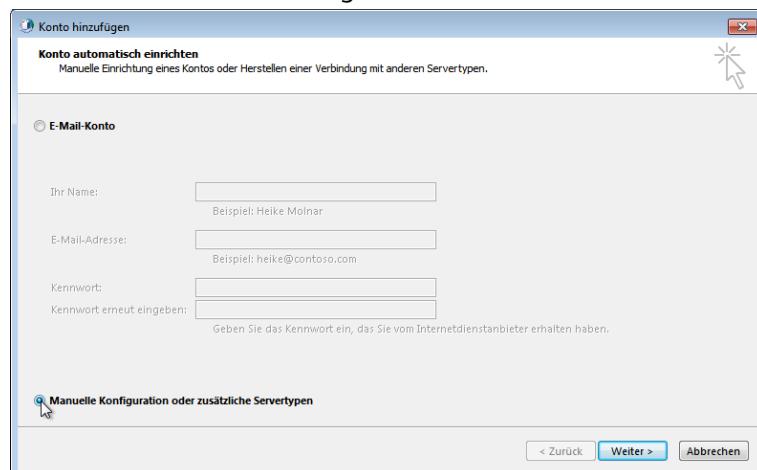
1. Öffnen Sie die Windows-Systemsteuerung, Menüpunkt E-Mail (32-Bit).
2. Öffnen Sie den Profil-Editor

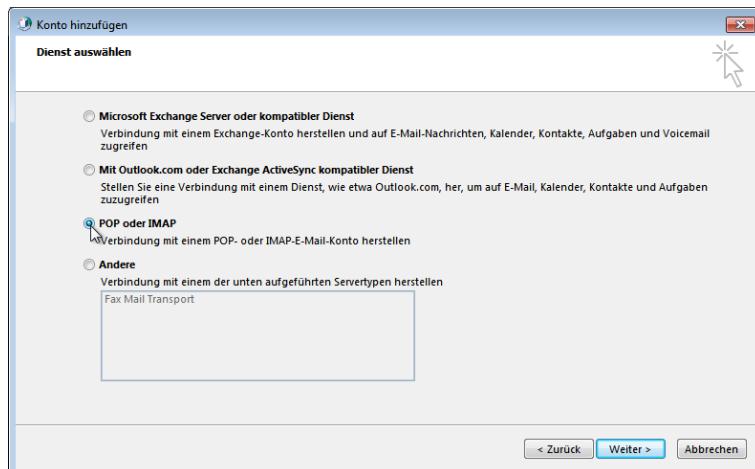


- Fügen Sie ein neues Profil hinzu und vergeben einen Namen



- Wählen Sie manuelle Konfiguration mit POP oder IMAP.

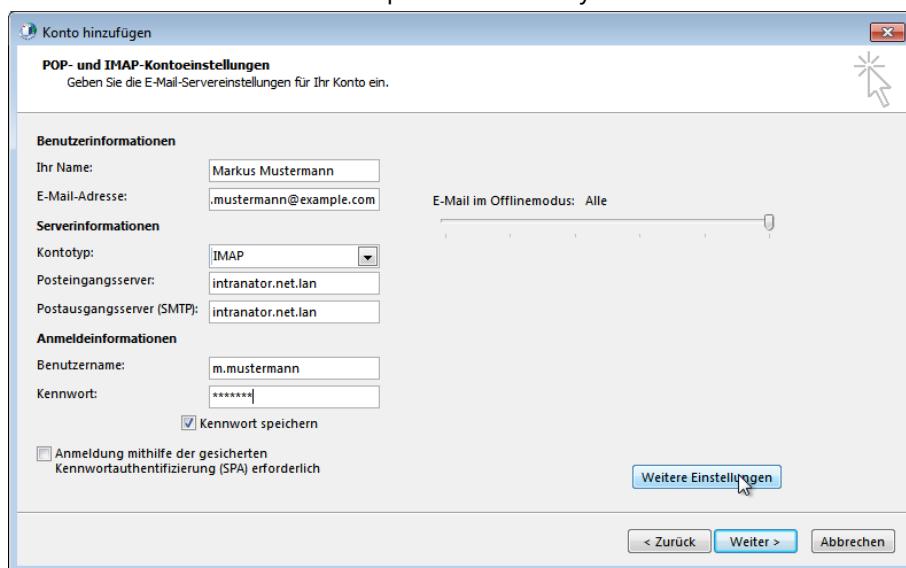




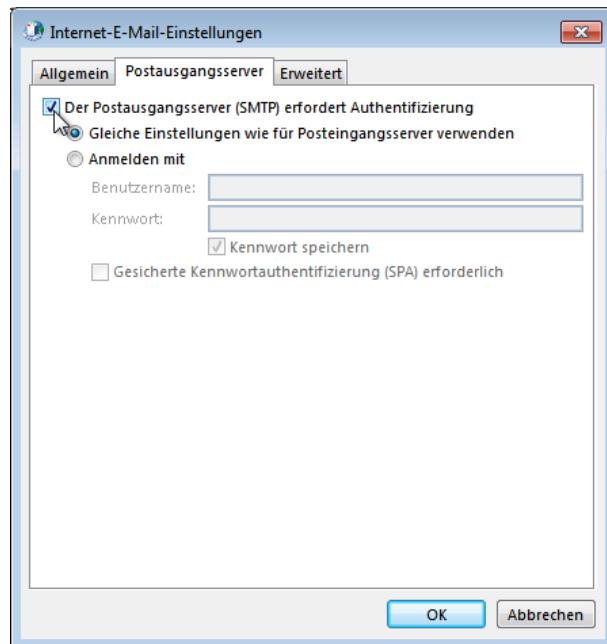
5. Stellen Sie den Kontotyp auf IMAP und tragen die Benutzer- und Serverdaten ein.

Verwenden Sie als Postein- und -ausgangsserver Ihren Intranator Server. Verwenden Sie unbedingt den vollständigen DNS-Namen inkl. Domain Ihres Intranator Servers, tragen Sie keine IP-Adressen ein.

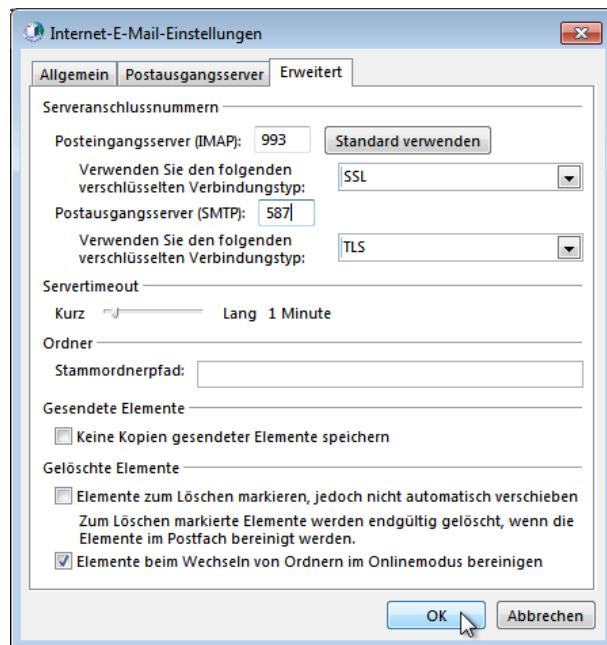
Soll der Client auch von außerhalb des lokalen Netzes zugreifen können, so verwenden Sie den externen DNS-Namen des Intranator Servers. Verwenden Sie auch hier keine IP-Adresse, sondern registrieren gegebenenfalls für Ihren Intranator Server einen DNS-Namen bei Ihrem Domainprovider oder DynDNS-Anbieter.



6. Öffnen Sie die Weiteren Einstellungen und den Reiter Postausgangsserver. Aktivieren Sie die SMTP-Authentifizierung mit den gleichen Einstellungen wie für den Posteingangsserver.

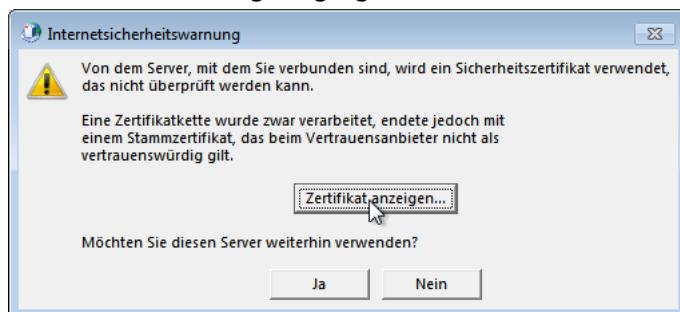


7. Öffnen Sie den Reiter Erweitert. Stellen Sie die Verschlüsselung für IMAP auf SSL und die für SMTP auf TLS. Ändern Sie die Portnummer für den Postausgangsserver auf 587 (für SMTP Submission / MSA). Schließen Sie die E-Mail-Einstellungen.

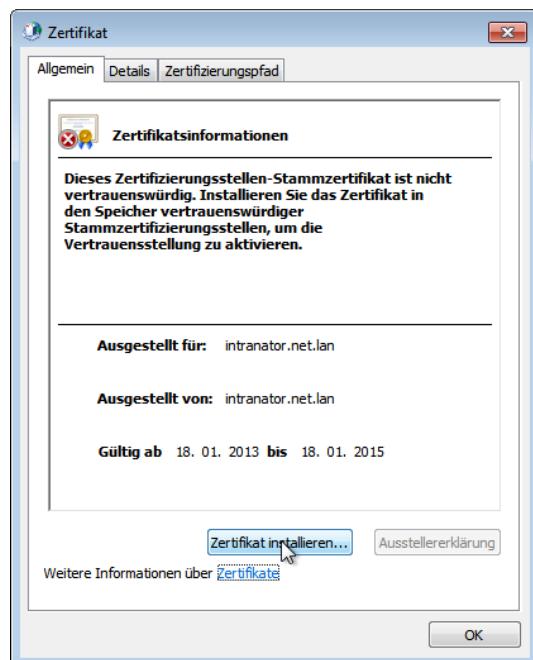


8. Testen Sie die Kontoeinstellungen durch einen Klick auf Weiter.
 - a. Geht der Test erfolgreich durch, können Sie die nächsten Schritte zur Zertifikatsinstallation überspringen.
 - b. Wird Ihnen die Fehlermeldung *Der Zielprinzipalname ist falsch oder eine Fehlernachricht zum Gültigkeitszeitraum des Zertifikats angezeigt*, müssen Sie zuerst auf dem Intranator Server ein passendes Zertifikat anlegen und/oder die DNS-Einstellungen anpassen. Weitere Informationen finden Sie im 10. Kapitel, „SSL-Verschlüsselung und Zertifikate“.

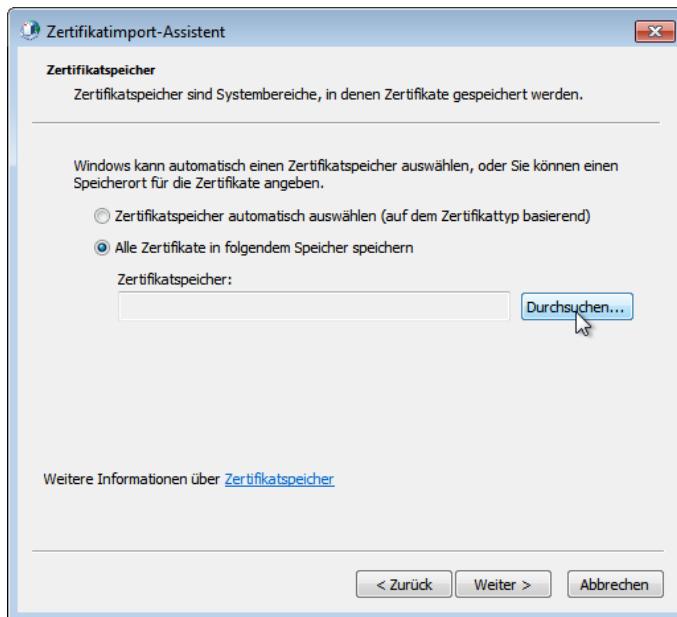
- c. Wird Ihnen eine Internetsicherheitswarnung wegen eines nicht vertrauenswürdigen Stammzertifikats angezeigt, gehen Sie auf Zertifikat anzeigen....



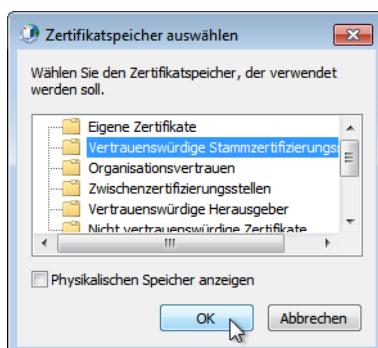
9. Gehen Sie auf Zertifikat installieren....



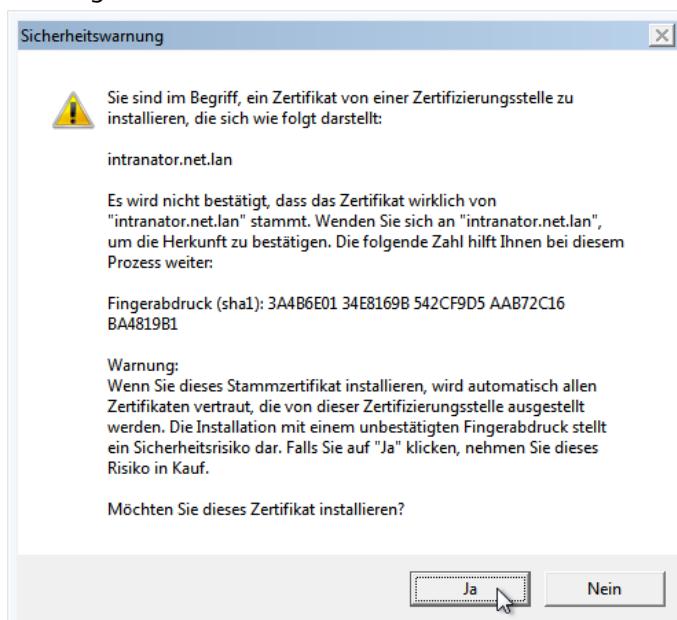
10. Es öffnet sich der Assistent zur Zertifikatsinstallation. Lassen Sie das Zertifikat in einem speziellen Speicher ablegen und klicken auf Durchsuchen.



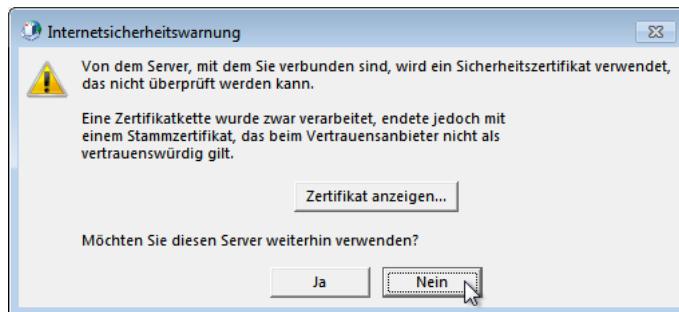
11. Wählen Sie den Zertifikatsspeicher Vertrauenswürdige Stammzertifizierungsstellen aus.



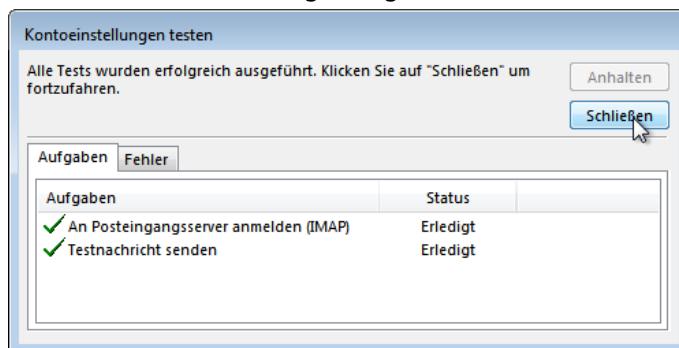
12. Bestätigen Sie die Installation des Zertifikats.



13. Brechen Sie die Sicherheitswarnung mit Nein ab und schließen das Testfenster.



14. Starten Sie erneut einen Test der Kontoeinstellungen. Diesmal muss die Verbindung ohne Sicherheitswarnung erfolgreich durchlaufen.



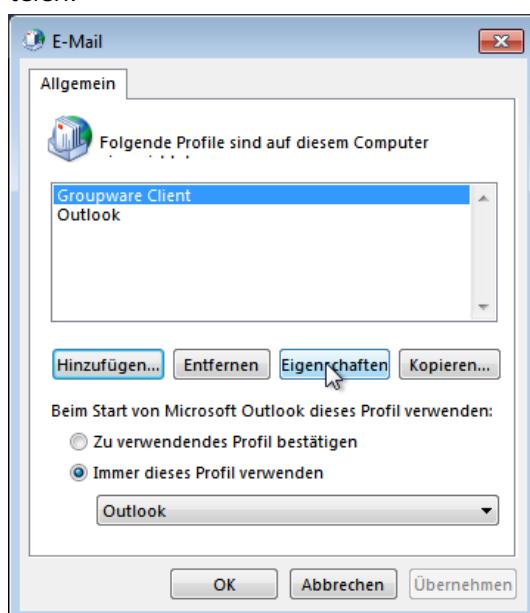
15. Beenden Sie die Kontokonfiguration.

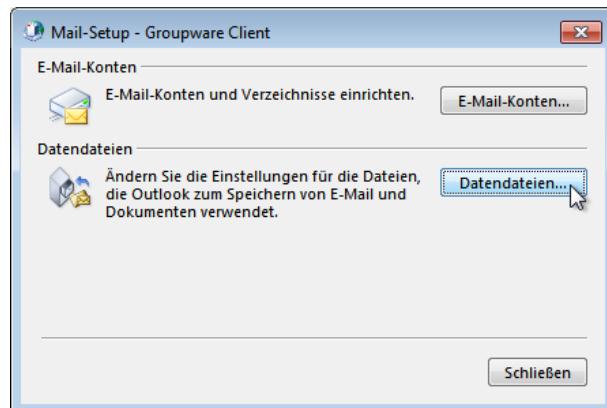


Achtung

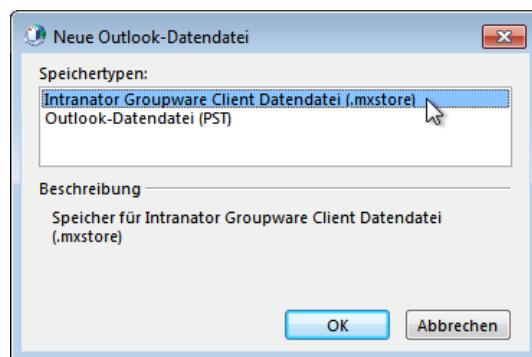
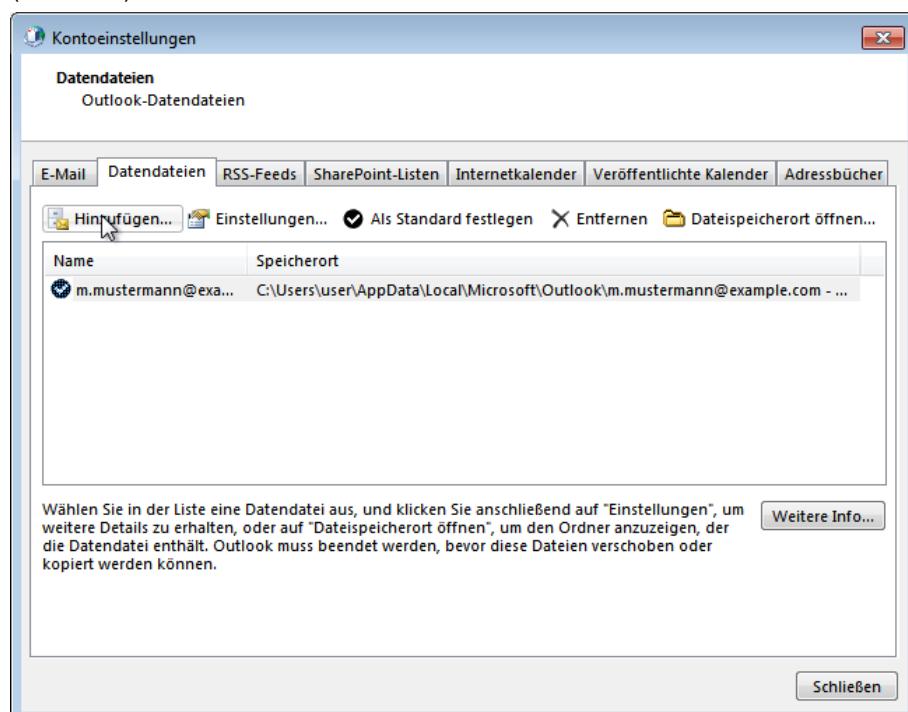
Starten Sie in diesem Zustand auf keinen Fall Outlook. Gehen Sie zuerst die folgenden Schritte dieser Anleitung durch. Ein Start von Outlook in diesem Moment würde alle Groupware-Standardordner in der falschen Datendatei anlegen und damit das Profil unbrauchbar machen.

16. Öffnen Sie die Eigenschaften des neuen Profils. Wählen Sie Bearbeiten der Datendateien.

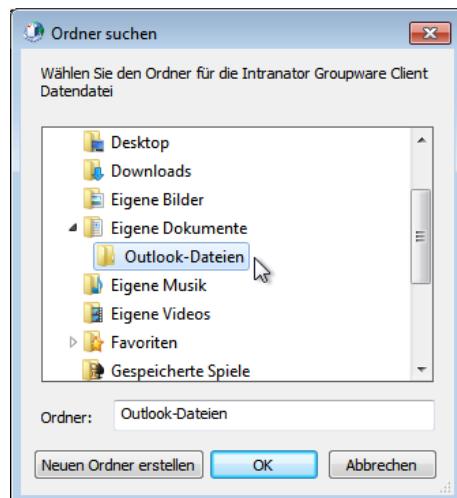




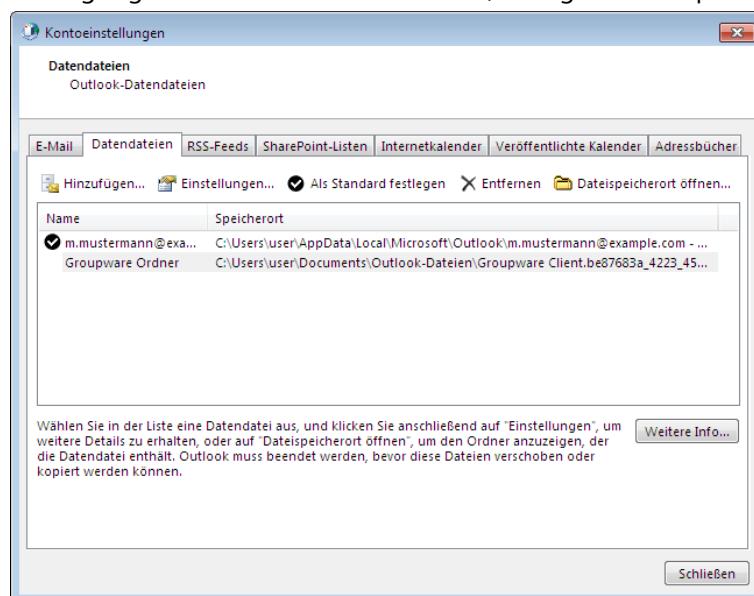
- Fügen Sie eine neue Datendatei vom Typ Intranator Groupware Client Datendatei (.mxstore) hinzu.



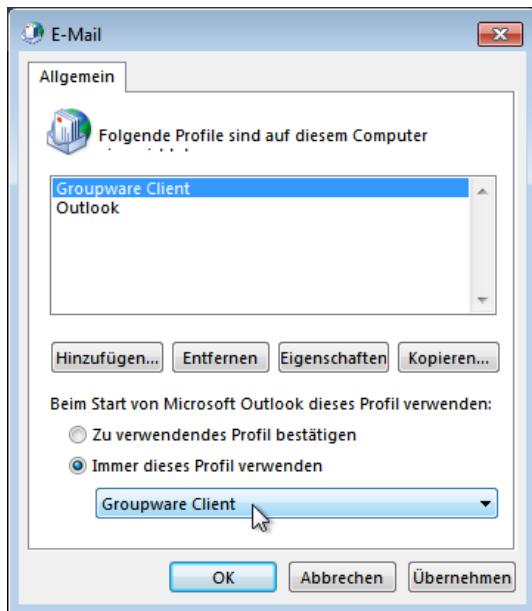
- Wählen Sie einen Ordner in dem die Datendatei des Intra2net Groupware Clients gespeichert werden soll.



19. Die neue Datendatei wurde hinzugefügt. Nehmen Sie keine Veränderung an der Festlegung der Standarddatendatei vor, dies geschieht später automatisch.



20. Schließen Sie den Dialog.
21. Wenn Sie möchten, können Sie Outlook automatisch beim Start das eben erstellte Profil öffnen lassen.



22. Starten Sie Outlook mit dem eben neu erstellten Profil. Es öffnet sich automatisch der Dialog Server-Konten des Intra2net Groupware Clients.
23. Fahren Sie mit der Einrichtung im 20. Kapitel, „Konten konfigurieren“ fort. Kehren Sie bei Synchronisationsproblemen mit den E-Mails zu Abschnitt 19.3.1, „Beheben von falsch erkannten Ordnerhierarchien“ zurück.

19.3.1. Beheben von falsch erkannten Ordnerhierarchien

Microsoft hat für Outlook 2013 die Unterstützung des IMAP-Protokolls vollständig neu entwickelt. Diese neuen Programmteile können in einigen Konstellationen aber noch Probleme machen. Im Folgenden wird erklärt wie man diese behebt.

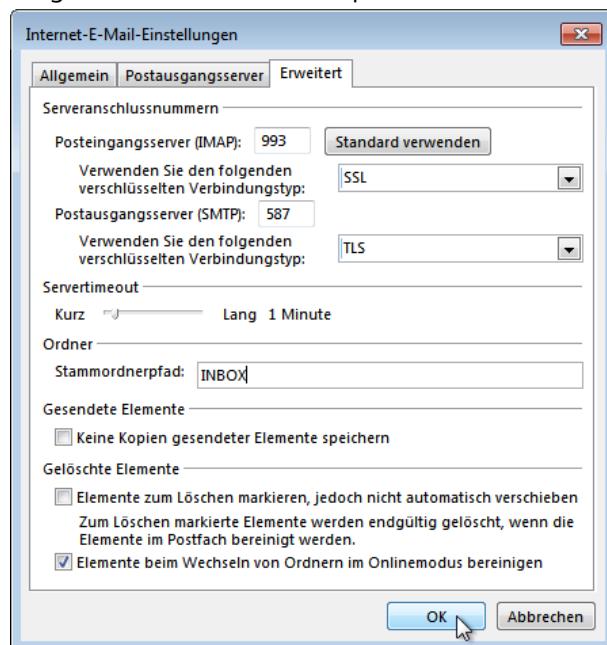
Die Probleme äußern sich meist dadurch, daß bei einigen oder allen E-Mail-Ordnern Synchronisationsprobleme auftreten. Dies bedeutet, daß E-Mails vom Server nicht angezeigt und lokale Änderungen nicht auf den Server geschrieben werden. Gleichzeitig erscheinen Fehlermeldungen im Ordner *Synchronisierungsprobleme (Nur dieser Computer)*. In vielen Fällen wird der Posteingang selbst korrekt synchronisiert, die Unterordner darunter aber nicht.

In anderen Fällen kommt es vor, dass Outlook die auf dem Server liegenden Ordner an einer falschen Stelle in der Hierarchie oder doppelt anzeigt.

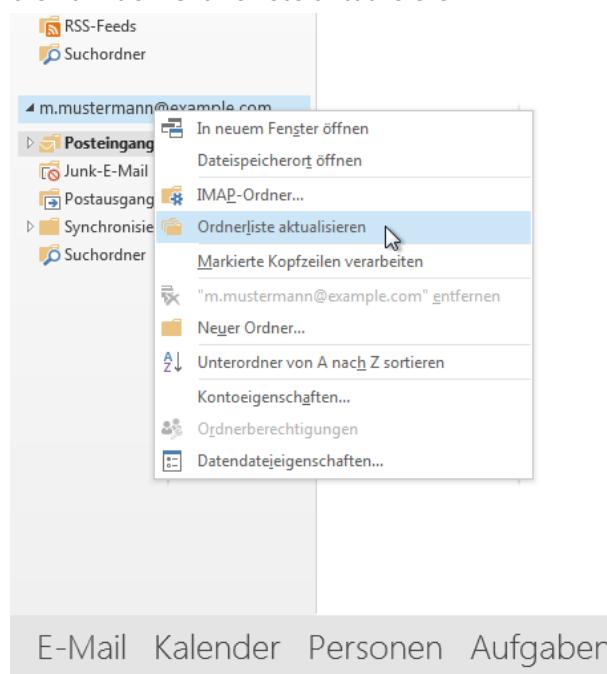
Ursache hinter diesen Problemen ist, dass Outlook die auf dem Server vorliegende Ordnerhierarchie falsch der lokalen Ordnerhierarchie zuordnet. Mit folgenden Schritten bringen Sie Outlook dazu, die Ordnerhierarchie korrekt zuzuordnen:

1. Öffnen Sie die Windows-Systemsteuerung, Menüpunkt E-Mail (32-Bit).
2. Öffnen Sie den Profil-Editor
3. Wählen Sie das mit dem Intra2net Groupware Client verwendete Profil und öffnen dessen Eigenschaften.
4. Wählen Sie E-Mail-Konten..., markieren das IMAP-Konto und Ändern....

5. Öffnen Sie die Weitere Einstellungen und darin den Reiter Erweitert.
6. Tragen Sie im Stammordnerpfad den Text **INBOX** ein und speichern mit OK.

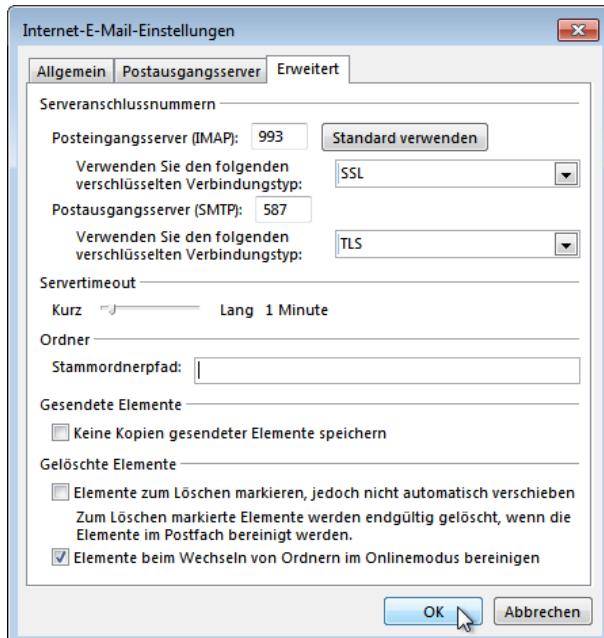


7. Schließen Sie die Systemsteuerung und starten Outlook
8. Klicken Sie mir Rechts auf das Wurzelverzeichnis der E-Mail-Datendatei und wählen die Funktion Ordnerliste aktualisieren.



9. Warten Sie kurz bis Outlook die Ordnerliste aktualisiert hat. Es ist nicht ungewöhnlich, wenn in diesem Zustand einige Ordner doppelt angezeigt werden.
10. Schließen Sie Outlook.
11. Öffnen Sie wieder die Systemsteuerung und gehen zum Erweitert-Reiter des IMAP-Kontos (siehe oben).

12. Löschen Sie die Einstellung bei Stammordnerpfad wieder.



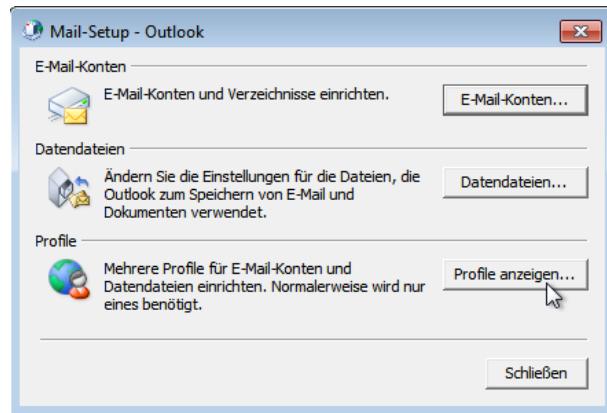
13. Speichern Sie und öffnen Outlook.
14. Klicken Sie mit Rechts auf das Wurzelverzeichnis der E-Mail-Datendatei und wählen die Funktion Ordnerliste aktualisieren.
15. Jetzt sollte die Ordnerhierarchie korrekt dargestellt werden. In einigen Fällen kann es nötig sein, mehrfach die Ordnerliste zu aktualisieren.
16. Vergleichen Sie den Inhalt der Ordner mit der Webgroupware und prüfen damit, ob jetzt alle Ordner korrekt synchronisiert werden.

19.4. Grundkonfiguration mit Outlook 2010

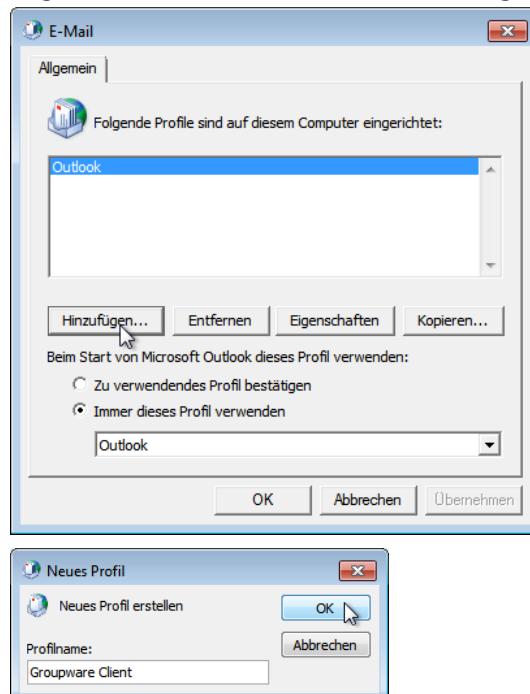
Outlook verwendet den Intra2net Groupware Client, indem ein spezieller Typ von Datendatei in ein Outlook-Profil eingebunden wird. Legen Sie wie im Folgenden beschrieben ein neues, leeres Profil an, konfigurieren ein E-Mail-Konto und binden die spezielle Datendatei ein.

Legen Sie unbedingt immer ein neues Profil an, auch wenn Sie Daten aus einer bestehenden Outlook-Konfiguration übernehmen wollen. Bestehende Daten können nach der Grundkonfiguration in das neue Profil importiert werden. Dies wird in Abschnitt 20.3, „Bestehende Daten übernehmen“ beschrieben.

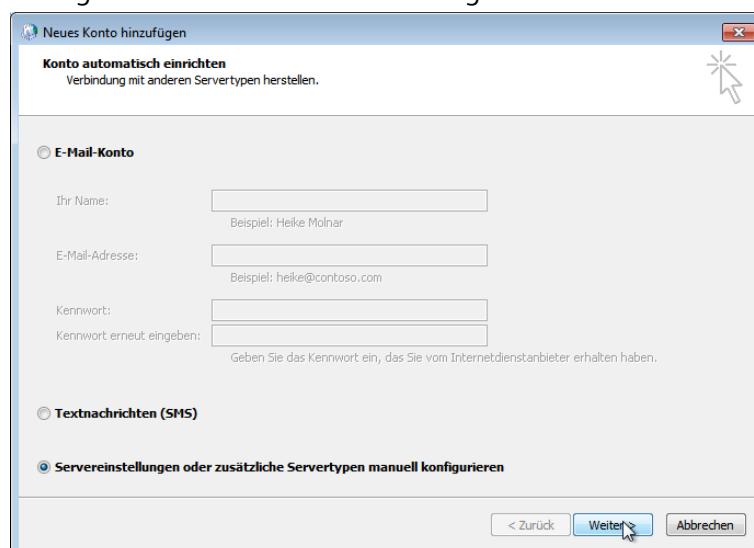
1. Öffnen Sie die Windows-Systemsteuerung, Menüpunkt E-Mail Setup (32-Bit).
2. Öffnen Sie den Profil-Editor

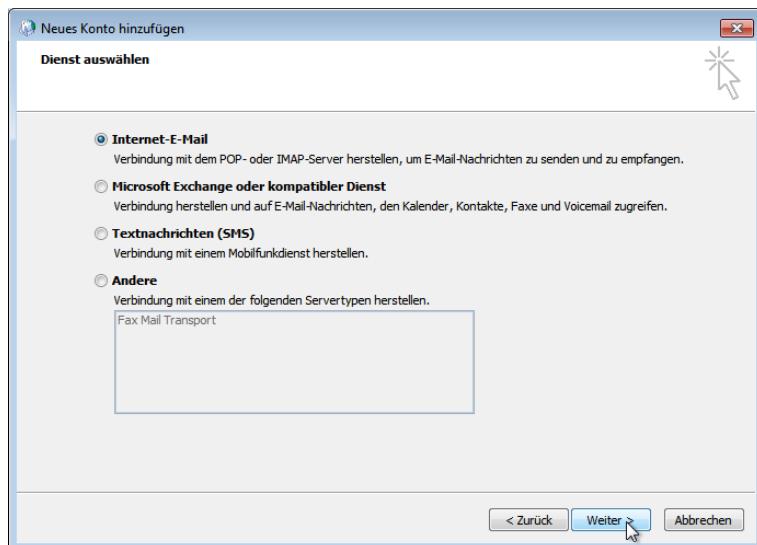


- Fügen Sie ein neues Profil hinzu und vergeben einen Namen



- Konfigurieren Sie die Servereinstellungen für Internet-E-Mail.

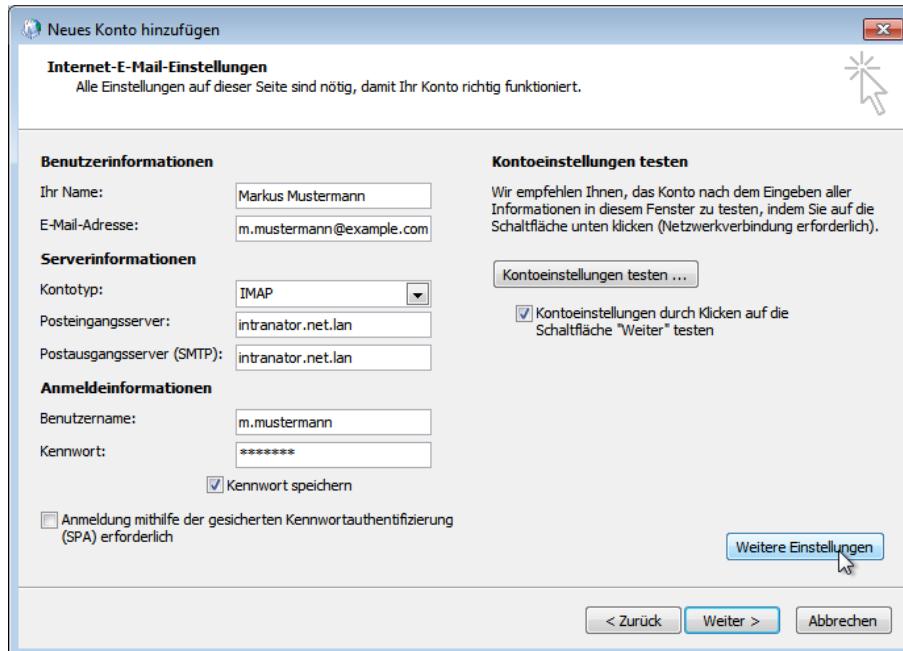




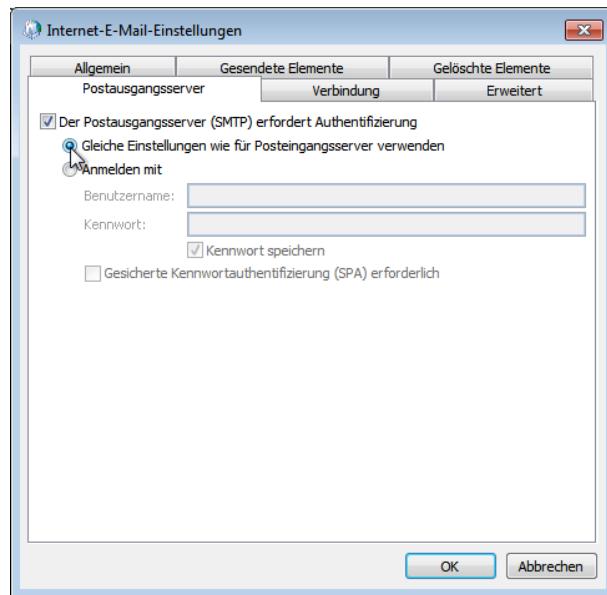
5. Stellen Sie den Kontotyp auf IMAP und tragen die Benutzer- und Serverdaten ein.

Verwenden Sie als Postein- und -ausgangsserver Ihren Intranator Server. Verwenden Sie unbedingt den vollständigen DNS-Namen inkl. Domain Ihres Intranator Servers, tragen Sie keine IP-Adressen ein.

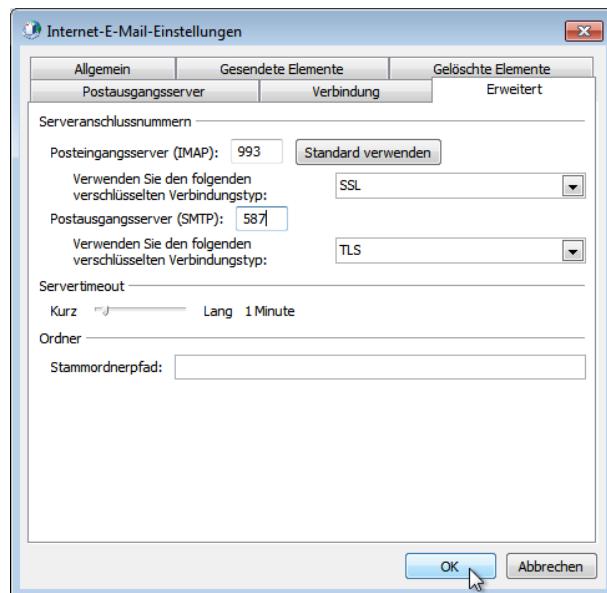
Soll der Client auch von außerhalb des lokalen Netzes zugreifen können, so verwenden Sie den externen DNS-Namen des Intranator Servers. Verwenden Sie auch hier keine IP-Adresse, sondern registrieren gegebenenfalls für Ihren Intranator Server einen DNS-Namen bei Ihrem Domainprovider oder DynDNS-Anbieter.



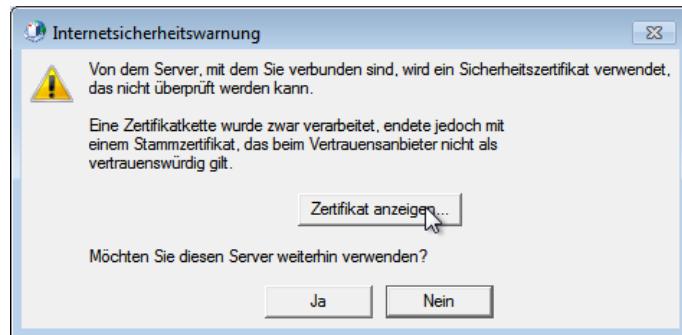
6. Öffnen Sie die Weiteren Einstellungen und den Reiter Postausgangsserver. Aktivieren Sie die SMTP-Authentifizierung mit den gleichen Einstellungen wie für den Posteingangsserver.



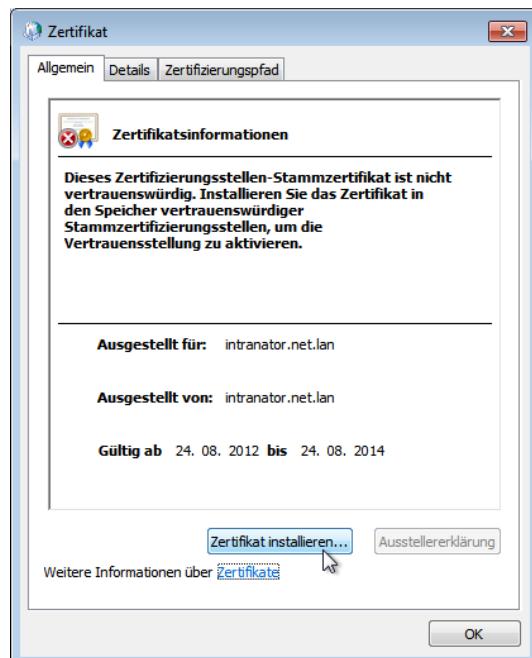
7. Öffnen Sie den Reiter Erweitert. Stellen Sie die Verschlüsselung für IMAP auf SSL und die für SMTP auf TLS. Ändern Sie die Portnummer für den Postausgangsserver auf **587** (für SMTP Submission / MSA). Schließen Sie die E-Mail-Einstellungen.



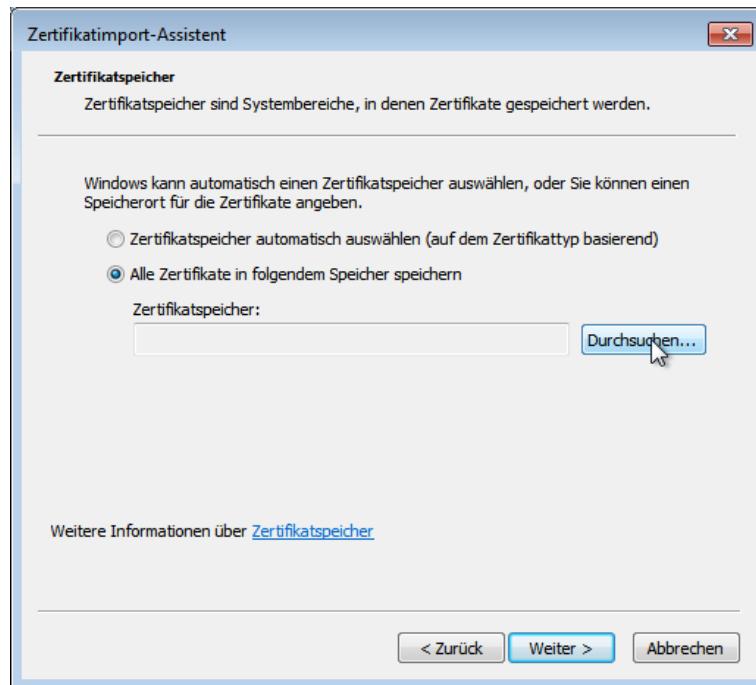
8. Testen Sie die Kontoeinstellungen.
 - a. Geht der Test erfolgreich durch, können Sie die nächsten Schritte zur Zertifikatsinstallation überspringen.
 - b. Wird Ihnen die Fehlermeldung `Der Zielprinzipalname ist falsch oder eine Fehlermeldung zum Gültigkeitszeitraum des Zertifikats angezeigt`, müssen Sie zuerst auf dem Intranator Server ein passendes Zertifikat anlegen und/oder die DNS-Einstellungen anpassen. Weitere Informationen finden Sie im 10. Kapitel, „SSL-Verschlüsselung und Zertifikate“.
 - c. Wird Ihnen eine Internetsicherheitswarnung wegen eines nicht vertrauenswürdigen Vertrauensanbieter angezeigt, gehen Sie auf `Zertifikat anzeigen....`



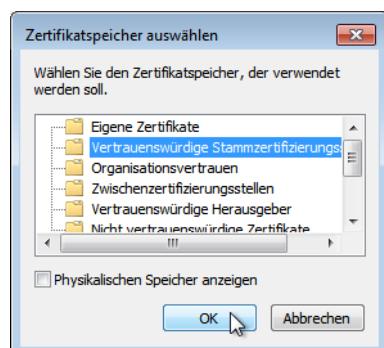
9. Gehen Sie auf Zertifikat installieren....



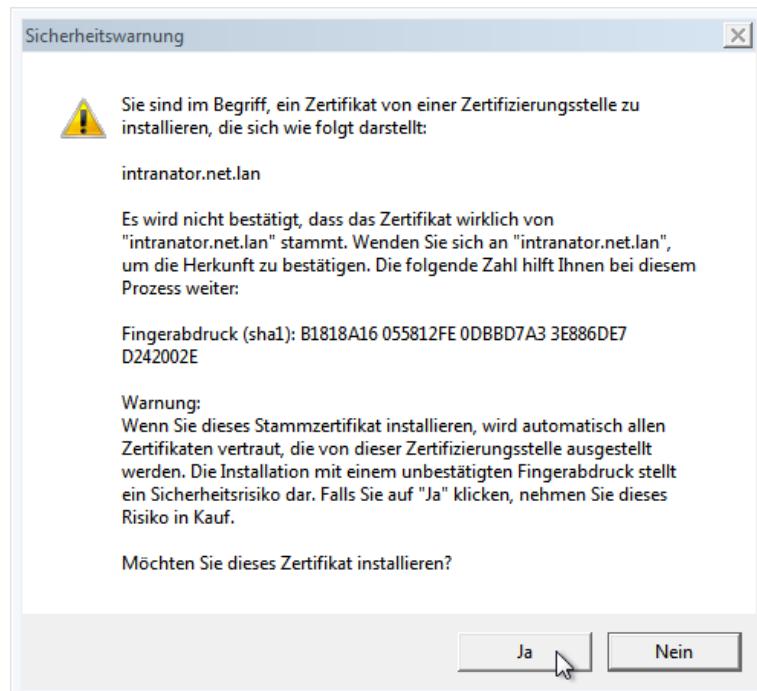
10. Es öffnet sich der Assistent zur Zertifikatsinstallation. Lassen Sie das Zertifikat in einem speziellen Speicher ablegen und klicken auf Durchsuchen.



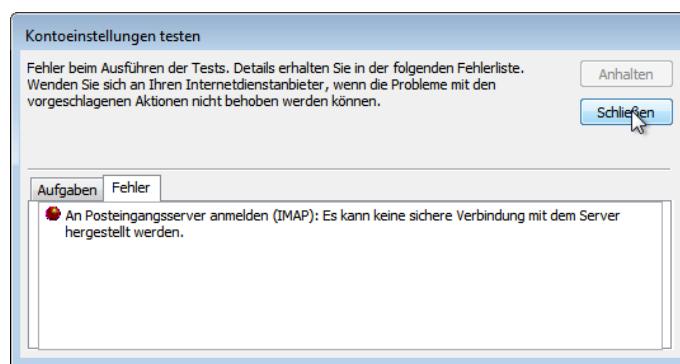
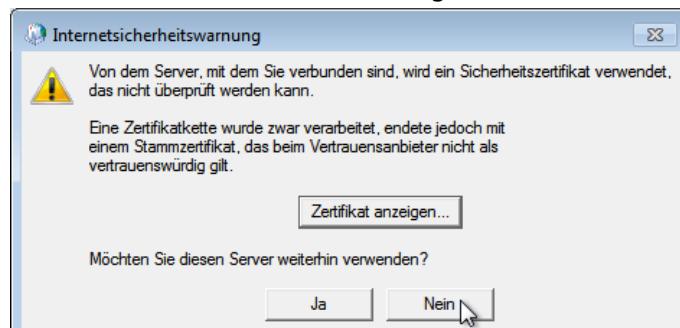
11. Wählen Sie den Zertifikatsspeicher Vertrauenswürdige Stammzertifizierungsstellen aus.



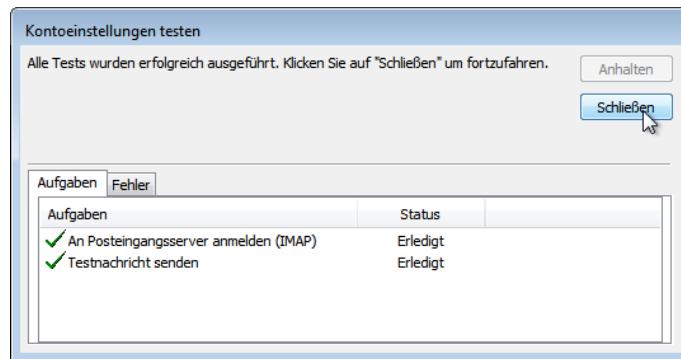
12. Bestätigen Sie die Installation des Zertifikats.



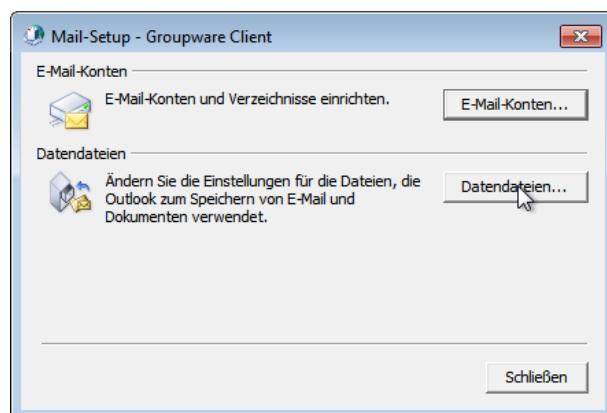
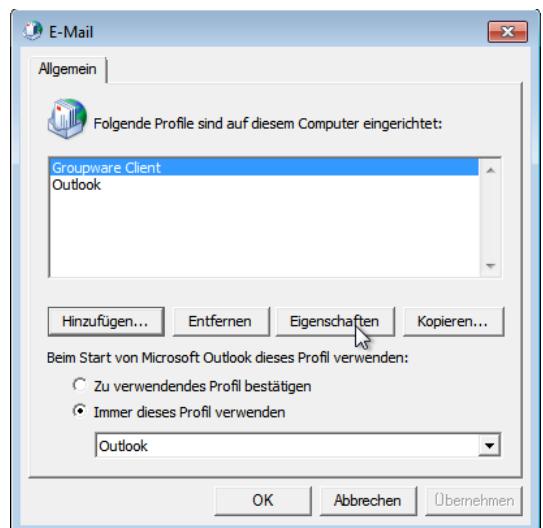
13. Brechen Sie die Sicherheitswarnung mit Nein ab und schließen das Testfenster.



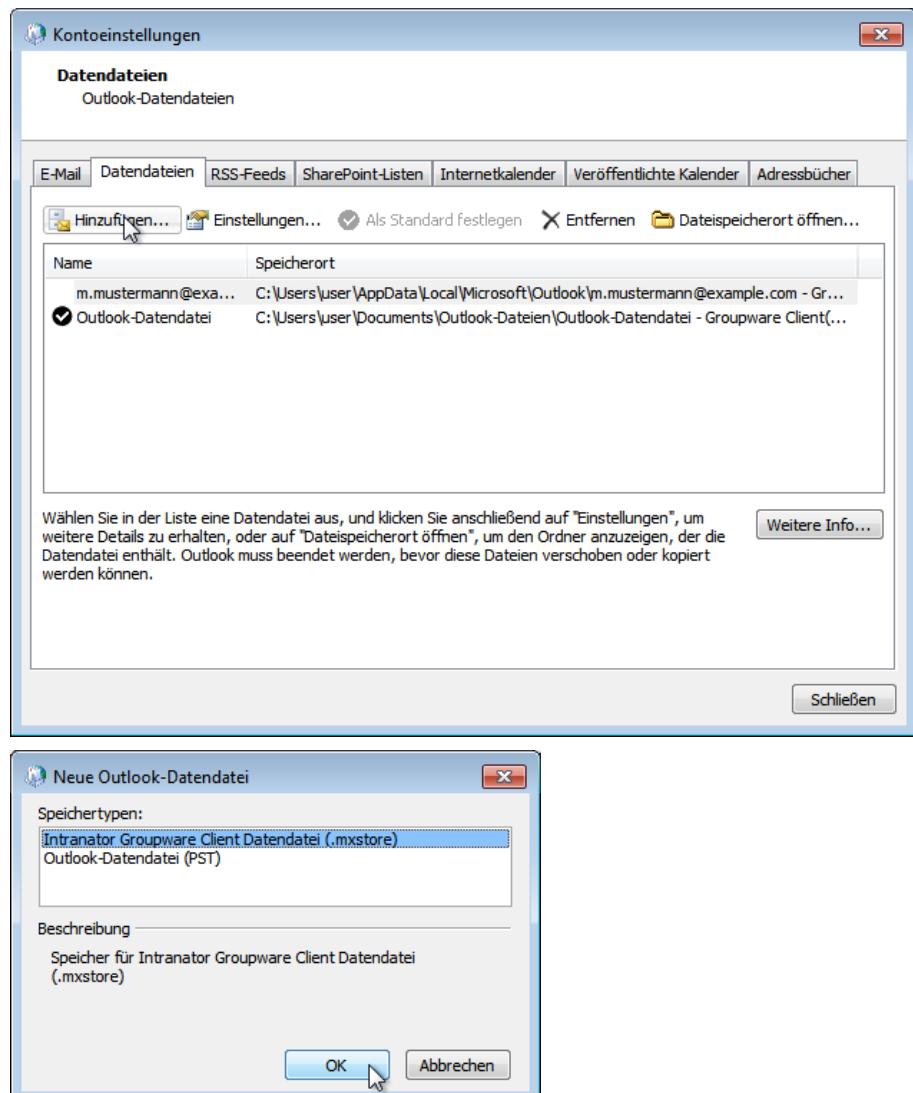
14. Starten Sie erneut einen Test der Kontoeinstellungen. Diesmal muss die Verbindung ohne Sicherheitswarnung erfolgreich durchlaufen.



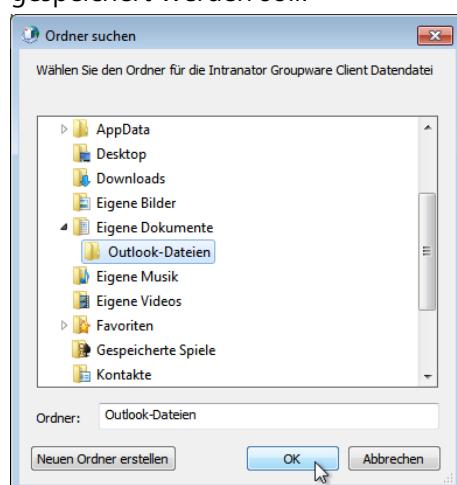
15. Beenden Sie die Kontokonfiguration und öffnen Sie die Eigenschaften des neuen Profils. Wählen Sie Bearbeiten der Datendateien.



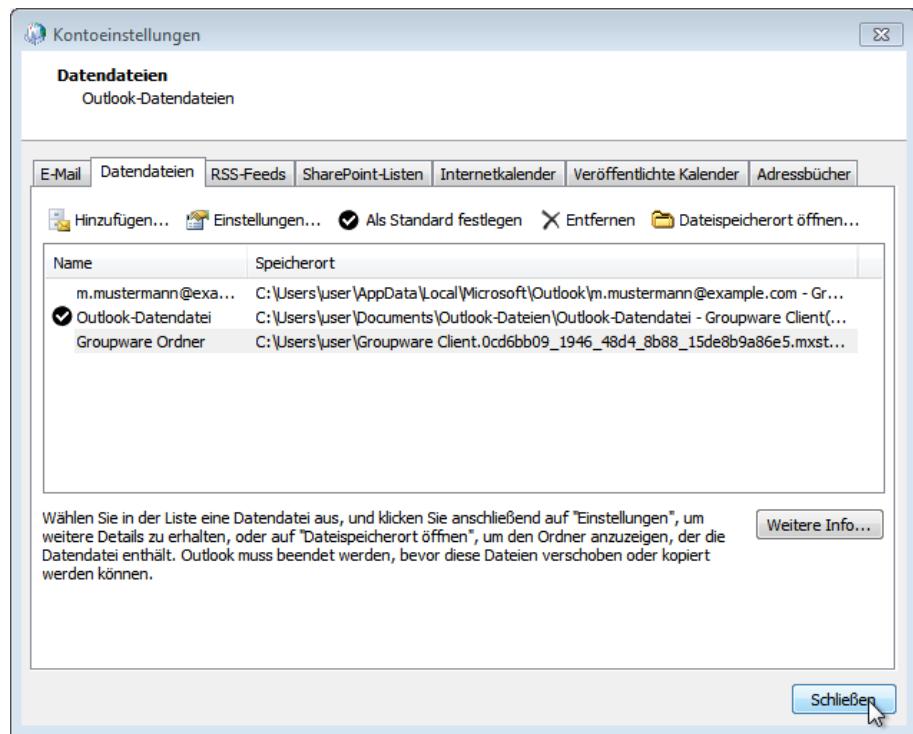
16. Fügen Sie eine neue Datendatei vom Typ Intranator Groupware Client Datendatei (.mxstore) hinzu.



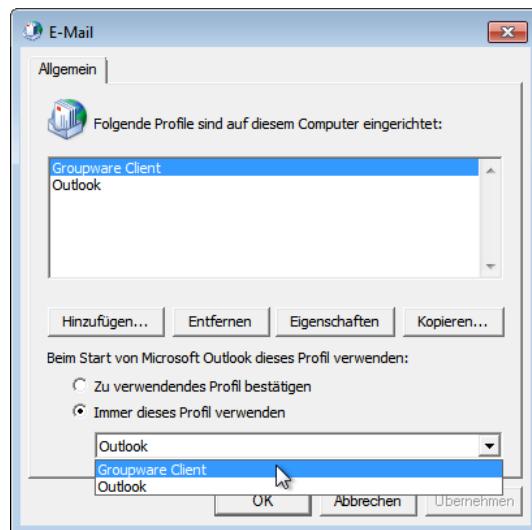
17. Wählen Sie einen Ordner in dem die Datendatei des Intra2net Groupware Clients gespeichert werden soll.



18. Schließen Sie den Dialog.



19. Wenn Sie möchten, können Sie Outlook automatisch beim Start das eben erstellte Profil öffnen lassen.



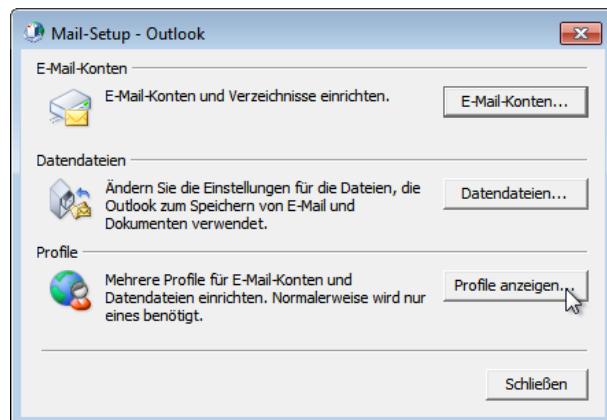
20. Starten Sie Outlook mit dem eben neu erstellten Profil. Es öffnet sich automatisch der Dialog Server-Konten des Intra2net Groupware Clients.
21. Fahren Sie mit der Einrichtung im 20. Kapitel, „Konten konfigurieren“ fort.

19.5. Grundkonfiguration mit Outlook 2007

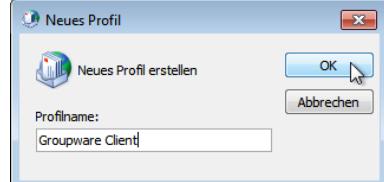
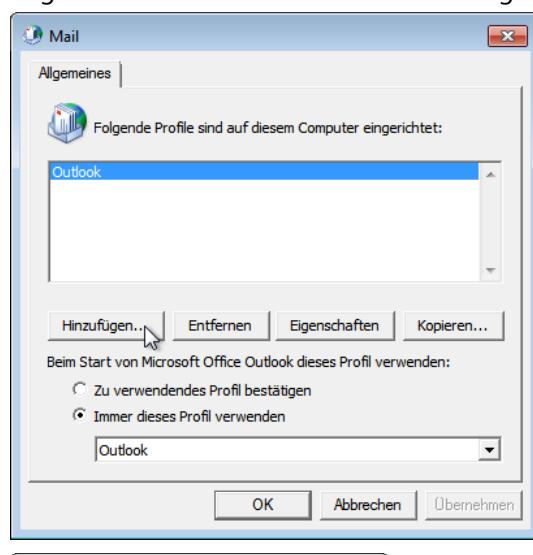
Outlook verwendet den Intra2net Groupware Client, indem ein spezieller Typ von Datendatei in ein Outlook-Profil eingebunden wird. Legen Sie wie im Folgenden beschrieben ein neues, leeres Profil an, konfigurieren ein E-Mail-Konto und binden die spezielle Datendatei ein.

Legen Sie unbedingt immer ein neues Profil an, auch wenn Sie Daten aus einer bestehenden Outlook-Konfiguration übernehmen wollen. Bestehende Daten können nach der Grundkonfiguration in das neue Profil importiert werden. Dies wird in Abschnitt 20.3, „Bestehende Daten übernehmen“ beschrieben.

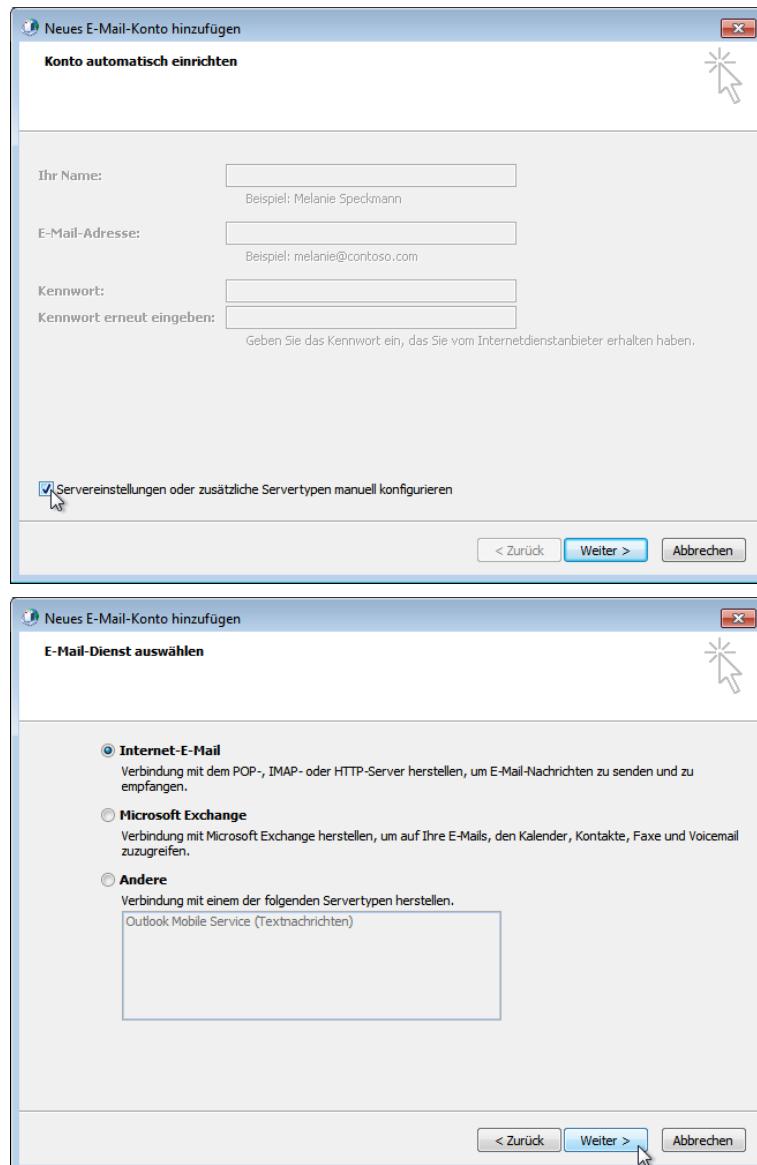
1. Installieren Sie das Zertifikat des Intranator Servers auf diesem Client. Die nötigen Schritte finden Sie im 10. Kapitel, „SSL-Verschlüsselung und Zertifikate“ beschrieben. Fahren Sie erst hier fort, wenn dies erfolgreich abgeschlossen ist.
2. Öffnen Sie die Windows-Systemsteuerung, Menüpunkt Mail (32-Bit).
3. Öffnen Sie den Profil-Editor



4. Fügen Sie ein neues Profil hinzu und vergeben einen Namen



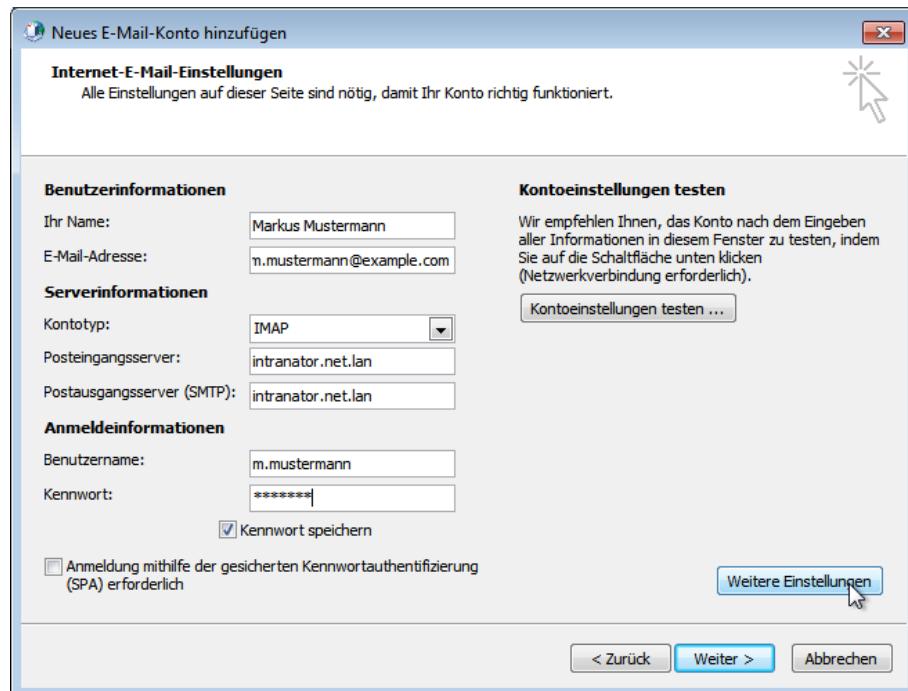
5. Konfigurieren Sie die Servereinstellungen für Internet-E-Mail.



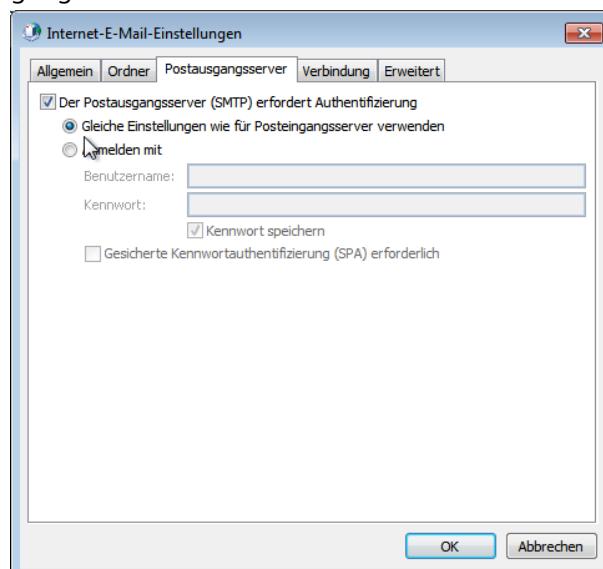
6. Stellen Sie den Kontotyp auf IMAP und tragen die Benutzer- und Serverdaten ein.

Verwenden Sie als Postein- und -ausgangsserver Ihren Intranator Server. Verwenden Sie unbedingt den vollständigen DNS-Namen inkl. Domain Ihres Intranator Servers, tragen Sie keine IP-Adressen ein.

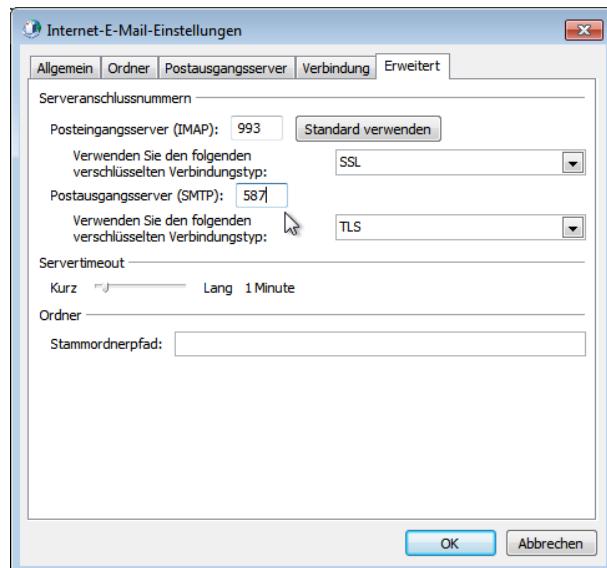
Soll der Client auch von außerhalb des lokalen Netzes zugreifen können, so verwenden Sie den externen DNS-Namen des Intranator Servers. Verwenden Sie auch hier keine IP-Adresse, sondern registrieren gegebenenfalls für Ihren Intranator Server einen DNS-Namen bei Ihrem Domainprovider oder DynDNS-Anbieter.



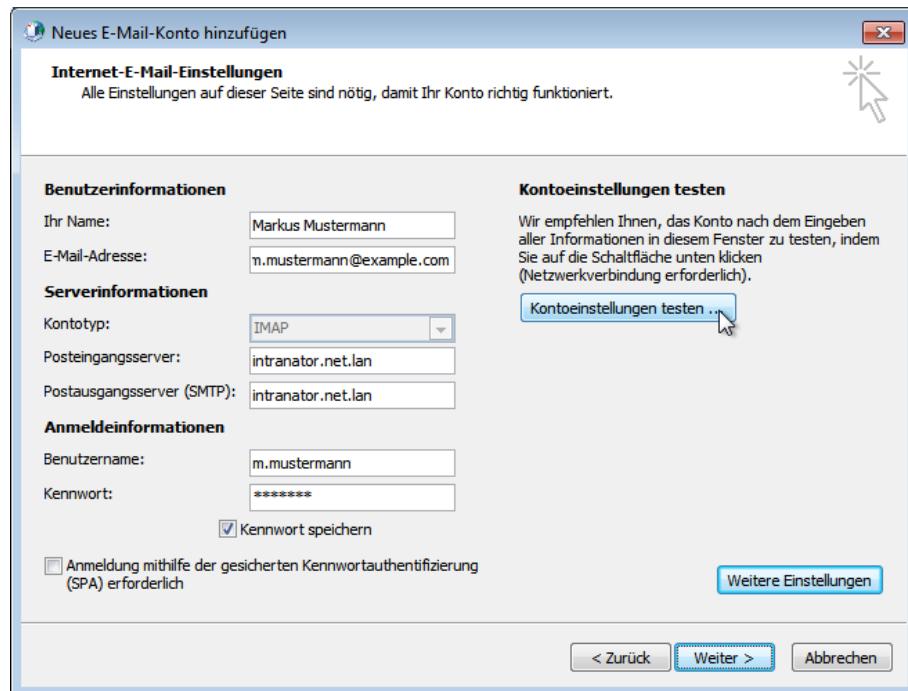
7. Öffnen Sie die Weiteren Einstellungen und den Reiter Postausgangsserver. Aktivieren Sie die SMTP-Authentifizierung mit den gleichen Einstellungen wie für den Posteingangsserver.



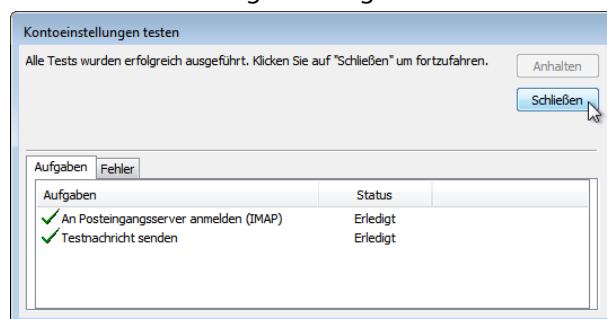
8. Öffnen Sie den Reiter Erweitert. Stellen Sie die Verschlüsselung für IMAP auf SSL und die für SMTP auf TLS. Ändern Sie die Portnummer für den Postausgangsserver auf 587 (für SMTP Submission / MSA). Schließen Sie die E-Mail-Einstellungen.



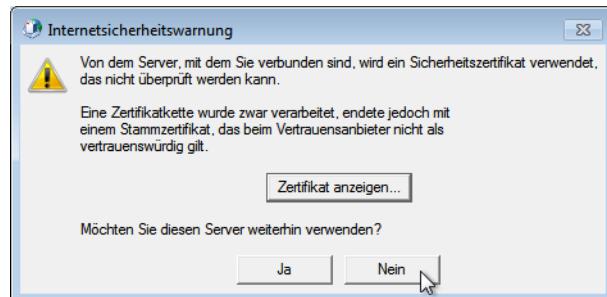
9. Testen Sie die Kontoeinstellungen.



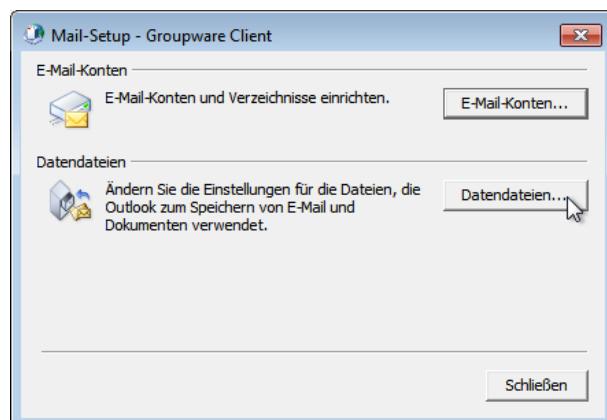
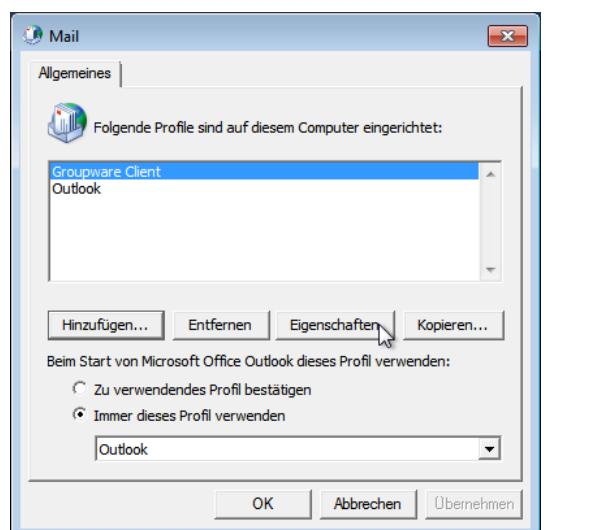
10. Der Test muss erfolgreich abgeschlossen werden.



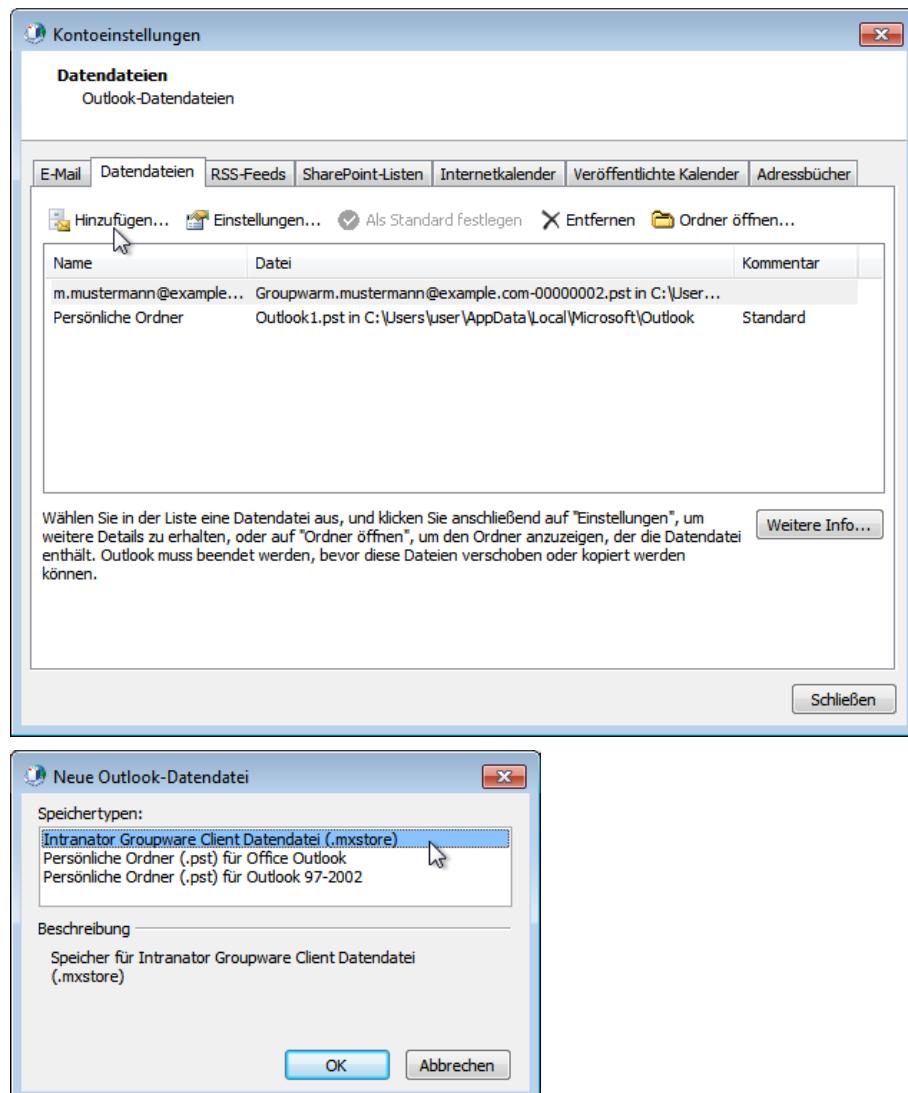
Wird Ihnen stattdessen eine Internetsicherheitswarnung angezeigt, so ist das Zertifikat nicht korrekt konfiguriert oder installiert. Wiederholen Sie Schritt 1 und versuchen es erneut bis der Test erfolgreich ist.



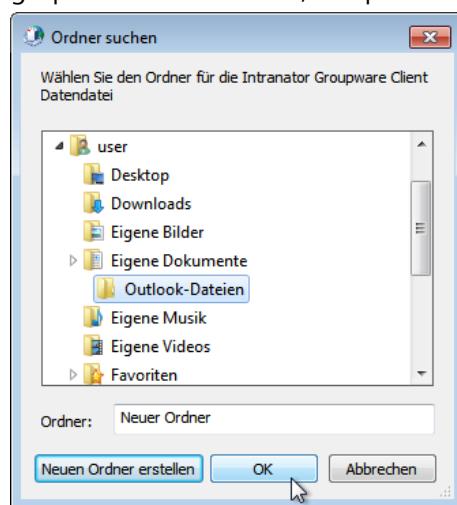
11. Beenden Sie die Kontokonfiguration und öffnen Sie die Eigenschaften des neuen Profils. Wählen Sie Bearbeiten der Datendateien.



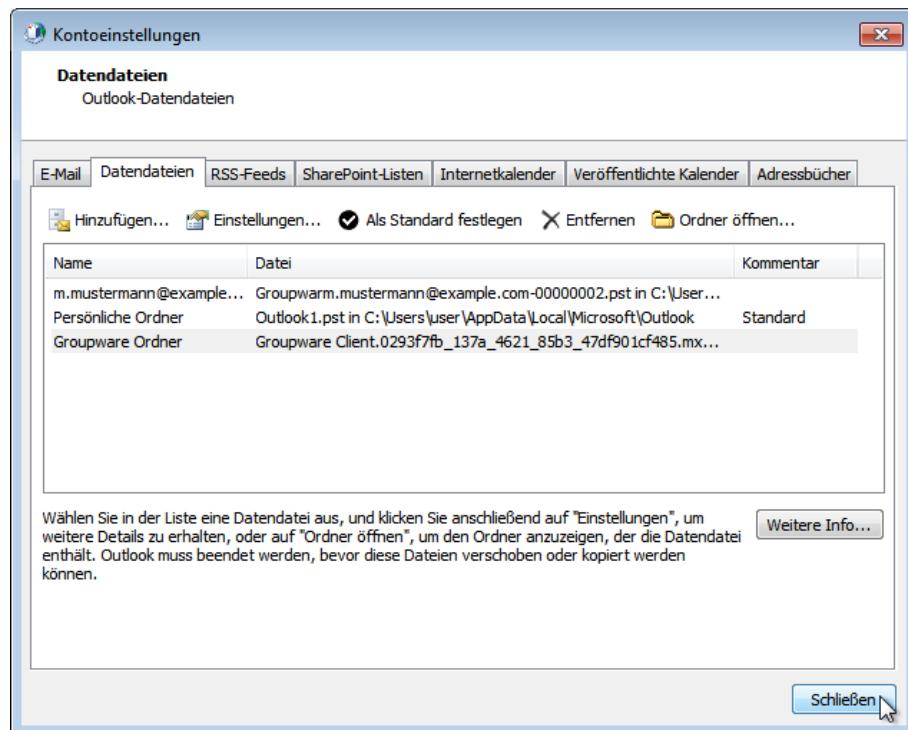
12. Fügen Sie eine neue Datendatei vom Typ Intranator Groupware Client Datendatei (.mxstore) hinzu.



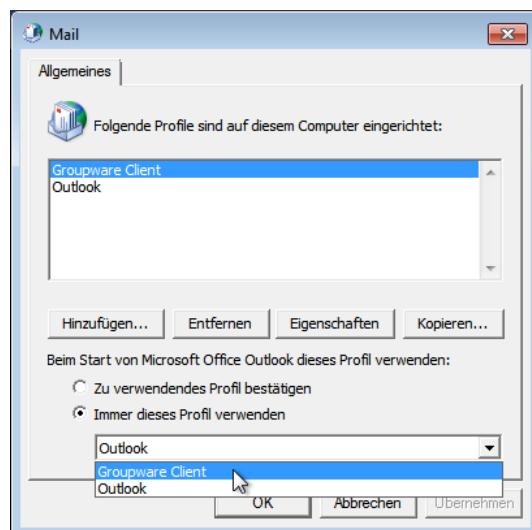
13. Wählen Sie einen Ordner in dem die Datendatei des Intra2net Groupware Clients gespeichert werden soll, beispielsweise Eigene Dokumente\Outlook-Dateien.



14. Schließen Sie den Dialog.



15. Wenn Sie möchten, können Sie Outlook automatisch beim Start das eben erstellte Profil öffnen lassen.



16. Starten Sie Outlook mit dem eben neu erstellten Profil. Es öffnet sich automatisch der Dialog Server-Konten des Intra2net Groupware Clients.
17. Fahren Sie mit der Einrichtung im 20. Kapitel, „Konten konfigurieren“ fort.

19.6. Grundkonfiguration mit Outlook 2003



Achtung

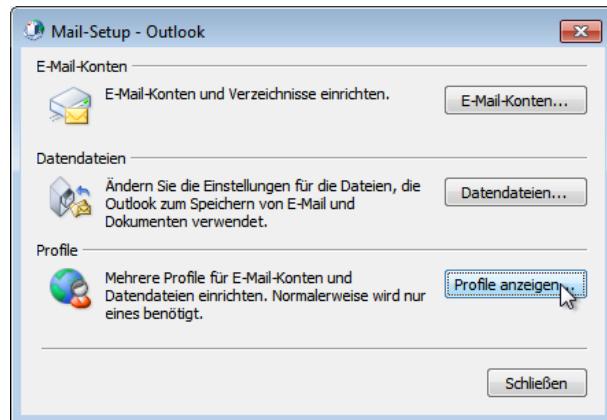
Outlook 2003 wird von Microsoft nicht mehr unterstützt. Es gibt keinerlei Updates mehr, auch nicht für kritische Sicherheitslücken. Wir empfehlen daher dringend, baldmöglichst auf eine neue Version zu migrieren.

Weitere Informationen finden Sie unter <http://www.microsoft.com/de-de/windows/xp/default.aspx>.

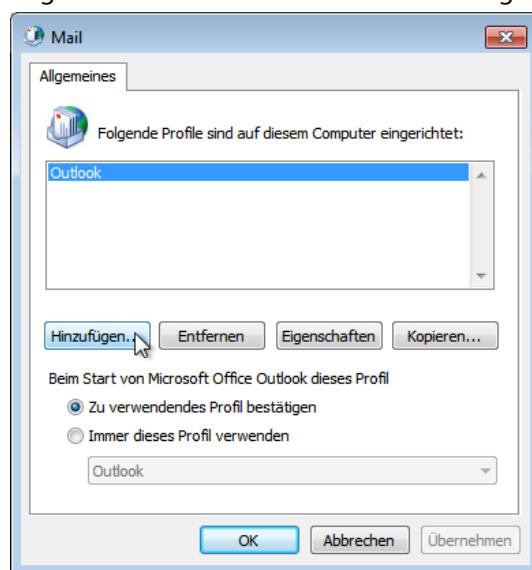
Outlook verwendet den Intra2net Groupware Client, indem ein spezieller Typ von Datendatei in ein Outlook-Profil eingebunden wird. Legen Sie wie im Folgenden beschrieben ein neues, leeres Profil an, konfigurieren ein E-Mail-Konto und binden die spezielle Datendatei ein.

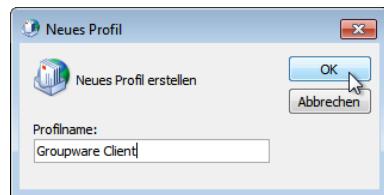
Legen Sie unbedingt immer ein neues Profil an, auch wenn Sie Daten aus einer bestehenden Outlook-Konfiguration übernehmen wollen. Bestehende Daten können nach der Grundkonfiguration in das neue Profil importiert werden. Dies wird in Abschnitt 20.3, „Bestehende Daten übernehmen“ beschrieben.

1. Installieren Sie das Zertifikat des Intranator Servers auf diesem Client. Die nötigen Schritte finden Sie im 10. Kapitel, „SSL-Verschlüsselung und Zertifikate“ beschrieben. Fahren Sie erst hier fort, wenn dies erfolgreich abgeschlossen ist.
2. Öffnen Sie die Windows-Systemsteuerung, Menüpunkt Mail (32-Bit).
3. Öffnen Sie den Profil-Editor

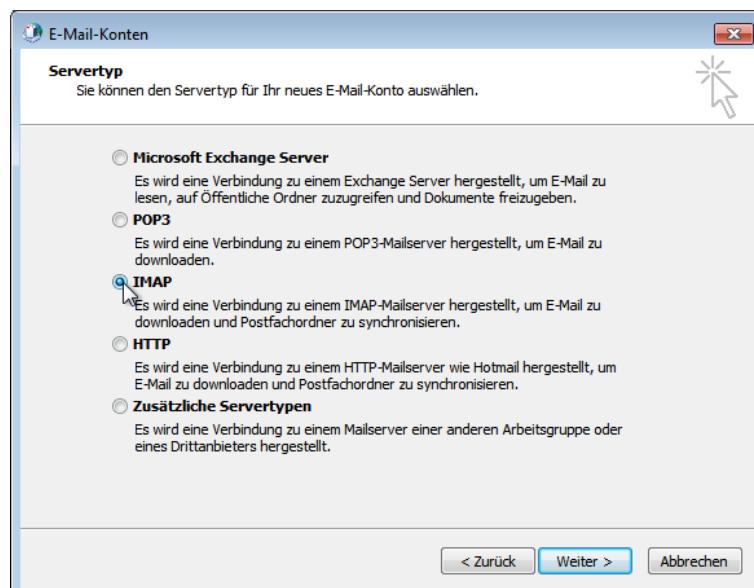
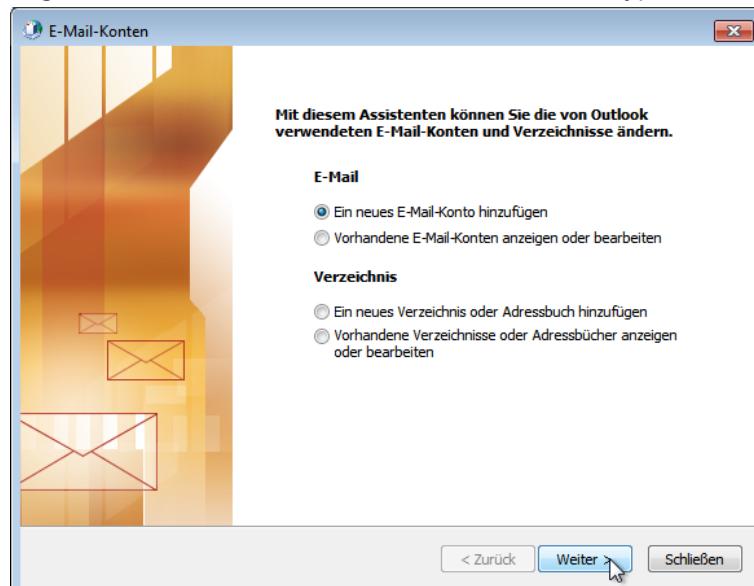


4. Fügen Sie ein neues Profil hinzu und vergeben einen Namen





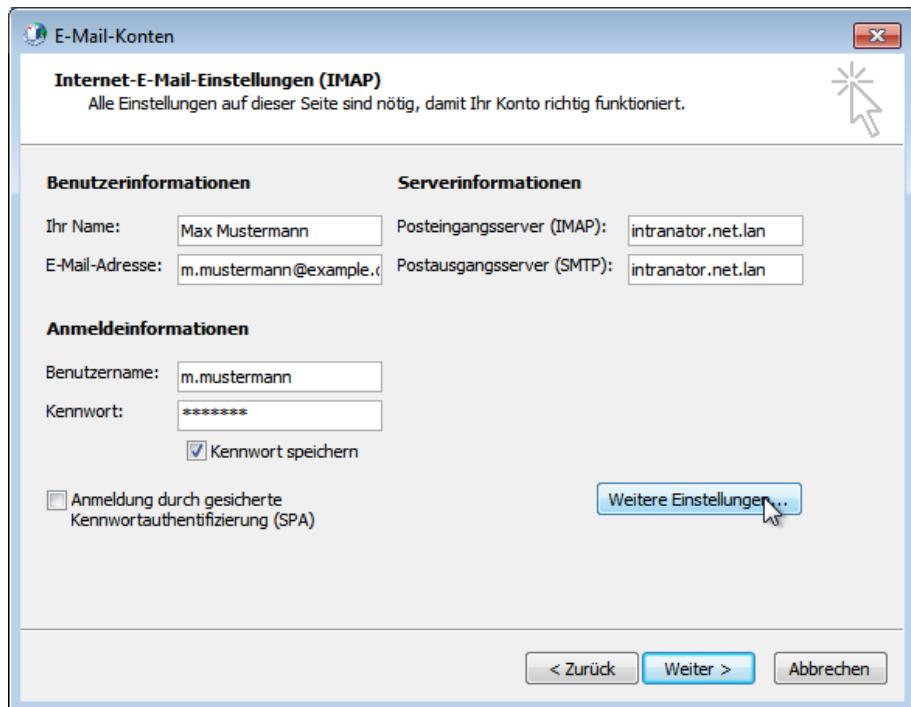
5. Fügen Sie ein neues E-Mail-Konto mit dem Servertyp IMAP hinzu.



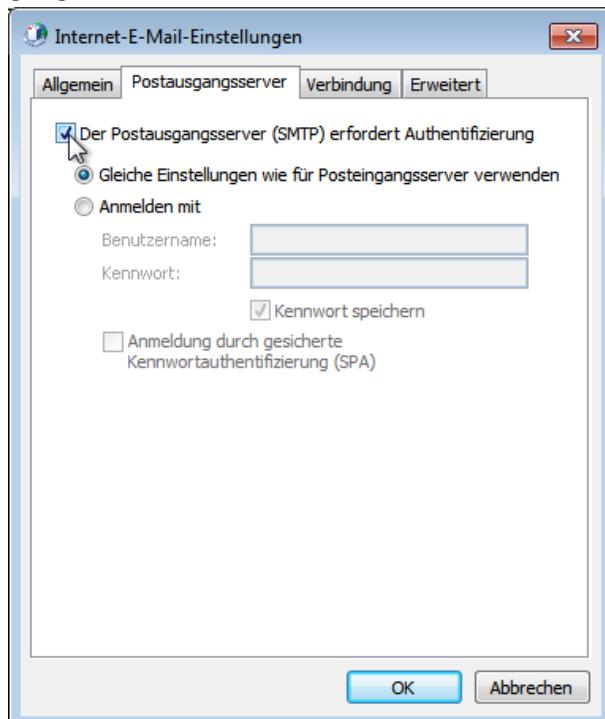
6. Tragen Sie die Benutzer- und Serverdaten ein.

Verwenden Sie als Postein- und -ausgangsserver Ihren Intranator Server. Verwenden Sie unbedingt den vollständigen DNS-Namen inkl. Domain Ihres Intranator Servers, tragen Sie keine IP-Adressen ein.

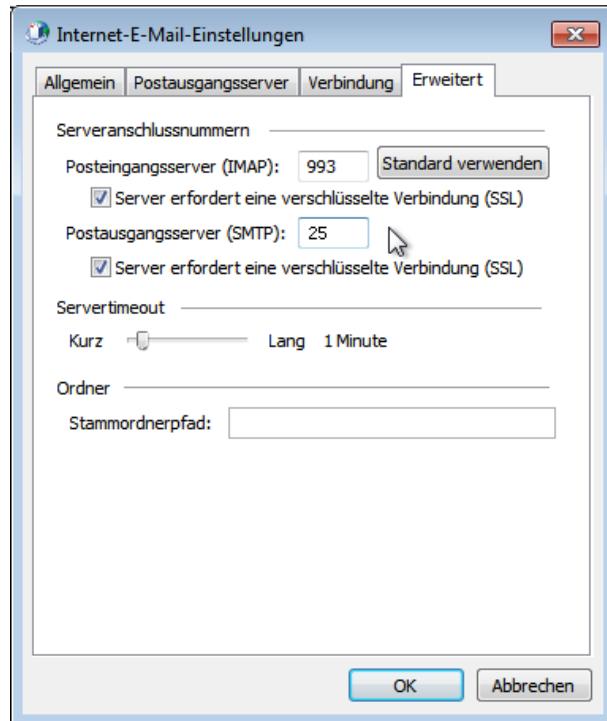
Soll der Client auch von außerhalb des lokalen Netzes zugreifen können, so verwenden Sie den externen DNS-Namen des Intranator Servers. Verwenden Sie auch hier keine IP-Adresse, sondern registrieren gegebenenfalls für Ihren Intranator Server einen DNS-Namen bei Ihrem Domainprovider oder DynDNS-Anbieter.



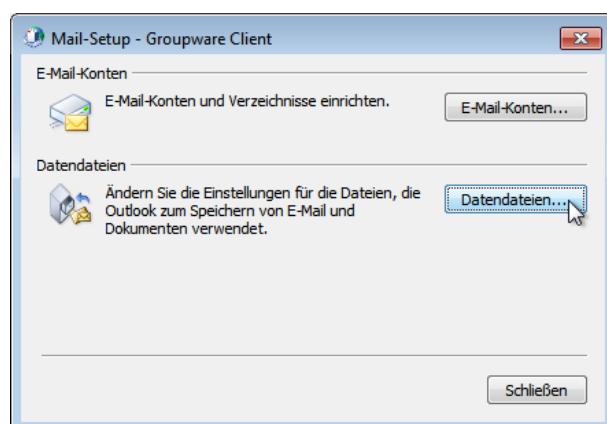
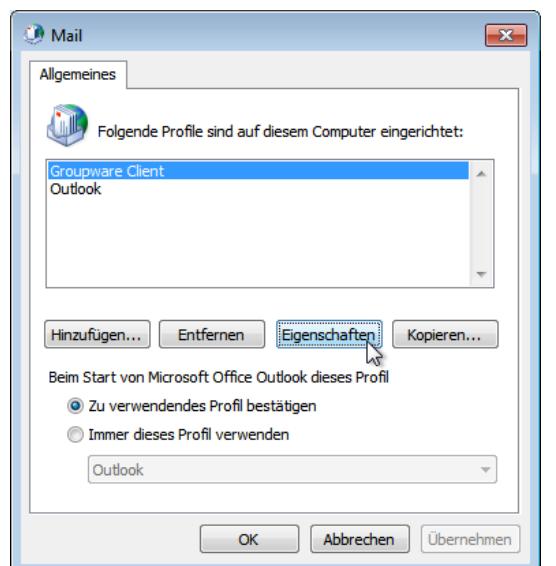
7. Öffnen Sie die Weiteren Einstellungen und den Reiter Postausgangsserver. Aktivieren Sie die SMTP-Authentifizierung mit den gleichen Einstellungen wie für den Posteingangsserver.



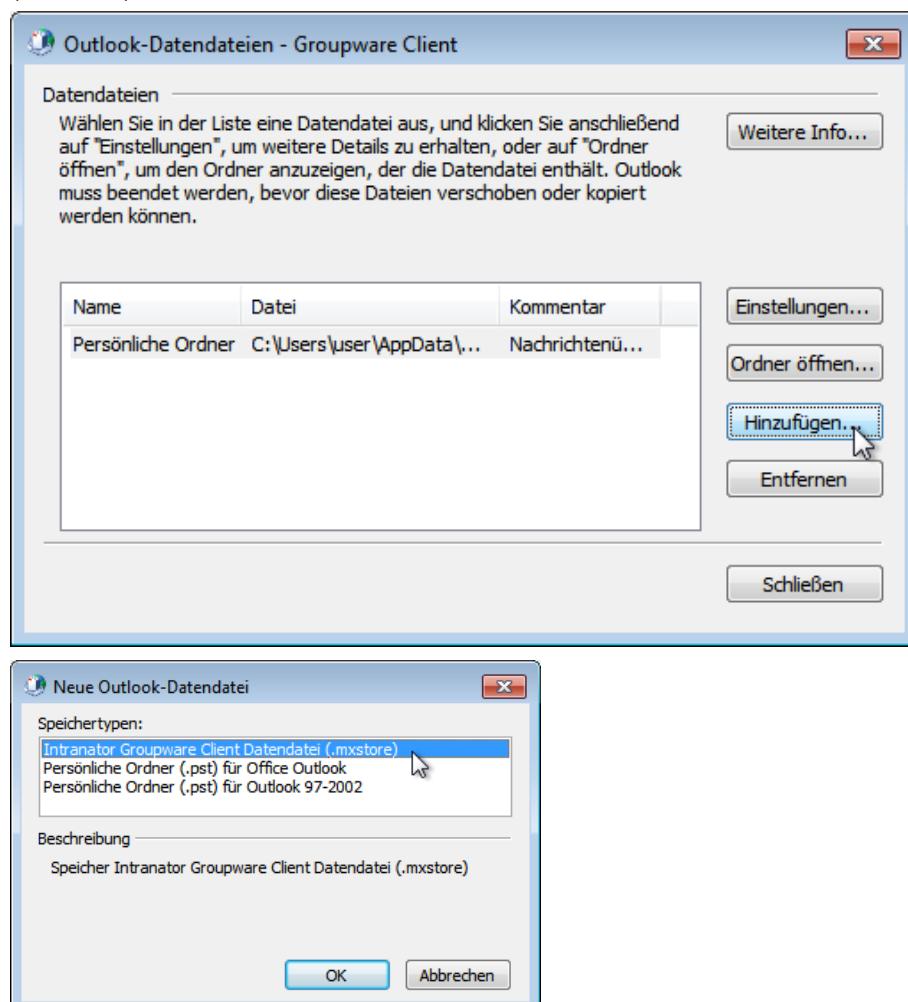
8. Öffnen Sie den Reiter Erweitert. Aktivieren Sie die Verschlüsselung der Verbindung per SSL für IMAP und SMTP. Schließen Sie die E-Mail-Einstellungen.



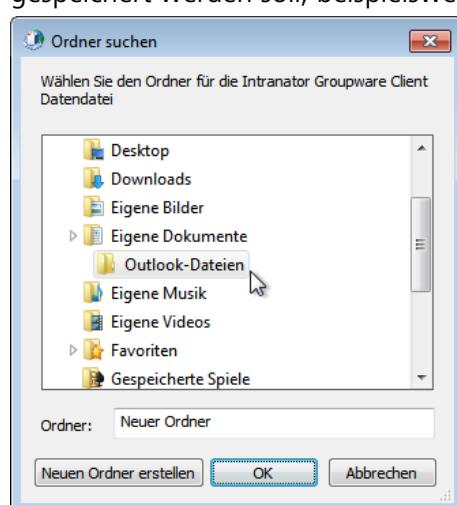
- Beenden Sie die Kontokonfiguration und öffnen Sie die Eigenschaften des neuen Profils. Wählen Sie Bearbeiten der Datadateien.



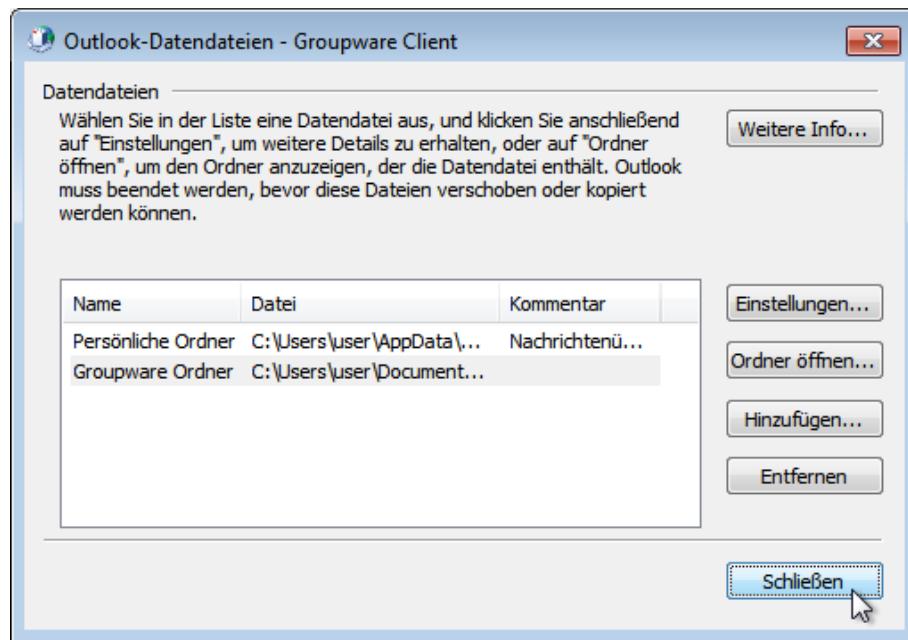
10. Fügen Sie eine neue Datendatei vom Typ Intranator Groupware Client Datendatei (.mxstore) hinzu.



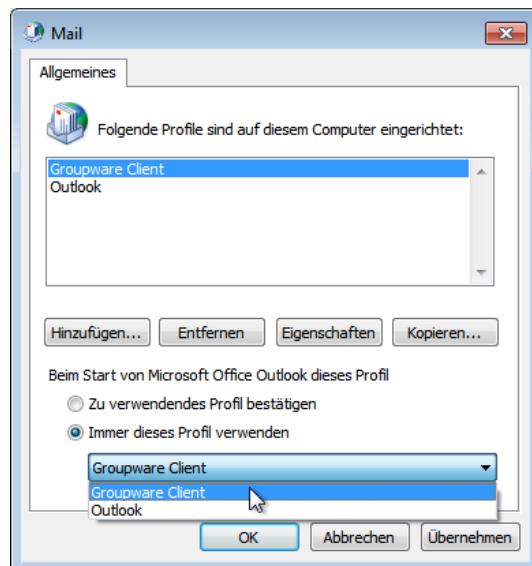
11. Wählen Sie einen Ordner in dem die Datendatei des Intra2net Groupware Clients gespeichert werden soll, beispielsweise Eigene Dokumente\Outlook-Dateien.



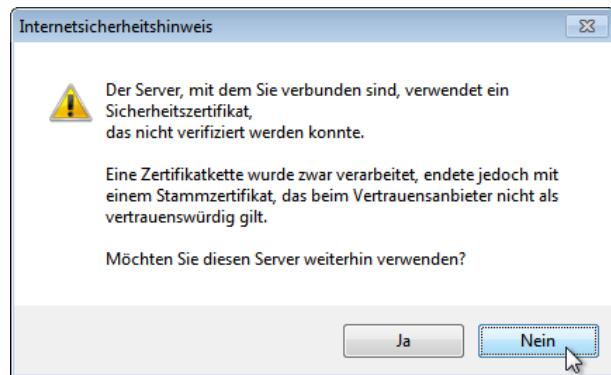
12. Schließen Sie den Dialog.



13. Wenn Sie möchten, können Sie Outlook automatisch beim Start das eben erstellte Profil öffnen lassen.



14. Starten Sie Outlook mit dem eben neu erstellten Profil.
15. Wird Ihnen ein Internetsicherheitshinweis angezeigt, so ist die Zertifikatskonfiguration nicht korrekt. Klicken Sie dann auf Nein und beenden Outlook. Prüfen Sie dann die Zertifikatskonfiguration wie in 10. Kapitel, „SSL-Verschlüsselung und Zertifikate“ beschrieben und starten Outlook neu. Fahren Sie erst fort, wenn keine Internetsicherheitswarnungen mehr angezeigt werden.



16. Es öffnet sich automatisch der Dialog Server-Konten des Intra2net Groupware Clients.
17. Fahren Sie mit der Einrichtung im 20. Kapitel, „Konten konfigurieren“ fort.

20. Kapitel - Konten konfigurieren

Das Outlook-Profil enthält nun 2 Datendateien:

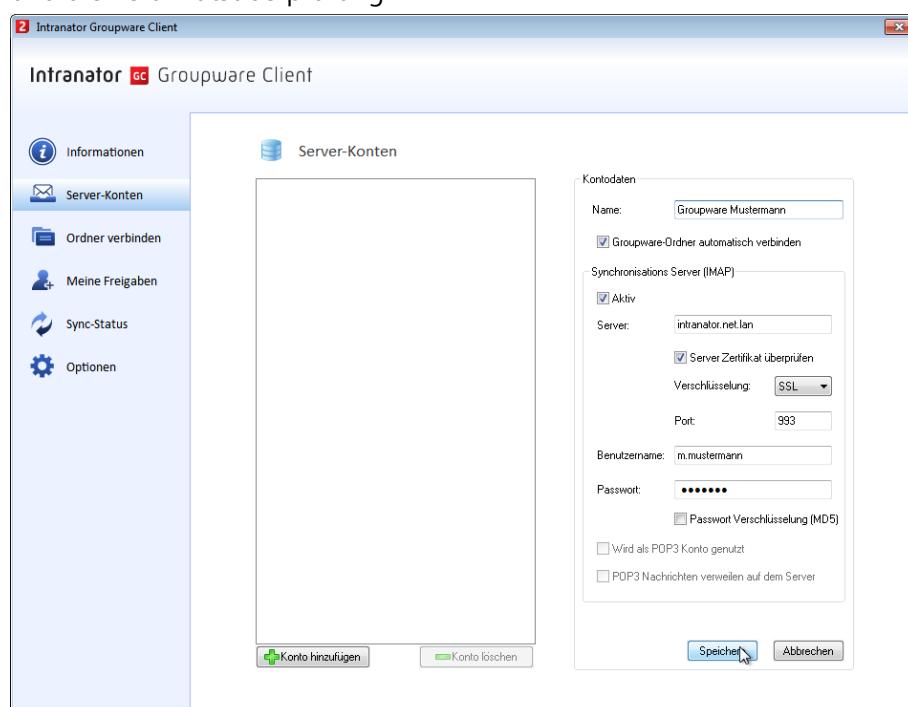
- Ein vom Intra2net Groupware Client verwaltetes Groupware-Konto für Groupware-Objekte wie Kontakte, Termine, Aufgaben und Notizen. Dies ist die Standarddatendatei und mit Groupware Ordner benannt.
- Ein direkt von Outlook verwaltetes IMAP-Konto für die Synchronisation und Versand von E-Mails. Dies ist normalerweise mit der E-Mail-Adresse benannt.

Wir empfehlen diese Aufteilung in 2 Konten, da der Zugriff auf E-Mails über IMAP schneller und effizienter ist als über den Groupware Client. Generell wäre es aber auch möglich, E-Mails und Groupware-Objekte gemeinsam über den Intra2net Groupware Client zu verwalten.

20.1. Groupware-Konto

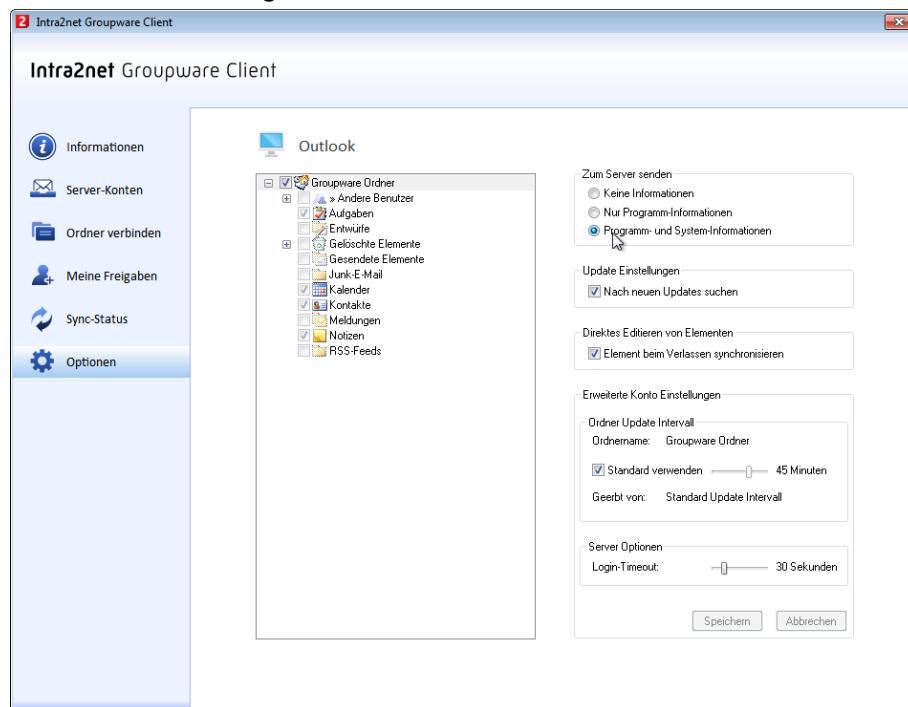
Zuerst werden dem Intra2net Groupware Client die Zugangsdaten bekannt gemacht.

1. Starten Sie Microsoft Outlook und öffnen das Profil mit dem Intra2net Groupware Client.
2. Ist für die Groupware noch kein Konto konfiguriert, öffnet sich automatisch der entsprechende Dialog.
3. Tragen Sie die Kontodaten ein. Verwenden Sie als Server den vollständigen DNS-Namen Ihres Intranator Servers inkl. Domain. Aktivieren Sie die SSL-Verschlüsselung und die Zertifikatsüberprüfung.



4. Klicken Sie auf Speichern, um die Kontodaten zu speichern. Das Konto wird nun in der Kontenliste aufgeführt.

5. Wechseln Sie auf den Reiter Optionen und lassen Programm- und System-Informationen zum Server senden. Dadurch werden beim Login Informationen über die Hard- und Software des lokalen Rechners an den Server übermittelt. Diese können dann unter anderem zur zentralen Planung und Überwachung von Updates des Groupware Clients und Outlook genutzt werden.



Alle Groupware-Ordner (nicht aber die E-Mail-Ordner) auf dem Server werden automatisch mit den entsprechenden Ordnern in Outlook verbunden. Später neu angelegte Ordner werden auch automatisch verbunden.

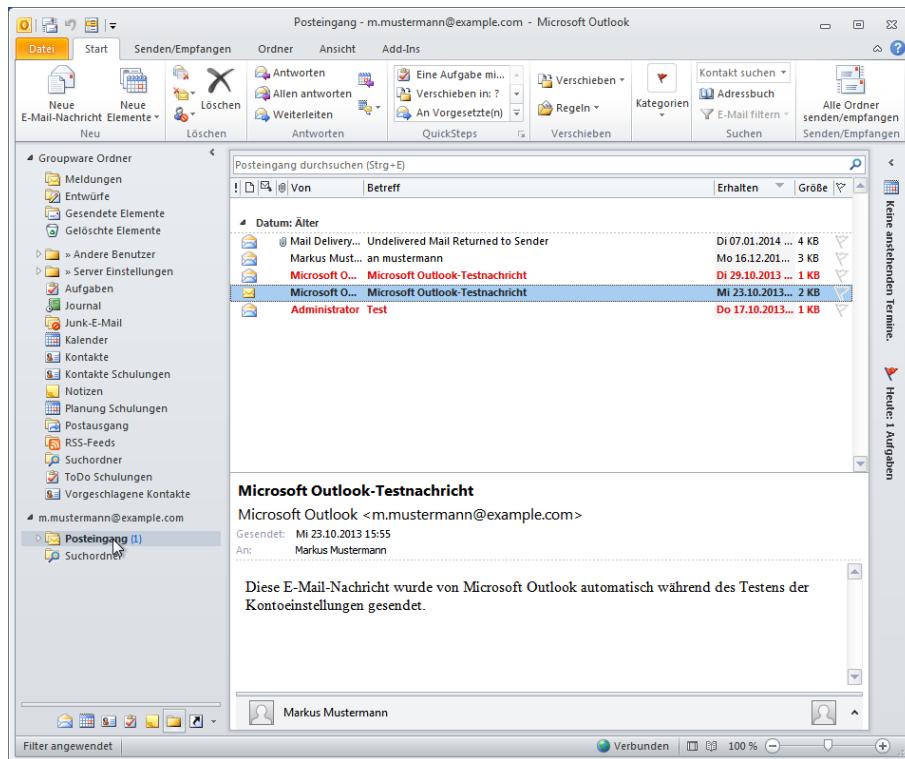
Der Intra2net Groupware Client gibt dem Benutzer im Ordner Meldungen Hinweise zu Problemen, neu verfügbaren Freigaben, installierten Updates etc.

20.2. IMAP E-Mail-Konto

20.2.1. Ansicht

In der Ordnerliste von Outlook auf der linken Seite werden diese beiden Konten angezeigt. Das E-Mail-Konto ist dabei standardmäßig mit der E-Mail-Adresse benannt.

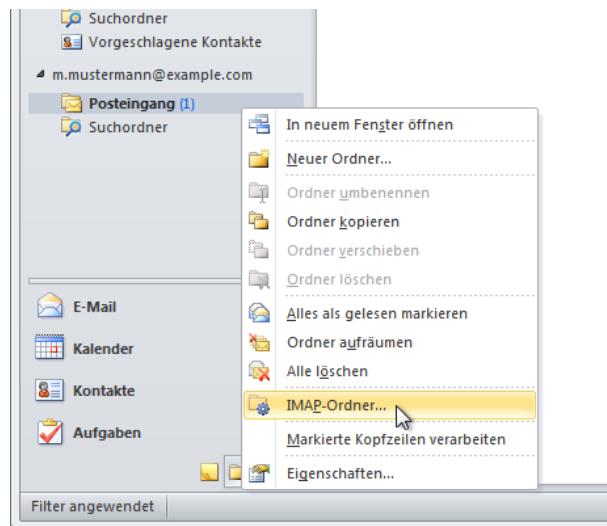
Neu eingehende E-Mails erscheinen im Ordner Posteingang dieses Kontos.



20.2.2. Abonnieren von Ordner

Outlook zeigt nicht alle in dem Konto verfügbaren Ordner an, sondern nur die abonnierten. Wollen Sie weitere Ordner nutzen, müssen Sie diese zuerst abonnieren. Gehen Sie dazu wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf den Posteingang in der Ordnerliste. Es öffnet sich ein Kontextmenü. Wählen Sie dort IMAP-Ordner...



2. Klicken Sie auf Abfrage um eine Liste aller verfügbaren Ordner vom Server abzurufen.



3. Es werden alle verfügbaren eigenen Ordner, sowie die von anderen Benutzern für Sie freigegebenen Ordner, angezeigt. Es werden sowohl Ordner mit E-Mails, als auch Ordner mit Groupware-Objekten angezeigt. Achten Sie darauf, in dieser Maske nur Ordner zu abonnieren, die tatsächlich E-Mails enthalten.

Markieren Sie alle gewünschten Ordner und klicken auf Abonnieren.

Um Ordner mit Groupware-Inhalten zu abonnieren siehe Abschnitt 21.2, „Fremde Ordner verbinden“ bzw. Abschnitt 22.2, „Ordner manuell verbinden“ (Eigene Ordner).

20.2.3. Ordner für Gesendete Elemente

In der Standardkonfiguration werden gesendete E-Mails und Einladungen nicht auf dem Server, sondern nur lokal gespeichert. Sie können daher nicht von anderen Geräten aus genutzt oder mit Kollegen geteilt werden. Außerdem sind sie nicht im Backup enthalten.

Gehen Sie wie folgt vor, um die E-Mails auf dem Server zu speichern und diese Nachteile zu beheben:

20.2.3.1. Outlook 2013

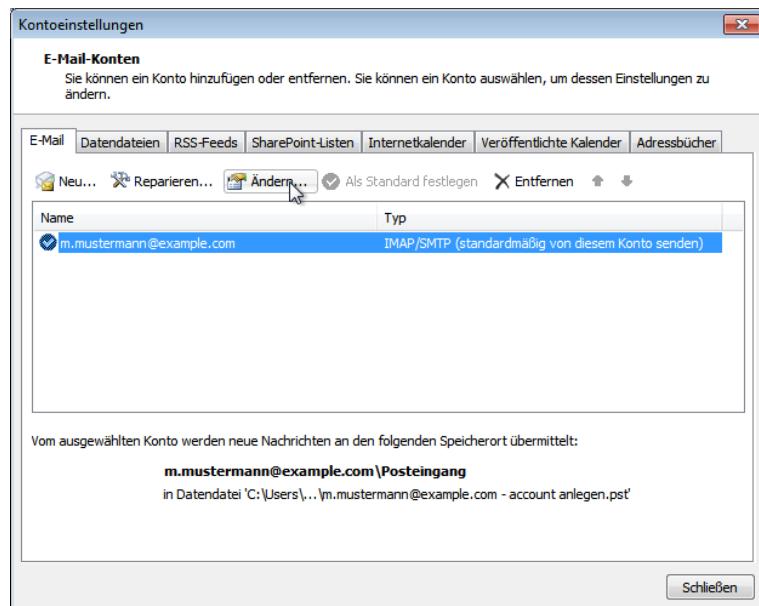
In Outlook 2013 können die Ordner für gesendete E-Mails, gelöschte E-Mails und Entwürfe nicht manuell eingestellt werden, sondern müssen vom IMAP-Server übermittelt werden (XLIST-Erweiterung). Die übermittelten Ordnernamen werden aber nur beim ersten Einrichten des Kontos in Outlook ausgelesen, spätere Änderungen auf dem Server werden von Outlook nicht nachvollzogen. Daher müssen die Ordner bereits vor dem Einrichten von Outlook auf dem Server richtig konfiguriert sein.

Auf dem Intranator Server können die per XLIST übermittelten Ordner im Menü Benutzermanager > Benutzer : Groupware konfiguriert werden.

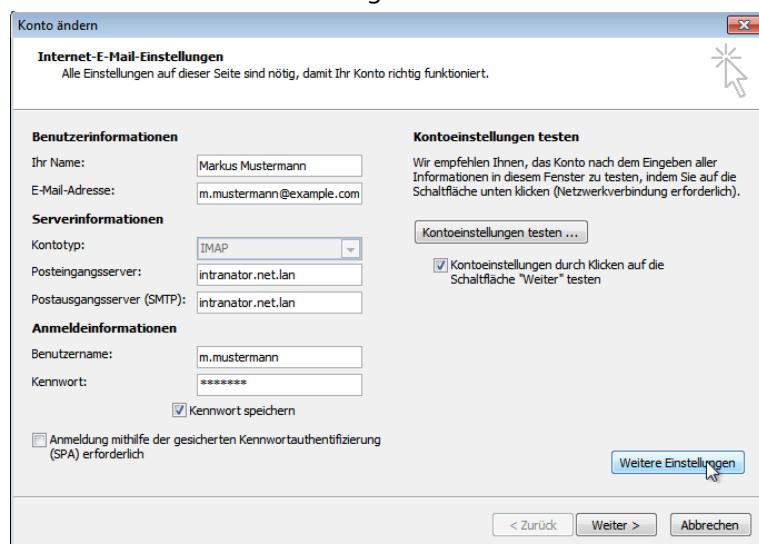
Sollen Änderungen auf dem Server in einem bereits bestehenden Outlook-Konto wirksam werden, so entfernen Sie das Konto über die Outlook-Kontensteuerung und fügen es danach neu hinzu. Sie müssen dabei nur das Outlook-IMAP-Konto entfernen, die Datendatei des Groupware Clients oder weitere Konten können bestehen bleiben.

20.2.3.2. Outlook 2010 und Outlook 2007

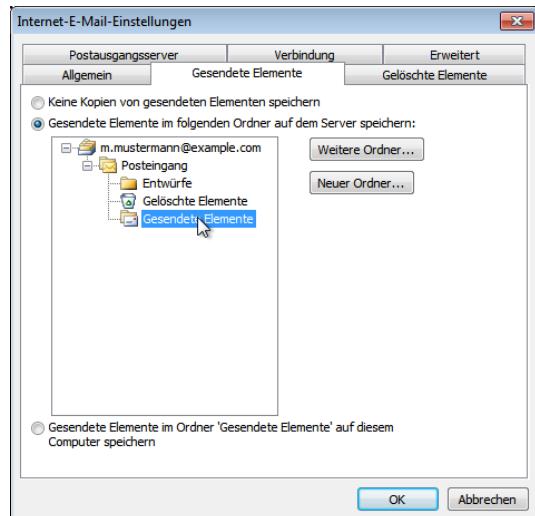
1. Öffnen Sie das Menü Datei > Kontoeinstellungen, bzw. Extras > Kontoeinstellungen in Outlook 2007. Wählen Sie das IMAP-Konto aus und klicken auf Ändern.



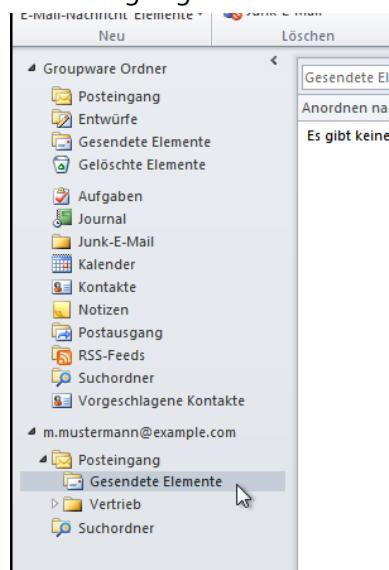
2. Öffnen Sie Weitere Einstellungen.



3. Wechseln Sie auf den Reiter Gesendete Elemente.
4. Lassen Sie die gesendeten Elemente in einem Ordner auf dem Server speichern und markieren den Ordner Gesendete Elemente unterhalb des Posteingangs.



5. Bestätigen Sie die Änderungen mit OK und schließen den Assistenten zur Kontoänderung ab. Alle gesendeten E-Mails und Einladungen werden von nun an auf dem Server abgelegt.

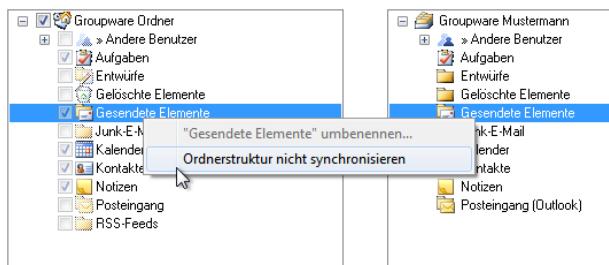


20.2.3.3. Outlook 2003

Die in Outlook 2003 integrierte IMAP-Funktionalität ermöglicht nicht, die gesendeten E-Mails auf dem Server abzulegen. Diese Funktion übernimmt daher der Intra2net Groupware Client.

Gehen Sie wie folgt vor um dies zu konfigurieren:

1. Öffnen Sie das Menü Groupware Client > Ordner verbinden.
2. Klicken Sie mit der rechten Maustaste auf den Ordner **Gesendete Objekte**. Es öffnet sich das Kontextmenü.
3. Deaktivieren Sie die Option **Ordnerstruktur nicht synchronisieren**.



20.2.4. Behandlung von gelöschten E-Mails

Das IMAP-Protokoll sieht beim Löschen von E-Mails vor, dass sie mit einer speziellen Löschmarkierung in ihrem bisherigen Ordner verbleiben. Die so markierten E-Mails werden dann mit einem speziellen Befehl endgültig gelöscht.

Dies unterscheidet sich von der in Outlook üblichen Vorgehensweise, die gelöschten Elemente in einen speziellen Ordner zu verschieben und sie dort nach einiger Zeit endgültig zu löschen.

Im Folgenden wird beschrieben, wie die einzelnen Outlook-Versionen mit diesem Unterschied umgehen und was es für Anpassungsmöglichkeiten für die Benutzer gibt.

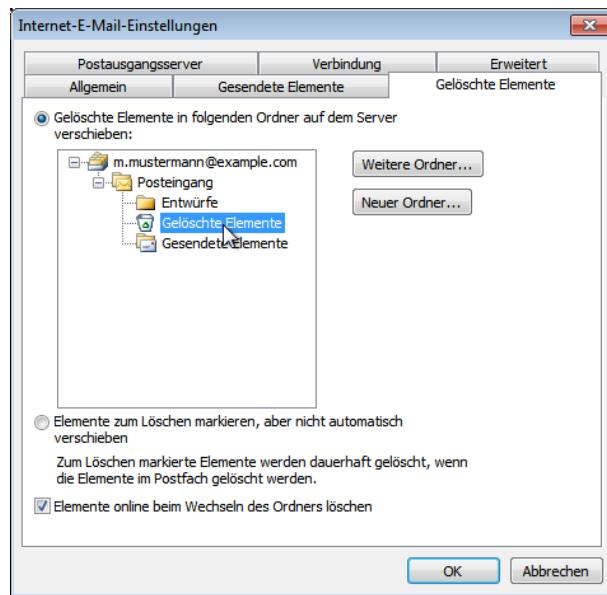
20.2.4.1. Outlook 2013

In Outlook 2013 werden gelöschte E-Mails auf dem Server sofort gelöscht und in Outlook lokal im Ordner "Gelöschte Elemente (Nur dieser Computer)" abgelegt.

Abhängig von der Einstellung Beim Beenden von Outlook die Ordner "Gelöschte Elemente" leeren im Menü Datei > Optionen > Erweitert wird dieser Ordner endgültig aufgeräumt.

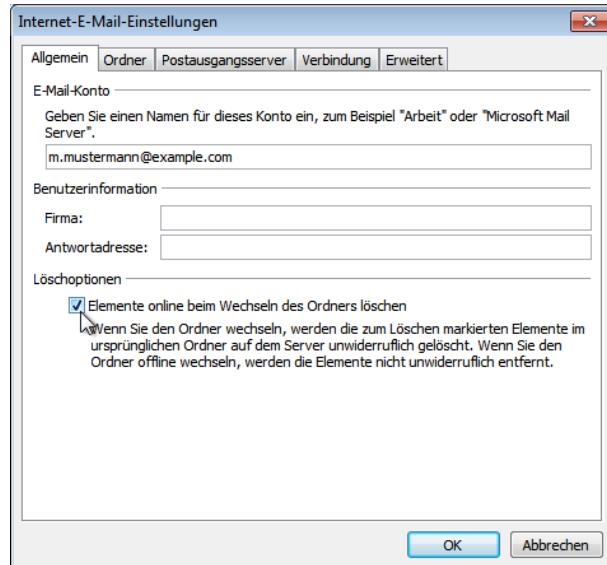
20.2.4.2. Outlook 2010

1. Öffnen Sie das Menü Datei > Kontoeinstellungen. Wählen Sie das IMAP-Konto aus und klicken auf Ändern.
2. Öffnen Sie Weitere Einstellungen und den Reiter Gelöschte Elemente.
3. Sie haben jetzt die Möglichkeit, die gelöschten E-Mails beim Verlassen eines Ordners endgültig löschen zu lassen, oder die E-Mails beim Löschen in einen speziellen Order zu verschieben.



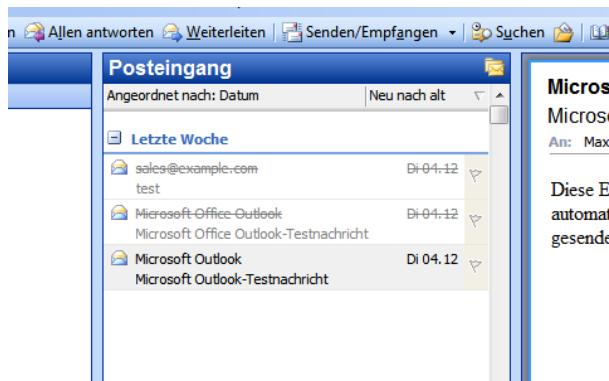
20.2.4.3. Outlook 2007

1. Öffnen Sie das Menü Extras > Kontoeinstellungen. Wählen Sie das IMAP-Konto aus und klicken auf Ändern.
2. Öffnen Sie Weitere Einstellungen und den Reiter Allgemein.
3. Sie haben jetzt die Möglichkeit, die gelöschten E-Mails automatisch beim Verlassen eines Ordners endgültig löschen zu lassen.

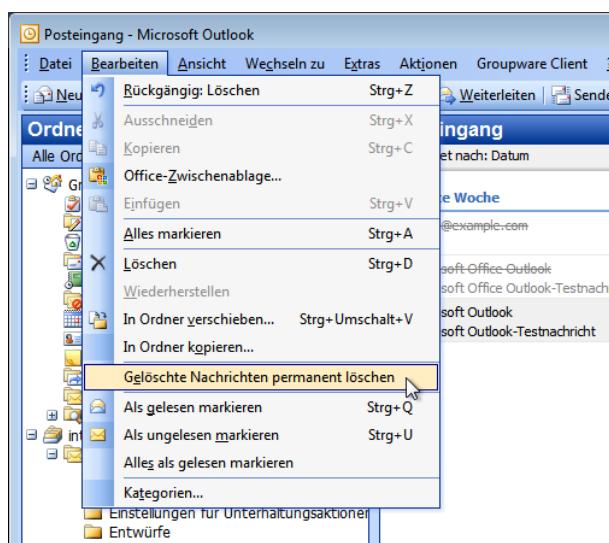


20.2.4.4. Outlook 2003

Gelöschte E-Mails werden nach dem Löschen durchgestrichen dargestellt.



Um Sie endgültig zu Löschen verwenden Sie das Menü Bearbeiten > Gelöschte Nachrichten permanent löschen. Das endgültige Löschen ist nur für den aktuell geöffneten Ordner wirksam.



20.3. Bestehende Daten übernehmen

Verwenden Sie bisher Outlook mit einem anderen Profil und möchten die dortigen Daten jetzt mit dem Intra2net Groupware Client nutzen, gehen Sie wie im Folgenden beschrieben vor.

20.3.1. Vorbereiten der Datendatei

Voraussetzung für die Übernahme von Daten ist eine Outlook-Datendatei (.pst) die alle Daten enthält. Outlook legt die Datendateien eines Profils in einem von der Outlook-Version abhängigen Verzeichnis ab. Sie finden den Pfad zur Outlook-Datendatei wie im Folgenden beschrieben heraus:

1. Öffnen Sie die Windows-Systemsteuerung, Menüpunkt E-Mail Setup (32-Bit).
2. Öffnen Sie den Profil-Editor.
3. Wählen Sie das bisherige Profil und lassen Sie sich die Eigenschaften und dort die Datendateien anzeigen.
4. Lassen Sie sich den Dateispeicherort der Datendatei anzeigen und notieren sich den vollständigen Pfad dieser Datendatei.

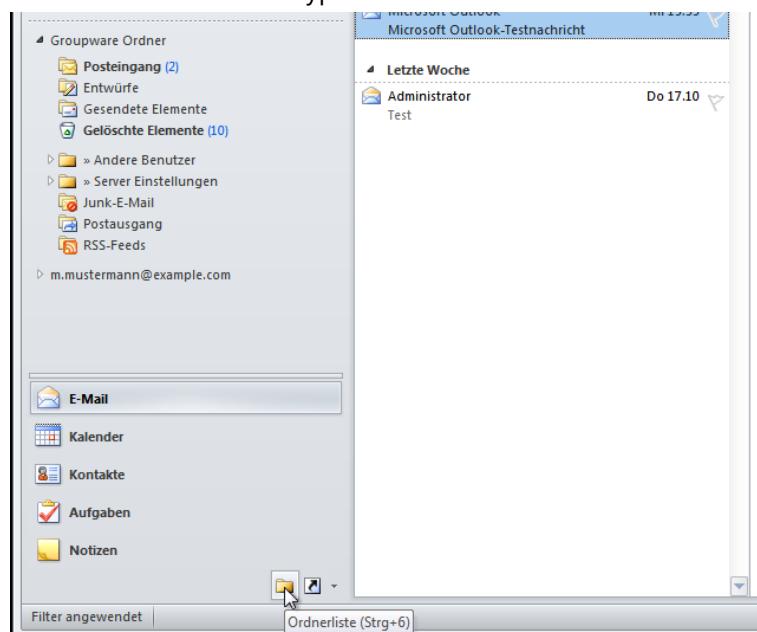
5. Legen Sie mit einem Dateimanager eine Sicherheitskopie dieser Datendatei an.

Verwenden Sie zum Übernehmen der Daten unbedingt eine lokale .pst-Datei. Versuchen Sie nicht das bisherige Groupwaresystem und den Groupware Client gleichzeitig in einem Profil einzusetzen, da dies zu Störungen führen kann.

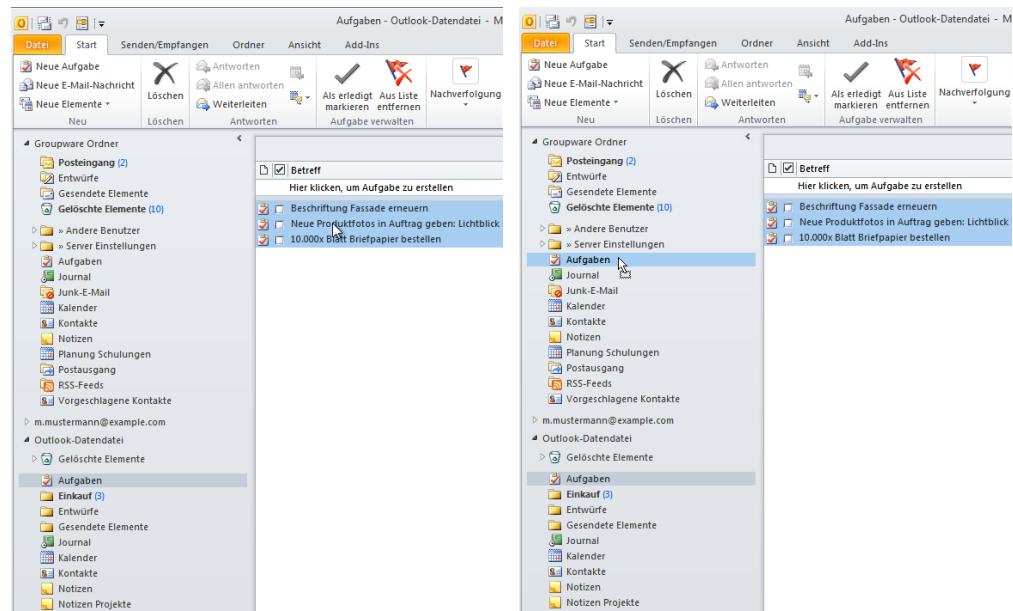
20.3.2. Übernehmen der Groupwaredaten

Gehen Sie nun wie folgt vor um die Groupwaredaten durch Kopieren zu übernehmen:

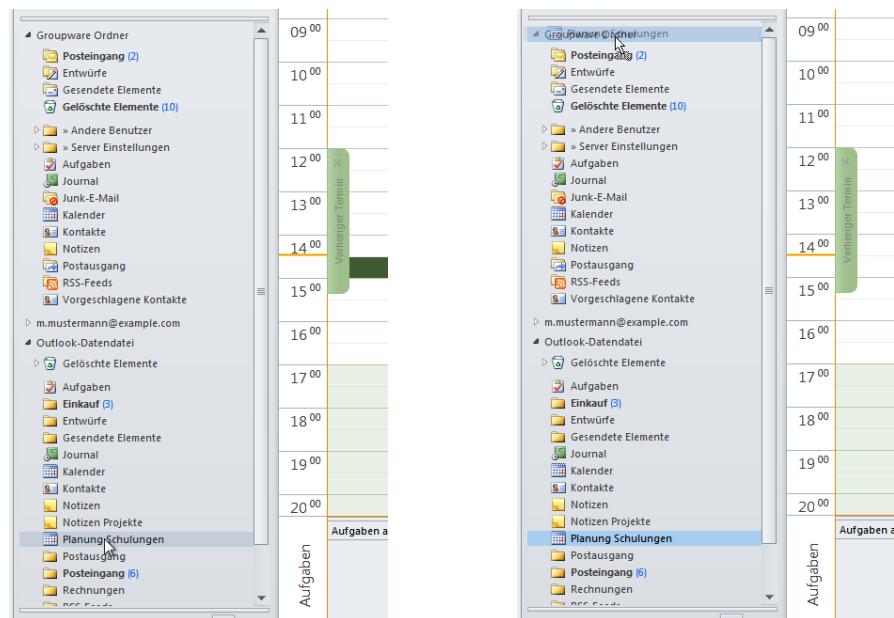
1. Prüfen Sie, dass Ihre eben erstellte Sicherheitskopie der Outlook-Datendatei wirklich vollständig ist.
2. Starten Sie Outlook mit dem Profil des Groupware Clients.
3. Öffnen Sie das Menü Datei > Öffnen > Outlook-Datendatei öffnen (ab Outlook 2010), bzw. Datei > Öffnen > Outlook-Datendatei (frühere Versionen).
4. Wählen Sie die Datendatei mit den zu übernehmenden Daten aus.
5. Machen Sie alle Ordnerarten sichtbar in dem Sie auf die Ordnerliste umschalten.

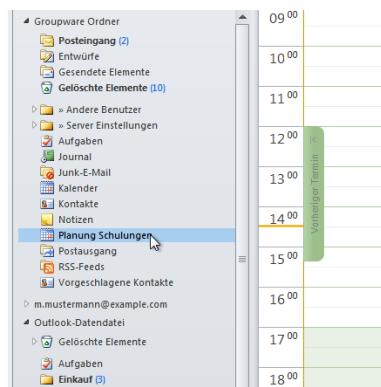


6. Öffnen Sie den ersten Standard-Groupwareordner (z.B. Aufgaben) in der eben geöffneten Datendatei.
7. Markieren Sie alle Elemente und verschieben sie per Drag & Drop in den entsprechenden Ordner des Groupware Clients (unterhalb von Groupware Ordner). Um alle Kalendereinträge markieren zu können, verwenden Sie die Listenansicht (Menü Ansicht > Ansicht ändern > Liste).



8. Wiederholen Sie die letzten beiden Schritte für alle Standard-Groupwareordner (Aufgaben, Kalender, Kontakte und Notizen).
9. Verschieben Sie alle nicht-Standard-Groupwareordner, nicht aber die E-Mail-Ordner, Ordner für Ordner per Drag & Drop in den Groupware Client (unter Groupware Ordner).





20.3.3. Übernehmen der E-Mails

Prüfen Sie zuerst, ob Sie die E-Mails aus der Outlook-Datendatei wirklich noch übernehmen müssen, oder ob sie bereits auf dem Intranator Server liegen. Letzteres ist z.B. der Fall wenn der Intranator Server bisher bereits als reiner E-Mail-Server ohne Groupware verwendet wurde, oder wenn die E-Mails bereits per IMAP vom bisherigen E-Mail-Server kopiert wurden.

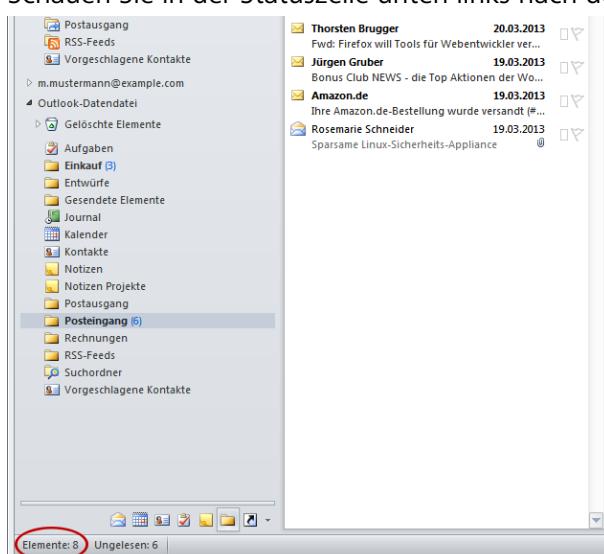
Für letzteres kann z.B. das Programm IMAPCopy
[<http://home.arcor.de/armin.diehl/imapcopy/imapcopy.html>] eingesetzt werden.



Liegen die E-Mails bereits auf dem Intranator Server, sollten Sie im von Outlook verwalteten IMAP-Konto (typischerweise mit der E-Mail-Adresse benannt) zu sehen sein. Es ist möglich, dass Unterordner erst abonniert werden müssen bevor sie sichtbar werden. Die dazu nötigen Schritte sind in Abschnitt 20.2.2, „Abonnieren von Ordnern“ beschrieben.

Ist ein Übernehmen der E-Mails nötig, gehen Sie dafür wie folgt vor:

1. Öffnen Sie den Posteingang der zu importierenden Datendatei
2. Schauen Sie in der Statuszeile unten links nach der Anzahl der E-Mails.



- a. Wenn es sich um weniger als 1000 Elemente handelt, können Sie alle E-Mails markieren und per Drag & Drop in den Posteingang des von Outlook verwalteten IMAP-Kontos (typischerweise mit der E-Mail-Adresse benannt) verschieben.
- b. Wenn es sich um mehr als 1000 Elemente handelt, markieren Sie die ersten ca. 1000 E-Mails. Sie können die markierte Anzahl anhand der Größe des Scrollbalkens rechts und der Gesamtanzahl abschätzen. Verschieben Sie diese 1000 E-Mails dann per Drag & Drop in den Posteingang des von Outlook verwalteten IMAP-Kontos (typischerweise mit der E-Mail-Adresse benannt). Wiederholen Sie dies immer in Blöcken von ca. 1000 für die restlichen E-Mails.

Wenn Sie versuchen zu viele E-Mails auf einmal in ein IMAP-Konto zu verschieben, wird Outlook erfahrungsgemäß instabil und kann abstürzen. Daher ist ein blockweises Verschieben notwendig.

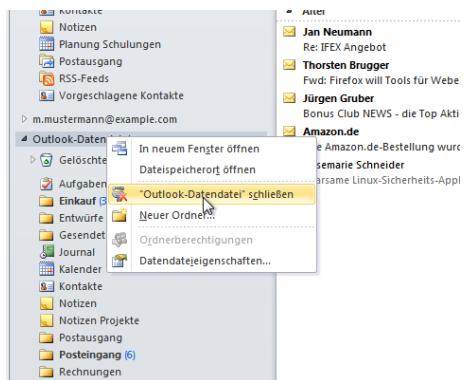
3. Öffnen Sie den nächsten E-Mail-Ordner der zu importierenden Datendatei.
4. Schauen Sie in der Statuszeile unten links nach der Anzahl der E-Mails. Prüfen Sie ob der Ordner weitere Unterordner enthält. Wenn ja, dann addieren sich die Zahlen der E-Mails aller Unterordner.
 - a. Wenn es sich um weniger als 1000 Elemente handelt, können Sie den gesamten Ordner per Drag & Drop in das von Outlook verwaltete IMAP-Konto (typischerweise mit der E-Mail-Adresse benannt) verschieben.
 - b. Wenn es sich um mehr als 1000 Elemente handelt, legen Sie zuerst den entsprechenden Ordner im von Outlook verwalteten IMAP-Konto an. Markieren Sie dann die ersten ca. 1000 E-Mails. Sie können die markierte Anzahl anhand der Größe des Scrollbalkens rechts und der Gesamtanzahl abschätzen. Verschieben Sie diese 1000 E-Mails dann per Drag & Drop in den entsprechenden Ordner des von Outlook verwalteten IMAP-Kontos (typischerweise mit der E-Mail-Adresse benannt). Wiederholen Sie dies immer in Blöcken von ca. 1000 für die restlichen E-Mails.

Wenn Sie versuchen zu viele E-Mails oder zu komplexe Ordnerstrukturen auf einmal in ein IMAP-Konto zu verschieben, wird Outlook erfahrungsgemäß instabil und kann abstürzen. Daher ist ein blockweises Verschieben notwendig.

20.3.4. Datendatei schließen

Nachdem die Daten erfolgreich von der bisherigen Datendatei übernommen wurden, sollte sie wieder aus dem Profil entfernt werden um den Benutzer nicht zu verwirren.

Klicken Sie dazu mit der rechten Maustaste auf den Wurzelordner der Datendatei und wählen Outlook-Datendatei schließen.

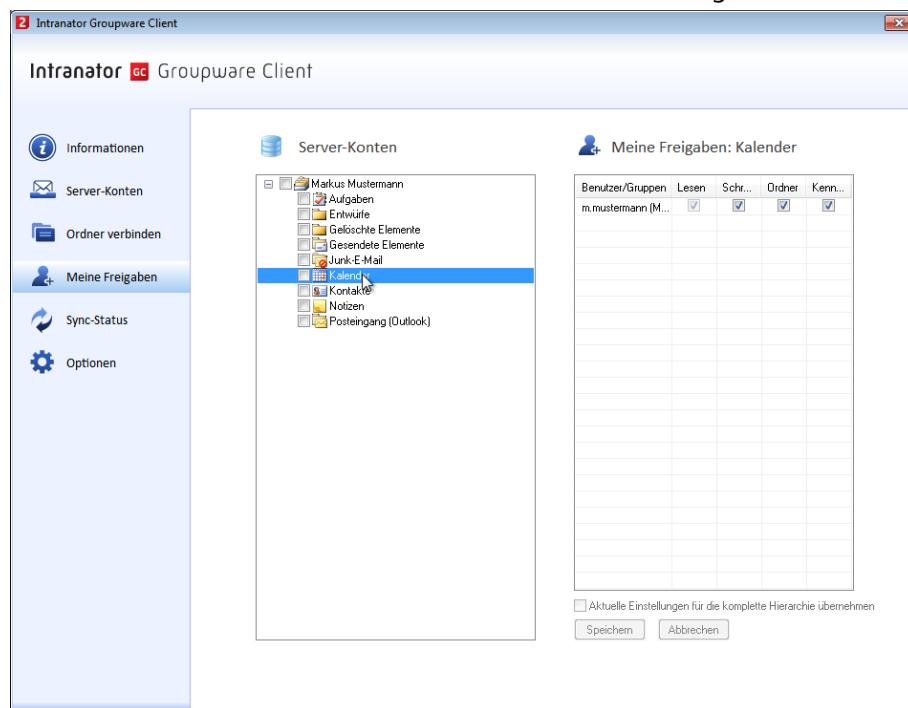


21. Kapitel - Freigaben und Zugriff auf fremde Ordner

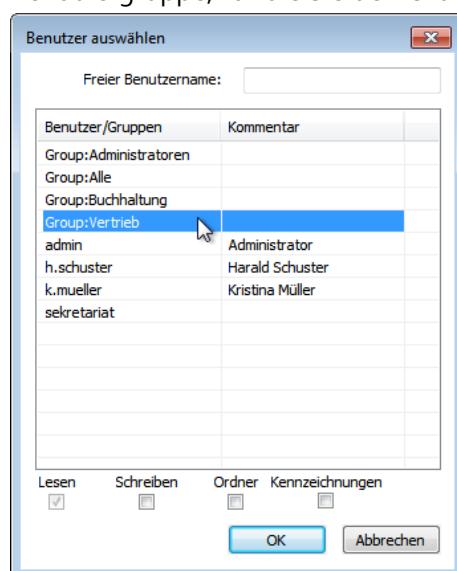
21.1. Eigene Ordner freigeben

Damit andere Benutzer auf einen Ordner zugreifen können, muss der Eigentümer ihn zuerst wie folgt freigeben:

1. Öffnen Sie das Menü Groupware Client > Meine Freigaben.
2. Klicken Sie auf der linken Seite (Server-Konten) den freizugebenden Ordner an.



3. Machen Sie einen Doppelklick auf der rechten Seite (Meine Freigaben). Es erscheint der Dialog für eine neue Freigabe. Markieren Sie den Benutzernamen oder die Benutzergruppe, für die Sie den Ordner freigeben möchten.



4. Wählen Sie mit den Checkboxen am unteren Rand des Dialogs die Rechte, die Sie dem anderen Benutzer erteilen möchten.
5. Klicken Sie auf Speichern, um die neuen Rechte auf den Server zu schreiben.

Es empfiehlt sich, die Freigaben nicht für einzelne Benutzer, sondern für Benutzergruppen auf dem Intranator Server zu erteilen. Dies vereinfacht die Verwaltung der Freigaben vor allem bei Benutzerfluktuation und Umstrukturierung.

Die einzelnen Rechte haben folgende Bedeutung:

Lesen	Der Benutzer kann den Ordner und all seine Inhalte sehen.
Schreiben	Der Benutzer darf neue Einträge in diesem Ordner anlegen und bestehende ändern oder löschen.
Ordner	Der Benutzer darf den Ordner löschen und umbenennen sowie neue Unterordner unterhalb dieses Ordners anlegen. Außerdem bekommt der Benutzer Administrationsrechte auf den Ordner und darf die Freigaben an andere Benutzer verändern.
Kennzeichnungen	Der Benutzer darf die Kennzeichnungen Gelesen, Beantwortet und Nachverfolgung (ohne Datum, Flaggensymbol in Outlook) der bestehenden Inhalte ändern.

Die eingestellten Rechte gelten normalerweise nur für den markierten Ordner selbst. Über die entsprechende Option können die für den markierten Ordner eingestellten Rechte auch für alle Unterordner übernommen werden. Dabei werden nicht nur die momentan geänderten Rechte angepasst, sondern die kompletten, für den markierten Ordner gesetzten Rechte, bei allen Unterordnern übernommen.

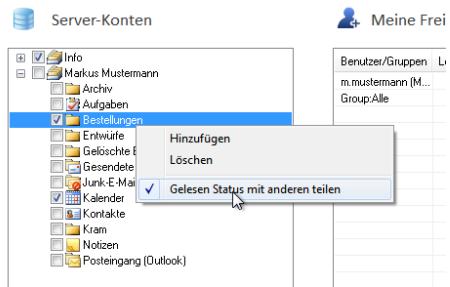
Neu angelegte Ordner übernehmen beim Anlegen immer die Rechte ihres Überordners.

21.1.1. Gelesen-Status gemeinsam/individuell

Der Intranator Server bietet die Möglichkeit, den Status "gelesen" oder "ungelesen" von neu eingegangenen E-Mails entweder für alle Nutzer gemeinsam zu verwalten, oder für jeden Nutzer mit Zugriffsrechten auf diesen Ordner individuell. Welche Variante besser geeignet ist, hängt vom Nutzungsszenario und dem Grund für die Freigabe eines E-Mail-Ordners an andere Nutzer ab. Daher können beide Varianten eingestellt werden.

Wird im Menü Groupware Client > Meine Freigaben eine neue Freigabe an andere Nutzer mit dem Recht "Kennzeichnungen" gesetzt, wird automatisch der gemeinsame Gelesen-Status aktiviert.

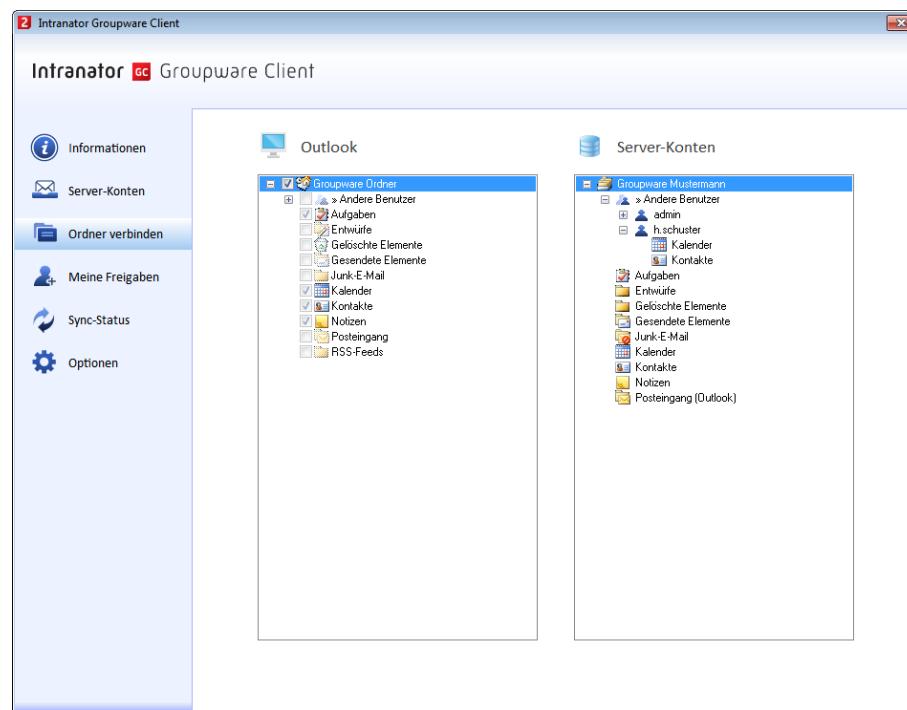
Soll der Gelesen-Status individuell pro Benutzer verwaltet werden, so öffnen Sie das Kontextmenü des Ordners über einen Rechtsklick und schalten die Option Gelesen Status mit anderen teilen aus.



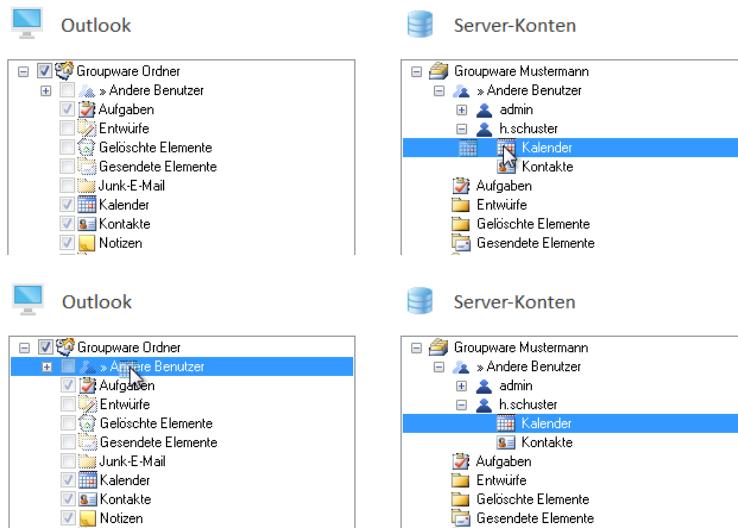
21.2. Fremde Ordner verbinden

Gehen Sie wie folgt vor, um Ordner zu verbinden, die Ihnen andere Benutzer freigegeben haben:

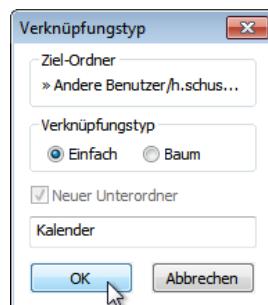
1. Klären Sie zuerst, ob es sich um einen Ordner mit E-Mails oder mit Groupware-Daten handelt. Das Abonnieren von Ordnern mit E-Mails als Inhalt ist in Abschnitt 20.2.2, „Abonnieren von Ordnern“ beschrieben. Handelt es sich um einen Ordner mit Groupware-Daten, fahren Sie hier fort.
2. Öffnen Sie das Menü Groupware Client > Ordner verbinden.
3. Auf der rechten Seite (Server-Konten) erscheinen die Ihnen freigegebenen Ordner unterhalb von »Andere Benutzer«.



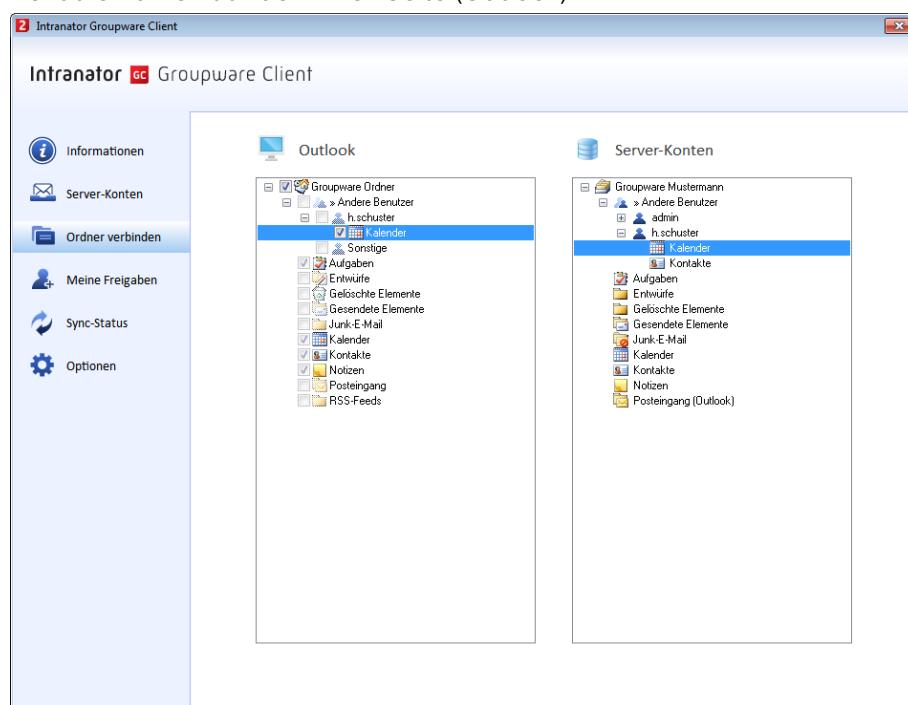
4. Klicken Sie den gewünschten Ordner auf der rechten Seite an und halten Sie die Maustaste gedrückt. Ziehen Sie den Ordner dann mit gedrückter Maustaste auf den Ordner »Andere Benutzer« auf der linken Seite (Outlook). Lassen Sie dort die Maustaste los.



- Sie werden nun gefragt, was für eine Art von Verbindung Sie erstellen möchten. Eine Verbindung vom Typ Einfach verbindet nur den einen gewählten Ordner. Eine Verbindung vom Typ Baum verbindet den gewählten Ordner und alle seine freigegebenen Unterordner.



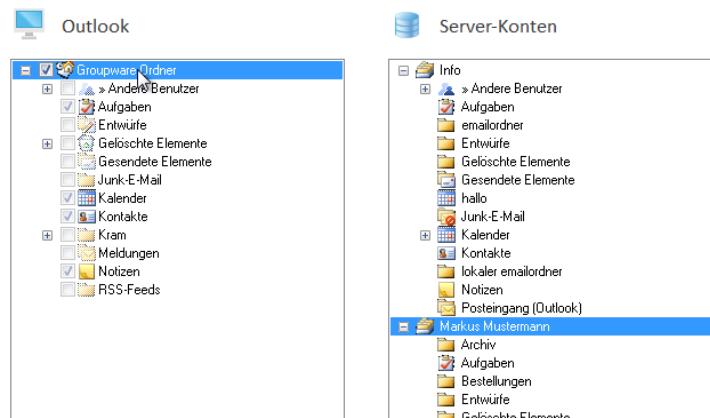
- Der verbundene Ordner erscheint nun unterhalb von »Andere Benutzer und dem Benutzernamen auf der linken Seite (Outlook).



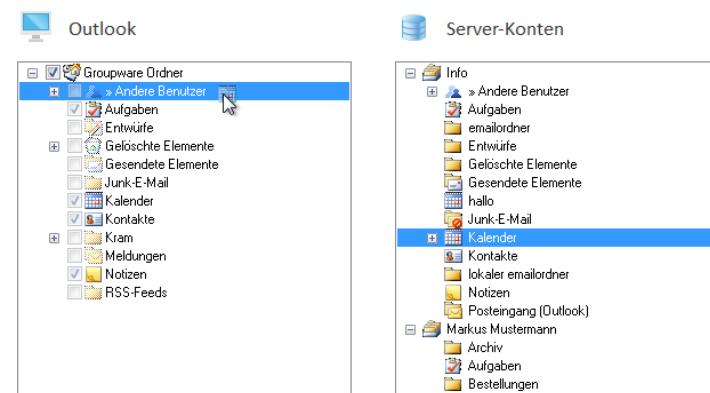
21.3. Mehrere Serverkonten

Im Menü Groupware Client > Server-Konten können mehrere Serverkontakte hinterlegt werden. Normalerweise ist davon ein Serverkonto automatisch mit dem lokalen Outlook verbunden, das heißt alle Ordner, die lokal neu angelegt werden, werden automatisch mit dem Server verbunden und umgekehrt.

Klicken Sie im Menü Groupware Client > Ordner verbinden auf den Wurzelordner der Seite Outlook und das entsprechende Serverkonto auf der anderen Seite wird markiert.



Möchten Sie Ordner anderer Serverkontakte verbinden und damit in Outlook nutzbar machen, so verbinden Sie sie, genau wie die freigegebenen Ordner anderer Nutzer, unterhalb von *Andere Benutzer*. Die dazu nötigen Schritte finden Sie in Abschnitt 21.2, „Fremde Ordner verbinden“ beschrieben.



22. Kapitel - Erweiterte Funktionen

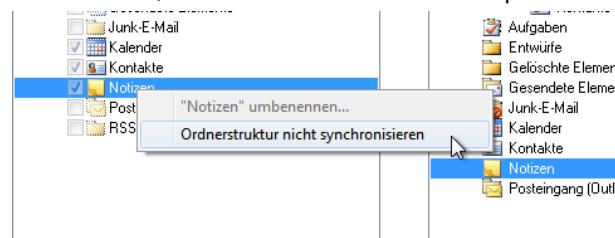
22.1. Ordner von der Synchronisation ausschließen

Normalerweise werden alle Groupwareordner (nicht E-Mail-Ordner) mit dem Server verbunden. E-Mail-Ordner werden dagegen normalerweise nicht mit dem Groupware Client verbunden, sondern über das separate, von Outlook verwaltete, IMAP-Konto abgerufen.

Es gibt die Möglichkeit, einzelne Groupwareordner von der Synchronisation auszuschließen und nicht zu verbinden. Genauso können E-Mail-Ordner bei Bedarf mit dem Groupware Client verbunden werden.

Gehen Sie dafür wie folgt vor:

1. Öffnen Sie das Menü Groupware Client > Ordner verbinden.
2. Klicken Sie auf der linken Seite (Outlook) den entsprechenden Ordner mit der rechten Maustaste an. Es öffnet sich das Kontextmenü.
3. Aktivieren Sie Ordnerstruktur nicht synchronisieren um die Verbindung dieses Ordners aufzuheben, bzw. deaktivieren Sie die Option um den Ordner zu verbinden.



Die Einstellung betrifft immer den Ordner selber und alle seine Unterordner.



Hinweis

Diese Vorgehensweise funktioniert nur für automatisch verbundene oder unterhalb einer Baum-Verbindung verbundene Ordner. Handelt es sich um einen einzeln verbundenen Ordner, gehen Sie stattdessen vor wie in Abschnitt 22.2.3, „Verbindung eines Ordners aufheben“ beschrieben.

22.2. Ordner manuell verbinden

Normalerweise verbindet der Intra2net Groupware Client die Ordner automatisch zwischen dem Server und Outlook:

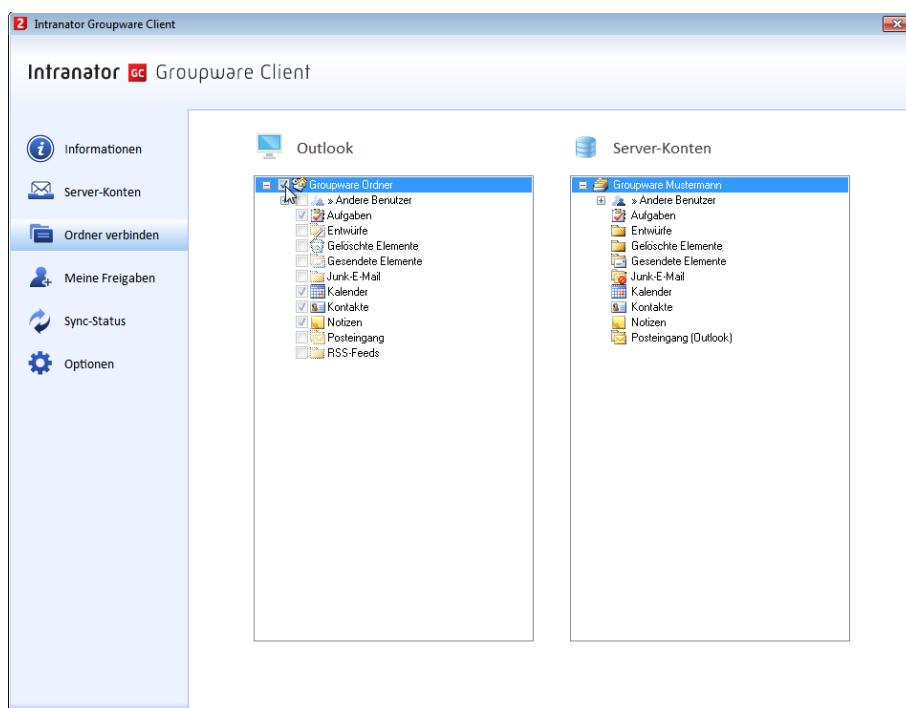
- Auf dem Server angelegte Groupware-Ordner (nicht E-Mail-Ordner) erscheinen automatisch auch in Outlook
- In Outlook angelegte Ordner werden automatisch auf dem Server angelegt und mit diesem verbunden
- Lokal gelöschte Ordner werden auch auf dem Server gelöscht
- Auf dem Server gelöschte Ordner werden lokal in den Ordner Gesicherte Daten verschoben
- Ordnernamen und Hierarchie sind in Outlook und auf dem Server identisch

Der Benutzer muss die Ordner nicht einzeln manuell verbinden, bekommt dafür aber keine Möglichkeit lokal in Outlook die Ordnerhierarchie umzugestalten oder Ordner lokal anders zu benennen als auf dem Server.

22.2.1. Umstellen auf Manuelles Verbinden

Um dies zu ermöglichen gibt es auch die Möglichkeit die Automatik abzuschalten und die Ordner manuell zu verbinden. Gehen Sie dafür wie folgt vor:

1. Öffnen Sie das Menü Groupware Client > Ordner verbinden.
2. Klicken Sie den Wurzelordner auf der linken Seite (Outlook) an und entfernen die Checkbox vor dem Namen.

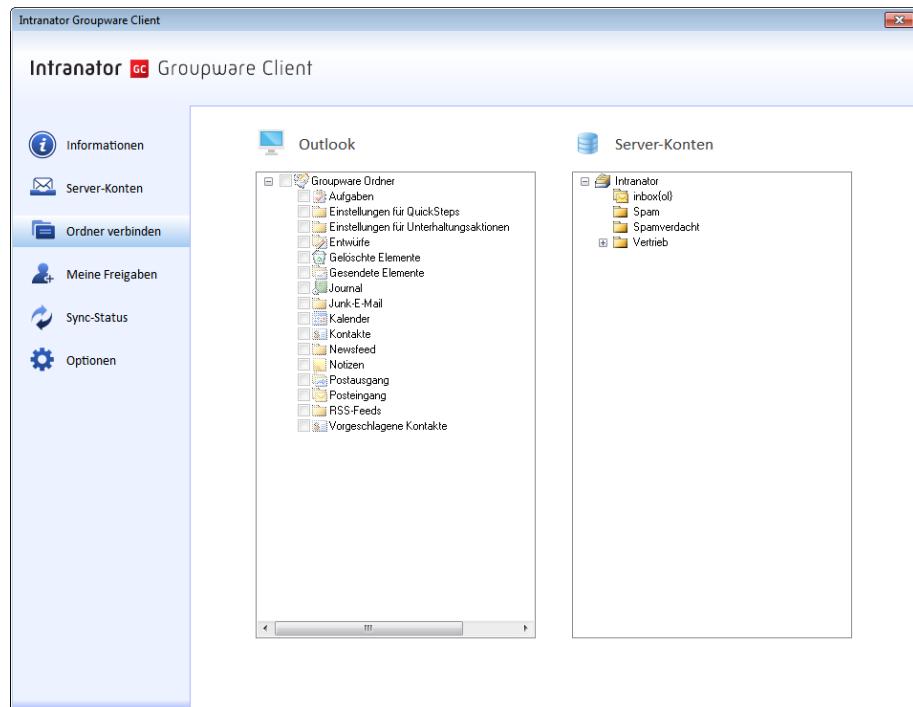


3. Sie werden gefragt ob Sie die Verbindung wirklich aufheben wollen. Antworten Sie mit OK.

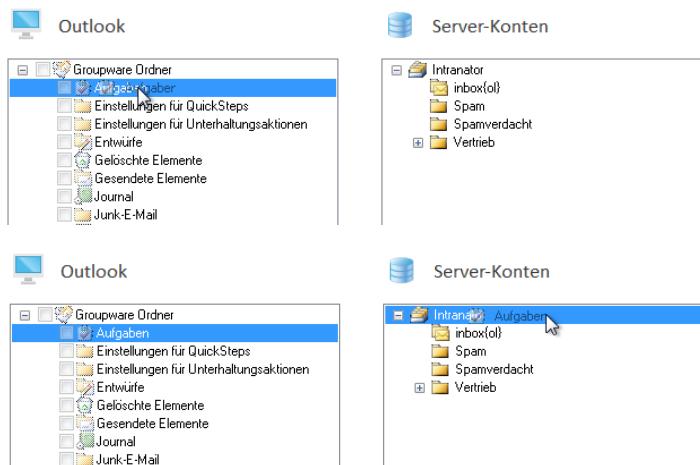
Die einzelnen Unterordner sind zuerst weiterhin verbunden wie bisher. Wenn lokal oder auf dem Server neue Ordner auf der obersten Ordnerebene angelegt werden, müssen diese aber ab sofort manuell verbunden werden (wenn gewünscht). Außerdem ist es jetzt möglich die Verbindung einzelner Ordner aufzuheben oder diese an einer anderen Stelle in der Ordnerhierarchie als auf dem Server zu verbinden.

22.2.2. Einen einzelnen Ordner verbinden

1. Öffnen Sie das Menü Groupware Client > Ordner verbinden.
2. Auf der rechten Seite wird das Konto auf dem Server angezeigt, auf der linken die Ordnerhierarchie im lokalen Outlook.



- Ziehen Sie den gewünschten Ordner auf der Outlook-Seite, hier Aufgaben, mit gedrückter Maustaste auf den Stammordner auf der rechten Seite und lassen dort die Maustaste los (Drag & Drop). Befindet sich der zu verbindende Ordner auf dem Server, so ziehen Sie ihn in die andere Richtung.



Sie haben nun die Wahl wie die Verbindung genau gestaltet werden soll:

Verknüpfungstyp	<ul style="list-style-type: none"> Einfach: Es wird nur der eine ausgewählte Ordner verbunden. Unterordner des Ordners werden nicht verbunden. Baum: Der Ordner wird inkl. aller seiner Unterordner verbunden. Werden lokal in Outlook oder auf dem Server neue Ordner hinzugefügt oder gelöscht, wird die Verbindung so angepasst, dass die Ordnerhierarchie lokal in Outlook und auf dem Server synchron sind.
-----------------	--

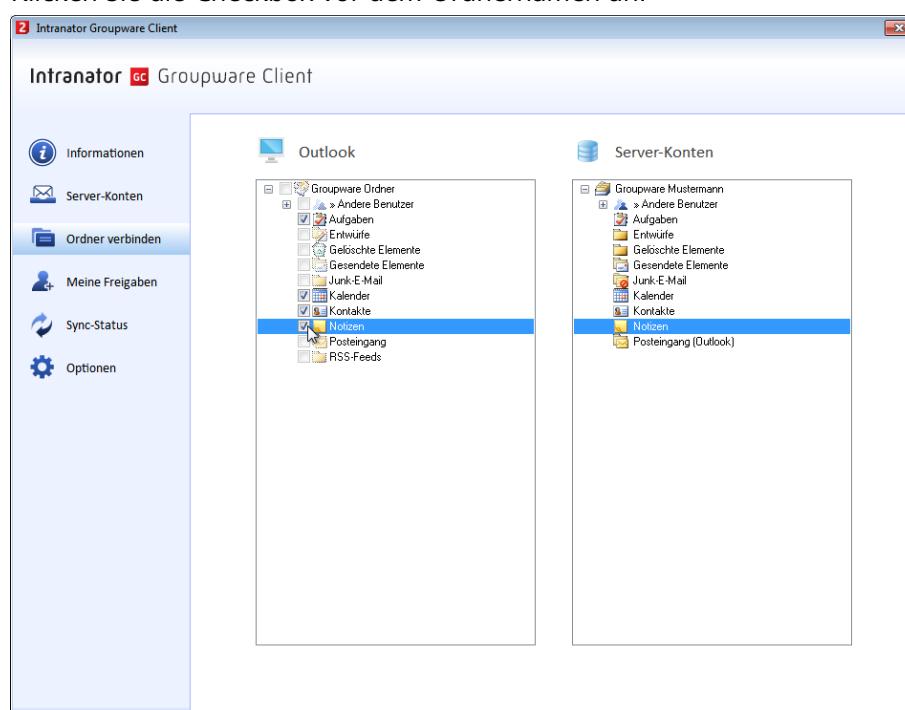
Neuer Unterordner	Wenn aktiviert, wird unterhalb des oben angegebenen Ziel-Ordners ein neuer Ordner angelegt und dieser mit dem Server verbunden.
Ordnername	Soll ein neuer Ordner angelegt werden, kann hier der Name einge-stellt werden. Damit können lokal in Outlook und auf dem Server unterschiedliche Namen für den selben Ordner verwendet werden. So kann z.B. der Ordner Kalender des Benutzers <code>meier</code> lokal in Outlook Kalender meier genannt werden.



22.2.3. Verbindung eines Ordners aufheben

Um die Verbindung eines manuell verbundenen Ordners aufzuheben gehen Sie wie folgt vor:

1. Öffnen Sie das Menü Groupware Client > Ordner verbinden.
2. Markieren Sie den Ordner, dessen Verbindung Sie aufheben möchten, auf der linken Seite (Outlook).
3. Klicken Sie die Checkbox vor dem Ordnernamen an.



4. Bestätigen Sie, dass Sie die Verbindung aufheben wollen.



Hinweis

Diese Vorgehensweise funktioniert nur für manuell verbundene Ordner. Handelt es sich um den Unterordner einer Baum-Verbindung, gehen Sie stattdessen vor wie in Abschnitt 22.1, „Ordner von der Synchronisation ausschließen“ beschrieben.

22.3. Posteingang/Meldungen

22.3.1. Ordnername

Im 20. Kapitel, „Konten konfigurieren“ empfehlen wir, E-Mails und Groupware-Objekte auf zwei verschiedene Datendateien aufzuteilen. Jede Datendatei hat normalerweise einen Ordner Namens `Posteingang`. Das zusammen hätte zur Folge, dass der Benutzer zwei Posteingänge angezeigt bekommt. Davon wird aber nur einer für neue E-Mails genutzt, der andere für Meldungen des Groupware Clients.

Letzterer wird daher mit dem Namen `Meldungen` angezeigt.

Sollte entgegen unserer Empfehlung der Groupware Client auch für E-Mails und nicht nur für Groupware-Objekte genutzt werden, kann der `Meldungen`-Ordner mit dem Posteingang auf dem Server verbunden werden. Er bekommt dann automatisch wieder seinen ursprünglichen Namen `Posteingang`.

Bei Bedarf (z.B. für Kompatibilität mit anderen Programmen und Add-Ins) kann dieses Verhalten auch unterdrückt werden, siehe hierzu Abschnitt 25.2.1, „Einstellungen für den Store“.

22.3.2. Ordnerhierarchie

In Outlook wird der Ordner `Posteingang` normalerweise auf der selben Hierarchieebene wie `Kalender`, `Kontakte` etc. angezeigt. Auf dem IMAP-Server ist der `Posteingang` dagegen der Wurzelordner eines Benutzers und alle anderen Ordner wie `Kalender`, `Kontakte` etc. sind Unterordner des Posteingangs.

Der Groupware Client übersetzt diese beiden unterschiedlichen Konzepte und stellt die Ordner innerhalb von Outlook so dar, wie es in Outlook üblich ist.

In Outlook ist es allerdings möglich Unterordner des Posteingangs anzulegen. Auf dem IMAP-Server lässt sich ein solcher Unterschied zwischen Unterordnern des Posteingangs und Ordnern auf der selben Ebene des Posteingangs normalerweise nicht darstellen. Der Groupware Client legt in diesem Fall einen Ordner Namens `ibx_sub` auf dem IMAP-Server an und legt alle Unterordner des Outlook-Posteingangs darunter ab.

22.4. Ordneroptionen

Im Menü Groupware Client > Optionen können Verbindungsoptionen zu den E-Mail-Konten eingestellt werden. Insbesondere wird hier eingestellt, wie häufig die einzelnen Ordner im Hintergrund mit dem Server synchronisiert werden.

Generell gilt, dass jeder Ordner, unabhängig von den Einstellungen hier, synchronisiert wird, sobald der Benutzer ihn in Outlook öffnet. Die Einstellungen hier betreffen nur das Synchronisieren im Hintergrund während in Outlook vom Benutzer kein Ordnerwechsel vorgenommen wird.



Hinweis

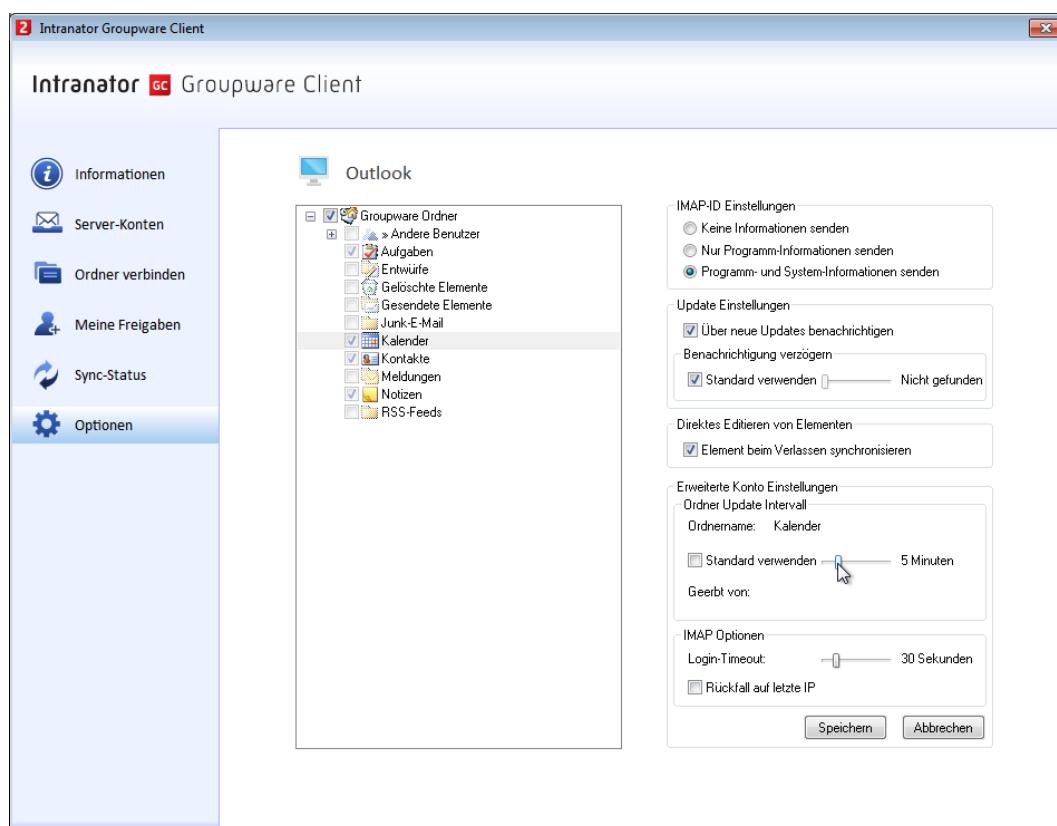
Diese Einstellungen betreffen nur Ordner, die über den Intra2net Groupware Client synchronisiert werden. Wie Sie die Synchronisationsfrequenz von Ordner, die über die in Outlook integrierte IMAP-Funktionalität synchronisiert werden, ändern, wird im Abschnitt 22.6, „Synchronisationsfrequenz von E-Mails konfigurieren“ erklärt.

Jeder Ordner übernimmt standardmäßig die Einstellungen seines übergeordneten Ordners. Der Wurzelordner wird standardmäßig alle 45 Minuten synchronisiert. Möchten Sie die Frequenz anpassen, mit der ein Ordner im Hintergrund synchronisiert wird, so markieren Sie den Ordner, deaktivieren die Kontrollfläche Standard verwenden und stellen die gewünschte Zeit ein. Alle Unterordner dieses Ordners übernehmen automatisch die eingestellte Zeit.

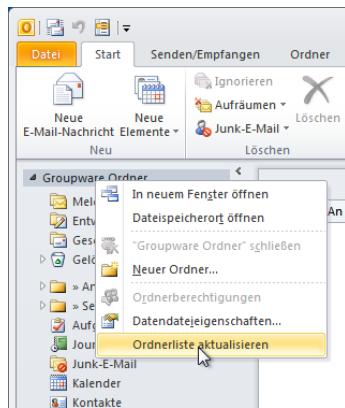


Achtung

Das Synchronisieren von vielen Ordner erzeugt eine deutliche Belastung auf dem Server. Achten Sie daher unbedingt darauf, dass nur ein oder sehr wenige Ordner pro Benutzer mit kurzem Zeitabstand synchronisiert werden. Werden alle Ordner im Takt von wenigen Minuten synchronisiert, so kann der Server bereits von wenigen Benutzern überlastet werden.



Die Einstellungen zu den Updateintervallen hier betreffen nur den Inhalt der Ordner, nicht Änderungen an der Ordnerstruktur. Diese werden, unabhängig vom hier eingestellten Intervall, immer beim Start von Outlook sowie danach alle 45 Minuten synchronisiert. Sie können den Groupware Client anweisen die Ordnerstruktur sofort zu aktualisieren, indem Sie mit einem Rechtsklick in der Ordnerliste das Kontextmenü eines vom Groupware Client verwalteten Ordners öffnen und dort die Option Ordnerliste aktualisieren aufrufen.



22.5. Serverseitige Einstellungen in Outlook bearbeiten

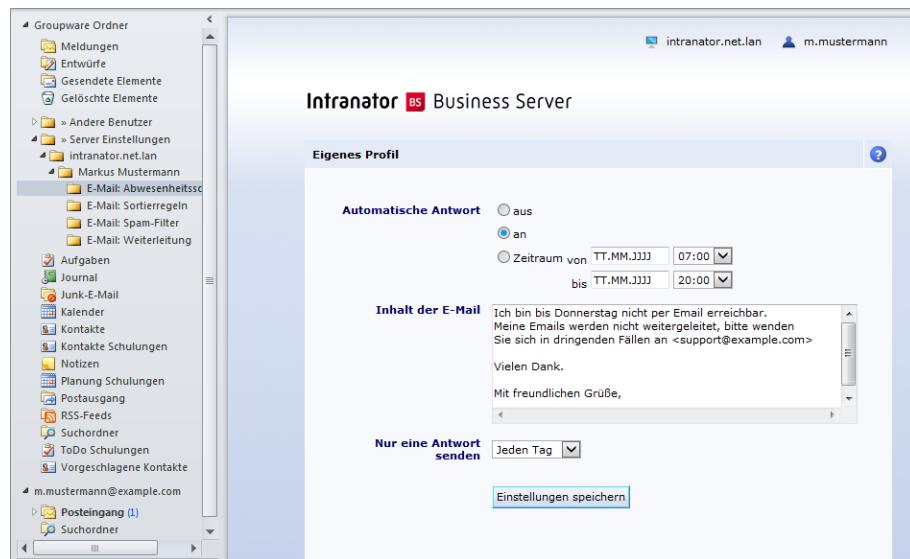
Der Intra2net Groupware Client bietet eine einfache Möglichkeit für die Benutzer, ihre serverseitigen Benutzereinstellungen direkt aus der Outlook-Oberfläche heraus zu verwalten.

Darüber können die Funktionen Abwesenheitsschaltung, E-Mail-Weiterleitung, Sortierregeln sowie der benutzerabhängige Spamfilter des Intranator Servers konfiguriert werden.

Voraussetzung ist natürlich, dass der Administrator des Intranator Servers den einzelnen Benutzern die Konfiguration dieser Einstellungen gestattet. Dies kann auf dem Server über das Menü Benutzermanager > Gruppen : Administrationsrechte z.B. bei der Alle-Gruppe geschehen, in dem die Seiten unterhalb von Benutzermanager > Eigenes Profil zu den erlaubten Seiten hinzugefügt werden.

Die einzelnen Benutzer können dann wie folgt die serverseitigen Einstellungen anpassen:

1. Prüfen Sie zuerst die Konfiguration des Kontos im Intra2net Groupware Client. Öffnen Sie dazu das Menü Groupware Client > Server-Konten. Kontrollieren Sie, ob die Verschlüsselung per SSL und die Überprüfung des Server Zertifikats aktiviert sind. Dies ist die beste Möglichkeit, eine korrekt gesicherte SSL-Verbindung zum Server sicherzustellen.
2. Sollte es zu SSL- oder Zertifikatsfehlern kommen, müssen Sie die Zertifikatskonfiguration anpassen. Beachten Sie dazu 10. Kapitel, „SSL-Verschlüsselung und Zertifikate“.
3. In der Outlook-Ordnerliste wird ein Ordner Server Einstellungen angezeigt. Darunter finden Sie Ordner für die einzelnen Konten und deren Einstellungen.
4. Klicken Sie die gewünschte Maske an und nun können Sie direkt innerhalb von Outlook z.B. die Automatische Antwort durch den Server (Abwesenheitsschaltung) konfigurieren.



Die Serverseitigen Einstellungen können nur aus Outlook aufgerufen werden, wenn die Datendatei des Groupware Clients im Outlook-Profil als Standarddatendatei festgelegt ist. Bei nicht als Standard festgelegten Datendateien erscheint zwar der Pfad in der Ordnerliste, die dahinterliegenden Seiten können aber nicht aufgerufen werden. Öffnen Sie in diesem Fall die Kontokonfiguration von Outlook und legen die Datendatei des Groupware Clients als Standarddatendatei fest.

22.6. Synchronisationsfrequenz von E-Mails konfigurieren

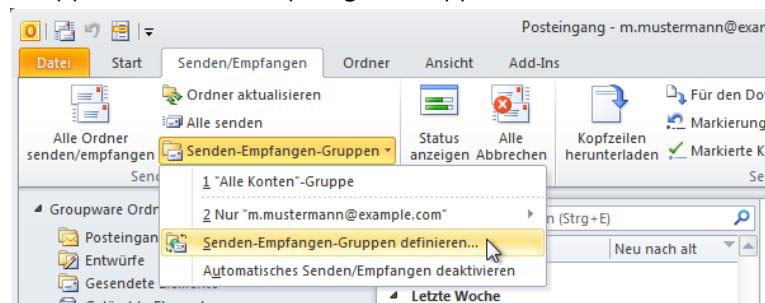
Mit den folgenden Schritten können Sie einstellen, wie häufig Outlook die E-Mail-Ordner auf neue Nachrichten und andere Änderungen überprüft.



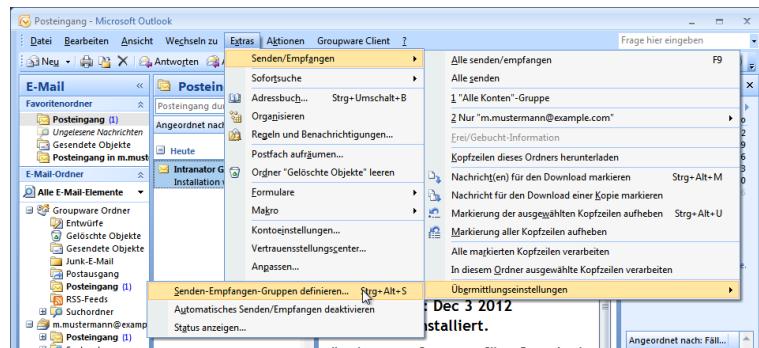
Hinweis

Diese Einstellungen betreffen nur Ordner, die über die in Outlook integrierte IMAP-Funktionalität synchronisiert werden. Wie Sie die Synchronisationsfrequenz von Ordner, die über den Intra2net Groupware Client synchronisiert werden, ändern, wird im Abschnitt 22.4, „Ordneroptionen“ erklärt.

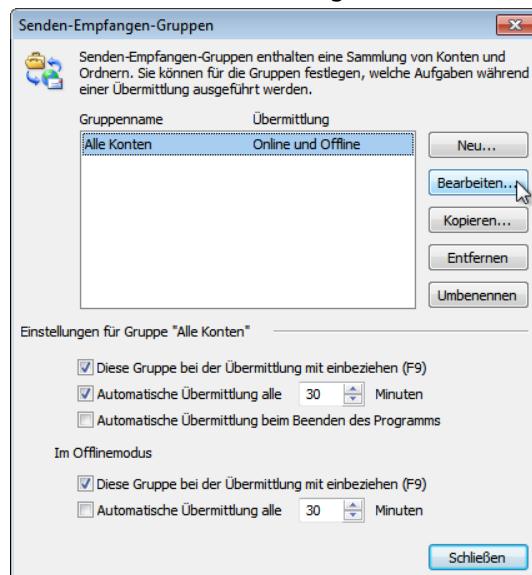
1. Öffnen Sie in der Registerkarte Senden/Empfangen das Menü Senden-Empfangen-Gruppen > Senden-Empfangen-Gruppen definieren.



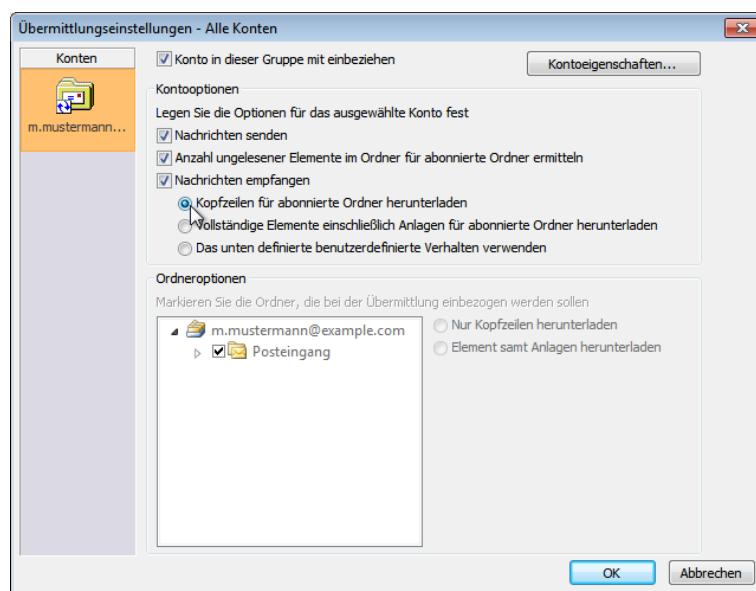
In Outlook 2007 ist dieses Menü erreichbar unter Extras > Senden/Empfangen > Übermittlungseinstellungen > Senden-Empfangen-Gruppen definieren.



2. Markieren Sie die Gruppe Alle Konten. Kontrollieren Sie, dass die Einstellung f r die automatische 脦bermittlung auf **30 Minuten** steht. Klicken Sie dann auf Bearbeiten.



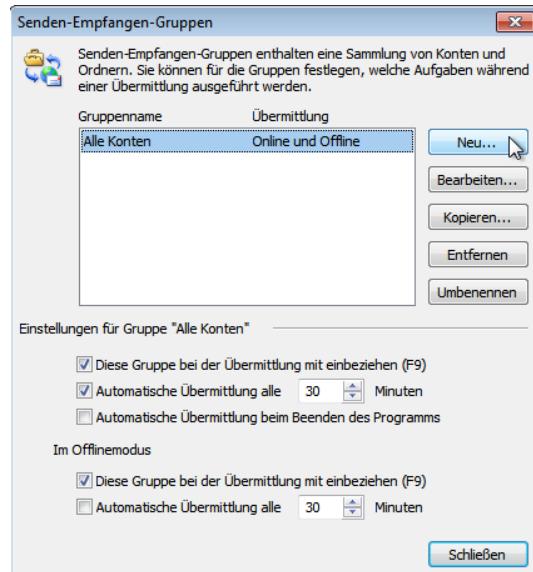
3. Stellen Sie den Nachrichtenempfang auf Kopfzeilen f r abonnierte Ordner herunterladen.



Durch diese Einstellung werden von den normalen E-Mail-Ordnern nur noch die Kopfzeilen in der lokalen Cache-PST gespeichert. Der Inhalt der E-Mails wird nur bei

Bedarf vom Server geladen. Dadurch verringert sich die Größe der lokalen Cache-PST wesentlich. Dies schont Ressourcen auf dem Client und beschleunigt das Reaktionsverhalten von Outlook.

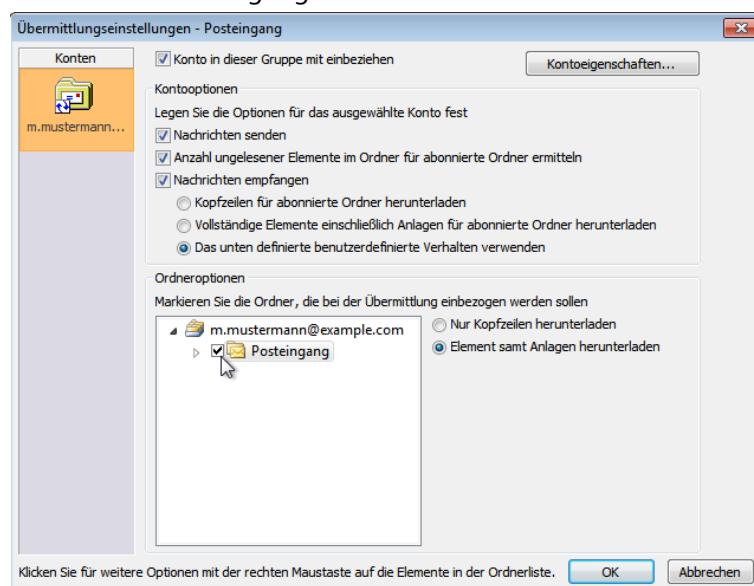
- Schließen Sie die Gruppenkonfiguration und legen eine neue Gruppe an.



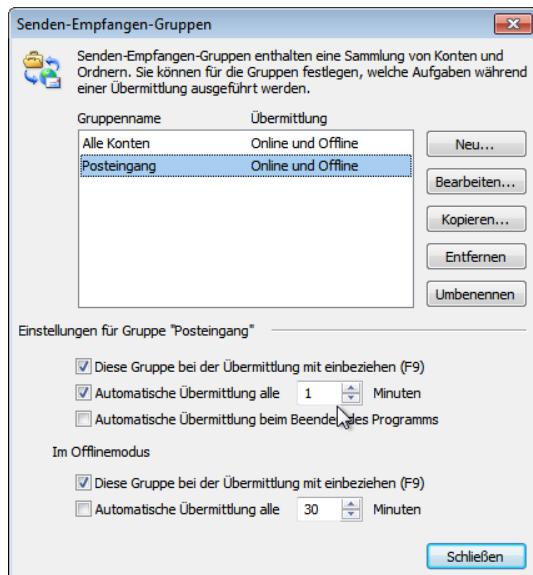
- Nennen Sie die neue Gruppe **Posteingang**.



- Stellen Sie den Nachrichtenempfang auf benutzerdefiniert. Markieren Sie dann nur den Ordner Posteingang und schalten auf Element samt Anlagen herunterladen.



- Schließen Sie die Gruppenkonfiguration. Stellen Sie die automatische Übermittlung für die Gruppe Posteingang z.B. auf **1 Minute**.



Achtung



Das Synchronisieren von vielen Ordnern erzeugt eine deutliche Belastung auf dem Server. Achten Sie daher unbedingt darauf, dass nur ein oder sehr wenige Ordner pro Benutzer mit kurzem Zeitabstand synchronisiert werden. Werden alle Ordner im Takt von wenigen Minuten synchronisiert, so kann der Server bereits von wenigen Benutzern überlastet werden.

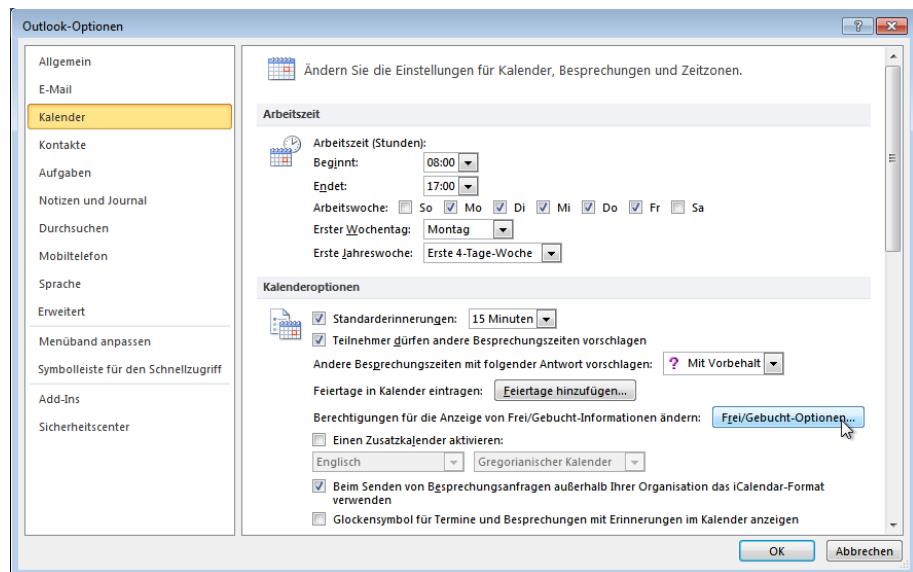
22.7. Frei-/Gebucht-Informationen verwenden

Sollten Ihnen Kollegen ihren Kalender nicht zum Lesen freigegeben haben, können Sie dennoch für die Organisation eines gemeinsamen Termins herausfinden, wann die Kollegen keine anderen Termine in ihren Kalendern eingetragen haben. Diese Information wird über das Frei-/Gebucht-System bereitgestellt.

Bevor Sie die Frei-/Gebucht-Daten nutzen können, müssen Sie zuerst die korrekte Adresse zum Abruf der Daten in Outlook hinterlegen. Gehen Sie dazu wie folgt vor:

22.7.1. Outlook 2013 und 2010

1. Wählen Sie in Outlook im Menü Datei den Punkt Optionen aus.
2. Klicken Sie auf die Schaltfläche Kalender.
3. Wählen Sie nun die Schaltfläche Frei/Gebucht-Optionen aus.

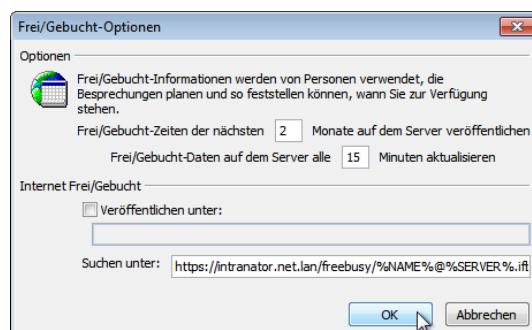


- Tragen Sie den Suchpfad bei Suchen unter ein.

Die Adresse lautet <https://intranator.net.lan/freebusy/%NAME%@%SERVER%.ifb>.

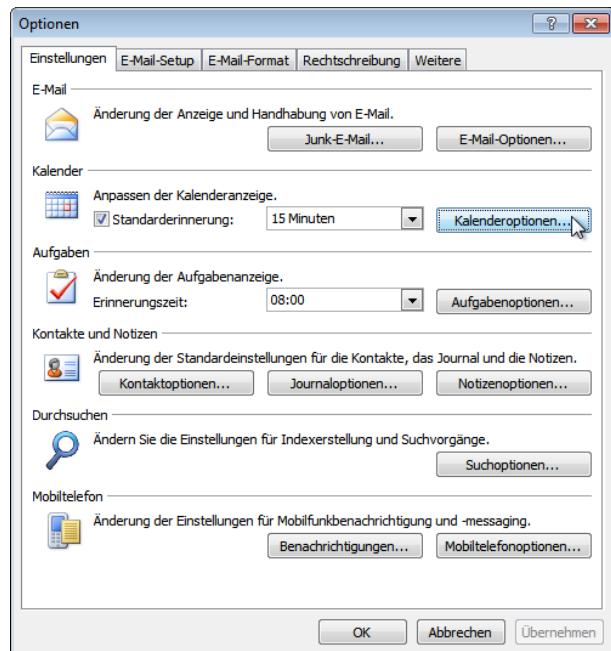
Verwenden Sie den Namen Ihres Intranator Servers und geben die Adresse ansonsten genau so wie hier gezeigt ein.

Da der Intranator Server die Frei/Gebucht-Informationen automatisch erzeugt, darf das Kontrollkästchen Veröffentlichen unter nicht gesetzt sein.

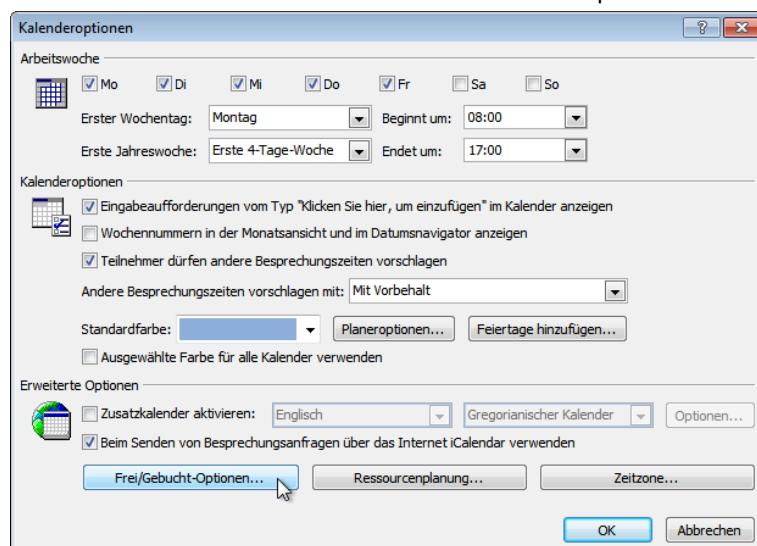


22.7.2. Outlook 2007 und Outlook 2003

- Wählen Sie in Outlook im Menü Extras den Punkt Optionen aus.
- Klicken Sie auf die Schaltfläche Kalenderoptionen.



- Wählen Sie nun die Schaltfläche Frei/Gebucht-Optionen aus.

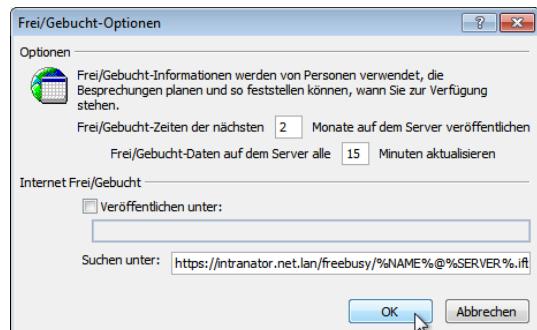


- Tragen Sie den Suchpfad bei Suchen unter ein.

Die Adresse lautet <https://intranator.net.lan/freebusy/%NAME%@%SERVER%.ifb>.

Verwenden Sie den Namen Ihres Intranator Servers und geben die Adresse ansonsten genau so wie hier gezeigt ein.

Da der Intranator Server die Frei/Gebucht-Informationen automatisch erzeugt, darf das Kontrollkästchen Veröffentlichen unter nicht gesetzt sein.

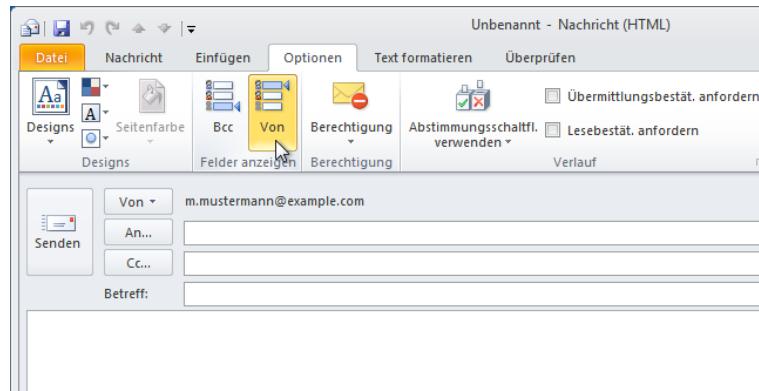


22.8. Mehrere Absenderadressen

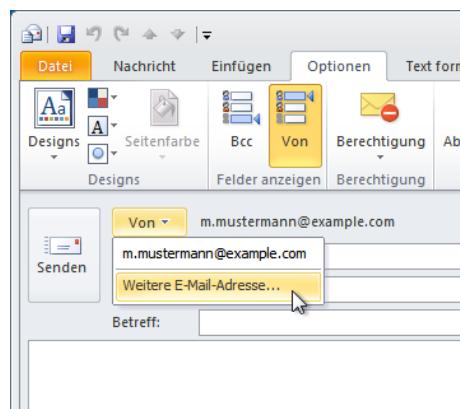
In der Standardkonfiguration steht nur die eigene E-Mail-Adresse als Absenderadresse zur Verfügung. Um z.B. einen anderen Mitarbeiter zu vertreten oder im Namen seiner Abteilung (z.B. Vertrieb) zu antworten, kann es sinnvoll sein, weitere Absenderadressen zu konfigurieren.

Um mehrere Absenderadressen in Ihrem Outlook zu konfigurieren, gehen Sie wie folgt vor:

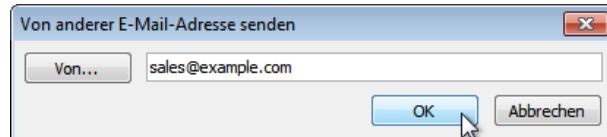
1. Klicken Sie auf Neue E-Mail-Nachricht.
2. Es öffnet sich das Fenster zum Verfassen einer neuen E-Mail. Wählen Sie das Menü Optionen und aktivieren die Schaltfläche Von.



3. Klicken Sie auf die Schaltfläche Von in den Kopfzeilen. Es öffnet sich ein Fenster. Wählen Sie Weitere E-Mail-Adresse....



4. Tragen Sie die gewünschte Absenderadresse ein.



5. Ab sofort steht Ihnen die eben eingegebene Adresse bei allen neuen E-Mails über die Von-Schaltfläche als Absenderadresse zur Verfügung.

Beachten Sie, dass die gesendeten E-Mails weiterhin in Ihrem eigenen Ordner für gesendete Elemente gespeichert werden. Möchten Sie mit einer anderen Absenderadresse versendete E-Mails in einem anderen Ordner speichern lassen, so können Sie in Outlook eine E-Mail-Regel definieren, die abhängig vom zum Versenden verwendeten Konto eine Kopie in unterschiedliche Zielordner ablegt.

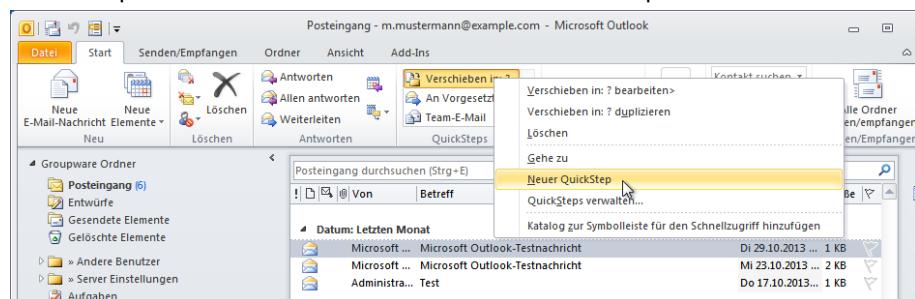
22.9. Erinnerungen und Nachverfolgen von E-Mails

Outlook bietet bei Verwendung eines POP-Kontos oder im Zusammenhang mit dem Exchange Server die Möglichkeit, Erinnerungen für E-Mails zu definieren und eine Liste von später zu Bearbeitenden E-Mails zu erstellen (Nachverfolgen-Funktion). Dies ist bei Verwendung von IMAP-Konten (wie sie für den Groupware Client empfohlen werden) nicht möglich. Außerdem können solche Erinnerungen und Nachverfolgen-Informationen nicht auf Mobilgeräte übertragen werden.

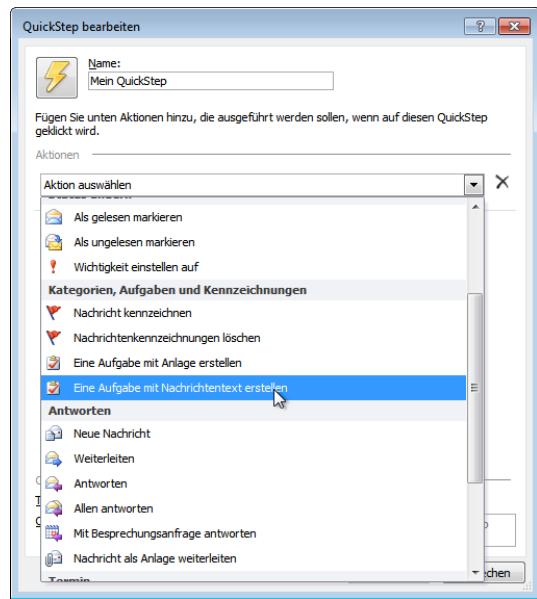
Daher empfehlen wir, statt der Nachverfolgen-Funktion für die E-Mail zu verwenden, eine separate Aufgabe zu erstellen. Diese kann dann in Outlook, der Webgroupware und auf per ActiveSync angebundenen Geräten verwendet werden. Bei Bedarf kann sie auch für andere Nutzer freigegeben und von diesen dann bearbeitet werden, z.B. im Falle von Vertretung.

Ab Outlook 2010 kann das Anlegen mit der QuickSteps-Funktion automatisiert werden. Gehen Sie zum einmaligen Einrichten wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf einen beliebigen bereits bestehenden QuickStep und wählen die Funktion Neuer QuickStep.

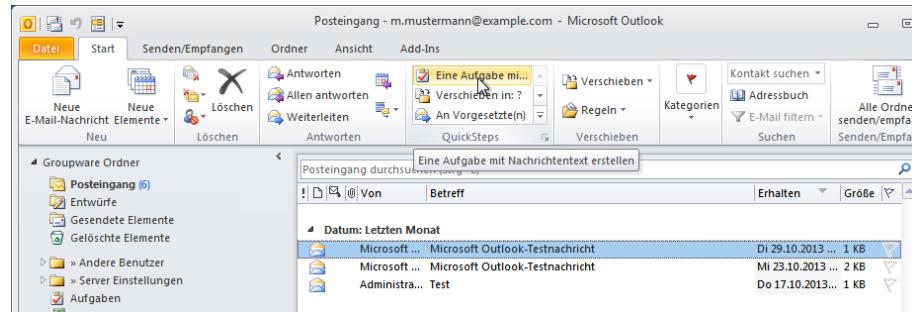


2. Wählen Sie die Aktion Eine Aufgabe mit Nachrichtentext erstellen.



3. Speichern Sie den QuickStep über die Schaltfläche Fertig stellen.

Der QuickStep ist nun fertig eingerichtet und kann verwendet werden. Öffnen Sie dazu die gewünschte E-Mail und klicken auf den vorher angelegten QuickStep. Es wird automatisch eine passende Aufgabe erzeugt.



22.10. Kennzeichnung als Privat

Termine, Aufgaben und Kontakte können in Outlook als "Privat" gekennzeichnet werden. Diese Daten werden, unabhängig von den Zugriffsrechten auf den Ordner, nur demjenigen angezeigt, der die Privat-Kennzeichnung gesetzt hat. Der Eigentümer des Objekts wird dabei über den Benutzerlogin identifiziert.

Für andere Benutzer werden die Daten vollständig ausgeblendet, bzw. bei Terminen nur ein Platzhalter angezeigt. Siehe dafür aber auch die Einstellungen für CalPrivatePlaceholder in Abschnitt 25.2.1, „Einstellungen für den Store“.



Achtung

Die als privat gekennzeichneten Daten werden bei anderen Benutzern mit Zugriffsrechten auf den Ordner nur ausgeblendet und in Outlook nicht angezeigt. Das bedeutet aber nicht, dass andere auf diese Daten nicht zugreifen könnten. Die Kennzeichnung als Privat erfüllt damit nicht die üblichen Ansprüche an Sicherheit und Datenschutz.

Andere Benutzer mit Zugriffsrechten auf den Ordner können die Daten u.a. über IMAP als XML-Daten auslesen. Folgendes Beispiel zeigt einen als privat gekennzeichneten Termin aus einem Kalender, der in einem E-Mail-Konto in Outlook abonniert wurde.

```

<?xml version="1.0" encoding="UTF-8"?>
<event version="1.0">
<uid>mystore(0cd6bb09-1946-48d4-8b88-15de8b9a86e5)<eidFld:<()-0x0-0x0-0x0><SE:0x200384><RK:5a77088496d1d043a89910e57219a37a></uid>
<uid>
<event>04000000820000074c5b7101a82e008000000010a066823f85cd0100000000000000000000000000000010000000e</event>
<body type="in-sync"></body>
<body-alt type="text/html"><div><p align="left"><font style = "color: #000000; font-size: 10pt; font-family: Calibri;"><font style = "color: #000000; font-size: 11pt; font-family: Calibri;"><font style = "color: #000000; font-size: 11pt; font-family: Calibri;"><p></p></font></font></p></div></body-alt>
<body-alt type="text/rtf-compressed">b90c0000d42700004c5a4675615a366b07000601010b606e6731303266350064007263700dd</body-alt>
<summary>Mein Termin</summary>
<conversation-topic>Mein Termin</conversation-topic>
<creation-date>2012-08-28T15:05:35Z</creation-date>
<last-modification-date>2012-08-28T15:06:52Z</last-modification-date>
<sensitivity>private</sensitivity>
<ol-sensitivity>Private</ol-sensitivity>
<product-id>Intranator Groupware Client</product-id>
<show-time-as>busy</show-time-as>
<ol-busy-status-intended>MaybeUnset</ol-busy-status-intended>
<start-date>2012-08-28T10:00:00Z</start-date>
<end-date>2012-08-28T10:30:00Z</end-date>
<organizer>
<display-name>Markus Mustermann</display-name>
<smtp-address>m.mustermann@example.com</smtp-address>
</organizer>
<creator>
<display-name>Markus Mustermann</display-name>
<smtp-address>m.mustermann@example.com</smtp-address>
</creator>
<priority>3</priority>
<ol-importance>Normal</ol-importance>
</event>

```

Wie man sieht, sind neben einigen nicht intuitiv deutbaren Informationen alle relevanten Daten des Termins im Klartext lesbar.

22.11. Erinnerungen in gemeinsam genutzten Ordnern

Outlook kann bei Terminen und Aufgaben Erinnerungen zur Fälligkeit auslösen. Wird ein Ordner von mehreren Benutzern gemeinsam verwendet, so werden die Erinnerungen für jeden Benutzer individuell behandelt.

Jeder Benutzer kann sich also auf jedes Objekt beliebig Erinnerungen setzen und diese erscheinen zur Fälligkeit nur bei ihm selbst. Zur Identifikation des Benutzers wird dabei das Benutzerlogin verwendet.

Der einzige Sonderfall ist, wenn ein Benutzer einen Termin oder eine Aufgabe neu anlegt und gleichzeitig die Erinnerung aktiviert. Hierbei wird dann die Erinnerung für den anlegenden Benutzer und zusätzlich eine für den Eigentümer des Ordners hinterlegt. Dadurch kann z.B. eine Sekretärin einen Termin mit Erinnerung für den Chef anlegen.

Ein nachträgliches Ändern der Erinnerung betrifft dann aber nur noch den ändernden Benutzer.

22.12. Festlegen des Speicherorts für IMAP-Cache-PSTs

Outlook legt für jedes konfigurierte IMAP-Konto auf dem PC eine .pst-Datei an um Ordnerstruktur, Kopfzeilen und Nachrichten lokal zwischenspeichern (Cache). Der genaue Speicherort dieser Dateien hängt von der verwendeten Version von Windows und Outlook ab.

Möchte man den Speicherort ändern, so kann man dies über einen Eintrag in der Registrierung unter folgendem Schlüssel festlegen:

`HKCU\Software\Microsoft\Office\nn.n\Outlook` Verwenden Sie statt `nn` die interne Version von Outlook (`12.0` für Outlook 2007, `14.0` für Outlook 2010 und `15.0` für Outlook 2013).

Legen Sie in diesem Schlüssel eine Zeichenkette mit dem Namen `ForcePSTPath` an. Darin können Sie dann den neuen Zielpfad angeben, z.B. `C:\Users\%username%\AppData\Roaming`.

Dieser Eintrag wird nur ausgewertet während ein neues IMAP-Konto angelegt wird. Bestehende Konten werden nicht verändert. Der Eintrag in der Registrierung muss also vor dem Konfigurieren des Profils bereits angelegt sein.

Beachten Sie, dass Microsoft davon abrät, .pst-Dateien auf Netzwerklaufwerken abzulegen. .pst-Dateien sind Datenbanken und müssen als solche gewisse Funktionen garantieren. Da aber auf einem Netzwerklaufwerk nicht alle Schutzmechanismen eines lokalen Laufwerks verfügbar sind, kann die .pst-Datei nicht alle geforderten Garantien geben. Verletzt man diese Anforderungen, kann dies daher Störungen und Datenverlust, inkl. schlechentlichem, erst deutlich später erkennbarem, Datenverlust, zur Folge haben.



Hinweis

Wird der Intra2net Groupware Client von Benutzern mit Servergespeicherten Profilen (Roaming Profiles) eingesetzt, muss die IMAP-Cache-PST im Verzeichnis des Servergespeicherten Profils liegen. Ansonsten kann Outlook die Datei beim Wechsel des PCs nicht laden.

22.13. Benutzerdefinierte Felder in Kontakten

Outlook erlaubt bei Kontakten zusätzlich zu den vordefinierten Feldern benutzerdefinierte Felder anzulegen (Menüband Kontakte > Anzeigen > Alle Felder, Auswählen aus Benutzerdefinierte Felder in diesem Element). Diese können pro Kontaktordner definiert und dann bei den einzelnen Kontakten mit Inhalten gefüllt werden.

Der Intra2net Groupware Client kann diese benutzerdefinierten Felder auch auf den Server synchronisieren und damit über verschiedene Workstations oder Benutzer hinweg nutzbar machen. Allerdings muss vor der ersten Nutzung eine Definitionsdatei für diese Felder auf allen Workstations vorliegen.

Die Definitionsdatei ist eine XML-Datei, heißt `userdefined_sync_fields.xml` und liegt standardmäßig in dem Programmordner, in den der Intra2net Groupware Client installiert wurde. Der Pfad dieser Datei kann aber über den Eintrag `syncTemplatesFilePath` in der Registrierung angepasst werden (siehe Abschnitt 25.2, „Erweiterte Einstellungen in der Registrierung“).

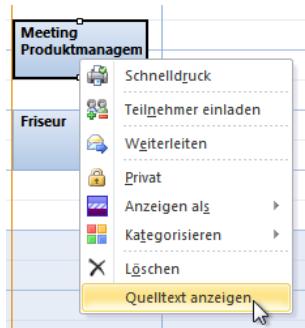
Mit dem Intra2net Groupware Client wird eine Beispieldatei als `userdefined_sync_fields_template.xml` mitgeliefert, die eine genaue Beschreibung und Beispiele enthält, wie benutzerdefinierte Felder definiert werden. Kopieren Sie diese Musterdatei auf `userdefined_sync_fields.xml` und öffnen sie mit einem XML-Editor (wie z.B. Oxygen [<http://www.oxygenxml.com/>], EditiX [<http://www.editix.com/>] oder XMLSpy [<http://www.altova.com/xmlspy.html>]). Alles weitere ist in der Musterdatei beschrieben.

Die benutzerdefinierten Felder können momentan nur mit dem Intra2net Groupware Client genutzt werden. In der Webgroupware oder über ActiveSync können Sie nicht bearbeitet oder angezeigt werden.

22.14. Anzeige des Quelltextes von Objekten

Zur Analyse von Codierungsproblemen und ähnlichem ist es möglich, die Objekte im Quelltext zu betrachten. Auch die Kopfzeilen (Header) der Objekte werden hier mit angezeigt.

Klicken Sie zur Anzeige des Quelltexts das Objekt mit der rechten Maustaste an um das Kontextmenü zu öffnen und wählen Quelltext anzeigen.



23. Kapitel - Kompatibilität und Zusammenarbeit

23.1. Personal-Firewalls auf dem Client

Der Intra2net Groupware Client muss aus dem Outlook-Prozess heraus per IMAP/IMAPS, SMTP und HTTP/HTTPS auf den Intranator Server zugreifen können. Sie müssen also die entsprechenden Ports in einer Firewall auf dem Client freischalten.

Wenn Sie die Firewall im Lernmodus betreiben, beachten Sie bitte, dass HTTP/HTTPS nur bei Änderungen im Kalender, Abfragen von Frei/Gebucht-Listen sowie zur Konfiguration von Weiterleitungen und Abwesenheitsautomatiken benötigt wird.

23.2. Virenscanner auf dem Client

Auf dem Client installierte VirensScanner greifen oft tief in das System ein, um Viren abfangen zu können. Dabei kann es teilweise zu Konflikten mit dem Intra2net Groupware Client kommen.

Kommt es zu Problemen beim Synchronisieren und haben Sie einen VirensScanner auf dem Client aktiviert, so versuchen Sie zuerst, das Scannen von IMAP zu deaktivieren. Neue E-Mails durchlaufen zuerst den Intranator Server und seinen VirensScanner, Sie gehen dadurch also kein zusätzliches Risiko ein.

Hier finden Sie detailliertere Informationen zu einigen Produkten (ohne Gewähr):

Hersteller	Produkt	Nötige Maßnahme
Avast	Alle Antivirus-Produkte	Keine Änderung notwendig
AVG	Antivirus Business Edition	Personal Email Scanner (für alle anderen E-Mail-Anwendungen) deaktivieren
Avira	Alle Antivirus-Produkte	Scannen des IMAP-Protokolls deaktivieren
Eset	NOD32 Antivirus	Scannen des IMAP-Protokolls deaktivieren
F-Secure	Internet Security	Keine Änderung notwendig
Kaspersky	Internet Security	Keine Änderung notwendig
McAfee	Alle Antivirus-Produkte	Keine Änderung notwendig, da nicht auf IMAP-Ebene gescannt wird (McAfee KB52786)
Symantec	Norton AntiVirus	Keine Änderung notwendig, da nicht auf IMAP-Ebene gescannt wird
TrendMicro	Titanium	Keine Änderung notwendig, da nicht auf IMAP-Ebene gescannt wird

23.3. Kompatibilität mit PDAs und Mobiltelefonen

Verwenden Sie wenn möglich die ActiveSync-Funktion des Intranator Servers um eine direkte Verbindung zwischen Intranator Server und Mobilgerät ohne einen Umweg über Outlook herzustellen. Dadurch können die Daten auf dem Mobilgerät auch von unterwegs aktualisiert werden. Außerdem ist kein Addin für Outlook notwendig welches unter Umständen Probleme hervorrufen kann.

Die Konfiguration von ActiveSync zwischen Intranator Server und Mobilgeräten finden Sie erklärt im 29. Kapitel, „Mobile Geräte per ActiveSync anbinden“.

23.4. Sonstige Programme

Wir empfehlen den Intra2net Groupware Client nicht zusammen mit dem Microsoft Business Contact Manager einzusetzen, da es in manchen Konfigurationen zu Synchronisationsstörungen kommen kann.

Die Zusammenarbeit mit anderen Addins oder Plugins für Outlook wird nicht garantiert.

24. Kapitel - Migration vom Intranator Groupware Connector

Wenn Sie bisher den Intranator Groupware Connector verwenden und nun auf den Intra2net Groupware Client umsteigen möchten, gehen Sie am besten wie im Folgenden beschrieben vor.

Die Migration der Daten auf dem Client PC durch den Intra2net Groupware Client ist nötig, um die Daten vollständig in das neue Datenformat des Intra2net Groupware Clients zu übertragen. Würde stattdessen nur ein neues Profil mit dem Intra2net Groupware Client eingerichtet und die Daten ohne Migration vom Server eingelesen, würden Teile der Daten verloren gehen (z.B. alle Serientermine). Nur durch die im Folgenden beschriebenen Migrationsschritte ist sichergestellt, dass es nicht zu Datenverlust kommt.

Der parallele Einsatz des Groupware Connectors und des Groupware Clients ist nur möglich, wenn sichergestellt ist, dass beide nicht auf die selben Daten zugreifen.

24.1. Wahl des Migrationsverfahrens

Die Migration kann entweder automatisch oder manuell erfolgen.

Bei der automatischen Migration werden alle Daten aus der Datendatei des alten Groupware Connectors vollautomatisch auf den Intranator Server migriert. Der Vorteil davon ist, dass bei vielen Groupwareordnern weniger manuelle Schritte durch den Benutzer vorgenommen werden müssen. Nachteilig dagegen ist, dass das Verfahren eine konsistente Datendatei voraussetzt und bei Fehlern in der Datendatei aus Sicherheitsgründen blockieren kann. Manuelle Eingriffsmöglichkeiten in den Migrationsprozess bestehen nicht.

Bei der manuellen Migration werden die zu migrierenden Daten auf dem Server gelöscht, von Hand per Drag&Drop Ordner für Ordner in den Groupware Client übernommen und auf den Server synchronisiert. Hierbei muss der Benutzer alle nötigen Schritte von Hand ausführen und hat daher die volle Kontrolle über den Prozess.

Beide Verfahren werden in den folgenden Abschnitten im Detail beschrieben.

24.2. Die automatische Migration

24.2.1. Überblick

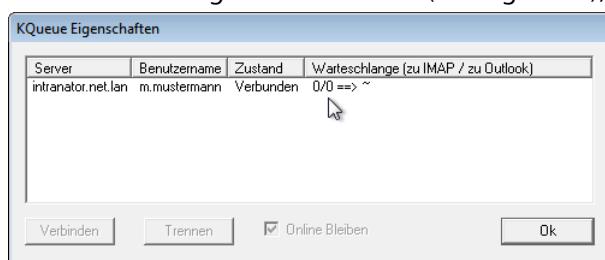
Hier ein grober Überblick darüber, wie die automatische Migration vor sich geht. Die einzelnen Schritte werden im folgenden Abschnitt ausführlich erklärt.

- Mit Hilfe des alten Groupware Connectors die bestehenden Daten vollständig mit dem Server synchronisieren.
- Ein Backup der Daten auf Client und Server erstellen.
- Den alten Groupware Connector deinstallieren, den neuen Intra2net Groupware Client installieren.
- Ein neues Profil ohne E-Mail-Konto anlegen, eine Datendatei vom Typ Intranator Groupware Client hinzufügen.

- Die Datendatei des neuen Profils mit der bestehenden Datendatei des Groupware Connectors überschreiben.
- Outlook starten und den Konvertierungs-Assistenten die Konvertierung durchführen lassen.
- Das Migrationsprofil löschen und ein neues Profil anlegen. Die Daten werden automatisch vom Server geladen.
- Abonnements von Groupwareordnern im direkt von Outlook verwalteten IMAP-Konto aufräumen; Kontrolle der Freigaben an andere Benutzer.

24.2.2. Die Migration in einzelnen Schritten

1. Öffnen Sie Outlook mit dem Profil des Groupware Connectors. Öffnen Sie die KQueue im Infobereich der Tastleiste und lassen sich den Zustand der Warteschlange anzeigen. Die Warteschlange muss leer sein (Anzeige: 0 / 0), bevor Sie fortfahren können.



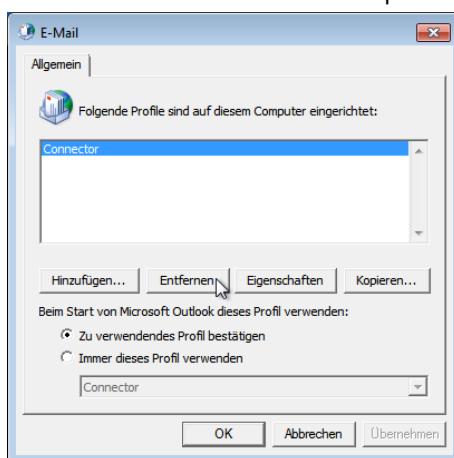
2. Schließen Sie Outlook.
3. Kontrollieren Sie, dass Sie über ein aktuelles Backup der Daten auf dem Intranator Server verfügen. Wenn nicht, so holen Sie dies über das Menü System > Backup > Einstellungen nach und warten, bis auf der Hauptseite nicht mehr angezeigt wird, dass das Backup momentan erstellt wird.
4. Stellen Sie sicher, dass das Konto dieses Benutzers von nun an nicht mehr mit dem Groupware Connector verwendet wird. Dies gilt auch für die Verwendung durch andere Benutzer über freigegebene Ordner.
5. Öffnen Sie die Windows-Systemsteuerung, Menü Programme, bzw. Programme und Funktionen.
6. Markieren Sie den Intranator Groupware Connector und wählen Deinstallieren.
7. Im Laufe der Deinstallation werden Sie aufgefordert den Outlook-Dienst des Groupware Connectors zu löschen. Markieren Sie den Dienst und klicken auf Löschen.



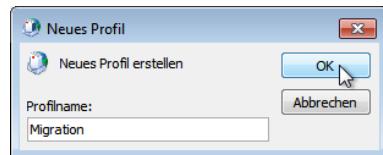
- Fahren Sie mit der Deinstallation fort, lassen Sie die Datendateien bestehen wie sie sind.



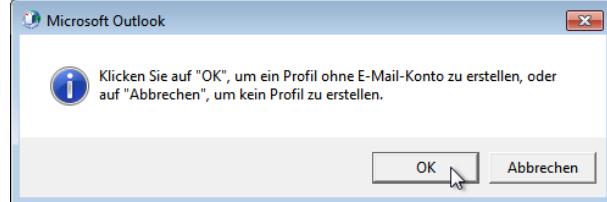
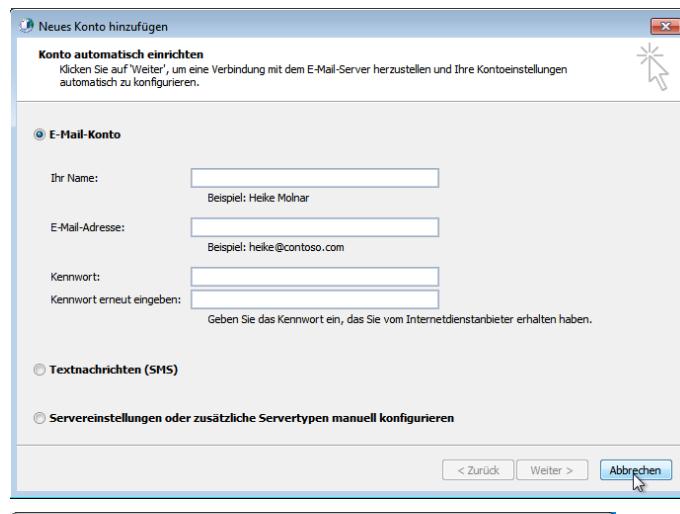
- Installieren Sie nun den Intra2net Groupware Client, falls Sie dies noch nicht getan haben.
- Öffnen Sie die Windows-Systemsteuerung, Menü E-Mail (32 Bit). Lassen Sie sich die Profile anzeigen.
- Wählen Sie das Profil des Groupware Connectors aus und klicken auf Entfernen.



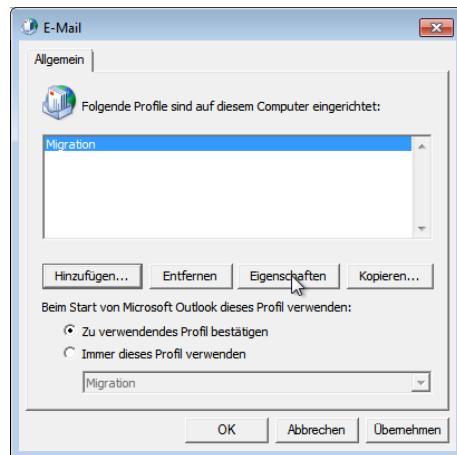
- Fügen Sie ein neues Profil hinzu. Dieses wird nur temporär für die Migration verwendet und danach wieder gelöscht.
- Geben Sie dem neuen Profil einen Namen, z.B. **Migration**.



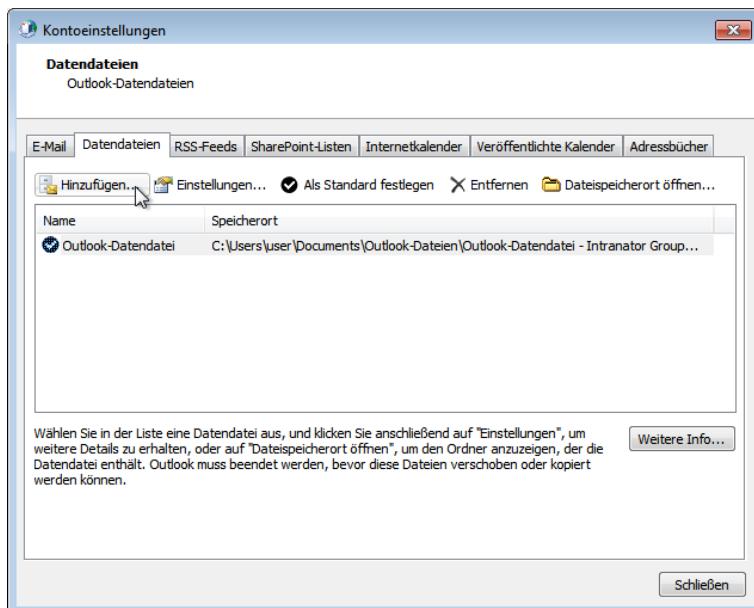
14. Brechen Sie den Assistenten zur Einrichtung eines Kontos ab und bestätigen, dass Sie ein Profil ohne E-Mail-Konto erstellen möchten.



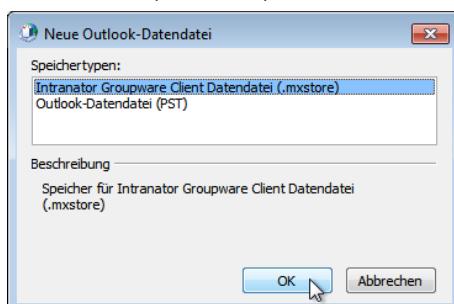
15. Markieren Sie das neue Profil und klicken auf Eigenschaften.



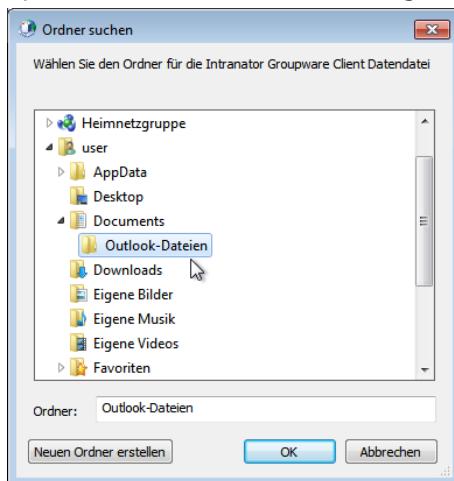
16. Wählen Sie Datendateien und fügen eine neue Datendatei hinzu.



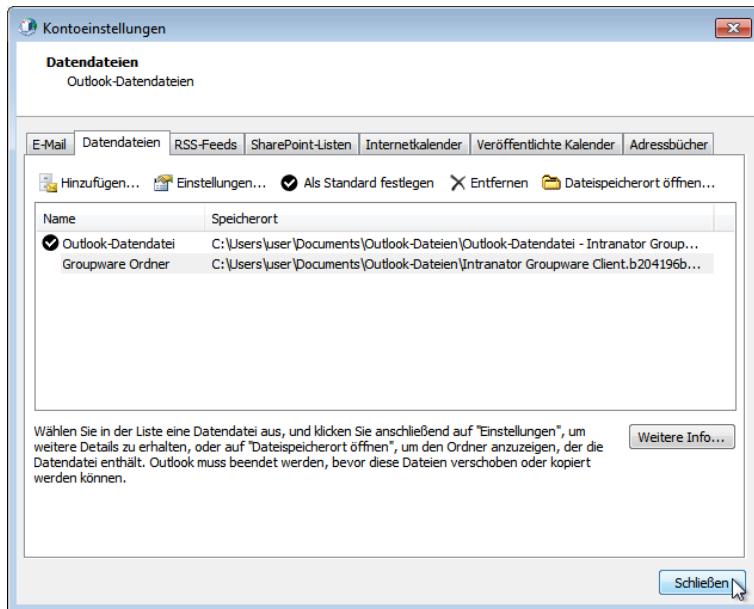
17. Wählen Sie als Speichertyp für die neue Datendatei Intranator Groupware Client Datendatei (.mxstore) aus.



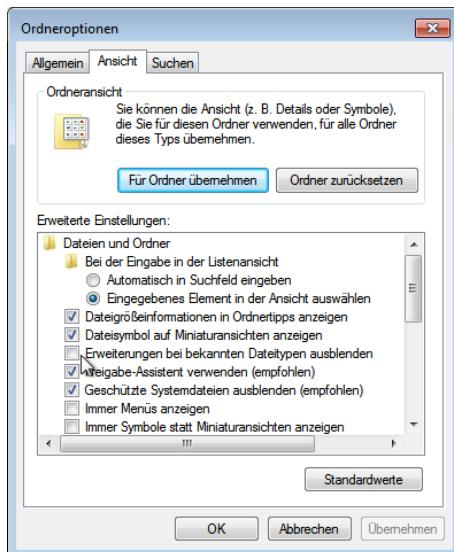
18. Wählen Sie den Speicherort für die neue Datendatei aus. Merken Sie sich diesen Speicherort, er wird in einem folgenden Schritt benötigt.



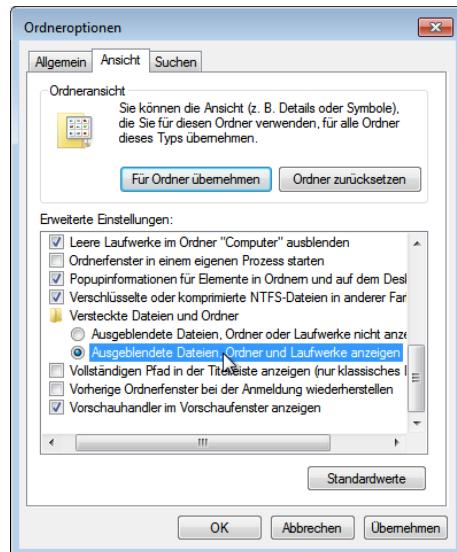
19. Wenn die neue Datendatei mit dem Namen Groupware Ordner angezeigt wird, können Sie die Kontoeinstellungen und die Systemsteuerung schließen.



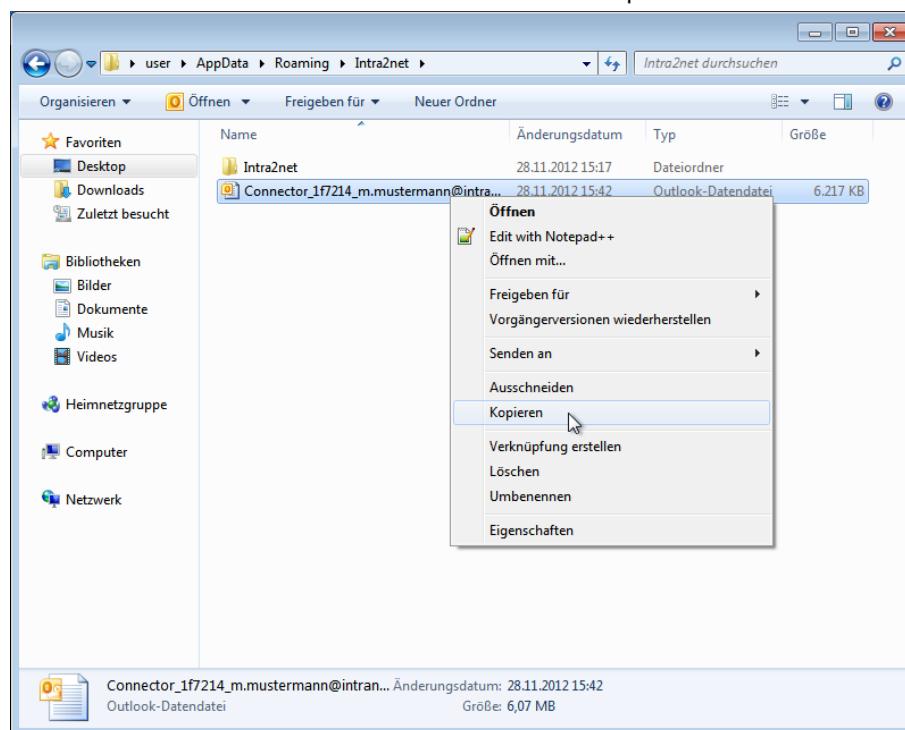
20. Öffnen Sie den Windows-Explorer und dort über das Menü die Ordner- und Suchoptionen.
21. Schalten Sie die Option Erweiterungen bei bekannten Dateitypen ausblenden ab.



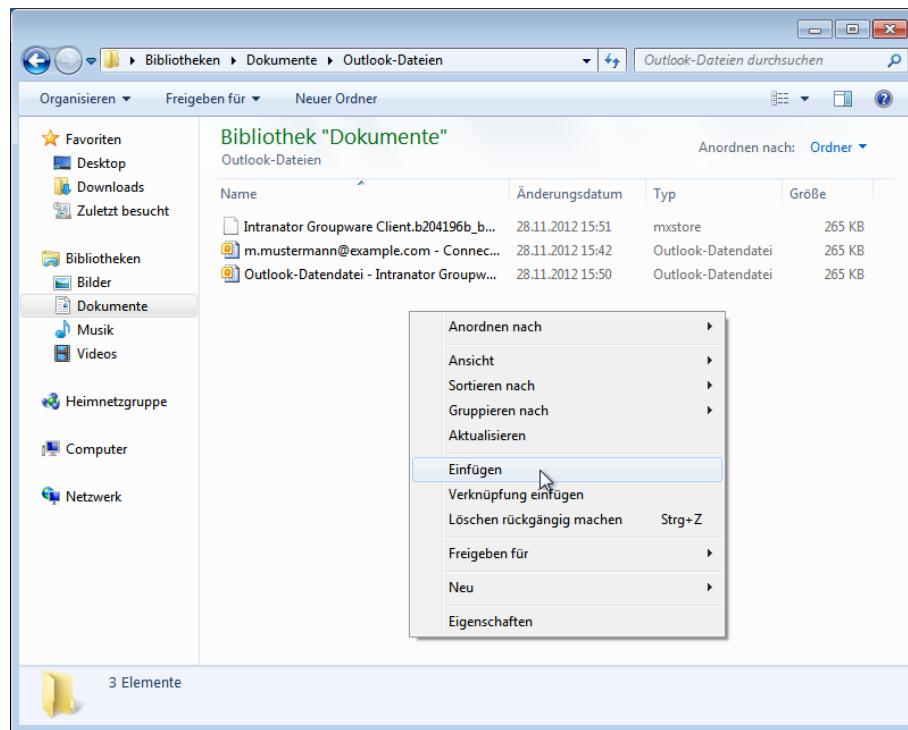
22. Lassen Sie ausgeblendete Dateien anzeigen



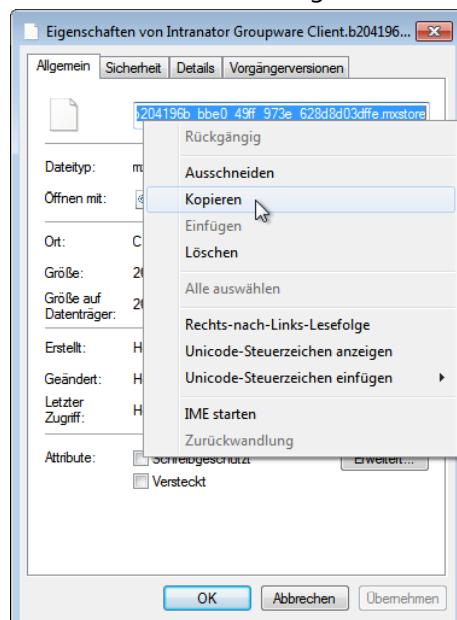
23. Navigieren Sie zum Speicherort der Outlook-Datendatei des bisherigen Groupware-Connector-Profil. Standardmäßig ist diese im Verzeichnis des Benutzers unter AppData\Roaming\Intra2net, bzw. Lokale Einstellungen\Anwendungsdaten\Intra2net zu finden.
24. Klicken Sie die Datei mit Rechts an und wählen Kopieren.



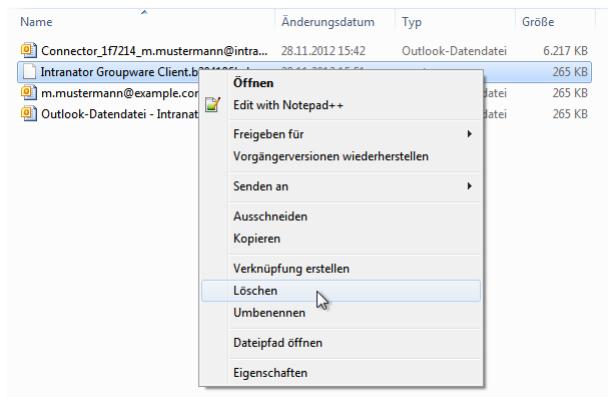
25. Navigieren Sie zum Speicherort, den Sie eben für die Outlook-Datendatei des Intra2net Groupware Clients gewählt haben.
26. Klicken Sie mit Rechts in einen leeren Bereich des Fensters und wählen Einfügen. Damit kopieren Sie die bisherige Datendatei an den neuen Speicherort. Gleichzeitig bleibt am alten Speicherort eine Sicherheitskopie der Datendatei bestehen.



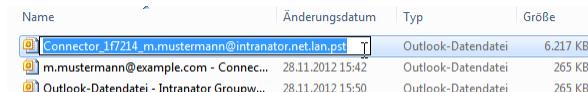
27. Klicken Sie die Datendatei des neuen Profils mit Rechts an. Sie erkennen die Datei am Typ `mxstore` und dem Dateinamen, der mit dem Namen des Profils beginnt. Wählen Sie Eigenschaften.
28. Markieren Sie den vollständigen Dateinamen inkl. der Endung `.mxstore`. Klicken Sie mit Rechts in den Dateinamen und wählen Kopieren. Der vollständige Dateiname ist nun in der Zwischenablage.



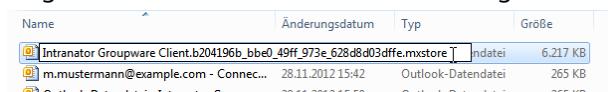
29. Löschen Sie die Datendatei des neuen Profils.



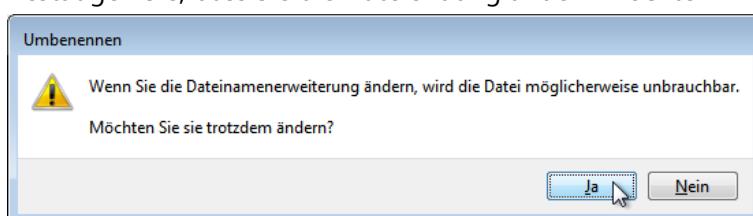
30. Klicken Sie mit Rechts auf die Datendatei des bisherigen Profils und wählen Umbenennen.
31. Markieren Sie den vollständigen Dateinamen der Datei, inkl. der Endung .pst. Sollte die Endung nicht angezeigt werden, müssen Sie Schritt 21 wiederholen.



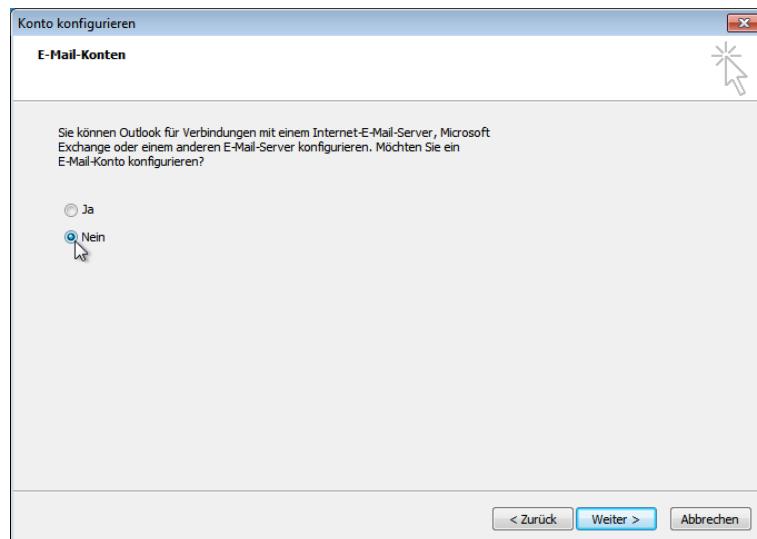
32. Überschreiben Sie den Dateinamen der alten Datendatei mit dem Namen der neuen Datendatei. Übernehmen Sie dazu den Namen aus der Zwischenablage in dem Sie Strg+V drücken. Damit erhält die bisherige Datendatei den Namen der neuen.



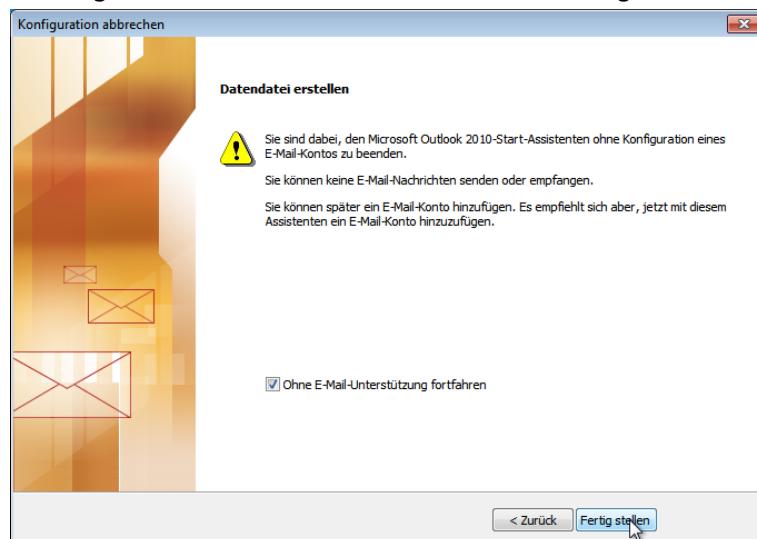
33. Bestätigen Sie, dass Sie die Dateiendung ändern möchten.



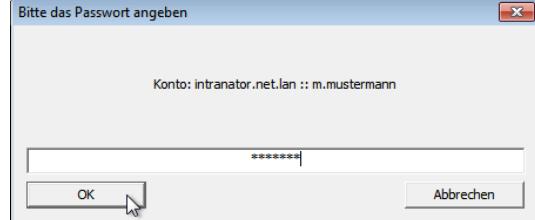
34. Starten Sie nun Outlook mit dem neuen Profil.
35. Bei Outlook 2010 erscheint nun ein Assistent zur Konfiguration. Gehen Sie auf Weiter und wählen, dass Sie kein E-Mail-Konto konfigurieren möchten.



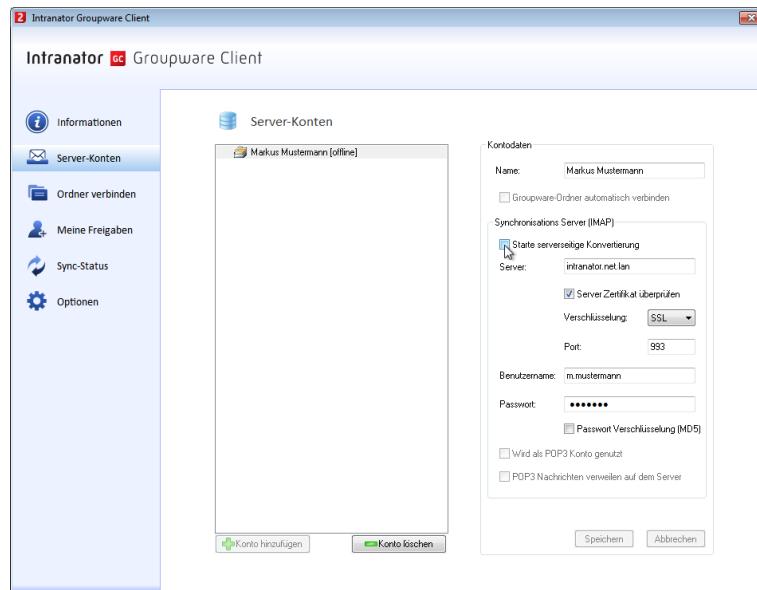
36. Bestätigen Sie, dass Sie ohne E-Mail-Unterstützung fortfahren wollen.



37. Der Konvertierungsassistent fragt Sie nun schrittweise, ob Sie die nötigen Voraussetzungen für die Konvertierung aus den vorigen Schritten geschaffen haben. Starten Sie die Konvertierung, wenn Sie so weit sind.
38. Geben Sie das Passwort des Benutzers auf dem Intranator Server ein.



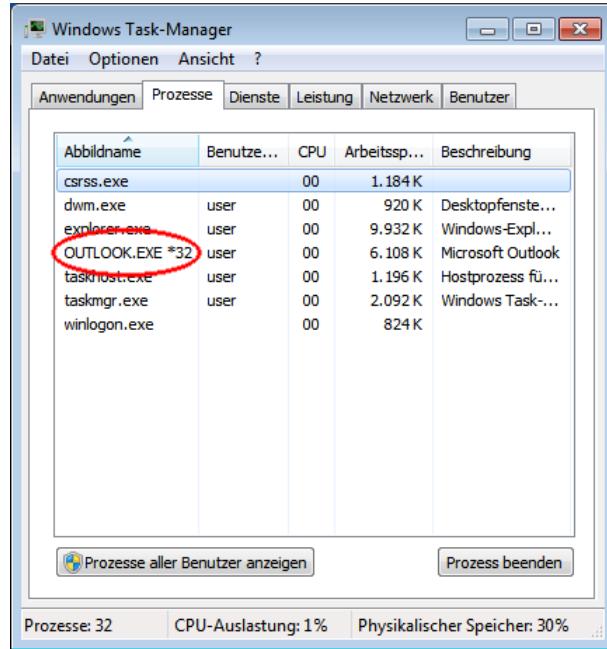
39. Es startet die lokale Konvertierung der Daten. Sobald dies abgeschlossen ist, öffnet sich die Oberfläche des Intra2net Groupware Clients. Prüfen Sie hier die Konfiguration des Kontos auf dem Server.
40. Ist die Konfiguration korrekt, so können Sie die serverseitige Konvertierung durch das Anklicken der Checkbox 'Starte serverseitige Konvertierung' anstoßen.



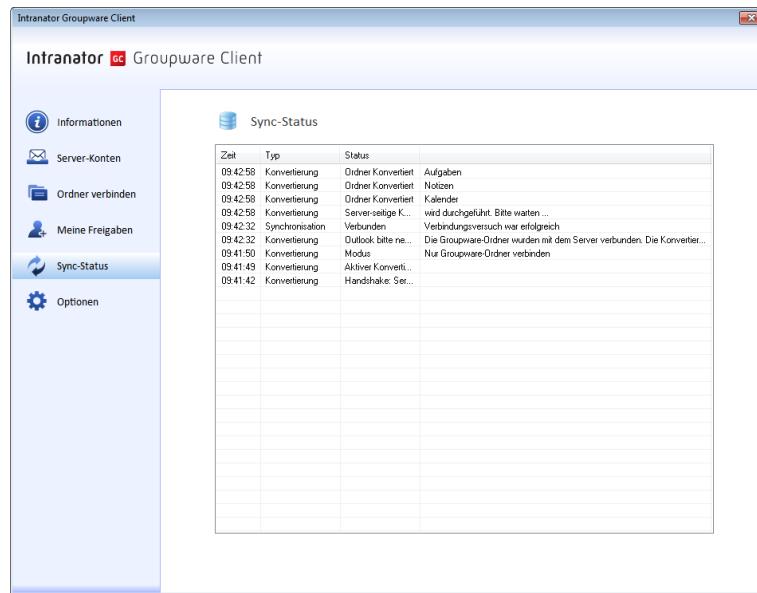
- Nach dem Start der serverseitigen Konvertierung werden Sie aufgefordert, Outlook neu zu starten.

Beenden Sie dazu Outlook. Warten Sie dann, bis sich Outlook vollständig beendet hat. Dies kann bis zu einer Minute dauern. Kontrollieren Sie am besten über den Task-Manager von Windows, dass kein Prozess namens OUTLOOK.EXE mehr läuft. Starten Sie erst dann Outlook neu.

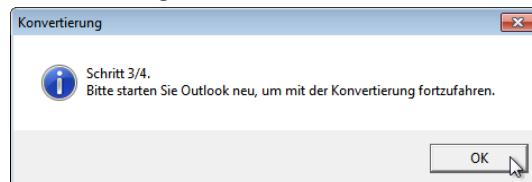
Beachten Sie diese Vorgehensweise bitte auch bei den folgenden Schritten.



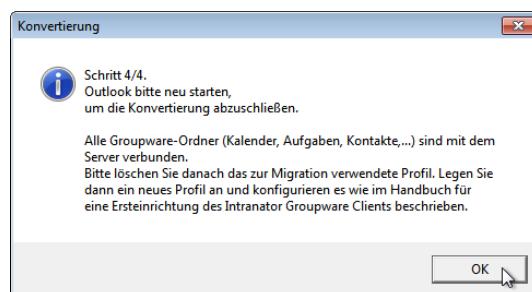
- Nach einem weiteren Neustart öffnet sich die Oberfläche des Intra2net Groupware Clients mit dem Menü Sync-Status. Es wird jetzt Ordner für Ordner auf den Server synchronisiert. Alle fertig konvertierten Ordner werden hier aufgeführt.



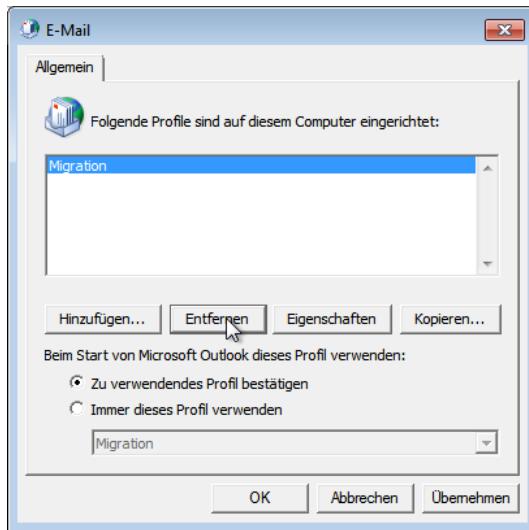
43. Warten Sie bis alle Ordner konvertiert sind. Sie werden dann zum Neustart von Outlook aufgefordert.



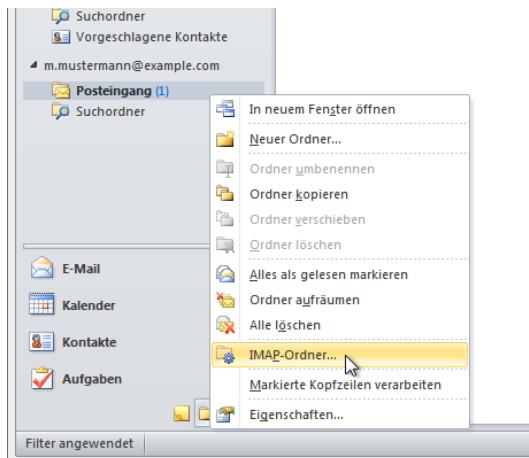
44. Nach einem weiteren Neustart von Outlook ist die Konvertierung abgeschlossen. Alle Groupware-Ordner wurden mit dem Konto auf dem Server verbunden, nicht aber die E-Mail-Ordner.



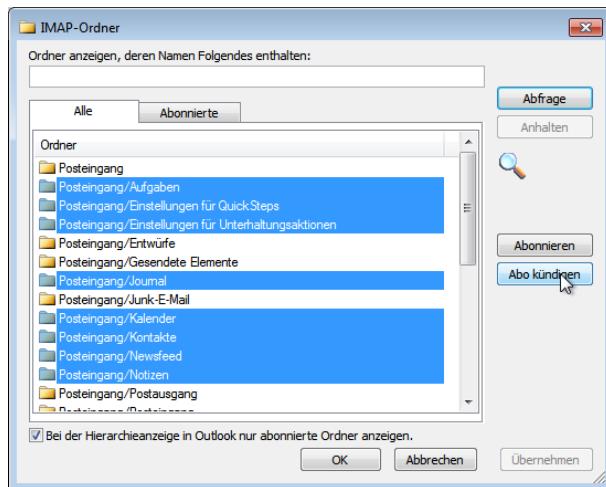
45. Beenden Sie Outlook, warten bis der Prozess wirklich beendet ist und starten es neu.
46. Warten Sie bis Outlook vollständig gestartet ist und schließen es wieder.
47. Öffnen die Windows-Systemsteuerung, Menü E-Mail (32 Bit). Lassen Sie sich die Profile anzeigen.
48. Das für die Migration verwendete Outlook-Profil wird nun nicht mehr benötigt. Löschen Sie es daher.



49. Legen Sie ein neues Profil an und konfigurieren es für den Groupware Client. Die dafür nötigen Schritte werden in Abschnitt 19.4, „Grundkonfiguration mit Outlook 2010“, bzw. für andere Versionen von Outlook in den anderen Abschnitten des selben Kapitels, erklärt.
50. Konfigurieren Sie das Konto für den Groupware Client wie in Abschnitt 20.1, „Groupware-Konto“ erklärt. Der Groupware Client beginnt danach automatisch, die Ordner mit Groupware-Daten vom Server zu synchronisieren.
51. Die Groupwareordner sind nun noch parallel im E-Mail-Konto abonniert und können Verwirrung beim Benutzer stiften. Diese Abos werden daher in den folgenden Schritten gekündigt.
52. Klicken Sie mit der rechten Maustaste auf den Posteingang des direkt von Outlook verwalteten IMAP-Kontos in der Ordnerliste. Es öffnet sich ein Kontextmenü. Wählen Sie dort IMAP-Ordner...



53. Klicken Sie auf Abfrage, um eine Liste aller verfügbaren Ordner vom Server abzurufen.
54. Markieren Sie alle Groupware-Ordner (wie z.B. Kalender, Kontakte, Notizen, etc.) und klicken auf Abo kündigen.



55. Öffnen Sie die Oberfläche des Intra2net Groupware Clients mit dem Menü Meine Freigaben. Gehen Sie Ordner für Ordner durch und kontrollieren, ob die Zugriffsrechte korrekt gesetzt sind. Korrigieren Sie diese bei Bedarf.
56. Sie können nun die freigegebenen Ordner anderer Benutzer wieder verbinden. Die dafür nötigen Schritte finden Sie in Abschnitt 21.2, „Fremde Ordner verbinden“ erklärt.

Wird dasselbe Konto auf dem Server auf verschiedenen Rechnern mit Outlook verwendet, können Sie nun die anderen Rechner umstellen. Konvertieren Sie auf diesen Rechnern nicht das Konto erneut wie hier beschrieben, da dies zu Duplikaten führen kann. Richten Sie dort stattdessen ein neues Profil für den Intra2net Groupware Client ein und laden die Daten vom Server.

24.3. Die manuelle Migration

24.3.1. Überblick

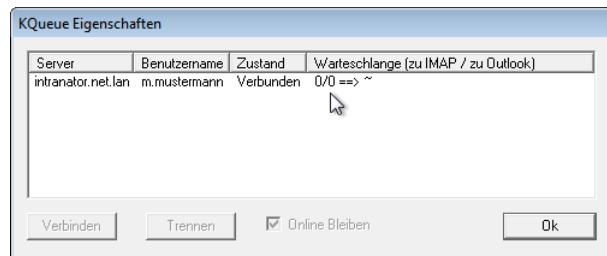
Hier ein grober Überblick darüber, wie die manuelle Migration vor sich geht. Die einzelnen Schritte werden im folgenden Abschnitt ausführlich erklärt.

- Mit Hilfe des alten Groupware Connector die bestehenden Daten vollständig mit dem Server synchronisieren.
- Ein Backup der Daten auf Client und Server erstellen.
- Den alten Groupware Connector deinstallieren, den neuen Intra2net Groupware Client installieren.
- Ein Profil für den neuen Groupware Client einrichten.
- Löschen aller Ordner mit Aufgaben-, Kontakt- und Kalenderdaten über das direkt von Outlook verwaltete IMAP-Konto.
- Die Datendatei des alten Groupware Connectors in Outlook zusätzlich öffnen.
- Die Ordner mit Aufgaben-, Kontakt- und Kalenderdaten per Drag & Drop in die Datendatei des Groupware Clients verschieben.

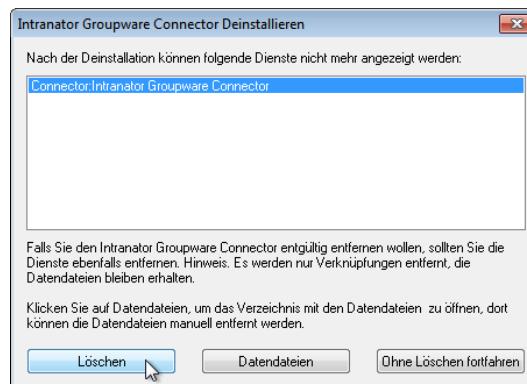
- Abonnements von Groupwareordnern im direkt von Outlook verwalteten IMAP-Konto aufräumen; Kontrolle der Freigaben an andere Benutzer.

24.3.2. Die Migration in einzelnen Schritten

1. Öffnen Sie Outlook mit dem Profil des Groupware Connectors. Öffnen Sie die KQueue im Infobereich der Taskleiste und lassen sich den Zustand der Warteschlange anzeigen. Die Warteschlange muss leer sein (Anzeige: 0 / 0), bevor Sie fortfahren können.



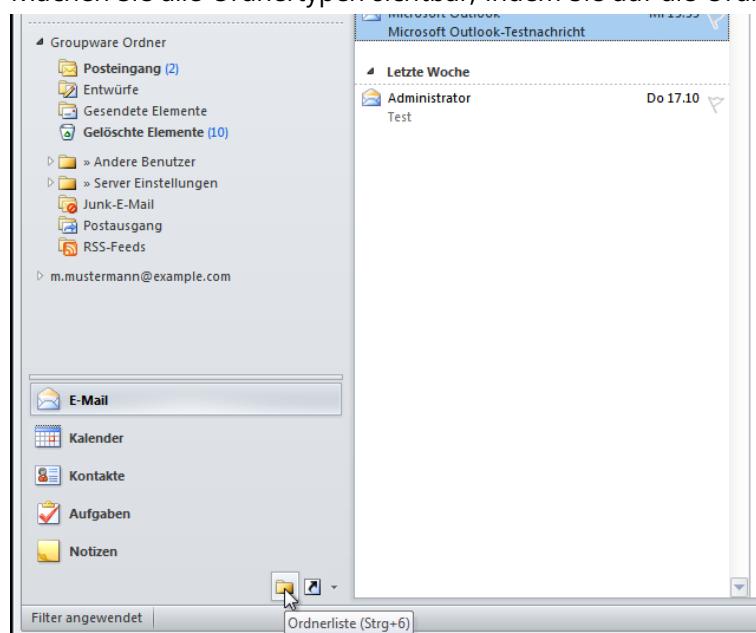
2. Schließen Sie Outlook.
3. Erstellen Sie eine Sicherheitskopie der Outlook-Datendatei des bisherigen Groupware-Connector-Profil. Standardmäßig ist diese im Verzeichnis des Benutzers unter AppData\Roaming\Intra2net, bzw. Lokale Einstellungen\Anwendungsdaten\Intra2net, zu finden.
4. Kontrollieren Sie, dass Sie über ein aktuelles Backup der Daten auf dem Intranator Server verfügen. Wenn nicht, so holen Sie dies über das Menü System > Backup > Einstellungen nach und warten, bis auf der Hauptseite nicht mehr angezeigt wird, dass das Backup momentan erstellt wird.
5. Stellen Sie sicher, dass das Konto dieses Benutzers von nun an nicht mehr mit dem Groupware Connector verwendet wird. Dies gilt auch für die Verwendung durch andere Benutzer über freigegebene Ordner.
6. Öffnen Sie die Windows-Systemsteuerung, Menü Programme, bzw. Programme und Funktionen.
7. Markieren Sie den Intranator Groupware Connector und wählen Deinstallieren.
8. Im Laufe der Deinstallation werden Sie aufgefordert den Outlook-Dienst des Groupware Connectors zu löschen. Markieren Sie den Dienst und klicken auf Löschen.



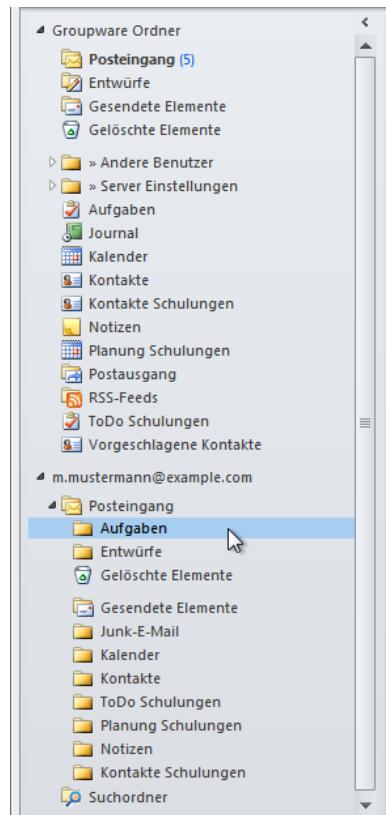
9. Fahren Sie mit der Deinstallation fort, lassen Sie die Datendateien bestehen wie sie sind.



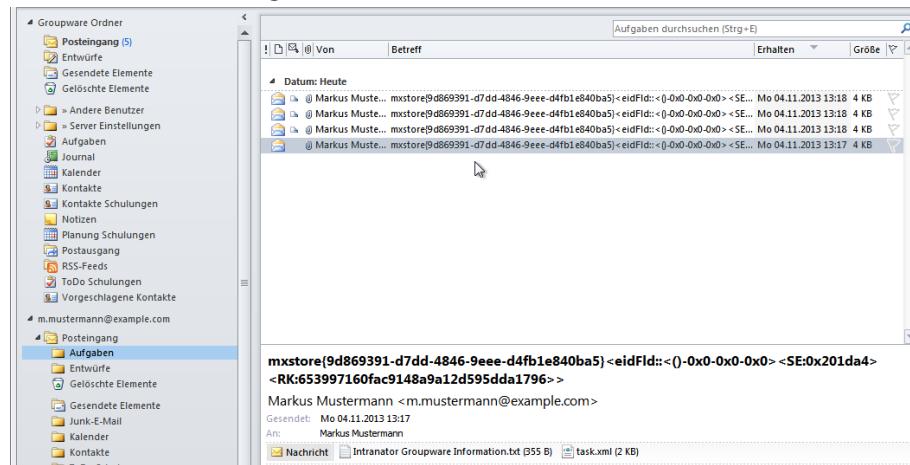
10. Installieren Sie nun den Intra2net Groupware Client, falls Sie dies noch nicht getan haben.
11. Legen Sie ein neues Outlook-Profil an und konfigurieren es für den Groupware Client. Die dafür nötigen Schritte werden in Abschnitt 19.4, „Grundkonfiguration mit Outlook 2010“, bzw. für andere Versionen von Outlook in den anderen Abschnitten des selben Kapitels, erklärt.
12. Konfigurieren Sie das Konto für den Groupware Client wie in Abschnitt 20.1, „Groupware-Konto“ erklärt. Der Groupware Client beginnt danach automatisch die Ordner mit Groupware-Daten vom Server zu synchronisieren.
13. Machen Sie alle Ordnerarten sichtbar, indem Sie auf die Ordnerliste umschalten.



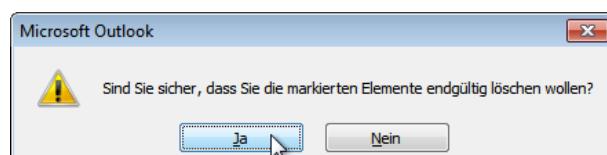
14. Öffnen Sie den Ordner Aufgaben. Allerdings nicht den normalen Aufgaben-Ordner unterhalb von Groupware Ordner, sondern den Aufgaben-Ordner unterhalb von Posteingang im direkt von Outlook verwalteten IMAP-Konto (normalerweise mit der E-Mail-Adresse benannt).



15. Kontrollieren Sie, dass keine normalen Aufgaben angezeigt werden, sondern nur E-Mails mit langen, unverständlichen Zeichenketten als Betreff. Ansonsten haben Sie den falschen Ordner geöffnet.



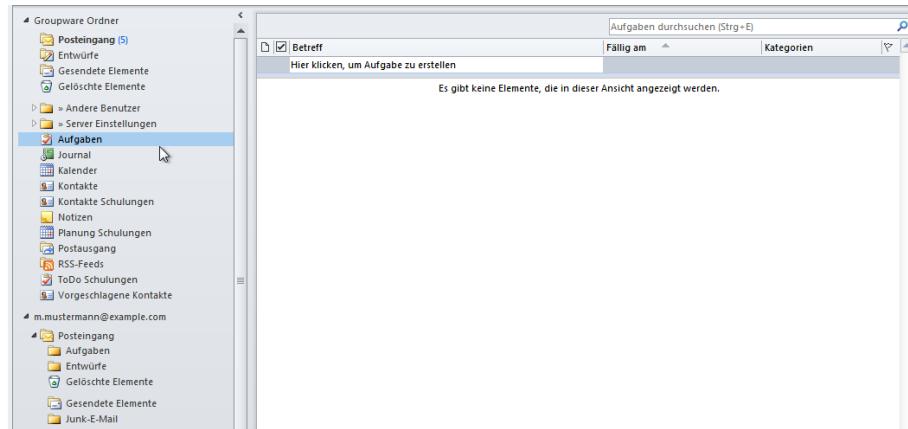
16. Markieren Sie alle E-Mails und löschen diese. Verwenden Sie zum Löschen Shift+Entf, um den Löschvorgang zu beschleunigen. Bestätigen Sie, dass Sie die E-Mails endgültig löschen wollen. Löschen Sie nur den Inhalt des Ordners, lassen aber den Ordner selbst bestehen.



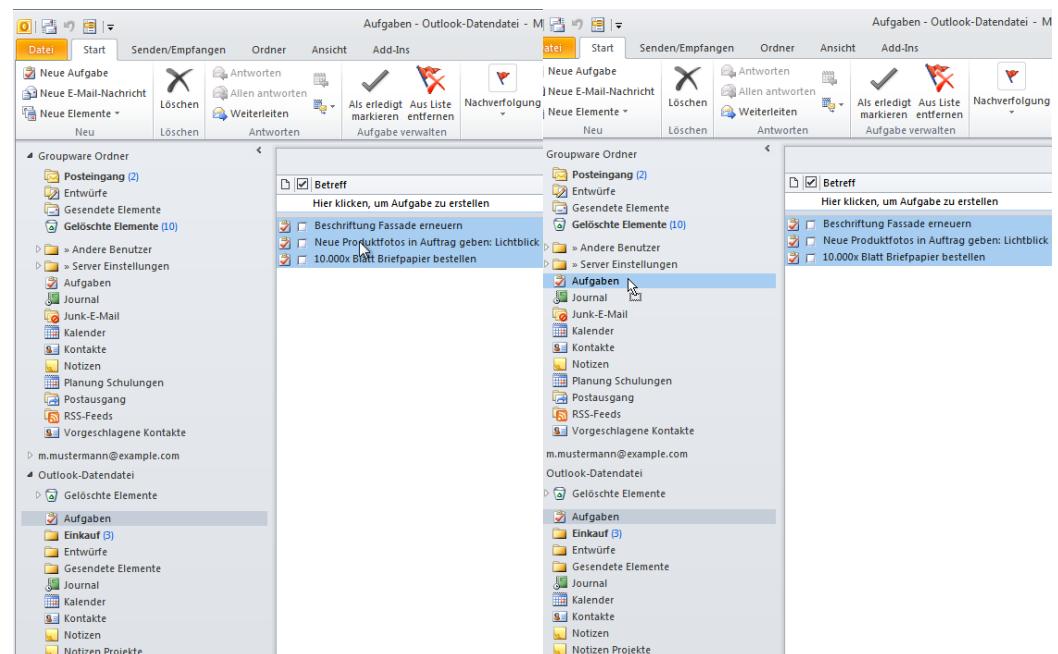
17. Werden alle E-Mails nun durchgestrichen dargestellt, wurden sie bisher nur zum Löschen markiert. Über das Menü Bearbeiten > Gelöschte Nachrichten permanent

löschen können Sie auf dem Server endgültig gelöscht werden. Dieser Schritt betrifft primär Outlook 2003.

18. Öffnen Sie nun den normalen Aufgaben-Ordner unterhalb von Groupware Ordner. Warten Sie, bis keinerlei Einträge mehr angezeigt werden.

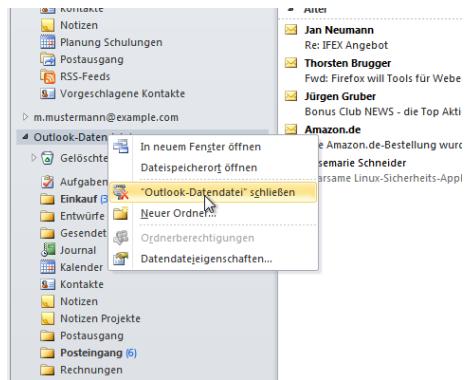


19. Wiederholen Sie die vorigen 5 Schritte für alle Ordner mit Aufgaben-, Kalender- und Kontaktdata.
20. Öffnen Sie in Outlook das Menü Datei > Öffnen > Outlook-Datendatei öffnen (ab Outlook 2010), bzw. Datei > Öffnen > Outlook-Datendatei (frühere Versionen).
21. Wählen Sie die Datendatei des alten Groupware Connectors aus.
22. Öffnen Sie den Aufgaben-Ordner in der eben geöffneten Datendatei.
23. Markieren Sie alle Elemente und verschieben sie per Drag & Drop in den Aufgaben-Ordner des Groupware Clients (unterhalb von Groupware Ordner).



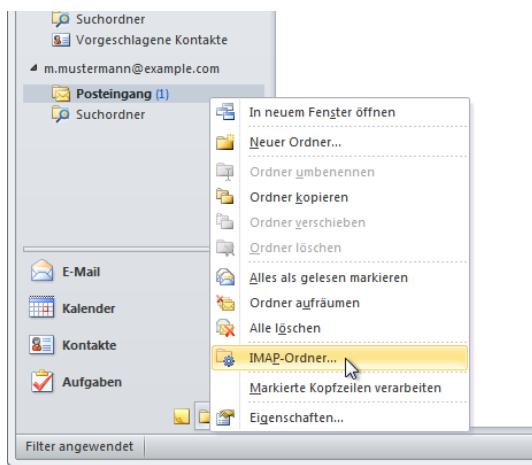
24. Wiederholen Sie dies für alle Ordner, die für Aufgaben, Kalender und Kontakte verwendet werden. Um alle Kalendereinträge markieren zu können, verwenden Sie die Listenansicht (Menü Ansicht > Ansicht ändern > Liste).

25. Schließen Sie nun die Datendatei des alten Groupware Connectors. Klicken Sie dazu mit der rechten Maustaste auf den Wurzelordner der Datendatei und wählen Outlook-Datendatei schließen.



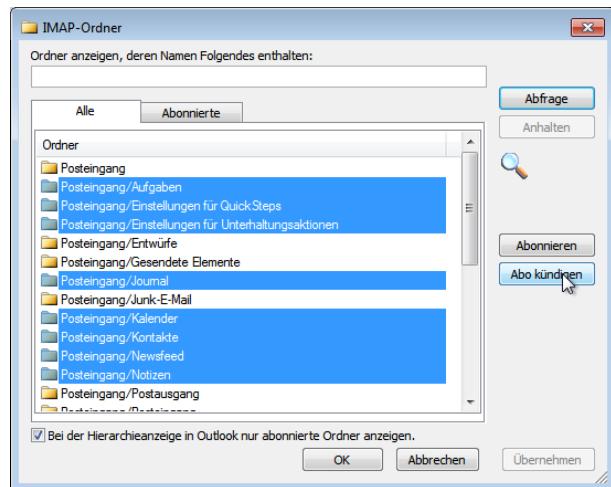
26. Die Groupwareordner sind nun noch parallel im E-Mail-Konto abonniert und können Verwirrung beim Benutzer stiften. Diese Abos werden daher in den folgenden Schritten gekündigt.

27. Klicken Sie mit der rechten Maustaste auf den Posteingang des direkt von Outlook verwalteten IMAP-Kontos in der Ordnerliste. Es öffnet sich ein Kontextmenü. Wählen Sie dort IMAP-Ordner...



28. Klicken Sie auf Abfrage, um eine Liste aller verfügbaren Ordner vom Server abzurufen.

29. Markieren Sie alle Groupware-Ordner (wie z.B. Kalender, Kontakte, Notizen, etc.) und klicken auf Abo kündigen.



30. Öffnen Sie die Oberfläche des Intra2net Groupware Clients mit dem Menü Meine Freigaben. Gehen Sie Ordner für Ordner durch und kontrollieren, ob die Zugriffsrechte korrekt gesetzt sind. Korrigieren Sie diese bei Bedarf.
31. Sie können nun die freigegebenen Ordner anderer Benutzer wieder verbinden. Die dafür nötigen Schritte finden Sie in Abschnitt 21.2, „Fremde Ordner verbinden“ erklärt.

25. Kapitel - Referenzinformationen

25.1. Synchronisierbare Daten

Der Intra2net Groupware Client synchronisiert die folgenden Daten aus Outlook mit dem Server. Alle hier nicht aufgeführten Einstellungen und Daten können in Outlook lokal zwar verändert werden, aber nicht auf den Server synchronisiert werden. Sie sind daher für andere Benutzer nicht sichtbar und sind in einem Backup nicht enthalten.

25.1.1. Aufgaben

25.1.1.1. Unterstützte Elemente

- Betreff
- Kategorien
- Text/Inhalt (Nur Text)
- Erstellungsdatum
- Sensitivität und Privat-Markierung
- Fertiggestellt in %
- Bearbeitungsstatus: In Arbeit,...
- Reisekilometer
- Abrechnunginfo
- Gesamtaufwand
- Istaufwand
- Zuweisung
- Besitzer
- Fällig am
- Beginnt am
- Erinnerung
- Fälligkeit
- Organisierer
- Ersteller
- Priorität/Wichtigkeit
- Firma

- Serienaufgaben mit Ausnahme von Serien, bei denen die folgende Aufgabe in einem definierten Zeitraum nach Abschluss der vorangegangenen Aufgabe erstellt wird
- Erledigt am
- Nachverfolgung (nur ja/nein, kein Zeitbezug)

25.1.1.2. Nicht unterstützte Elemente

Ohne Gewähr auf Vollständigkeit. Im Zweifel werden nur die explizit als unterstützt aufgeführten Elemente unterstützt.

- Text/Inhalt (Formatierter Rich-Text)

25.1.2. Termine

25.1.2.1. Unterstützte Elemente

- Betreff
- Kategorien
- Text/Inhalt (Nur Text)
- Sensitivität und Privat-Markierung
- Busy-Status / Anzeigen als
- Start- und Endzeitpunkt, bzw. Ganztags
- Zeitzonen bei Start- und Endzeitpunkt
- Organisierer
- Ersteller
- Priorität
- Ort
- Erinnerung (mit nutzerspezifischer Zuordnung)
- Teilnehmer
- Terminserien mit Ausnahme von Serien, deren wiederholte Einzeltermine die Tagesgrenze in der gewählten Zeitzone überschreiten

Folgende Ausnahmen können für einzelne Termine von Serien verwendet werden:

- Löschen eines Einzelterms
- Geänderter Betreff
- Geänderter Text/Inhalt (Nur Text)
- Geänderter Ort

- Änderungen der Zeit am selben Kalendertag

25.1.2.2. Nicht unterstützte Elemente

Ohne Gewähr auf Vollständigkeit. Im Zweifel werden nur die explizit als unterstützt aufgeführten Elemente unterstützt.

- Text/Inhalt (Formatierter Rich-Text)
- Zusage-Status einzelner Teilnehmer
- Frei wählbare Zeitzonen: Es wird immer die aktive Zeitzone verwendet

Folgende Ausnahmen können für einzelne Termine von Serien nicht verwendet werden:

- Geänderte Teilnehmer
- Verschieben auf einen anderen Kalendertag
- Ausnahmetermine, die die Tagesgrenze in der gewählten Zeitzone überschreiten (Ende des Termins an einem anderen Kalendertag als der Start)

25.1.3. Notizen

25.1.3.1. Unterstützte Elemente

- Betreff
- Kategorien
- Text/Inhalt

25.1.4. Kontakte

25.1.4.1. Unterstützte Elemente

- Vollständiger Name
- Anrede
- Vorname
- Weitere Vornamen
- Nachname
- Namenszusatz
- Initialien
- Geburtstag
- Jahrestag
- Partner/in
- Spitzname

- Sensitivität und Privat-Markierung
- Firma
- Webseite
- FTP-Site
- IM-Adresse
- Abteilung
- Büro
- Beruf
- Position
- Vorgesetzter
- Assistent
- Kinder
- Sprache
- Abrechnungsinformationen
- Hobbies
- Kundennummer
- Organisationsnummer
- Sozialversicherungsnummer
- Reisekilometer
- E-Mail 1 bis E-Mail 3
- Adresse geschäftlich
- Adresse privat
- weitere Adresse
- Ort
- bevorzugte Postanschrift
- Kategorien
- Notiz (Nur Text)
- Nachverfolgung (nur ja/nein, kein Zeitbezug)
- Telefon geschäftlich (1 und 2)

- Telefon privat (1 und 2)
- Autotelefon
- Funkruf
- Haupttelefon
- Mobiltelefon
- Pager
- Tel. für Rückmeldung
- Telefon Assistent
- Telefonzentrale Firma
- Texttelefon
- Weiteres Telefon
- Fax geschäftl.
- Fax privat
- Weiteres Fax
- ISDN
- Telex
- Nutzerfeld 1 bis 4
- Benutzerdefinierte Felder, siehe dazu Abschnitt 22.13, „Benutzerdefinierte Felder in Kontakten“

25.1.4.2. Bilder

Kontakten kann ein Bild zugeordnet werden. Dabei werden folgende Bildformate (MIME-Typen) unterstützt:

- image/jpeg
- image/png
- image/bmp, image/x-bmp und image/x-ms-bmp
- image/gif
- image/tiff
- image/x-wmf
- image/x-emf
- image/x-icon

Beachten Sie, dass Outlook 2010 und älter in der Übersicht nur JPG-Bilder anzeigen, die anderen Bildformate werden nur beim Öffnen des Kontakts angezeigt. Ab Outlook 2013 werden die anderen Bildformate auch in der Personenansicht angezeigt.

Mit Outlook 2003 können keine Kontaktbilder auf den Server geschrieben werden. Wird ein Kontakt mit Bild unter Outlook 2003 geändert, so wird dabei das Bild entfernt.

25.1.4.3. Nicht unterstützte Elemente

Ohne Gewähr auf Vollständigkeit. Im Zweifel werden nur die explizit als unterstützt aufgeführten Elemente unterstützt.

- Frei/Gebucht-URL
- Zertifikate für die Verschlüsselung/Signierung von Nachrichten
- Versandoptionen für E-Mails (E-Mail-Adresstyp, Internetformat)
- Darstellungsoptionen der Visitenkarte
- Sortierbasis (Speichern unter)
- Notiz (Formatierter Rich-Text)

25.1.5. Kontaktgruppen

25.1.5.1. Unterstützte Elemente

- Name der Kontaktgruppe
- Anzeigename jedes Mitglieds
- E-Mail-Adresse jedes Mitglieds
- Notiz zur Kontaktgruppe (Nur Text)

25.1.5.2. Nicht unterstützte Elemente

Ohne Gewähr auf Vollständigkeit. Im Zweifel werden nur die explizit als unterstützt aufgeführten Elemente unterstützt.

- Faxnummer jedes Mitglieds
- Notiz zur Kontaktgruppe (Formatierter Rich-Text)

25.1.6. E-Mails



Hinweis

Dieser Abschnitt betrifft nur E-Mails, die über den Intra2net Groupware Client synchronisiert werden. Über die in Outlook integrierte IMAP-Funktion synchronisierte E-Mails unterliegen den Fähigkeiten der jeweiligen Version von Outlook. Weitere Informationen dazu finden Sie in der Dokumentation von Outlook.

25.1.6.1. Unterstützte Elemente

- Absender
- Empfänger
- CC
- BCC
- Betreff
- Sendezeitpunkt
- Empfangszeitpunkt
- Wichtigkeit
- Internetkopfzeilen
- Inhalt (Nur Text und Formatierter Rich-Text)
- Dateianhänge
- Kategorien
- Nachverfolgung (nur ja/nein, kein Zeitbezug)

25.1.6.2. Nicht unterstützte Elemente

Ohne Gewähr auf Vollständigkeit. Im Zweifel werden nur die explizit als unterstützt aufgeführten Elemente unterstützt.

- Erinnerungen

25.1.7. Alle Objekte

Generell können folgende Elemente mit dem Intra2net Groupware Client nicht synchronisiert werden:

- Auto-Archivierung deaktivieren
- Anfügen anderer Outlook-Elemente oder Dateien
- Verknüpfung mit Kontakten

25.2. Erweiterte Einstellungen in der Registrierung

Der Intra2net Groupware Client kann über folgende Einstellungen in der Windows-Registry weiter angepasst werden.

Alle Registry-Keys sind auf 32-Bit Betriebssystemen unterhalb von `HKLM\SOFTWARE\Intra2net AG\Intranator Groupware Client` und auf 64-Bit Betriebssystemen unter `HKLM\SOFTWARE\Wow6432Node\Intra2net AG\Intranator Groupware Client` zu finden.

Wurde der Intra2net Groupware Client nur für einen Benutzer installiert, wird statt HKLM der entsprechende Schlüssel unterhalb von HKCU verwendet.

25.2.1. Einstellungen für den Store

Die Einstellungen für den Store sind im Schlüssel `mxstore_Store` zu finden.

Eintrag	Standardwert	Erklärung
DelayNonStandardFolders	0x00000000	Ist diese Option aktiv, wird die Synchronisation von allen Ordnern außer den Standardordnern von Outlook (Posteingang, Kalender, Kontakte,...) verlangsamt. Der Benutzer bekommt dadurch neue Elemente in den Standardordnern schneller angezeigt.
SkipPrc	SearchProtocolHost.exe	Dateinamen von Prozessen, deren Zugriffe nicht protokolliert werden um die Protokolldateien nicht unnötig zu vergrößern. Mehrere Einträge werden durch Semikolon getrennt angegeben.
Trace	0x00004800	Ist das Tracing von normalen Vorgängen aktiv, so werden hierüber die zu protokollierenden Ereignisse ausgewählt. Weitere Informationen erhalten Sie bei Bedarf über unseren Support.
TraceAttr	0x0000001b	Auswahl der Spalten, die bei einem zu protokollierenden Ereignis im Trace ausgegeben werden. Weitere Informationen erhalten Sie bei Bedarf über unseren Support.
TracerDisabled	0x00000000	Hiermit wird ausgewählt, ob nur Starts und Fehler protokolliert werden (Wert 1) oder auch normale Vorgänge im Betrieb (Wert 0).
PathLog		Vollständiger Pfad, in dem die Tracedateien abgelegt werden. Ist dieser Eintrag nicht vorhanden, werden sie im <code>Eigene Dokumente</code> -Verzeichnis des Benutzers angelegt.
TrgMin_FldChanged	300	Kürzestes Intervall (in Sekunden), welches vom Benutzer bei den Updateintervallen für Ordner verändert eingestellt werden kann.
TrgMin_FldTreeChanged	300	Kürzestes Intervall (in Sekunden), welches vom Benutzer bei den Updateintervallen für Ordnerbaum verändert eingestellt werden kann.
TrgMin_MailChanged	60	Kürzestes Intervall (in Sekunden), welches vom Benutzer bei den Updateintervallen für Inhalt verändert eingestellt werden kann.
TrgDefault_FldChanged	2700	Standardintervall (in Sekunden) für Ordner verändert, wenn der Benutzer nichts anderes eingestellt hat.

Eintrag	Standardwert	Erklärung
TrgDefault_FldTreeChanged	2700	Standardintervall (in Sekunden) für Ordnerbaum verändert, wenn der Benutzer nichts anderes eingestellt hat.
TrgDefault_MailChanged	2700	Standardintervall (in Sekunden) für Inhalt verändert, wenn der Benutzer nichts anderes eingestellt hat.
TrgDefault_Always	0	Wenn 1, werden die mit den TrgDefault-Einträgen eingestellten Intervalle immer verwendet, unabhängig davon was der Benutzer eingestellt hat. Der Administrator kann so die Updateintervalle für den Benutzer fest vorgeben.
Trigger_Reset	0	Wenn 1, werden beim nächsten Start die Trigger-Einstellungen für alle Ordner auf die Standardwerte zurückgesetzt. Danach wird dieser Wert in der Registrierung wieder auf 0 zurückgesetzt.
CalPrivatePlaceholder_Default	1	<p>Wenn 1, werden bei anderen Nutzern für neu erstellte oder geänderte und als privat markierte Kalendereinträge Platzhalter angezeigt. Wenn 0, werden privat markierte Kalendereinträge bei anderen Nutzern komplett versteckt.</p> <p>Dieser Wert wird nur beim ersten Öffnen einer neuen Datendatei mit Outlook ausgelesen und in diese übernommen. Bestehende Datendateien werden von dieser Einstellung nicht beeinflusst.</p>
CalPrivatePlaceholder_ResetOnOpen	0	Wenn 1, wird die Einstellung von CalPrivatePlaceholder_Default nicht nur beim ersten Öffnen einer Datendatei übernommen, sondern bei jedem Start.
ServerAdminStructure_Forwarding		Wenn 0, wird die E-Mail-Weiterleitung unterhalb der Server Einstellungen ausgeblendet.
ServerAdminStructure_Vacation		Wenn 0, wird die Abwesenheitsschaltung unterhalb der Server Einstellungen ausgeblendet.
ServerAdminStructure_Sorting		Wenn 0, wird die Sortierung unterhalb der Server Einstellungen ausgeblendet.
ServerAdminStructure_Spamfilter		Wenn 0, wird die Spamfilter unterhalb der Server Einstellungen ausgeblendet.
MemLoad_SyncOff	90	Schwellwert in Prozent des gesamten Arbeitsspeichers. Ist mehr Arbeitsspeicher belegt, wird die Synchronisation temporär deaktiviert. Dies vermeidet Fehler durch zu

Eintrag	Standardwert	Erklärung
		knapp werdenden Arbeitsspeicher. Ein Wert von über 100 deaktiviert diese Funktion.
IMAP ID: ALLOW Send Id Info To Server	1	Wenn 1, sendet der Groupware Client grundsätzlich Informationen über die lokal installierte Version und den Rechner über das IMAP-ID-Kommando an den Server. Der Umfang der übertragenen Informationen hängt von den anderen IMAP_ID -Schlüsseln ab.
IMAP ID: Send ONLY Product Version	1	Wenn 1, sendet der Groupware Client mit dem IMAP-ID-Kommando nur Informationen über den Groupware Client selber, nicht aber über den Rechner
IMAP ID: Send ALL Plattform-Information	0	Wenn 1, sendet der Groupware Client mit dem IMAP-ID-Kommando Informationen über den Groupware Client, die Outlook-Version, das verwendete Betriebssystem sowie die Hardwareausstattung des Rechners
ACL_ChangeNotification	1	Wenn 1, bekommt der Benutzer einen Hinweis in den Posteingang, sobald sich Zugriffsrechte auf Ordner verändert haben. Mit dem Wert 0 wird diese Funktion abgeschaltet.
ACL_ChangeNotificationScope	5	Wählt die Art der Änderungen an Zugriffsrechten, über die der Benutzer informiert wird. Bitfeld, daher die Werte für die gewünschten Optionen addieren. 1 Hinweise für Ordner anderer Benutzer 2 Hinweise für eigene Ordner 4 Hinweise nur für Änderungen der eigenen Rechte
ACL_ChangeNotificationView	0	Wählt die Art der Darstellung in der der Benutzer auf neue Zugriffsrechte hingewiesen wird. 0 Vereinfachte Darstellung 1 Vollständige ACLs als Kurztext 4 Vollständige IMAP-ACLs als Buchstaben (RFC 4314)
KeepOutlookInboxName	0	Wenn 0, wird ein nicht verbundener Posteingangsordner in Meldungen umbenannt. Wenn 1, behält der Ordner auch in unverbundenem Zustand den Namen Postein-

Eintrag	Standardwert	Erklärung
		gang. Wird der Ordner mit dem Server verbunden, ist er unabhängig von dieser Option immer Posteingang benannt.
SyncTemplatesFilePath	Installationsordner des Groupware Clients	Vollständigen Pfad des Ordners, aus dem die Datei <code>userdefined_sync_fields.xml</code> zur Definition benutzerdefinierter Felder geladen wird.
DoLastAuthorTagging	1	Wenn 1 wird der Benutzername des letzten Bearbeiters bei jedem Objekt als Kategorie hinterlegt.

25.2.2. Einstellungen für das Add-In

Die Einstellungen für das Outlook Add-In (GUI) sind im Schlüssel `mxstore_GUI` zu finden.

Eintrag	Standardwert	Erklärung
Trace	0x00004800	Ist das Tracing von normalen Vorgängen aktiv, so werden hierüber die zu protokollierenden Ereignisse ausgewählt. Weitere Informationen erhalten Sie bei Bedarf über unseren Support.
TraceAttr	0x0000001b	Auswahl der Spalten, die bei einem zu protokollierenden Ereignis im Trace ausgegeben werden. Weitere Informationen erhalten Sie bei Bedarf über unseren Support.
TracerDisabled	0x00000000	Hiermit wird ausgewählt, ob nur Starts und Fehler protokolliert werden (Wert 1) oder auch normale Vorgänge im Betrieb (Wert 0).
PathLog		Vollständiger Pfad in dem die Tracedateien abgelegt werden. Ist dieser Eintrag nicht vorhanden, werden sie im Eigene Dokumente-Verzeichnis des Benutzers angelegt.
AllowOnwRightsEdit	0x00000001	Ist diese Einstellung aktiv, so darf der Benutzer seine eigenen Rechte auf einen Ordner bearbeiten.
ShowAdvancedOptions	0x00000001	Ist diese Einstellung aktiv, so wird der Optionen-Dialog (u.a. zur Einstellung der Synchronisationshäufigkeit) angezeigt.

25.3. Datenformate

Alle Groupware-Objekte werden auf dem IMAP-Server als einzelne E-Mails abgelegt. Die Groupware-Daten werden dabei XML codiert und als Anhang in der E-Mail gespeichert.

Das verwendete XML-Format basiert dabei auf dem Kolab Storage Format Version 2.0. Die Definition dieses Formats ist zu finden unter <http://www.intra2net.com/de/download/handbuch/kolabformat-2.0.pdf>.

Zusätzlich werden vom Intra2net Groupware Client implementationsspezifische Daten als E-Mail-Kopfzeilen abgelegt. Deren Namen beginnen mit `x-mxstore` sowie `x-Sync`. Das Format dieser Kopfzeilen kann sich jederzeit ohne Ankündigung ändern. Diese Kopfzeilen sollten daher nicht von anderer Software interpretiert werden.

Teil 4. Web-Groupware und ActiveSync

26. Kapitel - Einführung in die Web-Groupware

Die Web-Groupware ermöglicht es, mit einem gewöhnlichen Webbrower auf E-Mails und Groupwaredaten wie Kalender, Aufgaben, Kontakte und Notizen zuzugreifen.

Sie ist auf der Intranator Oberfläche über das Menü Groupware erreichbar. Beim Zugriff aus dem Internet ohne das Recht Fernadministration über HTTPS (Menü Benutzermanager > Gruppen : Administrationsrechte) öffnet sie sich direkt nach dem Login.

26.1. Die Anzeigemodi

Die Web-Groupware kann in verschiedenen Anzeigemodi verwendet werden. Diese sind für unterschiedliche Browser und Endgeräte optimiert:

Dynamisch	Für aktuelle Browser. Hoher Bedienkomfort durch AJAX und dynamische Aktualisierung im Hintergrund.
Klassisch	Maximale Kompatibilität mit einfachen oder älteren Browsern. Bietet nicht alle Funktionen des Dynamischen Anzeigemodus.
Smartphone	Optimiert für Smartphones und Tablets mit Touch-Bedienung. Übersichtliche Darstellung auch auf kleinen Bildschirmen. Adressen und Kalendereinträge können momentan nur angezeigt werden.

Beim Login auf dem Intranator kann man auswählen, welchen Anzeigemodus man verwenden möchte. Standardmäßig versucht der Intranator anhand der Browserkennung automatisch den am besten passenden Anzeigemodus zu ermitteln (Einstellung Automatisch).

Die folgende Dokumentation bezieht sich auf den dynamischen Modus.

27. Kapitel - E-Mail

27.1. E-Mails lesen und bearbeiten

27.1.1. E-Mails anzeigen

Unter dem Menüpunkt Webmail findet sich in der Web-Groupware die Möglichkeit, E-Mails zu lesen, zu schreiben und zu bearbeiten.

The screenshot shows the Intranator Webmail interface. On the left is a sidebar with navigation links like 'Neue Nachricht', 'Posteingang', 'Entwürfe', 'Ordneraktionen', 'Bestellungen', 'Gesendete Elemente', 'Projekte', 'Fischer', 'Hollmann&Schmidt', 'Müller KG', 'Virtuelle Ordner', and 'Virtueller Posteingang'. The main area has tabs for 'Webmail', 'Kalender', 'Adressbuch', 'Aufgaben', 'Notizen', and 'Hauptseite'. A search bar at the top right says 'Suche (Gesamte Nachricht)' with a magnifying glass icon. Below it, a table lists emails with columns for 'Von', 'Betreff', 'Datum', and 'Größe'. One email from 'Markus Mustermann' is selected. The right side shows the detailed view of this email, including the recipient ('Von: Markus Mustermann'), date ('Datum: Di, 10.05.2011 (11:26:30 CET)'), and subject ('An: info@intra2net.com'). The email body contains a greeting, an order summary, and a closing note. There are buttons for 'Text-Nachrichtenteil (2 KB)', 'Download', and 'Print'.

In der E-Mail-Liste des aktuellen Ordners können die einzelnen E-Mails mit der rechten Maustaste angeklickt werden. Es öffnet sich ein Kontextmenü, welches Funktionen zum Löschen, Weiterleiten und Markieren von E-Mails bietet.

E-Mails können aus der E-Mail-Liste per Drag&Drop in einen anderen Ordner verschoben werden.

This screenshot shows the same Intranator Webmail interface as above, but with a different focus. A mouse cursor is hovering over the 'Bestellungen' folder in the sidebar. An arrow points from the 'Bestellungen' folder to the 'Markus Mustermann' email in the list, indicating that the email is being moved. The context menu options '1 Nachricht nach Bestellungen verschieben' and 'Bestellungen' are visible near the cursor. The rest of the interface remains the same, showing the email details and body.

27.1.2. Gelöschte E-Mails

E-Mails werden durch den Löschbefehl in den Papierkorb verschoben.

Soll eine gelöschte E-Mail wiederhergestellt werden, so kann Sie ganz normal per Drag&Drop aus dem Papierkorb wieder in den richtigen Ordner zurück verschoben werden.

Der Papierkorb kann automatisch nach einiger Zeit vom System aufgeräumt werden (Menü Benutzermanager > Benutzer : Groupware), standardmäßig geschieht dies nach 30 Tagen. Alternativ kann der komplette Papierkorb über den Befehl Leeren im Kontextmenü des Papierkorbs (Rechtsklick auf den Ordnernamen) manuell aufgeräumt werden.

Einige E-Mail-Clients (z.B. Mozilla Thunderbird und Outlook 2003) verschieben gelöschte E-Mails nicht in den Papierkorb, sondern lassen sie im Ursprungsordner liegen und versehen Sie mit einer Löschmarkierung. Je nach Programm werden die E-Mails dann automatisch beim Beenden des Programms oder nur auf manuellen Befehl hin endgültig gelöscht (IMAP Expunge).

Aktualisieren			Sonstige ▾	Filter ▾
Von	Betreff	Datum	Größe	
Anna Sommer	Nicht im Büro / Out of the office.	04.01.2011	3 KB	
1&1 Partner Team	1&1 DSL Premium-Tarife bieten deutlich mehr!	07.01.2011	4 KB	
Faxserver	FAX von +497071159270	09.04.2011	25 KB	
<input checked="" type="checkbox"/>  christine.richter@heise.de	IX kompakt - Das große Speicherheft	11.04.2011	691 KB	
<input checked="" type="checkbox"/>  European_Media_Servic...	Danke für Ihre Bestellung durch European_Media_Service über Amazon.de	06.04.2011	8 KB	

Sie können die so markierten E-Mails mit der Webgroupware endgültig löschen oder ausblenden. Diese Funktionen finden Sie im Menü Sonstige.

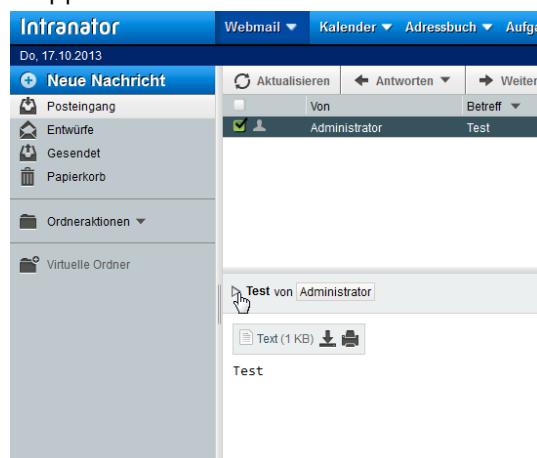
Aktualisieren			Sonstige ▾	Filter ▾
Von	Betreff	Vorschau ausblenden	Vertikales Layout	
Anna Sommer	Nicht im Büro / Out of the office.	<input type="checkbox"/>	<input type="checkbox"/>	
1&1 Partner Team	1&1 DSL Premium-Tarife bieten deutlich mehr!	<input type="checkbox"/>	<input type="checkbox"/>	
Faxserver	FAX von +497071159270	<input type="checkbox"/>	<input type="checkbox"/>	
<input checked="" type="checkbox"/>  christine.richter@heise.de	IX kompakt - Das große Speicherheft	<input type="checkbox"/>	 Endgültig löschen	
<input checked="" type="checkbox"/>  European_Media_Servic...	Danke für Ihre Bestellung durch European_Media_Service über Amazon.de	<input type="checkbox"/>	<input type="checkbox"/> Wiederherstellen	

27.1.3. E-Mails exportieren

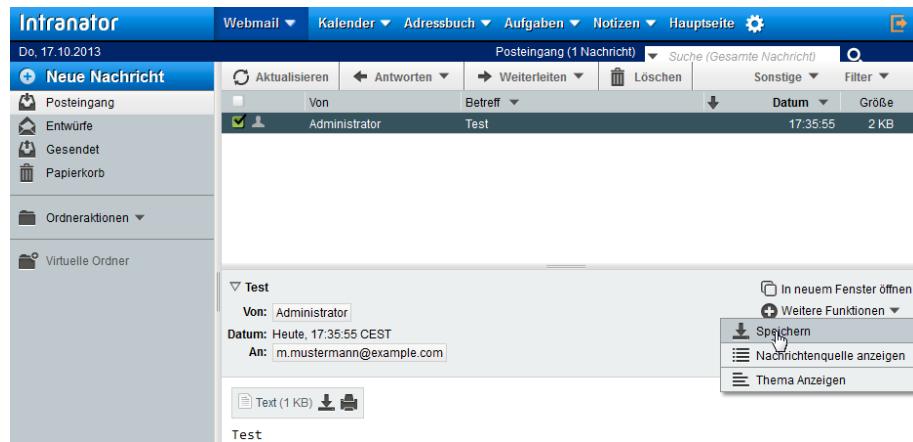
Um einzelne E-Mails in anderen Programmen weiterzuverarbeiten oder sie für die Fehler-suche genauer analysieren zu können, gibt es die Möglichkeit E-Mails im RFC822-Format (zum Teil auch nach der Dateiendung .EML genannt) zu exportieren.

Gehen Sie dafür wie folgt vor:

1. Öffnen Sie die betroffene E-Mail
2. Klappen Sie die Detaildaten mit dem Pfeil auf



3. Wählen Sie das Menü Weitere Funktionen auf der rechten Seite, Menüpunkt Speichern. Sie können nun in Ihrem Browser das passende Zielverzeichnis wählen.



- Möchten Sie die exportierte E-Mail z.B. zur Fehleranalyse wieder per E-Mail weiterleiten, so packen Sie die .EML-Datei vorher am besten nochmal mit einem Packprogramm wie z.B. Zip. So wird sichergestellt, dass die E-Mail auf dem Versandweg nicht aus Versehen noch verändert wird.

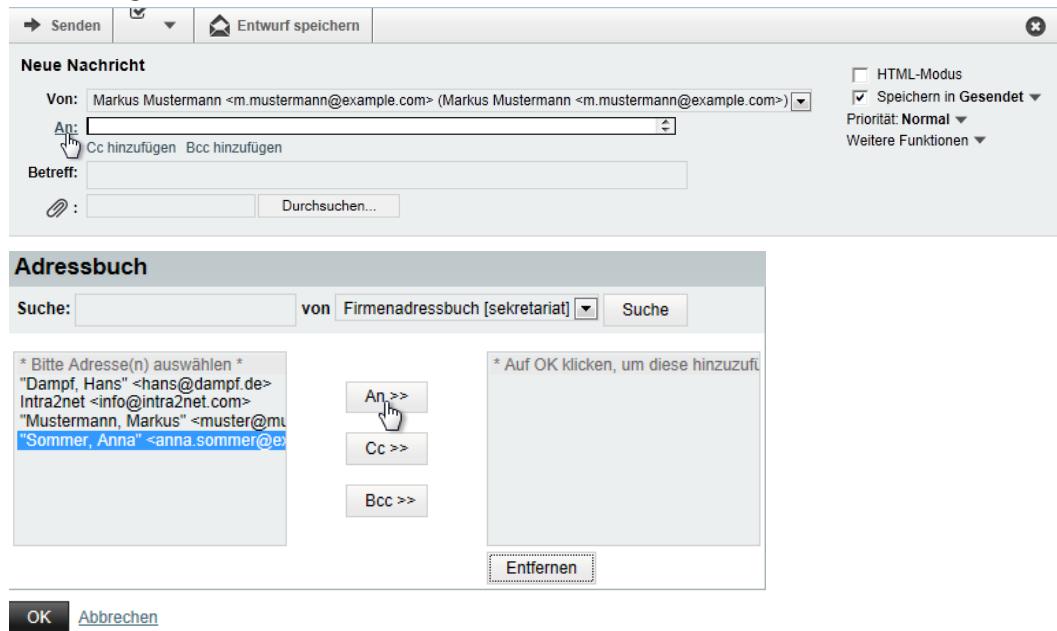
27.2. E-Mails senden

27.2.1. Neue Nachricht

Klicken Sie links oben auf die Schaltfläche Neue Nachricht und es öffnet sich ein Fenster zum Verfassen einer neuen E-Mail.

Wenn Sie in den Feldern An, Cc oder Bcc beginnen, einen Namen einzugeben, werden automatisch im Hintergrund alle erreichbaren Adressbücher nach diesem Namen durchsucht. Dabei gefundene Kontakte werden dann in einer Auswahlbox angeboten.

Alternativ kann man auf An klicken, um passende Empfänger aus den Adressbüchern hinzuzufügen.



27.2.2. Signaturen anhängen

Es ist möglich eine Signatur zu definieren, die automatisch beim Versand einer neuen E-Mail ans Ende angefügt wird.

Jeder Benutzer kann seine Signatur im Menü Benutzermanager > Eigenes Profil > Groupware konfigurieren. Zum Aufrufen dieses Menüs muss die Web-Groupware zuerst über die Schaltfläche Hauptseite verlassen werden. Der Administrator kann die Signaturen aller Benutzer über das Menü Benutzermanager > Benutzer : Groupware konfigurieren.

Hinweis



Die Signatur wird im E-Mail-Editor nicht angezeigt. Sie wird dennoch automatisch beim Versand an die E-Mail angehängt.

27.3. Ordner verwalten

27.3.1. Ordnerhierarchie

In der linken Bildschirmhälfte wird die Liste aller E-Mail-Ordner angezeigt. Dabei wird der Wurzelordner des Benutzers (in IMAP "INBOX" genannt) ganz oben als Posteingang angezeigt. Darunter werden die Ordner für Entwürfe, Gesendete E-Mails und Papierkorb angezeigt. Diese werden immer mit den Namen Entwürfe, Gesendet und Papierkorb angezeigt, unabhängig davon, wie sie tatsächlich benannt sind.

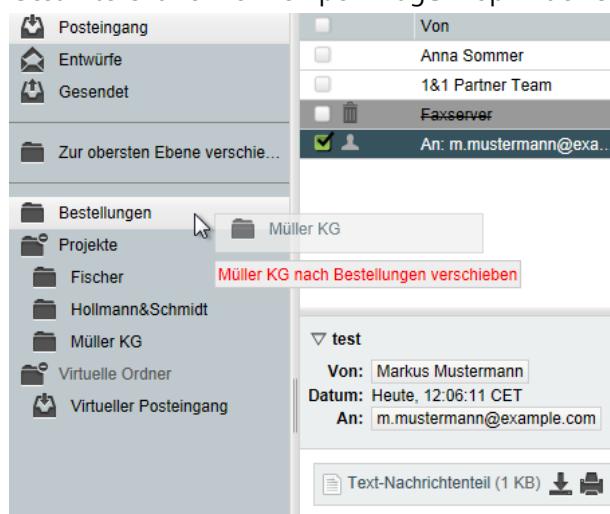
Der tatsächliche Name dieser Ordner kann im Menü Benutzermanager > Eigenes Profil > Groupware bzw. vom Administrator im Menü Benutzermanager > Benutzer : Groupware konfiguriert werden.

Alle weiteren Unterordner des Benutzers werden unterhalb von Ordneraktionen in alphabetischer Reihenfolge dargestellt.

27.3.2. Ordner organisieren

Die Ordnernamen in der Ordnerliste können mit der rechten Maustaste angeklickt werden. Es öffnet sich ein Kontextmenü, welches Funktionen wie Löschen, Umbenennen oder das Erstellen von Unterordnern erlaubt.

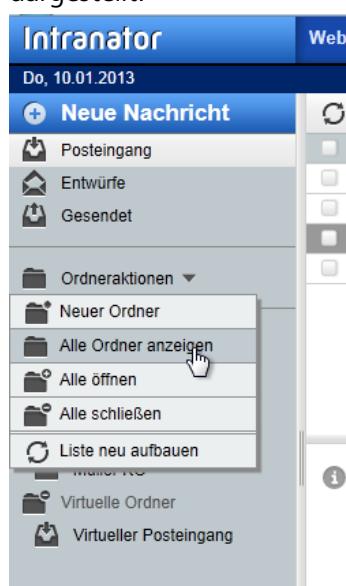
Gesamte Ordner können per Drag&Drop in der Ordnerhierarchie verschoben werden.



27.3.3. Ordner abonnieren

Das Webmail-System zeigt normalerweise nur die abonnierten Ordner an, alle anderen Ordner sind ausgeblendet.

Möchten Sie einen Ordner abonnieren, schalten Sie zuerst auf die Ansicht aller Ordner um. Verwenden Sie dazu das Menü Ordneraktionen > Alle Ordner anzeigen. Nun werden auch die nicht abonnierten Ordner angezeigt, diese werden mit kursivem Ordernamen dargestellt.



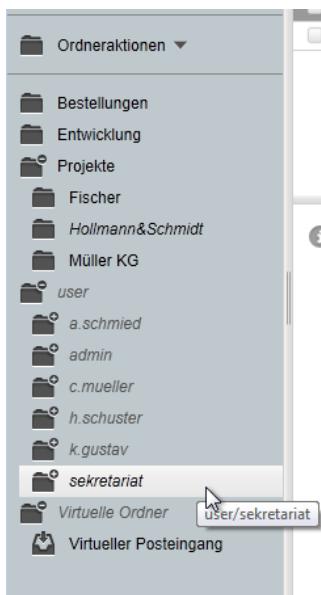
Um einen Ordner zu abonnieren, öffnen Sie mit der rechten Maustaste das Kontextmenü des entsprechenden Ordners und wählen Einblenden.



Haben Sie alle gewünschten Ordner abonniert, können Sie die nicht abonnierten Ordner über die Funktion Ordneraktionen > Ausgeblendete Ordner verstecken wieder verstecken.

Die Liste der abonnierten Ordner wird auf dem IMAP-Server gespeichert. Die meisten E-Mail-Programme greifen auf diese serverseitige Abonnementliste zu. So muss ein Ordner nur einmal abonniert werden und er wird dann in allen verwendeten E-Mail-Programmen und Geräten angezeigt.

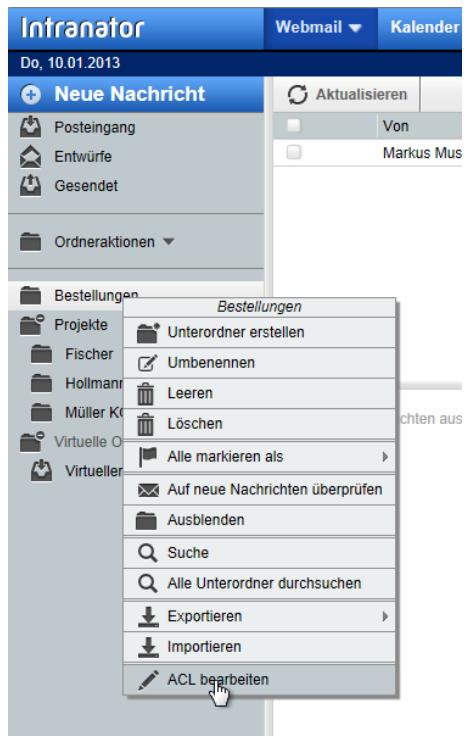
Hat ein anderer Benutzer Ihnen einen seiner E-Mail-Ordner freigegeben, so ist dieser in der Hierarchie `user` und darunter dem Benutzerlogin zu finden. Hat ein anderer Benutzer Ihnen seinen Posteingang freigegeben, so entspricht das dem Benutzernamen selbst; es wird kein Unterordner `Posteingang` angezeigt.



Freigegebene Ordner anderer Benutzer sind nach der Freigabe erst mal versteckt und müssen wie oben beschrieben abonniert werden bevor sie dauerhaft angezeigt werden.

27.3.4. Ordner freigeben

Um Ordner für andere Benutzer freizugeben, klicken Sie den Ordnernamen in der Ordnerliste mit der rechten Maustaste an und öffnen den Menüpunkt ACL bearbeiten.



Es öffnet sich ein Fenster, in dem die Zugriffsrechte auf diesen Ordner im Detail bearbeitet werden können.

In der linken Spalte unter Benutzer können die Logins von anderen Benutzern eingegeben werden. Nach Eingabe des Benutzernamens können Sie entweder die IMAP-ACLs einzeln über die Kontrollkästchen steuern, oder Sie können häufig verwendete Rechtekombinationen in den Vorlagen auswählen.

Soll ein Ordner nicht nur für einen Benutzer, sondern gleich für eine ganze Benutzergruppe freigegeben werden, so verwenden Sie als Benutzername **group:** und dahinter den Namen der Benutzergruppe auf dem Intranator, also z.B. **group:Alle**.

28. Kapitel - Adressbuch



Hinweis

Dieses Kapitel, sowie weitere über Kalender und Aufgaben, sind momentan noch in Arbeit und werden in Kürze veröffentlicht.

29. Kapitel - Mobile Geräte per ActiveSync anbinden

29.1. Einführung

ActiveSync ist ein von Microsoft entwickeltes Protokoll, um Groupwaredaten zwischen einem Server und mobilen Endgeräten wie Smartphones und Tablets zu synchronisieren. Mittlerweile kann es aber auch von vollständigen Office-Programmen wie Outlook 2013 genutzt werden.

Die meisten mobilen Geräte enthalten von Haus aus eine Schnittstelle für die Synchronisation von E-Mails, Kontakten, Terminen und Aufgaben per ActiveSync. Da das Protokoll zuerst vom Microsoft Exchange Server angeboten wurde, ist es auf den Geräten häufig unter den Stichworten "Microsoft Exchange Server", "Exchange Server ActiveSync" oder ähnlichem zu finden.

ActiveSync ist mit allen Lizenzen des Intranator Servers nutzbar, die die Funktion Mail Server enthalten.

29.2. Einstellungen auf dem Server

Um Geräte per ActiveSync mit dem Intranator Server zu verbinden, müssen auf dem Server zuerst folgende Grundeinstellungen vorgenommen bzw. überprüft werden:

1. Prüfen Sie, wie der Intranator mit dem Internet verbunden ist. Kontrollieren Sie dazu im Menü Netzwerk > Provider > Profile den Typ des aktiven Providers. Handelt es sich um eine (DSL-)Wahlleitung ist alles in Ordnung und Sie können zum nächsten Schritt weitergehen.

Handelt es sich um einen Providertyp mit einem Router, dann prüfen Sie ob dieser Router dem Intranator Server eine unveränderte offizielle IP zuweist, oder ob er per NAT eine IP aus einem privaten Adressbereich zuweist. In letzterem Fall muss auf dem Router ein Portforwarding für TCP Port 443 (https) auf die IP des Intranator Servers konfiguriert werden.

2. Kontrollieren Sie die Firewall-Regelliste für aus dem Internet eingehende Verbindungen. Sie wird im Menü Netzwerk > Provider > Profile : Firewall für den aktiven Provider ausgewählt und kann mit dem Lupen-Symbol untersucht werden. In ihr müssen Eingehende HTTPS-Verbindungen aktiviert sein.
3. Der Intranator muss für das Mobilgerät über das Internet adressierbar sein.

Bekommt der Intranator bei der Interneteinwahl regelmäßig eine neue IP zugewiesen, muss zur Adressierung ein DynDNS-Dienst eingerichtet werden. Siehe hierfür Abschnitt 11.12, „DynDNS“.

Hat der Intranator eine feste IP, empfehlen wir dringend für diese feste IP einen DNS-Eintrag in der eigenen offiziellen Domain einzurichten. Der Intranator ist dann unter einem Namen wie z.B. `intranator.kundenname.de` oder `mail.example.com` erreichbar. Dies kann normalerweise beim Webspace-Provider, der die eigene Domain verwaltet, kostenlos und zeitnah eingerichtet werden.

Eine feste IP direkt und ohne DNS-Namen sollte nur in Ausnahmefällen für ActiveSync verwendet werden. Hintergrund ist, dass bei einer Änderung der IP alle Geräte neu

eingerichtet werden müssen und offizielle Zertifizierungsstellen keine Zertifikate für IPs ausstellen.

4. Der Zugriff auf ActiveSync findet ausschließlich über HTTPS statt. Für die Verschlüsselung wird daher ein passendes Zertifikat benötigt, welches auf den verwendeten externen DNS-Namen (siehe oben) ausgestellt ist. Dieses Zertifikat muss im Menü System > Weboberfläche > Sicherheit als SSL Server Schlüssel für Verbindungen aus dem Internet gewählt sein.

Mehr Informationen zu SSL und Zertifikaten finden Sie im 10. Kapitel, „SSL-Verschlüsselung und Zertifikate“.



Tipp

Wir empfehlen ab ca. 5 anzubindenden Geräten oder Benutzern ein Zertifikat von einer offiziellen Zertifizierungsstelle zu verwenden. Dies vereinfacht die Administration, da die Geräte dann zur Ersteinrichtung nicht unbedingt über eine vertrauenswürdige Netzumgebung verbunden werden müssen.

Wie Sie das Zertifikat einer offiziellen Zertifizierungsstelle mit dem Intranator verwenden wird in Abschnitt 10.5, „Verwenden einer externen Zertifizierungsstelle“ erklärt.

5. Prüfen Sie die Qualität der Passwörter aller Benutzer, die ActiveSync verwenden sollen. Die Passwörter sollten ausreichend lang (mindestens 8 Stellen), aus Buchstaben, Zahlen und evtl. auch Sonderzeichen zusammengesetzt sein und nicht zu einem großen Teil aus einem Wort oder Eigennamen einer verbreiteten Sprache bestehen.
6. Bevor ein Benutzer ActiveSync verwenden darf, muss in einer seiner Benutzergruppen das Recht Zugriff auf Groupware-Daten via ActiveSync (Menü Benutzermanager > Gruppen : Rechte) vergeben sein.



Tipp

Wir empfehlen für ActiveSync eine separate Benutzergruppe einzurichten, und in diese wirklich nur Benutzer mit überprüfter Passwortqualität (siehe oben) aufzunehmen.

7. ActiveSync überträgt für jeden Objekttyp immer nur die Daten aus einem einzigen Ordner. Stellen Sie daher für jeden Benutzer im Menü Benutzermanager > Benutzer : Groupware die Ordner als Standardordner ein, die auch per ActiveSync übertragen werden sollen.
8. Konfigurieren Sie die einzelnen Geräte wie in den folgenden Kapiteln beschrieben.

29.3. Besonderheiten und Tipps

29.3.1. Löschen von E-Mails auf dem Server

Wird ein E-Mail-Konto parallel zum ActiveSync-Mobilgerät auch mit einem E-Mail-Client per IMAP verwendet, der das Löschen von E-Mails nicht über das Verschieben in einen Papierkorb, sondern über Löschmarkierungen abbildet, werden die von diesem E-Mail-

Client gelöschten E-Mails erst zum Zeitpunkt des endgültigen Löschens (Expunge-Befehl) auf dem ActiveSync-Gerät gelöscht.

Betroffene E-Mail-Clients sind u.a. Mozilla Thunderbird und Microsoft Outlook 2003.

29.3.2. Synchronisationsschritte

Meldet sich das Mobilgerät am Intranator Server zur Synchronisation, bekommt es alle Änderungen seit der letzten Synchronisation mitgeteilt und aktualisiert daraufhin seine Daten. Genauso werden auf dem Mobilgerät vorgenommene Änderungen an den Intranator Server übertragen.

Aus technischen Gründen benötigen einige Änderungsaktionen allerdings zwei Synchronisationsschritte zur vollständigen Übertragung. Zwischen diesen Schritten müssen mindestens 4 Minuten Zeitabstand sein. Beachten Sie dies vor allem bei mehrstündigen Synchronisationsintervallen. Rufen Sie im Zweifelsfalle die manuelle Synchronisation zwei mal hintereinander im Abstand von 4 Minuten auf dem Mobilgerät auf. Spätestens dann sind alle Daten aktuell.

29.3.3. Geräte verwalten und neu synchronisieren

Auf dem Intranator Server wird im Menü Benutzermanager > Benutzer : Groupware eine Liste aller mit dem entsprechenden Benutzerkonto verbundenen Geräte angezeigt. Diese ist gleichzeitig auch für jeden Benutzer selbst unter Benutzermanager > Eigenes Profil > Groupware erreichbar.

Über die Schaltfläche Zurücksetzen wird der Synchronisationsstand eines Geräts auf dem Server verworfen. Meldet sich das Gerät das nächste Mal zur Synchronisation, werden alle Daten erneut übertragen. Auf diese Weise können Synchronisations- oder Datenkonstanzprobleme gelöst werden. Dies wird auch automatisch beim Rückspielen eines Backups des Intranator Servers ausgelöst.

29.3.4. Synchronisieren von mehreren Kalendern oder Kontakteordnern

Über eine ActiveSync-Verbindung wird für jeden Groupware-Objekttyp (Termin, Adresse, Aufgabe,...) immer nur ein Ordner übertragen. In einigen Fällen ist aber gewünscht z.B. zusätzlich zum privaten Adressbuch noch ein firmenweites Adressbuch zu übertragen.

Dies kann durch das Einrichten zusätzlicher ActiveSync-Verbindungen realisiert werden. Da die zu übertragenden Ordner pro Benutzerkonto im Menü Benutzermanager > Benutzer : Groupware eingestellt werden, muss für jede dieser Verbindungen ein unterschiedliches Benutzerkonto verwendet werden.

Soll z.B. ein firmenweites Adressbuch übertragen werden, kann dafür direkt ein allgemeiner Benutzer wie z.B. **info** unter dem auch das gewünschte Adressbuch abgelegt ist, genutzt werden. Es gibt keine Beschränkung wie viele ActiveSync-Verbindungen parallel mit einem Benutzerkonto verbunden sein können.

Werden auf diese Weise Kalender oder Aufgabenlisten eingebunden, gelten Erinnerungseinstellungen darin immer für das gesamte Benutzerkonto. Wird dies von mehreren Benutzern geteilt, erscheinen die Erinnerungen auch bei allen.

30. Kapitel - ActiveSync mit Android-Geräten

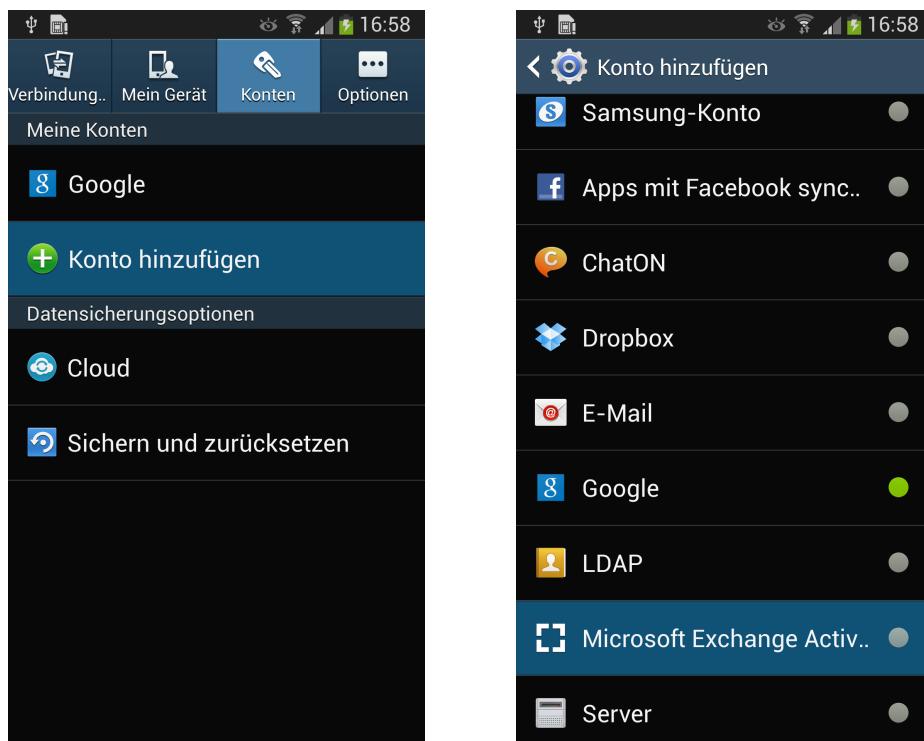
Bevor Sie das Gerät konfigurieren können, müssen Sie den Intranator Server für die Anbindung vorbereiten. Führen Sie dazu die in Abschnitt 29.2, „Einstellungen auf dem Server“ beschriebenen Schritte durch.

Haben Sie sich entschlossen, auf dem Intranator Server kein Zertifikat einer offiziellen Zertifizierungsstelle, sondern ein selbsterstelltes, einzusetzen, muss das Android-Gerät für den Zeitraum der Konfiguration über eine vertrauenswürdige Verbindung direkt mit dem Intranator verbunden sein. Hierfür kommt ein direkt an den Intranator angeschlossener und per WPA2 geschützter WLAN-Accesspoint oder eine VPN-Verbindung mit dem Intranator in Betracht.

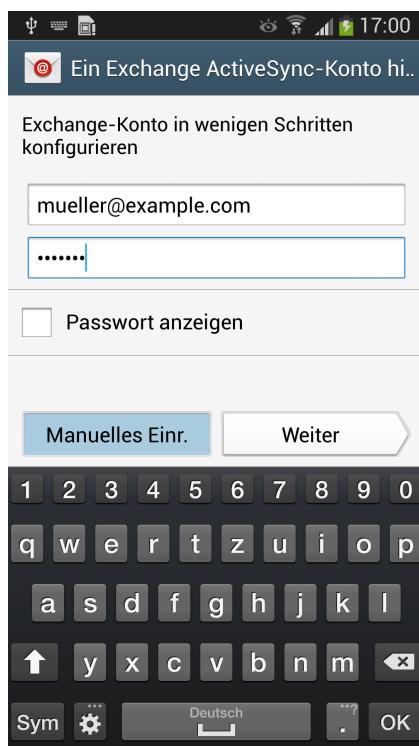
Eine UMTS-Verbindung oder ein nicht direkt lokal am Intranator angeschlossenes WLAN sind ungeeignet. Wollen Sie diese Verbindungsarten zur Konfiguration nutzen, muss ein Zertifikat einer offiziellen Zertifizierungsstelle verwendet werden.

Gehen Sie zur Konfiguration wie folgt vor:

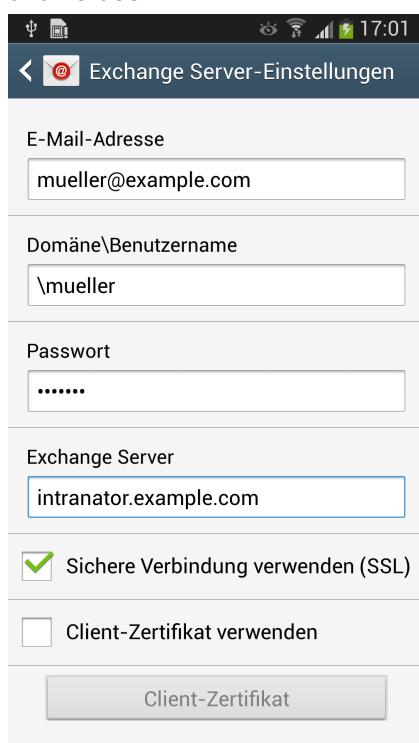
1. Haben Sie sich entschlossen, auf dem Intranator Server kein Zertifikat einer offiziellen Zertifizierungsstelle, sondern ein selbsterstelltes, einzusetzen, verifizieren Sie als erstes, dass die Internetverbindung über den Mobilfunkprovider (UMTS bzw. LTE) dauerhaft deaktiviert ist.
2. Stellen Sie als nächstes sicher, dass die Zugangsdaten vertraulich bleiben. Die dafür nötigen Schritte werden in Abschnitt 46.1, „Gerät vorbereiten“ beschrieben.
3. Öffnen Sie auf dem Android-Gerät die Einstellungen, Reiter Konten und wählen Konto hinzufügen. Der Typ des hinzuzufügenden Kontos ist Microsoft Exchange ActiveSync.



4. Geben Sie Ihre E-Mail-Adresse und das Passwort des Benutzerkontos auf dem Intranator Server ein. Wählen Sie dann Manuelles Einrichten.



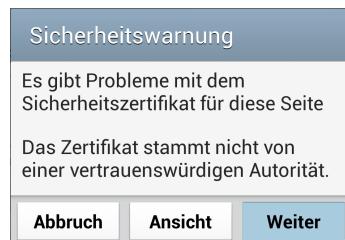
5. Tragen Sie unter Domäne/Benutzername einen \ (Backslash) direkt gefolgt vom Benutzernamen auf dem Intranator ein. Tragen Sie im Feld Exchange Server den externen DNS-Namen des Intranators ein. Die Option Sichere Verbindung (SSL) muss aktiviert sein.



6. Wird kein Zertifikat einer offiziellen Zertifizierungsstelle verwendet, erscheint nun eine Sicherheitswarnung. Da Sie ja sichergestellt haben, dass der vollständige Verbin-

dungsweg zwischen Android-Gerät und Intranator Server vertrauenswürdig ist, handelt es sich nicht um ein gefälschtes Zertifikat. Sie können daher an dieser Stelle auf Weiter gehen und das Zertifikat damit dauerhaft im Gerät als vertrauenswürdig speichern.

Wird das Zertifikat einer offiziellen Zertifizierungsstelle verwendet, darf eine solche Sicherheitswarnung nicht erscheinen. Tut sie es dennoch, gehen Sie auf keinen Fall auf Weiter, sondern überprüfen als erstes die Konfiguration auf dem Server und versuchen es dann über einen anderen Verbindungs weg erneut.



7. Als nächstes wird konfiguriert, wie häufig Daten zwischen Server und Mobilgerät synchronisiert werden sollen. Android bietet hier die Möglichkeit zwischen den normalen Abrufeinstellungen und Spitzenzeit zu unterscheiden. Die Spitzenzeit ist dabei für die Kernarbeitszeit vorgesehen und kann später genau auf Stunden und Wochentage eingestellt werden.

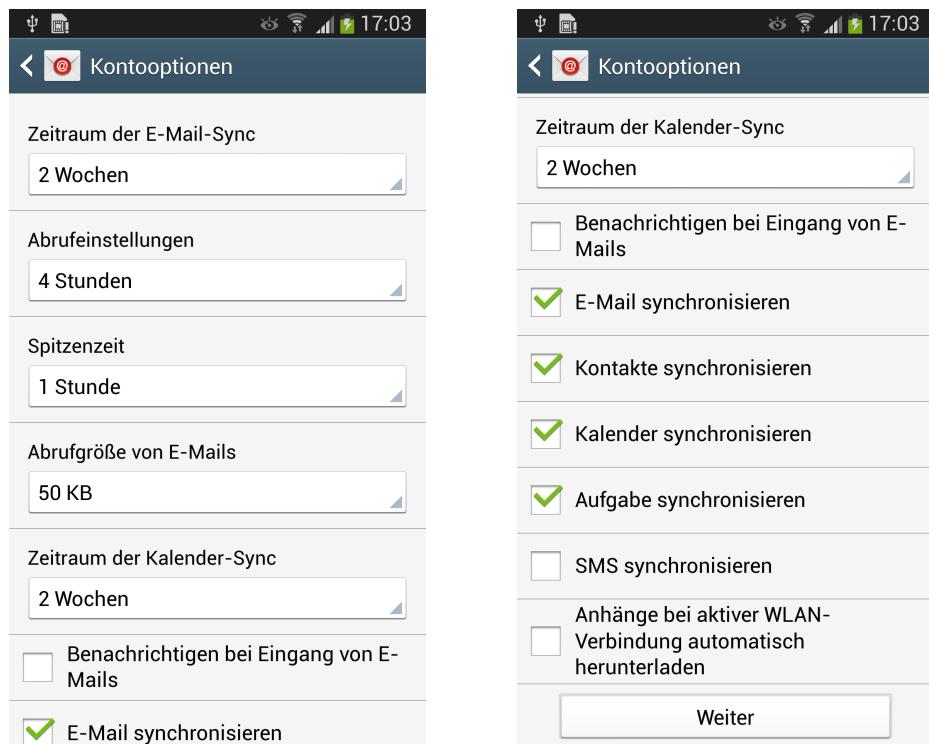


Tipp

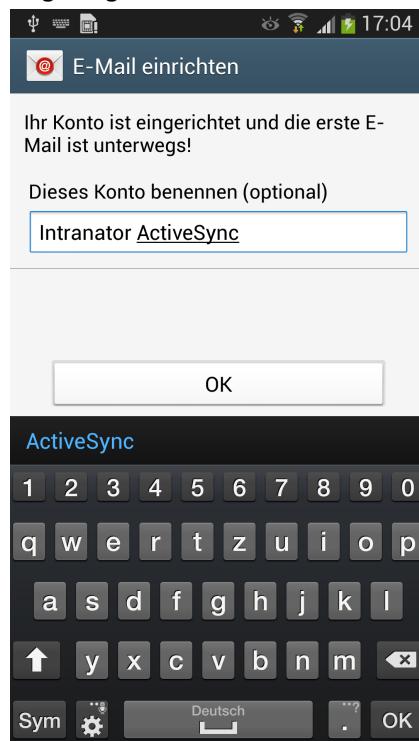
Wir empfehlen die Übertragungshäufigkeit auf 15 Minuten oder mehr zu stellen und raten von der Verwendung von Push ab. Im Push-Modus ist ständig eine Funkverbindung aktiv und das Gerät kann daher kaum noch Gebrauch von seinen Energiesparmodi machen. Dadurch sinkt die Batterie reichweite signifikant. Außerdem haben wir bei einigen Geräten im Push-Modus Übertragungsfehler beobachtet, die zu einer Verdopplung von E-Mails und Terminen führen.

Außerdem kann konfiguriert werden, dass nur die E-Mails und Kalendereinträge eines bestimmten Zeitraums übertragen werden. Dies spart Übertragungsvolumen, Speicherplatz auf dem Mobilgerät und lässt die Anwendungen auf dem Mobilgerät nicht träge werden.

Im unteren Bereich des Dialogs kann ausgewählt werden, welche Objekttypen synchronisiert werden sollen. Der Intranator Server bietet keine Synchronisation von SMS an, deaktivieren Sie diese daher.



8. Geben Sie dem Konto als Letztes einen aussagekräftigen Namen. Dieser wird in den verschiedenen Applikationen bei der Auswahl zwischen den verschiedenen Konten angezeigt.



Das neue Konto wird nun bei E-Mails, den Kontakten und Terminen/Aufgaben in den entsprechenden Applikationen zur Auswahl angeboten. Bei neu anzulegenden Objekten besteht die Möglichkeit, zwischen den verschiedenen auf dem Gerät eingerichteten Konten zu wählen.

Alle betroffenen Applikationen bieten auch die Möglichkeit, manuell eine Synchronisation der Daten auszulösen. Diese Möglichkeit ist einem sehr kurzen Synchronisationsintervall typischerweise vorzuziehen.

31. Kapitel - ActiveSync mit Apple iOS-Geräten

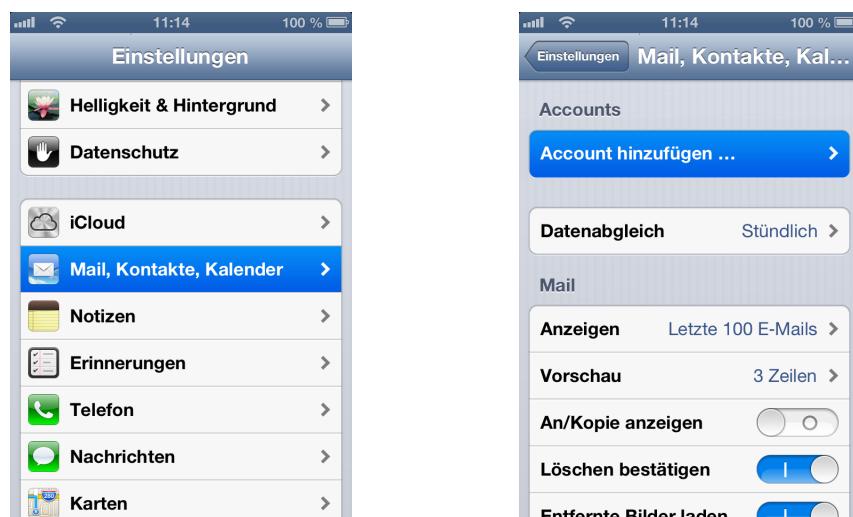
Bevor Sie das Gerät konfigurieren können, müssen Sie den Intranator Server für die Anbindung vorbereiten. Führen Sie dazu die in Abschnitt 29.2, „Einstellungen auf dem Server“ beschriebenen Schritte durch.

Haben Sie sich entschlossen, auf dem Intranator Server kein Zertifikat einer offiziellen Zertifizierungsstelle, sondern ein selbsterstelltes, einzusetzen, muss das iOS-Gerät für den Zeitraum der Konfiguration über eine vertrauenswürdige Verbindung direkt mit dem Intranator verbunden sein. Hierfür kommt ein direkt an den Intranator angeschlossener und per WPA2 geschützter WLAN-Accesspoint oder eine VPN-Verbindung mit dem Intranator in Betracht.

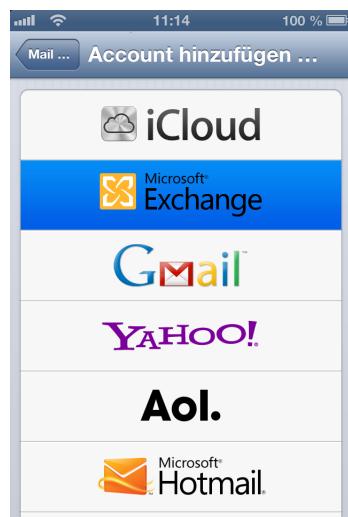
Eine UMTS-Verbindung oder ein nicht direkt lokal am Intranator angeschlossenes WLAN sind ungeeignet. Wollen Sie diese Verbindungsarten zur Konfiguration nutzen, muss ein Zertifikat einer offiziellen Zertifizierungsstelle verwendet werden.

Gehen Sie zur Konfiguration wie folgt vor:

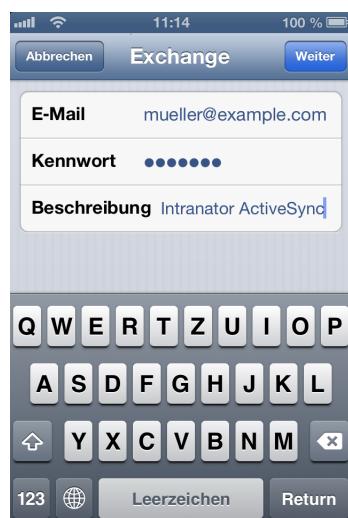
1. Haben Sie sich entschlossen, auf dem Intranator Server kein Zertifikat einer offiziellen Zertifizierungsstelle, sondern ein selbsterstelltes, einzusetzen, verifizieren Sie als erstes, dass die Internetverbindung über den Mobilfunkprovider (UMTS bzw. LTE) dauerhaft deaktiviert ist.
2. Öffnen Sie die Einstellungen, Unterpunkt Mail, Kontakte, Kalender und wählen Account hinzufügen.



3. Der Typ des hinzuzufügenden Kontos ist Microsoft Exchange.



4. Tragen Sie die E-Mail-Adresse, das Kennwort des Benutzerkontos auf dem Intranator Server und einen Namen für das Konto auf dem iOS-Gerät ein.



5. Tragen Sie den externen DNS-Namen des Intranators im Feld Server ein. Tragen Sie den Benutzernamen (Login) des Kontos ein.



- Wird kein Zertifikat einer offiziellen Zertifizierungsstelle verwendet, erscheint nun eine Sicherheitswarnung. Da Sie ja sichergestellt haben, dass der vollständige Verbindungsweg zwischen iOS-Gerät und Intranator Server vertrauenswürdig ist, handelt es sich nicht um ein gefälschtes Zertifikat. Sie können daher an dieser Stelle auf Fortfahren gehen und das Zertifikat damit dauerhaft im Gerät als vertrauenswürdig speichern.

Wird das Zertifikat einer offiziellen Zertifizierungsstelle verwendet, darf eine solche Sicherheitswarnung nicht erscheinen. Tut sie es dennoch, gehen Sie auf keinen Fall auf Fortfahren, sondern überprüfen als erstes die Konfiguration auf dem Server und versuchen es dann über einen anderen Verbindungs weg erneut.



- Wählen Sie, welche Objekttypen Sie synchronisieren möchten.



- Öffnen Sie als letztes das Menü Datenabgleich und stellen ein, wie häufig die Daten synchronisiert werden sollen.



Tipp

Wir empfehlen die Übertragungshäufigkeit auf 15 Minuten oder mehr zu stellen und raten von der Verwendung von Push ab. Im Push-Modus ist ständig eine Funkverbindung aktiv und das Gerät kann daher kaum noch Gebrauch von seinen Energiesparmodi machen. Dadurch sinkt die Batteriereichweite signifikant.



Das neue Konto wird nun bei E-Mails, den Kontakten, Terminen und Erinnerungen (Aufgaben) in den entsprechenden Applikationen zur Auswahl angeboten. Bei neu anzulegenden Objekten besteht die Möglichkeit, zwischen den verschiedenen auf dem Gerät eingerichteten Konten zu wählen.

Aus den betroffenen Applikationen heraus besteht normal auch die Möglichkeit, manuell eine Synchronisation der Daten auszulösen. Diese Möglichkeit ist einem sehr kurzen Syncronisationsintervall typischerweise vorzuziehen.

32. Kapitel - Referenzinformationen

Die Web-Groupware und die ActiveSync-Schnittstelle unterstützen nicht alle Felder, die per ActiveSync oder vom Intranator Groupware Client gesendet werden können. Die in diesen Feldern gespeicherten Daten können daher bei Nutzung der Webgroupware oder ActiveSync verloren gehen.

Weitere Informationen folgen in Kürze.

Teil 5. Firewall

33. Kapitel - Auswahl der Firewall-Regellisten

Die Firewall des Intranators besteht aus einzelnen, separaten Firewall-Regellisten. Diese Regellisten können einzelnen Objekten, wie z.B. Rechnern oder Netzen, zugewiesen werden. Beim Anlegen eines neuen Objekts kann eine bestehende Firewallregelliste wiederverwendet werden. Außerdem werden die wichtigsten Grundregeln schon vorinstalliert mitgeliefert. Dies vereinfacht die Konfiguration deutlich.

33.1. Regellisten im LAN

Jedem Rechner, IP-Bereich, Routing, Netz und VPN kann über das passende Menü (z.B. „Netzwerk > Intranet > Rechner“) genau eine Firewall-Regelliste zugewiesen werden.

Da sich Rechner oder IP-Bereiche gleichzeitig auch immer in einem Netz oder Routing befinden, sind ihnen 2 Firewall-Regellisten zugeordnet. Hier gilt immer nur die dem Rechner oder IP-Bereich zugeordnete Regel, die dem Netz oder Routing zugeordnete kommt nicht zum Einsatz. Diese gelten nur für IPs aus dem Netz, für die kein Rechner oder IP-Bereich konfiguriert ist.



Achtung

Allein die Quelle eines Pakets entscheidet, welche Firewall-Regelliste verwendet wird.

Daher finden Sie in einer Regelliste für einen Rechner sowohl Regeln für den Zugriff auf andere lokale Netze als auch ins Internet, in VPNs etc. Alles was von einem Rechner kommt wird unabhängig vom Ziel anhand der dem Rechner zugewiesenen Regelliste überprüft.

In dem Rechteckblock für z.B. einen Rechner finden Sie außer der Firewall-Regelliste auch noch Einstellungen zum Proxy-Profil sowie zum DNS- und E-Mail-Relaying. Die Firewall-Regelliste hat Vorrang vor diesen Einstellungen. Das heißt, erst, wenn die Firewall-Regelliste den Zugriff auf den Proxy zulässt, kommt die Einstellung des Proxy-Profiles überhaupt zum Tragen.

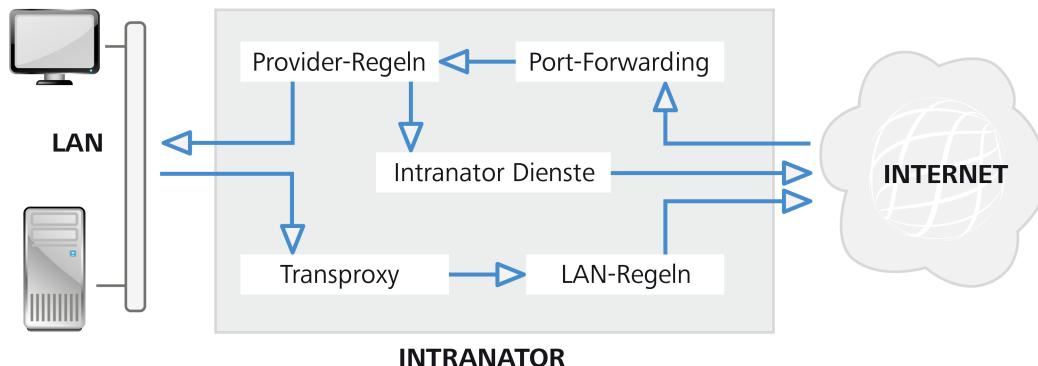
33.2. Regellisten fürs Internet

Unter „Netzwerk > Provider > Profile : Firewall“ wird jedem Provider eine Firewall-Regelliste zugeordnet. Die dem aktiven Internet-Provider zugeordnete Firewall-Regelliste entscheidet, welche Pakete aus dem Internet in die lokalen Netze dürfen und welche nicht.

Auch hier gilt, dass nur die der Quelle der Pakete (hier: Internet und damit Provider) zugeordnete Firewall-Regelliste darüber entscheidet, ob die Pakete durchgelassen werden oder nicht.

33.3. Weg der Pakete durch die Firewall

33.3.1. Paketwege im LAN und Internet



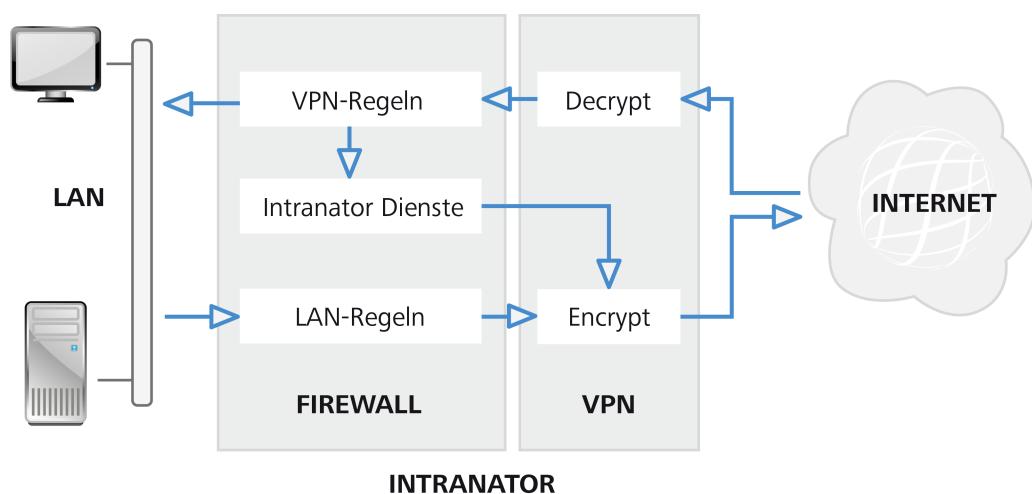
Der Weg der Pakete lässt sich relativ einfach zusammenfassen:

- Die verwendeten Regellisten hängen immer von der Quelle der Pakete ab.
- Regeln, welche Pakete verändern, werden immer zuerst ausgeführt. Dies betrifft NAT, Port-Forwarding, Statische NAT und Transparenter Proxy. Alle folgenden Regeln bekommen dann nur die bereits veränderten Pakete zu sehen.
- Die Verbindungen des Intranators selbst können nicht beschränkt werden.

33.3.2. Paketwege bei VPN-Verbindungen

Bei VPNs werden die Pakete vor der Verschlüsselung und nach der Entschlüsselung durch die Firewall geprüft.

Aus dem VPN kommende Pakete werden nach der Entschlüsselung durch die dem VPN zugewiesene Regelliste geprüft. Nur diese Regelliste entscheidet, ob die Pakete durchgelassen werden.



34. Kapitel - Firewall-Profile

Einfache Regellisten

Es gibt drei verschiedene Klassen von Firewall-Regellisten: einfache Firewall-Profile, vollständige Regellisten und Providerprofile. Regeln aller drei Typen werden gemeinsam in Netzwerk > Firewall > Regeln verwaltet.

Für Standard-Szenarien werden im Intranator keine komplexen Firewall-Regellisten benötigt, sondern es können über die Firewall-Profile mit wenigen Klicks die wichtigsten Einstellungen vorgenommen werden.

Sollte eines dieser Firewall-Profile einmal für seinen Einsatzzweck nicht mehr ausreichen, so kann es über den Knopf Umwandeln in eine Vollständige Regelliste umgewandelt und dann entsprechend erweitert werden.

34.1. Basis-LAN Grundregeln

Alle Firewall-Rechnerprofile bauen auf der Regelliste „Basis LAN“ oder „Basis LAN und lokale Netze“ auf. Diese enthalten Grundrechte für den Zugriff auf den Intranator selbst, erlauben aber keinerlei Zugriff ins Internet oder auf E-Mails.

„Basis LAN“ erlaubt den Zugriff auf folgende Dienste des Intranators:

- DNS
- Weboberfläche per HTTPS
- Windows-Freigabe (SMB) für Backups
- ICMP-Basisdienste wie z.B. Ping
- SSH für Zugriff auf die Systemkonsole des Intranators

„Basis LAN und lokale Netze“ erlaubt zusätzlich noch vollen Zugriff auf alle anderen an den Intranator angeschlossenen lokale Netze und Routings. Welches der beiden Regellisten „Basis LAN“ oder „Basis LAN und lokale Netze“ verwendet wird, entscheidet die Einstellung bei Zugriff auf lokale Netze erlaubt.

„Basis LAN und lokale Netze“ oder die Option Zugriff auf lokale Netze erlaubt sollten daher auf keinen Fall bei De-Militarized-Zones (DMZ) zum Einsatz kommen.

34.2. Rechnerprofile

Über die Option Zugriffsberechtigung können Sie die Grund-Zugriffsrechte festlegen. „Kein Zugriff“ entspricht den Rechten von „Basis LAN“ oder „Basis LAN und lokale Netze“. „Nur E-Mail“ erlaubt zusätzlich zu „Basis LAN“ den Zugriff über die E-Mail-Protokolle SMTP, POP3(S) und IMAP(S). „Nur VPN“ erlaubt zusätzlich zu „Basis LAN“ den Zugriff auf über den Intranator verbundene VPN-Netze. In diese VPN-Netze ist dann der Zugriff mit allen Protokollen möglich.

Die Option Webzugriff über Proxy entscheidet darüber, in welcher Weise der HTTP- und FTP-Proxy des Intranators genutzt werden kann. „Freier Zugriff“ ermöglicht den Zugang zum Proxy-Port, erzwingt ihn aber nicht. Erst, wenn der Benutzer den Proxy im Browser

eingetragen hat, wird er genutzt. „Proxzywang“ sorgt dafür, dass der direkte Zugriff auf HTTP-Server im Internet unterbunden wird. Der Benutzer muss daher den Proxy im Browser eintragen. Bei „Transparenter Proxy“ leitet der Intranator alle Zugriffe auf HTTP-Server für den Benutzer unsichtbar auf den Proxy des Intranators um. Daher muss im Browser nichts speziell umkonfiguriert werden.

Über die Option Zusätzliche Dienste können weitere Ports (wie z.B. HBCI) für den Zugriff ins Internet freigegeben werden.

Die Option Mailtransfer nur über Intranator sorgt dafür, dass die E-Mail-Protokolle auf den Intranator beschränkt werden. Damit wird der Zugriff von E-Mail-Programmen direkt auf Mailserver im Internet unterbunden und so sichergestellt, dass alle E-Mails über den Intranator laufen müssen. Dies macht Sinn um z.B. dafür zu sorgen, dass der E-Mail-Virenschanner oder eine Archivierungsfunktion nicht umgangen werden können.

34.3. Providerprofile

Providerprofile sind sehr einfach strukturiert. Jeder der Dienste, auf die typischerweise von außen auf den Intranator zugegriffen wird, kann separat freigeschaltet werden.

Die Providerprofile decken nur den Zugriff auf den Intranators selbst sowie Port-Forwarding ab. Soll eine De-Militarized-Zone (DMZ) verwendet werden, muss eine Vollständige Regelliste konfiguriert werden.

35. Kapitel - Vollständige Regellisten

Vollständige Firewall-Regellisten erlauben die volle Funktionalität der Firewall einzusetzen und sind daher etwas komplexer zu konfigurieren als die Firewall-Profile.

35.1. Komponenten

Um die Firewall-Konfigurationsoberfläche nicht mit IP-Adressen und Portnummern zu überfrachten, werden IPs, Netze etc. in Netzgruppen sowie Protokolle, Portnummern und -bereiche in Diensten zusammengefasst. Diese werden vorher zentral zusammengestellt und können dann in allen Firewall-Regeln eingesetzt werden. Zusätzlich werden die wichtigsten Dienste bereits in der Grundkonfiguration vordefiniert mit ausgeliefert.

35.1.1. Dienste

Unter „Netzwerk > Firewall > Dienste“ können Protokolle und Portnummern unter einem Dienst-Namen zusammengefasst werden. Dadurch werden sie in Firewall-Regeln nutzbar.

Ein Dienst besteht aus frei eingetragenen Ports und Protokollen (Freier Dienst) sowie aus anderen, bereits konfigurierten Diensten (Verwendete Dienste). Dadurch können Dienste aus mehreren anderen Diensten zusammengesetzt werden. Dies macht vor allem dann Sinn, wenn ein Protokoll aus mehreren Unterprotokollen besteht. Ein gutes Beispiel hierfür ist FTP, welches sich aus der FTP-Kontrollverbindung und der FTP-Datenverbindung zusammensetzt.

Bei den Protokollen TCP und UDP können sowohl Quell- als auch Zielports angegeben werden. Beide Male sind Sie nicht auf einzelne Ports beschränkt, sondern können auch komplett Portbereiche (wie z.B. Zielports 5000 bis 5050 für die Fernwartung des Intranator-Herstellers) konfigurieren.



Hinweis

Beachten Sie bitte, dass bei TCP typischerweise nur die Zielports festgelegt sind und der Quellport vom Client frei gewählt werden kann. Daher wird normalerweise nur der Zielport im Intranator eingetragen.

35.1.2. Netzgruppen

Unter „Netzwerk > Firewall > Netzgruppen“ können IPs, IP-Netze und IP-Bereiche als Netzgruppe zusammengefasst werden. Dadurch sind sie in Firewall-Regeln nutzbar. Alle Rechner, Netzbereiche, Routings etc., die Sie im Intranator in den entsprechenden Menüs eingetragen haben, sind direkt als Netzobjekte in der Firewall verfügbar und müssen nicht zuerst als Netzgruppe konfiguriert werden.

Genau wie bei den Diensten kann eine Netzgruppe andere Netzgruppen enthalten.

Einzelne IPs werden unter Freier Rechner/Subnetz mit der Netzmaske 255.255.255.255 eingetragen. Möchten Sie einen Netzbereich konfigurieren, der auch als IP-Netz darstellbar ist (z.B. IPs von 192.168.1.0 bis 192.168.1.255), dann empfiehlt es sich, diesen als IP-Netz mit der passenden Netzmaske (im Beispiel IP 192.168.1.0 mit Netzmaske 255.255.255.0) einzutragen. Dies führt intern zu schlankeren und schnelleren Firewallregeln.

35.1.3. Automatische Objekte

Der Intranator fasst ihm bekannte Objekte zu automatischen Objekten zusammen. Einige dieser Objekte hängen auch vom aktuellen Zustand ab, z.B. der aktuellen Internet-IP. Diese können direkt in Firewall-Regeln eingesetzt werden und bedürfen keiner weiteren Konfiguration.

Liste der automatischen Objekte:

Objekt	Beschreibung
Rechner und Bereiche	Alle im Intranator definierten Rechner und Bereiche. Bei DHCP-Bereichen betrifft dies nur die belegten IPs.
DHCP-Bereiche	Alle DHCP-Bereiche (auch die nicht belegten IPs).
Fernzugriff-Anschlüsse	IP-Adressen, die für Fernzugriff konfiguriert sind.
Entfernte VPN Netze	Die Netze hinter den aktuell aktiven VPN-Gegenstellen. Bei „LAN zu Host“-Verbindungen ist dies die VPN-Gegenstelle selbst.
Intranator LAN IPs	IP-Adressen des Intranators in allen seinen Netzen vom Typ „LAN mit NAT“ und „LAN ohne NAT“.
Alle lokalen Netze	Alle Netze („LAN mit NAT“ und „LAN ohne NAT“) und Routings.
Broadcast-IPs aller lokalen Netze	Broadcast-IPs aller lokalen Netze.
Aktuelle Internet IP	Aktuelle IP des Intranators im Internet. Ist das System offline, so trifft diese Bedingung nicht mehr zu.
Internet	Alles außerhalb der lokalen Netze und VPNs.

35.2. Regellisten

35.2.1. Grundeinstellungen

Bei jeder Regelliste wird eingestellt, ob Sie für das Lokale Netz und VPNs oder für den Zugriff vom Internet (Provider) genutzt werden kann. Diese Unterscheidung ist ein zusätzlicher Schutz, damit man nicht aus Versehen z.B. eine Regel mit Vollzugriff für Verbindungen aus dem Internet festlegen kann.

Beinahe alle Protokolle erwarten auf ein gesendetes IP-Paket eine Antwort. Bei TCP können z.B. überhaupt erst Daten fließen, sobald die Gegenstelle den Aufbau der Verbindung bestätigt hat. Daher muss eigentlich für fast alle Protokolle nicht nur der Hinweg der Pakete in der Firewall zugelassen werden, sondern auch der Rückweg für die Antwortpakete geöffnet werden.

Damit man nun nicht jede Regel an zwei oder mehr Stellen eintragen muss, kann der Intranator jedes Antwortpaket automatisch der entsprechenden Verbindung zuordnen (Stateful Firewall). Über die Option Automatische Antwortregel werden diese Antwortpakete automatisch durch die Firewall gelassen. Nur in ganz wenigen Ausnahmen macht es Sinn, auf die automatische Antwortregel zu verzichten.

35.2.2. Durchlaufen der Regelliste

Eine Regelliste wird von oben nach unten abgearbeitet. Treffen alle Bedingungen einer Regel zu („Match“), wird die Aktion der Regel ausgeführt. Bei den meisten Aktionen ist der Durchlauf für dieses Paket beendet, spätere Regeln haben keine Auswirkung (die erste zutreffende Regel entscheidet).

Trifft keine Regel einer Regelliste zu, wird das Paket verworfen (implizites Deny). Dies wird durch die unveränderliche Regel am Schluss der Regelliste visualisiert. Wird ein Paket an eine andere Regelliste weitergeleitet und trifft dort keine Regel zu, wird das Paket an die ursprüngliche Regelliste zurückverwiesen. Die in der weitergeleiteten Regelliste angezeigte „Deny“ Regel gilt nicht für den Rücksprung.

35.2.3. Verknüpfung der Regel-Kriterien

Sind verschiedene Kriterien einer Regel aktiviert (z.B. Quelle, Dienst und Verbindungsstatus), so müssen alle diese Kriterien zum Ausführen der Aktion auf das Paket zutreffen. Sind bei einer Regel keine Kriterien eingetragen, wird die Aktion immer ausgeführt.

Bei den Kriterien „Quelle“, „Ziel“ und „Dienst“ können mehrere Möglichkeiten eingestellt werden. Es reicht, wenn eine davon zutrifft (Oder-Verknüpfung).

Beispiel:

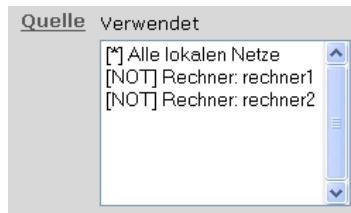


Quelle	Dienst	Trifft zu
Rechner1	Ping	Nein
Rechner1	HTTP	Ja
Rechner1	FTP	Ja
Rechner2	HTTP	Ja
Rechner2	FTP	Ja

Es können auch Objekte mit „Not“ in eine Regel eingefügt werden. Die Aktion wird ausgeführt, wenn dieses Objekt nicht im Paket vorkommt. Werden mehrere Objekte mit „Not“ eingestellt, darf keines davon vorkommen (Und-Verknüpfung).

Werden Objekte mit „Not“ und normale Objekte in einer Bedingung gemeinsam verwendet, muss mindestens eines der normalen Objekte zutreffen (Oder-Verknüpfung), aber keines der Objekte mit „Not“ (Und-Verknüpfung).

Beispiel:



Quelle	Trifft zu
Rechner1	Nein
Rechner2	Nein
Rechner3	Ja
Rechner aus dem Internet	Nein

35.2.4. Die Aktionen

Die Aktionen im Überblick:

Aktion	Beschreibung
Accept	Paket durchlassen.
Deny	Paket verwerfen, der Absender bekommt keine explizite Fehlermeldung (muss auf Timeout warten).
Reject	Paket verwerfen, zusätzlich dem Absender eine Fehlermeldung senden (ICMP Port unreachable).
Nothing	Nichts tun, Paket durchläuft die weiteren Regeln. Die Log-Option wird dennoch ausgeführt.
Weiterleiten an	Weiterleitung an eine andere Regelliste; Weiterleitung ist nur an vollständige Regellisten gleichen Typs möglich.
Return	Rücksprung an ursprüngliche Regelliste. Wurde keine Weiterleitung verwendet, ist dies gleichbedeutend mit „Deny“.
Transproxy	Umleitung auf den HTTP-Proxy des Intranators (nur bei Typ „LAN, Fernzugriff und VPN“). Regeln für den transparenten Proxy müssen immer an Anfang einer Regelliste stehen.

Wir empfehlen für das Blocken von Paketen aus dem LAN „Reject“ zu verwenden. Der Vorteil gegenüber „Deny“ ist, dass der Benutzer sofort eine Fehlermeldung bekommt und nicht erst auf einen Timeout warten muss.

Für Pakete aus dem Internet (in einer Provider-Regel) empfehlen wir dagegen „Deny“, denn die sofortigen Rückmeldungen von „Reject“ beschleunigen und vereinfachen einen Portscan aus dem Internet erheblich.

35.2.5. Extra-Optionen

Auf der Karteikarte „Extra“ sind noch weitere Bedingungen untergebracht.

35.2.5.1. Zeitprofile

Sie können unter Netzwerk > Firewall > Zeiten Zeitprofile definieren. Diese Zeitprofile können dann bei jeder Regel als Bedingung hinzugefügt werden. Nur innerhalb des definierten Zeitprofils trifft die Bedingung zu; nur dann kann die Aktion ausgeführt werden.

35.2.5.2. Logging

Logging ist keine Bedingung, sondern wie eine weitere Aktion: Ist das Logging aktiv und alle Bedingungen treffen zu, dann wird die Daten des Pakets plus der in der Regeln angegebene Logging-Text in der messages-Logdatei protokolliert.

35.2.5.3. Limitierung

Limits können für die Aktion und für das Logging separat konfiguriert werden. Eine Limitierung für die Aktion bedeutet, dass die Aktion nicht ausgeführt wird, sobald das Limit überschritten wurde. Eine Limitierung für das Log bedeutet, dass das Paket nicht protokolliert wird, sobald das Limit überschritten wurde.

Limitiert werden kann auf eine bestimmte Anzahl von Paketen pro Zeiteinheit. Über den Spitzenwert kann das Limit kurzfristig überschritten werden. Wurde in einer Zeiteinheit der Spitzenwert ausgenutzt, steht er in den folgenden Zeiteinheiten erst wieder zur Verfügung, wenn zwischendurch das Limit in einer Zeiteinheit nicht ausgenutzt wurde.

35.2.5.4. Paketgröße

Eine Bedingung, die zutrifft, sobald das Paket eine Größe in dem angegebenen Bereich hat.

35.2.5.5. Verbindungsstatus

Der Intranator verwendet eine stateful Firewall. Das bedeutet, er ordnet jedes Paket einer Verbindung zu und kann sich für jede dieser Verbindungen den Zustand merken. Über die Bedingung Verbindungsstatus kann man auf diese Daten zugreifen.

Neu	Erstes Paket, das eine neue Verbindung aufbaut
Ungültig	Das Paket setzt entweder eine bestehende Verbindung voraus, die nicht existiert, oder passt nicht zu einem bestehenden Verbindungsstatus
Aufgebaut	Das Paket gehört zu einer bereits bestehenden Verbindung
Zugehörig	Die Verbindung dieses Pakets gehört logisch zu einer anderen, bereits bestehenden Verbindung (z.B. Pakete von ftp-data sind zugehörig zu ftp-control)
Portforwarding	Die Verbindung des Pakets wird über Portforwarding weitergeleitet
Statische NAT	Die Verbindung des Pakets wird über statische NAT weitergeleitet

35.2.5.6. TCP-Flags

Diese Bedingung wird normalerweise nicht benötigt, der Verbindungsstatus bietet mehr Möglichkeiten.

35.2.6. Besonderheiten bei Provider-Regellisten

Einige Server (vor allem öffentliche FTP-Server) versuchen bei einem Verbindungsauftbau Benutzerdaten über das ident-Protokoll zu ermitteln. Dazu baut der Server eine Verbindung zu TCP-Port 113 des aufrufenden Clients auf. Wegen NAT landet dieser Aufruf normalerweise beim Intranator und wird durch die Provider-Regel blockiert.

Die meisten dieser Server warten aber auf einen Timeout oder eine Fehlermeldung vom ident, bevor sie einen Login erlauben. Daher hat es sich bewährt, in jede Providerregel ein „Reject“ für das ident-Protokoll einzufügen.

36. Kapitel - Weitere Funktionen

36.1. MAC-Adressen überprüfen

Unter „Netzwerk > Firewall > Einstellungen“ kann die Überprüfung der MAC-Adressen aktiviert werden. Die MAC-Adressen der einzelnen Rechner werden unter „Netzwerk > Intranet > Rechner“ eingetragen. Dann wird bei jedem eingehenden Paket geprüft, ob es wirklich von der zur IP gehörenden MAC kommt. Außerdem wird sichergestellt, dass von einer MAC nur die hinterlegte IP verwendet wird.

Sollte bei einem Rechner keine MAC hinterlegt sein, so ignoriert die MAC-Überprüfung die IP dieses Rechners. Auch bei IP-Bereichen können keine MACs hinterlegt oder überprüft werden.

Sollten IP und MAC nicht übereinstimmen, wird jeglicher Zugriff verweigert und mit der Kennung „BADMAC“ in der messages-Logdatei protokolliert.

36.2. Spoofing im LAN verhindern

Der Intranator stellt in allen Fällen sicher, dass lokale IP-Adressen nur über die entsprechenden LAN-Schnittstellen auf den Intranator zugreifen können. Sollte ein Paket mit einer Quelladresse aus einem der lokalen Netze über die Internetverbindung hereinkommen, wird es auf jeden Fall sofort verworfen.

Über die Option Vortäuschung von IP-Adressen (Spoofing) im LAN verhindern kann darüber hinaus noch sichergestellt werden, dass bei mehreren Routings im lokalen Netz die Pakete nicht über beliebige LAN-Schnittstellen auf dem Intranator eintreffen dürfen, sondern nur über die, die mittels der Gateway-IP des Routings ausgewählt wurde.

36.3. Blockieren von IPs nach zu vielen Loginfehlern

Ist diese Option aktiviert, zählt der Intranator die Loginfehler jeder IP auf allen von ihm angebotenen Protokollen. Wird die Schwelle von 10 Loginfehlern innerhalb von 5 Minuten überschritten, wird die IP bei jedem weiteren Zugriffsversuch auf beliebige Dienste für 5 Minuten blockiert. Bei mehreren Versuchen addiert sich die Blockierdauer.

Die Zugriffsversuche von blockierten IPs werden mit der Kennung „BLOCKED_IP“ in der messages-Logdatei protokolliert.

36.4. Firewall-Notmodus

Für den Fall, dass Sie sich einmal selbst mit der Firewall aussperren: Im Kommandozeilenumenü (siehe Abschnitt 7.4, „Firewall-Notmodus“) kann der „Firewall Notmodus“ aktiviert werden. Dieser erlaubt den Zugriff aus dem lokalen Netz sowie Surfen ins Internet. Der Notmodus wird bei der nächsten Änderung an der Firewall automatisch deaktiviert.

Ist der Notmodus aktiv, wird ein Hinweis auf der Hauptseite angezeigt.

37. Kapitel - Fallbeispiele und Aufgaben

37.1. Aufgabe 1: Erweitern eines einfachen Rechnerprofils

Gegeben ist folgendes einfaches Rechnerprofil:

- Zugriffsberechtigung: WWW/FTP/E-Mail/News
- Zugriff auf lokale Netze nicht erlaubt
- keine zusätzlichen Dienste freigegeben
- Webzugriff über Proxy: Proxyzwang
- Faxversand erlaubt: aktiv
- E-Mail-Transfer nur über Intranator: aktiv

Legen Sie dieses Rechnerprofil an. Wandeln Sie es dann in eine vollständige Firewallregelliste um und fügen eine Regel hinzu, die den Zugriff per RDP-Protokoll auf einen Server im Internet mit der IP 11.22.33.44 erlaubt.

Legen Sie einen Rechner mit dem Namen "R10" und der IP 192.168.1.10 an und weisen ihm diese Firewallregelliste zu.

37.1.1. Musterlösung

Anlegen einer Netzgruppe für den Rechner 11.22.33.44 unter Netzwerk > Firewall > Netzgruppen

The screenshot shows the 'Netzwerk > Firewall > Netzgruppen' section of the Intra2net Business Server administration interface. On the left, a sidebar menu is visible with items like 'Hauptseite', 'Benutzermanager', 'Netzwerk' (selected), 'Provider', 'Intranet', 'Firewall' (selected), 'Regeln', 'Dienste', 'Netzgruppen' (selected), 'Zeiten', 'Port Forwarding', 'Statistische NAT', 'Einstellungen', 'DNS', 'Interfaces', 'Fernzugriff', 'Dienste', 'System', and 'Information'. The main panel has a title 'Gruppe' and 'Einstellungen'. It shows a list box containing 'rpdserver'. Below it are buttons for 'Neu', 'Löschen', and 'Anzeigen'. To the right, there's a form for 'Name' (set to 'rpdserver') and 'Verwendet' (set to '[Freier Rechner] 11.22.33.44'). A 'Löschen' button is also present. A 'Verfügbar' dropdown menu lists various network-related options like 'Rechner und Bereiche', 'DHCP Bereiche', and 'Alle lokalen Netze'. At the bottom, there's a 'Freier Rechner/Subnetz' section with fields for 'Kommentar', 'IP-Adresse' (set to '255'), 'Netzmaske' (set to '255.255.255.255'), and a 'Hinzufügen' button.

Firewall Regelliste

Name Aufgabe 1						
Verwendbar für LAN, Fernzugriff und VPN						
Automatische Antwortregel <input checked="" type="checkbox"/>						
#	Quelle	Ziel	Dienst	Aktion	Kommentar	Extra
01	Alle	Intranator LAN IPS, Aktuelle Internet IP	ntp, http-proxy, email, hylafax	Accept	Intranator Dienste	↑↓
02	Alle	Internet	nntp, https, nntps, ping, ftp	Accept	Internet	↑↓
03	Alle	Entfernte VPN Netze	Alle	Accept	Entfernte VPN Netze	↑↓
04	Alle	rpdserver	rdp	Accept	RDP auf 11.22.33.44	↑↓
05	Alle	Alle	Alle	→ Weiterleitung	Basis LAN	↑↓
	Alle	Alle	Alle	Deny		█

Dem Rechner R10 die neue Firewall Regelliste zuweisen

The screenshot shows the Intranator Business Server administration interface. On the left, a sidebar menu includes sections like Benutzermanager, Netzwerk, Rechner (selected), Bereiche, Import/Export, DHCP, Routing, Firewall (selected), DNS, Interfaces, Fernzugriff, Dienste, System, Information, and Webmail. The main area is titled "Rechner" and shows a list with "r10" selected. To the right, there's a "Einstellungen" panel for "r10". It contains fields for Name (r10),Aliases (with a "Hinzufügen" button), Kommentar, IP-Adresse (192.168.1.10), MAC-Adresse (für DHCP) (Erkennen, Wake-On-LAN), Firewallregelliste (Aufgabe 1), Proxy Profil (Freier Zugriff), Email Relaying erlaubt (checked), and DNS-Anfragen ins Internet erlaubt (checked). A "Änderungen vormerken" button is at the bottom.

37.2. Aufgabe 2: Oberfläche nur für eine externe IP erreichbar

Ein Login auf der Intranator-Oberfläche per HTTPS für Fernwartung und Webgroupware soll aus dem Internet nur von einer einzigen IP (33.44.55.66) aus möglich sein. Der Zugriff auf SMTP, SMTP-Submission und IMAPS, nicht aber für weitere Dienste, ist von überall her möglich.

Legen Sie eine entsprechende Firewallregel an und weisen sie dem Standardprovider zu.

37.2.1. Musterlösung

Name Aufgabe 2						
Verwendbar für Provider						
Automatische Antwortregel <input checked="" type="checkbox"/>						
#	Quelle	Ziel	Dienst	Aktion	Kommentar	Extra
01	Alle	Alle	ident	Reject	Ident Dienst ablehnen	↑↓
02	Alle	Aktuelle Internet IP	imaps, icmp-basis, smtp, smtp-submission	Accept	Externe Dienste	↑↓
03	fernwartungs-pc	Alle	https	Accept	Fernwartung von 33.44.55.66	↑↓
	Alle	Alle	Alle	Deny		█

37.3. Aufgabe 3: Separiertes Gästenetz

Der Intranator ist mit zwei lokalen Netzen verbunden, das eine Netz wird für die Mitarbeiter verwendet, das andere steht für Gäste zur Verfügung. Mitarbeiter- und Gästenetz sollen strikt voneinander getrennt werden.

Im Detail:

- Das Mitarbeiter-Netz verwendet 192.168.1.0/24, das Gäste-Netz verwendet 192.168.5.0/24. Jedes der beiden Netze verwendet eine separate Schnittstelle des Intranators.
- Die Workstations im Mitarbeiter-Netz dürfen nur über den Proxy ins Internet, E-Mail ist nur über den Intranator möglich.
- Aus dem Gäste-Netz ist Vollzugriff ins Internet erlaubt. Zugriff auf den Intranator ist nur für DNS zulässig. Ein Zugriff ins Mitarbeiter-Netz darf auf keinen Fall möglich sein.
- Der Intranator ist DHCP-Server, aber nur für das Gäste-Netz. Richten Sie einen DHCP-Pool für das Gäste-Netz ein und achten darauf, dass die Gäste bei einer DHCP-Anfrage die korrekte Firewall-Regelliste zugewiesen bekommen.

37.3.1. Musterlösung

The screenshot displays two configuration screens for network rules (Regeln) under the Network (Netzwerk) section of the Intra2net Administrator.

Top Screen (Einstellungen):

- Regelliste:** Shows a list of network zones: LAN: Basis LAN, LAN: Basis LAN und lokale Netze, LAN: Gäste, LAN: Mitarbeiter, LAN: Nur E-Mail, LAN: Nur Vollzugriff, LAN: WWW, FTP, E-Mail + Transp. Proxy, Provider: Basis Provider, Provider: Provider mit HTTPS, VPN Socks: Nur Internet.
- Einstellungen:**
 - Name:** Mitarbeiter
 - Zugriffsberechtigung:** WWW/FTP/E-Mail/News (radio button selected)
 - Zugriff auf lokale Netze erlaubt:** Unchecked
 - Zusätzliche Dienste:** Freigegeben (checkbox checked), Verfügbar (checkbox checked)
 - Webzugriff über Proxy:** Kein Zugriff (radio button selected)
 - Faxversand erlaubt:** Unchecked
 - Mailtransfer nur über Intranator:** Checked
- Buttons:** Neu, Löschen, Anzeigen, Kopieren, Umwandeln, Einstellungen speichern.

Bottom Screen (Übersicht):

- Regelliste:** Shows a list of network zones: LAN: Basis LAN, LAN: Basis LAN und lokale Netze, LAN: Gäste, LAN: Mitarbeiter, LAN: Nur E-Mail, LAN: Nur Vollzugriff, LAN: WWW, FTP, E-Mail + Transp. Proxy, Provider: Basis Provider, Provider: Provider mit HTTPS, VPN Socks: Nur Internet.
- Übersicht:**
 - Name:** Gäste
 - Verwendbar für:** LAN, Fernzugriff und VPN
 - Automatische Antwortregel:** Checked
 - Tabelle (Rules):**

#	Quelle	Ziel	Dienst	Aktion	Kommentar	Extra
01	Alle	Intranator LAN IPs	dns	Accept	DNS auf Intranator	Up/Down
02	Alle	Internet	Alle	Accept	Vollzugriff ins Internet	Up/Down
03	Alle	Alle	Alle	Reject	Reject für alles andere	Up/Down
	Alle	Alle	Alle	Deny		Deny
 - Buttons:** Neu, Löschen, Anzeigen, Kopieren, IP Adressen anzeigen, Regel 01 an Position Ende Verschieben, Neue Regel an Position Ende Einfügen, Änderungen vormerken (Warteschlange wird aktiviert).

The figure consists of three vertically stacked screenshots of the Intra2net Administrator web interface, specifically the 'Netzwerk' (Network) section.

Screenshot 1: Interfaces Configuration

- Left Sidebar:** Shows 'Interfaces' selected under 'Netzwerk'.
- Central Area:** Shows a list of interfaces: eth0 (192.168.1.101), eth1 (DSL/Router), and eth2 (192.168.5.254). Buttons for 'Neu', 'Löschen', and 'Anzeigen' are present.
- Right Area: Einstellungen (Settings)**
 - Name: eth2
 - Kommentar: Gäste
 - Typ: LAN mit NAT (selected)
 - IP-Adresse: 192 . 168 . 5 . 254
 - Netzmaske: 255 . 255 . 255 . 0
 - Addressen anderer Netze umschreiben (NAT):
 - Firewallregelliste: Gäste
 - Proxy Profil: [Freier Zugriff]
 - E-Mail Relaying erlaubt:
 - DNS-Anfragen ins Internet erlaubt:

Screenshot 2: DHCP Configuration

- Left Sidebar:** Shows 'DHCP' selected under 'Netzwerk'.
- Central Area:** Shows settings for DHCP:
 - DHCP aktiv:
 - DNS Server 1: [] . [] . [] . []
 - DNS Server 2: [] . [] . [] . []
 - WINS Server: [] . [] . [] . []
 - Anderes Standard-Gateway: [] . [] . [] . []
 - NTP Server: []
 - IP Adresse überlassen für (Lease Time): 24 Stunden
 - DHCP-Server deaktivieren für: eth0 (192.168.1.101) (selected), eth2 (192.168.5.254) (button), Löschen (button), Hinzufügen (button)
- Bottom Button:** Einstellungen speichern (Save Settings)

Screenshot 3: DHCP Pool Configuration

- Left Sidebar:** Shows 'Bereiche' selected under 'Netzwerk'.
- Central Area:** Shows a 'Bereich' (Range) configuration for 'Gäste-Pool':
 - Bereich: DHCP: Gäste-Pool
 - Buttons: Neu, Löschen, Anzeigen
 - Einstellungen (Settings):
 - Name: Gäste-Pool
 - Kommentar:
 - Bereich von: 192 . 168 . 5 . 1
 - Bereich bis: 192 . 168 . 5 . 253
 - Als DHCP Pool verwenden:
 - Firewallregelliste: Gäste
 - Proxy Profil: [Freier Zugriff]
 - E-Mail Relaying erlaubt:
 - DNS-Anfragen ins Internet erlaubt:
- Bottom Area: DHCP Pool Informationen (DHCP Pool Information)**
 - Anzahl IPs gesamt: 253
 - Belegt: 0
 - Frei: 253
 - Freie IPs: 192.168.5.1-192.168.5.253
 - Belegte IPs: none

37.4. Aufgabe 4: Beschränkter Zugang aus dem VPN

Szenario:

- Eine Filiale ist per VPN an die Zentrale angebunden. Sie nutzt das Netz 192.168.4.0/24, die Zentrale 192.168.1.0/24.
- Die Rechner in der Filiale dürfen nur auf TCP Port 3306 (MySQL) des Datenbankservers (192.168.1.40) und per SMB/CIFS (vordefinierte Dienste: netbios und cifs) auf den

Fileserver (192.168.1.50) zugreifen; Zugriff auf Clients oder andere Rechner in der Zentrale ist nicht gestattet.

- Eine Applikation auf dem Datenbankserver druckt auf dem Netzwerkdrucker in der Filiale (IP 192.168.4.5) Aufträge aus (Protokolle IPP und printserver).
- Die Workstation des Administrators in der Zentrale (IP 192.168.1.20) hat Vollzugriff ins Internet und auf die Filiale
- Die sonstigen Workstations in der Zentrale dürfen nur über den Proxy ins Internet, E-Mail ist nur über den Intranator möglich

37.4.1. Musterlösung

Regel für die Rechner im LAN der Zentrale: umgesetzt mit einem Firewall Profil für Rechner

The screenshot shows the configuration for a 'Proxyzwang' firewall profile. Key settings include:

- Name:** Proxyzwang
- Zugriffsberechtigung:** WWW/FTP/Email/News (selected)
- Zugriff auf lokale Netze erlaubt:** Unchecked
- Zusätzliche Dienste:** Freigegeben (selected)
- Verfügbar:** A list of services including 'ah', 'bittorrent', 'bittorrent-dst', 'bittorrent-src', and 'chat'.
- Webzugriff über Proxy:** Proxyzwang (selected)
- Faxversand erlaubt:** Checked
- Mailtransfer nur über Intranator:** Checked

Der Workstation des Administrators wird die vordefinierte Regelliste Vollzugriff zugewiesen.

Firewall Regelliste für den Datenbankserver

The screenshot shows the 'Datenbank' firewall rule list. It includes:

- Name:** Datenbank
- Verwendbar für:** LAN, Fernzugriff und VPN
- Automatische Antwortregel:** Checked
- Rules:**

#	Quelle	Ziel	Dienst	Aktion	Kommentar	Extra
01	Alle	Netzwerkdrucker Filiale	ipp, printserver	Accept	Drucken in Filiale	Up/Down
	Alle	Alle	Alle	Deny		Up/Down

Dem Fileserver kann die vordefinierte Regelliste Basis LAN zugewiesen werden.

Regel für das VPN von der Filiale

The screenshot shows the 'VPN von Filiale' firewall rule list. It includes:

- Name:** VPN von Filiale
- Verwendbar für:** LAN, Fernzugriff und VPN
- Automatische Antwortregel:** Checked
- Rules:**

#	Quelle	Ziel	Dienst	Aktion	Kommentar	Extra
01	Alle	datenbank	mysql	Accept		Up/Down
02	Alle	fileserver	netbios, cifs	Accept		Up/Down
	Alle	Alle	Alle	Deny		Up/Down

37.5. Aufgabe 5: Webserver in der DMZ

Szenario:

- Ein Webserver steht in einer DMZ (De-Militarized Zone) und hat eine offizielle IP (LAN ohne NAT). Es wird klassisches Routing verwendet (siehe Abschnitt 11.7.1, „Klassisches Routing“).
- Der Router des Providers hat die IP 88.89.90.1, die externe IP des Intranators ist 88.89.90.2 (Netzmaske 255.255.255.252).
- Die DMZ nutzt das Netz 88.89.90.4/255.255.255.252 (30 Bit Netz mit 4 IPs), der Intranator hat die IP 88.89.90.5, der Webserver 88.89.90.6
- Vom Internet her ist der Zugriff auf die TCP-Ports 80 und 443 (vordefinierte Dienste http und https) des Webservers gestattet.
- Die Rechner aus dem LAN haben vollen Zugriff auf den Webserver
- Die Rechner aus dem LAN dürfen nur über den Proxy ins Internet, E-Mail ist nur über den Intranator möglich
- Der Webserver hat ausschließlich Zugriff auf TCP-Port 3306 eines Datenbankservers (IP 192.168.1.40) im LAN.
- Der Webserver darf die Dienste DNS und SMTP des Intranators nutzen.

37.5.1. Musterlösung

Den Rechnern im LAN wird ein Firewall Profil für Rechner zugewiesen, siehe vorige Aufgabe. Für den Vollzugriff auf den Webserver ist es nötig, die Checkbox bei Zugriff auf Lokale Netze erlaubt zu setzen.

Regel für die DMZ

Regel für die DMZ								
#	Quelle	Ziel	Dienst	Aktion	Kommentar	Extra		
01	Alle	datenbank	mysql	Accept	Datenbankzugriff			
02	Alle	Intranator LAN IPs	smtp, dns	Accept	Email-Versand und DNS			
	All	All	All	Deny				

Providerregel

Providerregel								
#	Quelle	Ziel	Dienst	Aktion	Kommentar	Extra		
01	Alle	Alle	ident	Reject	Ident Dienst ablehnen			
02	Alle	Aktuelle Internet IP	icmp-basis	Accept	Externe Dienste			
03	Alle	webserver	http, https	Accept	Zugriff von außen auf Webserver			
	All	All	All	Deny				

Teil 6. VPN

38. Kapitel - IPSec Grundlagen

38.1. IPSec

IPSec ist ein Standard, um lokale Netzwerke sicher über das Internet zu verbinden. Dabei legt IPSec so genannte Virtual Private Networks (VPN) an.

IPSec arbeitet dabei auf der IP-Ebene. Dies bedeutet, es werden keine Veränderungen (wie z.B. Verschlüsselungsmodule) in den verwendeten Programmen benötigt. Deshalb ist es auch mit allen TCP/IP basierten Netzwerkprogrammen kompatibel.

IPSec kann lokale Netze oder auch einzelne Clients mit privaten Netzwerkadressen über das Internet verbinden. Dazu werden die ursprünglichen IP-Pakete verschlüsselt und in neue Pakete eingepackt. Beim Empfänger werden die Pakete wieder ausgepackt, entschlüsselt, geprüft und weitergeleitet.

Bevor allerdings eine verschlüsselte Verbindung aufgebaut werden kann, müssen sich die beiden Verbindungspartner sicher sein, dass Ihr Gegenüber auch der ist, für den er sich ausgibt (Authentifizierung). Hierzu gibt es zwei Verfahren. Das eine wird Pre-Shared Key (PSK) oder auch Shared Secret genannt. Hierbei kennen beide Seiten ein gemeinsames Passwort. Bei dem anderen Verfahren wird die so genannte Public-Key Kryptographie eingesetzt.

38.2. Public-Key Kryptographie

Public-Key Kryptographie basiert auf einem mathematischen Verfahren, bei dem ein Schlüsselpaar aus einem geheimen Schlüssel (Private Key) und einem dazugehörigen öffentlichen Schlüssel (Public Key) erzeugt wird. Mit dem Public Key verschlüsselte Nachrichten können nur mit dem dazugehörigen Private Key entschlüsselt werden. Hat jemand nur den Public Key, so kann er nur verschlüsseln, nicht aber entschlüsseln.

Daher können die Public Keys problemlos auf unsicheren Kanälen (z.B. per E-Mail) ausgetauscht werden.

Die einzige Gefahr besteht darin, dass ein Angreifer den Schlüssel vertauscht haben könnte (sog. Man-in-the-middle Angriff). Wenn Sie ganz sicher gehen wollen, können daher nach dem Schlüsselaustausch die Signaturen (auch Fingerprint genannt) der Schlüssel z.B. am Telefon verglichen werden.

38.3. Zertifikate

Als Erweiterung zum Konzept von öffentlichen und privaten Schlüsseln gibt es Zertifikate. Dabei wird der öffentliche Schlüssel von einer Zertifizierungsstelle (engl. Certification Authority, abgekürzt CA), digital signiert. Das ermöglicht bei größeren Installationen, dass eine Gegenstelle anhand der digitalen Signatur feststellen kann, ob ein Schlüssel gültig ist, ohne dass der Schlüssel selbst vorher installiert wurde.

Für den Intranator bringt eine solche Zertifizierungsstelle normalerweise nur wenig Vorteile, dennoch setzt der Intranator konsequent den Zertifikatsstandard X.509 ein. Dieser Standard hat sich in der Praxis anstatt einfachen Public-/Private-Key-Paaren durchgesetzt.

Um die Bedienung zu vereinfachen, erzeugt der Intranator normalerweise selbstsignierte Zertifikate, bei denen der Inhaber (Subject genannt) auch gleichzeitig der Zertifikatsaus-

steller (Issuer) ist. Dadurch sind bei der Bedienung keine zusätzlichen Schritte für die Verwendung von Zertifikaten nötig. Selbstverständlich können aber auch externe Zertifizierungsstellen verwendet werden.

38.4. IPSec Verbindungen

Ein IPSec Verbindungsaufbau geschieht mit dem Protokoll Internet Key Exchange (IKE) in zwei Phasen.

Phase 1: Zuerst wird eine gesicherte Verbindung (ISAKMP SA oder IKE SA genannt) aufgebaut. Diese Verbindung wird über UDP Port 500 aufgebaut. Erkennt das System, dass eine Seite hinter einem NAT-Router steht, wird auf UDP Port 4500 umgeschaltet. Es gibt zwei Modi für den Verbindungsaufbau: den Main Mode und den Aggressive Mode. Der Aggressive Mode beschleunigt den Verbindungsaufbau um einige Zehntelsekunden, kann aber leichter geknackt werden. Der Intranator unterstützt daher nur den sicheren Main Mode.

Phase 2: Die zuvor aufgebaute gesicherte Verbindung wird nun genutzt, um die eigentlichen Verbindungsdaten und Sitzungsschlüssel auszuhandeln (Quick Mode). Ist dies erfolgreich, wird eine sog. IPSec SA konfiguriert und kann dann genutzt werden, um verschlüsselt Daten zu übertragen.

Beide Phasen der Verbindung haben aus Sicherheitsgründen nur eine begrenzte Lebensdauer und werden daher regelmäßig aktualisiert.

Aus Sicherheitsgründen und um das Routing zu vereinfachen überprüft jede Seite der Verbindung, dass nur genau die Pakete durch die Verbindung kommen, die vorher konfiguriert wurden. Daher ist es wichtig, dass auf beiden Seiten identische Werte für Start- und Zielnetz eines Tunnels angegeben wurden.

Damit die Sicherheitsrichtlinien sehr eng konfiguriert werden können, ist es möglich, zwischen zwei Rechnern beliebig viele verschiedene IPSec Verbindungen aufzubauen.

38.5. Algorithmen

Beide Seiten einigen sich beim Verbindungsaufbau über die für Verschlüsselung und Datensignierung zu verwendenden kryptographischen Algorithmen. Die Algorithmen sind für jede Phase separat einstellbar. Im Intranator können im Menü Dienste > VPN > Verschlüsselung Profile mit Algorithmen konfiguriert werden.

Eine Verschlüsselungsmethode besteht dabei aus je einem Algorithmus für Verschlüsselung, für Hashing (Signatur) und einer Diffie Hellman Gruppe für den Aufbau einer gesicherten Verbindung. Die meisten Algorithmen werden in verschiedenen Längen angeboten. Die Länge wird in Bit angegeben und der Algorithmus ist desto stärker, je mehr Bit verwendet werden. Allerdings steigt mit der Bitzahl auch der nötige Rechenaufwand.

Für beide Phasen wird nun eine Liste von möglichen Methoden hinterlegt. Diese Liste wird in der eingestellten Reihenfolge der Gegenstelle angeboten, die dann die oberste, von ihr auch unterstützte Methode verwendet.

Auch die Verwendung von Perfect Forward Secrecy (PFS) in Phase 2 wird im Intranator über die Verschlüsselungsprofile konfiguriert. Ist auf dem Intranator eine PFS-Gruppe vorgegeben, wird diese beim Verbindungsaufbau verwendet. Baut die Gegenseite die Verbindung auf, akzeptiert der Intranator die eingestellte und alle stärkeren Gruppen. Ist

die PFS-Gruppe auf ~~Keine~~ gestellt, werden Verbindungen ohne PFS aufgebaut. Baut die Gegenseite die Verbindung auf, werden Verbindungen mit und ohne PFS akzeptiert.

Alle angebotenen Algorithmen bieten aus heutiger Sicht eine ausreichende Stärke. Nicht mehr empfohlene Algorithmen wie z.B. einfaches DES mit 64 Bit werden vom Intranator gar nicht erst angeboten. Allerdings wurden in letzter Zeit in der kryptographischen Forschung einige mögliche Schwachstellen von vor allem MD5 als auch SHA diskutiert. Wir empfehlen daher, so bald wie möglich auf eine der stärkeren SHA2-Varianten (256, 384 und 512 Bit) umzusteigen.

38.6. Einschränkungen

Bei der Entwicklung von IPSec war Voraussetzung, dass keinerlei Information unverschlüsselt oder an nicht autorisierte Gegenstellen versendet werden darf. Leider bringt dies auch einige Einschränkungen in Verbindung mit dynamischen IP-Adressen mit sich:

Alle Informationen werden verschlüsselt übertragen, also auch die Kennung einer Station. Da bei dynamischen IPs weder anhand der IP-Adresse noch anhand der Kennung entschieden werden kann, welcher Schlüssel zur Entschlüsselung verwendet werden soll, müssen alle diese Gegenstellen denselben Schlüssel verwenden.

Zum Glück gilt diese Einschränkung nur für das Pre-Shared Key Verfahren; beim Einsatz von Public Key Verfahren kann jede Gegenstelle einen eigenen Schlüssel haben. Durch die Trennung von Public und Private Key ist dies möglich, ohne dass Daten gefährdet werden. Wir empfehlen daher, ausschließlich das Public Key Verfahren zu verwenden.

38.7. Kompatibilität mit anderen IPSec-Gegenstellen

IPSec ist standardisiert und der Intranator kann grundsätzlich mit allen standardkonformen Gegenstellen Verbindungen aufbauen. Allerdings erlaubt der IPSec-Standard sehr viele Wahlmöglichkeiten und Optionen, die teilweise auf beiden Seiten identisch eingestellt oder implementiert sein müssen. Daher können wir eine Kompatibilität nicht generell garantieren.

Viele einfache Geräte (z.B. kleine Router) unterstützen ausschließlich eine Authentifizierung mit Pre-Shared Keys. Wegen den im vorherigen Abschnitt beschriebenen Einschränkungen können wir dazu nur dann raten, wenn beide Seiten über feste IP-Adressen verfügen.

Sind keine festen IP-Adressen verfügbar, sollten Sie Router verwenden, die Public Key unterstützen. Die Konfiguration einiger dieser Router wird in den folgenden Kapiteln vorgestellt.

39. Kapitel - Schlüsselmanagement

Für Public-Key Verschlüsselungsverfahren müssen vor dem Verbindungsaufbau auf jeder Seite geheime Schlüssel erzeugt und die dazugehörigen öffentlichen Schlüssel mit der Gegenstelle ausgetauscht werden.

Hierzu ist im Intranator eine Schlüsselverwaltung vorgesehen.

39.1. Eigene Schlüssel

Im Menü System > Schlüssel > Eigene Schlüssel können eigene Schlüsselpaare aus Public- und Private-Key erzeugt werden.

Die Schlüssel werden nach dem X.509-Standard erstellt. Die meisten IPSec-Implementierungen beherrschen diesen Schlüsseltyp. Er hat einen etwas komplexeren Aufbau und kommt außer für IPSec auch für SSL/TLS (z.B. bei HTTPS) und zur Verschlüsselung von E-Mails (S/MIME) zum Einsatz.

Die Sicherheit der Verschlüsselung hängt unter anderem von der Schlüssellänge in Bit ab. Der Intranator unterstützt Schlüssellängen von 512 bis 4096 Bit. Je länger der Schlüssel, desto sicherer ist die Verbindung. Einige Gegenstellen unterstützen nicht alle Schlüssellängen oder werden durch zu lange Schlüssel überlastet. Wir empfehlen die Verwendung von 2048 Bit.

Als Inhaberdaten können bei X.509 Schlüsseln Landeskürzel (2-stellig), Bundesland, Stadt, Firmenname, Abteilungsname, Rechnername und E-Mail-Adresse angegeben werden. Es muss dabei entweder ein Rechnername oder eine E-Mail-Adresse angegeben sein, der Rest der Daten ist freiwillig.



Achtung

Die Inhaberdaten eines Schlüssels müssen unbedingt eindeutig sein. Die Inhaberdaten eines Schlüssels dürfen also auf diesem und allen per VPN verbundenen Geräten nur einmal vorkommen.

Aus Sicherheitsgründen ist die Gültigkeitsdauer eines X.509-Schlüssels beschränkt. Nach dem Ablauf der Gültigkeitsdauer wird der Schlüssel nicht mehr akzeptiert und muss erneuert werden. Eine Verlängerung der Gültigkeit ist nicht möglich.

Um den Public-Key an die Gegenstelle zu übermitteln, kann er mit Zertifikat exportieren in eine Datei gespeichert werden.

Wenn Sie auf dem Intranator mehrere VPNs einrichten, müssen Sie nicht für jede Verbindung extra einen eigenen Schlüssel anlegen: Sie können einen eigenen Schlüssel für alle VPNs verwenden. Nur von jeder der Gegenstellen benötigen Sie natürlich den öffentlichen Schlüssel.

39.1.1. Zertifizierungsstellen (CAs)

Um die Bedienung zu vereinfachen, erzeugt der Intranator normalerweise selbstsignierte Zertifikate, bei denen der Inhaber (Subject genannt) auch gleichzeitig der Zertifikatsaussteller (Issuer) ist.

Wenn Sie stattdessen eine CA verwenden wollen, so erzeugen Sie zuerst einen normalen Schlüssel. Unter dem Reiter CA können Sie eine Zertifikatsanforderung exportieren. Diese Zertifikatsanforderung wird von der CA signiert und kann dann als Zertifikat wieder in den Intranator importiert werden.

Einige VPN-Gegenstellen akzeptieren keine selbstsignierten Schlüssel, sondern fordern Schlüssel, die von einer CA signiert wurden. Um Kompatibilität mit solchen Gegenstellen einfach herzustellen, gibt es die Option Schlüssel mit einem anderen Schlüssel signieren.

Wenn Sie es mit einer solchen Gegenstelle zu tun haben, gehen Sie wie folgt vor:

1. Legen Sie einen neuen eigenen Schlüssel vom Typ X.509 an. Dieses Zertifikat wird nur indirekt zum Signieren verwendet, nennen Sie es deshalb beispielsweise **intranator-ca**.
2. Exportieren Sie dieses Zertifikat und importieren es auf der Gegenseite als vertrauenswürdige Root-CA.
3. Legen Sie nun auf dem Intranator einen weiteren eigenen Schlüssel an. Dieser wird nachher vom Intranator für das VPN genutzt.
4. Verwenden Sie die Option Schlüssel mit einem anderen Schlüssel signieren um diesen Schlüssel mit dem vorher erstellen CA-Schlüssel zu signieren.

39.2. Fremde Schlüssel

Damit der Intranator eine Verbindung aufbauen kann, muss er zuerst den Public-Key der Gegenstelle kennen. Exportieren Sie ihn daher auf der Gegenstelle, übertragen und importieren ihn.

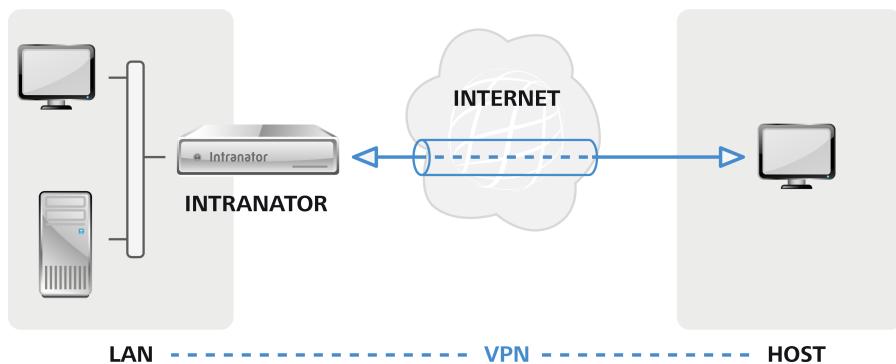
Gehen Sie zum Importieren auf die Seite System > Schlüssel > Fremde Schlüssel, wählen einen Namen und stellen den Schlüsseltyp ein. Öffnen Sie nun den Schlüssel in einem Texteditor, markieren und kopieren ihn in die Zwischenablage. Nun können Sie ihn in das Copy & Paste Feld einfügen.

Falls Sie die Schlüssel übers Internet übertragen haben, können Sie die Signaturen (auch Fingerprint genannt) der Schlüssel am Telefon vergleichen. Ein Angreifer könnte sonst den Schlüssel unbemerkt vertauscht haben und damit die Verschlüsselung unterwandern (so genannter Man-in-the-middle Angriff). Aus Kompatibilitätsgründen unterstützt der Intranator die beiden gängigsten Fingerprint-Verfahren MD5 und SHA1. Es reicht aus, wenn Sie einen der beiden Fingerprints vergleichen.

40. Kapitel - Anbinden von einzelnen PCs

40.1. Konzept

Um einen einzelnen Rechner mit dem Firmennetz zu verbinden, kann man eine IPSec-VPN-Clientsoftware auf dem Rechner installieren und darüber eine VPN-Verbindung herstellen.



Solche einzelnen Rechner befinden sich meistens hinter Routern, die ihr lokales Netz per NAT maskieren. Bei mobilen Rechnern ändert sich die IP im lokalen Netz zusätzlich bei jedem Standortwechsel oder Einwahlvorgang. Das stellt an sich kein Problem dar, aber deshalb können VPN-Clients nicht einfach Ihre IP im aktuellen lokalen Netz für das VPN verwenden, sondern greifen auf eine vorher festgelegte, virtuelle IP zurück. Diese wird im Intranator und im Client einmal beim Einrichten festgelegt und gilt ab da dauerhaft für diesen einen Client.

Sollte das lokale Netz, in dem sich der Client gerade befindet, das selbe IP-Netz verwenden wie das Firmennetz, mit dem Sie die VPN-Verbindung aufbauen möchten, können die IPs nicht mehr eindeutig zugeordnet werden und die Verbindung schlägt fehl.

40.2. Konfiguration auf dem Intranator

40.2.1. Voraussetzungen

Als erstes müssen Sie dafür sorgen, dass jede Seite über einen eigenen Schlüssel verfügt und die Gegenseite den öffentlichen Schlüssel oder das Zertifikat der Gegenseite hat. Es empfiehlt sich, auf jedem System einen eigenen Schlüssel nur für VPNs anzulegen.

Wenn Sie auf dem Intranator mehrere VPNs einrichten, müssen Sie nicht für jede Verbindung extra einen eigenen Schlüssel anlegen: Sie können einen eigenen Schlüssel für alle VPNs verwenden. Nur von jeder der Gegenstellen benötigen Sie natürlich den öffentlichen Schlüssel.

Weitere Details zur Schlüsselverwaltung finden Sie im 39. Kapitel, „Schlüsselmanagement“.

Eine auf dem Intranator konfigurierte Verbindung gilt für die Verbindung zwischen einem Client und einem Netz hinter dem Intranator. Möchten Sie vom Client auf mehrere Netze hinter dem Intranator zugreifen, können Sie einfach mehrere Verbindungen konfigurieren. Achten Sie darauf, für jede dieser Verbindungen immer dieselbe Kombination an Schlüsseln/Zertifikaten zu verwenden.

40.2.2. Grundeinstellungen

Im Menü Dienste > VPN > Verbindungen können Sie VPN-Verbindungen im Intranator konfigurieren.

Auf der ersten Seite stellen Sie die Gegenstelle ein. Die Gegenstelle ist bei einzelnen Rechnern üblicherweise nicht bekannt. Stellen Sie sie daher auf "Dynamische IP (Road Warrior)".

Über das Verschlüsselungsprofil können die verwendeten Verschlüsselungsalgorithmen ausgewählt werden; zu Details siehe Abschnitt 38.5, „Algorithmen“. Wichtig ist vor allem, dass die Einstellung für PFS (Perfect Forward Secrecy) auf beiden Seiten identisch ist.

Über die Kapselung wird kontrolliert, wie die Pakete für den VPN-Tunnel eingepackt werden. Bei ESP wird die Verschlüsselung und Authentifizierung in eine Hülle eingepackt. Bei ESP+AH werden Verschlüsselung und Authentifizierung separat vorgenommen. ESP+AH kann nicht durch NAT geleitet werden, daher sollten Sie für einzelne Rechner auf jeden Fall ESP verwenden. Diese Einstellung muss auf beiden Seiten der Verbindung identisch sein.

40.2.3. Authentifizierung

Wählen Sie den eigenen und den Schlüssel der Gegenseite aus.



Einige Clientprogramme bieten die Möglichkeit, zusätzlich zu einer Authentifizierung per Pre-Shared Key (PSK) oder Zertifikaten noch Login und Passwort eines Benutzers zu überprüfen. Dies geschieht mittels des Protokolls Extended Authentication (XAUTH). Soll dies von Clients genutzt werden, aktivieren Sie die Option XAUTH Servermodus.

Der XAUTH Servermodus fordert jetzt vom Client dieser Verbindung die Anmeldung mit den Daten eines Intranator-Benutzers, der Mitglied einer Gruppe mit dem Recht Anmeldung am VPN mit XAUTH ist. Dieses Gruppenrecht können Sie auf der Seite Benutzermanager > Gruppen : Rechte vergeben.

Wir raten aus den in Abschnitt 38.6, „Einschränkungen“ genannten Gründen davon ab, Verbindungen per Pre-Shared Key (PSK) zu authentifizieren. Vor allem bei mehreren mobilen Rechnern ist diese Lösung besonders gefährlich.

40.2.4. Tunnel konfigurieren

Auf der Seite "Tunnel" wird konfiguriert, welches Netz durch diese VPN-Verbindung mit welcher virtuellen Client-IP verbunden wird.

Über den Punkt Lokales Netz wird das zu verbindende Netz auf Seite des Intranators gewählt. Wählen Sie bei der Option Lokale Netze eines der direkt an den Intranator angeschlossenen oder gerouteten Netze aus.

Möchten Sie, dass jeglicher Datenverkehr des Clients über den Intranator läuft und damit auch von der Firewall und dem Proxyserver profitiert, stellen Sie bei Lokales Netz die Option Alles (0.0.0.0/0.0.0.0) ein.

Wählen Sie bei Netz auf Gegenseite den Typ Freies Netz. Wählen Sie eine bislang unbekannte IP, die auch nicht in einem der Netze des Intranators oder des Clients liegt. Dies ist die virtuelle IP, die Sie auch im Client eintragen müssen. Verwenden Sie immer 255.255.255.255 als Netzmaske.

Die meisten VPN-Clients können sich ihre virtuelle IP und zugehörigen DNS-Server über die Protokollerweiterung Mode Config automatisch zuweisen lassen. Wenn Ihr Client dies unterstützt (z.B. Shrew Soft, NCP oder iPhone, siehe Beschreibung der einzelnen Clients), stellen Sie die Option Netz auf Gegenseite auf IP zuweisen und tragen die IP ein, die der Client bekommen soll. Als DNS-Server übermittelt der Intranator automatisch seine eigene IP.

The screenshot shows the 'Verbindungen' (Connections) section of the Intranet Business Server. Under 'Schritt 2 von 4: Tunneleigenschaften festlegen' (Step 2 of 4: Tunnel properties), the 'Lokales Netz' (Local Network) is set to 'Aktuelle Internet IP oder Intranator LAN IPs' (Current Internet IP or Intranator LAN IPs) with the value '192.168.1.0 / 255.255.255.0'. The 'Netz auf Gegenseite (an Gegenstelle übermittelt)' (Network on the other side (sent to the opposite side)) is set to 'IP zuweisen (mode-config)' with the value '192.168.99.1'. Under 'Adressumschreibung (NAT)', the 'Locale IPs umschreiben (an Gegenstelle übermittelt)' (Local IPs rewrite (sent to the opposite side)) is set to 'unverändert'. The 'Gegenseiten-IPs 1:1 auf Netz umschreiben' (Peer-side IPs 1:1 rewrite to network) and 'Gegenseiten-IPs bei Internetzugriff umschreiben (NAT)' (Peer-side IPs rewrite during Internet access (NAT)) checkboxes are checked. A 'Einstellungen speichern' (Save settings) button is at the bottom.

Wurde unter Lokales Netz ein Netz eingestellt, welches Adressen enthält, die nicht in lokalen oder anderen VPN-Netzen liegen, kann der Client über das VPN aufs Internet zugreifen. Dies gilt insbesondere für die Einstellung Alles. Da die virtuelle IP normalerweise aus einem privaten Adressbereich stammt, kann sie über die Option Gegenseiten-IPs bei Internetzugriff umschreiben auf die externe Adresse des Intranators umgeschrieben werden (NAT). Diese NAT wird nur bei Zugriffen ins Internet aktiv, Zugriffe aufs lokale Netz geschehen weiterhin mit der virtuellen IP.

Die weiteren Optionen der Adressumschreibung (NAT) werden im 54. Kapitel, „Lösen von IP-Adresskonflikten in VPNs durch NAT“ erklärt.

40.2.5. Rechte

In diesem Menü werden die Rechte des VPN-Clients definiert. Dies betrifft alle Pakete, die vom VPN-Client kommen. Eine Beschreibung der Rechteoptionen finden Sie unter Abschnitt 9.2, „Zugriffsrechte eines Netzwerkobjekts“.

The screenshot shows the 'Verbindungen' (Connections) section of the Intranet Business Server. Under 'Schritt 3 von 4: Rechte konfigurieren' (Step 3 of 4: Configure rights), there are dropdown menus for 'Firewallregelliste' (Firewall rule list) set to 'Vollzugriff' and 'Proxy Profil' (Proxy profile) set to 'Freier Zugriff'. Below these are checkboxes for 'Email Relaying erlaubt' (Email relay allowed) and 'DNS-Anfragen ins Internet erlaubt' (DNS queries to the Internet allowed), both of which are checked. A 'Einstellungen speichern' (Save settings) button is at the bottom.

40.2.6. Aktivierung

In diesem Menü wird konfiguriert, wann die Verbindung aufgebaut und bestehende Sitzungen verlängert werden. Bei VPN-Clients kann der Intranator selbst die Verbindung nicht initiieren. Stellen Sie daher den Start auf Passiv / manuell und verwenden für die restlichen Optionen die vorgegebenen Werte.

The screenshot shows the Intranator Business Server administration interface. The left sidebar menu is visible, with 'Verbindungen' (Connections) selected. The main content area is titled 'Schritt 4 von 4: Aktivierungsart festlegen' (Step 4 of 4: Define Activation Type). The configuration options are as follows:

- Start:** Radio button selected for 'Passiv / manuell' (Passive / manual).
- Aufbauversuche:** Input field set to 3.
- Lebensdauer IKE/Phase 1:** Input field set to 480 Minuten (Minutes).
- Lebensdauer IPSec SA/Phase 2:** Input field set to 60 Minuten (Minutes).
- Offline-Erkennung alle:** Input field set to 0 Sekunden (Seconds).

At the bottom right of the configuration area is a blue button labeled 'Einstellungen speichern' (Save settings).

41. Kapitel - VPN mit dem NCP Secure Entry Client

Den NCP Secure Entry Client für Windows können Sie von dieser URL als 30-Tage-Testversion herunterladen: <http://www.ncp-e.com/de/downloads/software.html>

41.1. Installation

1. Starten Sie das Installationsprogramm, installieren die Software mit allen Modulen und starten Sie den Rechner neu.
2. Laden Sie vom Intranator unter "Information > Download >" das "Programm zum Erzeugen von Zertifikaten" (makecert) herunter und entpacken Sie es in ein Verzeichnis auf Ihrem Rechner.

41.2. Zertifikate

Der NCP Secure Entry Client kann keine eigenen Zertifikate erstellen. Dies übernimmt daher das Programm makecacert, welches im makecert-Paket enthalten ist. Der Unterschied zwischen makecacert und makecert ist, dass makecert selbstsignierte Zertifikate erzeugt, makecacert dagegen welche, die von einer (dummy) Zertifizierungsstelle (CA) signiert wurden.

1. Starten Sie die makecacert-Batchdatei und wählen eine Laufzeit in Jahren für Ihr Zertifikat.

```
c:\makecert>makecacert.bat
Gueltigkeit des neuen Zertifikats:
1. Ein Jahr
2. Zwei Jahre
3. Drei Jahre
4. Vier Jahre
5. Fuenf Jahre
Ihre Wahl: 1

c:\makecert>openssl req -newkey rsa:2048 -days 365 -x509 -out cacert.pem -keyout
cakey.pem -config openssl-ca.cnf -batch -passout pass:geheim -set_serial 31659

Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'cakey.pem'
-----

c:\makecert>openssl req -newkey rsa:2048 -nodes -config openssl.cnf -keyout priv
atekey.pem -out request.pem
Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'privatekey.pem'
-----
```

2. Sie werden nach den Inhaberdaten des neuen Zertifikats gefragt. Es kommt vor allem darauf an, dass die dort eingetragen Daten eindeutig sind und in dieser Form nicht in einem anderen Zertifikat verwendet werden. Wir empfehlen, z.B. den Benutzernamen

in das Feld "Common Name" einzufügen. Hier in diesem Beispiel ist dies "Markus Mustermann".

Bitte verwenden Sie keine Umlaute und Sonderzeichen, da dies zu Problemen führen kann.

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

```
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:Markus Mustermann
Email Address []:
```

```
c:\makecert>openssl x509 -days 365 -out newkey_cert.cer -in request.pem -req -CA cacert.pem -CAkey cakey.pem -set_serial 1 -passin pass:geheim
Loading 'screen' into random state - done
Signature ok
subject=/CN=Markus Mustermann
Getting CA Private Key

c:\makecert>del request.pem

c:\makecert>rem --- please enter the transport password now (just used for trans
port, enter this one while importing) ---

c:\makecert>openssl pkcs12 -export -in newkey_cert.cer -inkey privatekey.pem -ce
rtfile cacert.pem -out newkey.p12
Loading 'screen' into random state - done
```

3. Als nächstes müssen Sie ein Passwort für Ihr Zertifikat wählen. Mit diesem Passwort wird das Zertifikat (und damit der VPN-Zugang) geschützt. Sie müssen es beim Aufbau der VPN-Verbindung eingeben. Die Standardrichtlinie von NCP verlangt mindestens 6 Zeichen.

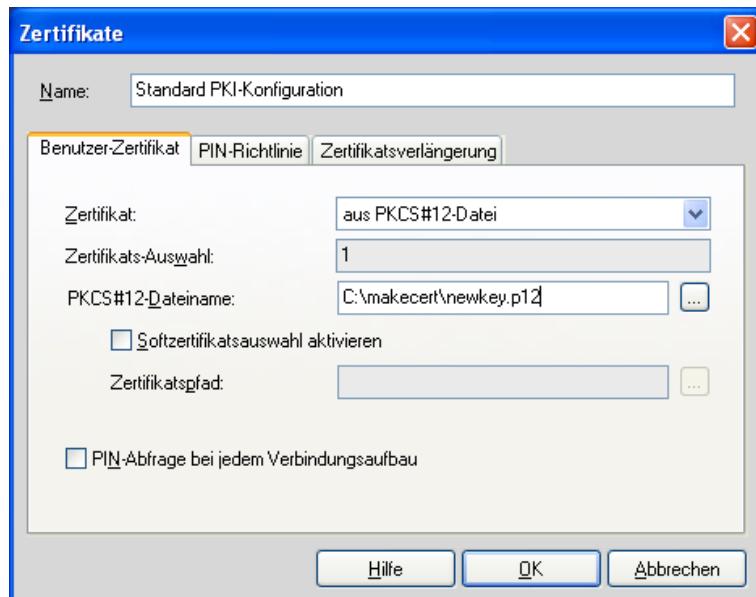
```
Enter Export Password:
Verifying - Enter Export Password:

c:\makecert>del privatekey.pem

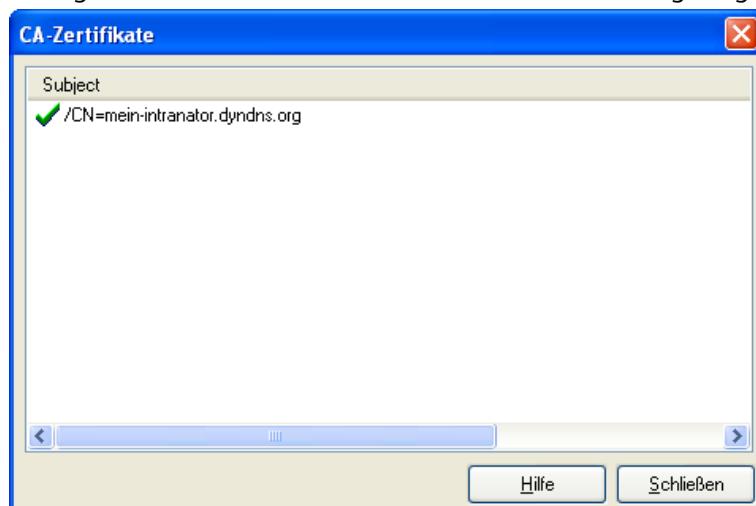
c:\makecert>del cacert.pem

c:\makecert>del cakey.pem
```

4. Das Schlüsselpaket für den Client liegt nun im PKCS#12-Format in der Datei newkey.p12, das Zertifikat für den Intranator (PEM-Format) in der Datei newkey_cert.cer.
5. Starten Sie den NCP Client Monitor und öffnen das Menü Konfiguration, Zertifikate. Bearbeiten Sie die Standard PKI-Konfiguration. Lassen Sie das Zertifikat aus einer PKCS#12-Datei laden und wählen die eben erzeugte Schlüsselpaket-Datei aus.

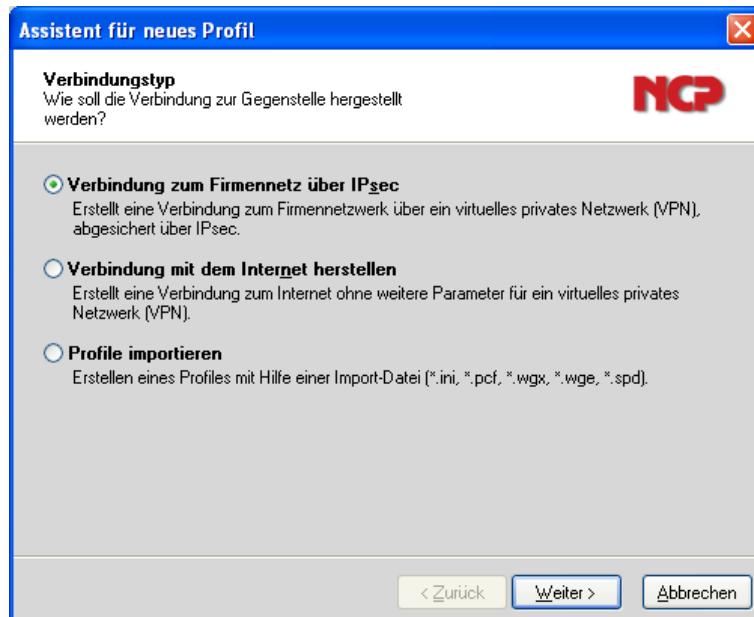


6. Als nächstes muss das Zertifikat des Clients auch dem Intranator bekannt gemacht werden. Öffnen Sie dazu die Zertifikatsdatei (`newkey_cert.cer`) mit einem Texteditor (z.B. Wordpad) und übernehmen den gesamten Inhalt der Datei in die Zwischenablage.
7. Öffnen Sie im Intranator das Menü System > Schlüssel > Fremde Schlüssel und legen einen neuen an. Vergeben Sie einen Namen für den Schlüssel (z.B. den Namen des Mitarbeiters) und fügen dann die Zertifikatsdaten aus der Zwischenablage in das Feld "Copy > Paste Schlüssel" ein.
8. Als letztes muss der NCP Client noch das Zertifikat des Intranators bekommen. Öffnen Sie das Menü System > Schlüssel > Eigene Schlüssel und wählen das Zertifikat aus, das Sie für die Verbindung verwenden wollen. Über den Link "Zertifikat exportieren" im Reiter "Daten" kann das Zertifikat in eine .pem-Datei gespeichert werden. Speichern Sie die Datei in das Verzeichnis `c:\Programme\NCP\SecureClient\CaCerts`.
9. Öffnen Sie im NCP Client Monitor das Menü Verbindung, Zertifikate, CA-Zertifikate anzeigen. Das Zertifikat Ihres Intranators sollte nun angezeigt werden.



41.3. Verbindungen

1. Öffnen Sie den NCP Client Monitor, Menü Konfiguration, Profil-Einstellungen. Starten Sie über Hinzufügen / Import den Konfigurations-Wizard.
2. Wählen Sie eine IPSec-Verbindung



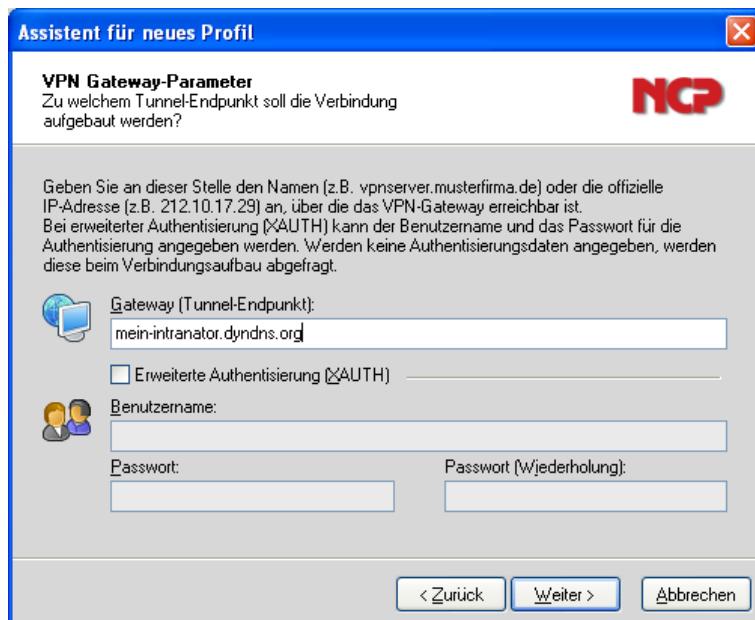
3. Vergeben Sie einen Namen für die Verbindung



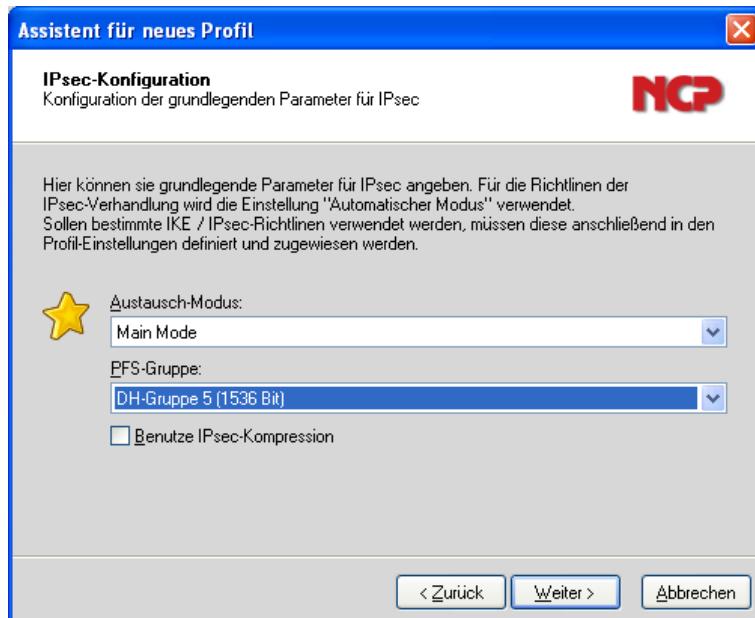
4. Verwenden Sie die automatische Medienerkennung.



5. Tragen Sie die (externe) IP oder den (Dyn-)DNS-Namen des Intranators als Gateway ein. Wenn Ihr Intranator über eine feste IP verfügt, ist es besser diese einzutragen, anstatt den DNS-Namen zu verwenden. Lassen Sie XAUTH inaktiv.



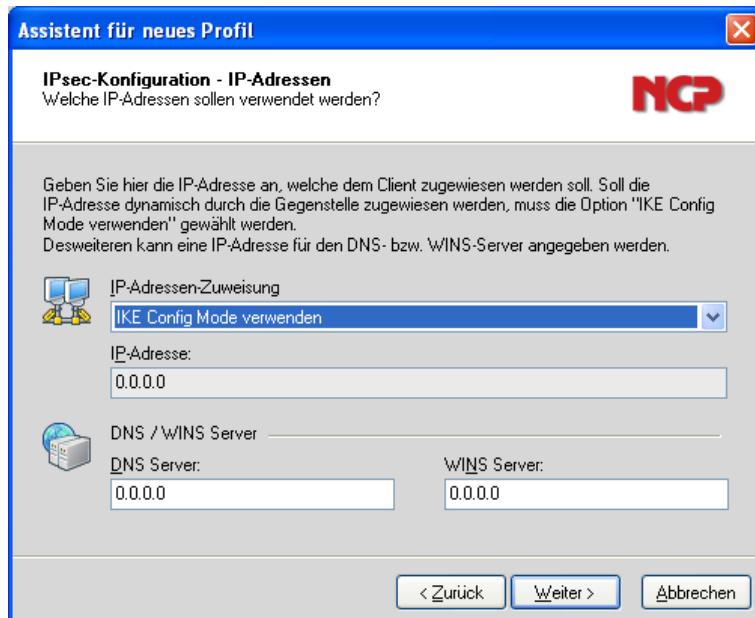
6. Verwenden Sie den "Main Mode" als Austausch-Modus und verwenden Sie die DH-Gruppe 5 (1536 Bit) für PFS (Perfect Forward Secrecy).



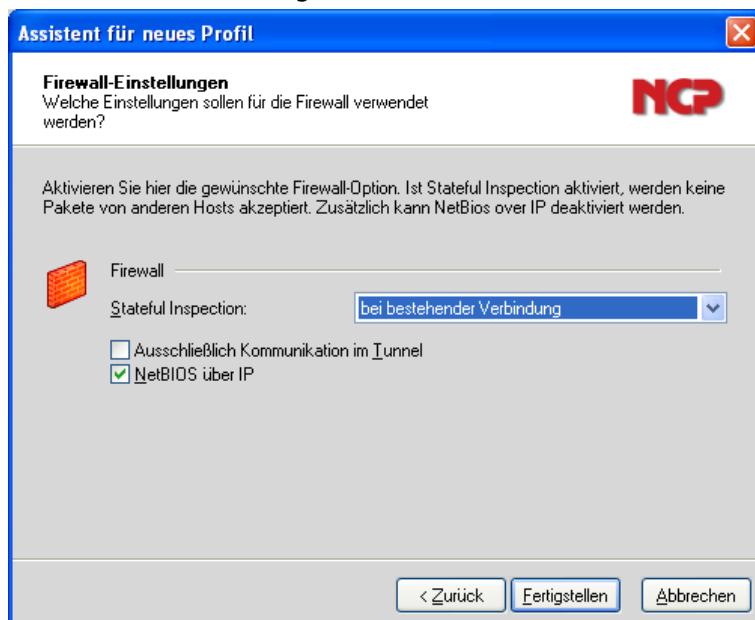
7. Lassen Sie die Einstellungen für Pre-shared Key leer und stellen den Typ der lokalen Identität auf "ASN1 Distinguished Name". Dadurch werden die Daten aus dem Zertifikat zur Identifizierung übertragen.



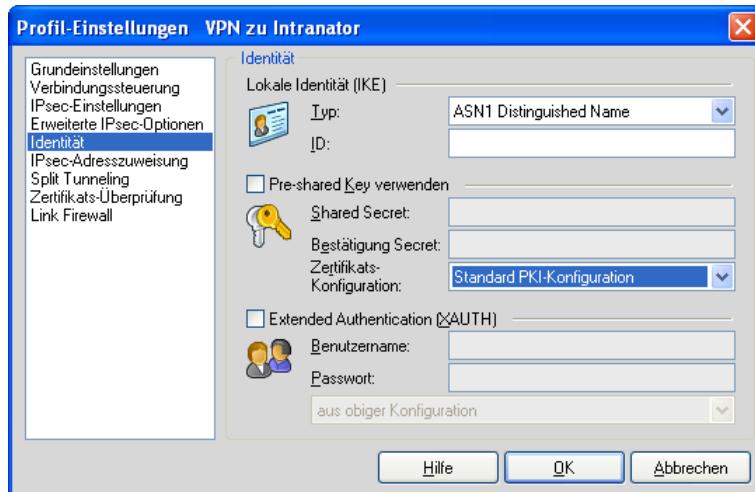
8. Stellen Sie die IP-Adressen-Zuweisung auf "IKE Config Mode verwenden". Damit wird die virtuelle IP durch den Intranator zugewiesen. Lassen Sie die Felder für IP, DNS-Server und WINS-Server alle auf 0.0.0.0 stehen. So werden die durch den Intranator zugewiesenen Werte verwendet.



9. Aktivieren Sie die Firewall des NCP Clients, indem Sie die Stateful Inspection auf "bei bestehender Verbindung" stellen.



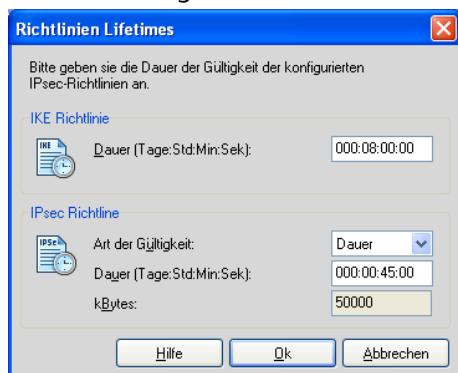
10. Als nächstes müssen Sie dem Client mitteilen, bei dieser Verbindung das Zertifikat zur Authentifizierung zu verwenden. Markieren Sie in den Profil-Einstellungen die eben erzeugte VPN-Verbindung und klicken auf Bearbeiten. Im Menüpunkt Identität können Sie die Zertifikats-Authentifizierung aktivieren, indem Sie die Option Zertifikats-Konfiguration auf Standard PKI-Konfiguration stellen.



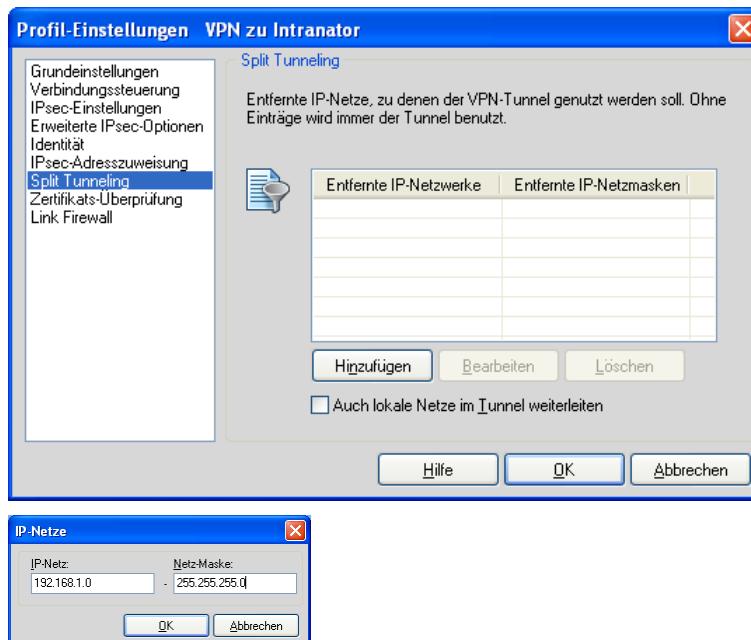
- Passen Sie nun die Gültigkeitszeitspannen für die Verbindung an. Öffnen Sie dazu den Reiter IPSec-Einstellungen, Schaltknopf Gültigkeit.



Eine optimale Verbindungsstabilität auch über längere Zeiträume wird erreicht, wenn die Gültigkeit für IPsec-Richtlinien auf dem Client etwas kürzer eingestellt ist als auf dem Intranator. Stellen Sie daher die Dauer auf 45 Minuten (auf dem Intranator wird standardmäßig 60 Minuten verwendet).



- Als letztes müssen Sie noch das zu verbindende VPN-Netz konfigurieren. Im Menüpunkt Split Tunneling können Sie das Netz hinter dem Intranator eintragen.



Wenn Sie mehr als ein Netz mit einem Intranator verbinden möchten, können Sie auf Seite des NCP Clients mehrere Netze in dieses Menü eintragen. Auf dem Intranator müssen Sie hingegen mehrere separate Verbindungen konfigurieren.

Soll das VPN auch für den Internetzugang verwendet werden, tragen Sie hier kein Netz ein und stellen auf dem Intranator das Lokale Netz auf **Alles (0.0.0.0/0.0.0.0)**.

41.4. Intranator

Auf dem Intranator muss die Verbindung auch entsprechend konfiguriert werden. Für VPN-Clients wird dies im 40. Kapitel, „Anbinden von einzelnen PCs“ beschrieben.

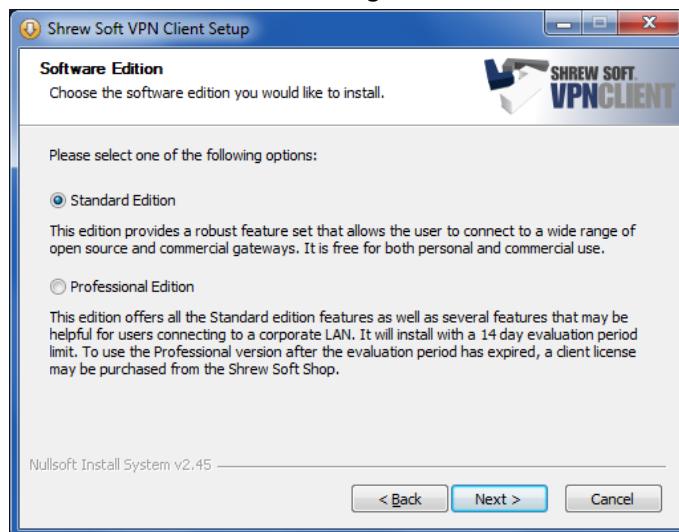
42. Kapitel - VPN mit dem Shrew Soft VPN Client

Der Shrew Soft VPN Client für Windows ist ein kostenlos verfügbarer VPN Client für Windows 8, 7, Vista und XP. Er ist unter 32 Bit und 64 Bit Plattformen lauffähig.

Sie können die jeweils aktuelle Version von dieser URL herunterladen:
<http://www.shrew.net/download/vpn>

Diese Anleitung setzt Version 2.2.1 oder neuer voraus. Verzichten Sie wenn möglich auf den Einsatz von Beta-Versionen des Clients.

Wählen Sie bei der Installation die Standard Edition. Diese enthält alle für die Verbindung mit dem Intranator notwendigen Funktionen.



42.1. Zertifikate

- Der Client kann selbst keine eigenen Zertifikate erstellen. Dies übernimmt daher das Programm makecert.

Laden Sie vom Intranator unter Information > Download das Programm zum Erzeugen von Zertifikaten (makecert) herunter und entpacken Sie es in ein Verzeichnis auf Ihrem Rechner.

- Starten Sie die makecert-Batchdatei und wählen eine Laufzeit in Jahren für Ihr Zertifikat.

```
C:\makecert>makecert
Gueltigkeit des neuen Zertifikats:
1. Ein Jahr
2. Zwei Jahre
3. Drei Jahre
4. Vier Jahre
5. Fuenf Jahre
Ihre Wahl: 5
```

```
C:\makecert>openssl req -x509 -newkey rsa:2048 -days 1825 -new -nodes -config
openssl.cnf -outform PEM -keyform PEM -keyout privatekey.pem -out newcert.cer
Using configuration from openssl.cnf
Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
.....+++
.....+++
```

```
writing new private key to 'privatekey.pem'  
----  
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.
```

3. Geben Sie jetzt die Daten des Rechners ein. Für einige Felder gibt es einen Standardwert der in eckigen Klammern angegeben ist. Wollen Sie diesen verwenden, so drücken Sie einfach nur Return. Verwenden Sie keine Umlaute und andere Sonderzeichen, da es sonst zu Problemen kommen kann. Der "Common Name" (oder "Rechnername" auf dem Intranator) muss eindeutig sein und darf nicht auf anderen Rechnern oder für eine CA wiederverwendet werden.

```
Country Name (2 letter code) []:  
State or Province Name (full name) []:  
Locality Name (eg, city) []:  
Organization Name (eg, company) []:Firma GmbH  
Organizational Unit Name (eg, section) []:  
Common Name (eg, your name or your server's hostname) []:Notebook Mueller  
Email Address []:
```

```
C:\makecert>openssl pkcs12 -export -in newcert.cer -inkey privatekey.pem  
-out newcert.p12  
Loading 'screen' into random state - done
```

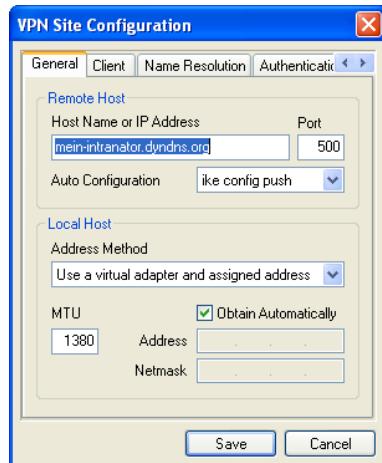
4. Wählen Sie ein Passwort für die Schlüsseldatei. Dieses muss vom Benutzer aus Sicherheitsgründen bei jedem Aufbau der Verbindung eingegeben werden. Das Passwort muss mindestens 4 Zeichen lang sein.

```
Enter Export Password:  
Verifying password - Enter Export Password:  
C:\makecert>del privatekey.pem
```

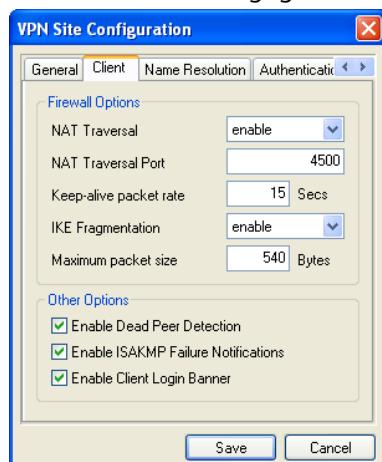
5. Gehen Sie im Intranator in das Menü System > Schlüssel > Fremde Schlüssel und klicken auf Neu. Tragen Sie einen beliebigen Namen ein und öffnen Sie die newcert.cer-Datei aus dem makecert-Verzeichnis in einem beliebigen Editor (z.B. wordpad). Kopieren Sie den Inhalt in die Zwischenablage und fügen Sie sie in das Schlüsselfeld auf dem Intranator ein.
6. Gehen Sie im Intranator in das Menü System > Schlüssel > Eigene Schlüssel und wählen den Schlüssel, der für diese Verbindung zum Einsatz kommen soll. Im Reiter Daten können Sie den öffentlichen Teil des Zertifikats über die Funktion Zertifikat exportieren als .pem-Datei speichern.

42.2. Verbindung im Client konfigurieren

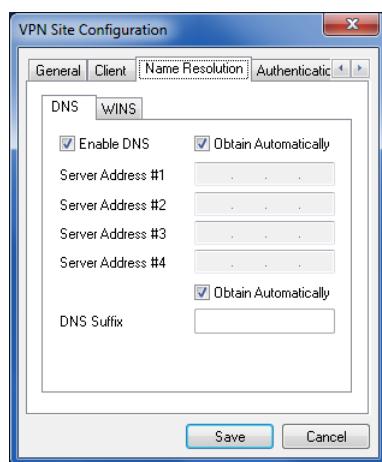
1. Starten Sie den Shrew Soft VPN Access Manager. Legen Sie über die Schaltfläche Add eine neue Verbindung an.
2. Tragen Sie bei Host Name or IP Address den externen DNS-Namen oder die externe IP Ihres Intranators ein. Stellen Sie die Auto Configuration auf ike config push. Die virtuelle IP wird dadurch vom Intranator zugewiesen.



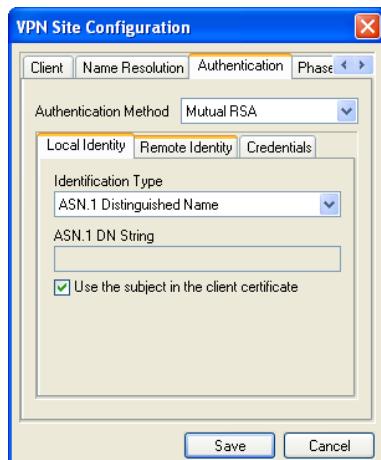
3. Belassen Sie die vorgegebene Konfiguration auf dem Reiter Client.



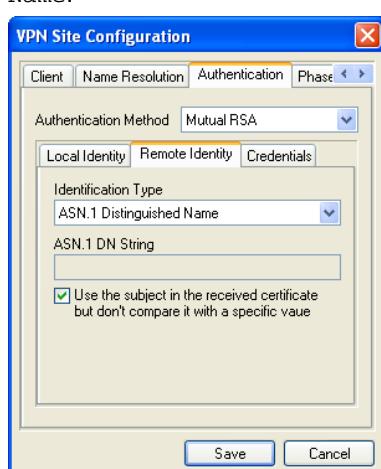
4. DNS und WINS werden automatisch vom Intranator konfiguriert.



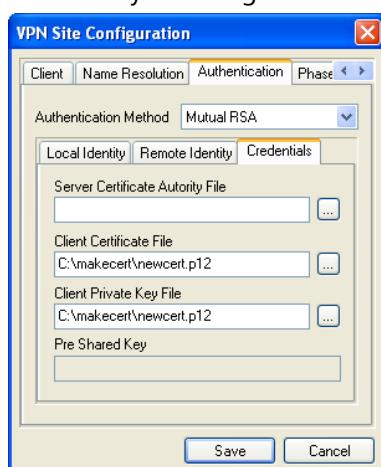
5. Stellen Sie die Authentication Method auf `Mutual RSA`. Lassen Sie den Client (Local Identity) sich per `ASN.1 Distinguished Name` identifizieren.



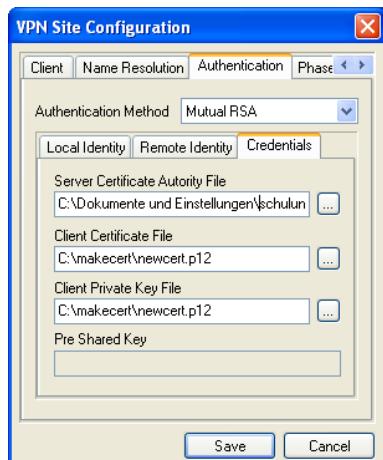
6. Auch die Gegenseite (Remote Identity) identifiziert sich per ASN.1 Distinguished Name.



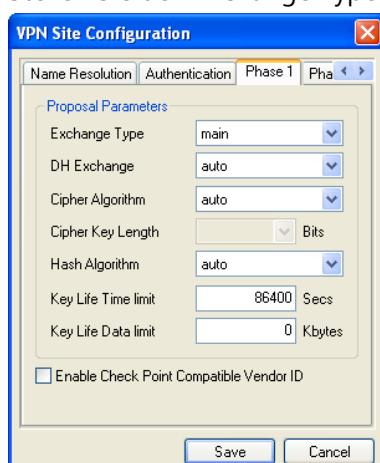
7. Wählen Sie bei Credentials zuerst das eigene Zertifikat des Clients aus. Es wurde im PKCS#12-Format (Endung .p12) vorher mit makecert erzeugt und heißt standardmäßig newcert.p12. Diese Datei muss sowohl bei Client Certificate File als auch bei Client Private Key File ausgewählt werden.



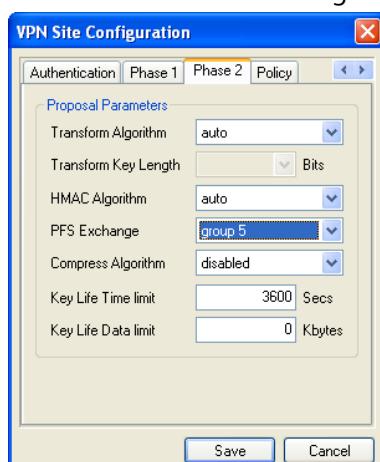
8. Hinterlegen Sie als nächstes im Feld Server Certificate Authority File die Datei mit dem Zertifikat des Intranators. Sie wurde vorher vom Intranator exportiert und auf dem PC gespeichert.



9. Stellen Sie den Exchange Type auf den main-mode.



10. Stellen Sie den PFS Exchange auf group 5.



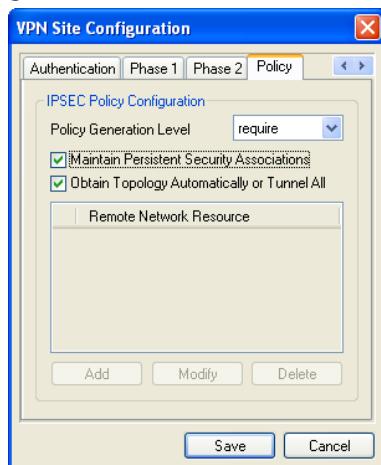
11. Im Reiter Policy hinterlegen Sie alle Netze, mit denen Sie sich verbinden wollen.

Stellen Sie das Policy Generation Level auf **require** und aktivieren Sie Maintain Persistent Security Associations.

Deaktivieren Sie nun die Option Obtain Topology Automatically or Tunnel All und fügen dann mit Add ein neues Netz auf der Gegenseite hinzu.



Sollen alle Verbindungen (auch ins Internet) über dieses VPN laufen, tragen Sie hier keine Netze ein und aktivieren die Checkbox Obtain Topology Automatically or Tunnel All. Auf dem Intranator muss dann bei Lokales Netz die Option Alles (0.0.0.0/0.0.0.0) gewählt sein.



42.3. Intranator

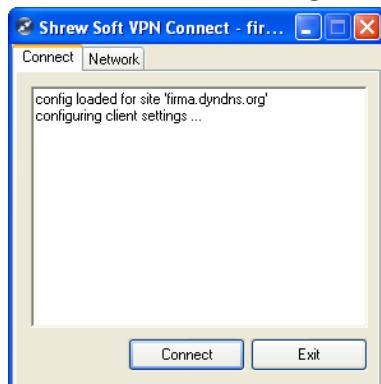
Auf dem Intranator muss die Verbindung auch entsprechend konfiguriert werden. Für VPN-Clients wird dies im 40. Kapitel, „Anbinden von einzelnen PCs“ beschrieben.

42.4. Verbindung aufbauen

1. Öffnen Sie im Hauptmenü des Access Managers die eben konfigurierte Verbindung durch einen Doppelklick oder die Schaltfläche Connect.



2. Bauen Sie die Verbindung durch einen Klick auf Connect auf.

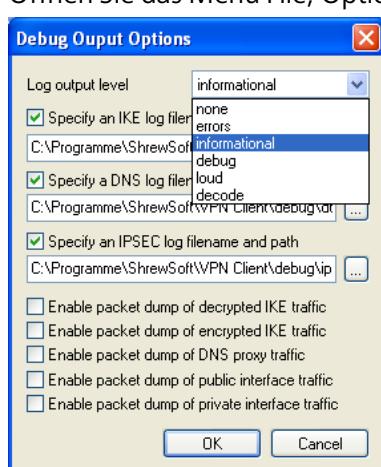


3. Sie werden nun nach dem vorher gewählten Passwort des eigenen Schlüssels gefragt. Geben Sie es ein und die Verbindung wird aufgebaut.

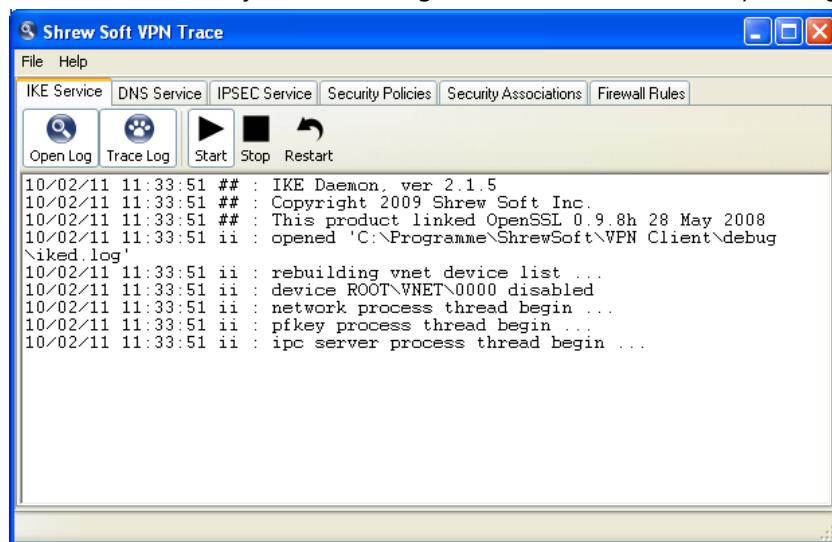
42.5. Verbindungsprotokolle

Um Fehler im Verbindungsauflauf zu analysieren, bieten sich die Verbindungsprotokolle des Clients an.

1. Starten Sie das Trace Utility, Sie finden es im Programmordner des Shrew Soft VPN-Clients.
2. Öffnen Sie das Menü File, Options. Stellen Sie das Log output level auf **informational**.



3. Starten Sie den IKE Service mit der neuen Trace-Option durch einen Klick auf Restart neu. Aktivieren Sie jetzt die Anzeige durch einen Klick auf Open Log.



43. Kapitel - VPN mit dem NetGear ProSafe Client

Der Netgear ProSafe VPN Client™ (Netgear-Artikelnr. VPN01L) und einige weitere VPN-Clients sind OEM-Versionen von (und damit vom Funktionsumfang identisch mit) SafeNet SoftRemote.

Diese Anleitung gilt nur für den ProSafe VPN Client™ (Artikelnr. VPN01L). Der ProSafe VPN Client Professional™ (Artikelnr. VPNG01L) ist ein vollkommen anderes Produkt und wird hier nicht beschrieben.



Hinweis

Intra2net rät, diesen Client nicht mehr für neue Installationen zu verwenden. Diese Dokumentation ist nur noch als Referenz für Bestandsinstallationen gedacht.

Der Netgear ProSafe VPN Client™ wird häufig in einer älteren Version (Version 10.1 aus dem Jahre 2003) ausgeliefert. Bei diesen alten Versionen kann es vorkommen, dass sie sich nicht installieren lassen oder im Betrieb Störungen auftreten (u.a. kann der virtuelle Adapter nicht angelegt werden). Wir empfehlen daher, immer von Anfang an eine aktuelle Version zu installieren.

Sollten Sie eine alte Version geliefert bekommen haben, können Sie vom Netgear-Support mit der Seriennummer (siehe Aufkleber auf dem Karton) eine aktuelle Version anfordern. Rufen Sie beim deutschen Netgear Support an und Sie bekommen erfahrungsgemäß ohne großen Aufwand und zeitnah eine neue Version per E-Mail zugesendet.

43.1. Kompatibilität

Ab Version 10.8 wird Microsoft Windows Vista in der 32-Bit-Version unterstützt. Wenn Sie Windows 7 (32- und 64-Bit) oder die 64-Bit-Version von Vista einsetzen, empfehlen wir den NCP Secure Entry Client, beschrieben im 41. Kapitel, „VPN mit dem NCP Secure Entry Client“.

Stellen Sie sicher, dass auf dem Rechner keine weiteren VPN-Clients (z.B. von Cisco, Nortel, etc.) installiert sind. Es kann, bis auf ganz wenige Ausnahmen, immer nur eine VPN-Software auf einem Rechner installiert sein.

Stellen Sie sicher, dass auf dem Rechner keine „Netzwerk-Manager“-Software installiert ist. Diese versucht typischerweise auch ohne DHCP die Netzwerkkonfiguration automatisch an das aktuelle Netz anzupassen und wird vor allem von einigen Notebook-Herstellern bei der Auslieferung vorinstalliert. Diese Software klinkt sich in den meisten Fällen in die Netzwerksteuerung von Windows ein und stört dabei die Funktion des VPN-Clients. Deinstallieren Sie den Netzwerk-Manager und starten den Rechner neu.

Von Kunden wurde berichtet, dass es mit bestimmten Versionen von TrendMicro-Produkten sowie ZoneAlarm zu Kompatibilitätsproblemen kommen kann. Diese äußern sich darin, dass beim Verbindungsaufbau der virtuelle Adapter nicht angelegt werden kann. Verwenden Sie in diesem Fall ein anderes Client-Firewall-Produkt oder versuchen es mit einem anderen VPN-Client, wie z.B. dem NCP Secure Entry Client, beschrieben im 41. Kapitel, „VPN mit dem NCP Secure Entry Client“.

43.2. Installation

1. Starten Sie das Installationsprogramm des Netgear VPN-Clients, installieren die Software mit allen Modulen und starten Sie den Rechner neu.
2. Laden Sie vom Intranator unter "Information > Download" das "Programm zum Erzeugen von Zertifikaten" (makecert) herunter und entpacken Sie es in ein Verzeichnis auf Ihrem Rechner.

43.3. Zertifikate

1. Netgear ProSafe kann keine eigenen Zertifikate erstellen. Dies übernimmt daher das Programm makecert. Starten Sie die makecert-Batchdatei und wählen eine Laufzeit in Jahren für Ihr Zertifikat.

```
C:\makecert>makecert
Gueltigkeit des neuen Zertifikats:
1. Ein Jahr
2. Zwei Jahre
3. Drei Jahre
4. Vier Jahre
5. Fuenf Jahre
Ihre Wahl: 5
```

```
C:\makecert>openssl req -x509 -newkey rsa:2048 -days 1825 -new -nodes -config
openssl.cnf -outform PEM -keyform PEM -keyout privatekey.pem -out newcert.cer
Using configuration from openssl.cnf
Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
.....+ ++
.....+ ++
writing new private key to 'privatekey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
```

2. Geben Sie jetzt die Daten des Rechners ein. Für einige Felder gibt es einen Standardwert der in eckigen Klammern angegeben ist. Wollen Sie diesen verwenden, so drücken Sie einfach nur Return. Verwenden Sie keine Umlaute und andere Sonderzeichen, da es sonst zu Problemen kommen kann. Der "Common Name" (oder "Rechnername" auf dem Intranator) muss eindeutig sein und darf nicht auf anderen Rechnern oder für eine CA wiederverwendet werden.

```
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:Intra2net AG
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:Netgear Client
Email Address []:
```

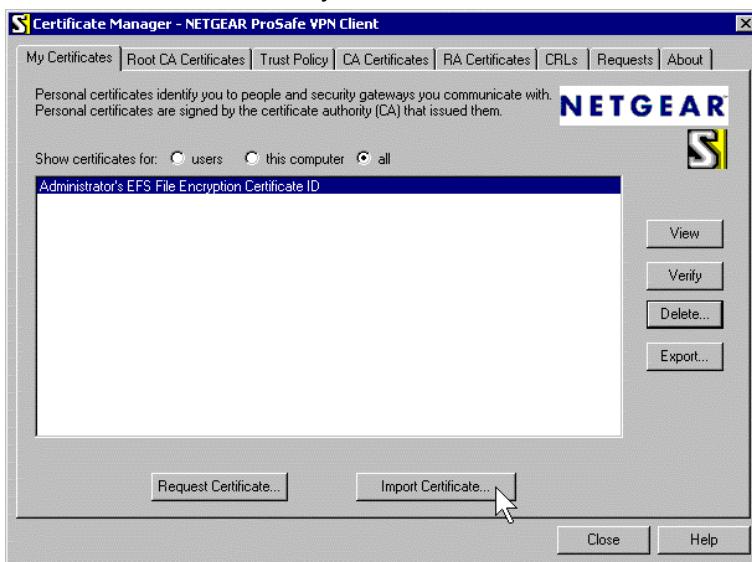
```
C:\makecert>openssl pkcs12 -export -in newcert.cer -inkey privatekey.pem
-out newcert.p12
Loading 'screen' into random state - done
```

- Wählen Sie ein Transportpasswort, mit dem die Schlüsseldatei auf dem Weg zum VPN-Client geschützt wird. Netgear ProSafe akzeptiert keine leeren Passwörter.

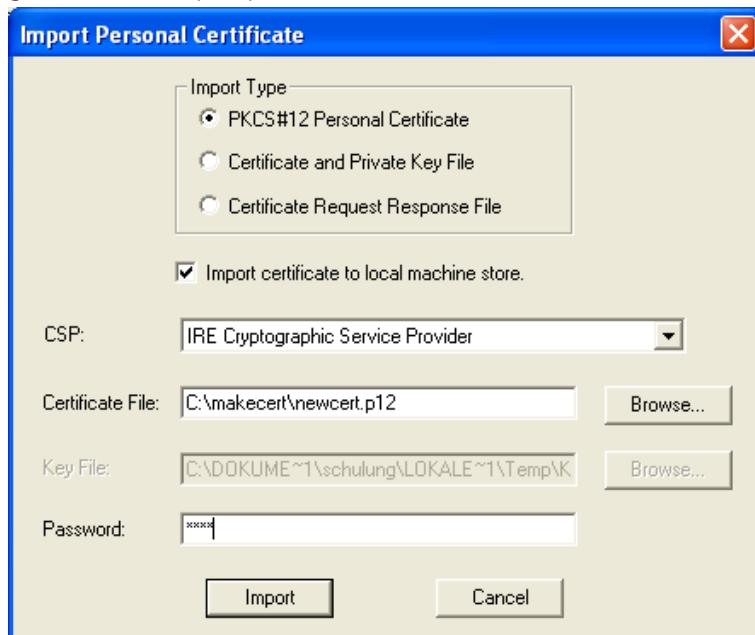
```
Enter Export Password:  
Verifying password - Enter Export Password:
```

```
C:\makecert>del privatekey.pem
```

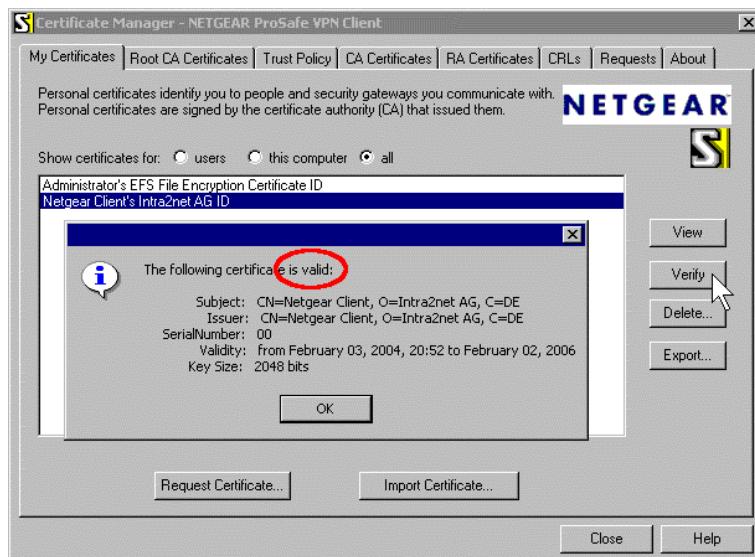
- Starten Sie den Netgear Certificate Manager aus dem Kontextmenü (Rechtsklick) des SafeNet Symbols in der Traybar
- Wählen Sie den Reiter "My Certificates" und klicken Sie auf "Import Certificate".



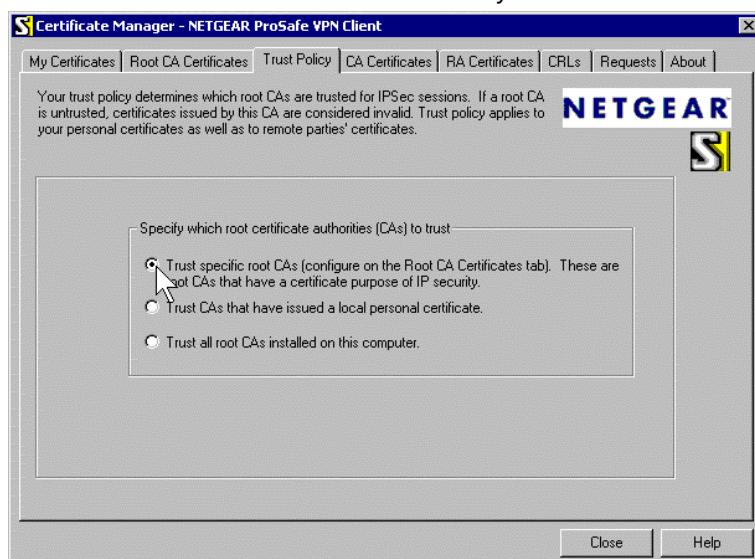
- Aktivieren Sie "Import certificate to local machine store", wählen das Zertifikatspaket newcert.p12 aus dem makecert-Verzeichnis aus und geben Sie das von Ihnen gewählte Transportpasswort ein.



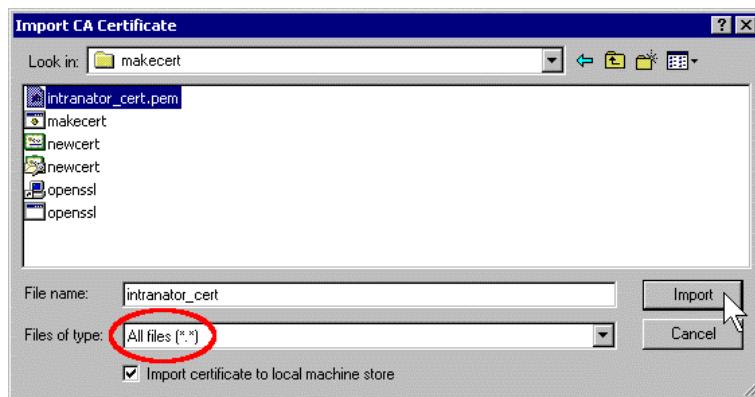
- Überprüfen Sie, ob das Zertifikat vertrauenswürdig ist. Wählen das eben installierte Zertifikat aus und klicken auf "Verify". Das Zertifikat muss als "is valid" eingestuft sein.



8. Wechseln Sie auf den Reiter "Trust Policy" und schalten auf "Trust specific root CAs"



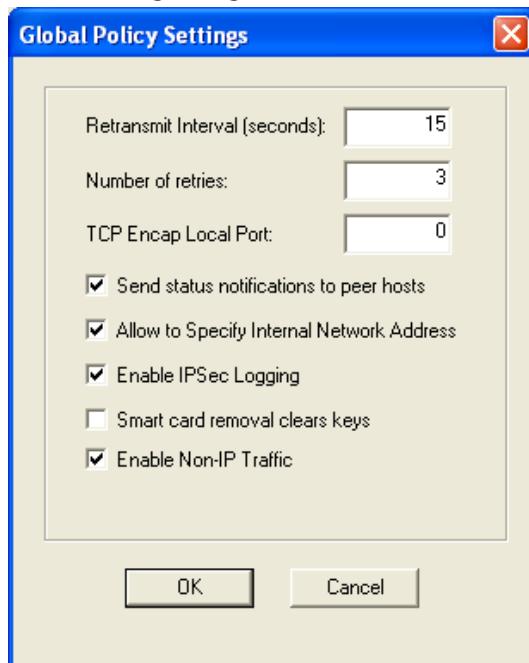
9. Gehen Sie auf dem Intranator in das Menü "System > Schlüssel > Eigene Schlüssel". Wählen Sie einen Schlüssel für diese Verbindung aus oder erstellen Sie einen neuen. Wechseln Sie auf den Reiter "Daten", gehen Sie auf "Zertifikat exportieren" und speichern das Zertifikat.
10. Gehen Sie im Netgear Certificate Manager auf den Reiter "Root CA Certificates" und klicken auf "Import Certificate". Wählen Sie als Dateityp "All files" und importieren das eben aus dem Intranator gespeicherte Zertifikat.



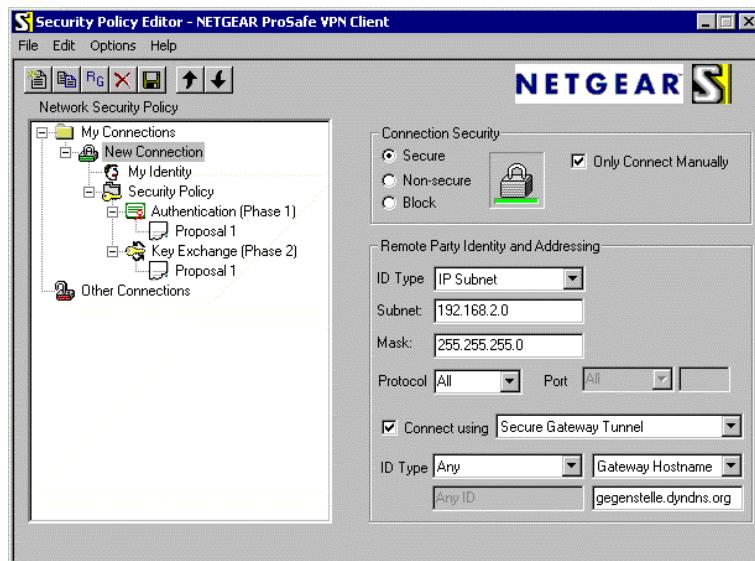
11. Gehen Sie im Intranator in das Menü System > Schlüssel > Fremde Schlüssel und klicken auf Neu. Tragen Sie einen beliebigen Namen ein und öffnen Sie die newcert.cer-Datei aus dem makecert-Verzeichnis in einem beliebigen Editor (z.B. wordpad). Kopieren Sie den Inhalt in die Zwischenablage und fügen Sie sie in das Schlüsselfeld auf dem Intranator ein.

43.4. Verbindungen

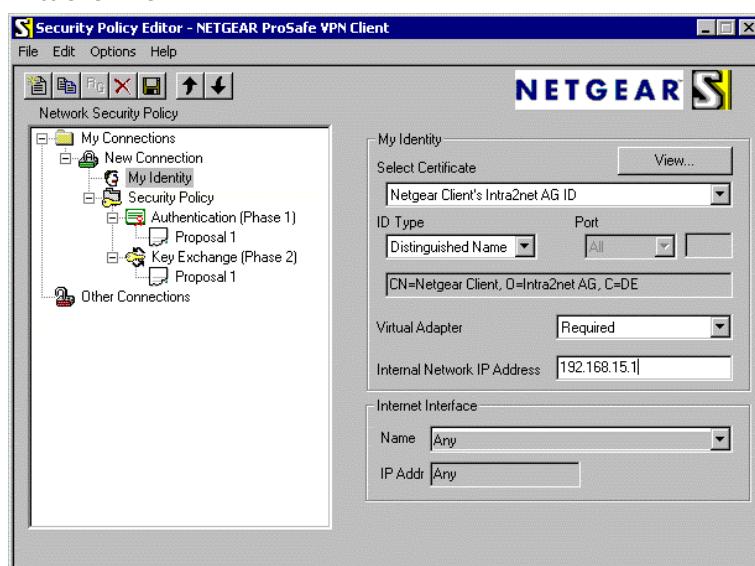
1. Starten Sie den Netgear Security Policy Editor aus dem Kontextmenü (Rechtsklick) des SafeNet Symbols in der Traybar.
2. Schalten Sie als erstes die Verwendung virtueller IPs frei. Gehen Sie dazu in das Menü "Options > Global Policy Settings" und aktivieren Sie "Allow to Specify Internal Network Address". Es macht Sinn auch gleich "Enable IPSec Logging" zu aktivieren um im Fehlerfall aussagefähige Protokolldateien zur Verfügung zu haben.



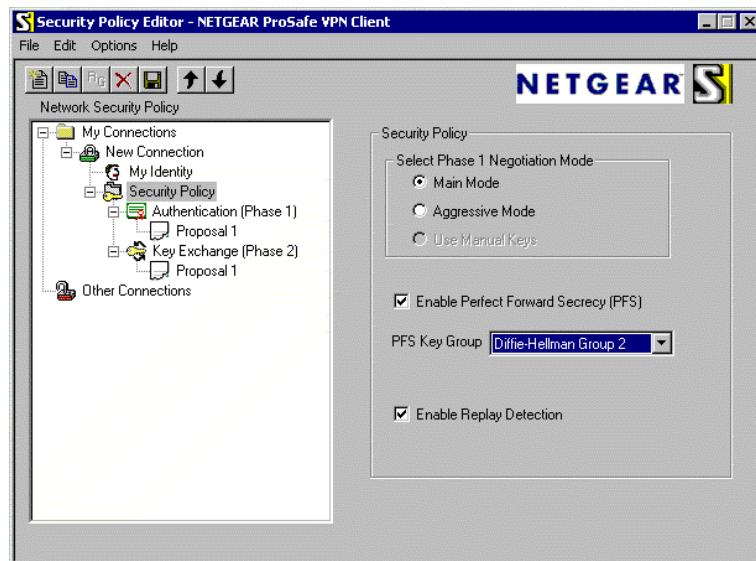
3. Klicken Sie auf das Symbol ganz links um eine neue Verbindung anzulegen. Wählen Sie diese mit einem Klick aus.



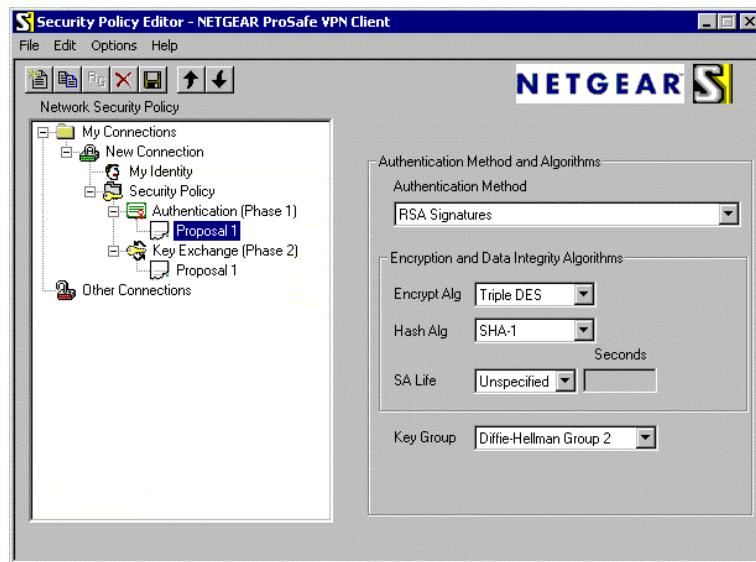
4. Wählen Sie als ID Type "IP Subnet" und tragen IP und Netzmaske des Netzes hinter dem Intranator ein.
5. Wählen Sie "Secure Gateway Tunnel" mit ID Type "Any". Tragen Sie entweder bei "Gateway Hostname" den DNS-Namen des Intranators oder bei "Gateway IP" die offizielle IP des Intranators ein.
6. Gehen Sie auf "My Identity" und wählen das vorher mit makecert erstellte Zertifikat aus
7. Stellen Sie den Virtual Adapter auf "Required" und tragen die im Intranator hinterlegte virtuelle IP ein.



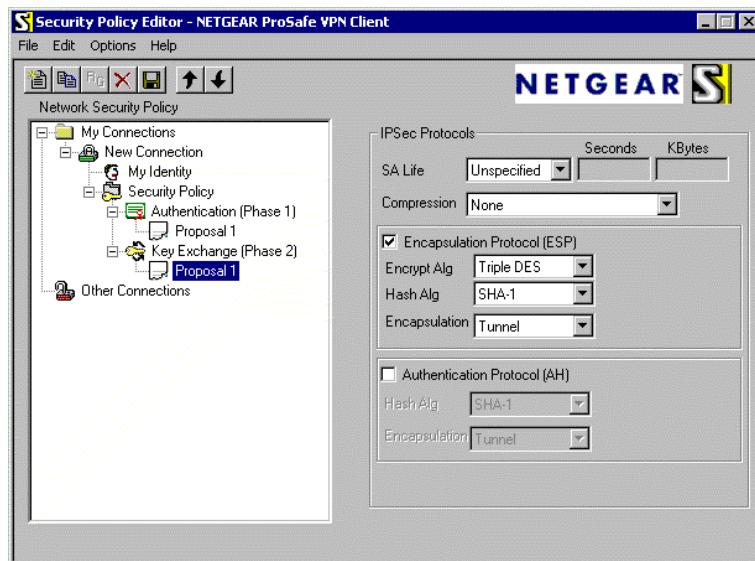
8. Gehen Sie auf "Security Policy" und stellen den Negotiation Mode auf "Main Mode". Stellen Sie PFS genauso wie auf dem Intranator ein (Diffie-Hellman Group 2 wenn aktiviert).



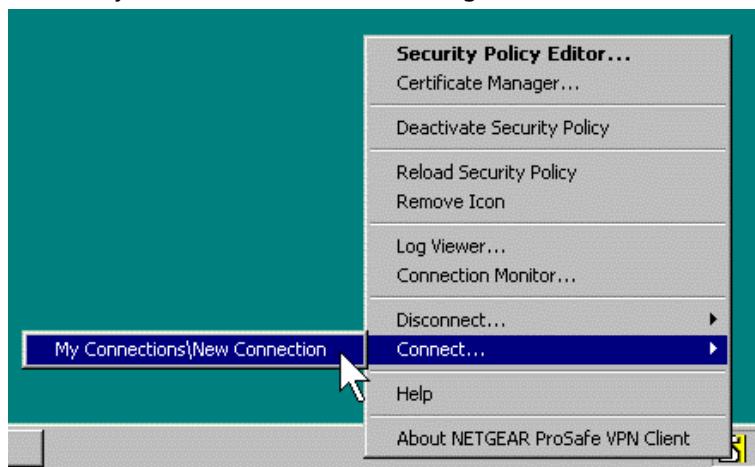
9. Gehen Sie auf das Proposal von Phase 1. Wählen Sie AES oder Triple-DES als Algorithmus und SHA-1 für den Hash.



10. Gehen Sie auf das Proposal von Phase 2. Wählen Sie hierfür dieselben Algorithmen wie für Phase 1 und stellen die Encapsulation auf "Tunnel".



11. Speichern Sie die Konfiguration. Ist die Verbindung auch auf dem Intranator konfiguriert, kann sie jetzt aus dem Kontextmenü gestartet werden.



43.5. Intranator

Auf dem Intranator muss die Verbindung auch entsprechend konfiguriert werden. Für VPN-Clients wird dies im 40. Kapitel, „Anbinden von einzelnen PCs“ beschrieben.

44. Kapitel - VPN mit Mac OS X

44.1. Installation

Mac OS X enthält bereits einen voll funktionsfähigen IPSec-Stack im Betriebssystem. Allerdings ist keine Oberfläche zur Konfiguration vorhanden. Diese Oberfläche liefert die frei verfügbare Software IPSecuritas.

Sie können Sie von <http://www.lobotomo.com/products/IPSecuritas/> herunterladen und installieren.

44.2. Zertifikate erzeugen

IPSecuritas kann selbst keine Zertifikate erzeugen. Deshalb wird dafür das Programm OpenSSL eingesetzt.

1. Öffnen Sie ein Unix-Terminal (Programme > Dienstprogramme > Terminal)
2. Geben Sie folgenden Befehl in einer Zeile ein:

```
openssl req -x509 -newkey rsa:2048 -days 730 -new -nodes -outform PEM -  
keyform PEM -keyout private_key.pem -out newcert.pem
```

3. Das Schlüsselpaar wird berechnet und Sie werden nach den Zertifikatsdaten gefragt. Die eingegebenen Werte sind für die Funktion nicht relevant, sie müssen nur auf allen per VPN verbundenen Systemen eindeutig sein. Wir empfehlen, keine Umlaute zu verwenden.

```
Generating a 2048 bit RSA private key  
.....  
.....+++++  
writing new private key to 'private_key.pem'  
-----  
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.  
-----  
Country Name (2 letter code) [GB]:DE  
State or Province Name (full name) [Berkshire]:BW  
Locality Name (eg, city) [Newbury]:Tuebingen  
Organization Name (eg, company) [My Company Ltd]:Intra2net  
Organizational Unit Name (eg, section) []:  
Common Name (eg, your name or your server's hostname) []:MeinRechnerName  
Email Address []:
```

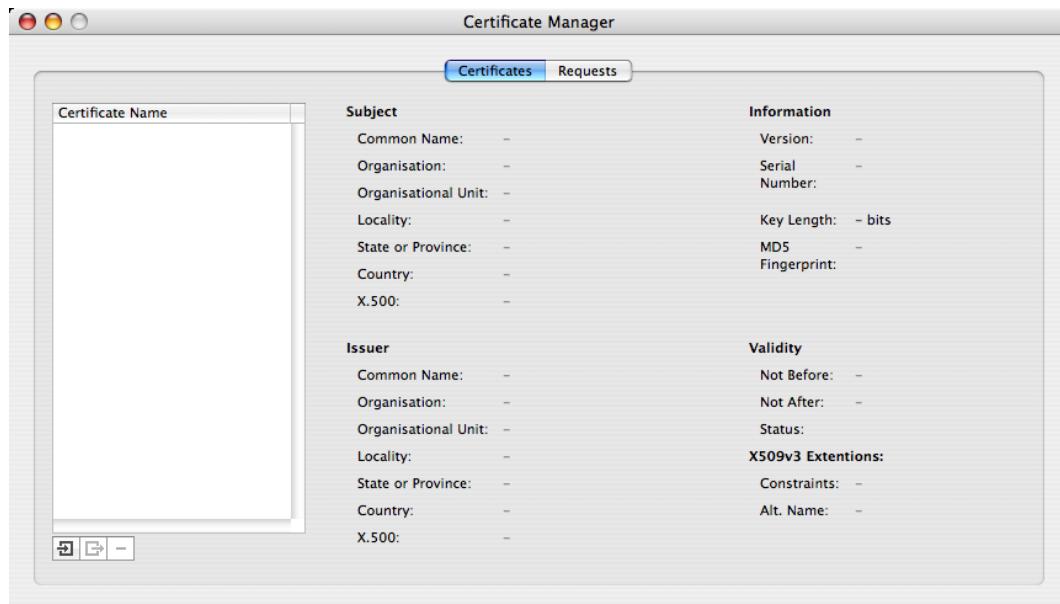
4. Das Zertifikat ist jetzt für 2 Jahre (730 Tage) gültig und liegt in der Datei `newcert.pem`. Der private Schlüssel ist in der Datei `private_key.pem`. Sie können die Gültigkeitsdauer über den Parameter `-days` auf der Kommandozeile verändern.
5. Bei neueren Versionen von IPSecuritas kann es passieren, daß der Client das PEM-Format nicht einliest. In diesem Fall muß man auf das PKCS 12-Format ausweichen. Hierzu ist ein zusätzlicher Schritt auf der Kommandozeile vonnöten:

```
openssl pkcs12 -export -in newcert.pem -inkey private_key.pem -out newcert.p12
```

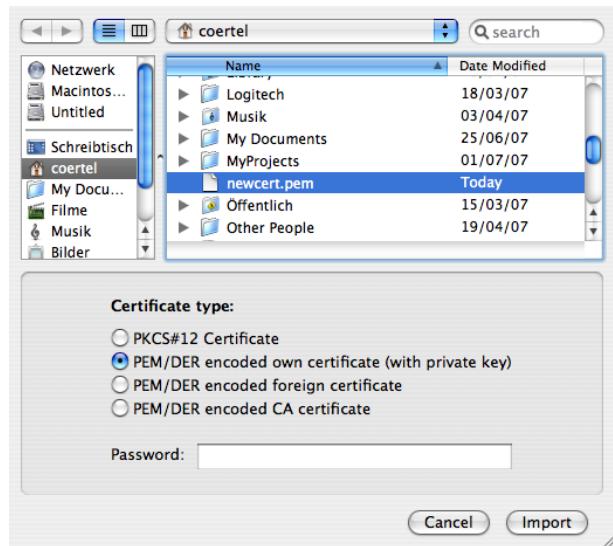
Wobei die Dateien `newcert.pem` und `private_key.pem` wie gehabt erstellt wurden. An dieser Stelle fragt OpenSSL nach einem Passwort, mit welchem Schlüssel und Zertifikat gesichert werden: Dieses Passwort wird später beim Import in IPSecuritas benötigt. Das Resultat legt OpenSSL unter dem Namen `newcert.p12` ab.

44.3. Zertifikate importieren

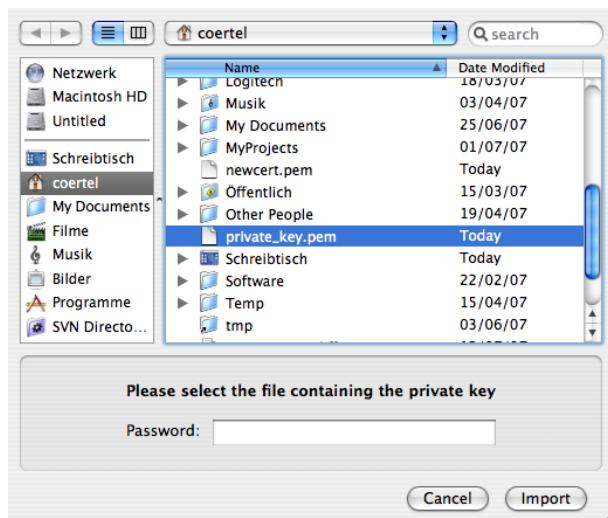
- Starten Sie IPSecuritas und öffnen das Menü Certificates, Edit certificates.



- Klicken Sie links unten auf das Importieren-Symbol.
- Wählen Sie die Datei mit dem eigenen Zertifikat (im Beispiel `newcert.pem`) und stellen den Typ auf PEM/DER encoded own certificate.

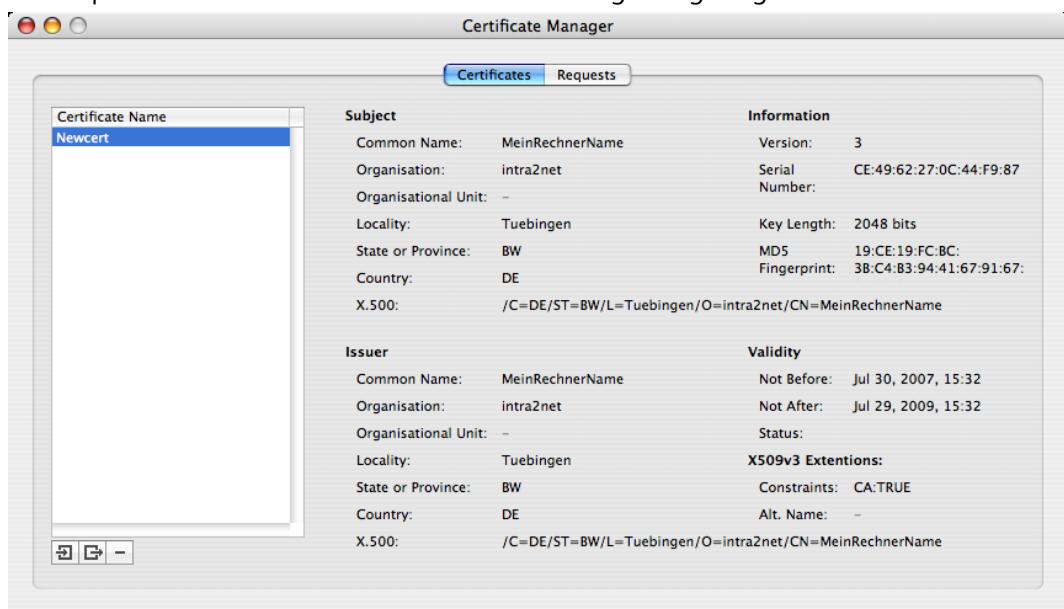


- Als nächstes werden Sie nach der Datei mit dem passenden privaten Schlüssel gefragt (im Beispiel `private_key.pem`). Ein Passwort ist nicht notwendig.



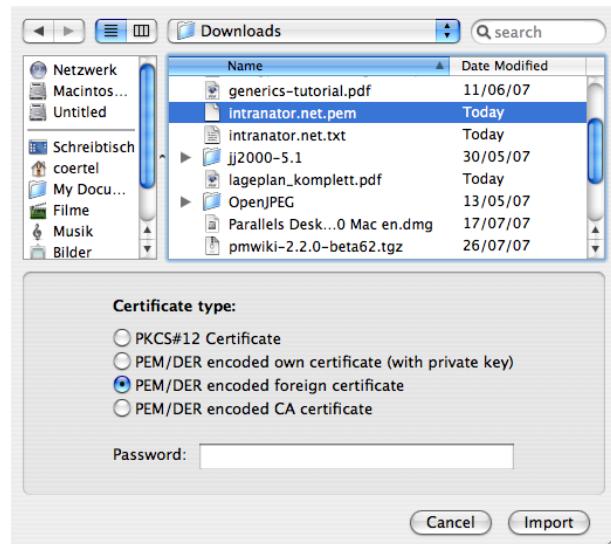
Neuere Versionen von IPSecuritas erwarten, daß Schlüssel und Zertifikat gemeinsam im Format PKCS 12 vorliegen. Anstelle der Dateien `newcert.pem` und `private_key.pem` muß dann, wie im letzten Abschnitt beschrieben, die Datei `newcert.p12` ausgewählt und der Zertifikatstyp auf PKCS#12 Datei gesetzt werden. Außerdem tragen Sie das bei der Erstellung verwendete Passwort in das entsprechende Feld ein.

- Das importierte Zertifikat wird im Zertifikatsmanager angezeigt.

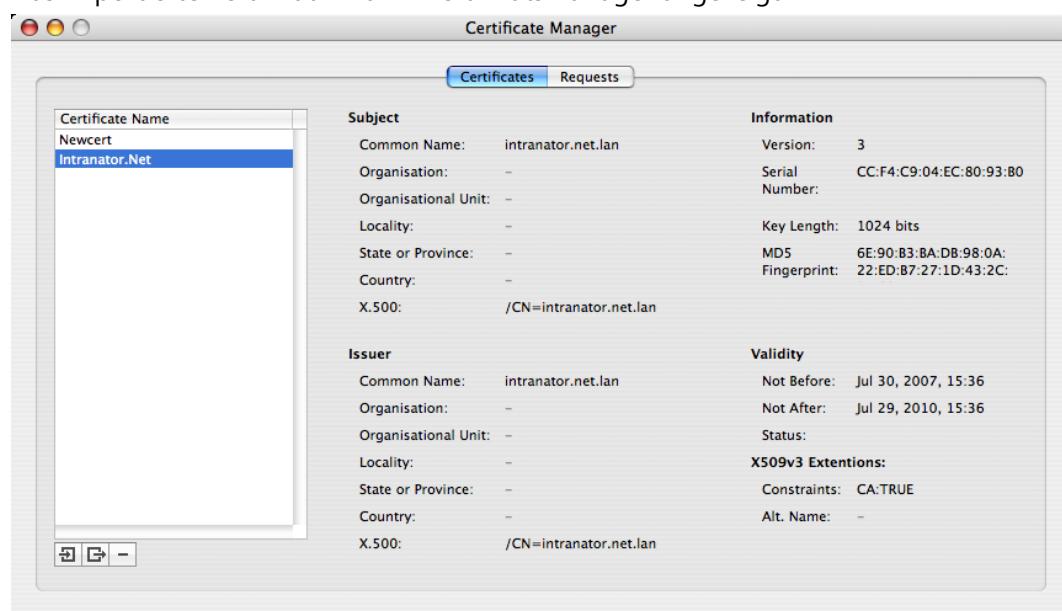


- Öffnen Sie das eigene Zertifikat (z.B. `newcert.pem`) in einem Texteditor und übernehmen den Inhalt in die Zwischenablage. Öffnen Sie im Intranator das Menü System > Schlüssel > Fremde Schlüssel und legen einen neuen an. Geben Sie dem Schlüssel einen Namen (z.B. den des Benutzers) und kopieren Sie die Zertifikatsdaten aus der Zwischenablage in das Feld Copy & Paste Schlüssel.
- Öffnen Sie im Intranator das Menü System > Schlüssel > Eigene Schlüssel : Daten. Wählen Sie das gewünschte Zertifikat aus und exportieren es über den Menüpunkt Zertifikat exportieren in eine .pem-Datei.

8. Wählen Sie im Certificate Manager von IPSecuritas wieder die Import-Funktion. Importieren Sie die eben vom Intranator gespeicherte Zertifikatsdatei und stellen den Typ auf PEM/DER encoded foreign certificate.

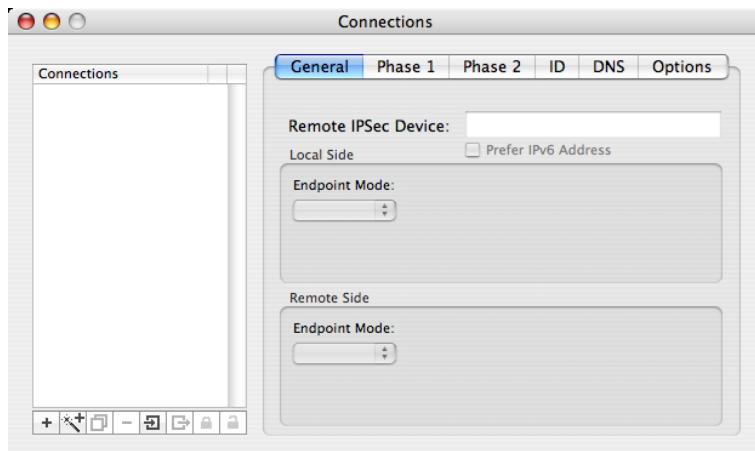


9. Das importierte Zertifikat wird im Zertifikatsmanager angezeigt.

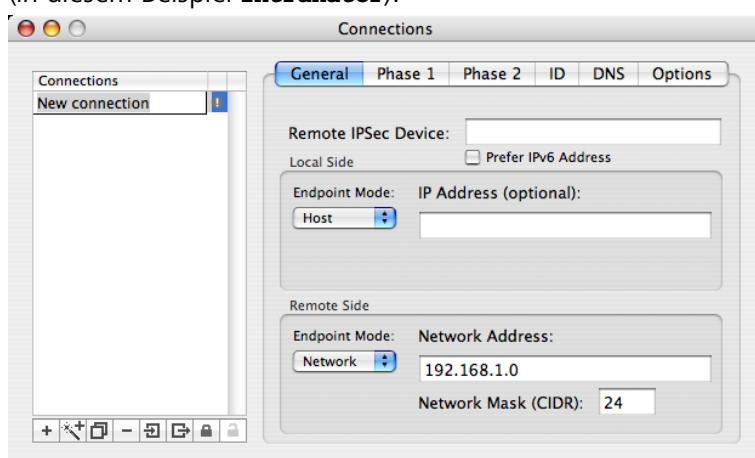


44.4. Verbindungen konfigurieren

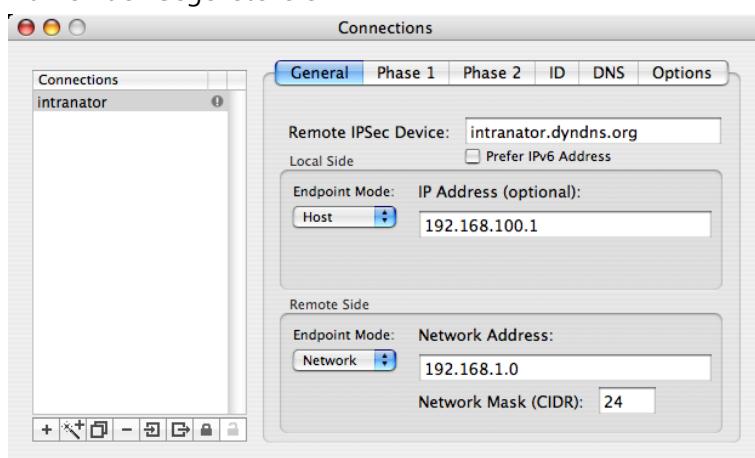
1. Öffnen Sie das Menü Connections, Edit connections in IPSecuritas.



2. Legen Sie über das New-Symbol eine neue Verbindung an und geben ihr einen Namen (in diesem Beispiel **Intranator**).

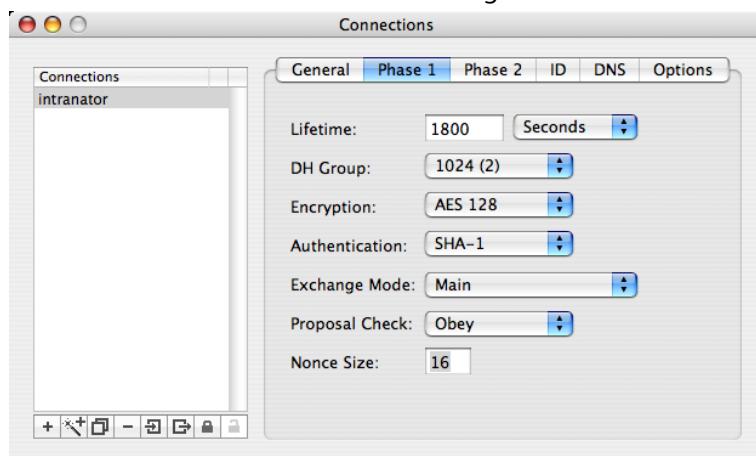


3. Im Menü General tragen Sie unter Remote IPSec Device die (offizielle) IP oder den DNS-Namen der Gegenstelle ein.

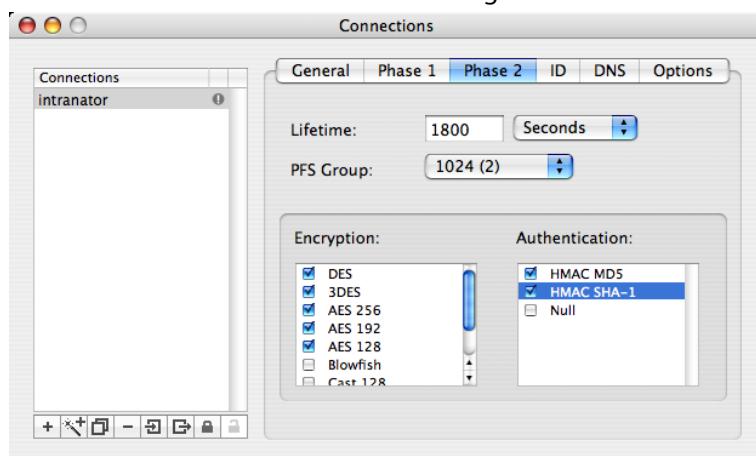


4. Stellen Sie bei Local Side den Endpoint Mode auf Host und geben die virtuelle IP ein, die der Mac-Client innerhalb des VPNs verwenden soll.
5. Stellen Sie bei Remote Side den Endpoint Mode auf Network und geben die Adresse des Netzes hinter dem Intranator ein. Die Netzmaske wird in CIDR-Notation eingegeben; **24** (Bit) entspricht **255.255.255.0**.

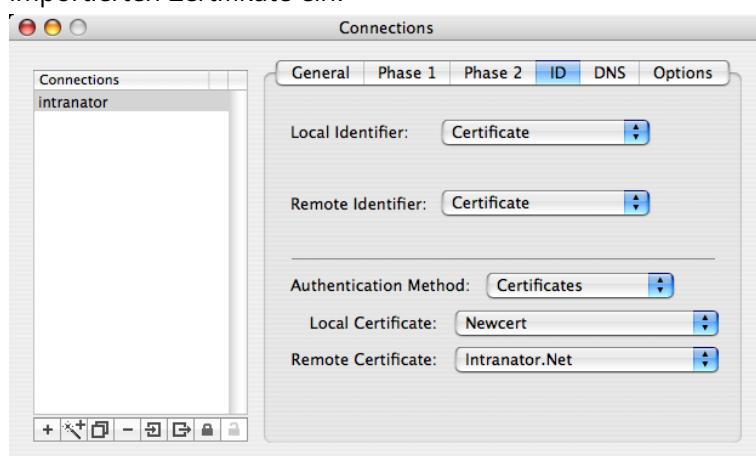
6. Im Menü Phase 1 können Sie die Verschlüsselungsparameter für Phase 1 konfigurieren. Diese müssen zum auf dem Intranator gewählten Verschlüsselungsprofil passen.



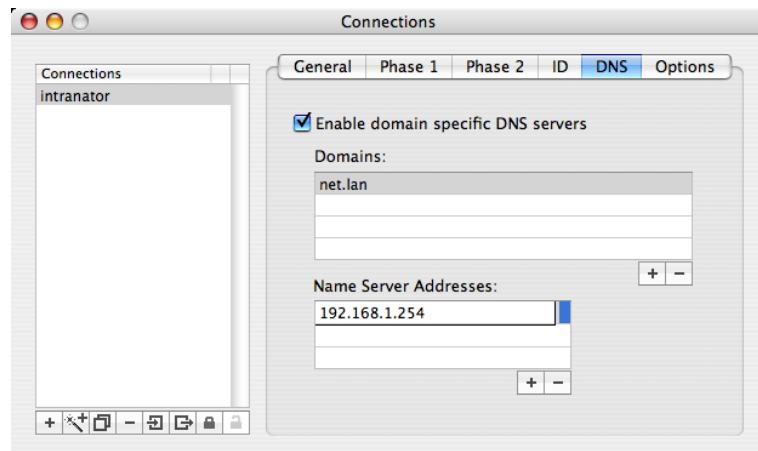
7. Im Menü Phase 2 können Sie die Verschlüsselungsparameter für Phase 2 konfigurieren. Diese müssen zum auf dem Intranator gewählten Verschlüsselungsprofil passen.



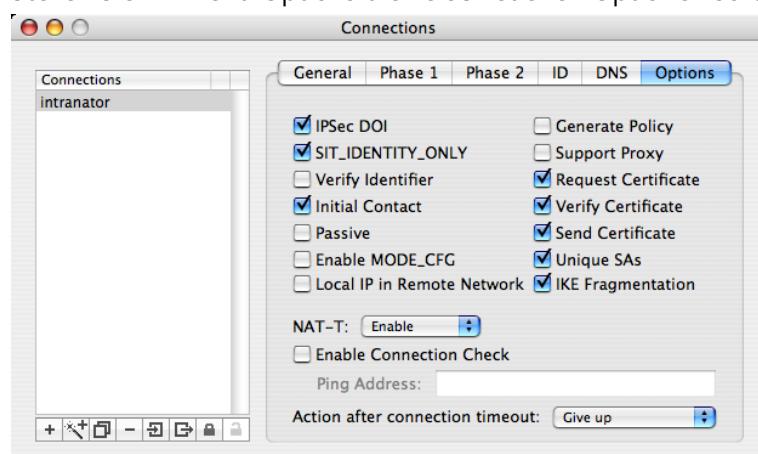
8. Stellen Sie im Menü ID bei Local Identifier und Remote Identifier jeweils Certificate ein. Wählen Sie Certificates als Authentication Method und stellen die beiden vorher importierten Zertifikate ein.



9. Im Menü DNS haben Sie die Möglichkeit, eine bestimmte Domain von einem Server im VPN (z.B. dem Intranator) auflösen zu lassen.



10. Stellen Sie im Menü Options die verschiedenen Optionen so ein, wie hier gezeigt.



11. Nun können Sie im Hauptfenster die Verbindung über den Start-Knopf aufbauen.



44.5. Intranator

Auf dem Intranator muss die Verbindung auch entsprechend konfiguriert werden. Für VPN-Clients wird dies im 40. Kapitel, „Anbinden von einzelnen PCs“ beschrieben.

45. Kapitel - VPN mit dem Apple iPhone

Um VPN-Verbindungen mit dem Intranator aufzubauen zu können, benötigen Sie Apple iPhone OS Version 3.1 oder neuer.

Außerdem ist zur einmaligen Konfiguration ein PC mit dem iPhone Konfigurationsprogramm, Version 2.1 oder neuer, nötig. Dieses bekommen Sie von Apple unter der URL <http://www.apple.com/de/support/iphone/enterprise/>.

45.1. Zertifikat für das iPhone

1. Das iPhone kann selbst keine eigenen Zertifikate erstellen. Dies übernimmt daher das Programm `makecert`.

Laden Sie vom Intranator unter Information > Download das Programm zum Erzeugen von Zertifikaten (`makecert`) herunter und entpacken Sie es in ein Verzeichnis auf Ihrem Rechner.

2. Starten Sie die `makecert`-Batchdatei.

```
C:\makecert>makecert
Gueltigkeit des neuen Zertifikats:
1. Ein Jahr
2. Zwei Jahre
3. Drei Jahre
4. Vier Jahre
5. Fuenf Jahre
Ihre Wahl: 5
```

```
C:\makecert>openssl req -x509 -newkey rsa:2048 -days 1825 -new -nodes -config
openssl.cnf -outform PEM -keyform PEM -keyout privatekey.pem -out newcert.cer
Using configuration from openssl.cnf
Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
.....+ ++
.....+ ++
writing new private key to 'privatekey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
```

3. Geben Sie jetzt die Daten des Rechners ein. Für einige Felder gibt es einen Standardwert, der in eckigen Klammern angegeben ist. Wollen Sie diesen verwenden, so drücken Sie einfach nur Return. Verwenden Sie keine Umlaute und andere Sonderzeichen, da es sonst zu Problemen kommen kann. Der "Common Name" (oder "Rechnername" auf dem Intranator) muss eindeutig sein und darf nicht auf anderen Rechnern oder für eine CA wiederverwendet werden.

```
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:Firma GmbH
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:iPhone Mueller
Email Address []:
```

```
C:\makecert>openssl pkcs12 -export -in newcert.cer -inkey privatekey.pem
-out newcert.p12
Loading 'screen' into random state - done
```

- Wählen Sie ein Transportpasswort, mit dem die Schlüsseldatei auf dem Weg zum VPN-Client im iPhone geschützt wird. Das Passwort muss mindestens 4 Zeichen lang sein.

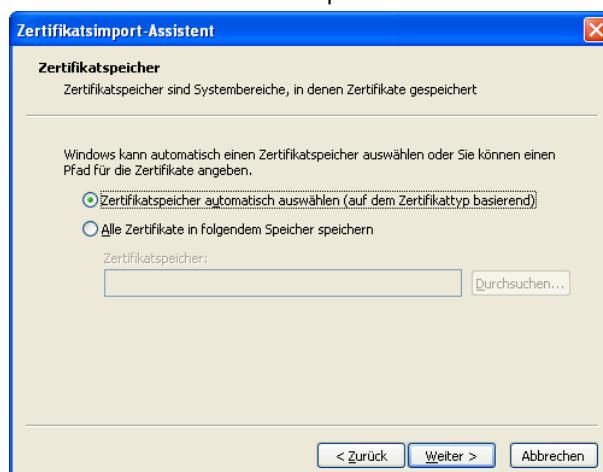
```
Enter Export Password:
Verifying password - Enter Export Password:
```

```
C:\makecert>del privatekey.pem
```

- Der eigene Schlüssel für das iPhone muss nun auf dem PC mit dem iPhone Konfigurationsprogramm installiert werden. Dies ist normalerweise über einen Doppelklick auf die Datei `newcert.p12` im Windows Explorer möglich.
- Es startet der Zertifikatsimport-Assistent. Geben Sie das eben gewählte Transportpasswort ein und markieren den Schlüssel als exportierbar (ansonsten kann er nicht auf das iPhone transferiert werden).



- Lassen Sie den Zertifikatsspeicher automatisch auswählen.



- Starten Sie nun das iPhone Konfigurationsprogramm und legen ein neues Konfigurationsprofil an.



9. Wechseln Sie zum Menü Zertifikate und fügen ein neues Zertifikat hinzu.



10. Sie bekommen den Inhalt mehrerer Zertifikatsspeicher angezeigt. In der Spalte Ausgestellt für sind die Zertifikate nach dem Inhalt des Feldes Common Name sortiert. Wählen Sie das eben erstellte eigene Zertifikat aus.



11. Geben Sie das vorhin gewählte Transportpasswort ein.



12 Als nächstes muss das Zertifikat des iPhones auch dem Intranator bekannt gemacht werden. Öffnen Sie dazu im "makecert"-Programmverzeichnis die Zertifikatsdatei (`newcert.cer`) mit einem Texteditor (z.B. Wordpad) und übernehmen den gesamten Inhalt der Datei in die Zwischenablage.

13. Öffnen Sie im Intranator das Menü System > Schlüssel > Fremde Schlüssel und legen einen neuen Schlüssel an. Vergeben Sie einen Namen für den Schlüssel (z.B. den Namen des Mitarbeiters) und fügen dann die Zertifikatsdaten aus der Zwischenablage in das Feld Copy & Paste Schlüssel ein.

45.2. Zertifikat für den Intranator

Das iPhone benötigt eine besondere Konfiguration des Zertifikats auf dem Intranator. Es wird kein selbstsignierter Schlüssel akzeptiert, sondern ein CA-signiertes Zertifikat. Außerdem muss der Servername im Feld Alternativer Schlüsselname (Subject Alternative Name) hinterlegt sein. Im Folgenden wird gezeigt, wie ein solcher Schlüssel auf dem Intranator erzeugt wird.

1. Legen Sie im Menü System > Schlüssel > Eigene Schlüssel ein neues Zertifikat vom Typ X.509 für den Intranator an. Dieses Zertifikat wird nachher nur indirekt zum Signieren verwendet, wir nennen es deshalb beispielsweise `intranator-ca`.

INTRANATOR BUSINESS SERVER 10

Intranator

System > Schlüssel > Eigene Schlüssel

Hauptseite Benutzermanager Netzwerk Dienste System Update Backup Diagnose Herunterfahren ISDN Sicherheit Schlüssel Eigene Schlüssel	Schritt 2 von 2: Schlüsseleigenschaften festlegen Schlüssellänge <input type="text" value="2048"/> <input type="button" value="..."/> Landeskürzel (C) <input type="text"/> Bundesstaat (ST) <input type="text"/> Stadt (L) <input type="text"/> Firma/Organisation (O) <input type="text"/> Abteilung (OU) <input type="text"/> Rechnername (CN) <input type="text" value="intranator-ca"/> Email (Email) <input type="text"/> Alternativer Schlüsselname <input type="text" value="Keine"/> <input type="button" value="..."/> Gültigkeitsdauer <input type="text" value="5 Jahre"/> <input type="button" value="..."/> <input type="button" value="Schlüssel erzeugen"/>
--	---

2. Wechseln Sie nach dem Erstellen auf den Reiter Daten und exportieren das Zertifikat in eine .cer-Datei.
3. Importieren Sie das Zertifikat über den Zertifikatsimport-Assistenten. Lassen Sie auch hier den Zertifikatsspeicher automatisch auswählen.
4. Fügen Sie nun dem iPhone-Konfigurationsprofil das eben erstellte und importierte CA-Zertifikat hinzu.





5. Legen Sie nun auf dem Intranator einen weiteren Schlüssel an. Dieser wird nachher vom Intranator genutzt und muss im Feld Alternativer Schlüsselname den externen DNS-Namen (z.B. von Dyndns) oder die externe feste IP des Intranators enthalten. Es bietet sich an denselben Namen auch bei Rechnername zu verwenden.

6. Nach Erstellen des Schlüssels öffnen Sie das Untermenü CA dieses eben erstellten Schlüssels. Signieren Sie nun den Schlüssel mit der vorher erstellten CA.

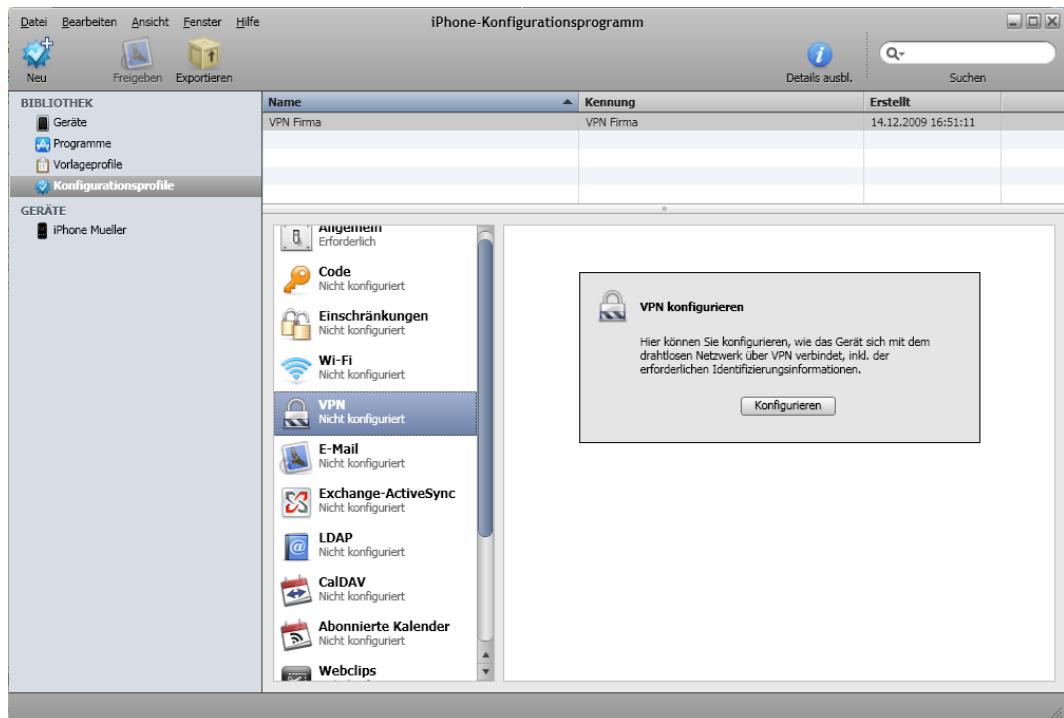
45.3. Verbindung auf dem Intranator

Legen Sie die VPN-Verbindung wie grundsätzlich in Abschnitt 40.2, „Konfiguration auf dem Intranator“ beschrieben. Beachten Sie dabei folgende Punkte:

1. Sie müssen ein Verschlüsselungsprofil ohne PFS verwenden
2. Der Tunnel bekommt als Lokales Netz die Einstellung Alles (0.0.0.0/0.0.0.0). Die virtuelle IP auf Gegenseite wird per mode-config zugewiesen.
3. Verwenden Sie den eben signierten Schlüssel (nicht die CA) als Eigenen Schlüssel.
4. Aktivieren Sie den XAUTH Servermodus
5. Legen Sie unter Benutzermanager > Gruppen eine neue Benutzergruppe an und verleihen ihr das Recht Anmeldung am VPN mit XAUTH. Fügen Sie nun alle Benutzer, die sich per iPhone verbinden können sollen, zu dieser Gruppe hinzu.

45.4. Verbindung auf dem iPhone

1. Öffnen Sie das iPhone Konfigurationsprogramm und fügen Ihrem Konfigurationsprofil eine neue VPN-Verbindung hinzu.



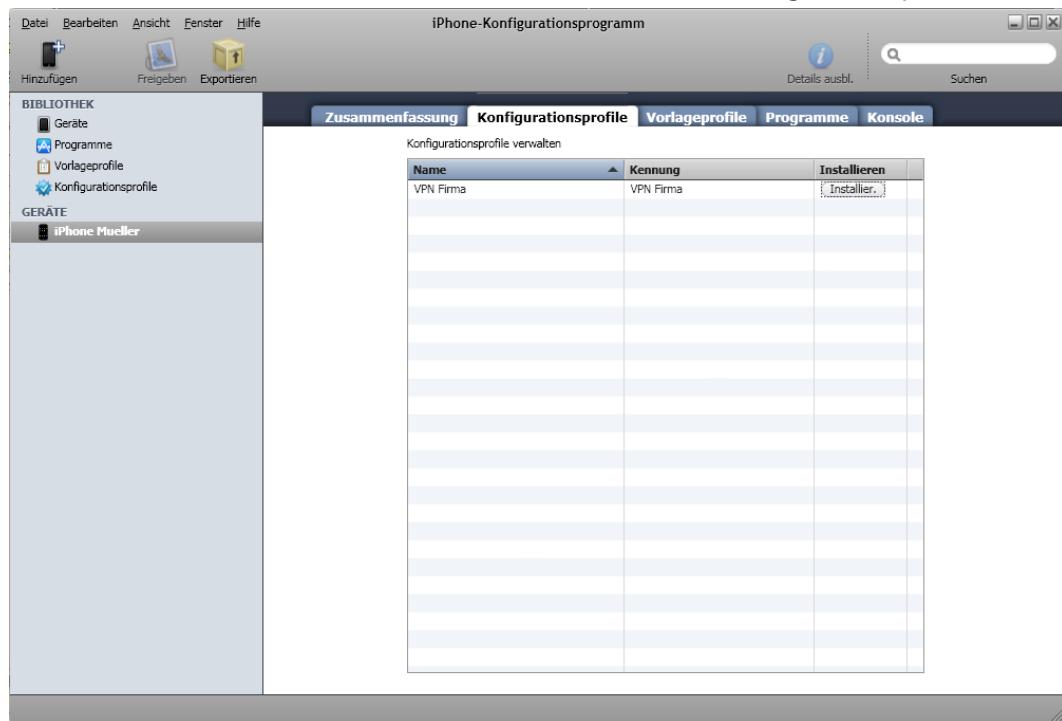
2. Wählen Sie als Verbindungstyp IPSec (Cisco). Der Server ist der externe DNS-Name oder IP Ihres Intranators. Diese Einstellung muss identisch zu den Daten im Feld Alternativer Schlüsselname des Intranator-Zertifikats sein.

Tragen Sie den Login des Benutzers aus dem Benutzermanager des Intranators im Feld Account ein.

Lassen Sie das Gerät per Zertifikat identifizieren und verwenden das vorher importierte Zertifikat.



3. Verbinden Sie das iPhone mit dem PC und installieren das Konfigurationsprofil.



4. Auf dem iPhone müssen Sie die Installation des Konfigurationsprofils bestätigen.



5. Geben Sie das vorhin gewählte Transportpasswort des eigenen Schlüssels ein.



6. Sie können die VPN-Verbindung nun im Menü Einstellungen über den Schalter VPN aufbauen.



Hinweis

Achten Sie aus Sicherheitsgründen darauf, dass vor Aufbau der VPN-Verbindung immer entweder die iPhone-PIN oder Benutzername und Passwort abgefragt werden. Ansonsten ist bei Verlust oder Diebstahl des Geräts der Zugang ins Firmennetz nicht geschützt.

46. Kapitel - VPN mit Android

Geräte mit Android Version 4 (Ice Cream Sandwich) oder neuer enthalten von Haus aus alles nötige, um VPN-Verbindungen mit dem Intranator aufzubauen zu können. Zusätzliche Software, Rootrechte und ähnliches werden nicht benötigt.

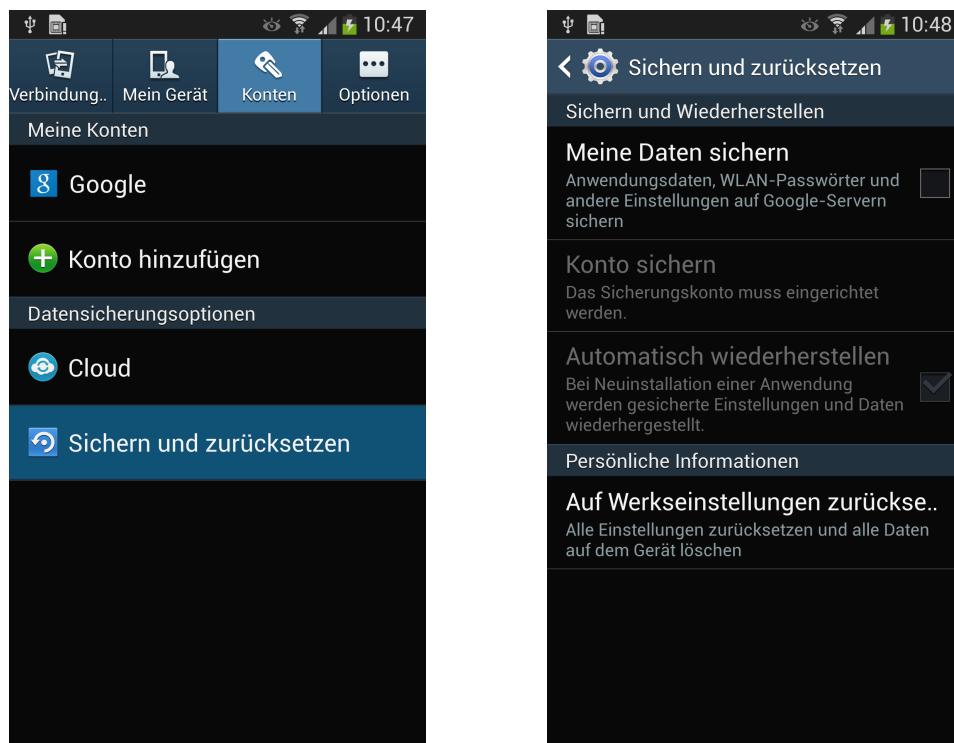
Geräte mit Android werden von vielen verschiedenen Herstellern angeboten. Jeder Hersteller hat die Möglichkeit, das Original-Android von Google auf seinen Geräten anzupassen. Daher können wir die Funktionsfähigkeit nicht für alle Geräte garantieren. Außerdem kann sich die Bedienung in Details von der hier vorgestellten unterscheiden. Diese Anleitung und Screenshots wurden mit einem Samsung Galaxy S4 erstellt.

Zur erstmaligen Einrichtung wird ein PC mit Windows und einer USB-Verbindung zum Android-Gerät benötigt.

46.1. Gerät vorbereiten

Kontrollieren Sie vor dem Einrichten der VPN-Verbindung, ob die Zugangsdaten geheim bleiben oder nicht. Öffnen Sie dazu die Einstellungen, Reiter Konten, Menüpunkt Sichern und zurücksetzen.

Die Einstellung Meine Daten sichern sollte deaktiviert sein. Ist diese Einstellung aktiv, werden die Zugangsdaten zu Google übertragen und dort unverschlüsselt gespeichert. Jeder, der das Passwort zu dem mit dem Gerät verknüpften Google-Account kennt, kann sie abrufen. Genauso Google selbst, sowie Dritte, die von Google dazu ermächtigt wurden.



Hinweis



War die Einstellung bisher aktiv, so sind alle auf dem Gerät gespeicherten Zugangsdaten (u.a. von E-Mail-Accounts, WLANs, Social-Media,...) als kompromittiert zu betrachten und sollten sofort geändert werden. Es ist davon

auszugehen, dass die Daten weiterhin bei Google gespeichert bleiben, auch wenn die Übertragung neuer Daten deaktiviert wurde.

46.2. Zertifikate

1. Android kann selbst keine eigenen Zertifikate erstellen. Dies übernimmt daher das Programm `makecert` auf einem PC.

Laden Sie vom Intranator unter Information > Download das Programm zum Erzeugen von Zertifikaten (`makecert`) herunter und entpacken Sie es in ein Verzeichnis auf Ihrem Rechner.

2. Starten Sie die `makecert`-Batchdatei.

```
C:\makecert>makecert  
Gueltigkeit des neuen Zertifikats:  
1. Ein Jahr  
2. Zwei Jahre  
3. Drei Jahre  
4. Vier Jahre  
5. Fuenf Jahre  
Ihre Wahl: 5
```

```
C:\makecert>openssl req -x509 -newkey rsa:2048 -days 1825 -nodes -config  
openssl.cnf -outform PEM -keyform PEM -keyout privatekey.pem -out newcert.cer  
Using configuration from openssl.cnf  
Loading 'screen' into random state - done  
Generating a 2048 bit RSA private key  
.....+++  
.....+  
writing new private key to 'privatekey.pem'  
-----  
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.
```

3. Geben Sie jetzt die Daten des Rechners ein. Für einige Felder gibt es einen Standardwert der in eckigen Klammern angegeben ist. Wollen Sie diesen verwenden, so drücken Sie einfach nur Return. Verwenden Sie keine Umlaute und andere Sonderzeichen, da es sonst zu Problemen kommen kann. Der "Common Name" (oder "Rechnername" auf dem Intranator) muss eindeutig sein und darf nicht auf anderen Rechnern oder für eine CA wiederverwendet werden.

```
Country Name (2 letter code) []:  
State or Province Name (full name) []:  
Locality Name (eg, city) []:  
Organization Name (eg, company) []:Firma GmbH  
Organizational Unit Name (eg, section) []:  
Common Name (eg, your name or your server's hostname) []:Android Mueller  
Email Address []:
```

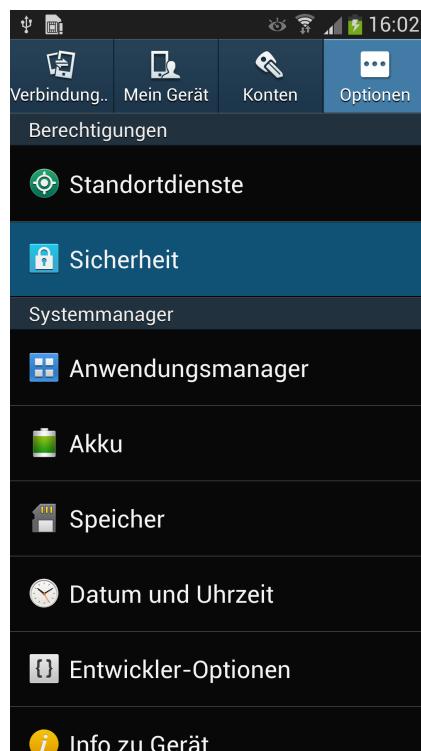
```
C:\makecert>openssl pkcs12 -export -in newcert.cer -inkey privatekey.pem  
-out newcert.p12  
Loading 'screen' into random state - done
```

4. Wählen Sie ein Transportpasswort, mit dem die Schlüsseldatei auf dem Weg zum VPN-Client im Gerät geschützt wird. Das Passwort muss mindestens 4 Zeichen lang sein.

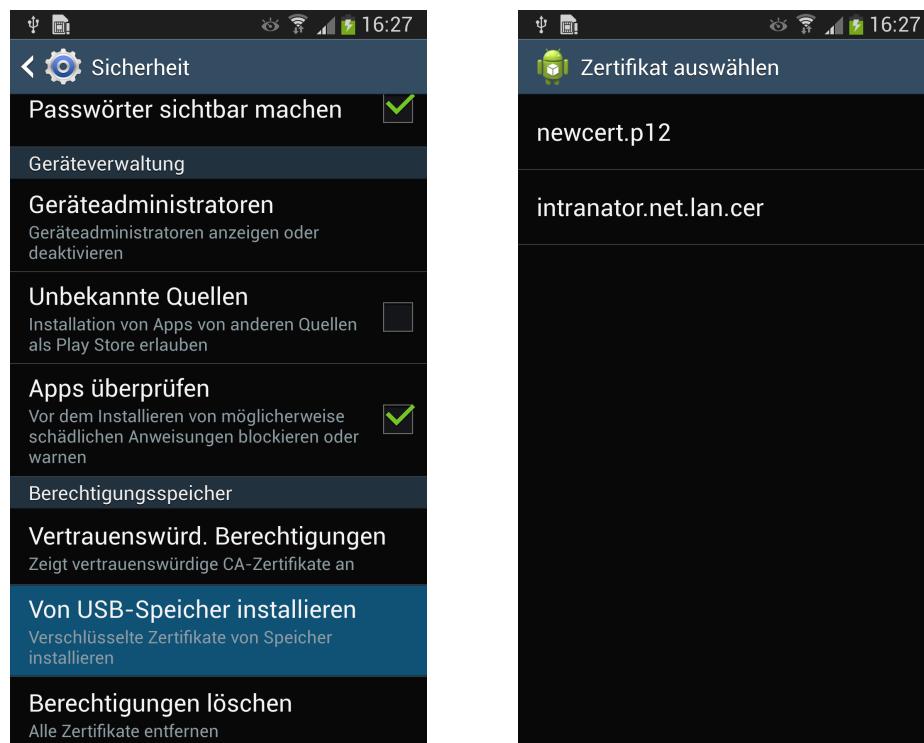
```
Enter Export Password:  
Verifying password - Enter Export Password:
```

```
C:\makecert>del privatekey.pem
```

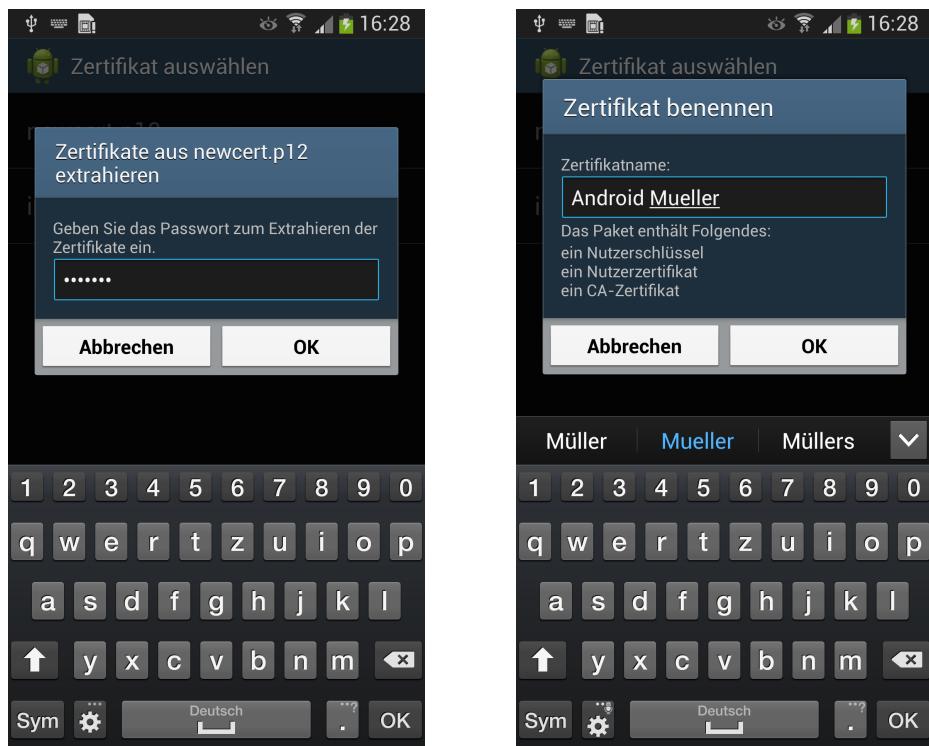
5. Das Schlüsselpaket für den Client liegt nun im PKCS#12-Format in der Datei `newkey.p12`, das Zertifikat für den Intranator (PEM-Format) in der Datei `newkey_cert.cer`.
6. Das Zertifikat des Clients wird nun dem Intranator bekannt gemacht. Öffnen Sie dazu die Zertifikatsdatei (`newkey_cert.cer`) mit einem Texteditor (z.B. Wordpad) und übernehmen den gesamten Inhalt der Datei in die Zwischenablage.
7. Öffnen Sie im Intranator das Menü System > Schlüssel > Fremde Schlüssel und legen einen neuen an. Vergeben Sie einen Namen für den Schlüssel (z.B. den Namen des Mitarbeiters) und fügen dann die Zertifikatsdaten aus der Zwischenablage in das Feld "Copy & Paste Schlüssel" ein.
8. Als nächstes bereiten wir das Zertifikat des Intranators für den Import in Android vor. Öffnen Sie dazu das Menü System > Schlüssel > Eigene Schlüssel und wählen das Zertifikat aus, das Sie für die Verbindung verwenden wollen. Es bietet sich an, für alle VPNs auf Seite des Intranators nur ein Zertifikat zu verwenden. Exportieren Sie nun das Zertifikat als .cer-Datei auf Ihren lokalen Rechner.
9. Verbinden Sie nun das Android-Gerät per USB mit Ihrem Rechner. Bei vielen Geräten haben Sie verschiedene Verbindungsmodi zur Auswahl. Wählen Sie einen Modus, in dem Sie Dateien zwischen PC und Android-Gerät austauschen können, z.B. Mediengerät (MTP) oder Laufwerk. Konsultieren Sie bei Unklarheiten das Handbuch Ihres Android-Geräts zum Thema Datenaustausch zwischen PC und Gerät.
10. Kopieren Sie nun (z.B. mit dem Windows Explorer) das vorher erstellte Schlüsselpaket (Dateiname `newcert.p12`) in das Wurzelverzeichnis des Android-Laufwerks.
11. Kopieren Sie auch die eben mit dem Browser heruntergeladene Zertifikatsdatei des Intranators in das Wurzelverzeichnis des Android-Laufwerks. Der Dateiname ist der im Intranator vergebene Name mit der Endung `.cer`.
12. Trennen Sie die Verbindung zwischen PC und Android-Gerät ordnungsgemäß über die Trennen-Funktion in der Taskleiste von Windows.
13. Öffnen Sie auf dem Android-Gerät die Einstellungen, Reiter Optionen, Sicherheit.



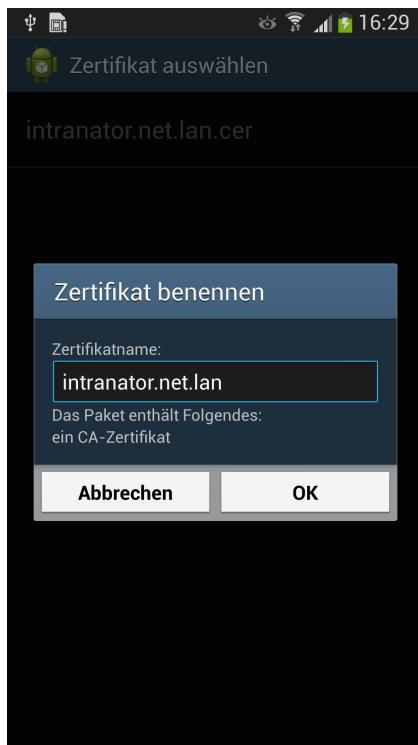
14. Öffnen Sie in der Kategorie Berechtigungsspeicher den Menüpunkt Von USB-Speicher installieren.



15. Klicken Sie den privaten Schlüssel (Dateiname newcert.p12) an um diesen zu importieren. Sie werden nach dem vorhin vergebenen Transportpasswort gefragt und bekommen dann die Möglichkeit, einen passenden Namen für das Zertifikat zu vergeben.



16. Klicken Sie das Zertifikat des Intranators an und vergeben einen passenden Namen.



17. Die Zertifikate sind nun zwischen den Geräten ausgetauscht und installiert.

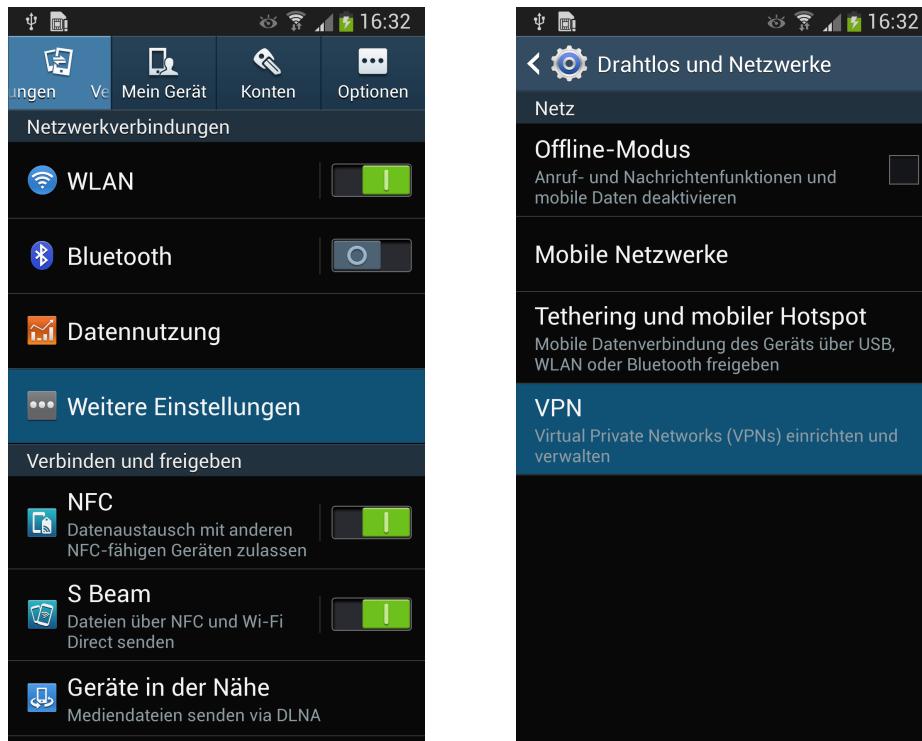
46.3. Verbindung auf dem Intranator

Legen Sie die VPN-Verbindung wie grundsätzlich in Abschnitt 40.2, „Konfiguration auf dem Intranator“ beschrieben an. Beachten Sie dabei folgende Punkte:

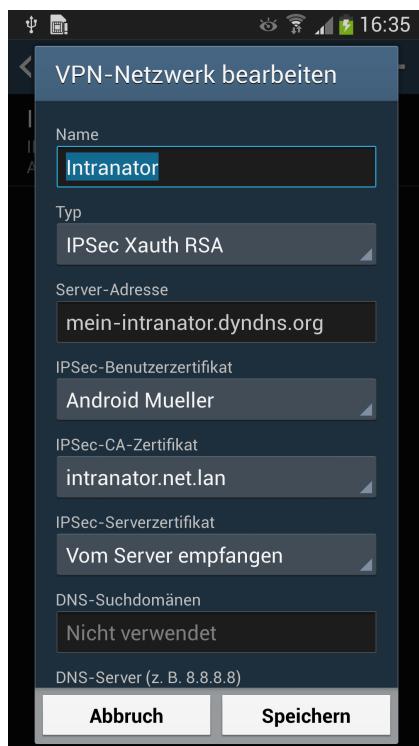
1. Sie müssen ein Verschlüsselungsprofil ohne PFS verwenden.
2. Der Tunnel bekommt als Lokales Netz die Einstellung Alles (0.0.0.0/0.0.0.0). Die virtuelle IP auf Gegenseite wird per mode-config zugewiesen.
3. Aktivieren Sie den XAUTH Servermodus.
4. Legen Sie unter Benutzermanager > Gruppen eine neue Benutzergruppe an und verleihen ihr das Recht Anmeldung am VPN mit XAUTH. Fügen Sie nun alle Benutzer, die sich von Android-Geräten verbinden können sollen, zu dieser Gruppe hinzu.

46.4. Verbindung auf Android

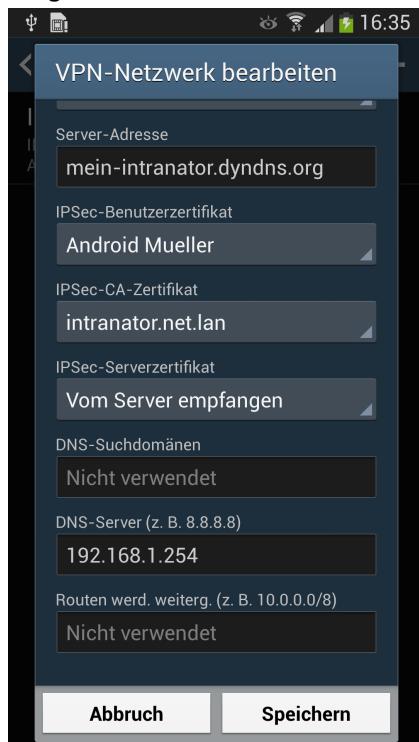
1. Öffnen Sie auf dem Android-Gerät die Einstellungen, Reiter Verbindungen, Kategorie Netzwerkverbindungen, Menüpunkt Weitere Einstellungen. Im darauf folgenden Menü öffnen Sie den Menüpunkt VPN.



2. Fügen Sie ein neues VPN hinzu und vergeben einen passenden Namen für die Verbindung.
3. Wählen als Typ für das VPN IPSec Xauth RSA aus.
4. Server-Adresse ist der extern erreichbare, offizielle DNS-Name Ihres Intranators (besser) oder zur Not seine externe, feste IP.
5. Wählen Sie nun das IPSec-Benutzerzertifikat, welches Sie vorhin vom PC importiert haben.
6. Wählen Sie bei IPSec-CA-Zertifikat das Zertifikat des Intranators aus.
7. Das IPSec-Serverzertifikat lassen Sie auf der Voreinstellung (Vom Server empfangen).

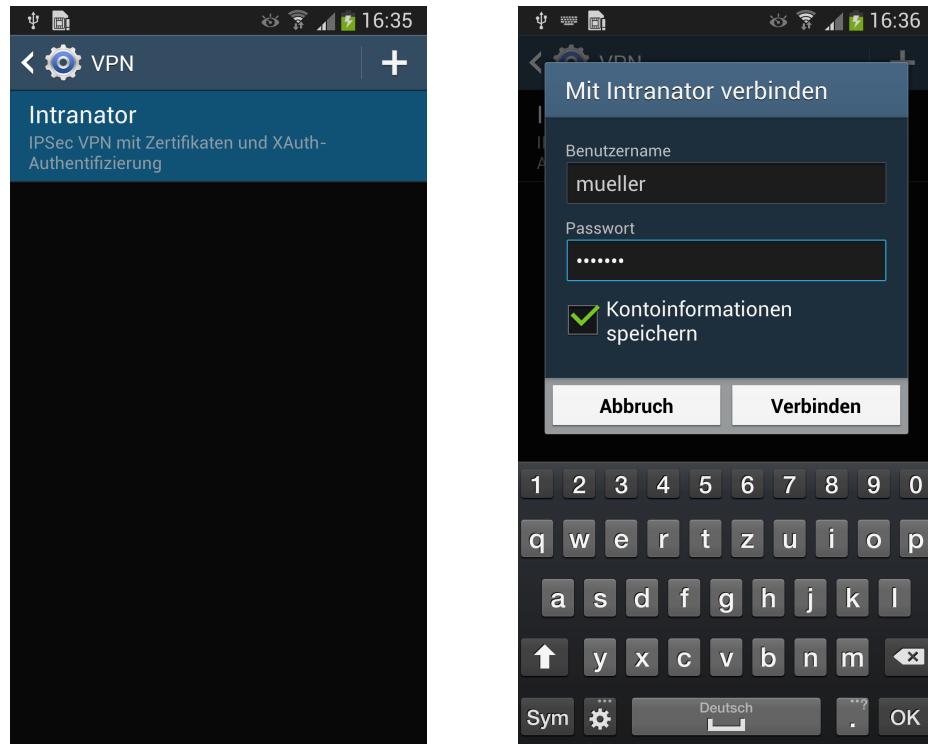


8. Aktivieren Sie Erweiterte Optionen anzeigen.
9. Tragen Sie bei DNS-Server die interne IP Ihres Intranators ein.



10. Speichern Sie die Verbindung.
11. Bei einem Klick auf den Namen der Verbindung werden Sie aufgefordert, Benutzernamen und Passwort einzugeben. Geben Sie die Login-Daten ein, wie auf dem Intranator im Benutzermanager hinterlegt. Der Benutzer muss sich auf dem Intranator

in einer Benutzergruppe befinden, die das Recht hat sich am VPN mit XAUTH anzumelden.



12. War der Verbindungsaufbau erfolgreich, wird oben links in der Statusleiste ein Schlüsselsymbol angezeigt.

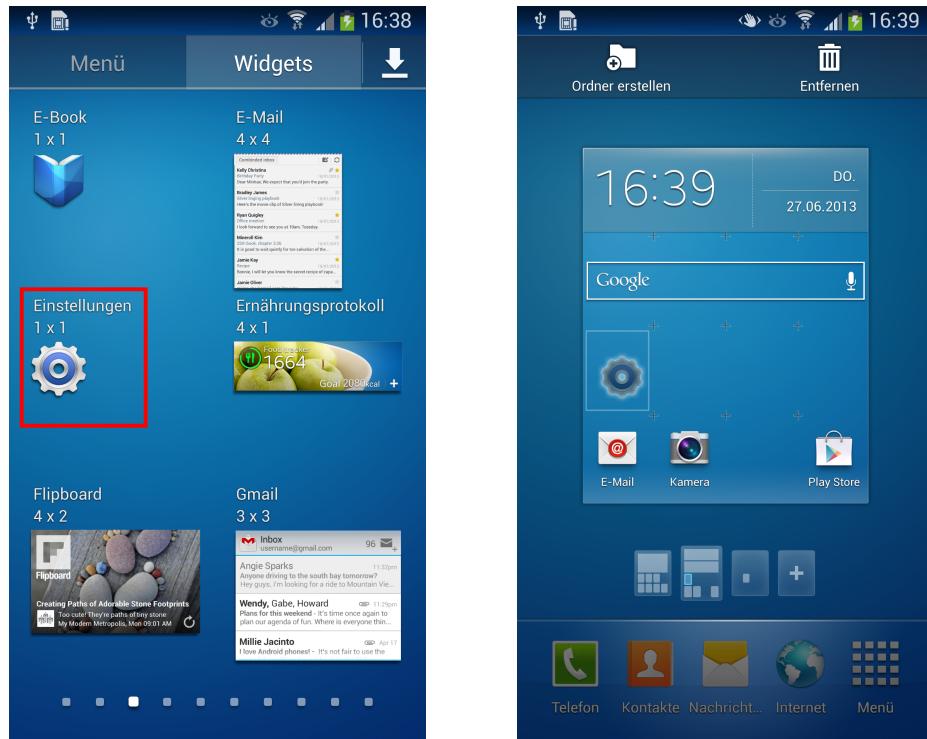
46.5. Verbindundsaufbau vereinfachen

Die Verbindung wird immer über das VPN-Menü aufgebaut. Damit dies einfacher aufgerufen werden kann, gehen Sie wie folgt vor:

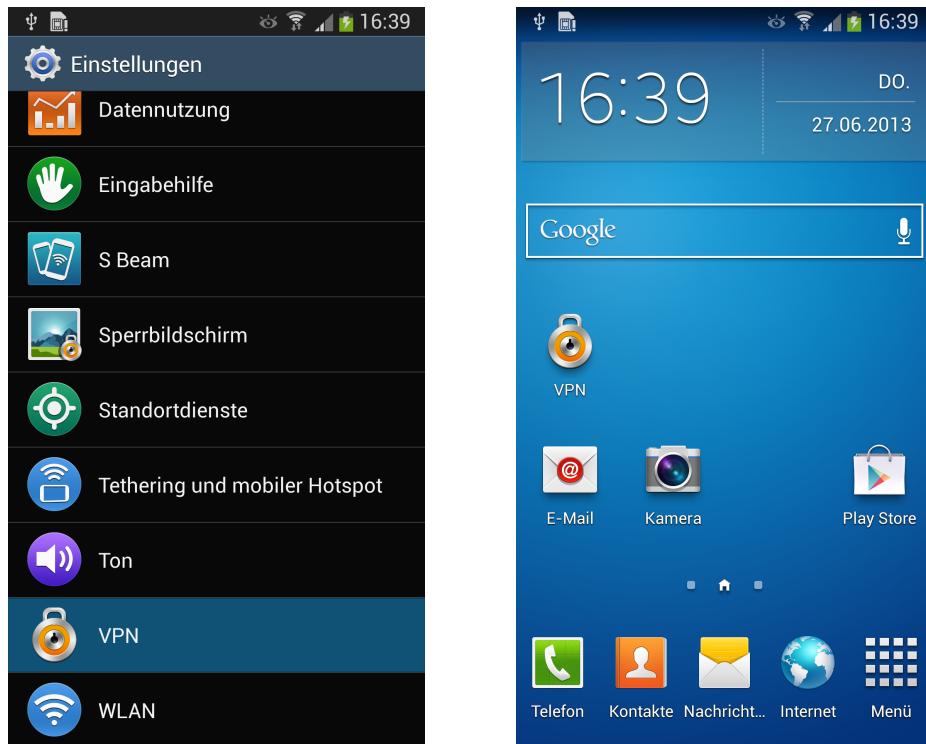
1. Gehen Sie auf den Hauptbildschirm und wählen Apps und Widgets hinzufügen.



2. Öffnen Sie den Reiter Widgets und suchen die Einstellungen. Halten Sie Ihren Finger auf den Einstellungen gedrückt bis der Hauptbildschirm angezeigt wird. Schieben Sie nun das Einstellungen-Widget auf einen freien Platz und lassen los.



3. Wählen Sie nun VPN. Das VPN-Menü ist nun direkt vom Hauptbildschirm erreichbar.



46.6. Verbindungsprotokolle

In Android ist ein Protokollierungssystem (logcat) integriert, welches Protokollmeldungen von allen Applikationen, wie dem VPN-System, entgegennimmt und zwischenspeichert. Zum Anzeigen und Exportieren wird eine zusätzliche App benötigt. Da die Logdateien typischerweise recht umfangreich und breit sind, empfiehlt es sich, sie nicht auf dem Gerät selbst zu analysieren, sondern sie per E-Mail oder Datei an einen PC zu senden. Es gibt verschiedene Apps, die diese Funktion beherrschen.

Als einfache und zuverlässige App können wir SendLog von Neil Boyd [<https://play.google.com/store/apps/details?id=org.l6n.sendlog>] empfehlen.



Wählen Sie in SendLog das Format time aus und senden Sie das Log z.B. per E-Mail an einen PC.

Einträge des VPN-Systems sind nach Datum und Uhrzeit mit dem Programmnamen „racoon“ gekennzeichnet.

Ein erfolgreicher Verbindungsauflaufbau sieht im Log dann beispielsweise so aus:

```
I/racoon (12321): 192.168.3.66[500] used for NAT-T
I/racoon (12321): 192.168.3.66[500] used as isakmp port (fd=10)
I/racoon (12321): 192.168.3.66[4500] used for NAT-T
I/racoon (12321): 192.168.3.66[4500] used as isakmp port (fd=11)
I/racoon (12321): initiate new phase 1 negotiation:
                 192.168.3.66[500]<=>88.89.90.1[500]
I/racoon (12321): begin Identity Protection mode.
I/racoon (12321): received Vendor ID: CISCO-UNITY
I/racoon (12321): received Vendor ID: draft-ietf-ipsra-isakmp-xauth-06.txt
I/racoon (12321): received Vendor ID: DPD
```

```
I/racoon (12321): received Vendor ID: RFC 3947
I/racoon (12321): Selected NAT-T version: RFC 3947
I/racoon (12321): Hashing 88.89.90.1[500] with algo #2
I/racoon (12321): Hashing 192.168.3.66[500] with algo #2
I/racoon (12321): Adding remote and local NAT-D payloads.
I/racoon (12321): Hashing 192.168.3.66[500] with algo #2
I/racoon (12321): NAT-D payload #0 verified
I/racoon (12321): Hashing 88.89.90.1[500] with algo #2
I/racoon (12321): NAT-D payload #1 verified
I/racoon (12321): NAT not detected
W/racoon (12321): unable to get certificate CRL(3) at depth:
                  0 SubjectName:/CN=mein-intranator.dyndns.org
I/racoon (12321): ISAKMP-SA established 192.168.3.66[500]-88.89.90.1[500]
                  spi:9188e3843d64a14d:e6b839a89f64ea7f
W/racoon (12321): Ignored attribute UNITY_BANNER
W/racoon (12321): Ignored attribute APPLICATION_VERSION
V/Vpn   (17141): interface tun0 added
D/VpnJni (17141): Route added on tun0: 0.0.0.0/0
V/LegacyVpnRunner(17141): set routes 0.0.0.0/0 on tun0
D/ConnectivityService(17141): adding dns 192.168.13.254 for VPN
I/LegacyVpnRunner(17141): Connected!
```

Android baut in diesem Moment wie man sieht nur Phase 1 auf und konfiguriert eine Route sowie den DNS-Server. Erst wenn tatsächlich Daten zur Übertragung anstehen wird Phase 2 aktiviert:

```
I/racoon (12321): initiate new phase 2 negotiation:
                  192.168.3.66[500]<=>88.89.90.1[500]
W/racoon (12321): low key length proposed, mine:256 peer:128.
W/racoon (12321): authtype mismatched: my: hmac-md5 peer: hmac-sha
I/racoon (12321): IPsec-SA established: ESP/Tunnel
                  192.168.3.66[500]->88.89.90.1[500] spi=80734113(0x4cf7a1)
I/racoon (12321): IPsec-SA established: ESP/Tunnel
                  192.168.3.66[500]->88.89.90.1[500] spi=3232115548(0xc0a62b5c)
```

47. Kapitel - VPN mit dem NCP Client für Windows Mobile

Den NCP Secure Entry Windows Mobile Client können Sie von dieser URL als 30-Tage-Testversion herunterladen: <http://www.ncp-e.com/de/downloads/software.html>

47.1. Installation

1. Installieren Sie Microsoft ActiveSync und verbinden Ihr Mobiltelefon mit dem PC.
2. Starten Sie das Installationsprogramm des NCP Secure Entry Windows Mobile Client. Nach Abschluss der Installation wird der Windows Mobile Teil des Clients automatisch an das angeschlossene Handy übertragen.
3. Laden Sie vom Intranator unter Information > Download das "Programm zum Erzeugen von Zertifikaten" (makecert) herunter und entpacken Sie es in ein Verzeichnis auf Ihrem Rechner.

47.2. Zertifikate

Der NCP Secure Windows Mobile Client kann keine eigenen Zertifikate erstellen. Dies übernimmt daher das Programm makecacert, welches im makecert-Paket enthalten ist. Der Unterschied zwischen makecacert und makecert ist, dass makecert selbstsignierte Zertifikate erzeugt, makecacert dagegen welche, die von einer (dummy) Zertifizierungsstelle (CA) signiert wurden.

1. Starten Sie die Batchdatei makecacert.bat und wählen eine Laufzeit in Jahren für Ihr Zertifikat.

```
c:\makecert>makecacert.bat
Gueltigkeit des neuen Zertifikats:
1. Ein Jahr
2. Zwei Jahre
3. Drei Jahre
4. Vier Jahre
5. Fuenf Jahre
Ihre Wahl: 5
```

```
c:\makecert>openssl req -newkey rsa:2048 -days 1825 -x509 -out cacert.pem -keyout
cakey.pem -config openssl-ca.cnf -batch -passout pass:geheim -set_serial 31659
```

```
Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'cakey.pem'
-----
```

```
c:\makecert>openssl req -newkey rsa:2048 -nodes -config openssl.cnf -keyout priv
atekey.pem -out request.pem
Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'privatekey.pem'
-----
```

2. Sie werden nach den Inhaberdaten des neuen Zertifikats gefragt. Es kommt vor allem darauf an, dass die dort eingetragenen Daten eindeutig sind und in dieser Form nicht in einem anderen Zertifikat verwendet werden. Wir empfehlen, z.B. den Benutzernamen in das Feld "Common Name" einzufügen. Hier in diesem Beispiel ist dies "Markus Mustermann".

Bitte verwenden Sie keine Umlaute und Sonderzeichen, da dies zu Problemen führen kann.

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

```
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:Markus Mustermann
Email Address []:
```

```
c:\makecert>openssl x509 -days 365 -out newkey_cert.cer -in request.pem -req -CA cacert.pem -CAkey cakey.pem -set_serial 1 -passin pass:geheim
Loading 'screen' into random state - done
Signature ok
subject=/CN=Markus Mustermann
Getting CA Private Key

c:\makecert>del request.pem

c:\makecert>rem --- please enter the transport password now (just used for transport, enter this one while importing) ---

c:\makecert>openssl pkcs12 -export -in newkey_cert.cer -inkey privatekey.pem -certfile cacert.pem -out newkey.p12
Loading 'screen' into random state - done
```

3. Als nächstes müssen Sie ein Passwort für Ihr Zertifikat wählen. Mit diesem Passwort wird das Zertifikat (und damit der VPN-Zugang) geschützt. Sie müssen es beim Aufbau der VPN-Verbindung eingeben. Die Standardrichtlinie von NCP verlangt mindestens 6 Zahlen oder Zeichen.

```
Enter Export Password:
Verifying - Enter Export Password:

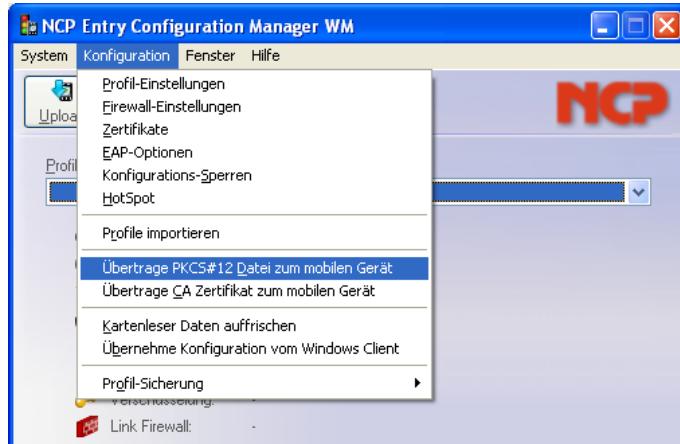
c:\makecert>del privatekey.pem

c:\makecert>del cacert.pem

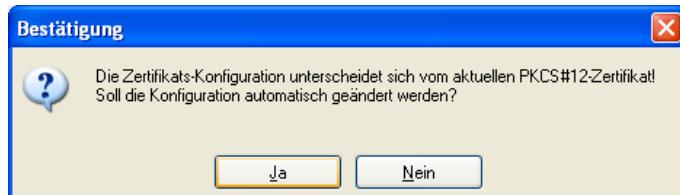
c:\makecert>del cakey.pem
```

4. Das Schlüsselpaket für den Client liegt nun im PKCS#12-Format in der Datei `newkey.p12`, das Zertifikat für den Intranator (PEM-Format) in der Datei `newkey_cert.cer`.

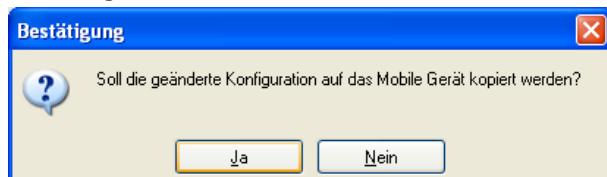
5. Starten Sie den Entry Configuration Manager WM und öffnen das Menü Konfiguration, Übertrage PKCS#12 Datei zum mobilen Gerät. Kopieren Sie die newkey.p12-Datei auf das mobile Gerät.



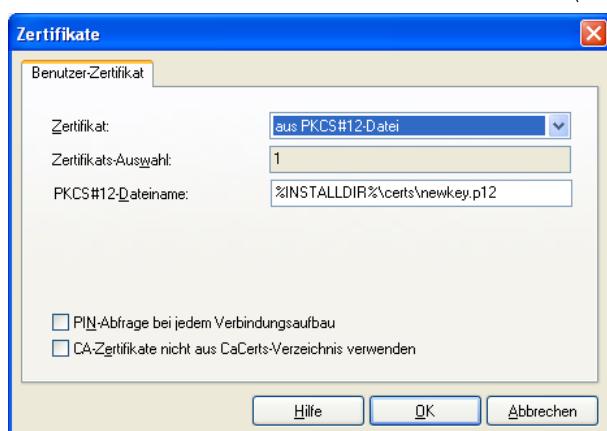
6. Lassen Sie die Zertifikats-Konfiguration automatisch vom Client anpassen.



7. Übertragen Sie die geänderte Konfiguration auf das mobile Gerät. Es erscheint die Meldung Upload wurde erfolgreich durchgeführt.

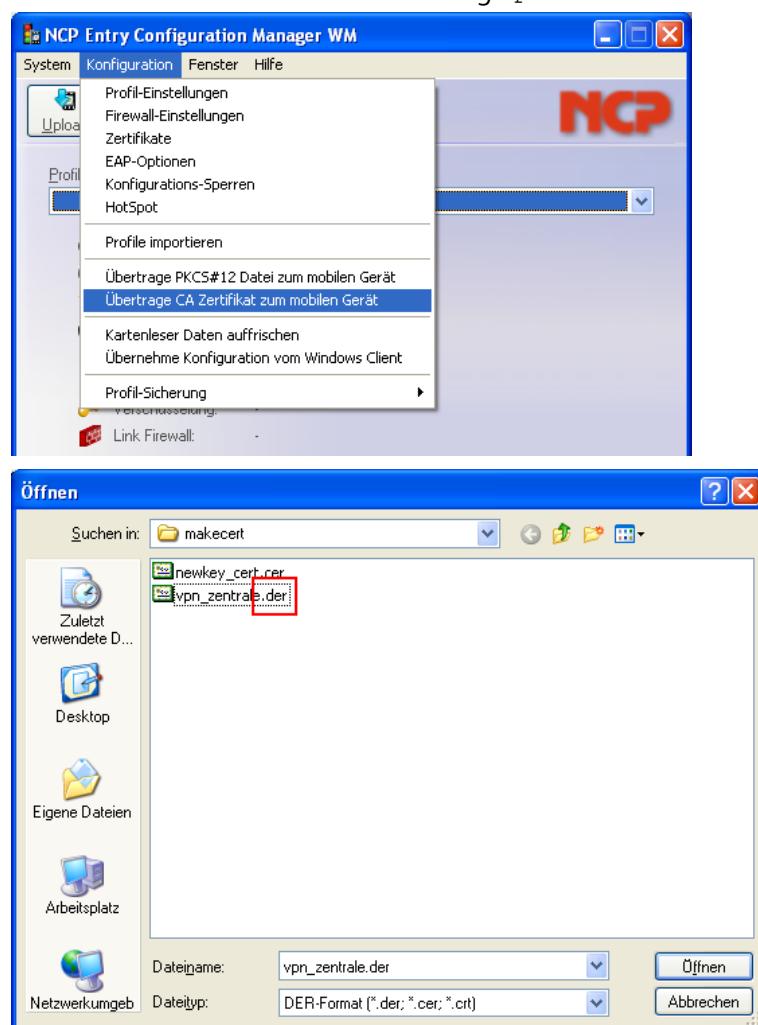


8. Öffnen Sie das Menü Konfiguration, Zertifikate und kontrollieren Sie die Einstellungen. Der PKCS#12-Dateiname sollte %INSTALLDIR%\certs\newkey.p12 sein.



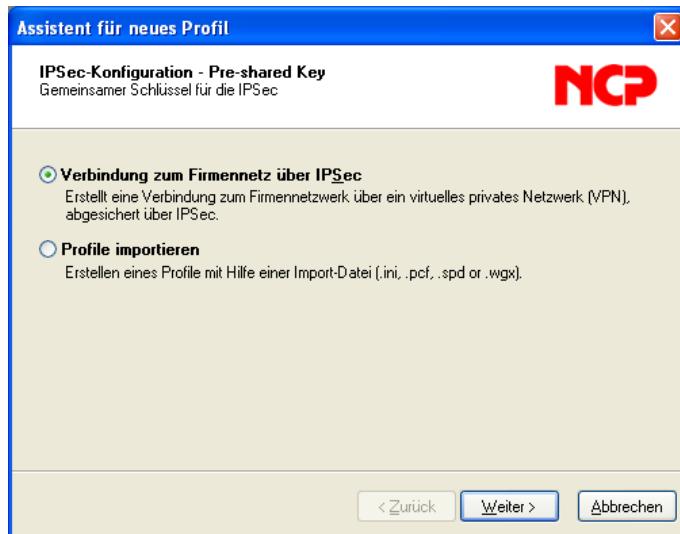
9. Als nächstes muss das Zertifikat des Clients auch dem Intranator bekannt gemacht werden. Öffnen Sie dazu die Zertifikatsdatei (newkey_cert.cer) mit einem Texteditor (z.B. Wordpad) und übernehmen den gesamten Inhalt der Datei in die Zwischenablage.

10. Öffnen Sie im Intranator das Menü System > Schlüssel > Fremde Schlüssel und legen einen neuen Schlüssel an. Vergeben Sie einen Namen für den Schlüssel (z.B. den Namen des Mitarbeiters) und fügen dann die Zertifikatsdaten aus der Zwischenablage in das Feld Copy & Paste Schlüssel ein.
11. Als letztes muss der NCP Client noch das Zertifikat des Intranators bekommen. Öffnen Sie das Menü System > Schlüssel > Eigene Schlüssel auf dem Intranator und wählen das Zertifikat aus, das Sie für die Verbindung verwenden wollen. Über den Link Zertifikat exportieren im Reiter Daten kann das Zertifikat in eine .pem-Datei gespeichert werden. Speichern Sie Datei in das Verzeichnis des makecert-Programms unter dem Namen `vpn_zentrale.pem`.
12. Das Zertifikat des Intranators muss nun vom PEM-Dateiformat in das für den NCP Windows Mobile Client geeignete DER-Format konvertiert werden. Starten Sie dazu folgenden Befehl im makecert-Programmverzeichnis: `openssl x509 -in vpn_zentrale.pem -inform PEM -out vpn_zentrale.der -outform DER`
13. Öffnen Sie im Entry Configuration Manager WM das Menü Konfiguration, Übertrage CA Zertifikat zum mobilen Gerät. Kopieren Sie die `vpn_zentrale.der`-Datei auf das mobile Gerät. Es erscheint die Meldung Upload wurde erfolgreich durchgeführt.



47.3. Verbindungen

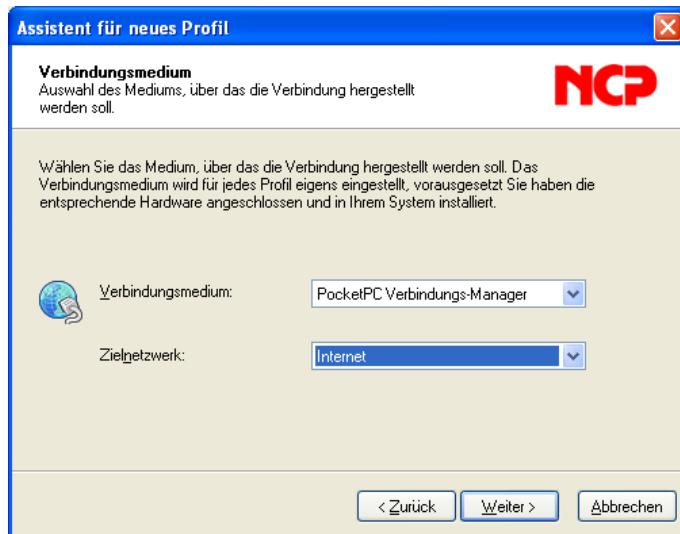
1. Öffnen Sie das Menü Konfiguration, Profil-Einstellungen. Starten Sie über Hinzufügen den Konfigurations-Wizard.
2. Wählen Sie die Option Verbindung zum Firmennetz über IPSec.



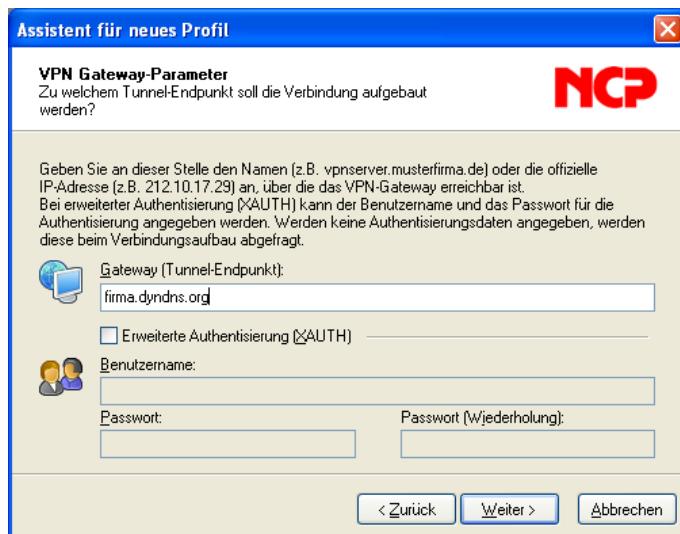
3. Vergeben Sie einen Namen für die Verbindung



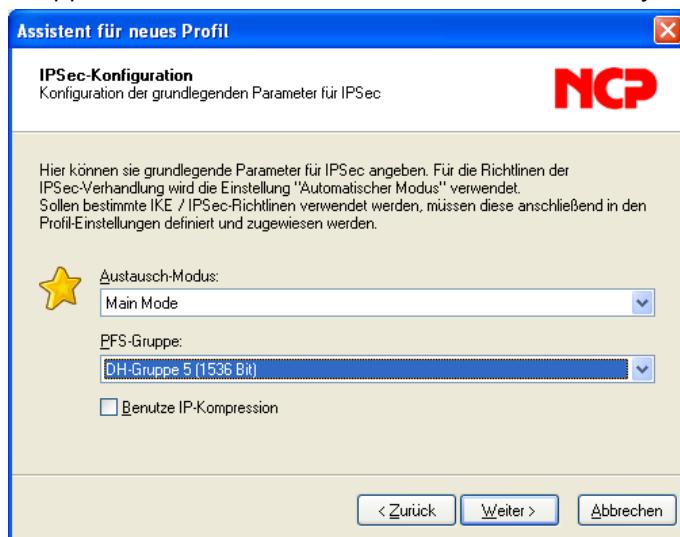
4. Wählen Sie das passende Verbindungsmedium.



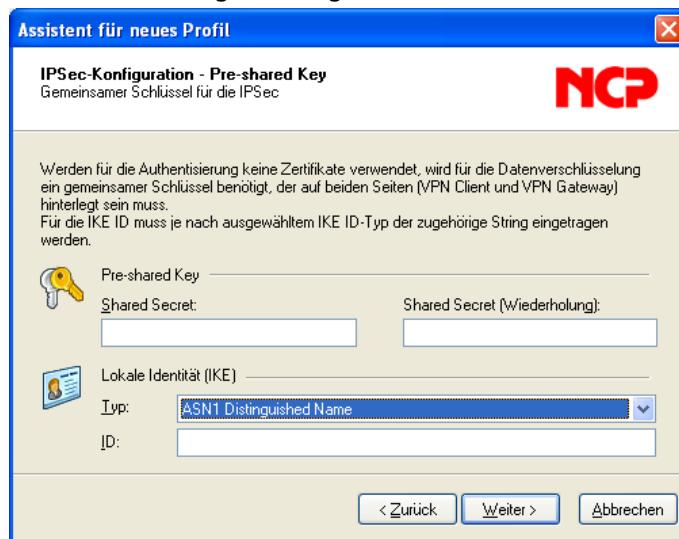
5. Tragen Sie die (externe) IP oder den (Dyn-)DNS-Namen des Intranators als Gateway ein. Lassen Sie XAUTH inaktiv.



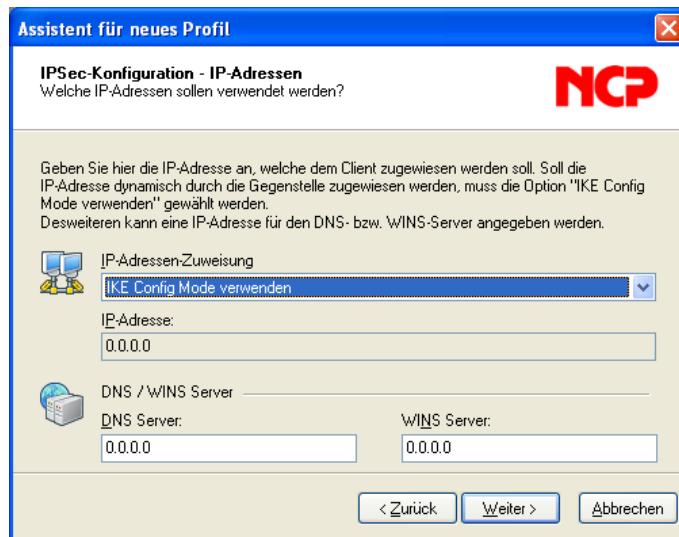
6. Verwenden Sie den "Main Mode" als Austausch-Modus und verwenden Sie die DH-Gruppe 5 (1536 Bit) für PFS (Perfect Forward Secrecy).



7. Lassen Sie die Einstellungen für Pre-shared Key leer und stellen den Typ der lokalen Identität auf ASN1 Distinguished Name. Dadurch werden die Daten aus dem Zertifikat zur Identifizierung übertragen.



8. Stellen Sie die IP-Adressen-Zuweisung auf IKE Config Mode verwenden. Eine eindeutige IP aus einem privaten Netzbereich wird später im Intranator bei Netz auf Gegenseite als IP zuweisen (mode-config) vergeben. Der DNS-Server wird automatisch vom Intranator übermittelt.



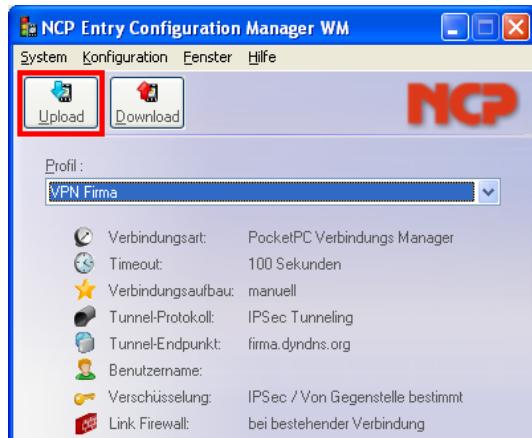
9. Aktivieren Sie die Firewall des NCP Clients, indem Sie die Stateful Inspection auf bei bestehender Verbindung stellen. Deaktivieren Sie NetBIOS über IP.



10. Als letztes müssen Sie noch das zu Verbindende VPN-Netz konfigurieren. Markieren Sie in den Profil-Einstellungen die eben erzeugte VPN-Verbindung und klicken auf Bearbeiten. Im Menüpunkt VPN-IP-Netze können Sie das Netz hinter dem Intranator eintragen.

Wenn Sie mehr als ein Netz mit einem Intranator verbinden möchten, können Sie auf Seite des NCP Clients mehrere Netze in dieses Menü eintragen. Auf dem Intranator müssen Sie hingegen mehrere separate Verbindungen konfigurieren.

11. Laden Sie das erstelle Profil mit Hilfe des Upload Buttons auf das mobile Gerät.



- 12 Konfigurieren Sie die VPN-Verbindung auf dem Intranator wie zuvor beschrieben mit Netz auf Gegenseite als IP zuweisen (mode-config).
13. Den NCP Client finden Sie auf Ihrem mobilen Gerät über Start Programme NCP Security Client. Sobald Sie die Verbindung aktivieren, müssen Sie das beim Erzeugen des privaten Schlüssels gewählte Passwort eingeben.

47.4. Intranator

Auf dem Intranator muss die Verbindung auch entsprechend konfiguriert werden. Für VPN-Clients wird dies im 40. Kapitel, „Anbinden von einzelnen PCs“ beschrieben.

48. Kapitel - VPN mit dem NCP Client für Symbian

Den NCP Secure Entry Symbian Client können Sie von dieser URL als 30-Tage-Testversion herunterladen: <http://www.ncp-e.com/de/downloads/software.html>

48.1. Installation

1. Installieren Sie die Nokia PC Suite und verbinden Ihr Mobiltelefon mit dem PC.
2. Starten Sie das Installationsprogramm des NCP Security Entry Client für Symbian. Nach Abschluss der Installation wird der Symbian Teil des Clients automatisch an das angegeschlossene Handy übertragen.
3. Laden Sie vom Intranator unter "Information > Download" das "Programm zum Erzeugen von Zertifikaten" (makecert) herunter und entpacken Sie es in ein Verzeichnis auf Ihrem Rechner.

48.2. Zertifikate

Der NCP Secure Entry Client kann keine eigenen Zertifikate erstellen. Dies übernimmt daher das Programm makecacert, welches im makecert-Paket enthalten ist. Der Unterschied zwischen makecacert und makecert ist, dass makecert selbstsignierte Zertifikate erzeugt, makecacert dagegen welche, die von einer (dummy) Zertifizierungsstelle (CA) signiert wurden.

1. Starten Sie die Batchdatei makecacert.bat und wählen eine Laufzeit in Jahren für Ihr Zertifikat.

```
c:\makecert>makecacert.bat
Gueltigkeit des neuen Zertifikats:
1. Ein Jahr
2. Zwei Jahre
3. Drei Jahre
4. Vier Jahre
5. Fuenf Jahre
Ihre Wahl: 5
```

```
c:\makecert>openssl req -newkey rsa:2048 -days 1825 -x509 -out cacert.pem -keyout
cakey.pem -config openssl-ca.cnf -batch -passout pass:geheim -set_serial 31659
```

```
Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'cakey.pem'
-----
```

```
c:\makecert>openssl req -newkey rsa:2048 -nodes -config openssl.cnf -keyout priv
atekey.pem -out request.pem
Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'privatekey.pem'
-----
```

2. Sie werden nach den Inhaberdaten des neuen Zertifikats gefragt. Es kommt vor allem darauf an, dass die dort eingetragenen Daten eindeutig sind und in dieser Form nicht in einem anderen Zertifikat verwendet werden. Wir empfehlen, z.B. den Benutzernamen in das Feld "Common Name" einzufügen. Hier in diesem Beispiel ist dies "Markus Mustermann".

Bitte verwenden Sie keine Umlaute und Sonderzeichen, da dies zu Problemen führen kann.

```
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.  
-----
```

```
Country Name (2 letter code) []:  
State or Province Name (full name) []:  
Locality Name (eg, city) []:  
Organization Name (eg, company) []:  
Organizational Unit Name (eg, section) []:  
Common Name (eg, your name or your server's hostname) []:Markus Mustermann  
Email Address []:
```

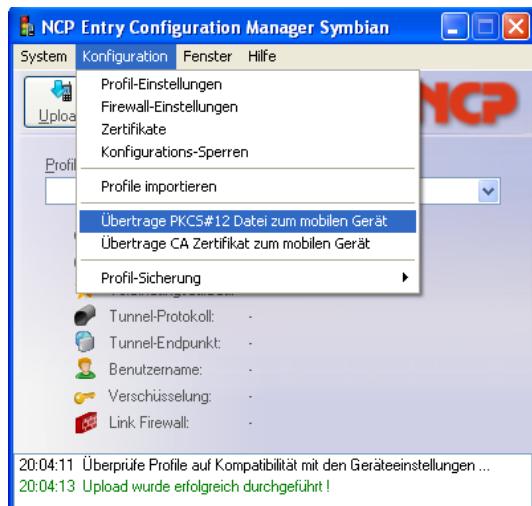
```
c:\makecert>openssl x509 -days 365 -out newkey_cert.cer -in request.pem -req -CA  
cacert.pem -CAkey cakey.pem -set_serial 1 -passin pass:geheim  
Loading 'screen' into random state - done  
Signature ok  
subject=/CN=Markus Mustermann  
Getting CA Private Key  
  
c:\makecert>del request.pem  
  
c:\makecert>rem --- please enter the transport password now (just used for trans  
port, enter this one while importing) ---  
  
c:\makecert>openssl pkcs12 -export -in newkey_cert.cer -inkey privatekey.pem -ce  
rtfile cacert.pem -out newkey.p12  
Loading 'screen' into random state - done
```

3. Als nächstes müssen Sie ein Passwort für Ihr Zertifikat wählen. Mit diesem Passwort wird das Zertifikat (und damit der VPN-Zugang) geschützt. Sie müssen es beim Aufbau der VPN-Verbindung eingeben. Verfügt Ihr Mobiltelefon nicht über eine QWERTZ-Tastatur, bietet es sich an, hier nur Zahlen zu verwenden. Die Standardrichtlinie von NCP verlangt mindestens 6 Zahlen oder Zeichen.

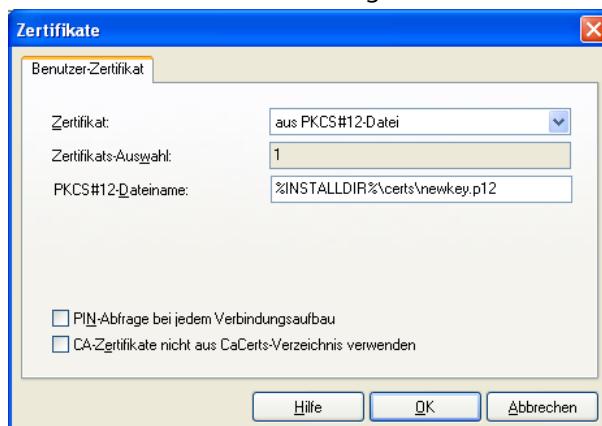
```
Enter Export Password:  
Verifying - Enter Export Password:  
  
c:\makecert>del privatekey.pem  
  
c:\makecert>del cacert.pem  
  
c:\makecert>del cakey.pem
```

4. Das Schlüsselpaket für den Client liegt nun im PKCS#12-Format in der Datei newkey.p12, das Zertifikat für den Intranator (PEM-Format) in der Datei newkey_cert.cer.

- Starten Sie den Entry Configuration Manager Symbian und öffnen das Menü Konfiguration, Übertrage PKCS#12 Datei zum mobilen Gerät. Kopieren Sie die newkey.p12-Datei auf das mobile Gerät. Es erscheint die Meldung Upload wurde erfolgreich durchgeführt.



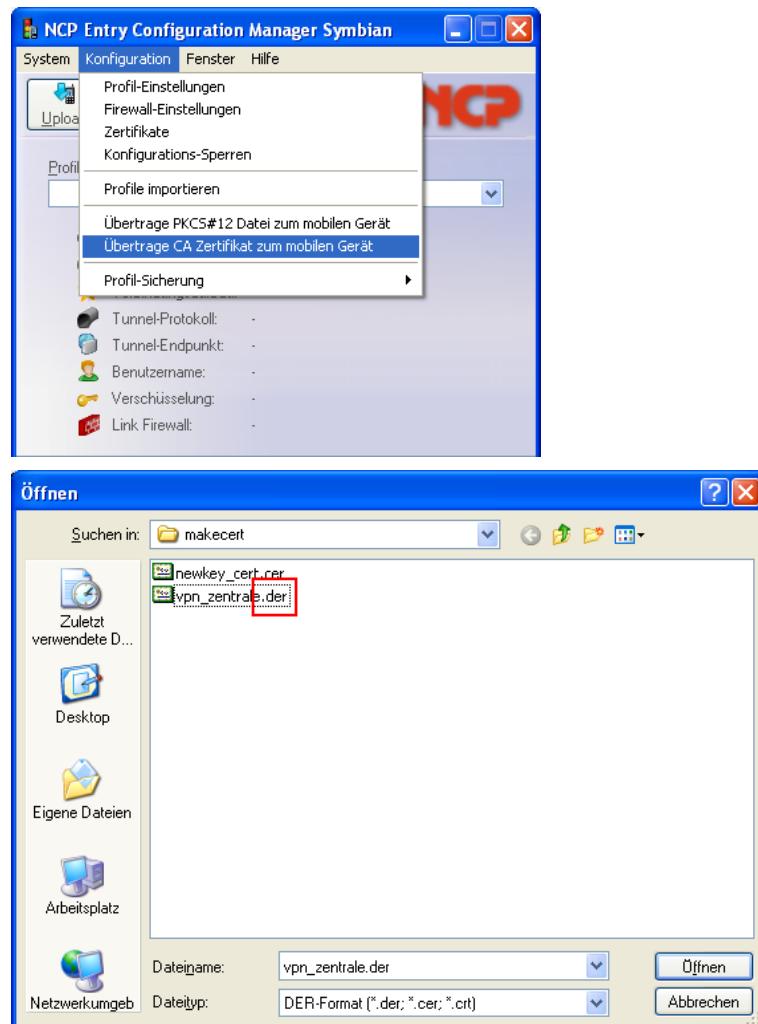
- Öffnen Sie das Menü Konfiguration, Zertifikate. Lassen Sie das Zertifikat aus einer PKCS#12-Datei laden und tragen als Pfad %INSTALLDIR%\certs\newkey.p12 ein.



- Als nächstes muss das Zertifikat des Clients auch dem Intranator bekannt gemacht werden. Öffnen Sie dazu die Zertifikatsdatei (newkey_cert.cer) mit einem Texteditor (z.B. Wordpad) und übernehmen den gesamten Inhalt der Datei in die Zwischenablage.
- Öffnen Sie im Intranator das Menü System > Schlüssel > Fremde Schlüssel und legen einen neuen Schlüssel an. Vergeben Sie einen Namen für den Schlüssel (z.B. den Namen des Mitarbeiters) und fügen dann die Zertifikatsdaten aus der Zwischenablage in das Feld "Copy & Paste Schlüssel" ein.
- Als letztes muss der NCP Client noch das Zertifikat des Intranators bekommen. Öffnen Sie das Menü System > Schlüssel > Eigene Schlüssel und wählen das Zertifikat aus, das Sie für die Verbindung verwenden wollen. Über den Link "Zertifikat exportieren" im Reiter Daten kann das Zertifikat in eine .pem-Datei gespeichert werden. Speichern Sie Datei in das Verzeichnis des makecert-Programms unter dem Namen vpn_zentrale.pem.
- Das Zertifikat des Intranators wird nun vom PEM Dateiformat in das für den NCP Client für Symbian geeignete DER Format konvertiert. Starten Sie folgenden Befehl im

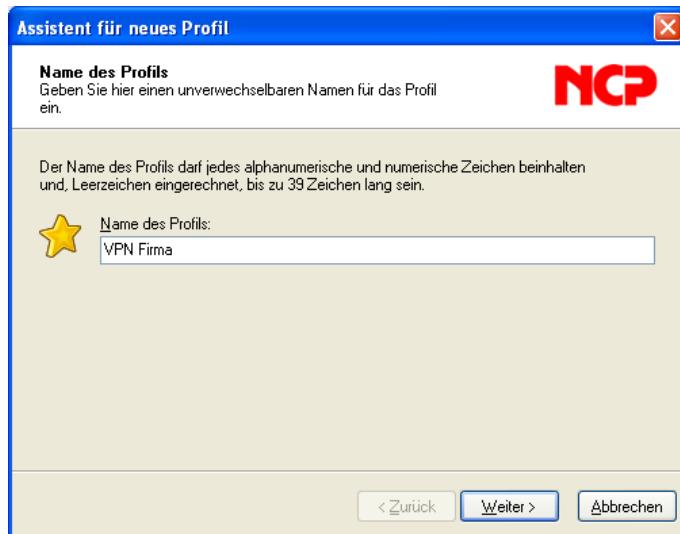
makecert-Programmverzeichnis: `openssl x509 -in vpn_zentrale.pem -inform PEM -out vpn_zentrale.der -outform DER`

11. Öffnen Sie im Entry Configuration Manager Symbian das Menü Konfiguration, Übertrage CA Zertifikat zum mobilen Gerät. Kopieren Sie die `vpn_zentrale.der`-Datei auf das mobile Gerät. Es erscheint die Meldung Upload wurde erfolgreich durchgeführt.



48.3. Verbindungen

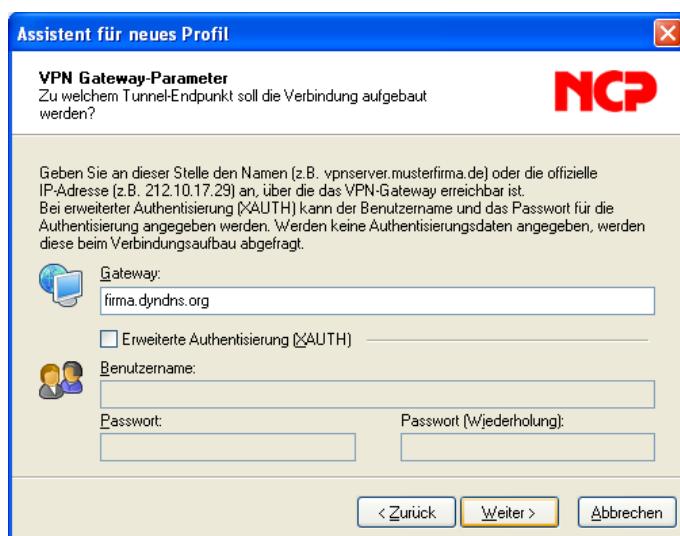
1. Öffnen Sie das Menü Konfiguration, Profil-Einstellungen. Starten Sie über Neuer Eintrag den Konfigurations-Wizard.
2. Vergeben Sie einen Namen für die Verbindung



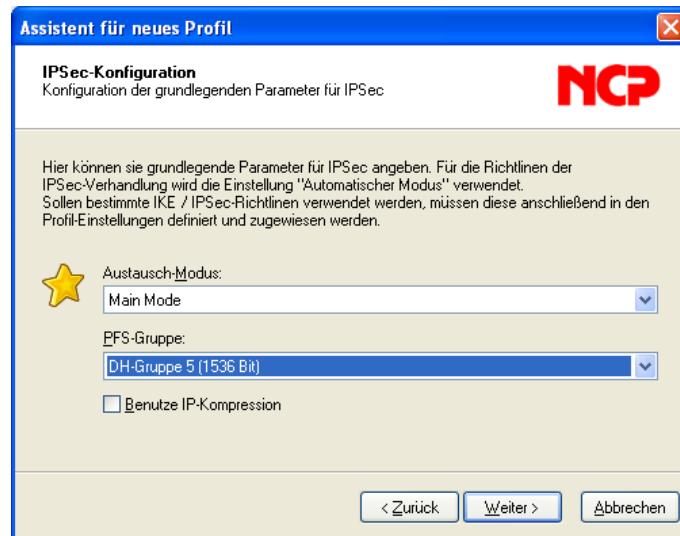
3. Wählen Sie den passenden Verbindungs- und Zugangspunkt.



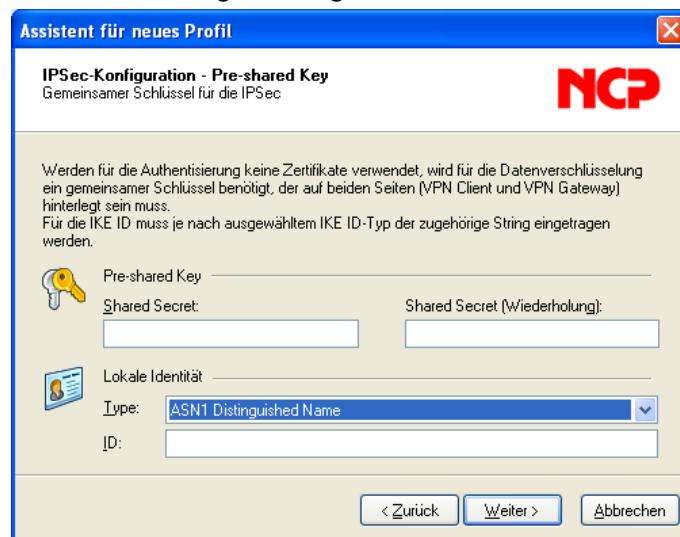
4. Tragen Sie die (externe) IP oder den (Dyn-)DNS-Namen des Intranators als Gateway ein. Lassen Sie XAUTH inaktiv.



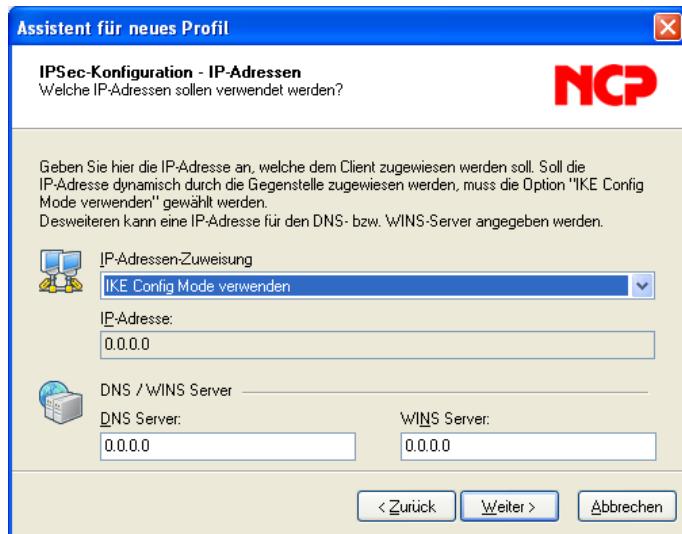
5. Verwenden Sie den "Main Mode" als Austausch-Modus und verwenden Sie die DH-Gruppe 5 (1536 Bit) für PFS (Perfect Forward Secrecy).



6. Lassen Sie die Einstellungen für Pre-shared Key leer und stellen den Typ der lokalen Identität auf "ASN1 Distinguished Name". Dadurch werden die Daten aus dem Zertifikat zur Identifizierung übertragen.



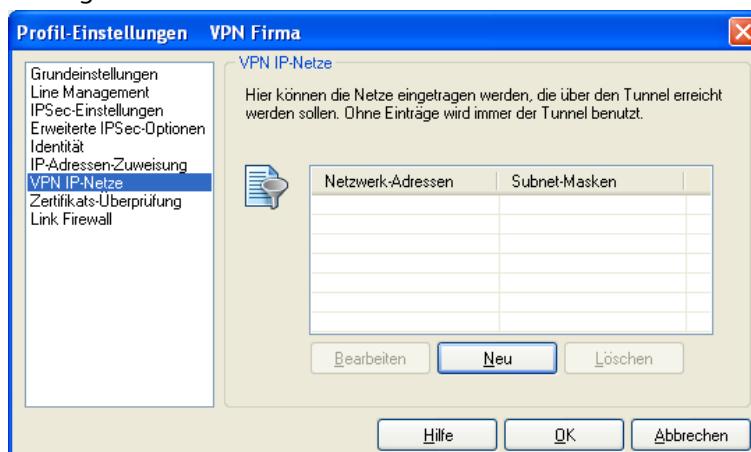
7. Stellen Sie die IP-Adressen-Zuweisung auf "IKE Config Mode verwenden". Eine eindeutige IP aus einem privaten Netzbereich wird später im Intranator bei Netz auf Gegenseite als IP zuweisen (mode-config) vergeben. Der DNS-Server wird automatisch vom Intranator übermittelt.

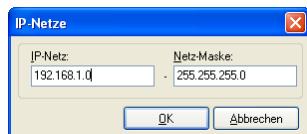


8. Aktivieren Sie die Firewall des NCP Clients, indem Sie die Stateful Inspection auf "bei bestehender Verbindung" stellen.



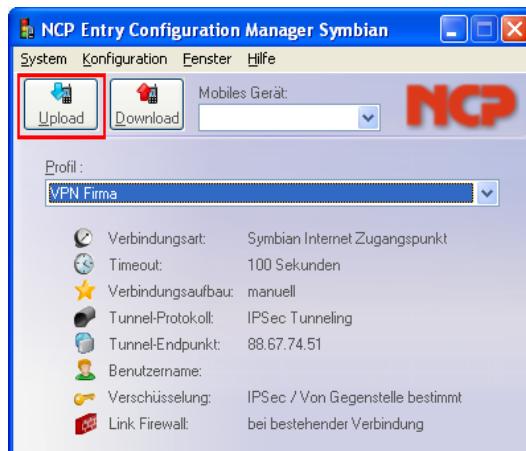
9. Als letztes müssen Sie noch das zu Verbindende VPN-Netz konfigurieren. Markieren Sie in den Profil-Einstellungen die eben erzeugte VPN-Verbindung und klicken auf Konfigurieren. Im Menüpunkt VPN-IP-Netze können Sie das Netz hinter dem Intranator eintragen.





Wenn Sie mehr als ein Netz mit einem Intranator verbinden möchten, können Sie auf Seite des NCP Clients mehrere Netze in dieses Menü eintragen. Auf dem Intranator müssen Sie hingegen mehrere separate Verbindungen konfigurieren.

10. Laden Sie das erstelle Profil mit Hilfe das Upload Buttons auf das mobile Gerät.



11. Konfigurieren Sie die VPN-Verbindung auf dem Intranator wie zuvor beschrieben mit Netz auf Gegenseite als IP zuweisen (mode-config).
12. Den NCP Client finden Sie auf Ihrem mobilen Gerät über Menü (Symbian Taste Programme Persönlich NCP Security Client. Sobald Sie die Verbindung aktivieren, werden Sie zur Eingabe des PINs für den privaten Schlüssel aufgefordert.

48.4. Intranator

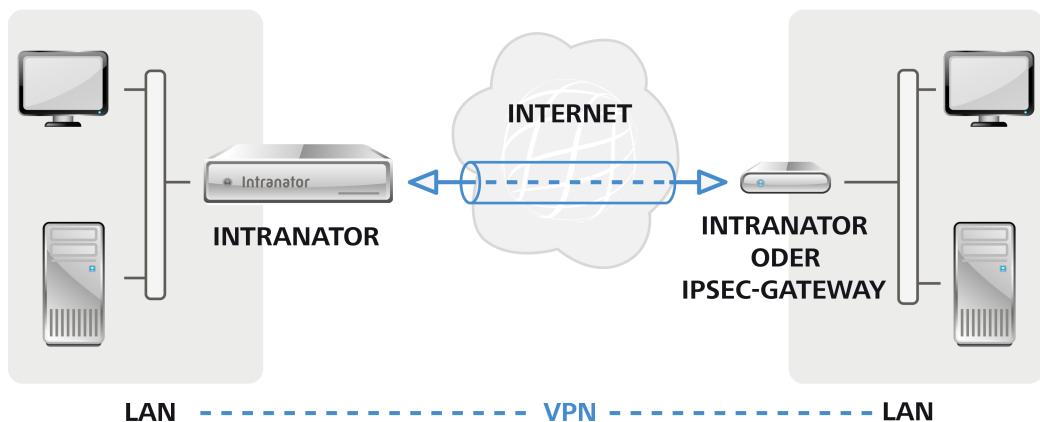
Auf dem Intranator muss die Verbindung auch entsprechend konfiguriert werden. Für VPN-Clients wird dies im 40. Kapitel, „Anbinden von einzelnen PCs“ beschrieben.

49. Kapitel - Anbinden von kompletten Netzen

49.1. Konzept

Wenn in einem entfernten Netz mehrere Rechner mit einem Netz hinter dem Intranator verbunden werden sollen (z.B. in einer Filiale), ist es normalerweise sinnvoller, ein VPN zwischen den beiden Netzen aufzubauen anstatt für jeden dieser Rechner ein einzelnes VPN.

Dieses VPN wird dann zwischen dem Intranator und einem IPSec Gateway vor dem anderen Netz aufgebaut. Dieses IPSec Gateway kann ein Intranator sein, es kann sich aber auch um ein anderes kompatibles Produkt handeln.



Über einen VPN-Tunnel können auch Netze mit privaten IPs verbunden werden. Die IPs dienen aber weiterhin zur Adressierung. Daher können Sie keine Netze mit identischen oder überlappenden Netzbereichen per VPN verbinden.

Achten Sie darauf, dass der Intranator und das IPSec Gateway auf der Gegenstelle selbst eine offizielle IP bekommen und nicht hinter einem Router stehen, der NAT macht. VPN hinter einem NAT-Router ist zwar möglich, kann jedoch vor allem dann zu Schwierigkeiten führen, wenn beide Seiten hinter NAT-Routern sind.

Es ist nicht notwendig, fest zugewiesene IPs zu verwenden, es können ohne Schwierigkeiten auf einer oder beiden Seiten dynamische IPs mit DynDNS zum Einsatz kommen.

Wenn die Verbindung auf einer Seite regelmäßig getrennt wird (z.B. durch Zwangstrennung bei DSL), sollten Sie dafür sorgen, dass die Verbindung von beiden Seiten her aufgebaut werden kann und nicht nur von einer.

Eine auf dem Intranator konfigurierte Verbindung gilt für die Verbindung von einem Netz auf Seite der Gegenstelle und einem Netz hinter dem Intranator. Möchten Sie mehrere Netze miteinander verbinden, können Sie für jede Netzkombination eine eigene Verbindung konfigurieren. Achten Sie darauf, für jede dieser Verbindungen immer dieselbe Kombination an Schlüsseln/Zertifikaten zu verwenden.

49.2. Konfiguration auf dem Intranator

49.2.1. Voraussetzungen

Als erstes müssen Sie dafür sorgen, dass jede Seite über einen eigenen Schlüssel verfügt und die Gegenseite den öffentlichen Schlüssel oder das Zertifikat der Gegenseite hat. Es empfiehlt sich, auf jedem System einen eigenen Schlüssel nur für VPNs anzulegen.

Wenn Sie auf dem Intranator mehrere VPNs einrichten, müssen Sie nicht für jede Verbindung extra einen eigenen Schlüssel anlegen: Sie können einen eigenen Schlüssel für alle VPNs verwenden. Nur von jeder der Gegenstellen benötigen Sie natürlich den öffentlichen Schlüssel.

Weitere Details zur Schlüsselverwaltung finden Sie im 39. Kapitel, „Schlüsselmanagement“.

49.2.2. Grundeinstellungen

Im Menü Dienste > VPN > Verbindungen können Sie VPN-Verbindungen im Intranator konfigurieren.

Auf der ersten Seite stellen Sie die Gegenstelle ein. Die Gegenstelle ist die offizielle IP, unter der der Intranator das IPSec-Gateway auf der anderen Seite der Verbindung erreichen kann. Verwechseln Sie diese nicht mit der IP, die die Gegenseite in ihrem eigenen Netz hat (typischerweise aus einem privaten Netzbereich).

Hat die Gegenseite eine feste IP, ist es vorteilhaft, diese IP einzutragen und nicht den DNS-Namen, der evtl. auch noch vorhanden ist. Ist die Gegenseite vom Intranator aus nicht erreichbar oder hat keinen DynDNS-Namen (z.B. weil Sie in einem UMTS-Netz liegt und dort hinter NAT nicht erreichbar ist), können Sie als Typ "Dynamische IP (Road Warrior)" eintragen. Diese Einstellung ist aber eher für einzelne Clients und nicht so sehr für dauerhaft aktive Verbindungen zwischen Netzen gedacht.

Über das Verschlüsselungsprofil können die verwendeten Verschlüsselungsalgorithmen ausgewählt werden; für Details siehe Abschnitt 38.5, „Algorithmen“. Wichtig ist vor allem, dass die Einstellung für PFS (Perfect Forward Secrecy) auf beiden Seiten identisch ist.

Über die Kapselung wird kontrolliert, wie die Pakete für den VPN-Tunnel eingepackt werden. Bei ESP wird die Verschlüsselung und Authentifizierung in eine Hülle eingepackt. Bei ESP+AH werden Verschlüsselung und Authentifizierung separat vorgenommen. ESP+AH kann nicht durch NAT geleitet werden, daher hat sich ESP durchgesetzt. Diese Einstellung muss auf beiden Seiten der Verbindung identisch sein.

49.2.3. Authentifizierung

Wählen Sie den eigenen und den Schlüssel der Gegenseite aus.

Wir raten aus den in Abschnitt 38.6, „Einschränkungen“ genannten Gründen davon ab, Verbindungen per Pre-Shared Key (PSK) zu authentifizieren. Sollten Sie es dennoch verwenden wollen, müssen Sie zusätzlich zu dem gemeinsamen Schlüssel die IPSec IDs der beiden Seiten wählen. Haben beide Seiten feste IPs, können Sie die IPs direkt als IPSec IDs verwenden. Bei dynamischen IPs empfiehlt es sich, E-Mail-Adressen als IPSec IDs einzutragen.

49.2.4. Tunnel konfigurieren

Auf der Seite "Tunnel" wird konfiguriert, welche Netze durch diese VPN-Verbindung miteinander verbunden werden.

Über den Punkt Lokales Netz wird das zu verbindende Netz auf Seite des Intranators gewählt. Wählen Sie bei der Option Lokale Netze eines der direkt an den Intranator angeschlossenen oder gerouteten Netze aus.

Wählen Sie bei Netz auf Gegenseite den Typ Freies Netz und tragen Sie IP und Netzmaske des Netzes hinter dem IPSec Gateway auf der Gegenseite ein.

Die Optionen zur Adressumschreibung (NAT) werden im 54. Kapitel, „Lösen von IP-Adresskonflikten in VPNs durch NAT“ erklärt.

49.2.5. Rechte

In diesem Menü werden die Rechte des VPN-Netzes auf der Gegenseite definiert. Dies betrifft alle Pakete, die aus diesem VPN-Netz kommen. Eine Beschreibung der Rechteoptionen finden Sie unter Abschnitt 9.2, „Zugriffsrechte eines Netzwerkobjekts“.

49.2.6. Aktivierung

In diesem Menü wird konfiguriert, wann die Verbindung aufgebaut und bestehende Sitzungen verlängert werden.

Beim passiven oder manuellen Start wartet der Intranator, bis entweder die Gegenseite die Verbindung aufbaut oder der Benutzer über die Hauptseite die Verbindung manuell aufbaut. Wird die Verbindung immer gestartet, versucht der Intranator kontinuierlich die Verbindung aufzubauen und offen zu halten.

Die Anzahl der Aufbauversuche betrifft nur den manuellen Aufbau über die Hauptseite. In Verbindung mit der Startvariante Immer hat diese Option keine Relevanz.

Die Lebensdauern für die beiden Phasen geben an, nach wie viel Minuten eine Verbindung wieder neu authentifiziert und neue Sitzungsschlüssel ausgehandelt werden. Die Zeit für Phase 1 sollte größer sein als die für Phase 2. Diese Werte müssen nicht mit den Einstellungen auf der Gegenseite übereinstimmen.

Ist bei Offline-Erkennung ein Wert eingetragen, sendet der Intranator mindestens so oft wie angegeben ein Paket an die Gegenseite. Kommt darauf mehrfach keine Antwort, wird die Verbindung getrennt und neu aufgebaut. Für diese Funktion wird die Dead-Peer-Detection (DPD) des IPSec-Standards verwendet.

50. Kapitel - VPN mit ZyXEL ZyWALL Routern

50.1. Überblick

Diese Anleitung wurde mit der ZyXEL ZyWALL P1 und ZyWALL 2 Plus getestet. Die größeren Modelle ZyWALL 5 UTM bis ZyWALL 70 UTM sind von der VPN-Konfiguration her identisch und daher sollte diese Anleitung auch für diese Modelle geeignet sein.

Die Modelle ZyXEL ZyWALL P1 und 2 Plus sind nicht mehr erhältlich. Eine Anleitung für die Nachfolgemodelle ZyXEL ZyWALL USG finden Sie in 51. Kapitel, „VPN mit ZyXEL ZyWALL USG“.

Die ZyXEL ZyWALL Router unterstützen VPN auch mit X.509-Zertifikaten und nicht nur Authentifizierung per Pre-Shared Key. Dadurch lassen sich die unter Abschnitt 38.6, „Einschränkungen“ beschriebenen Einschränkungen umgehen.

50.2. Vorbereitung

Der Router überprüft bei der Authentifizierung auch den Gültigkeitszeitraum des Zertifikats. Daher muss die Systemzeit immer korrekt sein, wenn eine VPN-Verbindung aufgebaut werden soll.

Der Router aktualisiert seine Zeit über das NTP-Protokoll. Dies kann im Menü "Maintenance" überprüft und konfiguriert werden. Öffnen Sie das Menü und überprüfen, ob die angezeigte Zeit korrekt ist.

Stellen Sie den Router am besten so ein, wie hier im Screenshot gezeigt.

General	Password	Time and Date	F/W Upload	Configuration	Restart																						
Current Time and Date <table> <tr> <td>Current Time</td> <td>20:11:48 GMT</td> </tr> <tr> <td>Current Date</td> <td>2006-02-13</td> </tr> </table> Time and Date Setup <table> <tr> <td><input checked="" type="radio"/> Manual</td> <td><input type="radio"/> Get from Time Server</td> </tr> <tr> <td>New Time (hh:mm:ss)</td> <td>20 : 11 : 21</td> </tr> <tr> <td>New Date (yyyy-mm-dd)</td> <td>2006 - 2 - 13</td> </tr> <tr> <td colspan="2"> Time Protocol NTP (RFC-1305) Time Server Address* de.pool.ntp.org <input type="button" value="Synchronize Now"/> </td> </tr> <tr> <td colspan="2"> <small>* Optional. There is a pre-defined NTP time server list.</small> </td> </tr> </table> Time Zone Setup <table> <tr> <td>Time Zone</td> <td>(GMT+01:00) Berlin, Stockholm, Rome, Bern, Brussels, Vienna</td> </tr> <tr> <td><input type="checkbox"/> Enable Daylight Saving</td> <td><input type="checkbox"/></td> </tr> <tr> <td>Start Date</td> <td>First Sunday of January (2006-01-01) at 0 o'clock</td> </tr> <tr> <td>End Date</td> <td>First Sunday of January (2006-01-01) at 0 o'clock</td> </tr> </table>						Current Time	20:11:48 GMT	Current Date	2006-02-13	<input checked="" type="radio"/> Manual	<input type="radio"/> Get from Time Server	New Time (hh:mm:ss)	20 : 11 : 21	New Date (yyyy-mm-dd)	2006 - 2 - 13	Time Protocol NTP (RFC-1305) Time Server Address* de.pool.ntp.org <input type="button" value="Synchronize Now"/>		<small>* Optional. There is a pre-defined NTP time server list.</small>		Time Zone	(GMT+01:00) Berlin, Stockholm, Rome, Bern, Brussels, Vienna	<input type="checkbox"/> Enable Daylight Saving	<input type="checkbox"/>	Start Date	First Sunday of January (2006-01-01) at 0 o'clock	End Date	First Sunday of January (2006-01-01) at 0 o'clock
Current Time	20:11:48 GMT																										
Current Date	2006-02-13																										
<input checked="" type="radio"/> Manual	<input type="radio"/> Get from Time Server																										
New Time (hh:mm:ss)	20 : 11 : 21																										
New Date (yyyy-mm-dd)	2006 - 2 - 13																										
Time Protocol NTP (RFC-1305) Time Server Address* de.pool.ntp.org <input type="button" value="Synchronize Now"/>																											
<small>* Optional. There is a pre-defined NTP time server list.</small>																											
Time Zone	(GMT+01:00) Berlin, Stockholm, Rome, Bern, Brussels, Vienna																										
<input type="checkbox"/> Enable Daylight Saving	<input type="checkbox"/>																										
Start Date	First Sunday of January (2006-01-01) at 0 o'clock																										
End Date	First Sunday of January (2006-01-01) at 0 o'clock																										
<input type="button" value="Apply"/> <input type="button" value="Reset"/>																											

Der Router erwartet in der Standardkonfiguration ein von der Zertifizierungsstelle "RSA Data Security" signiertes Zertifikat. Um mit dem Intranator auch ohne ein solches Zertifikat kommunizieren zu können, muss diese Einstellung geändert werden.

Öffnen Sie das Menü Security > Certificates, Reiter Trusted CAs und löschen dort die voreingestellte Zertifizierungsstelle.

CERTIFICATES

#	Name	Subject	Issuer	Valid From	Valid To	CRL Issuer	Modify
1	VeriSign.cer	OU=Secure Server Certification Authority, O=RSA Data Security, Inc., C=US	OU=Secure Server Certification Authority, O=RSA Data Security, Inc., C=US	1994 Nov 9th, 00:00:00 GMT	2010 Jan 7th, 23:59:59 GMT	No	

50.3. Installieren des Intranator-Zertifikats

Als nächstes muss der Router den Intranator als vertrauenswürdig erkennen. Sie können das Intranator-Zertifikat auf dem Intranator unter System > Schlüssel > Eigene Schlüssel als .pem-Datei exportieren.

Öffnen Sie auf dem Router das Menü Security > Certificates und wechseln auf den Reiter "Trusted Remote Hosts". Klicken Sie auf Import und importieren das Zertifikat des Intranators.

CERTIFICATES

#	Name	Subject	Valid From	Valid To	Modify
1	intranator_vpn_cert	CN=intranator-vpn	2007 Sep 28th, 15:02:54 GMT	2012 Sep 26th, 15:02:54 GMT	

50.4. Erzeugen und Installieren des Router-Zertifikats

Nun muss für den Router ein Zertifikat erzeugt werden. Öffnen Sie auf dem Router das Menü Security > Certificates und wechseln auf den Reiter My Certificates. Klicken Sie auf Create, um einen neuen Schlüssel zu erzeugen.

Geben Sie dem Zertifikat einen Namen, unter dem es auf dem Router geführt wird. Der Common Name muss auf E-Mail umgestellt werden. Tragen Sie hier eine von allen anderen VPN-Schlüsseln unterschiedliche E-Mail-Adresse ein. Für ein gutes Sicherheitsniveau sollten Sie eine Schlüssellänge von 2048 Bit wählen. Als Enrollment Options verwenden Sie Create a self-signed certificate.

CERTIFICATES - MY CERTIFICATE - CREATE

Certificate Name: Zywall_VPN_Cert

Subject Information

Common Name:
 Host IP Address
 Host Domain Name
 E-Mail zywall@meine-firma.de
Organizational Unit
Organization
Country

Key Length: 2048 bits

Enrollment Options

Create a self-signed certificate
 Create a certification request and save it locally for later manual enrollment
 Create a certification request and enroll for a certificate immediately online

Enrollment Protocol: Simple Certificate Enrollment Protocol (SCEP)

CA Server Address:

CA Certificate: VeriSign.cer (See [Trusted CAs](#))

Request Authentication: Key

Buttons: Apply, Cancel

Nach Erstellung des Zertifikats erscheint wieder die Übersichtsseite. Wechseln Sie in die Detailansicht des neuen Zertifikats. Kopieren Sie den Text aus dem Feld Certificate in PEM (Base-64) Encoded Format in die Zwischenablage.

```
-----BEGIN CERTIFICATE-----
MIIDdCCALygAwIBAgIEQ/Do1DANBgkqhkiG9w0BAQUFADBaMRAwDgYDVQQGEwdH
ZXJtYWN5MRUwEwYDVQQKEwxJbnRyYTJuZQgQCxFTATBgvNVAstDEF1c3N1bnN0
ZWxsZTEYMBGA1UEAwwPen13YNxSGZpcm1hLmR1MB4XDA2MDIxMjIwMTUxNlOx
DTASMDIxMjIwMTUxNlOwWjEQMA4GA1UEBhMHR2VybNfueTEVMBNGA1UEChMMSw50
cmEybmV0IEFHHRUwEwYDVQQLExxBdXlzzW5zdGVsbGUxDwBgvNBAMHD3p5d2F5
bEMaXjtY55kZTCAS1wDQYJKoZIhvcNAQEBBQADggEPADCCAQcggEBAMzC5Plz
zSSU/sL1A00KrZXNiIIMbr+AcGiV1jyBRu/sKzO2vzDK2ScISkpbfeykmEzELM
Gab8bEn2TOH9lo02GEiZeikYYVfr45F9xNTXcnLSw41BGUYmzpE/p5LV10CVf0Fl
MBF95RrJPZN+A2k/RDU1bdQ7s5448i180dLOBD2NEPOOrv1mPN/xng0dy8qAF9m0
RG7j4PqlITS9f1dhO2v1GL5bOD0Etfo/cloJPKGJLJj8uOoRUP69D+9LAm6G+m
```

Installieren Sie das Zertifikat auf dem Intranator im Menü System > Schlüssel > Fremde Schlüssel.

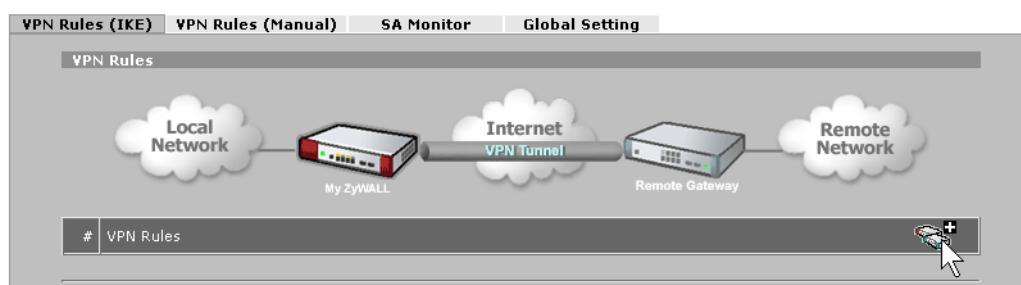
Nach dem Importvorgang wählen Sie im Feld IPSec ID die alleinstehende E-Mail-Adresse aus.

50.5. Konfiguration der VPN-Verbindung

Als nächstes muss die VPN-Verbindung konfiguriert werden. Auf dem Router ist die Konfiguration nach den beiden Phasen des Verbindungsaufbaus aufgeteilt.

Öffnen Sie das Menü Security > VPN, Reiter VPN Rules (IKE) und klicken auf das Add Gateway Policy Symbol.

VPN



Geben Sie der Verbindung einen Namen. Sollte der Intranator oder die Zywall hinter einem NAT-Router sein, müssen Sie die NAT Traversal Option aktivieren.

Unter Gateway Policy Information lassen Sie My ZyWall / My Address auf 0.0.0.0 stehen. Dies bedeutet, dass die Standard-Internet-IP der ZyWall verwendet wird.

Bei Primary Remote Gateway tragen Sie die externe IP (wenn vorhanden) oder den DNS-Namen des Intranators ein.

Bei Authentication Key aktivieren Sie Certificate und wählen das eben erstellte Zertifikat der Zywall aus. Den Peer ID Type stellen Sie auf Any.

Extended Authentication bleibt deaktiviert. Unter IKE Proposal stellen Sie den Negotiation Mode auf Main. Encryption Algorithm, Authentication Algorithm und Key Group (Entspricht Diffie Hellman Gruppe auf dem Intranator) müssen zu dem im Intranator gewählten Ver-

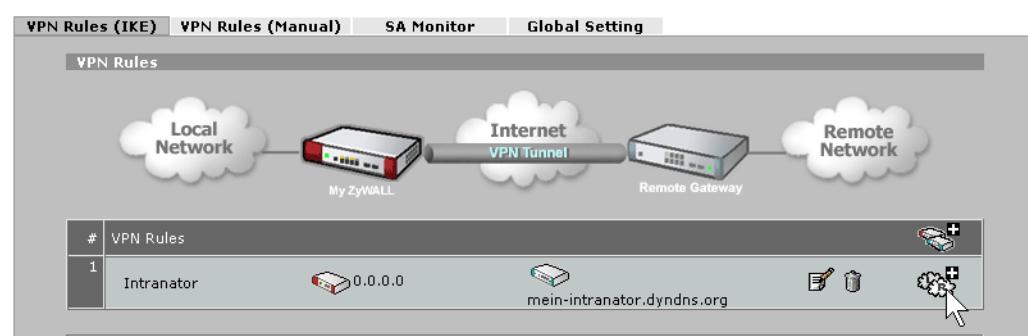
schlüsselungsprofil passen. Die Werte AES, SHA1 und DH2 sind mit dem Standardverschlüsselungsprofil des Intranators kompatibel.

VPN - GATEWAY POLICY - EDIT

Property																
Name: <input type="text" value="Intranator"/>																
<input checked="" type="checkbox"/> NAT Traversal																
Gateway Policy Information																
<table border="0"> <tr> <td></td> <td>My ZyWALL</td> </tr> <tr> <td><input checked="" type="radio"/> My Address</td> <td><input type="text" value="0.0.0"/> (Domain Name or IP Address)</td> </tr> <tr> <td><input type="radio"/> My Domain Name</td> <td><input type="text" value="None (See DDNS)"/></td> </tr> <tr> <td></td> <td>Primary Remote Gateway <input type="text" value="mein-intranator.dyndns.org"/> (Domain Name or IP Address)</td> </tr> <tr> <td><input type="checkbox"/> Enable IPSec High Availability</td> <td></td> </tr> <tr> <td></td> <td><input type="text"/> (Domain Name or IP Address)</td> </tr> <tr> <td><input type="checkbox"/> Fail back to Primary Remote Gateway when possible</td> <td><input type="text" value="28800"/> (180~86400 seconds)</td> </tr> <tr> <td colspan="2">*Fail Back Check Interval: The time interval for checking availability of Primary Remote Gateway. IPSec SA life time will be superseded by this value when it is larger than this value.</td> </tr> </table>		My ZyWALL	<input checked="" type="radio"/> My Address	<input type="text" value="0.0.0"/> (Domain Name or IP Address)	<input type="radio"/> My Domain Name	<input type="text" value="None (See DDNS)"/>		Primary Remote Gateway <input type="text" value="mein-intranator.dyndns.org"/> (Domain Name or IP Address)	<input type="checkbox"/> Enable IPSec High Availability			<input type="text"/> (Domain Name or IP Address)	<input type="checkbox"/> Fail back to Primary Remote Gateway when possible	<input type="text" value="28800"/> (180~86400 seconds)	*Fail Back Check Interval: The time interval for checking availability of Primary Remote Gateway. IPSec SA life time will be superseded by this value when it is larger than this value.	
	My ZyWALL															
<input checked="" type="radio"/> My Address	<input type="text" value="0.0.0"/> (Domain Name or IP Address)															
<input type="radio"/> My Domain Name	<input type="text" value="None (See DDNS)"/>															
	Primary Remote Gateway <input type="text" value="mein-intranator.dyndns.org"/> (Domain Name or IP Address)															
<input type="checkbox"/> Enable IPSec High Availability																
	<input type="text"/> (Domain Name or IP Address)															
<input type="checkbox"/> Fail back to Primary Remote Gateway when possible	<input type="text" value="28800"/> (180~86400 seconds)															
*Fail Back Check Interval: The time interval for checking availability of Primary Remote Gateway. IPSec SA life time will be superseded by this value when it is larger than this value.																
Authentication Key																
<table border="0"> <tr> <td><input type="radio"/> Pre-Shared Key</td> <td><input type="text"/></td> </tr> <tr> <td><input checked="" type="radio"/> Certificate</td> <td><input type="text" value="Zywall_VPN_Cert"/> (See My Certificates)</td> </tr> <tr> <td>Local ID Type</td> <td>E-mail</td> </tr> <tr> <td>Content</td> <td><input type="text" value="zywall@meine-firma.de"/></td> </tr> <tr> <td>Peer ID Type</td> <td><input type="text" value="Any"/></td> </tr> <tr> <td>Content</td> <td><input type="text"/></td> </tr> </table>	<input type="radio"/> Pre-Shared Key	<input type="text"/>	<input checked="" type="radio"/> Certificate	<input type="text" value="Zywall_VPN_Cert"/> (See My Certificates)	Local ID Type	E-mail	Content	<input type="text" value="zywall@meine-firma.de"/>	Peer ID Type	<input type="text" value="Any"/>	Content	<input type="text"/>				
<input type="radio"/> Pre-Shared Key	<input type="text"/>															
<input checked="" type="radio"/> Certificate	<input type="text" value="Zywall_VPN_Cert"/> (See My Certificates)															
Local ID Type	E-mail															
Content	<input type="text" value="zywall@meine-firma.de"/>															
Peer ID Type	<input type="text" value="Any"/>															
Content	<input type="text"/>															
Extended Authentication																
<table border="0"> <tr> <td><input type="checkbox"/> Enable Extended Authentication</td> <td>(Search Local User first then RADIUS)</td> </tr> <tr> <td><input type="radio"/> Server Mode</td> <td></td> </tr> <tr> <td><input checked="" type="radio"/> Client Mode</td> <td></td> </tr> <tr> <td>User Name</td> <td><input type="text"/></td> </tr> <tr> <td>Password</td> <td><input type="text"/></td> </tr> </table>	<input type="checkbox"/> Enable Extended Authentication	(Search Local User first then RADIUS)	<input type="radio"/> Server Mode		<input checked="" type="radio"/> Client Mode		User Name	<input type="text"/>	Password	<input type="text"/>						
<input type="checkbox"/> Enable Extended Authentication	(Search Local User first then RADIUS)															
<input type="radio"/> Server Mode																
<input checked="" type="radio"/> Client Mode																
User Name	<input type="text"/>															
Password	<input type="text"/>															
IKE Proposal																
<table border="0"> <tr> <td>Negotiation Mode</td> <td><input type="text" value="Main"/></td> </tr> <tr> <td>Encryption Algorithm</td> <td><input type="text" value="AES"/></td> </tr> <tr> <td>Authentication Algorithm</td> <td><input type="text" value="SHA1"/></td> </tr> <tr> <td>SA Life Time (Seconds)</td> <td><input type="text" value="28800"/></td> </tr> <tr> <td>Key Group</td> <td><input type="text" value="DH2"/></td> </tr> <tr> <td><input type="checkbox"/> Enable Multiple Proposals</td> <td></td> </tr> </table>	Negotiation Mode	<input type="text" value="Main"/>	Encryption Algorithm	<input type="text" value="AES"/>	Authentication Algorithm	<input type="text" value="SHA1"/>	SA Life Time (Seconds)	<input type="text" value="28800"/>	Key Group	<input type="text" value="DH2"/>	<input type="checkbox"/> Enable Multiple Proposals					
Negotiation Mode	<input type="text" value="Main"/>															
Encryption Algorithm	<input type="text" value="AES"/>															
Authentication Algorithm	<input type="text" value="SHA1"/>															
SA Life Time (Seconds)	<input type="text" value="28800"/>															
Key Group	<input type="text" value="DH2"/>															
<input type="checkbox"/> Enable Multiple Proposals																
Associated Network Policies																
<table border="1"> <thead> <tr> <th>#</th> <th>Name</th> <th>Local Network</th> <th>Remote Network</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	#	Name	Local Network	Remote Network												
#	Name	Local Network	Remote Network													
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>																

Nach Erstellung der Verbindung erscheint wieder die Übersichtsseite. Klicken Sie auf das Add Network Policy Symbol, um die zweite Phase der Verbindung zu konfigurieren.

VPN



Aktivieren Sie die Active Checkbox und geben der Policy einen Namen. Soll die Verbindung ständig aufgebaut bleiben, so aktivieren Sie zusätzlich Nailed-Up.

Im Block Local Network wird die lokale Seite des VPN-Tunnels konfiguriert. Stellen Sie den Address Type auf Subnet Address und stellen IP und Netzmase des lokalen Netzes an der Zywall ein.

Im Block Remote Network wird mit Typ Subnet Address das Netz am Intranator eingestellt.

Im Block IPSec Proposal werden die Kapselungs- und Verschlüsselungsverfahren konfiguriert. Diese müssen zur Konfiguration der Verbindung auf dem Intranator passen. Wählen Sie bei Encapsulation Mode die Option Tunnel. Zur Standardkonfiguration des Intranators passen die Werte ESP, AES, SHA1 und DH2.

VPN - NETWORK POLICY - EDIT

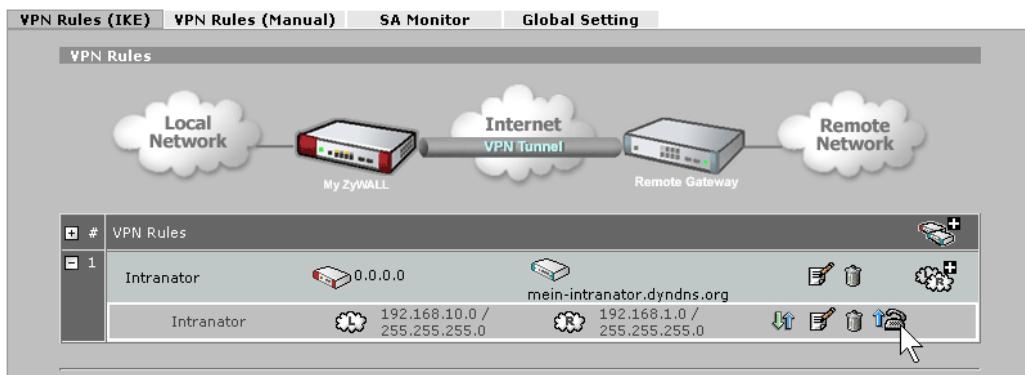
The screenshot shows the 'VPN - NETWORK POLICY - EDIT' configuration window with several tabs:

- Property:**
 - Active
 - Name: Intranator
 - Protocol: 0
 - Nailed-Up
 - Allow NetBIOS Traffic Through IPSec Tunnel
 - Check IPSec Tunnel Connectivity: Log, Ping this Address: 0.0.0.0
- Gateway Policy Information:**
 - Gateway Policy: Intranator
- Virtual Address Mapping Rule:**
 - Active
 - Virtual Address Mapping Rule: Port Forwarding Rules, One-to-One
 - Type: Private Starting IP Address: 0.0.0.0, Private Ending IP Address: 0.0.0.0
 - Virtual Starting IP Address: 0.0.0.0, Virtual Ending IP Address: 0.0.0.0
- Local Network:**
 - Address Type: Subnet Address
 - Starting IP Address: 192.168.10.0, Ending IP Address / Subnet Mask: 255.255.255.0
 - Local Port: Start 0, End 0
- Remote Network:**
 - Address Type: Subnet Address
 - Starting IP Address: 192.168.1.0, Ending IP Address / Subnet Mask: 255.255.255.0
 - Remote Port: Start 0, End 0
- IPSec Proposal:**
 - Encapsulation Mode: Tunnel
 - Active Protocol: ESP
 - Encryption Algorithm: AES
 - Authentication Algorithm: SHA1
 - SA Life Time (Seconds): 28800
 - Perfect Forward Secrecy (PFS): DH2
 - Enable Replay Detection
 - Enable Multiple Proposals

At the bottom are 'Apply' and 'Cancel' buttons.

Jetzt ist die VPN-Verbindung fertig konfiguriert. In der Verbindungsübersicht erscheint nun ein kleines Telefonsymbol. Klicken Sie auf dieses, um die Verbindung aufzubauen.

VPN



50.6. Intranator

Auf dem Intranator muss die Verbindung auch entsprechend konfiguriert werden. Für VPN-Router wird dies im 49. Kapitel, „Anbinden von kompletten Netzen“ beschrieben.

51. Kapitel - VPN mit ZyXEL ZyWALL USG

51.1. Überblick

Diese Anleitung funktioniert für die ZyXEL ZyWALL USG-Linie. Diese unterstützen VPN mit X.509-Zertifikaten und nicht nur Authentifizierung per Pre-Shared Key. Dadurch lassen sich die unter Abschnitt 38.6, „Einschränkungen“ beschriebenen Einschränkungen umgehen.

Der Router unterstützt selbstsignierte Zertifikate und kann diese auch selbst erstellen. Die Einrichtungszeit wird dadurch deutlich verkürzt.

Selbstverständlich unterstützt der Intranator auch Verbindungen mit anderen Routern. Dieser Router wird jedoch genauer beschrieben, da er im Vergleich zu anderen Routern mit Unterstützung von X.509-Zertifikaten relativ preisgünstig und gut verfügbar ist.

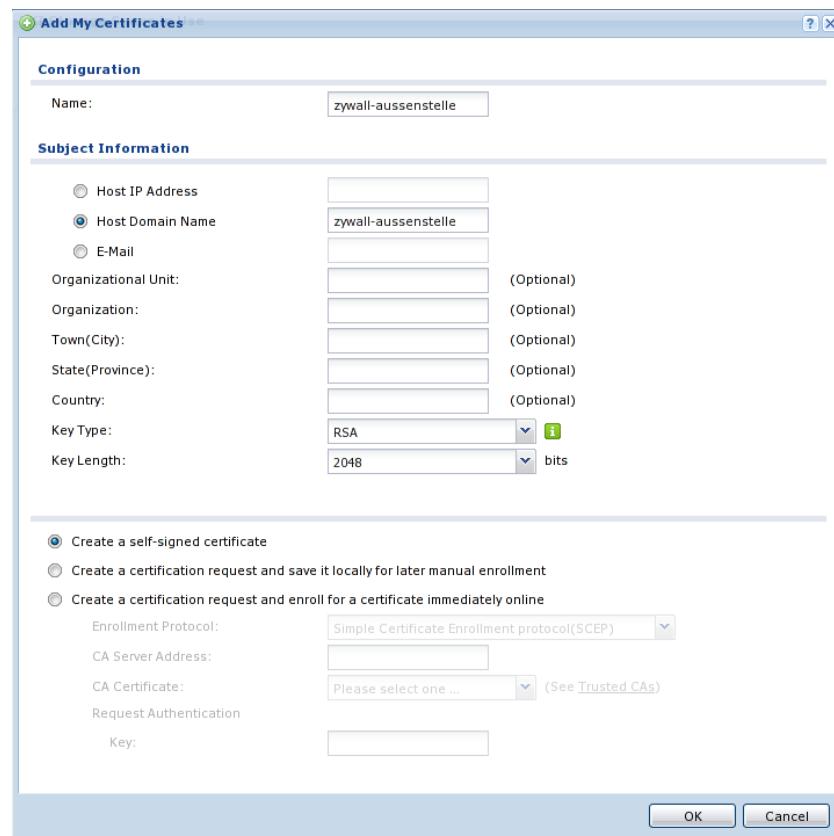
51.2. Vorbereitung

Der Router überprüft bei der Authentifizierung auch den Gültigkeitszeitraum des Zertifikats. Daher muss die Systemzeit immer korrekt sein, wenn eine VPN-Verbindung aufgebaut werden soll.

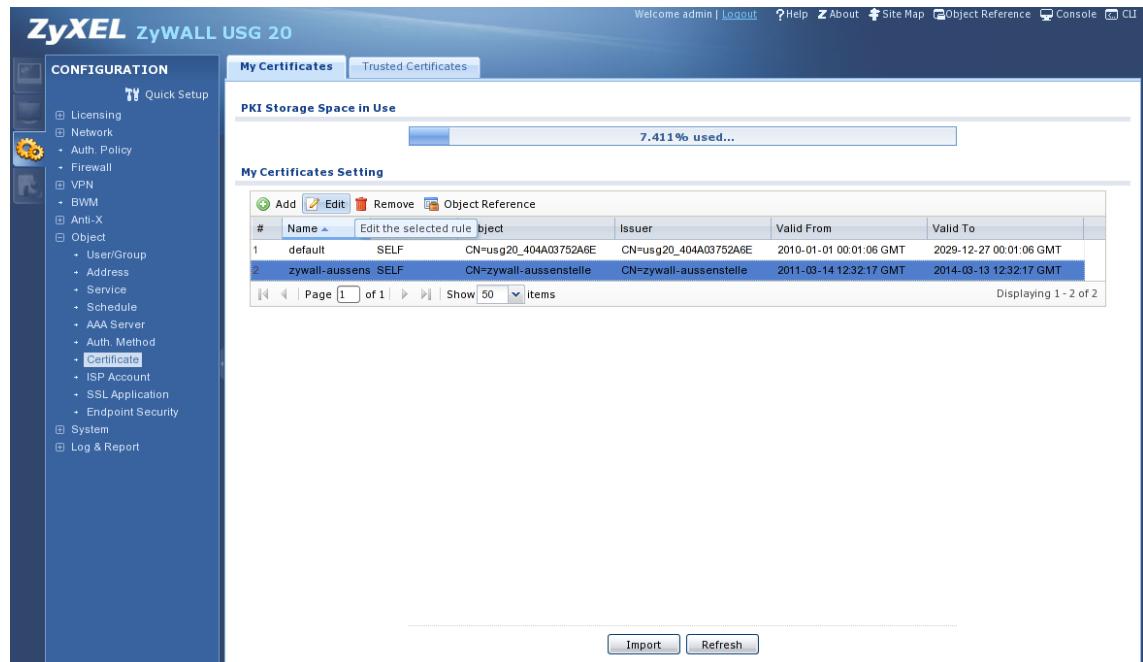
Der Router aktualisiert seine Zeit über das NTP-Protokoll. Dies kann im Menü Configuration > System > Date/Time überprüft und konfiguriert werden. Öffnen Sie das Menü und stellen Sie Zeitzone und Sommerzeitumstellung (Daylight Saving) korrekt ein. Testen Sie über den Knopf Sync Now ob die Synchronisation per NTP wirklich funktioniert.

51.3. Zertifikate

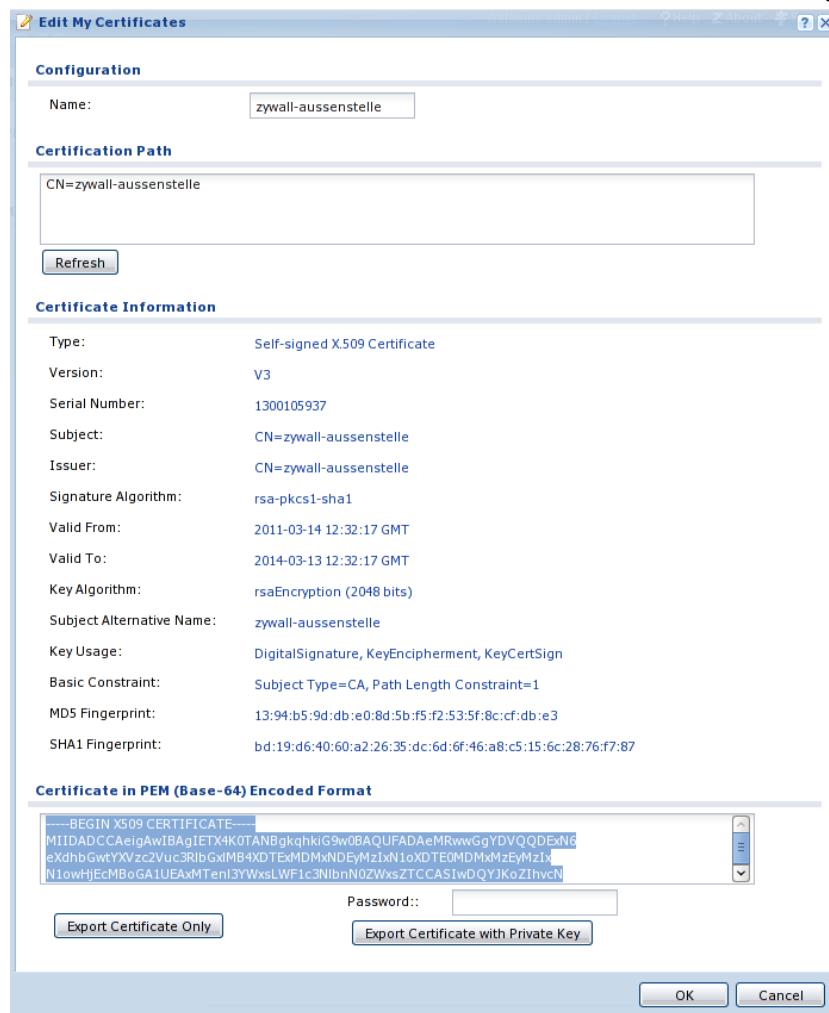
1. Öffnen Sie das Menü Configuration > Object > Certificates. Über den Menüpunkt Add können Sie ein neues Zertifikat anlegen.
2. Geben Sie dem neuen Zertifikat einen Namen, tragen einen Host Domain Name für die ZyWALL ein (muss nicht real existieren) und legen ein self-signed Certificate mit 2048 Bit RSA an.



3. Das Erstellen des Zertifikats dauert bis zu 5 Minuten.
4. Öffnen Sie die Detail-Daten des Zertifikats über die Option Edit.



5. Übernehmen Sie das Zertifikat im PEM-Format in die Zwischenablage.



6. Importieren Sie das Zertifikat aus der Zwischenablage in den Intranator über das Menü System > Schlüssel > Fremde Schlüssel.

- Wählen Sie unter IPSec ID den puren DNS-Hostnamen, nicht den Inhaber des Zertifikats ("/CN=" etc.).

- Exportieren Sie das eigene Zertifikat des Intranators als .pem-Datei (Menü System > Schlüssel > Eigene Schlüssel, Reiter Daten).
- Importieren Sie das Zertifikat des Intranators in die ZyWALL, Menü Configuration > Object > Certificate, Reiter Trusted Certificates. Klicken Sie unten auf Import.

10. Wählen Sie die Datei aus, in die Sie das Zertifikat des Intranators gespeichert haben.



11. Das Zertifikat des Intranators wird nun als Trusted Certificate angezeigt.

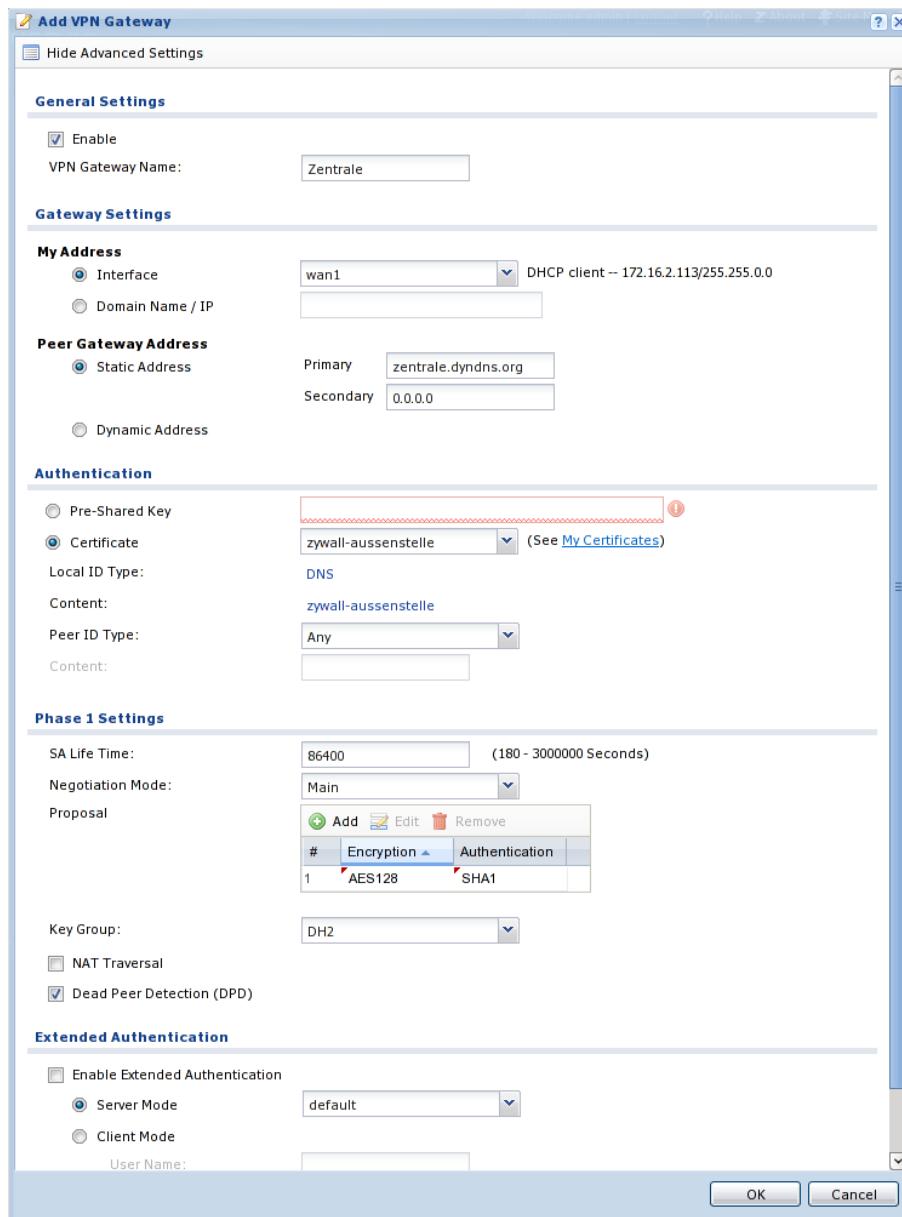
#	Name	Subject	Issuer	Valid From	Valid To
1	intranator_zentrale	CN=intranator-zentrale	CN=intranator-zentrale	2011-03-14 12:40:48 GMT	2016-03-12 12:40:48 GMT

51.4. Verbindung

51.4.1. IKE / Phase 1

- Öffnen Sie das Menü Configuration > VPN > IPSec VPN, Reiter VPN Gateway. Legen Sie mit Add eine neue IKE-Verbindung zu einer Gegenstelle an.
- Klicken Sie auf Show Advanced Settings, um alle nötigen Felder angezeigt zu bekommen.
- Geben Sie die IP oder den DNS-Namen des Intranators als Peer Gateway Address ein. Auch wenn der Intranator eine dynamische IP mit DynDNS verwendet, müssen Sie Static Address wählen.
- Stellen Sie die Authentifizierung auf Zertifikate und wählen das vorhin erstellte Zertifikat für die ZyWALL aus.

5. Wählen Sie AES128 und SHA1 als Proposal aus, die passende Key Group ist DH2.
6. Sollte sich die Zywall oder der Intranator hinter einem NAT-Router befinden, müssen Sie die Option NAT Traversal aktivieren.

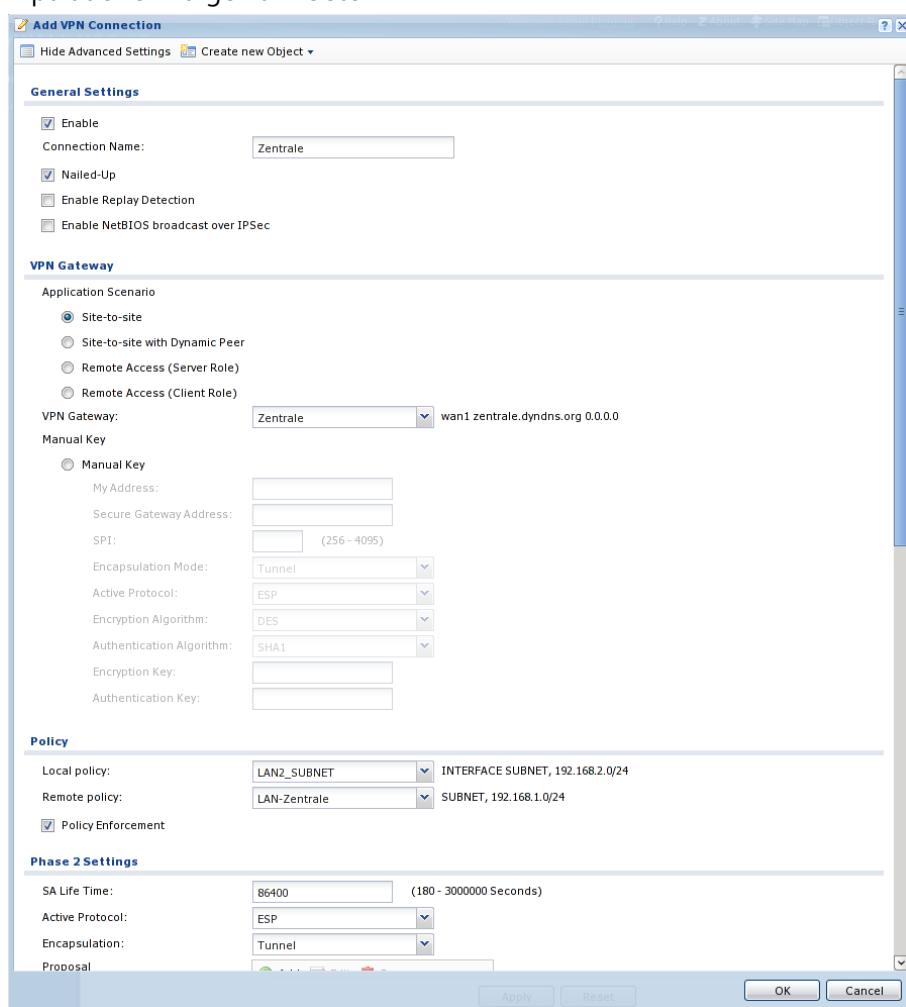


51.4.2. IPSec / Phase 2

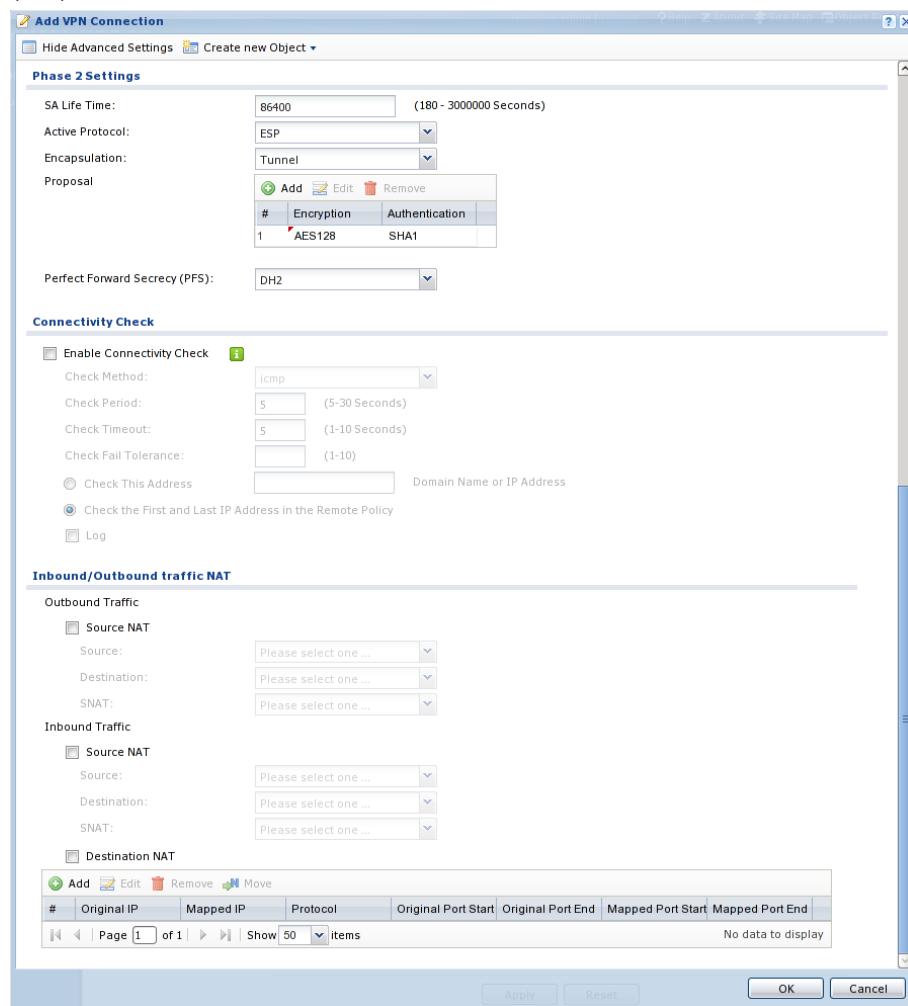
1. Öffnen Sie das Menü Configuration > VPN > IPSec VPN, Reiter VPN Connection. Legen Sie mit Add eine neue IPSec-Verbindung an.
2. Legen Sie ein Netzwerkobjekt für das Netz der Gegenstelle an. Verwenden Sie dazu das Menü Create new Object > Address. Verwenden Sie als Typ SUBNET und tragen die Netzadresse und Netzmaske ein.



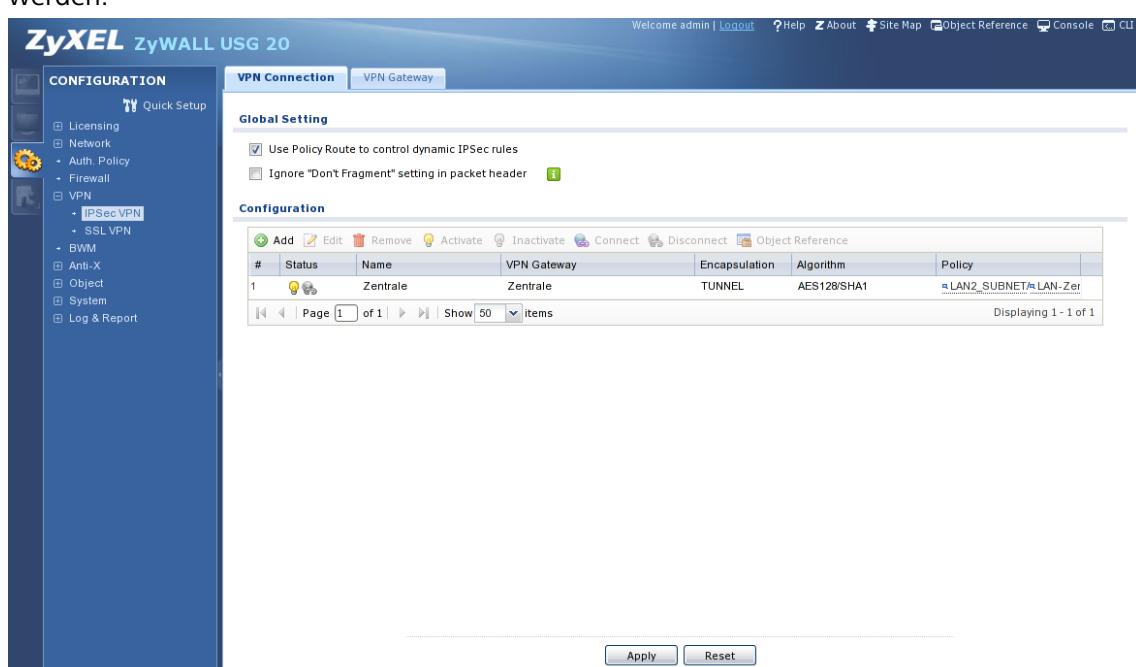
3. Klicken Sie auf Show Advanced Settings, um alle nötigen Felder angezeigt zu bekommen.
4. Stellen Sie die Verbindung auf Nailed Up, damit die ZyWALL die Verbindung von sich aus offen hält.
5. Wählen Sie Site-to-site und wählen als Gateway die eben angelegte IKE-Verbindung zum Intranator.
6. Wählen Sie als Local policy das zu verbindende Netz hinter der Zywall. Wählen Sie als Remote Policy das eben angelegte Netzwerkobjekt mit dem Netz des Intranators.
7. Aktivieren Sie Policy Enforcement, um die Sicherheit der Verbindung gegen Netzmanipulationen zu gewährleisten.



- Wählen Sie als Proposal AES128 und SHA1. Stellen Sie die Perfect Forward Secrecy (PFS) auf DH2.



Die Verbindung ist nun fertig konfiguriert und sollte im Hintergrund bereits aufgebaut werden.



51.5. Intranator

Auf dem Intranator muss die Verbindung auch entsprechend konfiguriert werden. Für VPN-Router wird dies im 49. Kapitel, „Anbinden von kompletten Netzen“ beschrieben.

51.6. Logs

Die ZyWALL protokolliert alle VPN-Ereignisse. Diese Protokolle können im Menü Monitor > Log eingesehen werden. Wählen Sie für Ereignisse aus Phase 1 als Anzeigefilter IKE, für Phase 2 IPSec.

#	Time	Prior	Category	Message	Source	Destination	Note
3	2011-03-14 14:17:58	info	IKE	Recv [HASH][DEL]	172.16.1.147.500	172.16.2.113.500	IKE_LOG
4	2011-03-14 14:17:58	info	IKE	The cookie pair is : 0xeb1b43faef447338 / 0x932d547e21aa6cd3	172.16.1.147.500	172.16.2.113.500	IKE_LOG
5	2011-03-14 14:17:58	info	IKE	Send [HASH][DEL]	172.16.2.113.500	172.16.1.147.500	IKE_LOG
6	2011-03-14 14:17:58	info	IKE	Tunnel [Zentrale.Zentrale.0xc4366098] is disconnected	172.16.2.113.500	172.16.1.147.500	IKE_LOG
7	2011-03-14 14:17:58	info	IKE	The cookie pair is : 0x932d547e21aa6cd3 / 0xeb1b43faef447338 [count=2]	172.16.2.113.500	172.16.1.147.500	IKE_LOG
9	2011-03-14 14:17:29	info	IKE	Tunnel [Zentrale.Zentrale.0xc4366098] rekey successfully	172.16.2.113.500	172.16.1.147.500	IKE_LOG
10	2011-03-14 14:17:29	info	IKE	[ESP aes-cbq]mac-sha1-96[SPI 0xcc409b0f]0xc4366098[PFS:DH2][Lifetime 3620]	172.16.2.113.500	172.16.1.147.500	IKE_LOG
11	2011-03-14 14:17:29	info	IKE	[Responder:172.16.2.113][Initiator:172.16.1.147][Policy: ipv4(192.168.2.0-192.168.2.255)-ipv6(192.168.2.0-192.168.2.255)]	172.16.2.113.500	172.16.1.147.500	IKE_LOG
12	2011-03-14 14:17:29	info	IKE	Recv [HASH]	172.16.1.147.500	172.16.2.113.500	IKE_LOG
13	2011-03-14 14:17:29	info	IKE	Send [ID][CERT][SIG]	172.16.2.113.500	172.16.1.147.500	IKE_LOG
14	2011-03-14 14:17:26	info	IKE	Recv [ID][CERT][CR][SIG]	172.16.1.147.500	172.16.2.113.500	IKE_LOG
15	2011-03-14 14:17:26	info	IKE	Tunnel [Zentrale.Zentrale.0xcbc293ef] built successfully	172.16.2.113.500	172.16.1.147.500	IKE_LOG
16	2011-03-14 14:17:26	info	IKE	[ESP aes-cbq]mac-sha1-96[SPI 0xeb14562c]0xcbc293ef[PFS:DH2][Lifetime 86400]	172.16.2.113.500	172.16.1.147.500	IKE_LOG
17	2011-03-14 14:17:26	info	IKE	[Initiator:172.16.2.113][Responder:172.16.1.147][Policy: ipv4(192.168.2.0-192.168.2.255)-ipv6(192.168.2.0-192.168.2.255)]	172.16.2.113.500	172.16.1.147.500	IKE_LOG
18	2011-03-14 14:17:26	info	IKE	Send [HASH]	172.16.1.147.500	172.16.1.147.500	IKE_LOG
19	2011-03-14 14:17:26	info	IKE	Recv [HASH][SA][NONCE][KE][ID][ID] [count=2]	172.16.1.147.500	172.16.2.113.500	IKE_LOG
20	2011-03-14 14:17:26	info	IKE	Recv [KE][NONCE]	172.16.1.147.500	172.16.2.113.500	IKE_LOG
21	2011-03-14 14:17:26	info	IKE	Send [HASH][SA][NONCE][KE][ID][ID] [count=2]	172.16.2.113.500	172.16.1.147.500	IKE_LOG
22	2011-03-14 14:17:26	info	IKE	Phase 1 IKE SA process done [count=2]	172.16.2.113.500	172.16.1.147.500	IKE_LOG
23	2011-03-14 14:17:26	info	IKE	Recv [ID][CERT][SIG]	172.16.1.147.500	172.16.2.113.500	IKE_LOG
24	2011-03-14 14:17:26	info	IKE	Send [SA][VID][VID][VID][VID][VID]	172.16.2.113.500	172.16.1.147.500	IKE_LOG
25	2011-03-14 14:17:26	info	IKE	The cookie pair is : 0x932d547e21aa6cd3 / 0xeb1b43faef447338 [count=8]	172.16.2.113.500	172.16.1.147.500	IKE_LOG

52. Kapitel - VPN mit Lancom Routern

52.1. Überblick

VPN-fähige Router von Lancom können ab LCOS Version 6 Verbindungen mit Zertifikaten aufbauen und sind mit dem Intranator kompatibel. Diese Anleitung wurde für Version 8.84 erstellt. An der VPN-Konfiguration ändert sich aber in den meisten Versionen erfahrungsgemäß nicht viel.

52.2. Zertifikat für das Lancom-Gerät

1. Laden Sie vom Intranator unter "Information > Download" das "Programm zum Erzeugen von Zertifikaten" (makecert) herunter und entpacken Sie es in ein Verzeichnis auf Ihrem Rechner.
2. Lancom Router können keine eigenen Zertifikate erstellen. Dies übernimmt daher das Programm makecacert. Starten Sie die Batchdatei `makecacert.bat`

```
C:\makecert>makecacert
```

```
C:\makecert>openssl req -x509 -newkey rsa:2048 -days 730 -new -nodes -config
openssl.cnf -outform PEM -keyform PEM -keyout privatekey.pem -out newcert.cer
Using configuration from openssl.cnf
Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
.....+
.....+
writing new private key to 'privatekey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
```

3. Geben Sie jetzt die Daten des Routers ein. Für einige Felder gibt es einen Standardwert, der in eckigen Klammern angegeben ist. Wollen Sie diesen verwenden, so drücken Sie einfach nur Return. Verwenden Sie keine Umlaute und andere Sonderzeichen, da es sonst zu Problemen kommen kann. Der "Common Name" (oder "Rechnername" auf dem Intranator) muss eindeutig sein und darf nicht auf anderen Rechnern oder für eine CA wiederverwendet werden.



Tipp

Es empfiehlt sich, hier möglichst wenig Daten einzugeben (z.B. nur den Common Name), da diese bei der Konfiguration der Verbindung nochmals identisch eingegeben werden müssen.

```
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:lancom
Email Address []:

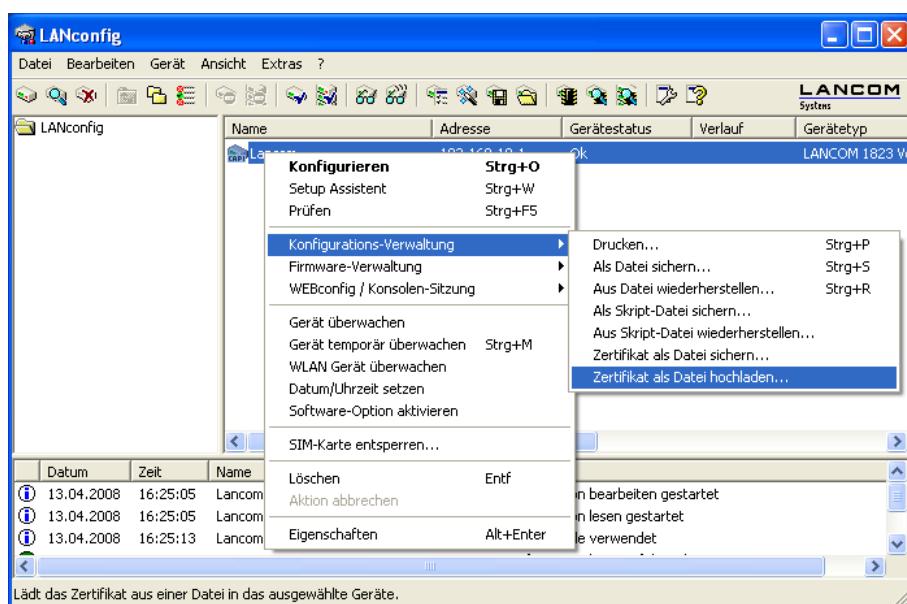
C:\makecert>openssl pkcs12 -export -in newcert.cer -inkey privatekey.pem
```

```
-out newcert.p12
Loading 'screen' into random state - done
```

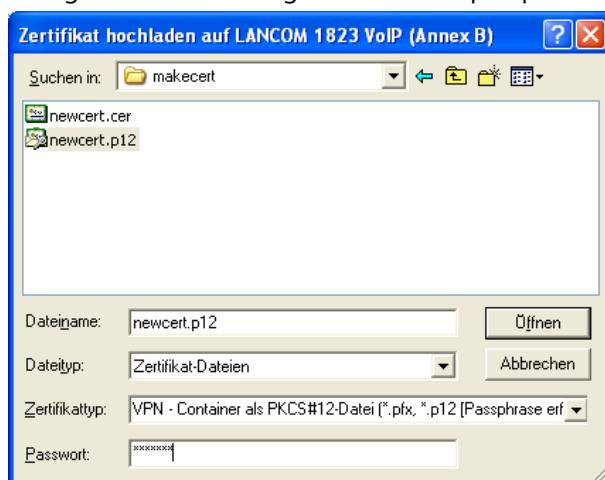
4. Wählen Sie ein Transportpasswort, mit dem die Schlüsseldatei auf dem Weg zum Router geschützt wird. Das Passwort muss mindestens 3 Zeichen lang sein.

```
Enter Export Password:
Verifying password - Enter Export Password:
C:\makecert>del privatekey.pem
```

5. Starten Sie das Programm LANconfig zur Konfiguration des Routers. Ihr Router muss von LANconfig erkannt werden.
6. Öffnen Sie das Kontextmenü Konfigurations-Verwaltung, Untermenü Zertifikat oder Datei hochladen.



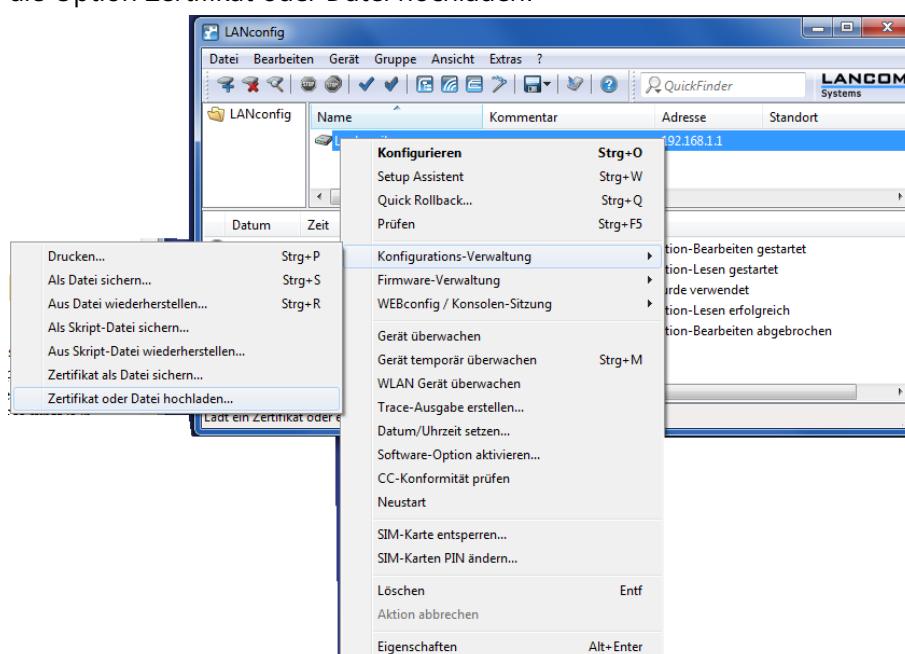
7. Wählen Sie die Datei `newcert.p12` aus, die Sie eben mit dem makecert-Programm erzeugt haben. Stellen Sie den Zertifikattyp auf VPN - Container als PKCS#12-Datei und geben das vorhin gewählte Transportpasswort ein.



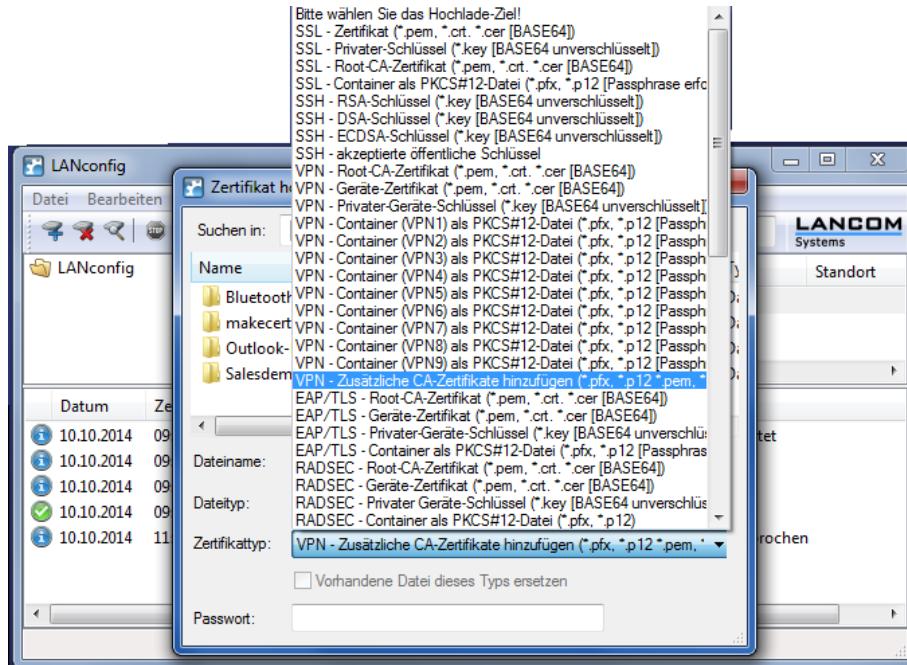
8. Öffnen Sie die Datei `newcert.cer` in einem Texteditor (z.B. write) und übernehmen den Inhalt in die Zwischenablage. Öffnen Sie im Intranator das Menü System > Schlüssel > Fremde Schlüssel und legen einen neuen an. Vergeben Sie einen Namen für den Schlüssel (z.B. den Namen des Routers) und fügen dann die Zertifikatsdaten aus der Zwischenablage in das Feld "Copy > Paste Schlüssel" ein.

52.3. Zertifikat für den Intranator

1. Der Lancom-Router erfordert eine besondere Konfiguration des Zertifikats auf dem Intranator. Seit den 8-er Versionen der LCOS-Firmware werden keine selbstsignierten Schlüssel mehr akzeptiert, sondern nur von einer eigenständigen CA signierte Zertifikate. Im folgenden wird gezeigt, wie ein solcher Schlüssel auf dem Intranator erzeugt und signiert wird.
2. Zunächst muss das Zertifikat für die CA erstellt werden: Öffnen Sie im Intranator das Menü System > Schlüssel > Eigene Schlüssel : Daten. Mit einem Klick auf den Menüpunkt "Neu" beginnen Sie die Schlüsselerstellung. Das Zertifikat wird allein zum Signieren der eigentlichen Verschlüsselungszertifikate verwendet, wir nennen es deshalb beispielsweise `intranator-ca` (einzutragen in den Feldern Name sowie Rechnername (CN)).
3. Dem Lancom-Router muss nun dieses CA-Zertifikat übermittelt werden. Dazu exportieren Sie es aus dem Intranator über die Option als .pem. Öffnen Sie dann in LANconfig das Kontextmenü Konfigurations-Verwaltung des entsprechenden Geräts. Wählen Sie hier die Option Zertifikat oder Datei hochladen.



Wählen Sie die soeben erzeugte .pem-Datei aus und laden Sie sie als Zertifikattyp VPN - Zusätzliche CA-Zertifikate hinzufügen hoch.

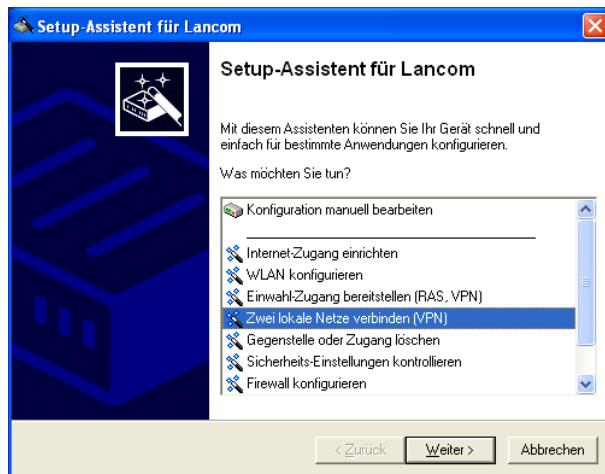


4. Wenden Sie sich nun wieder dem Intranator zu, unter dem Menü System > Schlüssel > Eigene Schlüssel : Daten. Legen Sie einen weiteren Schlüssel als Grundlage für das VPN-Zertifikat an. Bei der Erstellung ist zu beachten, dass der Wert des Feldes Rechnername (CN) (also der Common Name eines SSL-Zertifikats) wortwörtlich später im Lancom-Router eingetragen wird, ohne Toleranz für Abweichungen. Stellen Sie deshalb sicher, dass Ihnen an dieser Stelle kein Tippfehler unterläuft!
5. Navigieren Sie nun im Intranator zum Menü System > Schlüssel > Eigene Schlüssel : CA und wählen Sie hier den soeben erstellten VPN-Schlüssel des Intranators aus. Im Abschnitt Schlüssel mit einem anderen Schlüssel signieren wählen Sie den in den vorangehenden Schritten erzeugten CA-Schlüssel aus (**intranator-ca**) und klicken anschließend auf Signieren.

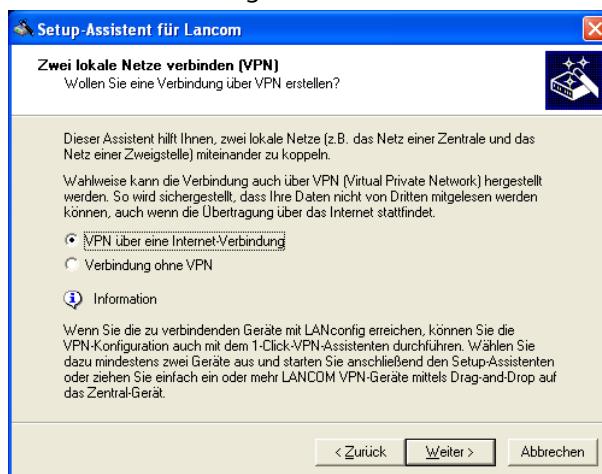
Überprüfen Sie nun unter System > Schlüssel > Eigene Schlüssel : Daten den Wert Aussteller/CA. In diesem sollte die bei der Erstellung des CA-Zertifikats angegebenen Daten zusammengefaßt sein. (Wenn Sie obigem Beispiel gefolgt sind, enthält dieses Feld die Zeichenkette **CN=intranator-ca**.) Der Schlüssel kann nun zum Aufbau einer VPN-Verbindung eingesetzt werden.

52.4. Verbindung

1. Starten Sie den Setup-Assistenten und wählen Zwei lokale Netze verbinden (VPN).



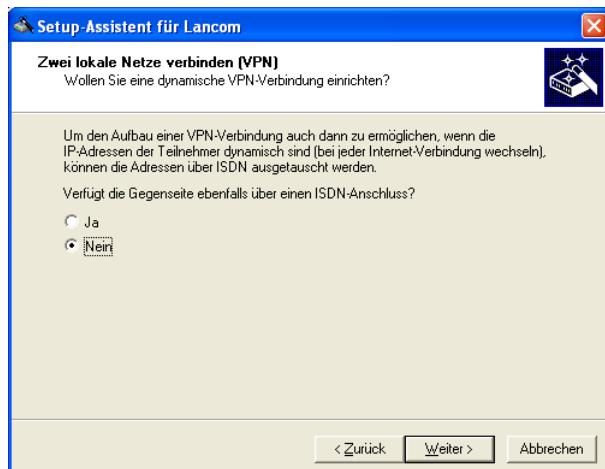
2. Die VPN-Verbindung soll über eine Internet-Verbindung laufen.



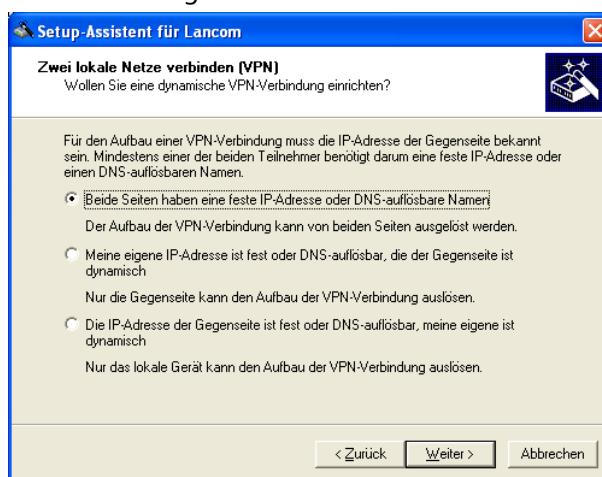
3. Der VPN-Typ muß bei IPSec belassen werden.



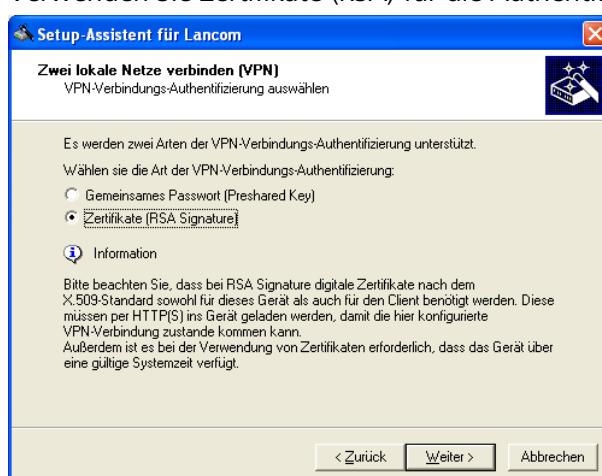
4. Verwenden Sie keinen ISDN-Anschluss, denn dafür wird ein Lancom-eigenes Protokoll verwendet.



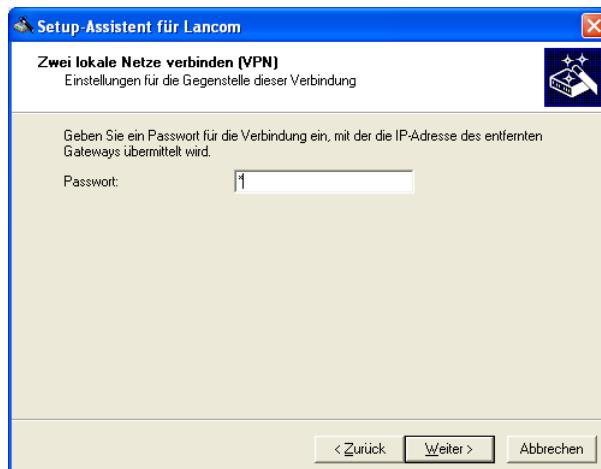
5. Die Verbindung wird über feste IP-Adressen oder DynDNS-Namen hergestellt.



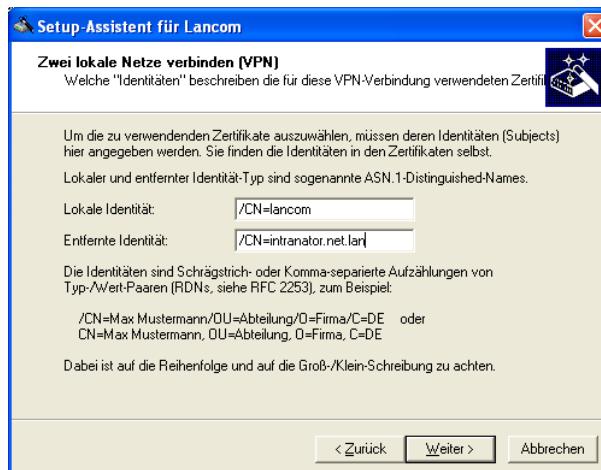
6. Geben Sie der eigenen Seite sowie der Gegenseite einen Namen. Der Name ist für die Verbindung nicht relevant, er muss nur eindeutig sein.
7. Verwenden Sie Zertifikate (RSA) für die Authentifizierung der Verbindung.



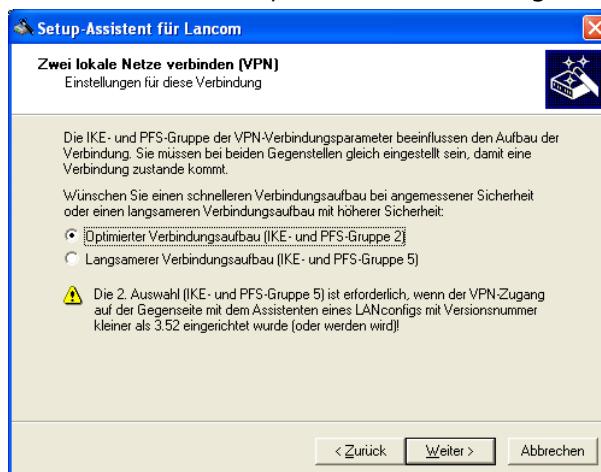
8. Tragen Sie ein beliebiges Passwort ein. Dieses Passwort wird nicht benötigt, es würde nur für das hier nicht verwendete Lancom-eigene ISDN-Protokoll gebraucht werden.



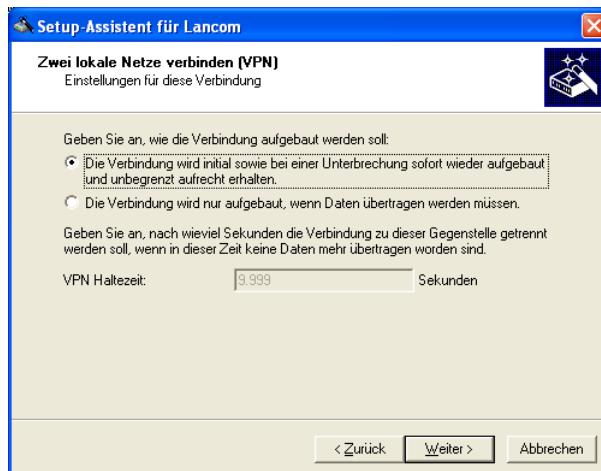
9. Geben Sie die Identität (=Inhaber) der Zertifikate für die eigene (Lancom) und entfernte (Intranator) Seite ein. Die Werte für die Distinguished Names finden Sie z.B. auf dem Intranator im Menü System > Schlüssel > Eigene Schlüssel bzw. Fremde Schlüssel, jeweils im Feld Inhaber (Subject). Die einzelnen Datenblöcke müssen in der umgekehrten Reihenfolge wie im Intranator angezeigt eingegeben werden.



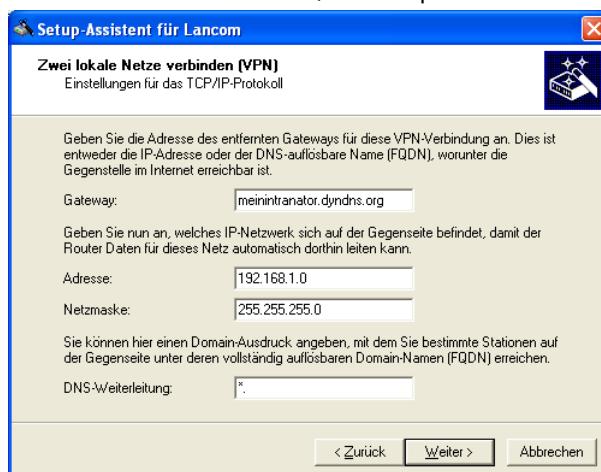
10. Verwenden Sie den optimierten Verbindungsaufbau (IKE- und PFS-Gruppe 2).



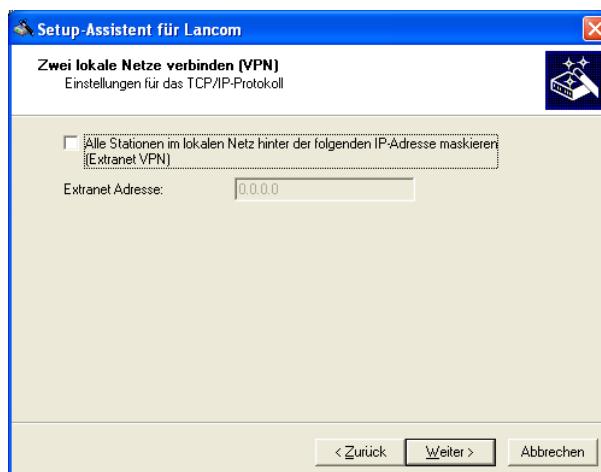
11. Sie können die Verbindung entweder ständig aufgebaut lassen, oder nur bei Bedarf starten. Stellen Sie am besten den Intranator auch entsprechend ein.



- 12 Tragen Sie als Gateway die feste IP oder den Dyndns-Namen des Intranators ein (im Beispiel `meinintranator.dyndns.org`). Geben Sie dann IP und Netzmaske des Netzes hinter dem Intranator ein, im Beispiel `192.168.1.0 / 255.255.255.0`.

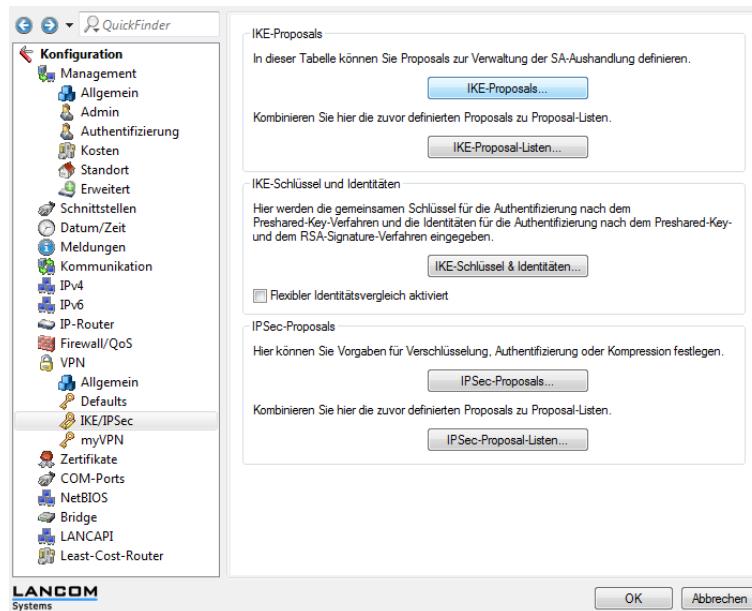


13. Der Lancom-Router kann alle IPs des eigenen Netzes per NAT auf eine einzige Adresse umschreiben. Dies kann unter Umständen helfen, wenn auf beiden Seiten derselbe Netzbereich verwendet wird. Lassen Sie diese Funktion im Zweifel deaktiviert.



14. Deaktivieren Sie auf jeden Fall die NetBIOS-Option. Sie basiert auf einem proprietärem Lancom-Protokoll und verhindert den Verbindungsaufbau. Sie wird normalerweise nicht mehr benötigt, da moderne Windows-Fileserver CIFS über IP verwenden.

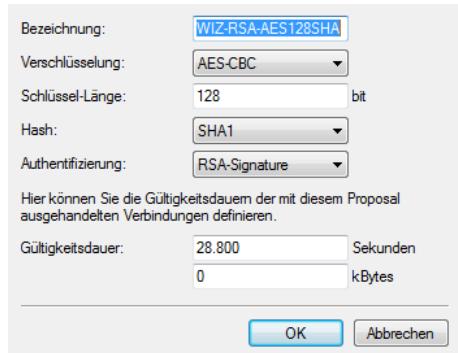
15. Schließen Sie den Assistenten ab und starten die Konfiguration des Routers ohne Assistenten. Wechseln Sie zu den VPN-Einstellungen, Reiter IKE-Param. und klicken auf IKE-Proposals.



16. Bearbeiten Sie das IKE-Proposal mit dem Namen WIZ-RSA-AES128SHA.

Bezeichnung	Verschlüsselung	Schlüssel	Hash	Authentifizierung	Gültigkeitsdauer	Gültigkeitsdauer	OK	Abbrechen
PSK-AES256-SHA	AES-CBC	256 bit	SHA1	Preshared Key	108.000 Sekunden	0 kBytes		
PSK-AES256-MD5	AES-CBC	256 bit	MD5	Preshared Key	108.000 Sekunden	0 kBytes		
PSK-AES-SHA	AES-CBC	128 bit	SHA1	Preshared Key	108.000 Sekunden	0 kBytes		
PSK-AES-MD5	AES-CBC	128 bit	MD5	Preshared Key	108.000 Sekunden	0 kBytes		
PSK-BLOW-SHA	BLOWFISH-CBC	128 bit	SHA1	Preshared Key	108.000 Sekunden	0 kBytes		
PSK-BLOW-MD5	BLOWFISH-CBC	128 bit	MD5	Preshared Key	108.000 Sekunden	0 kBytes		
PSK-CAST-SHA	CAST128-CBC	128 bit	SHA1	Preshared Key	108.000 Sekunden	0 kBytes		
PSK-CAST-MD5	CAST128-CBC	128 bit	MD5	Preshared Key	108.000 Sekunden	0 kBytes		
PSK-3DES-SHA	3DES-CBC	168 bit	SHA1	Preshared Key	108.000 Sekunden	0 kBytes		
PSK-3DES-MD5	3DES-CBC	168 bit	MD5	Preshared Key	108.000 Sekunden	0 kBytes		
PSK-DES-SHA	DES-CBC	56 bit	SHA1	Preshared Key	108.000 Sekunden	0 kBytes		
PSK-DES-MD5	DES-CBC	56 bit	MD5	Preshared Key	108.000 Sekunden	0 kBytes		
RSA-AES256-SHA	AES-CBC	256 bit	SHA1	RSA-Signature	108.000 Sekunden	0 kBytes		
RSA-AES256-MD5	AES-CBC	256 bit	MD5	RSA-Signature	108.000 Sekunden	0 kBytes		
RSA-AES-SHA	AES-CBC	128 bit	SHA1	RSA-Signature	108.000 Sekunden	0 kBytes		
RSA-AES-MD5	AES-CBC	128 bit	MD5	RSA-Signature	108.000 Sekunden	0 kBytes		
RSA-BLOW-SHA	BLOWFISH-CBC	128 bit	SHA1	RSA-Signature	108.000 Sekunden	0 kBytes		
RSA-BLOW-MD5	BLOWFISH-CBC	128 bit	MD5	RSA-Signature	108.000 Sekunden	0 kBytes		
RSA-CAST-SHA	CAST128-CBC	128 bit	SHA1	RSA-Signature	108.000 Sekunden	0 kBytes		
RSA-CAST-MD5	CAST128-CBC	128 bit	MD5	RSA-Signature	108.000 Sekunden	0 kBytes		
RSA-3DES-SHA	3DES-CBC	168 bit	SHA1	RSA-Signature	108.000 Sekunden	0 kBytes		
RSA-3DES-MD5	3DES-CBC	168 bit	MD5	RSA-Signature	108.000 Sekunden	0 kBytes		
RSA-DES-SHA	DES-CBC	56 bit	SHA1	RSA-Signature	108.000 Sekunden	0 kBytes		
RSA-DES-MD5	DES-CBC	56 bit	MD5	RSA-Signature	108.000 Sekunden	0 kBytes		
WIZ-RSA-AES256SHA	AES-CBC	256 bit	SHA1	RSA-Signature	28.800 Sekunden	0 kBytes		
WIZ-RSA-AES128SHA	AES-CBC	128 bit	SHA1	RSA-Signature	28.800 Sekunden	0 kBytes		
WIZ-RSA-AES128MD5	AES-CBC	128 bit	MD5	RSA-Signature	108.000 Sekunden	0 kBytes		
WIZ-RSA-BLOW-SHA	BLOWFISH-CBC	128 bit	SHA1	RSA-Signature	108.000 Sekunden	0 kBytes		
WIZ-RSA-BLOW-MD5	BLOWFISH-CBC	128 bit	MD5	RSA-Signature	108.000 Sekunden	0 kBytes		
WIZ-RSA-3DES-SHA	3DES-CBC	168 bit	SHA1	RSA-Signature	108.000 Sekunden	0 kBytes		
WIZ-RSA-3DES-MD5	3DES-CBC	168 bit	MD5	RSA-Signature	108.000 Sekunden	0 kBytes		

17. Tragen Sie bei Gültigkeitsdauer einen Wert kleiner als 86400 ein, da dies der Maximalwert ist, den der Intranator akzeptiert. Es empfiehlt sich, hier 28800 zu verwenden. Denn das entspricht der Standard-Lebensdauer für IKE/Phase 1 von 480 Minuten im Intranator.



52.5. Intranator

Auf dem Intranator muss die Verbindung auch entsprechend konfiguriert werden. Für VPN-Router wird dies im 49. Kapitel, „Anbinden von kompletten Netzen“ beschrieben.

52.6. Zertifikate löschen

VPN-Verbindungen können aus dem Lancom-Router über die Konfigurations-Oberfläche wieder gelöscht werden falls sie nicht mehr benötigt werden. Zertifikate können nicht über die Oberfläche gelöscht werden.

Die eine Möglichkeit ist die Konfiguration zu sichern, den Router komplett zu resetten und die Konfiguration dann wieder zurückzuspielen. Dann sind allerdings alle Zertifikate gelöscht.

Die andere Möglichkeit geht über die Kommandozeile per Telnet oder SSH. Wechseln Sie in das Zertifikatsverzeichnis mit `cd /status/File-System/Contents`. Lassen Sie sich nun den Inhalt des Verzeichnisses mit dem Befehl `ls` anzeigen. Es werden Ihnen verschiedene Zertifikate angezeigt, wie z.B. `vpn_rootcert vpn_pkcs12`. Sie können über den Befehl `del vpn_rootcert` z.B. das Zertifikat der Gegenstelle löschen.

53. Kapitel - VPN mit Linux

53.1. Überblick

Um eine VPN-Verbindung mit einer Linux-Gegenstelle aufzubauen, benötigen Sie eines der beiden Programm Pakete openswan oder strongswan. Bei den meisten aktuellen Distributionen sollte eines der Pakete bereits installiert oder über den Paketmanager auswählbar sein. Wie Sie prüfen, ob eines der Pakete installiert ist und falls nötig nachinstallieren können, sollte in der Dokumentation Ihrer Distribution erklärt sein.

53.2. Zertifikate erzeugen

1. Öffnen Sie ein Terminal / Kommandozeile und loggen sich als Benutzer root ein. Dafür wird normalerweise der Befehl `su` verwendet.

2. Geben Sie folgenden Befehl in einer Zeile ein:

```
openssl req -x509 -newkey rsa:2048 -days 730 -new -nodes -outform PEM -keyform PEM -keyout /etc/ipsec.d/private_key.pem -out /etc/ipsec.d/cert.pem
```

3. Das Schlüsselpaar wird berechnet und Sie werden nach den Zertifikatsdaten gefragt. Die eingegebenen Werte sind für die Funktion nicht relevant, sie müssen nur auf allen per VPN verbundenen Systemen eindeutig sein. Wir empfehlen, keine Umlaute zu verwenden.

```
Generating a 2048 bit RSA private key
-----
.....+++++
writing new private key to 'private_key.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:DE
State or Province Name (full name) [Berkshire]:BW
Locality Name (eg, city) [Newbury]:Tuebingen
Organization Name (eg, company) [My Company Ltd]:Intra2net
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:MeinRechnerName
Email Address []:
```

4. Das Zertifikat ist jetzt für 2 Jahre (730 Tage) gültig und liegt in der Datei `/etc/ipsec.d/cert.pem`. Der private Schlüssel ist in der Datei `/etc/ipsec.d/private_key.pem`. Sie können die Gültigkeitsdauer über den Parameter `-days` auf der Kommandozeile verändern.
5. Lassen Sie sich die Datei `/etc/ipsec.d/cert.pem` anzeigen, übernehmen sie in die Zwischenablage und importieren sie auf den Intranator unter System > Schlüssel > Fremde Schlüssel.
6. Öffnen Sie im Intranator das Menü System > Schlüssel > Eigene Schlüssel : Daten. Wählen Sie das gewünschte Zertifikat aus und exportieren es über den Menüpunkt

Zertifikat exportieren in eine Datei. Speichern Sie diese auf dem Linuxrechner z.B. nach /etc/ipsec.d/intranator.pem.

53.3. Verbindungen konfigurieren

1. Lassen Sie sich den Inhalt der Datei /etc/ipsec.conf ausgeben. Sie sollten hier die Zeile include /etc/ipsec.d/*.conf finden. Sie darf nicht mit dem Zeichen # beginnen, denn ansonsten wäre sie auskommentiert.
2. Lassen Sie sich den Inhalt der Datei /etc/ipsec.secrets ausgeben. Sie sollten hier die Zeile include /etc/ipsec.d/*.secrets finden. Auch sie darf nicht mit dem Zeichen # beginnen.
3. Wählen Sie einen Namen für die Verbindung. Er sollte keine Sonderzeichen oder Leerzeichen enthalten. In diesem Beispiel wird dafür **intranator** verwendet.
4. Legen Sie eine Datei mit dem Namen /etc/ipsec.d/intranator.conf (bzw. Ihrem Verbindungsnamen) an und öffnen sie in einem Texteditor (z.B. nano oder vi).
5. Die Konfigurationsdatei beginnt mit der Zeile conn **intranator** (bzw. Ihrem Verbindungsnamen). Wichtig ist, dass alle folgenden Zeilen mit Leerzeichen oder Tabulator eingerückt sein müssen. Leerzeilen sind nicht erlaubt, es muss mindestens das (eingerückte) Zeichen # für einen Kommentar in einer Zeile enthalten sein.
6. Geben Sie die Daten für die Verbindung analog zu folgendem Beispiel ein:

```
conn intranator
    auto=start
    keyingtries=0
    type=tunnel
    auth=esp
    authby=rsasig
    ike=aes128-sha-modp1024!
    esp=aes128-sha1!
    pfss=yes
    ikelifetime=480m
    keylife=60m
    rekey=yes
    #
    # left: our side
    left=%defaultroute
    leftid="/C=DE/S=BW/L=Tuebingen/O=Intra2net/CN=MeinRechnerName"
    leftrsasigkey=%cert
    leftcert=/etc/ipsec.d/cert.pem
    leftsubnet=192.168.10.0/24
    leftfirewall=yes
    #
    # right: intranator side
    right=meinintranator.dyndns.org
    rightid="/CN=intranator.net.lan"
    rightrsasigkey=%cert
    rightcert=/etc/ipsec.d/intranator.pem
    rightsubnet=192.168.1.0/24
```

Die Bedeutung der Einträge wird im Folgenden kurz erklärt. Die mit `left` beginnenden Einträge stehen für die lokale Seite, die mit `right` beginnenden für die Gegenseite (hier den Intranator). Alle Einträge die nicht extra erklärt werden, übernehmen Sie wie dargestellt.

auto	Bei add wird die Verbindung nur geladen, bei start automatisch aufgebaut.
keyingtries	Wie oft versucht werden soll, die Verbindung aufzubauen bis wegen einem Fehler abgebrochen wird. 0 steht für endlos.
ike	Verschlüsselungsalgorithmus für Phase 1. Die verwendete Kombination muss im Verschlüsselungsprofil des Intranators vorkommen.
esp	Verschlüsselungsalgorithmus für Phase 2. Die verwendete Kombination muss im Verschlüsselungsprofil des Intranators vorkommen.
pfs	Aktiviert/Deaktiviert Perfect Forward Secrecy
ikelifetime	Lebensdauer für Phase 1 (IKE)
keylife	Lebensdauer für Phase 2 (IPSec)
left/right	IP-Adresse oder DNS-Name. Für die lokale Seite %defaultroute . Wenn eine feste IP vorhanden ist, geben Sie immer die IP ein und nicht einen auch noch verfügbaren DNS-Namen.
leftid/rightid	IPSec-Id der entsprechenden Seite in Anführungszeichen. Geben Sie hier die Inhaberdaten der Zertifikate so ein, wie Sie im Intranator in den Schlüssel-Menüs angezeigt werden.
leftcert/rightcert	Dateinamen des Zertifikats der entsprechenden Seite
leftsubnet/rightsubnet	Netz mit Netzmaske hinter der entsprechenden Seite. Soll auf Seite des Linux-Rechners (left) nur die eine, auch extern verwendete IP per VPN verbunden werden, lassen Sie den Parameter leftsubnet weg und stellen im Intranator das Netz auf Gegenseite auf Externe IP.
leftfirewall	Versucht bei yes automatisch die lokale Firewall für die VPN-Verbindung zu öffnen. Dies funktioniert nur, wenn die Firewall nicht zu stark angepasst wurde.

7. Legen Sie eine Datei mit dem Namen `/etc/ipsec.d/intranator.secrets` (bzw. Ihrem Verbindungsnamen) an und öffnen sie in einem Texteditor (z.B. nano oder vi).
8. Die Datei muss auf den Dateinamen des privaten Schlüssels verweisen:

```
: RSA /etc/ipsec.d/private_key.pem
```
9. In den meisten Fällen müssen Sie dem IPSec-Dienst mitteilen, dass er neu starten soll um Konfigurationsdateien neu einzulesen. Dies wird normalerweise über den Befehl `/etc/init.d/ipsec restart` erreicht.
10. Haben Sie Ihre Verbindung auf automatisch starten gestellt, wird sie jetzt bereits im Hintergrund aufgebaut. Wenn Sie sie manuell starten möchten, können Sie dies mit `ipsec auto --up intranator` (bzw. Ihrem Verbindungsnamen) tun.

Protokolle des Verbindungsaufbaus finden Sie mit der Dienstkennung `pluto` in einer der Logdateien des Systems, bei aktuellen Distributionen meistens `/var/log/secure`.

53.4. Intranator

Auf dem Intranator muss die Verbindung auch entsprechend konfiguriert werden. Für VPN-Router wird dies im 49. Kapitel, „Anbinden von kompletten Netzen“ beschrieben.

54. Kapitel - Lösen von IP-Adresskonflikten in VPNs durch NAT

54.1. Das Problem

Alle IP-Kommunikation beruht darauf, dass IP-Adressen eindeutig vergeben sind und keine zwei Rechner oder Netze dieselben IPs verwenden. Da bei IPv4 aber die Adressen knapp sind, werden in lokalen Netzen normalerweise speziell dafür vorgesehene Adressen aus den Bereichen 192.168.0.0/16, 172.16.0.0/12 und 10.0.0.0/8 verwendet. Da jeder sich aus diesen Bereichen frei seine Adressen auswählt, kann es leicht zu Konflikten kommen.

Sollen jetzt zwei Netze mit den gleichen oder überlappenden IPs per VPN verbunden werden, sind die IPs nicht mehr eindeutig und das VPN wird nicht funktionieren.

Um dies zu lösen bietet der Intranator die Möglichkeit, IPs an Ein- und Ausgang vom VPN umzuschreiben (Network Address Translation, NAT). Dadurch ist die Gegenseite immer über einen anderen Netzbereich erreichbar. Die Adressierung ist wieder eindeutig und der Konflikt aufgelöst.

54.2. Konfiguration

Für jede VPN-Verbindung können im Menü Dienste > VPN > Verbindungen, Reiter Tunnel individuelle Einstellungen für die Adressumschreibung festgelegt werden.

Lokale IPs umschreiben	<p>Das lokale Netz dieses Intranators wird für die Gegenseite auf einen anderen IP-Bereich umgeschrieben. Das hier gewählte Netz wird als lokales Netz dieses Intranators an die Gegenseite übermittelt. Es muss daher auf der Gegenseite als Netz hinter dem Intranator eingetragen werden.</p> <p>Bei der Option auf freie IP wird das gesamte gewählte lokale Netz aus Sicht der Gegenseite zu einer einzigen IP zusammengefasst. Daher können Verbindungen innerhalb des VPNs nur vom lokalen Netz aus initiiert werden, nicht von der Gegenseite aus.</p> <p>Bei der Option 1:1 auf freies Netz wird das gewählte lokale Netz aus Sicht der Gegenseite auf das eingestellte Netz umgeschrieben. Das 1:1-NAT bedeutet, dass die 1. IP des realen Netzes zur ersten des NAT-Netzes umgeschrieben wird, die 2. zur 2. usw.</p>
Gegenseiten-IPs 1:1 auf Netz umschreiben	Wenn aktiv, ist das Netz der Gegenseite unter dem hier angegebenen Netz (Netzmaske siehe Netz auf Gegenseite) erreichbar. Diese Umschreibung gilt nur für das lokale Netz des Intranators und ist von der Gegenseite aus nicht erkennbar. Der Gegenseite wird beim Verbindungsauftbau ausschließlich das unter Netz auf Gegenseite eingestellte Netz übermittelt.
Gegenseiten-IPs bei Internetzugriff umschreiben	Siehe Abschnitt 40.2.4, „Tunnel konfigurieren“

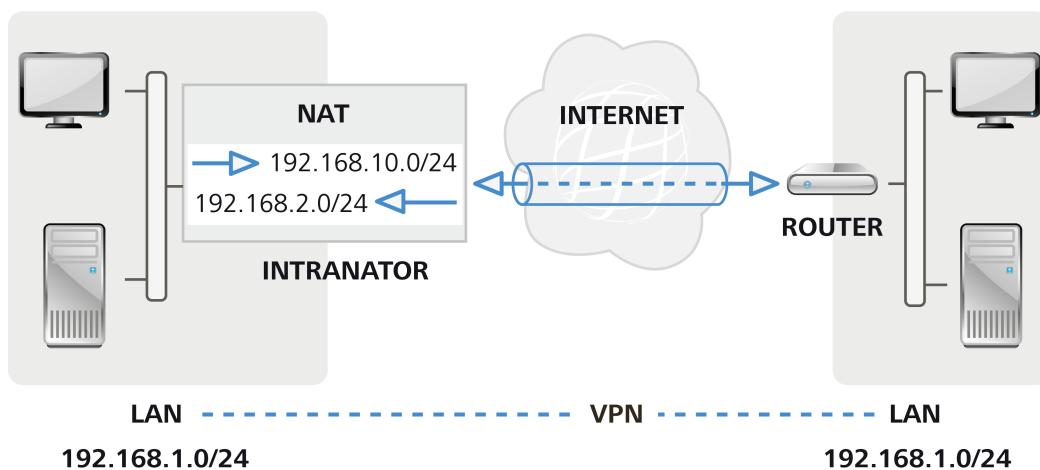
54.3. Gleiche IPs in LAN und auf der Gegenseite

Das lokale Netz des Intranators und der Gegenseite verwenden einen identischen oder zumindest überlappenden Netzbereich. In diesem Beispiel ist dies 192.168.1.0/24.

Um den Adresskonflikt zu lösen, wird das lokale Netz der Gegenseite auf 192.168.10.0/24 umgeschrieben. Möchte ein Rechner aus dem LAN des Intranators also die Gegenseite erreichen, muss er die entsprechende IP im Netz 192.168.10.0/24 ansprechen anstatt 192.168.1.0/24 zu verwenden.

Gleichzeitig ist das LAN des Intranators für die Gegenseite unter 192.168.2.0/24 zu erreichen.

Beide Adressumschreibungen finden auf dem Intranator statt, die Gegenseite bekommt davon nichts mit. Wird auf beiden Seiten des VPNs ein Intranator verwendet, darf die Adressumschreibung nur auf einer Seite eingestellt werden.



54.3.1. Umsetzung

The screenshot shows the Intranator Business Server administration interface. The left sidebar navigation includes: Hauptseite, Benutzermanager, Netzwerk, Dienste (Email, Emailfilter, Proxy, Fax, DynDNS), VPN, Verbindungen (selected), Verschlüsselung, Einstellungen, Zeitabgleich, Überwachung, System (Information, Webmail), and Abmelden [admin]. The main content area is titled 'Dienste > VPN > Verbindungen'. A sub-tab 'Tunnel' is selected. The configuration pane shows:

- Lokales Netz:** Lokale Netze 192.168.1.0 / 255.255.255.0
- Netz auf Gegenseite (an Gegenstelle übermittelt):** Freies Netz (IP: 192.168.1.1, Netzm: 255.255.255.0)
- Adressumschreibung (NAT):**
 - Lokale IPs umschreiben (an Gegenstelle übermittelt): 1:1 auf freies Netz (IP: 192.168.1.2, Netzm: 0)
 - Gegenseiten-IPs 1:1 auf Netz umschreiben (checkbox checked): 192.168.1.10 (Netzm: 0)
 - Gegenseiten-IPs bei Internetzugriff umschreiben (NAT) (checkbox unchecked):

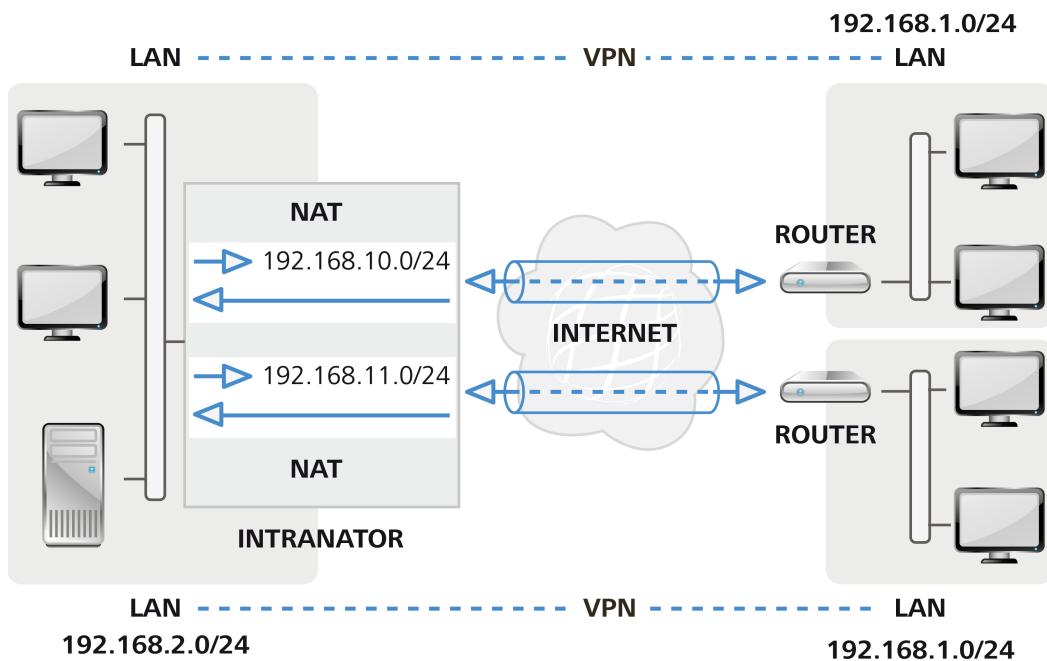
A 'Einstellungen speichern' button is at the bottom right.

54.4. Mehrere Gegenstellen mit gleichen IPs

Von einem Intranator aus sollen gleichzeitig VPNs zu mehreren Gegenstellen aufgebaut werden. Beispielsweise für Fernwartung von unterschiedlichen Kunden oder Standorten. Mehrere dieser Gegenstellen verwenden das gleiche IP-Netz, in diesem Beispiel 192.168.1.0/24.

Wenn sich das LAN des Intranators nicht mit einem Netz der Gegenseiten überschneidet, ist es nicht notwendig, die lokalen IPs des Intranators umzuschreiben.

Bei jeder VPN-Verbindung zu einer der Gegenstellen wird das Netz der Gegenseite auf ein anderes Netz (im Beispiel 192.168.10.0/24 und 192.168.11.0/24) umgeschrieben. Dadurch ist jedes dieser Gegenseiten durch eindeutige IPs ansprechbar.



54.4.1. Umsetzung

Intranator Business Server **Intra2net**

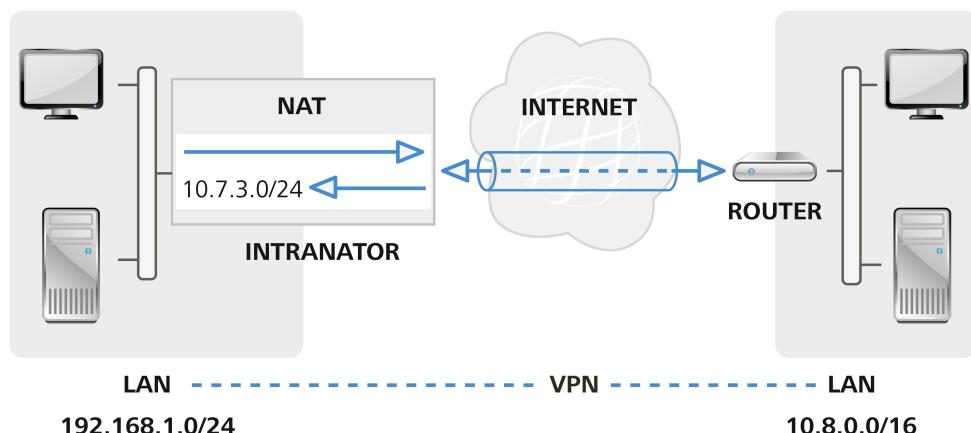
Dienste > VPN > Verbindungen

Hauptseite	Verbindung	Einstellungen	Authentifizierung	Tunnel	Rechte	Aktivierung	?
<ul style="list-style-type: none"> Benutzermanager Netzwerk Dienste <ul style="list-style-type: none"> Email Emailfilter Proxy Fax DynDNS VPN Verbindungen Verschlüsselung Einstellungen Zeitabgleich Überwachung System Information Webmail 	<p>Kunde A Kunde B</p> <p><input type="button" value="Neu"/> <input type="button" value="Löschen"/> <input type="button" value="Anzeigen"/></p>	<p>Lokales Netz</p> <p><input checked="" type="radio"/> Lokale Netze [192.168.2.0 / 255.255.255.0]</p> <p><input type="radio"/> Freies Netz [] . [] . [] . [] Netzmaske [] . [] . [] . []</p> <p><input type="radio"/> Alles (0.0.0.0/0.0.0.0)</p> <p>Netz auf Gegenseite (an Gegenstelle übermittelt)</p> <p><input checked="" type="radio"/> Freies Netz [192] . [168] . [1] . [0] Netzmaske [255] . [255] . [255] . [0]</p> <p><input type="radio"/> IP zuweisen (mode-config) [] . [] . [] . []</p>	<p>Adressumschreibung (NAT)</p> <p>Lokale IPs umschreiben (an Gegenstelle übermittelt)</p> <p><input checked="" type="radio"/> unverändert</p> <p><input type="radio"/> auf freie IP [] . [] . [] . []</p> <p><input type="radio"/> 1:1 auf freies Netz [] . [] . [] . []</p> <p>Gegenseiten-IPs 1:1 auf Netz umschreiben</p> <p><input checked="" type="checkbox"/> 192 . 168 . 10 . 0</p> <p>Gegenseiten-IPs bei Internetzugriff umschreiben (NAT)</p> <p><input type="checkbox"/></p>	<input type="button" value="Einstellungen speichern"/>			

54.5. Lokale IPs festgelegt durch Fernwartungs-Dienstleister

Ein Dienstleister soll bestimmte Systeme im LAN fernwarten können. Dafür wird ein VPN zwischen dem Netz des Dienstleisters (im Beispiel 10.8.0.0/16) und dem LAN aufgebaut. Damit es beim Dienstleister nicht zu Konflikten kommt, gibt der Dienstleister für das LAN einen bestimmten Netzbereich vor, hier 10.7.3.0/24.

Das lokale Netz ist aber bereits auf ein anderes Netz konfiguriert, im Beispiel 192.168.1.0/24. Damit das lokale Netz nicht komplett umgestellt werden muss, wird das lokale Netz für diese eine VPN-Verbindung auf die vorgegebenen IPs umgeschrieben.



54.5.1. Umsetzung

Das Bild zeigt den Benutzeroberfläche der Intranator Business Server Software. Die linke Seite zeigt ein Navigationsmenü mit Optionen wie Hauptseite, Benutzermanager, Netzwerk, Dienste, Email, Emailfilter, Proxy, Fax, DynDNS, VPN, Verbindungen (markiert), Verschlüsselung, Einstellungen, Zeitabgleich, Überwachung, System, Information und Webmail. Oben rechts befindet sich das Logo 'Intra2net'. Der zentrale Bereich zeigt die 'Verbindungen' Konfigurationsseite. Es sind verschiedene Registerkarten wie 'Einstellungen', 'Authentifizierung', 'Tunnel' (markiert), 'Rechte', 'Aktivierung' und '?' zu sehen. Die 'Tunnel' Registerkarte zeigt die Konfiguration für eine 'Filiale'. Es gibt zwei Hauptgruppen von Einstellungen:

- Lokales Netz:** Ein Radio-Button ist auf 'Lokale Netze 192.168.1.0 / 255.255.255.0' gesetzt. Weitere Optionen umfassen 'Freies Netz' (mit IP- und Netzmaskeneingaben), 'Alles (0.0.0.0/0.0.0.0)' und 'Externe IP' (mit IP- und Netzmaskeneingaben).
- Netz auf Gegenseite (an Gegenstelle übermittelt):** Ein Radio-Button ist auf 'Freies Netz' gesetzt, mit den Werten 10 . 8 . 0 . 0 und einer Netzmarske von 255 . 255 . 0 . 0. Weitere Optionen umfassen 'IP zuweisen (mode-config)' (mit IP- und Netzmaskeneingaben) und 'IP zuweisen' (mit IP- und Netzmaskeneingaben).

Unter diesen Gruppen befindet sich ein Abschnitt 'Adressumschreibung (NAT)'. Hier sind drei Optionen definiert:

- Lokale IPs umschreiben (an Gegenstelle übermittelt):** Ein Radio-Button ist auf '1:1 auf freies Netz' gesetzt, mit den Werten 10 . 7 . 3 . 0.
- Gegenseiten-IPs 1:1 auf Netz umschreiben:** Ein Kästchen ist unmarkiert.
- Gegenseiten-IPs bei Internetzugriff umschreiben (NAT):** Ein Kästchen ist unmarkiert.

Am unteren Rand befindet sich ein Button 'Einstellungen speichern'.

55. Kapitel - Fehlerdiagnose

55.1. Logs lesen

Leider ist uns keine IPSec-Implementation bekannt, die leicht verständliche Fehlermeldungen an den Benutzer ausgibt. Sobald daher ein Fehler in einer VPN-Verbindung auftritt, muss man die Logdateien analysieren und daraus auf den Fehler schließen. In vielen Fällen wird der tatsächliche Fehler nur auf der einen Seite der Verbindung protokolliert, die andere Seite bekommt nur eine etwas allgemeine Fehlermeldung wie z.B. „INVALID_ID“ mit. Daher ist es häufig nötig, die Logdateien beider Seiten zu analysieren.

Im Intranator sind die Protokolldaten der IPSec-Verbindungen in der messages-Logdatei zu finden (Menü „Information > System > Logdateien“) und sind nach Datum und Zeit mit „pluto“ gekennzeichnet. Wo die Logdateien in anderen Geräten zu finden sind, sollte im Handbuch dokumentiert sein. Häufig muss die Protokollierung von IPSec-Ereignissen auch erst aktiviert werden, bevor tatsächlich Daten gesammelt werden.

Der erste Schritt bei der Analyse eines Fehlers ist, festzustellen, in welcher Phase der Verbindung der Fehler auftritt.

55.2. Das Protokollformat des Intranators

Ein Beispiel für eine Zeile aus einer Intranator-Logdatei:

```
Nov 5 10:54:40 intranator pluto[2332]: "C2"[1] 192.168.1.200 #1:  
      responding to Main Mode from unknown peer 192.168.1.200
```

Nov 5 10:54:40	Datum und Uhrzeit des Ereignisses
intranator	Rechnername des Intranators
pluto[2332]	Kennung und Prozess-ID des IPSec-Dienstes
C2	Kennung der Verbindung; ist am Anfang nicht unbedingt korrekt, wird immer genauer, je mehr Daten der Intranator bekommt. Liste der Verbindungskennungen unter „Information > System > VPN“
192.168.1.200	IP der Gegenstelle. Wird nur angezeigt bei Verbindungstyp „Dynamische IP“
responding to ...	Nachricht

55.3. Fehler in Phase 1

Fehler in Phase 1 bedeuten meistens eine falsche Konfiguration der Authentifizierung (z.B. falsche Zertifikate konfiguriert oder eine andere IPSec-ID verwendet) oder in seltenen Fällen auch falsch konfigurierte Verschlüsselungsalgorithmen.

Am Anfang jeder Verbindung tauschen die Gegenstellen typischerweise Informationen über ihre Fähigkeiten aus und erkennen, ob die Verbindung durch NAT läuft:

```
packet from 192.168.1.200: received Vendor ID payload [draft-ietf-  
    ipsec-nat-t-ike-00]  
packet from 192.168.1.200: received Vendor ID payload [draft-ietf-  
    ipsec-nat-t-ike-02_n]  
responding to Main Mode from unknown peer 192.168.1.200  
ignoring Vendor ID payload [47bbe7c993f1fc13b4e6d0db565c68e50102010...]
```

```
ignoring Vendor ID payload [da8e937880010000]
received Vendor ID payload [Dead Peer Detection]
received Vendor ID payload [XAUTH]
NAT-Traversal: Result using draft-ietf-ipsec-nat-t-ike-02/03: no NAT detected
ignoring informational payload, type IPSEC_REPLAY_STATUS
ignoring informational payload, type IPSEC_INITIAL_CONTACT
```

Danach sendet derjenige, der die Verbindung initiiert, sein Zertifikat:

```
Peer ID is ID_DER_ASN1_DN: 'CN=client1'
```

Das System überprüft, ob das Zertifikat über Zertifizierungsstellen vertrauenswürdig ist. Da der Intranator diese Funktion nicht verwendet, schlägt das immer fehl:

```
issuer cacert not found
X.509 certificate rejected
```

Als nächstes wird geprüft, ob das Zertifikat bekannt ist. In diesem Beispiel schlägt das fehl, da ein anderes Zertifikat konfiguriert ist:

```
no RSA public key known for 'CN=client1'
```

Der Intranator sendet daher eine kurze Fehlerinformation an die Gegenstelle:

```
sending encrypted notification INVALID_KEY_INFORMATION to 192.168.1.200:500
```

Baut der Intranator hingegen von sich aus die Verbindung auf, bekommen wir bei dem selben Fehler nur wesentlich weniger Informationen:

```
we have a cert and are sending it
ignoring informational payload, type INVALID_CERTIFICATE
```

In diesem Fall sollte das Log der Gegenstelle genauer untersucht werden, hier sind dann meistens detailliertere Informationen zu finden.

Möchte die Gegenstelle die Verbindung mit einem nicht erlaubten Verschlüsselungsalgorithmus aufbauen (in diesem Beispiel einfaches DES), wird folgendes Protokolliert:

```
OAKLEY_DES_CBC is not supported. Attribute OAKLEY_ENCRYPTION_ALGORITHM
```

Die Gegenstelle kann mehrere Algorithmen vorschlagen. Ist kein akzeptabler dabei, protokolliert der Intranator dies und sendet der Gegenstelle eine entsprechende Meldung:

```
no acceptable Oakley Transform
sending notification NO_PROPOSAL_CHOSEN to 192.168.1.200:500
```

In diesem Fall muss das Verschlüsselungsprofil auf dem Intranator oder der Gegenseite so angepasst werden, dass mindestens eine Algorithmenkombination auf beiden Seiten zulässig ist.

Ist dagegen alles korrekt konfiguriert, wird die Phase 1 erfolgreich abgeschlossen:

```
sent MR3, ISAKMP SA established
```

55.4. Fehler in Phase 2

In Phase 2 werden die Daten für die IP-Tunnel ausgehandelt. Tritt hier ein Fehler auf, so sind meistens falsche IP-Adressen für den Tunnel hinterlegt. Allerdings kann es auch hier nicht passende Verschlüsselungsalgorithmen geben.

Nicht passende IP-Adressen werden wie folgt protokolliert:

```
cannot respond to IPsec SA request because no connection is known for  
192.168.2.0/24==192.168.1.254[CN=intranator-vpn]...192.168.1.200[CN=client1]
```

192.168.2.0/24	Netz hinter dem Intranator mit dem die Gegenseite die Verbindung aufbauen möchte
192.168.1.254	IP des Intranators die die Verbindung entgegengenommen hat
[CN=intranator-vpn]	IPSec-ID des Intranators
192.168.1.200	IP der Gegenstelle
[CN=client1]	IPSec-ID der Gegenstelle

In diesem Fall wurde beim Client vergessen, die virtuelle IP zu konfigurieren. Das kann man daran erkennen, dass hinter der IP des Clients kein Netz mehr angegeben ist. Daher möchte der Client eine Verbindung mit seiner realen IP statt mit der virtuellen aufbauen (was häufig wegen NAT fehlschlägt).

Ein Verbindungsversuch mit einer falschen virtuellen IP (hier 192.168.2.78) sähe dagegen so aus:

```
cannot respond to IPsec SA request because no connection is known for  
192.168.2.0/24==192.168.1.254[CN=intranator-vpn]...  
192.168.1.200[CN=client1]==192.168.2.78/32
```

Möchte die Gegenstelle eine Verbindung ohne PFS (Perfect Forward Secrecy) aufbauen, auf dem Intranator ist es aber aktiviert, sieht das in den Logs so aus:

```
we require PFS but Quick I1 SA specifies no GROUP_DESCRIPTION  
sending encrypted notification NO_PROPOSAL_CHOSEN to 192.168.1.200:500
```

Auch in Phase 2 müssen die Verschlüsselungsalgorithmen zusammenpassen. Tun sie dies nicht (im Beispiel möchte der Client mit einfacherem DES verschlüsseln), sieht dies wie folgt aus:

```
IPSec Transform [ESP_DES (64), AUTH_ALGORITHM_HMAC_SHA1] refused due  
to insecure key_len and enc. alg. not listed in "esp" string  
no acceptable Proposal in IPsec SA  
sending encrypted notification NO_PROPOSAL_CHOSEN to 192.168.1.200:500
```

Ein erfolgreicher Verbindungsauflauf wird dagegen so protokolliert:

```
IPsec SA established
```

Teil 7. Anhang

Anhang A. Lizenzen

A.1. Intranator Software Lizenzvertrag

Version 1.2 vom 17.07.2007

Dieser Lizenzvertrag räumt ein nicht ausschließliches Nutzungsrecht an dem von der Intra2net AG entwickelten "Intranator System Manager" unter den nachfolgenden Lizenzbedingungen ein. Mit der Installation der Software erklären Sie sich mit folgenden Lizenzbedingungen einverstanden.

§ 1 Vertragsgegenstand

1) Die "Intranator Software" besteht aus dem "Intranator System Manager", der "Linux Open-Source Distribution" sowie dem VirensScanner. Gegenstand dieses Lizenzvertrages ist - vorbehaltlich der Regelung in § 2 dieses Vertrags - nur der "Intranator System Manager". Die "Linux Open-Source Distribution" und der VirensScanner unterliegen eigenen Lizenzbedingungen, die den entsprechenden RPM-Paketen beigelegt sind.

2) Der "Intranator System Manager" besteht aus komprimierten Dateien zzgl. Installationsprogramm (RPM-Paket), die den lauffähigen Code der von der Intra2net AG programmisierten Software enthalten. Der "Intranator System Manager" wird nicht als Open-Source Software vertrieben. Das Copyright und alle Rechte verbleiben bei der Intra2net AG. Die Bestandteile des "Intranator System Manager" sind in den RPM-Paketen entsprechend gekennzeichnet.

§ 2 andere Lizenzen

1) Zusammen mit dem "Intranator System Manager" erhalten Sie sowohl einen VirensScanner, als auch eine Programmkopie einer "Linux Open-Source Distribution". Die Intra2net AG überlässt Ihnen die Programmkopie der "Linux Open-Source Distribution" unentgeltlich, weshalb sich eine Haftung der Intra2net AG nach §§ 521 ff. BGB richtet und folglich auf Vorsatz oder grobe Fahrlässigkeit beschränkt ist.

2) Die für eine Benutzung der "Linux Open-Source Distribution" zwingend erforderlichen urheberrechtlichen Nutzungsrechte an der Distribution, bekommen Sie nicht von der Intra2net AG eingeräumt, sondern direkt von den jeweiligen Autoren der entsprechenden Programmteile. Der Umfang Ihrer Nutzungsrechte bestimmt sich folglich ausschließlich nach den der "Linux Open-Source Distribution" beigelegten Lizenzbedingungen und nicht nach diesem Vertrag.

3) Die Lizenzbedingungen, die den Open-Source Programmpaketen von den jeweiligen Autoren zugeordneten wurden, sind vom Nutzer bei der Nutzung der gesamten "Intranator Software", neben den Vorschriften dieses Lizenzvertrages, im Rahmen eines direkten Nutzungsvertrages mit den jeweiligen Softwareherstellern ohne Zwischenschaltung der Intra2net AG zu beachten. Die entsprechenden Lizenzbedingungen sind in elektronischer Form der zugehörigen Software beigelegt.

4) Soweit Quelltexte der unentgeltlich überlassenen "Linux Open-Source Distribution" der GNU General Public License (GPL) oder der GNU Lesser General Public License (LGPL) unterliegen, bietet Ihnen die Intra2net AG (Intra2net AG, Möpelparder Weg 8, 72072 Tübingen, Deutschland) hiermit an, diese Quelltexte gegen einen Selbstkostenersatz von

10,- EUR zzgl. MwSt. und Porto auf CD an Sie zu liefern. Dieses Angebot gilt für 3 Jahre ab Auslieferung der Software durch Intra2net.

5) Soweit innerhalb der überlassenen Programme Libraries genutzt werden, die unter der LGPL lizenziert sind, werden diese entweder als shared libraries verwendet, oder Sie können - entsprechend der hierfür vorgesehenen Regelungen in der LGPL - die jeweiligen Quellen zu den in 4) genannten Konditionen anfordern.

§ 3 Installation

1) Die "Intranator Software" läuft nicht parallel mit anderen Betriebssystemen auf einem System. Insbesondere formatiert die "Intranator Software" bei Installation die gesamte Festplatte und löscht alle bestehenden Daten.

2) Die "Intranator Software" arbeitet nur mit dafür vom Lizenzgeber freigegebenen Hardwarekomponenten zusammen. Diese sind in der Dokumentation sowie auf der Webseite www.intranator.com aufgeführt und werden regelmäßig aktualisiert. Der Lizenzgeber hat das Recht, die Freigabe für Hardwarekomponenten für zukünftige Versionen zurückzuziehen, z.B. wenn diese von zukünftigen Basissystemen nicht mehr mit Gerätetreibern unterstützt werden. Alle beim Lizenzgeber registrierten Kunden werden per E-Mail mindestens 3 Monate vorher darüber in Kenntnis gesetzt (Abkündigung).

§ 4 Vervielfältigungsrechte und Zugriffsschutz

1) Der Lizenznehmer darf einen nicht modifizierten Originaldatenträger beliebig vervielfältigen. Lizenzcodes und Lizenzdateien dürfen nicht vervielfältigt werden.

2) Eine Vervielfältigung der installierten Programme und Daten ist nur gestattet, soweit die jeweilige Vervielfältigung für die Benutzung des Programms notwendig ist. Zu den notwendigen Vervielfältigungen zählen die Installation des Programms vom Originaldatenträger auf den Massenspeicher der eingesetzten Hardware sowie das Laden des Programms in den Arbeitsspeicher.

3) Ist aus Gründen der Datensicherheit oder der Sicherstellung einer schnellen Reaktivierung des Computersystems nach einem Totalausfall die turnusmäßige Sicherung des gesamten Datenbestands einschließlich der eingesetzten Computerprogramme unerlässlich, darf der Lizenznehmer Sicherungskopien in der zwingend erforderlichen Anzahl herstellen. Die betreffenden Datenträger sind entsprechend zu kennzeichnen. Die Sicherungskopien dürfen nur zu rein archivarischen Zwecken verwendet werden.

4) Der Lizenznehmer ist verpflichtet, den unbefugten Zugriff Dritter auf die installierten Programme und Daten durch geeignete Vorkehrungen zu verhindern. Die gelieferten Lizenzcodes sind an einem gegen den unberechtigten Zugriff Dritter gesicherten Ort aufzubewahren.

5) Die Mitarbeiter des Lizenznehmers sind nachdrücklich auf die Einhaltung der vorliegenden Vertragsbedingungen sowie der Bestimmungen des Urheberrechts hinzuweisen.

6) Der Lizenzgeber ist berechtigt, Lizenzcodes bei Verdacht auf Verstoß gegen diese Lizenz zu sperren, nachdem der rechtmäßige Eigentümer gegen Vorlage des Kaufbelegs kostenfrei einen neuen Lizenzcode ausgestellt bekommen hat oder innerhalb von 2 Wochen nach entsprechender Information kein Kaufbeleg vorgelegt wird.

§ 5 Nutzungsbeschränkungen

- 1) Der Lizenznehmer darf die Software auf einer ihm zur Verfügung stehenden Hardware einsetzen. Wechselt der Lizenznehmer jedoch die Hardware, muss er die Software von der bisher verwendeten Hardware löschen.
- 2) Ein zeitgleiches Einspeichern, Vorrätighalten oder Benutzen ist nur in der Zahl der im Lizenzschein angegebenen Anzahl von Instanzen zulässig. Möchte der Lizenznehmer die Software in mehr Instanzen zeitgleich einsetzen, muss er eine entsprechende Anzahl von weiteren Lizizenzen erwerben.
- 3) Der Lizenznehmer muss eine zeitgleiche Mehrfachnutzung über die Anzahl der erworbenen Lizizenzen hinaus durch Zugriffsschutzmechanismen unterbinden.
- 4) Handelt es sich um eine Lizenz mit einer Beschränkung der Benutzeranzahl, darf das System nur von der entsprechenden Anzahl an Benutzern genutzt werden.
- 5) Die Anzahl der Benutzer errechnet sich aus der Summe der Anzahlen von den im Menüpunkt "Benutzermanager" angelegten Benutzer, den Benutzerkonten auf Zielservern, die für durch das System weitergeleitete E-Mails genutzt werden, sowie den Benutzern, die nicht im Benutzermanager angelegt sind, aber die Möglichkeit haben, den Proxy-Server des Systems zu nutzen.

§ 6 Begleitende Dienstleistungen

- 1) Wurde mit der Lizenz das Recht auf zeitlich beschränkte Dienstleistungen (z.B. Update-Service) erworben, so beginnt deren Laufzeit mit Eingabe des Lizenzcodes, Registrieren der Software oder der Prüfung auf vorhandene Updates.
- 2) Wird das Recht auf diese Dienstleistungen verlängert, so beginnt die Laufzeit der Verlängerung rückwirkend zum letzten Ablauftermin.

§ 7 Evaluationslizenz

- 1) Wurde von einem Endkunden keine Lizenz käuflich erworben, erhält er eine Evaluationslizenz, d.h. für 30 Tage das Recht, die "Intranator Software" auf einer Hardware zu installieren und zu Testzwecken unter diesen Lizenzbedingungen zu nutzen. Mit der Eingabe eines nicht selbst erworbenen Lizenzkeys erlischt die Evaluationslizenz sofort.
- 2) Die Evaluationslizenz oder eine andere, zeitlich beschränkte Lizenz darf nur für den entsprechenden Zeitraum ab Installation genutzt werden. Die verbleibende Zeit wird auf der Bedienungsoberfläche der Software angezeigt.
- 3) Nach Ablauf dieses Zeitraums stellt die Software die Funktion ein. Der Kunde ist dafür verantwortlich, seine Daten rechtzeitig vorher zu sichern.
- 4) Eine Evaluationslizenz berechtigt nicht zu Gewährleistungsansprüchen, außer wenn etwaige Mängel durch die Intra2net AG vorsätzlich oder grob fahrlässig verursacht wurden.

§ 8 Dekompilierung und Programmänderungen

- 1) Die Rückübersetzung des überlassenen Programmcodes in andere Codeformen (Dekompilierung) sowie sonstige Arten der Rückerschließung der verschiedenen Herstellungsstufen der Software (Reverse-Engineering) einschließlich einer Programmänderung sind nur in den nachfolgend genannten Fällen zulässig.

2) Die Zustimmung des Rechtsinhabers ist nicht erforderlich, wenn die Vervielfältigung des Codes oder die Übersetzung der Codeform unerlässlich ist, um entweder a) die Bedingungen der LGPL zu erfüllen oder b) die erforderlichen Informationen zur Herstellung der Interoperabilität eines unabhängig geschaffenen Computerprogramms mit anderen Programmen zu erhalten, sofern folgende Bedingungen erfüllt sind:

1. Die Handlungen werden von dem Lizenznehmer oder von einer anderen zur Verwendung eines Vervielfältigungsstücks des Programms berechtigten Person oder in deren Namen von einer hierzu ermächtigten Person vorgenommen;
2. die für die Herstellung der Interoperabilität notwendigen Informationen sind für die in Nummer 1 genannten Personen noch nicht ohne weiteres zugänglich gemacht;
3. die Handlungen beschränken sich auf die Teile des ursprünglichen Programms, die zur Herstellung der Interoperabilität notwendig sind.

Bei unter a) und b) genannten derartigen Handlungen gewonnene Informationen dürfen nicht

1. zu anderen Zwecken als zur Herstellung der Interoperabilität des unabhängig geschaffenen Programms verwendet werden,
 2. an Dritte weitergegeben werden, es sei denn, dass dies für die Interoperabilität des unabhängig geschaffenen Programms notwendig ist,
 3. für die Entwicklung, Herstellung oder Vermarktung eines Programms mit im Wesentlichen ähnlicher Ausdrucksform oder für irgendwelche anderen das Urheberrecht verletzenden Handlungen verwendet werden.
- 3) Urhebervermerke, Lizenzcodes, Seriennummern sowie sonstige der Programmidentifikation dienende Merkmale dürfen auf keinen Fall entfernt oder verändert werden.
- 4) Wird auf dem System Software installiert, die nicht ausdrücklich vom Lizenzgeber dafür freigegeben ist, oder wird die installierte Software modifiziert, können Gewährleistungs- oder Garantieansprüche nur geltend gemacht werden, wenn der Kunde nachweisen kann, dass die Mängel nicht mit den Modifikationen in Zusammenhang stehen.

§ 9 Weiterveräußerung und Weitervermietung

- 1) Der Lizenznehmer darf die Software einschließlich des Benutzerhandbuchs und des sonstigen Begleitmaterials auf Dauer an Dritte veräußern oder verschenken, vorausgesetzt der erwerbende Dritte erklärt sich mit der Weitergeltung der vorliegenden Vertragsbedingungen auch ihm gegenüber einverstanden. Im Falle der Weitergabe muss der Lizenznehmer dem neuen Lizenznehmer sämtliche Programmkopien einschließlich gegebenenfalls vorhandener Sicherheitskopien übergeben oder die nicht übergebenen Kopien vernichten. Infolge der Weitergabe erlischt das Recht des alten Lizenznehmers zur Programmnutzung.
- 2) Der Lizenznehmer darf die Software einschließlich des Begleitmaterials Dritten nicht vermieten.
- 3) Der Lizenznehmer darf die Software Dritten nicht überlassen, wenn der begründete Verdacht besteht, der Dritte werde die Vertragsbedingungen verletzen, insbesondere unerlaubte Vervielfältigungen herstellen. Dies gilt auch im Hinblick auf Mitarbeiter des Lizenznehmers.

§ 10 Gewährleistung

- 1) Mängel der von der Intra2net AG programmierten Software einschließlich zugehöriger Unterlagen werden vom Lizenzgeber innerhalb der Gewährleistungsfrist von 24 Monaten gegenüber Verbrauchern bzw. 12 Monaten gegenüber Unternehmen ab Lieferung nach entsprechender Mitteilung durch den Lizenznehmer behoben. Dies geschieht nach Wahl des Lizenzgebers durch Nachbesserung oder Ersatzlieferung.
- 2) Bei einem zweimaligen Fehlschlagen der Nachbesserung oder Ersatzlieferung kann der Lizenznehmer Wandelung oder Minderung geltend machen.

§ 11 Haftung

- 1) Für Schäden wegen Rechtsmängeln und Beschaffenheitsgarantien haftet der Lizenzgeber unbeschränkt. Die Haftung für anfängliches Unvermögen wird auf das Fünffache des Überlassungsentgelts sowie auf solche Schäden begrenzt, mit deren Entstehung im Rahmen einer Softwareüberlassung typischerweise gerechnet werden muss.
- 2) Im Übrigen haftet der Lizenzgeber unbeschränkt nur für Vorsatz und grobe Fahrlässigkeit auch seiner gesetzlichen Vertreter und Erfüllungsgehilfen.
- 3) Für leichte Fahrlässigkeit haftet der Lizenzgeber nur, sofern eine Pflicht verletzt wird, deren Einhaltung für die Erreichung des Vertragszwecks von besonderer Bedeutung ist (Kardinalpflicht). Bei Verletzung einer Kardinalpflicht ist die Haftungsbeschränkung für anfängliches Unvermögen nach Abs. 1 dieser Haftungsreglung entsprechend heranzuziehen.
- 4) Die Haftung für Datenverlust wird auf den typischen Wiederherstellungsaufwand beschränkt, der bei regelmäßiger und gefahrenentsprechender Anfertigung von Sicherungskopien eingetreten wäre.
- 5) Die vorstehenden Regelungen gelten auch zugunsten der Mitarbeiter des Lizenzgebers.
- 6) Die Haftung nach dem Produkthaftungsgesetz bleibt unberührt (§ 14 ProdHG).
- 7) Für Mängel zusätzlich installierter Software wird eine Haftung nur bei Lieferung und Installation durch die Intra2net AG übernommen. Auch dann ist diese Haftung auf Vorsatz oder grobe Fahrlässigkeit des Lizenzgebers gemäß § 521 BGB beschränkt.

§ 12 Untersuchungs- und Rügepflicht

- 1) Der Lizenznehmer wird die gelieferte Software einschließlich der Dokumentation innerhalb von 8 Werktagen nach Lieferung untersuchen, insbesondere im Hinblick auf die Vollständigkeit der Datenträger und Handbücher sowie der Funktionsfähigkeit grundlegender Programmfunctionen. Mängel, die hierbei festgestellt werden oder feststellbar sind, müssen dem Lizenzgeber innerhalb weiterer 8 Werktagen gemeldet werden. Die Mängelrüge muss eine nach Kräften zu detaillierende Beschreibung der Mängel beinhalten.
- 2) Mängel, die im Rahmen der beschriebenen ordnungsgemäßen Untersuchung nicht feststellbar sind, müssen innerhalb von 8 Werktagen nach Entdeckung unter Einhaltung der dargelegten Rügeanforderungen gerügt werden.
- 3) Bei einer Verletzung der Untersuchungs- und Rügepflicht gilt die Software in Ansehung des betreffenden Mangels als genehmigt.

§ 13 Rücknahmepflicht nach dem ElektroG

Der Kunde übernimmt die Pflicht, die gelieferte Ware nach Nutzungsbeendigung auf eigene Kosten nach den gesetzlichen Vorschriften ordnungsgemäß zu entsorgen. Insbesondere stellt der Kunde die Intra2net AG von den Verpflichtungen nach § 10 Abs. 2 ElektroG (Rücknahmepflicht der Hersteller) und damit im Zusammenhang stehenden Ansprüchen Dritter frei.

§ 14 Schriftform

Sämtliche Vereinbarungen, die eine Änderung, Ergänzung oder Konkretisierung dieser Vertragsbedingungen beinhalten, sowie besondere Zusicherungen und Abmachungen sind schriftlich niederzulegen. Werden sie von Vertretern oder Hilfspersonen des Lizenzgebers erklärt, sind sie nur dann verbindlich, wenn der Lizenzgeber hierfür seine schriftliche Zustimmung erteilt.

§ 15 Rechtswahl

Die Parteien vereinbaren im Hinblick auf sämtliche Rechtsbeziehungen aus diesem Vertragsverhältnis die Anwendung des Rechts der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts.

§ 16 Gerichtsstand

Sofern der Lizenznehmer Vollkaufmann im Sinne des Handelsgesetzbuchs, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist, wird für sämtliche Streitigkeiten, die im Rahmen der Abwicklung dieses Vertragsverhältnisses entstehen, Tübingen als Gerichtsstand vereinbart.

§ 17 Schlussbestimmungen

Sollten einzelne Bestimmungen nichtig, unwirksam oder anfechtbar sein oder werden, sind sie so auszulegen bzw. zu ergänzen, dass der beabsichtigte wirtschaftliche Zweck in rechtlich zulässiger Weise möglichst genau erreicht wird; die übrigen Bestimmungen bleiben davon unberührt. Sinngemäß gilt dies auch für ergänzungsbedürftige Lücken.

A.2. Lizenzierte Software

Die Bestandteile der Linux Open-Source Distribution unterliegen eigenen Lizenzen. Einige dieser Lizenzen sind die GNU General Public License (GPL) und GNU Lesser General Public License (LGPL) in verschiedenen Versionen. Diese sind unter folgenden URLs einsehbar:

GPL v2	http://www.gnu.org/licenses/gpl-2.0.html
GPL v3	http://www.gnu.org/licenses/gpl-3.0.html
LGPL v2.1	http://www.gnu.org/licenses/lgpl-2.1.html
LGPL v3	http://www.gnu.org/licenses/lgpl-3.0.html

Some parts of this product includes software from the following copyright owners:

Copyright (c) 1988-1997 Sam Leffler Copyright; (c) 1991-1997 Silicon Graphics, Inc. HylaFAX is a trademark of Silicon Graphics, Inc.; Copyright 1990 Massachusetts Institute of Technology; Copyright (C) 1995,1996,1997 Lars Fenneberg; Copyright (c) 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006 Inferno Nettverk A/S, Norway; Copyright

(C) 2002 Roaring Penguin Software Inc.; Copyright 1991 by the Massachusetts Institute of Technology; Copyright 1992 Livingston Enterprises, Inc.; Copyright 1992, 1993, 1994 Henry Spencer; Copyright 1996 Willem van Schaik, Singapore (willem@schaik.com); Copyright 1999-2000 Greg Roelofs (newt@pobox.com); Original Code Copyright (C) 1994, Jeff Hostetler, Spyglass, Inc.; Portions of Content-MD5 code Copyright (C) 1993, 1994 by Carnegie Mellon University; Portions of Content-MD5 code Copyright (C) 1991 Bell Communications; Research, Inc. (Bellcore); Portions extracted from mpack, John G. Myers – jgm+@cmu.edu; Content-MD5 Code contributed by Martin Hamilton (martin@net.lut.ac.uk) these portions extracted from mpack, John G. Myers – jgm+@cmu.edu; (C) Copyright 1993, 1994 by Carnegie Mellon University; (c) Copyright 1989 Sun Microsystems, Inc. Sun design patents pending in the U.S. and foreign countries. OPEN LOOK is a trademark of AT&T. Used by written permission of the owners; (c) Copyright Bigelow & Holmes 1986, 1985.

This product includes software developed by:

Tim Hudson (tjh@cryptsoft.com); Computing Services at Carnegie Mellon University (<http://www.cmu.edu/computing/>); Paul Mackerras paulus@samba.org; Pedro Roque Marques pedro_m@yahoo.com; the Apache Software Foundation (<http://www.apache.org/>); the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>); by the University of California, Berkeley and its contributors; by Tommi Komulainen Tommi.Komulainen@iki.fi; Ian F. Darwin, 1987; the Regents of the University of Michigan and Merit Network, Inc.

This product includes:

"perl-Encode-Detect", which is licensed under the Mozilla Public License. The Source Code is available under the terms of this License at <http://search.cpan.org/~jgmyers/Encode-Detect/>; cryptographic software written by Eric Young (eay@cryptsoft.com); RSA Data Security, Inc. MD4 Message Digest Algorithm; RSA Data Security, Inc. MD5 Message Digest Algorithm and is based in part of the work of the FreeType Team and the Independent JPEG Group.

cryptographic software written by Eric Young (eay@cryptsoft.com); PHP software, freely available from <http://www.php.net/software/>; RSA Data Security, Inc. MD5 Message Digest Algorithm: software developed by: Inferno Nettverk A/S, Norway; Paul Mackerras paulus@samba.org; the Computer Systems Engineering Group at Lawrence Berkeley Laboratory and its contributors; the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>); the University of California, Berkeley and its contributors; Todd C. Miller.

Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England.

Anhang B. Lizenz

B.1. Intra2net Groupware Client Lizenzvertrag (EULA)

Version 1.1 vom 22.12.2014

Dieser Lizenzvertrag räumt ein nicht ausschließliches Nutzungsrecht an dem von der Intra2net AG entwickelten Groupware Client unter den nachfolgenden Lizenzbedingungen ein. Mit der Installation der Software erklären Sie sich mit folgenden Lizenzbedingungen einverstanden.

§ 1 Vertragsgegenstand

1) Vertragsgegenstand ist der „Intra2net Groupware Client“, welcher eine MAPI-Storage-Provider Applikation enthält. Diese Applikation ist nur zusammen mit Microsoft Outlook lauffähig.

2) Die Intra2net AG räumt dem Lizenznehmer das nicht ausschließliche Nutzungsrecht an oben genannten und entgeltlich erworbenen „Intra2net Groupware Client“ auf Dauer und nur nach Maßgabe der nachfolgenden Bestimmungen ein. Die Software ist urheberrechtlich geschützt (§§ 69a ff. UrhG).

§ 2 Vervielfältigungsrechte

1) Es wird eine Lizenz für eine bestimmte Benutzeranzahl an eine natürliche oder juristische Person ausgestellt. Diese Lizenz ist Bestandteil der Lizenz des „Intra2net Business Server“ oder der „Intra2net Enterprise Edition“ und gilt für die dort ausgewiesene Benutzeranzahl.

2) Ein zeitgleiches Einspeichern, Vorrätighalten oder Benutzen ist nur in der Zahl der im Lizenzzertifikat angegebenen Anzahl von Gesamtbenutzern zulässig. Möchte der Lizenznehmer die Software mit weiteren Benutzern einsetzen, muss er eine entsprechende Anzahl von weiteren Lizizenzen erwerben.

3) Der Lizenznehmer muss eine Mehrfachnutzung über die Anzahl der erworbenen maximalen Benutzeranzahl hinaus unterbinden. Die Funktionalität kann beim Überschreiten dieser Benutzerzahl für die überzählig angemeldeten Benutzer eingeschränkt werden.

§ 3 Begleitende Dienstleistungen

1) Wurde mit der Lizenz das Recht auf zeitlich beschränkte Dienstleistungen (z.B. Update-Service) erworben, so ist die Laufzeit an die Lizenz des „Intra2net Business Server“ oder der „Intra2net Enterprise Edition“ gebunden.

§ 4 Evaluationslizenzen

1) Wurde von einem Endkunden keine Lizenz käuflich erworben, erhält er ein Evaluationsrecht für 30 Tage, das ihn berechtigt die Software zu installieren und zu Testzwecken in nicht produktionskritischen Umgebungen unter diesen Lizenzbedingungen zu nutzen. Mit der Eingabe einer nicht selbst erworbenen Lizenz erlischt die Evaluationslizenz sofort.

2) Die Evaluationslizenz oder eine andere, zeitlich beschränkte Lizenz darf nur für den entsprechenden Zeitraum ab Installation genutzt werden und ist nur mit schriftlicher Zustimmung von der Intra2net AG verlängerbar. Die verbleibende Zeit wird auf der Bedienungsoberfläche der Software angezeigt.

3) Nach Ablauf dieses Zeitraums stellt die Software die Funktion ein. Der Kunde ist dafür verantwortlich, seine Daten rechtzeitig vorher zu sichern.

4) Eine Evaluationslizenz berechtigt nicht zu Gewährleistungsansprüchen, außer wenn durch uns Vorsatz oder grobe Fahrlässigkeit zu vertreten ist.

§ 5 Dekompilierung und Programmänderungen

1) Die Rückübersetzung des überlassenen Programmcodes in andere Codeformen (Dekompilierung) sowie sonstige Arten der Rückerschließung der verschiedenen Herstellungsstufen der Software (Reverse-Engineering) einschließlich einer Programmänderung sind nur in den nachfolgend genannten Fällen zulässig.

2) Die Zustimmung des Rechtsinhabers ist nicht erforderlich, wenn die Vervielfältigung des Codes oder die Übersetzung der Codeform unerlässlich ist, um entweder a) die Bedingungen der LGPL zu erfüllen oder b) die erforderlichen Informationen zur Herstellung der Interoperabilität eines unabhängig geschaffenen Computerprogramms mit anderen Programmen zu erhalten, sofern folgende Bedingungen erfüllt sind:

1. Die Handlungen werden von dem Lizenznehmer oder von einer anderen zur Verwendung eines Vervielfältigungsstücks des Programms berechtigten Person oder in deren Namen von einer hierzu ermächtigten Person vorgenommen;
2. die für die Herstellung der Interoperabilität notwendigen Informationen sind für die in Nummer 1 genannten Personen noch nicht ohne weiteres zugänglich gemacht;
3. die Handlungen beschränken sich auf die Teile des ursprünglichen Programms, die zur Herstellung der Interoperabilität notwendig sind.

Bei unter a) und b) genannten derartigen Handlungen gewonnene Informationen dürfen nicht

1. zu anderen Zwecken als zur Herstellung der Interoperabilität des unabhängig geschaffenen Programms verwendet werden,
2. an Dritte weitergegeben werden, es sei denn, dass dies für die Interoperabilität des unabhängig geschaffenen Programms notwendig ist,
3. für die Entwicklung, Herstellung oder Vermarktung eines Programms mit im Wesentlichen ähnlicher Ausdrucksform oder für irgendwelche anderen das Urheberrecht verletzenden Handlungen verwendet werden.

3) Urhebervermerke, Lizenzcodes, Seriennummern sowie sonstige der Programmidentifikation dienende Merkmale dürfen auf keinen Fall entfernt oder verändert werden.

4) Wird der "Intra2net Groupware Client" modifiziert, können Gewährleistungs- oder Garantieansprüche nur geltend gemacht werden, wenn der Kunde nachweisen kann, dass die Mängel nicht mit den Modifikationen in Zusammenhang stehen.

§ 6 Weiterveräußerung und Weitervermietung

1) Der Lizenznehmer darf die Software einschließlich des Benutzerhandbuchs und des sonstigen Begleitmaterials auf Dauer an Dritte veräußern oder verschenken, vorausgesetzt der erwerbende Dritte erklärt sich mit der Weitergeltung der vorliegenden Vertragsbedingungen auch ihm gegenüber einverstanden. Im Falle der Weitergabe muss der Lizenzneh-

mer dem neuen Lizenznehmer sämtliche Programmkopien einschließlich gegebenenfalls vorhandener Sicherheitskopien übergeben oder die nicht übergebenen Kopien vernichten. Infolge der Weitergabe erlischt das Recht des alten Lizenznehmers zur Programmnutzung.

2) Der Lizenznehmer darf die Software einschließlich des Begleitmaterials Dritten nicht vermieten.

3) Der Lizenznehmer darf die Software Dritten nicht überlassen, wenn der begründete Verdacht besteht, der Dritte werde die Vertragsbedingungen verletzen, insbesondere unerlaubte Vervielfältigungen herstellen. Dies gilt auch im Hinblick auf Mitarbeiter des Lizenznehmers.

§ 7 Gewährleistung

1) Mängel der von der Intra2net AG programmierten Software einschließlich zugehöriger Unterlagen werden vom Lizenzgeber innerhalb der Gewährleistungsfrist von 24 Monaten gegenüber Verbrauchern bzw. 12 Monaten gegenüber Unternehmen ab Lieferung nach entsprechender Mitteilung durch den Lizenznehmer behoben. Dies geschieht nach Wahl des Lizenzgebers durch Nachbesserung oder Ersatzlieferung.

2) Bei einem zweimaligen Fehlenschlagen der Nachbesserung oder Ersatzlieferung kann der Lizenznehmer Wandelung oder Minderung geltend machen.

§ 8 Haftung

1) Für Schäden wegen Rechtsmängeln und Beschaffenheitsgarantien haftet der Lizenzgeber unbeschränkt. Die Haftung für anfängliches Unvermögen wird auf das Fünffache des Überlassungsentgelts sowie auf solche Schäden begrenzt, mit deren Entstehung im Rahmen einer Softwareüberlassung typischerweise gerechnet werden muss.

2) Im Übrigen haftet der Lizenzgeber unbeschränkt nur für Vorsatz und grobe Fahrlässigkeit auch seiner gesetzlichen Vertreter und Erfüllungsgehilfen.

3) Für leichte Fahrlässigkeit haftet der Lizenzgeber nur, sofern eine Pflicht verletzt wird, deren Einhaltung für die Erreichung des Vertragszwecks von besonderer Bedeutung ist (Kardinalpflicht). Bei Verletzung einer Kardinalpflicht ist die Haftungsbeschränkung für anfängliches Unvermögen nach Abs. 1 dieser Haftungsreglung entsprechend heranzuziehen.

4) Die Haftung für Datenverlust wird auf den typischen Wiederherstellungsaufwand beschränkt, der bei regelmäßiger und gefahrenentsprechender Anfertigung von Sicherungskopien eingetreten wäre.

5) Die vorstehenden Regelungen gelten auch zugunsten der Mitarbeiter des Lizenzgebers.

6) Die Haftung nach dem Produkthaftungsgesetz bleibt unberührt (§ 14 ProdHG).

7) Für Mängel zusätzlich installierter Software wird eine Haftung nur bei Lieferung und Installation durch die Intra2net AG übernommen. Auch dann ist diese Haftung auf Vorsatz oder grobe Fahrlässigkeit des Lizenzgebers gemäß § 521 BGB beschränkt.

8) Es wird keine Haftung für die Kompatibilität der Software mit nicht explizit von der Intra2net AG dafür freigegebenen Versionen des Betriebssystems, von Microsoft Outlook und von der Grundversion abweichenden Konfigurationen von Microsoft Outlook über-

nommen. Dies gilt insbesondere bei der Verwendung weiterer Outlook-Plugins und -Addins.

§ 9 Untersuchungs- und Rügepflicht

1) Der Lizenznehmer wird die gelieferte Software einschließlich der Dokumentation innerhalb von acht Werktagen nach Lieferung untersuchen, insbesondere im Hinblick auf die Vollständigkeit der Datenträger und Handbücher sowie der Funktionsfähigkeit grundlegender Programmfunctionen. Mängel, die hierbei festgestellt werden oder feststellbar sind, müssen dem Lizenzgeber innerhalb weiterer acht Werktagen gemeldet werden. Die Mängelrüge muss eine nach Kräften zu detaillierende Beschreibung der Mängel beinhalten.

2) Mängel, die im Rahmen der beschriebenen ordnungsgemäßen Untersuchung nicht feststellbar sind, müssen innerhalb von acht Werktagen nach Entdeckung unter Einhaltung der dargelegten Rügeanforderungen gerügt werden.

3) Bei einer Verletzung der Untersuchungs- und Rügepflicht gilt die Software in Ansehung des betreffenden Mangels als genehmigt.

§ 10 Schriftform

Sämtliche Vereinbarungen, die eine Änderung, Ergänzung oder Konkretisierung dieser Vertragsbedingungen beinhalten, sowie besondere Zusicherungen und Abmachungen sind schriftlich niederzulegen. Werden sie von Vertretern oder Hilfspersonen des Lizenzgebers erklärt, sind sie nur dann verbindlich, wenn der Lizenzgeber hierfür seine schriftliche Zustimmung erteilt.

§ 11 Rechtswahl

Die Parteien vereinbaren im Hinblick auf sämtliche Rechtsbeziehungen aus diesem Vertragsverhältnis die Anwendung des Rechts der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts.

§ 12 Gerichtsstand

Sofern der Lizenznehmer Vollkaufmann im Sinne des Handelsgesetzbuchs, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist, wird für sämtliche Streitigkeiten, die im Rahmen der Abwicklung dieses Vertragsverhältnisses entstehen, Tübingen als Gerichtsstand vereinbart.

§ 13 Schlussbestimmungen

Sollten einzelne Bestimmungen nichtig, unwirksam oder anfechtbar sein oder werden, sind sie so auszulegen bzw. zu ergänzen, dass der beabsichtigte wirtschaftliche Zweck in rechtlich zulässiger Weise möglichst genau erreicht wird; die übrigen Bestimmungen bleiben davon unberührt. Sinngemäß gilt dies auch für ergänzungsbedürftige Lücken.

Index

A

Abgesicherter Modus, 6-7
ACPI, 6-7
Active Directory
 Empfängeradressprüfung, 78-80
 Softwareverteilung, 108-109
 Zertifikate verteilen, 48-49
ADSL, 51-52
Android
 VPN Client, 310-320
Anti-Virus
 E-Mail, 87
 Proxy, 63
APIC, 6-7
Appliance
 Eco, 8
 Pro, 8
 Ultimate, 8-9
ARP
 Proxy, 55-56
Auslieferungszustand
 Zurücksetzen in, 32
Ausschalten
 zeitgesteuert, 104
Ausweichen
 auf anderen Provider, 57

B

Backup
 Auslagern, 102
 Erstellen, 101-102
 Rücksichern, 102
 von anderer Version, 102
BADMAC, 251
Benutzer
 Gruppe, 67
 Import und Export, 69
 Rechte, 67-68
Bereich, 41
BIOS
 Einstellungen, 4-5
 zeitgesteuertes Einschalten, 104

C

Catch-All-Konto, 73-76
Certificate Authority (CA), 49, 262-263

D

Daten, bestehende importieren, 152-157

Datenschutz
 Statistik, 66
De-Militarized Zone (DMZ), 53-56
Demomodus, 34
DHCP, 40-41
 Pool, 41
DNS, 39-40
 Rebind, 40
 Weiterleitung, 39-40
Domain, 39-40
DSL-Modem, 51-52
DynDNS, 58-59

E

E-Mail
 Abwesenheitsschaltung, 81-82
 Adressen, 80-81
 Alias, 80-81
 Anhangfilter, 87-88
 Antivirus, 87
 Archivierung
 MailStore Server, 89-91
 Schnittstelle, 88-89
 Automatischer Transfer, 91
 Empfängeradressprüfung, 77-80
 Active Directory / LDAP, 78-80
 SMTP, 77-78
 Externer Servername (EHLO), 71
 Gelesen-Status, 159-160
 Größe, 92
 IMAP
 auf den Intranator, 71-72
 Kopfzeilen, 181
 Mailinglisten, 91-92
 POP3
 Abruf und Weiterleiten, 80
 Abruf von Provider, 72-74
 auf den Intranator, 71-72
 Postmaster
 Adresse, 92
 Quelltext, 181
 SMTP
 Authentifizierung, 68
 Empfang, 73-75
 Weiterleitung, 76-80
 Sortierung, 82
 Spamfilter
 Benutzerabhängig, 85
 Erkennung, 82-83
 Glaubwürdige Server, 85-87
 Global, 83-85
 Punktwerte, 83

- Quarantäne, 84-85
- SMTP, 82
- Spamverdacht, 83
- Versand
 - Client, 70
 - Direkt, 71
 - Relay-Berechtigung, 68
 - Relayserver, 70-71
 - SMTP-Submission, 70
 - Verteiler, 91-92
 - Warteschlange, 92
 - Weiterleitung
 - Domain, 76-80
 - E-Mails eines Benutzers, 81
 - POP-Konten, 80
 - E-Mail-Ordner (IMAP)
 - abonnieren, 146-147
 - freigeben, 158-159
 - Synchronisationsfrequenz, 167-173
 - E-Mails
 - löschen, 150-152
 - Nachverfolgen, 177
 - Erinnerungen, 179
 - Export
 - Benutzer, 69
 - Rechner, 41
- F**
 - Fallback, 57
 - Fax
 - auf virtueller Maschine, 10
 - Client, 96-98
 - Empfang, 95
 - Versand, 95-98
 - Fernwartung, 59
 - Fernzugriff
 - auf den Intranator, 59
 - Festplattenschaden, 102-103
 - Firewall
 - auf virtueller Maschine, 11-12
 - Automatische Antwortregel, 246
 - Bedingungen, 247
 - Blockieren nach Loginfehlern, 251
 - Dienste, 245
 - in VMware vSphere Hypervisor, 18-21
 - IPs eintragen, 245
 - MACs überprüfen, 251
 - Netzgruppen, 245
 - Notmodus, 32, 251
 - Ports eintragen, 245
 - Regellisten
 - Auswahl, 240-242
- Einfache Profile, 243-244**
- Internet, 240**
- LAN, 240**
- Vollständige, 245-250**
- Routing, 42**
- vor dem Intranator, 103-104**
- Free-/Busy, 173-176**
- Frei-/Gebucht, 173-176**
- Freigeben**
 - von E-Mail-Ordnern (IMAP), 158-159
- Fremde Ordner**
 - Erinnerungen, 179
 - verbinden, 160-162
- G**
 - Gelöschte E-Mails, 150-152**
 - Gesendete Elemente**
 - auf Server ablegen, 147-150
 - Groupware Connector**
 - Migration von, 184-197
 - Groupware-Daten**
 - bestehende importieren, 152-157
- H**
 - Haftung, 1**
 - Hardware**
 - Erkennung, 31
 - kompatibel, 3
 - Tausch oder Defekt, 102-103
 - Hauptseite, 34-36**
 - übers Internet erreichen, 59
 - Herunterfahren**
 - zeitgesteuert, 104
- I**
 - IKE, 260**
 - IMAP**
 - auf den Intranator, 71-72
 - IMAP-Konto einrichten**
 - Outlook 2003, 138-143
 - Outlook 2007, 130-136
 - Outlook 2010, 121-129
 - Outlook 2013, 110-120
 - Speicherort festlegen, 180
 - IMAP-Ordner**
 - abonnieren, 146-147
 - freigeben, 158-159
 - fremde verbinden, 160-162
 - Synchronisationsfrequenz, 167-173
 - Import**
 - Benutzer, 69
 - bestehender Groupwaredaten, 152-157

- Rechner, 41
- I**
- Installation
- auf Microsoft Hyper-V, 23-30
 - auf VMware vSphere Hypervisor, 13-22
 - von CD, 6
- Internet-Tachometer, 35
- IP
- Bereich, 41
 - Konfigurieren, 31, 38
 - offizielle, 53-56
 - private Netzbereiche, 31
- iPhone
- VPN Client, 301-309
- IPSec, 259
- Aggressive Mode, 260
 - Client
 - Android, 310-320
 - iPhone, 301-309
 - MacOS X, 294-300
 - Symbian, 330-337
 - Windows, 269-277, 286-293
 - Windows Mobile, 321-329
 - Client anbinden, 264-268
 - dynamische IP, 338
 - Logs, 376-378
 - Main Mode, 260
 - Mode Config, 266
 - NAT, 371-375
 - Netz-zu-Netz, 338-340
 - Perfect Forward Secrecy (PFS), 260-261
 - Pre-Shared Key, 259
 - Quick Mode, 260
 - Verbindungsphasen, 260
 - Verschlüsselungsalgorithmen, 260-261
 - Virtuelle IP, 266
 - XAUTH, 265-266
 - Zertifikate, 262-263
- IPSecuritas
- VPN Client, 294-300
- ISAKMP, 260
- ISDN
- Einwahl ins Internet, 51
 - Lockruf, 57-58
 - MSN, 95
- K**
- Kabelanschluss, 52
- Kompatibilitätsliste, 3
- Konfiguration
- bei Auslieferung, 2
 - Konflikt, 36
 - Überprüfung, 36
- Zurücksetzen, 32
- Konsole, 31
- Konvertierung
- vom Groupware Connector, 184-197
- L**
- Lancom
- VPN-Verbindungen, 357-366
- LDAP
- Empfängeradressprüfung, 78-80
- Linux
- Shell, 32-33
 - VPN, 367-370
- Lizenz
- Ablauf, 100
 - Code Eingeben, 100
 - Demomodus, 100
 - Groupware Client, 387-390
 - Intranator, 380-385
 - Open Source, 385-386
 - Lizenzcode, 34
 - Lockruf, 57-58
 - Logdateien
 - Proxy, 64
 - System, 104
 - Loginfehler
 - IPs blockieren, 251
- M**
- MAC
- Firewall, 251
 - hinterlegen, 40
- MailStore Server, 89-91
- Migration
- vom Groupware Connector, 184-197
- Mulitdrop, 73-76
- N**
- Nachverfolgen-Funktion, 177
- NAT
- für VPNs, 371-375
 - Masquerading (N:1), 57
 - statisch (1:1), 54-55
 - VPN-Gegenseite, 267
- NCP
- Secure Entry Client für Windows, 269-277
 - Secure Entry Symbian Client, 330-337
 - Secure Entry Windows Mobile Client, 321-329
- Netgear
- ProSafe VPN Client, 286-293
- Netzwerkkarte, 31, 38
- Typ, 31, 38

NTP, 98

O

Openswan, 367-370

Ordner (IMAP)

abonnieren, 146-147

freigeben, 158-159

fremde verbinden, 160-162

Synchronisationsfrequenz, 167-173

Outlook konfigurieren

2003, 136-143

2007, 129-136

2010, 120-129

2013, 109-120

Outlook-Profile

2003, 136-143

2007, 129-136

2010, 120-129

2013, 109-120

P

Passwort

Administrator, 2

root, 32

Perfect Forward Secrecy (PFS)

IPSec, 260-261

SSL/TLS, 50

POP3

Abruf und Weiterleiten, 80

Abruf von Provider, 72-74

auf den Intranator, 71-72

Sammelkonten (Multidrop, Catch-All), 73-76

Postmaster

Adresse, 92

PPPoE, 51

Passthrough, 51

PPTP, 51-52

Pre-Shared Key, 259

Privat-Kennzeichnung, 178-179

Proxy

Antivirus, 63

Port, 60

Profile, 61

Protokollierung, 64

Statistik, 64-65

Transparent, 60-61

URL-Filter, 61-62

Web-Content-Filter, 62

Zeitsteuerung, 62

Zielports, 61

Zugriffslisten, 61-62

Proxy-ARP, 55-56

R

RAID

Hardware, 5

Software, 5-6

Rechner

eintragen, 40

Import und Export, 41

Rechte

Benutzer, 67-68

Netzwerkobjekt, 38-39

Registry, 180, 210-214

root-Passwort, 32

Router, 51-53

Routing

DMZ, 53-56

Internet, 52-53

LAN, 42

S

SafeNet

SoftRemote, 286-293

Servergespeicherte Profile, 180

Shrew Soft

VPN Client für Windows, 278-285

SMTP

Authentifizierung, 68

Empfang, 73-75

Empfängeradressprüfung, 77-78

Versand

Direkt, 71

Relayserver, 70-71

Weiterleitung, 76-80

SNMP, 98-99

Spamfilter

Benutzerabhängig, 85

Erkennung, 82-83

Glaubwürdige Server, 85-87

Global, 83-85

Punktwerte, 83

Quarantäne, 84-85

SMTP, 82

Spamverdacht, 83

SSL

Perfect Forward Secrecy (PFS), 50

Prinzip, 43

Verschlüsselungsverfahren, 50

Zertifikate, 43-44

Standardeinstellungen, 2

Statistik

Datenschutz, 66

Internet, 65-66

Proxy, 64-65

Speicherverbrauch, 66
strongSwan, 367-370
Synchronisationsfrequenz
 E-Mail-Ordner, 170-173
 Groupware-Ordner, 167-169

T

TLS
 Prinzip, 43
 Zertifikate, 43-44

U

Überwachung
 SNMP, 98-99
Update
 Antivirus, 101
 Fernsteuerung über Partnerweb, 101
 Neustart, 101
 Spamfilter, 101
 System, 101
URL-Filter, 61-62

V

VDSL, 51
Verbindungsauflaufbau
 ins Internet, 56
 über Ersatzprovider, 57
Version, 1
Virenscanner
 E-Mail, 87
 Proxy, 63
Virtuelle Maschine, 10-30
VLAN, 51
VMDirectPath, 18-21
VPN, 259
 Adresskonflikt, 371-375
 Client anbinden, 264-268
 dynamische IP, 338
 NAT, 371-375
 Netz-zu-Netz, 338-340

W

Wake-On-LAN, 40
Web-Content-Filter, 62
Weboberfläche
 übers Internet erreichen, 59
Werkseinstellungen, 2

X

X.509
 für IPSec, 262-263
 für SSL/TLS, 43-44

XAUTH, 265-266

Z

Zeitabgleich, 98
Zertifikate
 auf Client installieren, 44-49
 für IPSec, 262-263
 für SSL/TLS, 43-44
 mit Active Directory verteilen, 48-49
Zertifizierungsstelle (CA), 49, 262-263
Zwangstrennung, 56
ZyWALL VPN-Router, 341-352